BOLETIM DE SEGURANÇA

Microsoft Identifica Grupo Norte-Coreano por trás do Novo Ransomware FakePenny

heimdall
security research
A DIVISION OF ISH

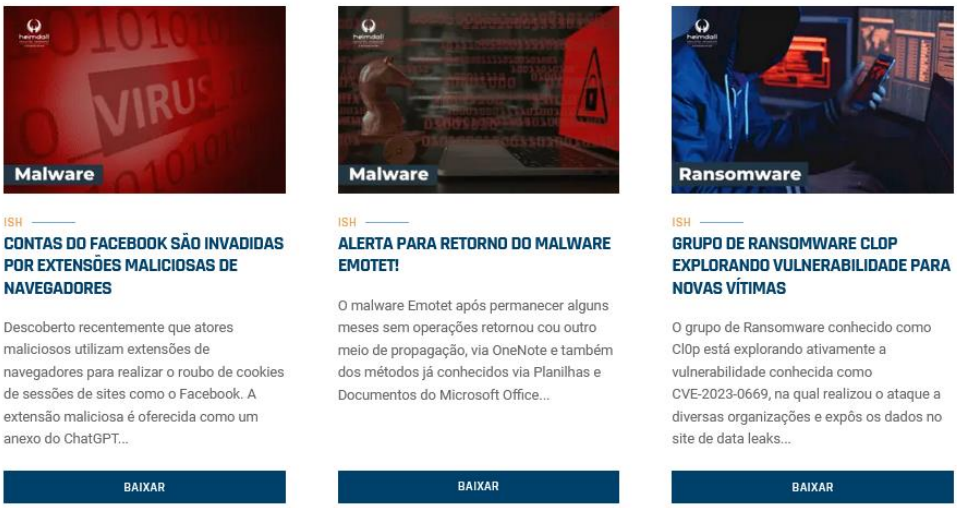
TLP: CLEAR

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 identificou um novo grupo de ameaça norte-coreano, agora chamado Moonstone Sleet (anteriormente conhecido como Storm-1789). Este grupo combina diversas técnicas amplamente utilizadas por outros grupos de ameaça norte-coreanos com métodos exclusivos para alcançar seus objetivos financeiros e de ciberespionagem. Moonstone Sleet é conhecido por criar empresas fictícias e oportunidades de emprego falsas para se aproximar de alvos em potencial, usar versões trojanizadas de ferramentas legítimas, desenvolver jogos maliciosos e distribuir um novo ransomware personalizado. As táticas, técnicas e procedimentos (TTPs) de Moonstone Sleet mostram uma forte semelhança com as empregadas por outros grupos de ameaça norte-coreanos nos últimos anos, destacando a interseção entre esses grupos. Inicialmente, Moonstone Sleet apresentava similaridades com Diamond Sleet, mas desde então passou a operar com sua própria infraestrutura e ataques, estabelecendo-se como um grupo de ameaça norte-coreano distinto e bem equipado.

2 INFORMAÇÕES SOBRE A AMEAÇA MOONSTONE SLEET

Moonstone Sleet é um grupo de ameaça responsável por uma série de atividades maliciosas que a Microsoft avalia estarem alinhadas com os interesses do estado norte-coreano. Este grupo utiliza uma combinação de técnicas amplamente testadas por outros atores de ameaças norte-coreanos, além de metodologias de ataque exclusivas. Quando a Microsoft detectou pela primeira vez as atividades do Moonstone Sleet, o grupo apresentava fortes semelhanças com o Diamond Sleet, reutilizando extensivamente o código do malware conhecido como Comebacker e empregando técnicas bem estabelecidas do Diamond Sleet, como o uso de mídias sociais para distribuir software trojanizado.

No entanto, Moonstone Sleet rapidamente passou a operar com sua própria infraestrutura e ataques personalizados. Posteriormente, a Microsoft observou que Moonstone Sleet e Diamond Sleet conduziam operações simultâneas, com Diamond Sleet continuando a utilizar grande parte de suas técnicas conhecidas e estabelecidas. As operações de Moonstone Sleet são amplas e apoiam seus objetivos financeiros e de espionagem cibernética. Essas operações incluem desde a implantação de ransomware personalizado até a criação de jogos maliciosos, a formação de empresas falsas e o recrutamento de profissionais de TI.

3 TÁTICAS UTILIZADAS PELO ATOR

A Microsoft identificou o grupo Moonstone Sleet distribuindo uma versão trojanizada do PuTTY, um emulador de terminal de código aberto, por meio de aplicativos como LinkedIn, Telegram e plataformas de freelancers. O método usado pelo grupo envolvia enviar um arquivo .zip para os alvos, contendo dois arquivos: uma versão comprometida do putty.exe e um arquivo url.txt com um endereço IP e uma senha. Quando o usuário inseria o IP e a senha no aplicativo PuTTY, este descriptografava e executava uma carga útil embutida.

```
lpPassword = *(const char **)(lpInputObj - 288);
if ( !strcmp(lpPassword, "LH2MStEgzesQPNwa") )
{
  *(_QWORD *)(lpInputObj - 288) = f_gen_pwd_buffer("FG6pEqFe5:b$Bzt");// replace pwd buffer
  nSizeDecompressed.m128i_i32[0] = 0x1D2338;
  lpPePayload = LocalAlloc(0x40u, 0x1D2338ui64);
  strcpy(keyBuff, "6x6s+>e:j~SVK9_0V?m;=Obxd=n+5%-@");
  f_crypt_payload(
    (unsigned int)keyBuff,
    (unsigned int)keyBuff,
    (unsigned int)&crypt_buffer,
    (unsigned int)&crypt_buffer,
    0x2E9ECi64);
  if ( !(unsigned int)f_zlib_decompress(lpPePayload, &nSizeDecompressed, &crypt_buffer, 0x2E9ECi64)
    && f_load_exec_pe_payload(lpPePayload) == -1 )
  {
    LocalFree(lpPePayload);
  }
}
else if ( !strcmp(lpPassword, "FG6pEqFe5:b$Bzt") )
{
  *(_QWORD *)(lpInputObj - 288) = f_gen_pwd_buffer("LH2MStEgzesQPNwa");// replace pwd buffer
}
```

Figura 1 – Código do executável PuTTY.

Conforme a análise de Microsoft, o O executável PuTTY trojanizado descarta um instalador personalizado que inicia a execução de uma série de estágios de malware, descrito abaixo:

- **Estágio 1** – PuTTY Trojanizado: Descriptografa, descompacta e executa a carga útil incorporada do estágio 2.
- **Estágio 2** – Instalador/Dropper SplitLoader: Descriptografa, descompacta e grava a carga útil do estágio 3, o arquivo DLL SplitLoader, no disco. O instalador também grava dois arquivos criptografados no disco e, em seguida, executa o SplitLoader por meio de uma tarefa agendada ou chave de execução do registro.
- **Estágio 3** – SplitLoader: Descriptografa e descompacta os dois arquivos criptografados descartados pela carga útil do estágio 2, combinando-os para criar o próximo estágio, um novo arquivo executável portátil (PE).
- **Estágio 4** – Carregador de Trojan: Aguarda um arquivo PE compactado e criptografado do C2. Quando o arquivo é recebido, o carregador de trojan o descompacta, descriptografa e executa.

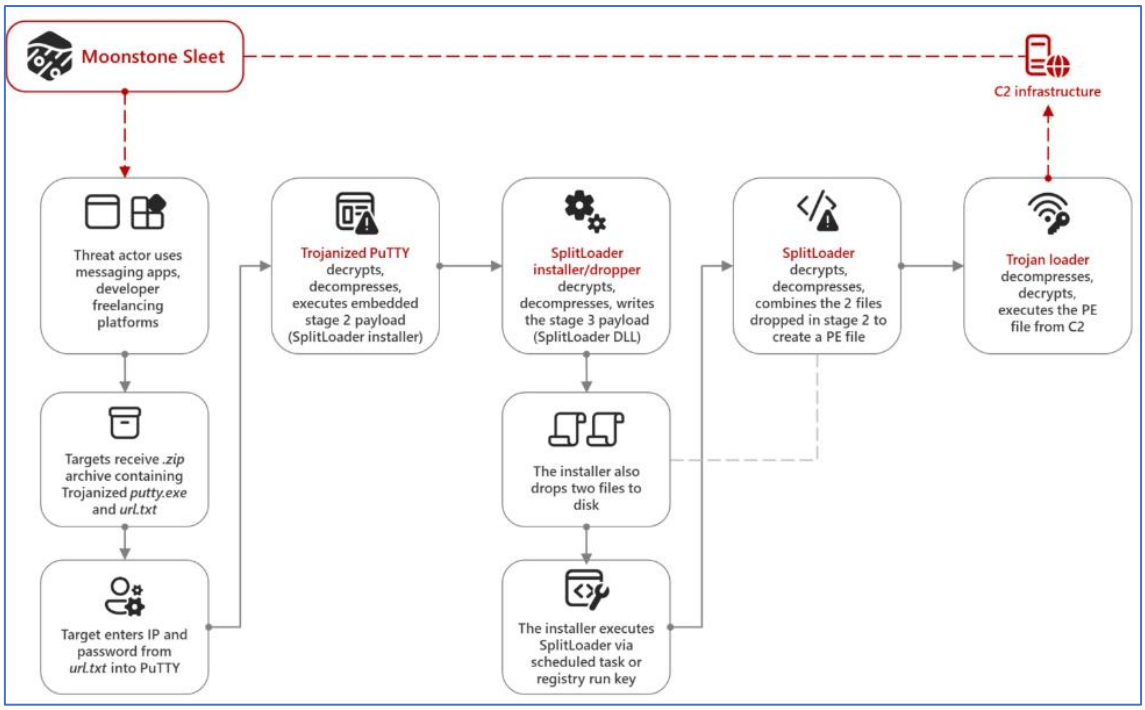


Figura 2 – Cadeia de ataques observada usando o PuTTY trojanizado.

A Microsoft também notou que o Moonstone Sleet utilizou outros carregadores de malware personalizados, fornecidos pelo PuTTY, que exibiram comportamentos semelhantes e compartilharam argumentos com artefatos de malware Diamond Sleet observados anteriormente. Entre eles estão:

```
cmd /c C:\ProgramData\USOShared\adb.bin 62
C:\ProgramData\USOShared\uso.bin SmLLPPZLb2vjue3d
```

Figura 3 – Carregador personalizado.

O ator de ameaças também foi visto utilizando pacotes **npm** maliciosos visando vítimas em potencial, os pacotes foram entregues por meio de sites de freelancers ou outras plataformas como o LinkedIn, entregando malware por meio de jogo de tanque. E realizando criação de empresas falsas que se faziam passar por desenvolvimento de software e serviços de TI, normalmente relacionados a blockchain e IA. O ator tem usado essas empresas para alcançar alvos potenciais, usando uma combinação de sites criados e contas de mídia social para adicionar legitimidade às suas campanhas.

4 ENTREGA DE RANSOMWARE

Em abril deste ano, a Microsoft identificou o Moonstone Sleet distribuindo uma nova variante de ransomware personalizada, denominada FakePenny, contra uma empresa que havia sido comprometida anteriormente em fevereiro. O FakePenny consiste em um carregador e um criptografador. Embora grupos de agentes de ameaça norte-coreanos já tenham desenvolvido ransomware personalizado, esta é a primeira vez que observamos este agente de ameaça específico implantando ransomware. A Microsoft avalia que o objetivo do Moonstone Sleet ao utilizar o ransomware é obter ganho financeiro, indicando que o grupo realiza operações cibernéticas tanto para coleta de inteligência quanto para geração de receita. É notável que a nota de resgate do FakePenny seja semelhante à usada pelo Seashell Blizzard em seu malware NotPetya. O pedido de resgate foi de US$ 6,6 milhões em BTC, um valor significativamente mais alto em comparação com as demandas de resgate de ataques anteriores de ransomware da Coreia do Norte, como WannaCry 2.0 e H0lyGh0st.

Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't wast your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption keys.

Please follow the instructions:

1. Send 100 btc to following address:

2. Send your Bitcoin desposit screenshot to Telegram ID.

- https://t.me/penygroup000
- https://t.me/penygroup11
- https://t.me/penygroup222

Remember !!!!

Don't reinstall OS and destroy encrypted files, if you reinstall OS or destroy encrypted files, then there is no recover way.

Important !!!!

You have until April 12th to recover your files. After April 12th, all data will be made public via the Internet.

@penygroup@

Figura 4 – Nota sobre ransomware FakePenny.

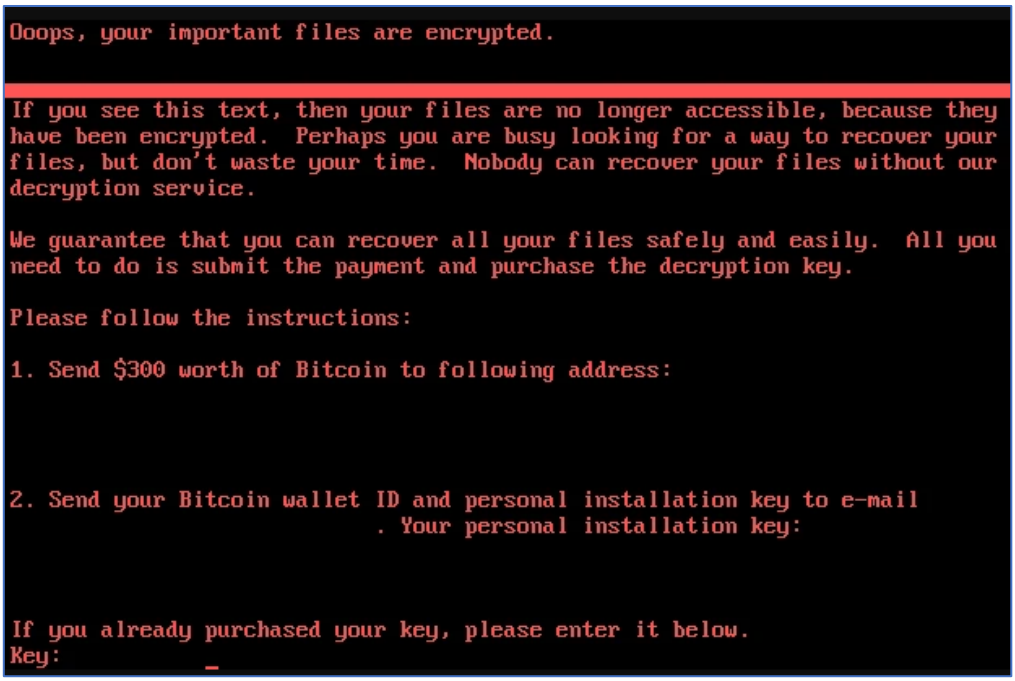


Figura 5 – Nota sobre ransomware NotPetya.

5 ALVOS DO MOONSTONE SLEET

Os principais objetivos do Moonstone Sleet parecem ser a espionagem e a geração de receitas. Os setores alvo até à data incluem indivíduos e organizações nos sectores de software e tecnologia da informação, educação e sectores de base industrial de defesa.

6 RECOMENDAÇÕES

Além dos indicadores de comprometimento elencados abaixo pela ISH, poderão ser adotadas medidas visando a mitigação da referida *ameaça*, como por exemplo:

Utilizar ferramentas de segurança robustas

- Microsoft Defender Antivírus ou outros: Ative a proteção em nuvem e a submissão automática de amostras. Essas funcionalidades utilizam inteligência artificial e aprendizado de máquina para identificar e bloquear ameaças novas e desconhecidas rapidamente.
- Proteção de rede: Ative a proteção de rede para impedir que aplicativos ou usuários acessem domínios maliciosos e outros conteúdos prejudiciais na internet.
- Investigação e remediação automatizadas: Habilite a investigação e remediação em modo totalmente automatizado no Microsoft Defender for Endpoint para permitir ações imediatas em alertas e resolver brechas de segurança de forma eficaz.

Gerenciamento de certificados

- Revogue e monitore certificados de código que possam ter sido comprometidos, como foi o caso com o certificado da CyberLink utilizado em ataques anteriores. Mantenha uma lista de certificados não permitidos para prevenir futuros usos maliciosos.

Monitoramento de Indicadores de Comprometimento (IoCs):

- Utilize indicadores de comprometimento fornecidos por fontes confiáveis como a Microsoft para detectar atividades relacionadas ao Diamond Sleet em sua rede. Isso inclui hashes de arquivos maliciosos, URLs suspeitas e comportamentos típicos do malware.

Segurança em software de terceiros

- Verifique a integridade dos instaladores de software de terceiros e valide a origem dos certificados de assinatura de código. Realize verificações regulares para garantir que os softwares não foram adulterados com código malicioso.

Treinamento e conscientização

- Realize treinamentos regulares de conscientização de segurança para todos os funcionários, focando em métodos de entrega comuns como spear phishing e compromissos drive-by, que são frequentemente utilizados por este grupo.

Atualizações e patches

- Aplique regularmente patches de segurança e atualizações de software para corrigir vulnerabilidades conhecidas que podem ser exploradas por atacantes, incluindo aquelas que permitem elevação de privilégio e execução remota de código.

7 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:	1d5ad4a60ec9be32c11ad99f234bfe8f
sha1:	be6909ba6e0b4d228da5b9daccc83f7082c06cf2
sha256:	f59035192098e44b86c4648a0de4078edbe80352260276f4755d15d354f5fc58
File name:	putty.exe.vir

Indicadores de compromisso do artefato	
md5:	14af3f039f2398b454bbb64c7fdf4a22
sha1:	f1f75da17e8c125b87fdafd76386f90213362bcf
sha256:	cb97ec024c04150ad419d1af2d1eb66b5c48ab5f345409d9d791db574981a3fb
File name:	putty.exe

Indicadores de compromisso do artefato	
md5:	66c45a736e165cf78cee7970bbc74ead
sha1:	b0479c5d4de5541a60923b5627ed62e6391efe2f
sha256:	39d7407e76080ec5d838c8ebca5182f3ac4a5f416ff7bda9cbc4efffd78b4ff5
File name:	66c45a736e165cf78cee7970bbc74ead.virus

Indicadores de compromisso do artefato	
md5:	330fff5b3c54a03fd59a64981e96814d
sha1:	550bdf367fba63a81276465a65dcb64280240dda
sha256:	70c5b64589277ace59db86d19d846a9236214b48aacabbaf880f2b6355ab5260
File name:	UTILITIES.PY._1

Indicadores de compromisso do artefato	
md5:	b8e1fe2955282a58fa3042b25f2ce19d
sha1:	dd91678f1d023607430d53b5ff5f1d6533a98469
sha256:	cafaa7bc3277711509dc0800ed53b82f645e86c195e85fbf34430bbc75c39c24
File name:	

Indicadores de compromisso do artefato	
md5:	608fb305734364e63513ef36da787f2b
sha1:	bda08d55f14827abf21abb79384039660f2fa198
sha256:	9863173e0a45318f776e36b1a8529380362af8f3e73a2b4875e30d31ad7bd3c1
File name:	nk.dll.MALWARE

Indicadores de compromisso do artefato	
md5:	c0bb453d00bf3d8acde09b691ca9b5f2
sha1:	2ebfcbf2deb09e9af046ae765797a654b49645c2
sha256:	f66122a3e1eaa7dcb7c13838037573dace4e5a1c474a23006417274c0c8608be

File name:	delfi-tank-unity.exe

Indicadores de compromisso do artefato	
md5:	6c76f795c4b3ff2e478766dee7c738d6
sha1:	e99d44e93069001129c8f88f7a5259fb21bb6b68
sha256:	56554117d96d12bd3504ebef2a8f28e790dd1fe583c33ad58ccbf614313ead8c
File name:	detankwar.exe

Indicadores de compromisso do artefato	
md5:	08f8353101fb2f11a1036a947f8fce83
sha1:	853d256bafd39426fad9bf5f7fad2971b7978c06
sha256:	ecce739b556f26de07adbfc660a958ba2dca432f70a8c4dd01466141a6551146
File name:	DeTankWar.exe

Indicadores de compromisso do artefato	
md5:	39898007146d7b436d013924db58ebc6
sha1:	dd8b8c4de92d9b6d1d04f0e995f4cc7e746d0a64
sha256:	09d152aa2b6261e3b0a1d1c19fa8032f215932186829cfcca954cc5e84a6cc38
File name:	3393aab1-sample

Tabela 1 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de Domínios	
Domínio	bestonlinefilmstudio[.]org blockchain-newtech[.]com ccwaterfall[.]com chaingrown[.]com defitankzone[.]com detankwar[.]com freenet-zhilly[.]org matrixane[.]com pointdnt[.]com starglowventures[.]com mingeloem[.]com

Tabela 2 – 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.

8 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Microsoft**

9 AUTORES

- **Ismael Pereira Rocha**

heimdall
security research
A DIVISION OF ISH