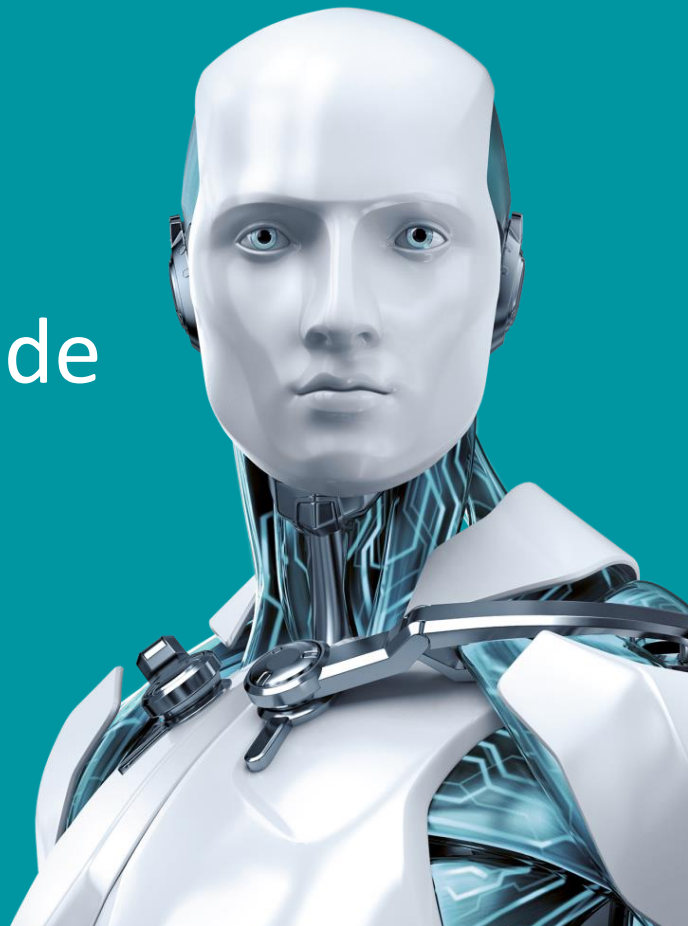
Mosquitos, serpientes, osos y otras herramientas avanzadas de espionaje



ENJOY SAFER TECHNOLOGY™

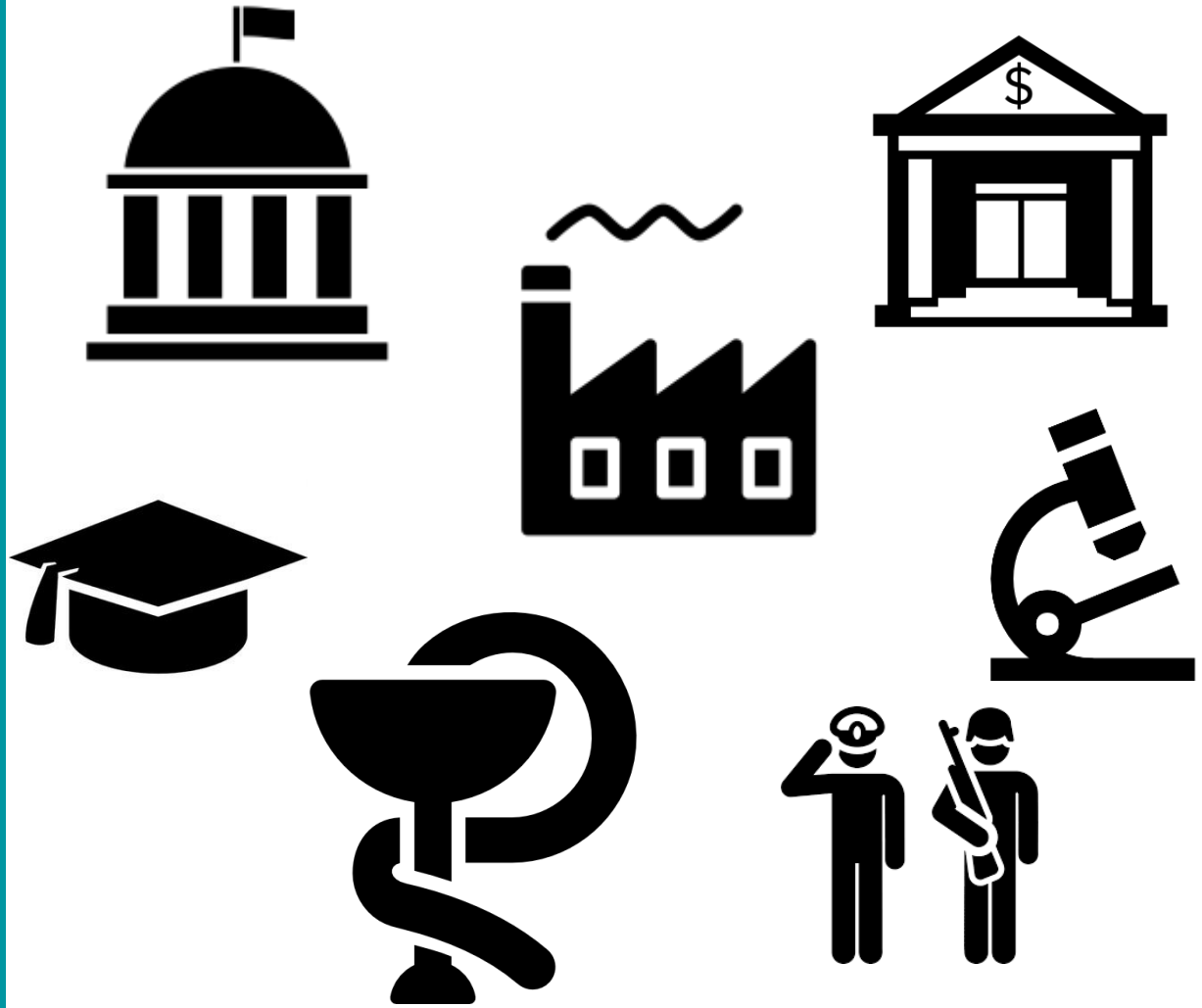
Situación Actual

Ataques dirigidos

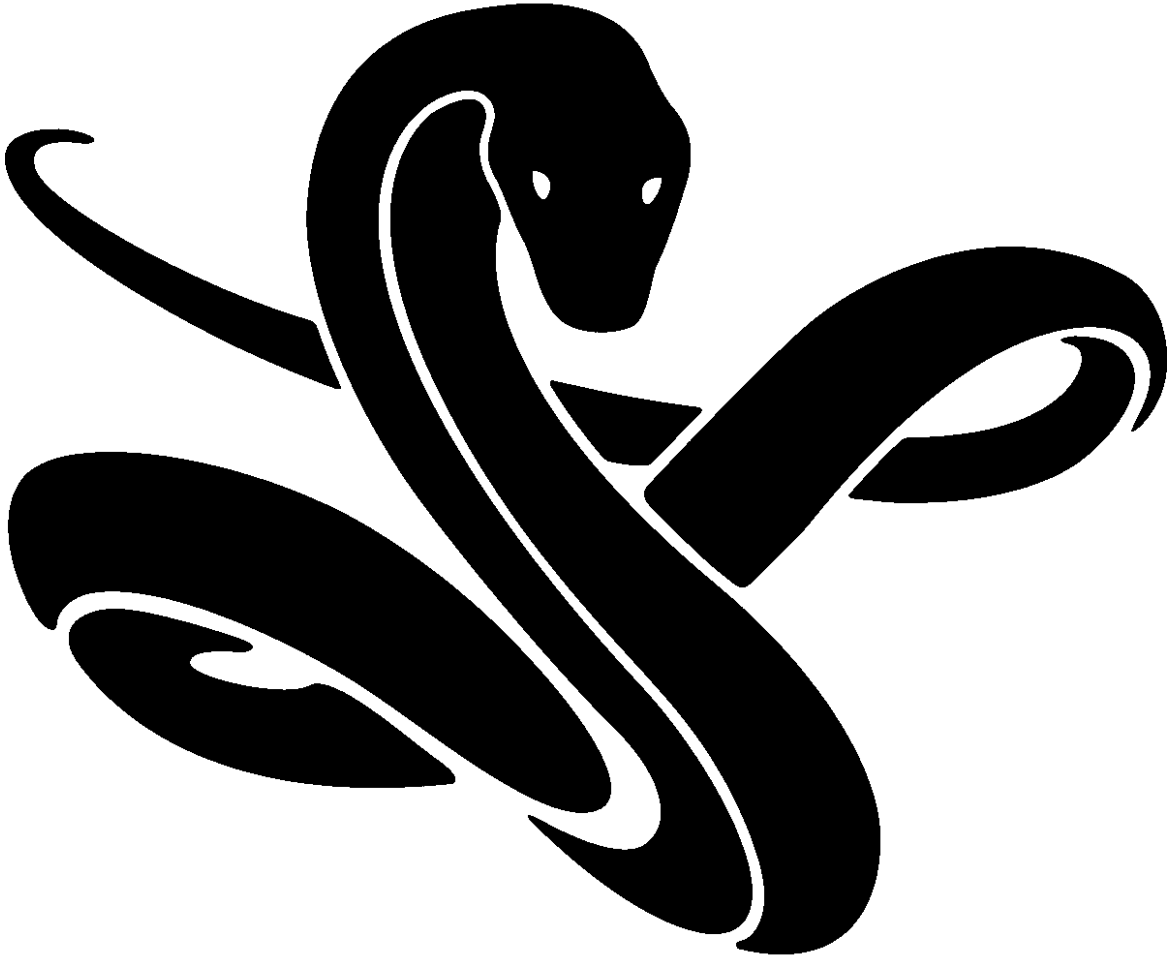
Grupos especializados

Fuente: FireEye

Objetivos



Grupo Turla
(Snake, Uroburos)



Víctimas

Federal Foreign Office

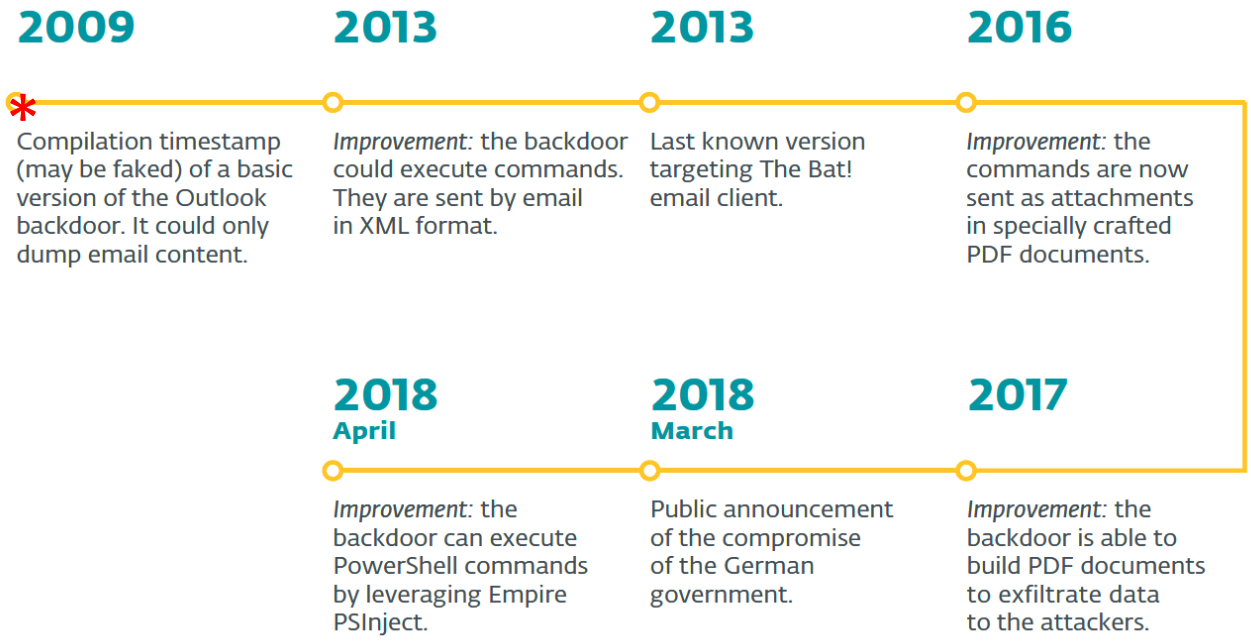
Cronología Turla

1996 Moonlight Maze (LOKI2 backdoor)

.

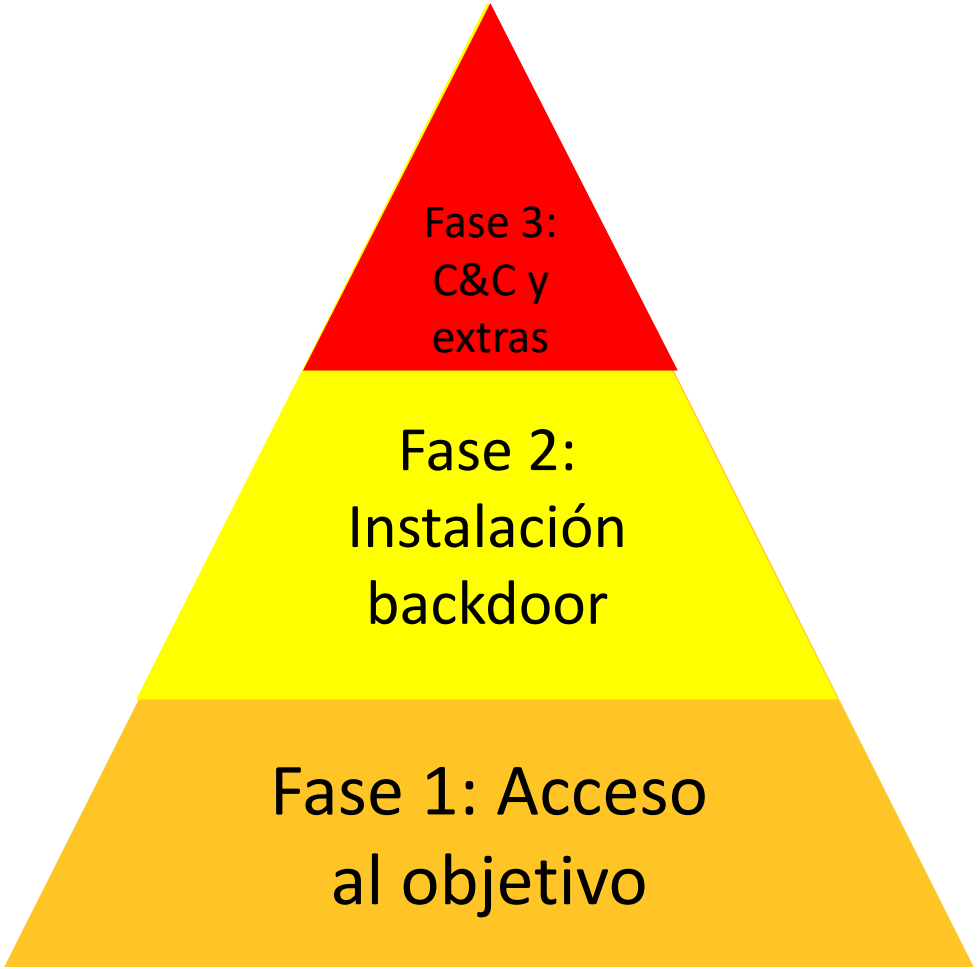
..

...



Fuente: WeLiveSecurity

Ataques Multifase



Vector de ataque: email

•.ؤتمر جنيفrar
NATO position on Syria.scr
Note_№107-41D.pdf
Talking Points.scr
border_security_protocol.rar
Security protocol.scr
Program.scr

Fuente: Securelist

ДЕВЯТЫЙ АРБИТРАЖНЫЙ АПЕЛЛЯЦИОННЫЙ СУД
127994, Москва, ГСП-4, проезд Соломенной сторожки, 12
адрес электронной почты: info@mail.9aac.ru
адрес веб-сайта: http://www.9aac.arbitr.ru

ОПРЕДЕЛЕНИЕ
о принятии апелляционной жалобы к производству
№ 09АП-37753/2013

г. Москва Дело № А40-37262/13
24 октября 2013 года
Судья Б.С. Веклич рассмотрев вопрос о принятии к производству апелляционной жалобы ООО "СТРОЙЭКСПОЛ" на решение Арбитражного суда г.Москвы от 20.09.2013 по делу №А40-37262/13, принятое судьей Ларионой Г.М. (30-321)
по иску ООО «Диамант» (ОГРН 1083123021057, 308007, г.Белгород, ул.Мичурина, д.56)
к ООО «СТРОЙЭКСПОЛ» (ОГРН 1027743009436, 125599, Москва, ул.Бусиновская Горка, 1Б, стр.1)
о взыскании 526 206,88 руб.

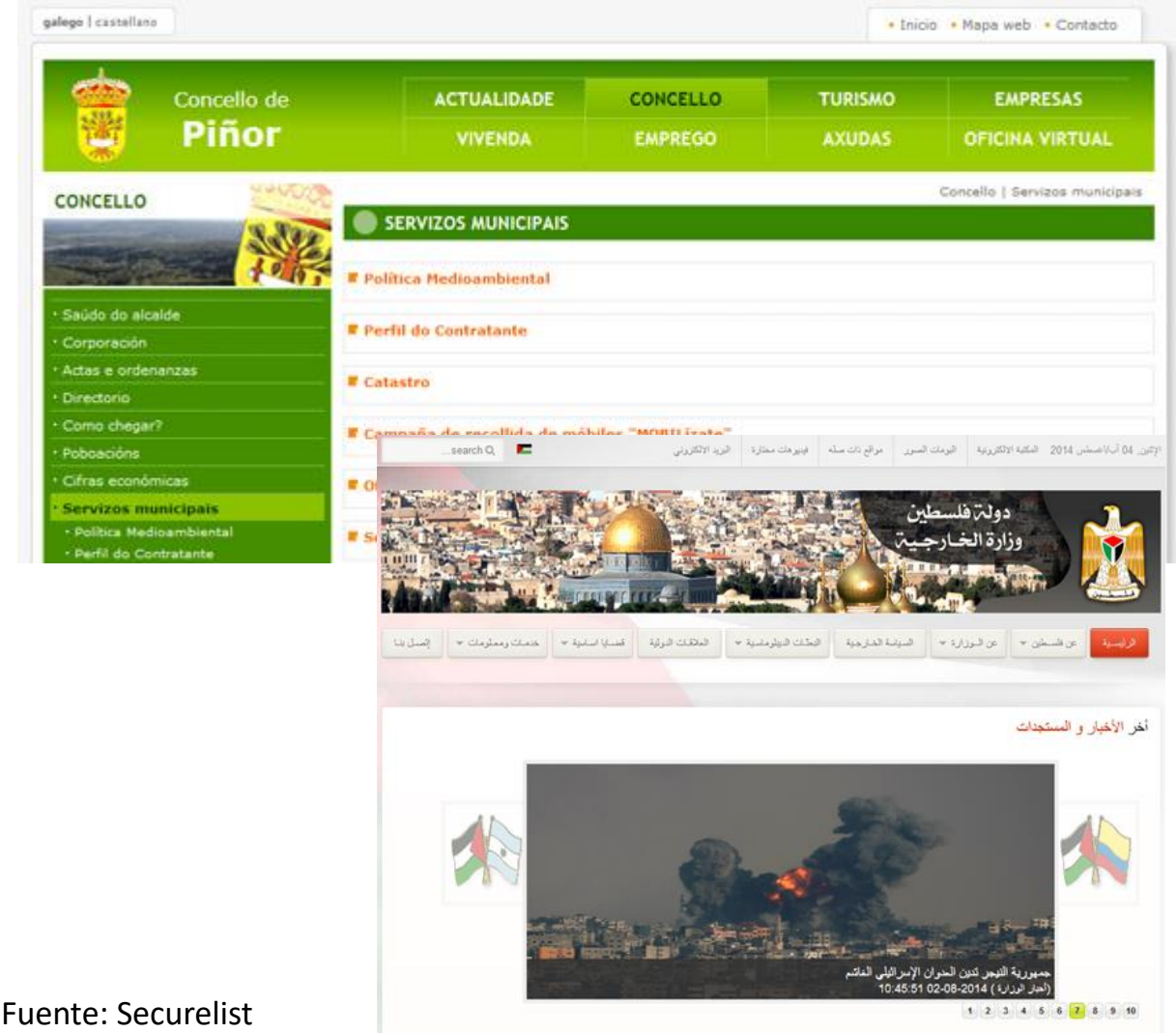
УСТАНОВИЛ:
Апелляционная жалоба подана с соблюдением требований, установленных ст. 260 Арбитражного процессуального кодекса Российской Федерации.
Руководствуясь ст.ст. 260, 261 Арбитражного процессуального кодекса Российской Федерации,

ОПРЕДЕЛИЛ:
1. Апелляционную жалобу ООО "СТРОЙЭКСПОЛ" принять к производству.
2. Назначить дело к судебному разбирательству **на 21 ноября 2013 года на 10 час. 45 мин.** в помещении суда по адресу: г. Москва, проезд Соломенной Сторожки, д.12, зал № 11 (кабинет 205) этаж 2.
3. В порядке подготовки к судебному разбирательству предлагается:
истцу - представить мотивированный и документально обоснованный отзыв на апелляционную жалобу в порядке статьи 262 Арбитражного процессуального кодекса Российской Федерации с доказательствами направления его другим лицам, участвующим в деле.
Лицам, участвующим в деле, обеспечить явку полномочных представителей или известить суд о возможности рассмотрения дела в их отсутствие.

Судья Б.С. Веклич

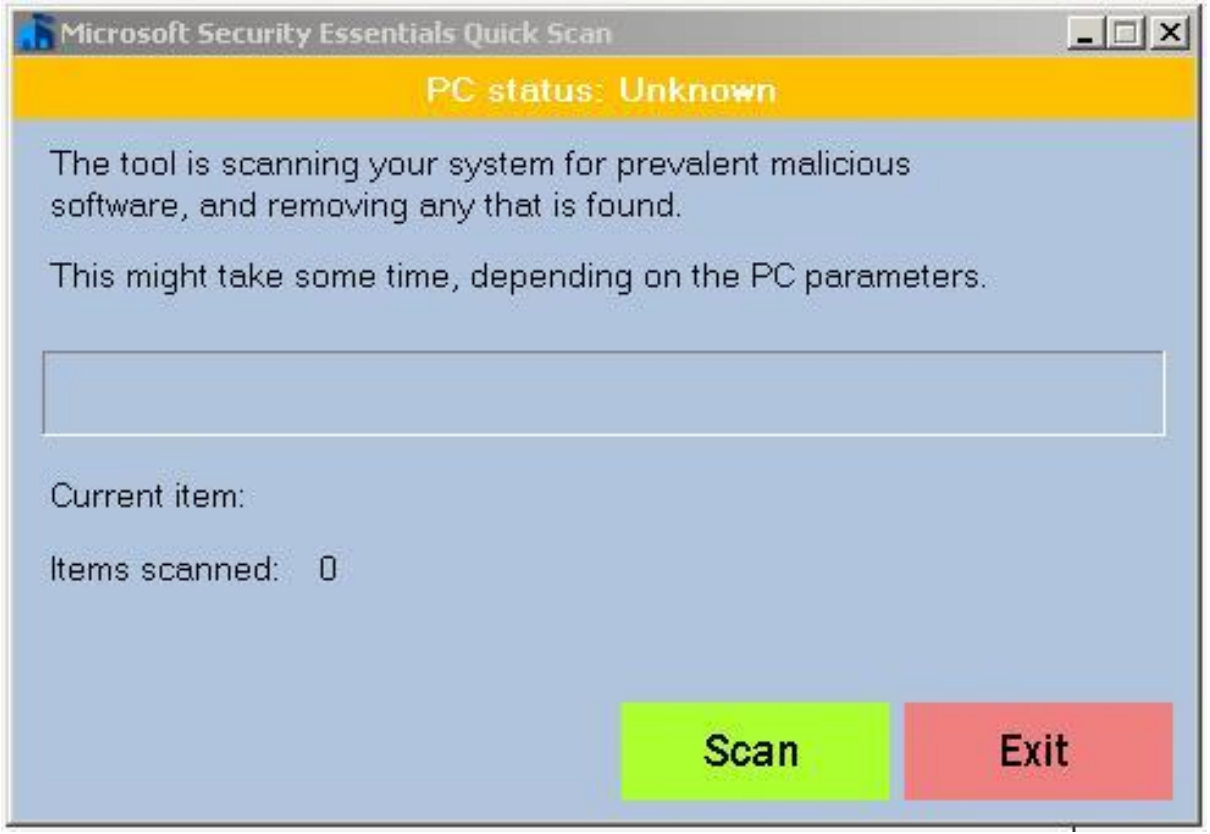
Телефон справочной службы суда – 8 (495) 987-26-00
Факс – 8 (495) 987-26-11
Информация о движении дела размещается на сайте суда в сети Интернет по веб-адресу: http://9aac.arbitr.ru/
в Картотеке арбитражных дел по веб-адресу: http://kad.arbitr.ru .

Vector de ataque:
watering hole



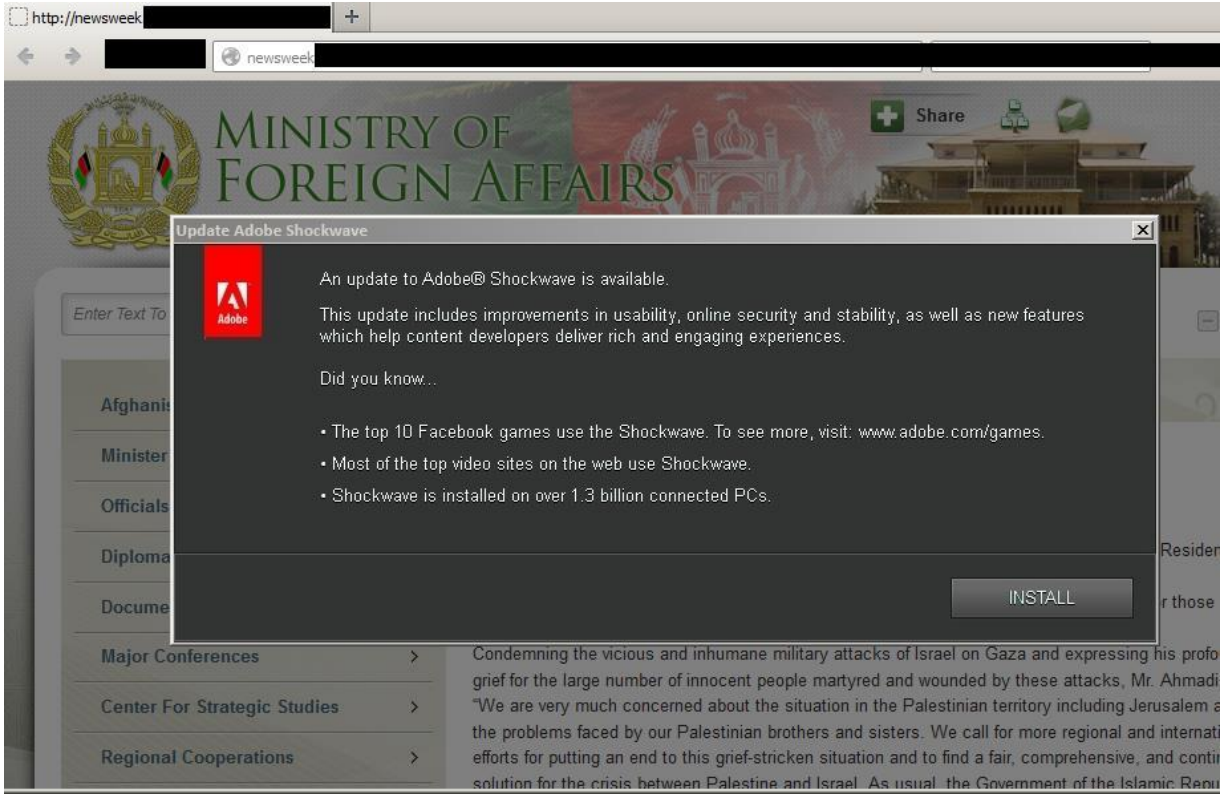
Fuente: Securelist

Vector de ataque:
falsas aplicaciones de seguridad



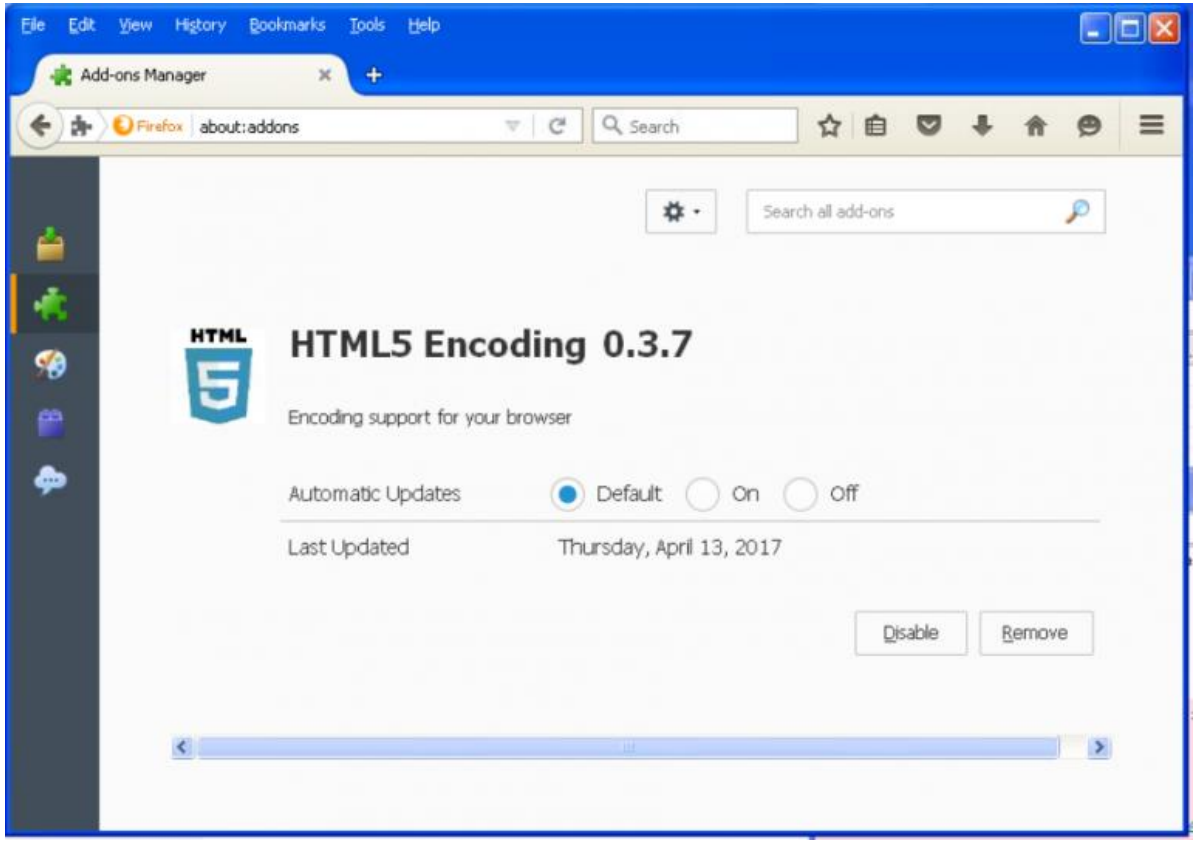
Fuente: Securelist

Vector de ataque:
falsos instaladores Flash Player



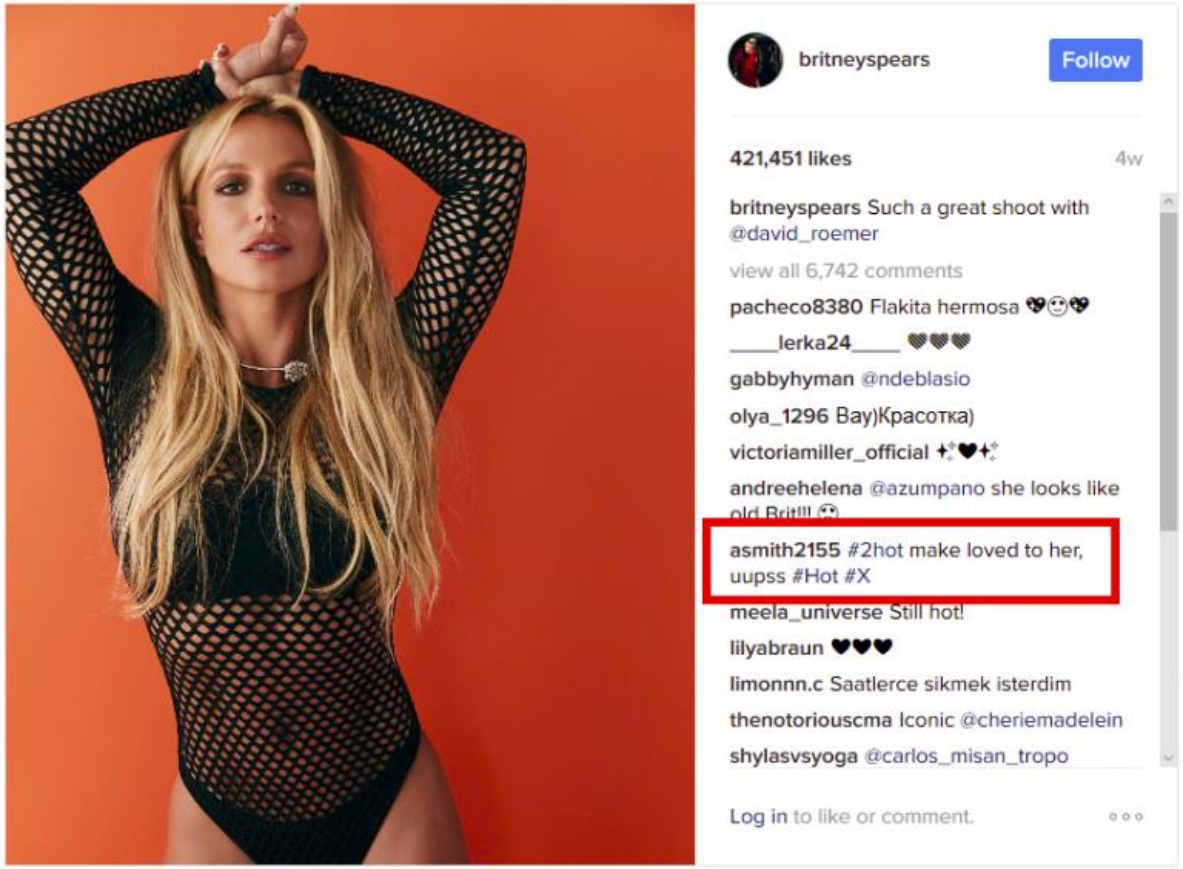
Fuente: Securelist

Vector de ataque: extensiones de Firefox



Fuente: WeLiveSecurity

Obtención del C&C vía **Instagram**



Fuente: WeLiveSecurity

Herramientas de fase 2

Herramientas personalizadas

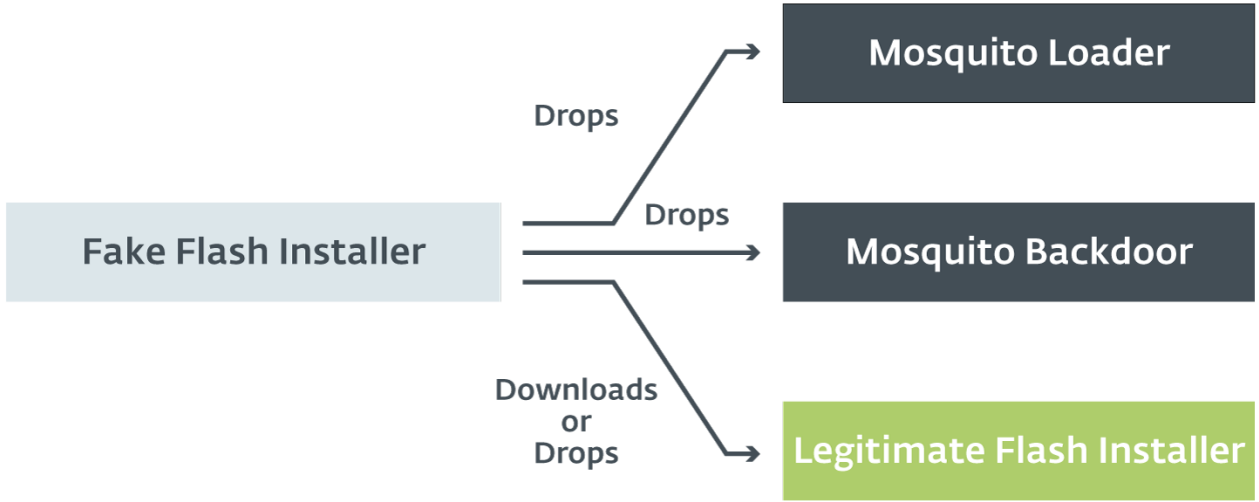
Carbon / Cobra
Gazer

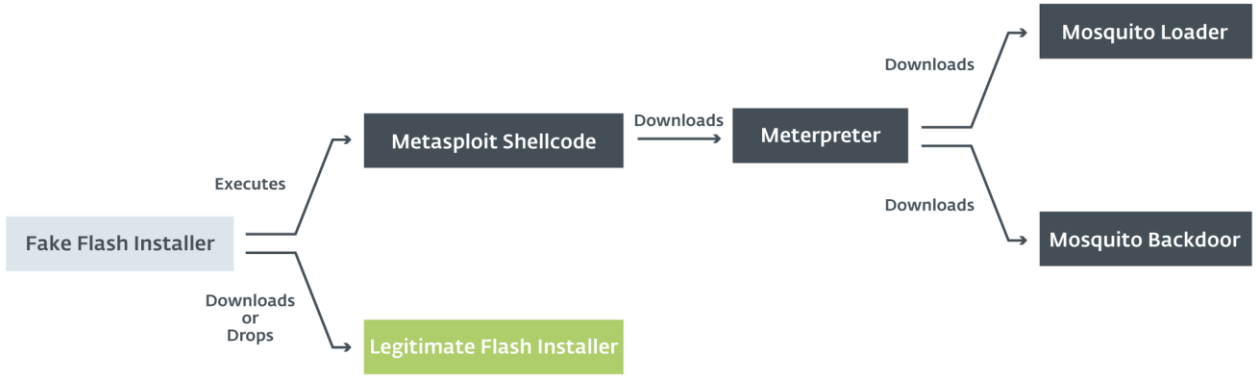
Objetivos:
Antiguos paises satélites URSS

Herramientas estándar

Herramienta Mosquito

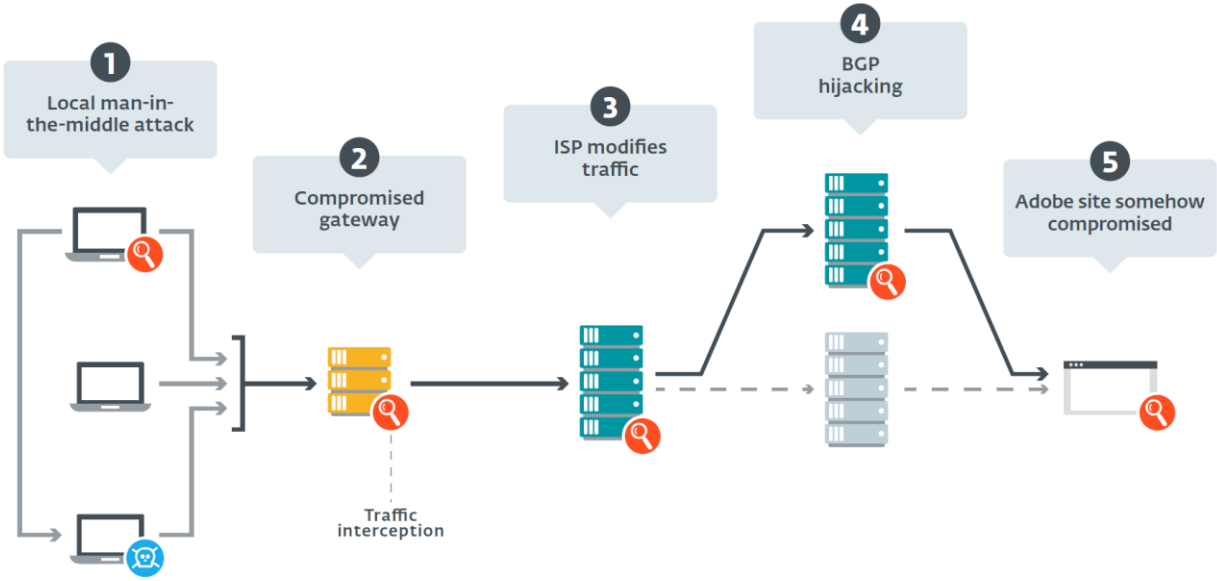
Herramienta Mosquito





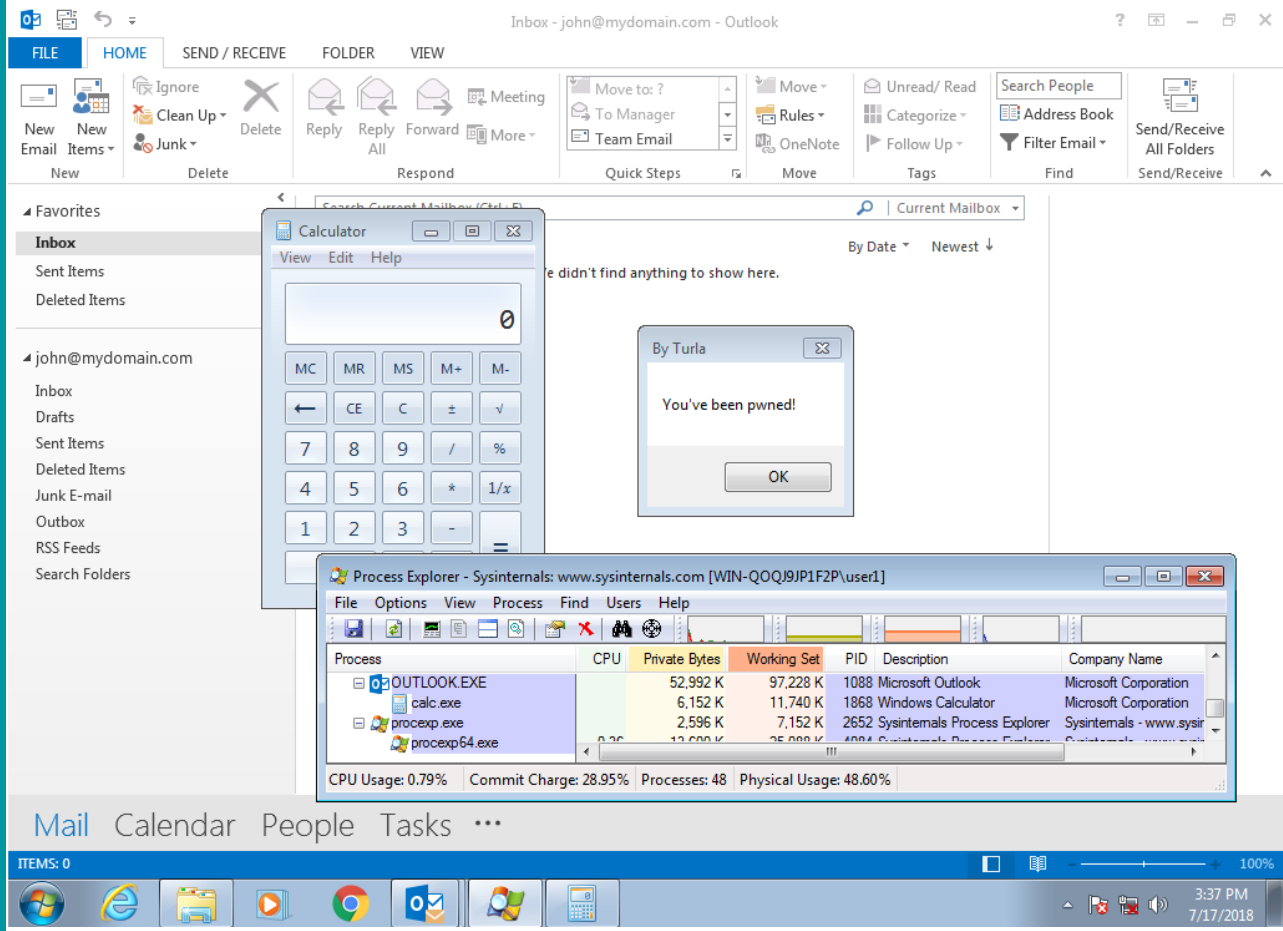
Fuente: WeLiveSecurity

Mosquito: posibles vías de infección



Fuente: WeLiveSecurity

Módulo para Outlook



Fuente: WeLiveSecurity

Sednit (Fancy bear, Apt28, Sofacy Group)

Víctimas

TV5MONDE

DNC

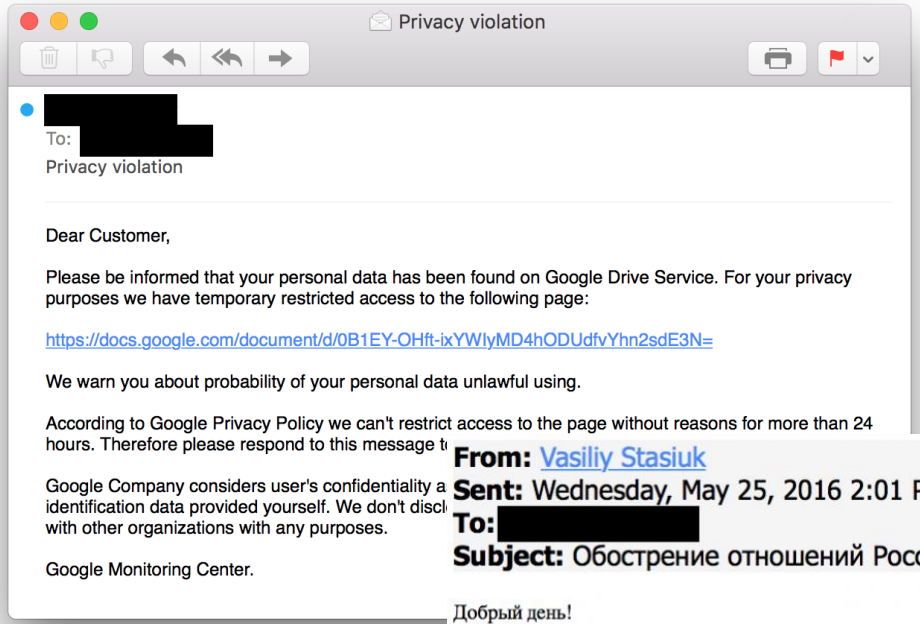
Deutscher Bundestag

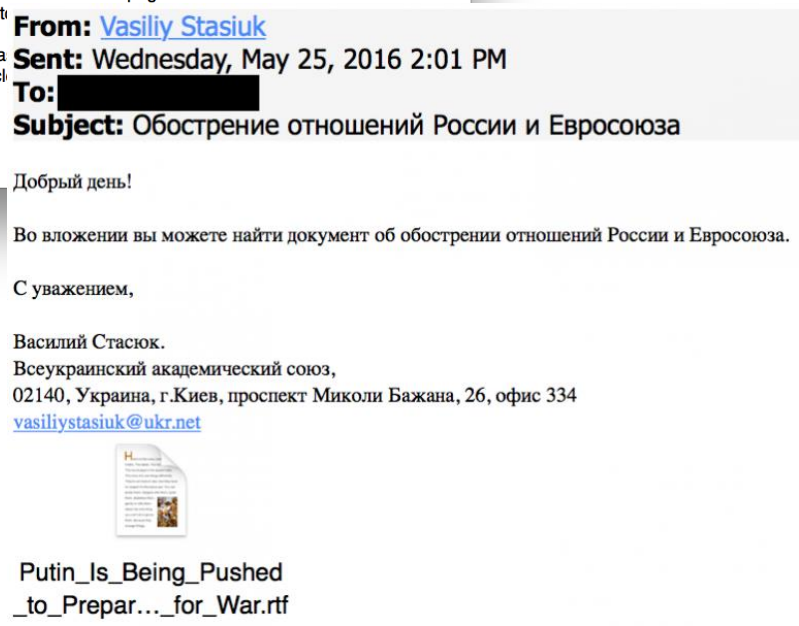
IAAF Athletics

International Association of Athletics Federations

Herramientas propias y de terceros

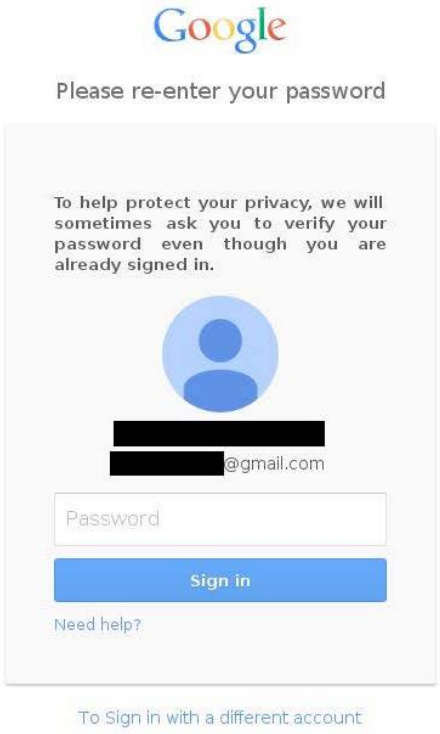
Vector de ataque: email



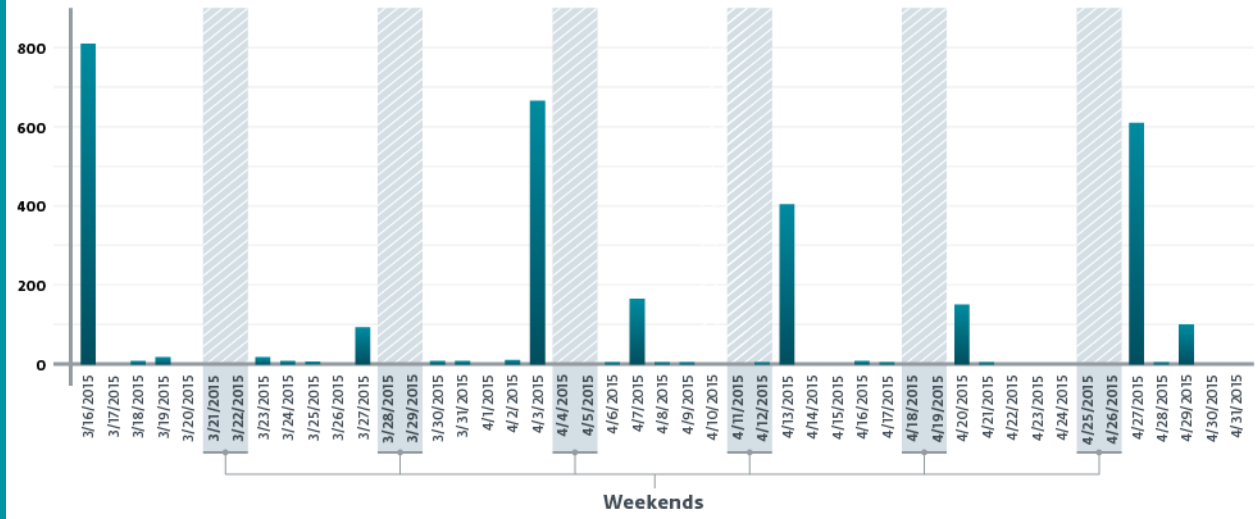


Fuente: WeLiveSecurity

Uso de Gmail

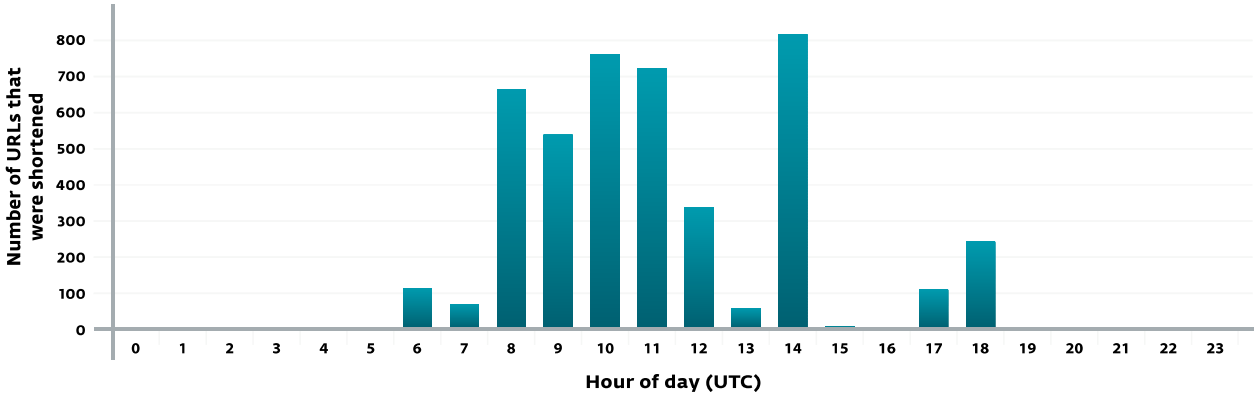

Google
Please re-enter your password
To help protect your privacy, we will sometimes ask you to verify your password even though you are already signed in.
[redacted]@gmail.com
Password
Sign in
Need help?
To Sign in with a different account

Campañas y horarios



Fuente: WeLiveSecurity

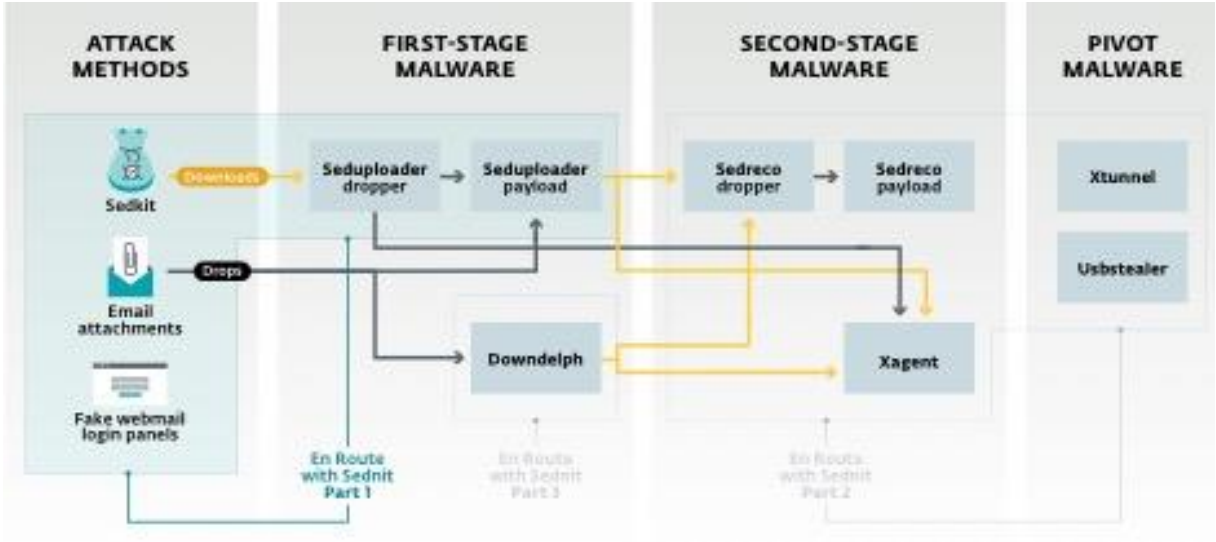
¿Atribuciones?



Fuente: WeLiveSecurity

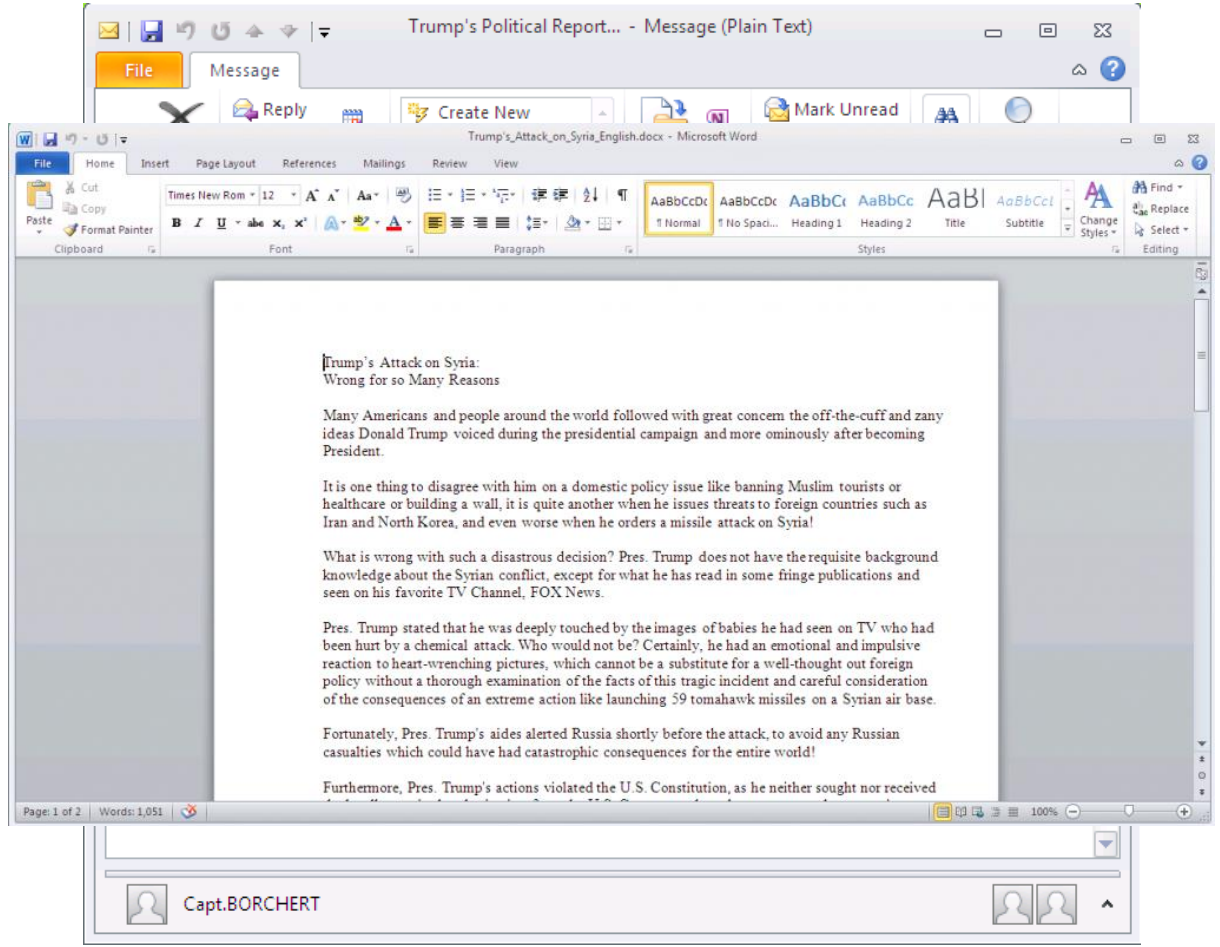
Herramientas propias

Backdoors	Downloader	Proxy
SEDRECO	DOWNDELPH	XTUNNEL
XAGENT	ZEBROCY	
	SEDUPLOADER	



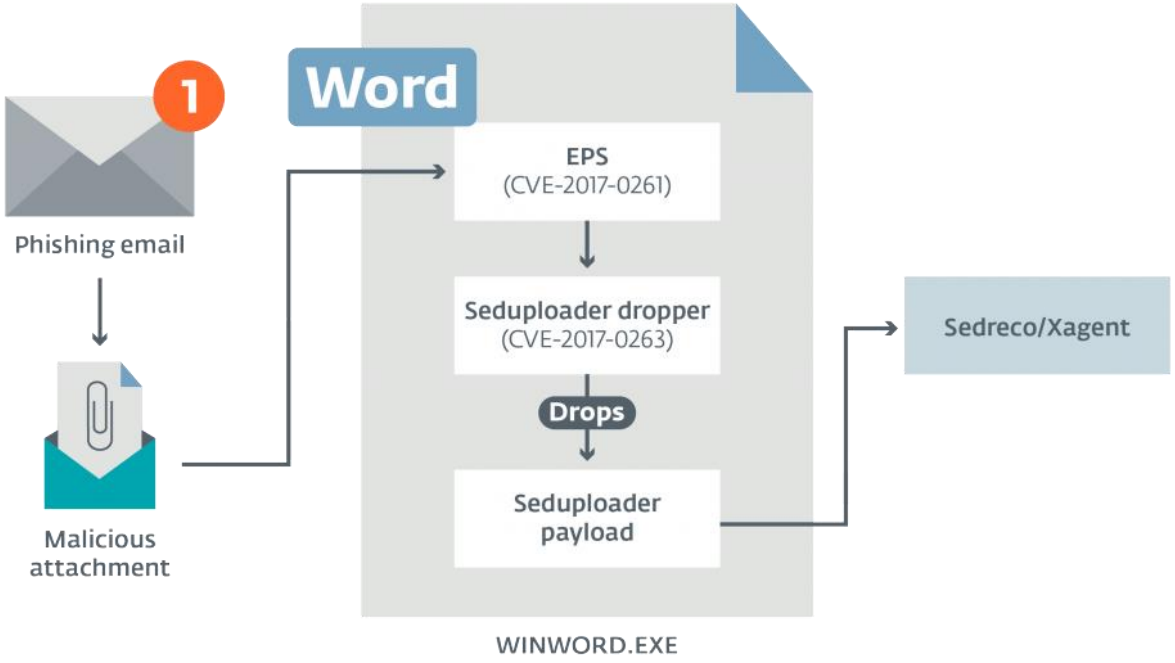
Fuente: WeLiveSecurity

Ejemplo: elecciones francesas



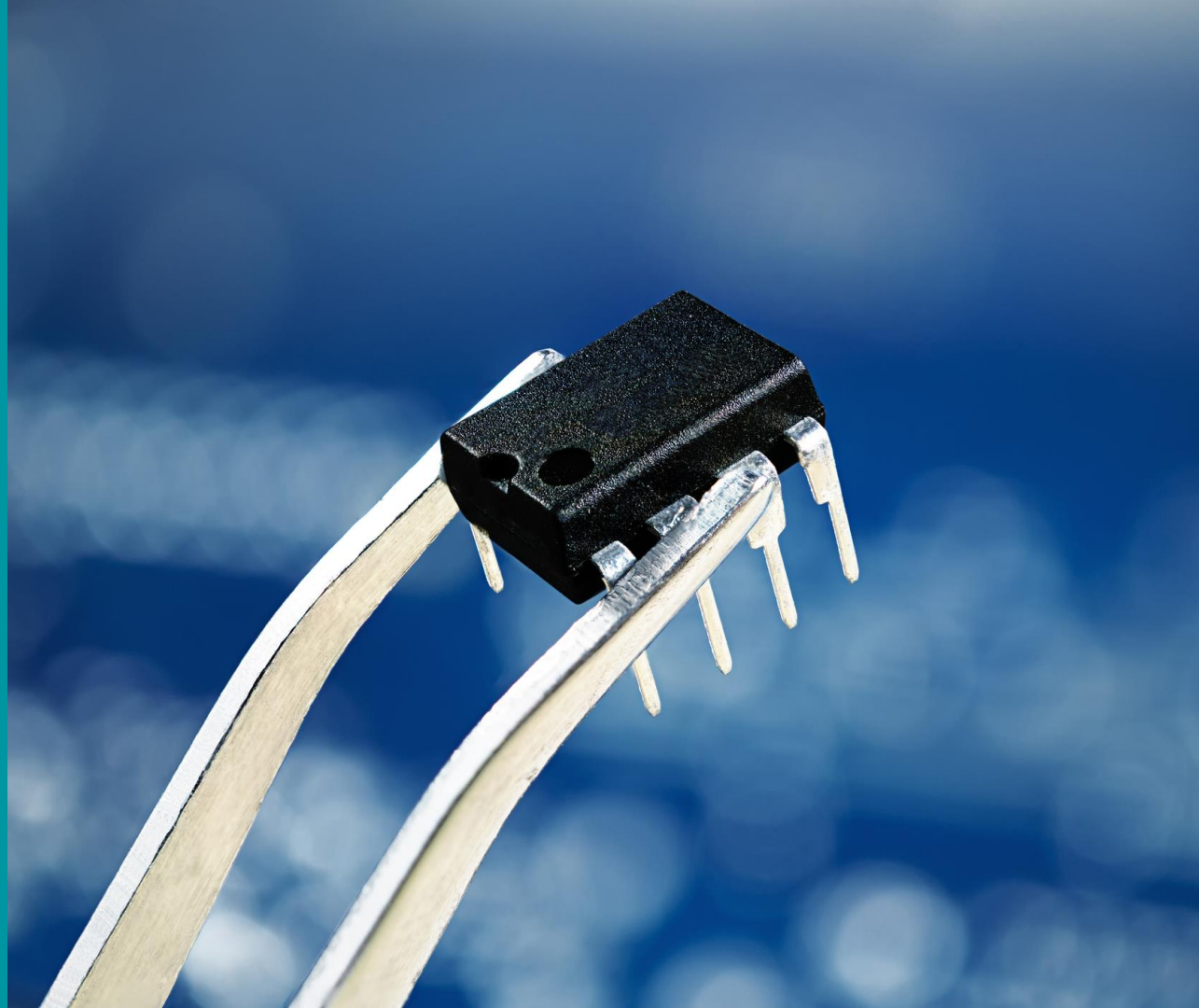
Fuente: WeLiveSecurity

Ejemplo: elecciones francesas



Fuente: WeLiveSecurity

LoJax: primer rootkit UEFI detectado en ciberataque



Objetivos

Antecedentes: LoJack

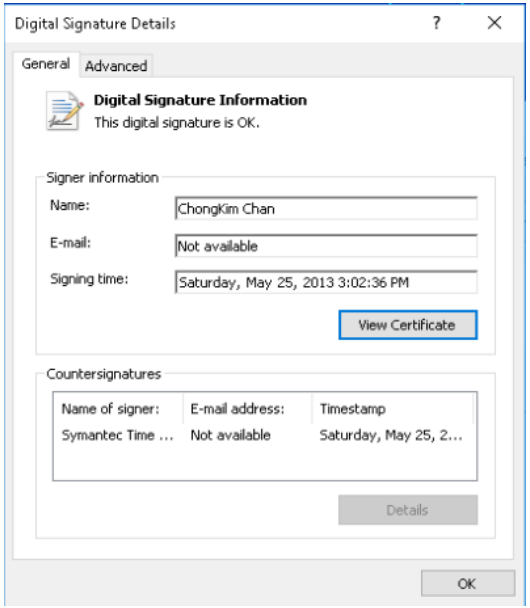
Lojack Becomes a Double-Agent

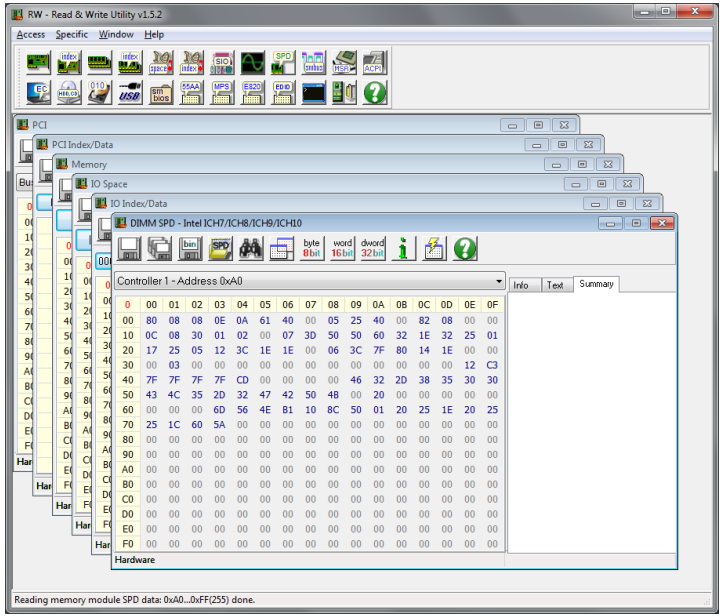
A ASERT team on May 1, 2018.

Fuente: Arbor Networks

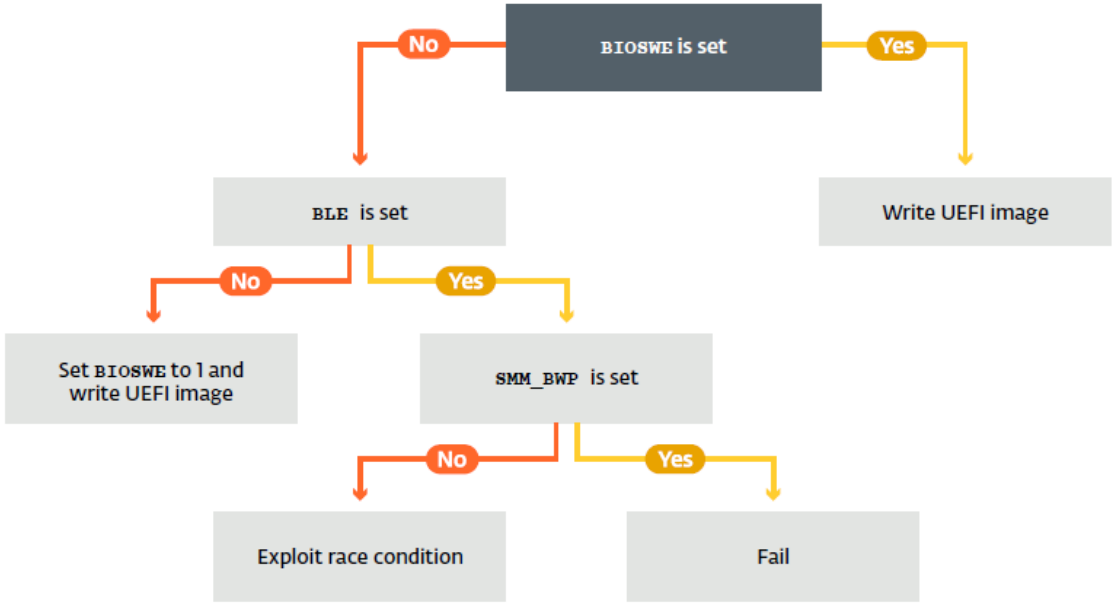
Computrace: sistema antirrobo comprometido

Uso de herramientas legítimas





Modificación en tres pasos



Fuente: WeLiveSecurity

Conclusiones

- Ataques dirigidos a objetivos o sectores muy concretos
- La mayoría de las veces buscan obtener una ventaja geopolítica
- Uso de herramientas propias avanzadas…
- …pero también de herramientas de terceros conocidas
- Los vectores de ataque iniciales son sobradamente conocidos
- Muchos de los incidentes nombrados podrían haberse evitado con buenas prácticas

Información detallada

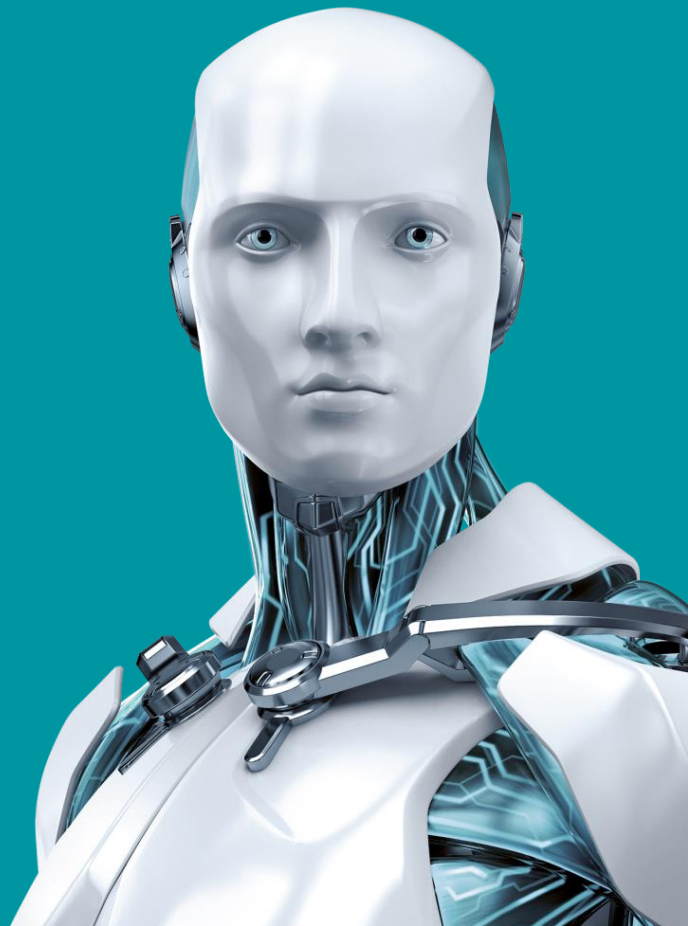
Agradecimientos

Agradecimientos

¡Gracias por la atención!

Josep Albors
Responsable de Investigación y Concienciación
josep@eset.es

ENJOY SAFER TECHNOLOGY™



ENJOY SAFER TECHNOLOGY™