IX JORNADAS STIC CCN-CERT

DETECCIÓN E INTERCAMBIO, FACTORES CLAVE

Madrid, 10 y 11 de diciembre 2015

APTs DESTACADOS

CCN Centro Criptológico Nacional

- Luis
- CCN-CERT
- ccn-cert@cni.es

Índice

1 Introducción

1. Introducción

Principales actores

- Los actores principales en el robo de información en España durante el 2015 son:
  - APT28
  - Snake
  - APT29
  - Emissary Panda

2 Caso de estudio 1

Owning a website like a boss

2. Caso de estudio 1

Owning a website like a boss

- En las pasadas Jornadas STIC…
  - Compromiso continuo de la web principal de una empresa
    - Septiembre 2013
    - Diciembre 2013
    - Febrero 2014
    - Septiembre 2014
    - Febrero 2015
    - …
  - Los responsables sobrescribían la web con un backup antiguo

2. Caso de estudio 1

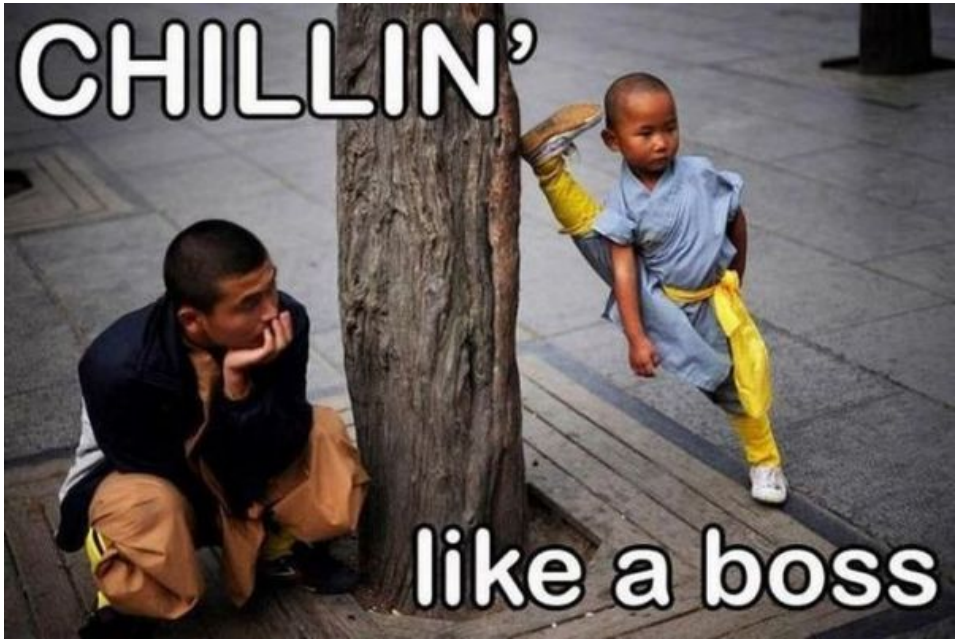
Owning a website like a boss

- En las pasadas Jornadas STIC…
  - Uso de técnica de *watering hole*

2. Caso de estudio 1

Owning a website like a boss

- Después de todo este tiempo el atacante cogió confianza …



2. Caso de estudio 1

Owning a website like a boss

… y clonó el portal de acceso de VPN de otra empresa en este website para el robo de credenciales

3 Caso de estudio 2

The Shaolin style

3. Caso de estudio 2

The Shaolin style

- Ciberatacantes chinos comprometieron las redes de varias empresas.
- Una vez dentro accedieron al servidor de correo OWA e instalaron una *backdoor*

3. Caso de estudio 2

The Shaolin style

17 de marzo de 2015

- El **17 de marzo de 2015**, el atacante accede a uno de los servidores de correo de YAESTOY en **lenguaje chino**

```
2015-03-17 06:40:18 172.20.2.83 GET
/owa/14.2.298.4/themes/resources/owafont_zh_chs.css - 443 -
192.168.1.140
Mozilla/5.0+(Windows+NT+6.1;+WOW64)+AppleWebKit/537.36+(KHTML,+like+
Gecko)+Chrome/39.0.2171.95+Safari/537.36 200 0 0 15
```

Ese mismo día, se envía el primer correo de *spear phishing* a STAR-AS. El correo incluía un Excel que explotaba la vulnerabilidad CVE-2012-0158.

3. Caso de estudio 2

The Shaolin style

- El **8 de mayo de 2015** STAR-AS recibe varios correos de *spear phishing* desde una cuenta de YAESTOY:

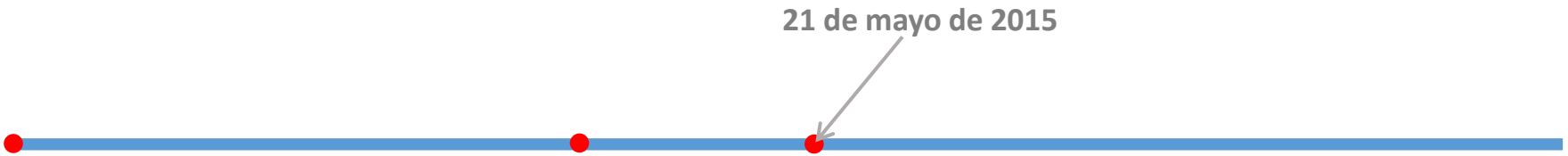
De: Martinez Gutierrez, Raul [mailto:Raul.Martinez@yaestoy.es]
Enviado el: viernes, 08 de mayo de 2015 16:39
Para: Arranda Federico; Lopez Martinez, Maria; López González, José Antonio; Herrero Garcia, Pablo
Asunto: password has expired

Your password has expired,Please sign in to change the password.

http://reports.pav.cascadeengineering.com/Reports/Pages/UILogon.aspx

3. Caso de estudio 2

The Shaolin style



- Otros correos como éste fueron enviados a otras empresas españolas desde YAESTOY, el **21 de mayo de 2015**.

3. Caso de estudio 2

The Shaolin style

- El atacante tenía instalada una **puerta trasera** en el servidor de correo OWA de YAESTOY, que le permitía realizar las siguientes acciones:
  - Listar las unidades disponibles en el equipo.
  - Listar ficheros y directorios.
  - Obtener el contenido de ficheros.
  - Crear, mover y eliminar ficheros y directorios.
  - Modificar las propiedades de un fichero o directorio.
  - Descargar ficheros de un servidor Web.
  - Crear procesos.
  - Establecer conexiones con bases de datos y llevar a cabo todo tipo de consultas.

3. Caso de estudio 2

The Shaolin style

- La **puerta trasera** consistía en la carga en memoria de **OwaAuth.dll**
  - El fichero tiene el mismo nombre que el original (pero con mayúsculas)

    `OwaAuth.dll` `ee7e8b2463073cc84c75fd219ed9bcde`
  - Está en una ruta parecida a la original:

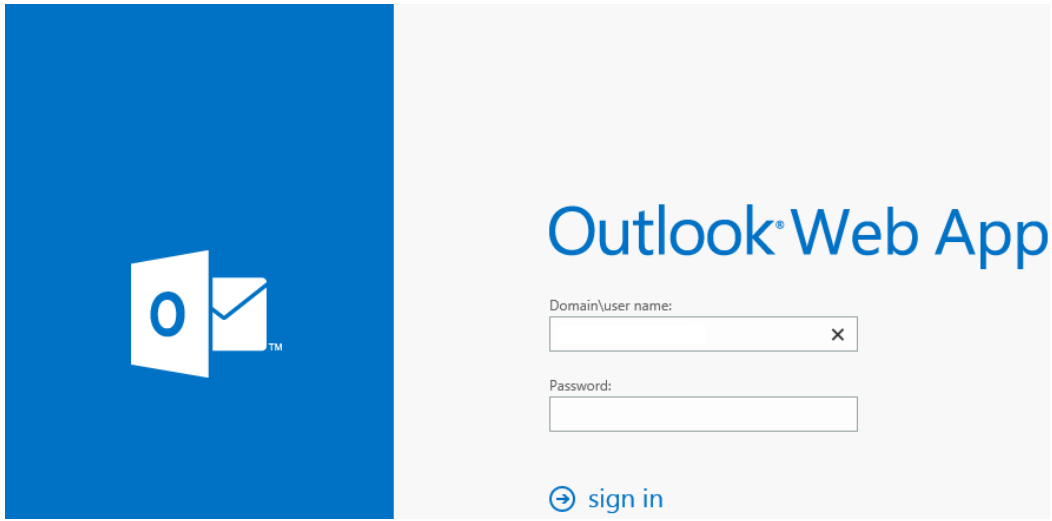
    `E:\Exchange\ClientAccess\Owa\Bin`
    `E:\Exchange\ClientAccess\Owa\auth`
  - Se carga mediante la modificación del fichero **web.config**:

```
<!-- OWA HTTP Modules -->
        <modules>
            <add type="Microsoft.Exchange.Clients.Owa.Core.OwaModule,
Microsoft.Exchange.Clients.Owa" name="OwaModule" />
                <add name="exppw" />
                <add type="Microsoft.Exchange.Clients.OwaAuth" name="OwaAuth"/>
        </modules>
```

3. Caso de estudio 2

The Shaolin style

- El atacante capturó **más de 1400 credenciales** de usuario diferentes de la empresa YAESTOY **desde el 17 de marzo hasta el 29 de mayo de 2015**



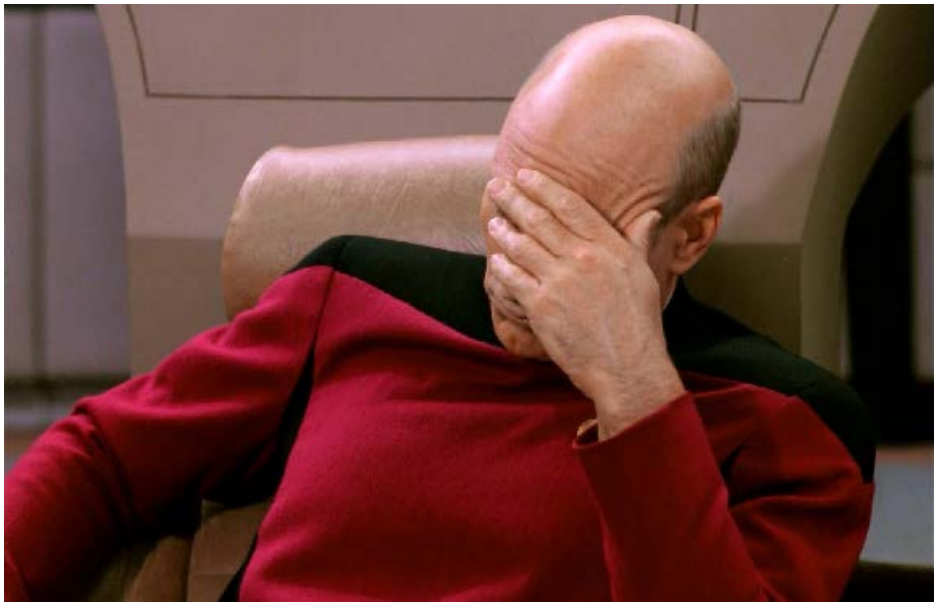
4 Caso de estudio 3

The lemon yogurth

4. Caso de estudio 3

The lemon yogurth

- Grupo muy activo desde, **al menos**, **2008**.



4. Caso de estudio 3

The lemon yogurth

- Grupo muy activo desde, **al menos**, **2008**.
- Les pillamos una vez…

4. Caso de estudio 3

The lemon yogurth

- Grupo muy activo desde, **al menos**, **2008**.
- Les pillamos una vez…
- Volvieron a entrar

4. Caso de estudio 3

The lemon yogurth

- Grupo muy activo desde, **al menos**, **2008**.
- Les pillamos una vez…
- Volvieron a entrar
- Volvimos a pillarlos…

4. Caso de estudio 3

The lemon yogurth

- Grupo muy activo desde, **al menos**, **2008**.
- Les pillamos una vez…
- Volvieron a entrar
- Volvimos a pillarlos…
- Ahora han vuelto para quedarse

4. Caso de estudio 3

The lemon yogurth

- **FASE 1**: reconocimiento
  - Se comprometen **páginas web legítimas** que ocasionalmente visitan posibles víctimas.
  - Se introduce código JavaScript en la página principal que **recopila información** del equipo y la manda a un servidor web remoto.
  - El atacante dispone de **cientos de estas páginas web**.
  - Es **difícil de detectar**.

4. Caso de estudio 3

The lemon yogurth

- **FASE 2**: *spear phishing*
  - Una vez identificadas las víctimas se construyen correos específicos con:
    - Un asunto atractivo para los destinatarios (generalmente sobre un asunto reciente)
    - Se incluye un adjunto que explota una de las vulnerabilidades del equipo obtenidas de la fase 1.

4. Caso de estudio 3

The lemon yogurth

- **FASE 3**: infección de las víctimas
  - Las víctimas son infectadas con el malware TAVDIG
    - Se utilizan varios saltos entre servidores web hackeados.
    - 2 conexiones diarias a los servidores C2.
    - Uso de clave pública para el cifrado de la información.
    - Monitorización periódica por parte de los atacantes.
  - En esta fase el atacante ya puede robar información.

4. Caso de estudio 3

The lemon yogurth

- **FASE 4**: explotación y colonización
  - El atacante infecta a las víctimas con **malware más complejo**.
    - Desde septiembre de 2015 está utilizando una **nueva muestra de malware** totalmente diferente a las utilizadas hasta ahora.
  - Se utilizan herramientas para el robo de credenciales.
  - Se utilizan otros canales para la exfiltración de la información.

5 Conclusiones

5. Conclusiones

- Si has sido objetivo de una APT vas a serlo **siempre**.
- Se debe **aumentar la capacidad de vigilancia.** Equipo de seguridad. Consultoría externa.
- **Intercambio de información**

SE DEBE TRABAJAR COMO SI SE ESTUVIERA COMPROMETIDO

E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sondas@ccn-cert.cni.es
- redsara@ccn-cert.cni.es
- organismo.certificacion@cni.es

Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es

Síguenos en Linked in