Boletin de Seguridad UNAM-CERT-2015-009 Simda Botnet

La botnet Simda,que infecta equipos en la red y autopropaga su malware, ha comprometido cerca de 770,000 equipos alrededor del mundo. United States Department of Homeland Security (DHS) en colaboración con la Interpol y el Federal Bureau of Investigation (FBI), han enviado esta alerta técnica para proporcionar información sobre la botnet Simda, junto con las recomendaciones de prevención y mitigación.

- **Fecha de Liberación:** 15-Abr-2015
- **Ultima Revisión:** 15-Abr-2015
- **Fuente:**
- **Riesgo** Crítico

1. Descripción

Desde 2009, los cibercriminales han tenido como objetivo a equipos con software sin actualizar y los han comprometido con el malware Simda. Este malware reenruta el tráfico en Internet del usuario a sitios web que se encuentran bajo el control de criminales o pueden ser utilizados para instalar malware.

Los responsables del software malicioso controlan la red del sistema comprometido a través de puertas traseras, dándoles acceso remoto para realizar ataques adicionales o de "vender" el control de la botnet a otros criminales. Las puertas traseras también transforman su presencia cada determinada hora, lo que permite bajas tasas de detección de los antivirus y medios para el funcionamiento sigiloso.

2. Impacto

Un sistema infectado con Simda quizá permita a los cibercriminales recolectar las credenciales del usuario, incluyendo información bancaria; instalar malware adicional; o causar algún ataque malicioso. La amplitud de sistemas infectados pemite a los operadores de Simda tener la flexibilidad para cargar características personalizadas y adaptarlas a objetivos específicos.

3. Solución

Utilizar y dar mantenimiento al antivirus. El antivirus reconoce y protege al equipo contra los virus más conocidos. Es importante mantener su antivirus actualizado (consulte Descripción de Software Antivirus para más información).

Cambie sus contraseñas. Las contraseñas originales quizá han sido comprometidas durante la infección, por lo que debe de cambiarlas (consulte Selección y protección de contraseñas para obtener más información).

Mantenga su sistema operativo y software de aplicación actualizado. Instale las actualizaciones de software para que los atacantes no puedan tomar ventaja de problemas conocidos o vulnerabilidades. Muchos sistemas operativos ofrecen actualizaciones automáticas. Si esta opción está disponible, debe habilitarla (consulte Descripción de parches para obtener más información).

Utilice herramientas antimalware. El uso de un programa legítimo que identifica y elimina el malware puede ayudar a eliminar una infección. Los usuarios pueden considerar el empleo de una herramienta de remediación (ejemplos abajo) que le ayudará con la eliminación de Simda de su sistema.

Kaspersky Lab: http://www.kaspersky.com/security-scan

Microsoft: http://www.microsoft.com/security/scanner/en-us/default.aspx

Trend Micro: http://housecall.trendmicro.com/

Compruebe si su sistema está infectado. El siguiente enlace ofrece una revisión simplificada para principiantes y una comprobación manual para expertos.

Cyber Defense Institute: http://www.cyberdefense.jp/simda/

4. Referencias

- https://www.us-cert.gov/ncas/alerts/TA15-105A
- http://www.interpol.int/en/News-and-media/News/2015/N2015-038
- http://blogs.technet.com/b/mmpc/archive/2015/04/12/microsoft-partners-with-interpol-industry-to-disr
- http://arstechnica.com/security/2015/04/botnet-that-enslaved-770000-pcs-worldwide-comes-crashing-

La Subdirección de Seguridad de la Información/UNAM-CERT agradece el apoyo en la elaboración ó traducción y revisión de éste Documento a:

- Edgar Israel Rubi Chavez (erubi at seguridad dot unam dot mx)
- Manuel Ignacio Quintero Martínez (mquintero at seguridad dot unam dot mx)

UNAM-CERT
Equipo de Respuesta a Incidentes UNAM
Subdirección de Seguridad de la Información

incidentes at seguridad.unam.mx
phishing at seguridad.unam.mx
http://www.cert.org.mx
http://www.seguridad.unam.mx
ftp://ftp.seguridad.unam.mx
Tel: 56 22 81 69
Fax: 56 22 80 47