Tratamiento de CIERRINCIDENTES

SIGESTIC'23

SEGU.INFO
SEGURIDAD DE LA INFORMACION

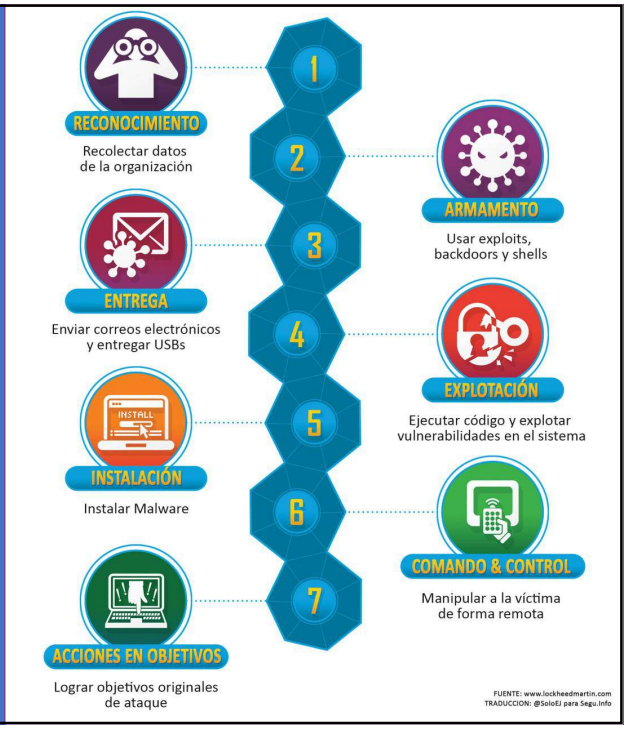
Lic. Cristian Borghello, CISSP – CCSK – CSFPC
www.segu-info.com.ar
info@segu-info.com.ar
@seguinfo

Sobre Cristian Borghello (AR)

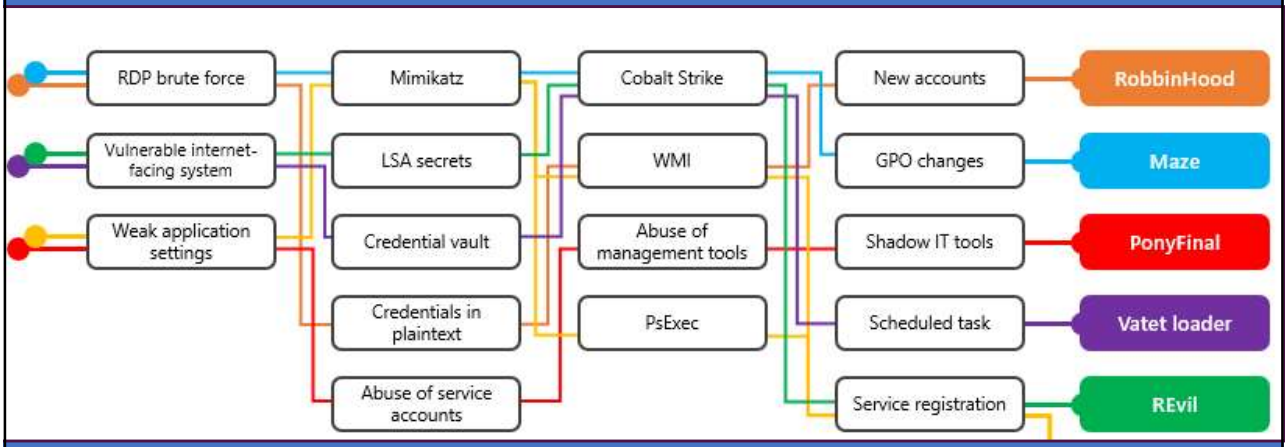
- Licenciado en Sistemas UTN desde 2000
- Desarrollador desde los 8 años
- CISSP *(Certified Information Systems Security Professional)*
- Microsoft MVP Security durante 10 años
- CCSK *(Certificate Cloud Security Knowledge)*
- CSFPC *(Certification Cyber Security Foundation)*
- Certificado en Ciberseguridad en Corea del Sur
- Profesor Universitario de Grado y Posgrado
- Consultor de Ciberseguridad de la ONU
- **Creador de Segu-Info, Segu-Kids, ODILA y Antiphishing.LA**

Cyber Kill Chain

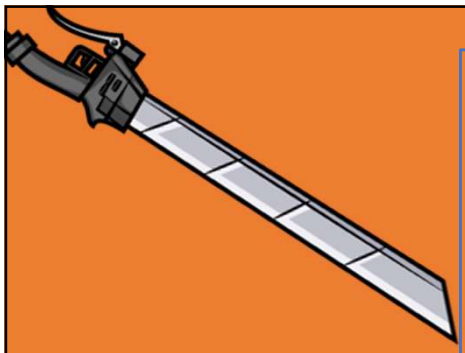
- **Kill Chain** es un modelo de ataque de los años noventa, desarrollado por la Fuerza Aérea de los Estados Unidos.
- La estrategia, conocida como **F2T2EA**, se basa en seis pasos para llevar a cabo una operación militar: encontrar *(Find)*, asegurar *(Fix)*; rastrear *(Track)*; elegir objetivo *(Target)*, abordar *(Engage)*, evaluar (Assess).
- A partir de esta secuencia de pasos, la empresa **LockheedMartin** propuso **Cyber Kill Chain**, una cadena de 7 pasos que describe cómo llevar a cabo ataques dentro de una organización.



Kill Chain del Ransomware



https://news.microsoft.com/es-xl/los-grupos-de-ransomware-continuan-dirigiendose-a-la-atencion-medica-y-a-los-servicios-criticos-aqui-les-decimos-como-reducir-el-riesgo/
https://blog.segu-info.com.ar/2021/02/los-sitios-de-los-principales.html



ATT&CK es una base de conocimiento con las Tácticas y Técnicas del adversario basada en observaciones del mundo real

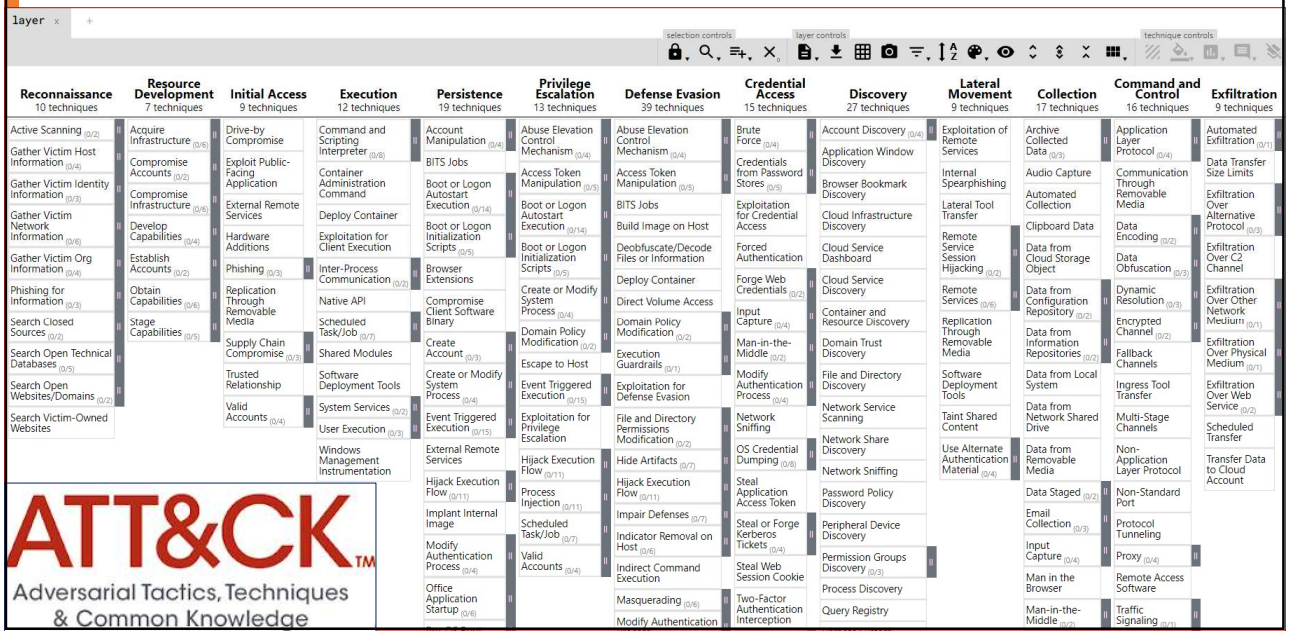
Conocer el comportamiento del atacante / actor (TTPs)

- Táctica: estrategias generales que utilizan los actores (qué)
- Técnicas: herramientas y/o métodos intermedios
- Procedimientos: descripción del paso a paso de cómo el atacante planea lograr su propósito

ATT&CK™
Adversarial Tactics, Techniques & Common Knowledge

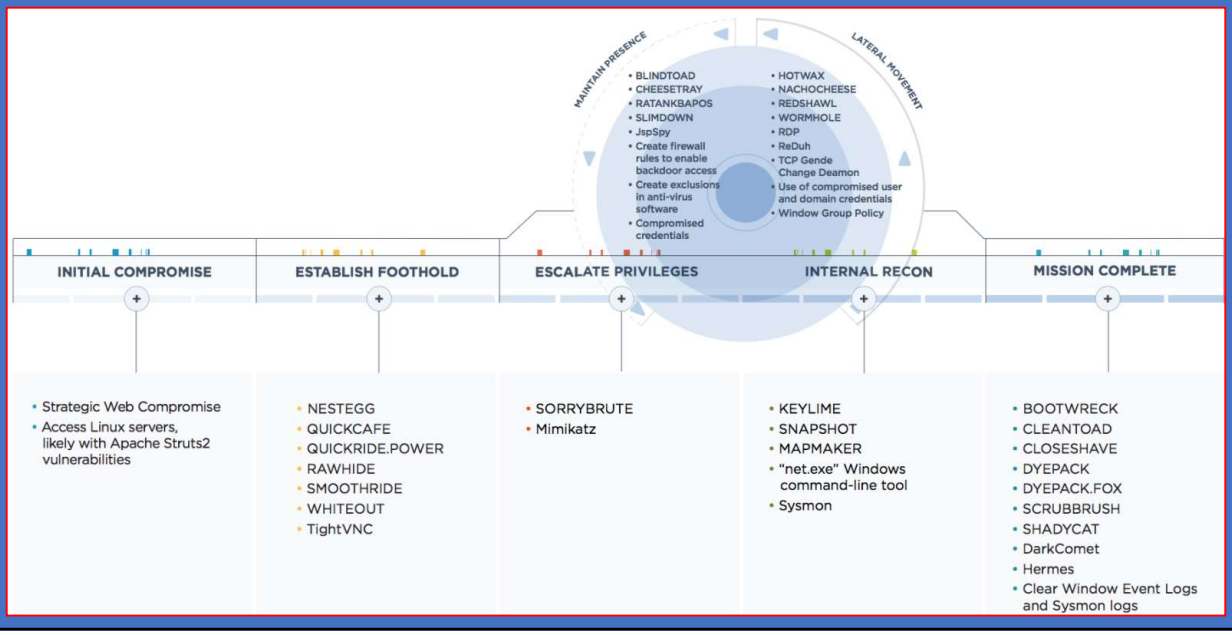
https://attack.mitre.org/

MITRE ATT&CK



Análisis de APT38

https://blog.segu-info.com.ar/2019/10/comenzar-usar-att-y-la-apt38.html



NIST CSF
CYBERSECURITY FRAMEWORK

I - ¿Qué procesos y activos necesitan protección?

P - ¿De qué contramedidas se dispone?

D - ¿Qué técnicas se utilizan para identificar incidentes?

R - ¿Qué técnicas se utilizan para contener incidentes?

R - ¿Qué técnicas permiten restaurar las capacidades?

Es una forma de pensar y un modelo sobre el cual organizar estrategias de defensa

https://www.nist.gov/cyberframework/framework

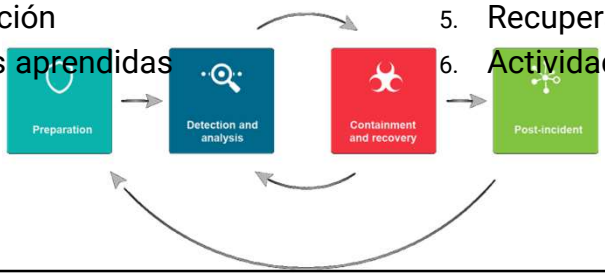
Fases de un Incidente

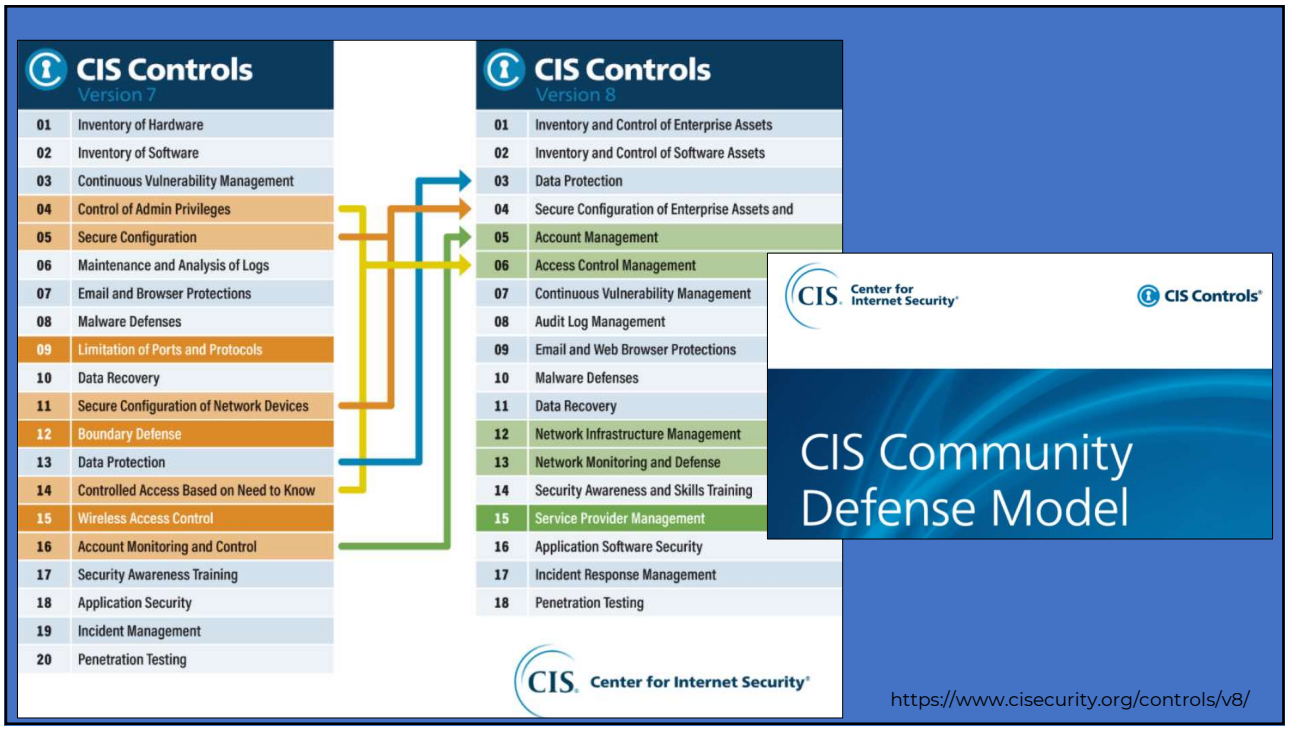
SANS PICERL

1. Preparación
2. Identificación
3. Contención
4. Erradicación
5. Recuperación
6. Lecciones aprendidas

NIST 800-61

1. Preparación
2. Detección y Análisis
3. Contención
4. Erradicación
5. Recuperación
6. Actividades Post Evento





Evolución continua

- El atacante siempre modifica sus técnicas para vulnerar controles (es su naturaleza)
- El comportamiento esperado es la modificación continua de las TTPs (por ej. Las APTs)
- Se debe implementar un modelo de madurez basado en las TTPs del atacante y la correlación de eventos
- Enfoque **TRIAGE**

Triage es el primer proceso de respuesta a incidentes. Es un proceso de clasificación de eventos que busca garantizar que solo las alertas válidas se promuevan al estado de "investigación"

Evento, Brecha e Incidente

EVENTO

Un suceso o tipo de cambio que no presenta resultados negativo para el negocio.

INCIDENTE

Evento de seguridad que compromete la CID de un activo de información.

BRECHA

Incidente que da como resultado la divulgación confirmada de datos a un tercero no autorizado.

Tienen connotación negativa

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
http://veriscommunity.net/veris-overview.html

Incidente

- **Un incidente es una amenaza para la organización y representa un riesgo potencial**

EXTERNO

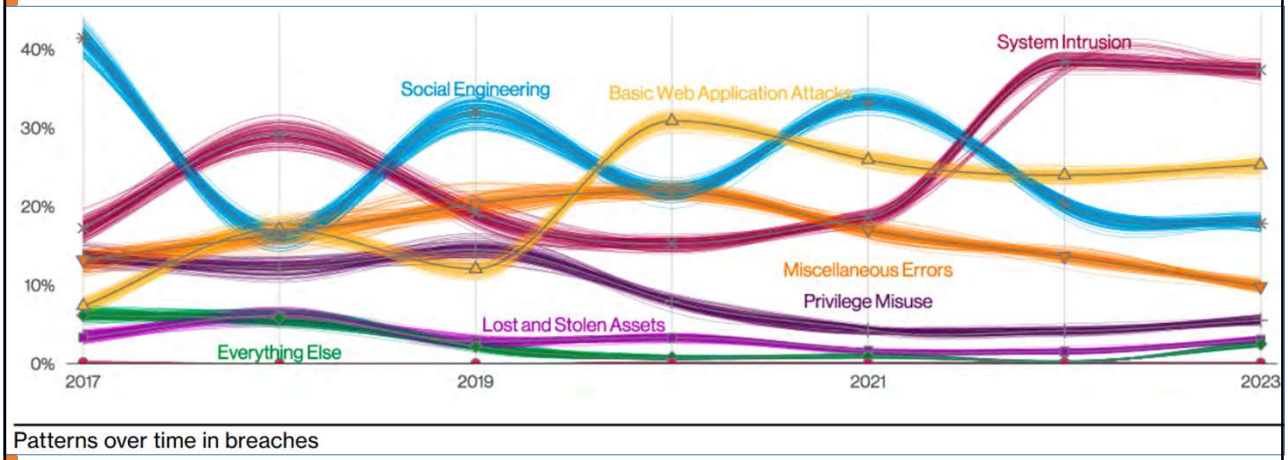
Se origina fuera de la red y es iniciada por actores maliciosos o delincuentes.

El atacante emplea varias tácticas para violar la red.

INTERNO

Se produce cuando una persona con información privilegiada provoca un incidente, al abusar de sus privilegios **(INSIDER)**

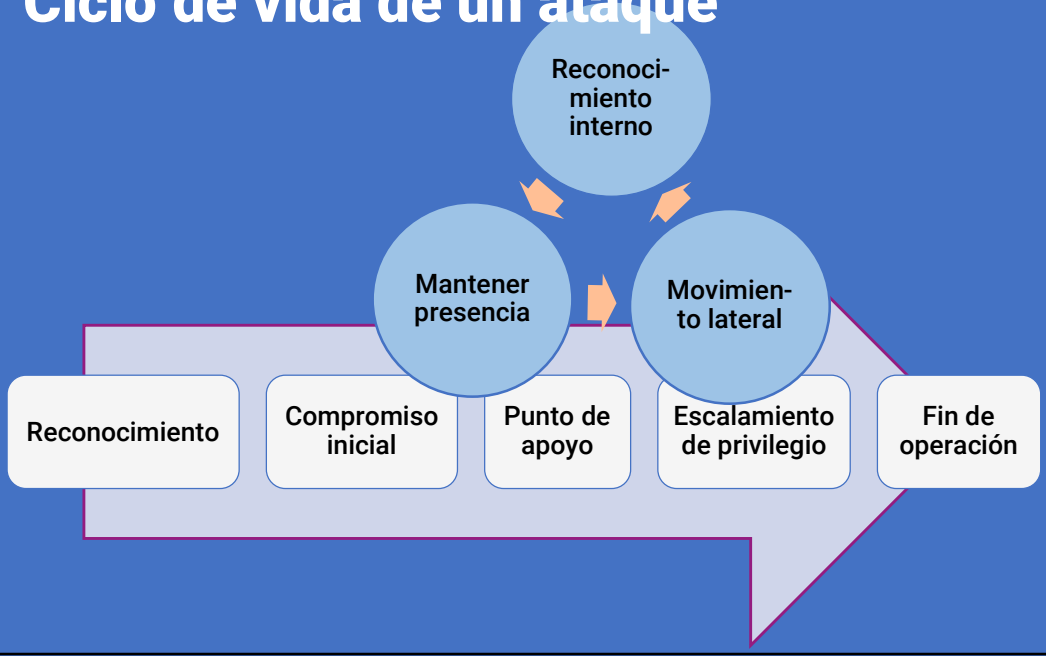
Brechas e Incidentes [DBIR]



Patterns over time in breaches

https://blog.segu-info.com.ar/2023/08/lo-siento-hubo-un-incidente-cuando.html

Ciclo de vida de un ataque

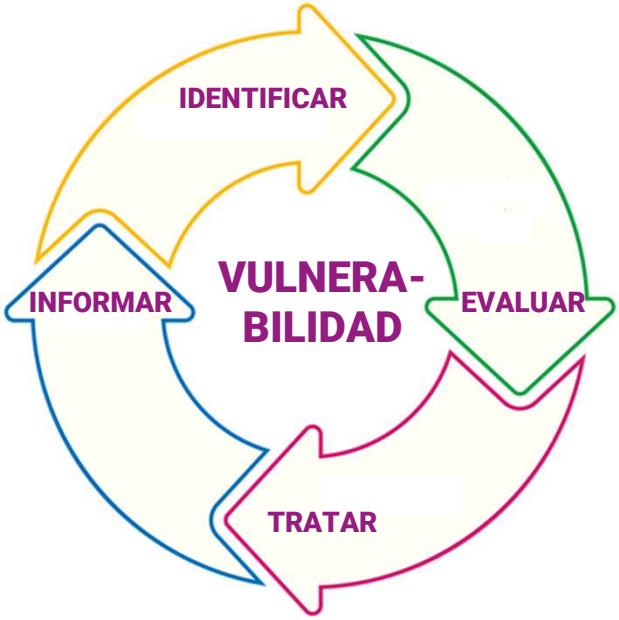


Gestión de Vulnerabilidades

Es el proceso de identificar, evaluar, tratar e informar sobre las vulnerabilidades de seguridad en los sistemas.

Es vital para que las organizaciones prioricen las posibles amenazas y minimicen su “superficie de ataque”.

Fases de la Gestión de Vulnerabilidades



Un Indicador de Compromiso (IoC) es un artefacto encontrado en un sistema que indica, con cierto grado de confianza, que el mismo ha sido comprometido. Es evidencia forense de posibles intrusiones en un sistema.

Los investigadores de seguridad utilizan IoCs para analizar las técnicas de ataque y obtener inteligencia de amenazas.

Se suelen compartir con la comunidad para mejorar la respuesta a incidentes y las estrategias de remediación.

IoCs comunes

- Direcciones IPs y URLs sospechosas
- Hashes conocidos
- Procesos o Servicios activos
- Tráfico de red inusual
- Irregularidades geográficas
- Cambios de configuración no autorizados
- Aplicaciones desconocidas en el sistema
- Actividad inusual de cuentas
- Solicitudes de permisos adicionales
- Solicitudes inusuales en servidores
- Archivos comprimidos
- Aumento en inicios de sesión
- Ataques de fuerza bruta
- Actividad anómala
- Aumento en el volumen en base de datos / logs
- Cambios sospechosos en archivos del sistema o registro
- Gran cantidad de solicitudes para el mismo archivo

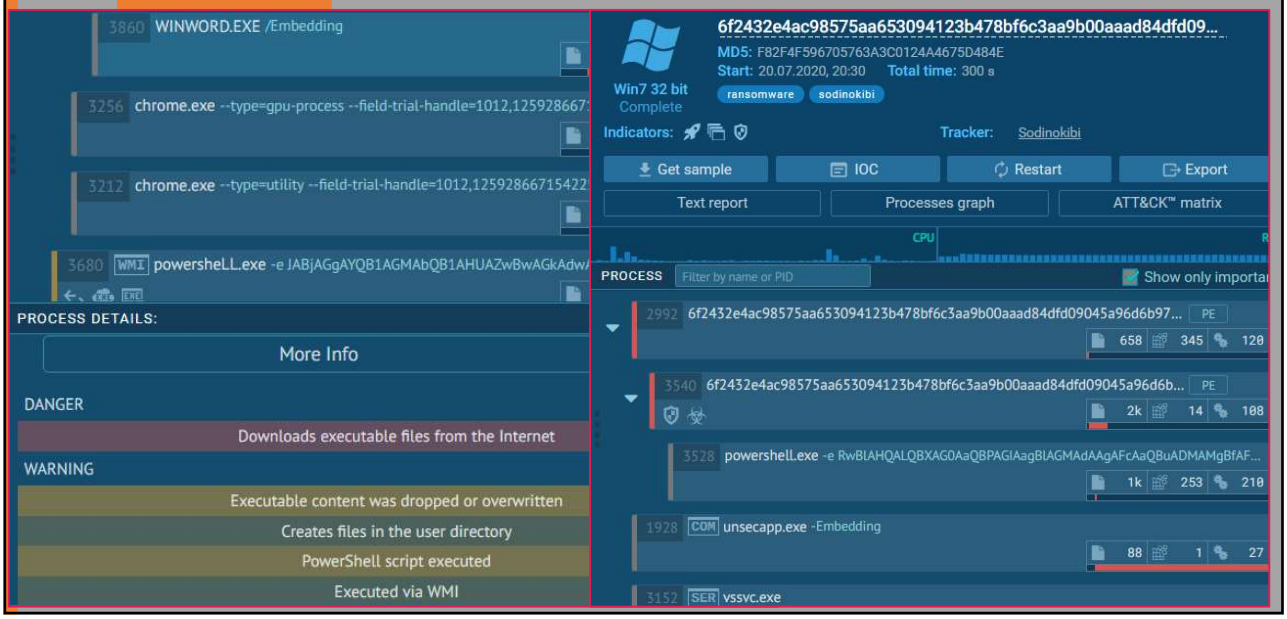
¡CORRELACIONAR!

IoCs de un malware

- Yara rules detected for file (2 events)
- Checks amount of memory in system, this can be used to detect virtual machines that have a low amount of memory available (1 event)
- One or more processes crashed (33 events)
- Changes read-write memory protection to read-execute (probably to avoid detection when setting all RWX flags at the same time) (1 event)
- Installs itself for autorun at Windows startup (33 events)
- Disables proxy possibly for traffic interception (1 event)
- File has been identified by 14 AntiVirus engine on IRMA as malicious (14 events)
- File has been identified by 57 AntiVirus engines on VirusTotal as malicious (50 out of 57 events)

Cadena de Ejecución

https://any.run



Medidas de Protección (SIN orden estricto)

- Firewall
- Web Proxy
- DLP
- IDS / IPS
- SIEM
- Files Sandboxing
- Email Security
- MFA
- Log Aggregation / Analysis
- Microsegmentación
- C2 Monitoring
- Threat Intelligence
- Antivirus / EDR
- Manejo de Privilegios
- White-Listing
- Integridad
- Data / Disk Encryption
- Patch Management
- Acceso Remoto / VPN
- Detección de Anomalías (*Baseline*)

Hardening (SIN orden estricto)

QUÉ

- Configuración de usuario
- Configuración de la red
- Configuración de roles y permisos
- Patching
- Configuración NTP
- Configuración de firewall
- Configuración de acceso remoto
- Configuración de servicios
- Configuración del SO
- Registro y monitoreo

PORQUÉ

- Proteger las credenciales
- Comunicaciones seguras
- Need to Know
- Solución de vulnerabilidades
- Sincronización de tiempos/reloj
- Minimizar la “huella externa”
- Acceso seguro
- Minimizar la superficie de ataque
- Proteger el SO y las aplicaciones
- Saber lo que sucede

Gracias!

SEGU.INFO
SEGURIDAD DE LA INFORMACION

SIGESTIC'23

Lic. Cristian Borghello, CISSP – CCSK – CSFPC
www.segu-info.com.ar
info@segu-info.com.ar
@seguinfo