BOLETIM DE SEGURANÇA

Setor educacional dos EUA é atacado por novo ransomware Fog através de VPNs comprometidas

heimdall
security research
A DIVISION OF ISH

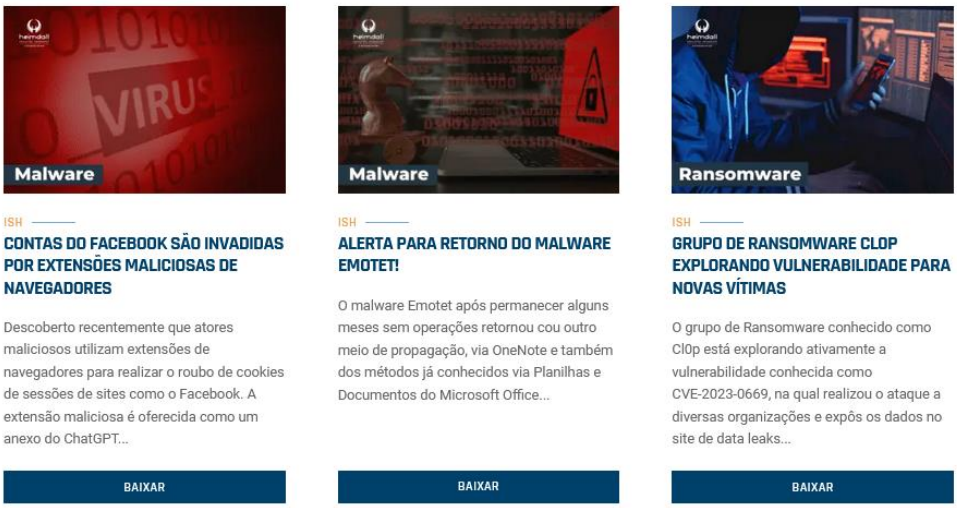
TLP: CLEAR

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

1 SUMÁRIO EXECUTIVO

Pesquisadores da Arctic Wolf Labs identificaram uma nova variante de ransomware, denominada Fog. Esta atividade maliciosa foi notada em diversas situações de resposta a incidentes, todos apresentando características similares. As organizações afetadas até o momento estão localizadas nos Estados Unidos, com uma predominância no setor educacional (80%) e também no setor de recreação (20%).

2 INFORMAÇÃO SOBRE A AMEAÇA

Desde o começo de maio, a equipe do Arctic Wolf tem se dedicado a analisar incidentes que envolvem a implementação de uma variante de ransomware chamada Fog, direcionada a organizações americanas nos setores educacional e recreativo. O termo Fog é usado para se referir a uma variante específica de ransomware, não a um grupo, para diferenciar as entidades que desenvolvem o software de criptografia das que executam os ataques reais. Essa distinção é crucial, pois os grupos de ransomware podem dar a impressão de serem uma única entidade, quando na verdade são compostos por vários grupos afiliados independentes. Atualmente, a organização interna do(s) grupo(s) que realizam ataques usando o ransomware Fog ainda é desconhecida.

Foi constatado que os atores conseguiram infiltrar-se nos sistemas das vítimas utilizando credenciais VPN comprometidas. O acesso remoto foi realizado por meio de dois diferentes provedores de gateway VPN. A atividade maliciosa mais recente registrada ocorreu em maio de 2024. Em um dos casos, notou-se a atividade pass-the-hash em contas de administrador, que foram usadas posteriormente para estabelecer conexões RDP com servidores Windows rodando Hyper-V e Veeam. Em uma outra situação, foram encontradas evidências de preenchimento de credenciais, o que se acredita ter facilitado a movimentação lateral no ambiente. Em todos os casos, o PsExec foi instalado em diversos hosts e o RDP/SMB foi empregado para acessar os hosts alvo.

Nos servidores Windows que foram alvo dos invasores, o Windows Defender foi desativado por eles. Foi observado que os invasores criptografaram arquivos VMDK no armazenamento de VM e apagaram backups do armazenamento de objetos na Veeam. Eles deixaram notas de resgate nos sistemas comprometidos e implementaram um ransomware funcionalmente igual em todos os casos. As notas de resgate eram idênticas, exceto por um código de bate-papo único. Apesar do endereço .onion ser usado para a comunicação entre a vítima e o invasor, não foi identificada nenhuma outra presença na dark web, como um site de vazamento de dados.

O binário do ransomware responsável por criptografar apresenta técnicas que são comumente usadas em outras variantes de ransomware. As amostras que examinamos de vários casos mostraram muitas similaridades, incluindo blocos de código funcionais e instruções idênticas, sugerindo que foram compiladas a partir da mesma fonte de código.

Na primeira execução do exemplo, ele tenta gerar um novo arquivo chamado DbgLog.sys no diretório especial **% AppData%**. O arquivo **DbgLog.sys** é preenchido com linhas de log que registram o status e as condições de erro do ransomware à medida que cada técnica é aplicada.

Durante a rotina de inicialização, o exemplo referência **NTDLL.DLL** e a função **NtQuerySystemInformation**. Vale ressaltar que a API do NT é parte das APIs internas do Windows e geralmente não é recomendado chamá-la diretamente, pois pode variar com cada versão do Windows. A função **NtQuerySystemInformation** permite ao invocador obter informações sobre os detalhes físicos do sistema atual, como o número de processadores lógicos disponíveis. Essas informações podem ser úteis para determinar quantos threads a rotina de criptografia multithread deve alocar.

Após a conclusão da rotina de inicialização, o sample verifica os argumentos da linha de comando para opções específicas:

- **NOMUTEX:** Permite a execução simultânea de várias instâncias do ransomware ao não criar um mutex.
- **ALVO:** Define um local específico para iniciar a exploração.
- **CONSOLE:** Anexa a saída padrão e o erro a uma nova janela de console para o processo de chamada.

O sample também possui um bloco de configuração baseado em JSON para personalização adicional. As seguintes opções configuráveis determinam as atividades que ocorrem antes e depois da criptografia:

- **RSAPubKey:** Chave pública embutida usada para criptografia.
- **LockedExt:** Extensão de arquivo após a criptografia.
- **NotefileName:** Nome do arquivo da nota de resgate.
- **ShutdownProcesses:** Assegura que os processos sejam encerrados antes da criptografia.
- **ShutdownServices:** Assegura que os serviços sejam interrompidos antes da criptografia.

O sample descobre volumes, recursos de rede e arquivos usando APIs padrão do Windows, como **FindFirstVolume, WNetOpenEnum** e **FindFirstFile**. Em todos os casos, foram utilizadas as variantes Unicode dessas funções.

Com base nas informações do sistema descobertas anteriormente, o exemplo configura um conjunto de threads dedicados à criptografia de todos os arquivos descobertos. Este conjunto de threads utiliza as informações do processador lógico, com um mínimo de dois processadores e um máximo de dezesseis processadores. Durante o processo, são chamadas as APIs obsoletas do Windows para **CryptImportKey** e **CryptEncrypt**.

Após a criptografia, a extensão do arquivo é adicionada a cada arquivo usando a versão Unicode da API **MoveFile** do Windows e a opção **LockedExt**. Nos casos observados, as extensões **.FOG** e **.FLOCKED** foram configuradas. Uma nota de resgate é gravada no disco usando a opção **Notefilename** configurada no bloco de configuração. Nos casos observados, o arquivo de notas foi denominado **readme.txt**.

Antes do exemplo terminar, a cópia de sombra do volume é excluída criando um novo processo através da função **CreateProcess** com a linha de comando: vssadmin.exe delete **shadows /all /quiet**. Ao usar a opção **/all** para excluir a cópia de sombra do volume, o exemplo excluirá todas as cópias de sombra do volume especificado e a opção **/quiet** garantirá que nenhuma mensagem seja exibida durante a exclusão.

3 MITRE ATT&CK - TTPs

Tática	Técnica	Detalhes
Initial Access	T1133 T1078	Consiste em técnicas que utilizam vários vetores de entrada para obter sua posição inicial dentro de uma rede.
Discovery	T1046 T1135	Trata-se de técnicas que um adversário pode usar para obter conhecimento sobre o sistema e a rede interna.
Lateral Movement	T1021 T1570	Consiste em técnicas que os adversários usam para entrar e controlar sistemas remotos em uma rede.
Credential Access	T1003 T1555 T1110	Trata-se de técnicas para roubar credenciais, como nomes de contas e senhas.
Persistence	T1136	Consiste em técnicas que os adversários usam para manter o acesso aos sistemas após reinicializações, alterações de credenciais e outras interrupções que podem interromper seu acesso.
Execution	T1059 T1569	Trata-se de técnicas que resultam na execução de código controlado pelo adversário em um sistema local ou remoto.
Defense Evasion	T1562 T1550 T1078 T1140 T1070	Consiste em técnicas que os adversários usam para evitar a detecção durante todo o seu comprometimento.
Impact	T1486 T1490 T1489	Trata-se de técnicas que os adversários usam para interromper a disponibilidade ou comprometer a integridade, manipulando processos comerciais e operacionais.

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:

Backup dos dados

- Mantenha cópias regulares de seus dados importantes em um local seguro.

Atualize o software regularmente

- Muitos ransomwares exploram vulnerabilidades em softwares desatualizados. Portanto, é essencial manter todos os seus softwares atualizados.

Use autenticação de dois fatores (2FA)

- Isso pode fornecer uma camada adicional de segurança e pode prevenir muitos ataques de ransomware.

Navegue online com segurança

- Evite clicar em links em mensagens de spam ou em sites desconhecidos.

Não abra anexos de e-mail suspeitos

- O ransomware também pode entrar em seu dispositivo por meio de anexos de e-mail.

Use uma solução de segurança abrangente

- Uma ferramenta anti-malware pode ajudar a evitar uma situação em que você tenha que pagar valores exorbitantes para a possível liberação de seus dados.

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:	617d79c02ebac68b613d5b7cdbf001fd
sha1:	83f00af43df650fda2c5b4a04a7b31790a8ad4cf
sha256:	e67260804526323484f564eebeb6c99ed021b960b899ff788aed85bb7a9d75c3
File name:	locker_out.exe

Indicadores de compromisso do artefato	
md5:	07c6b4756715d73304ec0ebc951dddad
sha1:	eeafa71946e81d8fe5ebf6be53e83a84dcca50ba
sha256:	9d00158489f0a399fc0bc3ce1e8fc309d29a327f6ea0097e34e0f49b72a85079
File name:	psexesvc.exe

Indicadores de compromisso do artefato	
md5:	4fdabe571b66ceec3448939bfb3ffcd1
sha1:	763499b37aacd317e7d2f512872f9ed719aacae1
sha256:	8b9c7d2554fe315199fae656448dc193accbec162d4afff3f204ce2346507a8a
File name:	advanced_port_scanner.exe

Indicadores de compromisso do artefato	
md5:	6a58b52b184715583cda792b56a0a1ed
sha1:	3477a173e2c1005a81d042802ab0f22cc12a4d55
sha256:	d0c1662ce239e4d288048c0e3324ec52962f6ddda77da0cb7af9c1d9c2f1e2eb
File name:	Advanced_Port_Scanner_2.5.3869.exe

Indicadores de compromisso do artefato	
md5:	4b69e562609d08ce8dfe703b9077e33b
sha1:	90be89524b72f330e49017a11e7b8a257f975e9a
sha256:	e11e7db705a11f8ca250d8d6826371e550b3214757f5bb9b648c7b0fad09294b
File name:	SharpShares.exe

Tabela 2 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
IP	5.230.33[.]176 77.247.126[.]200 107.161.50[.]26

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**
- **ArcticWolf**
- **Bleepingcomputer**

7 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH