APPENDIX D

'ONNX' MFA Bypass Targets Microsoft 365 Accounts

The service, likely a rebrand of a previous operation called "Caffeine," mainly targets financial institutions in the Americas and EMEA and uses malicious QR codes and other advanced evasion tactics.

Elizabeth Montalbano, Contributing Writer

June 19, 2024

4 Min Read

SOURCE: RONSTIK VIA ALAMY STOCK PHOTO

A highly organized phishing-as-a-service operation (PhaaS) is targeting Microsoft 365 accounts across financial firms with business email compromise (BEC) attacks that leverage

a two-factor authentication (2FA) bypass, QR codes, and other advanced evasion tactics to maximize success, researchers have found.

Security analysts from EclecticIQ in February discovered a broad phishing campaign targeting financial institutions, in which threat actors used embedded QR codes in PDF attachments to redirect victims to phishing URLs, according to a blog post published June 18. Specific organizations targeted included banks, private funding firms, and credit union service providers across the Americas and Europe, Middle East and Africa (EMEA) regions.

EclecticIQ eventually tracked the origin of the campaign to a PhaaS platform called ONNX Store, "which operates through a user-friendly interface accessible via Telegram bots," Eclectic IQ threat intelligence analyst Arda Büyükkaya wrote in the post.

A key part of the ONNX service is a 2FA bypass mechanism that intercepts 2FA requests from victims using encrypted JavaScript code, to decrease the likelihood of detection and bolster the success rate of attacks, Büyükkaya noted. Moreover, the phishing pages delivered in the attacks use typosquatting to closely resemble Microsoft 365 login interfaces, making them more likely to trick targets into entering their authentication details.

Snapshot of an ONNX Attack

A typical email used in the attack shows a threat actor purporting to send the employee a human resources-related PDF document, such as an employee handbook or a salary remittance slip. The document impersonates Adobe or Microsoft 365 to try to trick a recipient into opening the attachment via a QR code that, once scanned, directs victims to a phishing landing page.

The use of QR codes is an increasingly common tactic for evading endpoint detection, Büyükkaya noted: "Since QR codes are typically scanned by mobile phones, many organizations lack detection or prevention capabilities on employees' mobile devices, making it challenging to monitor these threats."

The attacker-controlled landing page is designed to steal login credentials and 2FA authentication codes using the adversary-in-the-middle (AitM) method, analysts found.

"When victims enter their credentials, the phishing server collects the stolen information via WebSockets protocol, which allows real-time, two-way communication between the user's browser and the server," Büyükkaya wrote. In this way, attackers can quickly capture and transmit stolen data without the need for frequent HTTP requests, making the phishing operation more efficient and harder to detect, he noted.

Another PhaaS operator, Tycoon, also has used a similar AitM technique and a multifactor authentication (MFA) bypass involving a Cloudflare CAPTCHA, demonstrating how malicious actors are learning from each other and adapting strategies accordingly, Büyükkaya said.

ONNX also shares overlap in both Telegram infrastructure and advertising methods with a phishing kit called Caffeine (first discovered by researchers at Mandiant in 2022), the researchers found — so it could be a rebranding of that operation, according to ElecticIQ.

Another scenario is that the Arabic-speaking threat actor MRxC0DER, who is believed to have developed and maintained Caffeine, is providing client support to the ONNX Store, while the broader operation "is likely managed independently by a new entity without central management," Büyükkaya wrote.

JavaScript Encryption Adds Level of Evasion

Another anti-detection measure in the ONNX phishing kit is the use of encrypted JavaScript code that decrypts itself during page load, and includes a basic anti-JavaScript debugging feature. "This adds a layer of protection against anti-phishing scanners and complicates analysis," according to the analysis.

EclecticIQ researchers observed a functionality in the decrypted JavaScript code that's specifically designed to steal 2FA tokens entered by the victims and relay them to the attacker, who then uses the stolen credentials and tokens in real time to log in to Microsoft 365.

"This real-time relay of credentials allows the attacker to gain unauthorized access to the victim's account before the 2FA token expires, circumventing multifactor authentication," Büyükkaya wrote.

Mitigating and Preventing ONNX Phishing Attacks

ElecticIQ provided countermeasures for combatting specific tactics used by ONNX Store. To mitigate threats from embedded QR codes in PDF documents, organizations should block PDF or HTML attachments from unverified external sources in email server settings. They also can educate employees on the risks associated with scanning QR codes from unknown sources.

To combat the typosquatted domains used by the threat actor to impersonate Microsoft, organizations can implement domain name system security extensions (DNSSEC), which protects domains from multiple cyber threats, including typosquatting.

There are also measures that defenders can take to combat the theft of 2FA tokens, such as implementing FIDO2 hardware security keys for 2FA; setting a short expiration time for login tokens that limits a cyberattacker's window of opportunity to use them; and using security monitoring tools to detect and alert for any unusual behavior, such as multiple failed login attempts or logins from unusual locations.

About the Author

Elizabeth Montalbano, Contributing Writer

Elizabeth Montalbano is a freelance writer, journalist, and therapeutic writing mentor with more than 25 years of professional experience. Her areas of expertise include technology, business, and culture. Elizabeth previously lived and worked as a full-time journalist in Phoenix, San Francisco, and New...

You May Also Like

Remote Workforce ond SolarWinds Critical Bug in Web Help Desk

Remote Workforce xel Phone Has a Verizon App that Doubles As a Backdoor

Remote Workforce or 'Evil Twin' Wi-Fi That Steals Airline Passenger Data

Remote Workforce ' Attackers Steal Millions of Career Records

More Insights

Webinars

Unleashing AI to Assess Cyber Security Risk
NOV 12, 2024

Securing Tomorrow, Today: How to Navigate Zero Trust
NOV 13, 2024

The State of Attack Surface Management (ASM), Featuring Forrester
NOV 15, 2024

Applying the Principle of Least Privilege to the Cloud
NOV 18, 2024

The Right Way to Use Artificial Intelligence and Machine Learning in Incident Response
NOV 20, 2024

More Webinars

Events

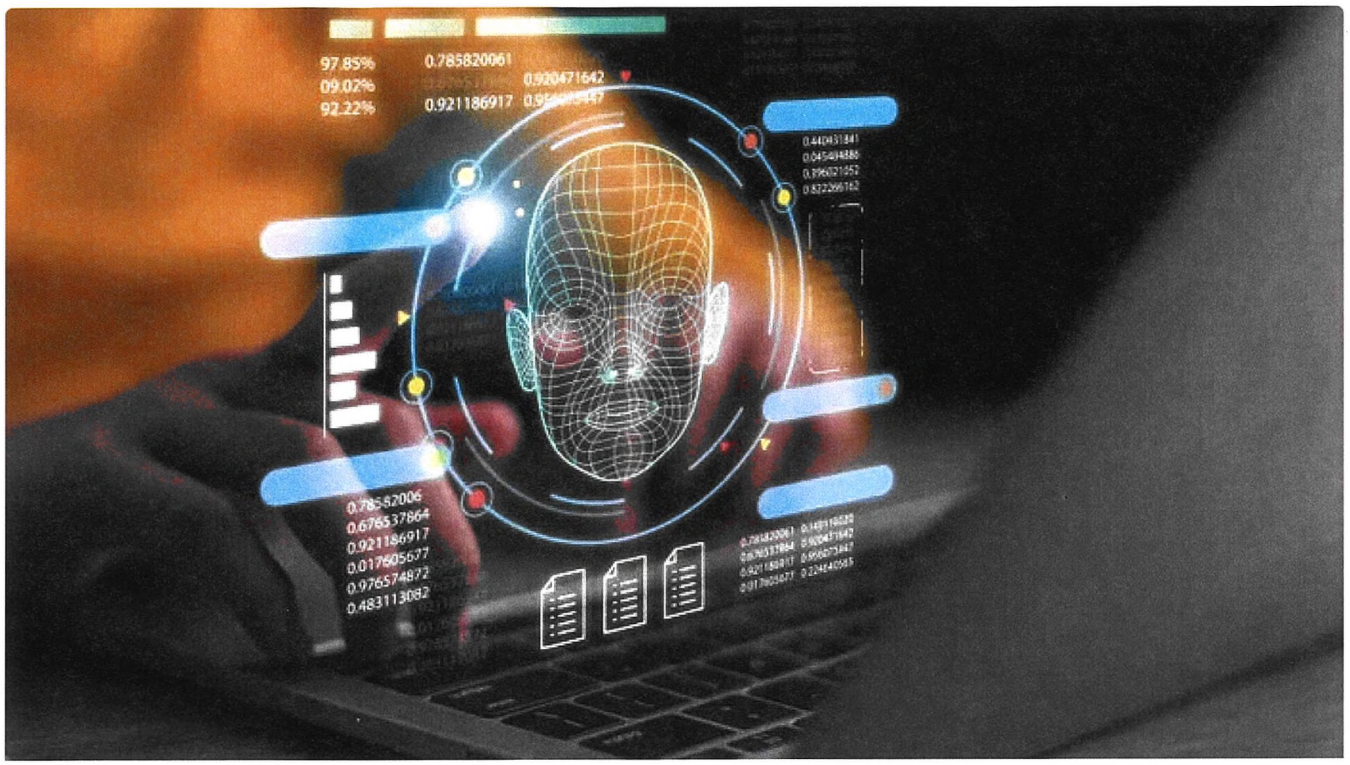
Know Your Enemy: Understanding Cybercriminals and Nation-State Threat Actors

Cybersecurity Outlook 2025

More Events

Editor's Choice

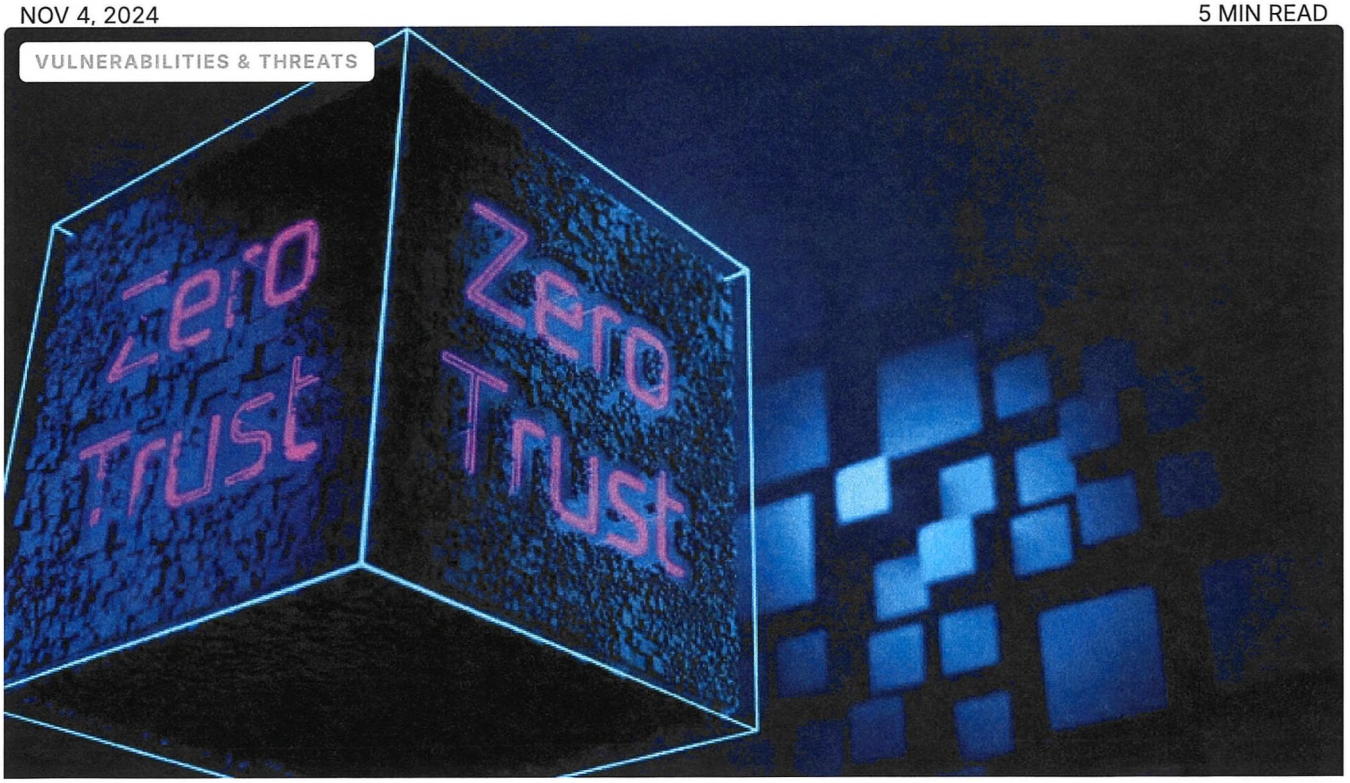
VULNERABILITIES & THREATS



OWASP Beefs Up GenAI Security Guidance Amid Growing Deepfakes

by **Robert Lemos, Contributing Writer**

NOV 4, 2024 5 MIN READ



How to Win at Cyber by Influencing People

by **Gregory R. Simpson**

NOV 5, 2024 5 MIN READ

Cybersecurity Job Market Stagnates, Dissatisfaction Abounds

by **Tara Seals, Managing Editor, News, Dark Reading**

OCT 31, 2024 4 MIN READ

Reports

Managing Third-Party Risk Through Situational Awareness
JUL 31, 2024

2024 InformationWeek US IT Salary Report
MAY 29, 2024

More Reports

Webinars

Unleashing AI to Assess Cyber Security Risk
NOV 12, 2024

Securing Tomorrow, Today: How to Navigate Zero Trust
NOV 13, 2024

The State of Attack Surface Management (ASM), Featuring Forrester
NOV 15, 2024

Applying the Principle of Least Privilege to the Cloud
NOV 18, 2024

The Right Way to Use Artificial Intelligence and Machine Learning in Incident Response
NOV 20, 2024

More Webinars

White Papers

Top 10 CI/CD Security Risks: The Technical Guide

The State of Vulnerability Management in the Enterprise

Product Review: Trend Vision One Cloud Security

IDC White Paper: The Peril and Promise of Generative AI in Application Security

Solution Brief: Introducing the runZero Platform

More Whitepapers

Events

Know Your Enemy: Understanding Cybercriminals and Nation-State Threat Actors
NOV 14, 2024

Cybersecurity Outlook 2025
DEC 5, 2024

More Events

DARKREADING

Discover More With Informa Tech

Black Hat

Omdia

Working With Us

About Us

Advertise

Reprints

Join Us

NEWSLETTER SIGN-UP

Follow Us

ONNX phishing service targets Microsoft 365 accounts at financial firms

By
Bill Toulas
(https://www.bleepingcomputer.com/author/bill-toulas/)

June 18, 2024 04:28 PM 0

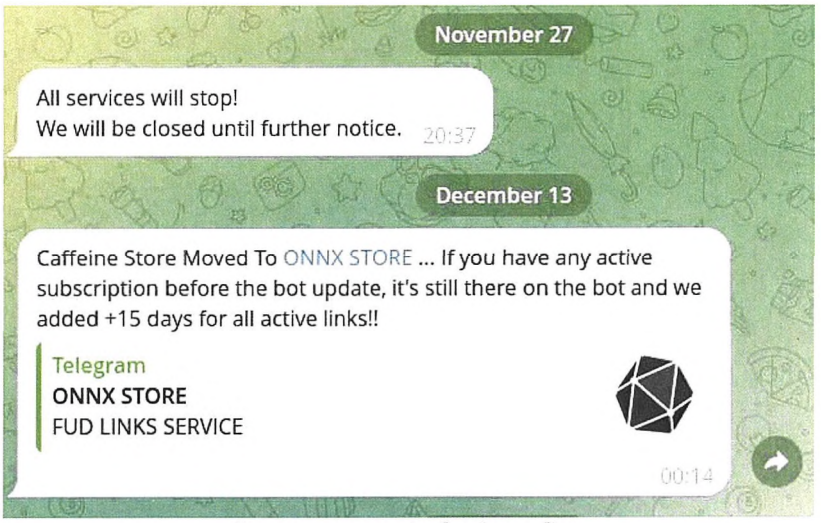
A new phishing-as-a-service (PhaaS) platform called ONNX Store is targeting Microsoft 365 accounts for employees at financial firms using QR codes in PDF attachments.

The platform can target both Microsoft 365 and Office 365 email accounts and operates via Telegram bots and features two-factor authentication (2FA) bypass mechanisms.

Researchers at EclecticIQ (https://blog.eclecticiq.com/onnx-store-targeting-financial-institution) who discovered the activity believe that ONNX is a rebranded version of the Caffeine phishing kit managed by

the Arabic-speaking threat actor MRxCoDER.

Mandiant discovered caffeine in October 2022, when the platform targeted Russian and Chinese platforms instead of Western services.



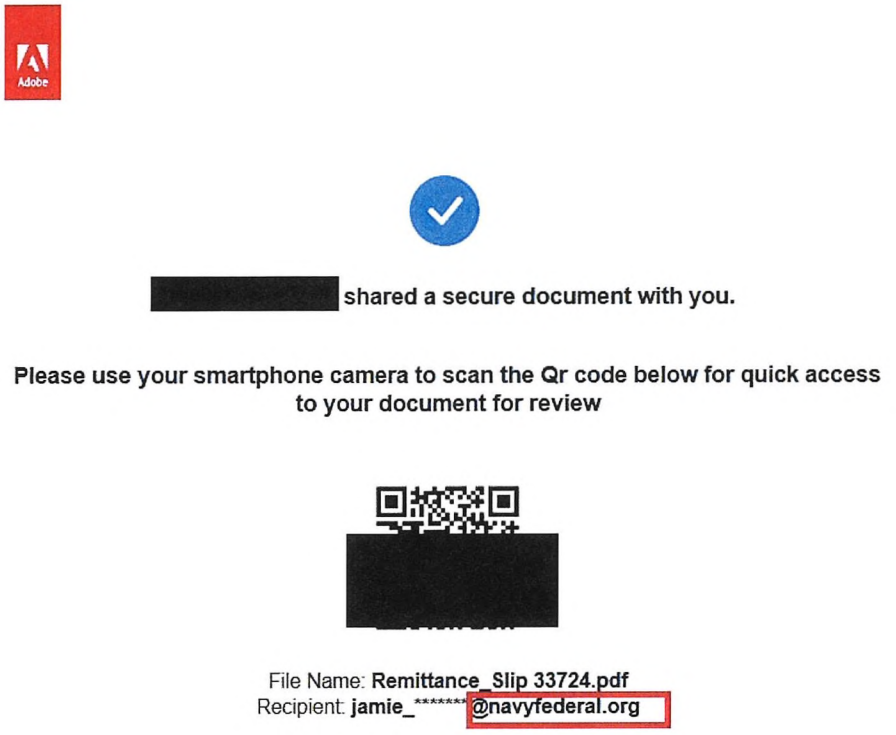
Announcement of rebranding

Source: EclecticIQ

ONNX attacks

EclecticIQ observed ONNX attacks in February 2024, distributing phishing emails with PDF attachments containing malicious QR codes that targeted employees at banks, credit union service providers, and private funding firms.

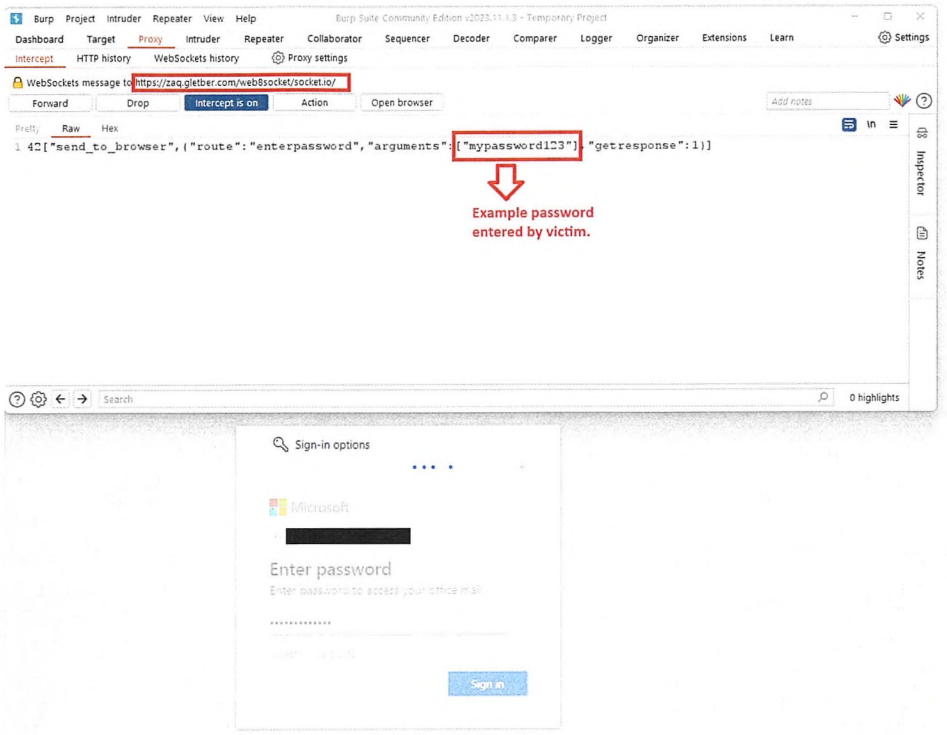
The emails impersonate human resources (HR) departments, using salary updates as lures to open the PDFs, which are themed after Adobe or Microsoft.



Malicious PDF attachment

Source: EclecticIQ

Scanning the QR code on a mobile device bypasses phishing protections on the targeted organizations, taking victims to phishing pages that mimic the legitimate Microsoft 365 login interface.



The Microsoft 365 phishing page

Source: EclecticIQ

The victim is prompted to enter their login credentials and 2FA token on the fake login page, and the phishing site captures these details in real-time.

The stolen credentials and 2FA token are immediately relayed to the attackers via WebSockets, allowing them to hijack the target's account before the authentication and MFA-validated token expires.

```
const verifyotpbtn = document.getElementById('btn_verifyotp');
verifyotpbtn.addEventListener('click', () => {
    const otpInput = document.getElementById("inp_otpcode");
    loadinganimation(0x0);
    sendAndReceive("enterotp", [otpInput.value], 0x1).then(response => {
        if (response) {
            loadinganimation(0x1);
            if (response.message == "valid otp") {
                document.getElementById('otpdesc').innerText = '';
                document.getElementById("section_otp").classList.toggle("d-none");
                document.getElementById("section_final").classList.remove("d-none");
                view = 'final';
            }
            if (response.message == "error" && response.description != "The wrong code was entered. Send yourself a new
code and try again.") {
                bottomsectionlinks("otp", response.bottomsection);
                changebackbutton("otp", response.backbutton);
                checkerrordesc("otp", 0x1, response.description);
            }
            if (response.message == "error" && response.description == "The wrong code was entered. Send yourself a new
code and try again.") {
                bottomsectionlinks("2fa", response.bottomsection);
                changebackbutton("2fa", response.backbutton);
                document.getElementById("error_otp").innerText = '';
                document.getElementById("section_otp").classList.toggle('d-none');
                document.getElementById("section_2fa").classList.remove("d-none");
            }
        }
    }).catch(error => {
        loadinganimation(0x1);
        console.error('Error:', error);
    });
});
```

The 2FA bypassing mechanism

Source: EclecticIQ

From there, the attackers can access the compromised email account to exfiltrate sensitive information such as emails and documents or sell the credentials on the dark web for malware and ransomware attacks.

Robust phishing platform

From the perspective of the cybercriminals using the service, ONNX is a compelling and cost-effective platform.

The center of operations is on Telegram, where bots enable clients to manage their phishing operations through an intuitive interface. Moreover, there are dedicated support channels to assist users with any issues.

The Microsoft Office 365 phishing templates are customizable, and webmail services are available for sending phishing emails to targets.

The ONNX phishing kit also uses encrypted JavaScript code that decrypts itself during page load, adding a layer of obfuscation to evade detection by anti-phishing tools and scanners.

Additionally, ONNX uses Cloudflare services to prevent its domains from being taken down, including an anti-bot CAPTCHA and IP proxying.

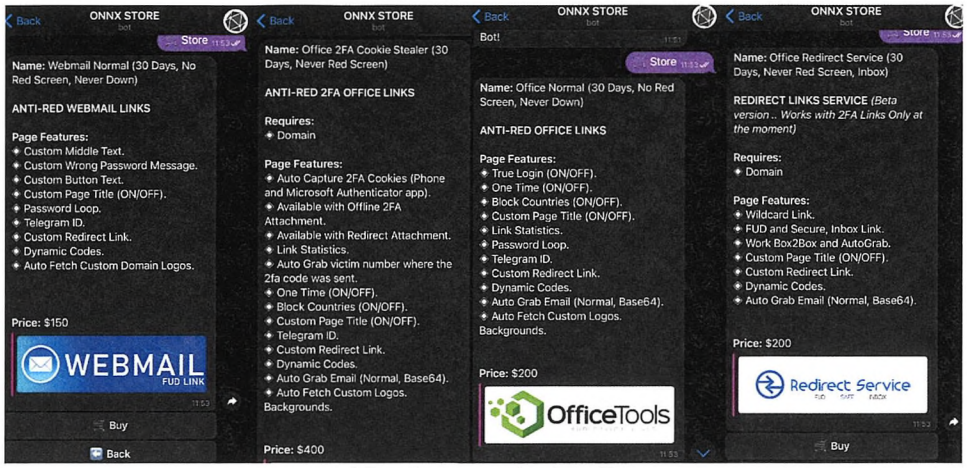
There is also a bulletproof hosting service to ensure that the operations aren't interrupted by reports and takedowns, as well as remote desktop protocol (RDP) services for managing the campaigns securely.

Bulletproof hosting offer

Source: EclecticIQ

ONNX offers four subscription tiers summarized as follows:

- **Webmail Normal ($150/month)**: Offers customizable text elements, a password loop, Telegram ID integration, custom redirect links, and auto-fetch custom domain logos.
- **Office Normal ($200/month)**: Includes true login, one-time passwords, country blocking, custom page titles, password loops, Telegram integration, and custom logos.
- **Office Redirect ($200/month)**: Provides wildcard links, fully undetectable inbox links, custom page titles, dynamic codes, and auto-grab email functionality for 2FA redirects.
- **Office 2FA Cookie Stealer ($400/month)**: Captures 2FA cookies, supports offline 2FA, and includes custom page titles, Telegram integration, dynamic codes, and link statistics.



Tier features in detail

Source: EclecticIQ

All in all, ONNX Store is a dangerous threat for Microsoft 365 account holders, especially for companies engaged in the broader financial services sectors.

To protect against its sophisticated phishing attacks, admins are recommended to block PDF and HTML attachments from unverified sources, block access to HTTPS websites with untrusted or expired certificates, and set up FIDO2 hardware security keys for high-risk, privileged accounts.

EclecticIQ has also shared YARA rules in its report to help detect malicious PDF files that contain QR codes leading to phishing URLs.

Related Articles:

New Mamba 2FA bypass service targets Microsoft 365 accounts (https://www.bleepingcomputer.com/news/security/new-mamba-2fa-bypass-service-targets-microsoft-365-accounts/)

Police dismantles phone unlocking ring linked to 483,000 victims (https://www.bleepingcomputer.com/news/security/police-dismantles-iserver-phone-unlocking-network-linked-to-483-000-victims/)

Scammers target UK senior citizens with Winter Fuel Payment texts (https://www.bleepingcomputer.com/news/security/scammers-target-uk-senior-citizens-with-winter-fuel-payment-texts/)

Hackers now use ZIP file concatenation to evade detection (https://www.bleepingcomputer.com/news/security/hackers-now-use-zip-file-concatenation-to-evade-detection/)

DocuSign's Envelopes API abused to send realistic fake invoices (https://www.bleepingcomputer.com/news/security/docusigns-envelopes-api-abused-to-send-realistic-fake-invoices/)

CAFFEINE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/CAFFEINE/)

MICROSOFT 365 (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/MICROSOFT-365/)

OFFICE 365 (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/OFFICE-365/)

ONNX (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/ONNX/)

PHAAS (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/PHAAS/)

PHISHING (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/PHISHING/)

PHISHING-AS-A-SERVICE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/PHISHING-AS-A-SERVICE/)

(https://www.bleepingcomputer.com/author/bill-toulas/)

BILL TOULAS (HTTPS://WWW.BLEEPINGCOMPUTER.COM/AUTHOR/BILL-TOULAS/)

(MAILTO:BILL.TOULAS@BLEEPINGCOMPUTER.COM)

(HTTPS://TWITTER.COM/BILLTOULAS)

Bill Toulas is a tech writer and infosec news reporter with over a decade of experience working on various online publications, covering open-source, Linux, malware, data breach incidents, and hacks.

PREVIOUS ARTICLE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/NEWS/SECURITY/AMAZON-TOP-BRANDS-AND-SERVICES-WITH-35-OFF-A-ONE-YEAR-BJS-CLUB-CARD/)

NEXT ARTICLE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/NEWS/SECURITY/AI INVESTIGATES-BREACH-AFTER-DATA-FOR-SALE-ON-HACKING-FORUM/)

You may also like:

POPULAR STORIES

Hackers now use ZIP file concatenation to evade detection
(https://www.bleepingcomputer.com/news/security/hackers-now-use-zip-file-concatenation-to-evade-detection/)

Unpatched Mazda Connect bugs let hackers install persistent malware
(https://www.bleepingcomputer.com/news/security/unpatched-mazda-connect-bugs-let-hackers-install-persistent-malware/)

Malicious PyPI package with 37,000 downloads steals AWS keys
(https://www.bleepingcomputer.com/news/security/malicious-pypi-package-with-37-000-downloads-steals-aws-keys/)

SPONSOR POSTS

Automate all things security in the Blink of AI
(https://www.blinkops.com/?utm_source=bleepingcomputer&utm_medium=article&utm_campaign=cloud_automation)

sponsored-
content&utm_content=K12funding)

FOLLOW US:

(https://www.bleepingcomputer.com)

MAIN SECTIONS

(https://www.bleepingcomputer.com/)

(https://www.bleepingcomputer.com/vpn/)

(https://www.bleepingcomputer.com/sysadmin/)

(https://www.bleepingcomputer.com/download/)

(https://www.bleepingcomputer.com/virus-removal/)

(https://www.bleepingcomputer.com/tutorials/)

(https://www.bleepingcomputer.com/startups/)

(https://www.bleepingcomputer.com/uninstall/)

(https://www.bleepingcomputer.com/glossary/)

COMMUNITY

(https://www.bleepingcomputer.com/forums/)

(https://www.bleepingcomputer.com/forum-rules/)

(https://www.bleepingcomputer.com/forums/t/730914/the-bleepingcomputer-official-discord-chat-server-come-join-the-fun/)

USEFUL RESOURCES

(https://www.bleepingcomputer.com/welcome-guide/)

(https://www.bleepingcomputer.com/sitemap/)

COMPANY

(https://www.bleepingcomputer.com/about/)

(https://www.bleepingcomputer.com/contact/)

(https://www.bleepingcomputer.com/news-tip/)

(https://www.bleepingcomputer.com/advertise/)

(https://www.bleepingcomputer.com/write-for-bleepingcomputer/)

(https://www.bleepingcomputer.com/rss-feeds/)

(https://www.bleepingcomputer.com/changelog/)