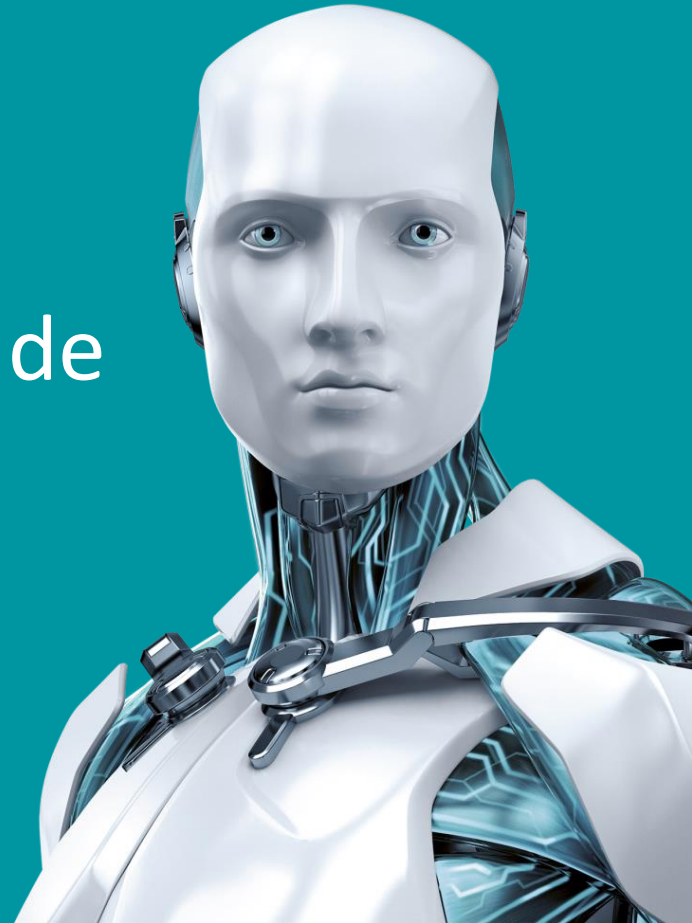


Mosquitos, serpientes, osos y otras herramientas avanzadas de espionaje



ENJOY SAFER TECHNOLOGY™

Situación Actual



Ataques dirigidos



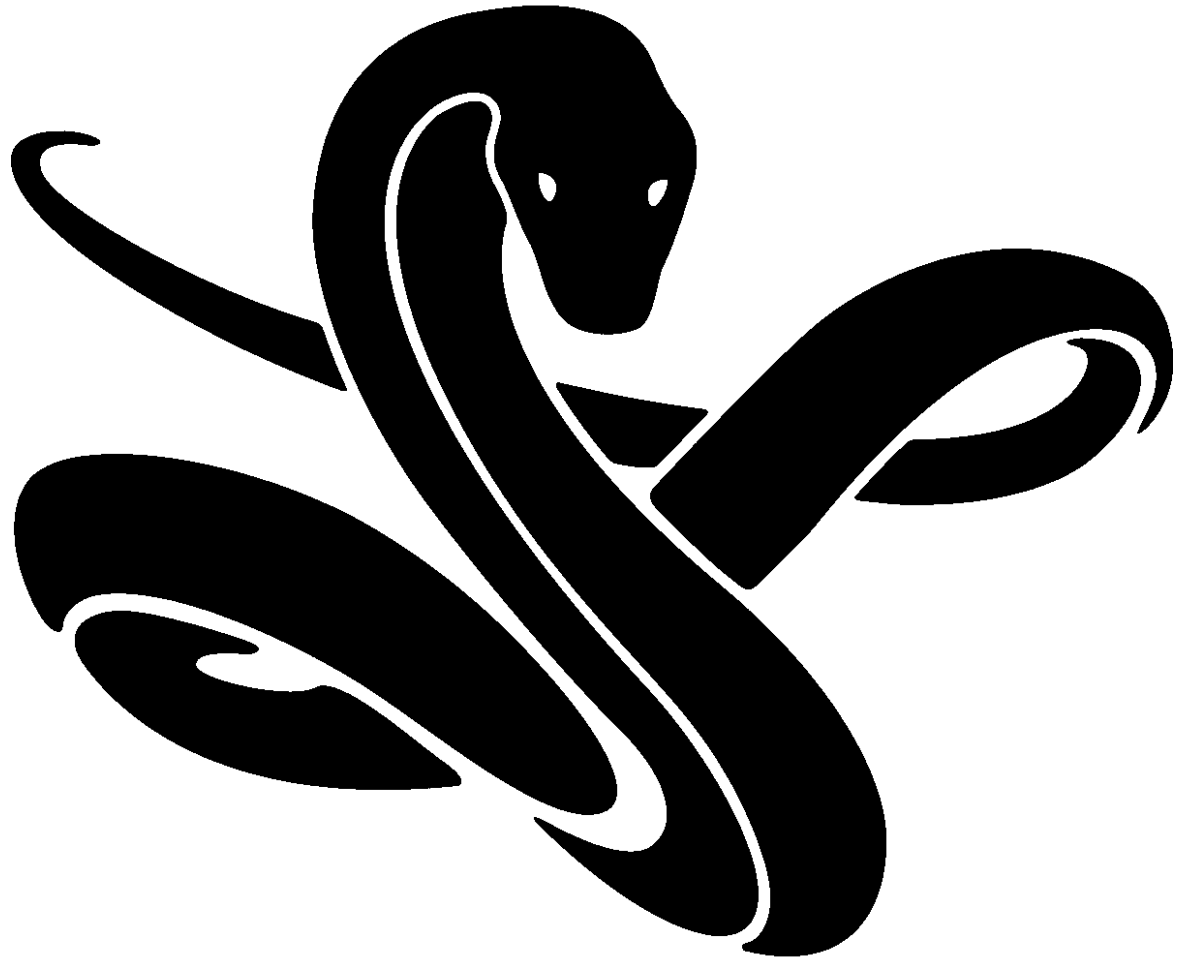
Grupos especializados



Objetivos



Grupo Turla
(Snake, Uroburos)



Víctimas



Federal Foreign Office



Cronología Turla

1996 Moonlight Maze (LOKI2 backdoor)

.
..
...

2009



Compilation timestamp (may be faked) of a basic version of the Outlook backdoor. It could only dump email content.

2013

Improvement: the backdoor could execute commands. They are sent by email in XML format.

2013

Last known version targeting The Bat! email client.

2016

Improvement: the commands are now sent as attachments in specially crafted PDF documents.

2018
April

Improvement: the backdoor can execute PowerShell commands by leveraging Empire PSInject.

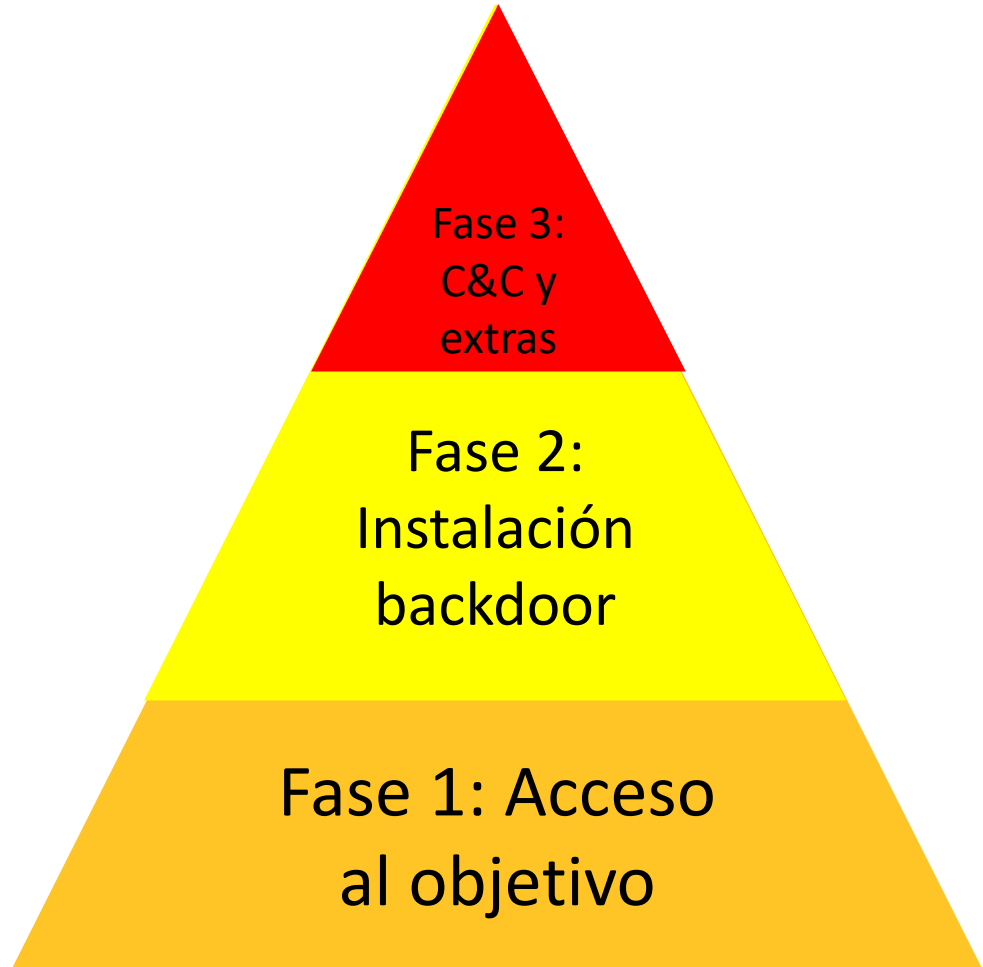
2018
March

Public announcement of the compromise of the German government.

2017

Improvement: the backdoor is able to build PDF documents to exfiltrate data to the attackers.

Ataques Multifase



Vector de ataque: email



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

Fuente: Securelist



430003-155103(1)



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

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

г. Москва Дело № А40-37262/13
24 октября 2013 года
Судья Б.С. Веклич рассмотрел 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 Лариной Г.М. (30-321)
по иску ООО «Диамайт» (ОГРН 1083123021057, 308007, г.Белгород, ул.Мичурина, д.56)
к ООО «СТРОЙЭКСПОЛ» (ОГРН 1027743009436, 125599, Москва, ул.Бусыновская 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.

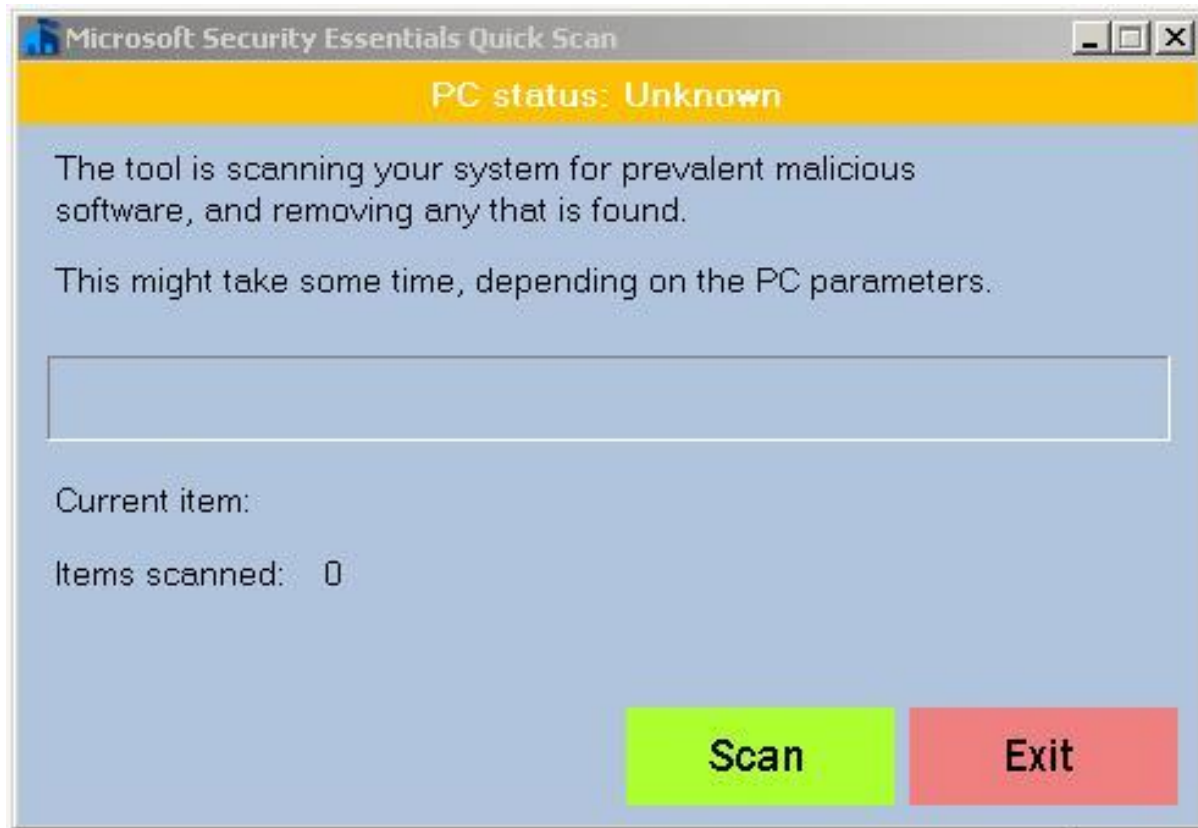
Лицам, участвующим в деле, обеспечить явку полномочных представителей или
известить суд о возможности рассмотрения дела в их отсутствие.

Судья Б.С. Веклич

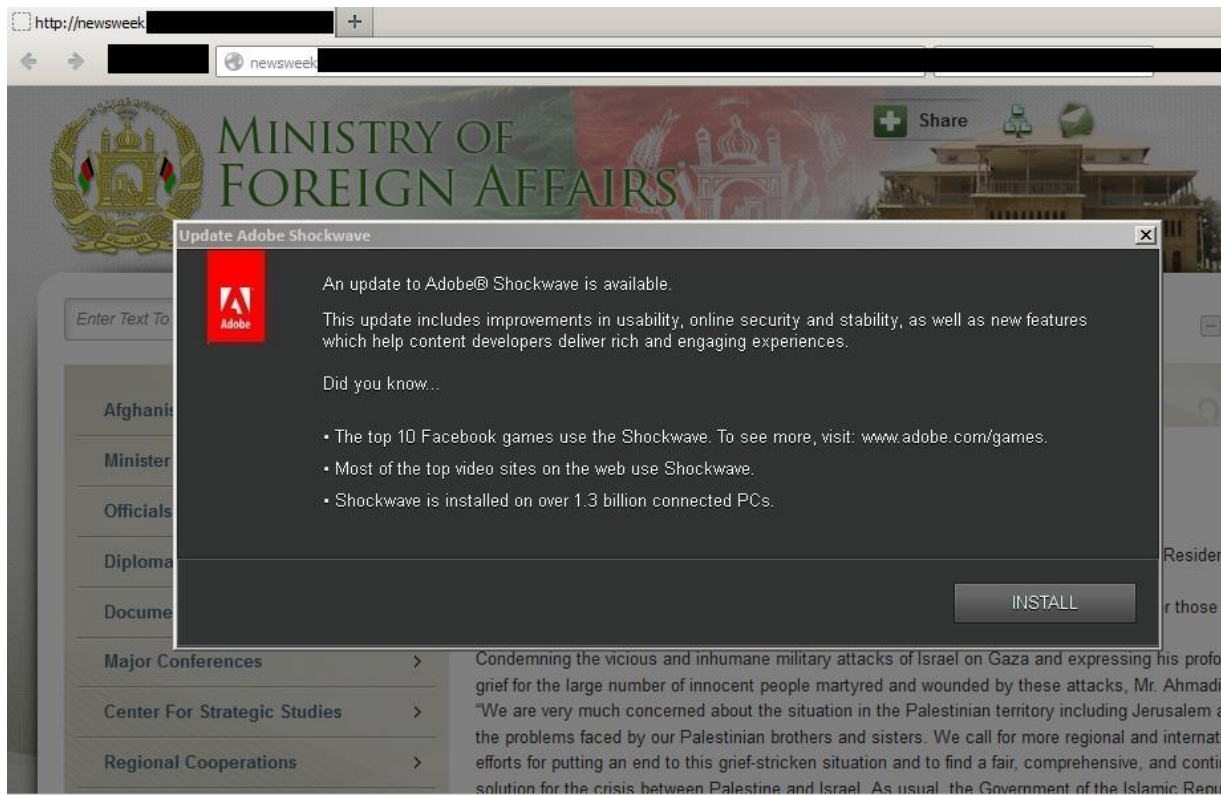
Телефон справочной службы суда – 8 (495) 985-2640
Факс - 8 (495) 987-29-11

Информация о движении дела размещается на сайте суда в сети Интернет по веб-адресу: www.9asc.arbitr.ru
в Картотеке арбитражных дел по веб-адресу: <http://kad.arbitr.ru>.

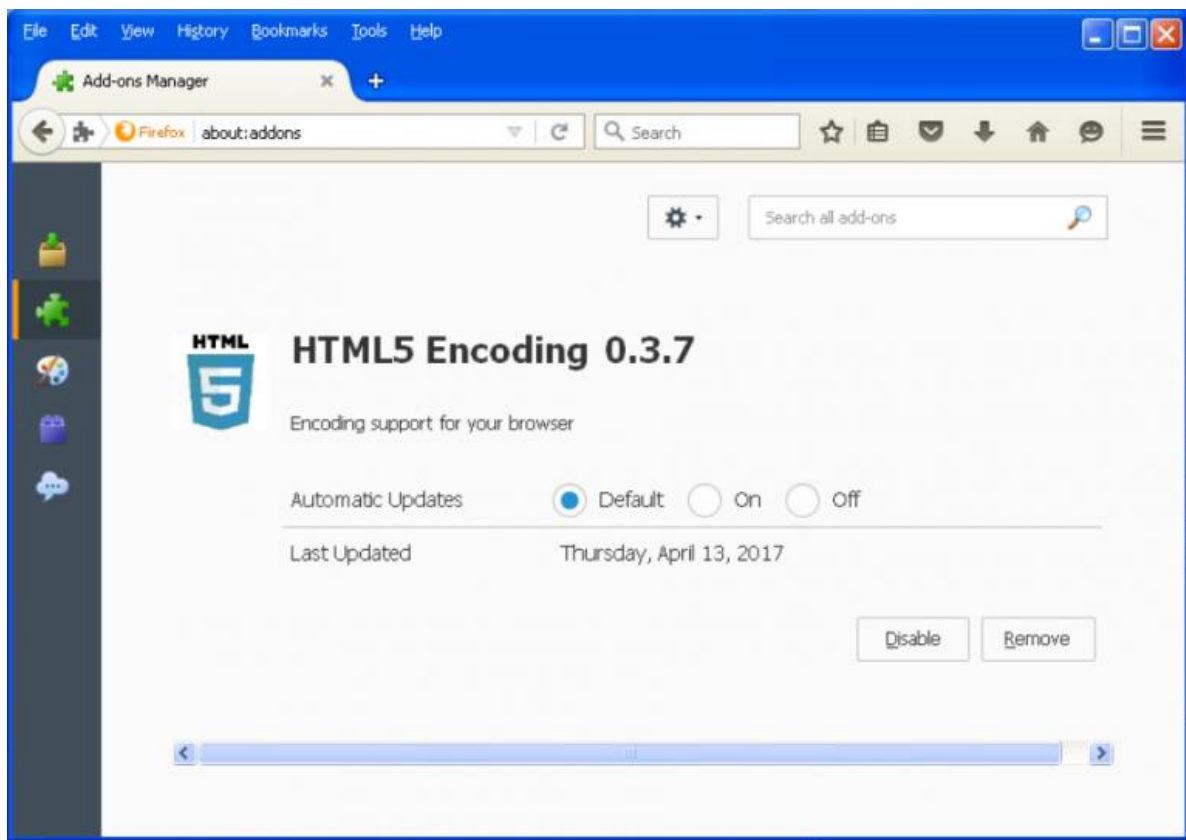
Vector de ataque: falsas aplicaciones de seguridad



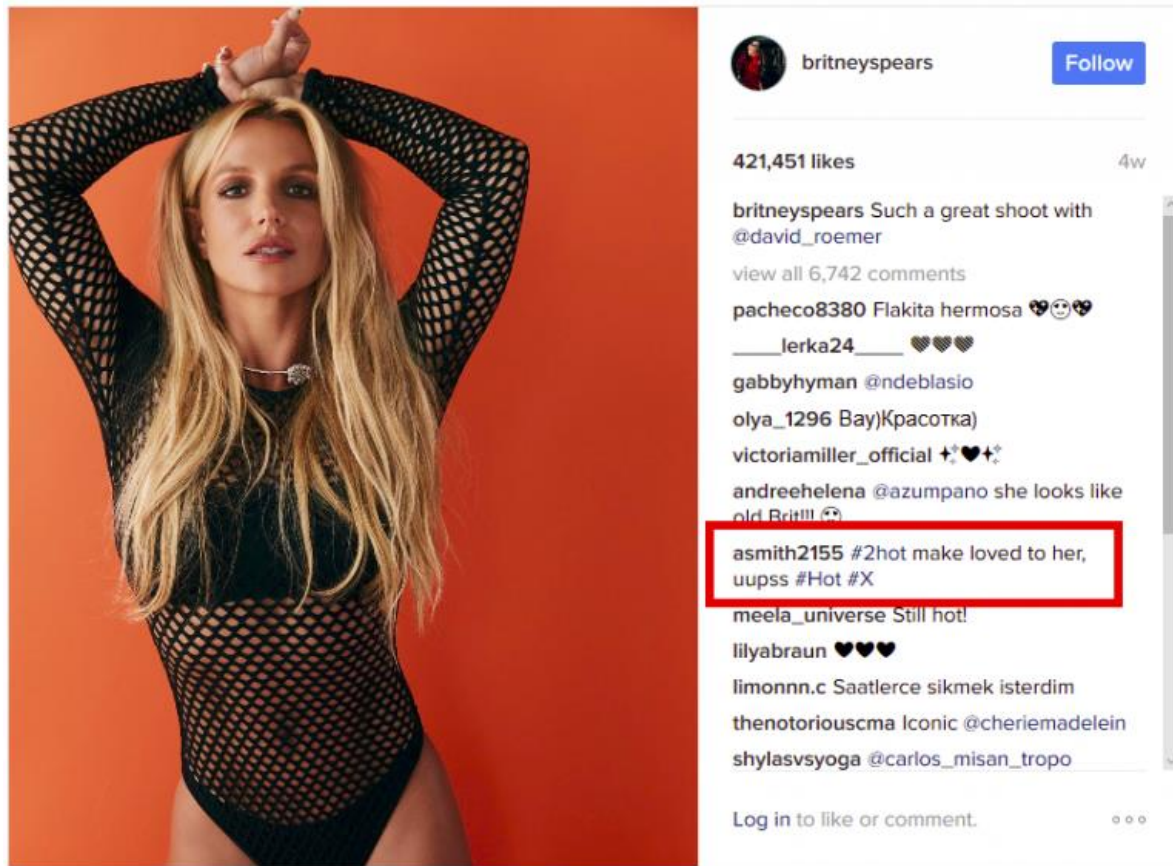
Vector de ataque: falsos instaladores Flash Player



Vector de ataque: extensiones de Firefox



Obtención del C&C vía Instagram



Herramientas de fase 2



Herramientas
personalizadas



Carbon / Cobra
Gazer

Objetivos:
Antiguos países
satélites URSS



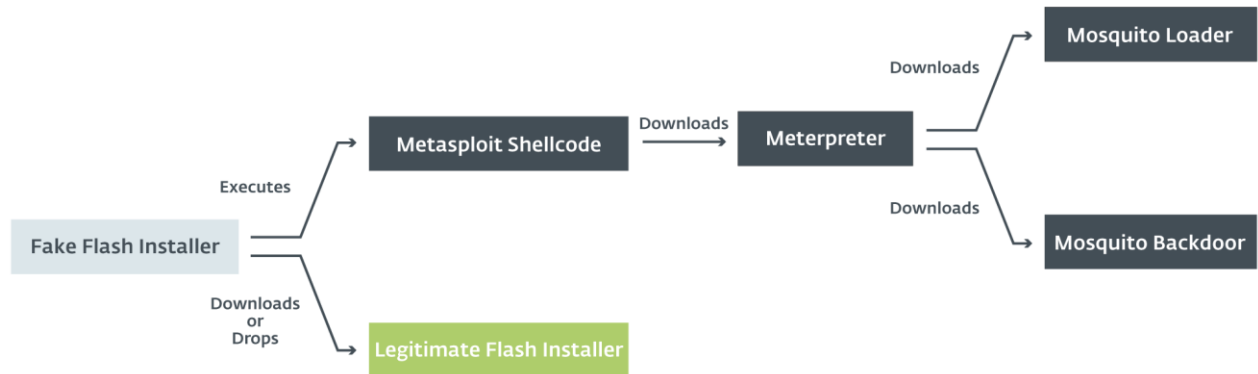
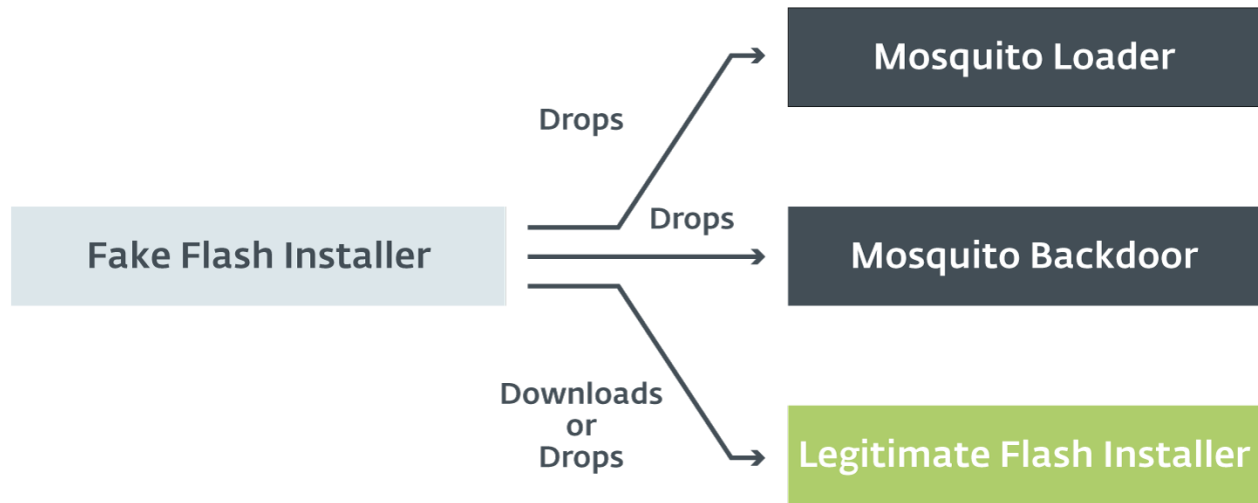
Herramientas estándar



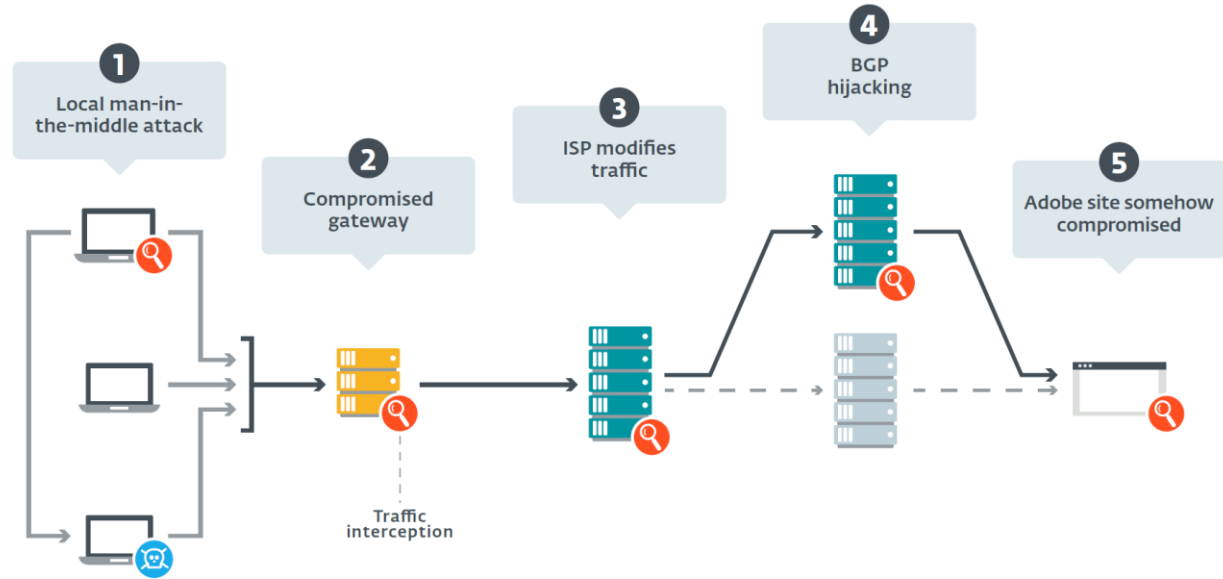
Herramienta Mosquito



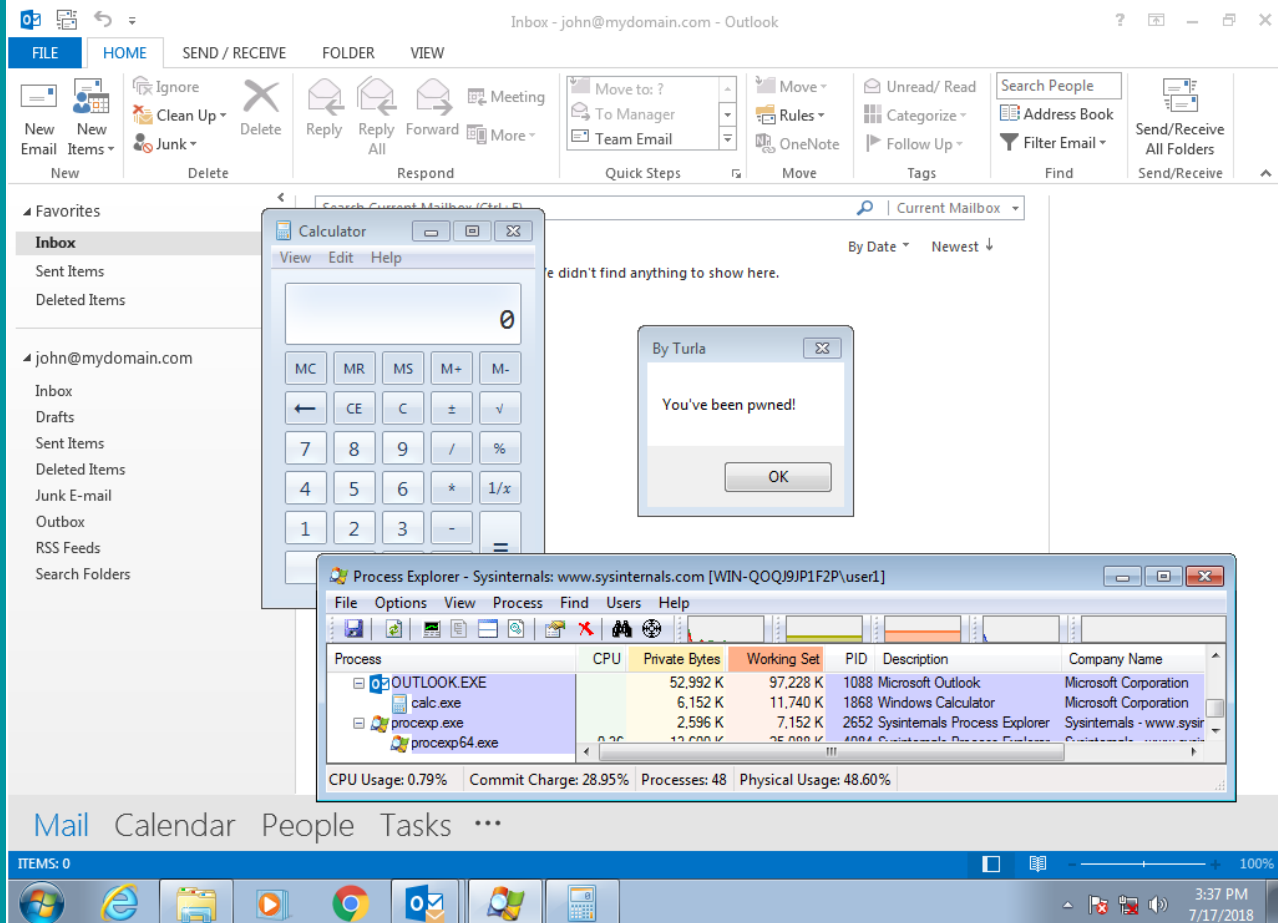
Herramienta Mosquito



Mosquito: posibles vías de infección



Módulo para Outlook



**Sednit (Fancy
bear, Apt28,
Sofacy Group)**



TV5MONDE

DNA

Víctimas



Deutscher
Bundestag

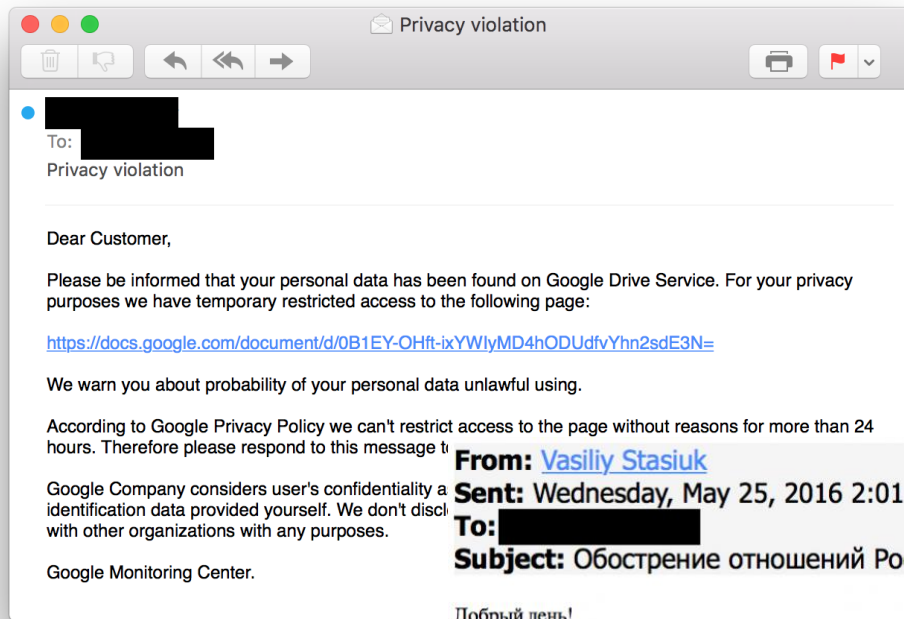


International Association
of Athletics Federations

Herramientas propias y de terceros



Vector de ataque: email



Добрый день!

Во вложении вы можете найти документ об обострении отношений России и Евросоюза.

С уважением,

Василий Стасюк.

Всеукраинский академический союз,

02140, Украина, г.Киев, проспект Миколи Бажана, 26, офис 334

vasiliystasiuk@ukr.net



Uso de Gmail



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.



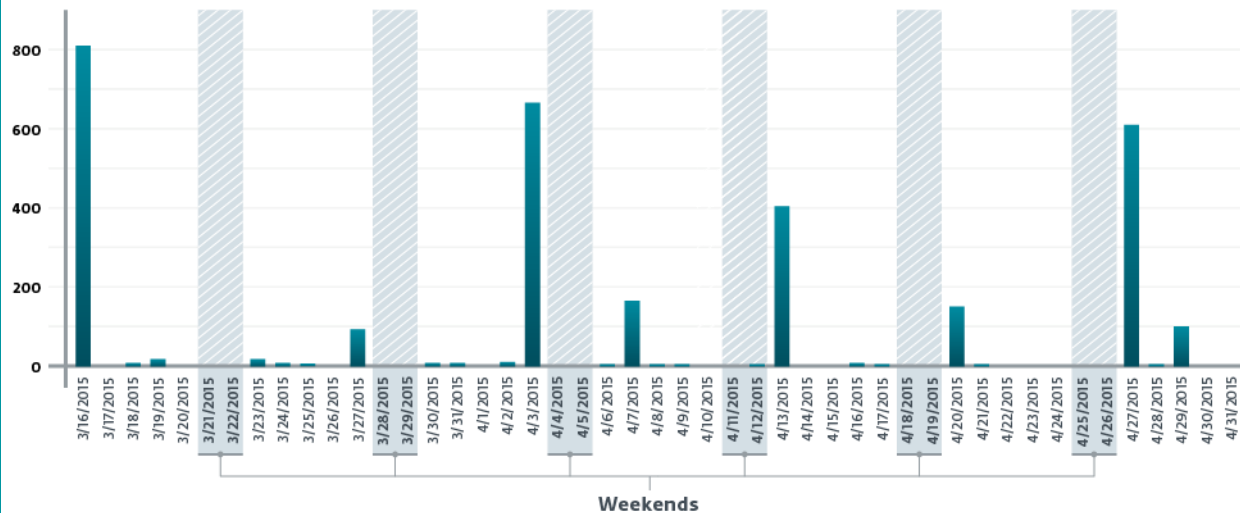
[Redacted]
[Redacted]@gmail.com

Sign in

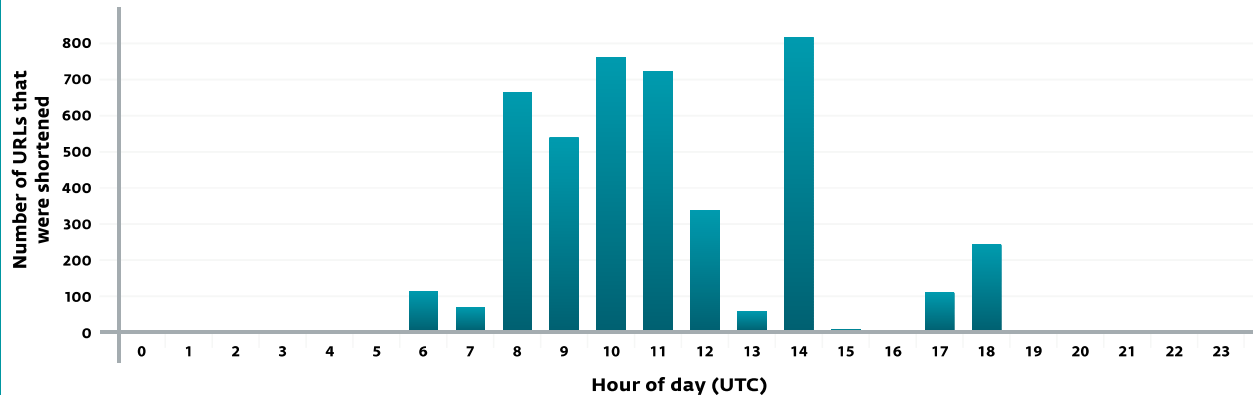
[Need help?](#)

[To Sign in with a different account](#)

Campañas y horarios



¿Atribuciones?



Fuente: WeLiveSecurity

Herramientas propias

Backdoors

SEDRECO

XAGENT

Downloader

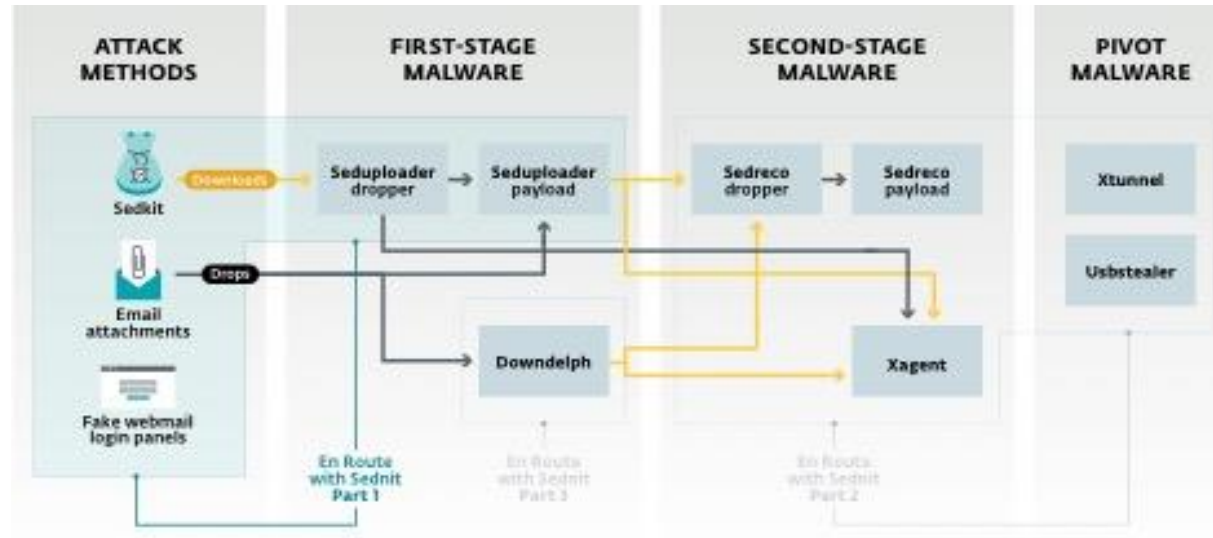
DOWNDDELPH

ZEBROCY

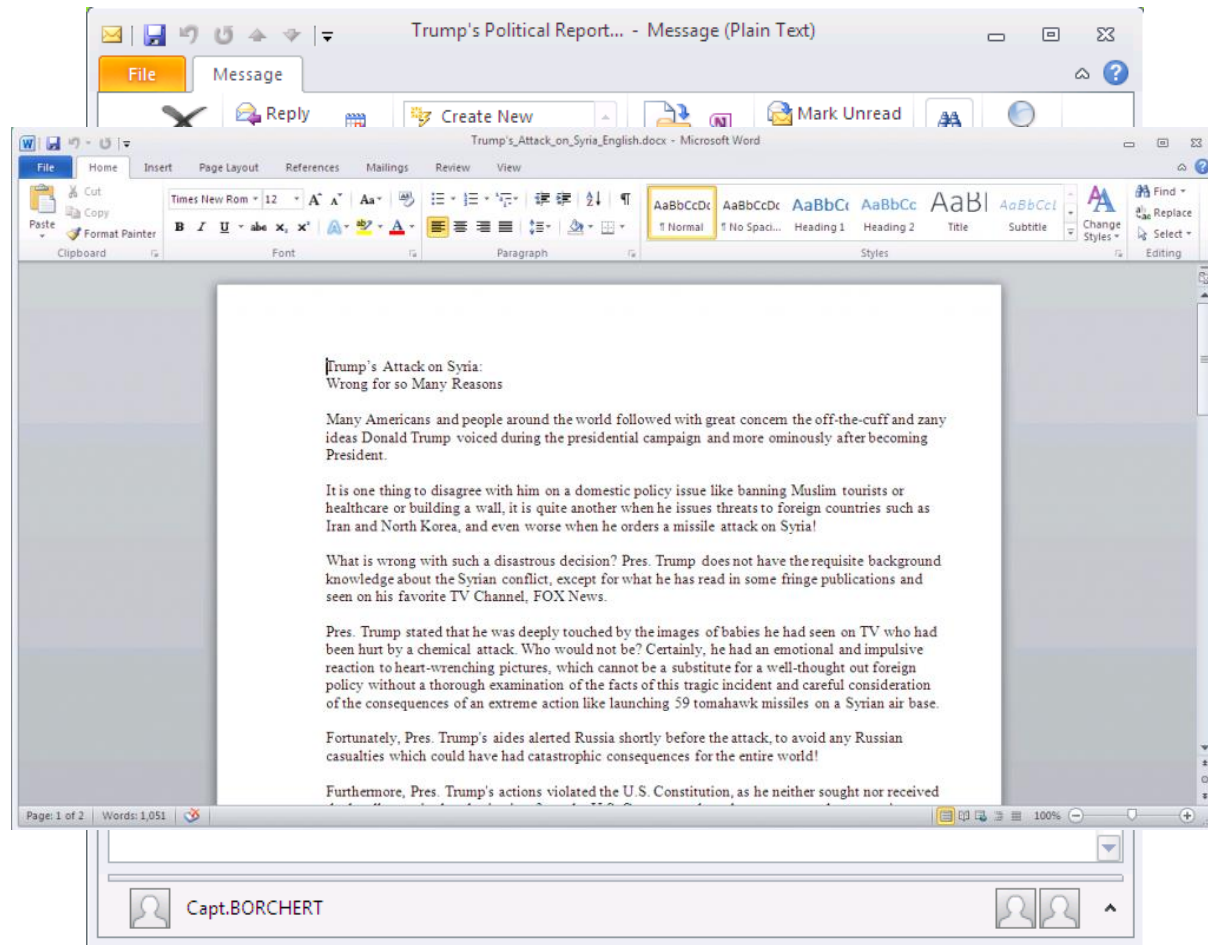
SEDUPLOADER

Proxy

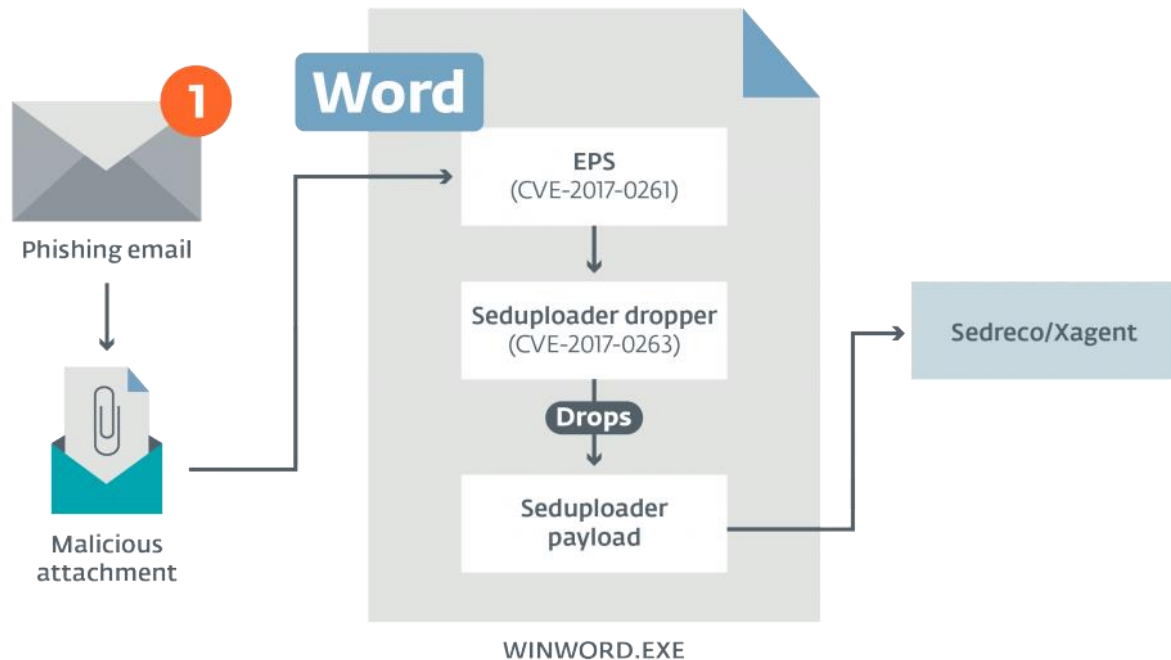
XTUNNEL



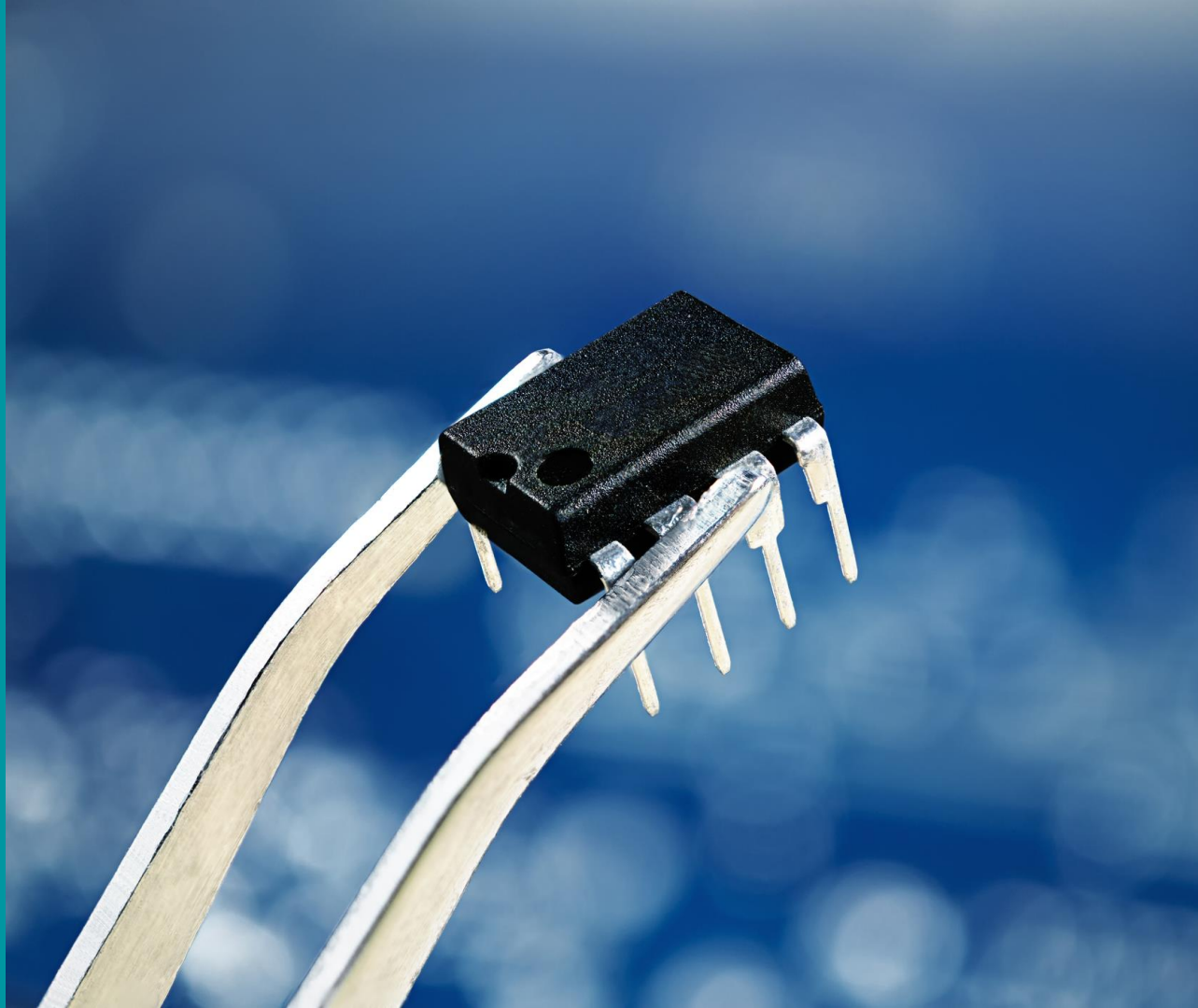
Ejemplo: elecciones francesas



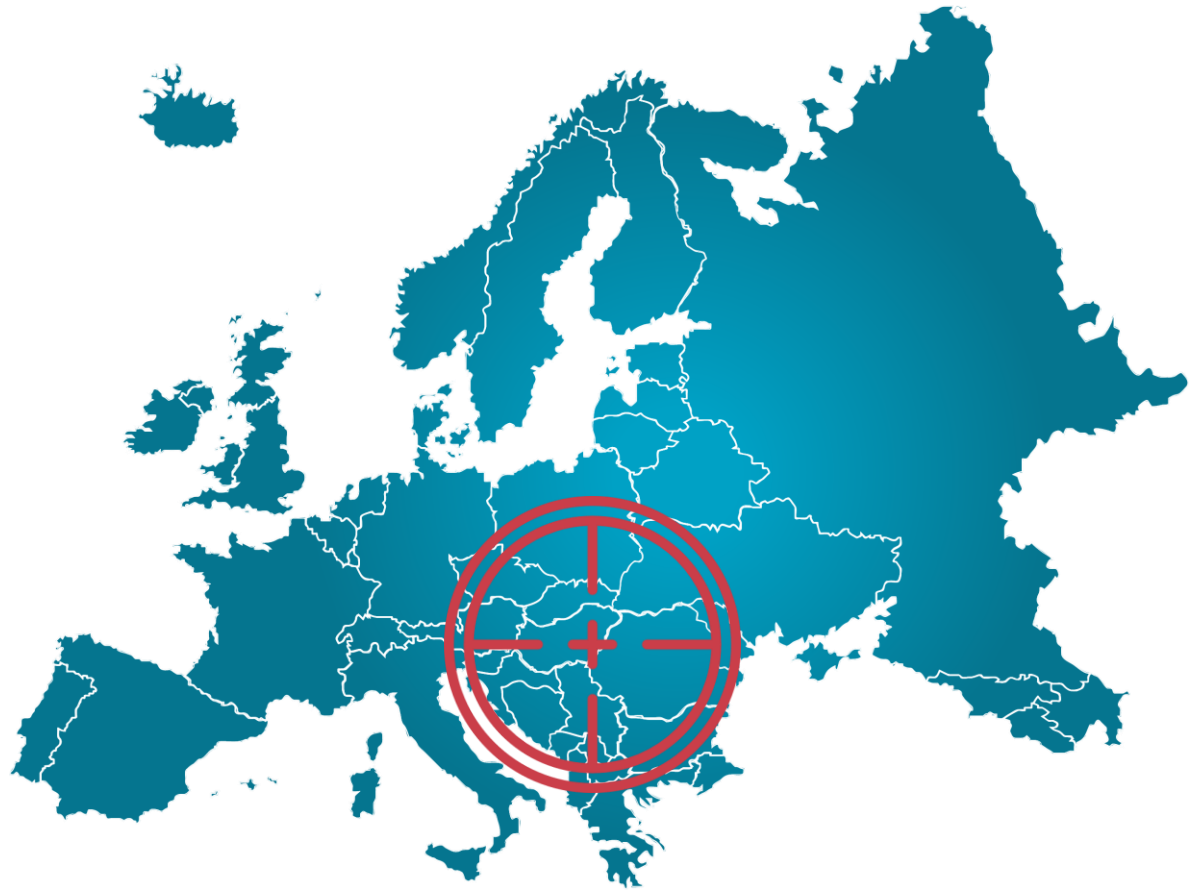
Ejemplo: elecciones francesas



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

ASUS UEFI BIOS Utility - EZ Mode Exit/Advanced Mode

09:29
Sunday 02/08/2015

P6277-M P80
BIOS Version : 2105
CPU Type : Intel(R) Core(TM) i7-3770S CPU @ 3.10GHz Speed : 3100 Mhz
Total Memory : 16384 MB (DDR3 1333Mhz)

Temperature
CPU: +104.0°F/+40.0°C
MB: +80.6°F/+27.0°C

Voltage
CPU: 0.960V 5V 5.120V
3.3V 3.370V 1.2V 12.300V

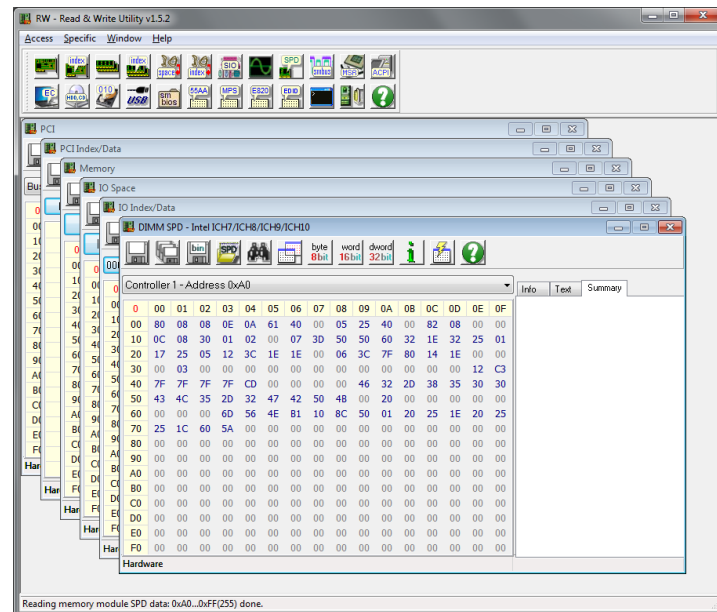
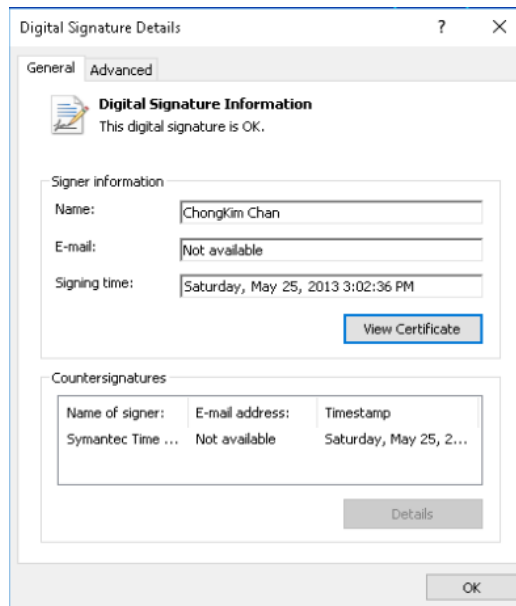
Fan Speed
CPU_FAN: 1314RPM
CHA_FAN1: 805RPM
CHA_FAN2: 800RPM
CHA_FAN3: N/A

System Performance
Quiet Performance Energy Saving Normal

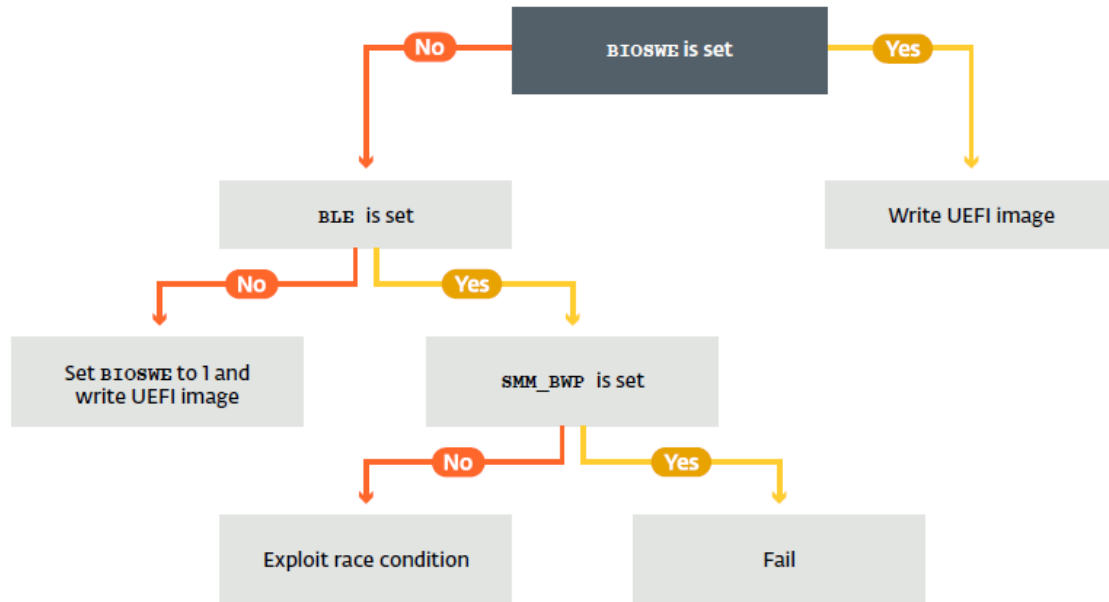
Boot Priority
Use the mouse to drag or keyboard to navigate to decide the boot priority.

Shortcut (F3) Advanced Mode (F7) Boot Menu (F8) Default (F9)

Uso de herramientas legítimas



Modificación en tres pasos



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

Lojax: First UEFI rootkit found in the wild, courtesy of the Sednit group

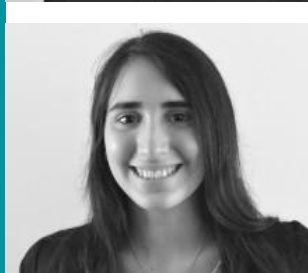
ESET researchers have shown that the Sednit operators used different components of the Lojax malware to target a few government organizations in the Balkans as well as in Central and Eastern Europe



Turla: In and out of its unique Outlook backdoor

The latest ESET research offers a rare glimpse into the mechanics of a particularly stealthy and resilient backdoor that the Turla cyberespionage group can fully control via PDF files attached to emails

Agradecimientos



Agradecimientos





¡Gracias por la atención!



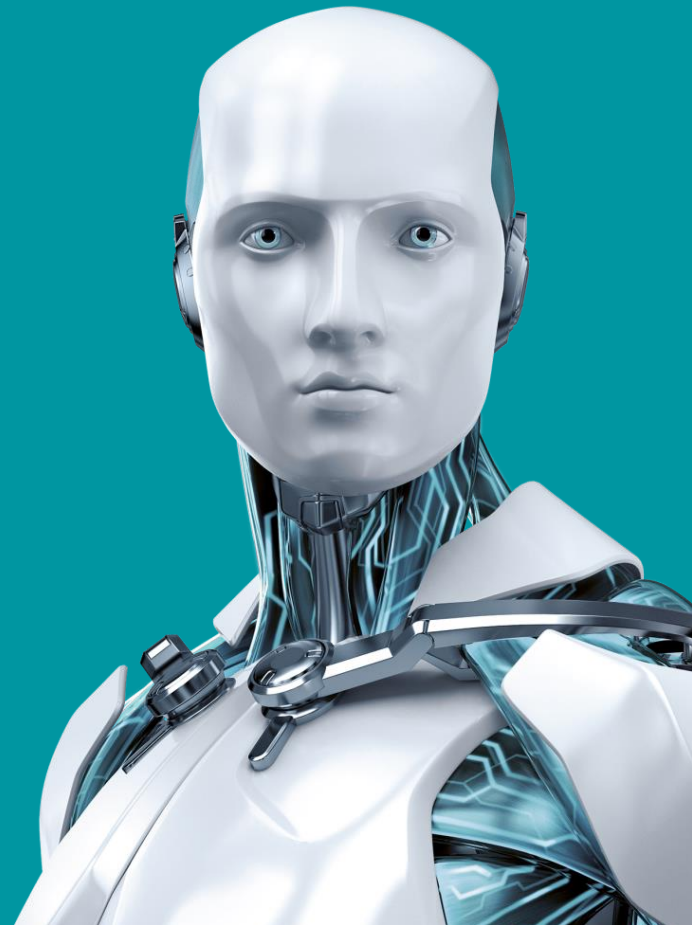
Josep Albors

Responsable de Investigación y Concienciación

josep@eset.es



ENJOY SAFER TECHNOLOGY™





ENJOY SAFER TECHNOLOGY™