#IntelCon2020

IntelCon
by Ginseg

TIBER: El Framework del futuro en el que TI manda

Pablo Bentanachs
@BentanachsPablo

Congreso Online de Ciberinteligencia
Julio 2020

IntelCon
by Ginseg

Índice

IntelCon
by Ginseg

Qué es el TIBER-EU

Definición del TIBER-EU

El TIBER-EU (Threat Intelligence Based Ethical Red Teaming) es un marco común desarrollado por el Banco Central Europeo en 2018 que ofrece una prueba de Red Team controlado y personalizado dirigido por Threat Intelligence.

Las pruebas del TIBER-EU imitan TTPs de los actores quienes, sobre la base de Threat Intelligence, son percibidos como una amenaza genuina para entidades.

Una prueba de Red Team dirigida por Threat Intelligence implica el uso de una variedad de técnicas para simular un ataque contra las funciones críticas de una entidad y los sistemas subyacentes (es decir, su gente, procesos y tecnologías).

Este tipo de test ayuda a una entidad a evaluar sus capacidades de protección, detección y respuesta.

Objetivos del TIBER-EU

IntelCon by Ginseg

#IntelCon2020

Mejorar la resiliencia (recuperación) cibernética de las entidades y del sector financiero.

Estandarizar la forma en que las entidades realizan el ejercicio de Red Team dirigido por Threat Intelligence en toda la UE, al tiempo que permite a cada jurisdicción un cierto grado de flexibilidad adaptar el marco de acuerdo con sus especificidades.

Orientar y capacitar a las autoridades sobre cómo pueden establecer, implementar y gestionar esta forma de prueba a nivel nacional o europeo.

Respaldar los ejercicios del Red Team dirigidos por Threat Intelligence entre jurisdicciones para entidades multinacionales.

Reducir la carga regulatoria sobre las entidades y fomentar el reconocimiento mutuo de pruebas en toda la UE.

Roles y Responsabilidades

IntelCon by Ginseg

#IntelCon2020

Las principales partes que pueden participar en las pruebas:

Equipo Blanco
(White Team)

Equipo
Azul
(Blue
Team)

OBJETIVO (ENTIDAD FINANCIERA)

Proveedor de
Threat Intelligence (TI)

Proveedor de Red Team (RT)

PROVEEDORES CIBERSEGURIDAD

Ciber-equipo TIBER
(TIBER CyberTeam)

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

CCN-CERT

Agencia de inteligencia gubernamental o centro nacional de ciberseguridad.

Fases

IntelCon by Ginseg

#IntelCon2020

[Opcional]

Informe genérico

1

Fase de preparación

2

Fase de pruebas

3

Fase de cierre

Generic Threat Landscape

Compromiso y alcance

Contratación de servicios TI / RT

1-2 meses

Threat Intelligence

1 mes

Red Teaming

3 meses

Planificación de remediación

Compartir resultados

1 mes o más

Base para el informe específico de inteligencia de seguridad.

Preferiblemente elaborado por institución referente gubernamental nacional o europea.

Lanzamiento formal de las pruebas.
Definición del alcance de pruebas.
Selección de proveedores.

Ejecución de las pruebas.
Informe específico de inteligencia de seguridad.

Informe de vulnerabilidades y recomendaciones.

Planes de mejora.

IntelCon
by Ginseg

2

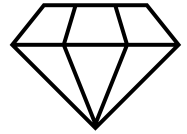
Fase de preparación

Alcance & Selección de vendors

Engagement y Scoping

El objetivo clave del Scope es que la entidad y las autoridades pertinentes acuerden el alcance de la prueba del Red Team.
El alcance debe incluir las FC de la entidad. La entidad puede decidir a su discreción incluir funciones adicionales no críticas.

Dentro del marco TIBER-UE, las FC se definen como:
"Las personas, procesos y tecnologías requeridas por la entidad para realizar un servicio que, si se interrumpe, podría tener un impacto negativo en la estabilidad financiera, el seguridad y solidez de la entidad, la base de clientes de la entidad o el mercado de la entidad conducta".



Al acabar esta fase, todas las partes relevantes, es decir, el TCT y la entidad, habrán acordado el alcance de la prueba y la identificación de las FC. Para tener éxito en esta fase, es importante que tanto el TCT como la entidad deben de tener un amplio conocimiento del modelo de negocio de la entidad, sus funciones y servicios.

Contratación de servicios de TI/RT

IntelCon by Ginseg

#IntelCon2020

Durante la contratación, la entidad debe llevar a cabo las siguientes actividades:

Identificar posibles proveedores de TI / RT

Emitir una licitación de conformidad con el marco TIBER-EU y cualquier legislación relevante

Evaluar respuestas y seleccionar proveedores

Establecer condiciones que rijan el intercambio, la confidencialidad y la retención de datos

IntelCon
by Ginseg

3

Fase de pruebas

Threat Intelligence & Red Teaming

IntelCon
by Ginseg

3.1 | Fase de pruebas

Threat Intelligence

General Threat Landscape (GTL)

IntelCon by Ginseg

#IntelCon2020

A pesar de ser opcional, el marco del TIBER-EU recomienda a las jurisdicciones nacionales producir un informe GTL nacional para el sector financiero para complementar el informe TTI.

- EL GTL debe centrarse en el landscape (panorama) especifico de amenazas del país teniendo en cuenta las amenazas geopoliticas y penales exclusivas de esa jurisdicción
- El informe debe considerar el sector financiero del país y sus FC (Funciones críticas) así como los diferentes threat actors (y sus TTPs) dirigidas a esta industria

El informe de GTL permitirá al proveedor de TI a:

- Traducción de la información contenida en el informe de GTL a información específica de inteligencia estrátegica, operativa y tactica relevantes para la entidad
- Centrar sus esfuerzos en un reconocimiento más detallado para proporcionarl al proveedor de RT con información más personalizada y específica

Información necesaria

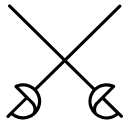
IntelCon by Ginseg

#IntelCon2020

La entidad debe dar al proveedor de TI la siguiente información para que el la fase de TI sea lo más eficiente y correcta posible:

Visión general comercial y técnica de cada sistema de apoyo de FC en el alcance

Evaluación de amenazas actual y / o el registro de amenazas



Ejemplos de ataques recientes

Informe de Targeted Threat Intelligence (TTI)

IntelCon
by Ginseg

#IntelCon2020

El TTI es un informe de inteligencia de amenazas personalizado y enfocado a la entidad a la que se le está haciendo el TIBER-EU.

El objetivo es utlizar inteligencia real relacionada con la entidad teniendo en cuenta los actores que pueden atacar a dicha entidad y diseñar escenarios de ataque que pueden seguir los atacantes.

Este proceso esta diseñado para crear escenarios de amenazas realistas que describan ataques contra la entidad. Los escenarios se basan en la evidencia disponible en el mundo real de adversarios, combinados con investigación de OSINT y conocimientos de las FC que forman parte del scope.

Aunque los escenarios buscan ser lo más realistas posibles hay ciertas limitaciones ya que el proveedor de TI (a diferencia de los posibles atacantes) tiene tiempo y recursos límitados además del cumplimiento de obligaciones éticas y legales.

Elementos de TTI

Durante el proceso de inteligencia de amenazas específicas, el proveedor de TI recopila, analiza y difunde inteligencia centrada en la FC relacionada con dos áreas clave de interés:

El objetivo (target): inteligencia o información sobre posibles superficies de ataque en toda la entidad

- Se debe de llevar a cabo reconocimiento de la entidad tal y como los atacantes suelen hacer. La meta es tener una imagen preliminar detallada de la entidad y de sus puntos débiles. Esto permitirá que la información encontrada sea puesta en contexto y que pueda ser incluida en el desarrollo de los escenarios.
- El resultado de esta actividad es la identificación de FC, de las superficies de ataque de personas, procesos y tecnologías relacionadas con la entidad y su huella digital.

La amenaza (threat): inteligencia o información sobre actores de amenaza relevantes y amenaza probable escenarios

- Utilizando el GTL o/y otras fuentes, el proveedor de TI debe identificar posibles atacantes, sus motivaciones, capacidades y TTPs. Esta información ayudará a crear los escenarios.

Elementos de TTI: Target (Objetivo) – 1/2

IntelCon by Ginseg

#IntelCon2020

Huella y exposición digital

- Funciones críticas
- Dominios/Subdominios
- Vulnerabilidades web
- Malware asociado
- IPs
- Rango de IPs
- Leaks
  - Credenciales
  - Documentos internos
- Servicios expuestos
- Perfiles digitales de VIPS y personas de interés
- APKs

Herramientas recomendadas

- VirusTotal
- DomainTools
- Shodan, Censys, Fofa, urlscan.io
- IntelX
- HaveIbeenPwned / Ghost Projetc / We leak / dehased
- Hunter.io
- PasteBin
- ExploitDB
- scans.io / Ipv4Info / Robtex
- Twint / SocialBearing
- Joesandbox.com / Hybrid Analysis

Elementos de TTI: Target (Objetivo) – 2/2

IntelCon by Ginseg

#IntelCon2020

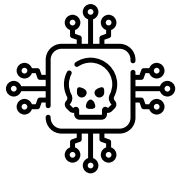
Situación estratégica

- Expansiones a otros países/sectores
- Presencia geográfica
- Fusiones y adquisiciones
- Nuevos productos/servicios
- Estrategia a corto/medio/largo plazo
- Importancia en la economía
- Geopolítica

Herramientas recomendadas

- Información interna
- Web de la entidad
- Google Dorks
- Webs/blogs especializados

Elementos de TTI: Threat (Amenaza)



Ataques conocidos

Ataques al sector financiero

Ataques al país/región

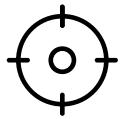
Ataques a funciones críticas

Posibles atacantes
Hipótesis

Herramientas OSINT recomendadas:

- MITRE
- Google Dorks
- X-Force
- OTX

Relación entre lo encontrado en investigación de los elementos de TTI



Objetivo

- Huella digital y exposición digital
- Situación estratégica

Amenaza

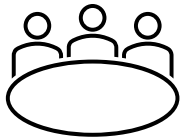
- TTPs de los posibles adversarios

Se obtiene un posible adversario que tiene capacidades y previa experiencia en atacar entidades como el objetivo. A partir de ahí se puede empezar a desarrollar los escenarios

Desarrollo de escenarios

El desarrollo del escenario representa el punto de transición clave entre TI y RT proveedores.

Usando los escenarios contenidos en el Informe TTI, el proveedor de RT debe desarrollar e integrar los escenarios de ataque en un borrador para el Plan de Test del Red Team.



Se puede realizar un taller involucrando a la entidad, al TTM y a los proveedores de TI / RT, durante lel cual el proveedor de TI va a través de los escenarios y el proveedor de RT explica el borrador del Plan de Test del Red Team.

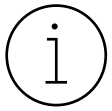
IntelCon
by Ginseg

3.2 | Fase de pruebas

Red Team

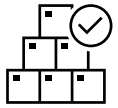
Ejecución del test

Durante la ejecución del test, el proveedor de RT debe ser lo más sigiloso posible. Los escenarios de ataque no son un libro de jugadas que debe seguirse con precisión durante el test, ya que si surgen obstáculos, el RT debe mostrar su creatividad para desarrollar formas alternativas de ataque.



Los proveedores de RT están limitados por el tiempo y los recursos disponibles, así como por límites morales, éticos y legales. Por lo tanto, es posible que el proveedor de RT pueda pedir ayuda al WT para poder progresar en el test.

El proveedor de RT debe actualizar el TTM al menos una vez a la semana, mientras que el WT debe mantenerse al tanto del progreso de manera continua.



El test debe ser realizado de manera controlada, adoptando un enfoque paso a paso, y de una manera que no conlleve riesgos para la entidad y sus FC.

Todas las acciones del RT deben registrarse para reproducirlas después con el BT

IntelCon
by Ginseg

4

Fase de cierre

Fase de cierre

IntelCon
by Ginseg

#IntelCon2020

Informes del Red Team y del Blue Team

Un borrador de los resultados del ejercicio de Red Team es mandado a la entidad y al TCT.
El Blue Team creará su propio informe basado en los resultados reflejados en el borrador del Red Team

Replay del ejercicio por parte de Red Team y Blue Team

En esta subfase se lleva a cabo una repetición del test en el que estan presentes tanto el Blue Team como el Red Team. La meta de esta etapa es la de aprender y mejorar el servicio.

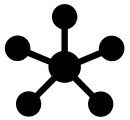
Feedback de 360º

Todos los involucrados en TIBER-EU se reunen para compartir las actividades que han ido bien y las que se pueden mejorar durante el ejercicio

Fase de cierre

La entidad, los proveedores de TI, RT y la autoridad principal deben proporcionar un certificado que confirme que la prueba se realizó de acuerdo con los requisitos básicos del marco TIBER-EU

El TCT debe analizar los resultados de todas las pruebas para identificar los hallazgos clave, las amenazas y vulnerabilidades comunes.



Después de analizarlo, el TCT puede anonimizar la información sensible y compartirlo con el TKC para ganar conocimiento y compartilo con las partes pertinentes

IntelCon
by Ginseg

5 Posible futuro del TIBER-EU

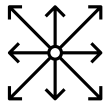
Posible futuro del TIBER-EU

IntelCon by Ginseg

#IntelCon2020

Obligación normativa

Ahora mismo realizar el TIBER-EU es optativo, sin embargo, dada la adopción de otros países (tanto de la Unión Europea como de fuera) , es posible que en un futuro sea obligatorio.



Expansión del marco financiero a otros sectores

El TIBER-EU fue concebido para ser realizado en entidades financieras, sin embargo, dada su popularidad y naturaleza, es factible la expansión y adaptabilidad a otros sectores: Telecomunicaciones, Infraestructuras críticas, sector público, industrial …

Estandarización

La implementación del TIBER-EU permitirá que haya una estandarización de procedimientos en relación a ejercicios de Red Team dirigidos por TI a nivel internacional.

IntelCon
by Ginseg

6

Escenario Ficticio de TI

Inicio

IntelCon by Ginseg

#IntelCon2020

IntelCon Bank – Ejercicio ficticio del TIBER

IntelCon Bank ha facilitado la siguiente información:

- El banco tiene 235 sucursales en Bélgica y 143 fuera del país
- Está llevando a cabo una transformación digital y en 5 años planea estar completamente digitalizado
- Es el banco Europeo que más ha facturado en 2019 aunque está notando el bajón a causa de la pandemia
- Ha listado como Funciones Críticas:
    - Las aplicaciones bancarias con las que monitorean el comportamiento de los clientes
    - SWIFT y conexiones terceras con proveedores bancarios y tecnológicos.
    - Aplicaciones con las que se llevan a cabo ecuaciones para calcular las tendencias del mercado

TI - Investigación del objetivo 1/2

Resultados de una investigación de huella y exposición digital perimetral

Se han descubierto

- 125 dominios asociados al objetivo
- 44 IPs
- 3 rangos de IP
- 16 documentos internos
- Emails corporativos de 407 empleados
  - 155 de ellos con contraseñas en claro
  - Emails corporativos de 32 personas de interés
  - 4 de ellos con contraseñas en claro
- 23 APKs presentes en mercados no legitimas
  - 15 de ellas con versiones sin actualizar
- 65 servicios expuestos
  - 3 FTP, 23 HTTP, 1 Telnet, etc
- 81 dominios de posible typosquatting
- 21 dominios de posible cybersquatting
- 14 vulnerabilidades web asociadas a dominios

TI – Investigación del objetivo (2/2)

IntelCon by Ginseg

#IntelCon2020

Resultados de una investigación de situación estratégica

Se ha descubierto lo siguiente:

Sobre IntelCon Bank

- En su esfuerzo por ser más digital, IntelCon Bank ha adquirido numerosas empresas de desarrollo de software
- Debido a la crisis del Covid-19 y la digitalización de servicios, el banco tiene planeado despedir a 2.000 empleados
- Sólo está presente en Europa, pero en el futuro planea expandirse a otros países fuera de Europa

Sobre la situación geopolítica

- Existen tensiones con EEUU y China
- Es el banco de elección para las principales instituciones Europeas con sede en Bruselas
- IntelCon Bank tiene gran influencia en el ámbito económico y social en Europa

TI – Investigación de la amenaza (1/3)

IntelCon by Ginseg

#IntelCon2020

Actores que tienen capacidades y motivación para atacar

Grupos apoyados por un país

Motivación Alta

Capacidad Alta

Grupos ciber criminales

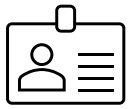
Motivación Alta

Capacidad Media

Hacktivistas

Motivación Media

Capacidad Media



Insiders

Motivación Alta

Capacidad Baja

TI – Investigación de la amenaza (2/3)

IntelCon by Ginseg

#IntelCon2020

Actores con experiencia en ataques a este tipo de cliente

Lazarus Group	• Ataques motivados por el dinero y la geopolítica • Experiencia atacando al sector financiero • Se conoce un caso de la explotación de SWIFT (una de las funciones críticas de IntelCon Bank)
Fancy Bear	• Ataques motivados por la geopolítica • Arsenal de TTPs muy sofísticado • Experiencia atacando a instituciones gubernamentales/diplomáticas/militares
Carbanak	• Ataques motivados por el dinero • Experiencia atacando al sector financiero • No parece haber discriminación por países/regiones

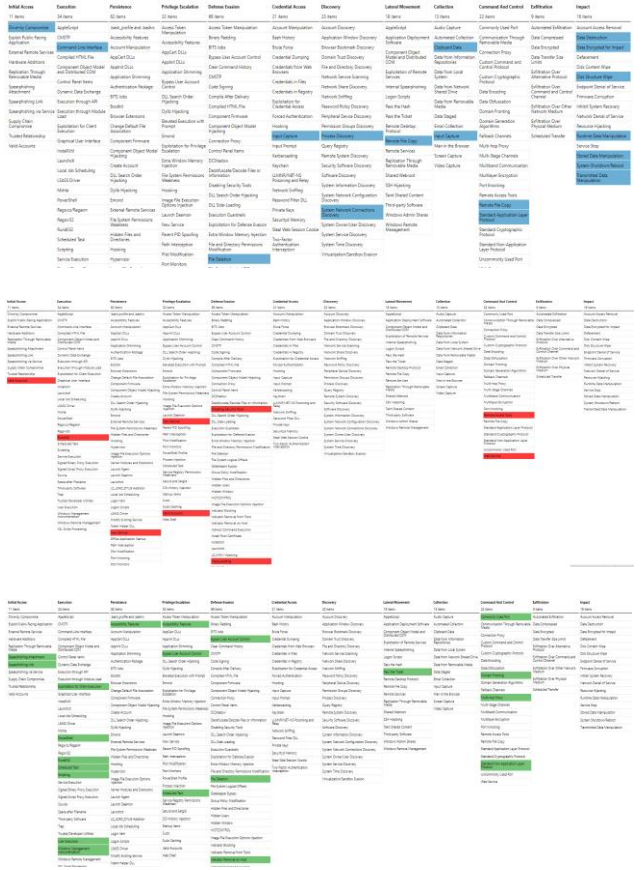
TI – Investigación de la amenaza (3/3)

Comparación de TTPs

A continuación, se analizan los TTPs de los actores que tienen más posibilidades de atacar a IntelCon Bank.

- Los TTPs del actor deben de encajar con la información proporcionada por el banco y con la inteligencia recopilada durante la fase de investigación

- Una vez encontrado el actor ideal, se procede a desarrollar un escenario



TI – Desarrollo del escenario

IntelCon by Ginseg

#IntelCon2020

Desarrollo del escenario

El escenario esta basado en toda la información obtenida en anteriores fases. Normalmente los escenarios siguen la metodología siguiente:

El objetivo del escenario es de proveer al Red Team de un plan de ataque realista basado en inteligencia real

#IntelCon2020

IntelCon
by Ginseg

Gracias por la atención

@BentanachsPablo

Congreso Online de Ciberinteligencia | Julio 2020