sedian

Seguridad Digital
de Andalucía

Charla virtual

Análisis de intrusiones: conoce a tu enemigo

Mayo 2020

Junta de Andalucía

SOBRE MÍ

Jose Luis Sánchez Martínez

- Cyber Threat Intelligence Manager MNEMO CSIRT FINANCIERO
- SANS FOR578 Cyber Threat Intelligence
- GIAC Cyber Threat Intelligence
- UCAM Máster en Ciberseguridad
- UDIMA Perito Informático Judicial
- UMA Ingeniería Inversa y Malware Intelligence

linkedin.com/in/joseluissm

@Joseliyo_Jstnk

joselsm94@mnemo.com

OBJETIVOS

- Definir los objetivos de la Inteligencia de Ciberamenazas (Cyber Threat Intelligence)
- Entender y aplicar diferentes marcos y metodologías en una intrusión
  - Cadena de Intrusión (Kill Chain)
  - Modelo diamante (Diamond Model)
  - ATT&CK de MITRE
- Identificar aquellas brechas de defensa que puedan existir y priorizar esfuerzos
- Generar agrupamientos de comportamientos

Y lo más importante: Entender cómo trabajan los equipos de Inteligencia de Ciberamenazas

¿Qué NO es Inteligencia de Ciberamenazas?

- Indicadores de compromiso
- Direcciones IP
- Dominios
- Hashes
- Nombres de ficheros
- Inteligencia únicamente
- APTs
- Malware
- Noticias
- Boletines

¿Qué es Inteligencia de Ciberamenazas?

El principal objetivo de CTI, es el **humano**, la **atribución**

CTI

Información analizada sobre un intento hostil, capacidades y oportunidades de un adversario para completar un requerimiento.

Es muy importante conocer las **motivaciones y objetivos** de los adversarios.

iveles de inteligencia y audiencias

Estratégico	• CISO • Toma de decisiones • Gestión de riesgos
Operacional	• CTI • TTPs • Atribución
Táctico	• SOC/CERT • IOCs • Bloqueos

Pueden existir diferentes reportes

Lo que llevaría a dirigirlos a diferentes audiencias según los contenidos.

- Reporte de análisis de malware
- Reporte con indicadores de compromiso
- Reporte de comportamiento de un APT
- Reporte del estado de seguridad frente un APT

¿Qué entendemos por intrusión?

CYBER INTRUSION

Cyber Intrusion is to compromise a computer system by breaking the security of such a system or causing it to enter into an insecure state. The act of intruding or gaining unauthorized access to a system typically leaves traces that can be discovered by Intrusion Detection Systems.

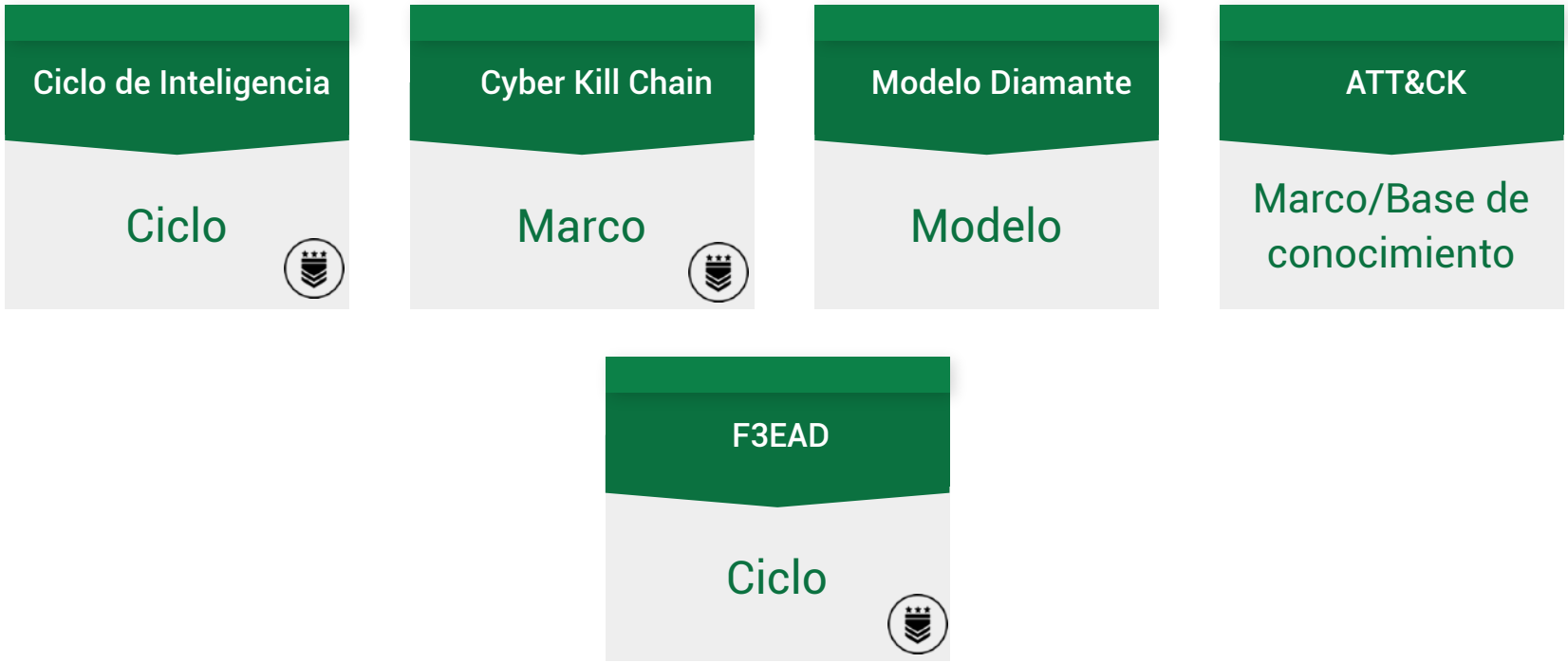
Cualquier intento de un adversario, ya sea **exitoso o fallido** para comprometer un sistema.

SANS INSTITUTE

U.S. DEPARTMENT OF HOMELAND SECURITY

CISA
CYBER+INFRASTRUCTURE

Metodologías, frameworks, modelos, ciclos…

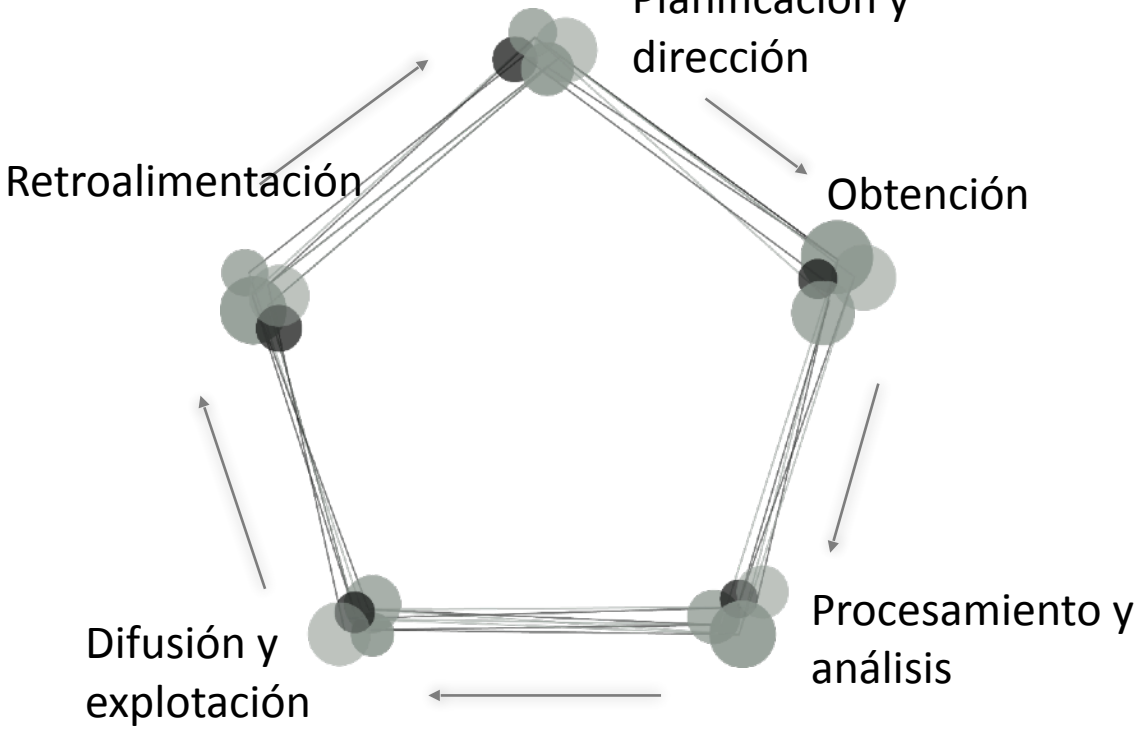


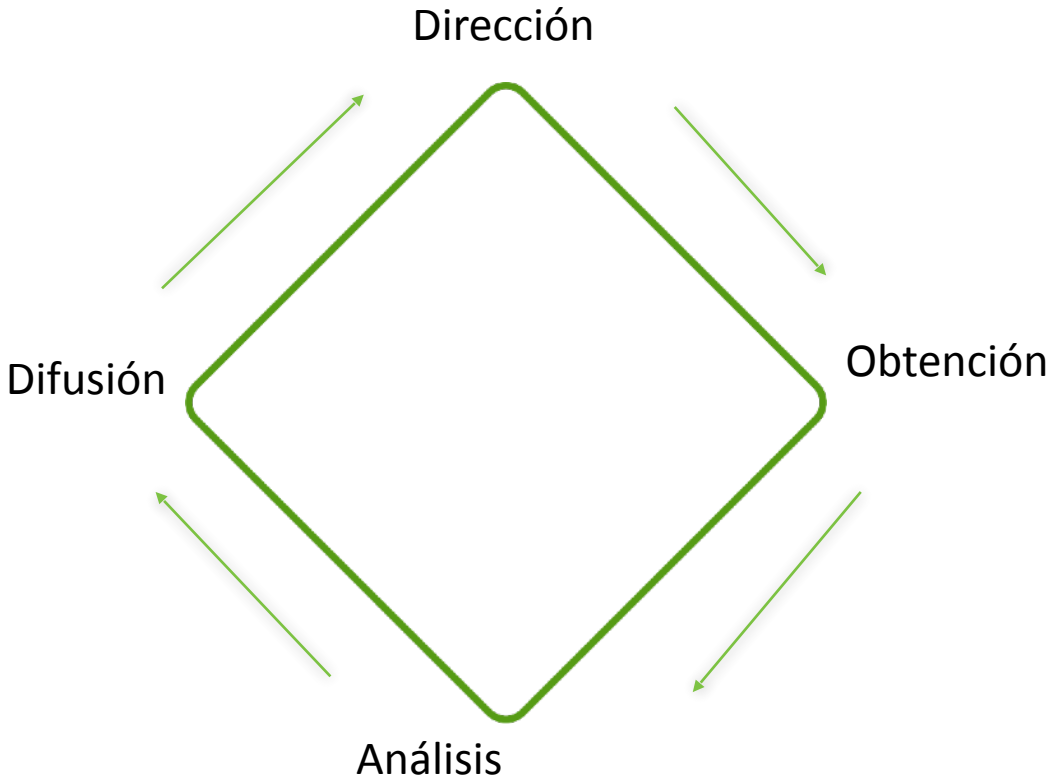
¿Qué tienen en común y por qué son importantes?

- Muchos de ellos vienen del mundo militar
- Nos ayudan a estructurar nuestro trabajo e ir paso a paso
- Nos pueden abstraer de sesgos analíticos
- Podemos adaptarlos a nuestras necesidades, son estándares pero no normativas

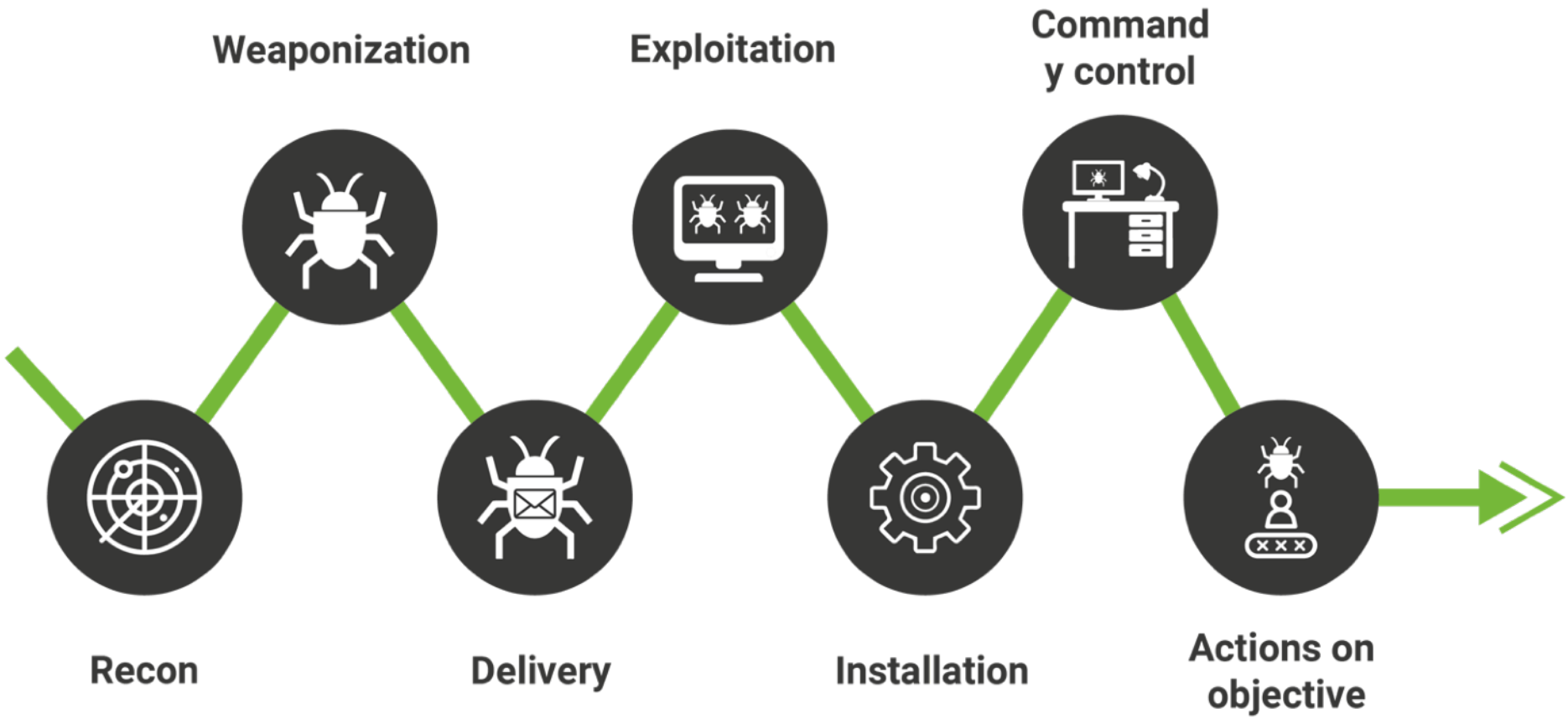
Data into buckets
(Datos en cubos)

Ciclo de inteligencia

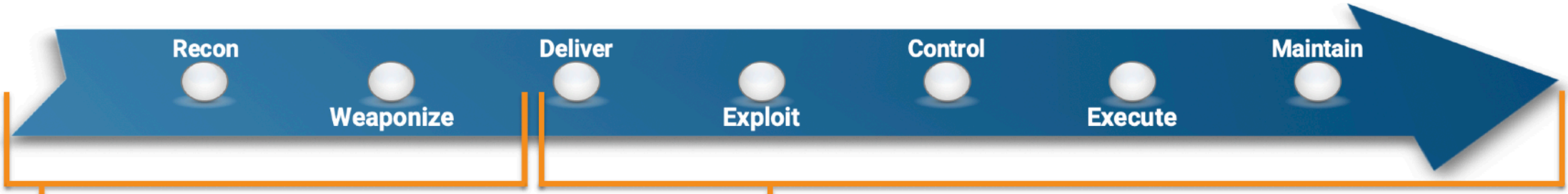




Cyber Kill Chain



ATT&CK MITRE



PRE-ATT&CK

- Priority Definition
  - Planning, Direction
- Target Selection
- Information Gathering
  - Technical, People, Organizational
- Weakness Identification
  - Technical, People, Organizational
- Adversary OpSec
- Establish & Maintain Infrastructure
- Persona Development
- Build Capabilities
- Test Capabilities
- Stage Capabilities

ATT&CK for Enterprise

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration
- Command and Control
- Impact

ATT&CK MITRE

MITRE ATT&CK® Navigator

Enterprise x +

selection controls | layer controls | technique controls

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Graphical User Interface	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	InstallUtil	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	Launchctl	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
	Local Job Scheduling	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Service Stop
	LSASS Driver	Create Account	Hooking	DCShadow	Keychain	Remote System Discovery	SSH Hijacking		Multilayer Encryption		Stored Data Manipulation
	Mshta	DLL Search Order Hijacking	Image File Execution Options	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Taint Shared Content		Port Knocking		System Shutdown/Reboot
	PowerShell	Dylib Hijacking		Disabling Security Tools	Network Sniffing	Software Discovery	Third-party Software		Remote Access Tools		Transmitted Data Manipulation
		Emond		DLL Search Order Hijacking	Password Filter DLL	System Information Discovery					
				DLL Side-Loading		System Network Configuration Discovery					
				Execution Guardrails							

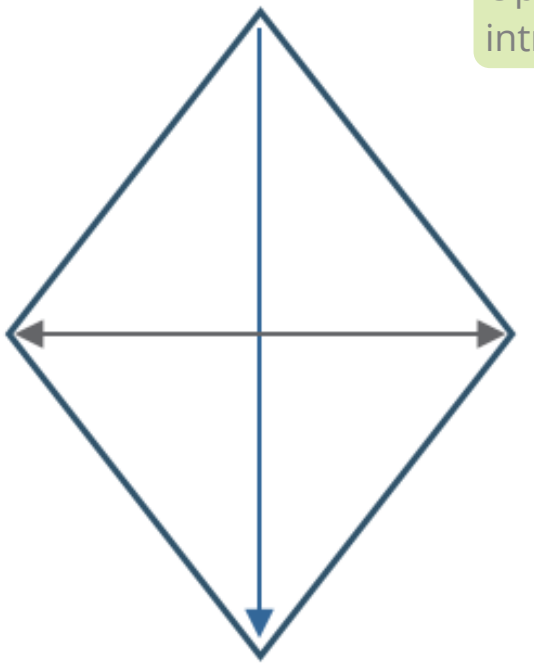
Modelo diamante

ADVERSARIO

Operador, adversario o actor de la intrusión

INFRAESTRUCTURA

Estructuras físicas y/o lógicas de comunicación que el adversario utiliza para mantener el control de sus capacidades desplegadas



CAPACIDADES

Herramientas, técnicas, métodos y vulnerabilidades utilizadas durante la intrusión para conseguir su objetivo

VÍCTIMA

Es el objetivo del adversario. Puede ser víctima física o víctima lógica.

En el contexto de CTI trabajamos en dos escenarios

1. Aquellas intrusiones que han ocurrido de manera interna en nuestra organización o de clientes y que necesitan respuestas como:

- ¿Quién?
- ¿Por qué?
- ¿Cómo?
- ¿Qué?
- ¿Cuándo?
- ¿Dónde?

2. Aquellas intrusiones públicas que pueden ser interesantes investigar y llevar a cabo acciones de seguridad activa en nuestra organización o de clientes.

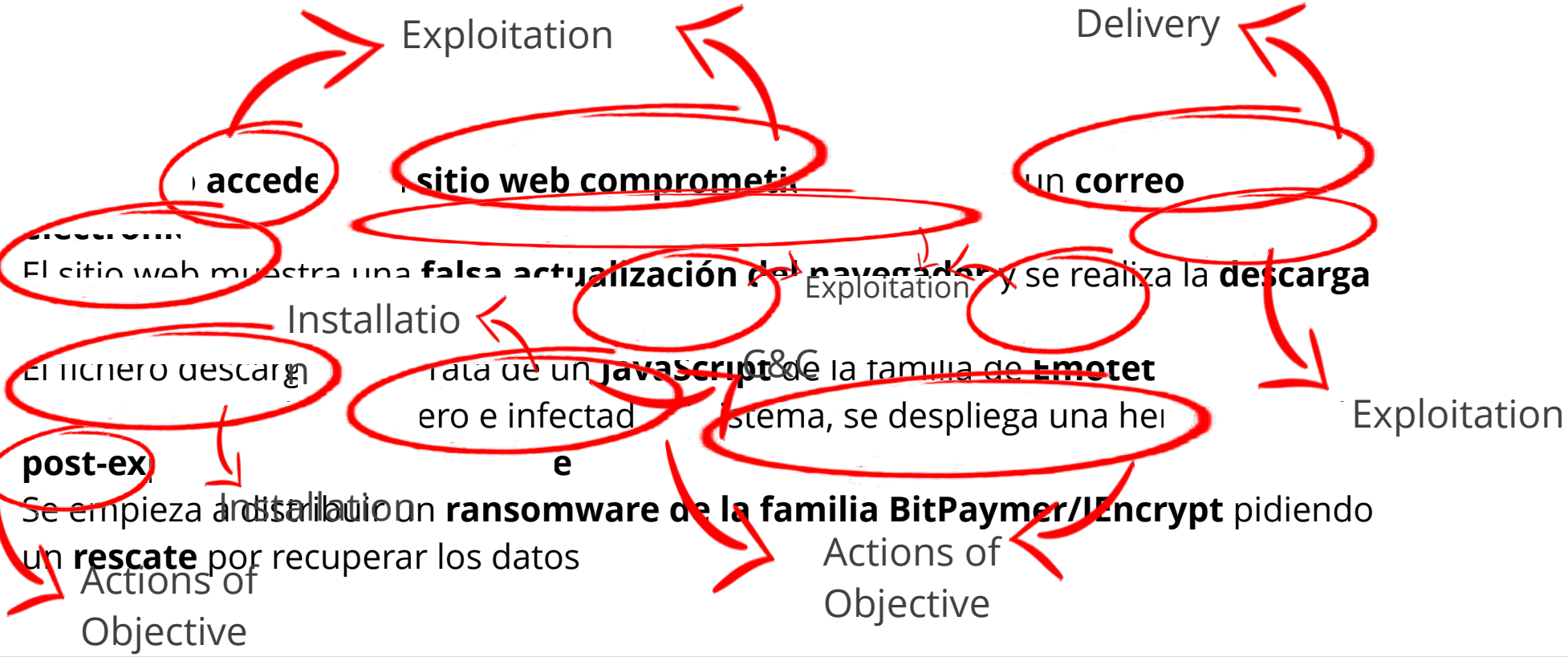
Intrusión – Poniéndonos en la piel de un analista CTI

1. Un usuario accede a un sitio web comprometido a través de un correo electrónico
2. El sitio web muestra una falsa actualización del navegador y se realiza la descarga de un fichero
3. El fichero descargado se trata de un JavaScript de la familia de Emotet
4. Una vez ejecutado el fichero e infectado el sistema, se despliega una herramienta de post-explotación llamada Empire
5. Se empieza a distribuir un ransomware de la familia BitPaymer/IEncrypt pidiendo un rescate por recuperar los datos

Intrusión – Poniéndonos en la piel de un analista CTI

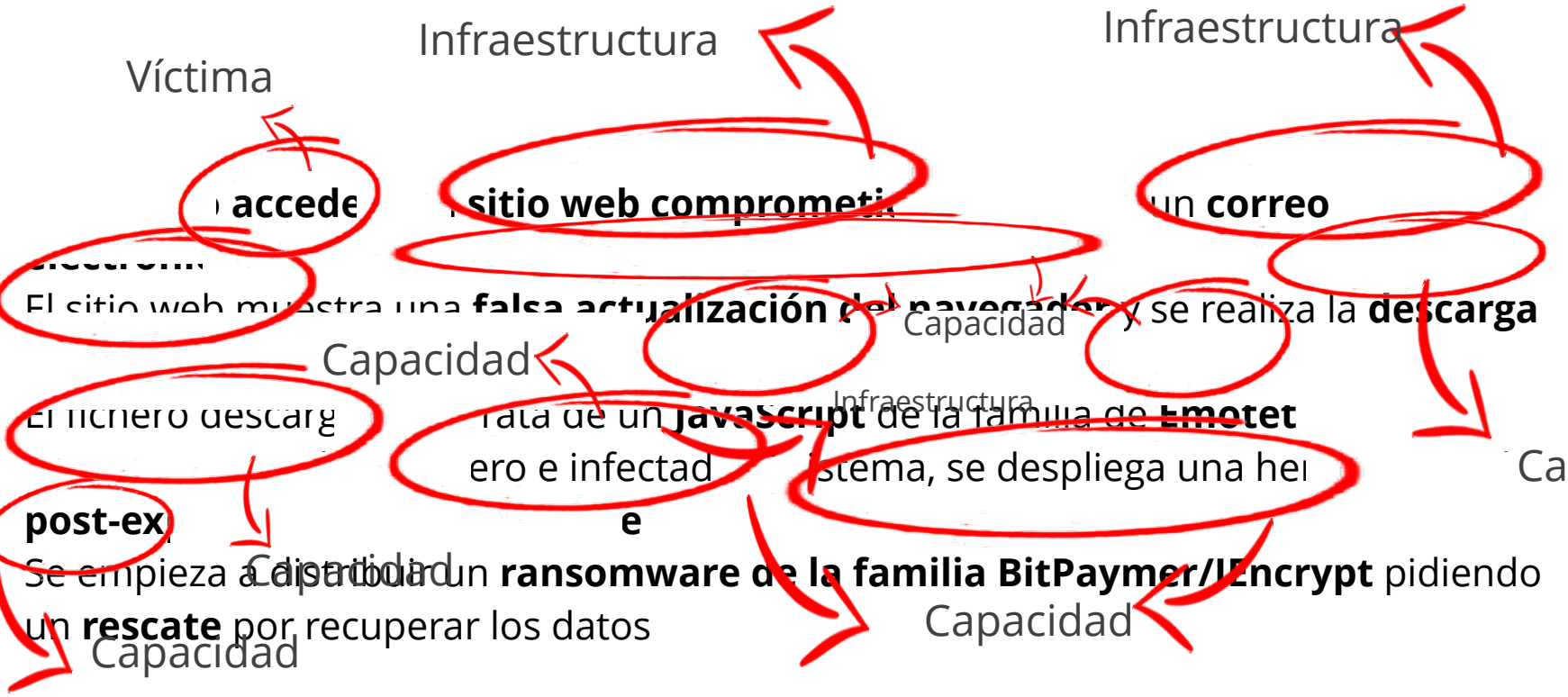
1. accede sitio web comprometido correo electrónico
2. falsa actualización del navegador descarga de un fichero
3. JavaScript Emotet
4. post-explotación Empire
5. ransomware familia BitPaymer/lEncrypt rescate

Intrusión – Poniéndonos en la piel de un analis
CTI



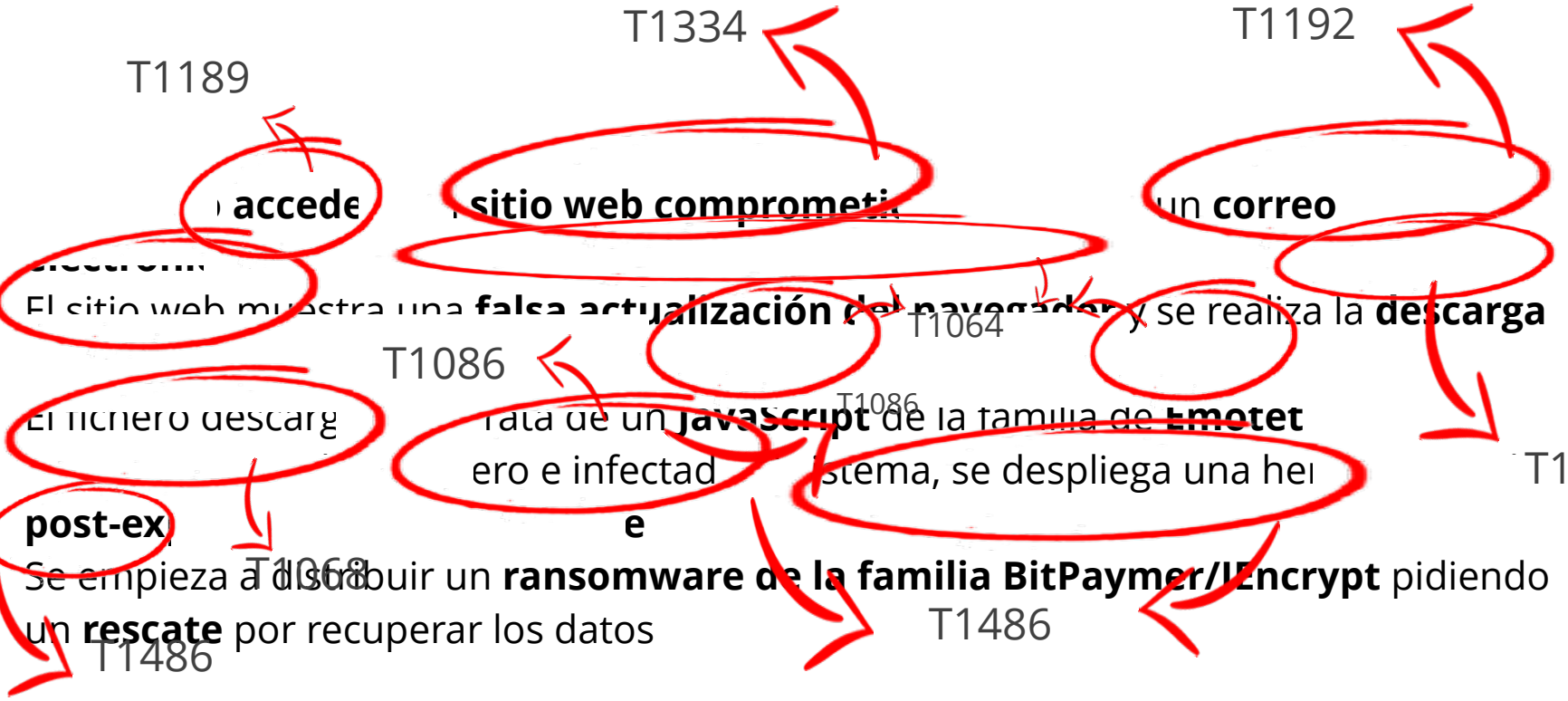
1. **accede** **sitio web comprometi** un **correo**
2. El sitio web muestra una **falsa actualización del navegador** y se realiza la **descarga**
3. El fichero descarg tata de un **javascript** de la familia de **Emotet**
4. ero e infectad stema, se despliega una her **post-ex** **e**
5. Se empieza a distribuir un **ransomware de la familia BitPaymer/IEncrypt** pidiendo un **rescate** por recuperar los datos

Intrusión – Poniéndonos en la piel de un analis
CTI



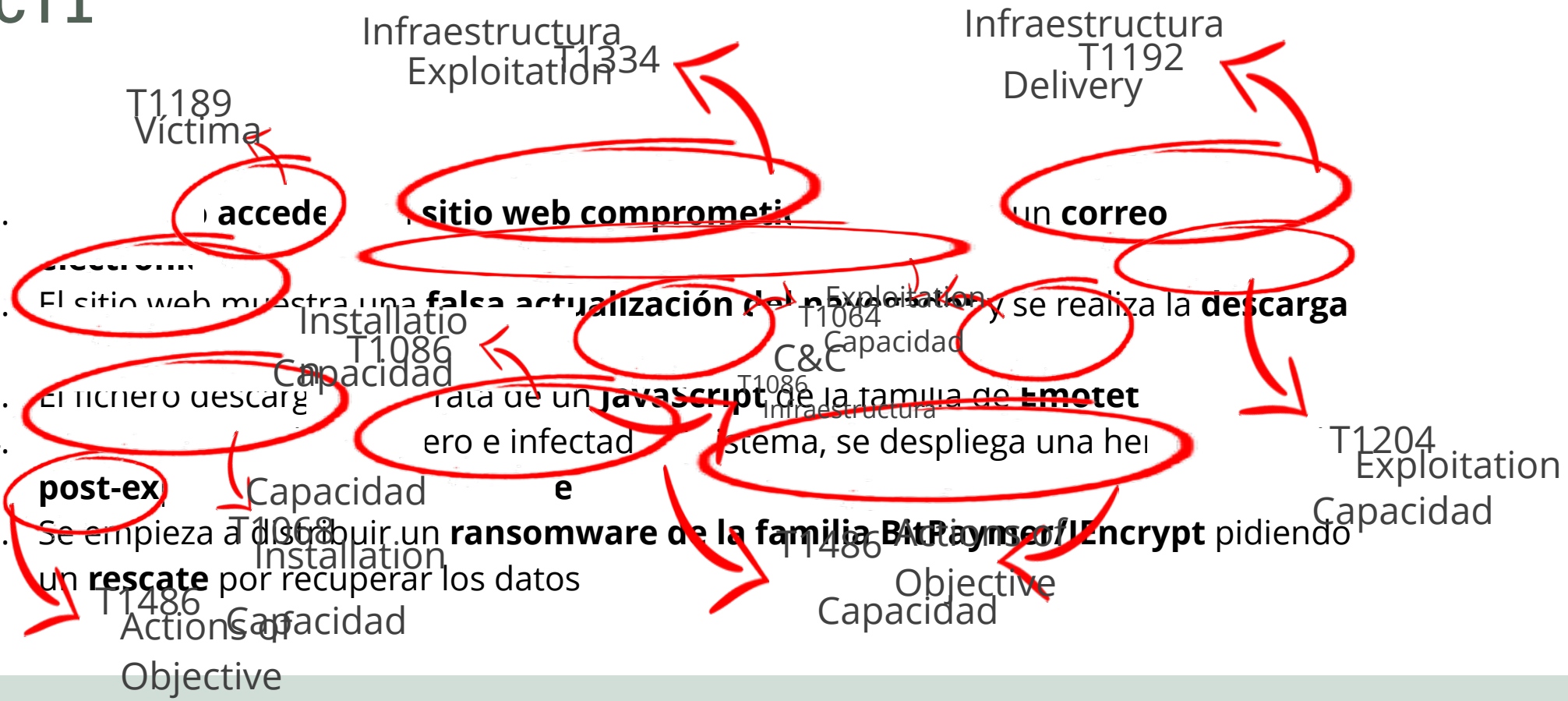
1. **accede** **sitio web comprometi** un **correo**
2. El sitio web muestra una **falsa actualización del navegador** y se realiza la **descarga**
3. El fichero descarg tata de un **javascript** de la familia de **Emotet**
4. ero e infectad stema, se despliega una her **post-ex** **e**
5. Se empieza a distribuir un **ransomware de la familia BitPaymer/IEncrypt** pidiendo un **rescate** por recuperar los datos

Intrusión – Poniéndonos en la piel de un analis CTI



1. **accede** **sitio web comprometi** un **correo**
2. El sitio web muestra una **falsa actualización del navegador** y se realiza la **descarga**
3. El fichero descarg fata de un **javascript** de la familia de **Emotet**
4. ero e infectad stema, se despliega una her **post-ex** **e**
5. Se empieza a distribuir un **ransomware de la familia BitPaymer/IEncrypt** pidiendo un **rescate** por recuperar los datos

Intrusión – Poniéndonos en la piel de un analis
CTI

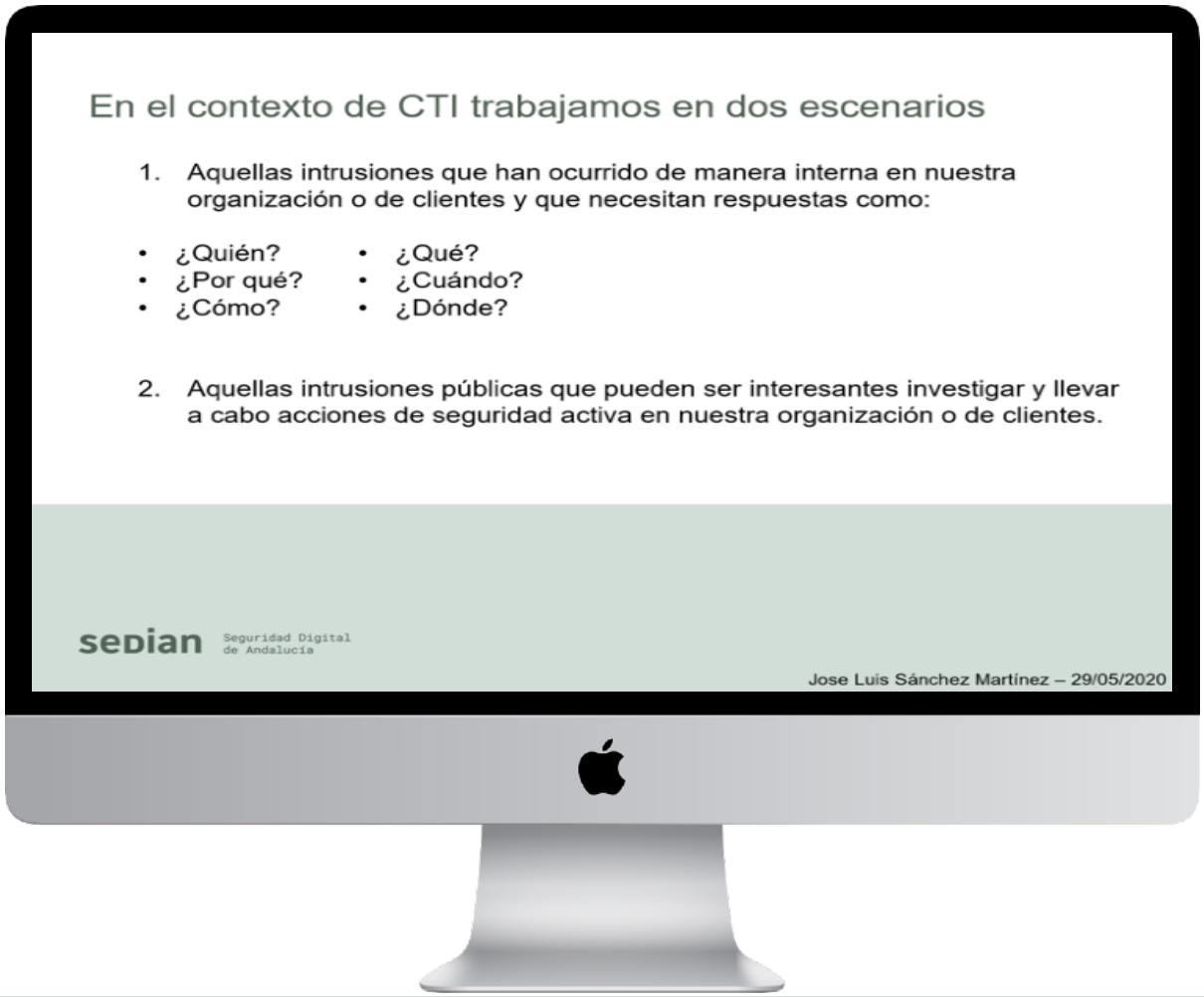


1. **accede** **sitio web comprometi** un **correo**
2. El sitio web muestra una **falsa actualización del navegador** y se realiza la **descarga**
3. El fichero descarg **fala de un javascript** de la familia de **Emotet**
4. **ero e infectad** **stema, se despliega una hei**
   post-ex **e**
5. Se empieza a distribuir un **ransomware de la familia BitPaymer/IEncrypt** pidiendo un **rescate** por recuperar los datos

¿Por dónde empiezo?

En este caso, como vamos a trabajar a partir de inteligencia de terceros, empezaremos desde la fase de Recon.

Cuando se investigue una intrusión que esté ocurriendo, se empezará por donde dicte el descubrimiento (C2, Installation, AoO, etc...)



welivesecurity BY ESET

Grandoreiro: análisis de un troyano bancario dirigido a Brasil, España, México y Perú

Una de las particularidades de este troyano bancario que se distribuye a través de correos spam es la forma de agrandar el tamaño de los archivos EXE para evitar la detección.

sedian Seguridad Digital de Andalucía

Reconocimiento (Reconnaissance)

En esta fase el cibercriminal realiza acciones de reconocimiento sobre sus víctimas. En aquellos casos donde no tengan víctima fija, pueden utilizar recolección de información a través de diferentes técnicas como herramientas de footprinting, fugas de emails, emails permutators, etc...

Por lo general, casi siempre vamos a desconocer como ha sido exactamente el reconocimiento, no obstante podemos llegar a intuirlo por el contexto de la intrusión, sino, se pueden generar hipótesis.

Algunos de los puntos que los actores llevan a cabo en esta fase son los siguientes:

Identificación de las víctimas

Personas
Organizaciones

Investigación de la organización

Tecnología
Negocio

Adquisición de infraestructuras

Dominios
Emails

Reconocimiento

EJEMPLO NO REAL

```
178.44.144.231 - - [03/Nov/2019:18:57:24 +0100] "GET /administrator/ HTTP/1.1" 200 4263 "-" "Mozilla/5.0 (Windows NT 6.0; rv:34.0) Gecko/20100101 Firefox/34.0" "-"
178.44.144.231 - - [03/Nov/2019:18:57:24 +0100] "POST /administrator/index.php HTTP/1.1" 200 4494 "https://www.google.es/search?ei=vzrDXYmUEPiZjLsPkNabuAk&q=site%3
213.24.134.32 - - [03/Nov/2019:18:58:50 +0100] "GET /administrator/ HTTP/1.1" 200 4263 "-" "Mozilla/5.0 (Windows NT 6.0; rv:34.0) Gecko/20100101 Firefox/34.0" "-"
213.24.134.32 - - [03/Nov/2019:18:58:51 +0100] "POST /administrator/index.php HTTP/1.1" 200 4494 "https://www.google.es/search?ei=yzrDXdyKGueBjLsP4M-B4A4&q=site%3A
213.24.134.32 - - [03/Nov/2019:19:02:35 +0100] "GET / HTTP/1.1" 200 10439 "https://www.google.es/search?ei=PzvDXZCdDvyLjLsP-siKmAc&q=site%3Aexample.com+Alberto+Ser
```

```
0 4263 "-" "Mozilla/5.0 (Windows NT 6.0; rv:34.0) Gecko/20100101 Firefox/34.0" "-"
TP/1.1" 200 4494 "https://www.google.es/search?ei=vzrDXYmUEPiZjLsPkNabuAk&q=site%3Aexample.com+filetype%3Apdf+%22admin%22&oq=site%3Aexample.com+filetype%3Apdf+%22ad
 4263 "-" "Mozilla/5.0 (Windows NT 6.0; rv:34.0) Gecko/20100101 Firefox/34.0" "-"
P/1.1" 200 4494 "https://www.google.es/search?ei=yzrDXdyKGueBjLsP4M-B4A4&q=site%3Aexample.com+intitle%3Aphpmyadmin&oq=site%3Aexample.com+intitle%3Aphpmyadmin&gs_l=p
://www.google.es/search?ei=PzvDXZCdDvyLjLsP-siKmAc&q=site%3Aexample.com+Alberto+Serrano+Caballero+-site%3Alinkedin.com+%22CEO%22&oq=site%3Aexample.com+Alberto+Serra
```

```
lla/5.0 (Windows NT 6.0; rv:34.0) Gecko/20100101 Firefox/34.0" "-"
 "https://www.google.es/search?ei=vzrDXYmUEPiZjLsPkNabuAk&q=site%3Aexample.com+filetype%3Apdf+%22admin%22
la/5.0 (Windows NT 6.0; rv:34.0) Gecko/20100101 Firefox/34.0" "-"
"https://www.google.es/search?ei=yzrDXdyKGueBjLsP4M-B4A4&q=site%3Aexample.com+intitle%3Aphpmyadmin&oq=sit
/search?ei=PzvDXZCdDvyLjLsP-siKmAc&q=site%3Aexample.com+Alberto+Serrano+Caballero+-site%3Alinkedin.com+%2
```

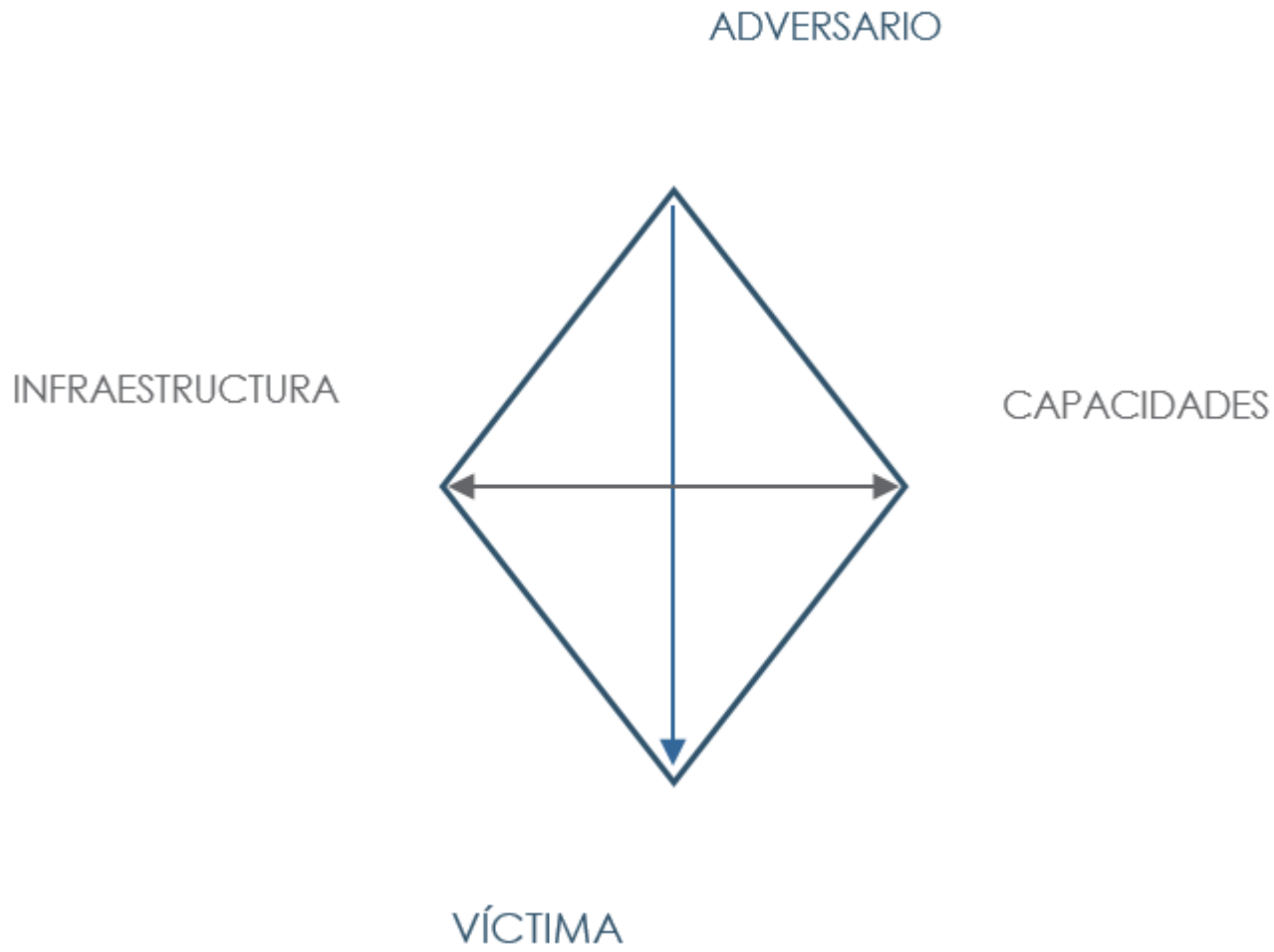
```
.la/5.0 (Windows NT 6.0; rv:34.0) Gecko/20100101 Firefox/34.0" "-"
 "https://www.google.es/search?ei=vzrDXYmUEPiZjLsPkNabuAk&q=site%3Aexample.com+filetype%3Apdf+%22admin%22
.a/5.0 (Windows NT 6.0; rv:34.0) Gecko/20100101 Firefox/34.0" "-"
'https://www.google.es/search?ei=yzrDXdyKGueBjLsP4M-B4A4&q=site%3Aexample.com+intitle%3Aphpmyadmin&oq=sit
'search?ei=PzvDXZCdDvyLjLsP-siKmAc&q=site%3Aexample.com+Alberto+Serrano+Caballero+-site%3Alinkedin.com+%2
```

Reconocimiento

RECON

- Selección de víctima
- Adquisición de información sobre la infraestructura

- Alberto Serrano Caballero
- 213.24.134.32
- 178.44.144.231
- Google Hacking
- SRVLDPHA10



Reconocimiento

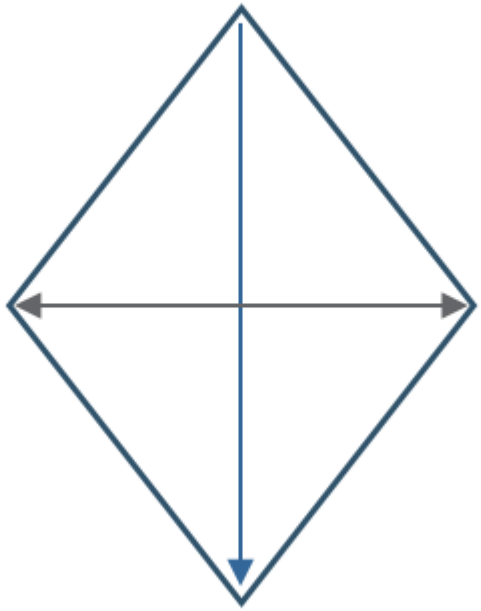
RECON

- Selección de víctima
- Adquisición de información sobre la infraestructura

ADVERSARIO

INFRAESTRUCTURA

213.24.134.32
178.44.144.231



CAPACIDADES

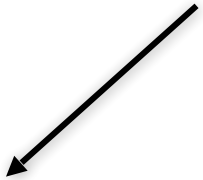
Google Hacking

VÍCTIMA

Alberto Serrano Caballero
SRVLDPHA10

Reconocimiento

- Alberto Serrano Caballero
- 213.24.134.32
- 178.44.144.231
- Google Hacking
- SRVLDPHA10



Reconnaissance

Weaponization

Delivery

Exploitation

Installation

Command y Control

Actions on objective

Armamento (Weaponization)

Proceso en el que el actor pone en conjunto todas las herramientas e infraestructura que va a usar en su misión

Preparan diferentes websites donde alojarán el malware. Además, utilizarán temáticas de Covid-19 para mostrar contenido en la web.

Preparan diferentes tipos de códigos maliciosos. Vistos hasta el momento los siguientes:

- MSI
- VB
- ZIP

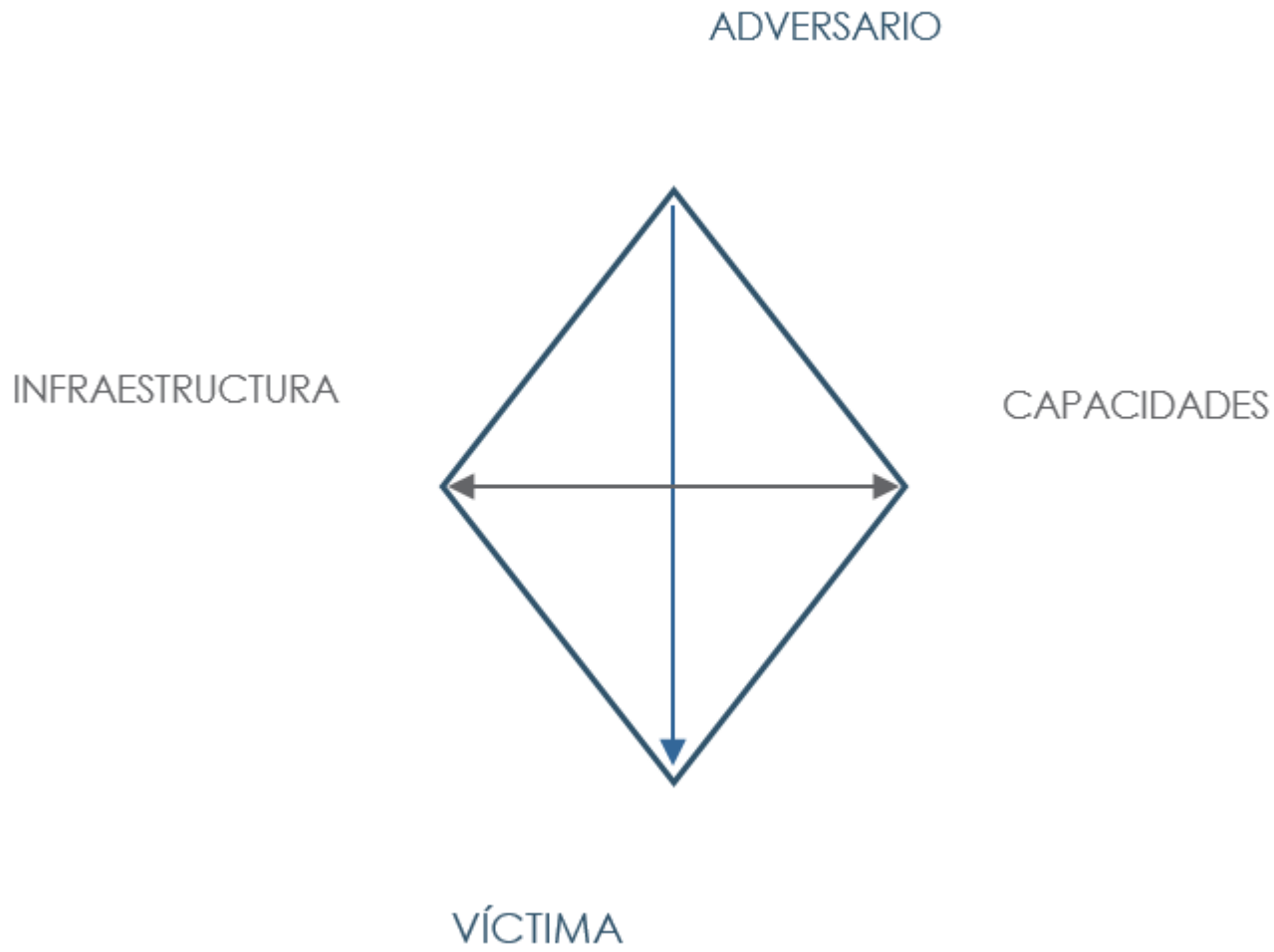
Configuración de los C&C alojados en Google Sites

Armamento

WEAPONIZATION

- Generación de código malicioso
- Adquisición de websites

- Malware en ficheros MSI
- Malware en ficheros VBS
- Malware comprimido en ZIP
- Adquisición de dominios
- Configuración de Google Sites
- Preparación de MalSpam



Armamento

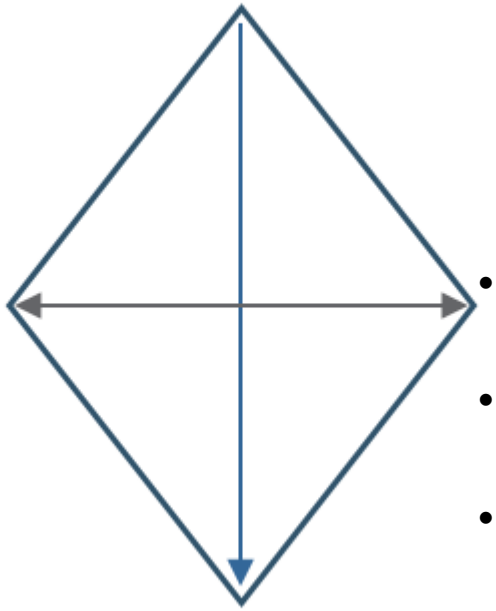
WEAPONIZATION

- Generación de código malicioso
- Adquisición de websites

ADVERSARIO

INFRAESTRUCTURA

- Adquisición de dominios
- Configuración de Google Sites

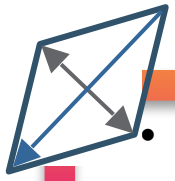


CAPACIDADES

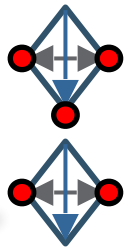
- Malware en ficheros MSI
- Malware en ficheros VBS
- Malware comprimido en ZIP
- Preparación de MalSpam

VÍCTIMA

Armamento



- Malware en ficheros MSI
- Malware en ficheros VBS
- Malware comprimido en ZIP
- Adquisición de dominios
- Configuración de Google Sites
- Preparación de MalSpam



Reconnaissance

Weaponization

Delivery

Exploitation

Installation

Command y Control

Actions on objective

Distribución (Delivery)

Momento en el que el actor empieza la operación contra su víctima. Puede ser un Spearphishing, seguimiento de una persona de manera física e incluso un iframe en un sitio web explotado.

Envían correos electrónicos genéricos con información relacionada al Covid-19, facturas, y falsas actualizaciones. Dichos correos, contienen links a sitios web controlados por los adversarios. Las víctimas son de oportunidad, es decir, reemplazables (no tienen una víctima de interés).

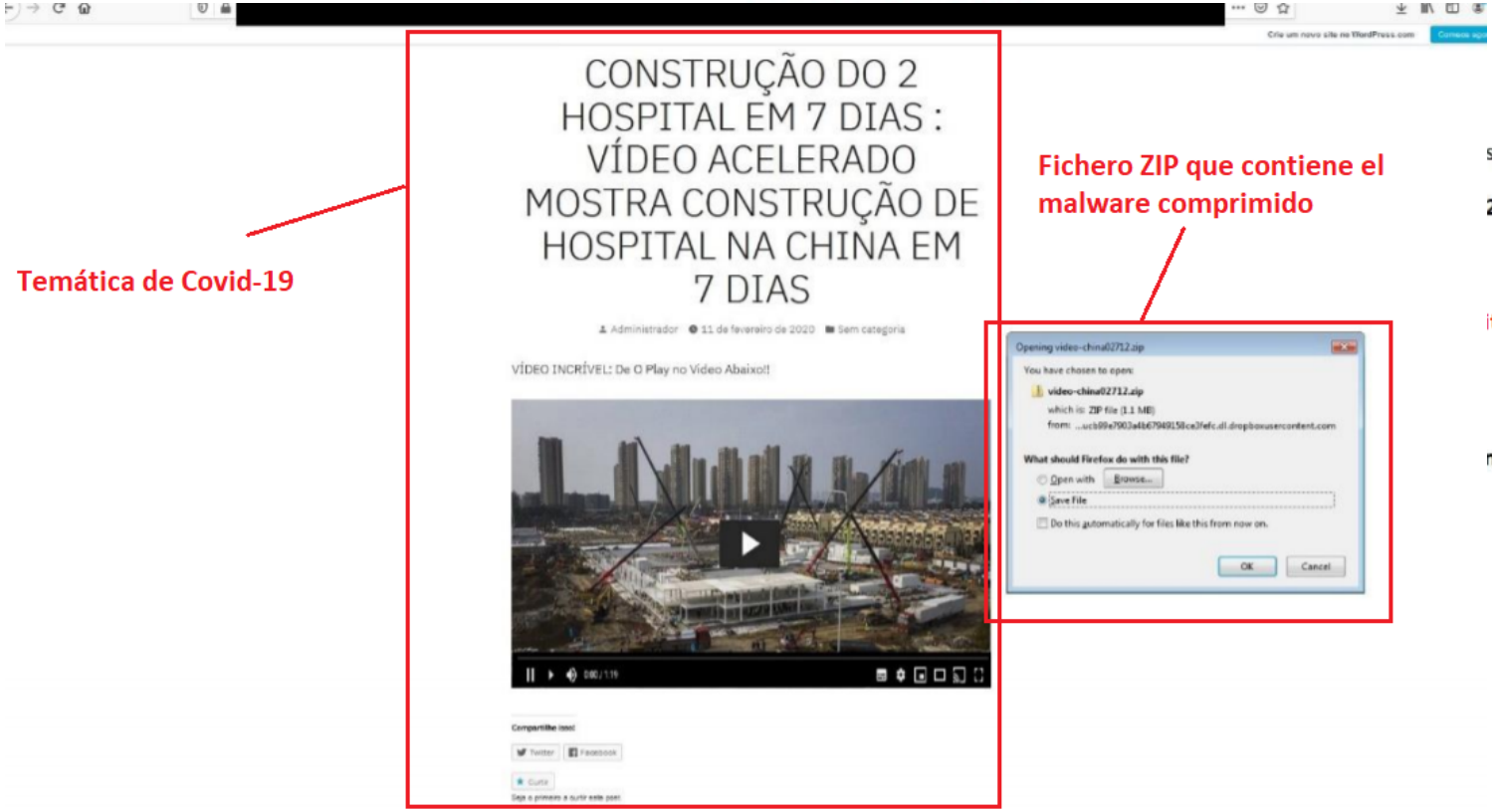
Dependiendo de la temática usada en el correo, la página web mostrará contenido relacionado. Desde estos sitios, se realiza la descarga de los diferentes códigos maliciosos preparados en la fase anterior.

Distribución

De: Cobro de pagos -008 <facturaoficial08@theprojectsecurity.onmicrosoft.com>
Enviado el: miércoles, 15 de abril de 2020 8:57
Para: [redacted]
Asunto: Factura - VU17R

Asunto del email

Nombre y correo electrónico usado para la distribución



Temática de Covid-19

Fichero ZIP que contiene el malware comprimido

s, la factura **7N6NOJJHS1AZAUZJ0ZHARYMH5**.

2020 suspenderemos los servicios y pasaremos su cuenta a nuestros

itio web

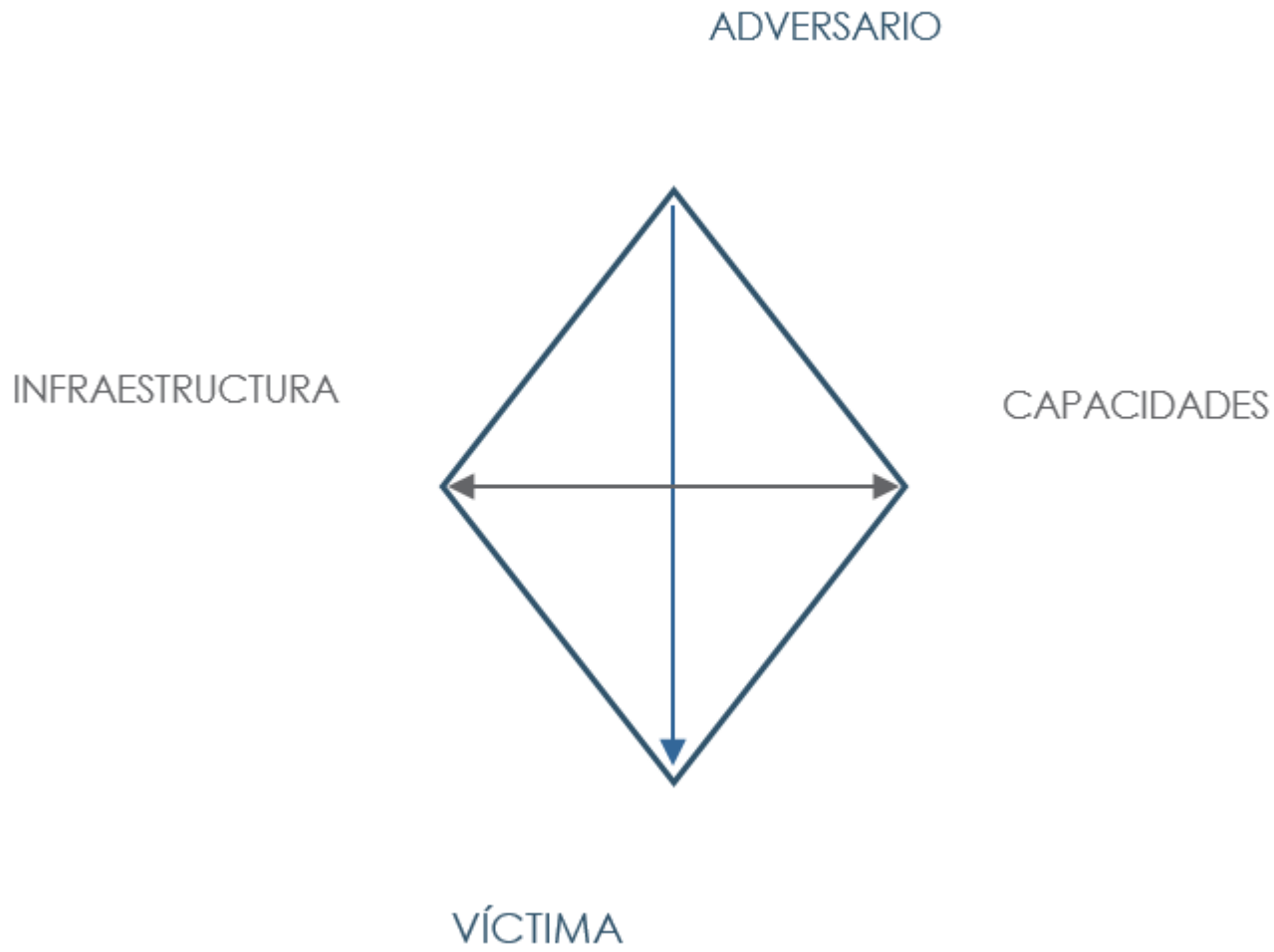
mputadora.

Distribución

DELIVERY

- Envío de correos a las víctimas
- Distribución de malware mediante aplicaciones web

- MalSpam a diferentes víctimas con link
- Template Covid-19
- Template Factura
- Template Falsa actualización
- facturaoficial08@theprojectsecurity.onmicrosoft.com
- Asunto: Factura - VU17R



Distribución

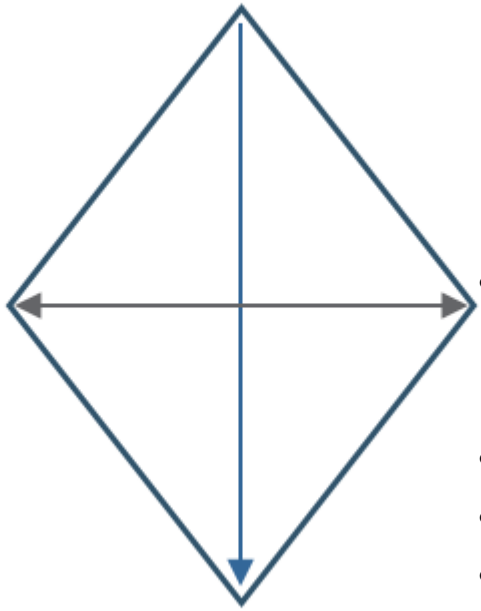
DELIVERY

- Envío de correos a las víctimas
- Distribución de malware mediante aplicaciones web

ADVERSARIO

INFRAESTRUCTURA

- facturaoficial08@theprojectsecurity.onmicrosoft.com
- Web maliciosa

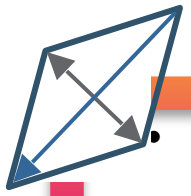


CAPACIDADES

- MalSpam a diferentes víctimas con link
- Template Covid-19
- Template Factura
- Template Falsa actualización

VÍCTIMA

Distribución



- MalSpam a diferentes víctimas con link
- Template Covid-19
- Template Factura
- Template Falsa actualización
- facturaoficial08@theprojectsecurity.onmicrosoft.com
- Asunto: Factura - VU17R

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command y Control
- Actions on objective

Explotación (Exploitation)

Esta fase toma lugar cuando el actor consigue realizar una intrusión sobre la víctima a través de alguna capacidad. En la mayoría de los casos, requiere interacción del usuario.

El usuario que recibe el correo electrónico hace click en el link que viene. Al ser redirigido a la web controlada por el adversario, en algunos casos requiere otra interacción para bajar el malware y en otros la descarga es automática simplemente con entrar.

Tras la descarga, el usuario hace click en el fichero (msi, vbs, zip con malware en su interior, etc...)
El malware ejecutado es de primera etapa, por lo general un loader, que tiene dos únicas funcionalidades:

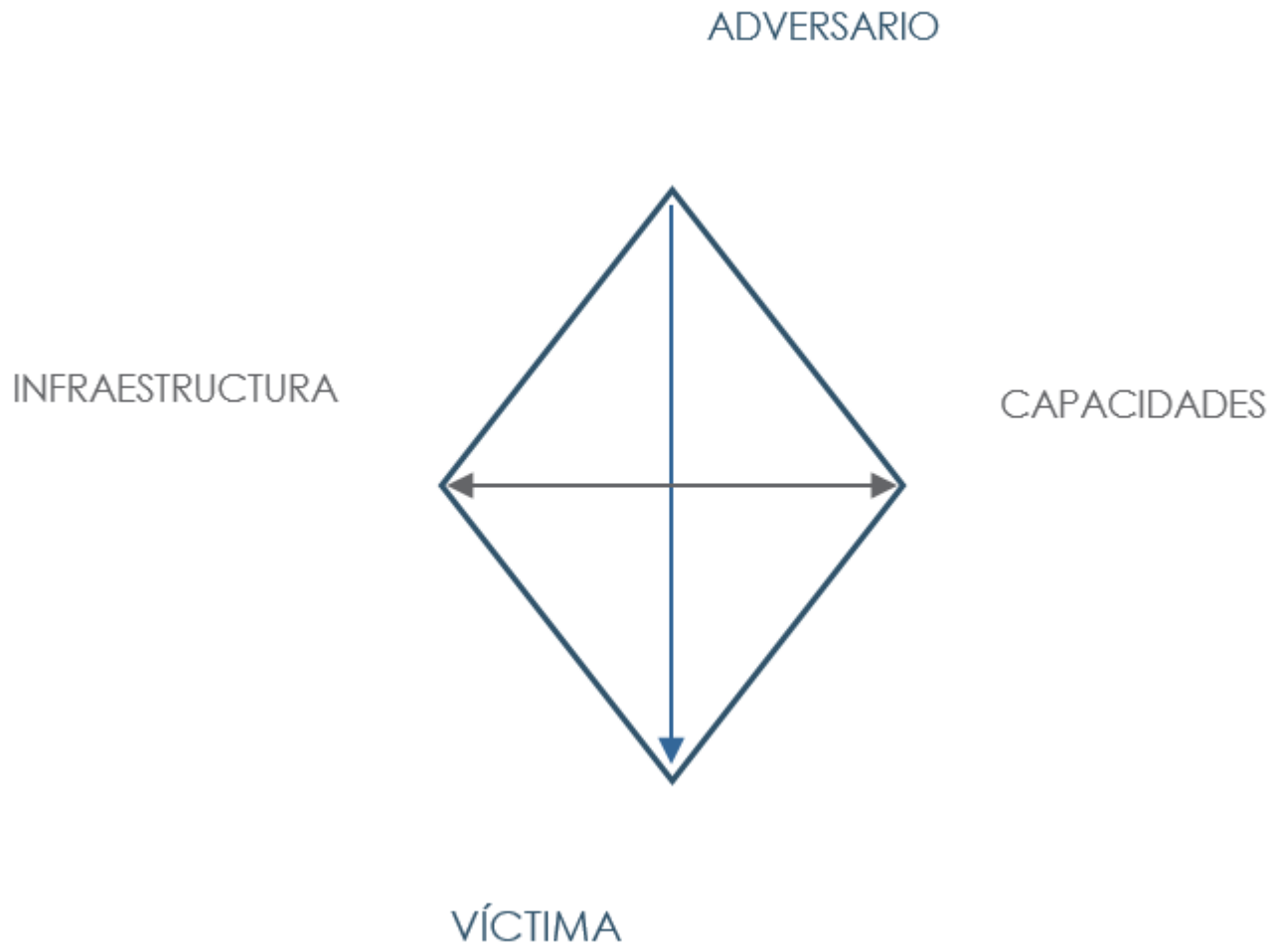
- Brinda acceso remoto al cibercriminal
- Descarga el payload de Grandoreiro

Explotación

EXPLOITATION

- Ejecución del malware descargado

- Ejecución de fichero ZIP, VBS o MSI
- Web maliciosa



Explotación

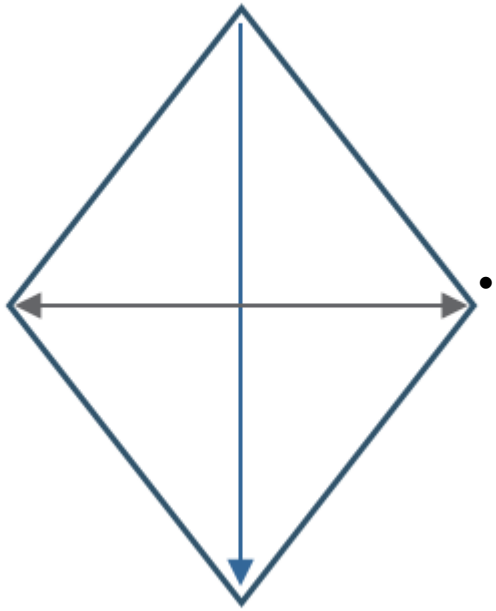
EXPLOITATION

- Ejecución del malware descargado

ADVERSARIO

INFRAESTRUCTURA

- Web maliciosa



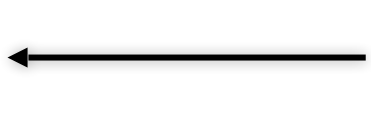
CAPACIDADES

- Ejecución de fichero ZIP, VBS o MSI

VÍCTIMA

Explotación

- Fichero ZIP, VBS o MSI
- Web maliciosa



Reconnaissance

Weaponization

Delivery

Exploitation

Installation

Command y Control

Actions on objective

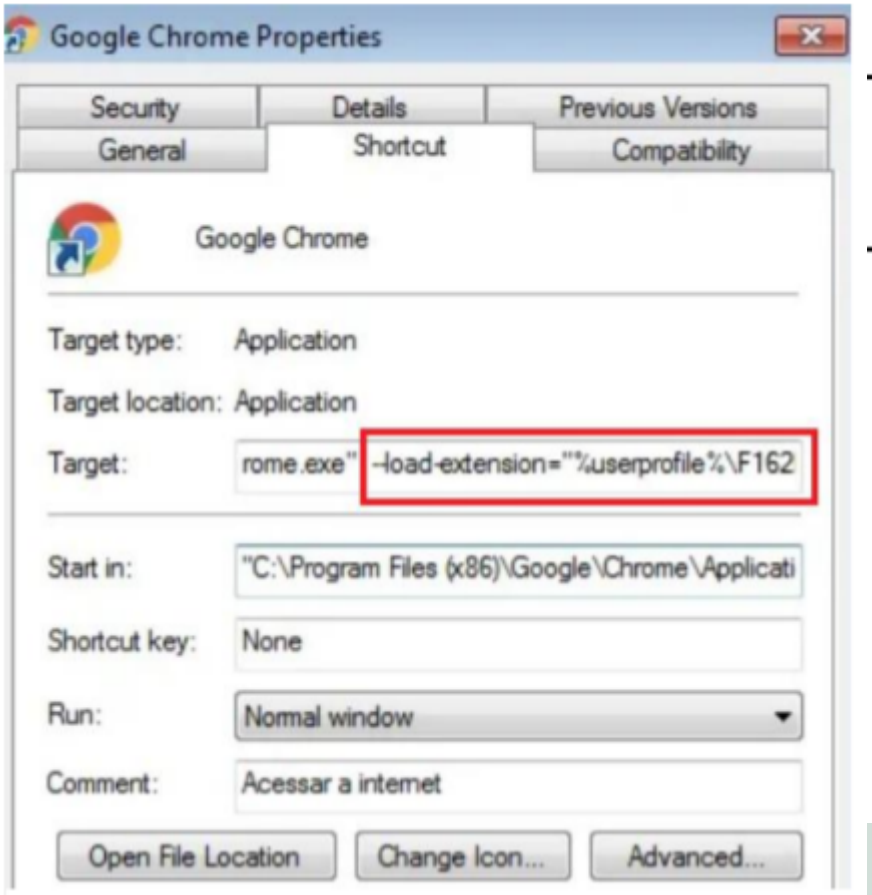
Instalación (Installation)

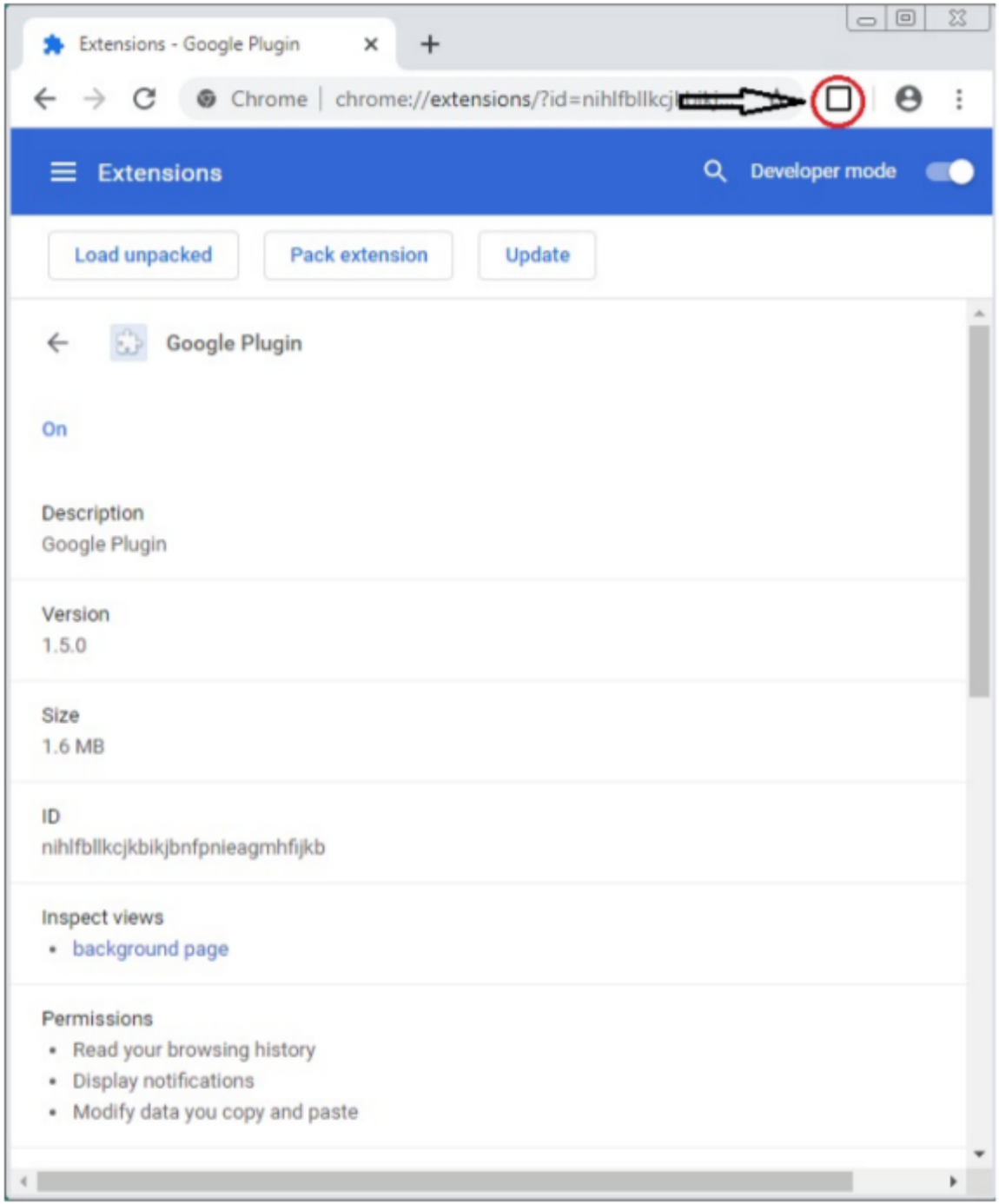
Durante la fase de instalación, la persistencia en el sistema empieza a realizarse en el sistema de la victima. Esto puede conseguir a través del malware de primera etapa o descargas posteriores.

El loader de la anterior fase realiza la descarga del payload de Grandoreiro y lo ejecuta (sin interacción del usuario). Este hace las siguientes acciones:

- Establece claves de registro para ganar persistencia y establece las comunicaciones con el C2
- Reinicia el sistema
- Al encenderse el sistema, genera un fichero llamado ext.zip en C:\%user%\<extension de la carpeta>* y se extrae sólo
- Los ficheros extraídos son extensiones modificadas de Google Chrome
- Genera un fichero .lnk de Chrome para que cada vez que se abra, cargue las cookies extraídas anteriormente.

Instalación



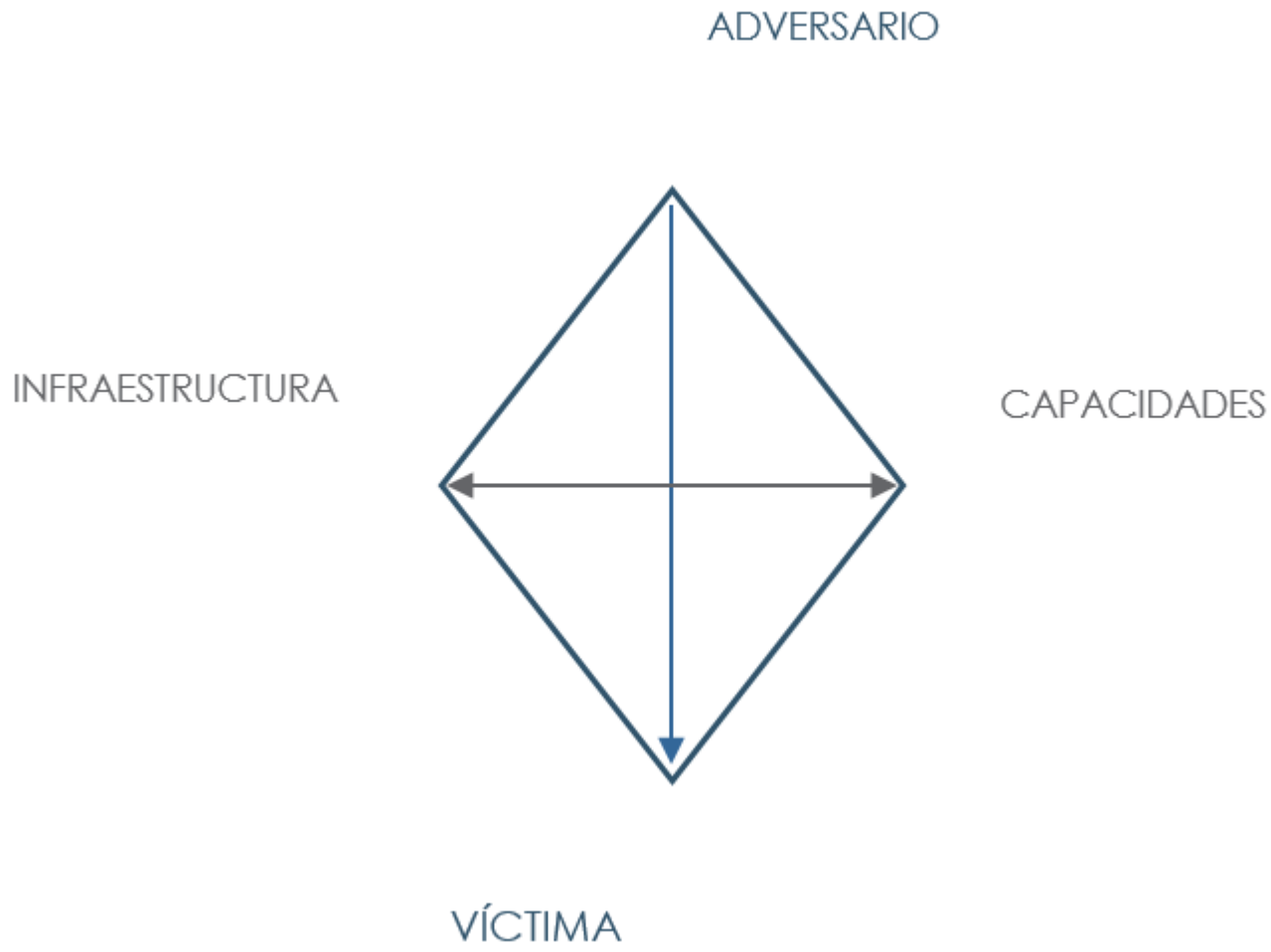


Instalación

INSTALLATION

- Persistencia en el sistema
- Descarga de complementos adicionales
- Primeras comunicaciones con el C2

- Claves de registro
- Comunicaciones C2 con Google Sites
- Extensiones modificadas de Chrome
- Generación de ficheros .lnk



Instalación

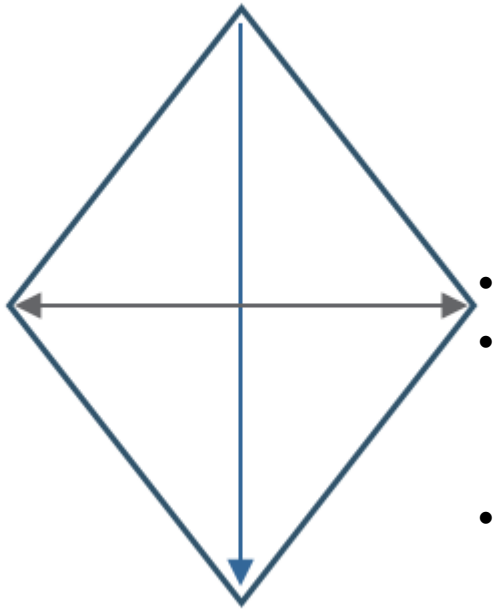
INSTALLATION

- Persistencia en el sistema
- Descarga de complementos adicionales
- Primeras comunicaciones con el C2

ADVERSARIO

INFRAESTRUCTURA

- Comunicaciones C2 con Google Sites

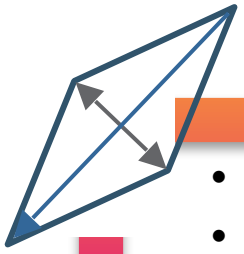


CAPACIDADES

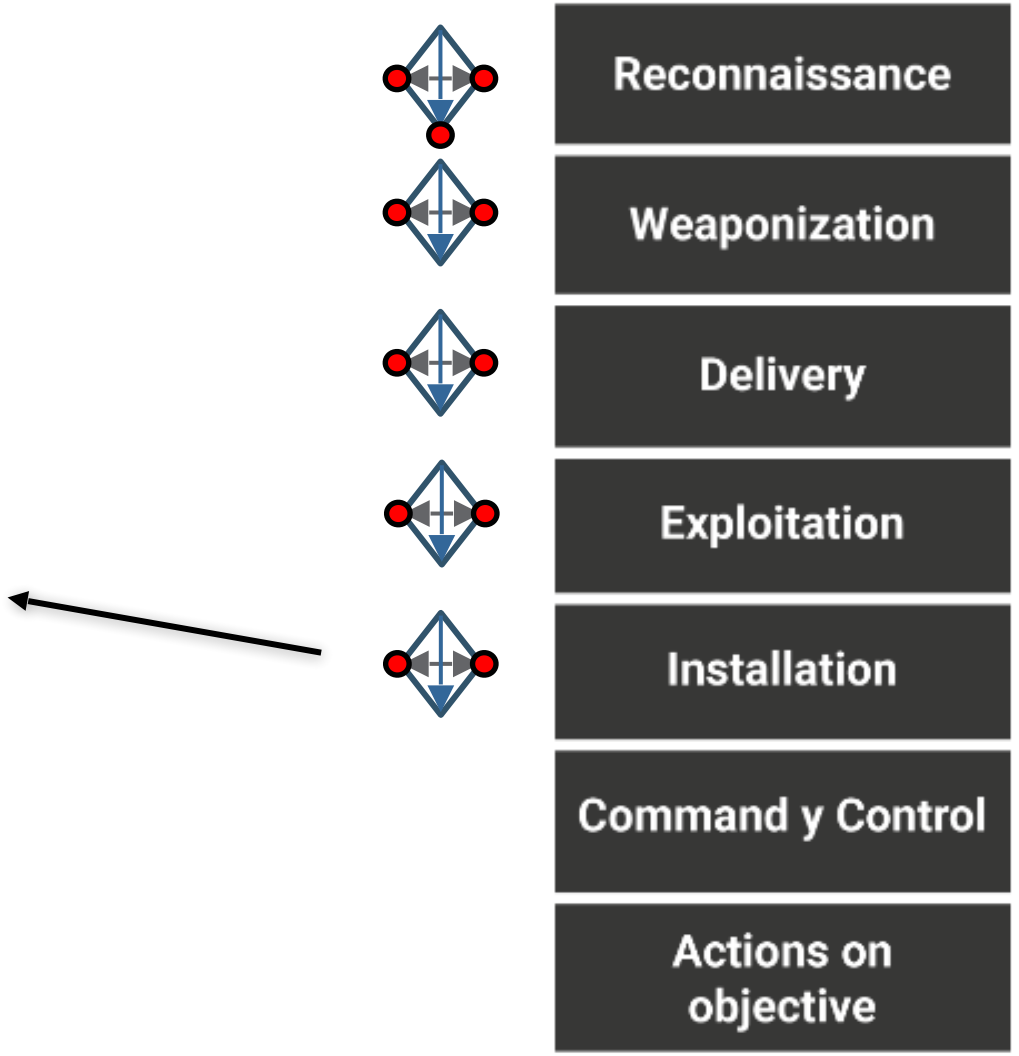
- Claves de registro
- Extensiones modificadas de Chrome
- Generación de ficheros .lnk

VÍCTIMA

Instalación



- Claves de registro
- Comunicaciones C2 con Google Sites
- Extensiones modificadas de Chrome
- Generación de ficheros .lnk
- Monitorización del browser para acceso a la banca



C2 y Acciones sobre los objetivos (Actions on Objective)

En la fase de C2 se establecen comunicaciones entre el adversario y el sistema de la víctima a través de las infraestructuras disponibles. Mientras que en AoO se describen todas las acciones que ha llevado a cabo un adversario tras conseguir el control del sistema.

C2

- Establece comunicaciones para controlar el sistema de la víctima

Actions on Objective

- Monitoriza el navegador para cuando el usuario acceda a la banca, tomar el control del sistema a través del C2
- Superpone contenido para mantener a la victima distraída mientras realiza acciones en la cuenta bancaria tras hacer login

C2 y Acciones sobre los objetivos

Web legítima de la entidad bancaria después de hacer login y controlada por el cibercriminal

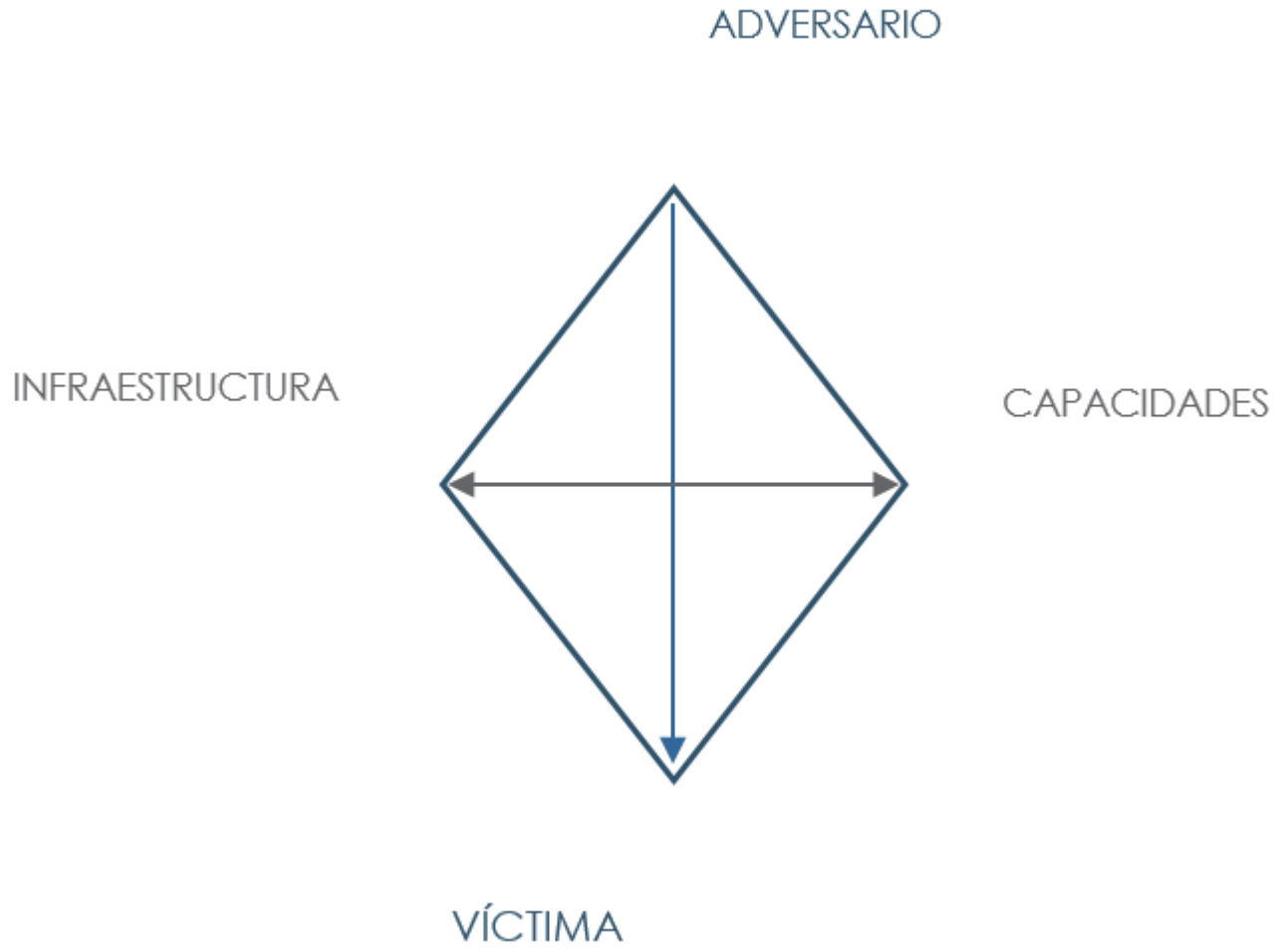
"Overlay" que superpone el cibercriminal para mantener a la víctima entretenida introduciendo información

C2 y Acciones sobre los objetivos

C2 & AoO

- Monitorización del navegador
- Comunicaciones C2
- Robo de información bancaria

- Monitorización del browser para cuando acceda a la banca
- Superposición de pantalla en la banca
- Comunicaciones C2 con Google Sites



C2 y Acciones sobre los objetivos

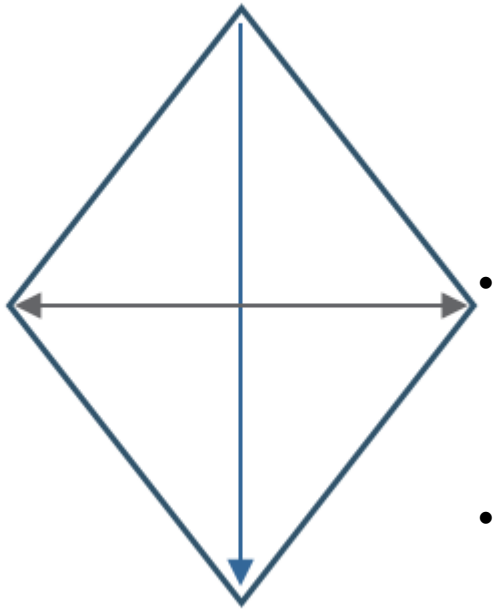
C2 & AoO

- Monitorización del navegador
- Comunicaciones C2
- Robo de información bancaria

ADVERSARIO

INFRAESTRUCTURA

- Comunicaciones C2 con Google Sites

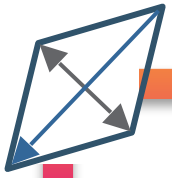


CAPACIDADES

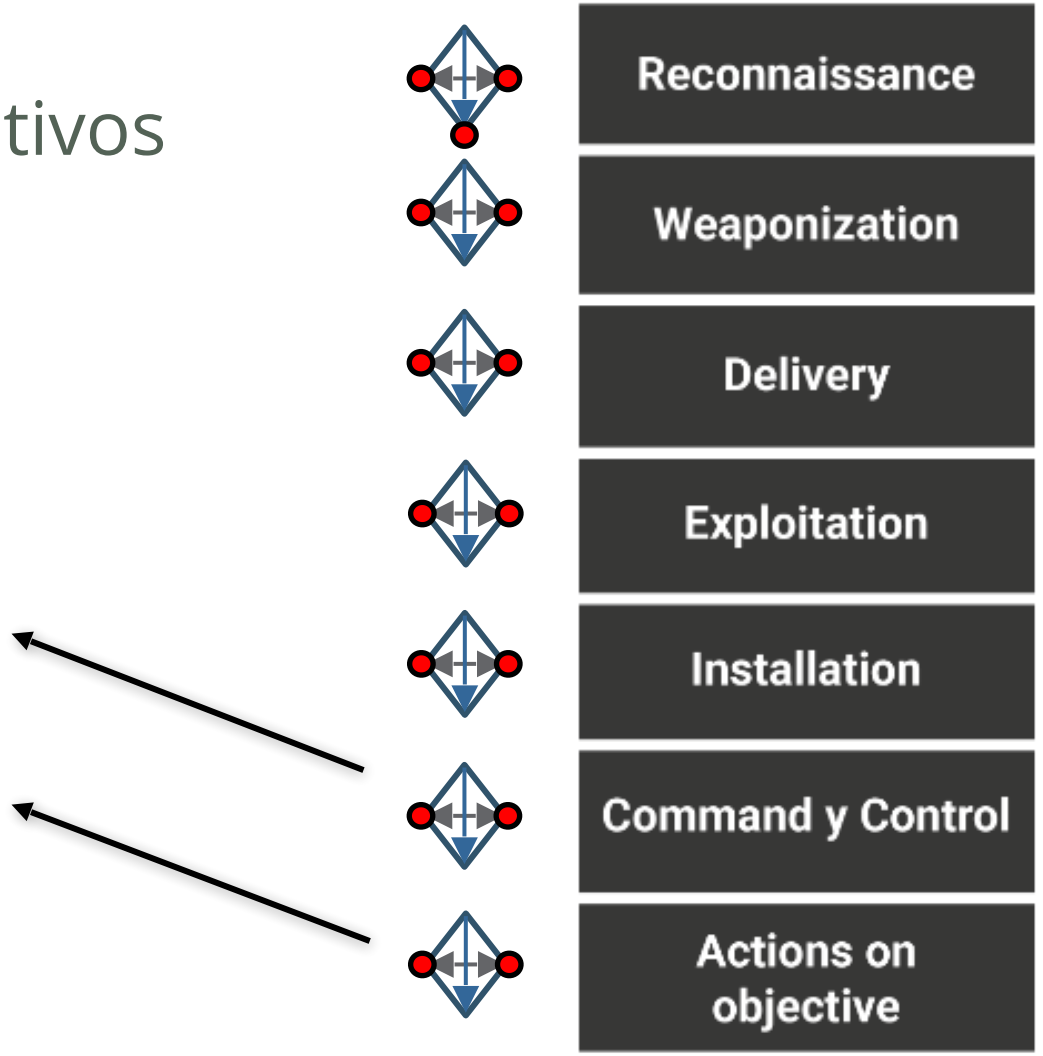
- Monitorización del browser para cuando acceda a la banca
- Superposición de pantalla en la banca

VÍCTIMA

C2 y Acciones sobre los objetivos



- Monitorización del browser para cuando acceda a la banca
- Superposición de pantalla en la banca
- Comunicaciones C2 con Google Sites



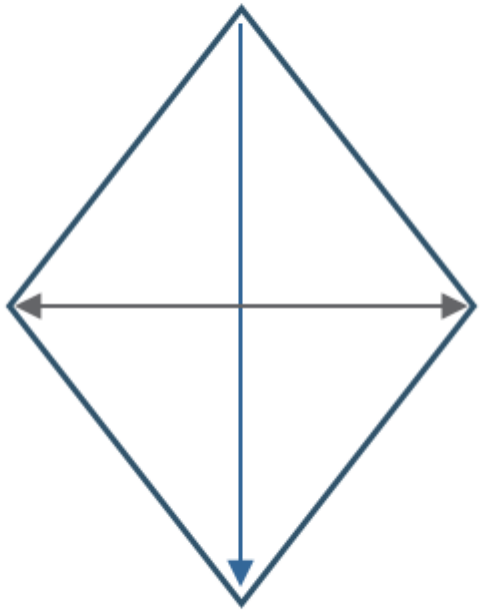
Modelo diamante

ADVERSARIO

- 213.24.134.32
- 178.44.144.231
- Adquisición de dominios
- Configuración de Google Sites

INFRAESTRUCTURA

- facturaoficial08@theprojectsecurity.onmicrosoft.com
- Web maliciosa
- Comunicaciones C2 con Google Sites



- Alberto Serrano Caballero
- SRVLDPHA10

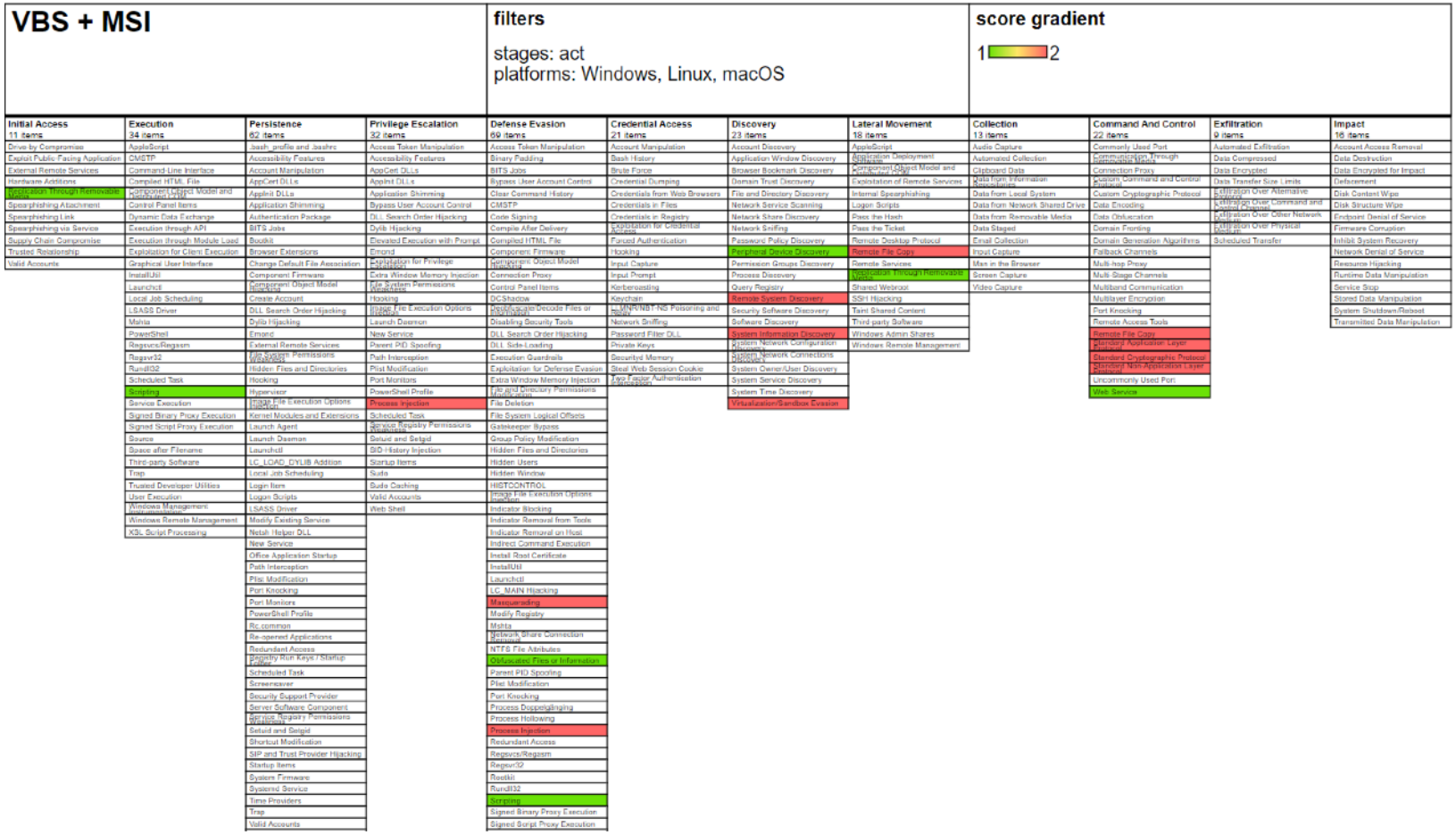
VÍCTIMA

- Claves de registro
- Extensiones modificadas de Chrome
- Generación de ficheros .lnk
- Monitorización del browser para cuando acceda a la banca
- Superposición de pantalla en la banca

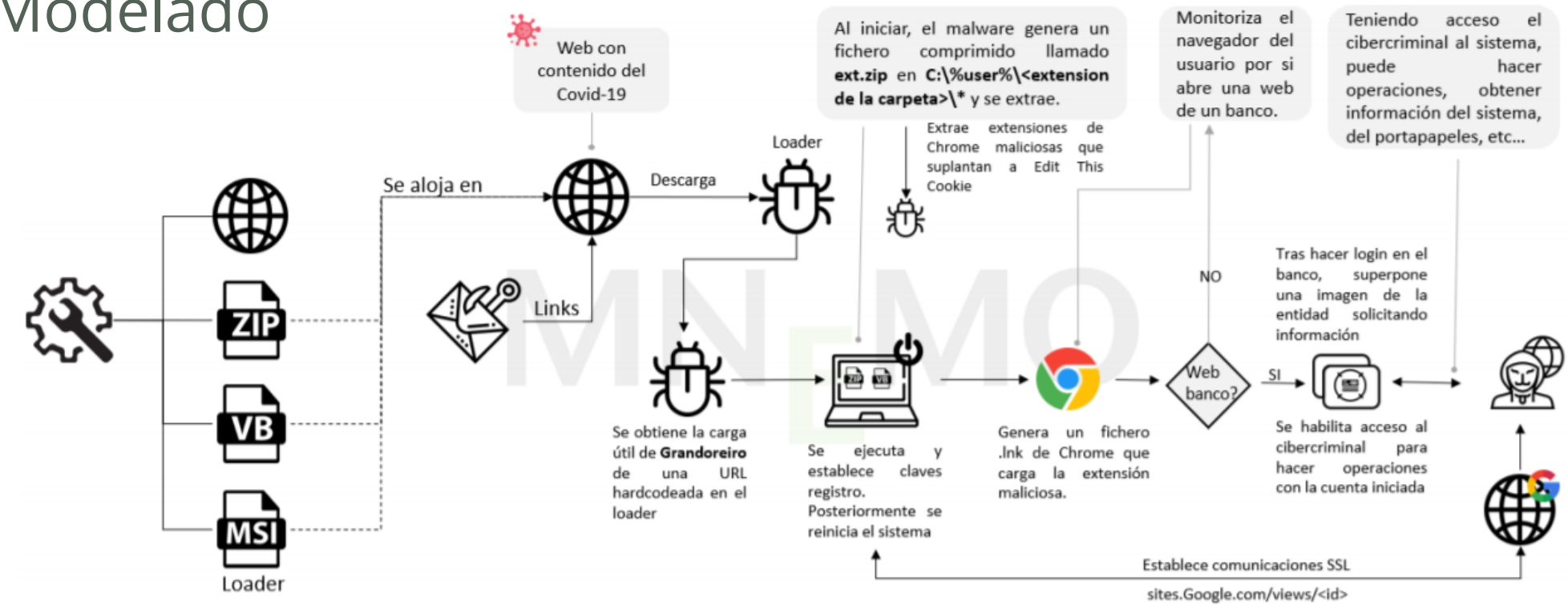
CAPACIDADES

- Google Hacking
- Malware en ficheros MSI
- Malware en ficheros VBS
- Malware comprimido en ZIP
- MalSpam a diferentes víctimas con link
- Template Covid-19
- Template Factura
- Template Falsa actualización

ATT&CK


VBS + MSI
filters
stages: act
platforms: Windows, Linux, macOS
score gradient
1
2
Initial Access
11 items
Drive by Compromise
Exploit Public Facing Application
External Remote Services
Hardware Additions
Replication Through Removable Media
Spearphishing Attachment
Spearphishing Link
Spearphishing via Service
Supply Chain Compromise
Trusted Relationship
Valid Accounts
Execution
34 items
AppleScript
CMSTP
Command-Line Interface
Compiled HTML File
Component Object Model and Distributed COM
Control Panel Items
Dynamic Data Exchange
Execution through API
Execution through Module Load
Exploitation for Client Execution
Graphical User Interface
InstallUtil
Launchctl
Local Job Scheduling
LSASS Driver
Mshta
PowerShell
Regsvcs/Regasm
Regsvr32
Rundll32
Scheduled Task
Scripting
Service Execution
Signed Binary Proxy Execution
Signed Script Proxy Execution
Source
Space after Filename
Third-party Software
Trap
Trusted Developer Utilities
User Execution
Windows Management Instrumentation
Windows Remote Management
XSL Script Processing
Persistence
62 items
.bash_profile and .bashrc
Accessibility Features
Account Manipulation
AppCert DLLs
AppInit DLLs
Application Shimming
Authentication Package
BITS Jobs
Bootkit
Browser Extensions
Change Default File Association
Component Firmware
Component Object Model Hijacking
Create Account
DLL Search Order Hijacking
Dylib Hijacking
Emond
External Remote Services
File System Permissions Weakness
Hidden Files and Directories
Hooking
Hypervisor
Image File Execution Options Injection
Kernel Modules and Extensions
Launch Agent
Launch Daemon
Launchctl
LC_LOAD_DYLIB Addition
Local Job Scheduling
Login Item
Login Scripts
LSASS Driver
Modify Existing Service
Netsh Helper DLL
New Service
Office Application Startup
Path Interception
Plist Modification
Port Knocking
Port Monitors
PowerShell Profile
Rc.common
Re-opened Applications
Redundant Access
Registry Run Keys / Startup Folder
Scheduled Task
Screensaver
Security Support Provider
Server Software Component
Service Registry Permissions Weakness
Setuid and Setgid
Shortcut Modification
SIP and Trust Provider Hijacking
Startup Items
System Firmware
Systemd Service
Time Providers
Trap
Valid Accounts
Privilege Escalation
32 items
Access Token Manipulation
Accessibility Features
AppCert DLLs
AppInit DLLs
Application Shimming
Bypass User Account Control
DLL Search Order Hijacking
Dylib Hijacking
Elevated Execution with Prompt
Emond
Exploitation for Privilege Escalation
Extra Window Memory Injection
File System Permissions Weakness
Hooking
Image File Execution Options Injection
Launch Daemon
New Service
Parent PID Spoofing
Path Interception
Plist Modification
Port Monitors
PowerShell Profile
Process Injection
Scheduled Task
Service Registry Permissions Weakness
Setuid and Setgid
SID-History Injection
Startup Items
Sudo
Sudo Caching
Valid Accounts
Web Shell
Defense Evasion
69 items
Access Token Manipulation
Binary Padding
BITS Jobs
Bypass User Account Control
Clear Command History
CMSTP
Code Signing
Compile After Delivery
Compiled HTML File
Component Firmware
Component Object Model Hijacking
Connection Proxy
Control Panel Items
DCShadow
Deobfuscate/Decode Files or Information
Disabling Security Tools
DLL Search Order Hijacking
DLL Side-Loading
Execution Guardrails
Exploitation for Defense Evasion
Extra Window Memory Injection
File and Directory Permissions Modification
File Deletion
File System Logical Offsets
Gatekeeper Bypass
Group Policy Modification
Hidden Files and Directories
Hidden Users
Hidden Window
HISTCONTROL
Image File Execution Options Injection
Indicator Blocking
Indicator Removal from Tools
Indicator Removal on Host
Indirect Command Execution
Install Root Certificate
InstallUtil
Launchctl
LC_MAIN Hijacking
Masquerading
Modify Registry
Mshta
Network Share Connection Removal
NTFS File Attributes
Obfuscated Files or Information
Parent PID Spoofing
Plist Modification
Port Knocking
Process Doppelgänging
Process Hollowing
Process Injection
Redundant Access
Regsvcs/Regasm
Regsvr32
Rootkit
Rundll32
Scripting
Signed Binary Proxy Execution
Signed Script Proxy Execution
Credential Access
21 items
Account Manipulation
Bash History
Brute Force
Credential Dumping
Credentials from Web Browsers
Credentials in Files
Credentials in Registry
Exploitation for Credential Access
Forced Authentication
Hooking
Input Capture
Input Prompt
Kerberoasting
Keychain
LLMNR/NBT-NS Poisoning and Relay
Network Sniffing
Password Filter DLL
Private Keys
Securityd Memory
Steal Web Session Cookie
Two Factor Authentication Interception
Discovery
23 items
Account Discovery
Application Window Discovery
Browser Bookmark Discovery
Domain Trust Discovery
File and Directory Discovery
Network Service Scanning
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery
Process Discovery
Query Registry
Remote System Discovery
Security Software Discovery
Software Discovery
System Information Discovery
System Network Configuration Discovery
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery
System Time Discovery
Virtualization/Sandbox Evasion
Lateral Movement
18 items
AppleScript
Application Deployment Software
Component Object Model and Distributed COM
Exploitation of Remote Services
Internal Spearphishing
Logon Scripts
Pass the Hash
Pass the Ticket
Remote Desktop Protocol
Remote File Copy
Remote Services
Replication Through Removable Media
Shared Webroot
SSH Hijacking
Taint Shared Content
Third-party Software
Windows Admin Shares
Windows Remote Management
Collection
13 items
Audio Capture
Automated Collection
Clipboard Data
Data from Information Repositories
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged
Email Collection
Input Capture
Man in the Browser
Screen Capture
Video Capture
Command And Control
22 items
Commonly Used Port
Communication Through Removable Media
Connection Proxy
Custom Command and Control Protocol
Custom Cryptographic Protocol
Data Encoding
Data Obfuscation
Domain Fronting
Domain Generation Algorithms
Fallback Channels
Multi-hop Proxy
Multi-Stage Channels
Multiband Communication
Multilayer Encryption
Port Knocking
Remote Access Tools
Remote File Copy
Standard Application Layer Protocol
Standard Cryptographic Protocol
Standard Non-Application Layer Protocol
Uncommonly Used Port
Web Service
Exfiltration
9 items
Automated Exfiltration
Data Compressed
Data Encrypted
Data Transfer Size Limits
Exfiltration Over Alternative Protocol
Exfiltration Over Command and Control Channel
Exfiltration Over Other Network Medium
Exfiltration Over Physical Medium
Scheduled Transfer
Impact
16 items
Account Access Removal
Data Destruction
Data Encrypted for Impact
Defacement
Disk Content Wipe
Disk Structure Wipe
Endpoint Denial of Service
Firmware Corruption
Inhibit System Recovery
Network Denial of Service
Resource Hijacking
Runtime Data Manipulation
Service Stop
Stored Data Manipulation
System Shutdown/Reboot
Transmitted Data Manipulation

Modelado



Generación de los ficheros maliciosos y contenido web. Reutilización de malware basado en screen overlay.

Envío de correos con links a una web con contenido del Covid-19 que aloja el malware.

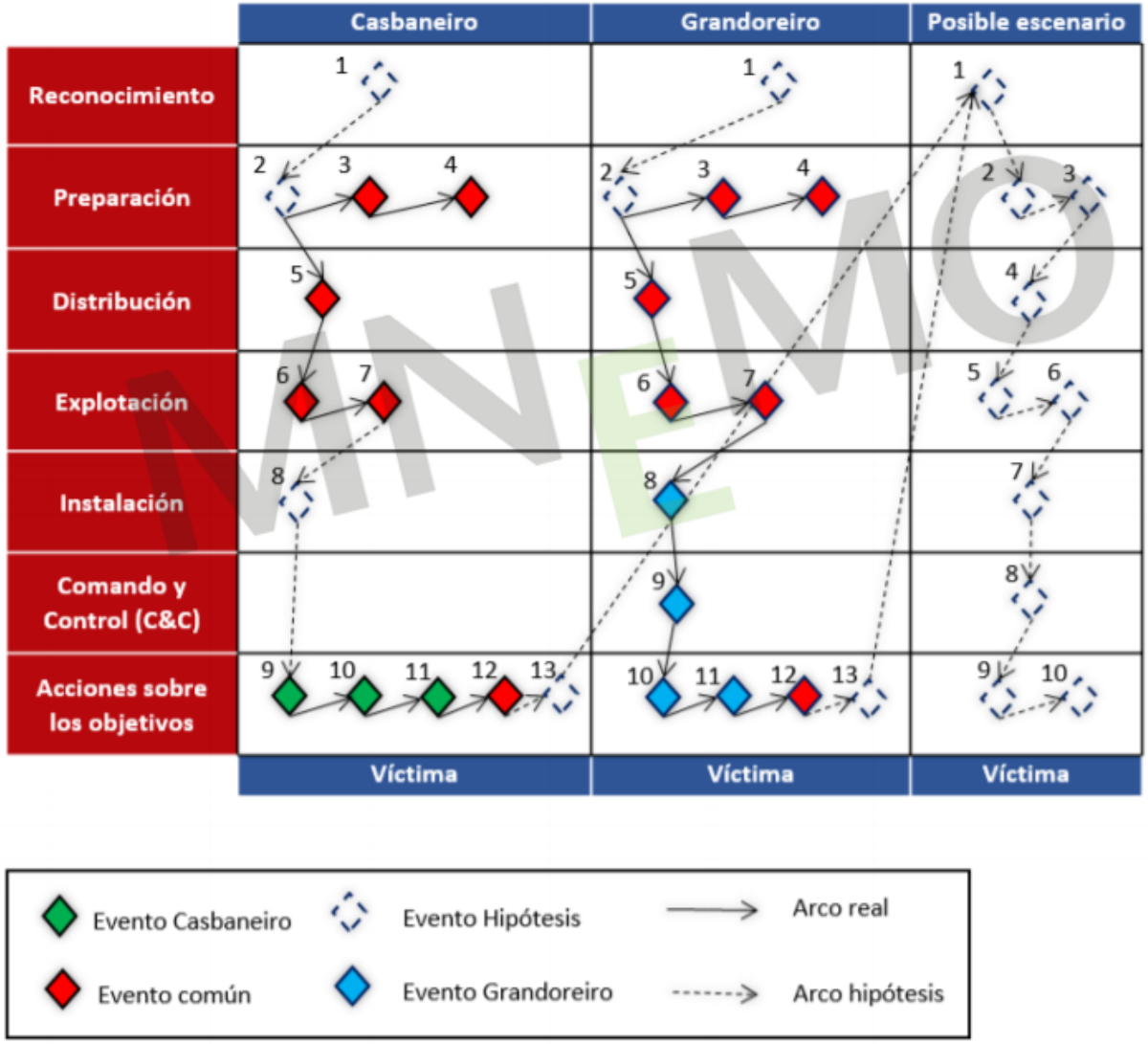
Un Loader es descargado desde la web maliciosa y obtiene la carga útil de Grandoreiro de una URL que tiene en su código.

Se descarga una extensión de Chrome maliciosa y se genera un fichero .lnk para que cuando abra el navegador se cargue la ext.

Cuando la víctima inicia sesión en su entidad bancaria, se superpone una imagen solicitando información y se establece una comunicación con el cibercriminal.

Weapon	Deliver	Exploit	Install & C2	Actions on Objectives

Correlación



Casbaneiro

Evento	Hipótesis/Real	Descripción
1	Hipótesis	El adversario no realiza un reconocimiento previo de sus objetivos, ya que se tratan de víctimas de oportunidad, es decir, víctimas reemplazables.
2	Hipótesis	El adversario, en base a una lista de correos electrónicos que dispone, probablemente de algún leak de información de cualquier organización, prepara sus víctimas para el envío masivo.
3	Real	Reutiliz… en esta
4	Real	Prepara… 1. Al… 2. Te… C2

Grandoreiro

Evento	Hipótesis/Real	Descripción
1	Hipótesis	El adversario no realiza un reconocimiento previo de sus objetivos, ya que se tratan de víctimas de oportunidad, es decir, víctimas reemplazables.
2	Hipótesis	El adversario, en base a una lista de correos electrónicos que dispone, probablemente de algún leak de información de cualquier organización, prepara sus víctimas para el envío masivo.
3	Real	Reutilización de malware y código ya existente para utilizarlo en esta campaña.
4	Real	Preparación y adquisición de infraestructura en dos vías: 1. Alojar el malware que se va distribuye 2. Tener un servidor con el que establecer comunicaciones C2

Grandoreiro & Casbaneiro

Initial Access	Execution	Persistence	Privilege Escalation
Replication Through Removable Media	Scripting	Registry Run Keys / Startup Folde	Process Injection
		Startup Items	Startup Items

Defense Evasion	Discovery	Lateral Movement	Command And Control
Masquerading	File and Directory Discovery	Remote File Copy	Remote File Copy
Obfuscated Files or Information	Peripheral Device Discovery	Replication Through Removable Media	Standard Application Layer Protocol
Process Injection	Remote System Discovery		Standard Cryptographic Protocol
Scripting	System Information Discovery		Standard Non-Application Layer Protocol
Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion		Web Service
Web Service			

Leyenda
Similitud en **1 muestra**
Similitud en **2 muestras**
Similitud en **3 muestras**

sedian Seguridad Digital de Andalucía