Boletin de Seguridad UNAM-CERT-2014-006 Malware GameOver Zeus P2P

GameOver Zeus (GOZ), una variante peer-to-peer de la familia Zeus del malware bancario utilizado para el robo de credenciales identificado en septiembre de 2011, [1] utiliza una infraestructura de red descentralizada de equipos personales comprometidos y servidores web usados para enviar señales de mando y control (command and control). El Departamento de Seguridad Interna (por sus siglas en inglés DHS) de Estados Unidos, en colaboración con la Buró Federal de Investigación (FBI) y el Departamento de Justicia (DOJ), publican esta Alerta Técnica para proporcionar información complementaria acerca de la botnet GameOver Zeus.

- **Fecha de Liberación:** 2-Jun-2014
- **Ultima Revisión:** 25-Sep-2014
- **Fuente:** us-cert.gov
- **Problema de Vulnerabilidad** Local y remoto

1. Descripción

GameOver Zeus (GOZ), usualmente se propaga mediante el envío de correos spam y phishing, es usado principalmente por cibercriminales para recolectar información bancaria, como son las credenciales de inicio, en los equipos de las víctimas. [2] Los sistemas infectados también pueden ser usados para realizar otras actividades maliciosas, como el envió de correo spam o participar en ataques distribuidos de denegación de servicio (DDoS).

Las versiones anteriores del malware Zeus utilizaban un servidor centralizado para el envío de mensajes de mando y control (C2) de la red de equipos infectados para ejecutar comandos en los equipos remotos. Los servidores centralizados C2 son continuamente rastreados y bloqueados por la comunidad de seguridad. [1] GOZ, sin embargo, utiliza redes punto a punto de hosts infectados para comunicarse y distribuir datos, además de utilizar comunicaciones cifradas para evadir la detección. Los equipos que son parte de la red Zeus actúan como una red proxy masiva que es utilizada para propagar actualizaciones del malware, distribuir archivos de configuración y enviar datos robados. [3] Sin ningún punto de falla, de la red P2P de GOZ dificulta más los esfuerzos por desactivar la red. [1]

2. Impacto

Un sistema infectado con GOZ puede ser empleado para enviar correos spam, participar en ataques de tipo DDoS, recolectar información de las credenciales de los usuarios de distintos servicios en línea, incluyendo servicios bancarios.

3. Solución

Se recomienda a los usuarios tomar las siguientes acciones para remediar infecciones por GOZ:

Usar y actualizar software antivirus. El software antivirus reconoce y protege los equipos de cómputo contra los virus más conocidos. Es importante mantener el software antivirus actualizado (ver Entendiendo el software antivirus para más información).

Cambia tus contraseñas. Es posible que las contraseñas que has utilizado fueran comprometidas durante la infección, así que deberías cambiarlas (ver Escogiendo y protegiendo contraseñas para más información).

Mantén tú sistema operativo y las aplicaciones instaladas actualizadas. Instalar los parches software evita que los atacantes puedan tomar ventaja de problemas conocidos o vulnerabilidades. Muchos sistemas operativos ofrecen actualizaciones automáticas. Si esta opción está disponible, tú debes de activarla (ver Entendiendo los parches para software para más información).

Usa herramientas anti malware. Usar un programa legítimo que identifique y remueva malware puede ayudar a eliminar la infección. Los usuarios pueden considerar emplear una herramienta de reparación (ejemplos en la parte inferior) que pueden ayudar a remover GOZ de su sistema.

F-Secure
http://www.f-secure.com/en/web/home_global/online-scanner (Windows Vista, 7 y 8)
http://www.f-secure.com/en/web/labs_global/removal-tools/-/carousel/view/142 (Windows XP)

Heimdal
http://goz.heimdalsecurity.com/ (Microsoft Windows XP, Vista, 7, 8 y 8.1)

McAfee
www.mcafee.com/stinger (Windows XP SP2, 2003 SP2, Vista SP1, 2008, 7 y 8)

Microsoft
http://www.microsoft.com/security/scanner/en-us/default.aspx (Windows 8.1, Windows 8, Windows 7, Windows Vista, y Windows XP)

Sophos

http://www.sophos.com/VirusRemoval (Windows XP (SP2) y posteriores)

Symantec
http://www.symantec.com/connect/blogs/international-takedown-wounds-gameover-zeus-cybercrime-network (Windows XP, Windows Vista y Windows 7)

Trend Micro
http://www.trendmicro.com/threatdetector (Windows XP, Windows Vista, Windows 7, Windows 8/8.1, Windows Server 2003, Windows Server 2008, y Windows Server 2008 R2)

Lo anterior son ejemplos y no es una lista exhaustiva. El Gobierno de los E.U.A. no apoya ni respalda ningún tipo de producto o vendedor en particular.

GOZ ha sido asociado con el malware CryptoLocker. Para más información de este malware, por favor visitar la página Infecciones por Ransomware CryptoLocker.

Referencias

[1] Botnes P2P altamente persistentes están aquí: Un análisis de Gameover Zeus
[2] Malware Enfocado a Cuentas Bancarias

[3] El ciclo de vida de Zeus (Gameover) P2P

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

- Fausto Perez (fperez at seguridad dot unam dot mx)
- José Roberto Sánchez Soledad (rsanchez 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