DGTIC UNAM CERT

2do Coloquio de Proyectos de Becarios en Seguridad Informática

Sandbox:
Análisis dinámico de malware

Mendoza García Leo Joaquín Rodrigo
Altamirano Guzmán Gabriel Norberto

¿Qué es una sandbox?

- Es un sistema que permite ejecutar aplicaciones no confiables dentro de un ambiente altamente controlado donde cuenta con permisos restringidos.

Ejemplos:

- Máquinas virtuales
  - Virtualbox
  - Xen
  - VMware
- Jaulas
  - Virtualización a nivel sistema operativo

Malware

- ¿Qué es un malware?
  - MALicious softWARE
- Tipos de malware
  - Virus
  - Gusanos
  - Troyanos
  - Adware, etc.

Análisis de malware

- Análisis estático
  - Código fuente
- Análisis dinámico
  - Comportamiento del malware

Sandbox para el análisis dinámico de malware

- Implementado en Cuckoo sandbox
  - Análisis del tráfico de red
  - Archivos que deja la muestra
  - Capturas de pantalla del sistema
  - Características del archivo
  - Uso de DLL’s
  - Cambios en la llaves de registro

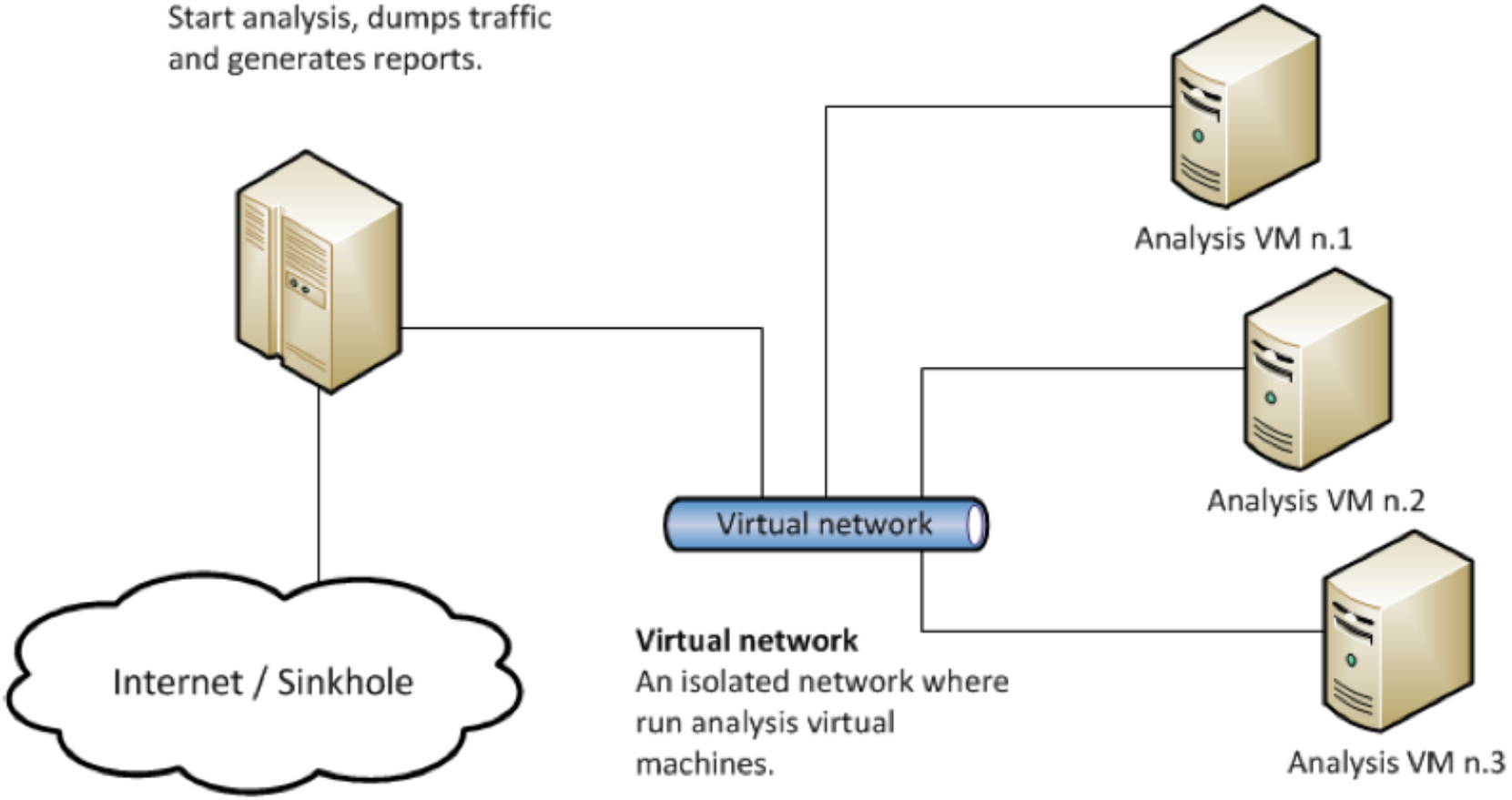
- Módulos externos (desarrollados en Python)
  - Análisis de tráfico mediante un IDS.
  - Análisis de la muestra con 4 antivirus.
  - Creación de un mapa del árbol de procesos.
  - Gráficas para estadísticas de red.
  - Concurrencia del análisis en varios sistemas.
  - Re-estructuración de la interfaz web (Python, PHP y JavaScript).

Capacidades de la Sandbox

- ¿Cómo funciona?
  - Uso de máquinas virtuales (clientes)
  - Servidor anfitrión y clientes

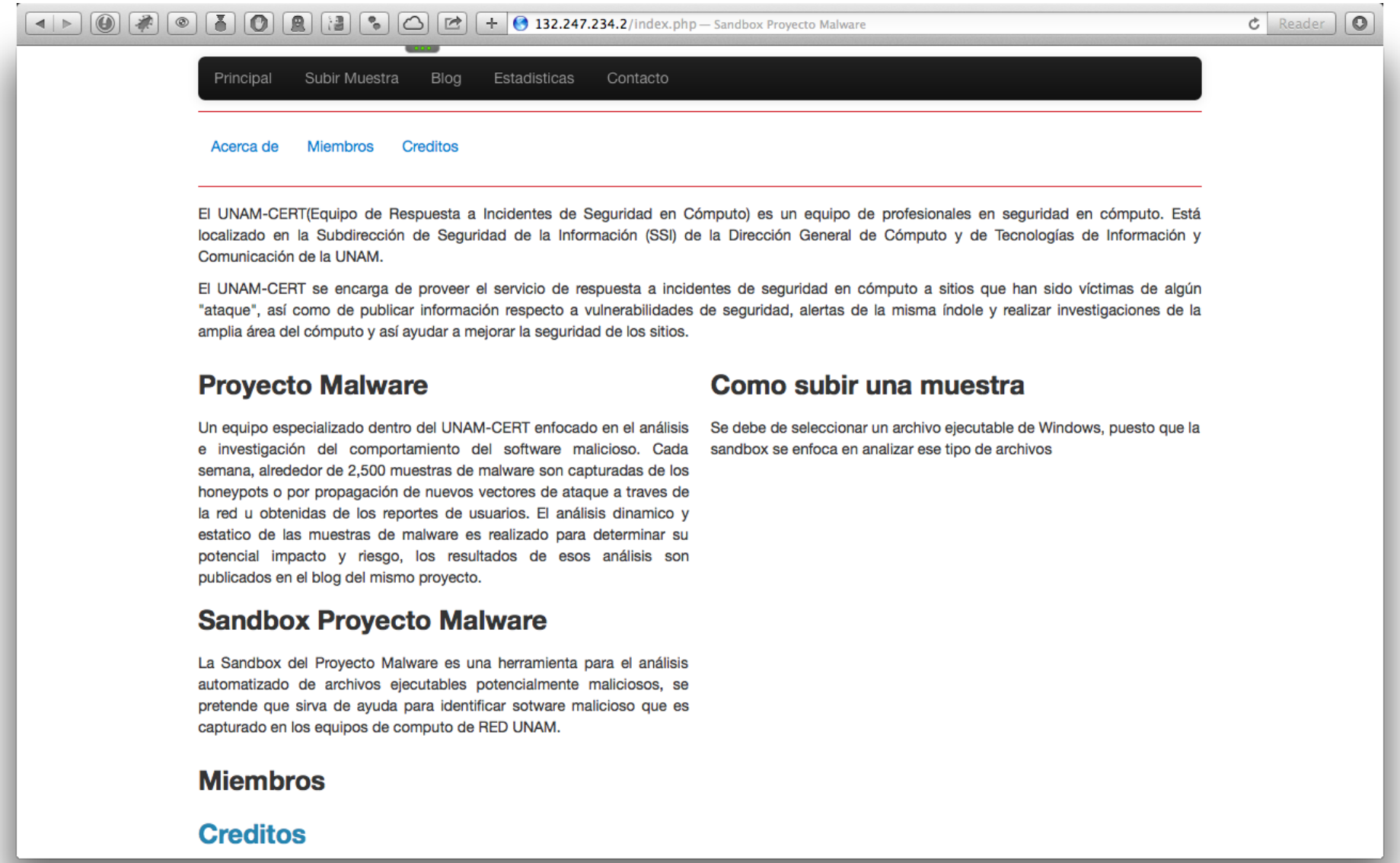
Cuckoo host
Responsible for guest and analysis management.
Start analysis, dumps traffic and generates reports.

Analysis Guests
A clean environment when run a sample.
The sample behavior is reported back to the Cuckoo host.



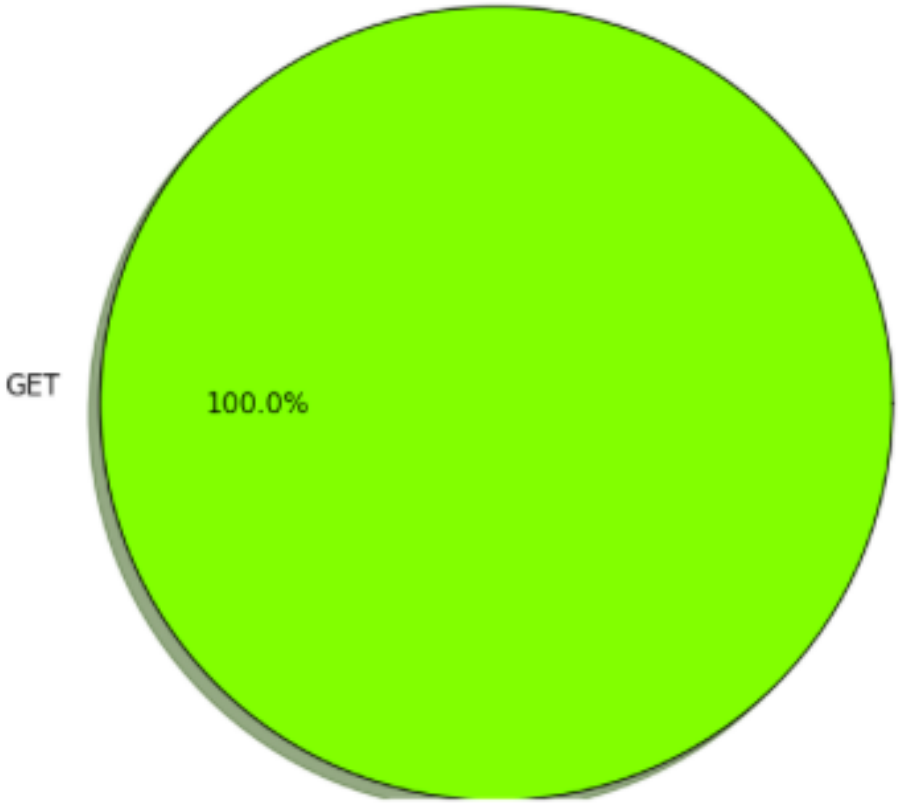
Virtual network
An isolated network where run analysis virtual machines.

- ¿Qué archivos es capaz de analizar?
  - Ejecutables
  - DLL’s
  - Archivos ZIP
  - PDF’s
  - Paquetería Office
  - Entre otros

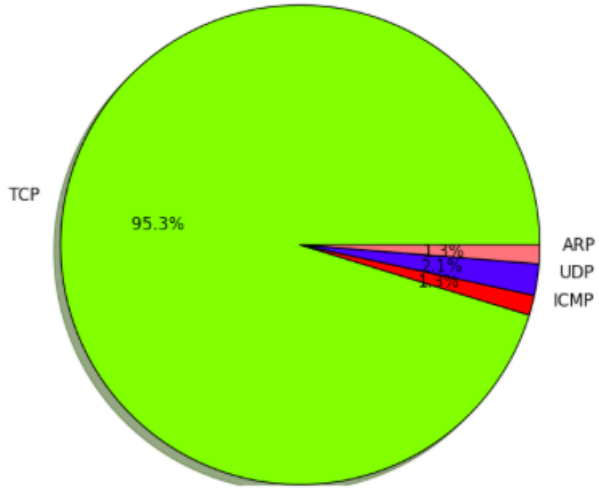

132.247.234.2/index.php — Sandbox Proyecto Malware
Reader
Principal
Subir Muestra
Blog
Estadisticas
Contacto
Acerca de
Miembros
Creditos
El UNAM-CERT(Equipo de Respuesta a Incidentes de Seguridad en Cómputo) es un equipo de profesionales en seguridad en cómputo. Está localizado en la Subdirección de Seguridad de la Información (SSI) de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación de la UNAM.
El UNAM-CERT se encarga de proveer el servicio de respuesta a incidentes de seguridad en cómputo a sitios que han sido víctimas de algún "ataque", así como de publicar información respecto a vulnerabilidades de seguridad, alertas de la misma índole y realizar investigaciones de la amplia área del cómputo y así ayudar a mejorar la seguridad de los sitios.
Proyecto Malware
Un equipo especializado dentro del UNAM-CERT enfocado en el análisis e investigación del comportamiento del software malicioso. Cada semana, alrededor de 2,500 muestras de malware son capturadas de los honeypots o por propagación de nuevos vectores de ataque a traves de la red u obtenidas de los reportes de usuarios. El análisis dinamico y estatico de las muestras de malware es realizado para determinar su potencial impacto y riesgo, los resultados de esos análisis son publicados en el blog del mismo proyecto.
Como subir una muestra
Se debe de seleccionar un archivo ejecutable de Windows, puesto que la sandbox se enfoca en analizar ese tipo de archivos
Sandbox Proyecto Malware
La Sandbox del Proyecto Malware es una herramienta para el análisis automatizado de archivos ejecutables potencialmente maliciosos, se pretende que sirva de ayuda para identificar sotware malicioso que es capturado en los equipos de computo de RED UNAM.
Miembros
Creditos

Estadisticas

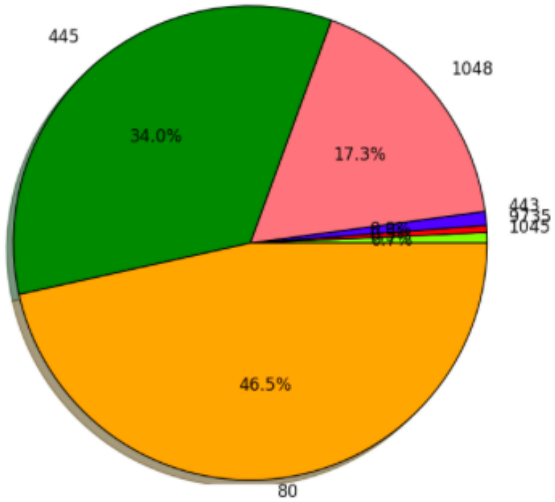
Metodos más utilizados

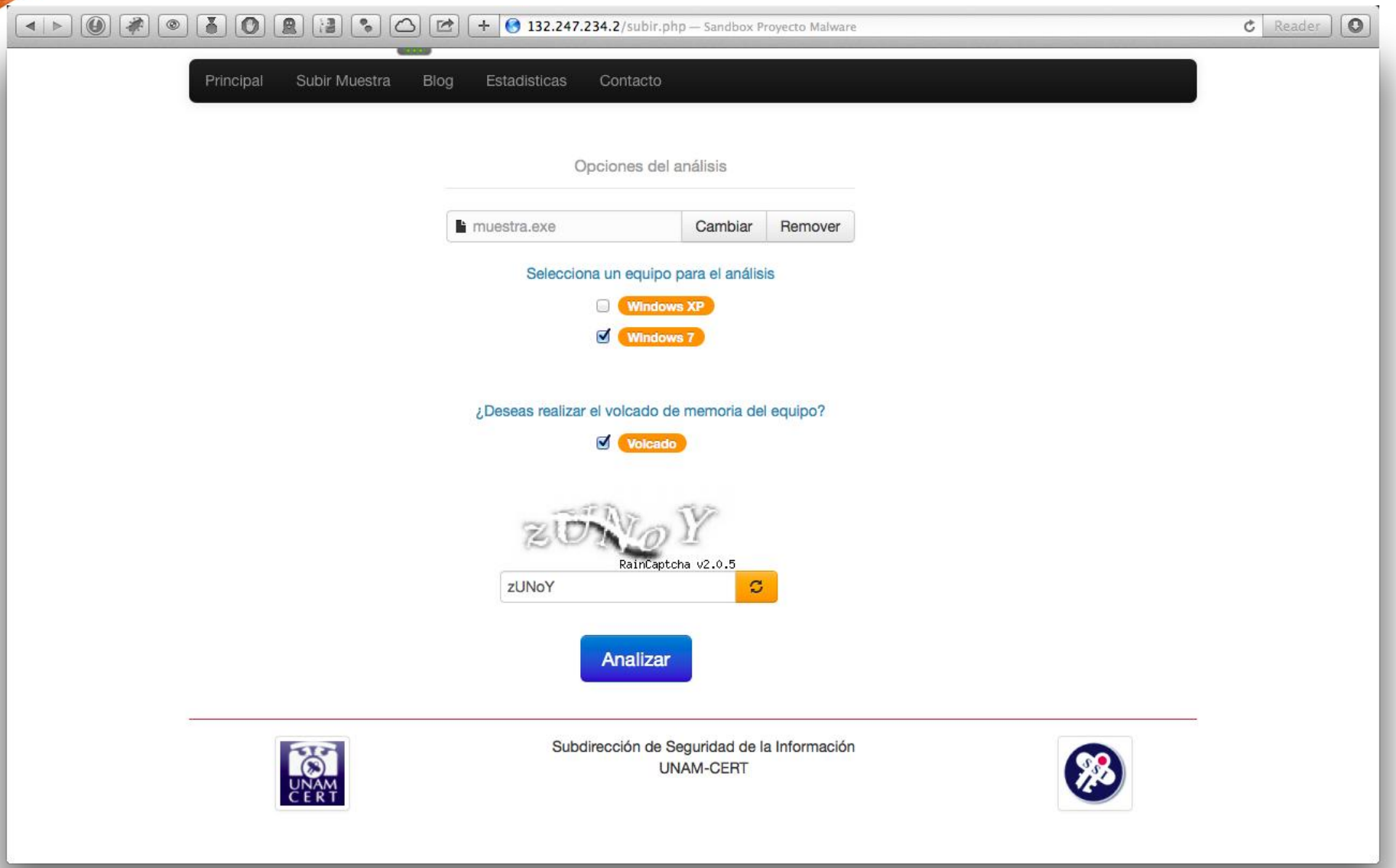


Protocolos más utilizados



Puertos más utilizados




132.247.234.2/subir.php — Sandbox Proyecto Malware
Reader
Principal
Subir Muestra
Blog
Estadisticas
Contacto
Opciones del análisis
muestra.exe
Cambiar
Remover
Selecciona un equipo para el análisis
Windows XP
Windows 7
¿Deseas realizar el volcado de memoria del equipo?
Volcado
RainCaptcha v2.0.5
zUNoY
Analizar
Subdirección de Seguridad de la Información
UNAM-CERT

Principal Subir Muestra Blog Estadisticas Contacto

El archivo fue subido exitosamente
Puedes ver el reporte de tu análisis aqui

UNAM CERT

Subdirección de Seguridad de la Información
UNAM-CERT

SSI

Principal Subir Muestra Blog Estadisticas Contacto

El archivo esta siendo analizado espera un momento mientras se genera el reporte

UNAM CERT

Subdirección de Seguridad de la Información
UNAM-CERT

SSI

Da click aqui para ver el reporte de tu analisis en Windows 7

File name	phpRKsjL2
File size	44420 bytes
File type	PE32 executable (GUI) Intel 80386, for MS Windows
CRC32	27E26763
MD5	de85ae919d48325189bead995e8052e7
SHA1	0f1892137e3a42997eaf21bef7540616c9d5fbc3
SHA256	3f3bb43c40be9b000fe0b5862eb906ed359e449ffc5a80067f15e45924758b86
SHA512	21e61a8f96154a1a19f94aa0327f8ccebe9f6ddfb0ab0e45d1cf42e4fd7aae4f846f60132db4d043ad3be7c370e4858dfb2d131301705a3993d62dc562f98704
Ssdeep	None
PEiD	• Armadillo v1.71
Yara	None matched

Static Analysis Dynamic Analysis Network Analysis

Static Analysis | Dynamic Analysis | Network Analysis

Signatures, Sections and Imports

Strings

Antivirus Analysis

Signatures

No signatures matched

Sections

Name	Virtual Address	Virtual Size	Size of Raw Data	Entropy
.text	0x1000	0x5c56	0x6000	6.49797989332
.rdata	0x7000	0xe60	0x1000	4.97847786101
.data	0x8000	0x2d84	0x2d84	2.04126359704

Imports

Library KERNEL32.dll:
- 0x407014 - DeleteFileA
- 0x407018 - CopyFileA
- 0x40701c - lstrcatA
- 0x407020 - GetTickCount
- 0x407024 - GetLocalTime
- 0x407028 - lstrcpyA
- 0x40702c - GetComputerNameA
- 0x407030 - GetLocaleInfoA
- 0x407034 - MultiByteToWideChar

Static Analysis | Dynamic Analysis | Network Analysis

- Signatures, Sections and Imports
- Strings
- Antivirus Analysis

Strings found

•!This program cannot be run in DOS mode.
•`.rdata
•@.data
•L$ PQSSSSS
•L$ j Q
•t.;t$$t(
•VC20XC00U
•HHtpHHtl
•8t9UW
•SS@SSPVSS
•t#SSUP
•t$$VSS
•_^][YY

Static Analysis | Dynamic Analysis | Network Analysis

- Signatures, Sections and Imports
- Strings
- Antivirus Analysis

Detections

ComodoAV	TrojWare.Win32.TrojanDownloader.Agent.~FIO
F-prot	[Found security risk] <W32/HLL-SysDlrSharer!Eldorado
AVG	Trojan horse Downloader.Agent2.BLSQ
ClamAV	Trojan.Downloader-73594 FOUND

Static Analysis | Dynamic Analysis | Network Analysis

Behavior
Processes
Dropped Files

Screenshots

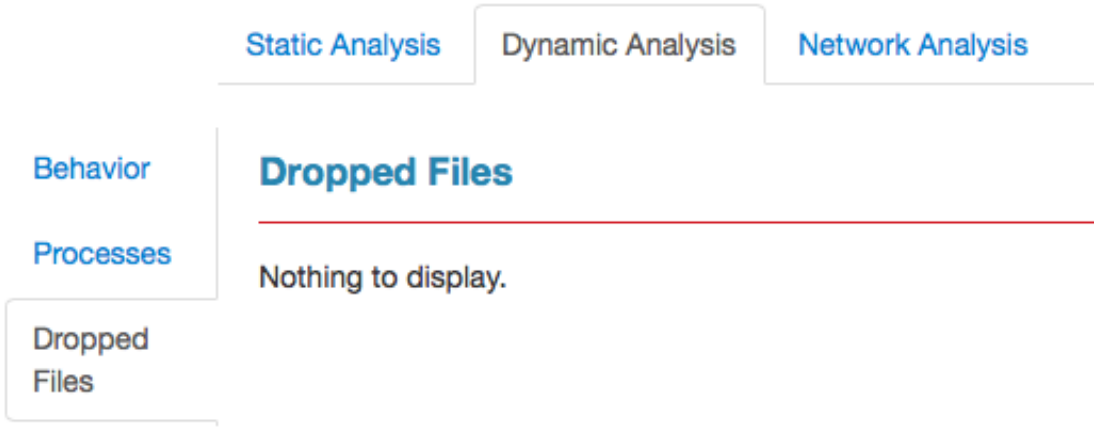
Behavior Summary

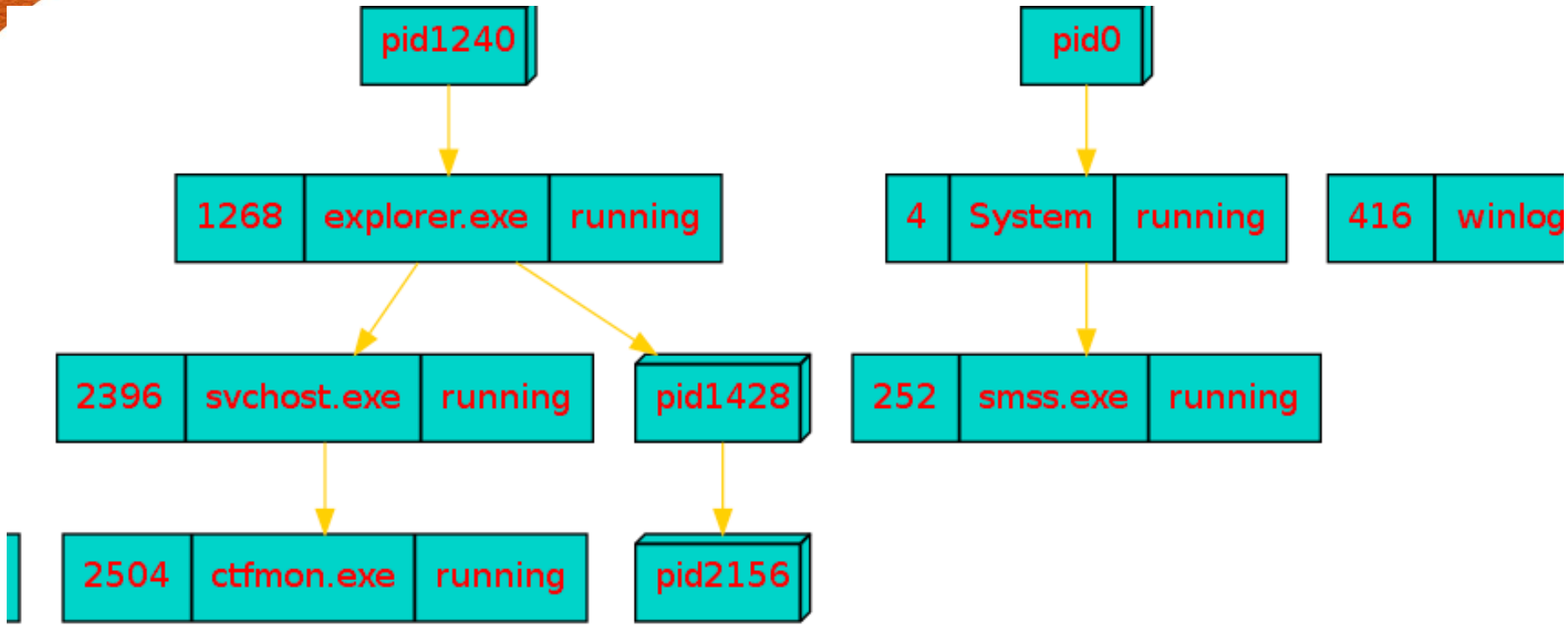
Files

- C:\Windows\system32\msupd.exe
- C:\Users\w7\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\
- C:\Users\w7\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat
- C:\Users\w7\AppData\Roaming\Microsoft\Windows\Cookies\
- C:\Users\w7\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
- C:\Users\w7\AppData\Local\Microsoft\Windows\History\History.IE5\
- C:\Users\w7\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
- C:\Windows\system32\en-US\urlmon.dll.mui
- C:\Users\w7\AppData\Roaming\Microsoft\Windows\IETldCache\
- C:\Users\w7\AppData\Roaming\Microsoft\Windows\IETldCache\index.dat
- C:\Windows\system32\WININET.dll

Registry Keys

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\feedplat
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\ietld
- HKEY_LOCAL_MACHINE\Software\Microsoft\DownloadManager
- HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
- HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings




pid1240
1268
explorer.exe
running
2396
svchost.exe
running
pid1428
2504
ctfmon.exe
running
pid2156
pid0
4
System
running
252
smss.exe
running
416
winlog

Static Analysis | Dynamic Analysis | Network Analysis

Hosts and Domains

Snort Alerts

Hosts Involved

IP Address
192.168.56.102
224.0.0.22
224.0.0.252
192.168.56.255
8.8.8.8
239.255.255.250
125.206.117.59

DNS Requests

Domain	IP Address
teredo.ipv6.microsoft.com	157.56.106.189
dns.msftncsi.com	131.107.255.255
fukyu.jp	

HTTP Requests

URL	Data

http://23.107.252.2/	`OPTIONS / HTTP/1.1`
	`Connection: Keep-Alive`
	`User-Agent: DavClnt`
	`translate: f`
	`Host: 23.107.252.2`

http://23.107.252.2/	`OPTIONS / HTTP/1.1`
	`Connection: Keep-Alive`
	`User-Agent: DavClnt`
	`translate: f`
	`Host: 23.107.252.2`

Static Analysis | Dynamic Analysis | Network Analysis

Hosts and Domains

Snort Alerts

Alerts

SCAN UPnP service discover attempt
ICMP Destination Unreachable Communication Administratively Prohibited
ICMP Destination Unreachable Host Unreachable
ICMP Destination Unreachable Port Unreachable
ICMP Destination Unreachable Network Unreachable
ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited

Gracias por su atención

¿Preguntas?