

Tratamiento de CIERINCIDENTES



Lic. Cristian Borghello, CISSP – CCSK – CSFPC
www.segu-info.com.ar
info@segu-info.com.ar
[@seguinfo](https://twitter.com/seguinfo)

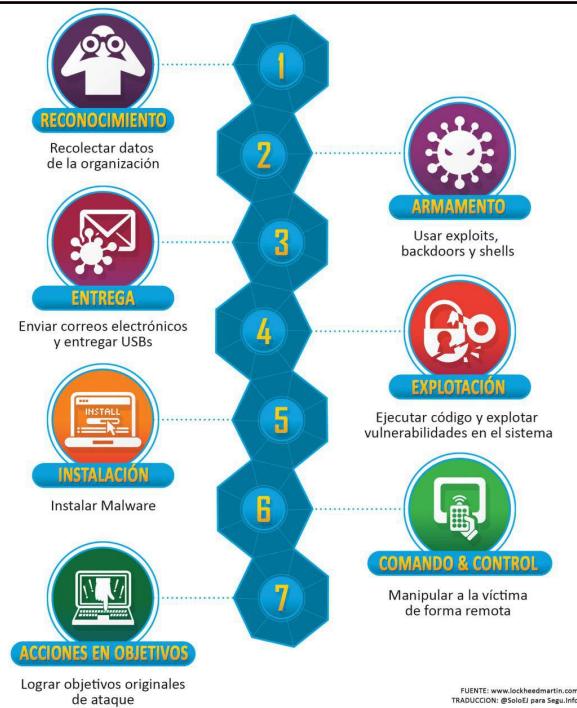
Sobre Cristian Borghello (AR)



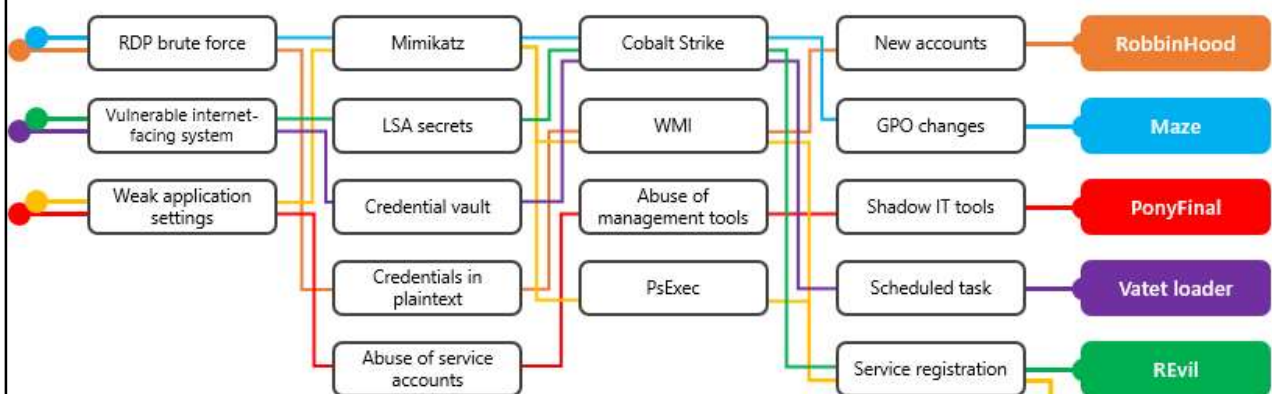
- Licenciado en Sistemas UTN desde 2000
- Desarrollador desde los 8 años
- CISSP (*Certified Information Systems Security Professional*)
- Microsoft MVP Security durante 10 años
- CCSK (*Certificate Cloud Security Knowledge*)
- CSFPC (*Certification Cyber Security Foundation*)
- Certificado en Ciberseguridad 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

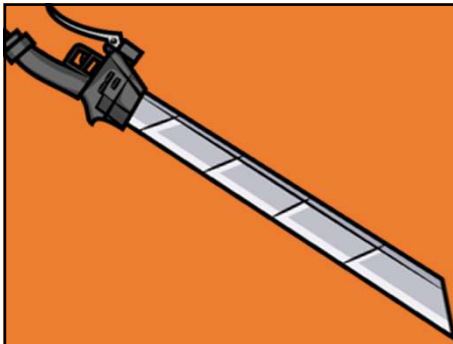
- **Kill Chain** es un modelo de ataque de los años noventa, desarrollado por la Fuerza Aérea de los Estados Unidos.
- La estrategia, conocida como **F2T2EA**, se basa en seis pasos para llevar a cabo una operación militar: encontrar (*Find*), asegurar (*Fix*); rastrear (*Track*); elegir objetivo (*Target*), 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



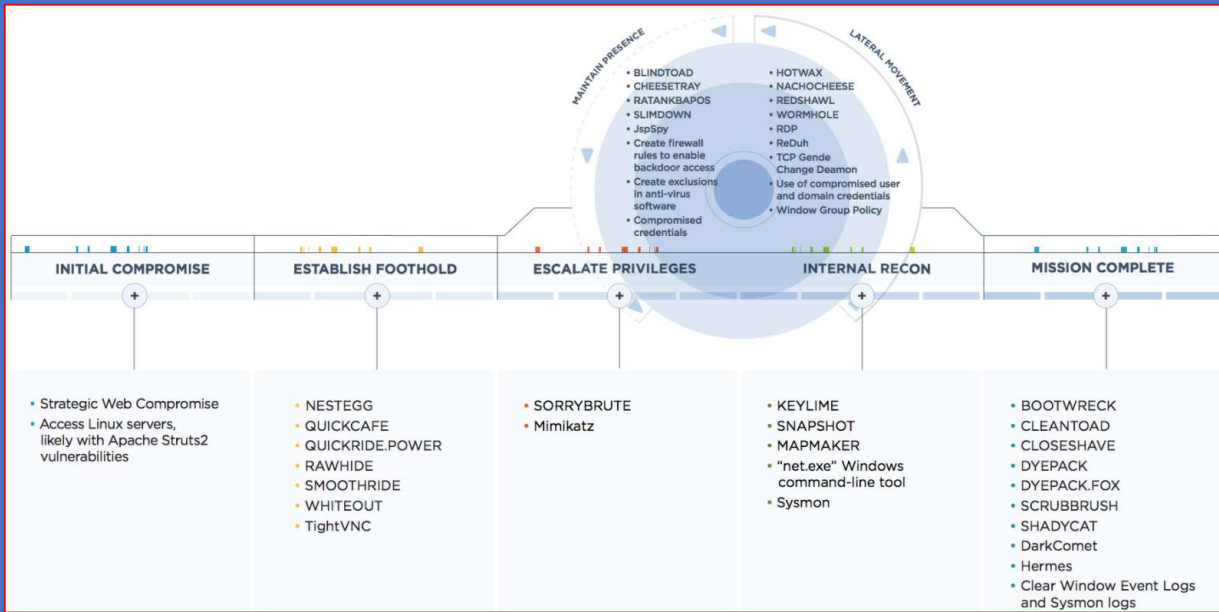
<https://attack.mitre.org/>

MITRE ATT&CK													
layer	Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques
Active Scanning (0,2)	Acquire Infrastructure (0,6)	Drive-by Compromise	Command and Scripting Interpreter (0,8)	Account Manipulation (0,4)	Abuse Elevation Control Mechanism (0,4)	Abuse Elevation Control Mechanism (0,4)	Brute Force (0,4)	Account Discovery (0,18)	Exploitation of Remote Services	Archive Collected Data (0,3)	Application Layer Protocol (0,4)	Automated Exfiltration (0,1)	
Gather Victim Host Information (0,4)	Compromise Accounts (0,2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0,5)	Access Token Manipulation (0,5)	Credentials from Password Stores (0,5)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	
Gather Victim Identity Information (0,3)	Compromise Infrastructure (0,6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (0,14)	Boot or Logon Autostart Execution (0,14)	Boot or Logon Autostart Execution (0,14)	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (0,2)	Exfiltration Over Alternative Protocol (0,3)	
Gather Victim Network Information (0,6)	Develop Capabilities (0,4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0,5)	Boot or Logon Initialization Scripts (0,5)	Boot or Logon Initialization Scripts (0,5)	Build Image on Host	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0,2)	Clipboard Data	Data Obfuscation (0,3)	Exfiltration Over C2 Channel	
Gather Victim Org Information (0,4)	Establish Accounts (0,2)	Phishing (0,3)	Inter-Process Communication (0,2)	Browser Extensions	Create or Modify System Process (0,4)	Create or Modify System Process (0,4)	Deobfuscate/Decode Files or Information	Cloud Service Dashboard	Remote Services (0,6)	Data from Cloud Storage Object	Dynamic Resolution (0,3)	Exfiltration Over Other Network Medium (0,1)	
Phishing for Information (0,3)	Obtain Capabilities (0,6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (0,2)	Domain Policy Modification (0,2)	Forge Web Credentials (0,2)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (0,2)	Encrypted Channel (0,2)	Exfiltration Over Physical Medium (0,1)	
Search Closed Sources (0,2)	Stage Capabilities (0,5)	Supply Chain Compromise (0,3)	Scheduled Task/Job (0,7)	Event Triggered Execution (0,15)	Event Triggered Execution (0,15)	Event Triggered Execution (0,15)	Input Capture (0,4)	Container and Resource Discovery	Data from Information Repositories (0,2)	Fallback Channels	Ingress Tool Transfer	Scheduled Transfer	
Search Open Technical Databases (0,5)	Trusted Relationship	Software Deployment Tools	Shared Modules	Create Account (0,1)	Escape to Host	Escape to Host	Man-in-the-Middle (0,2)	Domain Trust Discovery	Data from Local System	Network from Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	
Search Open Websites/Domains (0,2)	Valid Accounts (0,4)	System Services (0,2)	User Execution (0,3)	Create or Modify System Process (0,4)	Event Triggered Execution (0,15)	Event Triggered Execution (0,15)	Modify Authentication Process (0,4)	File and Directory Discovery	Software Deployment Tools	Network from Removable Media	Non-Standard Port		
Search Victim-Owned Websites	Windows Management Instrumentation	External Remote Services	Hijack Execution Flow (0,11)	External Remote Services	Hijack Execution Flow (0,11)	Hijack Execution Flow (0,11)	Network Sniffing	Network Service Scanning	Taint Shared Content	Data from Removable Media	Protocol Tunneling		
			Implant Internal Image	External Remote Services	Process Injection (0,11)	Process Injection (0,11)	OS Credential Dumping (0,8)	Network Share Discovery	Use Alternate Authentication Material (0,4)	Network Sniffing	Email Collection (0,3)		
			Modify Authentication Process (0,4)	External Remote Services	Scheduled Task/Job (0,7)	Scheduled Task/Job (0,7)	Steal Application Access Token	Password Policy Discovery	Peripheral Device Discovery	Input Capture (0,4)	Proxy (0,4)		
			Office Application Startup (0,6)	External Remote Services	Indicator Removal on Host (0,8)	Indicator Removal on Host (0,8)	Steal or Forge Kerberos Tickets (0,4)	Permission Groups Discovery (0,3)	Process Discovery	Man in the Browser	Remote Access Software		
				External Remote Services	Indirect Command Execution	Indirect Command Execution	Steal Web Session Cookie	Query Registry	Man-in-the-Middle (0,2)	Traffic Signaling (0,1)			
				External Remote Services	Masquerading (0,6)	Masquerading (0,6)	Two-Factor Authentication Interception						



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>

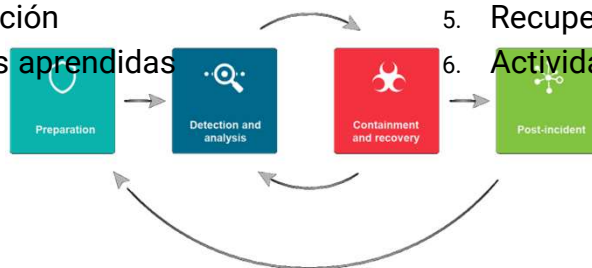
Fases de un Incidente

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



CIS Controls Version 7		CIS Controls Version 8	
01	Inventory of Hardware	01	Inventory and Control of Enterprise Assets
02	Inventory of Software	02	Inventory and Control of Software Assets
03	Continuous Vulnerability Management	03	Data Protection
04	Control of Admin Privileges	04	Secure Configuration of Enterprise Assets and
05	Secure Configuration	05	Account Management
06	Maintenance and Analysis of Logs	06	Access Control Management
07	Email and Browser Protections	07	Continuous Vulnerability Management
08	Malware Defenses	08	Audit Log Management
09	Limitation of Ports and Protocols	09	Email and Web Browser Protections
10	Data Recovery	10	Malware Defenses
11	Secure Configuration of Network Devices	11	Data Recovery
12	Boundary Defense	12	Network Infrastructure Management
13	Data Protection	13	Network Monitoring and Defense
14	Controlled Access Based on Need to Know	14	Security Awareness and Skills Training
15	Wireless Access Control	15	Service Provider Management
16	Account Monitoring and Control	16	Application Software Security
17	Security Awareness Training	17	Incident Response Management
18	Application Security	18	Penetration Testing
19	Incident Management		
20	Penetration Testing		

CIS Community Defense Model

<https://www.cisecurity.org/controls/v8/>

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 negativos 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

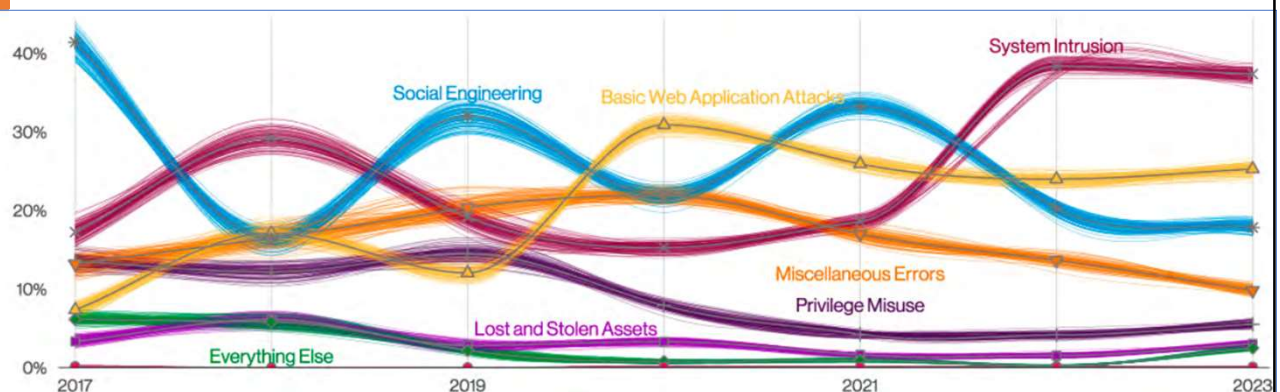
Se origina fuera de la red y es iniciada por actores maliciosos o delincuentes.

El atacante emplea varias tácticas para violar la red.

INTERNO

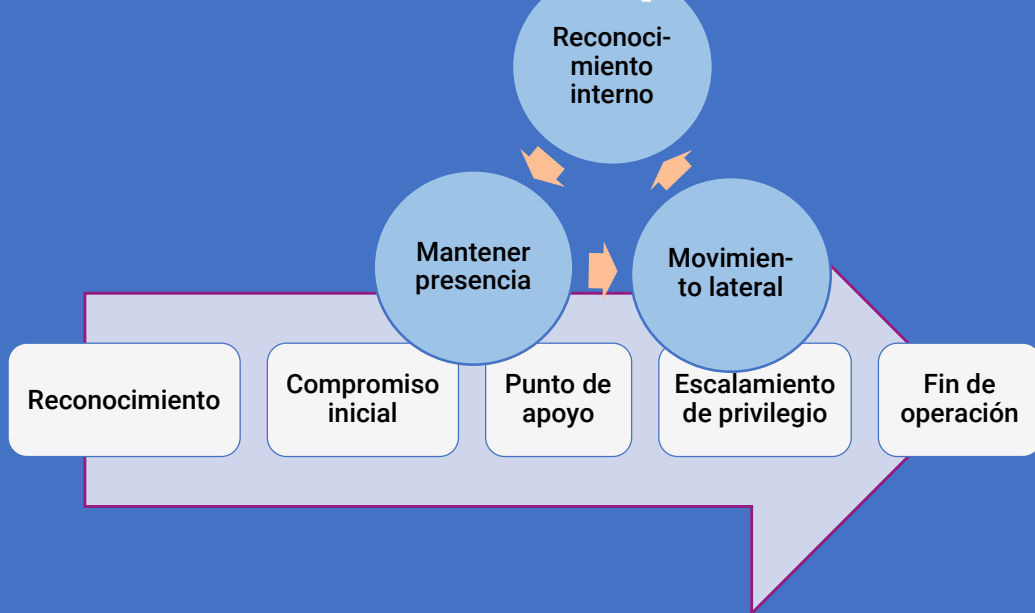
Se produce cuando una persona con información privilegiada provoca un incidente, al abusar de sus privilegios **(INSIDER)**

Brechas e Incidentes [DBIR]



Patterns over time in breaches

Ciclo de vida de un ataque



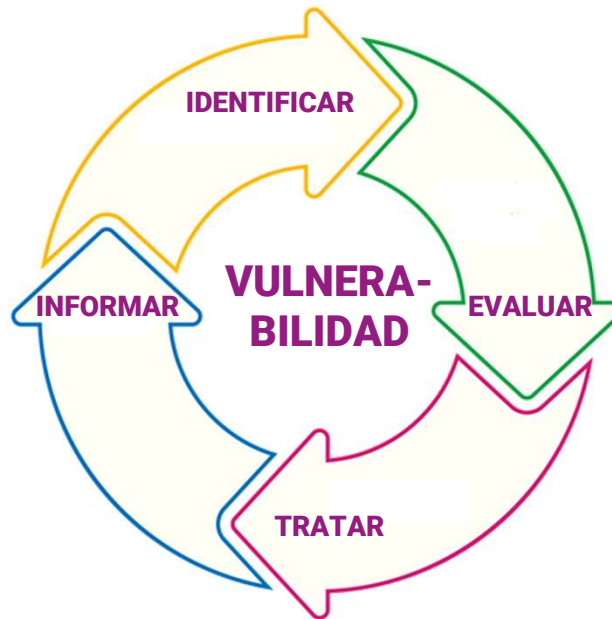
Gestión de Vulnerabilidades



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>

The screenshot displays a malware analysis tool interface. On the left, a vertical list shows a process chain: WINWORD.EXE /Embedding (PID 3860), chrome.exe (PID 3256), chrome.exe (PID 3212), and powershell.exe (PID 3680) with a WMI icon. Below this is a 'PROCESS DETAILS' section with a 'More Info' button. A 'DANGER' section highlights 'Downloads executable files from the Internet'. A 'WARNING' section lists several actions: 'Executable content was dropped or overwritten', 'Creates files in the user directory', 'PowerShell script executed', and 'Executed via WMI'. On the right, a detailed view of a process is shown, including a Windows logo, 'Win7 32 bit Complete', MD5 hash, start time, and total time. It features buttons for 'Get sample', 'IOC', 'Restart', and 'Export', along with 'Text report', 'Processes graph', and 'ATT&CK™ matrix'. A 'PROCESS' table lists several entries with their PIDs, hashes, names, and various metrics.

PID	Hash	Name	File Size	IOCs	Alerts
2992	6f2432e4ac98575aa653094123b478bf6c3aa9b00aaad84dfd09045a96d6b97...	PE	658	345	128
3540	6f2432e4ac98575aa653094123b478bf6c3aa9b00aaad84dfd09045a96d6b...	PE	2k	14	188
3528	powershell.exe -e RwbIAHQALQBxAG0AaQBPAgiAagBIAGMAdAAgAFcAaQBuADMAMgBfAF...		1k	253	218
1928	COM	unsecapp.exe -Embedding	88	1	27
3152	SER	vssvc.exe			

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!



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

