Ministerio de
TECNOLOGÍAS
DE LA INFORMACIÓN
Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL Paraguay de la gente

GESTIÓN DE INCIDENTES CIBERNÉTICOS

CLASE 6

Ing. Gabriela Ratti

Disclaimer

Todo el contenido de esta presentación es únicamente con fines didácticos y educativos. El uso indebido de las técnicas y/o conocimientos utilizadas en esta presentación puede ir en contra de las leyes nacionales e internacionales. El autor no se hace responsable por el uso del conocimiento contenido en la siguiente presentación. La información contenida debe ser utilizada únicamente para fines éticos y con la debida autorización.

Análisis de Incidentes de Correos Electrónico

Análisis de Cabecera

Primero se debe obtener el código fuente o cabecera, no se puede iniciar un análisis a partir de un correo re-enviado.

Guía: https://mxtoolbox.com/public/content/emailheaders/

Herramientas de análisis:

- http://www.cyberforensics.in/OnlineEmailTracer/index.aspx
- http://www.iptrackeronline.com/email-header-analysis.php
- MxToolbox:
  - https://mxtoolbox.com/EmailHeaders.aspx
  - https://mxtoolbox.com/Public/FreeInvestigator.aspx
- Whois
- Whois online: http://whois.domaintools.com/

Análisis de enlaces o adjuntos sospechosos

Multiengine scaners online:

Virustotal: https://www.virustotal.com/es/

VirScan: http://virscan.org/

Jotti: https://virusscan.jotti.org/

Sandbox online:

Hybris-Analysis: https://www.hybrid-analysis.com/

Joe Sandbox: https://www.joesandbox.com/

Malwr: https://malwr.com/

Análisis de sitio web online:

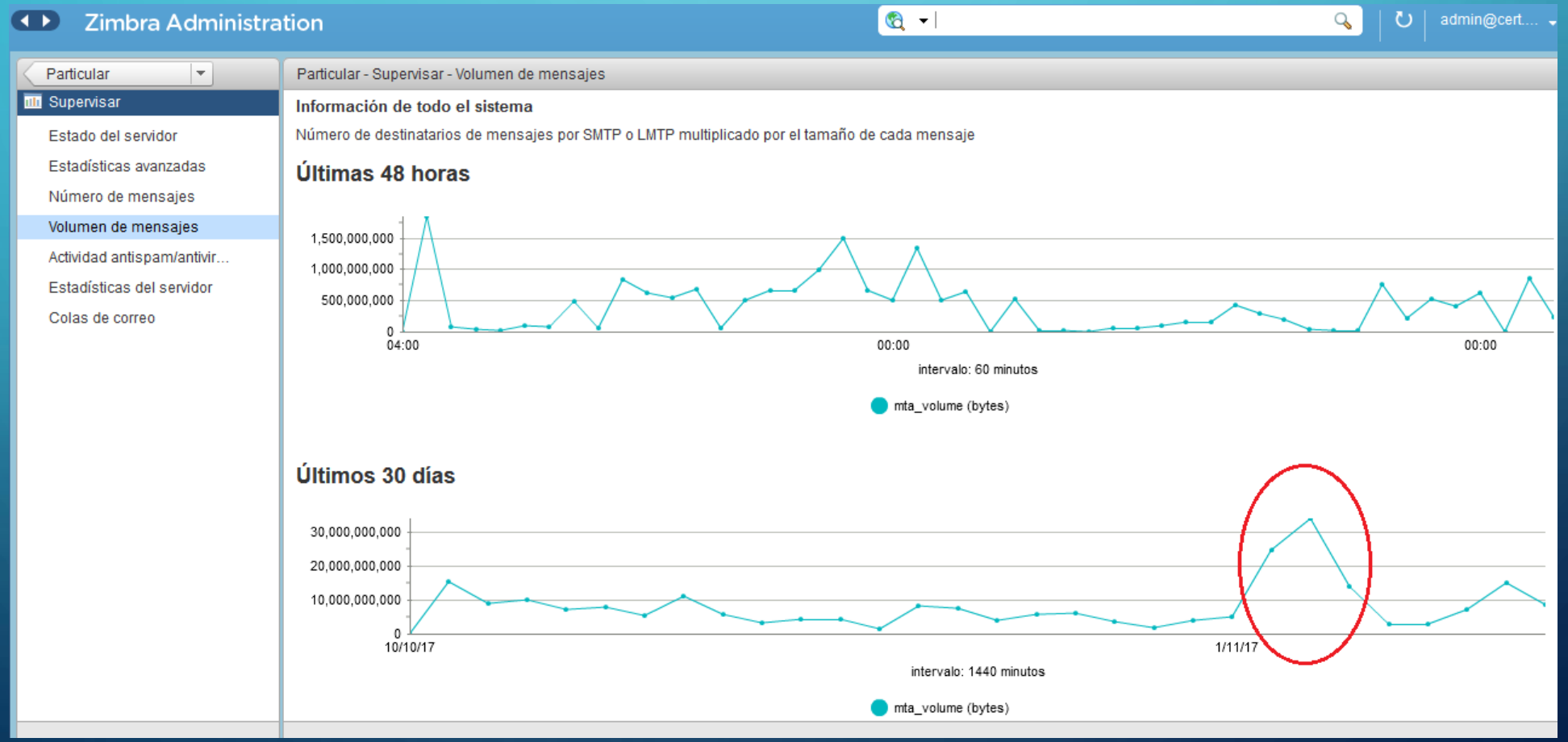
Sucuri: https://sitecheck.sucuri.net/

Quttera: https://www.quttera.com/

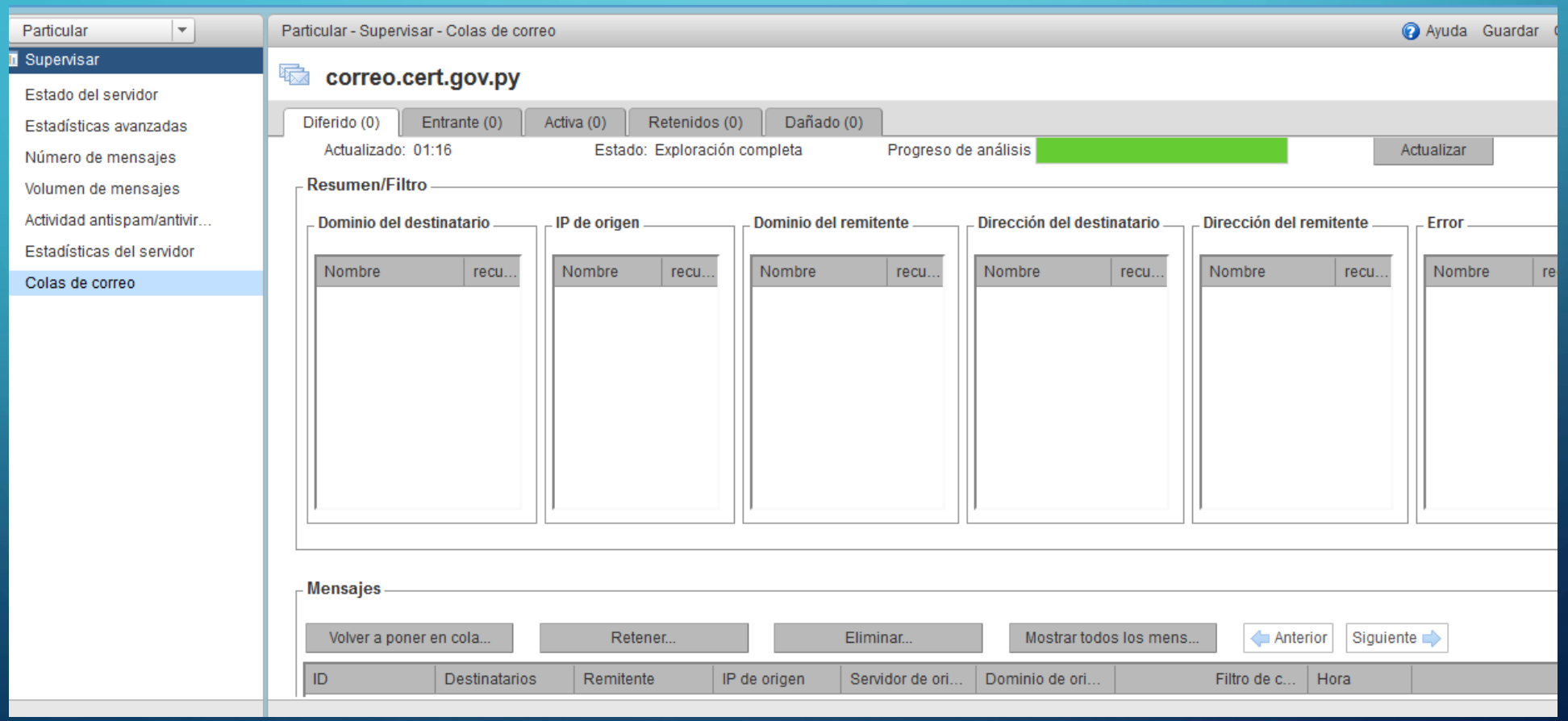
Web Inspecto: https://app.webinspector.com/

Cuentas comprometidas y Spam

Monitorización de actividad de Correo



Monitorización de actividad de Correo (I)



Rastreando la cuenta comprometida

Logs importantes:

/opt/zimbra/log/:

mailbox.log - log genérico, errores

audit.log - autenticación, actividad de administración

access_log.<fecha> - acceso HTTP (webmail)

/var/log/zimbra.log - MTA, estado de sistema;
postfix, amavisd

Rastreando la cuenta comprometida

Usuarios que se han autenticado muchas veces (SMTP Auth):

```
grep sasl_user | sed -n 's/.*sasl_username=//p' | sort | uniq -c |
sort -n
```

```
1 Auser@domain.com
3 Buser@domain.com
4 Cuser@domain.com
5 Duser@domain.com
36 SPAMMER@domain.com
```

IPs desde la que se ha conectado cada usuario:

```
zgrep -i 'authrequest.*name.*ip' /opt/zimbra/log/mailbox.log*|cut
-f3 -d[|cut -f1 -d]|sed 's/;ua.*$//g;s/;mid=[0-9]*//g;'|sort -u
```

Listar todos los envíos realizados por un usuario

```
zgrep 'from=<user@example.com' /var/log/zimbra.log*
```

Listas negras

Es una lista de direcciones IP o dominios que presuntamente envían spam y/o están comprometidas. Los servidores de correo usan las listas negras para decidir si aceptan o rechazan un correo electrónico.

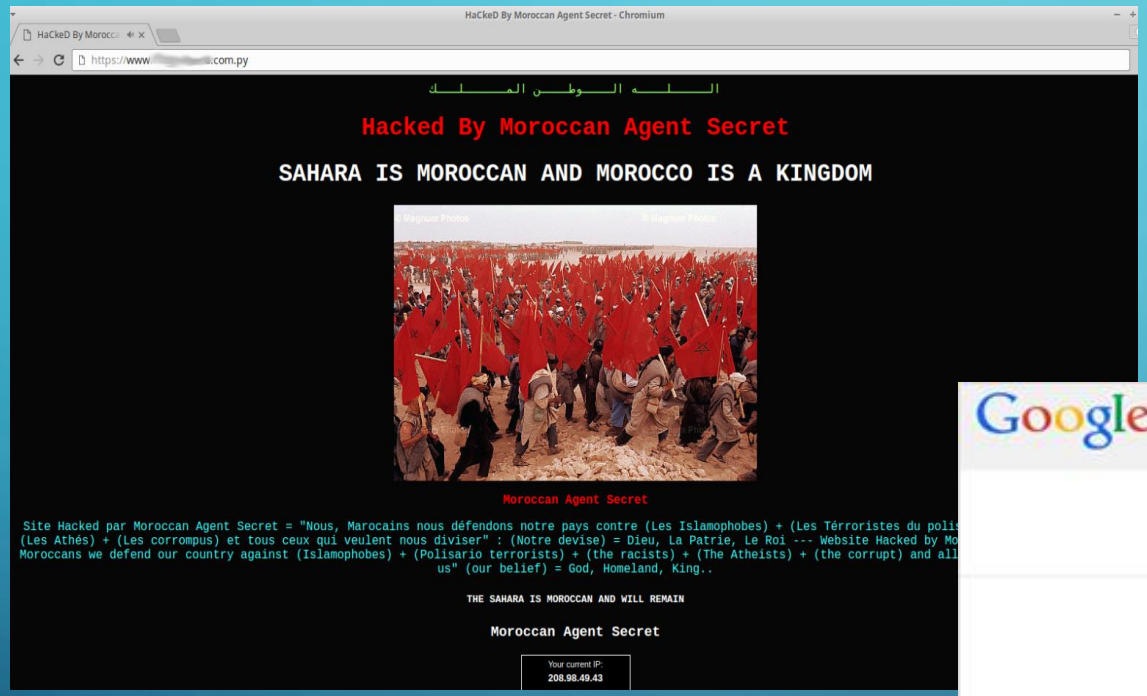
✓ No bloquean IPs, solo las listan!

- MultiRBL Valli: http://multirbl.valli.org/
- Mx Toolbox Blacklists: https://mxtoolbox.com/blacklists.aspx
- UltraTools: https://www.ultratools.com/tools/spamDBLookup
- Project Honeypot: https://www.projecthoneypot.org/
- Mircosoft: https://postmaster.live.com/snds/ (requiere registro previo)

Cómo salir de la lista negra

1. Análisis forense para detectar el origen del problema:
   a. Cuenta comprometida?
   b. Malware en la red o en un servidor?
   c. Servidor web comprometido?
2. Resolución del incidente - eliminar el problema de raíz
3. Asegurar que la actividad maliciosa paró
4. Implementar mejoras para evitar que vuelva a suceder
5. Solicitar la eliminación de la IP de la lista

Indicadores de compromiso de servidor web



Artefactos y técnicas para compromiso de servidor web

- Webshell / backdoor
- Escalación de privilegios
- Rootkit

Errores comunes

- Eliminar el archivo visible
- Backup viejo sin verificar
- Solo actualizar CMS/plugin

Qué es lo correcto?

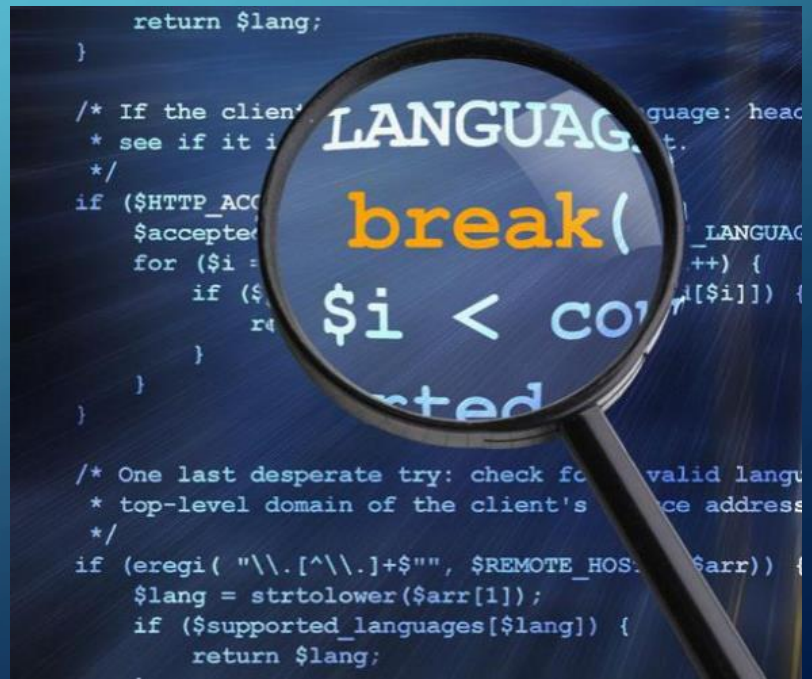
Auditoría!

¿Cómo entraron? ...

Cómo detectarlos?

Posibles indicadores de artefactos maliciosos:

- Nombres de archivos extraños o desconocidos
- Funciones sospechosas
- Patrones atípicos
- Permisos, dueños y grupos
- Fechas de creación y modificación
- Procesos extraños o desconocidos
- Usuarios desconocidos
- Conexiones y puertos extraños o desconocidos



Detectando webshell y artefactos maliciosos

Herramientas y técnicas:

- Findbot: https://www.abuseat.org/findbot.pl
- Shelldetect: http://shelldetector.com/
- Comandos útiles: grep, find, locate, ps, netstat, lsmod
  - Expresiones regulares
- Plugins y herramientas específicas según el CMS:
  - Wordpress: Sucuri scanner, CWIS
  - Joomla: Akeeba Admin Tools, SecurityChek Pro, Antivirus Website Protection
- Análisis de Logs

Análisis de Logs

Dónde buscar?

- **Logs de Apache:** /var/log/httpd o /var/log/apache2
  - access.log - peticiones HTTP
  - error.log - errores
- **Logs de SO:** /var/log/
  - /var/log/auth.log: log de autenticación.
  - /var/log/kern.log: registro del kernel
  - /var/log/cron.log: registro de la herramienta de crond
  - /var/log/maillog: registro del servidor de emails.
  - /var/log/boot.log: registro de inicio del sistema
  - /var/log/secure: log de autenticación, incluye SSH
  - /var/log/utmp o /var/log/wtmp: registro de logins. Ver con *last*
- **Logs de Base de Datos:** /var/log/mysqld.log o /var/log/mysql/

Análisis de Logs (1)

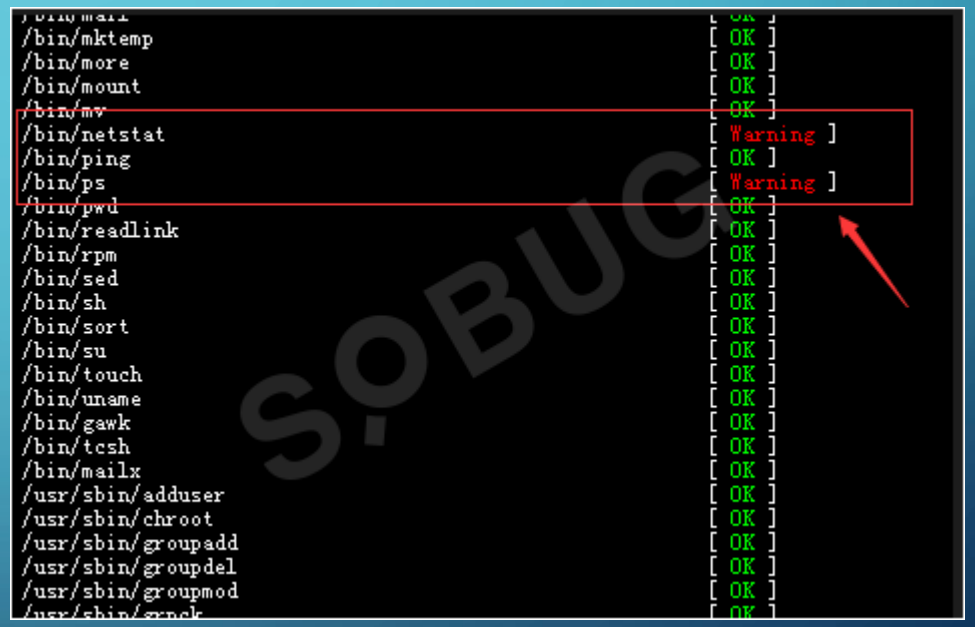
Qué buscar?

- Peticiones POST
- UA extraños
- Exclusión de patrones de peticiones comunes
- Exclusión de IPs confiables

Detectando Rootkits

En servidores Linux:

- ClamAV
- unhide.rb / unhide
- Rkhunter
- Chkrootkit
- Volatility (técnicas avanzadas)



REINSTALACIÓN DE S.O.

Servidor Web comprometido: acciones a seguir

1. Aislar el servidor de Internet
2. Verificar procesos y conexiones activas
3. Buscar webshells, backdoor y código malicioso y remover
4. Verificar y reparar integridad de archivos de aplicación web
   - ➢ *En caso de CMS, resguardar/exportar contenido, reinstalar core e importar contenido limpio.*
5. Buscar y eliminar usuarios no autorizados
6. Buscar rootkits, malware y/o otra modificación al SO
7. Buscar indicadores de escalación de privilegios
   - ➢ *En caso de que el paso 8 y/o 9 son afirmativos, considerar reinstalación de SO*
8. Revisar logs - identificación de punto de entrada y acciones
9. Corregir vulnerabilidades, actualizar y securización adicional

Ejemplo de recuperación - Wordpress

1. Análisis forense del servidor
2. Si encontramos que está comprometido el core, exportar el contenido: Panel de admin > Herramientas > Exportar > Todo el contenido
3. Copiar el contenido de /wp-content/uploads (asegurar que esté limpio!)
4. Eliminar todo el sitio
5. Reinstalar Wordpress
6. Importar el contenido: Panel de admin > Importar
7. Reinstalar plugins y plantillas

Otra guía:

https://sucuri.net/guides/how-to-clean-hacked-wordpress

Análisis de artefactos maliciosos

Técnicas de detección de artefactos maliciosos

- Análisis a nivel de host
  - Antivirus, antimalware, antispyware (Endpoint Security Solutions)
  - Monitor de procesos y conexiones del SO
  - Monitoreo y análisis de registros de auditoría
  - YARA
- Análisis a nivel de red:
  - Alertas de IDS/IPS
  - Soluciones de correlación de eventos (SIEM, UTM, …)
  - Análisis de peticiones de DNS y proxy
  - Captura y análisis de tráfico (Wireshark, tcpdump, Mitmproxy)

Técnicas de análisis de artefactos maliciosos

- **Análisis estático:**

  No se ejecuta el artefacto, se analiza sus metadatos y/o código

- **Análisis dinámico:**

  Se ejecuta el artefacto y se analiza su comportamiento: conexiones establecidas, llamadas de funciones, archivos y registros abiertos, creados y/o modificados, etc.

Herramientas de análisis estático básico

- **Multiengine scaners online:**
  - Virustotal: https://www.virustotal.com/es/
  - VirScan: http://virscan.org/
  - Jotti: https://virusscan.jotti.org/

- **Análisis de metadatos, empaquetado, strings:**
  - PEiD: http://www.woodmann.com/collaborative/tools/index.php/PEiD
  - Exeinfo PE: http://www.woodmann.com/collaborative/tools/index.php/ExeInfo_PE
  - File - Comando de Unix
  - Strings - Comando de Unix

- **Análisis de código- desensamblador estático:**
  - IDA Pro: https://www.hex-rays.com/products/ida/support/download.shtml

Herramientas de análisis dinámico básico

- **Sandbox online:**
  - Hybris-Analysis: https://www.hybrid-analysis.com/
  - Joe Sandbox: https://www.joesandbox.com/
  - Malwr: https://malwr.com/

- **Sandbox offline:**
  - Cuckoo Sandbox: https://cuckoosandbox.org/download

- **Desensambladores, decompiladores y debuggers:**
  - IDA Pro + Hex-Rays Decompiler
  - OllyDBG: http://www.ollydbg.de/
  - GDB: https://www.sourceware.org/gdb/
  - strace, ltrace - comandos de UNIX

Hands-On!

Instrucciones

Ejercicio 1:

1. Ingresa a: https://correo.cert.gov.py
   - Usuario: ceilac@cert.gov.py
   - Contraseña: test_ceilac2017
2. Analizar el primer correo (el más antiguo) y determinar el origen real y la URL real a la que redirige el enlace en el primer salto.
3. Analizar el adjunto del segundo correo y determinar el nombre del malware y la IP a la que se conecta luego de infectar a una víctima.
4. (Opcional) Analizar el adjunto del tercer correo y determinar qué vulnerabilidades explota y a qué IPs se conecta
5. (Opcional) Seleccionar un correo de tu bandeja de spam, y **sin abrirlo**, analiza su origen. Si en el código fuente ves un enlace, analízalo. Si tiene adjunto, abre el correo, descarga el adjunto **sin abrirlo** y analízalo.

Instrucciones

Ejercicio 2:

1. Ingresar a http://multirbl.valli.org/ u otros buscadores de listas negras y analizar las siguientes IPs:
    - 181.121.84.134
    - 186.17.128.18
    - 203.150.84.114
    - 181.123.9.170
1. Analizar por qué están listadas y cuales son los pasos a seguir para solucionar el problema
2. Analiza la IP de tu servidor de correo y determina si estás en lista negra o no

MUCHAS GRACIAS!

Ministerio de
TECNOLOGÍAS
DE LA INFORMACIÓN
Y COMUNICACIÓN