# Onnx Phishing Service Targets Microsoft 365 Accounts at Financial Firms

Date: 19th June 2024 | Severity: High

## Summary

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.

## Attack Vectors

- ONNX attacks 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.
- 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 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.
- 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.

# Indicator of compromise

| INDICATOR TYPE | INDICATORS |
|---|---|
| File Hash | • 432b1b688e21e43d2ccc68e040b3ecac4734b7d1d4356049f9e1297814627cb3<br>• 47b12127c3d1d2af24f6d230e8e86a7b0c661b4e70ba3b77a9beca4998a491ea<br>• 51fdaa65511e7c3a8d4d08af59d310a2ad8a18093ca8d3c817147d79a89f44a1<br>• f99b01620ef174bb48e22e54327ca9cffa4520868f49a41c524b81ab6d935070<br>• 52e04c615b08af10b4982506c1cee74cb062116d31f0300ed027f6efd3119b1a<br>• 3d58733b646431a60d39394be99ff083d6db3583796b503e8422baebed8d097e<br>• 702008cae9a145741e817e6c6566cd1d79c737d51b718f13a2d16d72a00cd5a7<br>• 908af49857b6f5d1e0384a5e6fc8ee53ca1df077601843ebdd7fc8a4db8bcb12<br>• d3b03f79cf1d088d2ed41e25c961e9945533aeabb93eac2d33ebc4b589ba6172<br>• 4751234ac4e1b0a5d4685b870de1ea1a7754258977f5d1d9534631c09c748732 |
| Domains | • authmicronlineonfication[.]com<br>• verify-office-outlook[.]com<br>• stream-verify-login[.]com<br>• zaq[.]gletber[.]com<br>• v744[.]r9gh2[.]com<br>• bsifinancial019[.]ssllst[.]cloud<br>• 473[.]kernam[.]com<br>• docusign[.]multiparteurope[.]com<br>• 56789iugtfrd5t69i9ei9die9di9eidy7u889[.]rhiltons[.]com<br>• agchoice[.]us-hindus[.]com |

# Recommendation

- Submit the File Hash to the Antivirus team to update their database with the file hashes.
- Submit the Domains to the Network team to update their database with the Domains.
- Secure RDP ports to prevent threat actors from abusing and leveraging RDP tools.
- Prioritize remediating known exploited vulnerabilities.
- Implement EDR solutions to disrupt threat actor memory allocation techniques.
- Make regular backups of important and critical files.
- Avoid browsing the unsafe websites, clicking on suspicious links, or opening unknown email attachments.
- Update and Patch operating system, applications, and security software's up to date with latest patches.

**NOTE:** The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

# Reference Links

- https://www.bleepingcomputer.com/news/security/onnx-phishing-service-targets-microsoft-365-accounts-at-financial-firms/
- https://blog.eclecticiq.com/onnx-store-targeting-financial-institution