Dissection of a ransomware attack

EKO – 2024

Indetectables.net - base4sec.com

Luciano López

En la actualidad soy consultor de ciberseguridad, con experiencia en respuesta a incidentes, detección e inteligencia de amenazas y análisis forense. Los últimos 7 años estuve colaborando en tareas defensivas, teniendo la oportunidad de formar y ayudar en equipos técnicos (CYBERSOC, CSIRT).

BASE4 SECURITY

Emmanuel Seoane (DSR!)

Soy un apasionado de la programación desde mi adolescencia, y me dedico a la consultoría en ciberseguridad y desarrollo. Mi rol principal actualmente es el de líder técnico y de equipo en proyectos web y móviles, utilizando diversos lenguajes de programación según las necesidades.

He participado en proyectos comunitarios como Metasploit y Home Assistant, entre otros. También soy el owner de la comunidad Indetectables.net.

Indetectables

Agenda

- Entendiendo la dinámica del Crimeware
- Evolución de las técnicas de Ransomware
- Mercados under su oferta y demanda
- Metodología para la selección de víctimas y despliegue del ataque
- Respuesta a incidentes (Etapas)
- Identificar y analizar
- Exfiltración de información
- Materialización del evento y análisis
- Eventos actuales
- Negociación y exposición
- Conclusiones

1.1 Cuando los “troyanos” iniciaron todo

Desde el nacimiento del primer RAT (Remote Administration Tool) hasta la llegada de los troyanos bancarios podemos ver como fue la evolución **tanto técnica como maliciosa**.

1.2 Entendiendo la dinámica del Crimeware

Saquemos algunas conclusiones de lo que nos puede ofrecer el Crimeware para nuestra operación

- Constante evolución
- Gran variedad de herramientas
- Técnicamente muy complejas y robustas
- Completamente privadas
- Modulares y trabajos a medida

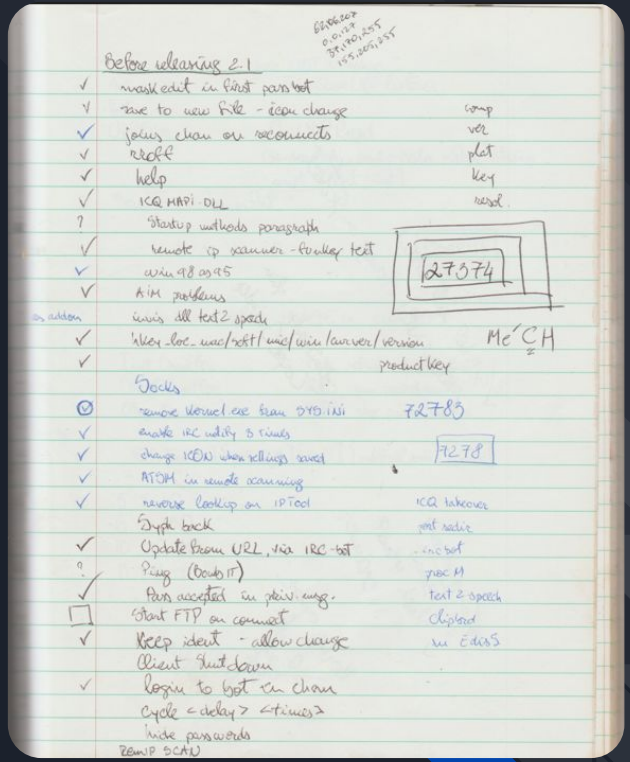


Foto del cuaderno donde mobman hacia notas sobre qué cosas tenía que tener el Sub7

2.1 Evolución de las Técnicas de Ransomware: Inicios

- **2006 - Lockers**: Aparecen los primeros especímenes de este tipo como lo fue GPcode.
- **2008 - Cifrados robustos**: cifrado de archivos específicos en el sistema, usando algoritmos robustos como RSA.
- **2010 - Técnicas de Evasión**: Con el tiempo, el ransomware ha adoptado técnicas para evadir la detección, como la ofuscación de código, uso de apis nativas, etc.
- **2015 - RaaS (Ransomware as a Service)**: La aparición del RaaS permitió a usuarios menos técnicos participar en campañas de ransomware, facilitando el acceso general a estas herramientas maliciosas.

Esta fue mi reacción en 2015 cuando vi los primeros incidentes de RaaS

2.2 Evolución de las Técnicas de Ransomware: Presente

- **2017 - Ataques Coordinados**: Ahora vemos ataques más sofisticados que se centran en organizaciones enteras, apuntando a servidores y sistemas de backup para maximizar el impacto.
- **2019 - Doble Extorsión**: Enfoques más recientes incluyen no sólo el cifrado de archivos, sino también la amenaza de publicar datos robados si no se paga el rescate.
- **2022 - Programas de Bug Bounty**: Lockbit y otros actores anunciaron que están haciendo uso de esta metodología para securizar sus productos.
- **2023 - Ataques a la Cadena de Suministro**: Los atacantes explotan vulnerabilidades en software ampliamente usado (3CX, MOVEit, etc) para infectar múltiples organizaciones a la vez, aprovechando la conectividad usada actualmente.

3.1 Mercados under y su oferta

Un **cibercriminal** nuevo en este mundo tendría que resolver estas incógnitas...

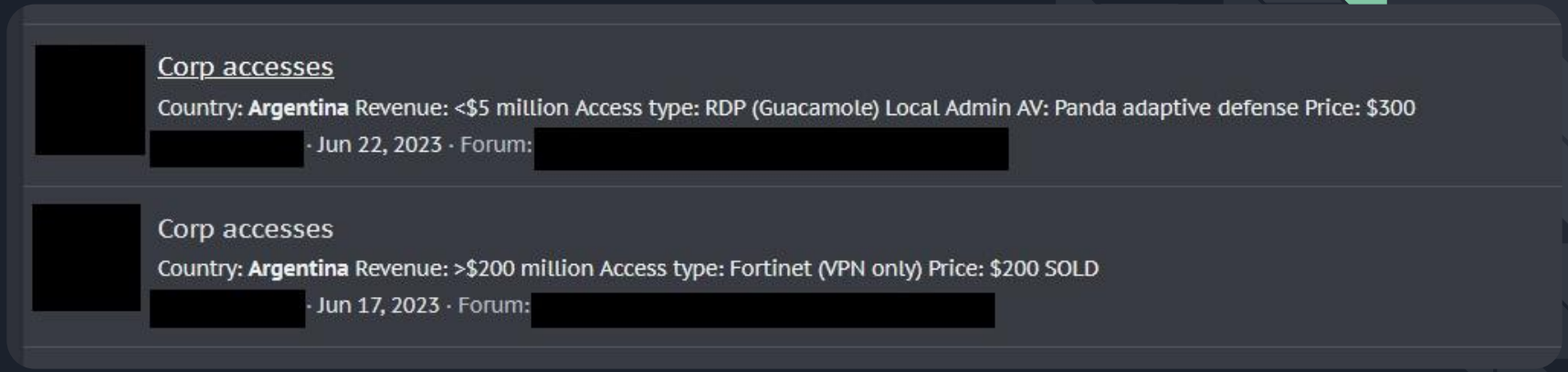
- Como una persona entra en este mundo?
- Como género los contactos?
- Qué herramientas necesito?
- Qué otras cosas puedo necesitar?

Los loaders son la evolución de los crypters. Son muy usados como Malware as a Service (MaaS).

3.2 Mercados under y su oferta

La “*receta*” del éxito...

- Crypter/Loaders
- Botnet, rats o ransomwares
- Tráfico o accesos
- Otras herramientas de apoyo y infraestructura



Captura de foro real...

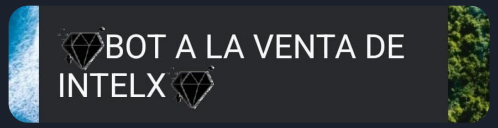
3.3 Hasta tienen mejores herramientas que vos

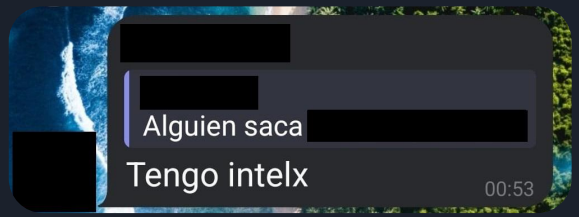
[redacted]

[SELL] Pentest/Red Team Software (Brute Ratel 1.7.4, Cobalt Strike 4.9.1, Core Impact 21.3 and Others)

...or so and you won't be able to use anymore [redacted] something like that). Don't use for anything seriou
original file exceeds the whole...

[redacted] · Sunday at 9:49 AM · Forum: [redacted]





Mas capturas de foros reales

4.1 Metodología para la selección de víctimas

Para entender la metodología de selección de **víctimas** hay que entender algo clave, y esto es que es primordial para el atacante ejercer el menor esfuerzo.

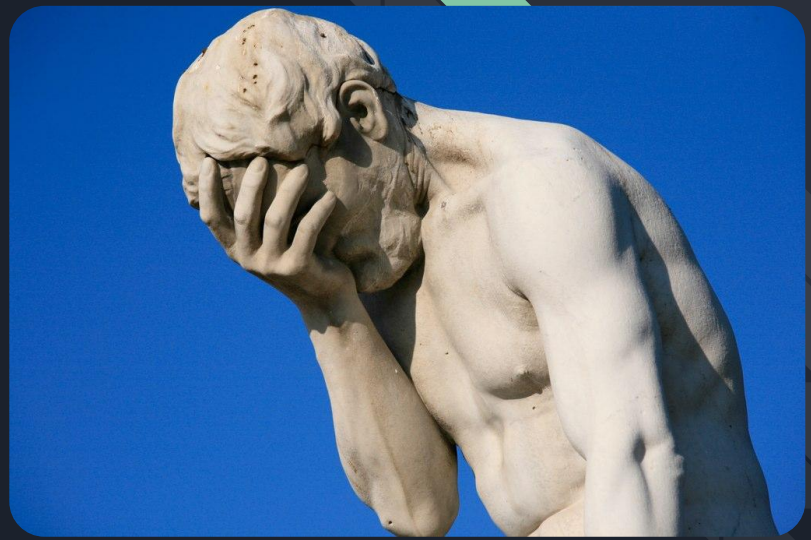
4.2 Despliegue del ataque

- **Phishing**: Engañan a los usuarios para que hagan click en enlaces maliciosos o abran adjuntos infectados, lo cual desencadena la descarga del ransomware.
- **Explotación de Vulnerabilidades**: Utilizan vulnerabilidades en software para infiltrar sistemas y desplegar ransomware.
- **Accesos Remotos**: Explotan accesos remotos mal configurados o débilmente protegidos, como RDP (Remote Desktop Protocol) y VPNs.
- **Malvertising**: Insertan código malicioso en anuncios en línea que, cuando se clickean, descargan ransomware.
- **Ingeniería Social**: Emplean tácticas sofisticadas de engaño para obtener acceso y distribuir ransomware.
- **Drive-by Downloads**: Facilitan la descarga automática y ejecución del ransomware simplemente visitando una página web maliciosa.
- **Redes de Entrega de Malware**: Utilizan infraestructuras de entrega de malware existentes para distribuir ransomware.
- **Compra de Credenciales**: Se adquieren en mercados clandestinos credenciales robadas de empleados o sistemas, permitiendo el acceso directo y la posterior instalación del ransomware.

4.3 El ataque ganador

Tu operatoria consiste en un RaaS (Ransomware as a Service) para atacar y lo distribuiste vía MaaS (Malware as a Service).

Un sysadmin se infecto buscando un crack de Office en el buscador y así infectaste toda la organización...



Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   [redacted]3HMuxXTuR2R1t78mGSdzaAt[redacted]

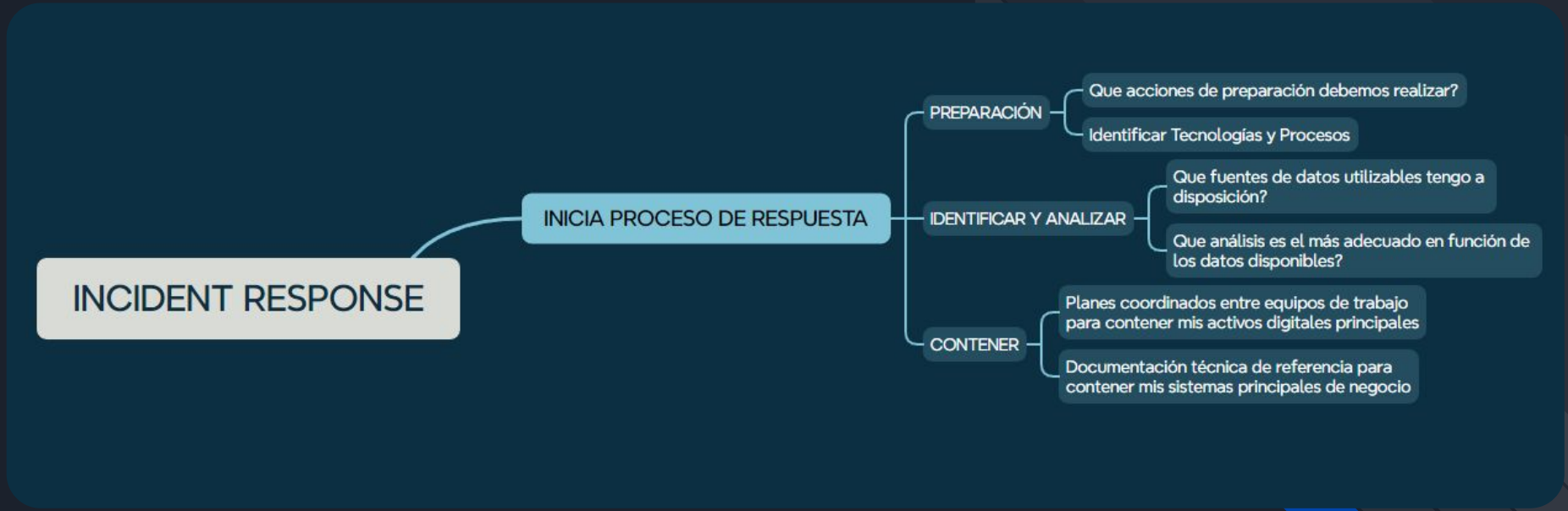
2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:

   [redacted]-maYbSA-wqxAgs-Fsn1L6-FrScbp-aoXt1o-vHdA9t-nHPBo9-DsiuZC-[redacted]

If you already purchased your key, please enter it below.
Key: _

5.1 Respuesta a Incidentes (Etapas)

A continuación se explican las 3 primeras fases de la respuesta a incidente



Fases iniciales de Incident Response

5.2 Identificar y analizar

Fuentes de Datos

- Dump de memoria
- Copia de disco hdd o ssd
- Imagenes E01 o raw
- Logs networking (*FW, PROXY*)
- **Logs**
- **Y más Logs**

Artefactos de Windows

- Windows Event Logs (*EVTX*)
- Prefetch y Shellbags
- Powershell History (*PSReadLine*)
- RDP Cache
- Browser History
- NTUSER.DAT (*Profile User*)
- SOFTWARE, SYSTEM (*Windows\System32\config*)

Collect + 20 Artifacts - Automated Forensics Collection
https://github.com/Starke427/Windows-Forensics
https://ericzimmerman.github.io/#!index.md

5.3 Identificar y analizar

Perfilamiento realizado por CISA GOV - #StopRansomware: Akira Ransomware - 18 de Abril de 2024.

- Descubrimiento:

```
nltest /dclist - nltest /DOMAIN_TRUSTS - net group "Domain admins" /dom - net localgroup "Administrators" /dom (+ 100 comandos)
```

- Acceso a Credenciales:

```
cmd.exe /Q /c esentutl.exe /y - powershell.exe -Command "Get-WmiObject Win32_Shadowcopy | Remove-WmiObject" -
"C:\Users\<username>\AppData\Roaming\Mozilla\Firefox\Profiles\<firefox_profile_id>.default-release\key4.db" /d
```

- Procesos de Exfiltración y Comunicación Alternativa:

```
ipscan-3.9.1-setup.exe - winrar-x64-623.exe - sshd.exe - VeeamHax.exe - WinSCP-6.1.2-Setup.exe - Rclone.exe - Sysmon.exe -
Cloudflarered.exe - PsExec.exe, Psexesvc.exe, Veeam-Get-Creds.ps1
```

6.1 Exfiltración de Información

- Las organizaciones confían en las soluciones **RMM** (*Remote Monitoring & Management*) para las operaciones típicas de TI.
- Es posible comprometer equipos sin levantar sospechas inmediatas entre los usuarios o el personal de TI (por el uso típico en el día a día).
- Ofrecen una gran capacidad para ***establecer conexiones remotas, transferir herramientas, ejecutar comandos o scripts y supervisión del sistema.***

6.2 Exfiltración de Información

- Rutas de Instalación
- Artefactos Forenses (Prioridad: Logs Nativos RMM - Network Artifacts)
- Detecciones
  - https://lolrmm.io/ - https://github.com/magicsword-io/LOLRMM

Action1	Panaorama	GetScreen	Sorillus	N-Able
AeroAdmin	Parsec	GoToMyPC GoToAs	Splashtop	Naverisk
AirDroid	PCVISIT	Goverlan	SpyAgent	Domotz
Alpemix	PhoneMyPc	Guacamole	Sunlogin	DWserviceDWAAgent?
AmmyyAdmin	Pocket Controller	Honeywell TotalCor	SuperOps	Electric
AnyDesk	PPDQ	HopToDesk	Supremo	Ericom AccessNow
Anyplace	Pulseway	hVNC	Surfly	FastViewer
AnyViewer	QuickAssist	Imperius	SynCro	Fixme.it
ASG Remote Desktop	RAdmin	Impero	Synergy	FleetDeck.io
Atera	Remote Manaulpator	Intel EMA	TacticalRMM	rudesk
Awsun	Remote Utiliies	IntelliAdmin	Take Control	ScreenConnect
Barracuda	Remotely	ISL Light	TeamViewer	Screenhero
BeAnywhere	RemotePC	Itarian	TightVNC	ScreenMeet
ChromeRDP	RemoteUtilities	Kaseya	tmate.io	ServerEye
ConnectWise	Remotix	Landesk	todesk	ShowMyPC
Continuum	Rexec	Level.io	TrendMicro Basecamp	SightCall
CrazyRemote	Rport	LiteManager	UltraViewer	MobaXterm
DameWare	Rsocx	LogMeIn	Viewabo	MoboRobo
Datto RMM (Formerly CentralStage)	Rsupport	ManageEngine RMM	Webroot SecureAnywhere	MRemoteNG
DeskShare	RustDesk	MeshCentral	Xeox	MSP360
Ngrok	NetSupport	NCentral	XMReality	NinjaOne
Zoho	ZeroTier	Optitune	Yoics	NinjaRMM

7.1 Materialización del Evento y Análisis

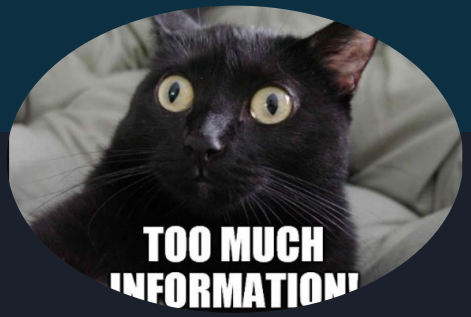
Qué servicios y herramientas para compartir/transferir información permito en mi red?

Podría detectar en donde se intenta utilizar determinadas aplicaciones y generar alertas en caso de ser observadas?

Preguntas para su análisis

Hago evaluaciones periódicas sobre las políticas de navegación? Hago un monitoreo sobre los cambios en dichas políticas y/o reglas?

Podría acceder y analizar los componentes de logs de dichas aplicaciones?



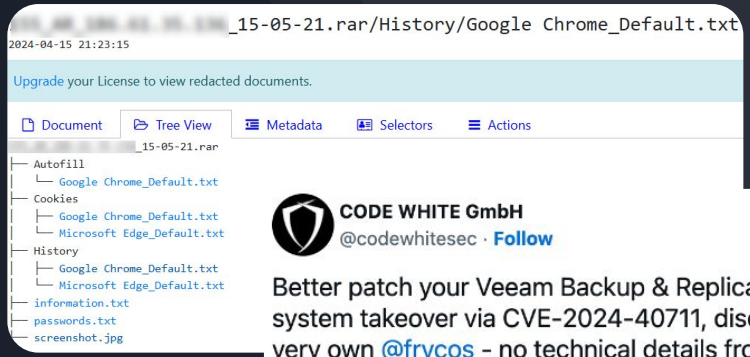
7.2 Materialización del Evento y Análisis

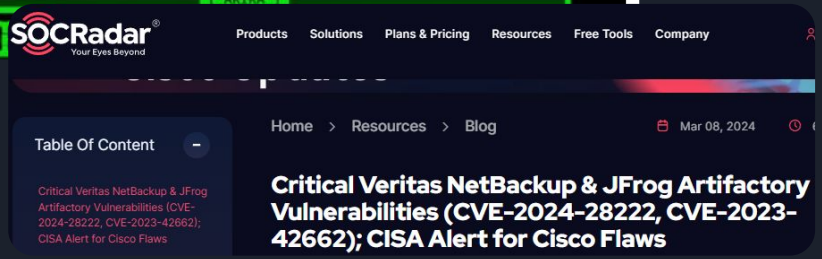
- **Identificar y familiarizarse** con los eventos o comportamientos ***habituales.***
- El objetivo es ***identificar patrones*** en las conexiones (*tráfico*) potencialmente anómalas.

- ➔ Transferencias realizadas (*bytes*)
- ➔ Usuarios autorizados según perfil de navegación
- ➔ Conexiones bloqueadas y permitidas
- ➔ Horarios poco habituales
- ➔ Orígenes de conexión (geografía)
- ➔ Nombres de host
- ➔ Políticas creadas y utilizadas
- ➔ Intentos de conexión a determinado segmento
- ➔ Puertos y servicio remotos

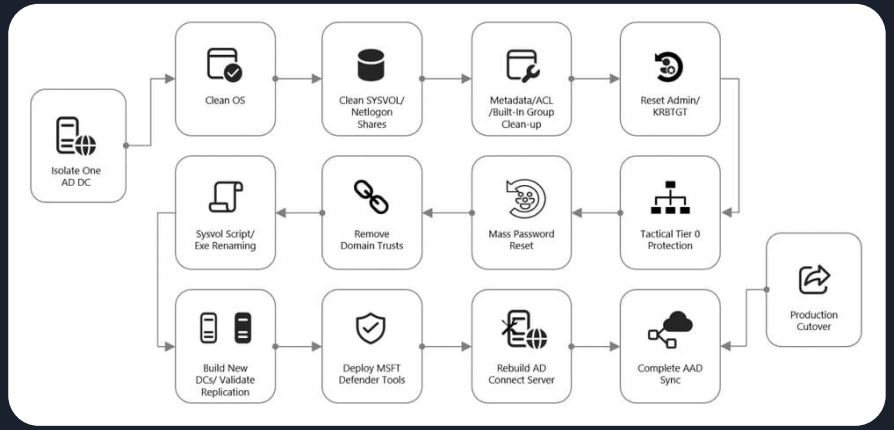
8.1 Eventos actuales

- Gestores de Backup
- Accesos VPN SSL Expuestos
- Tecnologías Virtualizadas
- Tecnologías de Seguridad Endpoint
- Vulnerabilidades Remotas (RCE)
- Info Stealers

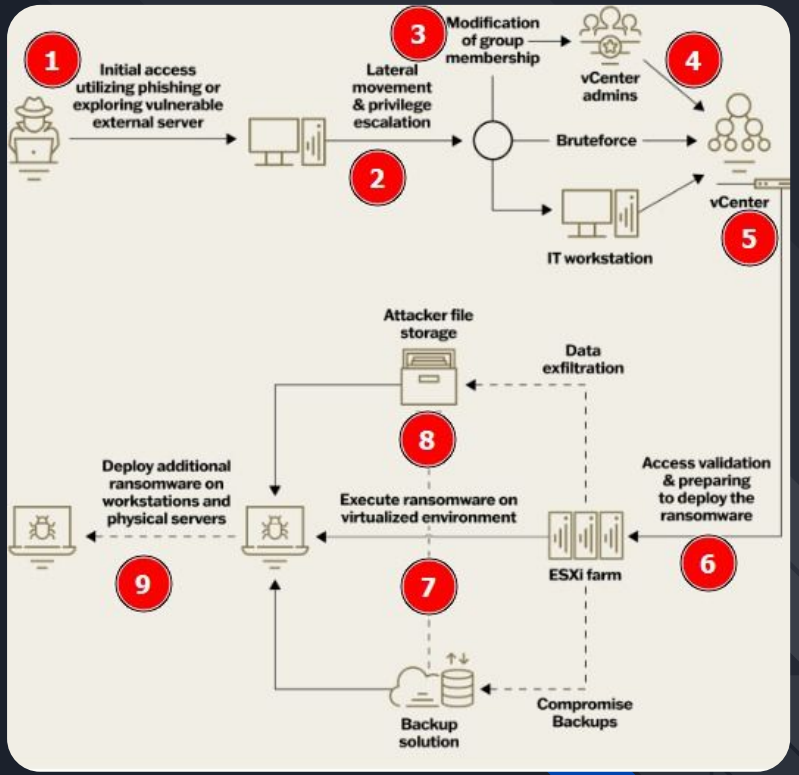




8.2 Eventos actuales



On-Premise Recovery AD Playbook

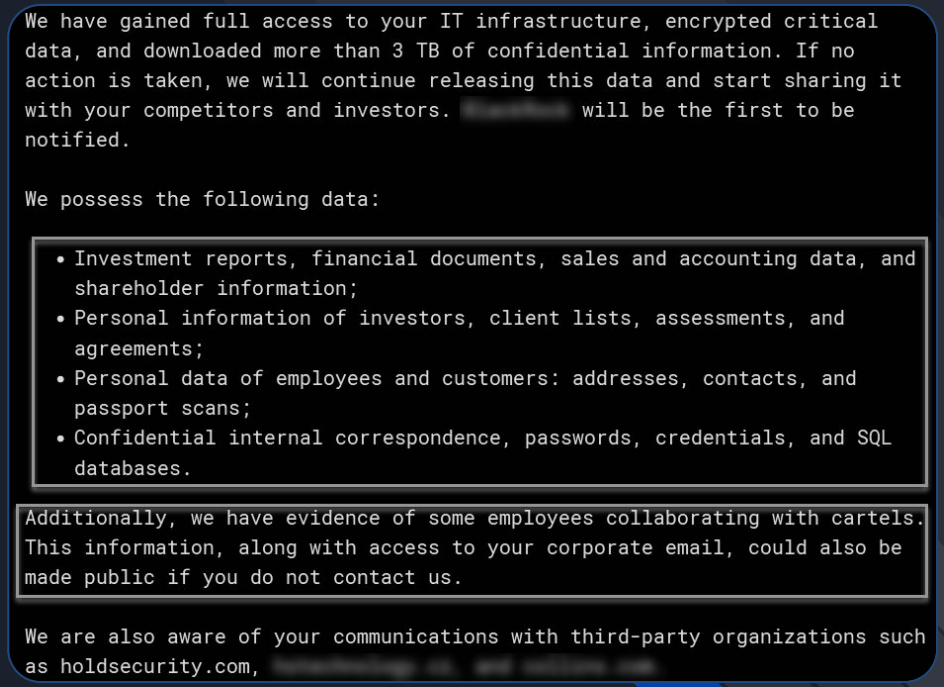


ESXi Ransomware Attack Kill-Chain

9.1 Negociación y Exposición

Motivos de Extorsión y/o Amenazas:

- Multas legales y gubernamentales.
- Evitar perder el tiempo y negociar urgente, “**por el bien del negocio**”.
- Amenazas con hacer público el evento a la competencia, entes reguladores o socios estratégicos.
- Amenazas con **reingresar a la red y exponer aún más datos** o directamente publican en su sitio nueva evidencia post-exposición**.**
- Ofrecen “combos” con determinados precios según la necesidad “del cliente”.
- Conocen el estado financiero al momento de negociar.



We have gained full access to your IT infrastructure, encrypted critical data, and downloaded more than 3 TB of confidential information. If no action is taken, we will continue releasing this data and start sharing it with your competitors and investors. [redacted] will be the first to be notified.

We possess the following data:

- Investment reports, financial documents, sales and accounting data, and shareholder information;
- Personal information of investors, client lists, assessments, and agreements;
- Personal data of employees and customers: addresses, contacts, and passport scans;
- Confidential internal correspondence, passwords, credentials, and SQL databases.

Additionally, we have evidence of some employees collaborating with cartels. This information, along with access to your corporate email, could also be made public if you do not contact us.

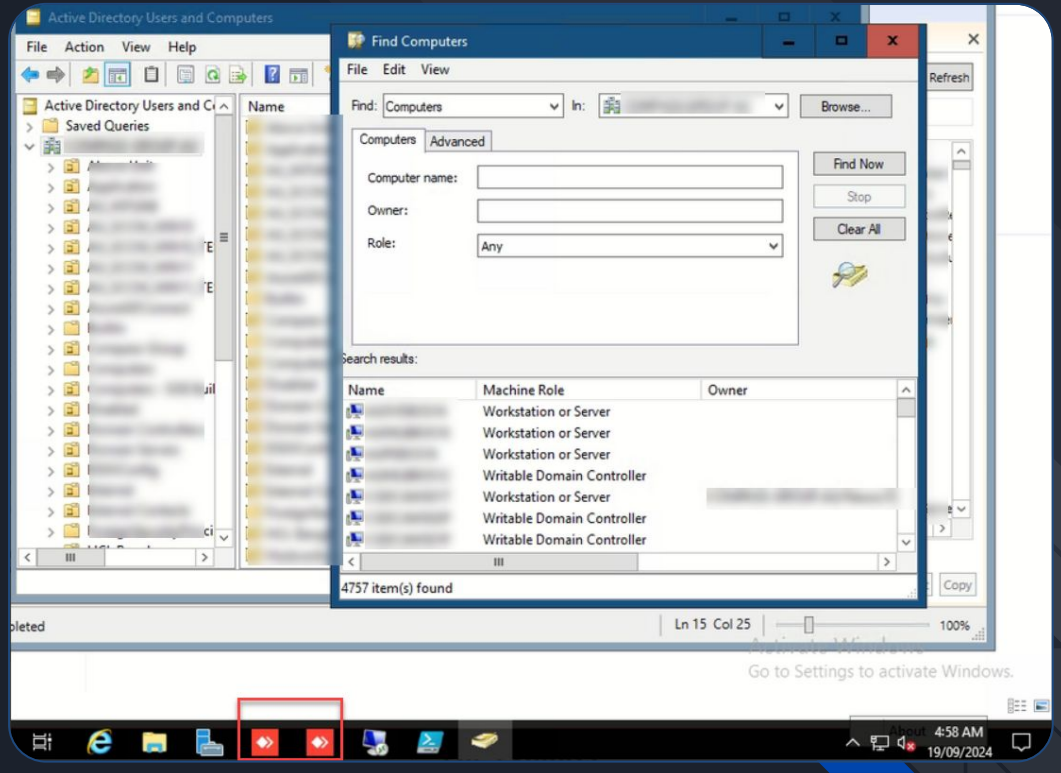
We are also aware of your communications with third-party organizations such as holdsecurity.com, [redacted]

RansomHub

9.2 Negociación y Exposición

[AnyDesk + ADExplorer] con estas herramientas es posible dumpear todos los objetos del AD y luego filtrarlos de la red.

La siguiente imagen corresponde a una publicación en el sitio del actor Medusa. **Volvieron a ingresar a la red de la víctima y publicaron nueva evidencia del acceso.**



Site Onion Medusa Ransomware - Imagen Extorsión

10. Conclusiones

- No es raro que el atacante tenga poca o **nula** experiencia técnica.
- Así como para defender buscamos las mejores herramientas el atacante hace lo mismo para concretar su operación.
- Prepararse de forma anticipada reduce los tiempos de respuesta en los escenarios de incidentes.
- Evalúe madurar sus procesos de monitoreo y detecciones en todas las tecnologías que le sea posible.
- Busque identificar sus procesos potencialmente débiles y establezca controles adicionales en sus líneas de defensa.