

Seminario de Actualización III: CiberSeguridad

Exposición: Casos Reales Relacionados a la CiberSeguridad – Stuxnet

```
CuteMouse v1.9.1 alpha 1 [FreeDOS]
Installed at PS/2 port          CuteMouse v1.9.1 alpha 1 [FreeDOS]
C:\>ver                         in drive C is FREEDOS_C95
FreeCom version 0.82 pl 3 XMS_Swap [Dec 10 2009]
C:\>dir
Volume in drive C is FREEDOS_C95
Volume Serial Number is 004F-192B
Directory of C:\>
FDOS               DIR  08-26-04   6:23p
AUTOEXEC.BAT      35    08-26-04   6:24p
BOOT.LST          512   08-26-04   6:23p
COMMAND.COM       93,963  08-26-04   6:24p
CONFIG.SYS        801   08-26-04   6:24p
FDOSBOOT.BIN      512   08-26-04   6:24p
KERNEL.SYS        45,815  04-17-04  9:19p
6 file(s)          142,038 bytes
                   1 dir(s)  1,064,517,632 bytes free
C:\>_ CuteMouse v1.9.1 alpha 1 [FreeDOS]
```

Grupo:

Quema Focos

Integrantes:

Albarenga Alexis

Britez Milagros

Espínola Gastón

Esteche Lucas

Sánchez Nahuel

Índice

Seminario de Actualización III: CiberSeguridad.....	1
Exposición: Casos Reales Relacionados a la CiberSeguridad – Stuxnet.....	1
Introducción.....	3
¿Qué es un Gusano Informático?.....	3
Diferencia entre Gusanos Informáticos y otros virus.....	3
¿Qué fue Stuxnet?.....	4
Origen y Autores Probables.....	5
Método de infiltración y propagación de Stuxnet.....	6
Qué son las Zero-Day Exploits.....	7
Flujo de ataque de Stuxnet.....	8
Una nueva forma de Guerra.....	8
Stuxnet salió de Irán.....	9
Como Stuxnet fue detenido en Israel.....	9
Como Stuxnet fue detenido en otros países :.....	9
Estados Unidos y Europa.....	9
India, Indonesia y Pakistán.....	9
Conclusión.....	10
Referencias.....	10

Introducción

En el respectivo trabajo vamos a abordar el caso de Stuxnet, uno de los ciberataques más reconocidos y con un impacto importante en la historia, el cual se considera como punto de inflexión en la ciberseguridad mundial. A lo largo del texto vamos a contar, qué fue Stuxnet, el contexto en que surge, las vulnerabilidades zero-day que explotó y su impacto en las infraestructuras industriales. También vamos a explorar su influencia en la evolución y desarrollo en la ciberseguridad global y el impacto en el ámbito político, tecnológico y social derivados de este ataque. Finalmente reflexionamos como el malware redefinió la forma en que los Estados y Organizaciones conciben la seguridad en el ciberespacio.

¿Qué es un Gusano Informático?

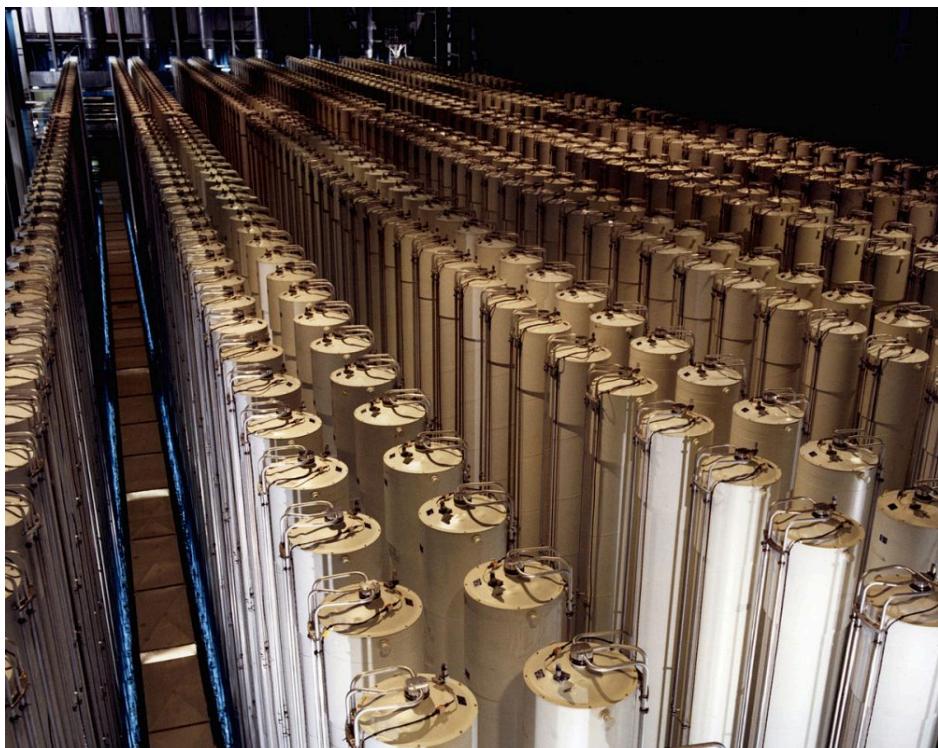
Es un tipo de malware que tiene la capacidad de propagarse automáticamente de una computadora a otra a través de redes, como internet o LAN, sin necesidad de intervención humana. A diferencia de otros tipos de malware, los gusanos no suelen infectar archivos en el ordenador, sino que se replican y envían copias de sí mismos a otros dispositivos en la red. Esto los convierte en una amenaza significativa, ya que pueden causar daños extensos y congestionar redes (Falliere, Murchu & Chien, 2011).

Diferencia entre Gusanos Informáticos y otros virus

CARACTERISTICAS	GUSANO INFORMATICO	VIRUS INFORMATICO	TROYANO	RANSOMWARE
FORMA DE PROPAGACIÓN	se replica automaticamente a traves de redes y sistemas sin intervencion del usuario.	Necesita infectar archivos ejecutables o programas y propagarse cuando estos se comparten/ejecutan.	No se replica solo, se oculta en programas aparentemente legitimos instalados por el usuario.	Se propaga como virus o troyano, pero su fin es cifrar archivos y pedir rescate.
DEPENDENCIAS DE ARCHIVOS	No necesita adjuntarse a otro archivo para propagarse.	Se adhiere a archivos o sectores de arranque.	Requiere que el usuario lo ejecute creyendo que es un software útil.	Puede estar adjunto o ejecutarse tras descarga/instalacion.
VELOCIDAD DE PROPAGACION	Muy rapida, puede infectar miles de equipos en minutos vía red.	Mas lenta, depende de la interaccion del usuario(abrir archivos, por ejemplo).	Lenta, porque depende del engaño al usuario.	Variable: rápida una vez dentro, al cifrar archivos.
DAÑO PRINCIPAL	Saturacion de red, consumo de recursos, puede abrir puertas a otros ataques.	Corrupcion de archivos, lentitud de sistema.	Robo de informacion, instalacion de malware.	Secuestro de archivos mediante cifrado y extorsion economica.
EJEMPLO FAMOSO	ILOVEYOU, Conficker, WannaCry(gusano + ransomware)	CIH(Chernobyl), Melissa.	Zeus, Trojan-Downloader.	WannaCry.Ryuk.

¿Qué fue Stuxnet?

Stuxnet fue un gusano informático diseñado para atacar instalaciones nucleares iraníes. Se lo considera uno de los primeros ejemplos de malware industrial especializado; poseía la capacidad de explotar vulnerabilidades en sistemas de control industrial. El gusano vulneró el software que controlaba las centrifugadoras tomando el control de más de mil máquinas que participaban en la producción de uranio enriquecido.



Origen y Autores Probables

El origen de Stuxnet ha sido objeto de múltiples investigaciones y debates desde su descubrimiento en 2010. Aunque ningún país ha reconocido oficialmente su autoría, la mayoría de los expertos en ciberseguridad coinciden en que fue desarrollado de manera conjunta por Estados Unidos e Israel dentro de una operación secreta conocida como *Operación Juegos Olímpicos* (Operation Olympic Games). El objetivo de este proyecto habría sido retrasar el avance del programa nuclear iraní sin recurrir a un ataque militar convencional, lo cual evitaba un posible conflicto bélico abierto en Medio Oriente (Kaspersky, 2020).

Diversas pruebas técnicas y políticas respaldan esta hipótesis. Por un lado, Stuxnet estaba diseñado específicamente para atacar centrífugadoras Siemens utilizadas en la planta nuclear de Natanz, en Irán, lo que muestra que no se trataba de un malware común, sino de una herramienta creada con un propósito militar y político muy concreto. Además, el nivel de sofisticación del virus era inusualmente alto: explotaba múltiples vulnerabilidades de día cero al mismo tiempo, utilizaba certificados digitales robados y se enfocaba en sistemas industriales muy específicos. El costo y la complejidad de su desarrollo hacen pensar que solo un Estado con grandes recursos podía haberlo financiado (Falliere, Murchu & Chien, 2011).



Años después, filtraciones de información y reportajes de investigación reforzaron estas sospechas. En 2012, *The New York Times* publicó que, según fuentes anónimas del propio gobierno estadounidense, el programa había comenzado bajo la administración de George W. Bush y continuado durante la presidencia de Barack Obama (Sanger, 2012). Incluso, documentos filtrados por Edward Snowden en 2013

apuntaron a la participación de agencias como la NSA y la CIA en conjunto con el servicio de inteligencia israelí, el Mossad (Greenwald, 2014).



Si bien nunca se confirmó oficialmente, la mayoría de la comunidad internacional considera a Stuxnet como la primera ciberarma desarrollada por un Estado.

Método de infiltración y propagación de Stuxnet

Los especialistas de la firma de seguridad cibernética Symantec estimaron que Stuxnet probablemente llegó al programa nuclear de Natanz en una o varias memorias USB infectadas. Alguien habría tenido que insertar físicamente el USB a una computadora conectada a la red local y el gusano penetró así en el sistema de la planta (Falliere, Murchu & Chien, 2011).

Con el tiempo, Kaspersky Lab encontró decenas de variaciones del malware en computadoras de Asia, por lo que elaboró la hipótesis sobre que se desarrollaron varios modelos para atacar otras instalaciones (Kaspersky, 2020).

Una de las facetas más intrigantes de Stuxnet fue su capacidad de propagarse a través de redes informáticas que no estaban conectadas a Internet. Esto permitía que el virus se moviera de una computadora a otra en entornos cerrados de red.

En primer lugar, hizo que las centrifugadoras giraran peligrosamente rápido, durante unos 15 minutos, antes de volver a la velocidad normal. Luego, aproximadamente un mes después, desaceleró las centrifugadoras durante unos 50 minutos. Eso se

repitió en distintas ocasiones durante varios meses, provocando daños físicos y comprometiendo su funcionamiento a largo plazo. Mientras eso ocurría, los tableros de control no reportaron fallas, por lo que los técnicos simplemente no sabían del desperfecto hasta que la máquina dejaba de funcionar (Zetter, 2014).

Se estima que el virus causó enormes retrasos en el programa nuclear de Irán, destruyendo aproximadamente un tercio de las centrifugadoras en funcionamiento. Su nivel de complejidad fue tal que utilizó múltiples vulnerabilidades desconocidas en ese momento, lo que en la jerga de la seguridad informática se denomina *zero-day exploits*. (Sanger, 2012).

Qué son las Zero-Day Exploits

Se refiere a un fallo de seguridad que ha sido descubierto recientemente y que aún no ha sido corregido por los desarrolladores. Esto significa que los atacantes pueden explotar esta vulnerabilidad antes de que se desarrolle e implemente un parche para solucionarla. La falta de un parche disponible representa un riesgo significativo, ya que los atacantes pueden aprovecharse de esta vulnerabilidad sin que los usuarios tengan conocimiento de ella (Falliere, Murchu & Chien, 2011).

“Día cero”: Se llama así porque, cuando una vulnerabilidad se descubre por los atacantes antes que por los desarrolladores, éstos han tenido cero días para preparar un parche o defensas. En otras palabras, es un fallo desconocido públicamente y sin corrección disponible en ese momento.

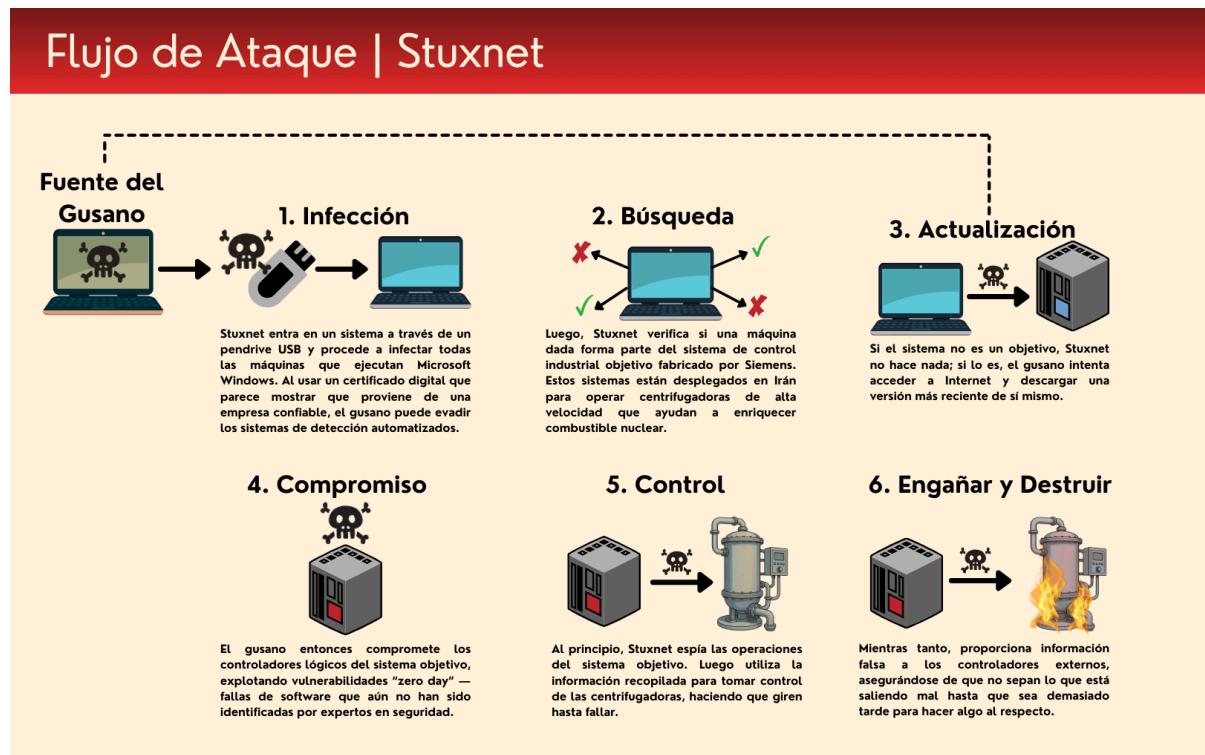
Entre los principales *zero-days* explotados se encontraba **CVE-2010-2568**, una vulnerabilidad en los accesos directos de Windows (.lnk), que permitía ejecutar código malicioso automáticamente al visualizar un ícono en un dispositivo extraíble infectado. Esto fue clave para penetrar en redes aisladas físicamente (*air-gapped*), como la de Natanz, ya que bastaba que un empleado conectara un USB contaminado para activar la infección. Otra vulnerabilidad crítica fue **CVE-2010-2729**, relacionada con el servicio de impresión (*Print Spooler*), que facilitaba la propagación del malware a otras computadoras de la misma red local sin requerir permisos de administrador.

Asimismo, Stuxnet aprovechó dos vulnerabilidades de escalación de privilegios en el kernel de Windows: **CVE-2010-2743**, vinculada al manejo del diseño del teclado, y **CVE-2010-2744**, relacionada con la creación de ventanas en *Win32k.sys*. Ambas permitieron al malware obtener control total del sistema operativo, ejecutando código con permisos de sistema y dificultando la detección por parte de los administradores (Symantec, 2011; Zetter, 2014).

En conjunto, estas vulnerabilidades demostraron cómo un ataque cibernético bien planificado podía comprometer entornos industriales de alto nivel, redefiniendo las prioridades globales en materia de defensa digital. Desde entonces, los gobiernos y

empresas comenzaron a invertir en la detección temprana de *zero-days*, en la segmentación de redes críticas y en el fortalecimiento de las políticas de ciberseguridad a escala mundial.

Flujo de ataque de Stuxnet



Una nueva forma de Guerra

Desde el ataque de Stuxnet, los gobiernos y corporaciones incrementaron la inversión en defensa cibernética y capacidades ofensivas, formando alianzas entre sector público y privado. Posteriormente, ataques como WannaCry y NotPetya evidenciaron que la evolución del malware no se detuvo con Stuxnet, convirtiendo la ciberseguridad en un campo en constante cambio (CiberInseguro, 2022).

El caso de Stuxnet dejó en claro que las guerras modernas no solo se libran con armas tradicionales, sino también en el terreno digital. Este malware marcó un antes y un después porque demostró que era posible dañar infraestructuras críticas de forma remota y sin intervención directa en el terreno.

Stuxnet salió de Irán

La forma en que Stuxnet salió de Irán fue mediante computadoras de contratistas, memorias USB y redes de empresas multinacionales. Se detectaron infecciones en diferentes países:

India e Indonesia: grandes focos de infección, miles de equipos contaminados.

Estados Unidos: Llegó a empresas industriales y organismos gubernamentales, aunque no causó sabotajes.

Pakistan: Otro de los países con fuerte presencia de Stuxnet.

Europa(Alemania, Reino Unido, Francia): Algunos equipos industriales con Siemens también se infectaron.

En total, según Symantec, alrededor del 60% de las infecciones se dieron en Irán, y el 40% se distribuyó en el resto del mundo.

Como Stuxnet fue detenido en Israel

Ingenieros iraníes, con ayuda de Siemens y expertos internacionales, desarrollaron procesos de limpieza de los sistemas infectados. Se aplicaron parches de seguridad en Windows y actualizaciones en el software de control.Siemens lanzó herramientas de eliminación con utilidad para detectar y remover Stuxnet de los controladores Step7.Gracias a esto en febrero de 2012 Irán había logrado neutralizar y purgar Stuxnet de su maquinaria nuclear. Como consecuencia, Irán invirtió fuertemente en el desarrollo de capacidades de ciberdefensa y ciberataque, lo que lo convirtió en un actor importante en el ciberespacio.

Como Stuxnet fue detenido en otros países :

Estados Unidos y Europa

Stuxnet también apareció en empresas y organismos, pero no causó sabotajes porque no encontró los sistemas industriales específicos que buscaba. En estas regiones, el virus fue eliminado principalmente mediante las actualizaciones de seguridad que publicó Microsoft para cerrar las vulnerabilidades zero-day, y gracias a las herramientas de detección y limpieza desarrolladas por Siemens y empresas de ciberseguridad como Symantec y Kaspersky. Así, fue tratado como un malware avanzado, pero sin consecuencias físicas.

India, Indonesia y Pakistán

Se registró un alto número de computadoras infectadas, convirtiéndose en los países más afectados después de Irán. Sin embargo, al igual que en otros lugares,

no sufrieron daños materiales porque no contaban con la infraestructura nuclear objetivo del ataque. Allí, la eliminación del gusano se realizó principalmente mediante antivirus, actualizaciones de Windows y recomendaciones técnicas de Siemens para clientes industriales.

Alemania y Reino Unido

Se detectaron infecciones en empresas con software Siemens, lo que generó gran preocupación. No obstante, al no cumplirse las condiciones específicas para activar la carga destructiva, los sistemas no sufrieron daños. Las autoridades y compañías respondieron aplicando parches, reforzando la seguridad en el uso de dispositivos externos y utilizando las herramientas de Siemens para limpiar los sistemas afectados.

Conclusión

El caso Stuxnet demostró que los ataques digitales podían trascender el mundo virtual y generar daños físicos, dando así evidencia que ningún sistema está completamente seguro. Además, los Estados invierten recursos significativos en ciberarmas, y la protección de infraestructuras críticas y protocolos de seguridad más robustos se volvió fundamental (Vanity Fair, 2011).

Referencias

- CiberInseguro. (2022). *Stuxnet: el malware que cambió la historia.* <https://ciberinseguro.com/stuxnet-el-malware-que-cambio-la-historia/>
- Falliere, N., Murchu, L. O., & Chien, E. (2011). *W32.Stuxnet Dossier.* Symantec Security Response. <https://docs.broadcom.com/doc/security-response-w32-stuxnet-dossier-11-en>
- Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State.* Metropolitan Books.
- Kaspersky. (2020). *What is Stuxnet?* Kaspersky Resource Center. <https://www.kaspersky.com/resource-center/definitions/what-is-stuxnet>
- Lee, R. M., Assante, M. J., & Conway, T. (2016). *ICS Cybersecurity: Case Study – Analysis of the Cyber Attack on the Ukrainian Power Grid.* SANS Institute.
- Rid, T. (2013). *Cyber war will not take place.* Oxford University Press.

- Sanger, D. E. (2012, June 1). Obama order sped up wave of cyberattacks against Iran. *The New York Times*.
<https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html>
- Vanity Fair. (2011, March). *Stuxnet: The Malware That Made History*.
<https://www.vanityfair.com/news/2011/03/stuxnet-201104>
- Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Crown Publishing Group.
- BBC News Mundo. (2015, octubre 7). *Stuxnet: el virus informático que cambió la historia de la ciberguerra*.
https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet
- Weston, J. (2017). *Stuxnet: The Original Cyber Weapon*.
<https://www.linkedin.com/pulse/stuxnet-original-cyber-weapon-james-weston/>

