TLP: CLEAR

BOLETIM DE SEGURANÇA

Banshee, o Stealer que "Roubou Código" do MacOS XProtect

heimdall
security research

Acesse a nossa nova comunidade através do WhatsApp!

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

heimdall
security research
A DIVISION OF ISH

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

1 INTRODUÇÃO EXECUTIVA

Este relatório de segurança, desenvolvido pela equipe de **Inteligência de Ameaças da ISH, Heimdall**, tem como objetivo proporcionar uma compreensão aprofundada e um dimensionamento preciso das ameaças cibernéticas identificadas. O documento está estruturado em três níveis de abordagem: ***Estratégico***, ***Tático*** e ***Operacional***, garantindo uma visão completa e integrada das ameaças e ações recomendadas.

2 ESTRATÉGICO

2.1 SEGMENTO DE MERCADO

Os alvos potencialmente afetados por essa ameaça que será descrita neste relatório, incluem:

- *Organizações que utilizam dispositivos macOS*
- *Design gráfico*
- *Mídia*
- *Desenvolvimento de software*
- *Setores educacionais*
- *Usuários individuais de macOS*

2.2 IMPACTO FINANCEIRO POTENCIAL

- *Roubo de credenciais e dados financeiros*
- *Perda de propriedade intelectual e dados sensíveis*
- *Custos de resposta e remediação*
- *Danos à reputação*
- *Penalidades legais e regulatórias*
- *Interrupção operacional*
- *Fraudes financeiras utilizando as informações roubadas*

2.3 OBJETIVO DA AMEAÇA

O principal objetivo do Banshee é coletar e exfiltrar dados sensíveis dos sistemas macOS comprometidos, incluindo credenciais de login, informações de navegadores, carteiras de criptomoedas e detalhes do sistema, para posterior uso malicioso ou venda em fóruns clandestinos.

3 TÁTICO

3.1 INFORMAÇÕES SOBRE A AMEAÇA

O Banshee foi identificado pela primeira vez em julho de 2024, atuando como um "stealer-as-a-service", oferecido por aproximadamente US$ 3.000 em fóruns clandestinos, como XSS e Exploit. Desde o início, seu foco principal foi a coleta e exfiltração de dados sensíveis de dispositivos macOS, incluindo credenciais de navegadores, carteiras de criptomoedas e outras informações críticas. Em setembro de 2024, uma versão atualizada do Banshee introduziu um algoritmo de criptografia de strings semelhante ao utilizado pelo XProtect, o antivírus nativo do macOS. Essa mudança tornou o malware mais sofisticado e capaz de evitar detecção por soluções de segurança por mais de dois meses. Mesmo após o vazamento de seu código-fonte em novembro de 2024, o Banshee continuou sendo distribuído ativamente por meio de campanhas de phishing e repositórios maliciosos hospedados no GitHub.

Recentemente, novas variantes do Banshee têm sido observadas, demonstrando a evolução contínua do malware. Ele agora é capaz de operar de forma furtiva, aproveitando técnicas avançadas de evasão para contornar as defesas de segurança do macOS. Descoberto pela CheckPoint, o malware utiliza criptografia de strings inspirada no próprio XProtect, permitindo que seus componentes maliciosos se camuflem de forma eficaz.

3.2 OPERAÇÃO E CAPACIDADE DA AMEAÇA

O Banshee Stealer demonstra o avanço das ameaças cibernéticas modernas, destacando sua complexidade e eficiência em comprometer sistemas. Conforme análise da Checkpoint, após ser instalado, o malware executa diversas ações maliciosas:

Coleta de dados do sistema

- O Banshee tem como foco navegadores populares como *Chrome*, *Brave, Edge* e *Vivaldi*, além de extensões de carteiras digitais de criptomoedas. Ele também visa extensões de autenticação em duas etapas (2FA) para capturar informações confidenciais. Entre os dados coletados estão detalhes do sistema operacional, informações de hardware e software, endereços IP públicos e senhas armazenadas no macOS.

Manipulação de usuários

- O malware exibe janelas pop-up falsas que simulam prompts legítimos do macOS, induzindo os usuários a inserir suas credenciais de sistema, como senhas administrativas.

Evasão de detecção

- Para evitar ser identificado, o Banshee emprega técnicas avançadas de evasão, incluindo mecanismos anti-análise que impedem a ação de ferramentas de depuração e softwares antivírus.

Exfiltração de dados

- As informações capturadas são enviadas para servidores de comando e controle, utilizando arquivos criptografados e codificados, garantindo que os dados roubados sejam transmitidos de forma segura e difícil de rastrear.

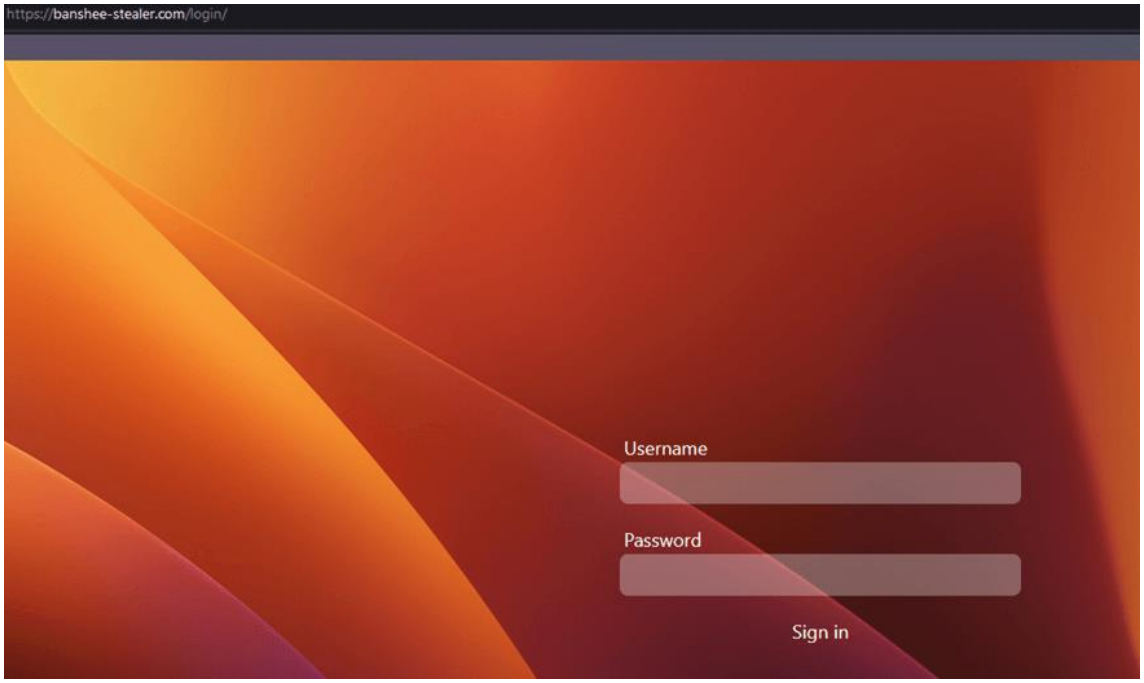

Figura 1 – Painel de login do Banshee.

Conforme já mencionado os agentes da ameaça utilizaram repositórios no GitHub como um canal para distribuir chaves associadas ao Banshee. Nessas campanhas, os alvos principais eram usuários de macOS, que recebiam o Banshee, enquanto usuários de Windows eram atingidos por outro malware, o Lumma Stealer, uma ameaça já conhecida. Durante três fases distintas, os atacantes criaram repositórios maliciosos que imitavam projetos populares de software para enganar os usuários e induzi-los a baixar os arquivos infectados. Esses repositórios eram cuidadosamente elaborados para parecer legítimos, com classificações positivas e estrelas, a fim de criar uma falsa sensação de segurança e confiança antes do lançamento das campanhas maliciosas.

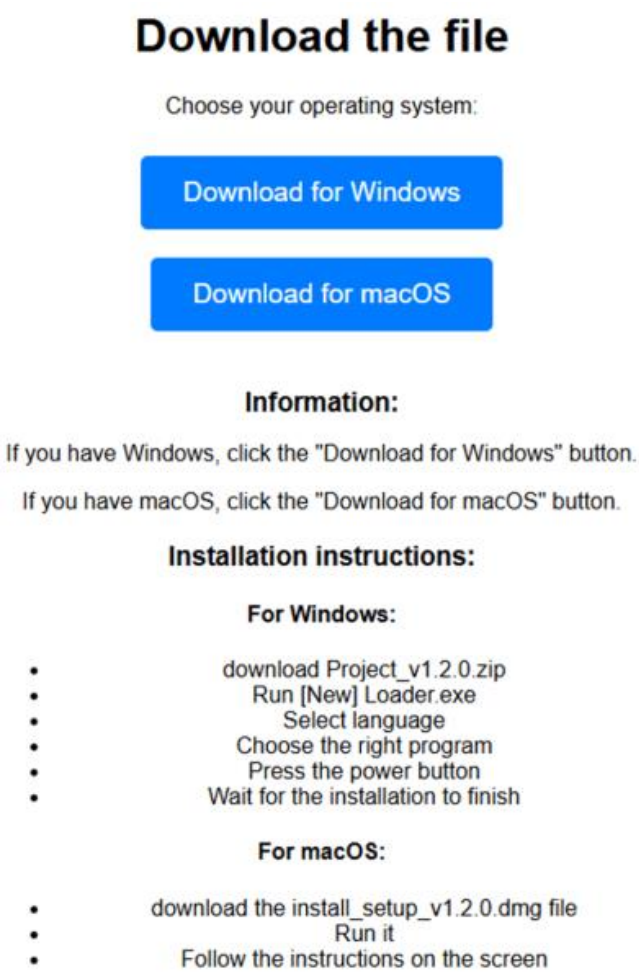

Figura 2 – Exemplo de página no Github hospedando o malware.

A ameaça representada pelo Banshee é séria e requer atenção por parte das organizações, especialmente aquelas que utilizam dispositivos macOS. Suas capacidades avançadas de coleta de dados e evasão de detecção, combinadas com uma distribuição bem elaborada por meio de engenharia social, tornam essa ameaça uma grande preocupação. As organizações devem adotar medidas proativas de segurança, como reforço de políticas de autenticação, implementação de soluções de segurança específicas para macOS e conscientização dos funcionários sobre os riscos de engenharia social.

3.3 TABELA MITRE ATT&CK

Este tópico apresenta as Táticas, Técnicas e Procedimentos (TTPs) identificados nesta ameaça, conforme o framework MITRE ATT&CK, oferecendo uma visão tática detalhada sobre o comportamento do adversário. O objetivo é permitir o mapeamento das técnicas utilizadas pelos atacantes, facilitando a implementação de contramedidas eficazes e o aprimoramento das defesas de segurança.

Tática	Técnica	Detalhes
Initial Access	T1566 Phishing	Os operadores do Banshee distribuíram o malware por meio de sites de phishing que se passavam por software legítimo, induzindo os usuários a baixá-lo.
Execution	T1204.002 User Execution: Malicious File	O Banshee requer que o usuário execute o software malicioso baixado, geralmente acreditando ser uma aplicação legítima.
Defense Evasion	T1027 Obfuscated Files or Information	O Banshee utiliza técnicas de ofuscação, incluindo a adoção de algoritmos de criptografia semelhantes aos usados pelo XProtect da Apple, para evitar a detecção por soluções de segurança.
Defense Evasion	T1070.004 Indicator Removal: File Deletion	O malware remove arquivos que possam indicar sua presença no sistema, auxiliando na evasão de detecção.
Credential Access	T1555.003 Credentials from Web Browsers	O Banshee é capaz de extrair credenciais armazenadas em navegadores web, incluindo senhas e cookies.
Collection	T1056 Input Capture	O Banshee pode capturar entradas do usuário, como pressionamentos de tecla, para coletar informações sensíveis.
Exfiltration	T1041 Exfiltration Over C2 Channel	O malware exfiltra dados coletados para servidores de comando e controle controlados pelos atacantes.

Tabela 1 – Tabela MITRE ATT&CK.

4 RECOMENDAÇÕES

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

Educação e conscientização

- Treine os usuários para reconhecer e evitar e-mails de phishing e sites suspeitos.

Verificação de software

- Baixe aplicativos apenas de fontes oficiais e verifique a legitimidade antes da instalação.

Soluções de segurança

- Utilize softwares antivírus e antimalware atualizados para complementar as defesas nativas do macOS.

Atualizações regulares

- Mantenha o sistema operacional e todos os softwares atualizados com os patches de segurança mais recentes.

Monitoramento de rede

- Implemente ferramentas de monitoramento para detectar atividades suspeitas ou anômalas na rede.

Gestão de senhas

- Utilize gerenciadores de senhas para criar e armazenar credenciais fortes e únicas.

Autenticação Multifator (MFA)

- Ative o MFA sempre que possível para adicionar uma camada extra de segurança às contas.

5 OPERACIONAL

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 Comprometimento (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

5.1 INDICADORES DE COMPROMETIMENTO (IOC)

Indicadores do artefato	
md5:	60a8e63db05a324ea69686712aed7d95
sha1:	af396b57c8afd3aca774898b30308cb4f137dc94
sha256:	1dcf3b607d2c9e181643dd6bf1fd85e39d3dc4f95b6992e5a435d0d900333416
File name:	install_setup_v1.2.0.dmg

Indicadores do artefato	
md5:	65c9c2fd1381ce9803cc528501e3b69d
sha1:	02f9b2ab38234f7b853f00e2fd26705bc5d0744e
sha256:	d8ecc92571b3bcd935dcab9cdbeda7c2ebda3021dda013920ace35d294db07be
File name:	Soft.Install.v1.4 (1).zip

Indicadores do artefato	
md5:	e4f1b38c8116249ccf8b6bdf033b622e
sha1:	db2b5a43521e44322652c58d8dfc7f1d2f19f298
sha256:	ce371a92e905d12cb16b5c273429ae91d6ff5485dda04bfedf002d2006856038
File name:	Setup

Tabela 2 – Indicadores de Comprometimento

5.2 INDICADORES DE URL, IPS E DOMÍNIOS

Indicadores de URL, IPs e Domínios	
URL	hxxps://steamcommunity[.]com/profiles/76561199724331900
Domínio	authorisev[.]site contemteny[.]site dilemmadu[.]site faulteyotk[.]site forbidstow[.]site goalyfeastz[.]site opposezmny[.]site seallysl[.]site servicedny[.]site
IP	41[.]216[.]183[.]49

Tabela 3 – Indicadores de Comprometimento 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.

6 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Checkpoint**
- **MITRE ATT&CK**

7 AUTORES

- **Leonardo Oliveira**
- **Ismael Rocha**

heimdall
security research
A DIVISION OF ISH