BOLETIM DE SEGURANÇA

Malware Hadooken tendo como alvo servidores Weblogic com fragilidades

heimdall
security research
A DIVISION OF ISH

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall

ISH

CONTAS DO FACEBOOK SÃO INVADIDAS POR EXTENSÕES MALICIOSAS DE NAVEGADORES

Descoberto recentemente que atores maliciosos utilizam extensões de navegadores para realizar o roubo de cookies de sessões de sites como o Facebook. A extensão maliciosa é oferecida como um anexo do ChatGPT...

BAIXAR

ISH

ALERTA PARA RETORNO DO MALWARE EMOTET!

O malware Emotet após permanecer alguns meses sem operações retornou cou outro meio de propagação, via OneNote e também dos métodos já conhecidos via Planilhas e Documentos do Microsoft Office...

BAIXAR

ISH

GRUPO DE RANSOMWARE CLOP EXPLORANDO VULNERABILIDADE PARA NOVAS VÍTIMAS

O grupo de Ransomware conhecido como Cl0p está explorando ativamente a vulnerabilidade conhecida como CVE-2023-0669, na qual realizou o ataque a diversas organizações e expôs os dados no site de data leaks...

BAIXAR

Sumário

1 Sumário Executivo 6
2 Cadeia de ataque observada 7
3 Servidores WebLogic expostos 8
4 MITRE ATT&CK - TTPs 9
5 Recomendações 10
6 Indicadores de Compromissos 12
7 Referências 13
8 Autores 14

Lista de Tabelas

Tabela 1 – Tabela MITRE ATT&CK. 9
Tabela 2 – Indicadores de Compromissos de artefatos. 12
Tabela 3 – Indicadores de Compromissos de Rede. 12

Lista de Figuras

Figura 1 – Cadeia de ataque observada. 7
Figura 2 – Mapa de calor para servidores WebLogic expostos na Internet-Fofa.info. 8

1 SUMÁRIO EXECUTIVO

Pesquisadores de segurança descobriram um novo malware direcionado a servidores **WebLogic** em sistemas Linux. A carga principal do malware se autodenomina **Hadooken**, uma referência ao golpe "surge fist" da famosa série Street Fighter. Após ser executado, o Hadooken ativa outro malware chamado Tsunami e instala um criptominerador. O WebLogic Server é um servidor de aplicativos Java EE desenvolvido pela Oracle, amplamente utilizado para criar, implementar e gerenciar aplicações distribuídas em grande escala. Ele é popular em setores como o bancário, e-commerce e outros negócios críticos devido ao seu suporte às tecnologias Java, gerenciamento de transações e capacidade de escalabilidade.

2 CADEIA DE ATAQUE OBSERVADA

As explorações têm como alvo o WebLogic, aproveitando falhas de desserialização, controles de acesso inadequados e principalmente configurações incorretas, como credenciais fracas ou consoles de administração expostos.

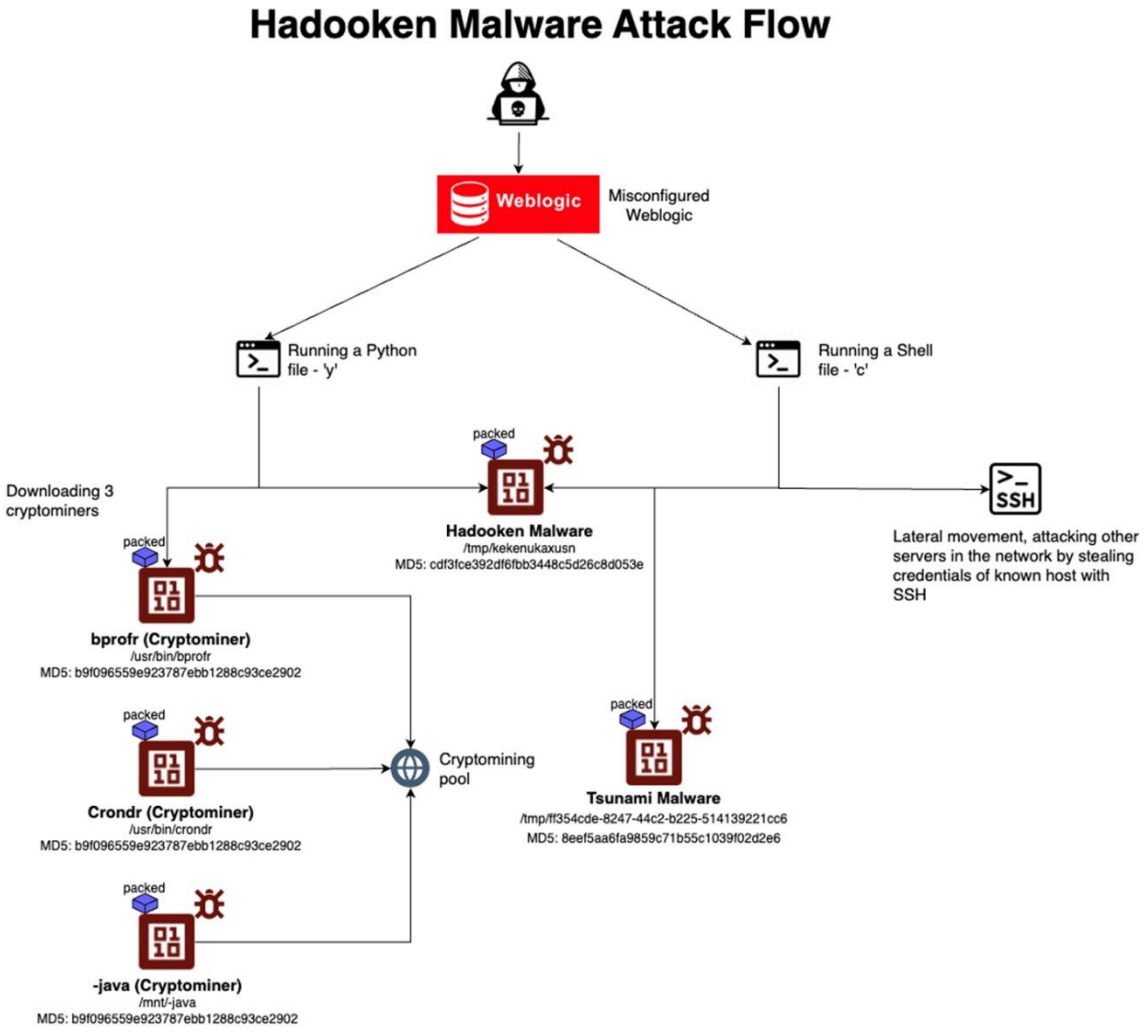

Figura 1 – Cadeia de ataque observada.

O fluxo de ataque do malware Hadooken começa com a exploração de um Weblogic mal configurado. O atacante pode executar um arquivo Python usando a flag -y ou um arquivo Shell com a flag -c. Após isso, o malware Hadooken é baixado e executado. Em seguida, ele baixa três cryptominers: bprofr, Crondr, e java, que são utilizados para minerar criptomoedas. Esses cryptominers estão localizados em diretórios como /usr/bin e /mnt/java, e possuem hashes MD5 específicos. Além disso, o Hadooken facilita a movimentação lateral na rede, roubando credenciais SSH de outros servidores. O Tsunami Malware também é baixado para contribuir na mineração em pools, visando maximizar a exploração de recursos das máquinas comprometidas.

3 SERVIDORES WEBLOGIC EXPOSTOS

Servidores WebLogic expostos na Internet representam um alto risco de segurança, especialmente quando possuem vulnerabilidades críticas não corrigidas ou configurações de segurança fracas. O Oracle WebLogic é frequentemente alvo de ataques devido às suas funcionalidades amplas e ao fato de ser utilizado para rodar aplicativos empresariais críticos. Em buscas por servidores WebLogic expostos na Internet, observa-se uma grande quantidade distribuída por vários países, sendo o Brasil um dos que apresentam uma quantidade significativa, conforme ilustrado na imagem abaixo.

Figura 2 – Mapa de calor para servidores WebLogic expostos na Internet-Fofa.info.

4 MITRE ATT&CK - TTPs

Tática	Técnica	Detalhes
Initial Access	T1190 Exploit Public-Facing Application	Explora servidores WebLogic vulneráveis aproveitando credenciais fracas para obter acesso.
Execution	T1059.001 Command and Scripting Interpreter – Unix Shell T1059.004 Command and Scripting Interpreter – Python T1059.006 Command and Scripting Interpreter – PowerShell	O uso de script de shell (`c`) para execução maliciosa. O uso do script Python (`y`) para execução maliciosa. script PowerShell `b.ps1` usado para distribuir malware.
Persistence	T1053.003 Scheduled Task/Job: Cron	Uso de tarefas cron para manter a persistência executando cargas maliciosas periodicamente.
Defense Evasion	T1070.004 Indicator Removal: File Deletion T1036.004 Masquerading: Masquerade Task or Service T1027 Obfuscated Files or Information	Uso de nomes conhecidos como -java, -bash. Uso de cargas úteis codificadas em base64 para evitar detecção. Exclusão de logs após a execução de atividades maliciosas.
Credential Access	T1110.002 Brute Force: Password Cracking	O acesso inicial é obtido por meio de força bruta bem-sucedida no painel de administração do Weblogic.
Lateral Movement	T1563.001 Remote Service Session Hijacking: SSH Hijacking	Iteração sobre chaves SSH para movimentação lateral pela rede.
Impact	T1496 Resource Hijacking T1486 Data Encrypted for Impact	Execução de um criptominerador como parte do malware Hadooken. Uso potencial de ransomware como RHOMBUS e NoEscape em versões futuras do ataque.

Tabela 1 – Tabela MITRE ATT&CK.

5 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 e patches

- Aplique imediatamente patches de segurança fornecidos pela Oracle para o WebLogic para vulnerabilidades conhecidas. Assegure-se de que todas as correções críticas de segurança estejam instaladas.
- Implemente um processo de gerenciamento de patches regular, garantindo que novos patches sejam aplicados assim que liberados.

Reforço de configurações de segurança do WebLogic

- Desative funções não utilizadas ou serviços que podem aumentar a superfície de ataque, como serviços de administração remota e consoles administrativos acessíveis publicamente.
- Habilite o SSL/TLS para todas as comunicações para proteger dados transmitidos e evitar que ataques interceptem ou modifiquem informações sensíveis.
- Limite o acesso ao Console Administrativo, configurando regras de firewall e utilizando uma lista branca para garantir que apenas endereços IP confiáveis possam acessar a interface de administração.

Firewall e IPS/IDS

- Configure regras de firewall rigorosas para restringir o acesso a portas e serviços desnecessários. Restrinja o acesso ao console de administração do WebLogic a uma rede interna ou VPN segura.
- Implemente sistemas de detecção/prevenção de intrusões (IDS/IPS) para monitorar e bloquear tentativas de exploração de vulnerabilidades conhecidas no WebLogic.

Monitoramento de anomalias

- Habilite o monitoramento de logs do WebLogic para detectar atividades suspeitas ou anômalas, como tentativas de execução de código remoto.
- Use soluções SIEM (Security Information and Event Management) para correlacionar logs e detectar padrões de ataque, especialmente os relacionados à exploração de vulnerabilidades conhecidas.
- Monitore o uso de CPU e rede. O malware Hadooken é frequentemente usado para mineração de criptomoedas, então um aumento inesperado no uso de CPU pode ser um sinal de comprometimento.

Controle de acesso e autenticação

- Implemente autenticação multifator (MFA) para todos os acessos administrativos ao WebLogic.
- Utilize senhas fortes e únicas para todas as contas administrativas e usuários do sistema WebLogic.
- Revise e minimize os privilégios de contas administrativas, garantindo que os usuários tenham o mínimo de permissões necessárias.

Backup e recuperação

- Garanta que backups regulares e offline dos servidores WebLogic sejam feitos, permitindo a recuperação rápida em caso de um ataque bem-sucedido.
- Teste a restauração de backups periodicamente para assegurar que são funcionais e abrangem todos os dados críticos.

Segregação de redes

- Implemente a segmentação de rede para isolar servidores WebLogic de outras partes da rede, limitando o movimento lateral caso haja comprometimento.

Testes de penetração (Pentest)

- Faça testes de penetração simulando ataques conhecidos, especialmente aqueles que envolvem vulnerabilidades que o Hadooken pode explorar, para identificar possíveis lacunas de segurança.

Malware defense

- Utilize soluções de EDR (Endpoint Detection and Response) e antivírus para detectar e responder rapidamente a tentativas de instalação do malware, como o Hadooken.
- Implemente listas de bloqueio (blacklists) de IPs maliciosos que tentam explorar servidores WebLogic, baseando-se em feeds de Threat Intelligence.

6 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:	cdf3fce392df6fbb3448c5d26c8d053e
sha1:	4a3dc35d4853665d4d08f0c5220e650f28eb9c06
sha256:	652f25d8f197ad00e4a64d1ad4066778e1bbc9a0e29faf09b90768c84f89c4ee
File name:	hadooken

Indicadores de compromisso do artefato	
md5:	4a12098c3799ce17d6d59df86ed1a5b6
sha1:	0e8a3699cfaa236b73fd5aab51649c296bc8f001
sha256:	89e16174f65709fecd11c620d57abdab53046734d5105bedce8bc357513dd64b
File name:	h2-mod.exe

Indicadores de compromisso do artefato	
md5:	b9f096559e923787ebb1288c93ce2902
sha1:	94851bcc8f9c651bcda0ff33d17356cb0b16cf12
sha256:	1fcc2061f767574044ca1e97f92ca1d44ee0b35e0a796e3bd6a949ad4b1175e5
File name:	-java

Indicadores de compromisso do artefato	
md5:	9bea7389b633c331e706995ed4b3999c
sha1:	b2d07deea8da1bf44f5103a8858c7f7000309130
sha256:	33926b0dfc908b518213d7608f701beca2373adad1f40025c17028cac5d4837f
File name:	java.bin

Indicadores de compromisso do artefato	
md5:	8eef5aa6fa9859c71b55c1039f02d2e6
sha1:	8fcbf737766a473e2f033b9ee161fcf837228da3
sha256:	10c2913361debb5f1db95c170ce2d6892d598d97b9f1f7f76a8bc7b5053e801a
File name:	4ed09844-484e-445e-9648-cf668bc13cba

Tabela 2 – Indicadores de Compromissos de artefatos

Indicadores de IPs

Indicadores de IPs	
IP	185.174[.]136[.]204

Tabela 3 – 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.

7 REFERÊNCIAS

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

8 AUTORES

- **Ismael Pereira Rocha**

heimdall
security research
A DIVISION OF ISH