BOLETIN DE ALERTA

Boletin Nro.: 2014-04

Fecha de publicación: 03/06/2014

Tema: GameOver Zeus P2P Malware

Descripción:
GameOver Zeus (GOZ) es una variante peer-to-peer (P2P) de la conocida familia de malware de robo de credenciales bancarias Zeus (Trojan.Zbt), que ha sido identificada en Setiembre de 2011. Esta nueva variante utiliza una infraestructura de red descentralizada de computadoras personales y servidores web para ejecutar comandos y controles de forma remota, formando una botnet. El GOZ malware afecta a los siguientes sistemas:

- Microsoft Windows 95, 98, Me, 2000, XP, Vista, 7, and 8
- Microsoft Server 2003, Server 2008, Server 2008 R2, and Server 2012

El malware GOZ se propaga generalmente a través de correos spam y mensajes de phishing y es utilizada principalmente por ciberdelincuentes para acceder a información bancaria, tales como credenciales de acceso (usuario, contraseña, número de cuenta, etc) de la computadora de la víctima, las cuales se utilizan en actividad fraudulenta en tiempo real. Esto lo logra a través de la técnica Man-in-the-Browser (MitB), robando las sesiones de usuario cuando éste navega por la web. También puede saltarse la autenticación de dos factores y desplegar mensajes fraudulentos para obtener información.
Los sistemas infectados pueden ser utilizados también para otras actividades maliciosas, tales como envío de spam, ataques de Denegación de Servicios Distribuida (DDoS), entre otras.
Anteriores versiones de Zeus utilizaban una infraestructura de botnet centralizada del tipo comando-control (C2) para ejecutar comandos. Los servidores centralizados C2 son normalmente rastreados y bloqueados por los organismos de seguridad. Sin embargo, la nueva variante GOZ utiliza una red P2P de equipos infectados para comunicarse y distribuir datos y utiliza encriptación para evadir la detección. Los pares actúan como una red proxy masiva que es utilizada para propagar actualizaciones binarias, distribuir archivos de configuración y para enviar datos robados.
Sin un punto de fallo único, la resistencia de la infraestructura P2P GOZ dificulta que ésta sea desactivada.
Recientemente en 2014, GOZ adoptó un driver de bajo nivel que previene que sea desinstalado fácilmente, agregando una capa adicional de resistencia.

Impacto:
Un sistema infectado por GOZ puede ser utilizado para enviar spam, participar de un ataque de denegación de servicio distribuido (*DDoS*) y puede sufrir el robo de credenciales, incluidas las credenciales para servicios bancarios.

Solución:

- Se recomienda a todos los usuarios de equipos tomar las siguientes medidas de prevención: usar y mantener actualizado un antivirus. Los antivirus reconocen y protegen el equipo de muchos virus conocidos. Es importante mantener siempre el antivirus actualizado.
- Cambiar las contraseñas: en caso de haber sido infectado, es muy probable que sus credenciales hayan sido comprometidas durante la infección, por lo que deben cambiarse por una nueva contraseña. Es importante elegir una contraseña sea robusta, así como también cambiar las contraseñas regularmente.
- Mantener el Sistema Operativo y las aplicaciones actualizados: instale siempre los parches de actualización de modo a prevenir que atacantes puedan aprovechar las vulnerabilidades conocidas. Muchos sistemas operativos y aplicaciones ofrecen actualizaciones automáticas. Si esta opción está disponible es recomendable activarla.
- Utilice herramientas anti-malware: para eliminar infecciones se recomienda la utilización de programas que identifiquen y remuevan malware. A continuación se expone una lista de herramientas que pueden ayudar a la remoción del malware GOZ de sus sistemas:

    - http://www.symantec.com/security_response/writeup.jsp?docid=2014-052915-1402-99
    - http://goz.heimdalsecurity.com/
    - http://www.f-secure.com/en/web/home_global/online-scanner
    - http://www.f-secure.com/en/web/labs_global/removal-tools/-/carousel/view/142
    - http://www.microsoft.com/security/scanner/en-us/default.aspx
    - http://www.sophos.com/en-us/products/free-tools/virus-removal-tool.aspx
    - http://about-threats.trendmicro.com/us/webattack/3136/GOZ%20and%20CryptoLocker%20Malware%20Affecting%20Users%20Globally

OBS.: Dicha lista solo incluye algunas de las herramientas existentes.

Información adicional:

- http://www.seguridad.unam.mx/noticia/?noti=1517
- http://www.secureworks.com/cyber-threat-intelligence/threats/The_Lifecycle_of_Peer_to_Peer_Gameover_ZeuS/
- http://www.fbi.gov/news/stories/2014/june/gameover-zeus-botnet-disrupted
- http://www.symantec.com/connect/blogs/international-takedown-wounds-gameover-zeus-cybercrime-network
- http://www.syssec-project.eu/m/page-media/3/zeus_malware13.pdf

CERT-PY Equipo de Respuesta ante Emergencias Cibernéticas (CERT-py)
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Mcal. Estigarribia 1349 c/Curupayty
cert@cert.gov.py | +595 21 217 9000 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py