BOLETIM DE SEGURANÇA

Ransomware Cerber explorando falha em Confluence para ataques direcionados

heimdall
security research
A DIVISION OF ISH

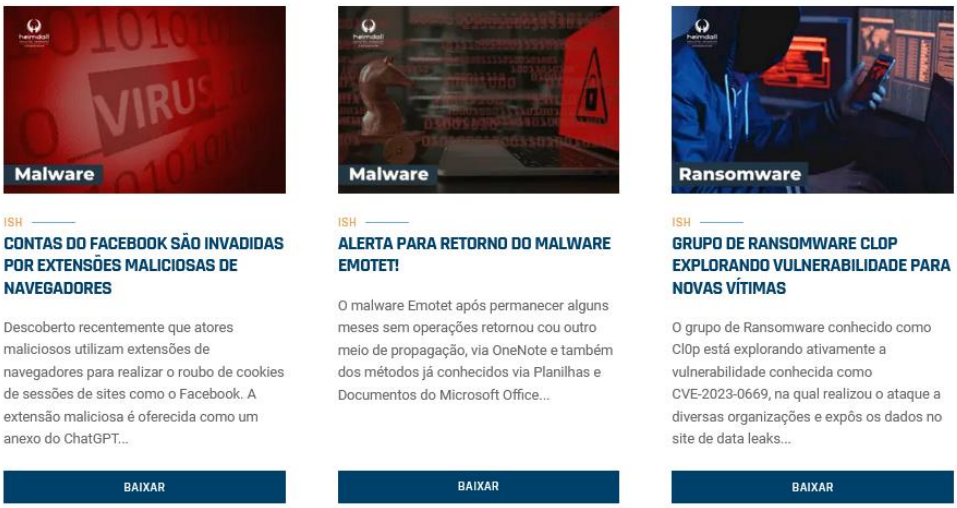
TLP: CLEAR

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 Cado Security informou em um relatório sobre a vulnerabilidade CVE-2023-22518 considerada como crítica, em que agentes de ameaças estão implantando uma variante Linux do ransomware Cerber (também conhecido como C3RB3R) em servidores que executam o aplicativo Atlassian Confluence não corrigidos.

2 DETALHES SOBRE A AMEAÇA

O Ransomware Cerber, que teve seu pico de atividades em 2016, segue ativo por meio de ações esporádicas, tendo como alvo recente uma falha de segurança no Confluence. Sua estrutura é composta por três cargas úteis em C++, que são fortemente ofuscadas e compiladas no formato ELF de 64 bits, um padrão para executáveis no sistema Linux, e são comprimidas utilizando o UPX, que é um compactador amplamente adotado por atores de ameaças, pois codifica o código do programa dentro do arquivo binário. Durante a execução, o código é descomprimido diretamente na memória, o que dificulta a detecção do código malicioso por programas de segurança. No ambiente Linux, a utilização de C++ como linguagem para desenvolvimento de cargas úteis está em declínio, sendo substituída por linguagens modernas como Rust e Go, preferidas por agentes de ameaças atuais. A carga útil do Cerber, lançada há aproximadamente 8 anos, é consideravelmente mais antiga que a maioria das ameaças monitoradas. Apesar de ter sido atualizada ao longo do tempo, é provável que mantenha suas ferramentas e linguagem originais durante seu ciclo de vida.

Foi detectado que a implementação do ransomware em sistemas que foram comprometidos através dessa exploração em instâncias do Confluence. Esta vulnerabilidade recente possibilita ao invasor reiniciar o aplicativo Confluence e estabelecer uma conta de administrador nova por meio de um ponto de extremidade de restauração de configuração que não possui proteção adequada, normalmente utilizado pelo assistente de configuração.

```
[19/Mar/2024:15:57:24 +0000] - http-nio-8090-exec-10 13.40.171.234 POST /json/setup-restore.action?synchronous=true HTTP/1.1 302 81796ms - - python-requests/2.31.0

[19/Mar/2024:15:57:24 +0000] - http-nio-8090-exec-3 13.40.171.234 GET /json/setup-restore-progress.action?taskId= HTTP/1.1 200 108ms 283 - python-requests/2.31.0
```

Figura 1 – Log do servidor web.

Uma vez estabelecida uma conta administrativa, ela habilita a execução de código através do carregamento e instalação de um módulo nocivo pelo painel administrativo. Especificamente, o plugin Effluence web shell é implementado, proporcionando uma interface web para a execução de comandos arbitrários no servidor. O atacante emprega o web shell para iniciar e rodar a carga inicial do malware Cerber. Normalmente, o Confluence opera sob o usuário "confluence", que possui direitos limitados. Portanto, o ransomware só pode criptografar arquivos que pertencem a este usuário. Isso inclui o banco de dados do Confluence, que contém dados valiosos. Caso o ransomware operasse sob um usuário com maiores privilégios, teria a capacidade de criptografar uma gama maior de arquivos, visando todos os arquivos acessíveis no sistema.

A principal carga útil é condensada utilizando UPX, a exemplo das cargas subsequentes. Seu propósito essencial é preparar o ambiente operacional e obter cargas adicionais para sua ativação. Uma vez executado, o programa realiza sua auto-descompactação e busca estabelecer um arquivo em **/var/lock/0init-ld.lo**. Presume-se que sua função seja atuar como um mecanismo de bloqueio para prevenir execuções repetidas do ransomware. Contudo, na presença prévia do arquivo de bloqueio, o processo é ignorado e a execução prossegue sem alterações.

Após estabelecer conexão com o servidor C2 (inativo) no endereço 45[.]145[.]6[.]112, o programa procede para baixar a carga secundária, um verificador de log chamado agttydck. Isso é feito através de uma requisição GET simples ao caminho /agttydcki64 no servidor via HTTP, salvando o conteúdo recebido no arquivo /tmp/agttydck.bat. Posteriormente, este arquivo é executado, tendo como parâmetros /tmp e ck.log. Os detalhes sobre a execução deste payload serão abordados na seção seguinte.

Uma vez finalizada a execução da carga secundária, a carga primária inspeciona a existência do arquivo de log /tmp/ck.log que foi criado. Caso confirmada, ela remove tanto o próprio arquivo quanto o agttydcki64 do sistema. Continuando ativa na memória, procede com o download da carga de criptografia, conhecida como agttydcb, armazenando-a em /tmp/agttydcb.bat. A natureza desta carga é intrincada, sendo identificada pelo comando file como um executável DOS, apesar de sua extensão bat e da ausência dos bytes mágicos esperados, além de uma entropia elevada que indica possível codificação ou criptografia. A carga primária então lê e reescreve um arquivo ELF decodificado no mesmo local, substituindo o anterior. O processo exato de decodificação do agttydcb não é claro. Após a decodificação, a carga primária executa o agttydcb, e os pormenores de seu funcionamento serão explicados posteriormente.

```
2283  openat(AT_FDCWD, "/tmp/agttydcb.bat", O_RDWR) = 4

…

2283  read(4, "\353[\254R\333\372\22,\1\251\f\235
'A>\234\33\25E3g\335\0252\344vBg\177\356\321"..., 450560) = 450560

…

2283  lseek(4, 0, SEEK_SET)             = 0

2283  write(4, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\2\0>\0\1\0\0\0X\334F\0\0\0\0\0"..., 450560)
= 450560

…

2283  close(4)                          = 0
```

Figura 2 – Saída truncada para o processo de decodificação.

O **agttydck**, que atua como verificador de log, aparentemente funciona a princípio como um controlador de acesso. Apresentando-se como uma carga útil de análise estática direta, mesmo com a presença de ofuscação. Assim como outras cargas, está compactada via UPX. Sua execução envolve a junção dos argumentos recebidos, separados por barras, para formar um caminho de arquivo completo. Por exemplo, ao receber **/tmp e ck.log**, ele forma o caminho **/tmp/ck.log**. O programa tenta então abrir o arquivo especificado para escrita, em caso de êxito, registra a palavra "success" e emite o código de retorno 0. Caso contrário, retorna o código 1.

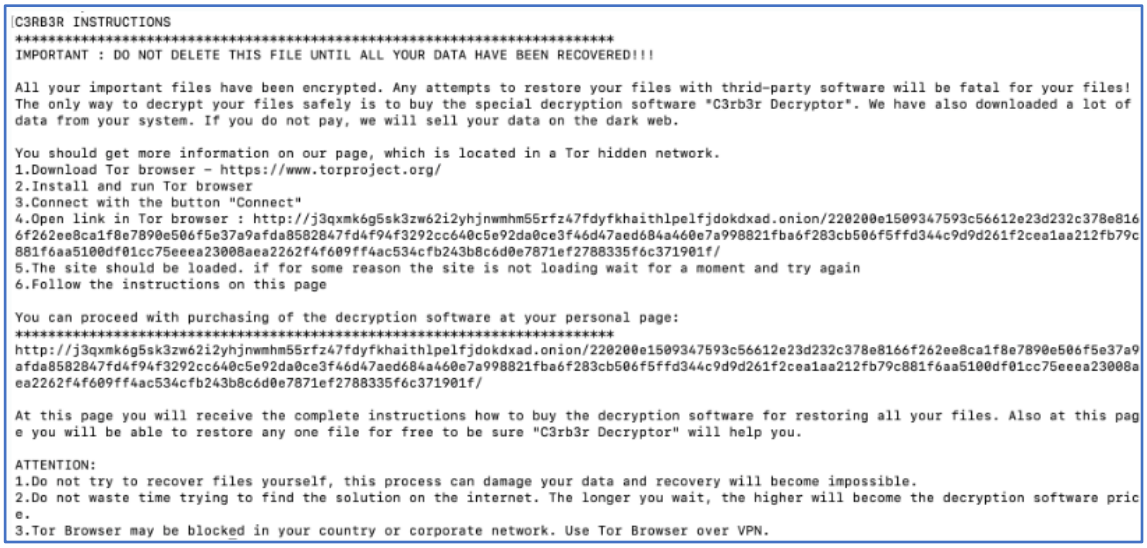
```
file_out = likely_open_file(combined_string, "w");
v8 = file_out;
if ( file_out )
{
  likely_write("success", 1LL, 7LL, file_out);
  likely_close(v8);
}
```

Figura 3 – Rotina limpa que escreve a frase de sucesso.

A finalidade específica deste teste permanece incerta. Uma possibilidade é que ele serve para testar a capacidade de escrita no diretório tmp, o que seria útil para determinar se o sistema possui restrições excessivas que poderiam impedir a operação de um encriptador. Considerando que o teste ocorre em um processo distinto da carga principal, outra hipótese é que ele visa identificar sandboxes que falham na manipulação adequada de arquivos, o que poderia resultar na não detecção, pela carga principal, do arquivo gerado pelo processo filho.

O encriptador agttydcb cumpre a função típica de um ransomware, que consiste em criptografar dados no sistema de arquivos do alvo. Assim como outras ferramentas mal-intencionadas, esta ameaça é compactada utilizando UPX e desenvolvido em C++ com técnicas de ofuscação avançadas. Quando ativado, o programa se autodestrói do disco para evitar deixar rastros. Inicialmente, ele cria um arquivo vazio chamado **/tmp/log.0**. Posteriormente, após concluir o processo de criptografia, o segundo arquivo vazio, **/tmp/log.1**, é gerado, sugerindo que possam ser vestígios de depuração acidentalmente esquecidos pelo atacante.

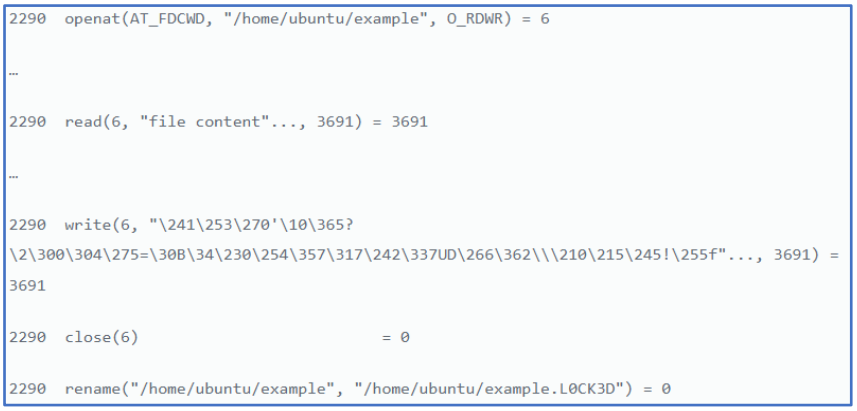
Para realizar a criptografia propriamente dita, o malware lança uma nova thread. Ele tenta criar um arquivo de texto com instruções para resgate, nomeado **/<directory>/read-me3.txt**. Caso obtenha êxito, o programa procede para criptografar todos os arquivos encontrados nesse diretório. Se não for possível, ele prossegue para o próximo diretório disponível. A seleção dos diretórios a serem criptografados é feita através de uma varredura sistemática do sistema de arquivos, começando por diretórios como **/usr** seguido por **/var**, entre outros.



```
C3RB3R INSTRUCTIONS
*************************************************************************
IMPORTANT : DO NOT DELETE THIS FILE UNTIL ALL YOUR DATA HAVE BEEN RECOVERED!!!

All your important files have been encrypted. Any attempts to restore your files with thrid-party software will be fatal for your files!
The only way to decrypt your files safely is to buy the special decryption software "C3rb3r Decryptor". We have also downloaded a lot of
data from your system. If you do not pay, we will sell your data on the dark web.

You should get more information on our page, which is located in a Tor hidden network.
1.Download Tor browser - https://www.torproject.org/
2.Install and run Tor browser
3.Connect with the button "Connect"
4.Open link in Tor browser : http://j3qxmk6g5sk3zw62i2yhjnwmhm55rfz47fdyfkhaithlpelfjdokdxad.onion/220200e1509347593c56612e23d232c378e816
6f262ee8ca1f8e7890e506f5e37a9afda8582847fd4f94f3292cc640c5e92da0ce3f46d47aed684a460e7a998821fba6f283cb506f5ffd344c9d9d261f2cea1aa212fb79c
881f6aa5100df01cc75eeea23008aea2262f4f609ff4ac534cfb243b8c6d0e7871ef2788335f6c371901f/
5.The site should be loaded. if for some reason the site is not loading wait for a moment and try again
6.Follow the instructions on this page

You can proceed with purchasing of the decryption software at your personal page:
*************************************************************************
http://j3qxmk6g5sk3zw62i2yhjnwmhm55rfz47fdyfkhaithlpelfjdokdxad.onion/220200e1509347593c56612e23d232c378e8166f262ee8ca1f8e7890e506f5e37a9
afda8582847fd4f94f3292cc640c5e92da0ce3f46d47aed684a460e7a998821fba6f283cb506f5ffd344c9d9d261f2cea1aa212fb79c881f6aa5100df01cc75eeea23008a
ea2262f4f609ff4ac534cfb243b8c6d0e7871ef2788335f6c371901f/

At this page you will receive the complete instructions how to buy the decryption software for restoring all your files. Also at this pag
e you will be able to restore any one file for free to be sure "C3rb3r Decryptor" will help you.

ATTENTION:
1.Do not try to recover files yourself, this process can damage your data and recovery will become impossible.
2.Do not waste time trying to find the solution on the internet. The longer you wait, the higher will become the decryption software pric
e.
3.Tor Browser may be blocked in your country or corporate network. Use Tor Browser over VPN.
```

Figura 4 – A nota de resgate do Cerber.

Ao localizar um arquivo alvo, o ransomware inicia um processo de leitura e escrita, carregando completamente o conteúdo do arquivo. O próximo passo é a criptografia do conteúdo na memória. Após a criptografia, o malware busca o início do arquivo para gravar os dados criptografados, substituindo o conteúdo original, o que resulta em um arquivo completamente inacessível. O arquivo é então renomeado, adicionando a extensão .L0CK3D ao seu nome. A estratégia de sobrescrever o arquivo existente, em vez de criar um novo e excluir o antigo, é particularmente eficaz no Linux, onde os diretórios podem ser configurados para permitir apenas adições, impedindo a remoção de arquivos. Além disso, essa técnica de reescrita pode alterar os dados no armazenamento físico, dificultando ainda mais a recuperação dos dados, mesmo com técnicas de análise forense sofisticadas.



```
2290  openat(AT_FDCWD, "/home/ubuntu/example", O_RDWR) = 6

…

2290  read(6, "file content"..., 3691) = 3691

…

2290  write(6, "\241\253\270'\10\365?
\2\300\304\275=\30B\34\230\254\357\317\242\337UD\266\362\\\210\215\245!\255f"..., 3691) =
3691

2290  close(6)                          = 0

2290  rename("/home/ubuntu/example", "/home/ubuntu/example.L0CK3D") = 0
```

Figura 5 – Rastreamento do processo de criptografia.

Após a conclusão do processo, o programa tenta se autodestruir mais uma vez, o que é inútil pois já foi removido anteriormente. Então, ele procede para criar o arquivo **/tmp/log.1** e encerra suas operações de maneira padrão. Contrariando as afirmações da mensagem de resgate, que insinua a exfiltração dos arquivos e as análises realizadas não identificaram nenhuma ação que comprovasse essa atividade.

3 RECOMENDAÇÕES

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

A Atlassian recomenda que você corrija cada uma das instalações afetadas para uma das versões mais recente.

Produtos	Versões recentes
Confluence Data Center and Server	7.19.16 8.3.4 8.4.4 8.5.3 8.6.1

Tabela 1 – Versões recentes.

Caso não seja possível realizar a correção, pode-se aplicar mitigações temporárias como:

- Realizando backup de sua instância.

- Removendo sua instância da Internet até que você possa corrigir, se possível. As instâncias acessíveis à Internet pública, incluindo aquelas com autenticação de usuário, devem ter acesso restrito à rede externa até que você possa corrigir.

- Se você não puder restringir o acesso à rede externa ou corrigir, aplique as seguintes medidas provisórias para mitigar vetores de ataque conhecidos, bloqueando o acesso nos seguintes endpoints nas instâncias do Confluence:

1. /json/setup-restore.action
2. /json/setup-restore-local.action
3. /json/setup-restore-progress.action

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:	9e0a8f1097176a5215648b9376db6611
sha1:	f4384ca1c2250d58a17e692ce2a8efd7dcc97a73
sha256:	4ed46b98d047f5ed26553c6f4fded7209933ca9632b998d265870e3557a5cdfe
File name:	agae.6x

Indicadores de compromisso do artefato	
md5:	97785731629f12ebd8fff838b82386bb
sha1:	47c6fdf51760c13d2602909ddbbb84ef8e33f992
sha256:	1849bc76e4f9f09fc6c88d5de1a7cb304f9bc9d338f5a823b7431694457345bd
File name:	agttydcbi64

Indicadores de compromisso do artefato	
md5:	4688f4714c15bcce034cb40e2b9794d6
sha1:	8988ef7abd931496d7bbdf7db1a67c9def0641d9
sha256:	ce51278578b1a24c0fc5f8a739265e88f6f8b32632cf31bf7c142571eb22e243
File name:	agttdtck.bat

Tabela 2 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
IP	45[.]145[.]6[.]112

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.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Confluence**
- **Cadosecurity**
- **Thehackernews**
- **NVD**

heimdall
security research
A DIVISION OF ISH