BOLETIM DE SEGURANÇA

Grupo Kinsing intensifica operações de criptojacking, explorando novas vulnerabilidades

heimdall
security research
A DIVISION OF ISH

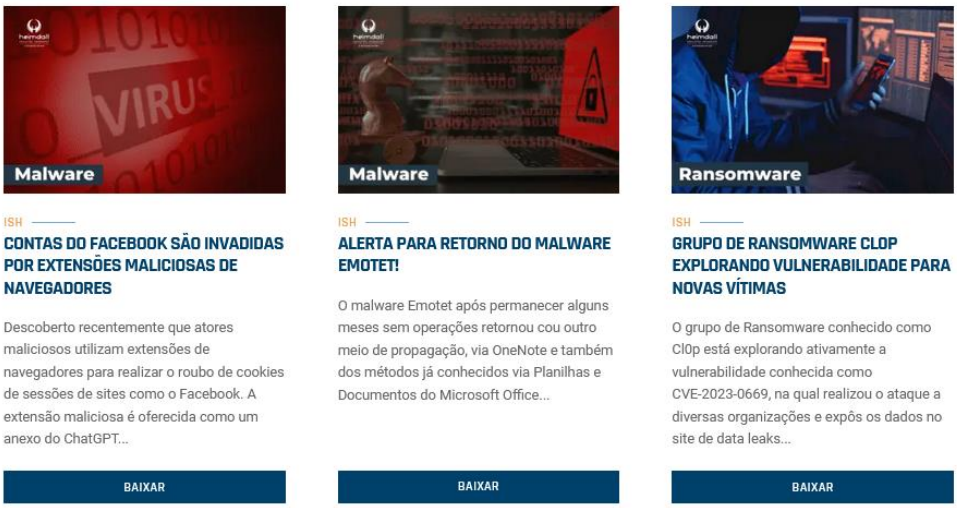
TLP: CLEAR

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

1 Sumário Executivo 6
2 Informação sobre a ameaça 7
3 Recomendações 10
4 Indicadores de Compromissos 11
5 Referências 12
6 Autores 13

LISTA DE TABELAS

Tabela 1 – Indicadores de Compromissos de artefatos. 11
Tabela 2 – Indicadores de Compromissos de Rede. 11

LISTA DE FIGURAS

Figura 1 – Campanha openfire de Kinsing. *7*

Figura 2 – Tabela de vulnerabilidades exploradas pelo agente de ameaça. *9*

1 SUMÁRIO EXECUTIVO

Pesquisadores da Aqua Security informaram que o grupo Kinsing, especializado em cryptojacking, tem mostrado uma habilidade notável para se adaptar e evoluir. Eles têm sido uma ameaça constante, incorporando novas vulnerabilidades divulgadas ao seu conjunto de ferramentas de ataque de forma ágil, o que lhes permite expandir sua rede de bots maliciosos.

2 INFORMAÇÃO SOBRE A AMEAÇA

Kinsing refere-se tanto ao malware quanto ao agente de ameaça, como sugerem alguns artigos. A arquitetura do agente de ameaça é complexa e tem sido ativa desde 2019. Durante esse tempo, diversos relatórios detalhando suas ações foram publicados, incluindo análises detalhadas de ataques específicos e ferramentas, bem como relatórios abrangentes que interligam múltiplos ataques.

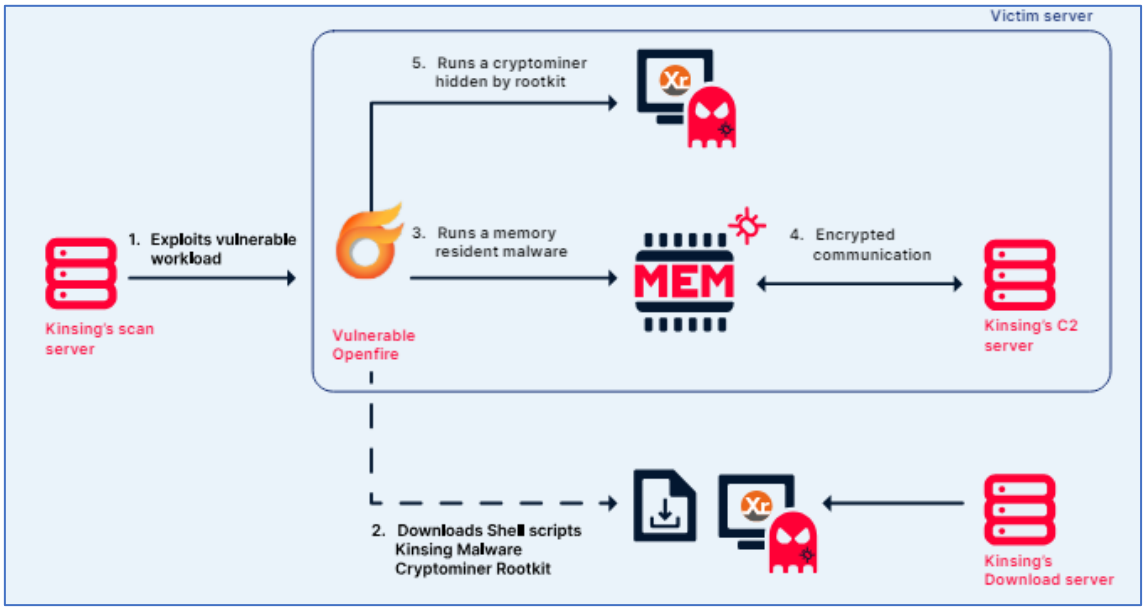


Figura 1 – Campanha openfire de Kinsing.

As campanhas do Kinsing são compostas pela varredura e exploração de servidores, sendo este o servidor inicial tem a função de detectar e explorar vulnerabilidades. Ele possui capacidades avançadas de varredura, provavelmente utilizando ferramentas como o masscan, e pode ter acesso a bancos de dados de servidores como Zoomeye ou Shodan. Embora o malware tenha capacidades de masscan, não há provas concretas de que o ator de ameaças o utilize ativamente. Servidores de download que funcionam como intermediários para o download de binários e scripts. Por exemplo, o ator de ameaças usa um endereço IP para baixar o payload principal, um script que, em seguida, obtém o malware Kinsing e, ocasionalmente, um rootkit. De outro servidor, o malware Kinsing baixa um minerador de criptomoeda Monero. Servidores de comando e controle (C2), que trata-se do último elemento, o servidor C2, gerencia a comunicação com servidores comprometidos. Após a implantação, o malware Kinsing se conecta a esses servidores. Historicamente, de abril de 2019 a agosto de 2020, o ator de ameaças se comunicava diretamente usando um endereço IP. No entanto, de agosto de 2020 a outubro de 2020, o operador do Kinsing começou a usar o site vocaltube.ru para interações C2.

Ao analisar as campanhas observou-se as tendências variadas de ataques. Alguns honeypots sofreram dezenas de ataques diários. Em média, os honeypots foram alvo do Kinsing oito vezes por dia, com o número de ataques variando de três a cinquenta. Por exemplo, o honeypot de API Docker mal configurado enfrentou uma média de cinquenta ataques diários, oscilando de centenas a vários por dia. Esse padrão foi consistente com outros honeypots. Esses ataques variaram entre tipos específicos de software, sugerindo que o ator de ameaça do Kinsing está constantemente mudando de alvos, focando em aplicações específicas em diferentes momentos. Quando novas vulnerabilidades são divulgadas, elas naturalmente se tornam uma prioridade, mas também podem receber mais atenção meses depois. Em uma pesquisa, revelou-se 2,5 milhões de instâncias das várias aplicações visadas, indicando que a operação de varredura do ator está sondando milhões de instâncias. A pesquisa indicou que o a ameaça incorpora novas vulnerabilidades assim que são divulgadas. Em setembro de 2021, a CyberArk publicou “Kinsing: O Malware com Duas Faces”, um excelente blog que analisa o binário do Kinsing e o compara com outra família de malware: NSPPS.

Outro aspecto notável das campanhas dos agentes da ameaça é que 91% dos aplicativos visados são de código aberto, com o grupo destacando principalmente aplicativos em tempo de execução (67%), bancos de dados (9%) e infraestrutura em nuvem (8).

Em uma investigação detalhada dos artefatos cibernéticos identificou-se três grupos principais de programas maliciosos, os scripts de Acesso Inicial (Tipo I e II), que são utilizados logo após a invasão inicial, esses scripts servem para descarregar componentes avançados de ataque, eliminar rivais, desativar defesas como firewalls, finalizar ferramentas de segurança (SELinux, AppArmor, Aliyun Aegis) e instalar rootkits para esconder atividades mal-intencionadas. Os scripts auxiliares que são empregados para explorar vulnerabilidades e garantir o acesso inicial, desabilitar componentes de segurança específicos em serviços de nuvem (Alibaba Cloud, Tencent Cloud), abrir um shell reverso para comunicação com o servidor do atacante e recuperar cargas úteis de mineração e por fim, os binários de Segundo Estágio: Incluem o malware Kinsing e um cripto-minerador para Monero, com funções de monitoramento do processo de mineração, compartilhamento do PID com o servidor C2, realização de testes de conectividade e envio de resultados de execução.

O Kinsing tem como alvo sistemas Linux e Windows, muitas vezes explorando vulnerabilidades em aplicativos da web ou configurações incorretas, como API Docker e Kubernetes para executar criptomineradores.

Vulnerability	Description
Misconfigured Remote Docker API	Docker APIs that are open to the Internet with weak password or without authentication
Misconfigured Redis Server	Redis server with weak password or without password protection
CVE-2020-25213	WordPress File Manager Plugin RCE
CVE-2020-23814	XXL-JOB RCE
CVE-2020-11651 and CVE-2020-11652	SaltStack RCE
CVE-2019-3396	Atlassian Confluence Widget Connector Macro Velocity Template Injection
CVE-2019-0193	RCE via DataImportHandler
CVE-2018-20062	NoneCMS ThinkPHP RCE
CVE-2017-15718	Apache Hadoop YARN NodeManager vulnerability
CVE-2017-11610	Supervisord RCE
CVE-2017-9841	PHPUnit RCE

Figura 2 – Tabela de vulnerabilidades exploradas pelo agente de ameaça.

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:

Atualize regularmente

- Mantenha todos os sistemas e softwares atualizados, especialmente aqueles conhecidos por serem alvos do Kinsing.

Patches de segurança

- Aplique imediatamente patches de segurança para vulnerabilidades críticas, que o Kinsing tem explorado ativamente.

Monitoramento contínuo

- Monitore constantemente os sistemas para detectar atividades suspeitas e vulnerabilidades não corrigidas.

Segurança de contêineres

- Configure corretamente os ambientes em contêineres para evitar a exploração por malware.

Ferramentas de segurança

- Utilize e mantenha ferramentas de segurança atualizadas, como firewalls, antivírus e sistemas de detecção de intrusão.

Backup e recuperação

- Implemente uma estratégia robusta de backup e recuperação para mitigar os danos em caso de comprometimento.

Isolamento de rede

- Isolar sistemas críticos e segmentar redes para limitar o movimento lateral de ameaças.

Análise de comportamento

- Implemente soluções de análise de comportamento para identificar padrões anormais que possam indicar uma infecção.

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:	b3039abf2ad5202f4a9363b418002351
sha1:	0ceb8ffb0be23b808b534d744440f4367e17b9c5
sha256:	787e2c94e6d9ce5ec01f5cbe9ee2518431eca8523155526d6dc85934c9c5787c
File name:	kinsing

Indicadores de compromisso do artefato	
md5:	2c44b4e4706b8bd95d1866d7867efa0e
sha1:	e545ceffc8948e3ca9900212807cf3a862d33581
sha256:	5d2530b809fd069f97b30a5938d471dd2145341b5793a70656aad6045445cf6d
File name:	write.dev-52.inode-2580630.pid-2948

Tabela 1 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
IP	194.38.22.53 194.38.21.25 45.15.158.124 194.87.252.159 194.38.21.37 185.17.0.226 194.38.20.196 45.138.157.202 194.38.20.27 194.38.20.32 194.38.20.11 93.185.166.75 194.38.20.225 185.209.29.94 194.40.243.205 194.40.243.206

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**
- **AquaSecurity**
- **Thehackernews**
- **Nautilus-aqua-IOCs**

6 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH