RECEIVED
MAR 14 2019
Clerk, U.S. District and Bankruptcy Courts

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

MICROSOFT CORPORATION, a Washington corporation, *Plaintiff,* v. JOHN DOES 1-2, CONTROLLING A COMPUTER NETWORK AND THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS, *Defendants.*	Case: 1:19-cv-00716 (JURY-DEMAND) Assigned To : Amy B. Jackson Assign. Date : 3/14/2019 Description: TRO/PI **FILED UNDER SEAL PURSUANT TO LOCAL RULE 5.1**

MICROSOFT'S MOTION FOR PROTECTIVE ORDER TEMPORARILY
<u>SEALING DOCUMENTS</u>

Pursuant to Fed. R. Civ. P. 26(c)(1) and Local Civil Rule 5, Plaintiff Microsoft Corp. ("Microsoft") hereby moves for a protective order temporarily sealing the pleadings associated with the *Ex Parte* Motion For Preliminary Injunction Order, and the following documents in particular, filed by Microsoft in this action:

1. The instant Motion for Protective Order Sealing Documents and accompanying documents, including the Brief in support of this Motion;
2. The declaration of Gabriel M. Ramsey in Support of Motion for Protective Order Sealing Documents;
3. Microsoft's *Ex Parte* Motion For Preliminary Injunction Order and accompanying documents;
4. The Declaration of David Anselmi in Support of Microsoft's *Ex Parte* Motion For Preliminary Injunction Order and attachments thereto;

5. [Proposed] Preliminary Injunction Order and accompanying documents.

Microsoft respectfully requests that these materials be sealed pending execution of the *ex parte* relief sought in Microsoft's Motion For Preliminary Injunction Order, in particular the disabling of the domains set forth in Appendix A to the proposed Preliminary Injunction Order. Microsoft respectfully requests that upon the execution of the portion of the Order disabling the domains in Appendix A to the Preliminary Injunction Order, the foregoing documents be filed in the public docket. Upon execution of that *ex parte* relief, Microsoft will file with the Clerk of the Court a Notice that the Preliminary Injunction Order has been executed. Microsoft further requests that upon execution of the Preliminary Injunction Order, Microsoft be permitted to disclose such materials as it deems necessary to commence its efforts to provide Defendants notice of any further hearings and service of pleadings associated with the instant Motion for Preliminary Injunction Order.

Microsoft respectfully requests that should the Court decide not to grant the *ex parte* temporary relief requested in Microsoft's *Ex Parte* Motion For Preliminary Injunction Order, that the materials be sealed indefinitely.

Dated: March 14, 2019

Respectfully submitted,

/s/ Julia R. Milewski

Julia R. Milewski (D.C. Bar No. 1008678)
Justin D. Kingsolver (D.C. Bar. No. 1033806)
Matthew B. Welling (*pro hac vice* pending)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington DC 20004-2595
Telephone: (202) 624-2500
Fax: (202) 628-5116
jmilewski@crowell.com
jkingsolver@crowell.com
mwelling@crowell.com

Gabriel M. Ramsey (*pro hac vice* pending)
CROWELL & MORING LLP
3 Embarcadero Center, 26th Floor
San Francisco, CA 94111
Telephone: (415) 986-2800
Fax: (415) 986-2827
gramsey@crowell.com

Richard Domingues Boscovich (*pro hac vice* pending)
MICROSOFT CORPORATION
One Microsoft Way
Redmond, WA 98052-6399
Telephone: (425) 704-0867
Fax: (425) 936-7329
rbosco@microsoft.com

Attorneys for Plaintiff Microsoft Corp.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

MICROSOFT CORPORATION, a Washington corporation, *Plaintiff,* v. JOHN DOES 1-2, CONTROLLING A COMPUTER NETWORK AND THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS, *Defendants.*	)	Civil Action No: **FILED UNDER SEAL PURSUANT TO LOCAL RULE 5.1**

BRIEF IN SUPPORT OF MICROSOFT'S MOTION FOR PROTECTIVE ORDER TEMPORARILY SEALING DOCUMENTS

Microsoft submits the following memorandum in support of its Motion for a Protective Order Sealing Documents.

BACKGROUND

Microsoft has filed an Ex Parte Motion for Preliminary Injunction ("Preliminary Injunction Motion") to prevent the activities of John Doe Defendants 1 and 2 (collectively "Defendants") who are engaged in harmful and malicious Internet activities directed at Microsoft, its customers, and the general public. In the Preliminary Injunction Motion, Microsoft seeks ex parte relief to disable the recently registered domains set forth in **Appendix A** to the Complaint. That will cease the irreparable harm resulting from Defendants' conduct. Microsoft seeks relief under seal, with respect to the portion of the Order disabling the domains in **Appendix A** to the Complaint, because advance public disclosure or notice of that requested relief would allow Defendants to evade such relief and

further prosecution of this action, thereby perpetuating the irreparable harm at issue. The reasons for Microsoft's request are set forth in detail in the Preliminary Injunction Motion filed concurrently herewith. Therefore, Microsoft requests that the Ex Parte Motion to Supplement Preliminary Injunction Order and associated pleadings be sealed pending execution of the ex parte relief sought in Microsoft's Preliminary Injunction Order, in particular disabling of the domains set forth in **Appendix A** to the Complaint. Microsoft's requested sealing order is narrowly tailored to impose the least restriction on the public's right of access to information as possible. Microsoft requests that all sealed documents be immediately unsealed upon execution of the portion of the Order disabling the domains set forth in **Appendix A** to the Complaint. As soon as that relief is executed, all papers will be made available on the public docket.

ARGUMENT

The right of access to court records is not absolute. *Nixon v. Warner Commc'ns, Inc.*, 435 U.S. 589, 597-98 (1978). Although both common law and the First Amendment afford the public a qualified right of access to judicial proceedings, *In re Fort Totten Metrorail Cases*, 960 F. Supp. 2d 2, 5 (D.C. Cir. 2013), the D.C. Circuit has expressed doubts about whether the First Amendment right of access applies outside of the criminal context. *SEC v. Am. Int'l Grp.*, 712 F.3d 1, 5 (D.C. Cir. 2013); *Ctr. for Nat'l Sec. Studies v. DOJ*, 331 F.3d 918, 935 (D.C. Cir. 2003); *In re Reporters Comm. for Freedom of the Press*, 773 F.2d 1325, 1337 (D.C. Cir. 1985) (Scalia, J.) (doubting that the benefits of open criminal trials inure to civil suits between private parties).

Competing interests may outweigh the public's common law right of access to judicial records. *United States v. Hubbard*, 650 F.2d 293, 317–22 (D.C. Cir. 1980). Indeed, "[a] district

court has authority to seal and unseal documents as part of its 'supervisory power over its own records and files.'" *United States v. Ring*, 47 F. Supp. 3d 38, 40 (D.D.C. 2014) (quoting *Nixon v. Warner Commc'ns, Inc.*, 435 U.S. 589, 598 (1978)); *In re Nat'l Broad. Co.*, 653 F.2d 609, 613 (D.C. Cir. 1981) ("Because of the difficulties inherent in formulating a broad yet clear rule to govern the variety of situations in which the right of access must be reconciled with legitimate countervailing public or private interests, the decision as to access is one which rests in the sound discretion of the trial court.").

Under D.C. Circuit law, the district court should weigh the following when presented with a motion to seal or unseal: "(1) the need for public access to the documents at issue; (2) the extent of previous public access to the documents; (3) the fact that someone has objected to disclosure, and the identity of that person; (4) the strength of any property and privacy interests asserted; (5) the possibility of prejudice to those opposing disclosure; and (6) the purposes for which the documents were introduced during the judicial proceedings." *Hubbard*, 650 F.2d at 317-22; *Metlife, Inc. v. Fin. Stability Oversight Council*, 865 F.3d 661, 666 (D.C. Cir. 2017) (Garland, C.J.) ("[T]he Hubbard test has consistently served as our lodestar because it ensures that we fully account for the various public and private interests at stake.").

The Federal Rules of Civil Procedure also recognize the important public and judicial interest in protecting confidential business information. *See* Fed. R. Civ. P. 26(c)(1)(G) (empowering courts to order "that a trade secret or other confidential research, development, or commercial information not be revealed or be revealed only in a specified way"). Likewise, Supreme Court and D.C. Circuit authority recognize the necessity of non-public ex parte proceedings. *See Granny Goose Foods, Inc. v. Teamsters,* 415 U.S. 423, 439, 94 S. Ct. 1113 (1974) ("Ex parte temporary restraining orders are no doubt necessary in certain

circumstances..."); *Carroll v. President and Com'rs of Princess Anne*, 393 U.S. 175, 180 (1968) ("There is a place in our jurisprudence for ex parte issuance, without notice, of temporary restraining orders."); *Omar v. Harvey*, 2006 WL 286861, at *1 (D.D.C. Feb. 6, 2006) (holding that an ex parte restraining order is appropriate where plaintiff demonstrates notice would render fruitless further prosecution of the action); *Council on American-Islamic Relations v. Gaubatz*, 667 F. Supp. 2d 67, 75 (D.D.C. Nov. 3, 2009) (noting that ex parte restraining orders may be appropriate in circumstances where notice is impossible).

In this case, Microsoft's rights and interests in protecting its ability to obtain ex parte temporary relief, and the necessity of sealing its pleadings in order to effectively disable the domains in **Appendix A** to the Complaint, is paramount over any competing public interest to *immediate* access to the information Microsoft requests be sealed. If Microsoft's papers are not sealed, the relief sought would very likely be rendered fruitless, and there is a substantial risk Defendants would destroy evidence. Defendants are highly-sophisticated cybercriminals. They access Microsoft's services without authorization; hack into high-value computer networks; install malware on the networks to gain and maintain long-term, surreptitious access to that network; and locate and exfiltrate sensitive information off of the networks. *See* Preliminary Injunction Motion, filed contemporaneously herewith. If Defendants knew Microsoft sought the relief set forth in the Preliminary Injunction Motion, they could quickly adapt the command and control infrastructure used to secretly establish themselves on a victim's network. *Id.* at 14.

In fact, Defendants have shown that this is their intention. Defendants continue to misuse Microsoft's trademarks and brand names to make their domains seem legitimate. Declaration of David Anselmi In Support Of Microsoft's Motion to Supplement Preliminary Injunction Order ("Anselmi Decl.") ¶ 4, set forth at **Appendix B** to this Brief. Given Microsoft's actions against

Defendants in this case, even disclosing that Microsoft has filed a Preliminary Injunction Motion gives Defendants the opportunity to change their command and control infrastructure, set forth at **Appendix A** to the Complaint.

Additionally, evidence shows that when the Phosphorus defendants become aware of efforts to mitigate or investigate their activities, they take steps to conceal their activities and to conceal the injury caused to their victims, making it more difficult for their victims to adequately assess the damage or take steps to mitigate that injury going forward. *Id.* ¶ 32. For example, once Defendants become aware that domains in Phosphorus' active infrastructure become known to the security community, they abandon that infrastructure and move to new infrastructure that is used to continue their efforts to intrude upon the computers of existing victims and new victims. *Id.* In the last five years, Microsoft has brought similar cases against John Doe defendants who have been conducting illegal activities through identifiable but movable infrastructures on the Internet very similar to that used by Phosphorus. Declaration of Gabriel M. Ramsey In Support Of Motion For Protective Order ("Ramsey Decl.") ¶ 5, set forth at **Appendix C** to this Brief. In four of those cases, the defendants immediately attempted to either destroy evidence or move their command and control infrastructure upon detecting the legal action being taken against them. *Id.* This underscores the risk that the Defendants in this case will take similar steps to destroy evidence and move their command and control infrastructure in **Appendix A** if they are given notice of the Preliminary Injunction Motion. *Id.* ¶ 6.

The harm that would be caused by the public filing of Microsoft's Preliminary Injunction Motion would far outweigh the public's right to access that information. There is no need for the public to have immediate access to the Preliminary Injunction Motion and supporting documents while Microsoft is seeking ex parte relief with respect to the domains in **Appendix A** to the

Complaint, which will only be effective if these materials remain under seal. Applying the balancing test set forth in governing law demonstrates that Microsoft's interest in obtaining effective relief outweigh any immediate public right to disclosure.

Microsoft only seeks to seal such information for a limited period of time, until after effective ex parte temporary relief has been obtained, disabling the domains in **Appendix A** to the Complaint. After such point, sealing will no longer be necessary, and Microsoft will immediately commence efforts to provide Defendants notice of future hearings and service of related pleadings—at which point, all documents will be unsealed and the public will be given full access to these proceedings. Microsoft, upon execution of the ex parte relief disabling the domains in **Appendix A** to the Complaint, will file with the Clerk of the Court a Notice that the temporary restraining order has been executed. The Clerk of the Court may then file all documents related to this request on the public docket.

Should, however, the Court decide not to grant the ex parte relief Microsoft requests, Microsoft asks that such materials remain sealed for an indefinite period, as public disclosure or notice absent the ex parte relief requested would facilitate Defendants' harmful and malicious Internet activities.

Given the limited period of sealing as an alternative that balances the public interest in access with Microsoft's important interests in maintaining these materials under seal for a brief period of time, granting the instant request to seal is warranted and consistent with the legal framework for addressing this issue.

Dated: March 14, 2019

Respectfully submitted,

/s/ Julia R. Milewski

Julia R. Milewski (D.C. Bar No. 1008678)
Justin D. Kingsolver (D.C. Bar. No. 1033806)
Matthew B. Welling (*pro hac vice* pending)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington DC 20004-2595
Telephone: (202) 624-2500
Fax: (202) 628-5116
jmilewski@crowell.com
jkingsolver@crowell.com
mwelling@crowell.com

Gabriel M. Ramsey (*pro hac vice* pending)
CROWELL & MORING LLP
3 Embarcadero Center, 26th Floor
San Francisco, CA 94111
Telephone: (415) 986-2800
Fax: (415) 986-2827
gramsey@crowell.com

Richard Domingues Boscovich (*pro hac vice* pending)
MICROSOFT CORPORATION
One Microsoft Way
Redmond, WA 98052-6399
Telephone: (425) 704-0867
Fax: (425) 936-7329
rbosco@microsoft.com

Attorneys for Plaintiff Microsoft Corp.

APPENDIX A

APPENDIX A

.ORG DOMAINS

Registry
Public Interest Registry (PIR)
1775 Wiehle Avenue
Suite 200
Reston Virginia 20190
United States

yahoo-verification.org	Domain Administrator Yahoo! Inc. 109 First Sunnyvale CA 94988 BA Phone: +1.4038493301 Fax: +1.4038493302 domainadmin@yahoo-verification.org

.COM, .NET, .NAME DOMAINS

Registry
VeriSign, Inc.
VeriSign Information Services, Inc.
12061 Bluemont Way
Reston Virginia 20190
United States

support-servics.com	Registrant Name: hash crypt Registrant Organization: hashcrypt Registrant Street: nbcj hjf,m Registrant City: losangles Registrant State/Province: Alabama Registrant Postal Code: 35004 Registrant Country: US Registrant Phone: +1.09876543567 Registrant Email: hashcrypt@protonmail.com
verification-live.com	Registrant Name: Domain Administrator Registrant Organization: Microsoft Corporation Registrant Street: AS8068 MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation, Registrant City: toranto Registrant State/Province: toranto Registrant Postal Code: 64043 Registrant Country: UM

	Registrant Phone: +1.6509234001 Registrant Fax: +1.6509234002 Registrant Email: test9179@porotonmail.com
com-mailbox.com	Registrant Name: Priview Service Registrant Organization: mish Registrant Street: No 885, Azar st Registrant City: Dubai Registrant State/Province: Dubai Registrant Postal Code: 98120 Registrant Country: AE Registrant Phone: +97.3218526 Registrant Fax: +97.3218526 Registrant Email: domain.seller2017@yandex.com
com-myaccuants.com	Registrant Name: Domain ID Shield Service Registrant Organization: Domain ID Shield Service CO., Limited Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registrant City: Hong Kong Registrant State/Province: Hong Kong Registrant Postal Code: 999077 Registrant Country: CN Registrant Phone: +852.21581835 Registrant Fax: +852.30197491 Registrant Email: co5940551458104@domainidshield.com
notification-accountservice.com	Registrant Name: mosa alnarjani Registrant Organization: Registrant Street: baqdad, alqusair st , no 246 Registrant City: baqdad Registrant State/Province: baqdad Registrant Postal Code: 548996 Registrant Country: IQ Registrant Phone: +964.7730061463 Registrant Email: meisam.bayat.sector@gmail.com
accounts-web-mail.com	Registrant Name: Domain Administrator Registrant Organization: Yahoo! Inc. Registrant Street: 107 First Avenue Registrant City: Sunnyvale Registrant State/Province: CA Registrant Postal Code: 94989 Registrant Country: US Registrant Phone: +1.4038493300 Registrant Fax: +1.4038493301 Registrant Email: test9179@yahoo.com
customer-certificate.com	Registrant Name: Domain ID Shield Service Registrant Organization: Domain ID Shield Service CO., Limited Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registrant City: Hong Kong

	Registrant State/Province: Hong Kong Registrant Postal Code: 999077 Registrant Country: HK Registrant Phone: +852.21581835 Registrant Fax: +852.30197491 Registrant Email: whoisprivacy@domainidshield.com
session-users-activities.com	Domain ID Shield Service Domain ID Shield Service CO., Limited FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Hong Kong Hong Kong 999077 HK Phone: +852.21581835 Fax: +852.30197491 whoisprivacy@domainidshield.com
user-profile-credentials.com	Domain ID Shield Service Domain ID Shield Service CO., Limited FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Hong Kong Hong Kong 999077 HK Phone: +852.21581835 Fax: +852.30197491 whoisprivacy@domainidshield.com
verify-linke.com	Registrant Name: sora bara Registrant Organization: narabara Registrant Street: ara Registrant City: mara Registrant State/Province: nara Registrant Postal Code: 7482957439 Registrant Country: BI Registrant Phone: +1.234124323 Registrant Fax: +1.2129876243 Registrant Email: test9179@protonmail.com
support-servics.net	Registrant Name: Support Services Inc. Registrant Organization: Support Services Inc. Registrant Street: 1901 Amphitheatre Parkway Registrant City: Mountain View Registrant State/Province: 64043 Registrant Postal Code: 64043 Registrant Country: US Registrant Phone: +1.6509234001 Registrant Fax: +1.6509188572 Registrant Email: test9179@protonmail.com
verify-linkedin.net	Registrant Name: sora bara Registrant Organization: none

	Registrant Street: ara Registrant City: mara Registrant State/Province: nara Registrant Postal Code: 748295743 Registrant Country: BI Registrant Phone: +75.234124323 Registrant Fax: +86.12124321 Registrant Email: dnsadmin@verify-linkedin.com
yahoo-verification.net	Registrant Organization: Yahoo! Inc. Registrant Street: 107 First Avenue Registrant City: Sunnyvale Registrant State/Province: CA Registrant Postal Code: 94989 Registrant Country: BA Registrant Phone: +1.4038493300 Registrant Fax: +1.4038493301 Registrant Email: test9179@yahoo.com
yahoo-verify.net	Registrant Name: Domain Administrator Registrant Organization: Yahoo! Inc. Registrant Street: 701 First Avenue Registrant City: Sunnyvale Registrant State/Province: CA Registrant Postal Code: 98089 Registrant Country: BI Registrant Phone: +1.4083893300 Registrant Fax: +1.4083893301 Registrant Email: domainadmin@yahoo-verify.net
hereyouare.ddns.net	Registrant Name: Dan Durrer Registrant Organization: No-IP.com Registrant Street: 425 Maestro Dr. Second Floor Registrant City: Reno Registrant State/Province: NV Registrant Postal Code: 89511 Registrant Country: US Registrant Phone: +1.7758531883 Registrant Email: domains@no-ip.com
outlook-verify.net	Registrant Name: Domain Administrator Registrant Organization: Microsoft Corporation Registrant Street: One Microsoft Way, Redmond, WA, 98052, US Registrant City: Washington Registrant State/Province: canada Registrant Postal Code: 7482957439 Registrant Country: US Registrant Phone: +1.234124323 Registrant Phone Ext: Registrant Fax: +1.2129876243 Registrant Fax Ext: Registrant Email: supportiveemail@protonmail.com
com-users.net	Registrant Name: Domain ID Shield Service Registrant Organization: Domain ID Shield Service CO., Limited

	Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registrant City: Hong Kong Registrant State/Province: Hong Kong Registrant Postal Code: 999077 Registrant Country: CN Registrant Phone: +852.21581835 Registrant Phone Ext: Registrant Fax: +852.30197491 Registrant Fax Ext: Registrant Email: co5806503530204@domainidshield.com
verifiy-account.net	Registrant Name: Domain ID Shield Service Registrant Organization: Domain ID Shield Service CO., Limited Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registrant City: Hong Kong Registrant State/Province: Hong Kong Registrant Postal Code: 999077 Registrant Country: HK Registrant Phone: +852.21581835 Registrant Fax: +852.30197491 Registrant Email: whoisprivacy@domainidshield.com
telegram.net	Registrant Name: NS-CLOUD-B1.GOOGLEDOMAINS.COM Registrant Organization: Domains By Proxy, LLC Registrant Street: clientTransferProhibited https://icann.org/epp#clientTransfe Registrant City: Arizona Registrant State/Province: Arizona Registrant Postal Code: 0056 Registrant Country: US Registrant Phone: +1.4806242505 Registrant Fax: +1.4806242506 Registrant Email: verdonew@protonmail.com
account-verifiy.net	Registrant Name: Domain ID Shield Service Registrant Organization: Domain ID Shield Service CO., Limited Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registrant City: Hong Kong Registrant State/Province: Hong Kong Registrant Postal Code: 999077 Registrant Country: HK Registrant Phone: +852.21581835 Registrant Fax: +852.30197491 Registrant Email: whoisprivacy@domainidshield.com
myaccount-services.net	Registrant Name: Domain ID Shield Service Registrant Organization: Domain ID Shield Service CO., Limited Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL

	TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registrant City: Hong Kong Registrant State/Province: Hong Kong Registrant Postal Code: 999077 Registrant Country: HK Registrant Phone: +852.21581835 Registrant Fax: +852.30197491 Registrant Email: whoisprivacy@domainidshield.com
com-identifier-servicelog.name	Registrant Name: Whois Agent Registrant Organization: Domain Protection Services, Inc. Registrant Street: PO Box 1769 Registrant City: Denver Registrant State/Province: CO Registrant Postal Code: 80201 Registrant Country: US Registrant Phone: +1.7208009072 Registrant Fax: +1.7209758725 Registrant Email: https://www.name.com/contact-domain-whois/com-identifier-servicelog.name abuse@name.com

.BID DOMAINS

Registry
c/o
Neustar, Inc.
21575 Ridgetop Circle
Sterling, VA 20166
United States

dot Bid Limited
2nd Floor, Leisure Island Business Centre
Ocean Village
GX11 1AA
Gibraltar

Global Registry Services Limited
327 Main Streeet,
Gibraltar GX11 1AA

microsoft-update.bid	Registrant Name: Chada Martini Registrant Organization: cavy Registrant Street: No 67, King st Registrant City: Tashkent Registrant State/Province: Tashkent Registrant Postal Code: 46543 Registrant Country: UZ Registrant Phone: +968.8007762430

	Registrant Fax: +968.8007762430 Registrant Email: chada.martini@yandex.com
outlook-livecom.bid	Registrant Name: Chada Martini Registrant Organization: cavy Registrant Street: No 67, King st Registrant City: Tashkent Registrant State/Province: Tashkent Registrant Postal Code: 46543 Registrant Country: UZ Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430 Registrant Email: chada.martini@yandex.com
update-microsoft.bid	Registrant Name: Chada Martini Registrant Organization: cavy Registrant Street: No 67, King st Registrant City: Tashkent Registrant State/Province: Tashkent Registrant Postal Code: 46543 Registrant Country: UZ Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430 Registrant Email: chada.martini@yandex.com

.CLOUD DOMAINS

Registry
c/o
Neustar, Inc.
21575 Ridgetop Circle
Sterling, VA 20166
United States

ARUBA PEC S.p.A.
Via Sergio Ramelli 8
52100 Arezzo (AR)
Italy

documentsfilesharing.cloud	Registrant Name: Whois Agent Registrant Organization: Domain Protection Services, Inc. Registrant Street: PO Box 1769 Registrant City: Denver Registrant State/Province: CO Registrant Postal Code: 80201 Registrant Country: US Registrant Phone: +1.7208009072 Registrant Fax: +1.7209758725 documentsfilesharing.cloud@protecteddomainservices.com

.CLUB DOMAINS

Registry
.CLUB DOMAINS, LLC
100 SE 3rd Ave. Suite 1310
Fort Lauderdale, FL 33394
United States

com-microsoftonline.club	Registrant Name: Chada Martini Registrant Organization: cavy Registrant Street: No 67, King st Registrant City: Tashkent Registrant State/Province: Tashkent Registrant Postal Code: 46543 Registrant Country: UZ Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430 Registrant Email: chada.martini@yandex.com

.INFO, .MOBI, .PRO DOMAINS

Registry
Afilias, Inc.
300 Welsh Road
Building 3, Suite 105
Horsham, PA 19044
United States

confirm-session-identifier.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
session-management.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
confirmation-service.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
document-share.info	Registrant Organization: Martini Registrant State/Province: Tashkent Registrant Country: UZ onlinenic-enduser@onlinenic.com
broadcast-news.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
customize-identity.info	Registrant Organization: Domain ID Shield Service CO., Limited

	Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
webemail.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
com-identifier-servicelog.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
customize-identity.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
documentsharing.info	Registrant Organization: will co Registrant State/Province: VA Registrant Country: AF onlinenic-enduser@onlinenic.com
notification-accountservice.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
identifier-activities.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
documentofficupdate.info	Registrant Organization: William Brown Registrant State/Province: VA Registrant Country: US onlinenic-enduser@onlinenic.com
recoveryusercustomer.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
serverbroadcast.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
account-profile-users.info	Registrant Organization: arsalan co. Registrant State/Province: Louisiana Registrant Country: US onlinenic-enduser@onlinenic.com
account-service-management.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
accounts-manager.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK

	onlinenic-enduser@onlinenic.com
activity-confirmation-service.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
com-accountidentifier.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
com-privacy-help.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
com-sessionidentifier.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
com-useraccount.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
confirmation-users-service.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
confirm-identity.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
confirm-session-identification.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
continue-session-identifier.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
customer-recovery.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
customers-activities.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
elitemaildelivery.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
email-delivery.info	Registrant Organization: Domain ID Shield Service CO., Limited

	Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
identify-user-session.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
message-serviceprovider.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notificationapp.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notification-manager.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
recognized-activity.info	Registrant Organization: will co Registrant State/Province: VA Registrant Country: VA onlinenic-enduser@onlinenic.com
recover-customers-service.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
recovery-session-change.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
service-recovery-session.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
service-session-continue.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
session-mail-customers.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
session-managment.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
session-verify-user.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK

	onlinenic-enduser@onlinenic.com
shop-sellwear.info	Registrant Organization: maryam s32 Registrant State/Province: tersite Registrant Country: US onlinenic-enduser@onlinenic.com
supportmailservice.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
terms-service-notification.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
user-activity-issues.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
useridentity-confirm.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
users-issue-services.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
verify-user-session.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
login-gov.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notification-signal-agnecy.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notifications-center.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
identifier-services-sessions.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
customers-manager.info	Registrant Organization: Home Registrant State/Province: TX Registrant Country: US onlinenic-enduser@onlinenic.com
session-manager.info	Registrant Organization: Home

	Registrant State/Province: TX Registrant Country: US onlinenic-enduser@onlinenic.com
customer-managers.info	Registrant Organization: Home Registrant State/Province: TX Registrant Country: US onlinenic-enduser@onlinenic.com
confirmation-recovery-options.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
service-session-confirm.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
session-recovery-options.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
services-session-confirmation.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notification-managers.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
activities-services-notification.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
activities-recovery-options.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
activity-session-recovery.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
customers-services.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
recovery-session-change.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notification-manager.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK

	onlinenic-enduser@onlinenic.com
session-managment.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
sessions-notification.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
download-teamspeak.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
services-issue-notification.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
microsoft-upgrade.mobi	Registrant Name: Chada Martini Registrant Organization: cavy Registrant Street: No 67, King st Registrant City: Tashkent Registrant State/Province: Tashkent Registrant Postal Code: 46543 Registrant Country: UZ Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430 Registrant Email: chada.martini@yandex.com
broadcastnews.pro	Registrant State/Province: UT Registrant Country: US abuse@name.com

.NETWORK, .WORLD DOMAINS

Registry
Binky Moon, LLC
Donuts Inc.
5808 Lake Washington Blvd NE, Suite 300
Kirkland, WA 98033
United States

mobile-messengerplus.network	Registrant Name: Cave Detector Registrant Organization: Masqat Co Registrant Street: No 64, Lion St Registrant City: Masqat Registrant State/Province: Masqat Registrant Postal Code: 85641 Registrant Country: OM Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430

	Registrant Email: cave.detector@yandex.com
sessions-identifier-memberemailid.network	Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Domain Protection Services, Inc. Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: CO Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registrar: Name.com, Inc. Registrar IANA ID: 625 Registrar Abuse Contact Email: abuse@name.com Registrar Abuse Contact Phone: +7.202492374

APPENDIX B

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

MICROSOFT CORPORATION, a Washington corporation, Plaintiff, v. JOHN DOES 1-2, CONTROLLING A COMPUTER NETWORK AND THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS, Defendants.	)	Civil Action No:

DECLARATION OF DAVID ANSELMI IN SUPPORT OF MICROSOFT'S APPLICATION FOR AN EMERGENCY EX PARTE TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

I, David Anselmi, declare as follows:

1. I am a Senior Investigator in the Digital Crimes Unit of Microsoft Corporation's Legal and Corporate Affairs Group. I make this declaration in support of Microsoft's application for an Emergency Ex Parte Temporary Restraining Order And Order To Show Cause Re Preliminary Injunction. I make this declaration of my own personal knowledge and, if called as a witness, I could and would testify competently to the truth of the matters set forth herein.

2. In my current role at Microsoft, I assess technical security threats to Microsoft and the impact of such threats on Microsoft's business and customers. Prior to my current role, I worked as Senior Technologist, dealing with security of Microsoft's online services. Among my responsibilities were protecting Microsoft's customer-facing online service assets from network-based attacks. Prior to that, while also employed by Microsoft, I worked as a Senior Technologist, dealing with protecting Microsoft's corporate resources from network-based

attacks. Before joining Microsoft, I worked for Excell Data Corporation as a Program Manager performing security firewall deployment, configuration, and administration. I am a graduate of the United States Military Academy, West Point, and served for 27 years as a United States Army Communications Electronics Officer (11 years active, 16 years reserve), attaining the rank of Lieutenant Colonel. I have been employed by Microsoft since February 1997.

I. OVERVIEW OF INVESTIGATION INTO PHOSPHORUS AND CONCLUSIONS

3. My declaration concerns an organization that is engaged in systematic criminal activity on the Internet. Because the identities of the individuals behind the activity addressed in this declaration are unknown, I therefore refer to them collectively by the codename that Microsoft has assigned to this group: "Phosphorus." Others in the security community who have researched this group of actors refer to the group by other names, including "APT 35," "Charming Kitten," and "Ajax Security Team." The defendants have been linked to an Iranian hacking group or groups. I have investigated the infrastructure described in this declaration and have determined that the defendants have registered Internet domains using fictitious names and fictitious physical addresses that are purportedly located in multiple cities and countries. Defendants have registered domains using functioning email addresses by which they communicated with domain registrars in order to complete the registration process.

4. Microsoft investigators have been monitoring and gathering information on the Phosphorus defendants. In the course of such investigation, I have been working with and directing a team that (1) engaged in the analysis and creation of "signatures" (which can be thought of as digital fingerprints) for the infrastructure used by the Phosphorus defendants, (2) discovered login activity into Microsoft services from Phosphorus-controlled infrastructure on the Internet, (3) matched reported Phosphorus phishing email campaigns to registered domains, (4) monitored domain registrations associated with the Phosphorus-controlled email addresses and other pertinent WHOIS record information, (5) monitored infrastructure frequently utilized by the Phosphorus defendants in order to identify new domains being registered by the Phosphorus defendants, (6) have confirmed resolution settings to particular Internet service

providers (ISPs) which have frequently been used by the Phosphorus defendants in the past, and (7) reviewed peer findings and public reporting on the Phosphorus defendants.

5. As alluded in paragraph 4 (1), the investigative team has developed methods to help us identify new domains registered by the Phosphorus actors. Particular features of the Phosphorus infrastructure have been identified and patterns of content, non-content, and technical features have been determined to be exclusively and specifically associated with the Phosphorus defendants. These features, when identified in the aggregate, provide a high level of confidence that a given domain is a Phosphorus domain. Each such domain is manually reviewed in detail by one or more subject matter experts as necessary to ascertain whether it is, in fact, a Phosphorus domain. Based on this analysis, we have identified characteristics of the registration and maintenance of certain domains which, when coupled with the nature of the activities observed being carried out through the domains, are a reliable method to correlate such domains to actions undertaken by the defendants.

6. Based on our investigation and analysis, Microsoft has determined that the Phosphorus defendants specialize in targeting and stealing credentials of prominent users of the Internet. The Phosphorus defendants target Microsoft and non-Microsoft customers in both the private and public sectors, including businesses in a variety of different industries. Based on our research, the Phosphorus defendants have targeted Microsoft customers, political dissidents, activist leaders, the Defense Industrial Base (DIB), journalists, and employees from multiple government agencies, including individuals protesting oppressive regimes in the Middle East. For example, attached as **Exhibit 1** is a true and correct copy of a research report by security research firm FireEye regarding the Phosphorus group (which that firm has called "Ajax Security Team").

7. The Phosphorus defendants' objectives appear to be obtaining account credentials to later retrieve sensitive communications within the accounts. We believe that the Phosphorus defendants have been active since 2013 and continue to pose a threat today and into the future.

II. PHOSPHORUS' METHOD OF COMPROMISING AND STEALING

INFORMATION FROM VICTIMS

8. The Phosphorus defendants typically attempt to compromise the personal (not work) accounts of the targeted individuals through a technique known as "spear phishing." Spear phishing attacks are conducted in the following fashion: After researching a victim organization, the spear phisher will identify individuals associated with that organization through gathering publicly available information and by social engineering. The spear phisher will then initiate communications with the victim by using names, companies, and/or contents that are familiar to the victim. The ensuing communications exchanges are used to social engineer information, identify additional targets, entice a target into opening up a malicious attachment, and more. Microsoft has observed fake social networking profiles being created by Phosphorus defendants which would obviously present significant leverage in carrying out such an attack. Attached as **Exhibit 2** are true and correct copies of such fake social networking profiles, created by the Phosphorus defendants on the LinkedIn social media service.

9. Another technique utilized by the Phosphorus defendants is to send a targeted individual an email specifically crafted to appear as if there is an issue with the targeted individual's account. Phishing emails often use generic domain names that appear to be tied to account activity and that require input of credentials for authentication. For example, domains such as service-accountrecovery.com. The Phosphorus defendants send the targeted individual an email specifically crafted to appear as if there is an issue with the targeted individual's account. Through research and investigation, Microsoft has determined that the Phosphorus defendants have used the domains listed in **Exhibit 3** (which is also reflected as **Appendix A** to the Complaint) in its command and control infrastructure. As can be seen in **Exhibit 3**, the Phosphorus defendants sometimes also disguise their command and control domains by incorporating the names and trademarks of some well-known companies and organizations, including Microsoft's "Microsoft" and Windows "Live" brands, as well as the "LinkedIn" brand. For example, the Phosphorus defendants use the domains com-microsoftonline.club, verification-live.com, and verify-linkedin.net.

10. The Phosphorus defendants' use of Microsoft trademarks is meant to confuse victims into clicking on links controlled by the Phosphorus defendants. When the user clicks on the links, they are taken to deceptive web pages that induce the victim to type in their Microsoft credentials, at which point the Phosphorus defendants obtain access to those credentials. This will result in the threat actors being able to log into the victim's account and access their email. The Phosphorus defendants can also download a copy of the victim's address book to be used for future targeting of additional intended victims. Not having safe emails impacts Microsoft's brands and services. Customers expect Microsoft to provide safe and trustworthy products and services. There is a great risk that Microsoft's customers, both individuals and the enterprises for which they work, may incorrectly attribute these problems to Microsoft's products and services, thereby diluting and tarnishing the value of these trademarks and brands.

11. The Phosphorus defendants send these emails from a variety of online email services. As discussed above, there are multiple Phosphorus created domains mimicking Microsoft brands, and those domains are clearly designed to be included in spear phishing emails as links to websites that the Phosphorus defendants have set up in advance and which they control. When a victim clicks on the link in the email, his or her computer is connected with the Phosphorus-controlled website. The victim is then presented a copy of a webpage that appears to be a login page for a webmail provider of which the victim is a subscriber. In fact, this is a fake login page that is designed to induce the user to type in their webmail credentials. If the victim enters the correct credentials, at that point the Phosphorus actors obtain the user's credentials and can thereafter access the user's webmail account to steal email content and other information.

12. **Figures 1 and 2** below show copies of such webpages created by the Phosphorus defendants, designed to look like legitimate Microsoft Outlook login pages:

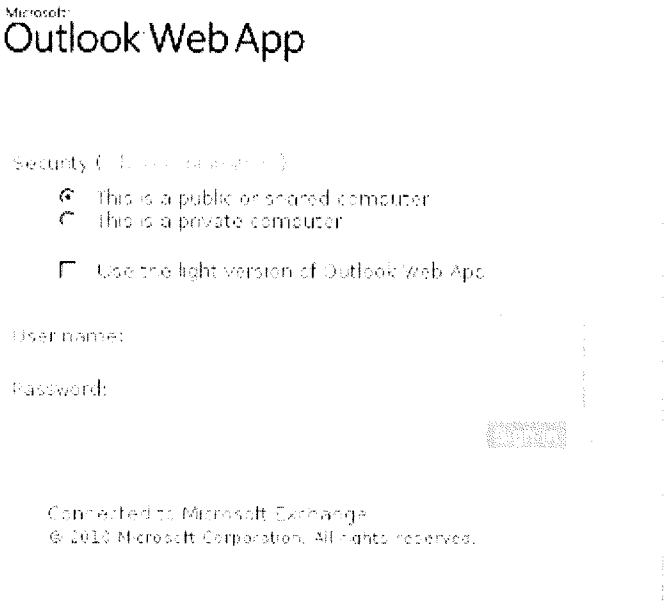


Figure 1

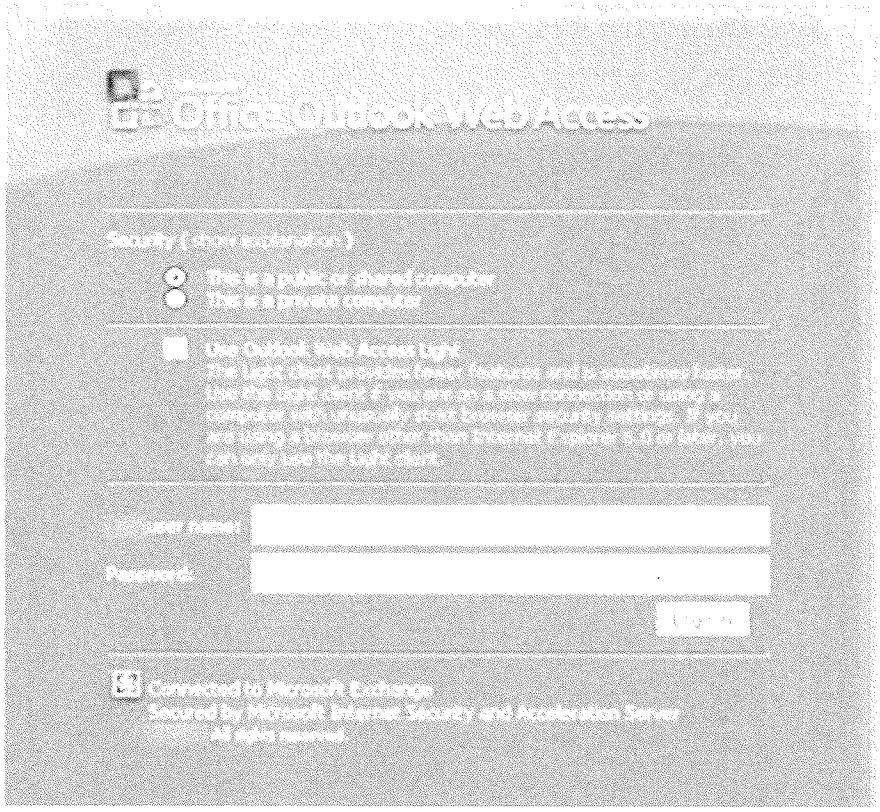
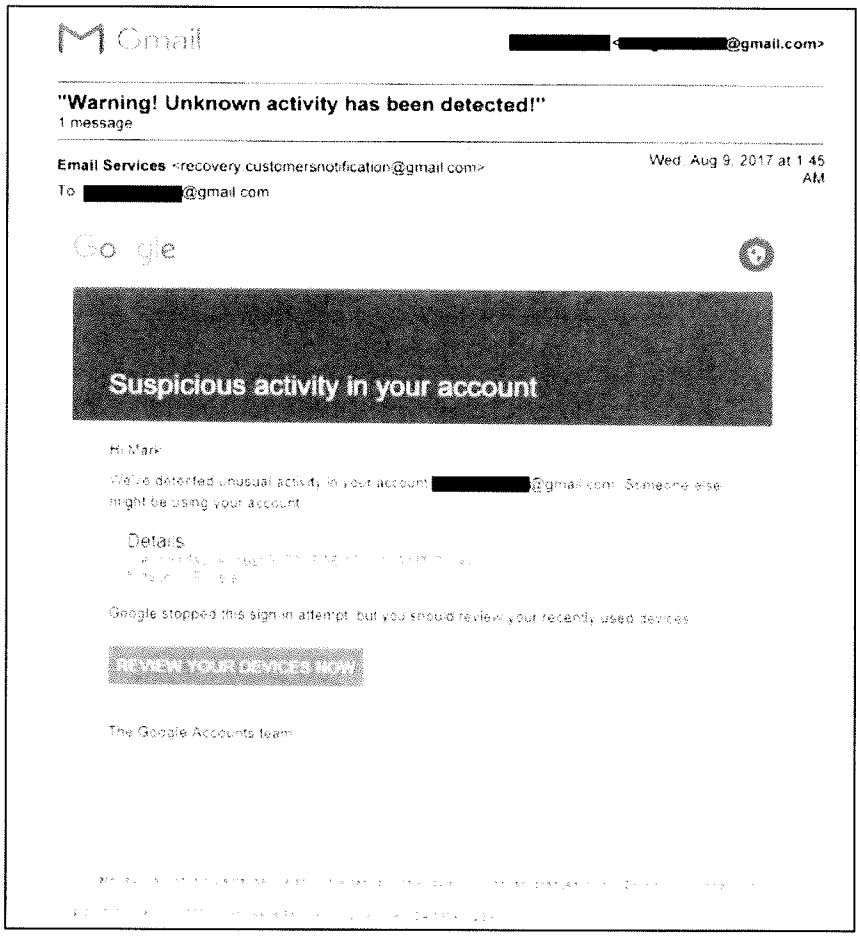


Figure 2

13. Phosphorus targets other brands beyond Microsoft and purport to be password reset or account login pages of other companies. For example, the Phosphorus defendants use fake emails instructing users to click links and type in credentials, fake "Verify" buttons prompting users to type their credentials into fraudulent login pages and fake "Sign in" pages instructing users to enter their user name and password. All of these methods are designed to induce users to type in credentials. As seen above with respect to the fake Microsoft login pages inviting users to type in their Microsoft Outlook "User name" and "Password," this scheme is typical of the Phosphorus defendants' activities. **Figures 3** through **6** are further examples of this tactic:


Gmail

[redacted] <[redacted]@gmail.com>

"Warning! Unknown activity has been detected!"
1 message

Email Services <recovery customersnotification@gmail com>
To [redacted]@gmail com

Wed Aug 9, 2017 at 1 45 AM

Google

Suspicious activity in your account

Hi Mark

We've detected unusual activity in your account [redacted]@gmail.com. Someone else might be using your account

Details

Google stopped this sign-in attempt but you should review your recently used devices

REVIEW YOUR DEVICES NOW

The Google Accounts team

Figure 3

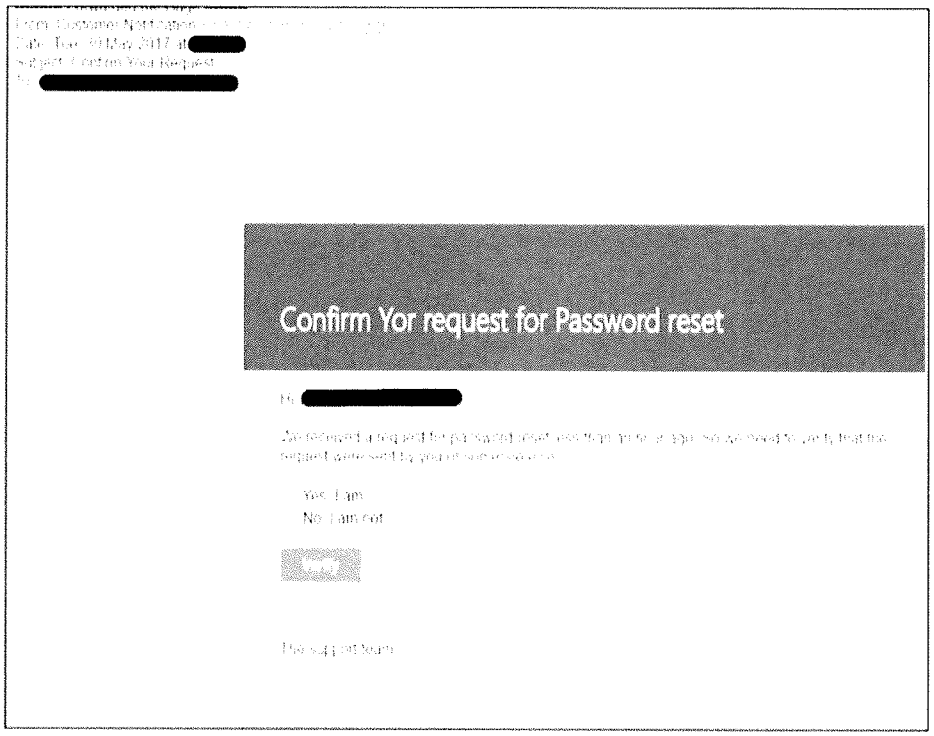


Figure 4

Figure 5

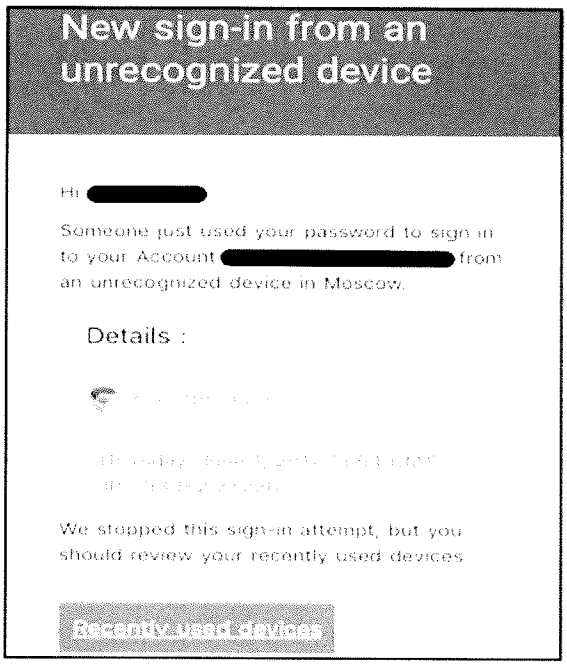


Figure 6

14. Upon successful compromise of a victim account, the Phosphorus defendants will not only be able to log into the account and review the victim's emails, but may also delete the spear phishing email that they previously sent to the user in an attempt to obfuscate their activities.

15. The Phosphorus defendants have targeted victims who are using Microsoft email services, and Microsoft investigators have confirmed that Phosphorus defendants have intruded into those accounts to steal information of Microsoft's users. **Figures 1 and 2** above demonstrate the Phosphorus defendants targeting users of Microsoft's Outlook email services.

16. Microsoft investigators were also able to locate the control panel used by the Phosphorus defendants to create links sent to intended victims as well as to track successfully compromised victims who clicked on those links, typed in their credentials and had those credentials stolen by the defendants. Microsoft analysts identified the Phosphorus domain confirm-session-identification.info which led to discovery of the control panel URL. This control panel was accessed by a URL that was open and required no authentication. The control panel that the Phosphorus defendants used to monitor and control their access to victim accounts

was present on the domain: confirm-session-identification.info. The domain confirm-session-identification.info was registered on 10/17/2018 as seen in the WHOIS record from a commonly used domain research tool called Domaintools.com. This WHOIS record is reflected in **Figure 7**:

```
Domain Name: CONFIRM-SESSION-IDENTIFICATION.INFO
Registry Domain ID: D503300000240279653-LRMS
Registrar WHOIS Server:
Registrar URL: https://www.onlinenic.com
Updated Date:
Creation Date: 2018-10-17T11:27:08Z
Registry Expiry Date: 2019-10-17T11:27:08Z
Registrar Registration Expiration Date:
Registrar: OnlineNIC, Inc.
Registrar IANA ID: 82
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Reseller:
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registrant Organization: Domain ID Shield Service CO., Limited
Registrant State/Province: Hong Kong
Registrant Country: CN
Name Server: NS1.DNS-DIY.NET
Name Server: NS2.DNS-DIY.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form is https://www.icann.org/wicf/

The Registrar of Record identified in this output may have an RDDS service that can be queried for addit
```

Figure 7

17. The domain confirm-session-identification.info resolved to IP address 190.2.154.35 (Netherlands) from October 18th – 20th, 2018 and then moved to CloudFlare IP address, 104.27.134.98 (US). The control panel below was obtained from the confirm-session-identification.info domain, when hosted on 104.27.134.98, on 11/04/2018. When visiting the URL http:// confirm-session-identification.info/recovery/ on 11/04/2018 the control panel did not require authentication to view its contents. Upon visiting this URL on 11/04/2018, we confirmed that the Phosphorus defendants use a unique ID (URL) for each targeted user. A redacted list of the users targeted can be seen in the email column in Figure 8 below.

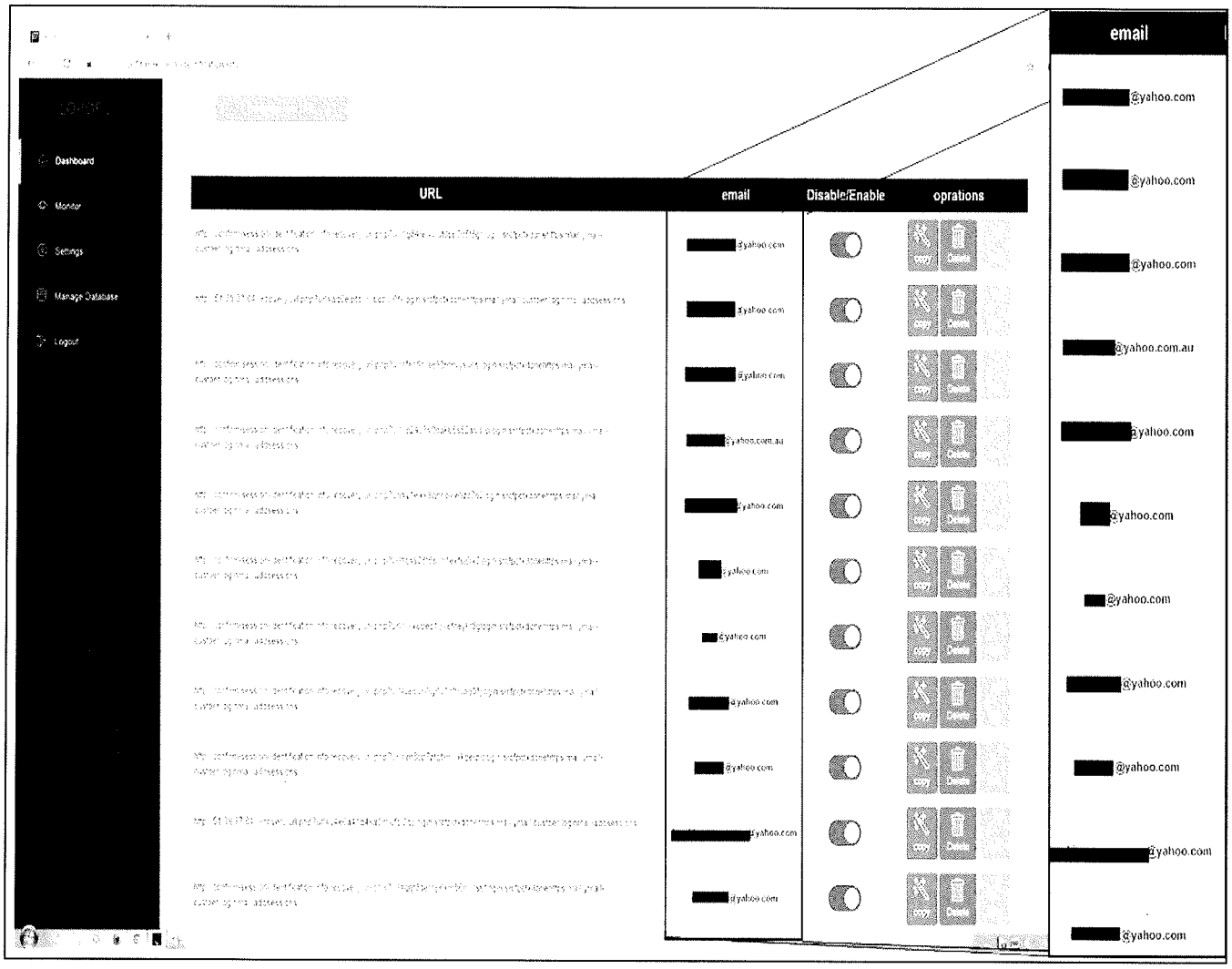


Figure 8

18. The Phosphorus defendants' email panel has a "Monitor" screen for tracking compromised users. As seen in the screenshot below (**Figure 9**), there is at least one victim observed at the time of accessing the unauthenticated email panel:

Target Email	Auth Type	Auth Result	Date and Time	password/code
[redacted]@yahoo.com	-	-	2018-10-25 01:56:36	-

User Agent	IP	country	city
Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36	38.122.191.174	United States	America/New_York

Figure 9

19. Additionally, the settings tab (**Figure 10**) shows that when users' credentials are compromised, the credentials stolen from Microsoft users and others are emailed to the Yahoo account soup_mctavish@yahoo.com with the subject line "Yahoo-Pishing." Note here that the Phosphorus defendants misspelled "Phishing").

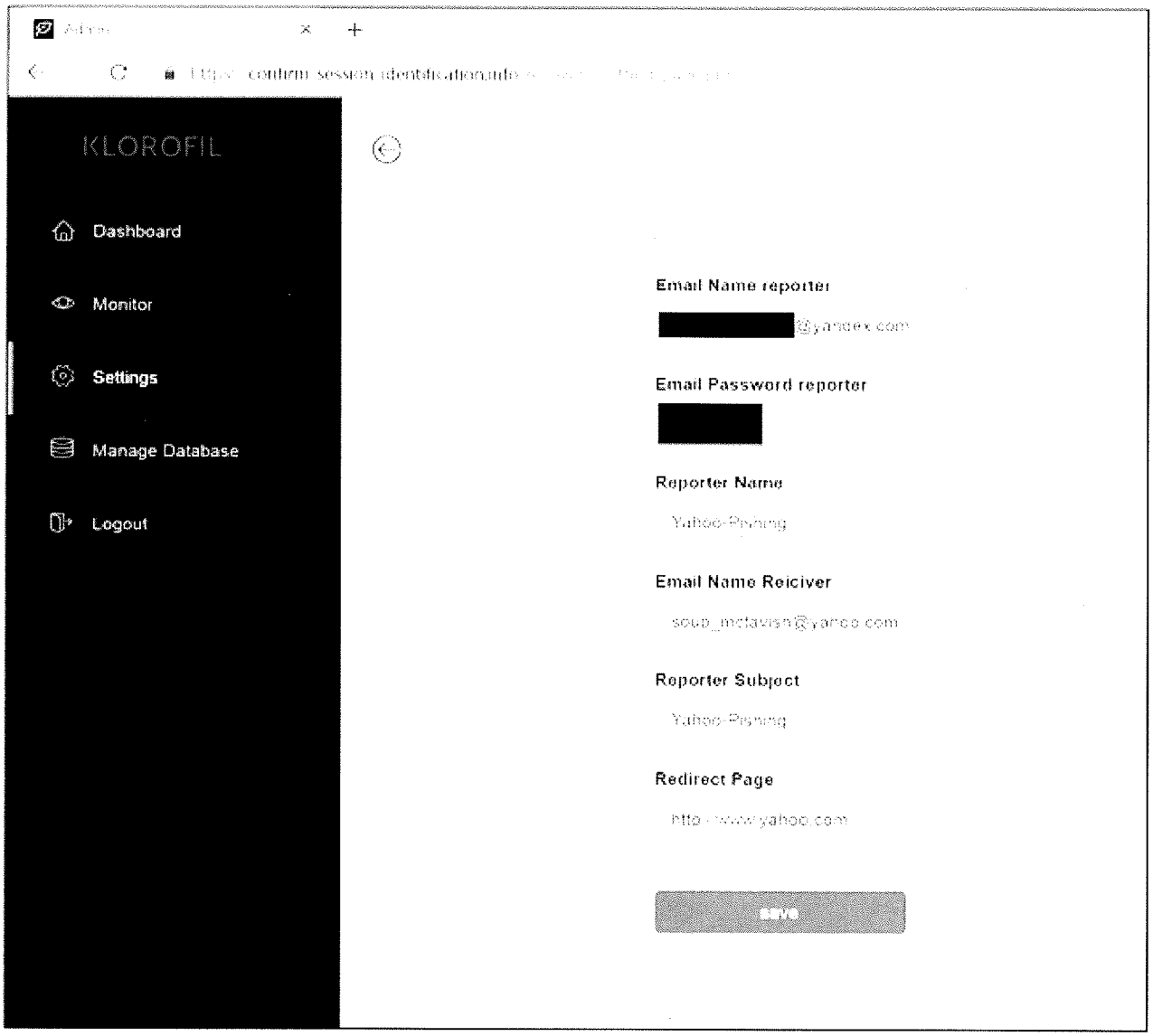


Figure 10

20. The Phosphorus defendants also intrude upon and cause injury to Microsoft and Microsoft's customers by damaging the customers' computers and the software installed on their computers. In particular, the Phosphorus defendants have sent deceptive email messages to victims, such as those discussed above, which include links to websites from which the defendants install malicious software onto the victims' computers. The defendants refer to the malicious software as "Stealer." Stealer, once installed, can record what the victim types on their keyboard, take screenshots of what is on the victim's computer screen, steal login credentials for instant messaging account (including information about victims' Microsoft-owned "Skype" messaging accounts), email accounts, and other credentials. The Stealer software is installed from, and stolen information may be transferred to, defendants using command and control domains such as those reflected in **Exhibit 3**.

21. The installation of this malicious software damages the victim's computer and the Windows operating system on the victim's computer. During the infection of a victim's computer, the malicious Stealer software makes changes at the deepest and most sensitive levels of the computer's Windows operating system. The consequences of these changes are that the user's version of Windows is essentially adulterated, and unknown to the user, has been converted into a tool to steal credentials and sensitive information from the user. This inherently involves abuse of Microsoft's trademarks and brands, and deceives users by presenting an unauthorized, modified version of Windows to those users. For example, the defendants create registry key paths bearing the Microsoft "Windows" trademark, within the Microsoft operating system, including, among others:

```
"C:\WINDOWS\system32\rundll32.exe" "C:\ Documents and
Settings\{USER}\ApplicationData\IntelRapidStart\AppTransferWiz.dll",#110
```

22. Further, as seen in **Figure 11** below, the Phosphorus defendants include metadata within the Stealer malicious software that expressly misrepresents that the software is created by "Microsoft" and that the software is a "Process for Windows."

File Version Information

[illegible]	Copyright [illegible] 2013
[illegible]	Process for Windows
[illegible]	Process for Windows
[illegible]	Stealer.exe
[illegible]	Stealer.exe
[illegible]	1.0.0.0
[illegible]	Process for Windows

ExifTool File Metadata

[illegible]	1.0.0.0
[illegible]	Unicode
[illegible]	224256
[illegible]	Process for Windows
[illegible]	Microsoft
[illegible]	0x38b1e
[illegible]	Process for Windows
[illegible]	0x0031
[illegible]	Win32
[illegible]	0
[illegible]	Win32 EXE
[illegible]	exe
[illegible]	1.0.0.0
[illegible]	1.0.0.0
[illegible]	Executable, 32-bit
[illegible]	0.0
[illegible]	2048
[illegible]	Stealer.exe
[illegible]	Neutral
[illegible]	Copyright 2013
[illegible]	11.0
[illegible]	application/octet-stream
[illegible]	Intel 386 or later, and compatibles
[illegible]	4.0

Figure 11

III. PHOSPHORUS HAS ATTACKED MANY MICROSOFT CUSTOMERS IN THE DISTRICT OF COLUMBIA AND AROUND THE WORLD

23. Through its investigation, Microsoft has determined that the Phosphorus defendants have targeted Microsoft customers in the District of Columbia and throughout the United States. In only the last few months alone, four new individual victims of the Phosphorus

defendants' email intrusion activities have been identified in the District of Columbia.

IV. HARM TO MICROSOFT AND MICROSOFT CUSTOMERS

24. Phosphorus irreparably harms Microsoft by damaging its reputation, brands, and customer goodwill. Microsoft is the provider of the Windows operating system and Outlook, Hotmail, OneDrive and Office 365 email and cloud services, as well as a variety of other software and services. Microsoft is the owner of the "Microsoft," "Windows," "Outlook," "Windows Live," "Hotmail," "OneDrive" and "Office 365" trademarks. Trademark registrations for marks infringed by the Phosphorus defendants are attached to Microsoft's complaint as **Appendix B**. Microsoft has invested substantial resources in developing high-quality products and services. Microsoft has also invested, through its subsidiaries, in high value brands and services such as the "LinkedIn" brand and service. Due to the high quality and effectiveness of Microsoft's products and services and the expenditure of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, has established a strong brand, and has developed the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. Microsoft has registered trademarks representing the quality of its products and service and its brand, including the trademarks listed above.

25. Microsoft's customers whose email accounts are compromised through the defendants' credential theft are damaged by these activities. Similarly, Microsoft's customers whose computers are infected with the malicious Stealer software are damaged by changes to Windows, which alter the normal and approved settings and functions of the user's operating system, destabilize it, and enable unauthorized monitoring of the user and theft of user data.

26. In effect, once infected, altered and controlled by the Stealer software, the Windows operating system ceases to operate normally and is now a tool of deception and theft aimed at the owner of the infected computer. Yet they still bear the Microsoft Windows trademark. This is obviously meant to mislead Microsoft's customers, and it causes extreme damage to Microsoft's brands and trademarks.

27. Customers are usually unaware of the fact that their email accounts are compromised, that their computers are infected, that they are being monitored by the defendants or that sensitive information is being stolen from them. Even if aware of an account intrusion or an infection of their computer, users often lack the technical resources or skills to resolve the problem, allowing their accounts and computers to be misused indefinitely, as manual steps to change account credentials or remove the malicious software may be difficult for ordinary users. They may be futile to a degree too where the Phosphorus defendants have software installed to observe the victim's activities and attempts to remediate the intrusion. Even with professional assistance, cleaning an infected end-user computer can be exceedingly difficult, time-consuming, and frustrating. This demonstrates the extreme problems that the activities of the Phosphorus defendants cause for Microsoft's customers and the irreparable injury to both Microsoft and its customers. Microsoft and other members of the public must invest considerable time and resources investigating and remediating the defendants' intrusion into accounts and computers.

28. The activities of the Phosphorus defendants injure Microsoft and its reputation, brand, and goodwill. Users subject to the negative effects of the Phosphorus defendants' spear phishing emails sometimes incorrectly believe that Microsoft is the source of the problem, and thus there is a significant risk that Microsoft customers will be confused in this way in the future. There is a great risk that Microsoft customers may incorrectly attribute these problems to Microsoft and associate these problems with Microsoft's products and services, thereby diluting and tarnishing the value of these trademarks and brands.

V. DISRUPTING PHOSPHORUS' ILLEGAL ACTIVITIES

29. The Phosphorus defendants' illegal activities will not be easy to disrupt. Evidence indicates that the Phosphorus defendants are highly sophisticated, well-resourced, organized, and patient. The Phosphorus defendants specialize in targeting individuals in organizations holding sensitive data, by gathering extensive information about their employees through publicly available information and social media, using that information to fashion phishing attacks intended to trick those employees into compromising their credentials, and

disguising its activities using the names and trademarks of Microsoft and other legitimate companies.

30. The most vulnerable point in the Phosphorus defendants' operations are a number of Internet domains through which the Phosphorus defendants obtain victim credentials, log into compromised accounts, and review sensitive information from victim accounts. A core subset of these is listed in **Appendix A** to the Complaint. These domains sometimes incorporate trademarks that are owned by Microsoft or by other companies that have been informed of and have no objection to Microsoft's proposal to take possession of these domains. Granting Microsoft possession of these domains will enable Microsoft to channel all communications to those domains to secure servers, and thereby cut off the means by which the Phosphorus defendants collect victim credentials. In other words, any time a user clicks on a link in a spear phishing email and provides their username and password, that information will be prevented from going to the defendants at the Phosphorus domains, because those domains will be hosted on a Microsoft-controlled, secure server, beyond the control of defendants. While it is not possible to rule out the possibility that the Phosphorus defendants could use fall back mechanisms to evade the requested relief, redirecting this core subset of Phosphorus domains will directly disrupt current Phosphorus infrastructure, mitigating risk and injury to Microsoft and its customers. The requested relief will also serve the public interest, in protecting customers of other web services companies who have consented to the relief sought in this action.

31. I believe that the most effective way to suspend the injury caused to Microsoft, its consumers, and the public, is to take the steps described in the [Proposed] Ex Parte Temporary Restraining Order and Order to show Cause Re Preliminary Injunction ("Proposed TRO"). This relief will significantly hinder the Phosphorus defendants' ability to compromise additional accounts and identify new potential victims to target. In the absence of such action, the Phosphorus defendants will be able to continue using this infrastructure to target new accounts, exposing potential new victims to the Phosphorus defendants' malicious activities.

32. The Phosphorus defendants' techniques are designed to resist technical mitigation efforts, eliminating easy technical means to curb the injury being caused. For example, once domains in the Phosphorus defendants' active infrastructure become known to the security community, the defendants abandon that infrastructure and move to new infrastructure that is used to continue the Phosphorus defendants' efforts to compromise accounts of new victims. For this reason, providing notice to the Phosphorus defendants in advance of redirection of the domains at issue would render attempts to disable the infrastructure futile. Further, when the Phosphorus defendants become aware of efforts to mitigate or investigate their activities, they take steps to conceal their activities and to conceal the injury that has been caused to victims, making it more difficult for victims to adequately assess the damage or take steps to mitigate that injury going forward. For this reason as well, providing notice to the Phosphorus defendants in advance of redirection of the domains at issue would render attempts to mitigate the harm futile, or at least much more difficult for Microsoft. Piecemeal requests to disable these domains, informal dispute resolution or notice to the defendants prior to redirecting the domains would be insufficient to curb the injury. Based on my experience observing the operation of numerous intrusions such as those carried out by the Phosphorus defendants, and prior investigations and legal actions involving such intrusions and actors, I believe that the Phosphorus defendants would take swift preemptive action to conceal the extent of the victimization of Microsoft and its customers and to defend their infrastructure, if they were to learn of Microsoft's impending action and request for relief.

33. I am informed and believe there have been prior instances where security researchers or the government attempted to curb injury caused by actors carrying out intrusions such as those in this case, but allowed those actors to receive notice. In these cases, the actors quickly concealed the scope and nature of their intrusion, and moved the infrastructure to new, unidentified locations on the Internet and took other countermeasures causing the actors to continue their operations and destroying or concealing evidence of their operations. Indeed, CERTFA published a report on this actor group on December 13, 2018 (**Exhibit 4**). Subsequent

to that report, the control panel cited in **Figures 8** through **10** was updated to require authentication. For all of these reasons, I believe that the only way to mitigate injury and disrupt the most recent, active Phosphorus infrastructure, is to redirect the domains at issue prior to providing notice to the defendants.

34. I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge. Executed this 13TH day of MARCH, 2019.

David E. Anselmi

EXHIBIT 1

SPECIAL REPORT

FireEye

OPERATION SAFFRON ROSE

2013

Authors: Nart Villeneuve, Ned Moran, Thoufique Haq and Mike Scott

SECURITY REIMAGINED

CONTENTS

We believe we're seeing an evolution and development in Iranian-based cyber activity. In years past, Iranian actors primarily committed politically-motivated website defacement and DDoS attacks.[1] More recently, however, suspected Iranian actors have destroyed data on thousands of computers with the Shamoon virus,[2] and they have penetrated the Navy Marine Corps Intranet (NMCI), which is used by the U.S. Navy worldwide.[3]

In this report, we document the activities of the Ajax Security Team, a hacking group believed to be operating from Iran. Members of this group have accounts on popular Iranian hacker forums such as ashiyane[.]org and shabgard[.]org, and they have engaged in website defacements under the group name "AjaxTM" since 2010. By 2014, the Ajax Security Team had transitioned from performing defacements (their last defacement was in December 2013) to malware-based espionage, using a methodology consistent with other advanced persistent threat actors in this region.

It is unclear if the Ajax Security Team operates in isolation or if they are a part of a larger coordinated effort. The Ajax Security Team itself uses malware tools that do not appear to be publicly available. We have seen this group leverage varied social engineering tactics as a means to lure their targets into infecting themselves with malware. Although we have not observed the use of exploits as a means to infect victims, members of the Ajax Security Team have previously used publicly available exploit code in web site defacement operations.

In sum, FireEye has recently observed the Ajax Security Team conducting multiple cyber espionage operations against companies in the defense industrial base (DIB) within the Unites States, as well as targeting local Iranian users of anti-censorship technologies that bypass Iran's Internet filtering system.

Background

The transition from patriotic hacking to cyber espionage is not an uncommon phenomenon. It typically follows an increasing politicization within the hacking community, particularly around geopolitical events. This is followed by increasing links between the hacking community and the state, particularly military and/or intelligence organizations.

In the late 1990's and early 2000's, a similar transition occurred within the Chinese hacking community. During that time period, the Chinese hacking community engaged in website defacements and denial of service attacks in conjunction with incidents such as the accidental bombing of the Chinese embassy in Belgrade in 1999, the collision of a U.S. spy plane and a Chinese military plane in 2001, and the Japanese Prime Minister's controversial visit to the Yasukuni shrine in 2005.[4] Around this time a significant shift in philosophy began to take place.

Members of the Chinese hacking community that participated in such attacks soon found that transitioning to cyber espionage was more rewarding—both in terms of developing a more advanced skill set as well as in monetary remuneration. One group known as NCPH (Network Crack Program Hacker), whose founding member "Wicked/Withered Rose" was a patriotic hacker, made the transition to cyber espionage by founding a "hacker-for-hire" group

1 HP Security Research. "Threat Intelligence Briefing Episode 11". February 2014.

2 Perlroth, N. "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back". October 2012.

3 Gallagher, S. "Iranians hacked Navy network for four months? Not a surprise". February 2014.

4 Key. "Honker Union of China to launch network attacks against Japan is a rumor". September 2010.

that simultaneously developed an association with the Chinese military.[5] The group began developing zero-day exploits, rootkits and remote access tools (RATs)—using them in attacks against a variety of targets including the U.S. Department of Defense.[6] (One of this group's associates, "whg", is still active and is believed to have developed one variant of the PlugX/SOGU malware.[7]) The rationale behind this transition within the Chinese hacking community is nicely summed up in a message by the "Honker Union of China" to its members in 2010:

What benefit can hacking a Web page bring our country and the people? It is only a form of emotional catharsis, please do not launch any pointless attacks, the real attack is to fatally damage their network or gain access to their sensitive information.[8]

In Iran, the hacking community appears to be undergoing a similar transformation. While a variety of Iranian hacker groups had engaged in politically motivated website defacements, the emergence of the "Iranian Cyber Army" in 2009 demonstrated "a concentrated effort to promote the Iranian government's political narrative online".[9] They targeted, among others, news organizations, opposition websites and social media.[10] This marked the beginning of a large-scale cyber offensive against the perceived enemies of the Iranian government.

Foreign news and opposition websites are routinely blocked in Iran, as are the tools that allow users in Iran to bypass these restrictions.[11] One of the key stakeholders in Iran's Internet censorship program is the Iranian Revolutionary Guard Corps (IRGC), under which the Basij paramilitary organization operates.

The Basij formed the Basij Cyber Council and actively recruits hackers in order to develop both defensive and offensive cyber capabilities.[12] There is increasing evidence to suggest that the hacker community in Iran is engaged in a transition from politically motivated defacements and denial of service attacks to cyber espionage activities. This model is consistent with the Basij's recruitment of paramilitary volunteer hackers to "engage in less complex hacking or infiltration operations" leaving the more technical operations to entities over which they have increasingly direct control.[13]

As such, the capabilities of threat actors operating from Iran have traditionally been considered limited.[14] However, the "Shamoon" attacks, which wiped computers in Saudi Arabia and Qatar, indicate an improvement in capabilities.[15] And unsurprisingly, Iran has reportedly increased its efforts to improve offensive capabilities after being targeted by Stuxnet and Flame.[16]

5 Elegant, S. "Enemies at The Firewall". December 2007. Dunham, K. & Melnick, J. "'Wicked Rose' and the NCPH Hacking Group". Wikipedia. "Network Crack Program Hacker Group".

6 Dunham, K. & Melnick, J. "'Wicked Rose' and the NCPH Hacking Group".

7 Blasco, J. "The connection between the Plugx Chinese gang and the latest Internet Explorer Zeroday". September 2012.

8 Key. "Honker Union of China to launch network attacks against Japan is a rumor". September 2010.

9 OpenNet Initiative. "After the Green Movement: Internet Controls in Iran 2009 – 2012". February 2013.

10 Rezvaniyeh, F. "Pulling the Strings of the Net: Iran's Cyber Army". February 2010. "Twitter hackers appear to be Shiite group". December 2009.

11 OpenNet Initiative. "Iran". June 2009.

12 The IRGC has also indicated that they would welcome hackers that support the Iranian government. Esfandiari, G. "Iran Says It Welcomes Hackers Who Work For Islamic Republic". March 2011. HP Security Research. "Threat Intelligence Briefing Episode 11". February 2014.

13 BBC Persian. "Structure of Iran's Cyber Warfare".

14 Mandiant. "M-Trends: Beyond the Breach, 2014", page 9. April 2014.

15 Mount, M. "U.S. Officials believe Iran behind recent cyber attacks". October 2012.

16 Shalal-Esa, A. "Iran strengthened cyber capabilities after Stuxnet: U.S. general". January 2013. Lim, K. "Iran's cyber posture". November 2013.

Attack Vectors

We have observed the Ajax Security Team use a variety of vectors to lure targets into installing malicious software and/or revealing login credentials. These attack vectors include sending email, private messages via social media, fake login pages, and the propagation of anti-censorship software that has been infected with malware.

Spear phishing

During our investigation, we discovered that these attackers sent targeted emails, as well as private messages through social media. For example, the attackers targeted companies in the DIB using a fake conference page as a lure to trick targets into installing malicious software. The attackers registered the domain "aeroconf2014[.]org" in order to impersonate the IEEE Aerospace conference—the conference's actual domain is aeroconf.org—and sent out an email with the following information:

From: invite@aeroconf2014[.]org
Subject: IEEE Aerospace Conference 2014

The email encouraged users to visit a fake conference website owned by the attackers:

Upon visiting the website, visitors were notified that they must install "proxy" software in order to access it, which is actually malware.

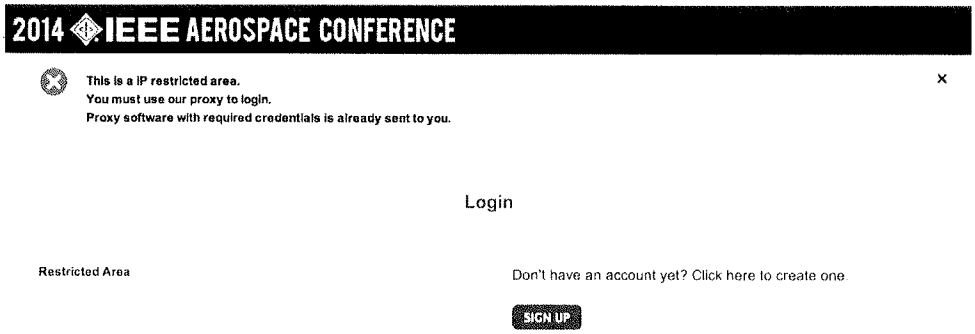


Figure 1: The Fake IEEE Aerospace Conference Website

[7] Bloomberg, "Neiman Marcus Hackers Set Off 60,000 Alerts While Bagging Credit Card Data," February 2014.

Credential Phishing

The attackers have also used phishing attacks, in which they set up Web pages to emulate various services that require security credentials. The attackers tailored these login pages for specific targets in the DIB and spoofed a variety of services such as Outlook Web Access and VPN login pages.

If users attempt to login through these fake Web pages, the attackers collect their login credentials.

Anti-censorship Tools

All Internet Service Providers (ISPs) in Iran are required to implement filtering technology that censors access to content which the Iranian government deems unacceptable.[17] This content includes categories such as pornography and political opposition.[18] In response to these restrictions, Iranians have been increasingly using software that bypasses such filtering technology.

To counter anti-censorship efforts, Iran has attempted to block the use of certain software tools.[19] In 2012, researchers found that an anti-censorship tool that is primarily used by Internet users in Iran was bundled with malware and redistributed.[20]

Our investigation found that malware-laden versions of legitimate anti-censorship software, such as Psiphon and Ultrasurf, were distributed to users Iran and Persian speaking people around the world.

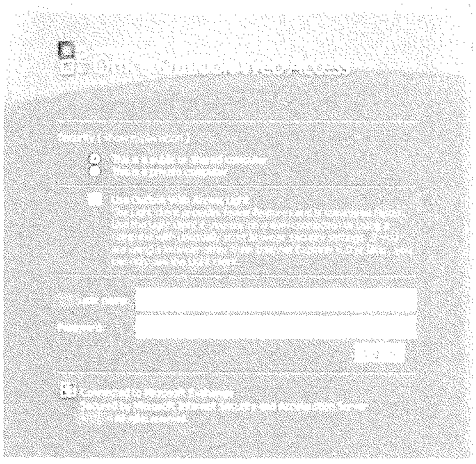


Figure 2: The Fake Outlook Web Access page

17 OpenNet Initiative. "Iran". June 2009.

18 OpenNet Initiative. "After the Green Movement: Internet Controls in Iran 2009 – 2012". February 2013.

19 Torbati, Y. "Iran blocks use of tool to get around Internet filter". March 2013.

20 Marquis-Boire, M. "Iranian anti-censorship software 'Simurgh' circulated with malicious backdoor". May 2012.

The "Stealer" Malware

Host-based Indicators and Malware Functionality

We have observed the Ajax Security Team use a malware family that they identify simply as 'Stealer'. They deliver this malware as a malicious executable (dropper). The executable is a CAB extractor that drops the implant IntelRS.exe. This implant, in turn, drops various other components into C:\Documents and Settings\{USER}\Application Data\IntelRapidStart\. The following files are written to disk in this location:

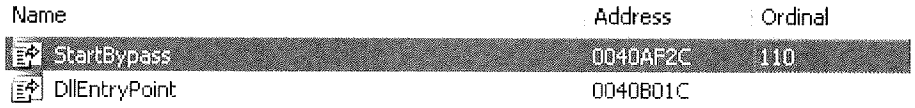
The IntelRS.exe is written in .NET and is aptly named "Stealer", as it has various data collection modules. It drops and launches AppTransferWiz.dll via the following command:

"C:\WINDOWS\system32\rundll32.exe" "C:\Documents and Settings\{USER}\Application

Data\IntelRapidStart\AppTransferWiz.dll",#110

110 is an ordinal that corresponds to "StartBypass" export in AppTransferWiz.dll.

File	Functionality
IntelRS.exe	Various stealer components and encryption implementation
DelphiNative.dll	Browser URL extraction, IE Accounts, RDP accounts (Imported by IntelRS.exe)
IntelRS.exe.config	Config containing supported .NET versions for IntelRS.exe
AppTransferWiz.dll	FTP exfiltration (Launched by IntelRS.exe)
RapidStartTech.stl	Base64 encoded config block containing FTP credentials, implant name, decoy name, screenshot interval and booleans for startup, keylogger and screenshot



Name	Address	Ordinal
StartBypass	0040AF2C	110
DllEntryPoint	0040B01C	

Figure 3: StartBypass Ordinal

Data exfiltration is conducted over FTP by AppTransferWiz.dll, which acts as an FTP client. This DLL is written in Delphi. There is code to exfiltrate data over HTTP POST as well, but it is unused. We also found incomplete code that would perform SFTP and SMTP exfiltration, which could be completed in a future version.

State is maintained between the stealer component IntelRS.exe and the FTP component AppTransferWiz.DLL using a file from the FTP server "sqlite3.dll", as well as a global atom "SQLiteFinish". IntelRS.exe waits in an indefinite loop, until AppTransferWiz.DLL defines this state.

Once the state is set, IntelRS.exe proceeds to collect data from various areas in the system as described below:

- Collects system information: hostname, username, timezone, IP addresses, open ports, installed applications, running processes, etc.
- Performs key logging
- Takes various screenshots
- Harvests instant messaging (IM) account information: GTalk, Pidgin, Yahoo, Skype
- Tracks credentials, bookmarks and history from major browsers: Chrome, Firefox, Opera
- Collects email account information
- Extracts installed proxy software configuration information
- Harvests data from installed cookies

IntelRS.exe loads a Delphi component called DelphiNative.DLL, which implements some additional data theft functionality for the following:

- Internet Explorer (IE) accounts
- Remote Desktop Protocol (RDP) accounts
- Browser URLs

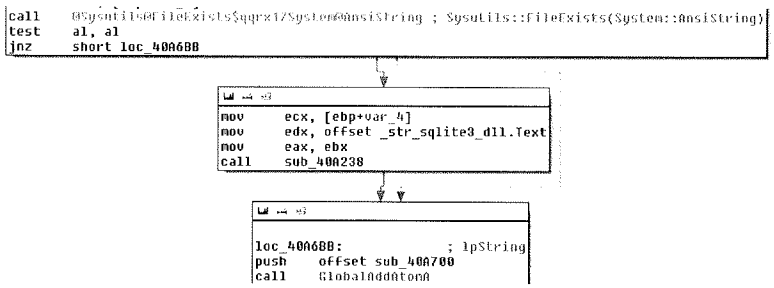


Figure 4: AppTransferWizard.dll creates sqlite3.dll and global atom

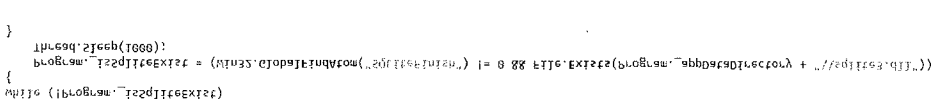


Figure 5: IntelRS.exe sleeps until global atom is set and sqlite3.dll is present

FireEye

The Stealer component uses common techniques to acquire credential data. For instance, it loads vaultcli.DLL and uses various APIs shown below to acquire RDP accounts from the Windows vault.

Harvested data is encrypted and written to disk on the local host. The filenames for these encrypted files follow this naming scheme:

{stolen data type}_{victim system name}_YYYYMMDD_HHMM.Enc

The {stolen data type} parameter indicates where the data was harvested from (e.g., a Web browser, an instant messenger application, installed proxy software).

Analysis of the malware indicates that the data is encrypted via a Rijndael cipher implementation; more specifically it uses AES which is a specific set of configurations of Rijndael. It uses a key size of 256 bytes and block size of 128 bytes, which conforms to the FIPS-197 specification of AES-256.[21] It utilizes the passphrase 'HavijeBaba' and a salt of 'salam!*%#' as an input to PBKDF2 (Password-Based Key Derivation Function 2) to derive the key and initialization vector for the encryption.[22] This key derivation implementation in .NET is done using the Rfc2898DeriveBytes class.[23] The passphrase and salt are Persian language words. "Havij" means "carrot", "Baba" means "father", and "Salam" is a common greeting that means "Peace".

Figure 6: Acquiring RDP Accounts

```
CODE:0040916D loc_40916D:                                ; CODE XREF: GetRDPAccounts+55↑j
CODE:0040916D                 push    offset aVaultenumerate ; "VaultEnumerateVaults"
CODE:00409172                 push    ebx             ; hModule
CODE:00409173                 call    GetProcAddress_0
CODE:00409178                 mov     [ebp+var_8], eax
CODE:0040917B                 push    offset aVaultopenvault ; "VaultOpenVault"
CODE:00409180                 push    ebx             ; hModule
CODE:00409181                 call    GetProcAddress_0
CODE:00409186                 mov     [ebp+var_C], eax
CODE:00409189                 push    offset aVaultclosevaul ; "VaultCloseVault"
CODE:0040918E                 push    ebx             ; hModule
CODE:0040918F                 call    GetProcAddress_0
CODE:00409194                 mov     [ebp+var_10], eax
CODE:00409197                 push    offset aVaultenumera_0 ; "VaultEnumerateItems"
CODE:0040919C                 push    ebx             ; hModule
CODE:0040919D                 call    GetProcAddress_0
CODE:004091A2                 mov     [ebp+var_14], eax
CODE:004091A5                 push    offset aVaultgetitem ; "VaultGetItem"
CODE:004091AA                 push    ebx             ; hModule
CODE:004091AB                 call    GetProcAddress_0
CODE:004091B0                 mov     [ebp+var_18], eax
CODE:004091B3                 push    offset aVaultgetitem ; "VaultGetItem"
CODE:004091B8                 push    ebx             ; hModule
CODE:004091B9                 call    GetProcAddress_0
CODE:004091BE                 mov     [ebp+var_1C], eax
CODE:004091C1                 push    offset aVaultfree ; "VaultFree"
```

[21] ShawnFa. "The Differences Between Rijndael and AES". October 2006.

[22] Wikipedia. "PBKDF2".

[23] Microsoft. "Rfc2898DeriveBytes Class".

Sample Timeline

We identified 17 droppers during this research, including:

- 9 samples compiled on 2013-02-17 07:00
- 4 samples compiled on 2009-07-13 23:42
- 3 sample compiled on 2013-10-14 06:48
- 1 sample compiled on 2013-10-13 09:56

The 2009 compile time appears to have been forged, while the 2013 compile times may be legitimate.

In some cases, we found an implant but not the parent dropper. In total, 22 of the 23 implants that we identified during our research had unique compile times ranging from 2013-10-29 until 2014-03-15. We identified two implants that were both compiled on 2014-3-15 at 23:16. These compile times appear to be legitimate and coincide with attempted intrusion activity attributed to these attackers.

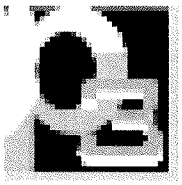
Spoofed Installers

Many of the malicious executables (droppers) that we collected were bundled with legitimate installers for VPN or proxy software. Examples include:

- 6dc7cc33a3cdcfee6c4edb6c085b869d was bundled with an installer for Ultrasurf Proxy software.
- 3d26442f06b34df3d5921f89bf680ee9 was bundled with an installer for Gerdoovpn virtual private network software.
- 3efd971db6fbae08e96535478888cff9 was bundled with an installer for the Psiphon proxy.
- 288c91d6c0197e99b92c06496921bf2f was bundled with an installer for Proxifier software.

These droppers were also designed to visually spoof the appearance of the above applications. These droppers contained icons used in the legitimate installers for these programs.

Figure 7: Icon for the Psiphon Anti-censorship Tool



Process Debug (PDB) Strings

Analysis of the PDB strings seen in the implants indicates that there may be more than one developer working on the source code for the Stealer builder. The following two PDB paths were seen in the collection of implants that we collected:

- d:\svn\Stealer\source\Stealer\Stealer\obj\x86\Release\Stealer.pdb
- f:\Projects\C#\Stealer\source\Stealer\Stealer\obj\x86\Release\Stealer.pdb

These strings indicate that the Stealer source code was stored in two different paths but not necessarily on two different computers. The f:\Projects\ path may be from an external storage device such as a thumb drive. It is therefore possible that only one person has access to the source code, but keeps a separate repository on an external storage device. Alternatively, the different file paths could be the result of two different actors storing their source code in two different locations.

Builder Artifacts

In nine of the implants that we collected, we found a consistent portable executable (PE) resource with a SHA256 of 5156aca994ecfcb40458ead8c830cd66469d5f5a031392898d323a8d7a7f23d3. This PE resource contains the VS_VERSION_INFO. In layman's terms, this can best be described as the metadata describing the executable file. This specific PE resource contained the following information:

```
VS_VERSION_INFO
VarFileInfo
Translation
StringFileInfo
000004b0
Comments
Process for Windows
CompanyName
Microsoft
FileDescription
Process for Windows
FileVersion
1.0.0.0
InternalName
Stealer.exe
LegalCopyright
Copyright
   2013
OriginalFilename
Stealer.exe
ProductName
Process for Windows
ProductVersion
1.0.0.0
Assembly Version
1.0.0.0
```

Note the InternalName of 'Stealer.exe'. This is the attackers' name for this malware family.

The "Stealer" Builder and Tools

During our research, we recovered two different tools used by the members of the Ajax Security Team in conjunction with targeted intrusion activities. The first tool, labeled the 'Stealer Builder' was compiled on 2014-04-08. This compile date may indicate that the group is still active.

Upon executing the 'Stealer Builder' the user is presented with an option to load the 'Builder' or to 'Decrypt' logs generated from a victim and exfiltrated to a command-and-control (CnC) server under the groups' control.

The Builder option enables an attacker to configure a new Stealer backdoor. The user can configure the new backdoor to connect to a specific CnC server with a personalized username and password. The attacker can bind the backdoor to a legitimate application of his or her choosing, or they can cloak it with an icon designed to make the backdoor appear as though it is a legitimate file. We also noted that the Builder did not allow the attacker to select a new passphrase or salt used to encrypt the stolen data. The passphrase 'HavijeBaba' and a salt of 'salam!*%#' are both hardcoded into the builder.

Figure 8: The Stealer Tool

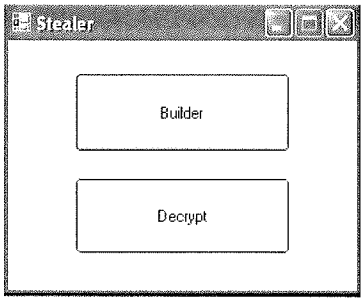
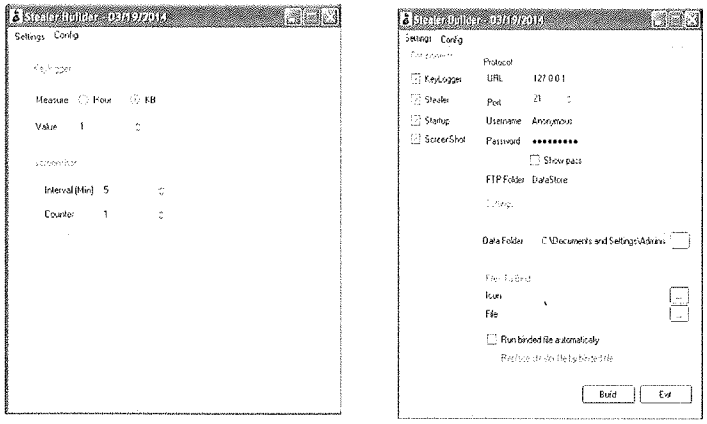


Figure 9: The Stealer Builder



FireEye

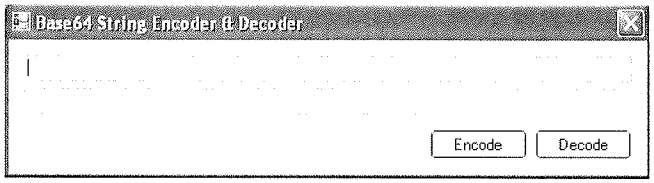
During testing, we observed that backdoors generated by this Stealer Builder had a timestamp of 2013-12-19. We had one backdoor in our repository with this same timestamp. This sample

(MD5 1823b77b9ee6296a8b997ffb64d32d21) was configured to exfiltrate data to ultrasms[.]ir. The VS_VERSION_INFO PE resource mentioned above (SHA256 5156aca994ecfcb40458ead8c830cd66469d5f5a031392898d323a8d7a7f23d3) is an artifact of the Stealer builder that we recovered. The builder generates an executable named IntelRapidStart.exe. This executable contains the aforementioned VS_VERSION_INFO PE resource.

We also recovered a tool designed to encode plaintext into Base64 encoded text or decode Base64 encoded text into plaintext. Members of the Ajax Security Team likely this use tool to encode the configuration data seen in RapidStartTech.stl files. As noted above, the RapidStartTech.stl contains the backdoor's FTP credentials, implant name, decoy name, and screenshot interval, along with boolean settings for startup, keylogger, and screenshot plugins.

Encoding and decoding Base64 data is a straightforward task and the standard Linux operating system offers a number of command line tools to achieve this task. The presence of a Windows-based GUI tool that simplifies encoding and decoding Base64 data indicates that these tools may have been developed for less adept users.

Figure 10: Base64 Encoder



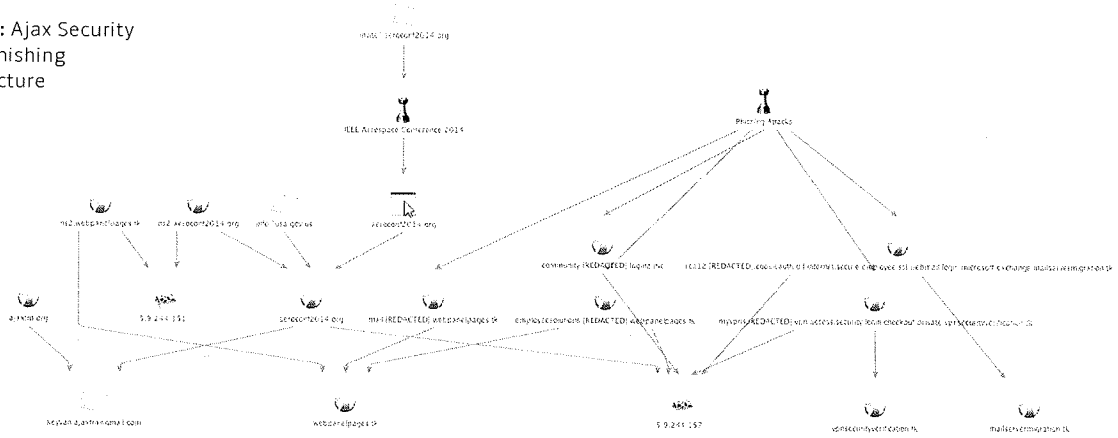
Command-and-Control Infrastructure

The CnC infrastructure consists of distinct, but linked, clusters that have targeted both the users of anti-censorship tools in Iran as well as defense contractor companies in the U.S.

The first cluster contains the domain used in the Aerospace Conference attack as well as the domains used in phishing attacks designed to capture user credentials:

The website used in the Aerospace Conference attack was aeroconf2014[.]org, which is registered to info@usa.gov[.]us. However, historical WHOIS information shows that the domain was registered by keyvan.ajaxtm@gmail[.]com—the same domain used to register ajaxtm[.]org, the website of the Ajax Security Team. The same email addresses were used to register variations of domain names associated with popular services provided by companies such as Google, Facebook, Yahoo and LinkedIn.

Figure 11: Ajax Security Team's Phishing Infrastructure



FireEye

The second cluster comprises the CnC infrastructure used in the anti-censorship attacks. The majority of the samples we analyzed connect to intel-update[.]com and update-mirror[.]com, which were registered by james.mateo@aim[.]com. The domain intel-update[.]com resolved to the IP address 88.150.227.197, which also hosted domains registered by osshom@yahoo[.]com, many of which are consistent with the pattern of registering domains with associations to Google and Yahoo services. We also observed crossover with a sample that connected to both intel-update[.]com and ultrasms[.]ir, which was registered by lvlr98@gmail[.]com.

Figure 12: Ajax Security Team's Stealer CnC Infrastructure

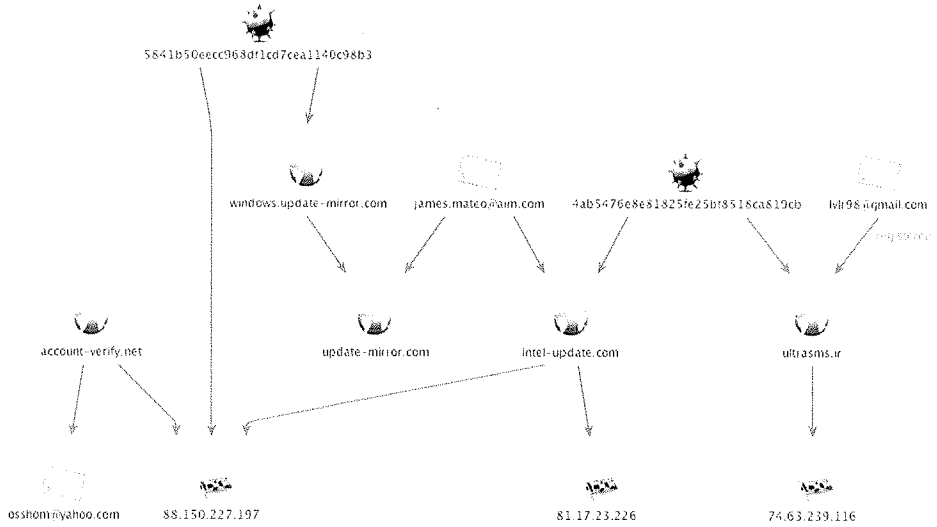
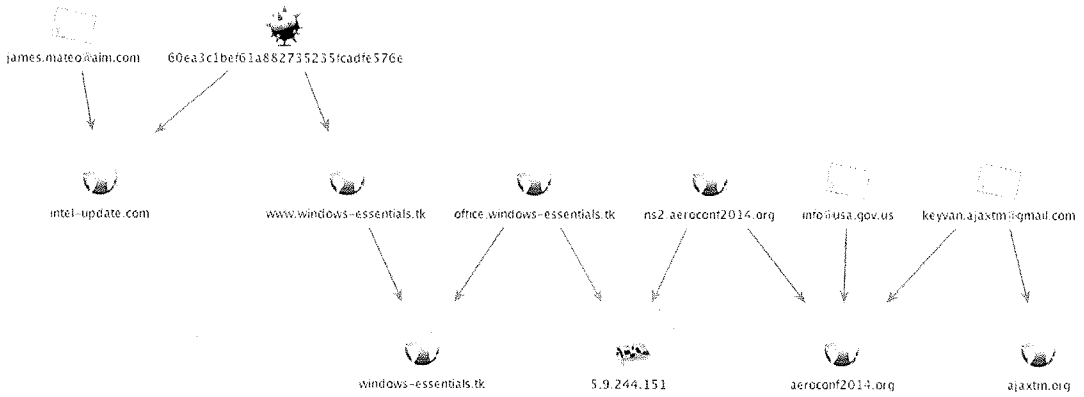


Figure 13: Overlap between the phishing and stealer clusters



FireEye

These two clusters are linked by a common IP address (5.9.244.151), which is used by both ns2.aeroconf2014[.]org and office.windows-essentials[.]tk.

A third cluster of activity was found via analysis of 1d4d9f6e6fa1a07cb0a66a9ee06d624a. This sample is a Stealer variant that connects to the aforementioned intel-update[.]com as well as plugin-adobe[.]com. The domain plugin-adobe[.]com resolved to 81.17.28.235. Other domains seen resolving to IP address nearby include the following:

Aside from the sample connecting to plugin-adobe[.]com, we have not discovered any malware connecting to these domains.

Victimology

During our investigation, we were able to recover information on 77 victims from one CnC server that we discovered while analyzing malware samples that were disguised as anti-censorship tools. While analyzing the data from the victims, we found that the majority had either their timezone set to "Iran Standard Time" or had their language setting set to Persian:

- 44 had their timezone set to "Iran Standard Time" (37 of those also have their language set to Persian)
- Of the remaining 33, 10 have Persian language settings
- 12 have either Proxifier or Psiphon installed or running (all 12 had a Persian language setting and all but one had their timezone set to "Iran Standard Time")

The largest concentration of victims is in Iran, based on the premise that Persian language settings and "Iran Standard Time" correlate the victim to be geographically located in Iran. As such, we believe that attackers disguised malware as anti-censorship tools in order to target the users of such tools inside Iran as well as Iranian dissidents outside the country.

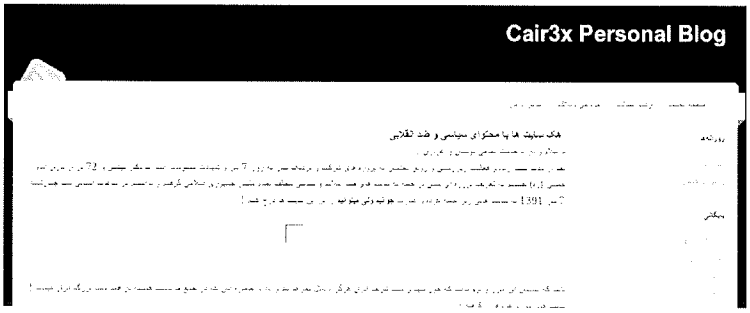
Domain	IP	First Seen	Last Seen
yahoomail.com.co	81.17.28.227	2013-11-28	2014-4-10
privacy-google.com	81.17.28.229	2014-02-14	2014-02-23
xn--google-yri.com	81.17.28.229	2013-12-08	2014-01-15
appleid.com.co	81.17.28.231	2014-02-20	2014-02-20
accounts-apple.com	81.17.28.231	2013-12-31	2014-02-20
users-facebook.com	81.17.28.231	2014-01-15	2014-01-15
xn--facebook-06k.com	81.17.28.231	2013-11-27	2014-03-07

Attribution

The Ajax Security Team appears to have been formed by personas named "HUrr!c4nE!" and "Cair3x" in 2010.[24] Both members were engaged in website defacements prior to the forming of the Ajax Security Team, and both were members of Iranian hacker forums such as ashiyane[.]org and shabgard[.]org. Other members include "0day", "Mohammad PK" and "Crim3r". The Ajax Security Team website at ajaxtm[.]org had a Web forum with at least 236 members. The group published several exploits for content management systems and engaged in defacements.[25] Initially, the defacements seemed to be motivated by a desire to demonstrate the group's prowess—they even defaced an Iranian government website.[26]

However, the group appears to have become increasingly political. For example, in a blog post in 2012, "Cair3x" announced the targeting of Iran's political opponents.

Figure 14: Cair3x's original blog post and translation



Hacking anti-revolution political and opposition websites

Hello to everyone, After a while of operating underground and enhancing our company's projects and getting close to 24 June 2012, and the martyrdom of Ayatollah Dr. Beheshti and 72 of Imam Khomeini's (First and Former supreme leader of Iran) followers, we have planned a project/ initiative to attack anti-revolution and political websites against the Islamic Republic. And in late hours of Wednesday, June 24, 2012, we attacked these websites and defaced them by writing the words "We are young but we can" on their websites. This is so the enemies of this country know that the blood of our martyr will never be in vain and they will always be remembered in the heart of gallant Iranians.

[24] By March 2010 HUrr!c4nE! was identifying as a member of Ajax Security Team in exploit releases http://www.exploit-db.com/exploits/17011/ and the first defacement archived by Zone-H, which lists both HUrr!c4nE! and Cair3x as members was December 2010 http://www.zone-h.org/mirror/id/12730879

[25] http://osvdb.org/affiliations/1768-ajax-security-team http://www.exploit-db.com/author/?a=3223 http://packetstormsecurity.com/files/author/9928/

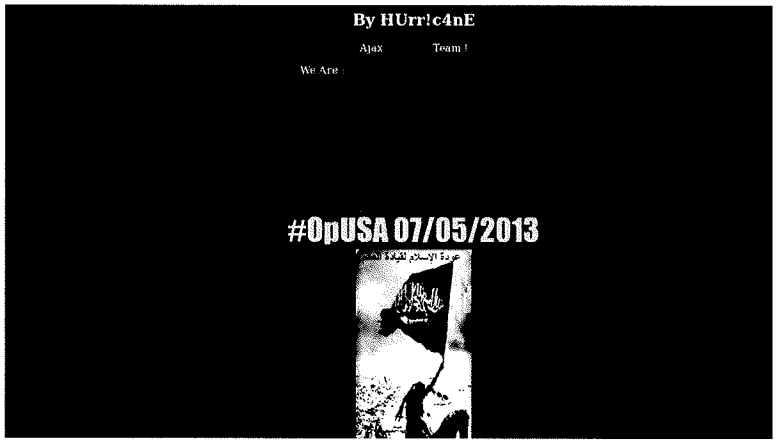
[26] http://www.zone-h.org/mirror/id/13225183

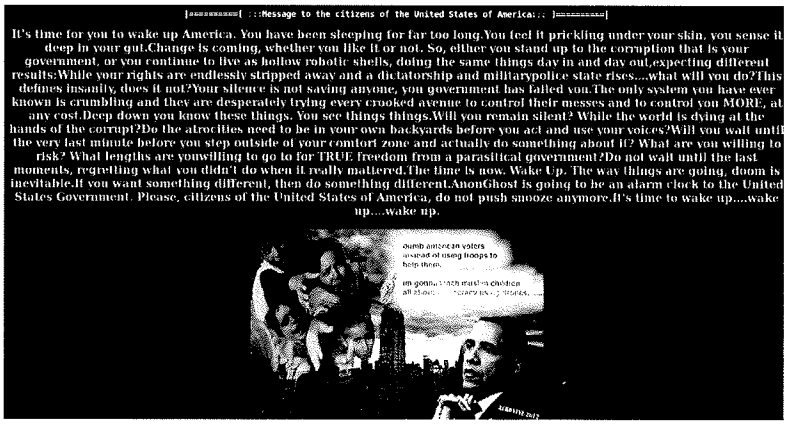
In 2013, the Ajax Security Team, and "HUrr!c4nE!" in particular, took part in "#OpIsrael" and "#OpUSA".27

By early 2014, the Ajax Security Team appears to have dwindled. There have been no defacements since December 2013. The website and forum at ajaxtm[.]org operated by "HUrr!c4nE!", aka "k3yv4n", is no longer active.

"HUrr!c4nE!" has the most open/documented Internet persona of the Ajax Security Team. He registered the ajaxtm[.]org domain name using the email address keyvan.ajaxtm@gmail[.]com. This was also the email address used to register the domain aerospace2014[.]org, which was used in spear phishing attacks against companies in the U.S. and is linked with malware activity directed at users of anti-censorship tools in Iran.

Figure 15: Screenshot of the defacement content used in #OpUSA





27 Ashraf, N. "#OpIsrael: Hacktivists Starting Cyber Attack against Israel on 7th of April". March 2013. "OpUSA Targeting Government & Financial Sectors on 07 May 2013: Likely Tools, Targets and Mitigating Measures". May 2013.

"HUrr!c4nE!" features prominently in all the group's activities and defacements. Although there has been a decline in public-facing Ajax Security Team activity, this coincides with an increase in malware activity linked to the group's infrastructure.

- ~2009—Membership in ashiyane.org and shabgard.org forums

- 2010 – 2012—Defacements, Release of exploits for CMS

- 2012 – 2013—Increasing politicization, participation on #OpIsrael, #OpUSA

- 2013 – 2014—Transition to cyber-espionage

The increasing politicization of the Ajax Security Team aligns with the timing of their activities against the perceived enemies of Iran. In addition to attacking companies in the U.S., they have targeted domestic users of anti-censorship technology.

While the objectives of this group are consistent with Iran's efforts at controlling political dissent and expanding offensive cyber capabilities, the relationship between this group and the Iranian government remains inconclusive.

For example, the Ajax Security Team could just be using anti-censorship tools as a lure because they are popular in Iran, in order to engage in activities that would be considered traditional cybercrime. In one case, "HUrr!c4nE!", using the email address keyvan.ajaxtm@gmail[.]com, has been flagged for possible fraud by an online retailer. While "HUrr!c4nE!" is engaged in operations that align with Iran's political objectives, he may also be dabbling in traditional cybercrime.

This indicates that there is a considerable grey area between the cyber espionage capabilities of Iran's hacker groups and any direct Iranian government or military involvement.

On the spectrum of state responsibility, these attacks align with state-encouraged attacks, which are defined as attacks in which:

Third parties control and conduct the attack, but the national government encourages them as a matter of policy.[28]

Recruiting hackers through this model allows Iran to influence their activities, and provides the Iranian government plausible deniability, but a lack of direct control also means that the groups may be unpredictable and engage in unsanctioned attacks.

Figure 16: Screenshot of an online retailer's fraud alert

OrderID	Customers ID	IP	E-mail	Shipping Address & ZIP	Customer Name	CC number	Payment Method	Expiration Date	Source	Created
110217MYSJ93	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

[28] Healey, J. "Beyond Attribution: Seeking National Responsibility for Cyber Attacks". January 2012.

Conclusion

The increased politicization of the Ajax Security Team, and the transition from nuisance defacements to operations against internal dissidents and foreign targets, coincides with moves by Iran aimed at increasing offensive cyber capabilities. While the relationship between actors such as the Ajax Security Team and the Iranian government is unknown, their activities appear to align with Iranian government political objectives.

The capabilities of the Ajax Security Team remain unclear. This group uses at least one malware family that is not publicly available. We have not directly observed the Ajax Security Team use exploits to deliver malware, but it is unclear if they or other Iranian actors are capable of producing or acquiring exploit code.

While the Ajax Security Team's capabilities remain unclear, we know that their current operations have been somewhat successful as measured by the number of victims seen checking into to an Ajax Security Team controlled CnC server. We believe that if these actors continue the current pace of their operations they will improve their capabilities in the mid-term.

About FireEye

FireEye has invented a purpose-built, virtual machine-based security platform that provides real-time threat protection to enterprises and governments worldwide against the next generation of cyber attacks. These highly sophisticated cyber attacks easily circumvent traditional signature-based defenses, such as next-generation firewalls, IPS, anti-virus, and gateways. The FireEye Threat Prevention Platform provides real-time, dynamic threat protection without the use of signatures to protect an organization across the primary threat vectors and across the different stages of an attack life cycle.

The core of the FireEye platform is a virtual execution engine, complemented by dynamic threat intelligence, to identify and block cyber attacks in real time. FireEye has over 1,500 customers across more than 40 countries, including over 100 of the Fortune 500.

We thank Kenneth Geers and Jen Weedon for their support and analysis on these findings.

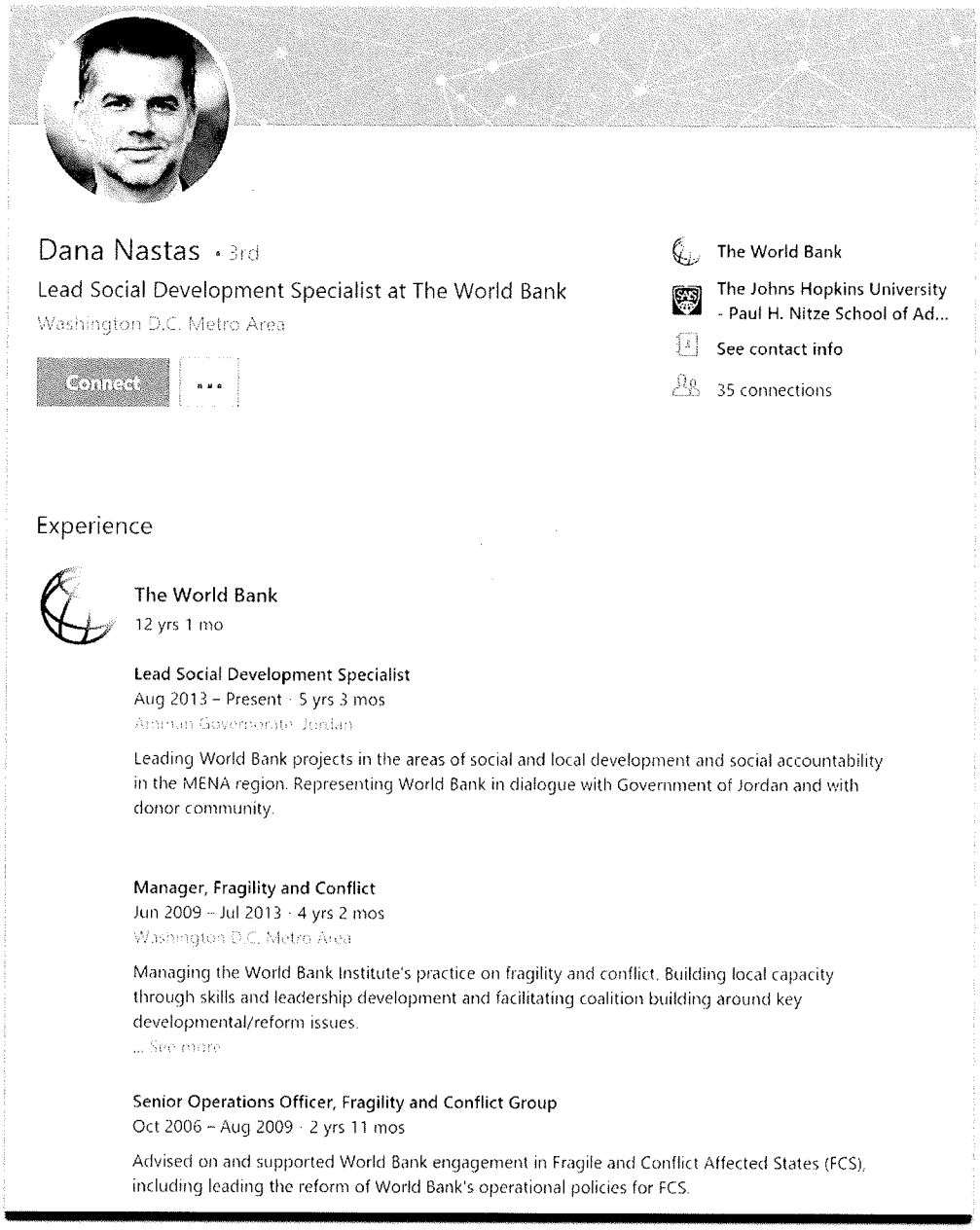
FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**

EXHIBIT 2

Phosphorus Fraudulent LinkedIn Profiles

On 10/02/2018, Microsoft Threat Intelligence Center analysts regarding three potential fake PHOSPHORUS LinkedIn pages. A trusted third party partner noted that several members of their organizations that work on economic sanctions received connection requests to connect from the following profiles.

Suspected Fake Profile #1: www.linkedin[.]com/in/dana-nastas-9a6b85171/



Dana Nastas • 3rd

Lead Social Development Specialist at The World Bank

Washington D.C. Metro Area

Connect

The World Bank

The Johns Hopkins University - Paul H. Nitze School of Ad...

See contact info

35 connections

Experience

The World Bank

12 yrs 1 mo

Lead Social Development Specialist

Aug 2013 – Present · 5 yrs 3 mos

Amman Governorate, Jordan

Leading World Bank projects in the areas of social and local development and social accountability in the MENA region. Representing World Bank in dialogue with Government of Jordan and with donor community.

Manager, Fragility and Conflict

Jun 2009 – Jul 2013 · 4 yrs 2 mos

Washington D.C. Metro Area

Managing the World Bank Institute's practice on fragility and conflict. Building local capacity through skills and leadership development and facilitating coalition building around key developmental/reform issues.

... See more

Senior Operations Officer, Fragility and Conflict Group

Oct 2006 – Aug 2009 · 2 yrs 11 mos

Advised on and supported World Bank engagement in Fragile and Conflict Affected States (FCS), including leading the reform of World Bank's operational policies for FCS.

The fake profile above appears to have been created by taking information from the following real profile:

www.linkedin.com/in/sima-kanaan-a622191b

Sima Kanaan · 3rd

Senior Development Advisor at United Nations High Commisioner for Refugees

Washington D.C. Metro Area

Message ...

United Nations High Commissioner for Refugees

The Johns Hopkins University - Paul H. Nitze School of...

See contact info

500+ connections

Experience

Senior Development Advisor

United Nations High Commissioner for Refugees

Sep 2017 - Present · 1 yr 2 mos

Amman, Jordan

Supporting UNHCR's MENA Director's office and country programs' ongoing efforts to collaborate with development organizations and host countries towards finding and implementing comprehensive and sustainable solutions for refugees

The World Bank

12 yrs 1 mo

Lead Social Development Specialist

Aug 2013 – Present · 5 yrs 3 mos

Amman, Jordan

Leading World Bank projects in the areas of social and local development and social accountability in the MENA region. Representing World Bank in dialogue with Government of Jordan and with donor community.

Manager, Fragility and Conflict

Jun 2009 – Jul 2013 · 4 yrs 2 mos

Washington D.C. Metro Area

Managing the World Bank Institute's practice on fragility and conflict. Building local capacity through skills and leadership development and facilitating coalition building around key developmental/reform issues.

Senior Operations Officer, Fragility and Conflict Group

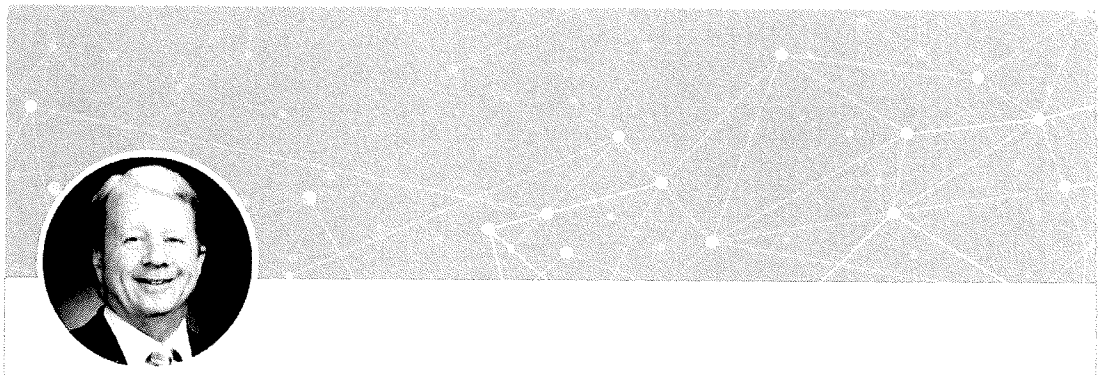
Oct 2006 – Aug 2009 · 2 yrs 11 mos

Advised on and supported World Bank engagement in Fragile and Conflict Affected States (FCS) including leading the reform of World Bank's operational policies for FCS.

Show fewer roles ^

With the exception of the position title used, the exact same verbiage was used in the summary section, experience, education, and interests. The major difference is that Sima Kanaan has over 500+ connections and the suspected fake account for Dana Nastas only had 35 as of 7PM on 10/02/2018.

Suspected Fake Profile #2: www.linkedin[.]com/in/emmanuel-tyler-227b86171/



Emmanuel Tyler • 3rd

Global Lead - Technology, Innovation, & Climate Smart Agriculture, The World Bank Group

Washington D.C. Metro Area

Message ...

The World Bank

North Carolina State University

See contact info

86 connections

Supporting investments in Climate Resilient Agriculture and Natural Resource Management. My work also involves analytical economic and sector studies. I hold a Higher National Certificate (HNC) in Quantitative Biology & Analytical Biochemistry from Hertfordshire University (England), a BSc in Forestry from the University of Aberdeen (Scotland), and a PhD in Soil Science & Agronomy from North Carolina State University (USA). My professional career is dedicated to facilitating global food security, sustainable livelihoods for farmers, and the conservation of natural resources and ecosystems services to ensure the equitable and sustainable development of societies globally. I have 35 years of agriculture and natural resource management experience in Sub-Saharan Africa, East Asia, Latin America, the Middle East and North Africa, and South Asia.

Currently, I am focusing on designing and managing climate resilient landscapes across the World Bank's Agriculture investments portfolio with cross cutting linkages to the Environment, Urban-Rural-Social, and Water investments.

Show less

The fake profile above appears to have been created by taking information from the following real profile:

linkedin.com/in/erickfernandes/

Erick Fernandes • 3rd

Global Lead - Technology, Innovation, & Climate Smart Agriculture, The World Bank Group

Washington D.C. Metro Area

Message

The World Bank

North Carolina State University

See contact info

500+ connections

Supporting investments in Climate Resilient Agriculture and Natural Resource Management. My work also involves analytical economic and sector studies. I hold a Higher National Certificate (HNC) in Quantitative Biology & Analytical Biochemistry from Hertfordshire University (England), a BSc in Forestry from the University of Aberdeen (Scotland), and a PhD in Soil Science & Agronomy from North Carolina State University (USA). My professional career is dedicated to facilitating global food security, sustainable livelihoods for farmers, and the conservation of natural resources and ecosystems services to ensure the equitable and sustainable development of societies globally. I have 35 years of agriculture and natural resource management experience in Sub-Saharan Africa, East Asia, Latin America, the Middle East and North Africa, and South Asia.

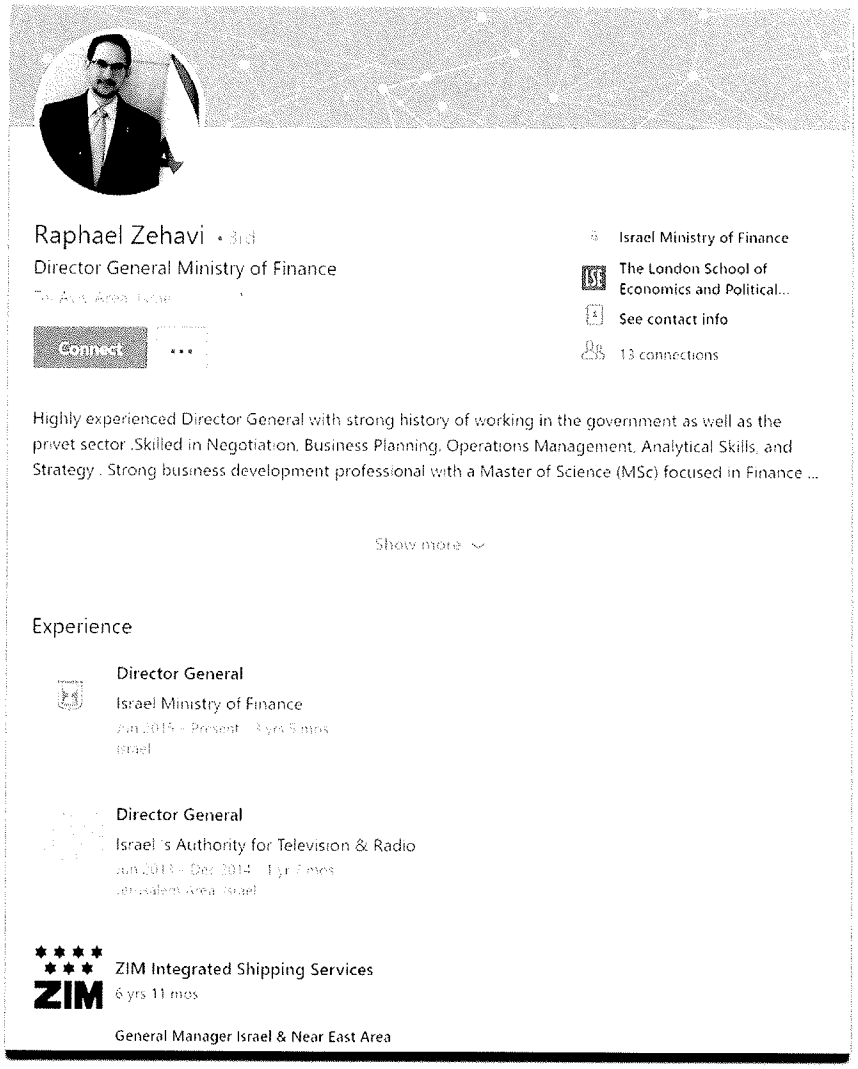
Currently, I am focusing on designing and managing climate resilient landscapes across the World Bank's Agriculture investments portfolio with cross cutting linkages to the Environment, Urban-Rural-Social, and Water investments.

ResearchGate profile

Show less

The exact same verbiage was used in the summary section, experience, education, and interests. The major difference is that Mr. Fernandes has over 500+ connections and the suspected fake account for Emmanuel Tyler only had 86 connections as of 7PM on 10/02/2018.

Suspected Fake Profile #3: https://www.linkedin[.]com/in/raphael-zehavi-23b065172/



The fake profile above appears to have been created by taking information from the following real profile:

https://www.linkedin.com/in/shai-babad-aa19a189/

Shai Babad • 3rd

Director General Ministry of Finance

Israel

Message

Israel Ministry of Finance

The London School of Economics and Political...

See contact info

500+ connections

Highly experienced Director General with strong history of working in the government as well as the privet sector .Skilled in Negotiation, Business Planning, Operations Management, Analytical Skills, and Strategy . Strong business development professional with a Master of Science (MSc) focused in Finance ...

Show more

Experience

Director General

Israel Ministry of Finance

May 2015 – Present · 3 yrs 6 mos

Israel

Director General

Israel 's Authority for Television & Radio

Jun 2013 – Dec 2014 · 1 yr 7 mos

Jerusalem, Israel

ZIM Integrated Shipping Services

6 yrs 11 mos

The exact same verbiage was used in the summary section, experience, education, and interests. The major difference is that Mr. Babad has over 500+ connections and the suspected fake account for Raphael Zehavi only had 13 connections as of 10/3/2018 at 10:00AM.

EXHIBIT 3

APPENDIX A

.ORG DOMAINS

Registry
Public Interest Registry (PIR)
1775 Wiehle Avenue
Suite 200
Reston Virginia 20190
United States

yahoo-verification.org	Domain Administrator Yahoo! Inc. 109 First Sunnyvale CA 94988 BA Phone: +1.4038493301 Fax: +1.4038493302 domainadmin@yahoo-verification.org

.COM, .NET, .NAME DOMAINS

Registry
VeriSign, Inc.
VeriSign Information Services, Inc.
12061 Bluemont Way
Reston Virginia 20190
United States

support-servics.com	Registrant Name: hash crypt Registrant Organization: hashcrypt Registrant Street: nbcj hjf,m Registrant City: losangles Registrant State/Province: Alabama Registrant Postal Code: 35004 Registrant Country: US Registrant Phone: +1.09876543567 Registrant Email: hashcrypt@protonmail.com
verification-live.com	Registrant Name: Domain Administrator Registrant Organization: Microsoft Corporation Registrant Street: AS8068 MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation, Registrant City: toranto Registrant State/Province: toranto Registrant Postal Code: 64043 Registrant Country: UM

	Registrant Phone: +1.6509234001 Registrant Fax: +1.6509234002 Registrant Email: test9179@porotonmail.com
com-mailbox.com	Registrant Name: Priview Service Registrant Organization: mish Registrant Street: No 885, Azar st Registrant City: Dubai Registrant State/Province: Dubai Registrant Postal Code: 98120 Registrant Country: AE Registrant Phone: +97.3218526 Registrant Fax: +97.3218526 Registrant Email: domain.seller2017@yandex.com
com-myaccuants.com	Registrant Name: Domain ID Shield Service Registrant Organization: Domain ID Shield Service CO., Limited Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registrant City: Hong Kong Registrant State/Province: Hong Kong Registrant Postal Code: 999077 Registrant Country: CN Registrant Phone: +852.21581835 Registrant Fax: +852.30197491 Registrant Email: co5940551458104@domainidshield.com
notification-accountservice.com	Registrant Name: mosa alnarjani Registrant Organization: Registrant Street: baqdad, alqusair st , no 246 Registrant City: baqdad Registrant State/Province: baqdad Registrant Postal Code: 548996 Registrant Country: IQ Registrant Phone: +964.7730061463 Registrant Email: meisam.bayat.sector@gmail.com
accounts-web-mail.com	Registrant Name: Domain Administrator Registrant Organization: Yahoo! Inc. Registrant Street: 107 First Avenue Registrant City: Sunnyvale Registrant State/Province: CA Registrant Postal Code: 94989 Registrant Country: US Registrant Phone: +1.4038493300 Registrant Fax: +1.4038493301 Registrant Email: test9179@yahoo.com
customer-certificate.com	Registrant Name: Domain ID Shield Service Registrant Organization: Domain ID Shield Service CO., Limited Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registrant City: Hong Kong

	Registrant State/Province: Hong Kong Registrant Postal Code: 999077 Registrant Country: HK Registrant Phone: +852.21581835 Registrant Fax: +852.30197491 Registrant Email: whoisprivacy@domainidshield.com
session-users-activities.com	Domain ID Shield Service Domain ID Shield Service CO., Limited FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Hong Kong Hong Kong 999077 HK Phone: +852.21581835 Fax: +852.30197491 whoisprivacy@domainidshield.com
user-profile-credentials.com	Domain ID Shield Service Domain ID Shield Service CO., Limited FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Hong Kong Hong Kong 999077 HK Phone: +852.21581835 Fax: +852.30197491 whoisprivacy@domainidshield.com
verify-linke.com	Registrant Name: sora bara Registrant Organization: narabara Registrant Street: ara Registrant City: mara Registrant State/Province: nara Registrant Postal Code: 7482957439 Registrant Country: BI Registrant Phone: +1.234124323 Registrant Fax: +1.2129876243 Registrant Email: test9179@protonmail.com
support-servics.net	Registrant Name: Support Services Inc. Registrant Organization: Support Services Inc. Registrant Street: 1901 Amphitheatre Parkway Registrant City: Mountain View Registrant State/Province: 64043 Registrant Postal Code: 64043 Registrant Country: US Registrant Phone: +1.6509234001 Registrant Fax: +1.6509188572 Registrant Email: test9179@protonmail.com
verify-linkedin.net	Registrant Name: sora bara Registrant Organization: none

	Registrant Street: ara Registrant City: mara Registrant State/Province: nara Registrant Postal Code: 748295743 Registrant Country: BI Registrant Phone: +75.234124323 Registrant Fax: +86.12124321 Registrant Email: dnsadmin@verify-linkedin.com
yahoo-verification.net	Registrant Organization: Yahoo! Inc. Registrant Street: 107 First Avenue Registrant City: Sunnyvale Registrant State/Province: CA Registrant Postal Code: 94989 Registrant Country: BA Registrant Phone: +1.4038493300 Registrant Fax: +1.4038493301 Registrant Email: test9179@yahoo.com
yahoo-verify.net	Registrant Name: Domain Administrator Registrant Organization: Yahoo! Inc. Registrant Street: 701 First Avenue Registrant City: Sunnyvale Registrant State/Province: CA Registrant Postal Code: 98089 Registrant Country: BI Registrant Phone: +1.4083893300 Registrant Fax: +1.4083893301 Registrant Email: domainadmin@yahoo-verify.net
hereyouare.ddns.net	Registrant Name: Dan Durrer Registrant Organization: No-IP.com Registrant Street: 425 Maestro Dr. Second Floor Registrant City: Reno Registrant State/Province: NV Registrant Postal Code: 89511 Registrant Country: US Registrant Phone: +1.7758531883 Registrant Email: domains@no-ip.com
outlook-verify.net	Registrant Name: Domain Administrator Registrant Organization: Microsoft Corporation Registrant Street: One Microsoft Way, Redmond, WA, 98052, US Registrant City: Washington Registrant State/Province: canada Registrant Postal Code: 7482957439 Registrant Country: US Registrant Phone: +1.234124323 Registrant Phone Ext: Registrant Fax: +1.2129876243 Registrant Fax Ext: Registrant Email: supportiveemail@protonmail.com
com-users.net	Registrant Name: Domain ID Shield Service Registrant Organization: Domain ID Shield Service CO., Limited

	Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registrant City: Hong Kong Registrant State/Province: Hong Kong Registrant Postal Code: 999077 Registrant Country: CN Registrant Phone: +852.21581835 Registrant Phone Ext: Registrant Fax: +852.30197491 Registrant Fax Ext: Registrant Email: co5806503530204@domainidshield.com
verifiy-account.net	Registrant Name: Domain ID Shield Service Registrant Organization: Domain ID Shield Service CO., Limited Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registrant City: Hong Kong Registrant State/Province: Hong Kong Registrant Postal Code: 999077 Registrant Country: HK Registrant Phone: +852.21581835 Registrant Fax: +852.30197491 Registrant Email: whoisprivacy@domainidshield.com
telegram.net	Registrant Name: NS-CLOUD-B1.GOOGLEDOMAINS.COM Registrant Organization: Domains By Proxy, LLC Registrant Street: clientTransferProhibited https://icann.org/epp#clientTransfe Registrant City: Arizona Registrant State/Province: Arizona Registrant Postal Code: 0056 Registrant Country: US Registrant Phone: +1.4806242505 Registrant Fax: +1.4806242506 Registrant Email: verdonew@protonmail.com
account-verifiy.net	Registrant Name: Domain ID Shield Service Registrant Organization: Domain ID Shield Service CO., Limited Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registrant City: Hong Kong Registrant State/Province: Hong Kong Registrant Postal Code: 999077 Registrant Country: HK Registrant Phone: +852.21581835 Registrant Fax: +852.30197491 Registrant Email: whoisprivacy@domainidshield.com
myaccount-services.net	Registrant Name: Domain ID Shield Service Registrant Organization: Domain ID Shield Service CO., Limited Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL

	TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registrant City: Hong Kong Registrant State/Province: Hong Kong Registrant Postal Code: 999077 Registrant Country: HK Registrant Phone: +852.21581835 Registrant Fax: +852.30197491 Registrant Email: whoisprivacy@domainidshield.com
com-identifier-servicelog.name	Registrant Name: Whois Agent Registrant Organization: Domain Protection Services, Inc. Registrant Street: PO Box 1769 Registrant City: Denver Registrant State/Province: CO Registrant Postal Code: 80201 Registrant Country: US Registrant Phone: +1.7208009072 Registrant Fax: +1.7209758725 Registrant Email: https://www.name.com/contact-domain-whois/com-identifier-servicelog.name abuse@name.com

.BID DOMAINS

Registry
c/o
Neustar, Inc.
21575 Ridgetop Circle
Sterling, VA 20166
United States

dot Bid Limited
2nd Floor, Leisure Island Business Centre
Ocean Village
GX11 1AA
Gibraltar

Global Registry Services Limited
327 Main Streeet,
Gibraltar GX11 1AA

microsoft-update.bid	Registrant Name: Chada Martini Registrant Organization: cavy Registrant Street: No 67, King st Registrant City: Tashkent Registrant State/Province: Tashkent Registrant Postal Code: 46543 Registrant Country: UZ Registrant Phone: +968.8007762430

	Registrant Fax: +968.8007762430 Registrant Email: chada.martini@yandex.com
outlook-livecom.bid	Registrant Name: Chada Martini Registrant Organization: cavy Registrant Street: No 67, King st Registrant City: Tashkent Registrant State/Province: Tashkent Registrant Postal Code: 46543 Registrant Country: UZ Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430 Registrant Email: chada.martini@yandex.com
update-microsoft.bid	Registrant Name: Chada Martini Registrant Organization: cavy Registrant Street: No 67, King st Registrant City: Tashkent Registrant State/Province: Tashkent Registrant Postal Code: 46543 Registrant Country: UZ Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430 Registrant Email: chada.martini@yandex.com

.CLOUD DOMAINS

Registry
c/o
Neustar, Inc.
21575 Ridgetop Circle
Sterling, VA 20166
United States

ARUBA PEC S.p.A.
Via Sergio Ramelli 8
52100 Arezzo (AR)
Italy

documentsfilesharing.cloud	Registrant Name: Whois Agent Registrant Organization: Domain Protection Services, Inc. Registrant Street: PO Box 1769 Registrant City: Denver Registrant State/Province: CO Registrant Postal Code: 80201 Registrant Country: US Registrant Phone: +1.7208009072 Registrant Fax: +1.7209758725 documentsfilesharing.cloud@protecteddomainservices.com

.CLUB DOMAINS

Registry
.CLUB DOMAINS, LLC
100 SE 3rd Ave. Suite 1310
Fort Lauderdale, FL 33394
United States

com-microsoftonline.club	Registrant Name: Chada Martini Registrant Organization: cavy Registrant Street: No 67, King st Registrant City: Tashkent Registrant State/Province: Tashkent Registrant Postal Code: 46543 Registrant Country: UZ Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430 Registrant Email: chada.martini@yandex.com

.INFO, .MOBI, .PRO DOMAINS

Registry
Afilias, Inc.
300 Welsh Road
Building 3, Suite 105
Horsham, PA 19044
United States

confirm-session-identifier.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
session-management.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
confirmation-service.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
document-share.info	Registrant Organization: Martini Registrant State/Province: Tashkent Registrant Country: UZ onlinenic-enduser@onlinenic.com
broadcast-news.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
customize-identity.info	Registrant Organization: Domain ID Shield Service CO., Limited

	Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
webemail.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
com-identifier-servicelog.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
customize-identity.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
documentsharing.info	Registrant Organization: will co Registrant State/Province: VA Registrant Country: AF onlinenic-enduser@onlinenic.com
notification-accountservice.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
identifier-activities.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
documentofficupdate.info	Registrant Organization: William Brown Registrant State/Province: VA Registrant Country: US onlinenic-enduser@onlinenic.com
recoveryusercustomer.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
serverbroadcast.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
account-profile-users.info	Registrant Organization: arsalan co. Registrant State/Province: Louisiana Registrant Country: US onlinenic-enduser@onlinenic.com
account-service-management.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
accounts-manager.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK

	onlinenic-enduser@onlinenic.com
activity-confirmation-service.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
com-accountidentifier.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
com-privacy-help.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
com-sessionidentifier.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
com-useraccount.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
confirmation-users-service.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
confirm-identity.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
confirm-session-identification.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
continue-session-identifier.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
customer-recovery.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
customers-activities.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
elitemaildelivery.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
email-delivery.info	Registrant Organization: Domain ID Shield Service CO., Limited

	Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
identify-user-session.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
message-serviceprovider.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notificationapp.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notification-manager.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
recognized-activity.info	Registrant Organization: will co Registrant State/Province: VA Registrant Country: VA onlinenic-enduser@onlinenic.com
recover-customers-service.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
recovery-session-change.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
service-recovery-session.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
service-session-continue.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
session-mail-customers.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
session-managment.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
session-verify-user.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK

	onlinenic-enduser@onlinenic.com
shop-sellwear.info	Registrant Organization: maryam s32 Registrant State/Province: tersite Registrant Country: US onlinenic-enduser@onlinenic.com
supportmailservice.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
terms-service-notification.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
user-activity-issues.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
useridentity-confirm.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
users-issue-services.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
verify-user-session.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
login-gov.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notification-signal-agnecy.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notifications-center.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
identifier-services-sessions.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
customers-manager.info	Registrant Organization: Home Registrant State/Province: TX Registrant Country: US onlinenic-enduser@onlinenic.com
session-manager.info	Registrant Organization: Home

	Registrant State/Province: TX Registrant Country: US onlinenic-enduser@onlinenic.com
customer-managers.info	Registrant Organization: Home Registrant State/Province: TX Registrant Country: US onlinenic-enduser@onlinenic.com
confirmation-recovery-options.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
service-session-confirm.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
session-recovery-options.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
services-session-confirmation.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notification-managers.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
activities-services-notification.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
activities-recovery-options.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
activity-session-recovery.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
customers-services.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
recovery-session-change.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notification-manager.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK

	onlinenic-enduser@onlinenic.com
session-managment.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
sessions-notification.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
download-teamspeak.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
services-issue-notification.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
microsoft-upgrade.mobi	Registrant Name: Chada Martini Registrant Organization: cavy Registrant Street: No 67, King st Registrant City: Tashkent Registrant State/Province: Tashkent Registrant Postal Code: 46543 Registrant Country: UZ Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430 Registrant Email: chada.martini@yandex.com
broadcastnews.pro	Registrant State/Province: UT Registrant Country: US abuse@name.com

.NETWORK, .WORLD DOMAINS

Registry
Binky Moon, LLC
Donuts Inc.
5808 Lake Washington Blvd NE, Suite 300
Kirkland, WA 98033
United States

mobile-messengerplus.network	Registrant Name: Cave Detector Registrant Organization: Masqat Co Registrant Street: No 64, Lion St Registrant City: Masqat Registrant State/Province: Masqat Registrant Postal Code: 85641 Registrant Country: OM Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430

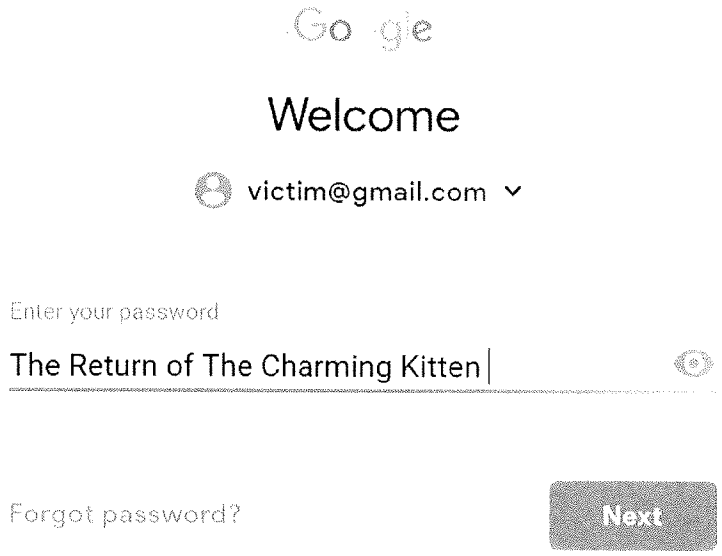
	Registrant Email: cave.detector@yandex.com
sessions-identifier-memberemailid.network	Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Domain Protection Services, Inc. Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: CO Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registrar: Name.com, Inc. Registrar IANA ID: 625 Registrar Abuse Contact Email: abuse@name.com Registrar Abuse Contact Phone: +7.202492374

EXHIBIT 4

The Return of The Charming Kitten

A review of the latest wave of organized phishing attacks by Iranian state-backed hackers

Certfa Lab · 2018.12.13



Abstract

Phishing attacks are the most common form of infiltration used by Iranian state-backed hackers to gain access into accounts. Certfa reviews the latest campaign of phishing attacks that has been carried out and dubbed as “The Return of The Charming Kitten”.

In this campaign, hackers have targeted individuals who are involved in economic and military sanctions against the Islamic Republic of Iran as well as politicians, civil and

human rights activists and journalists around the world.

Our review in Certfa demonstrates that the hackers - knowing that their victims use two-step verification - target verification codes and also their email accounts such as Yahoo! and Gmail. As a result, Certfa believes the safest existing way to confront these attacks is using Security Keys such as YubiKey.

Introduction

In early October 2018, *MD0ugh*, a Twitter user[1], revealed phishing attacks of a group of Iranian hackers against US financial institution infrastructure. According to this user, these attacks could possibly be a reaction to new sanctions against Iran.

The account mentioned a domain with the address *accounts[-]support[.]services* for the first time. This domain is linked to a group of hackers who are supported by the Iranian government, and that we believe have close ties with the Islamic Revolutionary Guard Corps (IRGC). ClearSky[2] has previously published detailed reports on their activities.

A month after these attacks, the administrators of *accounts-support[.]services* expanded their activities and started targeting civil and human rights activists, political figures and also Iranian and Western journalists.

Methods of Attacks

Our investigation illustrates that the attackers are utilising different methods to carry out their attacks. These methods can be put into two categories:

1. Phishing attacks through unknown email or social media and messaging accounts
2. Phishing attacks through email or social media and messaging accounts of public figures, which have been hacked by the attackers

We have also found that the hackers have collected information on their targets prior to the phishing attack. The hackers design specific plans for each target based on the level of targets' cyber knowledge, their contacts, activities, working time, and their geographic situation.

We also noticed that, unlike in previous phishing campaigns, in some cases the hackers did not change the password of their victims' accounts in these latest attacks. This allows them to remain undetected and monitor a victim's communications via their email in real time.

Fake alerts of unauthorised access

According to the samples of phishing attacks, the main trick used by these hackers to deceive their targets is that of sending fake alerts through email addresses such as *notifications.mailservices@gmail[.]com, noreply.customermails@gmail[.]com, customer]email-delivery[.]info* etc. stating that unauthorised individuals have tried to access their accounts.

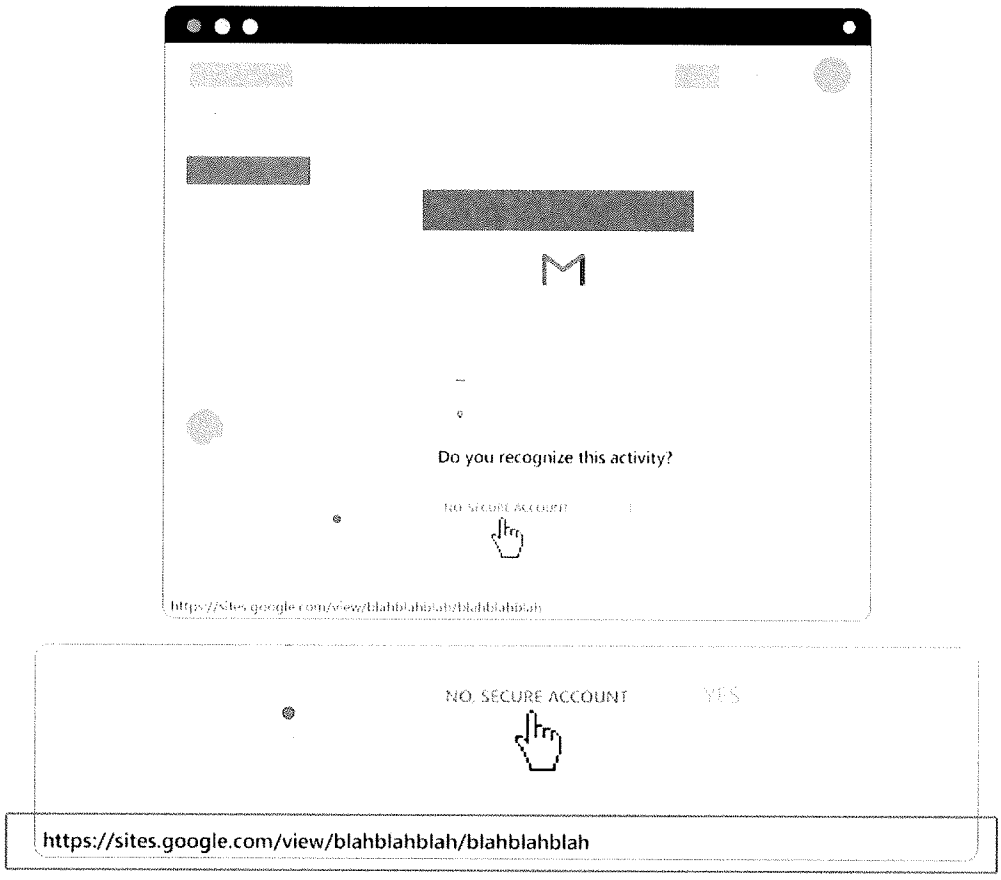


Figure1. Illustration of safe and secure looking fake links

By using this method, attackers pretend that the email provider has sent security alerts to the targets and they should immediately review and restrict suspicious accesses. More details are available in the “Destination Link” section.

Fake file sharing on Google Drive

Sending links with titles such as share files from Google Drive has been one of the most common tricks that hackers have used in recent years. A unique point of these attacks in comparison with the previous ones is that they use Google Site[3], which allows the hackers to show a fake download page of Google Drive, which tricks the users into thinking it’s a real Google Drive page.

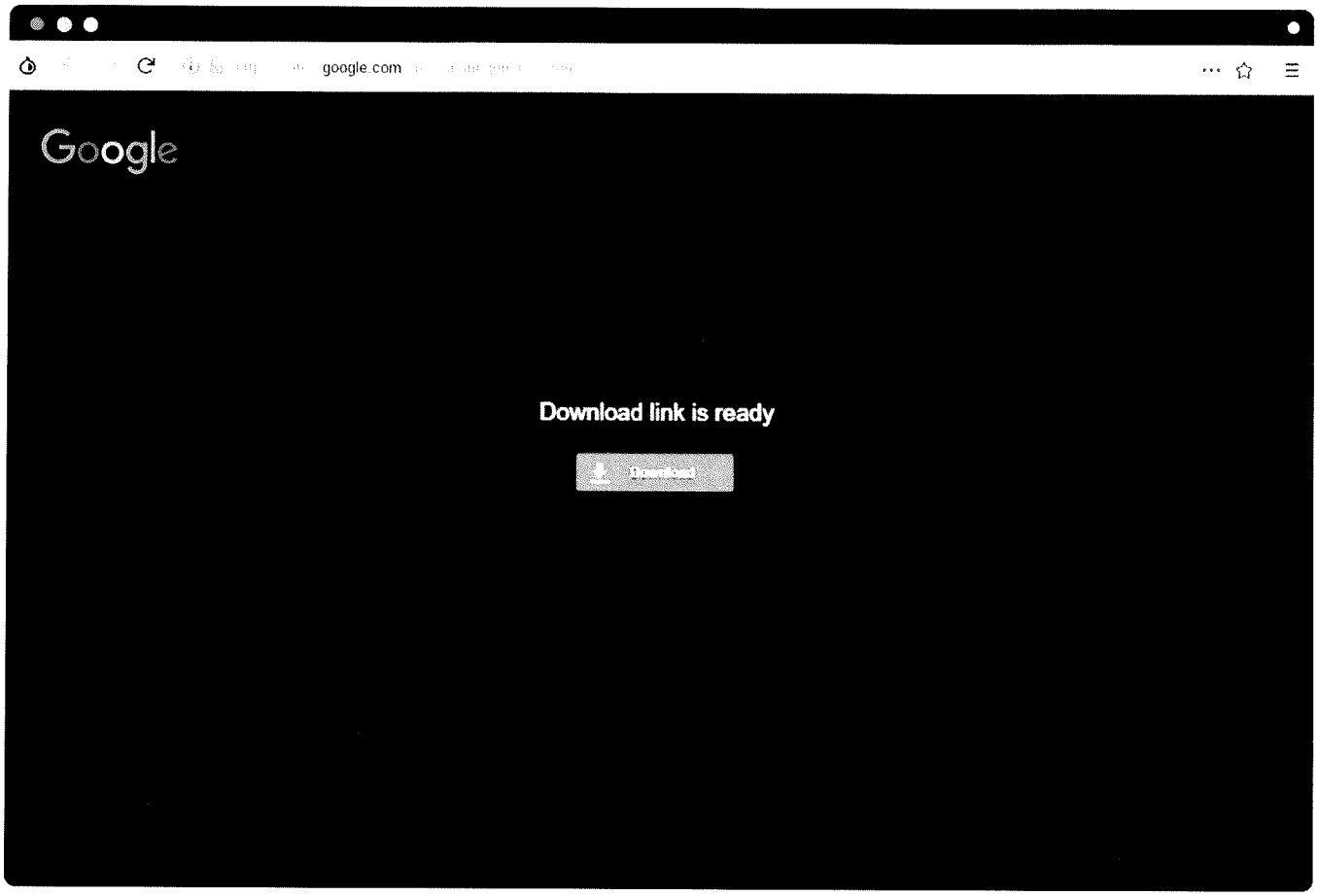


Figure 2. A fake page of Google Drive file sharing page

For example, the hacker had used *hxxps://sites.google[.]com/view/sharingdrivesystem* to deceive the users and convince them the page is the authentic Google Drive as users can see google.com in the address bar of their browsers. Certfa has reported this link and similar links to Google and Google has now terminated them.

By creating websites with the same design and look of Google Drive file sharing page, hackers pretend to be sharing a file with the user, which they should download and run it on their devices. They use hacked Twitter, Facebook and Telegram accounts to send these links and target new users. The truth is there is not any file and the hackers use this page to direct their targets to the fake Google login page, which the users enter their credential details including 2 factor authentication.

The Attack Structure

Most of these attacks are currently occurring through phishing emails. As a result, it would be useful to take a look the original content in recent phishing campaigns.

```
1 <a style="xxx" href="https://sites.google.com/view/[redacted]/google-security" target="_blank" rel="noreferrer">
2     <img src="https://screenshotscdn.firefoxusercontent.com/images/b4df1c19-[redacted]-[redacted].png">
  </a>
3 <img src="https://zohomailtracker.com/api/v1/img/show?hash=[redacted]" class="xxx">
```

Figure 3. An example of codes of phishing email sent to the user

1. Destination link

1.1. Trusted Stage: Internet users around the world consider Google's main domain (google.com) to be a safe and secure address. The attackers misuse this fact and create fake pages on sites.google.com (which is a subdomain of Google) to deceive their targets. Google's Site service gives its users an ability to show various contents on it. The attackers use this ability to send fake alerts and redirect their targets to insecure websites or embedded phishing pages as a iframe on those pages.

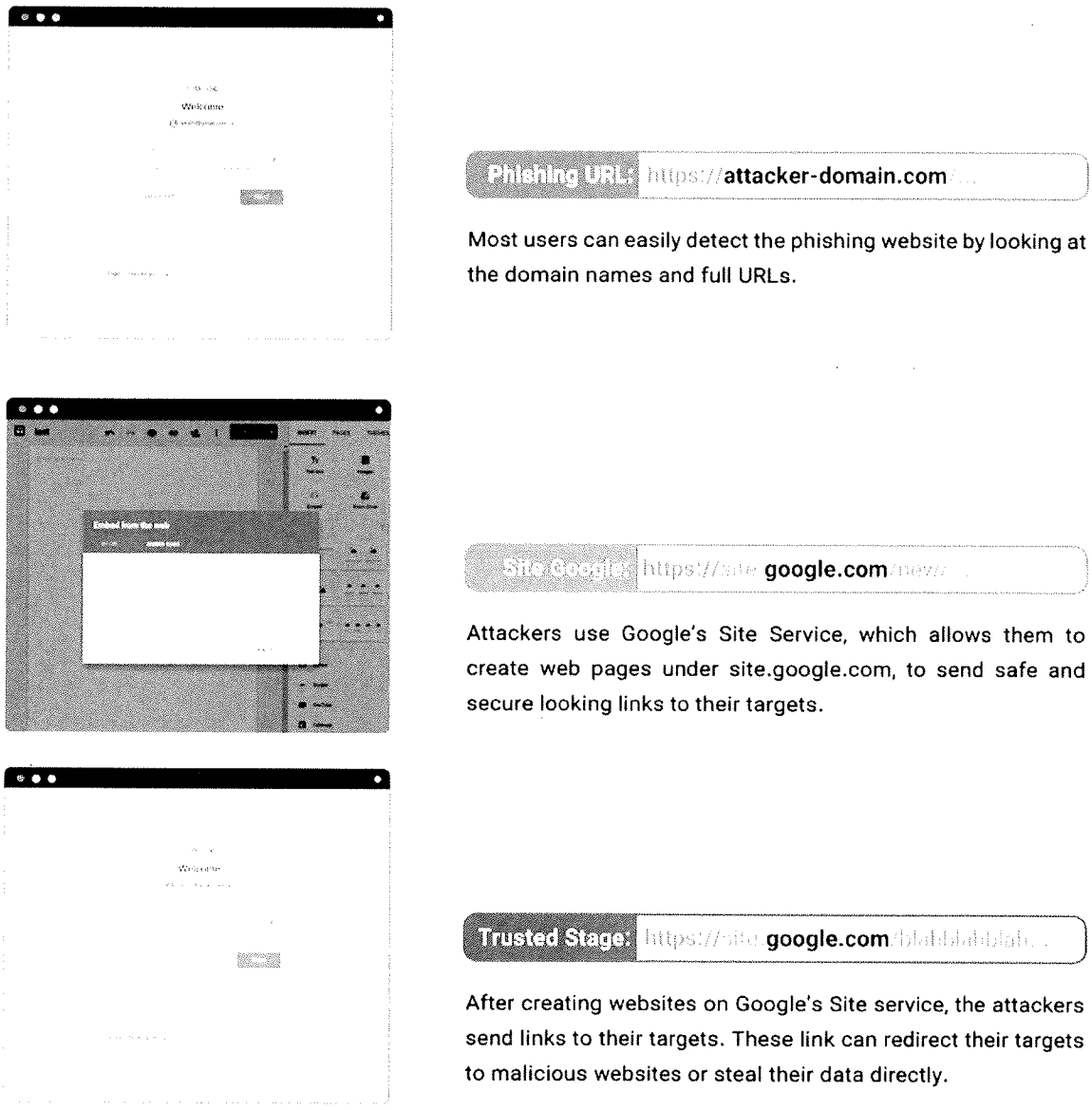


Figure 4. How attackers misuse site.google.com

1.2. Untrusted Stage: Since Google can quickly recognise and eliminate suspicious and malicious links on sites.google.com, the hackers use their own website. The links of phishing websites have similar patterns to a previous phishing campaign which was launched in the past years. For example, attackers use words such as "management", "customize", "service", "identification", "session", "confirm" etc. in the domains name and phishing URLs to deceive users who want to verify their website addresses.

2. Clickable image in emails

The hackers use an image, instead of texts, in the body of their emails, to bypass Google's security and anti-phishing system. For this purpose, attackers have also used

third party services such as Firefox Screenshot[4] to host their email images.

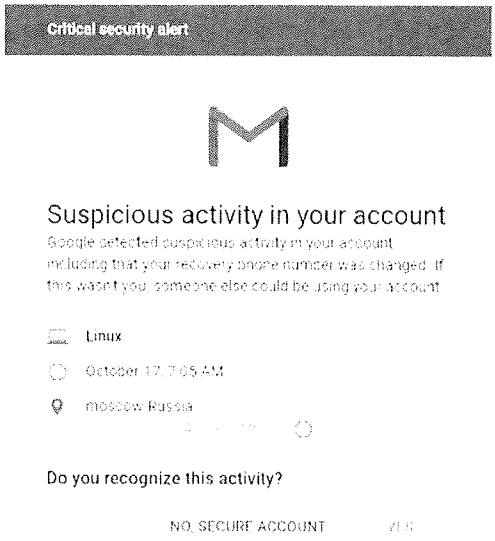


Figure 5. An example of a planted image of fake alarm in a phishing email

3. Hidden tracking image on emails

The attackers use a separate hidden image in the body of the email to notify them when their targets open the email. This trick helps the hackers to act immediately after the target opens the email and clicks on the phishing link.

Phishing Pages

Apart from the content structure of the emails and phishing links, we are sure that attackers use a customized platform to create and store users' credential details. We have also noticed that they have designed the phishing pages for both desktop and mobile versions of Google and Yahoo! mail services and they might use other services in the future.

An interesting technique they have used in recent attacks was once their target enters their username and password, attackers check those credentials on-the-fly and if that information was given correctly, they then ask for 2-step verification code.

In other words, they check victims' usernames and passwords in realtime on their own servers, and even if 2 factor authentication such as text message, authenticator app or one-tap login are enabled they can trick targets and steal that information too.

Figures 6 to 9 demonstrate some examples of the phishing pages, which have been sent to the targets by the Iranian hackers.

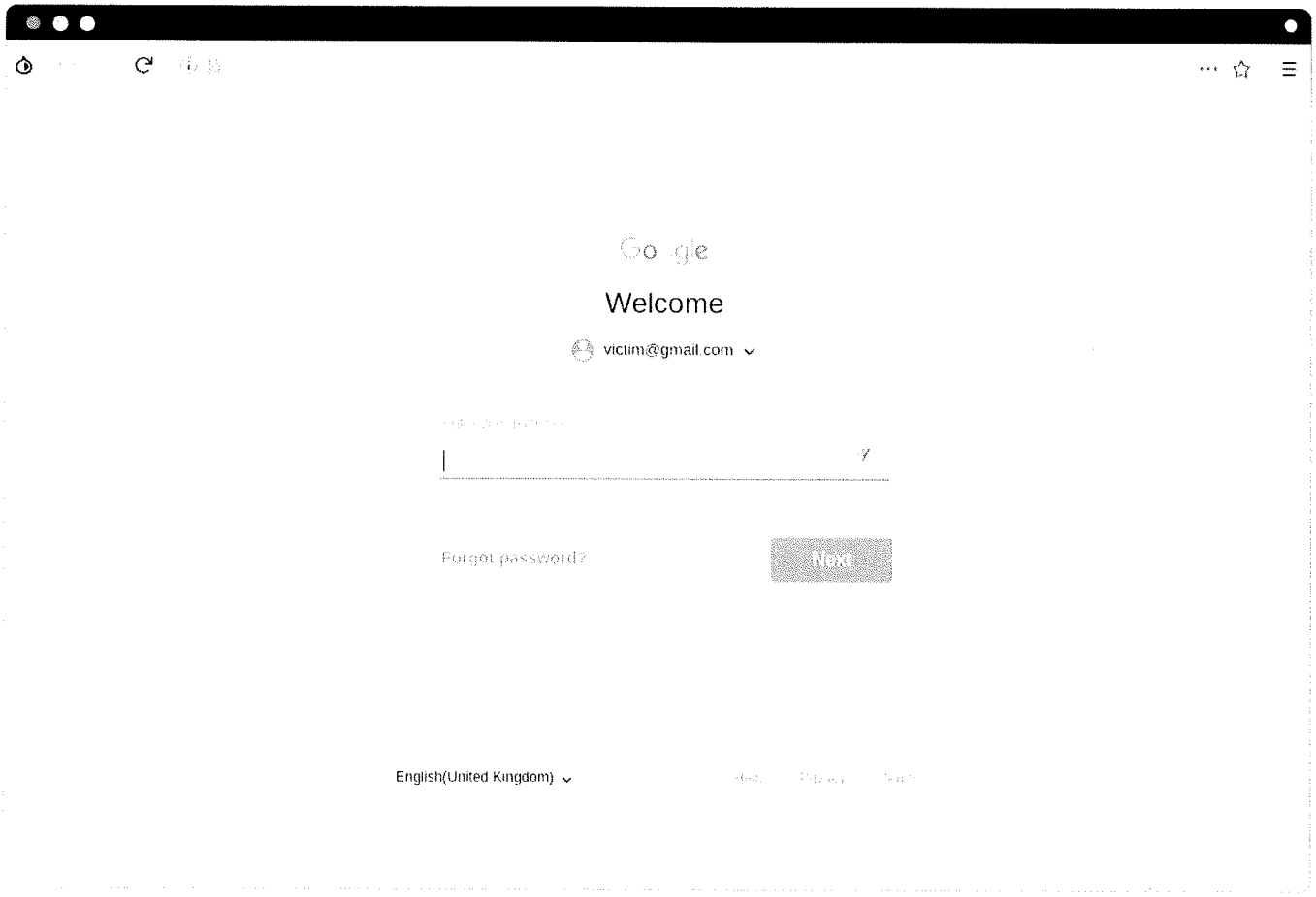


Figure 6. A fake page for entering password of Gmail accounts

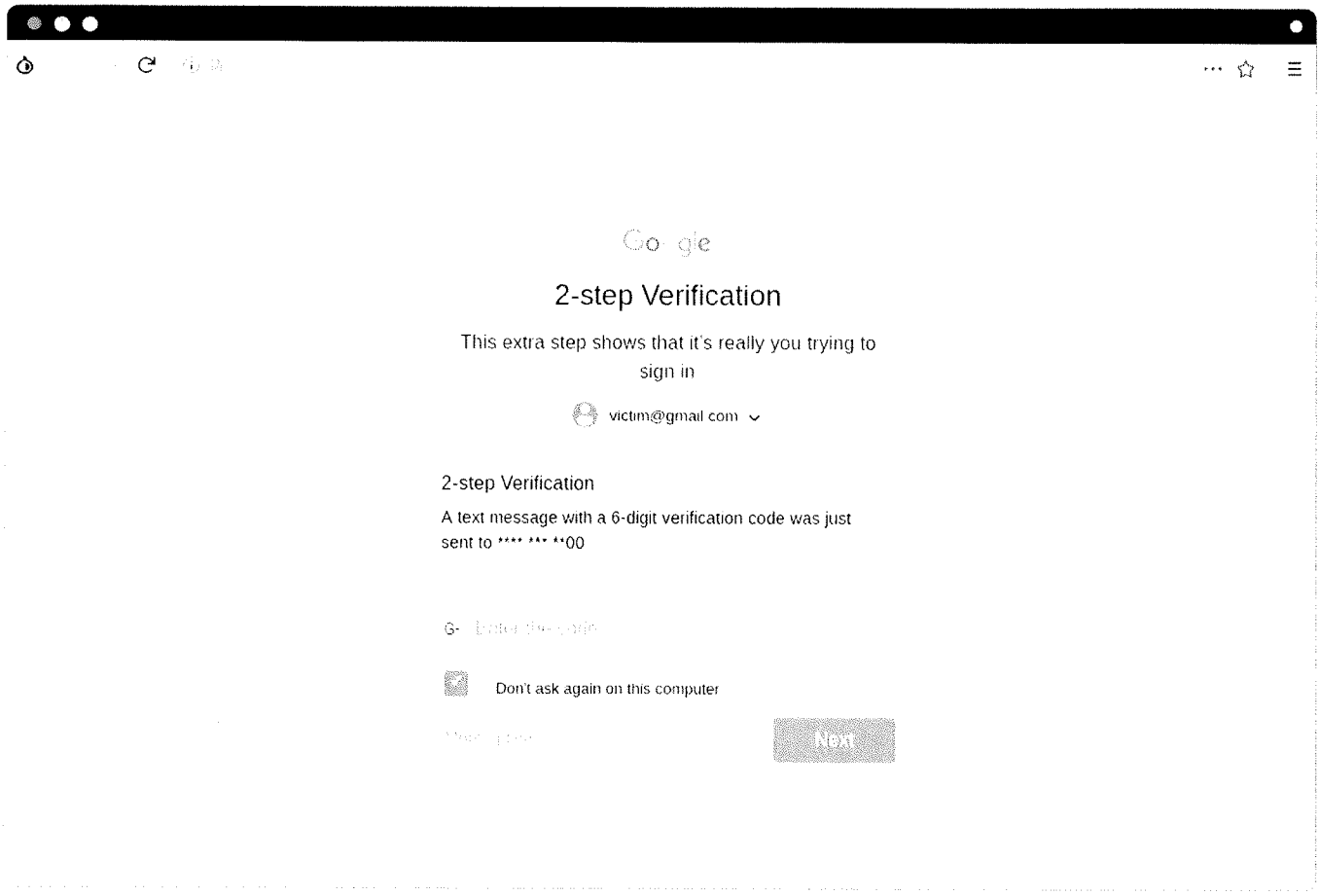


Figure 7. A fake page for entering 2-step verification code for Gmail accounts

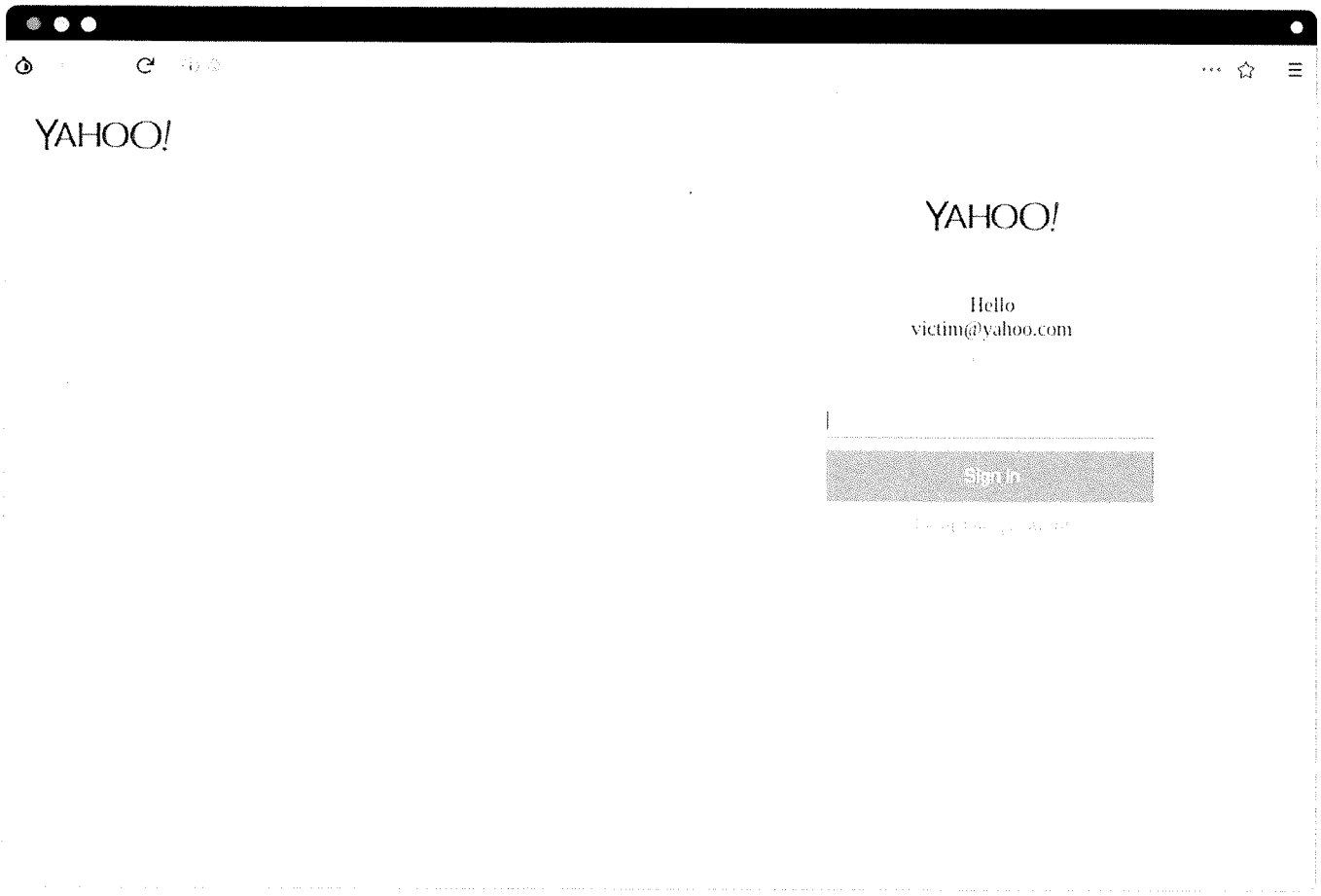


Figure 8. A fake page for entering password of Yahoo! accounts

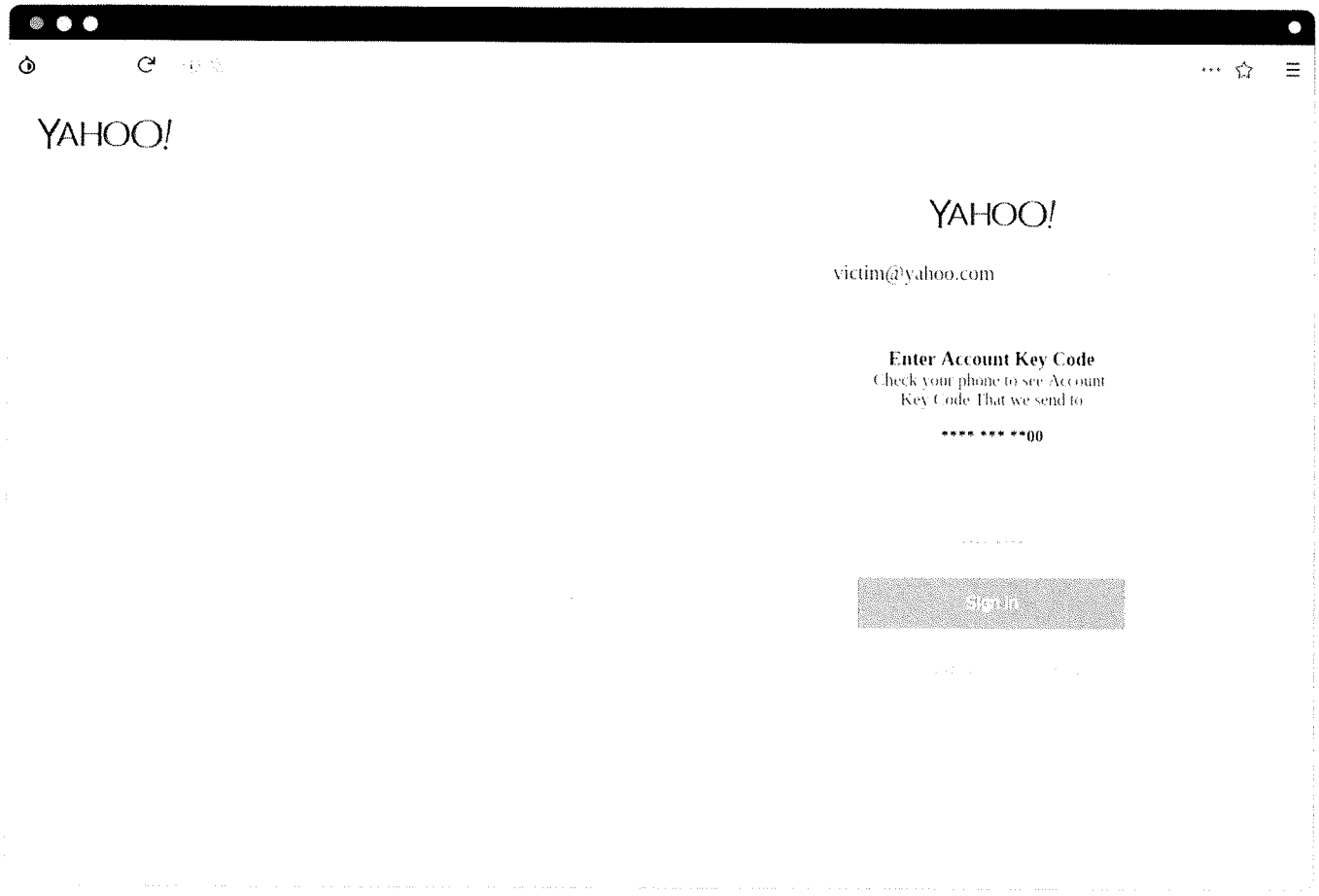
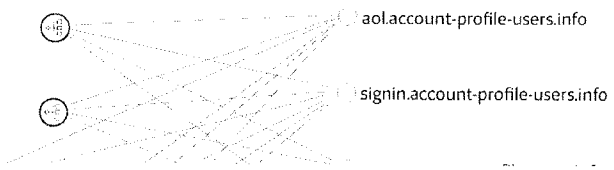
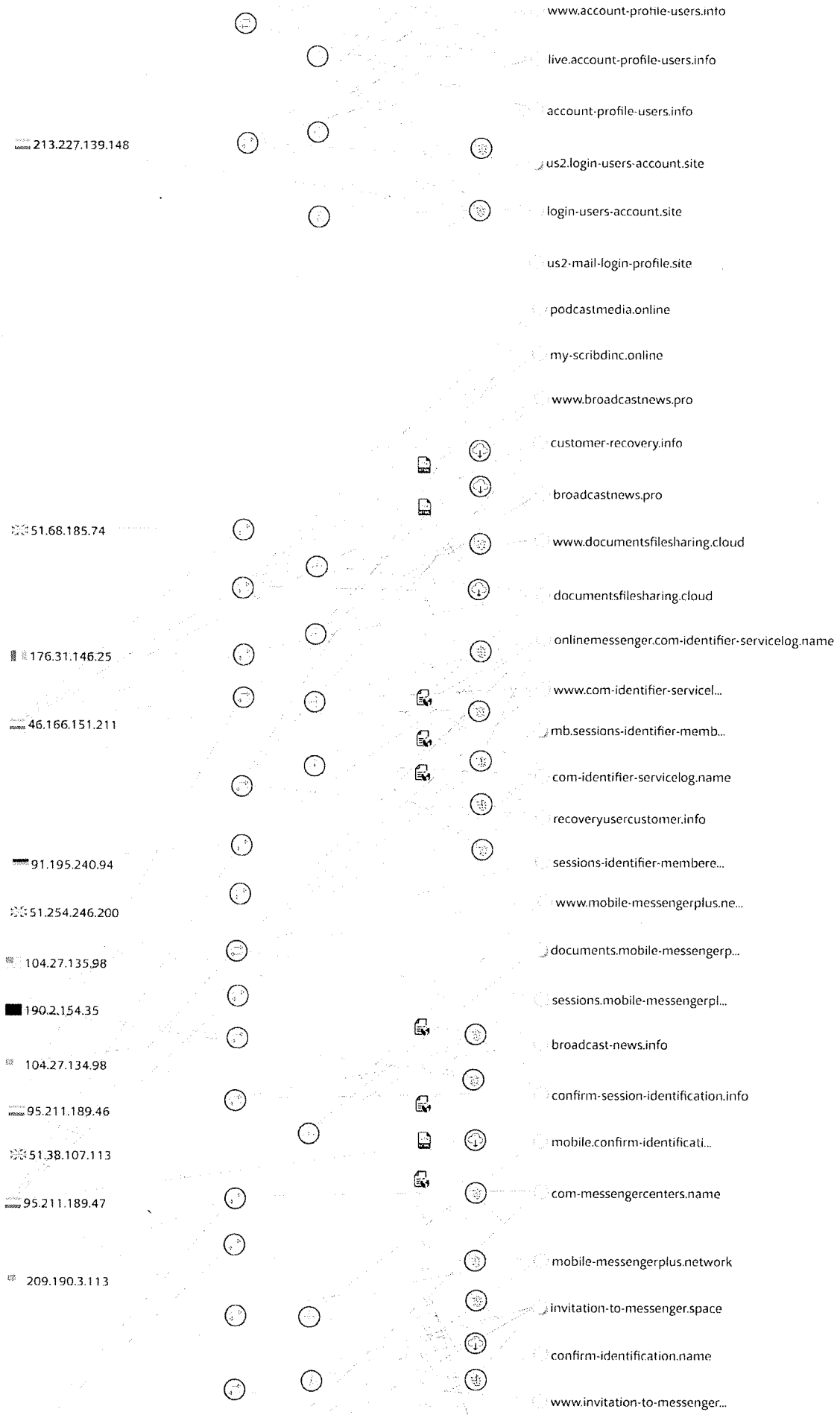


Figure 9. A fake page for entering 2-step verification code for Yahoo! accounts

Hacker's Footprints

Our primary reviews of the phishing websites linked to this campaign show that hackers have set up a remarkable number of domains. Our latest findings show that for this phishing campaign in a relatively short period of time, (September to November 2018), they have used more than 20 domain names. The number of phishing domains has increased at the time of writing this report. Closer investigation of these servers revealed how their network of domain names have been used in recent attacks.




www.account-profile-users.info
live.account-profile-users.info
account-profile-users.info
213.227.139.148
us2.login-users-account.site
login-users-account.site
us2-mail-login-profile.site
podcastmedia.online
my-scribdinc.online
www.broadcastnews.pro
customer-recovery.info
broadcastnews.pro
51.68.185.74
www.documentsfilesharing.cloud
documentsfilesharing.cloud
onlinemessenger.com-identifier-servicelog.name
176.31.146.25
www.com-identifier-servicel...
46.166.151.211
mb.sessions-identifier-memb...
com-identifier-servicelog.name
recoveryusercustomer.info
91.195.240.94
sessions-identifier-membere...
51.254.246.200
www.mobile-messengerplus.ne...
104.27.135.98
documents.mobile-messengerp...
190.2.154.35
sessions.mobile-messengerpl...
broadcast-news.info
104.27.134.98
confirm-session-identification.info
95.211.189.46
mobile.confirm-identificati...
51.38.107.113
95.211.189.47
com-messengercenters.name
mobile-messengerplus.network
209.190.3.113
invitation-to-messenger.space
confirm-identification.name
www.invitation-to-messenger...

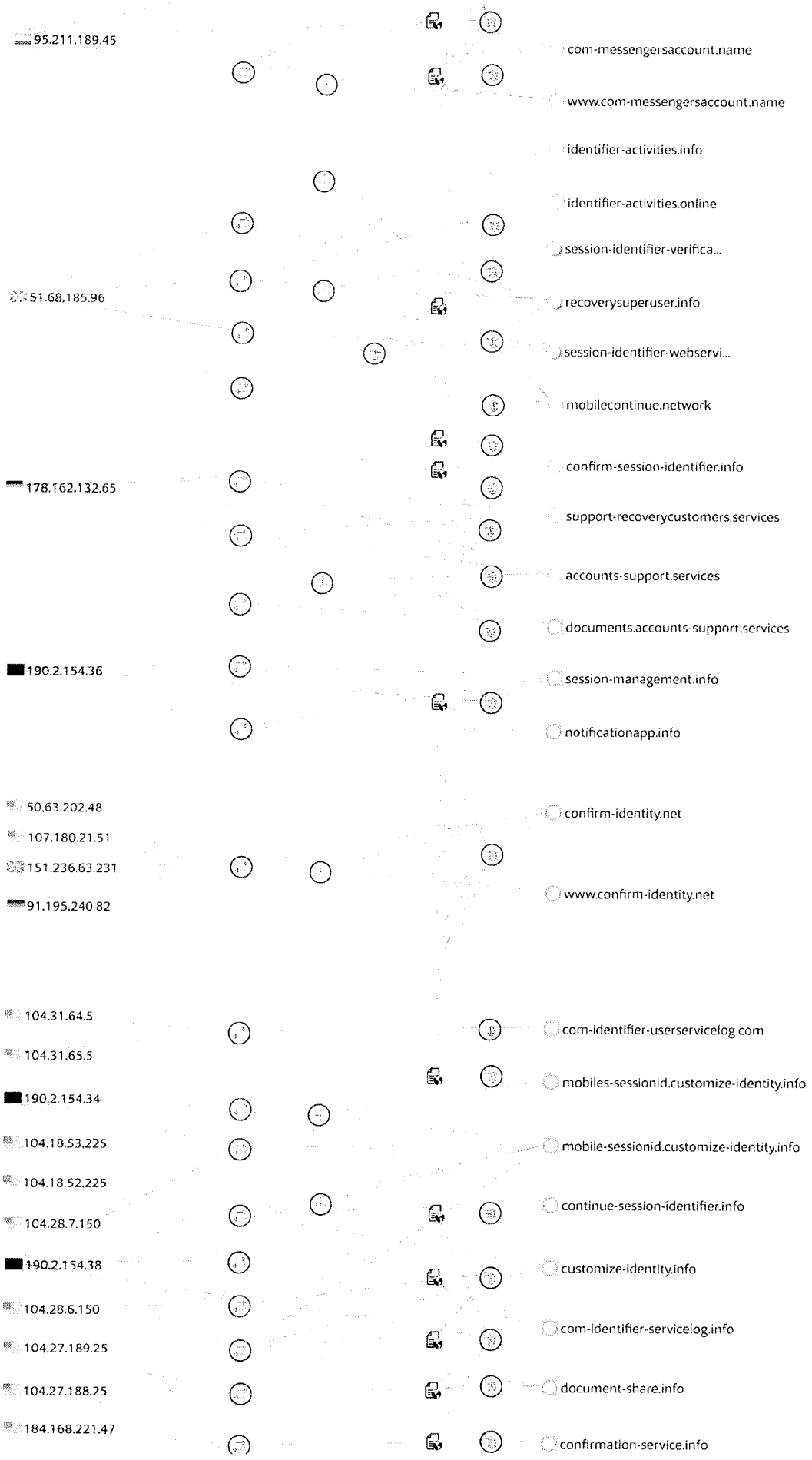

95.211.189.45
com-messengersaccount.name
www.com-messengersaccount.name
identifier-activities.info
identifier-activities.online
session-identifier-verifica...
51.68.185.96
recoverysuperuser.info
session-identifier-webservi...
mobilecontinue.network
confirm-session-identifier.info
178.162.132.65
support-recoverycustomers.services
accounts-support.services
documents.accounts-support.services
190.2.154.36
session-management.info
notificationapp.info
50.63.202.48
confirm-identity.net
107.180.21.51
151.236.63.231
www.confirm-identity.net
91.195.240.82
104.31.64.5
com-identifier-userservicelog.com
104.31.65.5
mobiles-sessionid.customize-identity.info
190.2.154.34
104.18.53.225
mobile-sessionid.customize-identity.info
104.18.52.225
continue-session-identifier.info
104.28.7.150
190.2.154.38
customize-identity.info
104.28.6.150
com-identifier-servicelog.info
104.27.189.25
104.27.188.25
document-share.info
184.168.221.47
confirmation-service.info

Figure 10. Deep data of the attackers' network in this phishing campaign, which gathered by Certfa[5]

Moreover, our technical reviews reveal that the individuals, who are involved in this campaign used Virtual Private Networks (VPNs) and proxies with Dutch and French IP addresses to hide their original location. In spite of their efforts, we have uncovered enough evidence to prove that the attackers were using their real IP addresses (i.e 89.198.179[.]103 and 31.2.213[.]18 from Iran during the preparation phase of their campaign).

Also, some domain names and servers of this campaign are very similar to the methods, techniques and targets that been used by Charming Kitten, a group of hackers who are linked to the Iranian government. Consequently, we believe Charming Kitten and the Iranian hacker(s) belonging to this group have returned and launched new cyber attacks against various people around the world and with more focus on Israeli and American citizens.

Conclusion

Phishing attacks are the most popular method of stealing data and hacking account amongst Iranian hackers, but the most significant fact about this campaign is its timing. This campaign launched weeks before 4 November 2018 which is when the U.S. imposed new sanctions on Iran. This campaign tries to collect information by infiltrating the accounts of non-Iranian political figures and authorities who work on economic and military sanctions against Iran.

In other words, hackers who are supported by the Iranian government pick their targets according to policies and international interests for the Iranian government and also where Iran wants to have impact indirectly.

A a result, we propose a series of recommendations to tech companies, policymakers, civil society actors and internet users to effectively lessen the threat of this type of attack and even thwart them.

Our recommendations to tech companies and policy makers:

- Stop using 2 factor authentication by text plain message/SMS.
- Start using Security Keys (i.e. YubiKey) for 2 factor authentication for high ranking individuals who have sensitive jobs or activities.
- Do not use one-tap login verification process.

Our recommendations to civil society and the Iranian diaspora media:

- Inform employees and colleagues about any phishing threats and encourage them to use Security Keys such as Yubikey for 2 factor authentication and activate Google's Advanced Protection Program.
- Always use company and institution email accounts instead of personal email for sensitive communications. Change Sender Policy Framework or SPF[6] settings according to the communication policy of the company/organisation such as restricting receiving emails from outside of the working network. For example, G Suite allows admins to block receiving emails from unauthorised address or domains[7].
- Encourage the public to enable 2 factor authentication on their account by mobile apps such as Google Authenticator.

Our recommendations to users:

- Do not click on unknown links. For reviewing suspicious activities on your account or change the password, instead of clicking on any link, you can go to your "My Account" settings from your email directly which is more safer.

- Use email encryption such PGP for sensitive emails which prevent hackers reading your emails in the first place.
- Do not store classified and sensitive information as a plain text in your mailbox.
- HTTPS being before a domain names in a URL does not mean that the content of a website is secure or trusted - it's just a secure extension of the HTTP protocol. Do not forget many phishing websites are currently operating under HTTPS protocol too.

IOCs

- 178.162.132[.]65
- 190.2.154[.]34
- 190.2.154[.]35
- 190.2.154[.]36
- 190.2.154[.]38
- 46.166.151[.]211
- 51.38.87[.]64
- 51.38.87[.]65
- 51.68.185[.]96
- 51.38.107[.]113
- 95.211.189[.]45
- 95.211.189[.]46
- 95.211.189[.]47
- 213.227.139[.]148
- 54.37.241[.]221
- 54.38.144[.]250
- 54.38.144[.]251
- 54.38.144[.]252
- 85.17.127[.]172

- 85.17.127[.]173
- 85.17.127[.]174
- 85.17.127[.]175
- 89.198.179[.]103
- 31.2.213[.]18
- accounts-support[.]services
- broadcast-news[.]info
- broadcastnews[.]pro
- com-identifier-servicelog[.]info
- com-identifier-servicelog[.]name
- com-identifier-userservicelog[.]com
- confirm-session-identification[.]info
- confirm-session-identifier[.]info
- confirmation-service[.]info
- customer-recovery[.]info
- customize-identity[.]info
- document-share[.]info
- document.support-recoverycustomers[.]services
- documentofficupdate[.]info
- documents.accounts-support[.]services
- documentsfilesharing[.]cloud
- email-delivery[.]info
- mobile-sessionid.customize-identity[.]info
- mobiles-sessionid.customize-identity[.]info
- my-scribdinc[.]online
- myyahoo.ddns[.]net
- notificationapp[.]info
- onlinemessenger.com-identifier-servicelog[.]name
- podcastmedia[.]online
- recoveryusercustomer[.]info
- session-management[.]info
- support-recoverycustomers[.]services

- continue-session-identifier[.]info
- mobilecontinue[.]network
- session-identifier-webservice.mobilecontinue[.]network
- com-messengersaccount[.]name
- invitation-to-messenger[.]space
- confirm-identification[.]name
- mobilecontinue[.]network
- mobile.confirm-identification[.]name
- services.confirm-identification[.]name
- mobile-messengerplus[.]network
- confirm.mobile-messengerplus[.]network
- com-messengercenters[.]name
- securemail.mobile-messengerplus[.]network
- documents.mobile-messengerplus[.]network
- confirm-identity[.]net
- identifier-sessions-mailactivityid[.]site
- activatecodeoption.ddns[.]net
- broadcastpopuer.ddns[.]net
- books.com-identifier-servicelog[.]name
- mb.sessions-identifier-memberemailid[.]network
- sessions-identifier-memberemailid[.]network
- sessions.mobile-messengerplus[.]network
- confirm-verification-process[.]systems
- accounts.confirm-verification-process[.]systems
- broadcastnews.ddns[.]net
- account-profile-users[.]info
- us2-mail-login-profile[.]site
- us2.login-users-account[.]site
- login-users-account[.]site
- live.account-profile-users[.]info
- signin.account-profile-users[.]info
- aol.account-profile-users[.]info

- users-account[.]site

Footnotes:

1. https://s.certfa.com/q1514c
   https://s.certfa.com/eNnnag
   https://s.certfa.com/ur93p2 ⇆
2. ClearSkye Cyber Security (2018), "Charming Kitten, Iranian cyber espionage against human rights activists, academic researchers and media outlets - and the HBO hacker connection". Accessed November 15, 2018. https://s.certfa.com/1ullxk ⇆
3. Sites. Accessed November 23, 2018. https://sites.google.com/ ⇆
4. Firefox Screenshots. Accessed November 15, 2018. https://screenshots.firefox.com/ ⇆
5. VirusTotal Graph. Accessed November 25, 2018. https://s.certfa.com/OgQUSC ⇆
6. Sender Policy Framework or SPF is an email authentication method to detect forged sender addresses in emails. SPF allows the recipient to check that an email claiming to come from a specific domain comes from an IP address authorized by that domain's administrators. ⇆
7. G Suite Administrator Help (2018), "Restrict messages to authorized addresses or domains". Accessed November 29, 2018. https://support.google.com/a/answer/2640542?hl=en ⇆

Tags: Charming Kitten APT Phishing Iran

APPENDIX C

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

MICROSOFT CORPORATION, a Washington corporation, *Plaintiff,* v. JOHN DOES 1-2, CONTROLLING A COMPUTER NETWORK AND THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS, *Defendants.*	)	Civil Action No: **FILED UNDER SEAL PURSUANT TO LOCAL RULE 5**

DECLARATION OF GABRIEL M. RAMSEY IN SUPPORT OF MOTION FOR PROTECTIVE ORDER TEMPORARILY SEALING DOCUMENTS

I, Gabriel M. Ramsey, declare as follow:

1. I am an attorney admitted to practice in the State of California and the District of Columbia. I am a partner at the law firm of Crowell & Moring LLP ("Crowell"), counsel of record for the Plaintiff in this matter, Microsoft Corporation ("Microsoft"). I make this declaration in support of Microsoft's Motion for a Protective Order Temporarily Sealing Documents. I have personal knowledge of the facts set forth in this declaration and, if called to testify as a witness, could and would testify to the following under oath.

2. This case arises out of the harmful and malicious Internet activities of Defendants John Does 1 and 2 (collectively "Defendants"). I am informed and on that basis believe that Defendants are sophisticated cybercriminals who specialize in stealing sensitive information from computer networks. I am informed and on that basis believe that Defendants make unauthorized access to Microsoft's services and software, hack into a target's computer network, and in

particular Microsoft's software, install malware on those networks giving them long-term and surreptitious access to those networks, and then locate and exfiltrate sensitive information from them.

3. I am informed and believe that, for reasons explained in detail in the declaration of David Anselmi In Support Of Microsoft's Application For Temporary Restraining Order And Order To Show Cause For Preliminary Injunction ("TRO Application"), filed contemporaneously herewith, permitting Defendants to learn of these proceedings prior to execution of the temporary ex parte relief sought in Microsoft's Motion For Preliminary Injunction Order—in particular the portion to disable the domains in Appendix A to that Order—would preclude Microsoft's ability to obtain effective relief against Defendants. This is because Defendants are highly sophisticated cybercriminals capable of quickly adapting the command and control infrastructure used to perpetrate Defendants' unlawful conduct in order to overcome Microsoft's remediation efforts.

4. I am informed and believe that, absent a protective order, there is a substantial risk that Defendants will learn of these proceedings before the temporary ex parte relief to disable the domains in Appendix A to the Preliminary Injunction Order can be effected and will take steps to evade the relief sought.

5. Over the past nine years, I, on behalf of Microsoft, have been involved with prosecuting twelve similar cases. These cases all involved similar litigation strategies and claims and have involved John Doe defendants conducting illegal activities through identifiable but movable online command and control infrastructures similar to that used by Phosphorus. In several of those cases, I personally observed that defendants also immediately took action to attempt to defy and evade the court's order as soon as they detected legal action being taken against them.

6. Thus, given Defendants' defiance of this Court's injunctive orders and my past experience with cases with very similar circumstance as those here, it is my belief that even

disclosing that Microsoft has requested a Preliminary Injunctive Order to disable the domains at Appendix A to that order gives Defendants the opportunity to adapt the command and control infrastructure so that they can continue to perpetrate their unlawful conduct. For this reason, Microsoft respectfully requests that all documents filed in this case be temporarily sealed.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct to the best of my knowledge. Executed on this 14th day of March 2019, in Washington, D.C.

Gabriel M. Ramsey

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

MICROSOFT CORPORATION, a Washington corporation, Plaintiff, v. JOHN DOES 1-2, CONTROLLING A COMPUTER NETWORK AND THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS Defendants.	)	Civil Action No: **FILED UNDER SEAL PURSUANT TO LOCAL RULE 5.1**

ORDER GRANTING MICROSOFT'S MOTION FOR A PROTECTIVE ORDER
TEMPORARILY SEALING DOCUMENTS

Before the Court is Microsoft's Motion for a Protective Order Temporarily Sealing Documents. Upon consideration of the Motion, the pleadings filed herein, and the arguments of counsel, the Court finding that the arguments of applicable rules and District of Columbia Circuit precedent are satisfied, that the requested order is the least restrictive means available to protect the interests of Microsoft and the public, and that there is a compelling need to enter a temporary sealing order,

Accordingly, **IT IS HEREBY ORDERED** that the following documents be filed and maintained UNDER SEAL in accordance with Fed. R. Civ. P. 26(c)(1) and Local Civil Rule 5, pending execution of the *ex parte* relief requested in Microsoft's Motion to Supplement Preliminary Injunction Order filed on March 14, 2019:

1. The instant Motion for Protective Order Temporarily Sealing Documents and accompanying documents, including the Brief in support of this

Motion;

2. The declaration of Gabriel M. Ramsey in Support of Motion for Protective Order Sealing Documents;
3. Microsoft's *Ex Parte* Motion For Preliminary Injunction Order and accompanying documents;
4. The Declaration of David Anselmi in Support of Microsoft's *Ex Parte* Motion For Preliminary Injunction Order and attachments thereto;
5. [Proposed] Preliminary Injunction Order and accompanying documents.

IT IS FURTHER ORDERED that, immediately upon execution of the *ex parte* relief disabling the domains set forth at Appendix A, sought in Microsoft's Motion to Supplemental Preliminary Injunction Order, Microsoft shall file with the Clerk of the Court a Notice that the Supplemental Preliminary Injunction Order has been executed, and the Clerk of the Court upon receiving such Notice shall file the foregoing documents on the public docket. Microsoft shall be permitted to disclose any such material as deemed necessary to commence its efforts to provide Defendants notice of any further hearings and service of pleadings associated with Motion To Supplement Preliminary Injunction Order.

IT IS SO ORDERED.

Entered this ____ day of March, 2019

_____
UNITED STATES DISTRICT JUDGE

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

MICROSOFT CORPORATION, Plaintiff, v. JOHN DOES 1-2, Defendants.	Case: 1:19-cv-00716 (JURY-DEMAND) Assigned To : Amy B. Jackson Assign. Date : 3/14/2019 Description: TRO/PI Chief Judge Beryl A. Howell

ORDER

Pending before the Court is plaintiff Microsoft Corp.'s Motion for a Temporary Sealing Order related to its instant action seeking an *ex parte* preliminary injunction. *See* LCvR 40.7(f) (stating that the Chief Judge shall "hear and determine . . . motions in any case not already assigned" including "motion[s] to seal the complaint"); *see also* LCvR 5.1(h)(1) ("Absent statutory authority, no case or document may be sealed without an order from the Court."). The motion is granted, subject to any further consideration by the United States District Judge to whom this case is randomly assigned.

I. LEGAL STANDARD

"The starting point in considering a motion to seal court records is a strong presumption in favor of public access to judicial proceedings." *Hardaway v. D.C. Hous. Auth.*, 843 F.3d 973, 980 (D.C. Cir. 2016) (quoting *EEOC v. Nat'l Children's Ctr., Inc.*, 98 F.3d 1406, 1409 (D.C. Cir. 1996)). Courts should consider six factors, originally identified in *United States v. Hubbard*, 650 F.2d 293 (D.C. Cir. 1980), in determining whether that presumption may be overcome, including:

> (1) the need for public access to the documents at issue; (2) the extent of previous public access to the documents; (3) the fact that someone has objected to disclosure,

> and the identity of that person; (4) the strength of any property and privacy interests asserted; (5) the possibility of prejudice to those opposing disclosure; and (6) the purposes for which the documents were introduced during the judicial proceedings."

Metlife, Inc. v. Fin. Stability Oversight Council, 865 F.3d 661, 665 (D.C. Cir. 2017) (quoting *Nat'l Children's Ctr.*, 98 F.3d at 1409 (citing *Hubbard*, 650 F.2d at 317–22)). In "motions to seal or unseal judicial records, the *Hubbard* test has consistently served as our lodestar because it ensures that we fully account for the various public and private interests at stake," *Metlife, Inc.*, 865 F.3d at 666.

II. DISCUSSION

The plaintiff, Microsoft, requests temporary sealing of its pleadings associated with the instant *ex parte* Motion for a Preliminary Injunction. Pl.'s Mot. for Sealing Order ("Pl.'s Mot.") at 1. Microsoft has filed the motion for a preliminary injunction "to prevent the activities of [defendants John Does 1 and 2] who are engaged in harmful and malicious Internet activities directed at Microsoft, its customers, and the general public." Pl's Mem. in Supp. of Mot. for Sealing Order ("Pl.'s Mem.") at 1. Specifically, Microsoft seeks to "disable the recent registered domains set forth in Appendix A to [its] Complaint," *id.* and warns that "advance public disclosure or notice of that requested relief would allow Defendants to evade such relief and further prosecution of this action, thereby perpetuating the irreparable harm at issue," *id.* at 1–2. Microsoft avers that its "rights and interests in protecting its ability to obtain ex parte temporary relief, and the necessity of sealing its pleadings in order to effectively disable the domains . . . , is paramount over any competing public interest to *immediate* access to the information Microsoft requests to be sealed." *Id.* at 4 (emphasis in original).

Moreover, Microsoft suggests that if its "papers are not sealed, the relief sought would very likely be rendered fruitless, and there is a substantial risk Defendants [elsewhere referred to

as 'highly sophisticated cybercriminals'] would destroy evidence." *Id.* Microsoft points to past experience suggesting that when the "defendants become aware of efforts to mitigate or investigate their activities, they take steps to conceal their activities and to conceal the injury caused to their victims, making it more difficult for their victims to adequately assess the damage or take steps to mitigate that injury." *Id.* at 5. This experience "underscores the risk that the Defendants in this case will take similar steps to destroy evidence and move their command and control infrastructure . . . if they are given notice of the" instant action. *Id.*

Microsoft notes that it "only seeks to seal [its pleadings] for a limited period of time, until after effective ex parte temporary relief has been obtained, disabling the domains. . . . [after which] all documents will be unsealed and the public will be given full access to these proceedings." *See id.* at 6. If the United States District Judge to whom this case is assigned grants Microsoft's request to disable the defendants' domains, Microsoft proposes to file a Notice with the Clerk of the Court when that order is executed, at which point the pleadings in this matter may be unsealed. *Id.* at 2, 6; Pl.'s Mot. at 2.

At this early stage of the litigation, the Court is persuaded that the plaintiff has met its burden of showing that the interests in temporarily sealing this case outweigh the public interest in disclosure because sealing is necessary in order to protect evidence and to prevent the defendants from taking steps to conceal their activities or any injuries caused to plaintiff or others. Therefore, the Court grants the plaintiff's motion to seal this case.

III. CONCLUSION

For the foregoing reasons, it is hereby

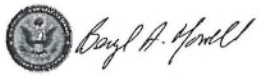
ORDERED that the plaintiff's Motion for a Temporary Sealing Order is **GRANTED**; and it is further

ORDERED that this action, and all papers and pleadings filed in connection therewith, shall remain sealed until further Order of the Court; and it is further

ORDERED that the plaintiff will be expected to discuss its proposal for the process of lifting the sealing order at the first scheduled Court conference on this matter.

SO ORDERED.

Date: March 14, 2019



BERYL A. HOWELL
Chief Judge