

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.

C

LOCKBIT 2.0

LEAKED DATA

CONDITIONS FOR PART



CONTI NEWS

If you are a client who declined the deal and did not find your data on cartel's website or did not find valuable files, this does not mean that we forgot about you, it only means that data was sold and only therefore it did not publish in free access!

Search



[Web mirror](#)

[Tor mirror](#)

emucor.es
80 20H 24M 50 S

private data of company

MORE →

noll-law.com
10 8H 31M 50 S

Part 2. Today's Noll Law Office represents the fourth and fifth generations of lawyers in the Noll-Herndon family. We are a small, family owned business whose roots in Central Illinois go back genera...

MORE →

huess
40 17M

Part 1. Hügger Torsysteme Rudolfstetten, AARGAU of the Architectural and Manufacturing Industry quality services for clients

MORE →

cronos.com.ar
30 18H 39M 50 S

Currently, CRONOS develops, manufactures, distributes and markets products and services that provide solutions for personnel management, access control, monitoring, process management, infrastructure...

MORE →

reitzner.de
30 23H 2M 50 S

Part 1. We hacked reitzner AG. We also stole the data of the companies they serve. From the network of this company, we penetrated into about 30 more companies. Negotiation: <https://www.sendspace.com>

MORE →

multin
70 8H

Part 1. Multimmobiliare founded in May 1998 with the purpose of selling real estate on the

MORE →

schriesheim.de
110 13H 20M 50 S

A lot of personal information such as passports, contracts etc. 170 gb of personal information

MORE →

kdaponte.com
60 5H 36M 50 S

We are a SDO Certified DBE sub-contractor that specializing in the installation of granite/precast curb, concrete sidewalks, masonry stone walls and all types of pavers. We also adjust/remodel manhole...

MORE →

ccfsin
50 8H

We provide our services and responsive operation Chemical, Fertilizer, Fire & Technology. Our division department. The

MORE →

enclosuresoluti...
PUBLISHED FILES

Leading manufacturer of switchboard

valoores.com
20 21H 0M 50 S

Enterprise Business Solutions in Financial

tigerg
20 20M

TIGER GROUP was fo

“INSTITUTO METEOROLÓGICO ...”

<https://imn.ac.cr/racsago.cr/email/ser>
Avenida 9 y Calle 17, San Jose, San Jose, Costa Rica
Instituto Meteorológico Nacional

PUBLISHED 13%

4/19/2022

216

[READ MORE >>](#)

“FOR COSTA RICA”

<https://www.hacienda.go.cr/>
We will continue to attack the ministries of costa rica until its government pays us
Attacks continue today

PUBLISHED 7%

4/19/2022

2675

[READ MORE >>](#)

“DEL SOL”

<https://www.delsol.com>
280 W 10200 S
Sandy, UT 84070
USA
1-888-660-1958
onlineservice@delsol.com

Having fun in the sun has always been at the core of Del Sol's culture. We stand for all that is good. For sunshine. For fun in the sun. For memory-filled vacations. For laughter. For joy. We do it for young and old alike. For the smiles that it brings. Customers are all smiles, giggling and showing off their toe nails, shirts and flip-flops that all change colors with only the tiniest touch of sunshine. We're proud to share a little sunshine with so many people every day.

PUBLISHED 60%

4/19/2022

132

[READ MORE >>](#)

“GIBSON HOMEWARES”

<https://www.gibsonusa.com>
Gibson Homewares HQ
2410 Yates Avenue
Commerce, CA 90040
Local 323.832.8900
Toll Free 800.281.2810
email: gibsonla@gibsonusa.com
Gibson is the nation's leading

“MILAN INSTITUTE”

<https://milaninstitute.edu>
Headquarters:
255 W Bullard Ave, Fresno, California, 93704, United States
(559) 323-2800
gyasuda@milaninstitute.edu
lharell@milaninstitute.edu

“PANASONIC”

<https://www.panasonic.com/ca/>
5770 Ambler DR Mississauga on l4w 2t3
Panasonic Canada Inc is located in Mississauga, ON, Canada and is part of the Household Appliances and Electrical and Electronic Goods Merchant Wholesalers Industry. Panasonic Canada

Ransomware Banjo

encrypted



All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail: furas@airmail.cc

Write this ID in the title of your message A [REDACTED] 61

In case of no answer in 24 hours write us to this e-mail: krasume@tutanota.com

Our online operator is available in the messenger Telegram: [@krasume](https://www.telegram.com/@krasume)

You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the tool that will decrypt all your files.

Free decryption as guarantee

Before paying you can send us up to 5 files for free decryption. The total size of files must be less than 4Mb (non archived), and files should not contain valuable information. (databases, backups, large excel sheets, etc.)

How to obtain Bitcoins

The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.

https://localbitcoins.com/buy_bitcoins

Also you can find other places to buy Bitcoins and beginners guide here:

<http://www.coindesk.com/information/how-can-i-buy-bitcoins/>

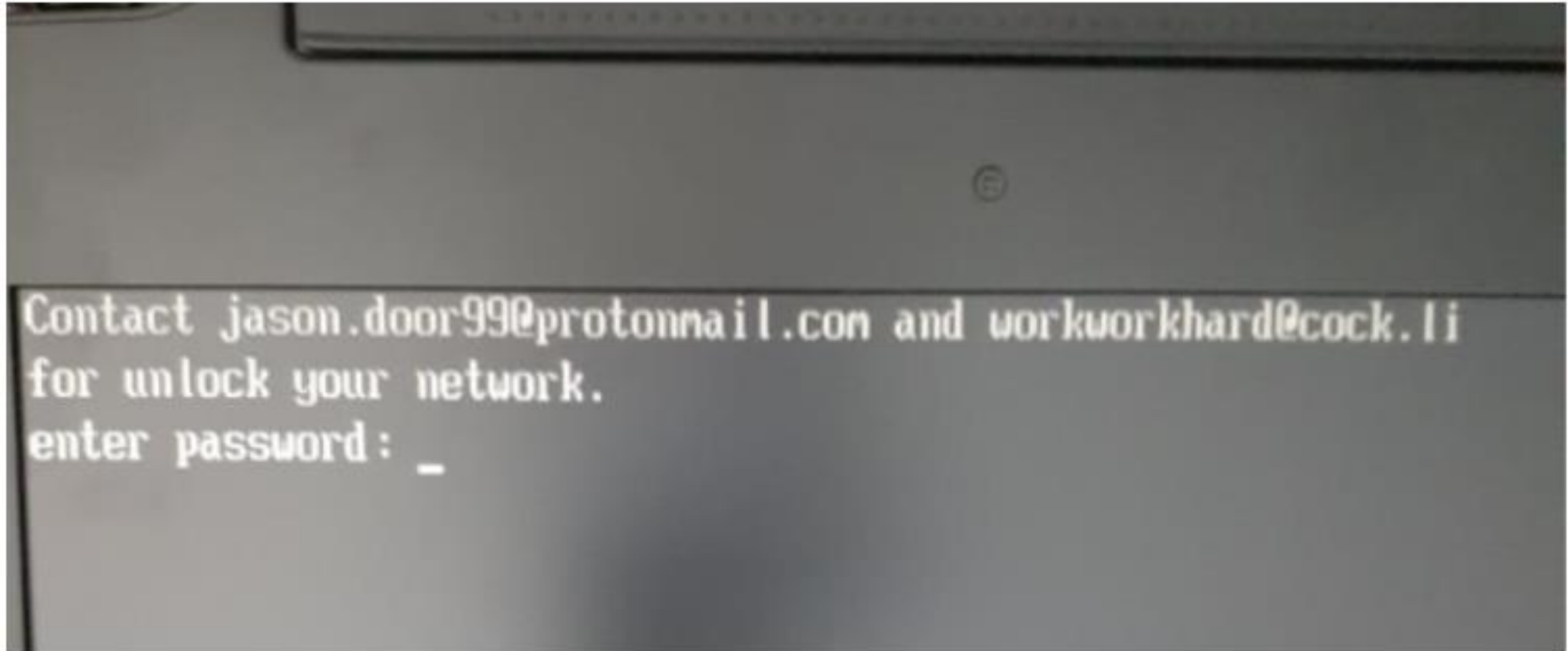
Attention!

- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

Ransomware Prometheus:

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

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



Ransomware lockbit 2.0:

```
1 |IGSé5£ªL°HÝÂÚENOôEÜ£Ñµ+»Ms¼²7"XSTX-8ôJÀ¹Ë[š8£V o¥VTúMÊLÊ-òò
2 |À>\èÝ¥%=j¹ >g¾ACK¾, ENOŽçž SOHh©®, Ý$µ]-ž6üªJ"Ê?:d5Âž¹li-eÜETX9f
3 |ž4NUL-]RS(¤İ×žzf@4ÁðXµETXwíXUSBoe
4 |ãòUS»+DC3¾{½ž-SæêP6SYNW SUBCAN@±ãDLEÿÖFF%·<K4žó`äETX,,äcDC3¶
```

Nombre

- lockbit
- lockbit

Restore-My-Files-2.txt: Bloc de notas

Archivo Edición Formato Ver Ayuda

LockBit 2.0 Ransomware

Your data are stolen and encrypted
The data will be published on the internet
You can contact us and decrypt
<http://lockbitsup4rtrtyezcd5enk>
<http://lockbitsap2orgyydaqhcun3>
OR
<https://decodinggfthdfhdhgdgd.f>.

Decryption ID: MX [REDACTED]



lockbit [REDACTED].onion

deryption service.

Write to support if you want to buy decryptor.

LockBit Ransomware uses AES and ECC cryptography algorithms.

TRIAL DECRYPT **CHAT WITH SUPPORT**

You can decrypt a single file for warranty - **we can do it.**

ATTENTION!
Decryption is available once for you

Upload the encrypted file
max. 256 kb

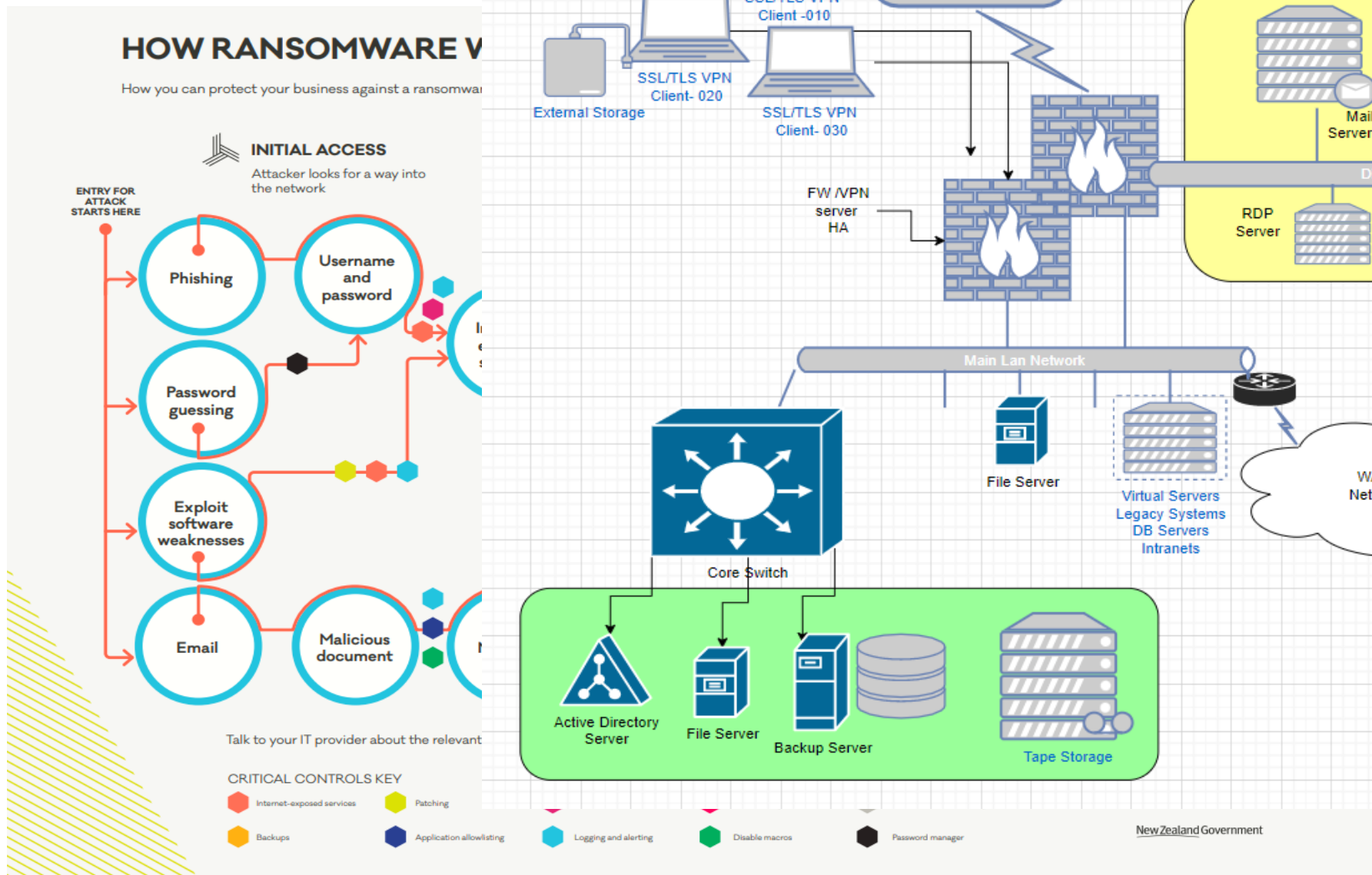
What is the cost of the data?
2022-02-20 15:05:20 readed

the price was 350k but we can lower to 150k .
you already contacted us on different id .
2022-02-20 18:16:16

It is a lot of money
2022-02-21 03:23:33 readed

Message... **SEND**

Introducción, topología



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. RussianFederatio	200. 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. LangFang	200. 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. RussianFederatio	200. 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. ShiJiaZhuang	200. 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. ShiJiaZhuang	200. 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. RussianFederatio	200. 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. RussianFederatio	200. 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. RussianFederatio	200. 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. RussianFederatio	200. 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. RussianFederatio	200. 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. RussianFederatio	200. Peru	RDP	TCP	Alert	ios_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		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. Suzhou(JiangSu)	200. 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. SuZhou(JiangSu)	200. 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. ChengDe	200. 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. ShangHai	200. 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. ShaanXi	200. 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. WenZhou	200. 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. UnitedKingdom	200. 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. UnitedKingdom	200. 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. UnitedKingdom	200. 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



KNOWN EXPLOITED VUL

[Download CSV version](#)

[Download JSON version](#)

[Download JSON schema](#)

[Subscribe to the Known Exploited Vulnerability](#)

[Back to previous page for background on known](#)

CVE	Vendor/Project	Product	Vulnerability Name	Date Added to Catalog	Short Description	Action	Due Date	Notes
			"BlueKeep"		A remote code execution vulnerability exists in Remote Desktop Client.			

Table 1: Top 15 Routinely Exploited Vulnerabilities in 2021

CVE	CVEs	Vendor	CVEs	Vendor	CVEs	Vendor	CVEs	Vendor		
CVE-2021-44228	<ul style="list-style-type: none"> CVE-2021-22893 CVE-2020-8260 CVE-2020-8243 CVE-2019-11539 CVE-2019-11510 	Pulse SecureVPN	<ul style="list-style-type: none"> CVE-2020-8196 CVE-2020-8195 CVE-2019-19781 CVE-2019-11634 	Citrix	<ul style="list-style-type: none"> CVE-2021-34523 CVE-2021-34473 CVE-2021-31207 CVE-2021-26855 	Microsoft Exchange	<ul style="list-style-type: none"> CVE-2020-12812 CVE-2019-5591 CVE-2018-13379 	Fortinet	<ul style="list-style-type: none"> CVE-2021-20016 CVE-2020-5135 CVE-2019-7481 	SonicWall
CVE-2021-40539	<ul style="list-style-type: none"> CVE-2021-22986 CVE-2020-5902 	F5	<ul style="list-style-type: none"> CVE-2020-2021 CVE-2019-1579 	Palo Alto	<ul style="list-style-type: none"> CVE-2021-28799 CVE-2020-36198 	QNAP	<ul style="list-style-type: none"> CVE-2020-12271 	Sophos	<ul style="list-style-type: none"> CVE-2019-0604 	SharePoint
CVE-2021-34523	<ul style="list-style-type: none"> CVE-2019-0708 CVE-2020-1472 CVE-2021-31166 CVE-2021-36942 	Microsoft Windows	<ul style="list-style-type: none"> CVE-2017-0199 CVE-2017-11882 CVE-2021-40444 	Microsoft Office	<ul style="list-style-type: none"> CVE-2021-21985 	vCenter	<ul style="list-style-type: none"> CVE-2021-27101 CVE-2021-27104 CVE-2021-27102 CVE-2021-27103 	Accellion	<ul style="list-style-type: none"> CVE-2021-20655 	FileZen
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										

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 el 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 unknown

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 el 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 unknown
- Fuente: rdpscan, 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 Credenciales

LAPSUS\$

LAPSUS\$
28 787 subscribers

*****What should we leak next?*****
Anonymous Poll

- Vodafone source code - around 5000 github repos. 200gb or so compressed
- Impresa source code and databases.
- MercadoLibre and MercadoPago source code - 24000 repos

13 120 votes

1 077 Comments

The above poll will end 03/13/22 00:00

993 Comments

Yesterday

We recruit employees/insider at the following!!!!

- Any company providing Telecommunications (Claro, Telefonica, ATT, and other similar)
- Large software/gaming corporations (Microsoft, Apple, EA, IBM, and other similar)
- Callcenter/BPM (Atento, Teleperformance, and other similar)
- Server hosts (OVH, Locaweb, and other similar)

TO NOTE: WE ARE NOT LOOKING FOR DATA, WE ARE LOOKING FOR THE EMPLOYEE TO PROVIDE US A VPN OR CITRIX TO THE NETWORK, or some anydesk

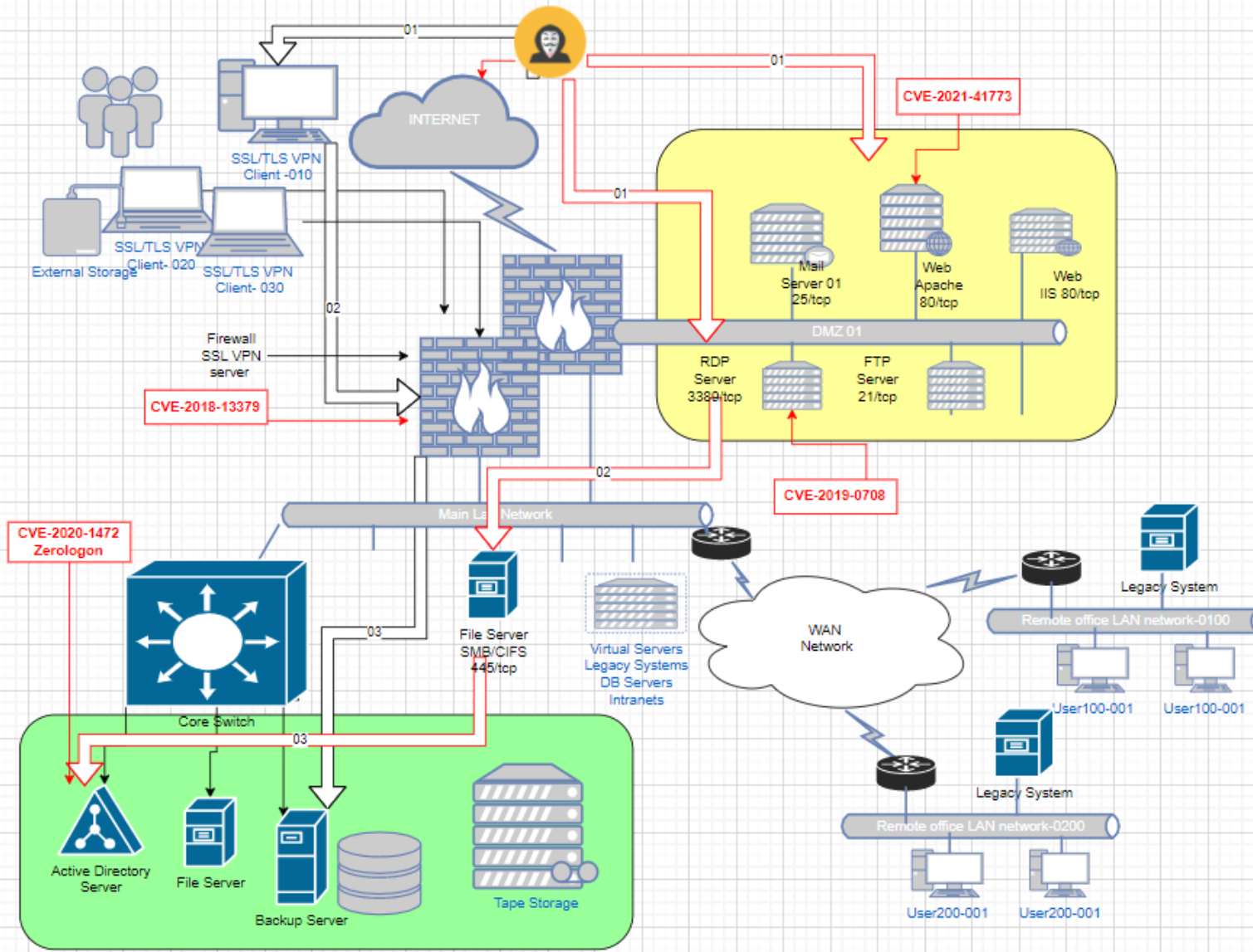
If you are not sure if you are needed then send a DM and we will respond!!!!
If you are not a employee here but have access such as VPN or VDI then we are still interested!!

You will be paid if you would like. Contact us to discuss that

@lapsusjobs

646 Comments

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



@lapsusjobs

3642 edited 15:36

156 comments

Vulnerabilidad CVE-2018-13379:

rfmirror.com/Thread-
session-6-7GB-CVE-2018-13379

websession 6.7GB [CVE-2018-13379]
by arendee2018 - November 24, 2020 at 09:00 PM

Pages (7): 1 2 3 4 5 ... 7 Next »

arendee2018
November 24, 2020 at 09:00 PM This post was last modified: November 25, 2020 at 12:37 PM by arendee2018.

this is the most complete achieve containing all exploit links and
contains links and all websessions files from the devices
not available anywhere else
6.7GB uncompressed
https://anonfiles.com/v8eaY3s3p9...-13379_rar

```
50k.txt  
1 https:// 044.  
2 https:// 044.  
3 https:// 044.  
4 https:// 104.  
5 https:// 104.  
6 https:// 104.  
7 https:// :10.  
8 https:// :10.  
9 https:// :10.  
10 https:// :10.  
11 https:// :10.
```

> -VPN-CVE-2018-13379

Nombre	Fecha de modificaci
50k	27/04/2021 19:55
pak	27/04/2021 19:55
50K (1).xlsx	13/05/2021 11:11
50k.rar	25/11/2020 19:01
50k.txt	10/02/2021 16:28
fuck israel.jpg	25/11/2020 19:01
pak.rar	25/11/2020 19:01
pak.txt	25/11/2020 19:01

```
50k.txt  
49561 https:// /r  
49562 https:// re  
49563 https:// re  
49564 https:// 10  
49565 https:// :1  
49566 https:// :1  
49567 https:// /r  
49568 https:// /r  
49569 https:// /r  
49570 https:// 44  
49571 https:// em  
49572 https:// re  
49573 https:// :1  
49574 https:// /r  
49575 https:// :1  
49576 https:// 04  
49577 https:// 10
```

Vulnerabilidad CVE-2018-13379:

- Desde un browser: [https://\"IP-FW-VPNServer\":10](https://\)

The image displays a browser window on the left showing a list of users and their connection details. Red boxes highlight specific fields: "IP address of the connection", "User01-SSL", "Password", "User02-SSL", "User03-SSL", "User04-SSL", "User05-SSL", "User06-SSL", "IP address of the connection", and "Password".

On the right, a terminal window shows the corresponding system logs for each user. Red arrows point from the highlighted fields in the browser to the corresponding log entries in the terminal. The terminal output includes fields such as "IP address of the connection", "User 01", "Password", and "Group SSL".

```
root
189.
ricardo
M
VPN SSL
full-access
root
BasLkR
xHxa
189.
mari
m
VPN SSL
full-access
root
187.
fab
M
VPN SSL
full-access
root
17
pi
M
VPN SSL
full-access
root
17
cris
M
VPN SSL
full-access
root
root@saturno_02mar20:~/CVE-2018-13379#
```


Parte 3: Detección y Respuesta:

Mimikatz:

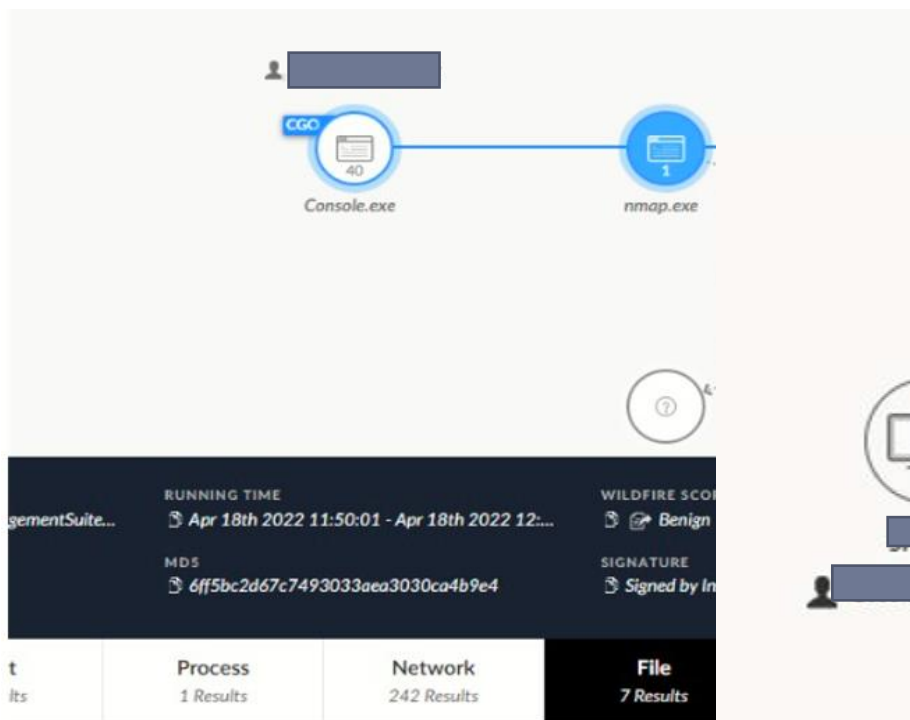
Behavioral Threat' al
42 Alerts
Overview Ke
42 Alerts 7 Ins

View children

Children Found 34 results

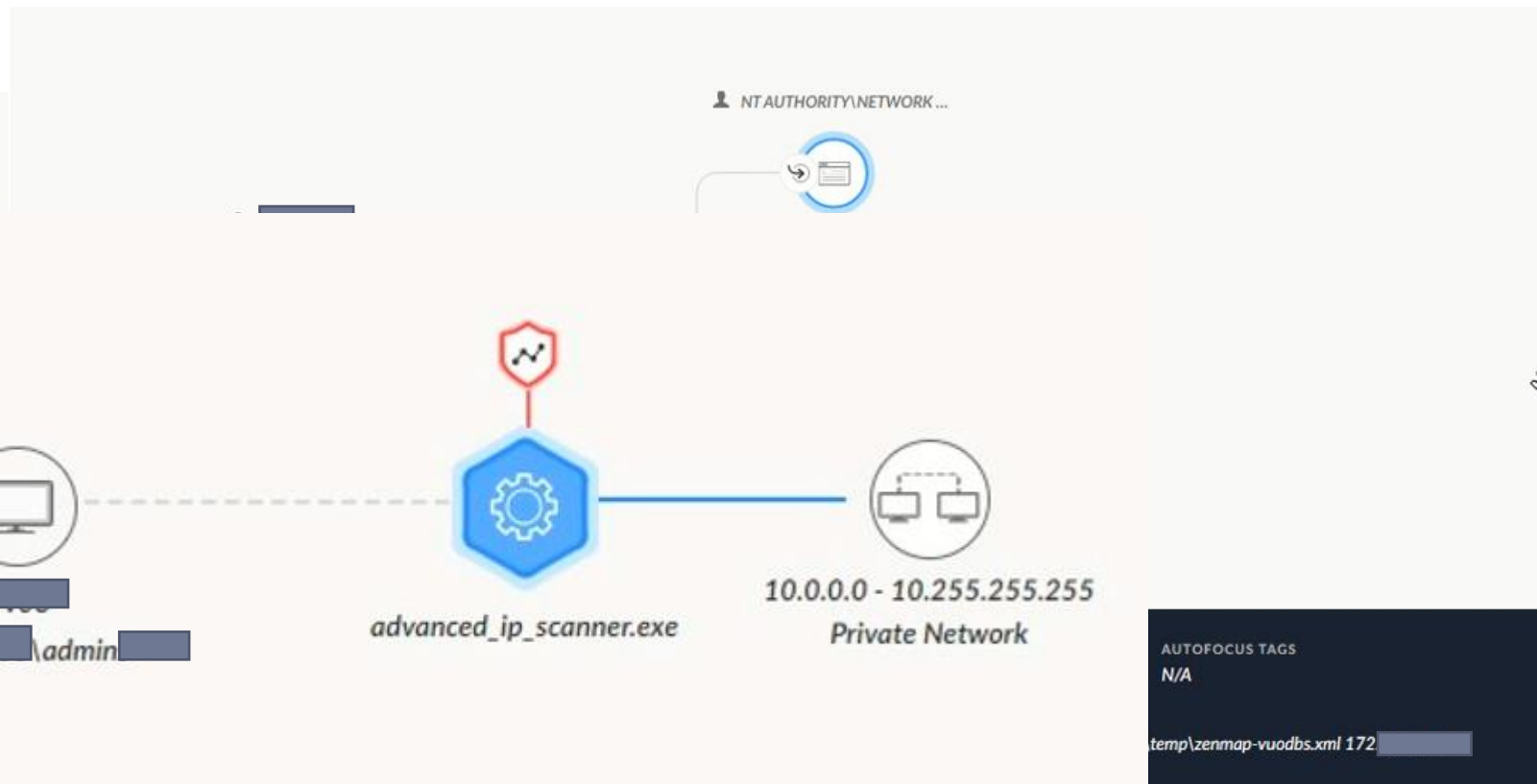
	PROCESS START TIME	NAME	CMD	USERNAME
<input type="checkbox"/>	Apr 15th 2022	Taskmgr.exe	"C:\Windows\system32\taskmgr.exe" /4	\admini
<input type="checkbox"/>	Apr 15th 2022	fsquirt.exe	"C:\Windows\System32\fsquirt.exe" -Register	\admini
<input type="checkbox"/>	Apr 15th 2022	notepad.exe	"C:\Windows\system32\notepad.exe" C:\Users\admini\Desktop\automim1\automim1\logs\Passwords.txt	\admini
<input type="checkbox"/>	Apr 15th 2022	notepad.exe	"C:\Windows\system32\notepad.exe" C:\Users\admini\Desktop\ArestoreNew\cepoass.txt	\admini
<input type="checkbox"/>	Apr 15th 2022	notepad.exe	"C:\Windows\system32\notepad.exe" C:\Users\admini\Desktop\automim1\automim1\mimikatz\x64\mimikatz.log	\admini
<input type="checkbox"/>	Apr 15th 2022	runonce.exe	C:\Windows\SysWOW64\runonce.exe /Run6432	\admini
<input type="checkbox"/>	Apr 15th 2022	ie4uinit.exe	"C:\Windows\System32\ie4uinit.exe" -UserConfig	\admini
<input type="checkbox"/>	Apr 15th 2022	rundll32.exe	"C:\Windows\System32\rundll32.exe" "C:\Windows\System32\iesetup.dll",IEHardenAdmin	\admini
<input type="checkbox"/>	Apr 15th 2022	rundll32.exe	"C:\Windows\System32\rundll32.exe" "C:\Windows\System32\iesetup.dll",IEHardenUser	\admini
<input type="checkbox"/>	Apr 15th 2022	unregmp2.exe	"C:\Windows\System32\unregmp2.exe" /FirstLogon	\admini
<input type="checkbox"/>	Apr 15th 2022	unregmp2.exe	"C:\Windows\System32\unregmp2.exe" /FirstLogon	\admini

nmap, zenmap, ip_scanner:



ManagementSuite...
 RUNNING TIME
 Apr 18th 2022 11:50:01 - Apr 18th 2022 12:00:00
 MDS
 6ff5bc2d67c7493033aea3030ca4b9e4
 WILDFIRE SCORE
 Benign
 SIGNATURE
 Signed by In...

Process	Network	File
1 Results	242 Results	7 Results



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

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



Administrator

explorer.exe was initiated from a remote terminal session. Client IP address: 10.11 [redacted]

10.11 [redacted] → CGO 45 → explorer.exe

Administrator

explorer.exe

windows

SEVERITY: High

MODULE: Anti-Ransomware Protection

PATH	RUNNING TIME	WILDFIRE SCORE	SHA256	AUTOFOCUS
C:\Windows\explorer.exe	Apr 15th 2022 10:27:45 - Apr 20th 2022 05:...	Benign	70506db080603a6a35004e92edb2ed5bfa5...	N/A
USERNAME	MDS	SIGNATURE	CMD	
Administrator	dfb52454da750523d816ce1373534378	Signed by Microsoft Corporation	C:\Windows\Explorer.EXE	

All Actions	Alert	Process	Network	File	Registry	Module	Injection	System
1,962 Results	1 Results	44 Results	1 Results	630 Results	508 Results	294 Results	395 Results	30 Res

IP	SRC_PROCESS_USER_NAME	SRC_HOST_OS	ACTION_TYPE	FILE_NAME	FILE_PREVIOUS_NAME
[redacted]	Administrator	Windows	File Read	thumbcache_256.db	
[redacted]	Administrator	Windows	File Write	f01b4d95cf55d32a.automaticDestinations...	
[redacted]	Administrator	Windows	File Write	766c6474ef2adc83.automaticDestinations...	
[redacted]	Administrator	Windows	File Create	766c6474ef2adc83.automaticDestinations...	
[redacted]	Administrator	Windows	File Write	D.reg	
[redacted]	Administrator	Windows	File Write	D.reg	
[redacted]	Administrator	Windows	File Create	D.reg	
[redacted]	Administrator	Windows	File Rename	windows.exe	LockBit_D85C0F0DDAC84072.exe
[redacted]	Administrator	Windows	File Write	LockBit_D85C0F0DDAC84072.exe	
[redacted]	Administrator	Windows	File Write	LockBit_D85C0F0DDAC84072.exe	
[redacted]	Administrator	Windows	File Create	LockBit_D85C0F0DDAC84072.exe	

Parte 4: Recomendaciones

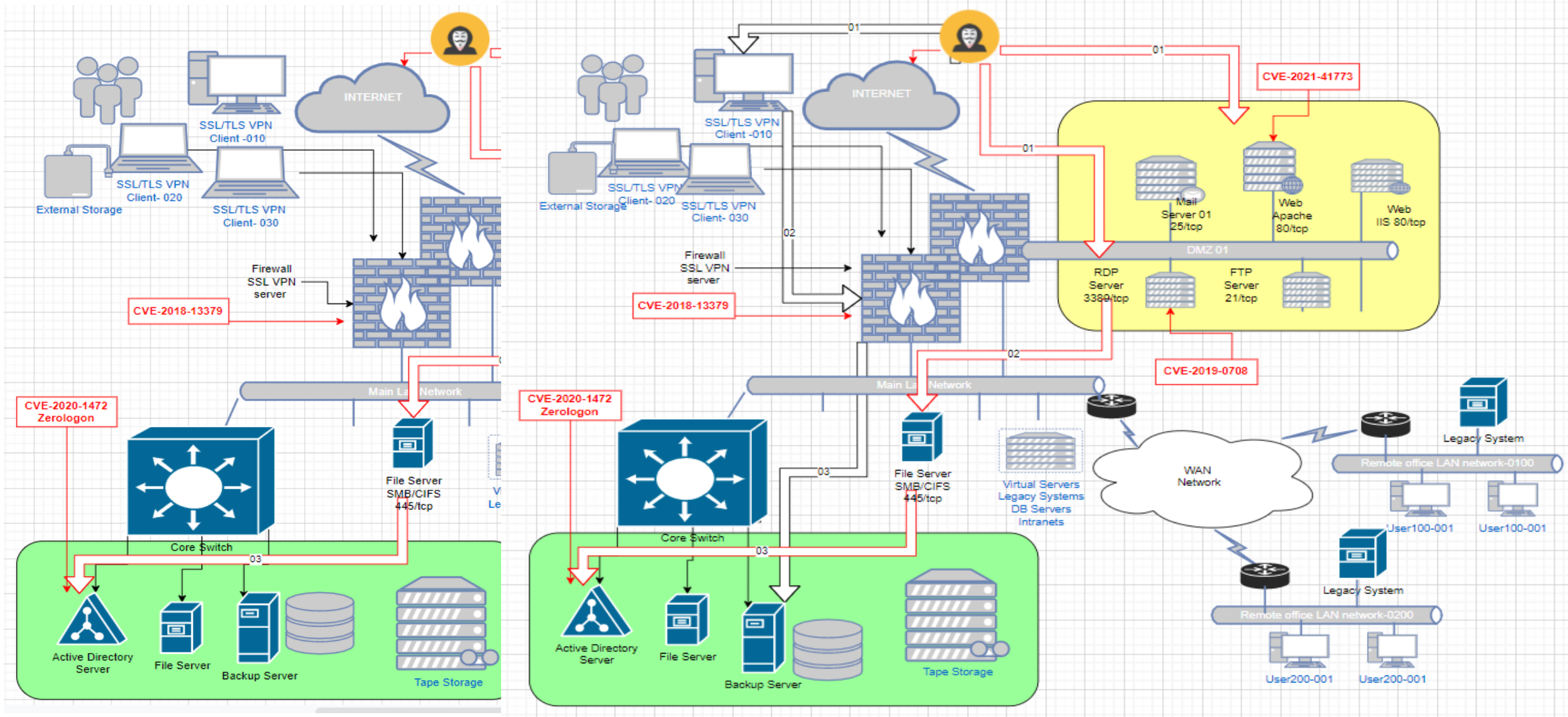
Buenas Prácticas, Brief:



- Actualización y parchado sistemas operativos 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.

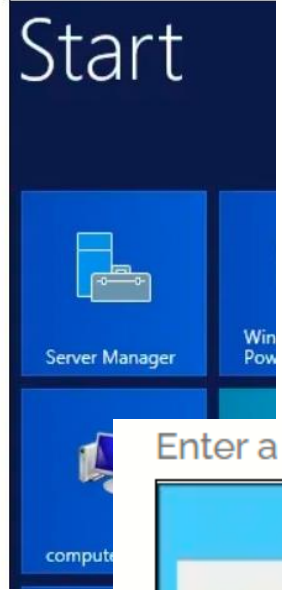
Fuente: <https://www.cisa.gov/stopransomware/ransomware-guide>

Contra medidas rápidas: Scanning Vulnerabilidades

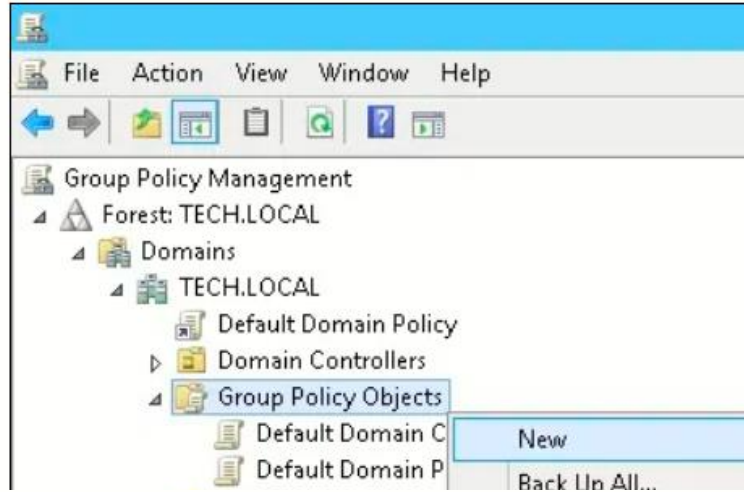


Contra medidas rápidas: Deshabilitar Powershell

Tutorial GPO - Pre
On the domain controller



Create a new group policy.

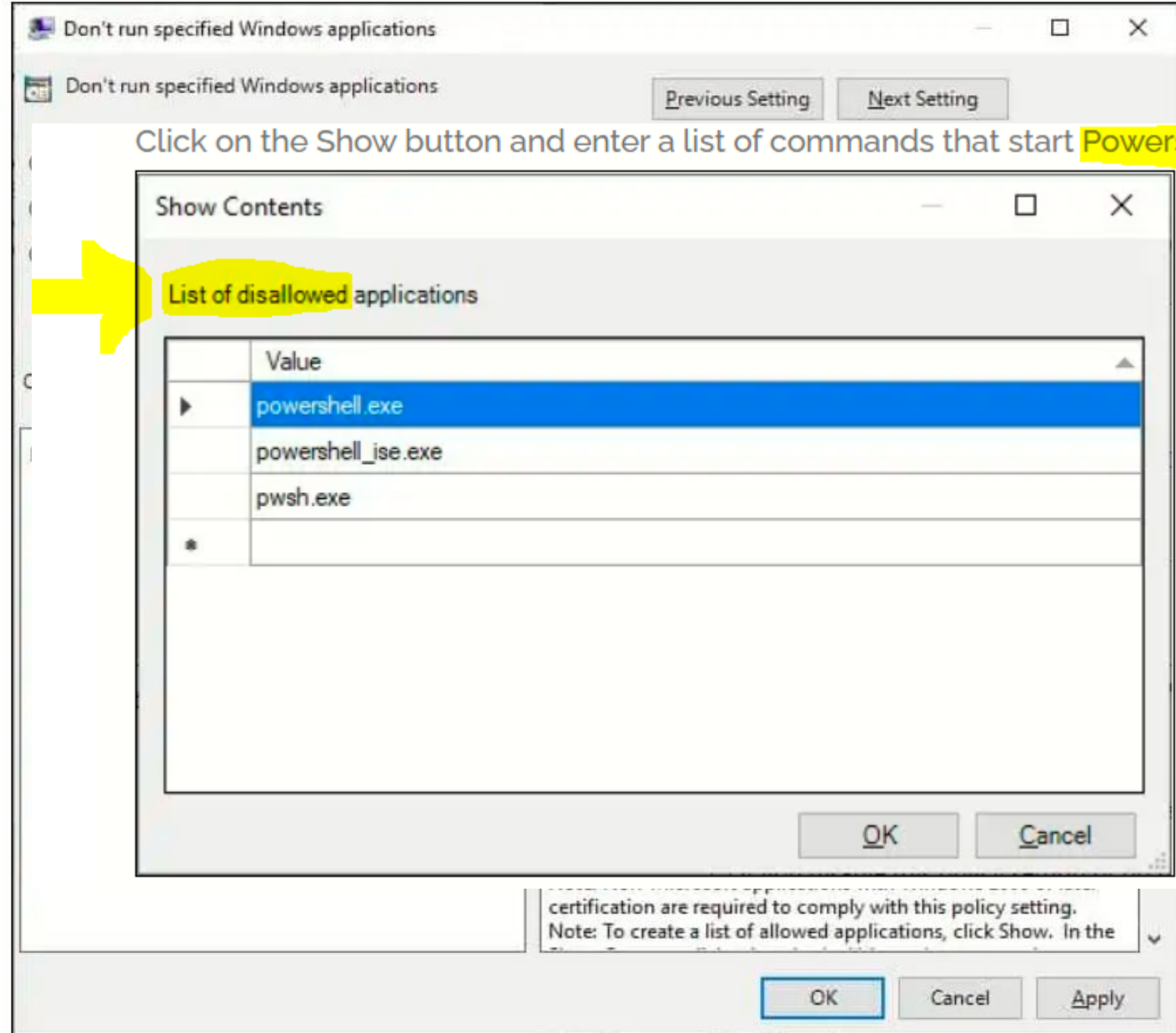


Enter a name for the new group policy.



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

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



Constramedidas rápidas: MFA

The image shows a sequence of steps in the Microsoft 365 admin center to enable Multi-Factor Authentication (MFA) for all users:

- Step 1:** In the Microsoft 365 admin center, navigate to **Services & add-ins**. The **Azure multi-factor authentication** tile is highlighted with a red box.
- Step 2:** Click on the **Azure multi-factor authentication** tile to open its settings page.
- Step 3:** On the settings page, click on **Manage multi-factor authentication** (highlighted with a red box).
- Step 4:** In the **Users | Sign-ins** section, the **Sign-ins** option is highlighted with a red box.
- Step 5:** A table shows the MFA status for users. The checkbox for **Rob Woodgate** is checked, and his status is **Disabled**. A red arrow points to this checkbox.
- Step 6:** A user's MFA verification options are shown, with the **Allow users to create app passwords to sign in to non-browser apps** option selected.
- Step 7:** A table of sign-in activity is shown, with the **Sign-ins** activity highlighted in the left sidebar.

View:	Sign-in allowed users	Multi-Factor Auth status:	Any
<input type="checkbox"/>	DISPLAY NAME	USERNAME	MULTI-FACTOR AUTHENTICATION STATUS
<input checked="" type="checkbox"/>	Rob Woodgate	rob	Disabled

Date	Request ID	User	Application
5/15/2020, 10:44:55 AM	7172730c-ccfb-4576-8...	Bala Sandhu	Azure Portal
5/14/2020, 1:15:57 PM	57675637-14d5-4a03-a...	Bala Sandhu	Azure Portal
5/14/2020, 11:07:45 AM	dcfd691d-7475-4005-9...	Alain Charon	Azure Portal
5/13/2020, 3:38:56 PM	0109afbc-2b48-4f8d-8c...	Bala Sandhu	Azure Portal
5/13/2020, 3:23:25 PM	bb641f5b-5559-4e91-9...	Tommy Weber	Azure Portal

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