FireEye

Malware y su impacto en el mundo digital

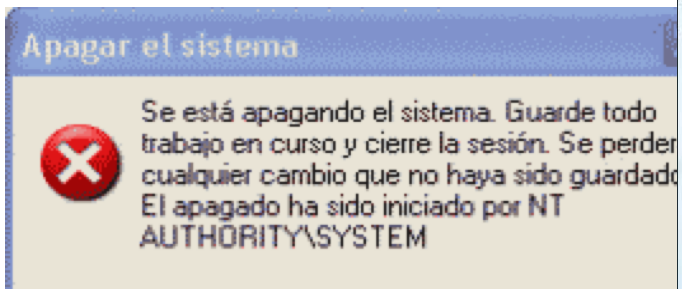
Alberto Rodríguez - Senior Security Engineer
México

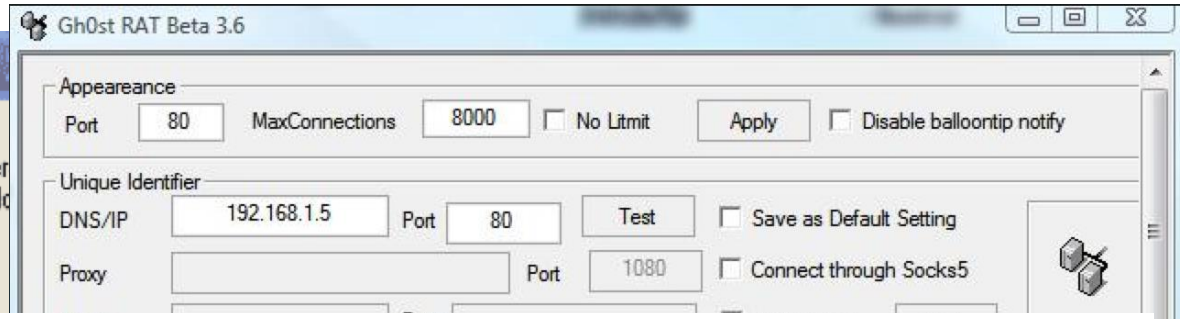
¿Qué significa Malware?

- Software que tiene como propósito explícito infiltrarse o dañar a la computadora.
- Proviene del término en inglés *malicious software*, y en español es conocido con el nombre de **software malicioso**.

FireEye

Malware Convencional vs. Moderno

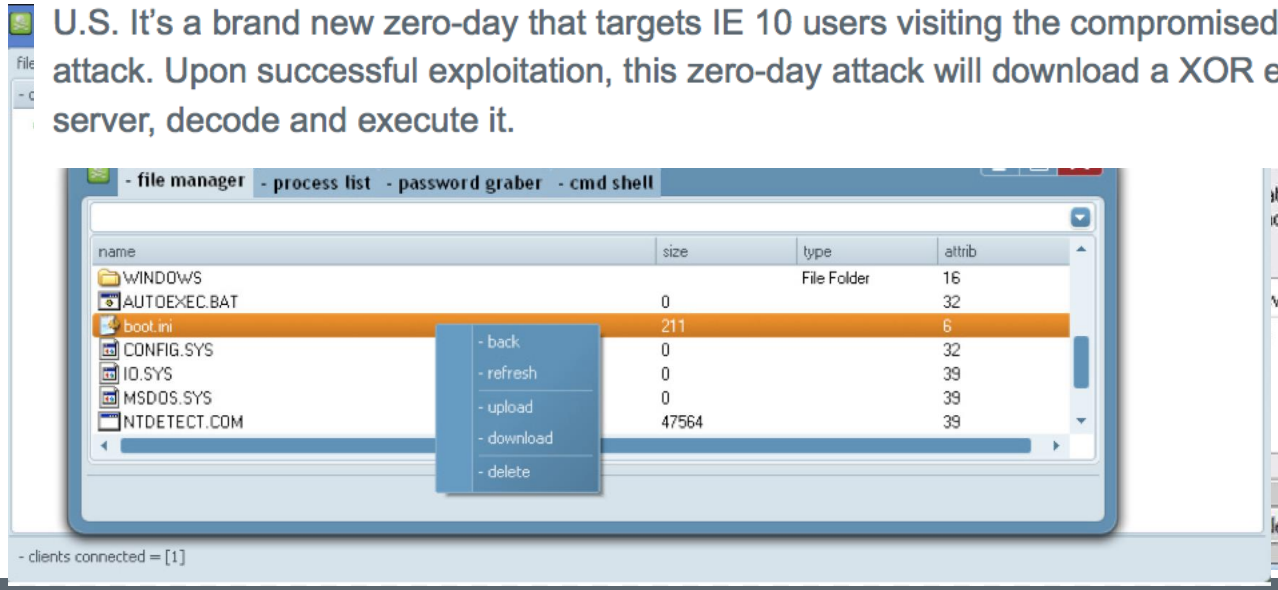




New IE Zero-Day Found in Watering Hole Attack

February 13, 2014 | By Yichong Lin | Exploits, Vulnerabilities | Comments 0

FireEye Labs has identified a new Internet Explorer (IE) zero-day exploit hosted on a breached website based in the U.S. It's a brand new zero-day that targets IE 10 users visiting the compromised website–a classic drive-by download attack. Upon successful exploitation, this zero-day attack will download a XOR encoded payload from a remote server, decode and execute it.



Algunos ataques cibernéticos

EL PERSONAJE DEL AÑO
Edición 1131
SUSCRÍBETE

CNN EXPANSIÓN

Registrate o Ingresa a través de:

Suscríbete al Newsletter

Ingresa tu búsqueda aquí | Buscar

Lunes 13 de enero de 2014 16:43:28 | México DF

Inicio | Empresas | Economía | Mercados | Finanzas Personales | Emprendedores | Carrera | Tecnología | Videos | Life & Style | Especiales | Rankings | Actualidad

Virus ataca cajeros bancarios en México

El 'malware' denominado Ploutus permite controlar el sistema para extraer dinero ilegalmente; el virus se instala físicamente en el cajero mediante un CD- Rom y se activa 24 horas después.

Por: Gabriela Chávez | Martes, 15 de octubre de 2013 a las 13:43

Like 437 | Twittear 345 | +1 28 | Compartir 782 | Email | + - Texto

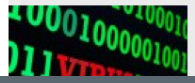
La Comisión Nacional Bancaria y de Valores recomendó utilizar de preferencia los cajeros al interior de las sucursales. (Foto: Archivo)

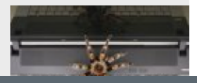
CNNExpansión — Clonar las tarjetas en puntos de venta o robar datos en línea para cometer fraudes cibernéticos ya no son las únicas herramientas de los ciberdelincuentes, firmas de seguridad digital detectaron que bandas utilizan métodos físicos para insertar virus en cajeros automáticos (ATM) para extraer dinero de forma ilegal.

Se trata del *software* pernicioso (*malware*) denominado Ploutus, cuya aplicación requiere cierto ingenio informático y capacidad física, descubierto en México el 13 de septiembre por la firma de seguridad Symantec.

El método de operación de Ploutus consiste en introducir un disco portátil (CD-Rom) con el virus al ATM. El *malware* se activará en unas 24 horas a partir de su inserción. Con ello, y de manera remota, los cibercriminales controlaran funciones como el dispensador de dinero y los menús: todo esto sin que se afecte el aspecto de la pantalla, de acuerdo con información de Symantec y de otras firmas de seguridad informática como Kaspersky Lab.

Artículos relacionados





Conoce al PERSONAJE DEL AÑO 2013

Lo más visto

Las más vistas | Comentadas | Enviadas

- La PGR tomará el control de tu celular
- Telefónica y Nextel se alían en México
- Pantene y P&G 'matan' campaña con Lucero

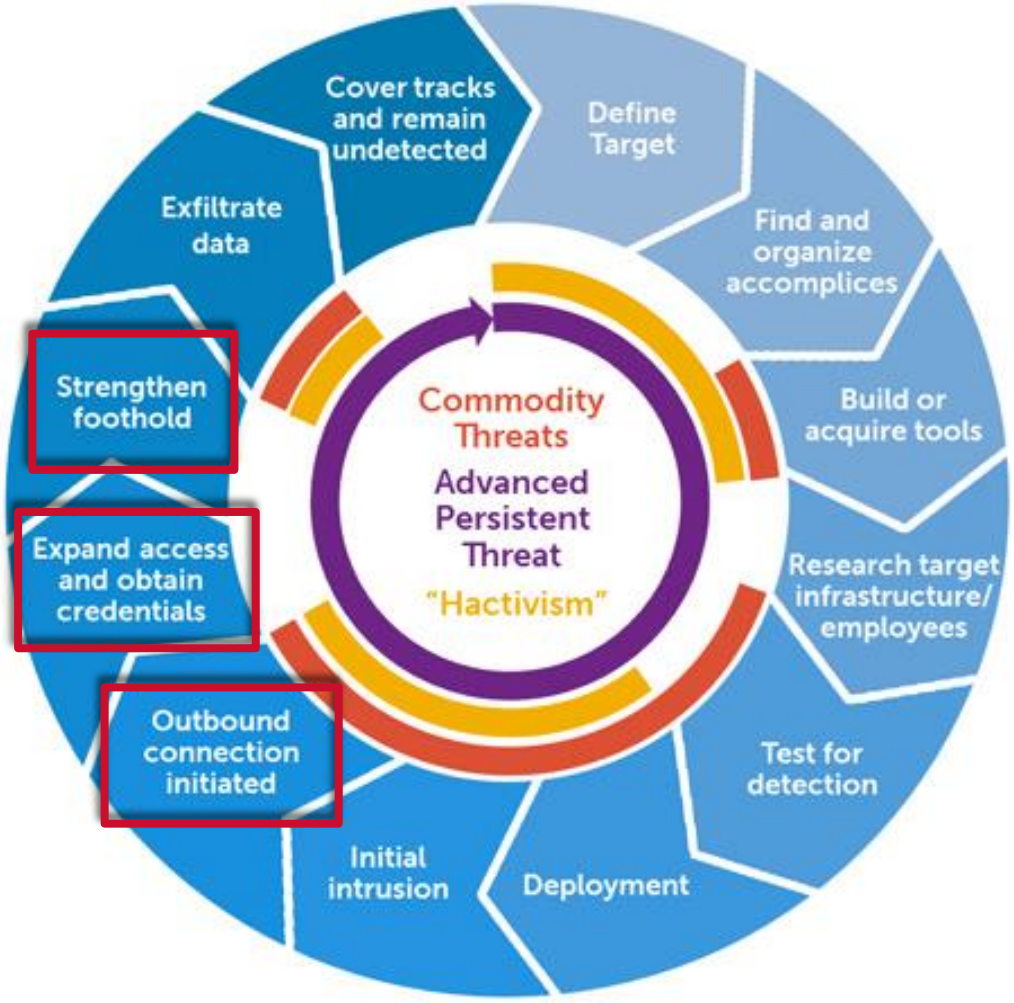
¿Qué es un APT?

FireEye

Video

Malware como parte de un APT

- Principales características - APT:
  - Objetivo específico
  - Inteligencia detrás del ataque
  - Sofisticados
  - Larga duración
  - Silenciosos. A veces incluso no son detectados hasta muy tarde
  - Apuntan por lo general al eslabón más débil: el usuario



FireEye

Ciclo de Vida del Ataque

Múltiples Etapas

Topic: Security Discover Follow via:

Yahoo update: Malware attacks more widespread that first thought

Summary: *[UPDATED] Initial reports that only European sites were affected were incorrect; a small number of users outside were also served Bitcoin mining malware from Yahoo ads.*

By Larry Seltzer for Zero Day | January 12, 2014 -- 13:28 GMT (05:28 PST)

Follow @lseltzer

A week ago reports emerged that Yahoo's ad network was serving malware. Those initial reports said that only European sites were affected between December 31 and January 3. After further investigation, Yahoo now says the period of attack was from December 27, 2013 - January 3, 2014, and that a small number of users outside of Europe may have been affected.

Yahoo adds that the vector for the attack was a compromised account. They have shut down that account and are working with law enforcement to investigate the breach.

ZDNet Follow @zdnet Like 188k Join | Log In | Privacy | Cookies

Related Stories

Yahoo ad malware spawned European Bitcoin mining network

Yahoo users drop email scanning allegations

Yahoo serves malicious ads

FireEye

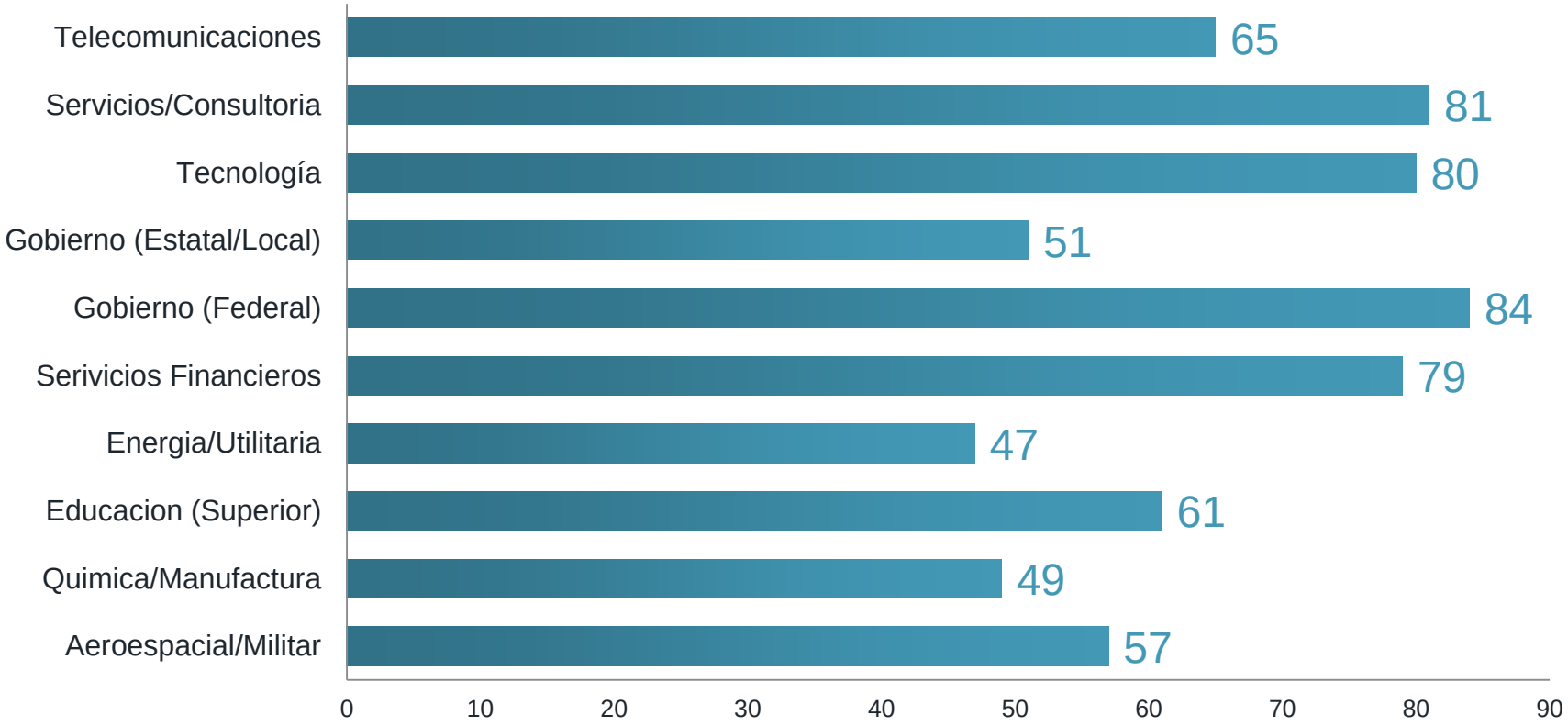
Ejemplo de infección vía Web - México

Top 10 objetivos 2013

1. **Educación**: investigaciones valiosas, redes no muy controladas
2. **Servicios Financieros**: personas, negocios, gobiernos
3. **Tecnología**: retorno de inversión exponencial
4. **Gobierno**: política, leyes, seguridad nacional
5. **Servicios/Consultoría**: cadenas de suministro, contratistas
6. **Energía/Utilitarios:** infraestructura crítica, armamento militar
7. **Manufactura/Químicos:** industria química, ciencias aplicadas
8. **Telecomunicaciones:** Internet, telefonía, tv
9. **Salud/Farmaceúticas:** medicinas, atención médica
10. **Aerospacial/Defensa/Aerolineas:** comercial y militar

FireEye

Número de familias de APT por vertical



- Top verticales basadas el número de APT dirigidos por familia detectados en 2013
- La vertical del Gobierno Federal se posiciona en primer lugar con 84 muestras únicas

FireEye

El alto costo de no estar preparados

63%

De las empresas supieron que estaban comprometidas a través de una entidad externa

100%

De las víctimas mantenian actualizadas las firmas de su Anti-Virus

Source: Mandiant M-Trends 2013

FireEye

Soluciones antes, durante y despues de una brecha

	Estoy preparado	Estoy comprometido	He sido vulnerado
Productos	FireEye **Plataforma de protección de amenazas** Network | Email | Mobile | Endpoint | Content		
Servicios	• Asesoria en preparación a incidentes • Defensas administradas	• Análisis de vulnerabilidades y amenazas avanzádas • Monitoreo continuo	• Servicios de respuesta a incidentes

FireEye

FireEye™

Security Reimagined

Gracias