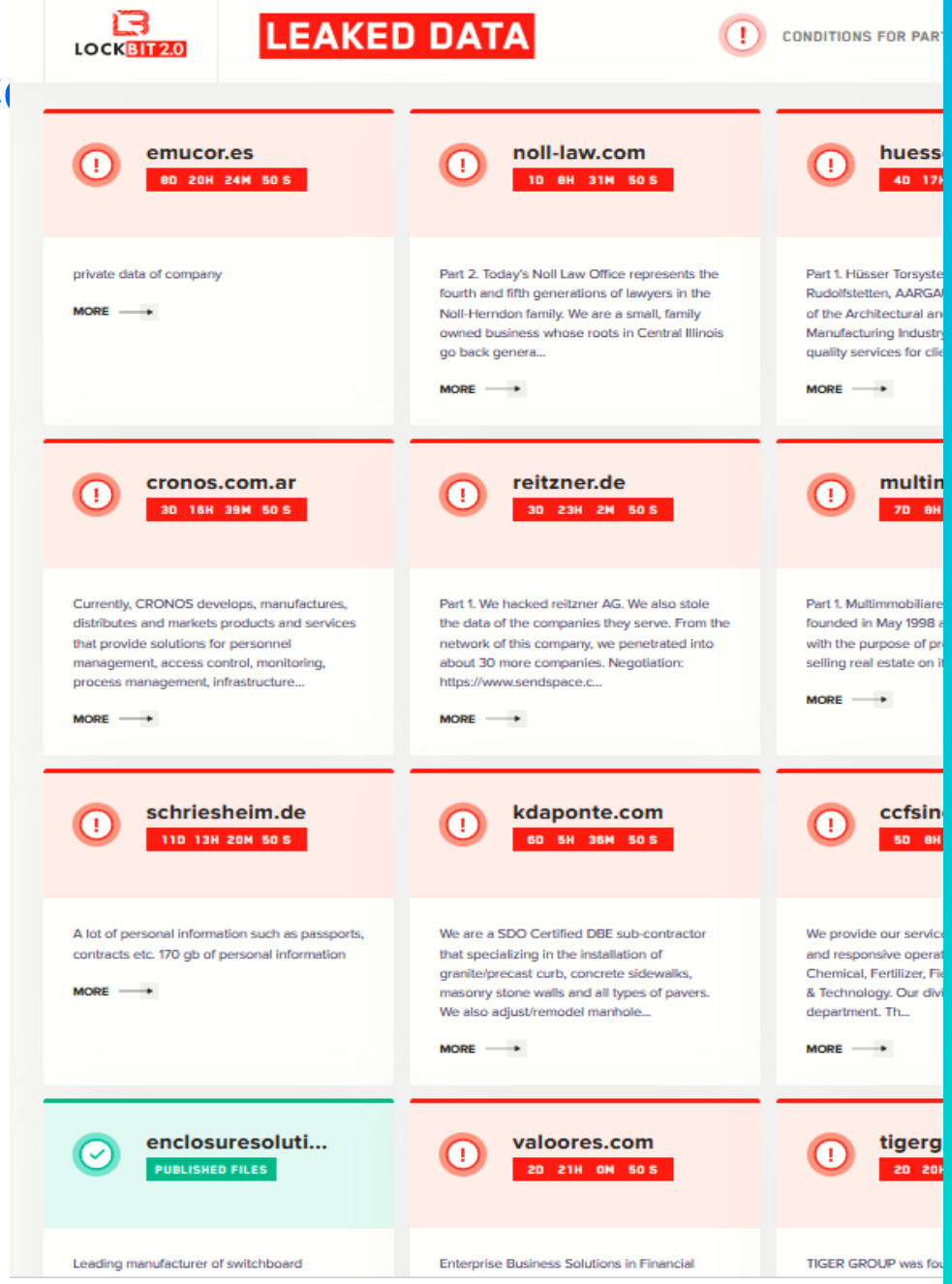
Casos de Ciberataques tipo Ransomware en Perú y medidas preventivas

Ing. César Farro
cesar.farro@telefonica.com
Área de Ciberseguridad

Parte 1: Casos y Vectores de Infección

Antecedentes:

- Por el Covid, se incrementó el uso de **conexiones remotas seguras VPN** SSL/TLS y VPN IPsec para la realización del Teletrabajo.
- Los atacantes de Ransomware se aprovechan de vulnerabilidades de los servicios públicos como **RDP, SMB, VPN Server**, etc.
- Los atacantes de Ransomware realizan **constantes scannings** y explotación para ingresar a los servicios públicos luego internamente realizar movimientos laterales para hackear el **Active Directory** y así apoderarse de toda la red.
- Las empresas en general **no tienen segmentación** de la red, procesos de actualización de parches de sistema operativo, procesos de gestión de vulnerabilidades, proceso de Backup/Restore y tampoco usan MFA para prevenir el robo y uso de una credencial válida.

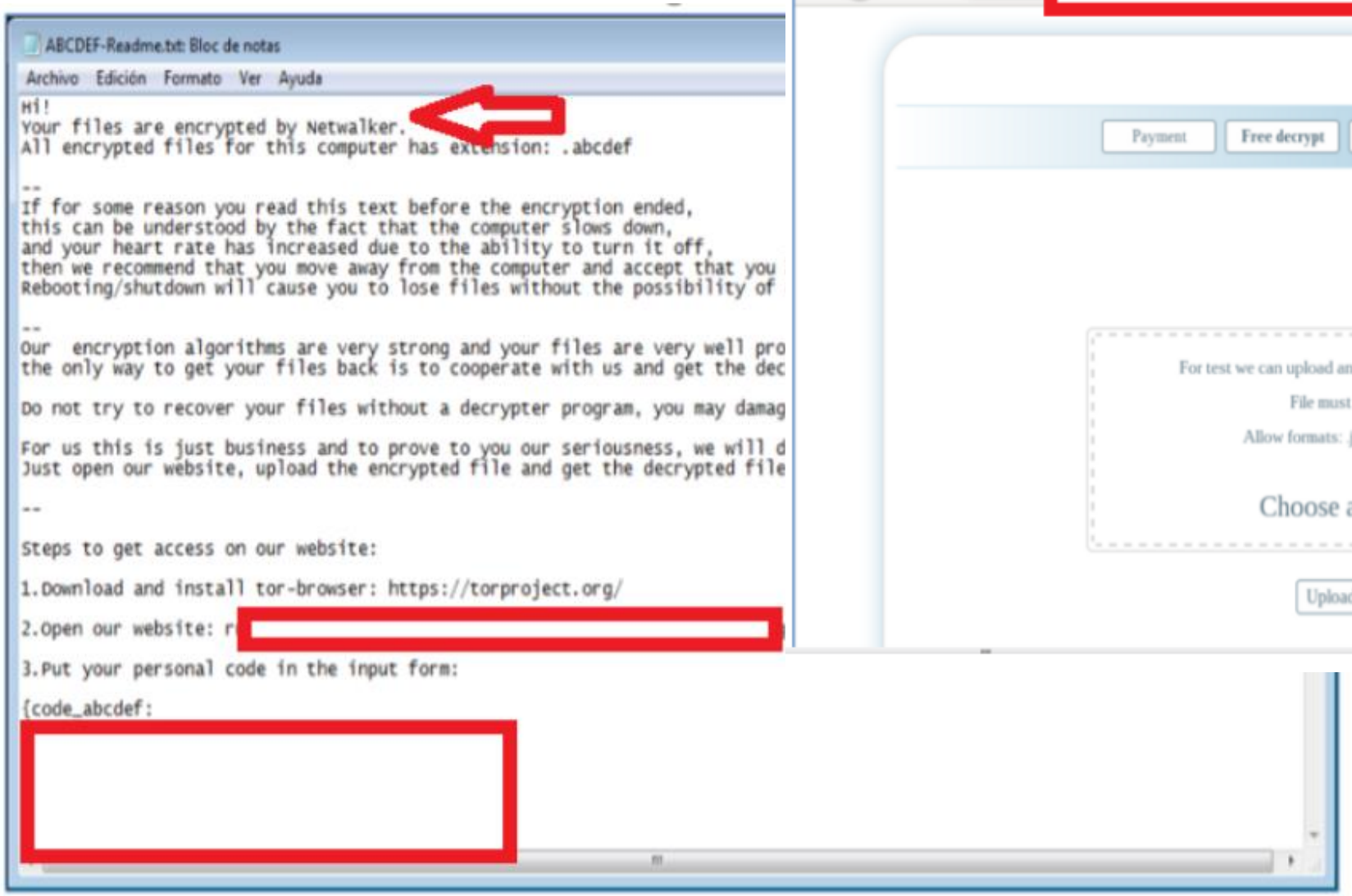


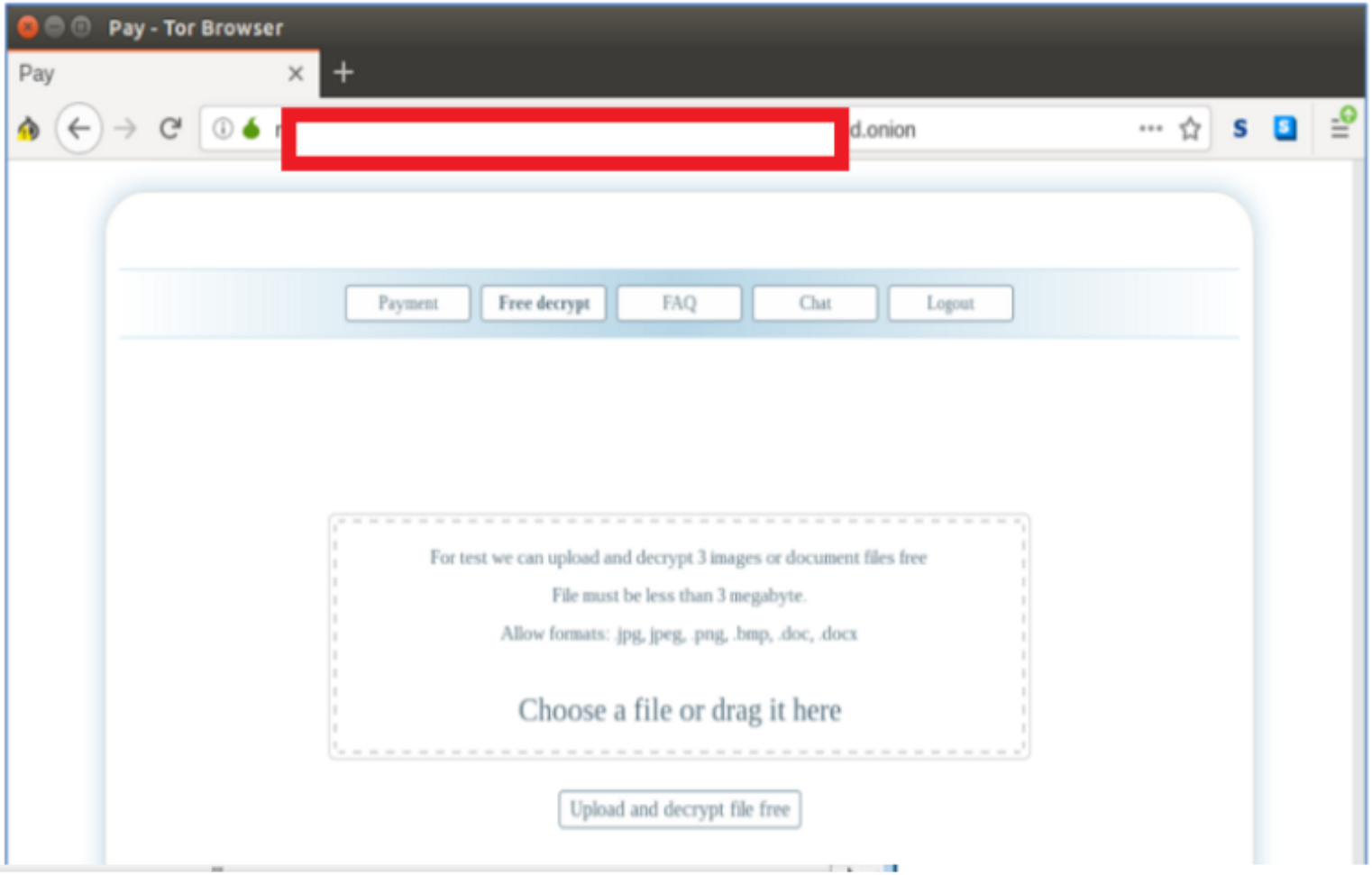
Telefónica Tech

Fuente:
Conti: https://continewsnv5otx5kaoje7krkto2qbu3gtqef22mnr7eaxw3y6ncz3ad.onion.ly/
Lockbit 2.0: http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion/

Ransomware Banjo

Ransomware Netwalker





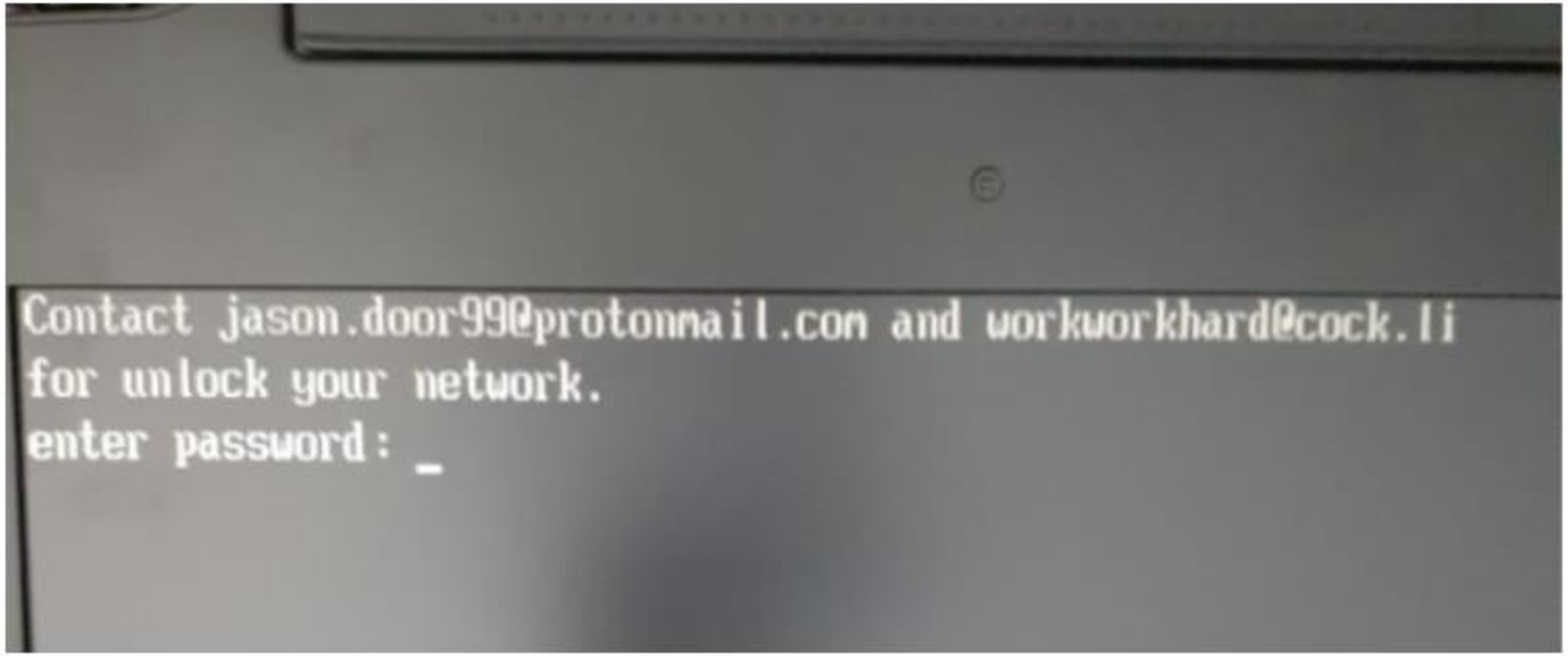
{XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

{XXXX==}

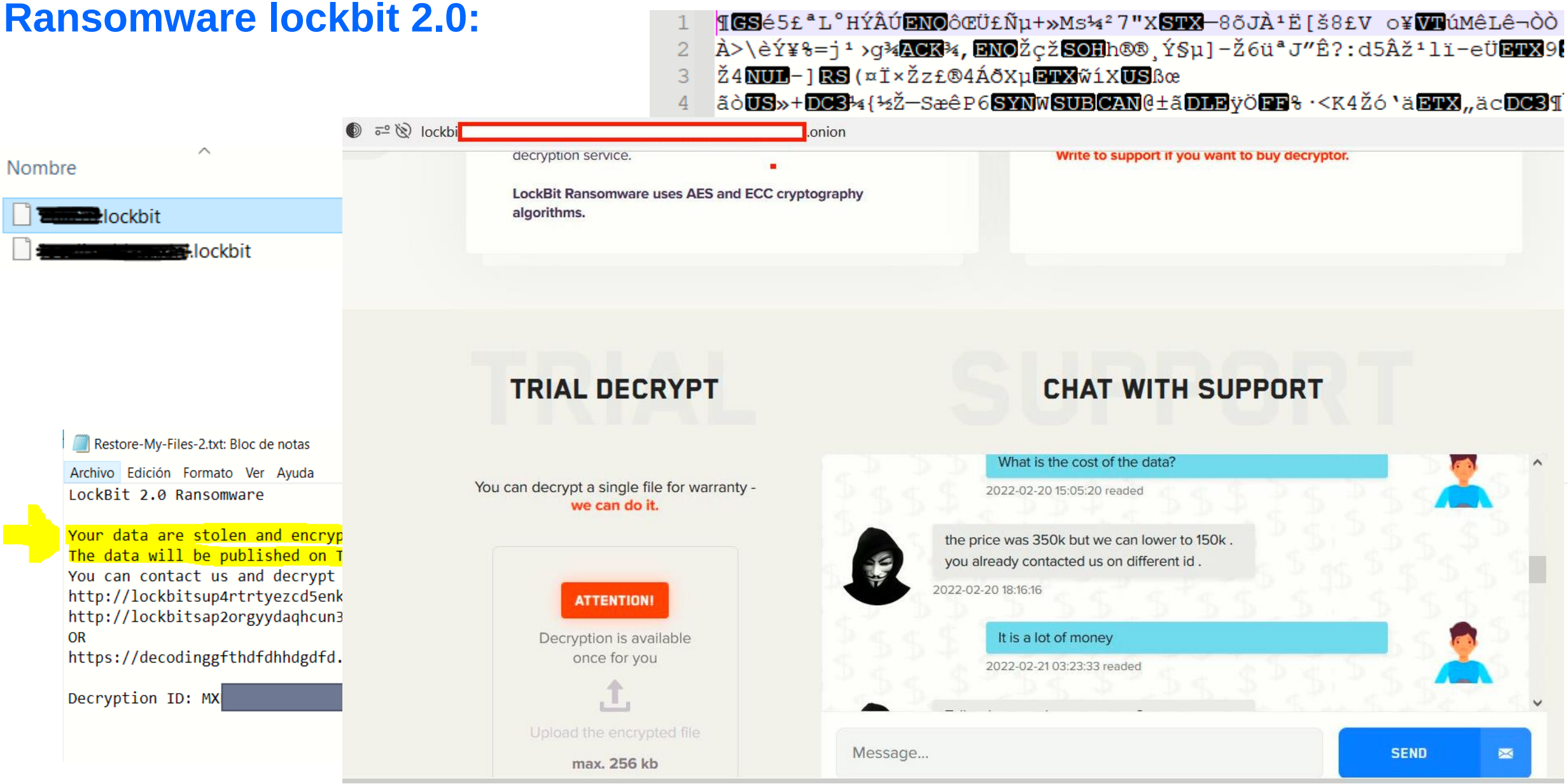
Ransomware Prometeus:

Afectación: Unidades de disco en grupos de servidores Microsoft Windows:

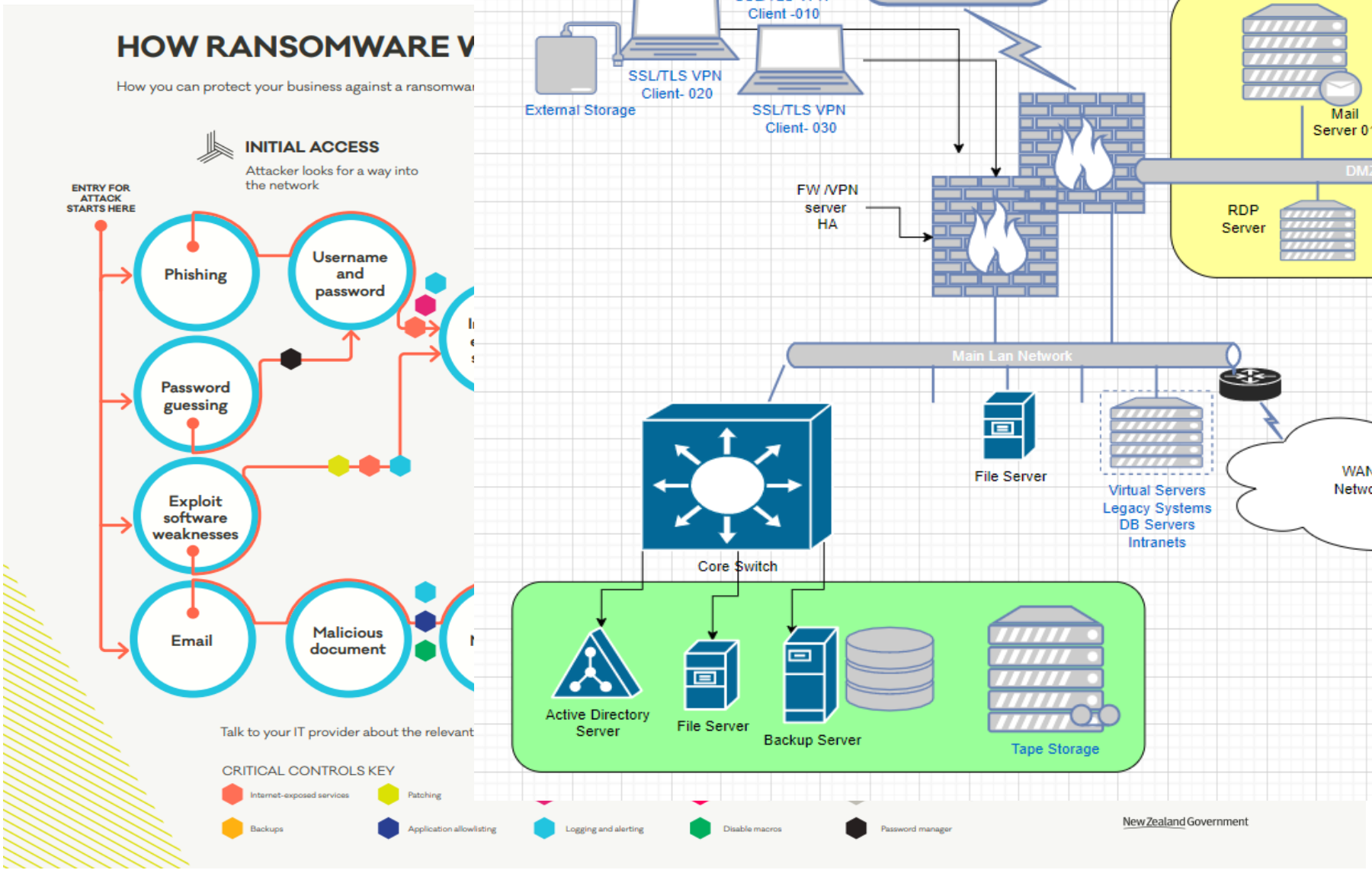
- **Grupo 1:** Los atacantes
  bitlocker, la cual pedía
- **Grupo 2:** Los atacantes
  instalaron diskcryptor y
  contacto: jason.door99



Ransomware lockbit 2.0:



Introducción, topo



Fuente:
https://www.cert.govt.nz/assets/ransomware/cert-lifecycle-of-a-ransomware-incident-with-controls-business-version.pdf

Vectores de Infección:

- **Servicios Vulnerables:**
  - ***Servicios públicos:***
    - Remote Desktop Protocol RDP 3389/tcp, Microsoft DS/SMB 445/tcp. Mysql 3306/tcp, Microsoft SQL Server 1433/tcp
  - ***Vulnerabilidades TODO:***
    - US Cert Vulnerabilidades + Exploited ++Usadas
  - ***VPN Server:***
    - VPN IPsec, IKE,500/udp, 4500/udp, https 443/tcp
  - ***Credenciales:***
    - Compra o Robo de credenciales de acceso remoto.

- **Ingeniería Social:**
  - A través de correo electrónico.
  - Enlaces dentro del correo.
  - Archivos adjuntos con malware.
  - Navegación a enlaces con malware.

Parte 2: Eventos y Vulnerabilidades

Eventos: Brute Force RDP, MS-SQL Server, SMB:

27/04/2018 21:34	Intrusion	Low	1000127	RDP Local Account Brute-force Attempt	185.156.177.4	200.1	RussianFederatio	200.1	Peru	RDP	TCP	Alert	ips_default	default
27/04/2018 21:37	Intrusion	Low	1000078	Microsoft SQL Server Authentication Brute-force Attempt	60.10.172.3	200.1	LangFang	200.1	Peru	MS_SQL9	TCP	Alert	ips_default	default
27/04/2018 21:40	Intrusion	Low	1000127	RDP Local Account Brute-force Attempt	185.156.177.4	200.1	RussianFederatio	200.1	Peru	RDP	TCP	Alert	ips_default	default
27/04/2018 21:41	Intrusion	Low	1000078	Microsoft SQL Server Authentication Brute-force Attempt	222.222.216.166	200.1	ShiJiaZhuang	200.1	Peru	MS_SQL9	TCP	Alert	ips_default	default
27/04/2018 21:43	Intrusion	Low	1000078	Microsoft SQL Server Authentication Brute-force Attempt	222.222.216.166	200.1	ShiJiaZhuang	200.1	Peru	MS_SQL9	TCP	Alert	ips_default	default
27/04/2018 21:46	Intrusion	Low	1000127	RDP Local Account Brute-force Attempt	185.156.177.4	200.1	RussianFederatio	200.1	Peru	RDP	TCP	Alert	ips_default	default
27/04/2018 21:51	Intrusion	Low	1000127	RDP Local Account Brute-force Attempt	185.156.177.4	200.1	RussianFederatio	200.1	Peru	RDP	TCP	Alert	ips_default	default
27/04/2018 21:57	Intrusion	Low	1000127	RDP Local Account Brute-force Attempt	185.156.177.4	200.1	RussianFederatio	200.1	Peru	RDP	TCP	Alert	ips_default	default
27/04/2018 22:03	Intrusion	Low	1000127	RDP Local Account Brute-force Attempt	185.156.177.4	200.1	RussianFederatio	200.1	Peru	RDP	TCP	Alert	ips_default	default
27/04/2018 22:09	Intrusion	Low	1000127	RDP Local Account Brute-force Attempt	185.156.177.4	200.1	RussianFederatio	200.1	Peru	RDP	TCP	Alert	ips_default	default
27/04/2018 22:14	Intrusion	Low	1000127	RDP Local Account Brute-force Attempt	185.156.177.4	200.1	RussianFederatio	200.1	Peru	RDP	TCP	Alert	ips_default	default

		RECEIVE TIME	TYPE	THREAT ID/NAME	FROM ZONE	TO ZONE	SOURCE ADDRESS	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION ADDRESS	DESTINA... DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION	ACTION	SEVERITY
		04/19 16:21:22	vulnerability	SMB: User Password Brute Force Attempt	RED_LAN	[redacted]	172.			172.			445	ms-ds-smbv3	alert	high
		04/18 16:38:31	vulnerability	SMB: User Password Brute Force Attempt	RED_LAN		172.			172.			445	ms-ds-smbv3	alert	high
		04/18 14:59:10	vulnerability	SMB: User Password Brute Force Attempt	RED_LAN		172.			172.			445	ms-ds-smbv3	alert	high
		04/18 14:59:04	vulnerability	SMB: User Password Brute Force Attempt	RED_LAN		172.			172.			445	ms-ds-smbv3	alert	high
		04/13 19:32:07	vulnerability	SMB: User Password Brute Force Attempt	RED_LAN		172.			172.			445	ms-ds-smbv3	alert	high
		04/13 18:39:28	vulnerability	SMB: User Password Brute Force Attempt	RED_LAN		172.			172.			445	ms-ds-smbv3	alert	high
		04/11 22:20:36	vulnerability	SMB: User Password Brute Force Attempt	RED_LAN		172.			172.			445	ms-ds-smbv3	alert	high

28/04/2018 04:21	Intrusion	Low	1000078	Microsoft SQL Server Authentication Brute-force Attempt	61.155.214.30	200.1	SuZhou(JiangSu)	200.1	Peru	MS_SQL9	TCP	Alert	ips_default	default
28/04/2018 04:23	Intrusion	Low	1000078	Microsoft SQL Server Authentication Brute-force Attempt	61.155.214.30	200.1	SuZhou(JiangSu)	200.1	Peru	MS_SQL9	TCP	Alert	ips_default	default
28/04/2018 05:26	Intrusion	Low	1000078	Microsoft SQL Server Authentication Brute-force Attempt	111.63.21.98	200.1	ChengDe	200.1	Peru	MS_SQL9	TCP	Alert	ips_default	default
28/04/2018 05:31	Intrusion	Low	1000078	Microsoft SQL Server Authentication Brute-force Attempt	182.254.157.192	200.1	ShangHai	200.1	Peru	MS_SQL9	TCP	Alert	ips_default	default
28/04/2018 06:37	Intrusion	Low	1000078	Microsoft SQL Server Authentication Brute-force Attempt	111.20.56.94	200.1	ShaanXi	200.1	Peru	MS_SQL9	TCP	Alert	ips_default	default
28/04/2018 07:01	Intrusion	Low	1000078	Microsoft SQL Server Authentication Brute-force Attempt	115.218.167.174	200.1	WenZhou	200.1	Peru	MS_SQL9	TCP	Alert	ips_default	default
28/04/2018 18:13	Intrusion	Low	370090	Microsoft IIS WebDAV ScStoragePathFromUrl Buffer Ove	194.72.112.130	200.1	UnitedKingdom	200.1	Peru	HTTP	TCP	Alert	ips_default	default
28/04/2018 18:13	Intrusion	Low	370091	Microsoft IIS WebDAV ScStoragePathFromUrl Buffer Ove	194.72.112.130	200.1	UnitedKingdom	200.1	Peru	HTTP	TCP	Alert	ips_default	default
28/04/2018 18:13	Intrusion	Low	403702	Oracle WebLogic Server WorkContextXmlInputAdapter In	194.72.112.130	200.1	UnitedKingdom	200.1	Peru	HTTP	TCP	Alert	ips_default	default

Vulnerabilidades:

cisa.gov/known-exploited-vulnerabilities-catalog

An official website of the United States government

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CYBERSECURITY

INFRASTR
SECURITY

KNOWN EXPLOITED VUL

Download CSV version

Download JSON version

Download JSON schema

Subscribe to the Known Exploited Vulnerabilit

Back to previous page for background on kno

CVE	Vendor/Project	Product	Vulnerability Name	Date Added to Catalog	Short Description	Action	Due Date	Notes
			"BlueKeep"		A remote code execution			

Table 1: Top 15 Routinely Exploited Vulnerabilities in 2021

CVE
CVE-2021-44228
CVE-2021-40539
CVE-2021-34523
CVE-2021-34473
CVE-2021-31207
CVE-2021-27065
CVE-2021-26858
CVE-2021-26857
CVE-2021-26855
CVE-2021-26084
CVE-2021-21972
CVE-2020-1472
CVE-2020-0688
CVE-2019-11510
CVE-2018-13379

- CVE-2021-22893
- CVE-2020-8260
- CVE-2020-8243
- CVE-2019-11539
- CVE-2019-11510

Pulse SecureVPN

- CVE-2020-8196
- CVE-2020-8195
- CVE-2019-19781
- CVE-2019-11634

Citrix

- CVE-2021-34523
- CVE-2021-34473
- CVE-2021-31207
- CVE-2021-26855

Microsoft Exchange

- CVE-2020-12812
- CVE-2019-5591
- CVE-2018-13379

Fortinet

- CVE-2021-20016
- CVE-2020-5135
- CVE-2019-7481

SonicWall

- CVE-2021-22986
- CVE-2020-5902

F5

- CVE-2020-2021
- CVE-2019-1579

Palo Alto

- CVE-2021-28799
- CVE-2020-36198

QNAP

- CVE-2020-12271

Sophos

- CVE-2019-0604

SharePoint

- CVE-2019-0708
- CVE-2020-1472
- CVE-2021-31166
- CVE-2021-36942

Microsoft Windows

- CVE-2017-0199
- CVE-2017-11882
- CVE-2021-40444

Microsoft Office

- CVE-2021-21985

vCenter

- CVE-2021-27101
- CVE-2021-27104
- CVE-2021-27102
- CVE-2021-27103

Accellion

- CVE-2021-20655

FileZen

- CVE-2021-26084

Atlassian

- CVE-2021-40539

Zoho Corp.

- CVE-2021-38647

Microsoft Azure

CVE-2018-13379		Fortinet FortiOS and FortiProxy	Path traversal

Telefónica Tech

Fuente: https://www.cisa.gov/kno

Puertos y Vulnerabilidades, candidatos

- Perú 3.2 Millones de Hosts:

RDP:
- 5,369 hosts, port 3389/tcp open, Remote Desktop Protocol

SMB:
- 3,022 hosts, port 445/tcp open, Microsoft-ds Data

Base de datos:
- 3,386 hosts, port 3306/tcp open, MySQL
- 4,206 hosts, port 1433/tcp open, Microsoft SQL Server

LDAP:
- 2,051 hosts, port 389/tcp open, LDAP
- 2,255 hosts, port 88/tcp open, Kerberos.

VMware:
- 1,902 hosts, port 903/tcp open, Remote Access to VM Console (TCP)

Notas:
-Scanning realizados entre ell 19 y 26 de abril 2022
-Fuente:Lacnic https://ftp.lacnic.net/pub/stats/lacnic/delegated-lacnic-extended-lates
-Fuente:masscan **https://github.com/robertdavidgraham/masscan**

Vulnerabilidad RDP: CVE-2019-0708 (1)
- 5,369 hosts, port 3389/tcp open
- 247/243 hosts vulnerable
- 2,966/2914 hosts safe
- 606/874 hosts unkonwn

Vulnerabilidad CVE-2018-13379 (2):
-9,822 hosts, port 10443/tcp open, 26abr22
-8,308 hosts, port 10443/tcp open, 28nov20
- 115 hosts vulnerable, 27abr20

Notas:
(1) CVE-2019-0708, realizado el 26 de abril 2020,
(1) RDPscan, https://github.com/robertdavidgraham/rdpscan
(2) CVE-2018-13379.

Puertos y Vulnerabilidades, candidatos

- Colombia 17.3 Millones de Hosts:

RDP:
- 12,948/13,194 hosts, port 3389/tcp open, Remote Desktop Protocol

SMB:
- 5,957 hosts, port 445/tcp open, Microsoft-ds Data

Base de datos:
- 5,543 hosts, port 3306/tcp open, MySQL
- 3,882 hosts, port 1433/tcp open, Microsoft SQL Server

LDAP:
- 2147 hosts, port 389/tcp open, LDAP
- 3036 hosts, port 88/tcp open, Kerberos.

VMware:
- 1329 hosts, port 903/tcp open, Remote Access to VM Console (TCP)

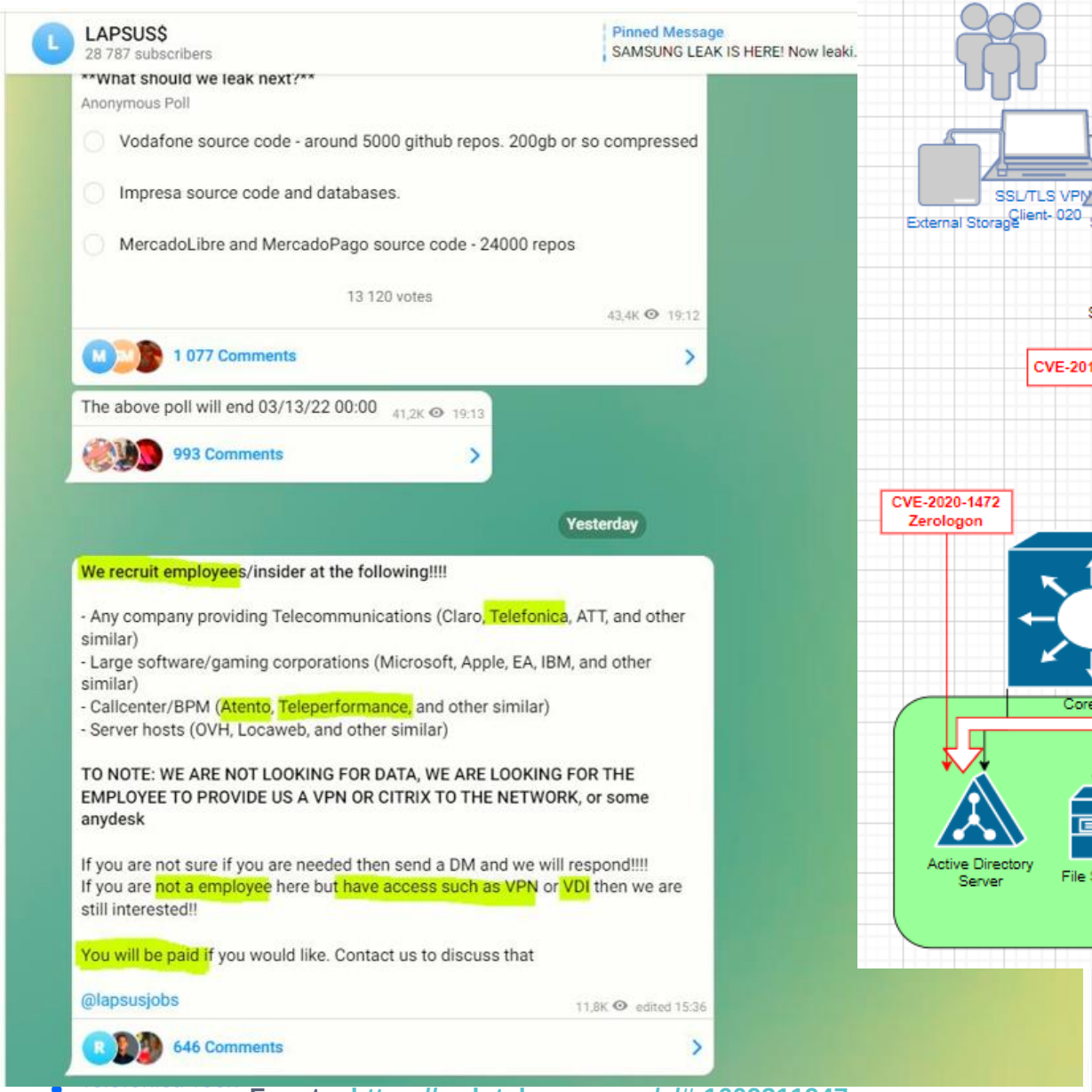
Notas:
-Scanning realizados entre ell 19 y 26 de abril 2022
-Fuente:Lacnic https://ftp.lacnic.net/pub/stats/lacnic/delegated-lacnic-extended-lates
-Fuente:masscan **https://github.com/robertdavidgraham/masscan**

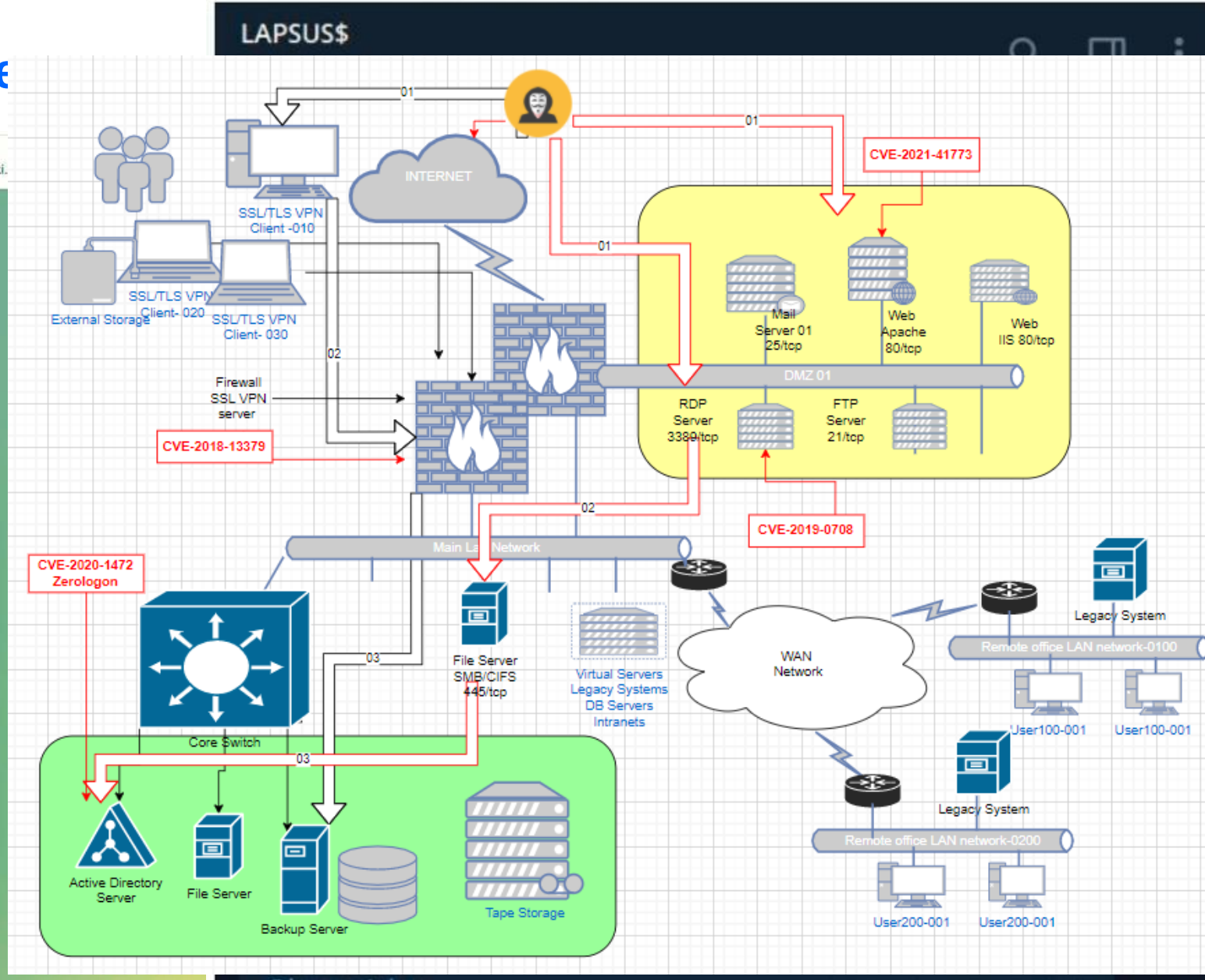
Vulnerabilidad RDP: CVE-2019-0708
- 13k hosts, port 3389/tcp open
- 697/616 hosts vulnerable
- 10k/9.2k hosts safe
- 2k/2.6k hosts unkonwn
- Fuente: rdpcan, manual 26abr22

Vulnerabilidad CVE-2018-13379:
-8,614 hosts, port 10443/tcp open,26abr22
-7,863 hosts, port 10443/tcp open,28nov20
- 120 hosts vulnerables

Notas:
(1) CVE-2019-0708, realizado el 26 de abril 2020,
(1) RDPscan, https://github.com/robertdavidgraham/rdpscan
(2) CVE-2018-13379.

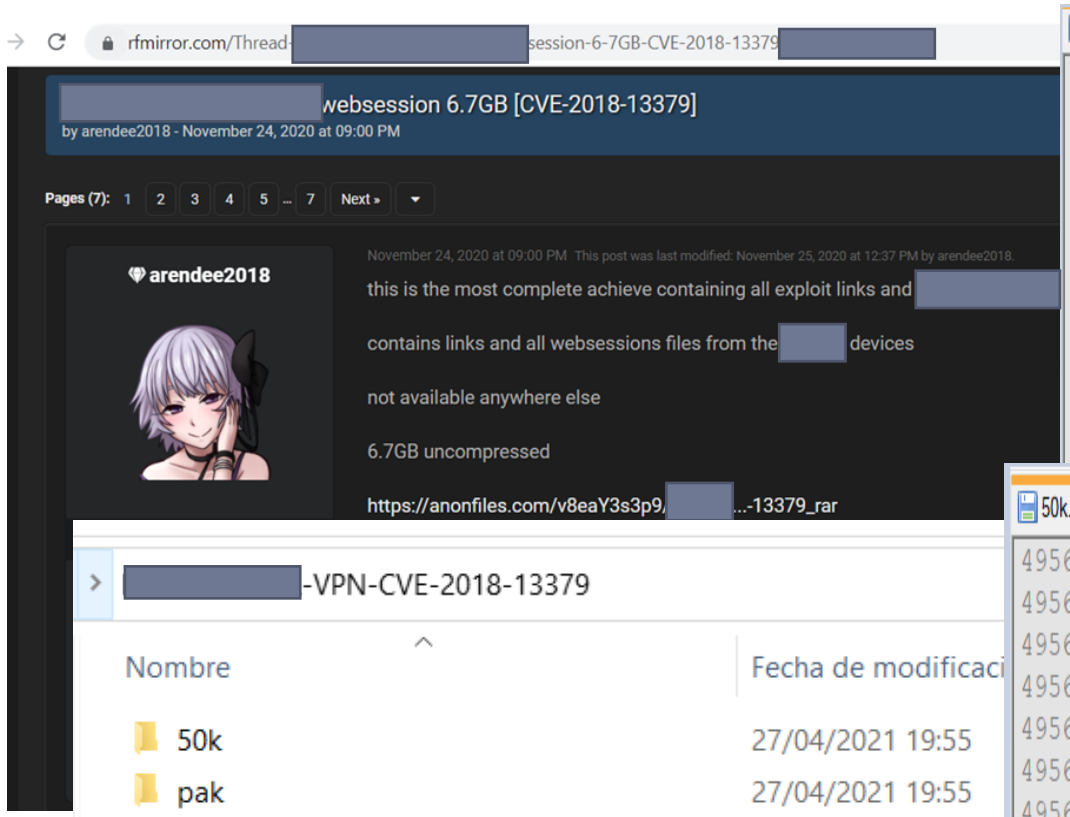
Robo o Compra de Credenciale

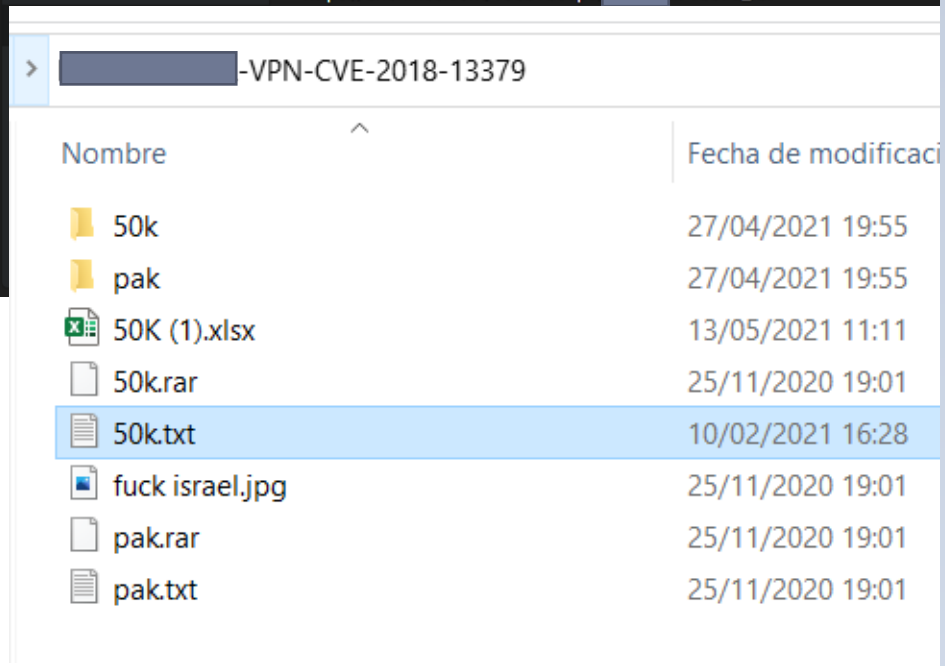


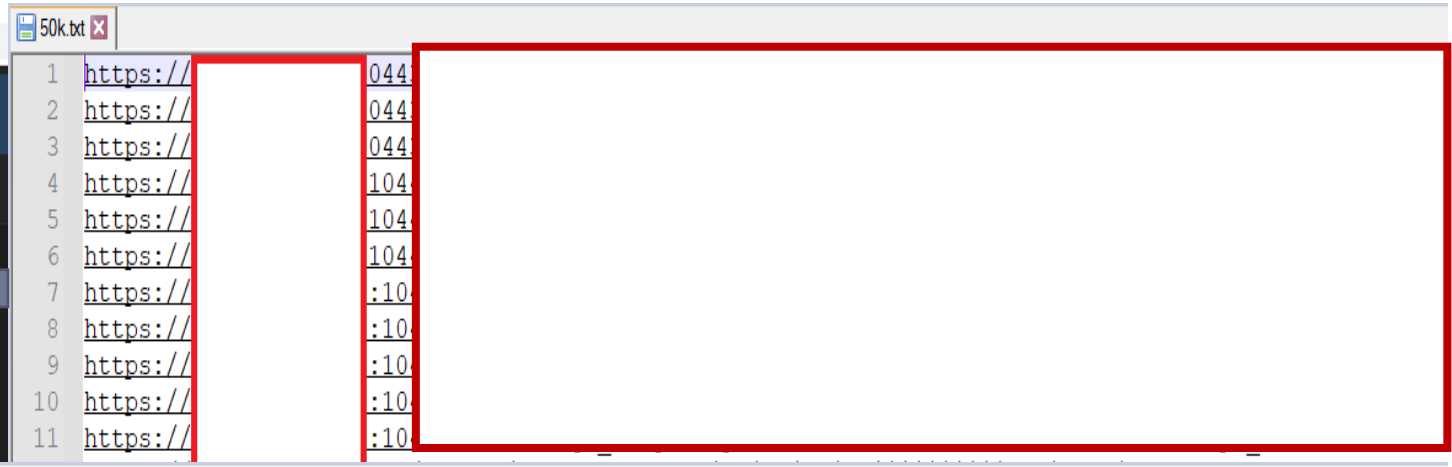


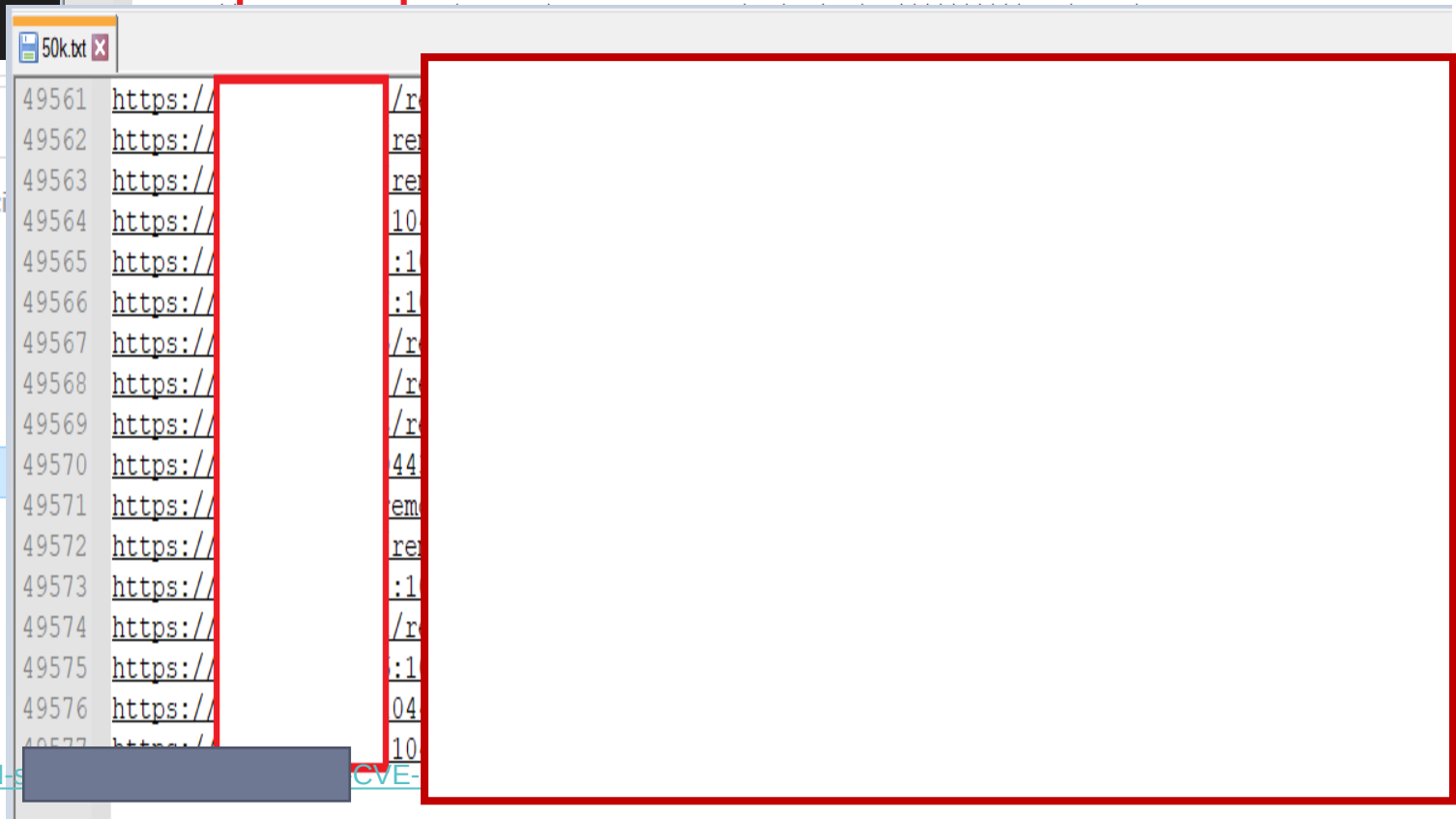
Fuente: https://web.telegram.org/z/#-1609311947

Vulnerabilidad CVE-2018-13379:







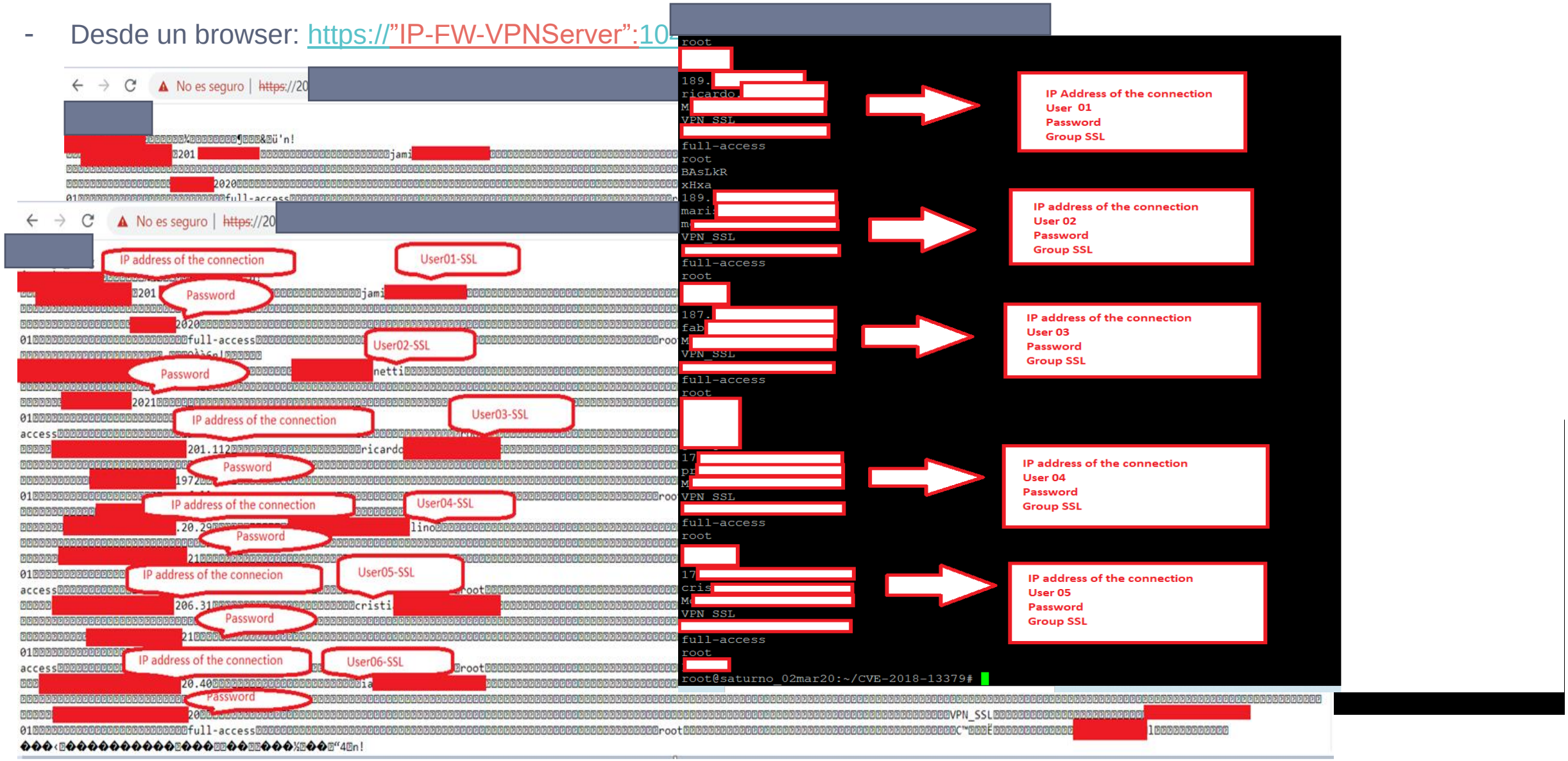


Telefónica Tech

Fuente: https://rfmirror.com/ -VPN- CVE-

Vulnerabilidad CVE-2018-13379:

- Desde un browser: https://"IP-FW-VPNServer":10[redacted]



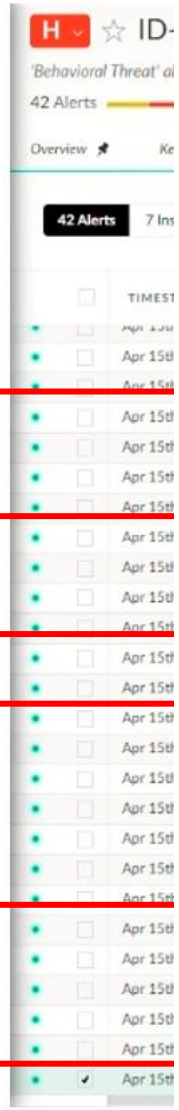
Fuente: https://rfmirror.com/[redacted]-6-7GB-CVE-2018-13379[redacted]

Vulnerabilidad CVE-2018-13379:

Fuente: Propia

Parte 3:
Detección y Respuesta:

Mimikatz:

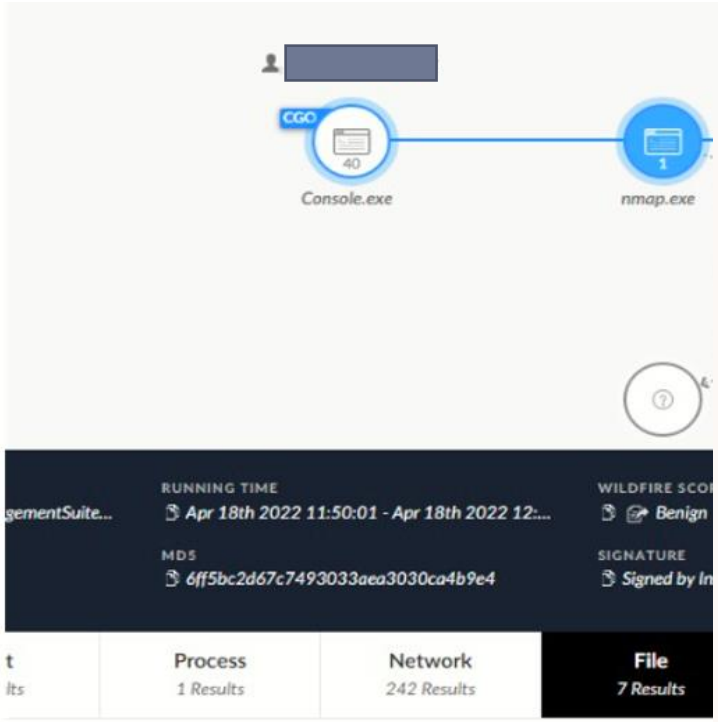


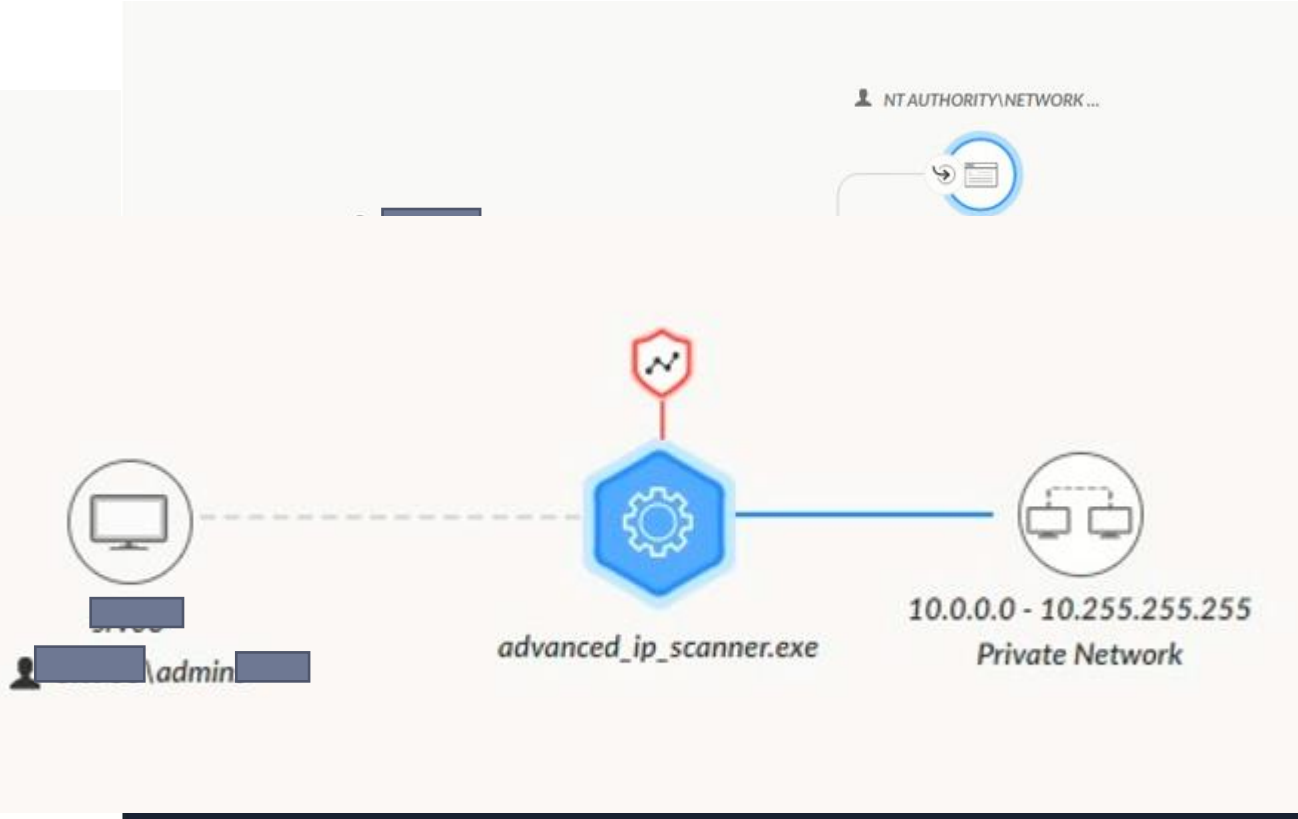
View children

Children Found 34 results

PROCESS START TIME	NAME	CMD	USERNAME
Apr 15th 2022	Taskmgr.exe	"C:\Windows\system32\taskmgr.exe" /4	\admi
Apr 15th 2022	fsquirt.exe	"C:\Windows\System32\fsquirt.exe" -Register	\admi
Apr 15th 2022	notepad.exe	"C:\Windows\system32\NOTEPAD.EXE" C:\Users\admins\Desktop\automim1\automim1\!logs\Passwords.txt	\admi
Apr 15th 2022	notepad.exe	"C:\Windows\system32\NOTEPAD.EXE" C:\Users\admins\Desktop\ArestorenNew\cepoass.txt	\admi
Apr 15th 2022	notepad.exe	"C:\Windows\system32\NOTEPAD.EXE" C:\Users\admins\Desktop\automim1\automim1\mimikatz\x64\mimikatz.log	\admi
Apr 15th 2022	runonce.exe	C:\Windows\SysWOW64\runonce.exe /Run6432	\admi
Apr 15th 2022	ie4uinit.exe	"C:\Windows\System32\ie4uinit.exe" -UserConfig	\admi
Apr 15th 2022	rundll32.exe	"C:\Windows\System32\rundll32.exe" "C:\Windows\System32\iesetup.dll",IEHardenAdmin	\admi
Apr 15th 2022	rundll32.exe	"C:\Windows\System32\rundll32.exe" "C:\Windows\System32\iesetup.dll",IEHardenUser	\admi
Apr 15th 2022	unregmp2.exe	"C:\Windows\System32\unregmp2.exe" /FirstLogon	\admi
Apr 15th 2022	unregmp2.exe	"C:\Windows\System32\unregmp2.exe" /FirstLogon	\admi

nmap, zenmap, ip_scanner:



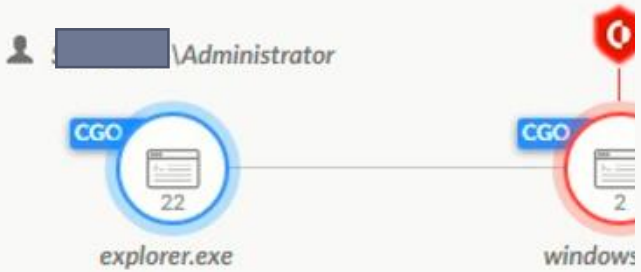


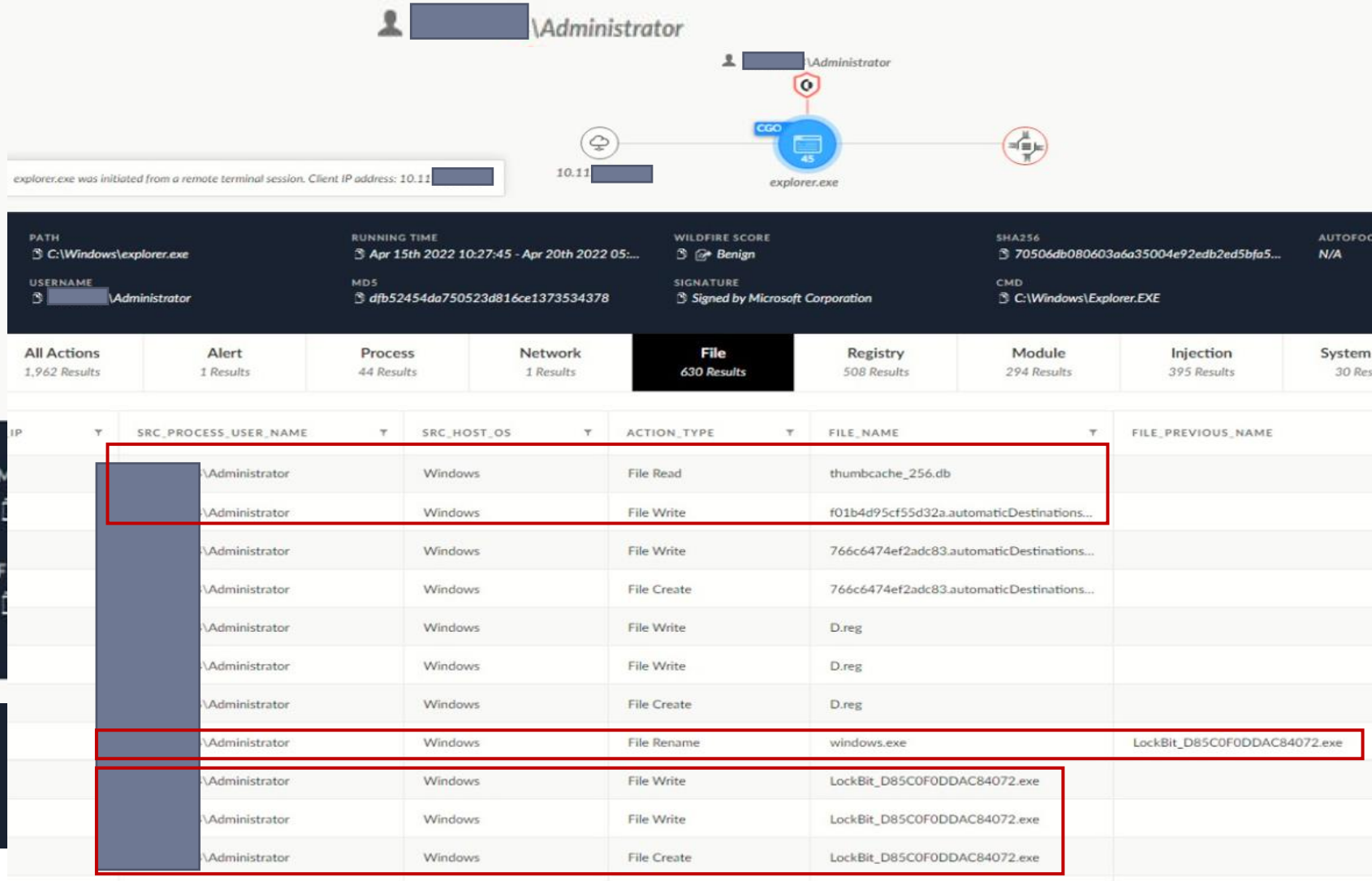
ACTI...	FILE_NAME	FILE_PREVIOUS_NAME	FILE_P
File Write	4xvlzsbd.xml		C:\Use
File Read	nmap-payloads		D:\Pro
File Read	hosts		C:\Wi
File Read	script.db		D:\Pro
File Read	nmap-services		D:\Pro

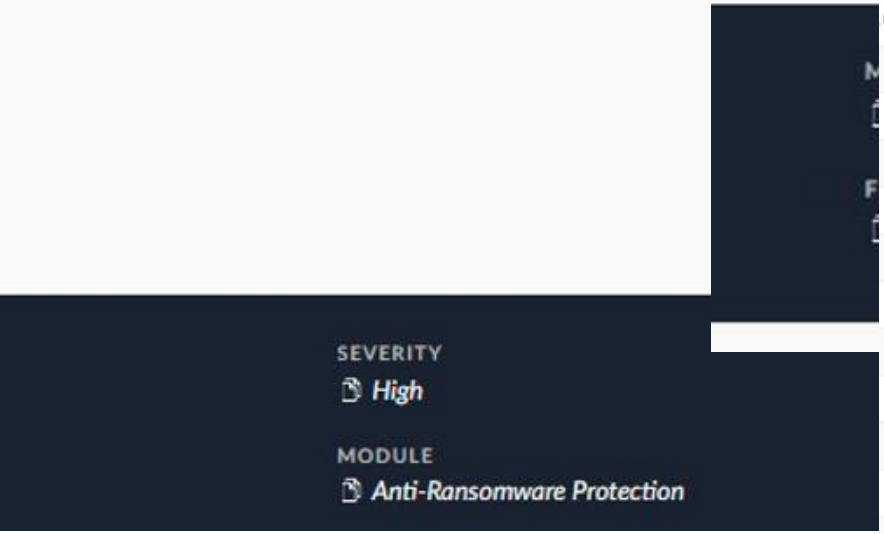
Network 1,089 Results | File 12 Results | Module 51 Results | System Calls 12 Results | Network Connections 1,089 Results

RC_HOST_IP	SRC_PROCESS_USER_NAME	SRC_HOST_OS	ACTION_TYPE	SRC_IP	SRC_PORT
		Windows	Network Outgoing	172.	5126
		Windows	Network Outgoing	172.	5124
		Windows	Network Outgoing	172.	5123
		Windows	Network Outgoing	172.	5122

LockBit:







Fuente: https://www.virustotal.com/gui/file/630e24cc1c4c95321965ad967e77e1888c48c4b1f653d800c7df08e879814787

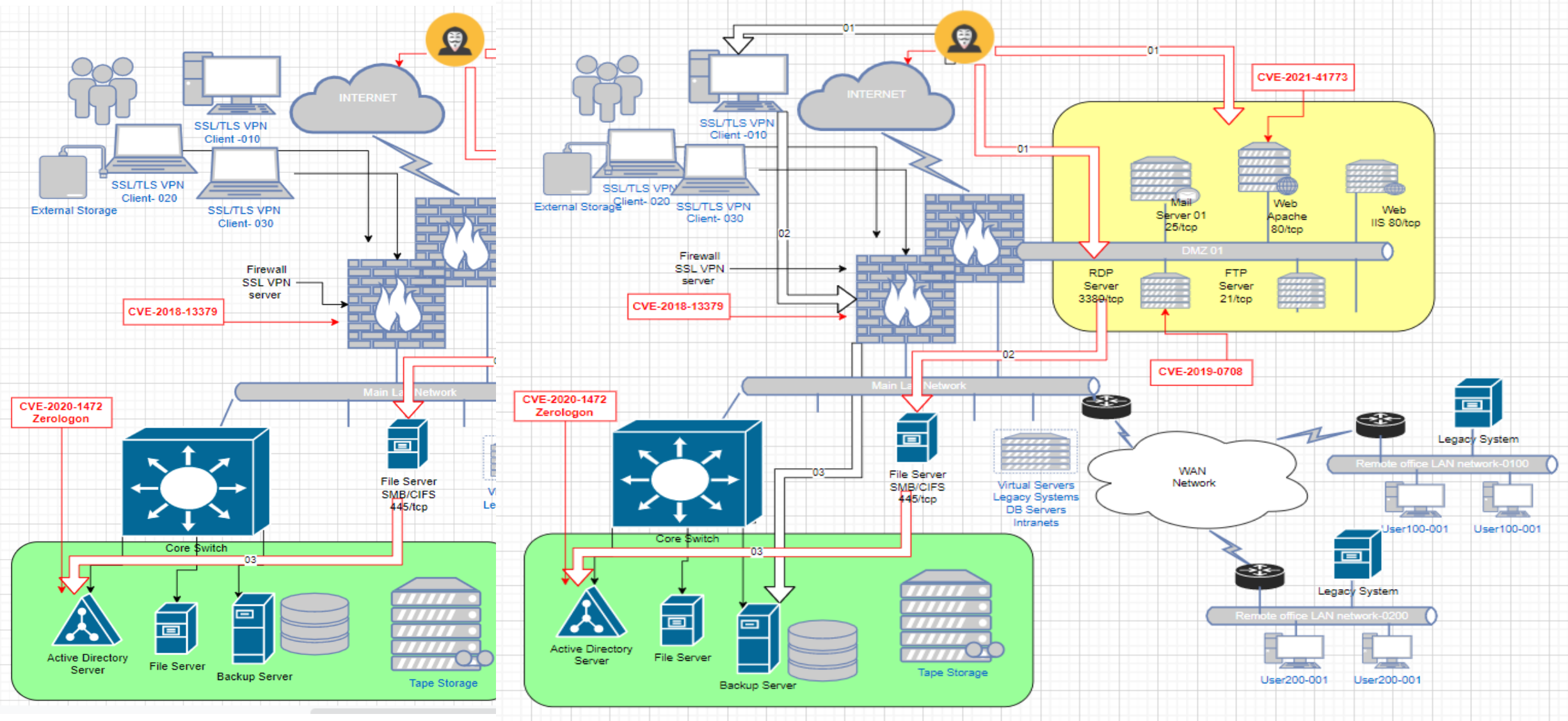
Parte 4: Recomendaciones

Buenas Prácticas, Brief:

- Actualización y parchado sistemas pperativos frecuentemente.
- Backup y Restore on premise, offsite and offline
- Implementar un proceso de Gestión de vulnerabilidades, Incidentes y Hardening.
- Hardening de S.O.: Desactivar PowerShell, quitar programas innecesarios, desactivar usuarios “admin”, Revisa GPOs and shared folders.
- Activar MFA.
- Realizar pruebas de hacking periódicas.
- Revisar las políticas de publicación en los firewalls, eventos, logs, alertas.
- Instalar agentes de seguridad en los servidores tipo EDR/XDR.
- Monitorear conexiones outbound
- Concientizar a los usuarios de la organización en correos falsos, archivos adjuntos.

Fuente: https://www.cisa.gov/stopransomware/ransomware-guide

Contramedidas rápidas: Scanning Vulnerabilidades

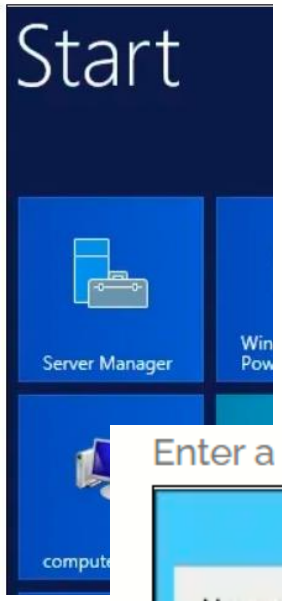


Fuente: Nmap, Nmap/NSE-Scrips, Masscan, Nessus/Tenable.

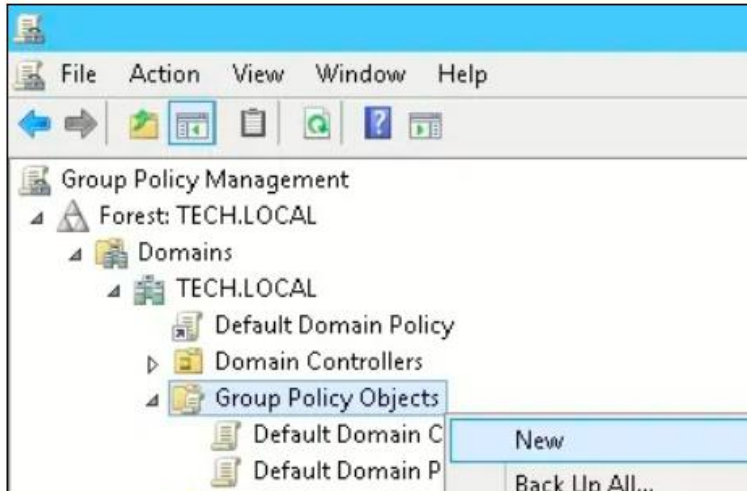
Contramedidas rápidas: Deshabilitar Powershell

Tutorial GPO - Pre

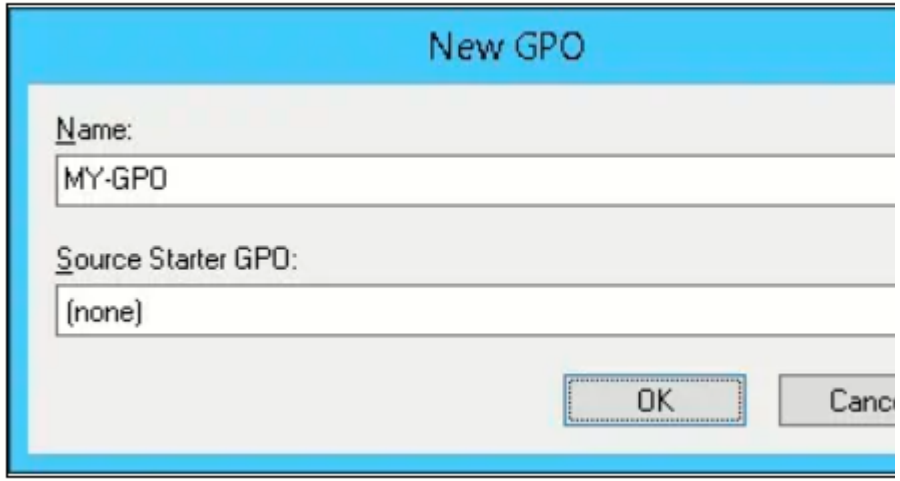
On the domain controlle



Create a new group policy.

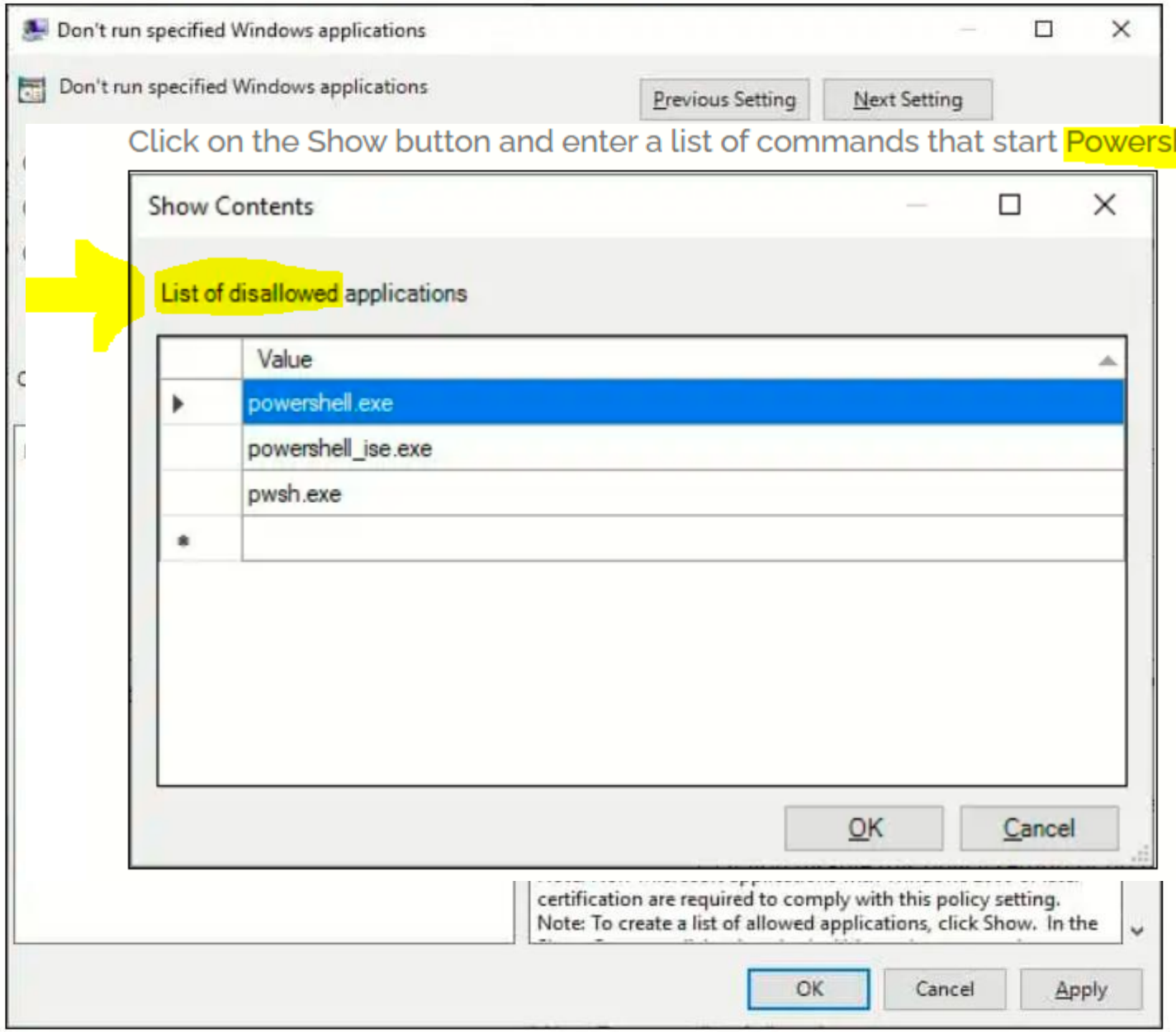


Enter a name for the new group policy.



In our example, the new GPO was named: MY-GPO.

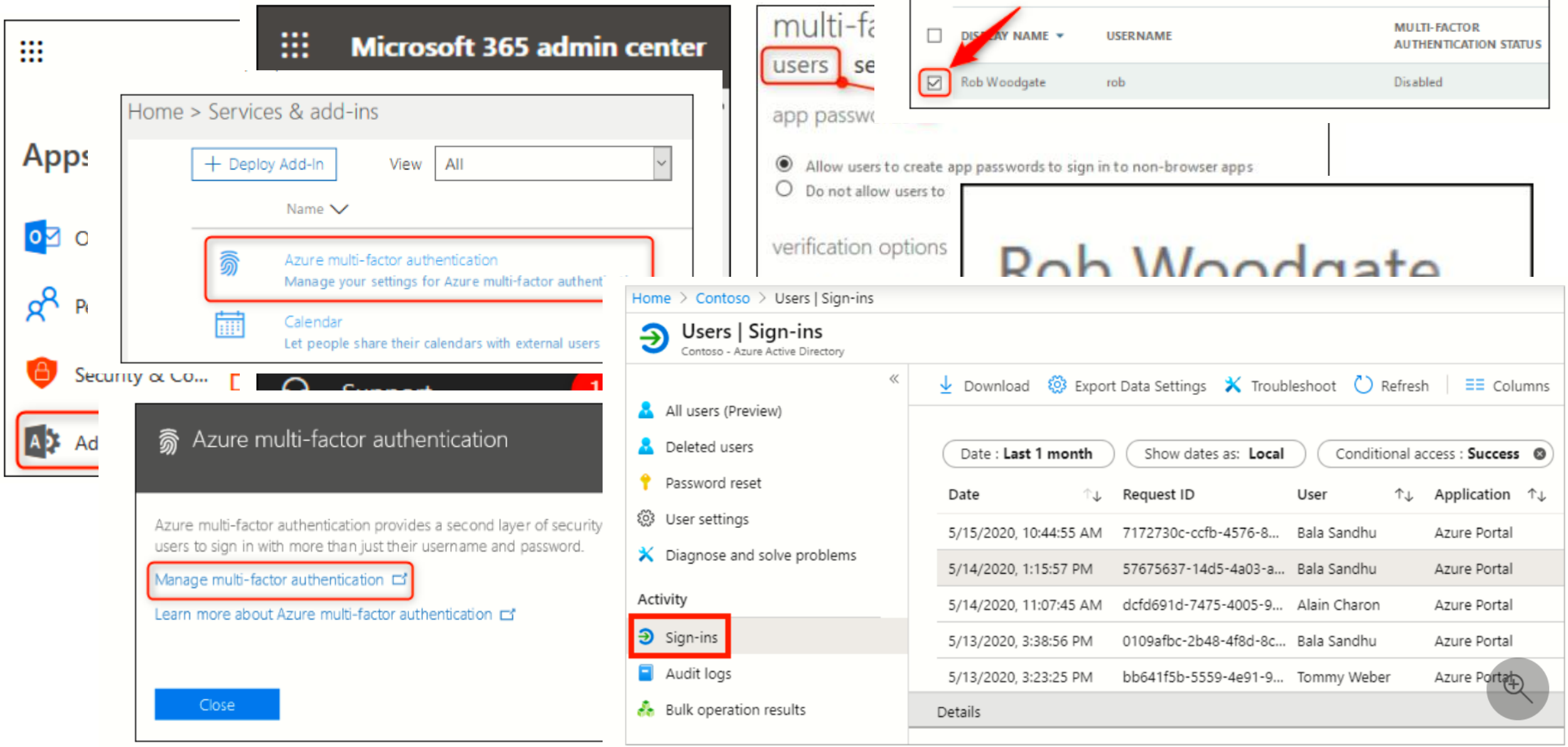
Enable the item named Don't run specified Windows applications.



Telefónica Tech

Fuente: https://techexpert.tips/powershell/gpo-prevent-a

Contramedidas rápidas: MFA



Fuente: https://www.thefastcode.com/article/how-to-enforce-multi-factor-authentication-for-all-users-of-your-office-365-subscription
Fuente: https://docs.microsoft.com/es-es/azure/active-directory/authentication/howto-mfa-reporting

Métodos de Recuperación: (No recomendable!!)

- Backup!! offline y Restore validado -> “Es tu Deber”

- Archivos que no han sido cifrados por tamaño, falta de tiempo del atacante, etc -> “Busca, copia y pega”

- Archivos que se podrían reconstruir -> “Evaluar c/archivo estructura y contenido” con herramientas de análisis forense.

- Buscar publicación del Decryptor “nomoreransomware.org”, “fabricantes” -> “Esperar 2 a 6 meses”

Fuente: https://www.nomoreransom.org/es/index.html

Recomendaciones Finales:

1. Establecer una **estrategia de seguridad en profundidad "Defense in Depth"** generando grupos técnicos, personal calificado, herramientas y procedimientos de acuerdo a los últimos ciberataques.

2. Considerar la **importancia** del **perfil del profesional de ciberseguridad** en el asesoramiento independiente y el conocimiento de "hacking".

3. Para prevenir y responder es necesario la **cooperación técnica e intercambio de experiencias** entre el sector público y privado con centros especialistas locales e internacionales.

4. **No depender** 100% de los fabricantes de seguridad.

5. Crear **entidades nacionales e internacionales** con el objetivo de proteger y defender frente a filtraciones de datos personales.

6. Desde el comité de **LACNIC**, Seguir difundiendo la importancia de la Ciberseguridad en nuestros países a través de Capacitación, Labs e intercambio de experiencias.


Telefónica Tech