El virus Conficker

by javier - Sábado, junio 27, 2015

http://memoriasdeunsysadmin.tk/2015/06/27/el-virus-conficker/

El mundo de las redes, y su seguridad, se ha convertirido en uno de mis principales intereses desde hace tiempo. Es un campo fascinante y que no deja de evolucionar, como así tampoco las amenazas y su complejidad. Conficker es un virus muy particular que ha ido haciéndose muy popular por su historia e inmortalidad.

Conficker vio la luz alrededor de Octubre del 2008, creado para explotar una vulnerabilidad propia del servicio "servidor", de Windows, en sus versiones 2000, XP, Vista, Server 2003 e incluso Server 2008. Explotando dicha vulnerabilidad, que consistía en un incorrecto manejo de solicitudes RPC(Llamada a procedimiento remoto) "alteradas", un atacante podría ejecutar código remoto sin necesitar autenticarse. Pueden ver más detalles sobre esta vulnerabilidad en el boletín de seguridad de Microsoft MS08-067(En Inglés) o en la CVE 2008-4250(También en Inglés).

Para el que no conocía CVE, es un diccionarioo online que recopila información sobre Vulnerabilidades Conocidas, utilizando un sistema estandarizado, de manera que pueda ser utilizado por algunas apps y servicios online. Tienen también un sistema que da puntaje a cada vulnerabilidad(CVSS), de acuerdo al cuál, MS08-067 recibe el puntaje máximo, 10, por su alto impacto, la facilidad de ser explotada y el hecho de no requerir autenticación. En el sitio de la National Vulnerability Database(En Inglés), pueden ver más datos sobre el impacto y cómo se aplica este puntaje:
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4250

Para explotar esta vulnerabilidad, es que nació el gusano Conficker, que se convirtió en uno de los más rápidos gusanos en propagarse. Más aún, pasó a ser la infección más grande después de Sasser, debido a su versatilidad(Infectó más de 11 millones de dispositivos). Conficker utiliza distintas técnicas bastante avanzadas de infección.

Por qué hablamos hoy de Conficker?

Esta se ha vuelto una de las amenazas más persistentes y peligrosas en los últimos años. Pero lo más importante no es su riesgo, sino que aún siga tan vigente. Hay varios factores que contribuyen a esto: Uno de los claves es, tal vez, el hecho de que Windows XP, un sistema tan viejo y obsoleto(que además ha perdido soporte hace unos meses ya) siga siendo uno de los Sistemas Operativos más utilizados y distribuidos a nivel mundial. La falta de confianza en Windows 7/8(en realidad el miedo al cambio) favorecen mucho a malware de este tipo que se alimenta de sistemas desactualizados. También la poca aceptación de linux como sistema de escritorio por parte de usuarios finales.

Como sea, es evidente que las consecuencias son nefastas. Solo Conficker causó más de 9 billones de dólares a nivel mundial, incluyendo pérdidas de datos, avnes de combate estrellados y un largo etcétera.

Conociendo al enemigo:

El gusano tiene mecanismos de defensa, tales como apagar servicios de Antivirus y alertas de Windows. También bloquear el acceso a páginas de seguridad. De este modo deja abierta la puerta a infecciones de otros viruses, troyanos y malware.

Puede "comunicarse" con sus creadores para recibir órdenes o instrucciones, conectándose a través de cientos de distintos dominios(es incluso capaz de generar una lista de nuevos dominios a diario). Un gusano tan eficiente pudo incluso ser usado. De este modo también puede descargar archivos a voluntad.

La Infección:

Conficker hace copias de si mismo en la carpeta System de Windows. También agrega claves en el registro de Windows, de manera que se convierte a sí mismo en un servicio legítimo. El próximo paso consiste en obtener la IP pública de la víctima, a través de sitios como getmyip.org, getmyip.co.uk, checkip.dyndns.org.

Una vez obtiene la IP, descarga un pequeño Servidor Web desde http://trafficconverter.biz/4vir/antispyware/loadadv.exe.Luego procede a instalarlo en un puerto al azar. Una vez el Servidor HTTP está funcionando, escanea la red para encontrar otros dispositivos vulnerables. Si encuentra más víctimas, se encarga de enviar la URL del de la máquina infectada a la próxima víctima, para infectarla a través de la vulnerabilidad mencionada. El equipo remoto descargará el gusano a través de la URL proporcionada y comenzará a infectar a su vez otros equipos creando, de esta manera, un sistema des-centralizado.

RPC es un protocolo que sirve de intermediario para aplicaciones de equipos remotos que necesiten interactuar con servicios dentro del servidor local. El servicio "Server" provee soporte RPC de manera de permitir acceso remoto a recursos compartidos locales, a través de una red.

Puede propagarse además a través de carpetas compartidas y dispositivos USB(Esta es una característica añadida en la variante B) . En este último caso, agrega un archivo al dispositivo, causando que el AutoPlay del equipo donde se inserte muestre una opción adicional(Ver imagen1). Solo falta que alguien elija esa opción, ignorando que se trata de una falsificación, para que el gusano se ejecute e infecte la máquina local.

Buenas y Malas noticias:

Gracias al gran impacto del virus y a los esfuerzos conjuntos de fuerzas policiales de distintos países, se sospecha que quién sea el creado del mismo(o el grupo creador) abandonó su creación. De otra manera, hoy podría ser fácilmente usado como base de una botnet de tamaños impensables. Aún así, hoy en día sigue siendo el malware más comúnmente encontrado, punto en el que coinciden distintas Compañías de soluciones antivirus al igual que entidades de Investigación. Se estima que hayan aún alreadedor de 500.000 dispositivos infectados, a 7 años de la aparición original del malware.

Síntomas de Infección:

- Los siguientes servicios se encuentran deshabilitados: Automatic Updates, Transferencia Inteligente en Segundo plano, Windows Defender y Reporte de Errores.

- Lentitud en la red.
- Controladores de dominio tardan mucho en responder.
- No se puede acceder a una gran mayoría de sitios de seguridad y antivirus.
- Descarga de archivos, arbitrariamente.
- Aumento de tráfico en el puerto 445
- Pérdida de puntos de restauración del sistema y archivos de backups.
- El acceso a recursos del administrador es denegado

Cómo remover el virus:

En la web se consiguen numerosas herramientas específicas para eliminar este gusano. Si por la misma infección es imposible descargar o ejecutarlas existe un método manual que pueden encontrar aquí

Conclusión:

Conficker es aún una amenaza fuerte, sin embargo lo más importante es la lección que deja. El sistema operativo debe estar siempre actualizado, ya que esta es la única y mejor manera de prevenir una gran mayoría de infecciones por virus y gusanos. También es notable que una de las puertas de entrada es el rechazo de la gente hacia sistemas más nuevos, eligiendo quedarse siempre con Windows XP.

Qué opinas?

Otras fuentes de información(En inglés):

https://www.microsoft.com/security/pc-security/conficker.aspx#EWC

http://www.sans.org/security-resources/malwarefaq/conficker-worm.php

---

memoriasdeunsysadmin.tk