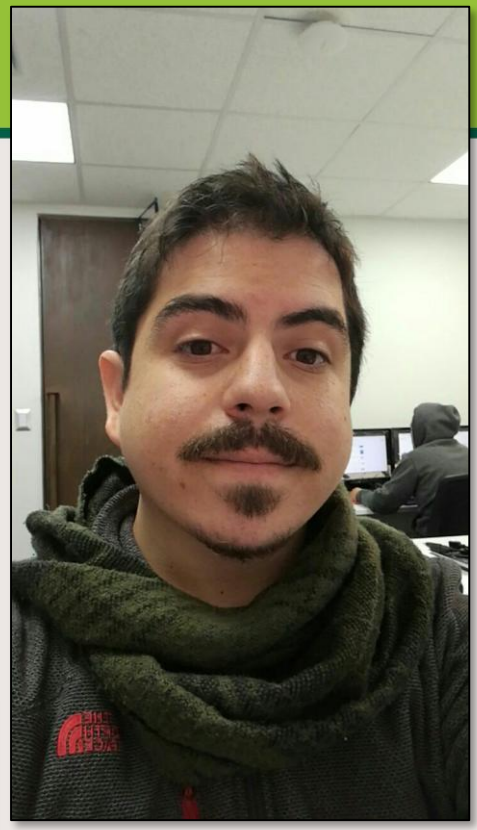
Ciberinteligencia: potenciando la gestión de seguridad

OFFICIAL (ISC)² CHAPTER | CHILE

About: Miguel Díaz

- Ing. Civil Informático – UTFSM
- CEHv8 – EC Council
- Consultor en Ciberseguridad
- Security Researcher
- Inquieto
- Líder de Operaciones de Ciberinteligencia en Entel CyberSecure



@mdiazlcl

Agenda

- **Contexto:** Operaciones de Ciberseguridad
- Modelo de Ciberinteligencia
- Casos interesantes

Operaciones de ciberseguridad

» Las operaciones de ciberseguridad

CHILE

¿Cómo están compuestos?

- Operadores revisando alarmas / eventos
- Dispositivos de seguridad (Muchos)
- Actualizaciones según “vendor”
- Gestionar actividades de ciberseguridad

CHILE

¿Qué se esconde detrás de esta realidad?

CHILE

» Operadores gestionando “requerimientos” e “incidentes”

- Falsos positivos!
- Agregar, quitar, modificar esta reglas Firewall
- No puedo acceder al servidor, debe ser el firewall
- Habilítame el sitio supermalware.ru
- La VPN no funciona, reinicia la contraseña
- La caja negra está con luces rojas

Many CSOCs expend more energy battling politics and personnel issues than they do identifying and responding to cyber attacks”

Ten Strategies of a World-Class Cybersecurity Operations Center
- Carson Zimmerman, The MITRE Corporation

» Dispositivos de Seguridad

- IPS/IDS, DLP, 2FA, SIEM, Firewall, WAF, Anti-DDOS, Endpoints, Anti-Malware, Sniffers, NACs, ACLs, Anti-SPAM, UTM, PPTs, AFPs, PSU, Fondos mutuos…

"El IPS ha bloqueado 6.780 firmas de intrusos"

"El AntiSPAM ha bloqueado satisfactoriamente una campaña de fraude"

"Anti-Malware ha bloqueado 3.405 virus este mes"

» Analogía

Los equipos de operaciones de ciberseguridad son los soldados en el campo de batalla, ganando cada combate, cada enfrentamiento con todas las armas posibles. Son especialistas en combate y nadie los supera en ello.


© Reuters

Rol de Ciberinteligencia

Estrategia versus Táctica

(en el contexto militar)

Estrategia

Se ocupa del planeamiento y dirección de las campañas bélicas, así como del movimiento y disposición estratégica de las fuerzas armadas.

Táctica

Cuando llega el momento del choque o enfrentamiento bélico, lo que la estrategia militar concibe, la táctica militar lo prosigue y pone en práctica, lo ejecuta, si puede ser con celeridad y sigilo

OFFICIAL (ISC)² CHAPTER | CHILE

Filosofía de Ciberinteligencia

Adquirir
Analizar
Identificar
Rastrear
Predecir
> Información

> Para descubrir
Tácticas
Técnicas y
Procedimientos
MALICIOSOS*

*TTPs

Encontrando

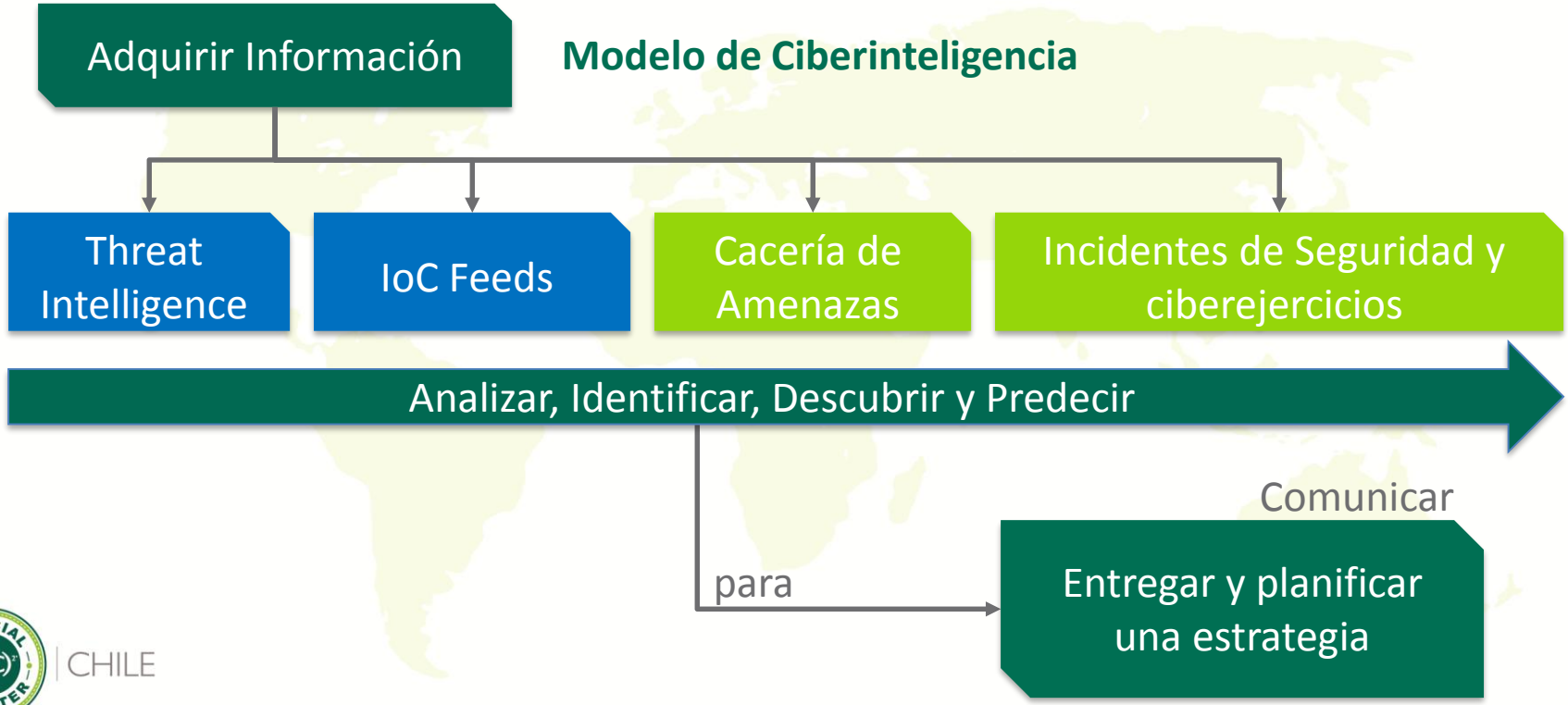
ESTRATEGIA DE CIBERSEGURIDAD_

Fuente: Advancing Cyber Intelligence Practices
https://www.youtube.com/watch?v=S_W3pRNuXss

OFFICIAL (ISC)² CHAPTER | CHILE

CICLO DE INTELIGENCIA

CHILE


Adquirir Información
Modelo de Ciberinteligencia
Threat Intelligence
IoC Feeds
Cacería de Amenazas
Incidentes de Seguridad y ciberejercicios
Analizar, Identificar, Descubrir y Predecir
Comunicar
para
Entregar y planificar una estrategia

Threat Intelligence

Procesamiento de información (**manual**)

- Vendors
- Blogs de seguridad (recomiendo inglés)
- Comunidades Internet (Facebook, Twitter, Telegram, Foros, DeepWeb)
- Investigación local y proactiva de amenazas
- Podcasts de seguridad
- Compañeros de rubro!

Entrega Contexto

OFFICIAL (ISC)² CHAPTER | CHILE

IoC Feeds

- Dominios maliciosos
- Direcciones IP’s
- Hashes (MD5/SHA)
- Análisis de archivos

THREAT CONNECT™

TALOS

ALIEN VAULT

virustotal

OFFICIAL (ISC)² CHAPTER | CHILE

Cacería de Amenazas

o threat Hunting

Def:

Es la ***búsqueda proactiva*** de amenazas de ciberseguridad que evaden los mecanismos tradicionales de control.

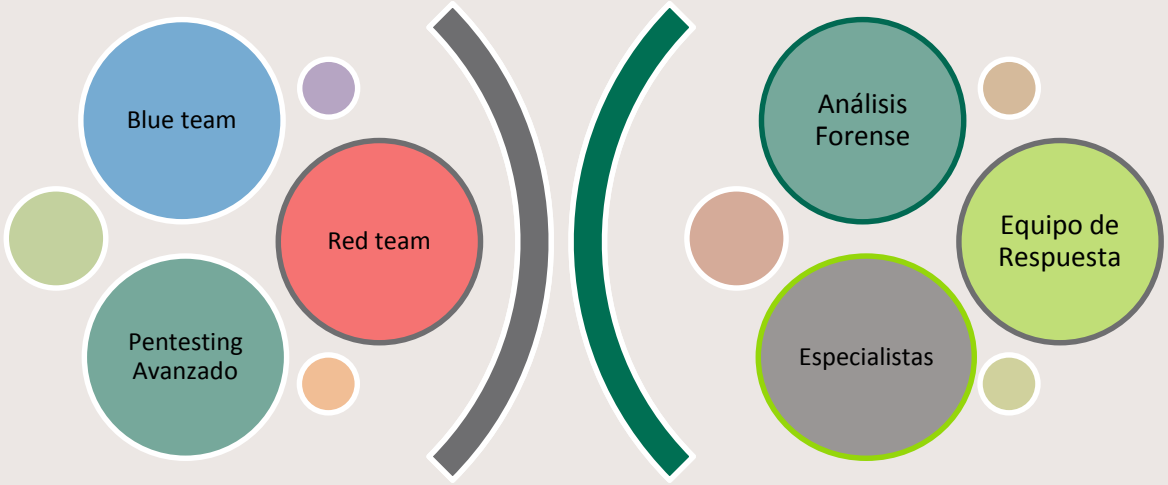
Se basa en una hipótesis y un estudio profundo de los eventos de seguridad, pensando desde la perspectiva que ya hay un APT en progreso.

Ejemplos

Herramienta	Grieta
Antivirus	Powershell, comandos elevados
Firewalls (c4)	Puertos conocidos Reglas mal configuradas
Filtro de Contenido	Webs no categorizadas
Antispam	Borde del sistema de scoring
Escáner de vulnerabilidades	Webs no “vulnerables” (*)
Control de accesos	Credenciales robadas

Aportan con una visión interna del comportamiento de anómalo de la organización

Incidentes de Seguridad y ciberejercicios



Ciberejercicios

Incidentes de Seguridad

CHILE

» La sinergia de componentes

“El todo es más que la sumatoria de sus partes”

- Gestalt

CHILE

Dónde aporta la Ciberinteligencia?

- Nuevos vectores de ataque
- Priorizar los riesgos
- Inteligencia sobre herramientas
- Apoyo en la toma de decisiones
- Conocimiento interno de la organización
- Descubrir APT
- Apoyo estratégico en la resolución de incidentes

OFFICIAL (ISC)² CHAPTER | CHILE

Desafíos

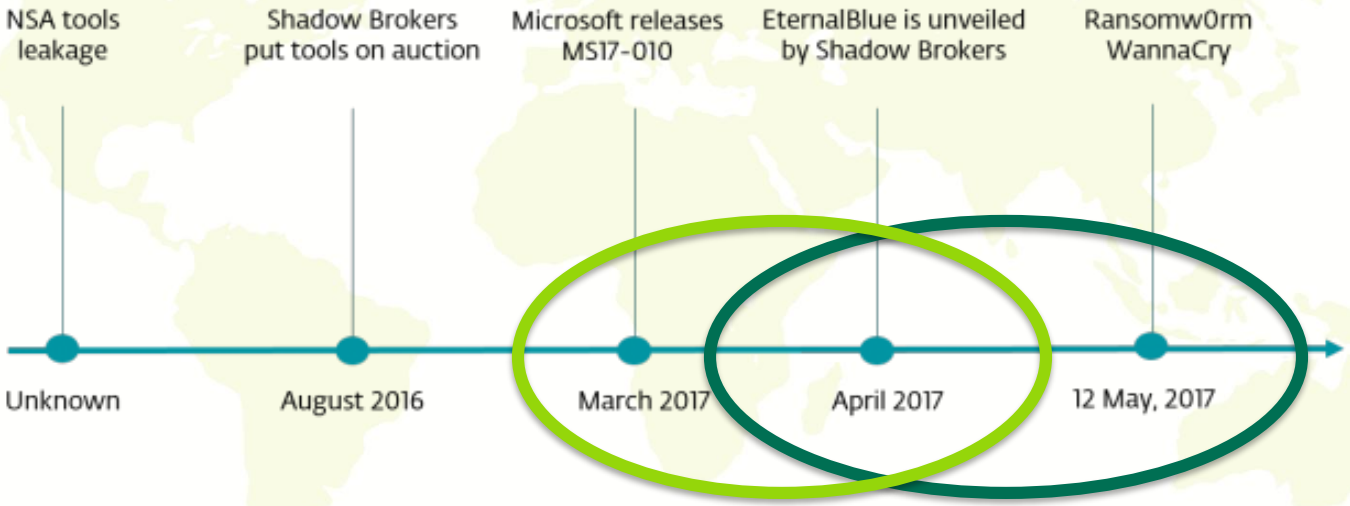
- Tener mucha información a veces es peor que tener poca información.
- Falta de personal capacitado para entender y transmitir las amenazas.
- Cantidad de trabajo manual que hay que hacer (excluyendo IoC Feeds)

Casos

(pido perdón de antemano)

OFFICIAL (ISC)² CHAPTER | CHILE

» Eternalblue (MS17-010)

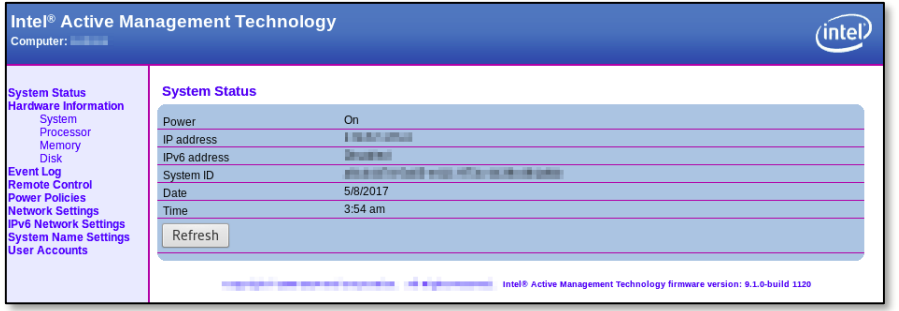


4 Casos Interesantes

CHILE

Intel AMT Login Bypass

- Origen: Threat Intelligence – Blog
- Fecha Exposición: 02/mayo/2017
- Amenaza: Intel AMT Login Bypass
- Exploit: Disponible
- Estrategia: Revisar equipos dentro de la red corporativa y perimetral que tengan el portal Intel AMT habilitado, y en caso de que sea vulnerable limitar acceso para mitigar o parchar para remediar.

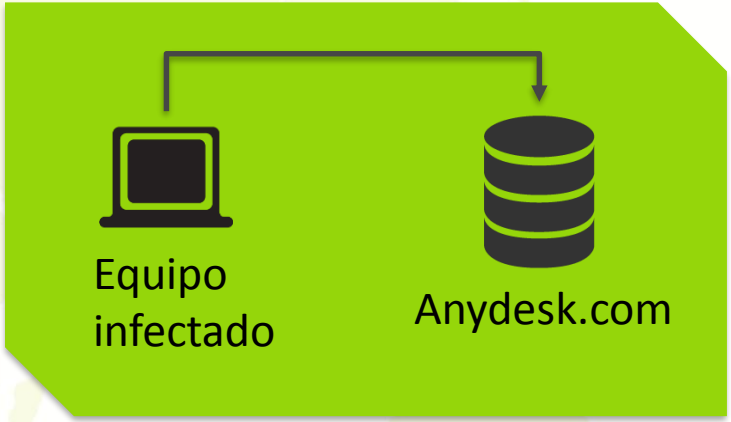


CVE-2017-5689

OFFICIAL (ISC)² CHAPTER | CHILE

Forense a equipo infectado

- Origen: Análisis Forense
- Fecha Estudio: Septiembre/2017
- Observado: Se detectó que una vez que el equipo fue comprometido se utilizó software de control remoto para realizar exiltración
- Amenaza: Anydesk como control remoto
- Estrategia: Analizar conexiones entrantes y salientes hacia servidores asociados a Anydesk.com



Incidente de seguridad
Análisis Forense

CHILE

Análisis de tráfico de Firewall

- Origen: Threat Hunting – Análisis FW
- Amenaza: Reglas de Firewall incongruentes
- Observado: Múltiples reglas gatilladas en el Firewall
- Estrategia: Realizar una auditoria sobre las reglas de firewall y analizar si funcionan de manera correcta.

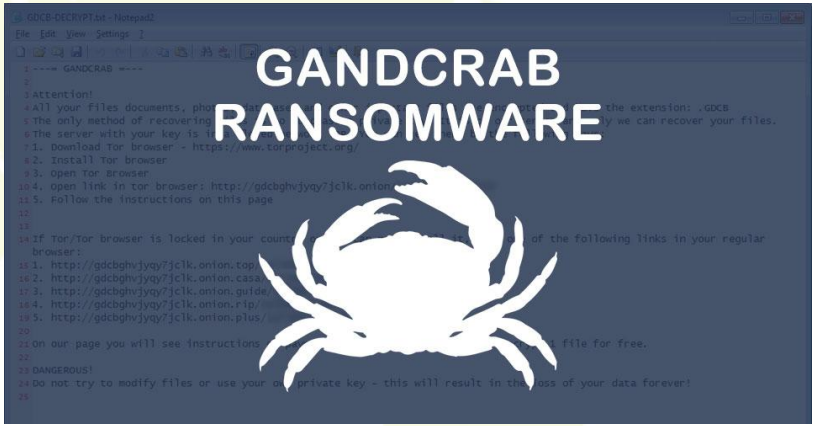
Ejemplos:

- Office_365
- Navegación Web
- Monitoreo

CHILE

Ransomware: GandCrab, incidente y recuperación

- Origen: Threat Intelligence
- Amenaza: Control del incidente de seguridad
- Estrategia: Entregar información sobre el comportamiento durante el incidente del malware y darle seguimiento al Malware. Apareció decryptor, comunicarlo.



Cierre

CHILE

Palabras finales

- No basta con ganar batallas si no estamos avanzando en la guerra.
- Los controles de seguridad son tan importantes como la inteligencia detrás de ellos!
- Es un trabajo colaborativo, entre las áreas operacionales y las áreas de inteligencia
- La Ciberinteligencia aporta la estrategia, la cual debe ser llevada a cabo por la operación. Es una simbiosis interesante.

Invitación de Cierre

- Subscribirse a feeds de Threat Intelligence.
- Aventurarse a cuestionar los dispositivos de seguridad! Prometo que se llevarán sorpresas interesantes.
- Comenzar con procesos simples de Ciberinteligencia y orientados a las necesidades locales de la empresa.