BOLETIM DE SEGURANÇA

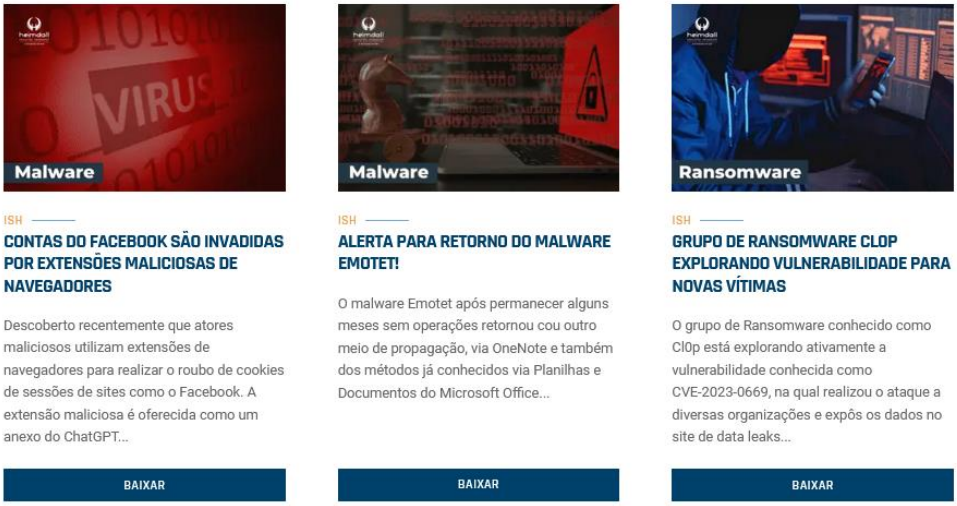
Novos malwares KLogEXE e FPSpy implantados por hackers Norte-Coreanos em ataques direcionados

heimdall
security research
A DIVISION OF ISH

TLP: CLEAR

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 Unit 42 identificaram duas novas amostras de malware utilizadas pelo grupo de ameaças Sparkling Pisces (também conhecido como Kimsuky). Entre elas, um keylogger inédito denominado KLogEXE e uma variante não documentada de um backdoor chamada FPSpy. Essas descobertas ampliam o arsenal do Sparkling Pisces, evidenciando a contínua evolução e o aumento das capacidades do grupo.

2 INFORMAÇÕES SOBRE A AMEAÇA

O grupo APT norte-coreano Sparkling Pisces, também conhecido como Kimsuky, THALLIUM ou Velvet Chollima, é renomado por suas operações avançadas de ciberespionagem e ataques sofisticados de spear phishing. Um dos ataques mais significativos do grupo foi contra a Korea Hydro and Nuclear Power (KHNP) em 2014. Inicialmente, o grupo focava em agências governamentais, instituições de pesquisa na Coreia do Sul. Com o tempo, expandiu suas operações para países ocidentais, incluindo os Estados Unidos, consolidando-se como uma ameaça global. Conhecido como "o rei do spear phishing", o grupo realizou centenas de ataques para induzir vítimas a baixar e executar cargas maliciosas. Recentemente, o grupo mirou em sul-coreanos, disfarçando-se como uma empresa legítima da Coreia e utilizando um certificado válido para assinar malware. O Sparkling Pisces também é reconhecido por sua infraestrutura complexa e em constante evolução, que se sobrepõe entre várias cepas e campanhas de malware.

Ao rastrear a infraestrutura do Sparkling Pisces, foram encontradas conexões entre diferentes operações e ferramentas, revelando o uso de malware novo e não documentado. Uma das amostras, KLogEXE, foi descoberta ao rastrear a infraestrutura usada pelo grupo como comando e controle (C2) de um keylogger do PowerShell documentado pelo JPCERT. O agente da ameaça entregou o keylogger do PowerShell, mencionado em um relatório anterior da ASEC, em uma campanha de spear phishing direcionada a usuários sul-coreanos. O keylogger do PowerShell mencionado no relatório JPCERT se comunica com www.vic.apollo-star7[.]kro.kr, que resolve para 152.32.138[.]167. Na investigação deste endereço IP, foi encontrado outro arquivo, um executável portátil (PE) chamado powershell.exe (a173a425d17b6f2362eca3c8ea4de9860b52faba414bbb22162895641dda0dc2). Ao examinar o arquivo, descobriu-se que ele se comunica com um domínio diferente que resolve para o mesmo endereço IP do keylogger do PowerShell. Ele também utiliza um padrão Uniform Resource Identifier (URI) desconhecido, não observado em outros malwares associados ao Sparkling Pisces.

O gráfico do Maltego mostra as sobreposições entre o malware PowerShell e os dois exemplos de malware PE descobertos, chamados KLogEXE e FPSpy, incluindo domínios semelhantes registrados pelo mesmo e-mail do registrante.

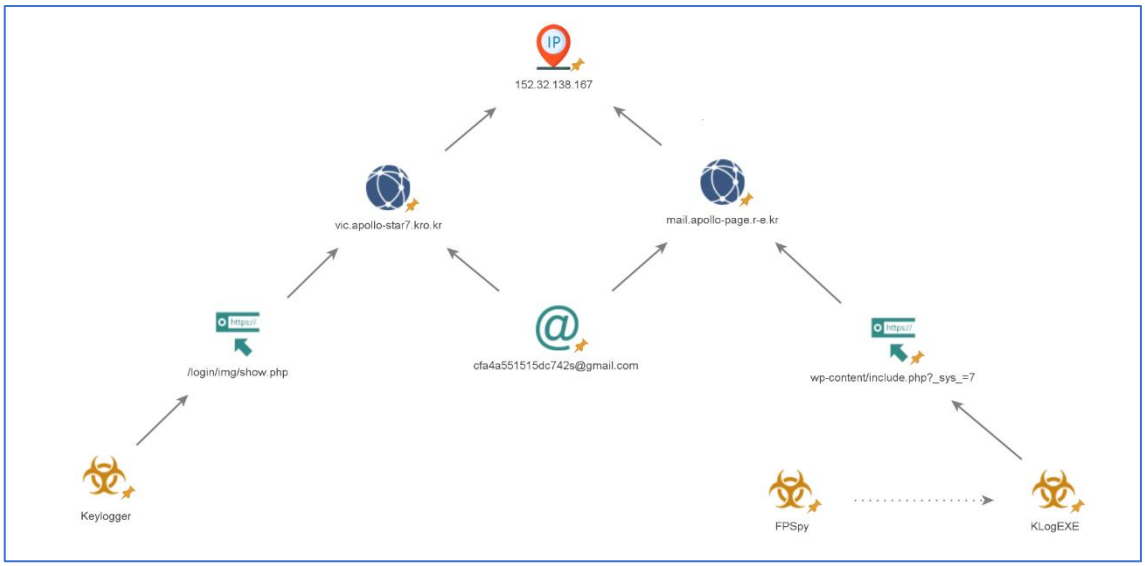


Figura 1 – Infraestrutura mostrando a conexão entre o malware.

O primeiro malware PE identificado, denominado **powershell.exe**, é um keylogger conhecido como **KLogExe**. A partir do recurso de diálogo, verificamos que seu nome interno é **KLogExe**. Este malware parece ser uma versão similar ao keylogger PowerShell previamente mencionado, porém desenvolvido em **C++**.

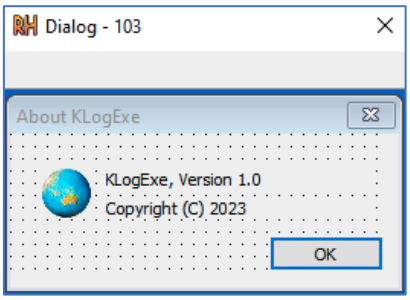


Figura 2 – Recurso de diálogo do KLogExe.

O KLogExe é responsável por coletar diversos dados da máquina infectada, incluindo:

- **Aplicativos em execução** no sistema comprometido.
- **Registro de teclas** pressionadas no teclado, utilizando o método **GetAsyncKeyState**.
- **Cliques do mouse**, com a identificação do nome do botão clicado.

Os dados coletados pelo KLogExe são armazenados em um arquivo **.ini** localizado em **C:\Users\user\AppData\Roaming\Microsoft\desktops.ini**. Quando o arquivo atinge seu limite de tamanho, o KLogExe adiciona a data ao nome do arquivo, gera um novo limite aleatório e envia os dados por **HTTP** para o servidor de comando e controle (C2) através do seguinte URI: **/wp-content/include.php?*sys*=7**.

O segundo malware PE identificado é o FPSpy, uma ameaça que tem se mantido relativamente discreta desde pelo menos 2022. Com base em semelhanças de código e comportamento, este malware parece ser uma variante do descrito na pesquisa da ASEC de 2022. Diversas características, como as convenções de nomenclatura de módulos e logs adicionais baixados, além dos recursos do malware, são muito semelhantes ao backdoor KGHSpy da Sparkling Pisces, descoberto em 2020. Assim como o KGHSpy, suspeitamos que os binários do FPSpy possam ter sido modificados com timestomping. Isso implica que os criadores da ameaça alteraram o tempo de compilação para esconder a data real de criação do malware.

O FPSpy foi carregado pela primeira vez no VirusTotal em 26 de junho de 2024, embora seu timestamp de compilação remonte a 2018. Além disso, descobrimos que o subdomínio codificado para o servidor C2 do malware, bitjoker2024.000webhostapp[.]com, foi visto pela primeira vez em 2024. Diferente do KLogExe, o FPSpy é uma DLL chamada sys.dll com uma única exportação chamada MazeFunc. A DLL está contida em um recurso chamado DB em seu carregador personalizado, cujo objetivo é soltar sys.dll na pasta **C:\Users\user\AppData\Local\Microsoft\WPSOffice** e carregá-lo. A Figura 4 abaixo ilustra o código do carregador.

```
nNumberOfBytesToWrite = 0;
v7 = (const void *)find_load_resource((void *)0xAF, (int)&nNumberOfBytesToWrite, L"DB", v4);
sub_401019(Buffer);
sub_401028(pszPath);
swprintf_s(FileName, 0x104u, L"%s%s", pszPath, L"sys.dll");
swprintf_s(WideCharStr, 0x104u, L"%srundll32.exe %s, %s %%1", Buffer, FileName, L"MazeFunc");
FileW = CreateFileW(FileName, 0x40000000u, 1u, 0, 2u, 0x80u, 0);
```

Figura 3 – Código do carregador sys.dll é responsável por carregar sys.dll.

O FPSpy possui diversas funcionalidades além do keylogging. Entre elas estão:

- Armazenar dados de configuração do dispositivo infectado em um arquivo chamado **Param.ini**.
- Guardar uma grande quantidade de informações do sistema em arquivos nomeados como **Sysinfo_<date>_.txt**.
- Baixar e executar módulos adicionais criptografados.
- Operar em um modelo multithreading, com uma thread dedicada ao download de módulos adicionais e outra ao envio de dados para o C2.
- Executar comandos arbitrários.
- Utilizar o comando PowerShell **tree** para listar unidades, pastas e arquivos no dispositivo infectado, armazenando essas informações em arquivos nomeados como **Drv_<drive letter>**.

OS arquivos mencionados, que são armazenados na pasta **C:\Users\user\AppData\Local\Microsoft\WPSOffice**.

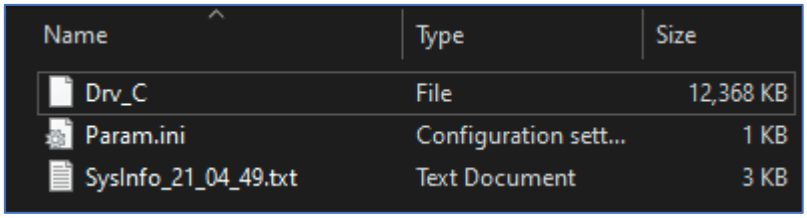


Figura 4 – Arquivos criados pelo FPSpy.

A análise revela que o FPSpy e o KLogExe compartilham a mesma base de código, sugerindo uma ligação entre eles.

Foram identificadas similaridades nas implementações de ambos os malwares, tais como:

- Utilização do mesmo código vazado do HackingTeam para chamadas de API dinâmicas, visando reforçar a detecção estática.
- Estrutura de pacote HTTP codificada de forma semelhante, incluindo cabeçalhos parecidos, uma string de limite gerada aleatoriamente e uma versão antiga do Chrome (Chrome/31.0.1650.57) usada como User-Agent.
- Armazenamento dos dados do malware (como dados de keylogging) em arquivos .ini com conteúdos similares.

Uma seção específica do código é responsável por iniciar o processo de keylogging. Essa mesma seção também constrói o pacote HTTP para a exfiltração de dados tanto do KLogExe quanto do FPSpy.

Figura 5 – Comparação entre a estrutura de pacotes HTTP do FPSpy e do KLogExe.

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:

Use um software antivírus confiável

- Instale e mantenha atualizado um software antivírus de renome que possa detectar e remover malwares como KLogExe e FPSpy.

Mantenha o sistema operacional e os aplicativos atualizados

- Certifique-se de que seu sistema operacional e todos os aplicativos estejam sempre atualizados com os patches de segurança mais recentes.

Evite clicar em links suspeitos

- Não clique em links ou abra anexos de e-mails de remetentes desconhecidos ou suspeitos, pois eles podem conter malwares.

Faça backups regulares

- Realize backups regulares de seus dados importantes em um local seguro e desconectado da rede para evitar perda de dados em caso de infecção.

Use autenticação de dois fatores (2FA)

- Ative a autenticação de dois fatores em todas as suas contas para adicionar uma camada extra de segurança.

Educação e conscientização

- Treine os colaboradores e usuários sobre os riscos de malwares e as melhores práticas de segurança para evitar infecções.

Monitore e analise o comportamento da rede

- Utilize ferramentas de monitoramento para detectar atividades suspeitas na rede e agir rapidamente em caso de anomalias.

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:	e1d683ee1746c08c5fff1c4c2b3b02f0
sha1:	65a76ccf28a6c9593683a874df1c9bca514fb9c4
sha256:	990b7eec4e0d9a22ec0b5c82df535cf1666d9021f2e417b49dc5110a67228e27
File name:	e1d683ee1746c08c5fff1c4c2b3b02f0N.exe

Indicadores de compromisso do artefato	
md5:	9760f489a390665b5e7854429b550c83
sha1:	e9a707ed1cc0a98d17a67a53b3220e8581e78fcc
sha256:	a173a425d17b6f2362eca3c8ea4de9860b52faba414bbb22162895641dda0dc2
File name:	powershell.exe

Indicadores de compromisso do artefato	
md5:	90946c6358eacd119fe1eb36ec7a0a18
sha1:	a5c11cc95a58613ba063522d411e1e5fc9640e13
sha256:	faf666019333f4515f241c1d3fcfc25c67532463245e358b90f9e498fe4f6801
File name:	spoolsv.exe

Indicadores de compromisso do artefato	
md5:	54c58b72f98cb63c44e7694add551e9d
sha1:	35bfaab9d1811f8b6f3126caced09e77fdfafdb9
sha256:	c69cd6a9a09405ae5a60acba2f9770c722afde952bd5a227a72393501b4f5343
File name:	upbit.exe

Indicadores de compromisso do artefato	
md5:	6d6c1b175e435f5564341cc1f2c33ddf
sha1:	a5d5263546cd2d67eb7941154cc24e6c64e78599
sha256:	2e768cee1c89ad5fc89be9df5061110d2a4953b336309014e0593eb65c75e715
File name:	sys.dll

Tabela 1 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
URL	hxxp[:]//mail.apollo-page.re[.]kr/wp-content/include.php?_sys_=7 hxxp[:]//mail.apollo-page.re[.]kr/plugin/include.php?_sys_=7 hxxps[:]//nidlogin.apollo.re[.]kr/cmd/index.php?_idx_=7
Domínio	mail.apollo-page.re[.]kr nidlogin.apollo.re[.]kr bitjoker2024.000webhostapp[.]com www.vic.apollo-star7[.]kro.kr
IP	152.32.138[.]167

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.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Unit42**
- **Thehackernews**

6 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH