BOLETIM DE SEGURANÇA

Descoberta variante macOS do LightSpy com capacidades de monitoramento sofisticadas

heimdall
security research
A DIVISION OF ISH

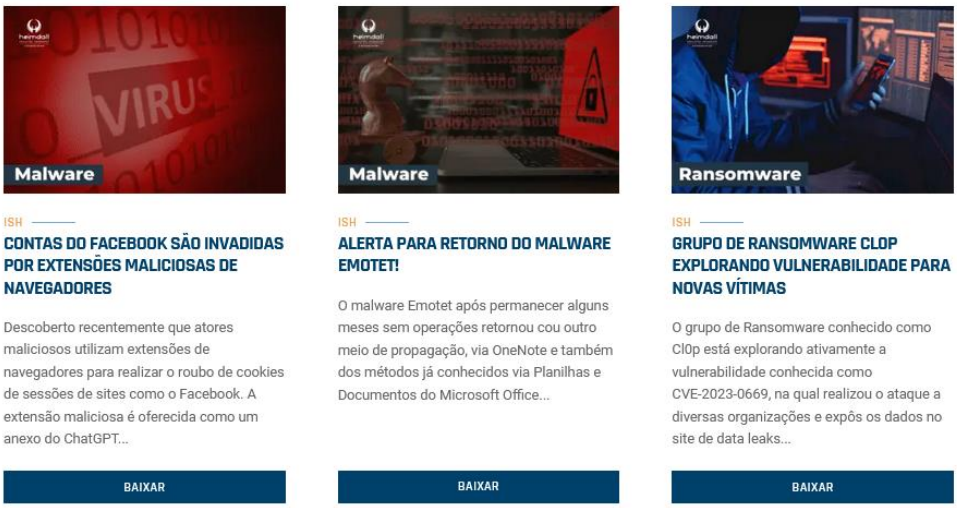
TLP: CLEAR

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

Pesquisadores de segurança cibernética do Huntress e do ThreatFabric revelaram que o spyware LightSpy, recentemente identificado como alvo de usuários do Apple iOS, é na verdade uma variante de um implante macOS não documentado anteriormente e que estão associados à estrutura de malware multiplataforma, que tem como potencial alvos sistemas Android, iOS, Windows, macOS, Linux e roteadores da NETGEAR, Linksys e ASUS.

2 INFORMAÇÃO SOBRE A AMEAÇA

Em outubro de 2023, um estudo revelou detalhes sobre a conhecida estrutura de espionagem LightSpy2. A pesquisa confirmou com grande certeza que os implantes para Android e iOS foram criados pelo mesmo desenvolvedor e utilizavam a mesma infraestrutura de rede. No entanto, esses implantes eram apenas uma fração de uma estrutura muito maior.

Na época, já se sabia que o framework deveria incluir implantes para outras quatro plataformas: Windows, macOS, Linux e o chamado Router. A suposição era de que os ciberatacantes poderiam ter acesso não somente a dispositivos móveis e de mesa, mas também a dispositivos de rede de marcas como Netgear, Linksys e Asus.

```
!('linux' !== t && 'unknown' !== t || !s.includes(e))
|| (!('S13' !== this.x_phone_info.mtype || !_.includes(e))
    || (!('ios' !== t || !i.includes(e))
        || (!('ipad' !== t || ![
    'phoneinfo',
    'location',
    'contacts',
    'files',
    'screenshot',
    'app',
    'wifi',
    'keychain',
    'shell',
    'command'
].includes(e)) || ('router' === t && o.includes(e) ?
        ('Linksys' !== this.show_flow_or_hijack || 'flow' !== e) && !(![
    'Netgear',
    'Linksys',
    'Asus'
].includes(this.show_flow_or_hijack) && 'hijack' === e) :
        !('windows' !== t || !a.includes(e))
        || (!('mac' !== t || !l.includes(e))
        || !('android' !== t || !r.includes(e))))));
```

Figura 1 – Fabricantes alvos do malware.

Em 11 de janeiro de 2024, uma série de URLs foram enviados para o VirusTotal. Todos eles incluíam o número “96382741”, anteriormente utilizado como nome de diretório para armazenar arquivos LightSpy Android e iOS. Esses URLs direcionavam para arquivos HTML e JavaScript, que continham strings idênticas e foram disponibilizados no Github. Esses arquivos estavam associados à vulnerabilidade CVE-2018-4233, identificada no WebKit, e visavam especificamente a versão 10.13.3 do macOS e versões do iOS anteriores à 11.4.

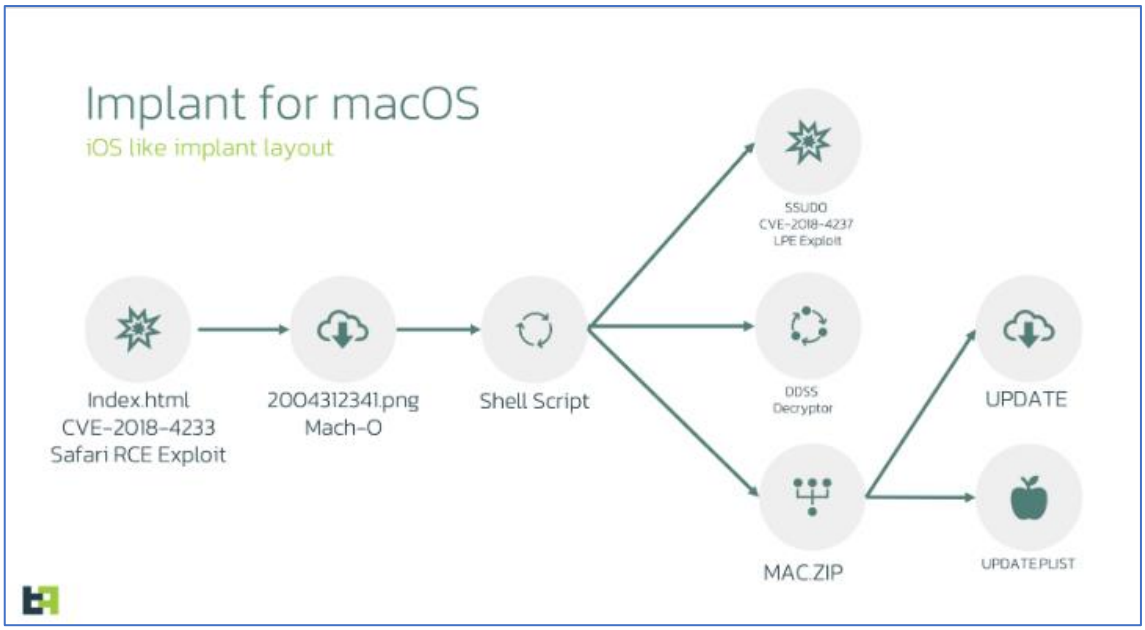


Figura 2 – Cadeia de implementação para dispositivos MacOS.

A ameaças empregou uma estratégia semelhante à usada para distribuir implantes iOS, ativando a vulnerabilidade do WebKit no Safari para executar códigos arbitrários sem privilégios. No caso do macOS, eles utilizaram o exploit CVE-2018-4233, cujo código foi divulgado em 18 de agosto de 2018. Dado que a vulnerabilidade afetou os WebKits tanto do iOS quanto do macOS, é possível que os implantes para ambos os sistemas operacionais tenham sido distribuídos de maneira similar por um período. A principal diferença residia no escalonamento de privilégios locais, que é específico para cada sistema operacional.

A exploração do RCE já foi amplamente documentada pelo autor e outros pesquisadores, portanto, não será discutida neste relatório. Contudo, é importante ressaltar que o propósito único dessa exploração é entregar a carga útil da próxima fase, denominada 20004312341.png.

```
get_png('20004312341.png', true, function()
{
        var buf = this.response;
        var arrayBuf = new Uint8Array(buf);
        window.binary = arrayBuf;
        resolve('ok');
}
);
```

Figura 3 – Entrega da carga útil 20004312341.png.

A estrutura das versões macOS do implante é idêntica à do Android e iOS: o Core atua como um despachante de comandos e a funcionalidade é ampliada por meio de plug-ins adicionais. Tanto o Core quanto os plug-ins podem ser atualizados dinamicamente através de um comando do C2. A lista e as funcionalidades dos plug-ins para a versão macOS são distintas dos outros implantes, variando conforme a plataforma alvo. Um aspecto importante a ser destacado é que a versão para desktop não possui tantas funções de exfiltração quanto a versão móvel.

O plug-in LanDevices tem a tarefa de extrair senhas, certificados e chaves do Keychain, permitindo que os atacantes acessem as senhas de Wi-Fi, já que essas também são armazenadas no Keychain. Além disso, ele realiza uma verificação básica da rede para identificar todos os dispositivos conectados à mesma rede que a vítima. Este plugin utiliza o framework SimplePing para realizar ping no host e verificar a disponibilidade do dispositivo correspondente, em seguida, elabora uma lista de dispositivos potencialmente interessantes usando o endereço IP da rede à qual está conectado no momento e a máscara de sub-rede. Depois, realiza ping em cada um desses dispositivos e tenta identificar uma lista de parâmetros específicos.

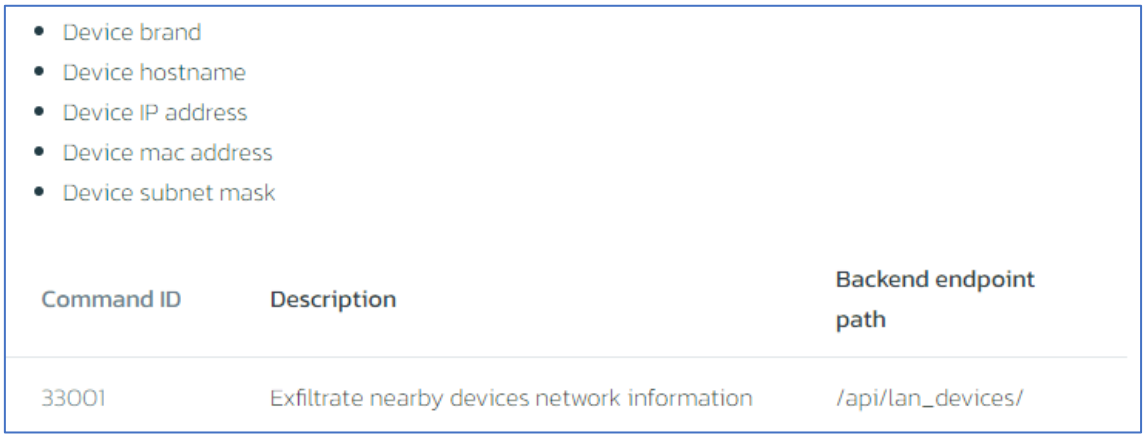


Figura 4 – Identificação do dispositivo pela rede

O plug-in Softlist tem a função de extrair duas listas distintas:

- Lista de aplicativos que estão instalados;
- Lista dos processos que estão sendo executados no momento.

Para listar os aplicativos instalados, o plugin irá percorrer a pasta de Aplicativos e, para cada subpasta encontrada, tentará acessar o arquivo Info.plist, que contém os detalhes do aplicativo. Os parâmetros a seguir serão obtidos de cada arquivo plist:

- CFBundleName: o nome do aplicativo que é exibido durante a instalação;
- CFBundleIdentifier: o nome do pacote do aplicativo;
- CFBundleShortVersionString: a versão do aplicativo.

Para listar os processos em execução no momento, o plugin invocará o método “runningApplications” da classe “sharedWorkspace”. Os seguintes parâmetros serão extraídos:

- Identificador do processo;
- Caminho do processo;
- Caminho de dados do processo;
- Nome do pacote.

Command ID	Description	Backend endpoint path
16001	Exfiltrate the list of installed applications	/api/app/
16002	Exfiltrate the list of currently running processes	/api/process/

Figura 5 – Diretórios para exfiltração de dados.

Em uma pesquisa foi analisados todos os hosts associados ao LightSpy conhecidos até então, porém não conseguiu-se identificar nenhum host, além do 103.27.109[.]217, vinculado à campanha do macOS. Contudo, observamos um painel quase idêntico em outros hosts ligados ao LightSpy.

Em março de 2024 que o conteúdo do painel apareceu pela primeira vez no VirusTotal, sendo este um plano de fundo de uma página web.

Os parâmetros a seguir foram extraídos:

- Identificador do processo;
- Caminho do processo;
- Caminho de dados do processo;
- Nome do pacote.

2024-03-21	0 / 93	200	https://103.27.109.217:3458/img/bg.d1087110.jpg
2024-03-19	0 / 93	-	https://103.27.109.217/963852741/mac/plugins/0408ece5a667ec06
2024-04-17	4 / 92	200	http://103.27.109.217:52202/963852741/mac/plugins/4d29ee714380cd29
2024-03-19	0 / 93	404	http://103.27.109.217:52202/963852741/ios/ios123-133/device.js
2023-12-15	0 / 90	200	http://103.27.109.217:52202/963852741/mmfile/ads/bbbb.jar

Figura 6 – Conteúdo submetido ao VírusTotal.

Ao examinar a relação de vítimas presentes no painel, percebeu-se que alguns indivíduos listados poderiam, na verdade, ser os agressores. Um exemplo disso é um dispositivo que apresentava um histórico de navegador repleto de URLs direcionadas para um arquivo HTML que explorava a infecção inicial por meio de um RCE.

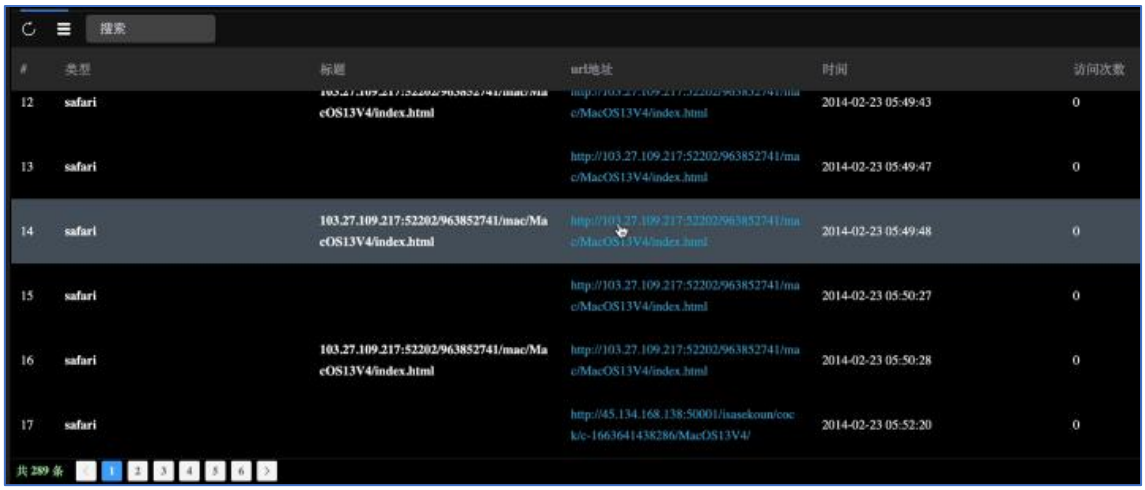


Figura 7 – Listagem das vítimas.

Observou-se a mesma marca nos aparelhos iOS; o histórico registrado no aplicativo de mensagens continha somente mensagens de teste.

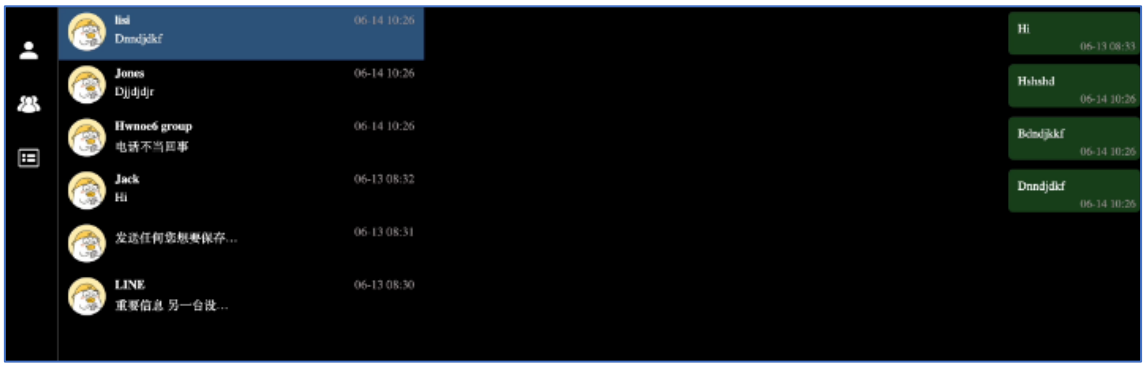


Figura 8 – Histórico de mensagem de aplicativo IOS.

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:

Atualizações do sistema operacional

- Mantenha seu sistema operacional atualizado. Os invasores do LightSpy têm usado falhas de segurança mais antigas para atacar sistemas. Portanto, instalar as versões mais recentes do sistema operacional pode ajudar a proteger seu dispositivo.

Cuidado com links

- Tenha muito cuidado ao abrir links, especialmente os enviados por estranhos. O ataque do LightSpy começa explorando uma vulnerabilidade através de páginas HTML maliciosas.

Software antivírus

- Considere o uso de um software antivírus confiável. Ele pode detectar e remover malwares, incluindo o LightSpy.

Informações sensíveis

- Esteja ciente de que o LightSpy pode roubar dados do navegador, registrar sua tela, tirar fotos e até recuperar informações sensíveis, como suas senhas do Apple Keychain.

Downloads seguros

- Faça download apenas de fontes confiáveis. Evite baixar aplicativos de fontes desconhecidas, pois eles podem conter malwares como o LightSpy.

Firewall

- Use um firewall. Ele pode bloquear conexões não autorizadas, impedindo que o LightSpy se comunique com os servidores de comando e controle.

Educação em segurança cibernética

- Esteja ciente das últimas ameaças e como evitá-las. A educação em segurança cibernética pode ajudá-lo a reconhecer e evitar ataques de phishing e outras táticas usadas pelos invasores do LightSpy.

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:	f21132daac7652c160453ff956655349
sha1:	7f4a770bee014750b2694d72c6105e489585639f
sha256:	4607dfdd78fcb8d6bf94ecc34cf125f20e4ea94ac9fce002d9e7cd7956a707dd
File name:	0408ece5a667ec06

Indicadores de compromisso do artefato	
md5:	31028fcdb5313ae7e7868df1d3f567eb
sha1:	d18d7430fcbd863f21950e215be63c4245986172
sha256:	75a571d33a7c11fb5515a08a46fcb67dabbcb3fd4cbf69894ab82e394e68679c
File name:	26f7d6b449f01571

Indicadores de compromisso do artefato	
md5:	54570441e91d8e65ea81bb265ba71c8c
sha1:	7aceb8db03b8b8c7899982b5befcaf455a86fe0b
sha256:	4511567b33915a4c8972ef16e5d7de89de5c6dffe18231528a1d93bfc9acc59f
File name:	libLanDevices

Indicadores de compromisso do artefato	
md5:	6371a942334444029f73b2faa2b76cf6
sha1:	0563225dcc2767357748d9f1f6ac2db9825d3cf9
sha256:	0f662991dbd0568fc073b592f46e60b081eedf0c18313f2c3789e8e3f7cb8144
File name:	libAudioRecorder

Tabela 1 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
IP	103.27.109[.]217

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**
- Threatfabric
- Thehackernews

6 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH