FORO EJECUTIVO

CIBERSEGURIDAD EN EL sector financiero

CIBERCRIMEN: INCERTIDUMBRE Y COMPLEJIDAD

¿Conocemos al enemigo?

Marcos Polanco
Director Ejecutivo de Ciberseguridad e Innovación
Telmex-Scitum

Scitum | TELMEX está contigo

Si te conoces
a ti mismo
y a tu enemigo
podrás ganar
cientos de batallas
sin riesgo

Sun-Tzu

V — Volatility
Fast change without a clear predictable trend or pattern.

U — Uncertainty
Frequently disruptive changes; past is not a predictor of the future.

C — Complexity
Multiple, interdependent causes.

A — Ambiguity
Little clarity about what is 'real' or 'true'.

¿Qué tanto realmente conocemos nuestros entornos digitales?

¿Qué tanto los atacantes saben de nosotros?

Scitum | TELMEX está contigo

¿Quiénes saben de nosotros?

EXTERNO

ATACANTES

AUDITORES

PROVEEDORES

INTERNO

USUARIOS

ALTA DIRECCIÓN

ÁREA DE SISTEMAS

ÁREA DE SEGURIDAD

Scitum | TELMEX está contigo

Modelo actual enfocado al ataque

Para combatir el cibercrimen de forma eficiente, no solo necesitamos desarrollar soluciones técnicas sino también entender su estructura de negocio y factores clave

¿Cuál es el modelo de negocio de los atacantes?

CANVAS del CaaS (Cybercrime as a Service)

Key Partners

VDaaS
EKaaS
EDaaS
AaaS
PPaaS
DMaaS
MLaaS
MRaaS
HTaaS
HRaaS

Key Activities

Descub. Vulnerab.
Desarrollo exploit
Distrib. de exploit
Ejecución ataque
Lavado de dinero

Key Resources

Reclutamiento
Mulas
Entrenamiento
Reputación

Value Proposition

Poder ejecutar ataques efectivos que se puedan monetizar maximizando la relación facilidad-costo-riesgo-beneficio

Customer Relationships

Foros de hackers
Redes sociales

Channels

Marketplace en el mercado negro

Customer Segments

Organizaciones criminales o no que desean ejecutar un ataque

Cost Structure

Costo psicológico
Costo esperado de sanción
Costo de la operación

Revenue Streams

Ganancias directas
Ganancias psicológicas (reputación, satisfacción, revancha, agenda política)
Ganancias económicas

Entender al adversario

ADVERSARIO

¿Cómo se llama, tiene un nickname?
¿Es un ciberactor o un colectivo?

CAPACIDADES

¿Qué daño es capaz de causar?
¿Qué tan grave es?

INFRAESTRUCTURA

¿Con qué tipo de armas cuenta, son propietarias?
¿Hay algo particular en su infraestructura, la renta?

VÍCTIMA

¿A quién suele atacar?
¿Quién es su víctima más recurrente?
¿A quien ha dicho que le gustaría atacar?

Lazarus Group
Otros alías: Who I am, DarkSeoul, Hidden Cobra

ADVERSARIO

Socio político: cíber atacantes patrocinados por el gobierno de Corea del Norte, que orquestan ataques hacía otros países, en especial aquellos en vías de desarrollo

CAPACIDADES

Conocimiento profundo de SWIFT, Windows y de herramientas validas del mismo SO

Borrado de rastros:
- ✓ Eliminación de rastros con borrado seguro
- ✓ Modificación de marcas de tiempo en archivos
- ✓ Deshabilitación de herramientas de seguridad

Técnicas utilizadas
- ✓ SpearPhising (CVE-2015-6585)
- ✓ Ataques de diccionario para movimientos laterales
- ✓ Separación de archivos (malware compuesto de múltiples documentos, para ofuscación)
- ✓ Malware protegido por contraseñas
- ✓ Desarrollo de malware propietario
- ✓ Instalación de servicios para persistencia
- ✓ Técnicas de persistencia con bootkits
- ✓ Uso de cifrado robusto

Técnicas de ofuscación:
- ✓ Artefactos maliciosos en idioma ruso

Motivación:
Fines financieros
Múltiples ataques a instituciones bancarias
Desarrollo de malware orientado a la red SWIFT
Afectaciones a gobiernos e infraestructura crítica
Financiamiento del programa nuclear, ciberguerra

VÍCTIMAS

Sony (2014): exfiltración y borrado de información
Gobierno de Corea del Sur (2013): Operation Troy
Compañías financieras y de medios en Corea del Sur (2013): Operation DarkSeoul
Banco de Bangladesh (2016)
Novetta (2016) Operation BluckBuster
Banca Europea – 2017
Gobierno de Polonia – 2017
Gobierno de México – 2017

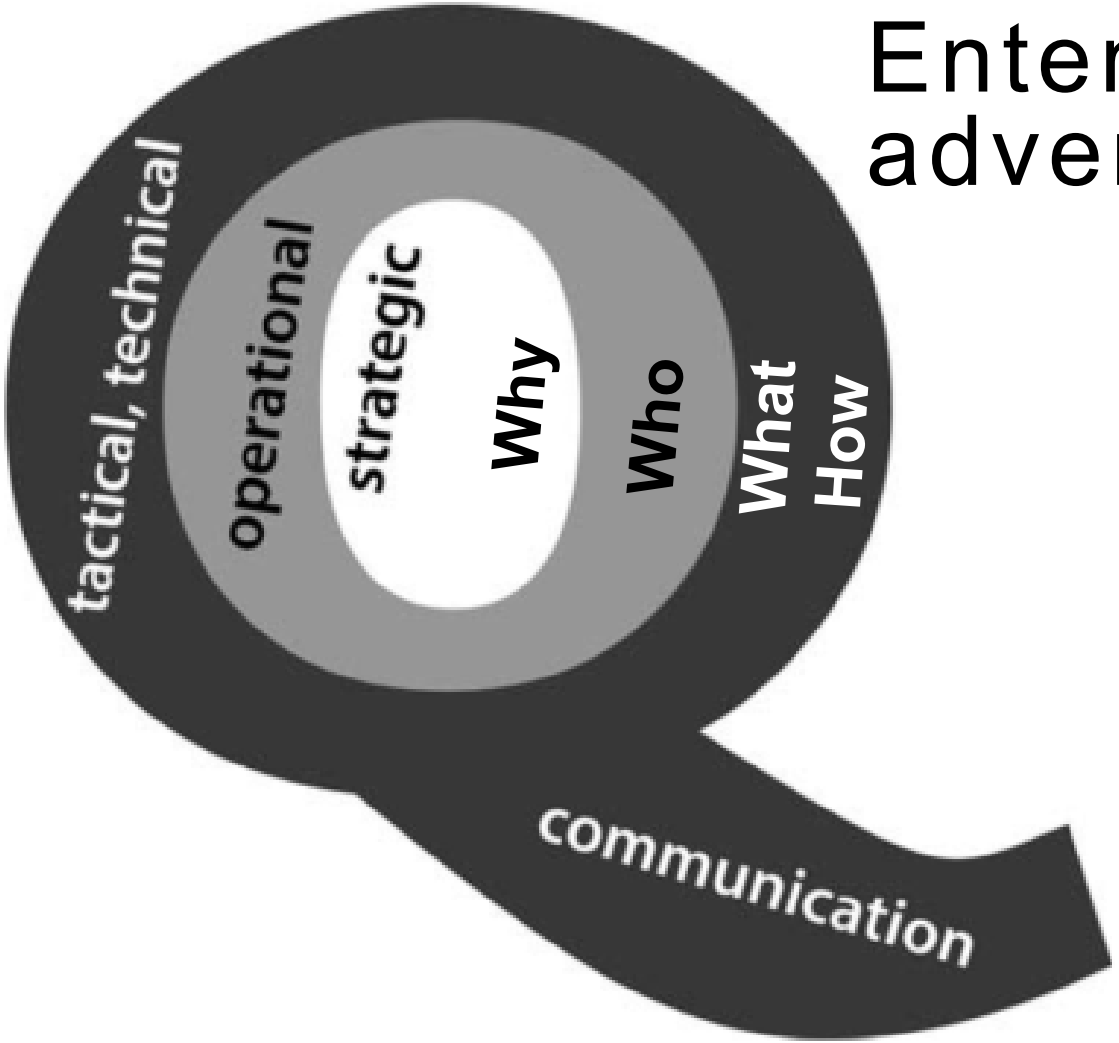
INFRAESTRUCTURA

Herramientas de sistema operativo:
- ✓ Netsves (persistencia)
- ✓ cmd.exe
- ✓ netsh.exe

Software comercial:
- ✓ Magnite Exploit Kit
- ✓ SoftEther VPN
- ✓ Keylogger

Malware propietario:
- ✓ Destover malware – Wiper
- ✓ Hangman malware – RAT
- ✓ Wild Positron/Douzer malware –RAT
- ✓ Romeo – Backdoor/RAT
- ✓ Proxy PapaAlfa
- ✓ Documentos Word con CVE- 2015-6585
- ✓ Malware específico para SWIFT

Entender al adversario



Scitum | TELMEX está contigo

Caso de WannaCry

Scitum | TELMEX está contigo

Modelado de amenazas en el sector financiero

Scitum | TELMEX está contigo

Entender al adversario

ADVERSARIO

Lazarus (Hidden Cobra)
Cobalt
Campaña Catasia y Ghostlive
Campaña Roaming Mantis
Operación Icarus

CAPACIDADES

Man in the Browser
Nuevo malware de segunda fase
Mayores capacidades de evasión
Reclutamiento de insiders en bancos y empresas de paquetería

INFRAESTRUCTURA

Emotet (Gozi, IceID)
Mutaciones de Zeus
Zeus Panda y Gootkit
Bankshot, Hardrain y Badcall
FakeBank, Andriod.banker.A9480
Nueva versión de Plotus.D, Cutler Maker

VÍCTIMA

Empresas que manejan Criptomonedas
Redes Swift
Sistemas de pago
Sistemas de tarjetas de

Principales hallazgos del 1Q 2018

- Técnica “man in the Browser” empleada más a menudo
- Uso más frecuente de malware tipo “fileless”
- Atacar la cadena de suministro
- Redes sociales como mecanismo de comunicación y organización
- Mayor empleo de las técnicas de Cloaking y Black SEO
- Uso de sitios para phishing a partir de errores tipográficos
- Más malware para ambientes móviles, capaz de implementar carátulas falsas, interceptar SMS y llamadas
- Los ataques combinan ingeniería social, malware y sitios de phishing

Fuentes: SCILabs® 1Q 2018 Report


CONCLUSIÓN
Debemos complementar el modelo de protección basado en el ataque con un modelo basado en el atacante

GRACIAS

DESCARGUE ESTA PRESENTACIÓN EN

resources | scitum

resources.scitum.com.mx

Scitum | TELMEX está contigo