To Defend Against Ransomware, We Must Start By Understanding It. Vargas, Araneda

Preprint · July 2022

DOI: 10.13140/RG.2.2.11484.87689

2 authors, including:

Sebastian Alejandro Vargas Yañez
University Center CIFE
4 PUBLICATIONS **0** CITATIONS

SEE PROFILE

Para Defendernos Del Ransomware, Debemos Partir Por Entenderlo.

To Defend Against Ransomware, We Must Start By Understanding It.
Vargas, Araneda. (2021)

Autor Mg. Ing. Sebastián Vargas Alejandro Vargas Yañéz

mgsebastianvargas@gmail.com https://orcid.org/0000-0003-1782-3153

Presidente de Fundación Sochisi (La Serena, Chile)

Coautor Luis Alberto Araneda Villegas

Voluntario de Fundación Sochisi (Santiago, Chile)

Resumen

La problemática del manejo del ransomware inicia, cuando las organizaciones y profesionales, abordan el problema, sin analiza y entender las distintas variables a nivel de tácticas, técnicas y procedimientos, con ello se propone un análisis basado en Adversarial Tactics, Techniques, and Common Knowledge MITRE ATT&CK®, y con ello tomar decisiones basados en las amenazas informadas.

***Palabras clave*:**
Educación en ciberseguridad, Ransomware, Ciberataques, Contra medidas

Abstract

The problem of ransomware management begins when organizations and professionals approach the problem without analyzing and understanding the different variables at the level of tactics, techniques and procedures, thus proposing an analysis based on Adversarial Tactics, Techniques, and Common Knowledge MITRE ATT&CK®, and thus making decisions based on informed threats.

Keywords:
Cybersecurity education, Ransomware, Cyberattacks, Countermeasures.

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

1. INTRODUCCIÓN

Si iniciamos este whitepaper diciendo, ***"¡Hemos fallado!, ¿Cambiemos la estrategia?"*** Probablemente usted como lector pensaría de qué estamos hablando, es ahí donde en este artículo de revisión, profundizaremos en conceptos que hacen sentido y fundamentan la afirmación inicial.

Los ataques cibernéticos caen en un contexto más amplio que lo que tradicionalmente se llama, operaciones de información. Las Operaciones de información y el uso integrado de las principales capacidades de guerra electrónica, psicológica, red informática, artimañas militares y operaciones de seguridad en coordinación con apoyo especial y habilidades relevantes para penetrar, detener, destruir o secuestrar decisiones humanas, es una de las decisiones procesos de las instituciones nacionales (Li et al., 2020).).

1.1. Para comenzar, entendamos en su contexto, el concepto de Ransomware.

Dentro de la gran variedad de distintos códigos maliciosos existentes que pueden ser considerados como amenazas (spyware, virus, worms, adware, etc.) sin duda alguna, uno de los más peligrosos y devastadores (dependiendo del caso y la organización) sería el ransomware.

Sin duda un nombre particular para este tipo de aplicación, el cual está compuesto por dos palabras: Ransom, en inglés "rescate"" y Ware, contracción de "software", en este caso, un "software de secuestro electrónico".

Esa sería la definición común de este tipo de software, pero la definición "correcta" o adecuada al caso sería la siguiente:

“El ransomware es un programa malicioso diseñado para negar a un usuario u organización el acceso a los archivos de su propiedad. Al encriptar estos archivos (dejándolos inútiles, ya que no se pueden "abrir" debido al cifrado, por ende, no se pueden ejecutar ni leer) y exigir el pago de un rescate por la clave de descifrado, con ello los ciber atacantes colocan a las organizaciones en una posición en la que el pago del rescate es la forma más fácil y rápida de recuperar el acceso a sus archivos”.

Debido a la capacidad relatada en el párrafo anterior, una organización sin las medidas adecuadas, los recursos correctos y los planes de respuesta específicos a tal situación, puede verse completamente paralizada en su funcionamiento, causando estragos en todos sus niveles, si la infección es crítica, por ende con ello afectando completamente el funcionamiento de la organización y empresa, y por consecuencia del negocio; Impactándolos económicamente, operacionalmente y dependiendo del resultado de la infección, su credibilidad frente al público y otras entidades relacionadas con esta.

1.2. Incremento del ransomware en Chile

Chile como país, está resultando sumamente atractivo para las bandas de ciberdelincuentes, así como posibles "actores estatales tipo FIN", como campo fértil para posibles operaciones de estos adversarios, debido a la posición de polo tecnológico dentro de la región, la situación económica del país, el cual es constantemente reforzado por el aumento del capital humano, el nacimiento de nuevas empresas del sector, últimamente muy vinculadas a los servicios y a la banca digital (principalmente Fintech y "Cloud natives"), así como también la llegada e instalación de grandes multinacionales tecnológicas (AWS, Huawei, Microsoft, Oracle, etc.); hace que Chile sea un "excelente objetivo de ataque", ya que el mercado cibercriminal en su quehacer delictivo estudia los entornos y las víctimas, y se sabe, que el desarrollo de Latinoamérica, no llega a los niveles de otros polos (Israel, EEUU, Estonia, etc.), pero sí demuestra valor e inversiones sumamente altas, quizás no tan cercanas a las que se podrían generar en los países anteriormente mencionados, pero no por eso dejan de ser relevantes.

Los ataques de ransomware activados en el país, han afectado a organizaciones y empresas de diversos sectores; desde la banca (el más célebre fue el ataque en el año 2019, a empresas chilenas ligadas al sector financiero, por el actor conocido como "The Lazarus Group" (Hidden Cobra, APT 38, del cual hay antecedentes de su relación con el gobierno de Corea del Norte y se conoce su vinculación con una variedad de ransomware conocida como "VHD", pero también es conocida su técnica de data destruction como medio de eliminación de evidencia).

Se puede complementar el punto anterior, con la evidencia presentada en Panorama amenazas Kaspersky Latam 2021, el punto de ataques por país (número e incidencia).

2. DESARROLLO

Entonces, continuando el enunciado, hacíamos las cosas mal, pero ¿Qué significa esto?
Por qué seguimos pensando en ransomware como la acción final de la pérdida del dato mediante la encriptación de estos, desde una vista completa estaríamos apreciando el problema sólo con lo coloreado en rojo.

¿Tiene sentido? ¿Es pertinente? ¿Soluciona el problema?, ¿Lo entendemos? claramente no.

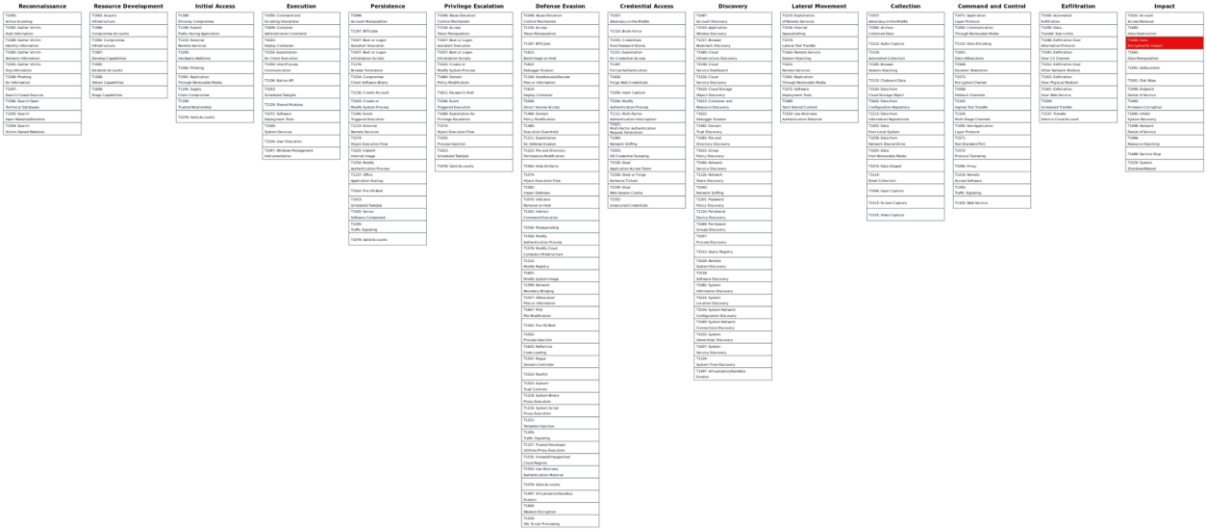

Ilustración 1 MITRE ATT&CK® v11- Mapa completo

Si sólo pensáramos en las consecuencias técnicas finales, el problema seguiría viéndose de forma parcelada, sin siquiera acercarnos al origen del problema que es el desconocimiento, inclusive si tuviéramos un DRP (Disaster Recovery Plan) bien estructurado que nos permitiese solucionar el problema del acceso a los datos, esto solo nos devolverá la continuidad operativa y parcial la single extortion, pero es ahí donde el problema comienza a revelarse,

¿Entendemos que la recuperación, no es intrínsecamente sinónimo de erradicación? con ello, sobre todo si no entendemos el KILL CHAIN de MITRE ATT&CK®, completo y tenemos soluciones a nivel de TTP (Tácticas, técnicas y procedimientos) para cada fase de este, podría darse el fatídico caso de la reinfección por Ransomware, puesto que no logramos mitigar el problema de raíz, y continua vivo.

Técnicamente esta táctica es conocida como TA0040 de Impact, y significa que el adversario intenta manipular, interrumpir o destruir sus sistemas y datos con propósitos maliciosos.
Entonces es ahí donde se incrementa el problema, puesto estamos viendo parcialmente, donde deberíamos ver el mapa completo.

Ilustración 2 MITRE ATT&CK® v11 - Táctica de impacto

Sigamos bajando un nivel más, simplemente pensemos en técnicas comunes como son:

T1486 Data Encrypted for Impact: Los adversarios pueden cifrar datos en los sistemas objetivo o en un gran número de sistemas en una red, para interrumpir la disponibilidad de los recursos del sistema y de la red.

Pueden intentar hacer inaccesibles los datos almacenados, cifrando archivos o datos en unidades locales y remotas y reteniendo el acceso a una clave de descifrado.

Esto puede hacerse para obtener una compensación monetaria de la víctima, a cambio del descifrado o de una clave de descifrado (ransomware) o para hacer que los datos sean permanentemente inaccesibles en los casos en que la clave no se guarde o transmita.

Para analizar este escenario se realizará una agrupación entre un grupo APT y un grupo FIN, dentro de la muestra seleccionada serán los adversarios:

G0082 APT38 es un grupo de amenazas patrocinado por el estado de Corea del Norte que se especializa en operaciones cibernéticas financieras; se ha atribuido a la Oficina General de Reconocimiento. Activo desde al menos 2014, APT38 se ha dirigido a bancos, instituciones financieras, casinos, intercambios de criptomonedas, puntos finales del sistema SWIFT y cajeros automáticos en al menos 38 países en todo el mundo. Las operaciones significativas incluyen el atraco al Banco de Bangladesh en 2016, durante el cual APT38 robó $ 81 millones, así como ataques contra Bancomext (2018) y Banco de Chile (2018); Algunos de sus ataques han sido destructivos.

El cual para graficar la problemática procederemos a identificar según las técnicas tácticas y procedimientos identificados.

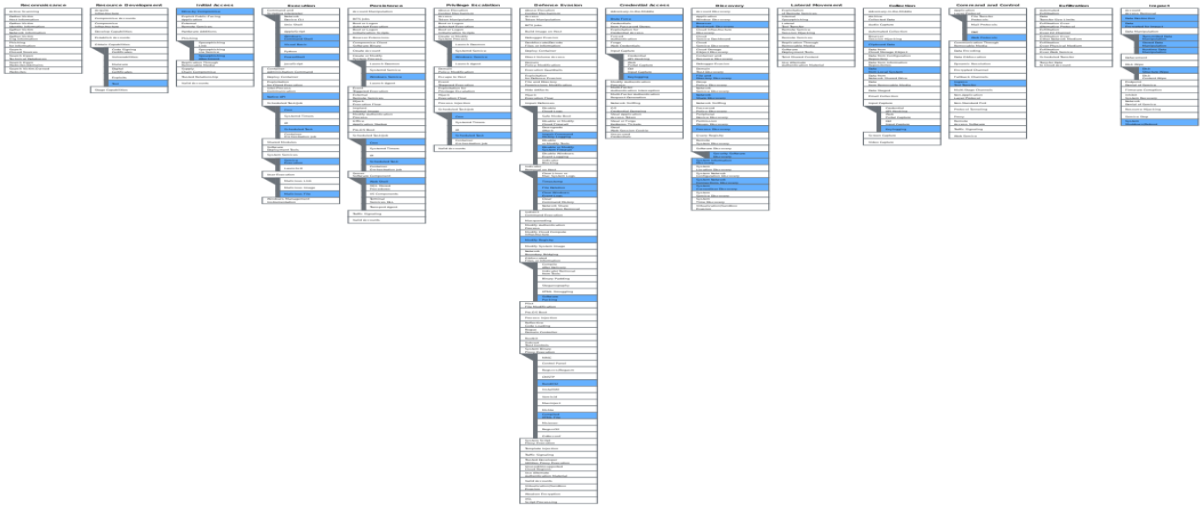

Ilustración 3 MITRE ATT&CK® v11 - APT 38

Como se puede apreciar en la imagen 3, para conseguir generar acciones efectivas frente a ese nivel de atacante, tenemos que pensar en cada una de las tácticas, podemos decir que desde el acceso inicial tenemos opciones de poder detener el ataque.

Como hemos visto hasta ahora el origen del problema radica en la forma que intentamos abordar el Ransomware, entendiéndolo parcialmente y pensando que todos los actores de amenaza utilizaran las mismas técnicas, tácticas y procedimientos.

G0046 FIN7

FIN7 es un grupo de amenazas motivado financieramente que ha estado activo desde 2013 y se dirige principalmente a los sectores minorista, de restaurantes y hotelero de EE. UU., a menudo utilizando malware de punto de venta.

Una parte de FIN 7 se quedó sin una empresa de fachada llamada Combi Security. Desde 2020 , FIN 7 cambió las operaciones a un enfoque de caza mayor (BGH) que incluye el uso de REvil ransomware y su propio Ransomware as a Service (RaaS), Darkside. FIN7 puede estar vinculado al Grupo Carbanak , pero parece que hay varios grupos que usan el malware Carbanak y, por lo tanto, se rastrean por separado

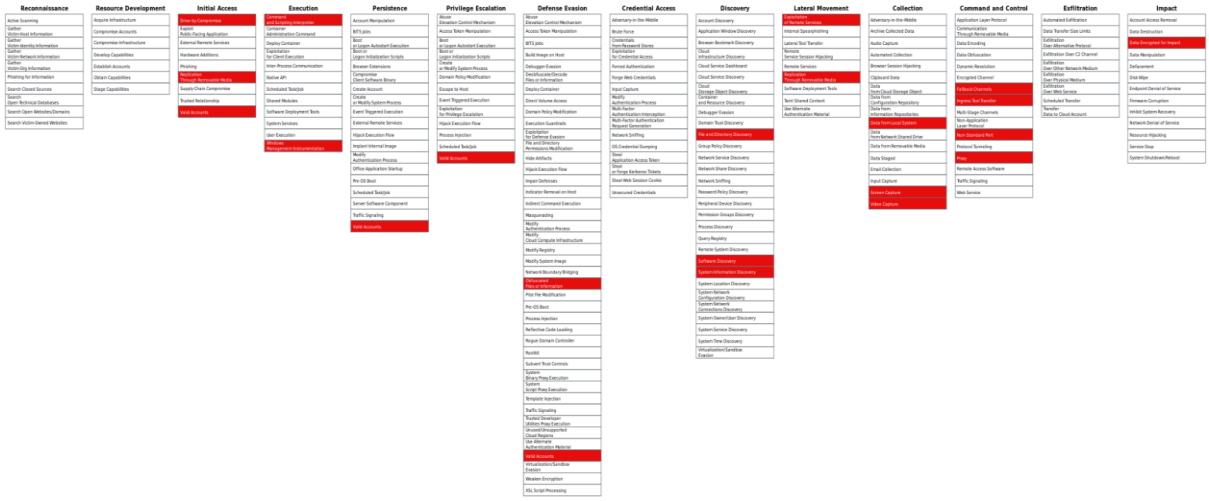

Ilustración 4 MITRE ATT&CK® v11 grupo FIN7

Podemos entender que existen marcadas diferencias en sus TTP, realizando un ejercicio de agregación.

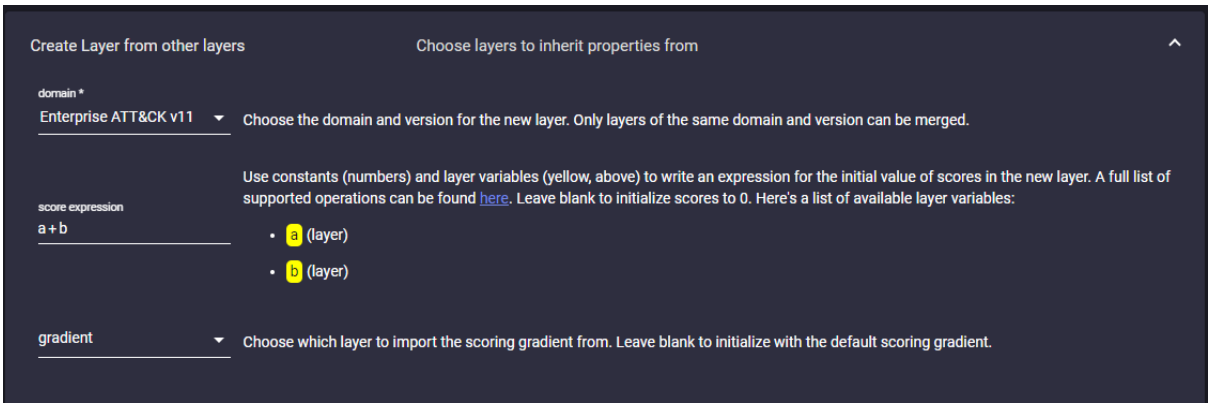

Ilustración 5 MITRE ATT&CK® v11- Agregación de APT 38 y FIN 7

Ilustración 6 MITRE ATT&CK® v11 - Mapa de relaciones en la agregación de APT 38 y FIN7

A continuación, podemos visualizar que las Tácticas, Técnicas y procedimientos, asociadas a la agrupación de los grupos APT38 Y FIN7 son los siguientes:

Tabla 1 MITRE ATT&CK® v11- TABLA de relaciones en la agregación de APT 38 y FIN7

Grupos	**Técnicas totales**
• APT38	17
• FIN7	16
• TÉCNICAS EN COMÚN	3

Continuando con lo obtenido, como resultado podemos ver que solo 3 técnicas existen en común entre ambos grupos criminales, las cuales a continuación se presentan:

2.1.1.1. ID: T1005 Datos del sistema local

Los adversarios pueden buscar fuentes del sistema local, como sistemas de archivos y archivos de configuración o bases de datos locales, para encontrar archivos de interés y datos confidenciales antes de la exfiltración.

2.1.1.2. T1105 Transferencia de herramienta de ingreso

Los adversarios pueden transferir herramientas u otros archivos desde un sistema externo a un entorno comprometido. Las herramientas o los archivos se pueden copiar desde un sistema externo controlado por el adversario a la red de la víctima a través del canal de comando y control o mediante protocolos alternativos como ftp. Una vez presentes, los adversarios también pueden transferir/difundir herramientas entre los dispositivos de la víctima dentro de un entorno comprometido (es decir, transferencia lateral de herramientas).

2.1.1.3. T1486 Datos cifrados para impacto

Los adversarios pueden cifrar los datos en los sistemas de destino o en una gran cantidad de sistemas en una red para interrumpir la disponibilidad de los recursos del sistema y de la red.

Pueden intentar hacer que los datos almacenados sean inaccesibles cifrando archivos o datos en unidades locales y remotas y reteniendo el acceso a una clave de descifrado. Esto se puede hacer para obtener una compensación monetaria de una víctima a cambio del descifrado o una clave de descifrado o para hacer que los datos sean permanentemente inaccesibles en los casos en que la clave no se guarde o transmita.

Los resultados demuestran claramente que seguir hablando de la generalidad tiene 0 impacto positivo, puedo decir que si no pasamos del ransomware a hablar de la banda específica con los TTP específicos será muy difícil poder tomar las acciones adecuadas.

2.2. Exfiltración de datos

Donde el Plan de recuperación de desastres o DRP no tiene poder es en las tácticas de exfiltración.

2.2.1. TA0010 Exfiltración

El adversario intenta robar datos, dicha exfiltración consiste en técnicas que los adversarios pueden utilizar para robar dichos datos desde la red. Una vez que han recogido los datos, los adversarios suelen empaquetarlos para evitar su detección. Esto puede incluir la compresión y el cifrado. Las técnicas para sacar o exfiltrar los datos de una red objetivo suelen incluir la transferencia de estos a través de su canal de mando y control o de un canal alternativo y también pueden incluir la puesta de límites de tamaño en la transmisión.

Si pensamos en ello, tendríamos como los ataques más peligrosos relacionados a las tácticas de Exfiltración.

2.2.1.1. T1041 Exfiltración a través del canal C2

Los adversarios pueden robar datos exfiltrándolos a través de un canal de mando y control existente.

2.2.1.2. T1567 Exfiltración a través de un servicio web

Los adversarios pueden utilizar un servicio web externo existente y legítimo para exfiltrar datos en lugar de su canal de mando y control principal.

2.2.1.3. T1537 Transferencia de datos a una cuenta en la nube:

Los adversarios pueden exfiltrar datos transfiriéndolo, incluidas las copias de seguridad de los entornos en la nube, a otra cuenta en la nube que controlen en el mismo servicio, para evitar las típicas transferencias/descargas de archivos y la detección de la exfiltración basada en la red.

Finalmente, las técnicas de MITRE ATTACK® V11, son las más comunes de un universo conocido de 13 técnicas finales. Sólo estas 3 a nivel de Ransomware y su impacto técnico han puesto de cabeza organizaciones completas en Chile y también en otras locaciones del mundo.

2.3. Las nuevas formas de rescate del ecosistema criminal

2.3.1. RaaS - Ransomware como Servicio

Ransomware as a Service

Según Meland, P. H., Bayoumy, Y. F. F., & Sindre, G. (2020). *El ransomware es una epidemia que afecta negativamente a la vida tanto de los particulares como de las grandes empresas, donde los delincuentes exigen pagos para liberar los activos digitales infectados. A raíz del éxito del ransomware, el ransomware como servicio (RaaS) se ha convertido en una franquicia que se ofrece a través de los mercados de la darknet, lo que permite a los aspirantes a ciberdelincuentes participar en esta dudosa economía.*

2.3.2. IABP - Corredores de acceso inicial

Initial-Access Brokerage Spike

Los corredores de acceso inicial son una suerte de cerrajeros, que actúan de forma oportunista, con trabajos a demanda o pedido, y al mejor postor, estos desde ahora conocidos como IAB se dedican a generar los accesos iniciales que los operadores de Ransomware necesitan.

En la mayoría de los casos, los atacantes identifican a las víctimas que tienen el ID: T1563.002 Remote Service Session Hijacking: RDP Hijacking o ID: T1190 Exploit Public-Facing Application, pero también software tipo VPN, y credenciales de acceso para sobre de administración remota.

Una vez que encuentran su punto de apoyo inicial, los corredores de acceso inicial exploran cuidadosamente la red ID: TA0007 ID: TA0007

Pueden también aplicar las tácticas de ID: TA0004 Privilege Escalation o ID: TA0008 Lateral Movement para ver a cuántos datos pueden acceder. Con esto completo, organizan su

información de acceso, la empaquetan en un producto presentable y calculan cuánto dinero les puede hacer ganar en la clandestinidad criminal.

Según Bankinfosecurity "E*stos listados se pueden encontrar en todos los foros criminales. Para el período comprendido entre el 1 de julio de 2020 y el 30 de junio, Kela informa que el precio promedio para el acceso remoto a una red fue de USD 5400, mientras que el precio medio fue de USD 1000".*

Finalmente, para poder ejemplificar el cambio de paradigma, desde la técnica inicial del adversario de pedir un rescate se han añadido cuatro fases posteriores que a continuación se enumeran.

1. **Extorsión Simple**
   Objetivo: Encriptación de Archivos
2. **Extorsión Doble**
   Objetivo: Exfiltración de datos
3. **Extorsión Triple**
   Objetivo: Denegación de servicio
4. **Extorsión Cuádruple**
   Objetivo: Contactar con los clientes de las víctimas y las partes interesadas
5. **Extorsión Quíntuple**
   Objetivo: Contactar con los competidores de las víctimas

2.4. Contramedidas

2.4.1. A nivel de mitre ransomware top ten

El Centro para la defensa informada sobre amenazas creó una lista de las 10 técnicas principales de ATT&CK para el ransomware. Esta lista puede servir como punto de partida para priorizar las técnicas de ATT&CK al planificar la defensa contra los ataques de ransomware.

Nuestros esfuerzos deberían estar pensados en poder resolver y mitigar las problemáticas asociadas a los TTP que se presentan a continuación.

1. T1486: Data Encrypted for Impact
2. T1490: Inhibit System Recovery
3. T1027: Obfuscated Files or Information
4. T1047: Windows Management Instrumentation
5. T1036: Masquerading
6. T1059: Command and Scripting Interpreter
7. T1562: Impair Defenses
8. T1112: Modify Registry
9. T1204: User Execution
10. T1055: Process Injection

2.4.2. Análisis de brechas de amenazas informadas

- ¿Cuáles son nuestras *Joyas de la Corona*?
- ¿Con qué contamos para defendernos a nivel estratégico, táctico y técnico?
- ¿Qué TTP tenemos alta confianza de poder detectar?
- ¿Qué TTP tenemos mediana confianza de poder detectar?
- ¿Qué TTP tenemos baja confianza de poder detectar?
- ¿Quién buscaría atacarnos?
- ¿Existen industrias, empresas cercanas que hayan sido víctimas ya?
- ¿Cuántas alertas somos capaces de gestionar por día, semana, mes?
- ¿Cuántos minutos podemos destinar a cada alerta?
- ¿Tenemos definidos los playbooks de respuesta a incidentes?

2.4.3. Estrategias de ciberseguridad

2.4.3.1. Táctico

Las organizaciones deben adoptar un enfoque proactivo que incluya protección de endpoints, redes y nube en tiempo real, incluida la detección automatizada de amenazas y la respuesta con inteligencia artificial. Todo con un enfoque de Zero Trust Access (ZTA) o del tipo Cybersecurity Mesh Architecture (CSMA).

2.4.3.2. Técnico

- Aumentar el monitoreo de tráfico no usual (incluyendo del tráfico DNS)
- Mantener los equipos actualizados, tanto sistemas operativos como otros softwares instalados.
- Generar o aumentar las campañas de concientización o Security Awareness dentro de las organizaciones
- Verificar y controlar los servicios de escritorio remoto (RDP).
- Bloqueo de script o servicios remotos no permitidos a través de políticas de grupo (GPO).
- Monitorear servicios SMB de forma horizontal en la red.
- Mantener actualizados las protecciones perimetrales de las instituciones
- Control de versiones en Hardware de redes a nivel de firmware.Aumentar los niveles de protección en los equipos que cumplan las funciones de AntiSpam, WebFilter y Antivirus. Control periodico, y alineación con política (auditable y controlable).
- Verificar el funcionamiento, y si no es necesario, bloquear las herramientas como PsExec y Powershell.
- Segmentar las redes en base a las necesidades de sus activos, permitiendo solamente los puertos necesarios a utilizar. Consideración especial en Ambientes OT sin segmentación aplicada.
- Monitorear los procesos de sistemas operativos
- Monitorear las tareas programadas. de sistemas operativos
- Restringir o eliminar protocolos de comunicación deprecados o inseguros
- Probar la efectividad de los controles implementados en forma periódica.

3. Conclusión

Pensar en un solo camino de la verdad es imposible, debemos tomar un enfoque proactivo basado en el **modelamiento informado de amenazas**, pero también ocupar los sistemas tradicionales de evaluación de impacto, para identificar dónde están las "*joyas de la corona*" que deseamos proteger. Los esfuerzos son imposibles de llevar si no es de una forma priorizada, ordenada y realista.

Al entender la cadena del ataque completa, entender que existen distintos grupos criminales y no una forma única de ser víctimas de un ransomware, es ahí donde radica las principales conclusiones de este ejercicio, el nuevo paradigma no trata solo de atender el impacto, los análisis de impacto al negocio ya existen hace décadas, no basta también solo con enfocarse en la recuperación, puesto con lo visto con los planes de recuperación de desastres y los planes de recuperación del negocio son Basic incluso higiénicos que no revisten un nuevo análisis ya deben estar. Podemos recuperarnos de un TTP especifico, pero eso no es garantía de erradicación de la amenaza o incluso una superación de la amenaza, debemos enfocarnos en entender el ecosistema hostil en el cual hoy las operaciones de las distintas organizaciones nacionales, mundiales se llevan a cabo y con ello dejar de generalizar todo al nombrarlo como la técnica final cuando el adversario, levanto la acción de rescate, y enfocarnos en los sistemas proactivos de mitigación antes de que la acción hostil sea realizada.

4. Bibliografía

Grief Gang's New Quadruple Extortion Scheme Doesn't Change the Game. (n.d.). Retrieved June 14, 2022, from https://www.cybereason.com/blog/ceo-series/grief-gangs-new-quadruple-extortion-scheme-doesnt-change-the-game

Ransomware as a Service (RAAS). (n.d.). Retrieved June 14, 2022, from https://academy.picussecurity.com/path-player?courseid=ransomware-attacks-basics-ttps-countermeasures-free-course-training&unit=61d68e8aa065191c90128140Unit

BlackMatter Ransomware | CISA. (n.d.). Retrieved June 14, 2022, from https://www.cisa.gov/uscert/ncas/alerts/aa21-291a

CSIRT. (n.d.). Retrieved June 14, 2022, from https://www.csirt.gob.cl/noticias/comunicado07062020/

Disclosure of Chilean Redbanc Intrusion Leads to Lazarus Ties | Flashpoint. (n.d.). Retrieved June 14, 2022, from https://flashpoint.io/blog/disclosure-chilean-redbanc-intrusion-lazarus-ties/

REvil Ransomware Dirigido A Chile (Indicadores De Compromiso) | CronUp Ciberseguridad. (n.d.). Retrieved June 14, 2022, from https://www.cronup.com/revil-ransomware-dirigido-a-chile-indicadores-de-compromiso/

Chile sufrió más de 2.100 millones de intentos de ciberataques en el primer semestre del año - TrendTICTrendTIC. (n.d.). Retrieved June 14, 2022, from https://www.trendtic.cl/2021/09/chile-sufrio-mas-de-2-100-millones-de-intentos-de-ciberataques-en-el-primer-semestre-del-ano/

MITRE ATT&CK™ : Design and Philosophy | The MITRE Corporation. (n.d.). Retrieved June 14, 2022, from https://www.mitre.org/publications/technical-papers/mitre-attack-design-and-philosophy

Zero Trust, ZTA, and ZTNA: What's the Difference? | CSO Online. (n.d.). Retrieved June 14, 2022, from https://www.csoonline.com/article/3611341/zero-trust-zta-and-ztna-what-s-the-difference.html

Threat-Informed Defense | The MITRE Corporation. (n.d.). Retrieved June 14, 2022, from https://www.mitre.org/news/focal-points/threat-informed-defense

Meland, P. H., Bayoumy, Y. F. F., & Sindre, G. (2020). The Ransomware-as-a-Service economy within the darknet. *Computers and Security*, *92*. https://doi.org/10.1016/J.COSE.2020.101762

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/J.EGYR.2021.08.126

Initial Access Brokers Report. (n.d.). Retrieved June 14, 2022, from https://resources.digitalshadows.com/whitepapers-and-reports/initial-access-brokers-report

Meet the Middlemen Who Connect Cybercriminals With Victims. (n.d.). Retrieved June 14, 2022, from https://www.darkreading.com/threat-intelligence/meet-the-middlemen-who-connect-cybercriminals-with-victims

APT38, NICKEL GLADSTONE, BeagleBoyz, Bluenoroff, Stardust Chollima, Grupo G0082 | MITRE ATT&CK®. (n.d.). Retrieved June 14, 2022, from https://attack.mitre.org/groups/G0082/

FIN7, GOLD NIAGARA, ITG14, Carbon Spider, Grupo G0046 | MITRE ATT&CK®. (n.d.). Retrieved June 14, 2022, from https://attack.mitre.org/groups/G0046/

10 tendencias de agentes de acceso inicial: el servicio de ciberdelincuencia evoluciona. (n.d.). Retrieved June 14, 2022, from https://www.bankinfosecurity.com/cybercrime-enabler-initial-access-brokers-keep-evolving-a-17249

Ciberataques en América Latina crecen un 24% durante los primeros ocho meses de 2021 | Blog oficial de Kaspersky. (n.d.). Retrieved June 14, 2022, from https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/

Top ATT&CK Techniques. (n.d.). Retrieved June 15, 2022, from https://top-attack-techniques.mitre-engenuity.org/

5. **Autores**

Sebastián Alejandro Vargas Yáñez

Ingeniero Civil en informática, Ingeniero en Informática, Licenciado en Ciencias de la Ingeniería de Universidad Tecnológica de Chile, Ingeniero en Ciberseguridad de Instituto Profesional CIISA, Diplomado en Gestión de la Seguridad de la Información de Universidad Adolfo Ibáñez, Diplomado en Estrategia de Inteligencia de Cibercrimen y Diplomado en Ciberdelincuencia en Universidad del Norte Santo Tomás de Aquino, Magíster en Gestión de Tecnologías de la Información de Universitat Oberta Catalunya, Profesional Certificado en Certified Ethical Hacker (Practical) de EC-Council, eLearnSecurity Junior Penetration Tester, ATT&CK® Adversary Emulation Methodology Certification y ATT&CK® Cyber Threat Intelligence Certification de Mitre-Ingenuity, Digital Forensic & Incident Response de Hack by Security, Certificado en Auditor Líder ISO 27.001 de Capacitación Usach.

Actualmente cursando Doctorado en socioformación y Sociedad del Conocimiento, Centro Universitario CIFE: un Máster en Ciberguerra, Ciberterrorismo y Ciberseguridad de la Universidad Pegaso de Italia, un máster en Ciberseguridad Industrial en Centro de Ciberseguridad Industrial de España.

LinkedIn: https://www.linkedin.com/in/mgsebastianvargasyanez/

COAUTOR

Luis Alberto Araneda Villegas

OCI Tech Architect y Professional Cloud. Actualmente cursando ingeniería informática y Computación en la Universidad Andrés Bello, poseedor de un diploma avanzado en TI con mención en seguridad en redes, así como diversos cursos en Informática Forense, Seguridad de la Información, Ciberseguridad y otros. Apasionado de la tecnología (ha trabajado desde soporte técnico hasta arquitectura de sistema y estudiante de la SDL, Ciberseguridad, la arquitectura Cloud y la Ciencia de datos.

LinkedIn: https://www.linkedin.com/in/luis-araneda-ba07499/

Revisado por:

Fundación Sociedad Chilena de Seguridad de la información