BOLETIM DE SEGURANÇA

Grupo APT44 utilizando backdoor Kapeka em ataques direcionados

heimdall
security research
A DIVISION OF ISH

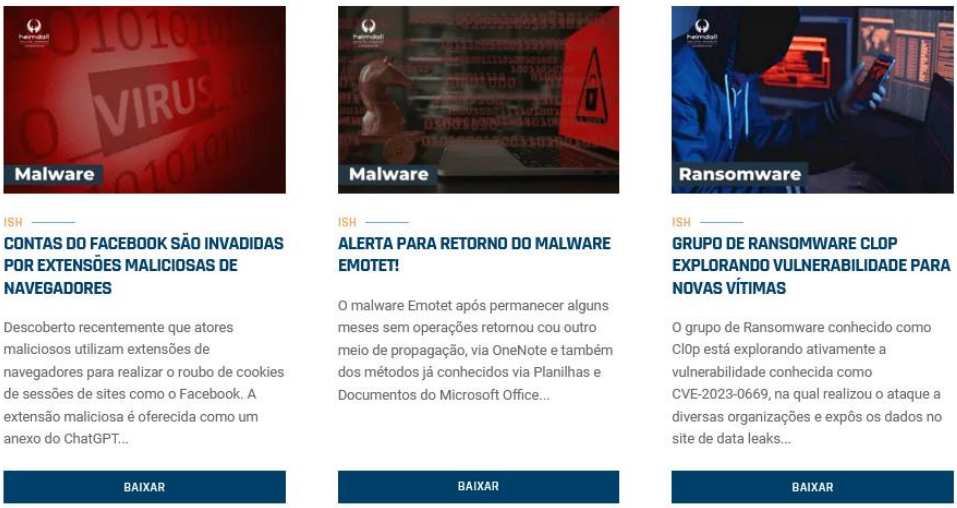
TLP: CLEAR

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

1 Sumário Executivo 6

2 Informações sobre a ameaça 7

3 MITRE ATT&CK - TTPs 9

4 Recomendações 10

5 Indicadores de Compromissos 11

6 Referências 12

LISTA DE TABELAS

Tabela 1 – Tabela MITRE ATT&CK. 9
Tabela 2 – Indicadores de Compromissos de artefatos. 11
Tabela 3 – Indicadores de Compromissos de Rede. 11

LISTA DE FIGURAS

Figura 1 – Fluxo do kapeka. *7*

1 SUMÁRIO EXECUTIVO

A WithSecure identificou um backdoor recém-descoberto, apelidado de "**Kapeka**", que vem sendo utilizado em ofensivas contra alvos no Leste Europeu desde meados de 2022. Este malware é caracterizado por sua versatilidade e conjunto completo de funcionalidades, que o tornam adequado tanto para operações iniciais quanto para manutenção de acesso prolongado aos sistemas comprometidos.

2 INFORMAÇÕES SOBRE A AMEAÇA

As investigações realizadas revelaram que o malware está associado a um grupo de ameaças cibernéticas avançadas e persistentes (APT), conhecido como Sandworm (ou APT44, Seashell Blizzard), com vínculos com a Rússia. Paralelamente, a Microsoft monitora esse mesmo software malicioso, denominando-o KnuckleTouch. A ameaça foi observada anteriormente esporadicamente em ataques cibernéticos contra a Europa Oriental, incluindo a Estónia e a Ucrânia, pelo menos desde meados de 2022.

De acordo com o pesquisador de segurança Mohammad Kazem, trata a backdoor como um malware versátil, equipado com funcionalidades completas para atuar tanto como um conjunto de ferramentas inicial para os atacantes quanto para garantir um acesso duradouro aos ativos digitais da entidade atacada.

O Kapeka possui um mecanismo de dropper que tem a função de ativar e operar a backdoor no sistema comprometido, e em seguida, se auto deleta. Além disso, o dropper estabelece a continuidade do backdoor, configurando-o para persistir via tarefa programada ou registro de inicialização automática, variando conforme o nível de privilégios de SYSTEM do processo.

Em fevereiro de 2024, a Microsoft relatou que o Kapeka está associado a múltiplas operações de disseminação de ransomware. Este malware é multifuncional, capaz de executar ações como expropriação de credenciais e dados, realização de ofensivas prejudiciais e facilitação do controle remoto do equipamento por agentes ameaçadores.

A DLL da backdoor, escrita em C++, é um componente malicioso do Windows que possui um mecanismo de comando e controle (C2) embutido para comunicação com um servidor externo sob o domínio de um invasor. Este servidor C2 determina a periodicidade de contato para novos comandos. Para se passar por legítima, a DLL se camufla como um add-on do Microsoft Word, coletando dados do sistema infectado. Ela opera com multithreading, permitindo que busque, execute e envie as instruções do servidor C2 de forma eficiente.

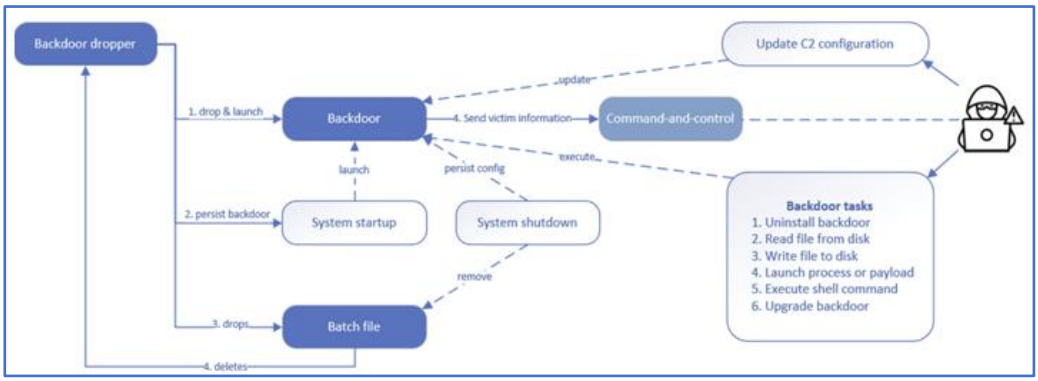


Figura 1 – Fluxo do kapeka.

O backdoor usa a interface COM WinHttp 5.1 (winhttpcom.dll) para implementar seu componente de comunicação de rede, se comunicando com seu C2 para pesquisar tarefas e enviar de volta informações de impressões digitais e resultados de tarefas. O backdoor utiliza JSON para enviar e receber informações de seu C2. O implante também é capaz de atualizar sua configuração C2 dinamicamente, recebendo uma nova versão do servidor C2 durante a pesquisa. Alguns dos principais recursos do backdoor permitem ler e gravar arquivos de e para o disco, iniciar cargas úteis, executar comandos shell e até mesmo atualizar e desinstalar a si mesmo. O método exato pelo qual o malware é propagado é atualmente desconhecido. No entanto, a Microsoft observou que o dropper é recuperado de sites comprometidos usando o utilitário certutil , ressaltando o uso de um binário legítimo de vida fora da terra (LOLBin) para orquestrar o ataque.

As ligações entre Kapeka e Sandworm são evidenciadas por semelhanças em conceitos e configurações com grupos de malware já conhecidos, como GreyEnergy, que é considerado o sucessor do BlackEnergy, e também com Prestige. Estas sobreposições indicam uma possível relação ou continuidade entre essas famílias de softwares maliciosos.

Um relatório detalhado intitulado "APT44: Unearthing Sandworm" está sendo divulgado, oferecendo novos detalhes sobre as operações recentes do grupo, análises históricas e insights sobre os ajustes do grupo para alinhar-se com as estratégias de guerra de Moscou.

O relatório detalha tecnicamente o backdoor e suas funcionalidades, além de explorar a relação entre Kapeka e Sandworm. Seu propósito é elevar o nível de alerta entre corporações, autoridades e a comunidade de segurança. A WithSecure compartilhou versões preliminares com governos e clientes específicos. Adicionalmente, foram liberados artefatos oriundos da pesquisa, que incluem um extrator de configuração, um script para decifrar e simular a comunicação do backdoor, e um conjunto de indicadores de comprometimento, regras YARA e correspondências com o framework MITRE ATT&CK.

3 MITRE ATT&CK - TTPs

Tática	Técnica	Detalhes
Execution	T1059.003 T1559.001	Os adversários podem abusar do shell de comando do Windows para execução. Os adversários podem usar o Component Object Model (COM) do Windows para execução de código local.
Persistence	T1053 T1547.001	Os adversários podem abusar da funcionalidade de agendamento de tarefas para facilitar a execução inicial ou recorrente de código malicioso. Os adversários podem obter persistência adicionando um programa a uma pasta de inicialização ou referenciando-o com uma chave de execução do Registro.
Defense Evasion	T1036.008 T1027	Os adversários podem mascarar cargas maliciosas como arquivos legítimos por meio de alterações na formatação da carga, incluindo a assinatura, a extensão e o conteúdo do arquivo. Os adversários podem tentar dificultar a descoberta ou análise de um arquivo executável ou arquivo criptografando, codificando ou ofuscando seu conteúdo no sistema ou em trânsito.
Discovery	T1124 T1033	Um adversário pode obter a hora e/ou fuso horário do sistema de um sistema local ou remoto. Os adversários podem tentar identificar o usuário principal, o usuário atualmente conectado, o conjunto de usuários que normalmente usa um sistema ou se um usuário está usando ativamente o sistema.
Command and Control	T1105 T1041	Os adversários podem transferir ferramentas ou outros arquivos de um sistema externo para um ambiente comprometido. Os adversários podem roubar dados exfiltrando-os através de um canal de comando e controle existente.

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:

Atualize regularmente

- Mantenha o sistema operacional e todos os aplicativos sempre atualizados para corrigir vulnerabilidades que possam ser exploradas por malwares.

Use antivírus

- Instale um programa antivírus confiável e mantenha-o atualizado para detectar e remover malwares.

Backup de dados

- Faça backups regulares dos seus dados para evitar perdas em caso de ataque de ransomware.

Evite downloads suspeitos

- Não faça download de arquivos de fontes desconhecidas ou não confiáveis.

Use senhas fortes

- Crie senhas complexas e únicas para cada conta e evite usar informações pessoais como parte da senha.

Descriptografia em firewalls

- Habilite recursos de descriptografia em firewalls de última geração para expor possíveis ameaças.

Educação em segurança

- Esteja informado sobre as últimas ameaças de segurança e melhores práticas para se proteger contra elas.

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:	50b5582904fe34451f5cb2362e11cb24
sha1:	80fb042b4a563efe058a71a647ea949148a56c7c
sha256:	bd07fb1e9b4768e7202de6cc454c78c6891270af02085c51fce5539db1386c3f
File name:	crdss.exe

Indicadores de compromisso do artefato	
md5:	2bebf05a9607f038f5407248fb075cd6
sha1:	97e0e161d673925e42cdf04763e7eaa53035338b
sha256:	272cfaebf22e0f6a34c0a93b7c9c5b67c725947ba0f17e60ed67dbf6e1602043
File name:	272cfaebf22e0f6a34c0a93b7c9c5b67c725947ba0f17e60ed67dbf6e1602043.exe

Indicadores de compromisso do artefato	
md5:	5294aaf2ff80547172ebb9e0bcb52e0f
sha1:	9bbde40cab30916b42e59208fbcc09affef525c1
sha256:	f30b9f6e913798ca52154c88725ee262a7bf92fe7caac1ae2e5147e457b9b08a
File name:	menoce.wll

Tabela 2 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
URL	https[:]//103[.]78[.]122[.]94/help/healthcheck https[:]//88[.]80[.]148[.]65/news/article https[:]//185[.]181[.]229[.]102/home/info https[:]//185[.]38[.]150[.]8/star/key

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**
- **Withsecure**
- **Mandiant**
- **Thehackernews**
- **Bleepingcomputer**

heimdall
security research
A DIVISION OF ISH