Análisis de malware

Presentación

Gustavo Romero López - gustavo@ugr.es

Updated: 21 de abril de 2025

Departamento de Ingeniería de Computadores, Automática y Robótica

Introducción

- El teléfono suena: "¡Estamos siendo atacados!"
- Escanea el ordenador con el antivirus para encontrar y eliminar la amenaza.
- Busca en el tráfico de red una firma para el sistema de detección de intrusiones.
- Tapa el agujero de seguridad que ha permitido el ataque.
- Varios días después el ataque prosigue.
- Solo podemos decir el nombre del malware causante.
  - ¿Que hace este malware?
  - ¿Cómo detectar una firma de red efectiva?
  - ¿Qué otras máquinas han sido afectadas?
  - ¿Hemos eliminado la amenaza por completo?

Malware = software malicioso

- Definición: cualquier tipo de software que cause daño a personas, ordenadores o redes.
- Tipos:
  - **gusanos**: código malicioso capaz de replicarse sin intervención humana.
  - **puertas traseras**: mecanismo para el acceso no autorizado.
  - **rootkits**: código que permite aumentar el nivel de privilegio.
  - **scareware**: atemoriza e intenta estafar.
  - **spammers**: difunde correo basura.
  - **spyware**: software espía.
  - **troyanos**: software malicioso disfrazado de contenido atractivo: software de pago, estrenos de cine, juegos,...
  - **virus**: código malicioso capaz de replicarse con intervención humana.
- Es común mezclar varias funcionalidades.

Técnicas de análisis de malware (Sikorski & Honig)

- **Análisis estático básico**: analizar ficheros ejecutables sin preocuparnos por las instrucciones que ejecutan sino solo de las funciones que ejecuta, el tamaño y tipo de sus componentes, las cadenas que contiene, su nivel de entropía,...
- **Análisis dinámico básico**: ejecutar el malware para observar su funcionamiento y ser así capaces de eliminarlo y crear huellas para detectarlo. Usa máquinas virtuales para evitar perjudicar a máquinas y redes.
- **Análisis estático avanzado**: ingeniería inversa mediante desensambladores para conocer al detalle lo que hace instrucción por instrucción. Requiere conocimientos avanzados de ensamblador, lenguajes de programación y sistemas operativos.
- **Análisis dinámico avanzado**: Ejecutar el malware bajo la supervisión de un depurador para ser capaces de analizar de manera precisa su comportamiento.

Análisis estático básico

- Antivirus: `https://www.virustotal.com`
- Identificación: md5deep, md5sum, sha*sum
- Búsqueda de cadenas: strings
- Detección de compresión: PEiD, UPX
- Funciones enlazadas: DependencyWalker
- Examinar ejecutables: PEview
- Recursos: Resource Hacker

Análisis dinámico básico

- Cajas de arena/Espacios aislados:
  - Cuckoo Sandbox
  - Joe Sandbox
  - Windows Sandbox
- Monitorización del registro, sistema de ficheros, actividad de procesos y red:
  - Procmon
  - Process Explorer
  - DependencyWalker
  - Regshot
  - ApateDNS, FakeDNS, INetSim
  - netcat
  - Wireshark

Análisis estático avanzado

- Herramientas de ingeniería inversa: combinación de depurador, desensamblador y descompilador:
  - IDA Pro
  - OllyDbg
  - WinDbg
  - radare2/iaito
  - rizin/cutter
  - Binary Ninja
- Descompiladores:
  - Ghidra

Análisis dinámico avanzado

- Usar las herramientas de análisis dinámico pero ejecutando el malware desde el interior de las herramientas de análisis estático.

Técnicas de análisis de malware (Lenny Zeltser)

- **Análisis de código**
  - PeStudio
  - IDA Freeware
  - x64dbg
  - Scylla
- **Análisis de comportamiento**
  - Process Monitor
  - ProcDOT
  - Process Hacker
  - Wireshark

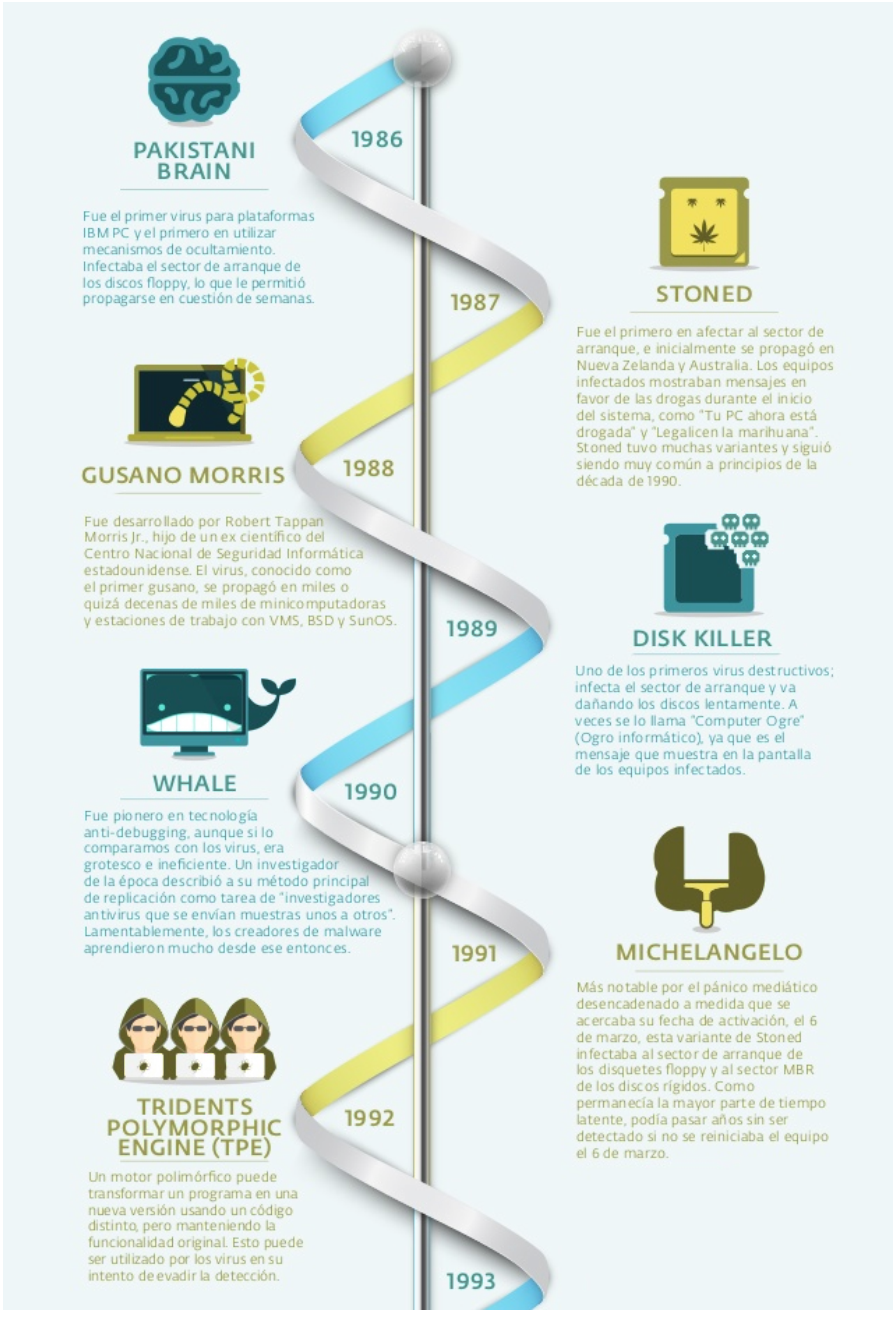
Máquinas virtuales

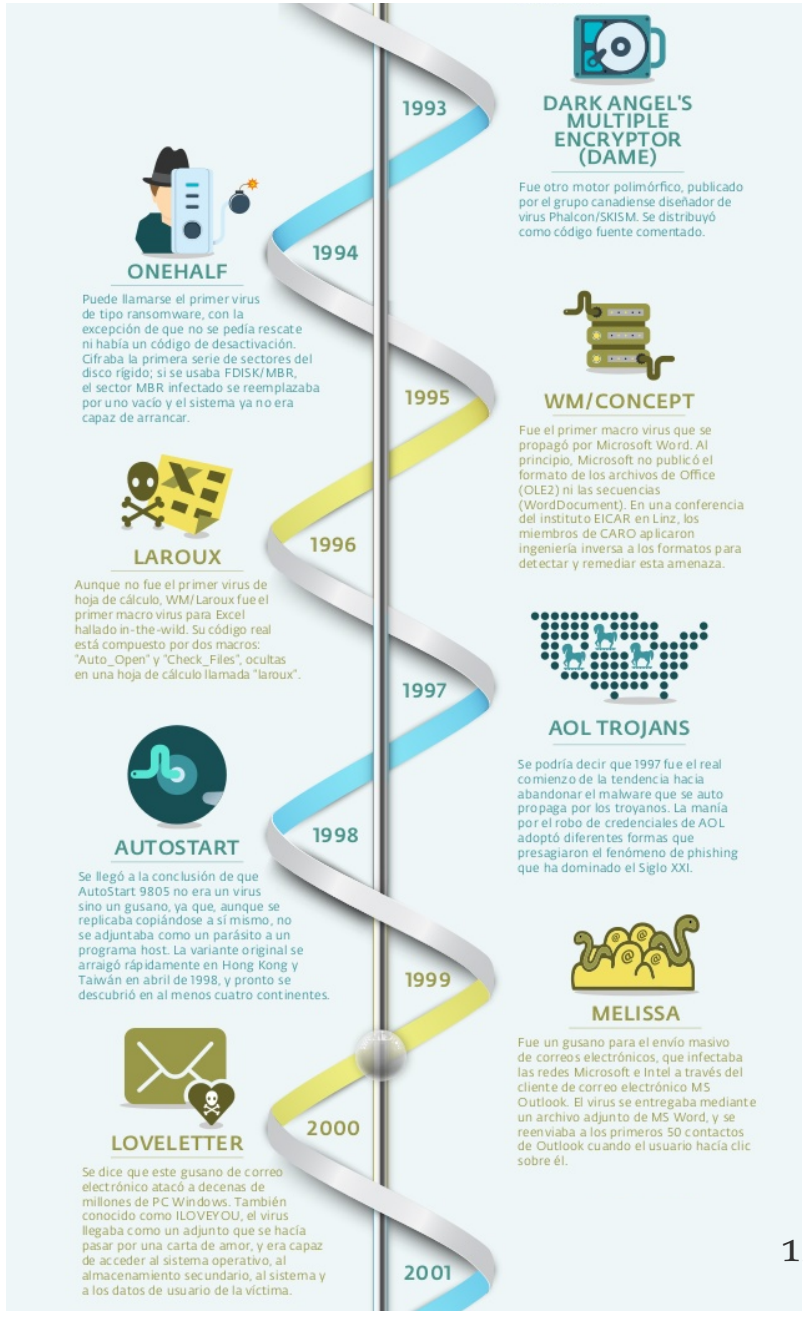
- Permiten ejecutar malware en un entorno seguro.
- Usar máquinas físicas supone un gran riesgo y más si están conectadas a la red.
- Ventajas:
  - seguridad tanto para nuestra red como internet
  - comodidad gracias a las imágenes/instantáneas
- Desventajas:
  - el aislamiento de la red puede alterar su interacción
  - diferencia de comportamiento frente a máquinas físicas
  - vulnerabilidades en el software de virtualización

Entorno aislado ("*SandBox*")

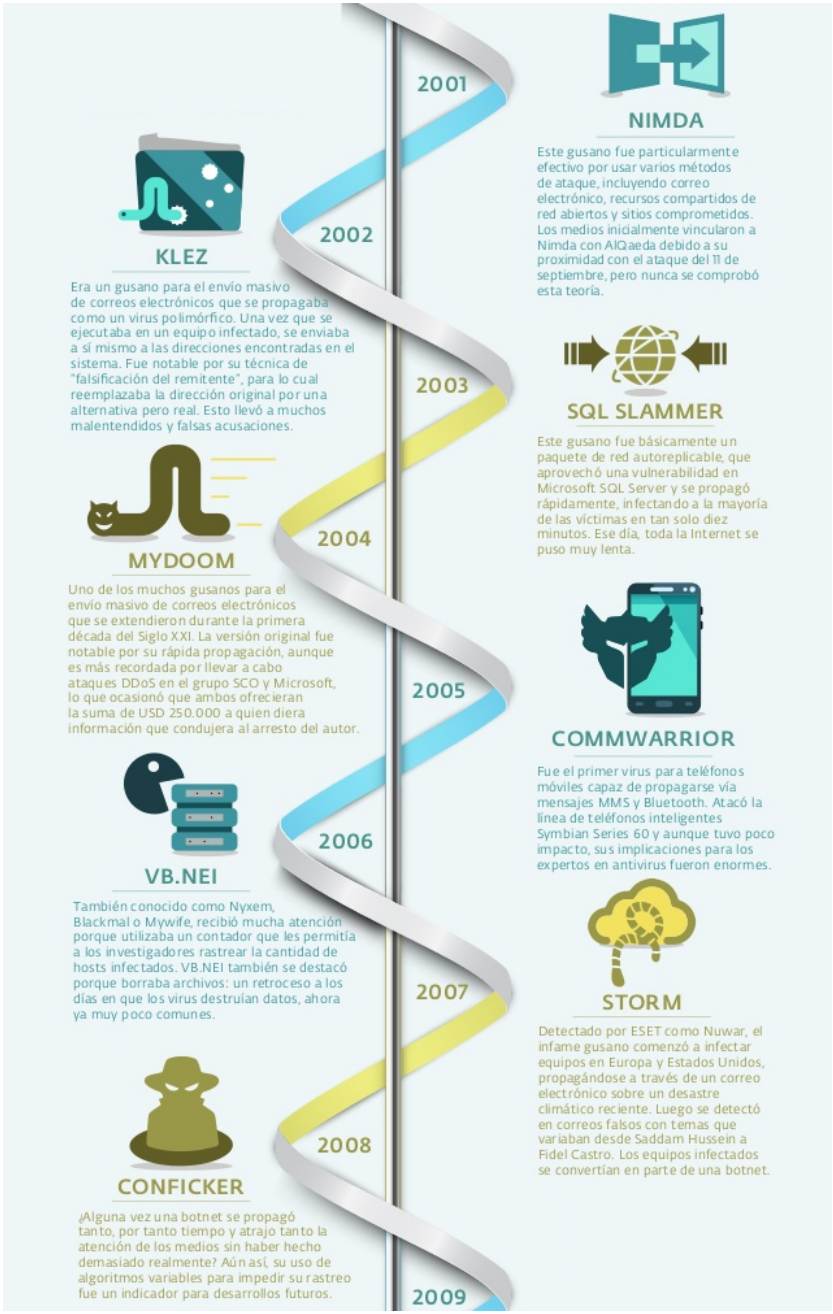
- Definición: mecanismo para ejecutar programas de dudosa fiabilidad de manera segura.
- Cuanto más se asemeje a un sistema real, más probable es que podamos identificar con exactitud el funcionamiento del malware.
- Algunos automatizan el proceso de rastreo de actividad y elaboran informes sobre el comportamiento del malware.
- Cuidado con los falsos positivos.
- Ejemplos:
  - Cuckoo Sandbox
  - Joe Sandbox
  - Microsoft Sandbox
  - VirusTotal

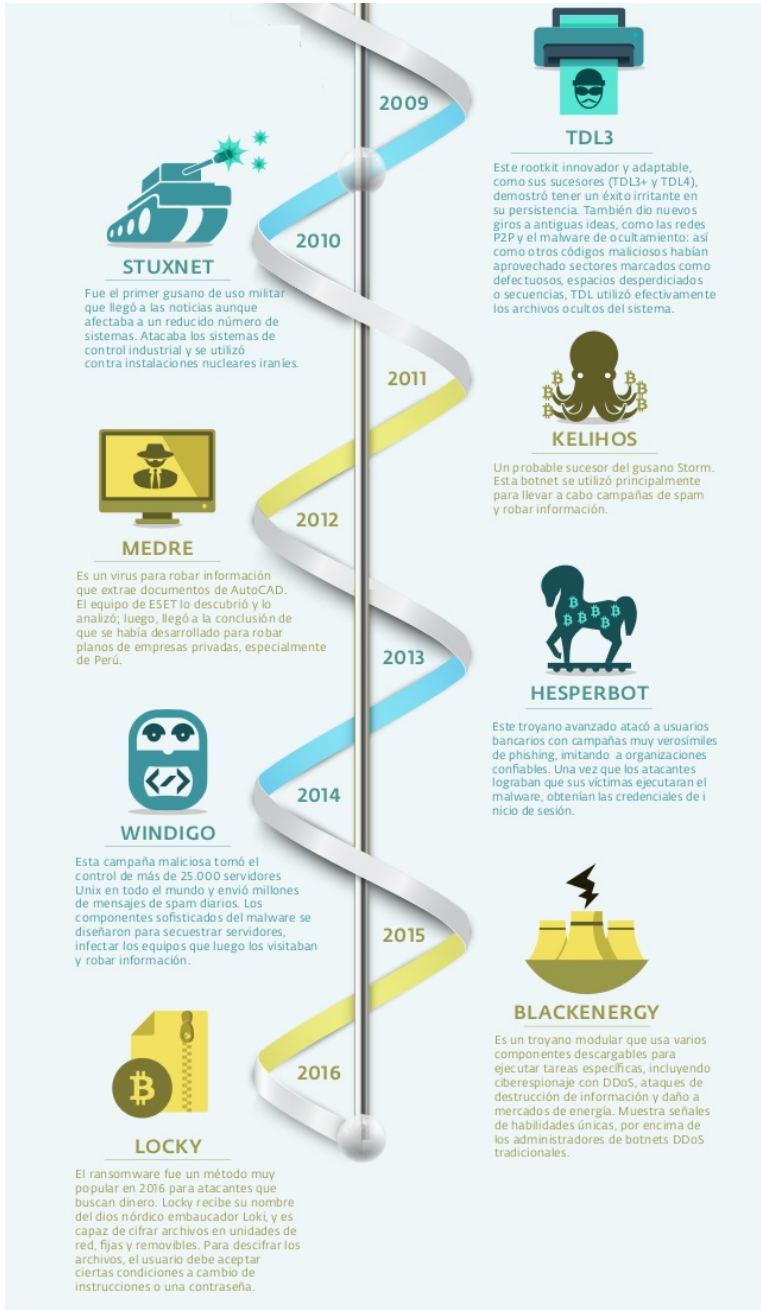
Historia (I)


1986
PAKISTANI BRAIN
Fue el primer virus para plataformas IBM PC y el primero en utilizar mecanismos de ocultamiento. Infectaba el sector de arranque de los discos floppy, lo que le permitió propagarse en cuestión de semanas.
1987
STONED
Fue el primero en afectar al sector de arranque, e inicialmente se propagó en Nueva Zelanda y Australia. Los equipos infectados mostraban mensajes en favor de las drogas durante el inicio del sistema, como "Tu PC ahora está drogada" y "Legalicen la marihuana". Stoned tuvo muchas variantes y siguió siendo muy común a principios de la década de 1990.
1988
GUSANO MORRIS
Fue desarrollado por Robert Tappan Morris Jr., hijo de un ex científico del Centro Nacional de Seguridad Informática estadounidense. El virus, conocido como el primer gusano, se propagó en miles o quizá decenas de miles de minicomputadoras y estaciones de trabajo con VMS, BSD y SunOS.
1989
DISK KILLER
Uno de los primeros virus destructivos; infecta el sector de arranque y va dañando los discos lentamente. A veces se lo llama "Computer Ogre" (Ogro informático), ya que es el mensaje que muestra en la pantalla de los equipos infectados.
1990
WHALE
Fue pionero en tecnología anti-debugging, aunque si lo comparamos con los virus, era grotesco e ineficiente. Un investigador de la época describió a su método principal de replicación como tarea de "investigadores antivirus que se envían muestras unos a otros". Lamentablemente, los creadores de malware aprendieron mucho desde ese entonces.
1991
MICHELANGELO
Más notable por el pánico mediático desencadenado a medida que se acercaba su fecha de activación, el 6 de marzo, esta variante de Stoned infectaba al sector de arranque de los disquetes floppy y al sector MBR de los discos rígidos. Como permanecía la mayor parte de tiempo latente, podía pasar años sin ser detectado si no se reiniciaba el equipo el 6 de marzo.
1992
TRIDENTS POLYMORPHIC ENGINE (TPE)
Un motor polimórfico puede transformar un programa en una nueva versión usando un código distinto, pero manteniendo la funcionalidad original. Esto puede ser utilizado por los virus en su intento de evadir la detección.
1993


1993
DARK ANGEL'S MULTIPLE ENCRYPTOR (DAME)
Fue otro motor polimórfico, publicado por el grupo canadiense diseñador de virus Phalcon/SKISM. Se distribuyó como código fuente comentado.
1994
ONEHALF
Puede llamarse el primer virus de tipo ransomware, con la excepción de que no se pedía rescate ni había un código de desactivación. Cifraba la primera serie de sectores del disco rígido; si se usaba FDISK/MBR, el sector MBR infectado se reemplazaba por uno vacío y el sistema ya no era capaz de arrancar.
1995
WM/CONCEPT
Fue el primer macro virus que se propagó por Microsoft Word. Al principio, Microsoft no publicó el formato de los archivos de Office (OLE2) ni las secuencias (WordDocument). En una conferencia del instituto EICAR en Linz, los miembros de CARO aplicaron ingeniería inversa a los formatos para detectar y remediar esta amenaza.
1996
LAROUX
Aunque no fue el primer virus de hoja de cálculo, WM/Laroux fue el primer macro virus para Excel hallado in-the-wild. Su código real está compuesto por dos macros: "Auto_Open" y "Check_Files", ocultas en una hoja de cálculo llamada "laroux".
1997
AOL TROJANS
Se podría decir que 1997 fue el real comienzo de la tendencia hacia abandonar el malware que se auto propaga por los troyanos. La manía por el robo de credenciales de AOL adoptó diferentes formas que presagiaron el fenómeno de phishing que ha dominado el Siglo XXI.
1998
AUTOSTART
Se llegó a la conclusión de que AutoStart 9805 no era un virus sino un gusano, ya que, aunque se replicaba copiándose a sí mismo, no se adjuntaba como un parásito a un programa host. La variante original se arraigó rápidamente en Hong Kong y Taiwán en abril de 1998, y pronto se descubrió en al menos cuatro continentes.
1999
MELISSA
Fue un gusano para el envío masivo de correos electrónicos, que infectaba las redes Microsoft e Intel a través del cliente de correo electrónico MS Outlook. El virus se entregaba mediante un archivo adjunto de MS Word, y se reenviaba a los primeros 50 contactos de Outlook cuando el usuario hacía clic sobre él.
2000
LOVELETTER
Se dice que este gusano de correo electrónico atacó a decenas de millones de PC Windows. También conocido como ILOVEYOU, el virus llegaba como un adjunto que se hacía pasar por una carta de amor, y era capaz de acceder al sistema operativo, al almacenamiento secundario, al sistema y a los datos de usuario de la víctima.
2001

Historia (II)


2001
NIMDA
Este gusano fue particularmente efectivo por usar varios métodos de ataque, incluyendo correo electrónico, recursos compartidos de red abiertos y sitios comprometidos. Los medios inicialmente vincularon a Nimda con AlQaeda debido a su proximidad con el ataque del 11 de septiembre, pero nunca se comprobó esta teoría.
2002
KLEZ
Era un gusano para el envío masivo de correos electrónicos que se propagaba como un virus polimórfico. Una vez que se ejecutaba en un equipo infectado, se enviaba a sí mismo a las direcciones encontradas en el sistema. Fue notable por su técnica de "falsificación del remitente", para lo cual reemplazaba la dirección original por una alternativa pero real. Esto llevó a muchos malentendidos y falsas acusaciones.
2003
SQL SLAMMER
Este gusano fue básicamente un paquete de red autoreplicable, que aprovechó una vulnerabilidad en Microsoft SQL Server y se propagó rápidamente, infectando a la mayoría de las víctimas en tan solo diez minutos. Ese día, toda la Internet se puso muy lenta.
2004
MYDOOM
Uno de los muchos gusanos para el envío masivo de correos electrónicos que se extendieron durante la primera década del Siglo XXI. La versión original fue notable por su rápida propagación, aunque es más recordada por llevar a cabo ataques DDoS en el grupo SCO y Microsoft, lo que ocasionó que ambos ofrecieran la suma de USD 250.000 a quien diera información que condujera al arresto del autor.
2005
COMMWARRIOR
Fue el primer virus para teléfonos móviles capaz de propagarse vía mensajes MMS y Bluetooth. Atacó la línea de teléfonos inteligentes Symbian Series 60 y aunque tuvo poco impacto, sus implicaciones para los expertos en antivirus fueron enormes.
2006
VB.NEI
También conocido como Nyxem, Blackmal o Mywife, recibió mucha atención porque utilizaba un contador que les permitía a los investigadores rastrear la cantidad de hosts infectados. VB.NEI también se destacó porque borraba archivos: un retroceso a los días en que los virus destruían datos, ahora ya muy poco comunes.
2007
STORM
Detectado por ESET como Nuwar, el infame gusano comenzó a infectar equipos en Europa y Estados Unidos, propagándose a través de un correo electrónico sobre un desastre climático reciente. Luego se detectó en correos falsos con temas que variaban desde Saddam Hussein a Fidel Castro. Los equipos infectados se convertían en parte de una botnet.
2008
CONFICKER
¿Alguna vez una botnet se propagó tanto, por tanto tiempo y atrajo tanto la atención de los medios sin haber hecho demasiado realmente? Aún así, su uso de algoritmos variables para impedir su rastreo fue un indicador para desarrollos futuros.
2009


2009
TDL3
Este rootkit innovador y adaptable, como sus sucesores (TDL3+ y TDL4), demostró tener un éxito irritante en su persistencia. También dio nuevos giros a antiguas ideas, como las redes P2P y el malware de ocultamiento: así como otros códigos maliciosos habían aprovechado sectores marcados como defectuosos, espacios desperdiciados o secuencias, TDL utilizó efectivamente los archivos ocultos del sistema.
2010
STUXNET
Fue el primer gusano de uso militar que llegó a las noticias aunque afectaba a un reducido número de sistemas. Atacaba los sistemas de control industrial y se utilizó contra instalaciones nucleares iraníes.
2011
KELIHOS
Un probable sucesor del gusano Storm. Esta botnet se utilizó principalmente para llevar a cabo campañas de spam y robar información.
2012
MEDRE
Es un virus para robar información que extrae documentos de AutoCAD. El equipo de ESET lo descubrió y lo analizó; luego, llegó a la conclusión de que se había desarrollado para robar planos de empresas privadas, especialmente de Perú.
2013
HESPERBOT
Este troyano avanzado atacó a usuarios bancarios con campañas muy verosímiles de phishing, imitando a organizaciones confiables. Una vez que los atacantes lograban que sus víctimas ejecutaran el malware, obtenían las credenciales de inicio de sesión.
2014
WINDIGO
Esta campaña maliciosa tomó el control de más de 25.000 servidores Unix en todo el mundo y envió millones de mensajes de spam diarios. Los componentes sofisticados del malware se diseñaron para secuestrar servidores, infectar los equipos que luego los visitaban y robar información.
2015
BLACKENERGY
Es un troyano modular que usa varios componentes descargables para ejecutar tareas específicas, incluyendo ciberespionaje con DDoS, ataques de destrucción de información y daño a mercados de energía. Muestra señales de habilidades únicas, por encima de los administradores de botnets DDoS tradicionales.
2016
LOCKY
El ransomware fue un método muy popular en 2016 para atacantes que buscan dinero. Locky recibe su nombre del dios nórdico embaucador Loki, y es capaz de cifrar archivos en unidades de red, fijas y removibles. Para descifrar los archivos, el usuario debe aceptar ciertas condiciones a cambio de instrucciones o una contraseña.