BOLETIM DE SEGURANÇA

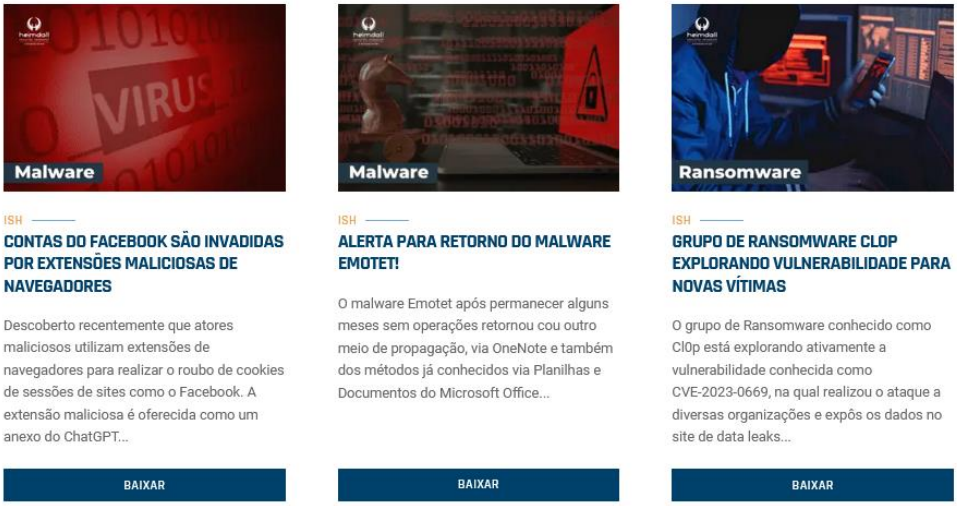
Nova variante do Malware RomCom SnipBot identificada em ataques de exfiltração de dados

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

Uma nova variante do malware **RomCom**, denominada **SnipBot**, foi detectada em ataques focados na rede, visando a exfiltração de dados de sistemas comprometidos.

2 INFORMAÇÕES SOBRE A AMEAÇA

Recentemente, foi descoberta uma nova versão da família de malware RomCom, chamada **SnipBot**. Pela primeira vez, foi possível observar a atividade pós-infecção do invasor em um sistema vítima. Esta nova cepa utiliza novos truques e métodos exclusivos de ofuscação de código, além dos já vistos nas versões anteriores RomCom 3.0 e PEAPOD (RomCom 4.0).

RomCom RAT é uma família de malware que tem evoluído ao longo dos anos, incorporando novos recursos e métodos de ataque. O grupo de ameaças que utiliza o RomCom está ativo desde pelo menos 2022, envolvendo-se em atividades como ransomware, extorsão e coleta direcionada de credenciais, provavelmente para apoiar operações de inteligência. O RomCom passou por várias melhorias, culminando em sua versão mais recente chamada SnipBot, que utiliza novos comandos e técnicas de evasão.

A variante SnipBot do RomCom possui um conjunto básico de funcionalidades que permite ao invasor executar comandos no sistema da vítima e baixar módulos adicionais. O payload inicial é sempre um downloader executável disfarçado como um arquivo PDF ou um arquivo PDF real enviado à vítima por e-mail, que leva a um executável. A primeira amostra do SnipBot encontrada foi um arquivo PDF que exibia texto distorcido, alegando que uma fonte estava faltando para exibição correta. Se a vítima clicasse no link para supostamente baixar e instalar o pacote de fontes, o downloader do SnipBot seria baixado.

O SnipBot opera em vários estágios, com o downloader inicial sendo sempre um arquivo executável, seguido por cargas úteis adicionais em formato EXE ou DLL. O downloader é sempre assinado com um certificado de assinatura de código legítimo e válido. Não se sabe exatamente como os agentes de ameaça obtêm esses certificados, mas é provável que sejam roubados ou adquiridos por meio de fraude. Os módulos subsequentes não são assinados.

Ao analisar os dados de telemetria do Cortex XDR e realizar a engenharia reversa da amostra inicial, foi possível reconstruir toda a cadeia de infecção. O vetor inicial de infecção foi um e-mail contendo um link que redirecionava duas vezes para o downloader do SnipBot.

A sequência de URLs, desde o e-mail inicial até o link final do arquivo de download do SnipBot. O invasor registrou os domínios fastshare[.]click e docstorage[.]link. O site temp[.]sh é um serviço legítimo de compartilhamento de arquivos, com um período de hospedagem de três dias.

Figura 1 – Cadeia de URL do e-mail para o downloader.

Foi identificada uma nova sequência de links que, provavelmente, foi utilizada pelo mesmo invasor para distribuir uma variante semelhante do downloader SnipBot. O domínio inicial diferente e o nome similar do arquivo do downloader sugerem que isso fazia parte de uma campanha direcionada a múltiplas vítimas. Outra sequência de URLs foi empregada em um ataque distinto. O invasor registrou o domínio publicshare[.]link, que não é um serviço legítimo de compartilhamento de arquivos.

Figura 2 – Cadeia de URL diferente do e-mail para o downloader.

A cadeia de infecção do SnipBot envolve vários estágios. O downloader inicial, Attachment_Medical report.exe, é um executável Windows de 64 bits (SHA256: 57e59b156a3ff2a3333075baef684f49c63069d296b3b036ced9ed781fd42312) disfarçado como um arquivo PDF. Este arquivo é assinado com um certificado possivelmente roubado ou falsificado da empresa dinamarquesa CC Byg og Udlejning ApS.

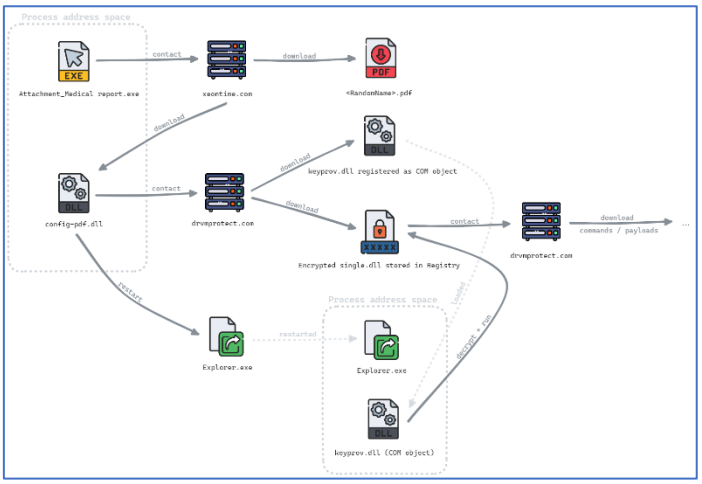


Figura 3 – Fluxo de execução do SnipBot do downloader EXE inicial para o arquivo principal do bot single.dll.

Este downloader utiliza dois métodos anti-sandbox simples, mas eficazes. O primeiro compara o nome do arquivo original com um valor codificado. O segundo verifica se há pelo menos 100 entradas na chave de registro HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs, algo comum em sistemas de usuários regulares, mas raro em sandboxes. Além disso, o downloader é ofuscado com um algoritmo baseado em mensagens de janela, dividindo o código em blocos acionados por mensagens personalizadas.

Para isso, uma janela é criada com uma mensagem de retorno de chamada contendo esses blocos de código. A fila de mensagens da janela chama cada bloco na ordem original. O primeiro bloco é acionado pela mensagem inicial, e cada bloco subsequente envia a próxima mensagem quando pronto. Blocos também podem enviar mensagens aninhadas, complicando o rastreamento do fluxo de execução.

A maioria das strings, como o domínio de comando e controle (C2) e nomes de funções de API, são criptografadas para evitar detecção estática, dificultando a análise de malware. Após a execução, o downloader contata o domínio C2 xeontime[.]com para obter um arquivo PDF e o primeiro payload. Embora o payload original não tenha sido recuperado, o invasor baixou o mesmo payload com dados de configuração diferentes e o iniciou manualmente, permitindo a continuação da análise.

O PDF é baixado para a pasta temporária do usuário com um nome aleatório antes de ser aberto. O primeiro payload é um arquivo DLL (config-pdf.dll) executado na memória, contendo uma função exportada chamada GetStore com código malicioso. Este DLL baixa o próximo estágio, keyprov.dll, do segundo C2 drvmcprotect[.]com e o injeta no Explorer, usando sequestro COM para registrá-lo como a biblioteca de cache de miniaturas no registro do usuário.

Ao reiniciar o explorer.exe, a DLL é carregada e executada. Embora confiável, este método pode causar falhas, como ocorreu na máquina da vítima.

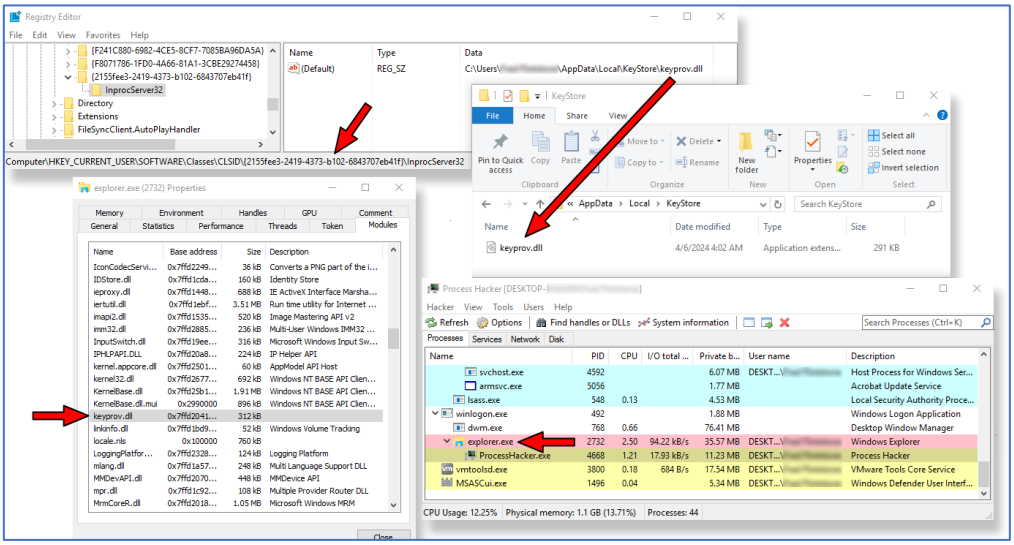


Figura 4 – Injeção do Explorer via sequestro de COM, conforme mostrado no Process Hacker 2.

Para esta publicação, monitoramos o VirusTotal em busca de amostras recentes de downloaders. Encontramos cinco versões recentes que, embora quase idênticas em função, diferem na implementação. Todas foram hospedadas em temp[.]sh, um serviço de compartilhamento de arquivos preferido pelo invasor.

A versão mais recente difere no conjunto de funções de API resolvidas dinamicamente em comparação com o downloader do nosso caso. Além disso, o código de ofuscação baseado em mensagens de janela foi removido. A amostra mais recente encontrada foi chamada Attachment_CV_June2024.exe (SHA256: 5390ba094cf556f9d7bbb00f90c9ca9e04044847c3293d6e468cb0aaeb688129), conectando-se ao domínio C2 linedrv[.]com para baixar o PDF de isca e a carga útil do próximo estágio.

Outra amostra, chamada atch_Medical_Report_Scan05202024.exe (SHA256: 0be3116a3edc063283f3693591c388eec67801cdd140a90c4270679e01677501), tinha o mesmo signatário e o domínio C2 drv2ms[.]com. A última amostra, cujo nome de arquivo é desconhecido (SHA256: 2c327087b063e89c376fd84d48af7b855e686936765876da2433485d496cb3a4), foi assinada pela Hangzhou Yueju Apparel Co., Ltd. e também contatou drv2ms[.]com.

Analisando o código do malware, nota-se que os autores concentraram todas as funcionalidades em poucas funções extensas. Os arquivos foram escritos em C++. O código apresenta pequenas falhas, sugerindo que o invasor tem alguma experiência como desenvolvedor de Windows, mas não é um especialista.

Um exemplo disso é a função da API CreateDirectory(), que é chamada duas vezes consecutivas, indicando um possível erro de copiar e colar.

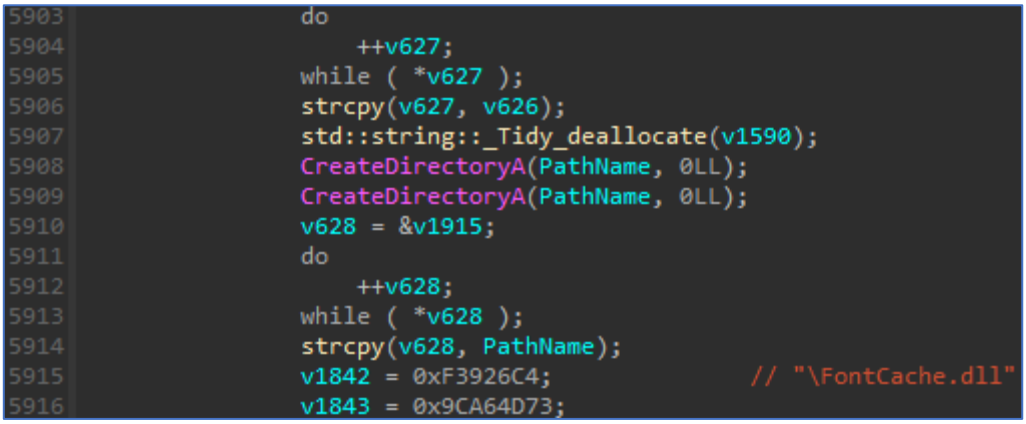


Figura 5 – Falha de código ao usar a função de API CreateDirectoryA() duas vezes.

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:

Cuidado com anexos de e-mail e links

- Evite abrir anexos ou clicar em links de remetentes desconhecidos. Verifique a autenticidade do e-mail antes de interagir com qualquer conteúdo.

Baixe software de fontes confiáveis

- Utilize apenas sites oficiais ou lojas de aplicativos reconhecidas para baixar arquivos e software. Evite sites de terceiros e nunca use software pirata.

Mantenha seu sistema atualizado

- Realize atualizações regulares do sistema operacional e aplicativos para proteger contra vulnerabilidades conhecidas que malwares como o SnipBot exploram.

Use antivírus e firewall

- Instale e mantenha atualizados programas antivírus e firewalls para detectar e prevenir infecções por malware.

Eduque a si mesmo e à sua equipe

- Conscientização é essencial. Aprenda sobre ameaças emergentes e treine os funcionários para reconhecer tentativas de phishing e outras táticas usadas por cibercriminosos.

Faça backups regulares

- Realize cópias periódicas dos seus dados para garantir que você possa recuperá-los em caso de infecção por malware.

Use autenticação forte

- Implemente a verificação em duas etapas sempre que possível e evite repetir senhas. Armazene suas senhas de forma segura e troque-as imediatamente se suspeitar de vazamento.

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:	7f2e4a44445b977ef8917cc0fb79035b
sha1:	983332a5660ec6c28123e745023b41105775ab6f
sha256:	0be3116a3edc063283f3693591c388eec67801cdd140a90c4270679e01677501
File name:	atch_scan052224_CV.exe

Indicadores de compromisso do artefato	
md5:	d69cf309cb0e5d91237c6454e0e0dc45
sha1:	b37640cc1ef9354808562ced599a5ff0923156ac
sha256:	2c327087b063e89c376fd84d48af7b855e686936765876da2433485d496cb3a4
File name:	bzb.exe

Indicadores de compromisso do artefato	
md5:	6fa6dd331844ee5cfe20c74353c1e442
sha1:	16572311d9007d226f2e6d0abc3b980ffbc7521d
sha256:	5390ba094cf556f9d7bbb00f90c9ca9e04044847c3293d6e468cb0aaeb688129
File name:	Attachment_CV_June2024.exe

Indicadores de compromisso do artefato	
md5:	c0e499402acb6c302228b4a7923d5db6
sha1:	cb3d3a7e39e7cdc8501ae0eff77d02a1c995bc31
sha256:	57e59b156a3ff2a3333075baef684f49c63069d296b3b036ced9ed781fd42312
File name:	Attachment_Medical report.exe

Indicadores de compromisso do artefato	
md5:	524dda2410cc7ee8cc326ca42cebd7dd
sha1:	42673214d773b6af23944a65f47d2841bad75de7
sha256:	a2f2e88a5e2a3d81f4b130a2f93fb60b3de34550a7332895a084099d99a3d436
File name:	42673214d773b6af23944a65f47d2841bad75de7.exe

Indicadores de compromisso do artefato	
md5:	fa400cb70d13cb329d05877b8fe73ed5
sha1:	0fa5bfed7dafbe248f436a6b6ca4b08e7e859fd4
sha256:	b9677c50b20a1ed951962edcb593cce5f1ed9c742bc7bff827a6fc420202b045
File name:	config-pdf.dll

Tabela 1 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
Domínio	fastshare[.]click docstorage[.]link publicshare[.]link xeontime[.]com drvmcprotect[.]com mcprotect[.]cloud cethernet[.]com sitepanel[.]top ilogicflow[.]com webtimeapi[.]com dns-msn[.]com certifysop[.]com drv2ms[.]com olminx[.]com linedrv[.]com adobe.cloudcreative[.]digital 1drv.fileshare[.]direct
IP	91.92.250[.]104

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**
- **Bleepingcomputer**

6 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH