BOLETIM DE SEGURANÇA

Microsoft alerta que hackers do APT28 exploram a falha do Windows relatada pela NSA

heimdall
security research
A DIVISION OF ISH

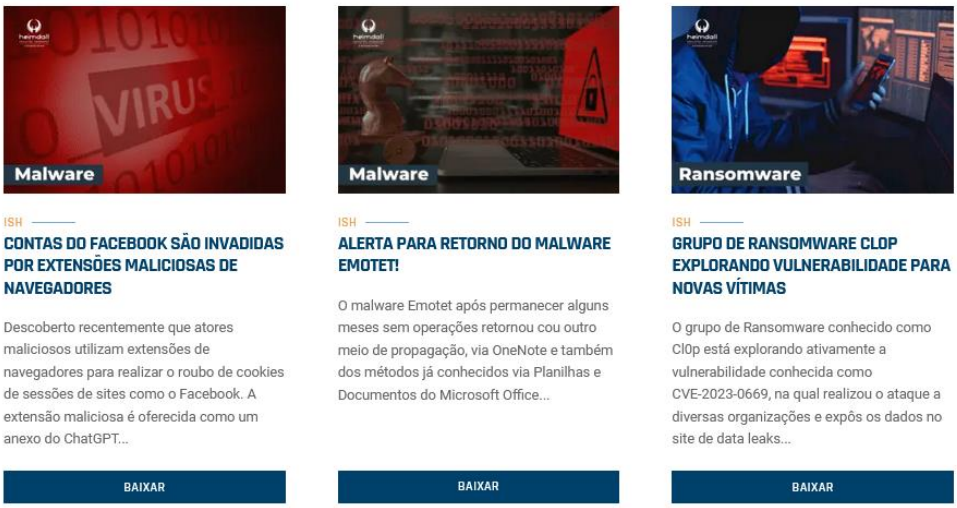
TLP: CLEAR

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 Microsoft publicou os resultados de uma investigação do grupo de ameaça russo conhecido como Forest Blizzard (STRONTIUM), informando que este grupo tem utilizado uma ferramenta personalizada, chamada GooseEgg, para explorar a vulnerabilidade CVE-2022-38028 no serviço Windows Print Spooler desde junho de 2020. A ferramenta permite elevar privilégios e roubar credenciais em redes comprometidas.

2 INFORMAÇÕES SOBRE A AMEAÇA

O grupo Forest Blizzard tem focado em setores críticos como governamental, energia e transporte, além de ONGs, principalmente nos EUA, Europa e Oriente Médio. A Microsoft detectou tentativas dessa operação também contra setores de mídia, TI, esportes e educação globalmente. Desde 2010, o objetivo desse agente de ameaça é coletar dados que beneficiem a política externa russa. Autoridades dos EUA e do Reino Unido associam a Forest Blizzard à Unidade 26165 da GRU, a inteligência militar russa. A mesma unidade é conhecida por outros nomes como APT28, Sednit, Sofacy e Fancy Bear, indicando grupos com ações parecidas ou conectadas.

A análise indicou que o grupo utiliza a ferramenta GooseEgg com o propósito de alcançar privilégios elevados em sistemas visados, além de extrair credenciais e dados. Os métodos e a infraestrutura empregados por esse agente podem variar. Conforme a identificação, uma vez que a Forest Blizzard consegue acesso a um sistema, ele emprega o GooseEgg para ampliar seus privilégios. O GooseEgg é geralmente introduzido através de um script batch, frequentemente nomeado **execute.bat** ou **doit.bat**. Esse script cria o arquivo servtask.bat, que executa comandos para armazenar e comprimir registros. Além disso, o script batch aciona o executável GooseEgg e estabelece sua persistência no sistema por meio de uma tarefa agendada que executa o **servtask.bat**.

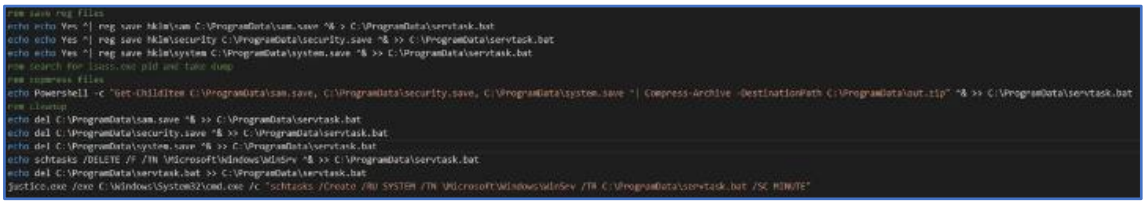


Figura 1 – Arquivo em lote.

O executável GooseEgg, que é identificado por vários nomes como **Justice.exe** e **DefragmentSrv.exe**, opera através de quatro comandos distintos, cada um seguindo um caminho de execução próprio. Embora à primeira vista o executável pareça realizar ações simples, ele as executa de forma complexa e única, possivelmente com o intuito de camuflar suas operações.

O primeiro comando gera um código de retorno específico, **0x6009F49F**, e encerra o processo, o que pode indicar uma versão do software. Os dois comandos seguintes são responsáveis por iniciar a exploração do sistema, ativando uma DLL específica ou um executável com privilégios elevados. O quarto e último comando realiza um teste para confirmar o sucesso da exploração, utilizando o comando whoami para tal verificação.

A Microsoft detectou que arquivos DLL suspeitos frequentemente contêm a palavra "**wayzgoose**" em seus nomes, como no exemplo **wayzgoose23.dll**. Esses arquivos DLL, juntamente com outros elementos do malware, são alocados em subdiretórios específicos dentro de **C:\ProgramData**. O nome de cada subdiretório é escolhido de uma lista pré-definida, que inclui:

- Microsoft
- Adobe
- Comms
- Intel
- Kaspersky Lab
- Bitdefender
- ESET
- NVIDIA
- UbiSoft
- Steam

Um subdiretório é criado com números gerados aleatoriamente e a string de formato **\v%u.%02u.%04u**, que serve como diretório de instalação. Por exemplo, pode ser criado um diretório como **C:\ProgramData\Adobe\v2.116.4405**. O binário então transfere os seguintes repositórios de drivers para este diretório:

- C:\Windows\System32\DriverStore\FileRepository\pnms003.inf_*
- C:\Windows\System32\DriverStore\FileRepository\pnms009.inf_*

```
if ( wcscpy_s(sourcePath, 0x164uLL, windDir)
  || wcscat_s(sourcePath, 0x164uLL, L"\\system32\\DriverStore\\FileRepository")
  || wcscpy_s(destPath, 0x184uLL, installDir)
  || wcscat_s(destPath, 0x184uLL, Source)
  || wcscat_s(destPath, 0x184uLL, L"\\system32\\DriVerStoRe\\FiLeRePoSiToRy") )
{
    return 0xE009F47A;
}
if ( SHCreateDirectoryExW(0LL, destPath, 0LL) )
    return 0xE009F45B;
result = copy_all_files(sourcePath, L"prnms003.inf_*", destPath);// Copy driver package to user controlled directory
if ( result >= 0 )
{
    result = copy_all_files(sourcePath, L"prnms009.inf_*", destPath);
    if ( result >= 0 )
```

Figura 2 – Binário GooseEgg adicionando armazenamentos de driver a um diretório.

Para a execução do ataque, são inicialmente estabelecidas chaves de registro que criam um manipulador de protocolo exclusivo e um novo CLSID é registrado para atuar como servidor COM de um protocolo não reconhecido oficialmente. A técnica utilizada altera o link simbólico da unidade C: no sistema de gerenciamento de objetos, redirecionando-o para o diretório recém-estabelecido. Assim, quando o serviço de PrintSpooler busca pelo arquivo **C:\Windows\System32\DriverStore\FileRepository\pnms009.inf_amd64_a7412a554c9bc1fd\MPDW-Constraints.js**, ele é desviado para o diretório sob controle do invasor, que contém as cópias dos drivers.

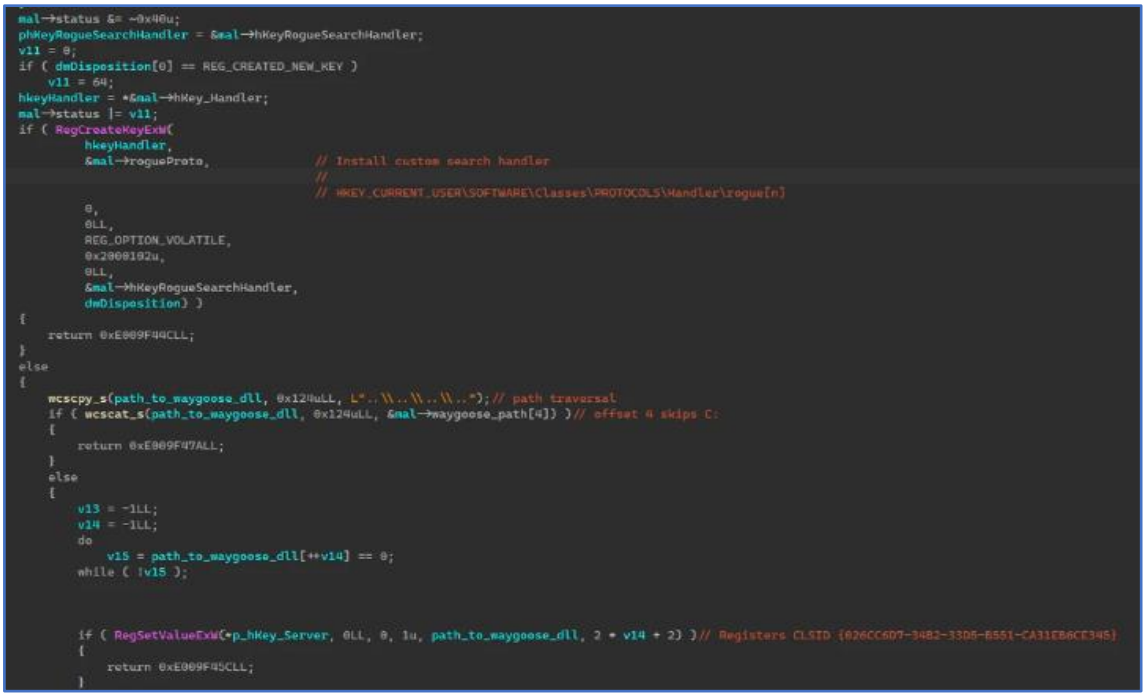


Figura 3 – Criação de chave de registro.

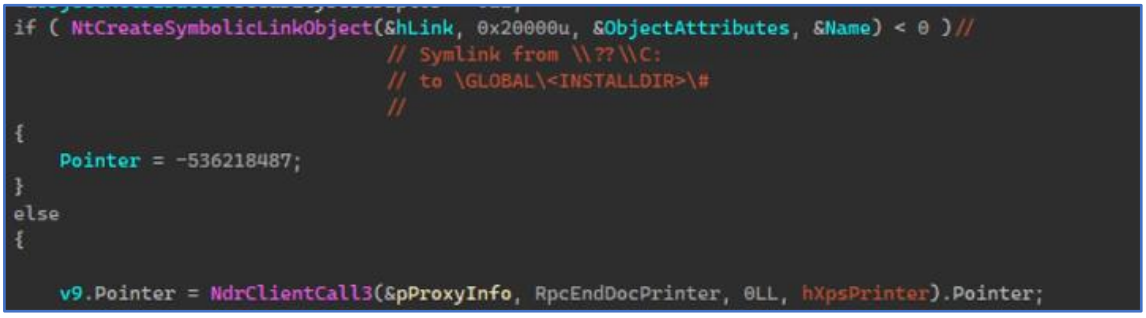


Figura 4 – Sequestro de link simbólico em C: .

No diretório sob domínio do atacante, o arquivo "**MPDW-constraints.js**" recebe uma modificação específica na função **convertDevModeToPrintTicket**. Esta alteração é parte do processo de comprometimento do sistema.

```
function convertDevModeToPrintTicket(devModeProperties, scriptContext, printTicket)
{try{ printTicket.XmlNode.load('rogue9471://go'); } catch (e) {}
```

Figura 5 – Função convertDevModeToPrintTicket invoca o CLSID do manipulador.

No arquivo "**MPDW-constraints.js**", localizado no diretório sob controle do atacante, um patch específico foi aplicado à função **convertDevModeToPrintTicket**. Este patch aciona o CLSID de um manipulador de protocolo de pesquisa não autorizado durante a execução da função **RpcEndDocPrinter**. Como resultado, a DLL auxiliar wayzgoose.dll é carregada no contexto do serviço PrintSpooler com privilégios SYSTEM. A **wayzgoose.dll**, sendo um aplicativo inicializador simples, tem a capacidade de iniciar outros programas especificados via linha de comando com permissões de nível SYSTEM, o que possibilita aos atacantes realizarem ações como instalar backdoors, movimentar-se lateralmente em redes comprometidas e executar códigos de forma remota.

3 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 seu software, navegador e sistema operacional

- Mantenha todos os seus programas atualizados para garantir que você tenha as últimas correções de segurança.

Use uma proteção antivírus

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

Habilite a descriptografia em firewalls de última geração

- Isso permite expor possíveis ameaças ocultas em tráfego criptografado.

Baixe programas de fontes conhecidas

- Evite seguir links em e-mails suspeitos e baixe softwares apenas de fontes confiáveis.

Segmentação de rede

- Divida os recursos da rede em zonas distintas para limitar o movimento de um atacante dentro da rede e reduzir o alcance de seus ataques.

Segurança de pontos de extremidade

- Utilize ferramentas robustas de detecção e resposta em endpoints (EDR) para detectar e responder a atividades suspeitas. Mantenha todo o software de segurança de endpoint atualizado para se defender contra as ameaças mais recentes.

Autenticação Multifator (MFA)

- Implemente MFA sempre que possível para adicionar uma camada adicional de segurança contra o roubo de credenciais, uma tática comum usada pelo APT28.

Educação e Conscientização dos Usuários

- Realize sessões de treinamento regulares para informar os funcionários sobre os mais recentes golpes de phishing e táticas de engenharia social. Este treinamento também deve cobrir a importância de usar senhas fortes e únicas e os riscos associados ao download de software não autorizado.

4 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:	bb5f3548b2d4561f9f9811365634bcc0
sha1:	bd1834afcd4d2709dd0a541b16521abe2410a9f2
sha256:	c60ead92cd376b689d1b4450f2578b36ea0bf64f3963cfa5546279fa4424c2a5
File name:	c60ead92cd376b689d1b4450f2578b36ea0bf64f3963cfa5546279fa4424c2a5.exe

Indicadores de compromisso do artefato	
md5:	fc6c9d17b2136ffb425bfb128d8c1ed8
sha1:	2635fe5b8029d65ed3229f5f14d7cf51df100542
sha256:	7d51e5cc51c43da5deae5fbc2dce9b85c0656c465bb25ab6bd063a503c1806a9
File name:	7d51e5cc51c43da5deae5fbc2dce9b85c0656c465bb25ab6bd063a503c1806a9.bat.vir

Indicadores de compromisso do artefato	
md5:	ea65b206ae11f120d7d93e22884c37d9
sha1:	d1dd6017cd0a82f1e000a84e166a20c40270215d
sha256:	6b311c0a977d21e772ac4e99762234da852bbf84293386fbe78622a96c0b052f
File name:	6b311c0a977d21e772ac4e99762234da852bbf84293386fbe78622a96c0b052f.exe

Indicadores de compromisso do artefato	
md5:	5bf931ae6c4eb9c14063ea03d05ba1aa
sha1:	c00c21b43dffd78391c232ff1290089f8993c757
sha256:	41a9784f8787ed86f1e5d20f9895059dac7a030d8d6e426b9ddcaf547c3393aa
File name:	41a9784f8787ed86f1e5d20f9895059dac7a030d8d6e426b9ddcaf547c3393aa.exe

Tabela 1 – Indicadores de Compromissos de artefatos

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- Microsoft
- Thehackernews
- Bleepingcomputer
- NVD

heimdall
security research
A DIVISION OF ISH