TIC Gobierno

Amenazas contra la información confidencial.

Impacto en los servicios a la ciudadanía.

Omar Alcalá


DELL


Pagamático
SAPAL


Módulo 19

Modelo de seguridad actual

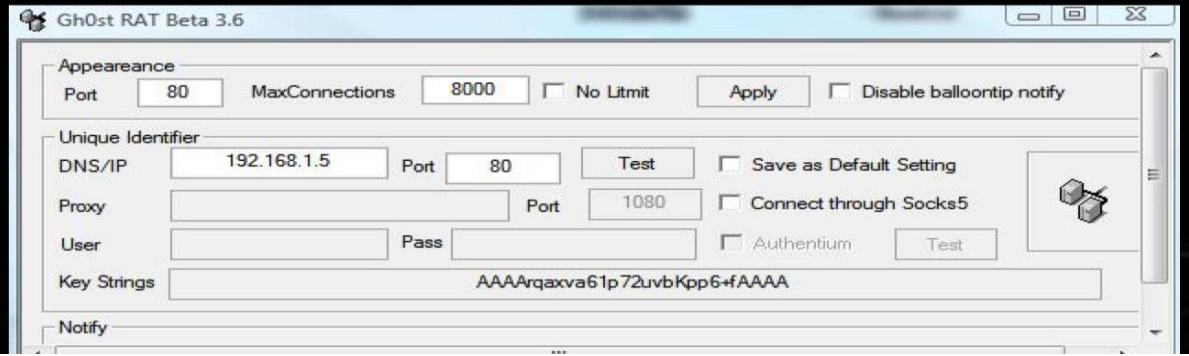
Modelo de detección basado en patrones (firmas)

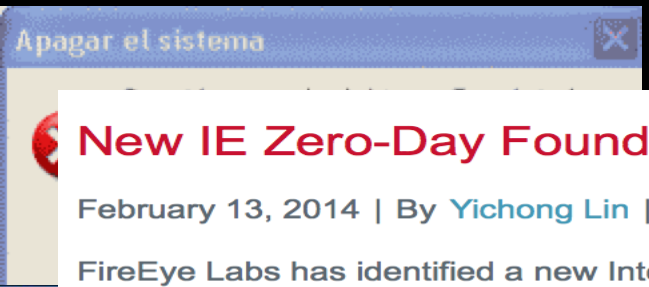
Altos índices de falsos positivos

Ataques conocidos solamente

$16MM+

USD, POR AÑO

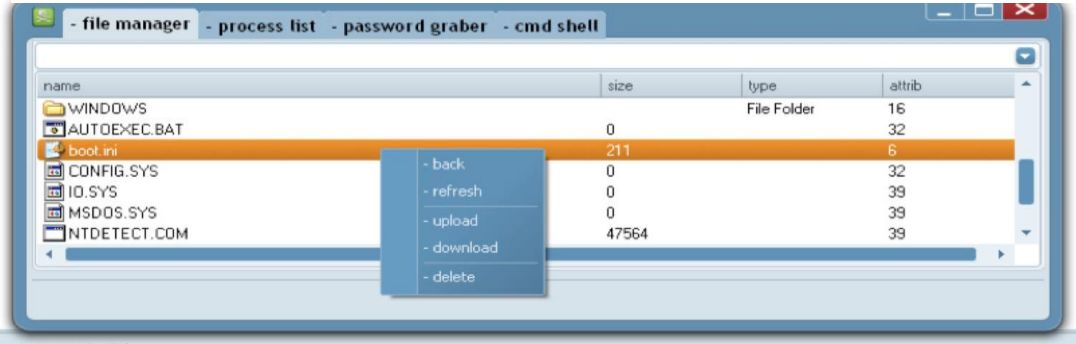


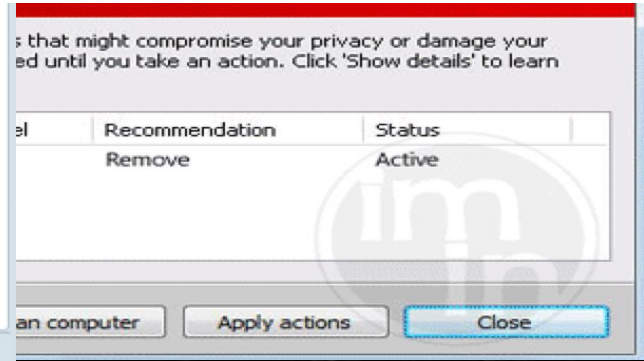


New IE Zero-Day Found in Watering Hole Attack

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.





Un día cualquiera…

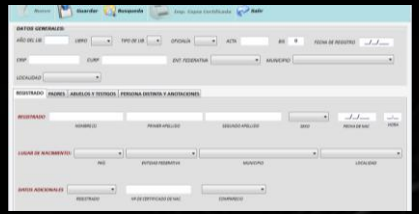
Pepe
Atención al cliente

Responsabilidad:
Captura de información personal para trámites de tesorería

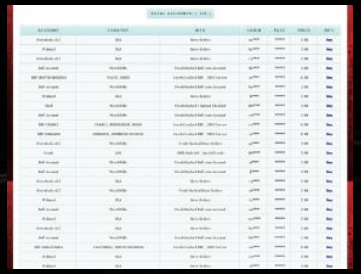
Intereses:
Fútbol, viajes, maratones

8:00am
Revisa email con noticias

9:00am
Trabajo normal



10:00am
Captura datos de contribuyentes nuevos



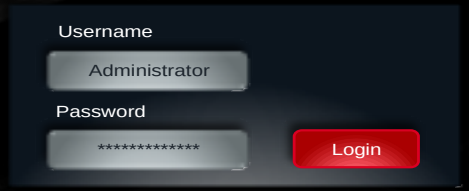
Fuga de información

Juan
Hacker malicioso

Objetivo:
Obtener información

Intereses:
Tecnología, Hacking, ¿cómo hacer bypass a la seguridad?

W W W



La vulnerabilidad es humana

1. **Los atacantes van hacia las personas**

   Aplicaciones clientes (troyanos)

   Ingeniería social

2. **El rango de operación es muy amplio**

¿Qué es un APT?


Objetivo
Investigación
Herramientas
Pruebas
Despliegue


Intrusión
Control inicial
Expansión
Fuga de información
Mantener control
Evasión (no detección)

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.

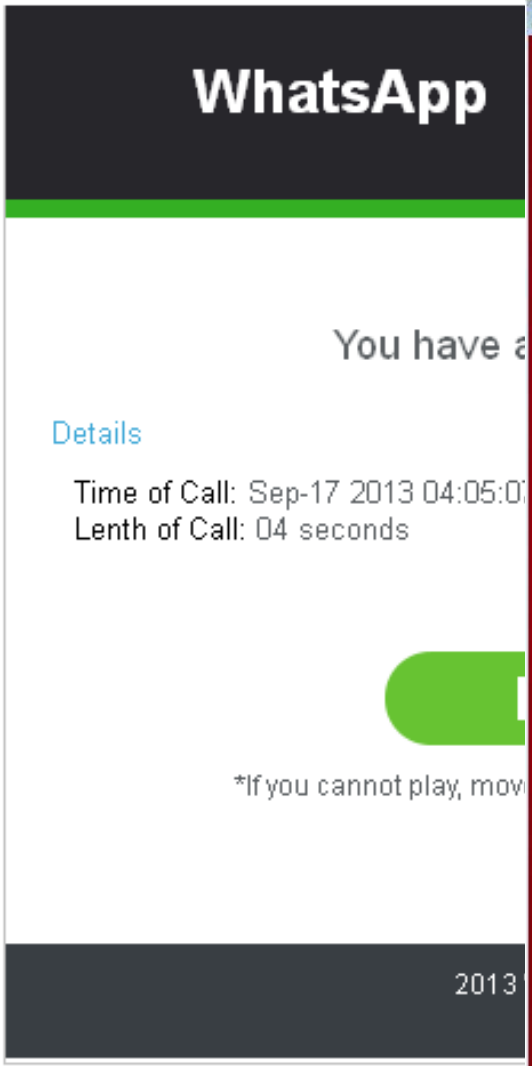
Yahoo adds that the vector for the attack was a compromised account. They have shut down that account and are working with law enforcement to investigate the breach.

Related Stories

Yahoo ad malware spawned European Bitcoin mining network

Yahoo users drop email scanning allegations

Yahoo serves malicious ads



CryptoLocker

Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt the files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD** / **300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
10/20/2013
12:37 PM

Time left
72 : 34 : 50

Next >>

---------- Mensaje reenviado ----------
De: [redacted]
Fecha: 18 de octubre de 2013 02:31
Asunto: No quiero lastimarte pero es peor que te sigan mintiendo
Para: [redacted]

Hola te mande este email hace 4 dias y no me respondes igual quiero que sepas esto por favor no te enojes

me tomo el atrevimiento de enviarte este email, porque no quiero decirtelo personalmente, pero me siento con l porque te aprecio mucho

necesitas abrir los ojos te estan siendo infiel, se que es dificil que me creas pero como las imagenes valen mas q fotos para que veas con tus propios ojos

no quiero lastimarte pero peor es que te sigan mintiendo

Estas son las imagenes: Foto1 Foto2 Foto3

Case #2877310911 From: "Better Business Bureau" <LorraineLaw@bbb.org>
Subject: Case #2877310911
From: "Better Business Bureau" <LorraineLaw@bbb.org>
To: [redacted]
Date: 2012-12-10 06:04:17

Owner/Manager

The Better Business Bureau has received the above-referenced complaint from
regarding their dealings with you. The details of the consumer's concern are incl
review this matter and advise us of your position.

As a neutral third party, the Better Business Bureau can help to resolve the matt
result of misunderstandings a company wants to know about and correct.

In the interest of time and good customer relations, please provide the BBB wit
position in this matter **by December 11, 2012**. Your prompt response will allo
you and your customer in reaching a mutually agreeable resolution. Please infor
your customer directly and already resolved this matter.

The Better Business Bureau develops and maintains Reliability Reports on com
States and Canada . This information is available to the public and is frequently
Your cooperation in responding to this complaint becomes a permanent part of
Business Bureau. **Failure to promptly give attention to this matter may be**
give to consumers about your company.

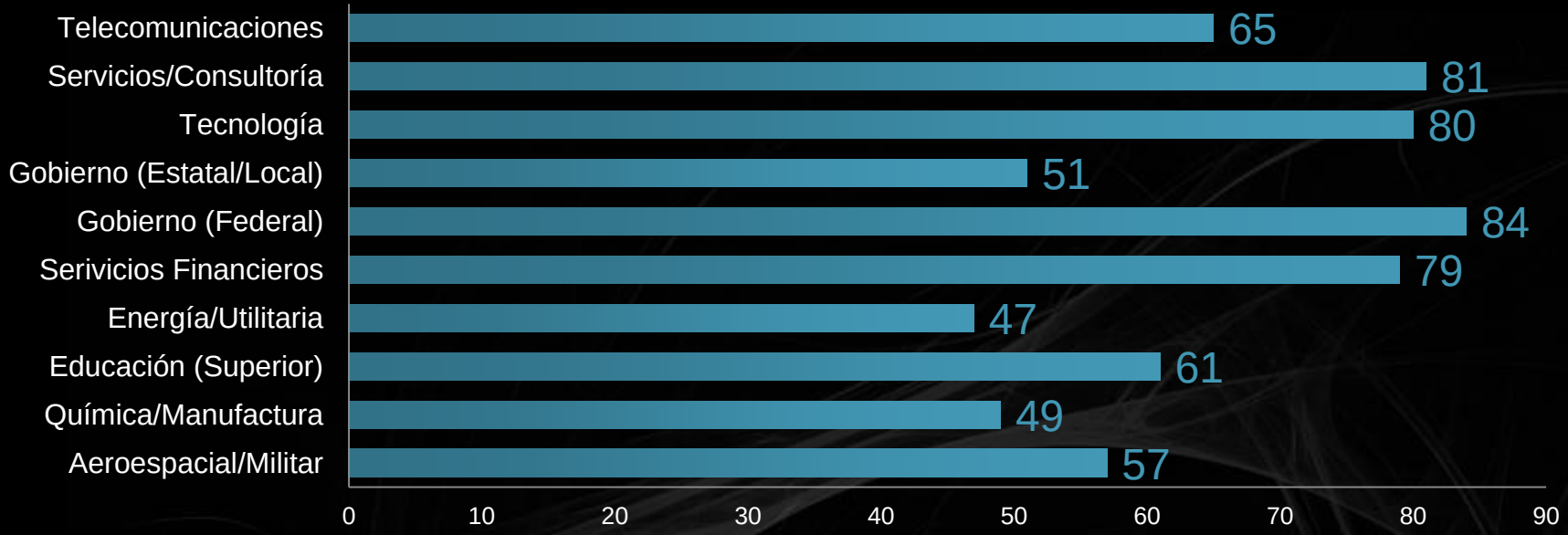
We encourage you to print this complaint (attached file), answer the ques

We look forward to your prompt attention to this matter.

Sincerely,

The Better Business Bureau Complaint Department

Número de familias de APT por vertical (2013)



- Se perciben ataques en todos los niveles.
- Gobierno federal (a nivel mundial) es más atacado que el local.

¿Qué hacer? (tecnológicamente hablando)

1. Defensas convencionales (FW, IPS, AV, etc) +

2. Nueva generación de defensas (sin firmas, contra amenazas nuevas y día cero, con detección y contención en minutos)

3. Concientizar al usuario

4. Buena suerte con el punto 3

5. Establecer una estrategia clara de seguridad

Las amenazas y las brechas siempre existirán

Lo importante es estar consciente y actuar rápidamente

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

Un nuevo día…

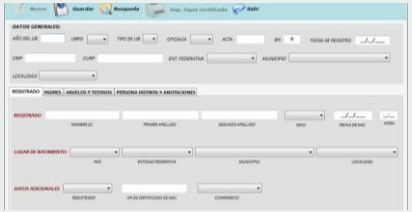
Pepe
Atención al cliente

Responsabilidad:
Captura de información personal para trámites de tesorería

Intereses:
Fútbol, viajes, maratones

8:00am
Revisa email con noticias

9:00am
SOC / Remediación



10:00am
Captura datos de contribuyentes nuevos

Protección Antimalware (EX / NX)

¡Registros a salvo!

Juan
Hacker malicioso

Objetivo:
Obtener información

Intereses:
Tecnología, Hacking, ¿cómo hacer bypass a la seguridad?

W W W

Buscando…

If you "follow the money" when you invest, you're too late to the game. You need to research and determine where the money will be going.

CVE-2013-3918 CVE-2014-0266

Si “seguimos las amenazas conocidas” al protegernos, estamos ya muy tarde en el “juego” de la seguridad

TIC Gobierno

¡Gracias!