BOLETIM DE SEGURANÇA

Phishing ONNX tem como alvo contas do Microsoft 365 em empresas financeiras

heimdall
security research
A DIVISION OF ISH

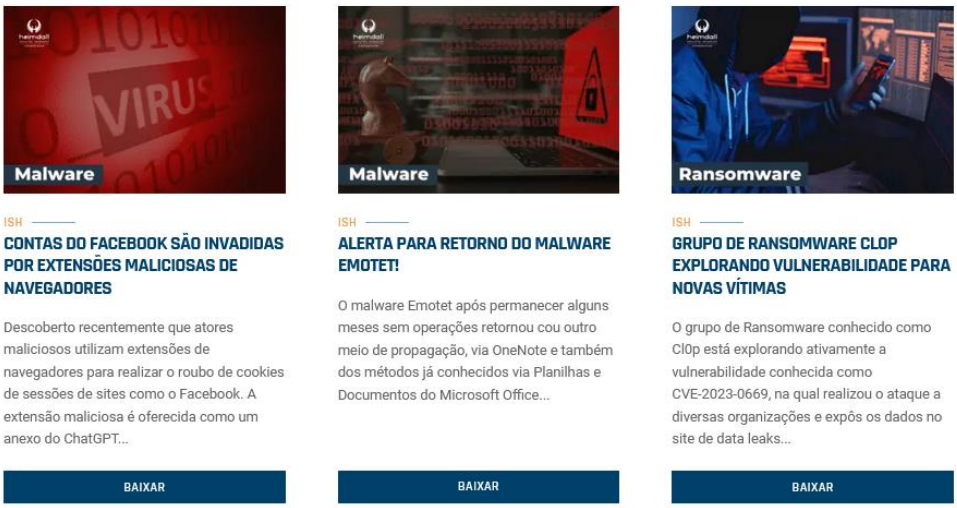
TLP: CLEAR

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso **X**.

[Heimdall Security Research]

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

[Boletins de Segurança – Heimdall]



SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

A ONNX Store, uma emergente plataforma de phishing como serviço (PhaaS), está direcionando suas ações para contas do Microsoft 365. O público-alvo principal são os funcionários de empresas financeiras. A estratégia utilizada envolve o uso de códigos QR em anexos de PDF, aumentando a sofisticação e a eficácia dos ataques de phishing.

2 INFORMAÇÃO SOBRE A AMEAÇA

Em fevereiro de 2024, campanhas de phishing voltadas para instituições financeiras foram identificadas por analistas da EclecticIQ. Os perpetradores dessas ameaças utilizaram códigos QR, inseridos em anexos de PDF, com o objetivo de redirecionar as vítimas para URLs de phishing. A plataforma responsável por impulsionar essas campanhas é a ONNX Store, uma Phishing-as-a-Service (PhaaS). Esta plataforma opera por meio de uma interface de fácil utilização, acessível através de bots do Telegram, facilitando a execução de ataques de phishing.

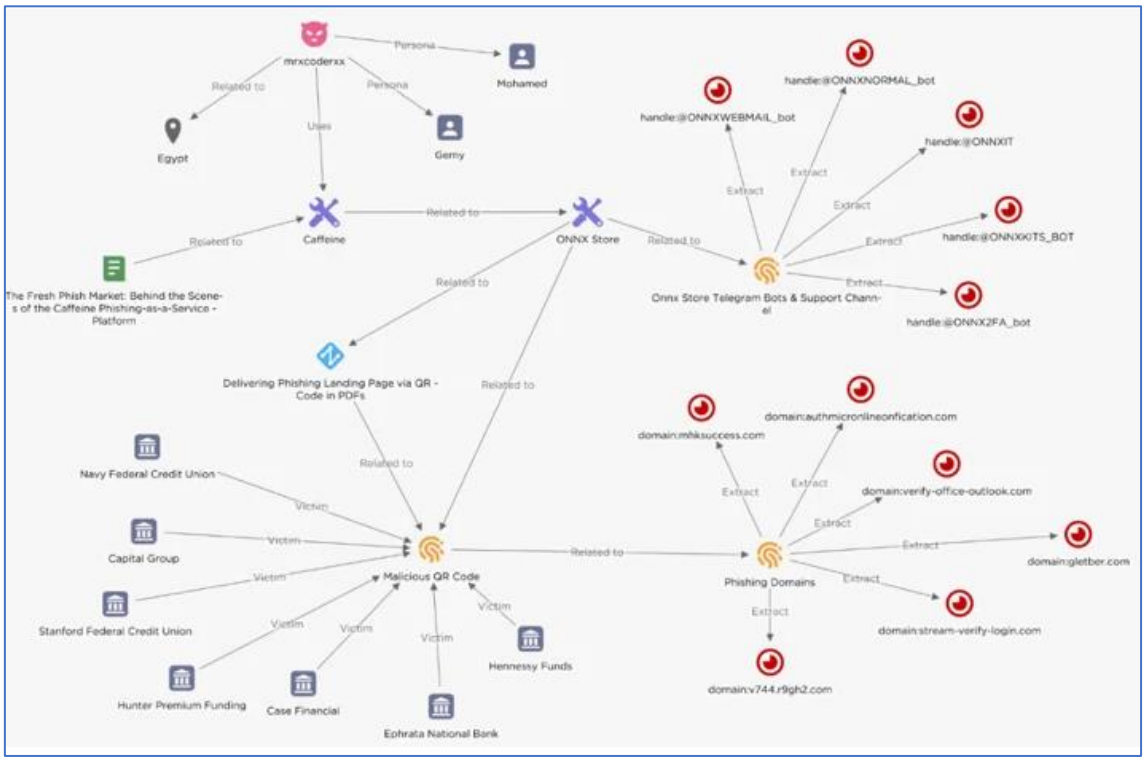


Figura 1 – Visão geral do armazenamento ONNX.

A ONNX Store, uma plataforma de phishing, possui um recurso que permite burlar a autenticação de dois fatores (2FA), interceptando as solicitações 2FA das vítimas. Isso aumenta a eficácia dos ataques de comprometimento de email comercial (BEC). As páginas de phishing da plataforma são semelhantes às interfaces de login do Microsoft 365, enganando os usuários a fornecerem suas credenciais. Acredita-se, que o kit de phishing da ONNX Store é provavelmente uma versão renomeada do kit de phishing de cafeína, descoberto pela Mandiant em 2022. Essa avaliação é baseada em semelhanças na infraestrutura e na publicidade nos canais do Telegram. Foi avaliado que o ator de ameaças de língua árabe, MRxC0DER (também conhecido como mrxcoderxx), é provavelmente o desenvolvedor e mantenedor do kit Caffeine. Essa conclusão é baseada em várias evidências, incluindo vídeos do autor da ameaça, onde as configurações do idioma árabe foram observadas como padrão no navegador.

A ONNX Store é provavelmente gerenciada de forma independente por uma nova entidade sem gerenciamento central, enquanto o MRxC0DER é provavelmente responsável pelo suporte ao cliente. Essa avaliação é baseada em publicações na conta de suporte do Telegram da ONNX Store. Os analistas da EclecticIQ acreditam, com alta confiança, que a ONNX Store é uma reformulação da marca da plataforma Caffeine, devido às semelhanças nas estratégias operacionais e nos padrões do servidor backend. Em 2023, o antigo canal Caffeine Telegram anunciou uma atualização de rebranding, informando que as operadoras adotaram um novo modelo operacional e lançaram um novo canal chamado ONNX Store.

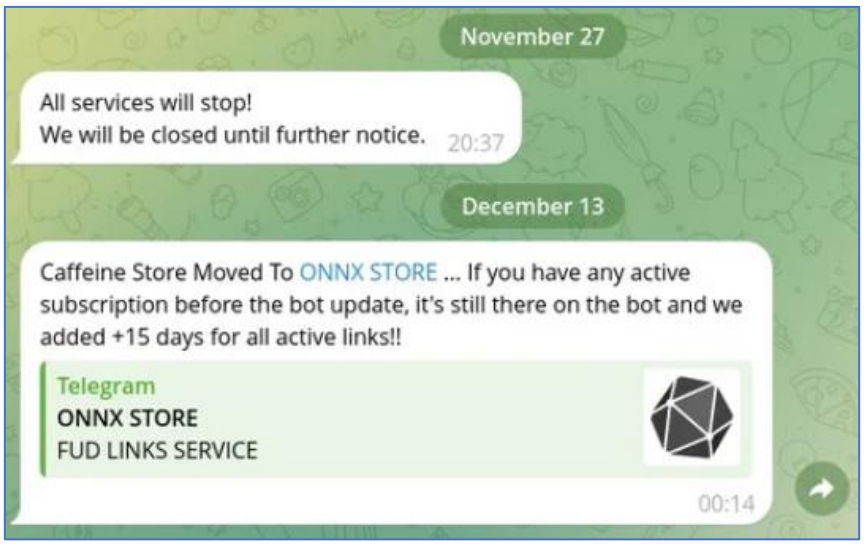


Figura 2 – Anúncio de rebranding.

A ONNX Store utiliza a Cloudflare para retardar a eliminação de domínios de phishing. A Cloudflare disponibiliza recursos legítimos de CAPTCHA anti-bot e proxy de IP para salvaguardar sites de diversas ameaças. Contudo, os agentes de ameaças exploram esses recursos para proteger seus serviços mal-intencionados. O CAPTCHA da Cloudflare auxilia na prevenção da detecção por scanners de sites de phishing e sandboxes de URL. Além disso, o proxy de IP da Cloudflare mascara o provedor de hospedagem original, dificultando a remoção de domínios de phishing estabelecidos através da ONNX Store.

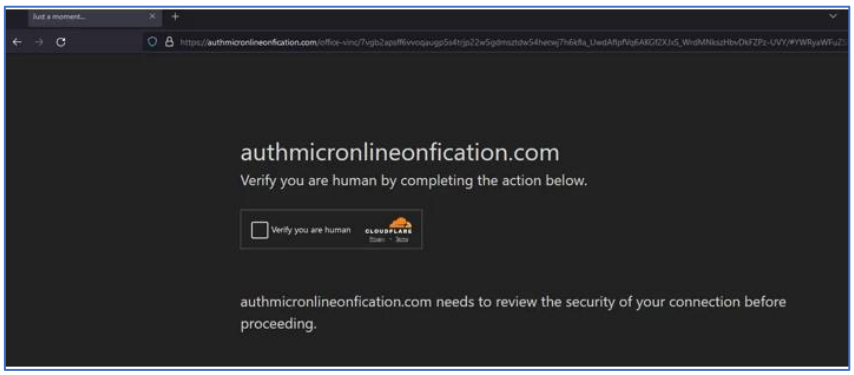


Figura 3 – Página de phishing está por trás do anti-bot Cloudflare..

Observou-se que os agentes de ameaças utilizam os serviços da ONNX Store para disseminar documentos PDF através de anexos de e-mails de phishing. Estes documentos imitam serviços confiáveis, como Adobe ou Microsoft 365, e empregam estratégias de engenharia social para se passarem por atualizações de salários do departamento de RH ou manuais de funcionários. Cada PDF possui um código QR que, ao ser escaneado, redireciona as vítimas para páginas de phishing mal-intencionadas.

Os agentes de ameaças optam por códigos QR para evitar a detecção de endpoints. Dado que os códigos QR são geralmente escaneados por celulares, muitas organizações não dispõem de recursos de detecção ou prevenção nos dispositivos móveis de seus funcionários, o que dificulta o monitoramento dessas ameaças. A maioria das campanhas de phishing observadas visam instituições financeiras, incluindo bancos, empresas de financiamento privado e provedores de serviços de cooperativas de crédito nas regiões EMEA e AMER.

O exemplo abaixo de documento PDF mal-intencionado direcionado à Navy Federal Credit Union, que presta serviços a membros de diversos ramos do pessoal do Departamento de Defesa dos Estados Unidos, veteranos e seus familiares.

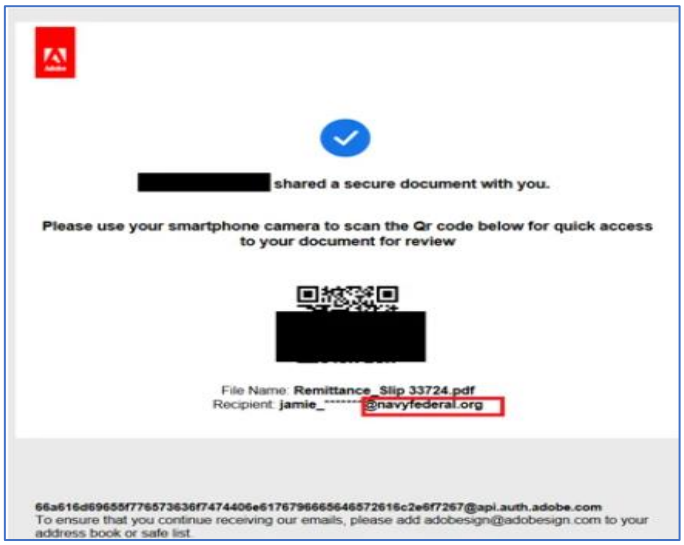


Figura 4 – Documento PDF com código QR malicioso.

Ao escanear o código QR, as vítimas são direcionadas para uma página de phishing sob o controle do invasor. Esta página tem como objetivo roubar credenciais de login e códigos de autenticação 2FA, utilizando o método Adversary-in-The-Middle (AiTM). Um exemplo disso é um site de phishing que se passa por uma página de login do Microsoft 365. Quando as vítimas inserem suas credenciais, o servidor de phishing recolhe as informações roubadas através do protocolo WebSockets. Este protocolo permite uma comunicação bidirecional em tempo real entre o navegador do usuário e o servidor. Os invasores utilizam WebSockets para capturar e transmitir rapidamente os dados roubados, sem a necessidade de solicitações HTTP frequentes, tornando a operação de phishing mais eficaz e mais difícil de ser detectada.

Foi observado que outra plataforma de Phishing como serviço, Tycoon, também utiliza uma técnica AiTM semelhante com Cloudflare CAPTCHA. Isso indica uma tendência de aprendizado e adaptação entre os agentes mal-intencionados, que aprimoram suas táticas emulando operações bem-sucedidas observadas no cenário do crime cibernético.

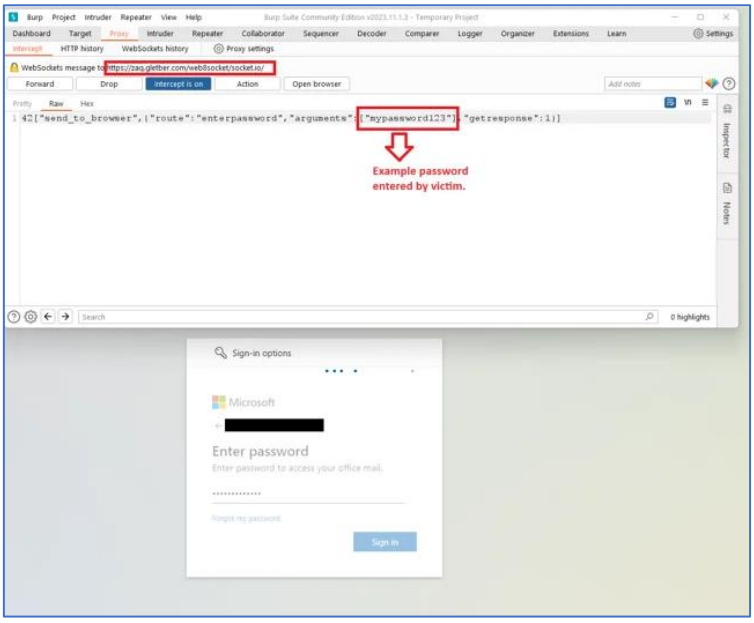


Figura 5 – Página inicial de phishing do Microsoft 365.

Um anúncio detectado em um grupo do Telegram revela um serviço de hospedagem Bulletproof em desenvolvimento, acessível via RDP (Remote Desktop Protocol). Este serviço é comercializado não só para phishing, mas também para uma variedade de campanhas maliciosas, oferecendo recursos de alto desempenho, como velocidades melhoradas de RAM, CPU e SSD, além de largura de banda ilimitada. A publicidade destaca a facilidade de gerenciamento através de bots automatizados e disponibilidade constante, tornando-o uma ferramenta eficaz para várias atividades maliciosas online.

Figura 6 – Anúncio de hospedagem RDP Bulletproof do ONNX.

Criminosos cibernéticos com motivação financeira estão criando serviços de kits de ferramentas de phishing, como o ONNX Store, para auxiliar outros atores de ameaças e gerar receita. Essas plataformas permitem que cibercriminosos lancem campanhas de phishing com facilidade, utilizando recursos como mecanismos de desvio de 2FA e páginas de phishing realistas. Eles também fornecem um nível de segurança operacional que pode ocultar a identidade real do executor da campanha.

As credenciais de e-mail roubadas por meio dessas campanhas de phishing são frequentemente vendidas em fóruns clandestinos. Grupos de ransomware valorizam essas credenciais, usando-as como um vetor inicial de comprometimento para infiltrar-se nas organizações alvo. Isso ressalta as implicações mais amplas dessas plataformas de phishing, pois elas não apenas permitem ganhos financeiros imediatos através do roubo de credenciais, mas também contribuem para comprometimentos em nível de domínio, como ataques de ransomware.

3 MITRE ATT&CK - TTPs

Tática	Técnica	Detalhes
Initial Access	T1566.001	Consiste em técnicas que utilizam vários vetores de entrada para obter sua posição inicial dentro de uma rede.
Execution	T1204	Consiste em técnicas que resultam na execução de código controlado pelo adversário em um sistema local ou remoto.
Credential Access	T1539 T1557	Consiste em técnicas para roubar credenciais, como nomes de contas e senhas. As técnicas usadas para obter credenciais incluem keylogging ou despejo de credenciais.
Exfiltration	T1567	Consiste em técnicas que os adversários podem usar para roubar dados da sua rede. Depois de coletar os dados, os adversários geralmente os empacotam para evitar a detecção enquanto os removem.
Command and Control	T1132.001 T1090.004	Consiste em técnicas que os adversários podem usar para se comunicar com sistemas sob seu controle dentro de uma rede vítima.
Defense Evasion	T1027	Consiste em técnicas que os adversários usam para evitar a detecção durante todo o seu comprometimento.
Collection	T1114	Consiste em técnicas que os adversários podem usar para coletar informações e nas fontes das quais as informações são coletadas que são relevantes para cumprir os objetivos do adversário.

Tabela 1 – Tabela MITRE ATT&CK.

4 RECOMENDAÇÕES

Além dos indicadores de comprometimento elencados abaixo pela ISH, poderão ser adotadas medidas visando a mitigação da infecção do referido *malware*, como por exemplo:

Verifique os e-mails com atenção

- Procure sinais reveladores de phishing em e-mails recebidos antes de responder ou seguir suas instruções.

Verifique o link antes de abrir

- Se o link tiver algum problema ortográfico, é provável que seja uma tentativa de enganá-lo com uma página falsa.

Mensagens de endereços duvidosos

- Evite clicar em links que pareçam suspeitos ou que redirecionem para sites não confiáveis.

Encerre a sessão de dispositivos

- É importante encerrar a sessão de qualquer programa, site ou aplicativo ao terminar de usá-lo.

Faça um backup

- O backup ajuda a proteger os dados mais importantes do usuário.

Educação e Conscientização

- Realize treinamentos regulares e simulações de phishing para ensinar os funcionários a reconhecer e reagir adequadamente a tentativas de phishing.

5 INDICADORES DE COMPROMISSOS

A ISH Tecnologia realiza o tratamento de diversos indicadores de compromissos coletados por meio de fontes abertas, fechadas e também de análises realizadas pela equipe de segurança Heimdall. Diante disto, abaixo listamos todos os Indicadores de Compromissos (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

Indicadores de compromisso do artefato	
md5:	0250a5ba26791e7ffddb4b294d486479
sha1:	ebcfcc832b957598354d3a2faacacf6fa91b58cb
sha256:	432b1b688e21e43d2ccc68e040b3ecac4734b7d1d4356049f9e1297814627cb3
File name:	Adobe_Epnb_Remittance 0MS9-HONZ7Q-NTW3.pdf

Indicadores de compromisso do artefato	
md5:	83dac37771e8592e006f671666ebf590
sha1:	6b2db1e10fcc74fe864dbe6399b6d26d0d67d3f3
sha256:	47b12127c3d1d2af24f6d230e8e86a7b0c661b4e70ba3b77a9beca4998a491ea
File name:	Adobe_Epnb_Remittance 6XR7-LBPS2T-EWI5.pdf

Indicadores de compromisso do artefato	
md5:	6193c137f3b5b0da106b86f74670cf6f
sha1:	5dfef0d6a7ae77355278706323e71ac96686615b
sha256:	51fdaa65511e7c3a8d4d08af59d310a2ad8a18093ca8d3c817147d79a89f44a1
File name:	Adobe_Hennessyfunds_Remittance 3VD3-UMCX1I-JFC1.pdf

Indicadores de compromisso do artefato	
md5:	10d6e16a05965be5bc0059131dc5ae7c
sha1:	2e68d5a9ae45af0c1faee31896269a0d9648026b
sha256:	f99b01620ef174bb48e22e54327ca9cffa4520868f49a41c524b81ab6d935070
File name:	2024_Employee Handbooks_Agreement 4LS5-SGBR0P-FBB7.pdf

Indicadores de compromisso do artefato	
md5:	2a0576dc8628b3f27190755d291750e4
sha1:	5aabe0b495218f8559b088395c375b27fef6eeb7
sha256:	52e04c615b08af10b4982506c1cee74cb062116d31f0300ed027f6efd3119b1a
File name:	potential-virus-2024_Employee Handbooks_Agreement 2YQ6-PQVF2B-YJA1.pdf

Indicadores de compromisso do artefato	
md5:	15ef89d1a2aa023ab664e1adcd75cbfd
sha1:	00610bfd4c015cefdad2149d9f2f3c89f4fe5452
sha256:	3d58733b646431a60d39394be99ff083d6db3583796b503e8422baebed8d097e
File name:	2024_Employee Handbooks_Agreement 5EN0-PXLU4U-OFV0.pdf

Tabela 2 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
URL	authmicronlineonfication[.]com verificar-office-outlook[.]com stream-verify-login[.]com zaq[.]gletber[.]com v744[.]r9gh2[.]com bsifinancial019[.]ssllst[.]nuvem 473[.]kernam[.]com docusign[.]multiparteurope[.]com 56789iugtfrd5t69i9ei9die9di9eidy7u889[.]rhiltons[.]com agchoice[.]us-hindus[.]com
Domínio	Onnx[.]su
IP	5[.]181[.]156[.]247

Tabela 3 – Indicadores de Compromissos de Rede.

Obs: Os *links* e endereços IP elencados acima podem estar ativos; cuidado ao realizar a manipulação dos referidos IoCs, evite realizar o clique e se tornar vítima do conteúdo malicioso hospedado no IoC.

6 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Eclecticiq**
- **Bleepingcomputer**

7 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH