

News Release

For Immediate Release

Estudio independiente de Georgia Tech revela cuáles son las mejores formas de decir a los clientes que sus máquinas están infectadas con un programa bot

SAN FRANCISCO, CA--(Marketwire - February 21, 2013) - Un programa robot (bot) que se cree ha producido ganancias netas ilícitas de USD 14 millones ha sido convertido en una oportunidad excelente de aprendizaje, brindando información importante sobre la mejor forma en que la comunidad en línea puede ayudar y alertar a clientes con sistemas infectados. Este martes, investigadores de Georgia Tech anunciaron los resultados de un estudio basado en la respuesta de la industria al troyano cambiador de DNS y ofrecieron las recomendaciones para ayudar a restringir futuros brotes de malware durante la vigésimo séptima Reunión General de la M3AAWG en San Francisco. El estudio de remediación del cambiador de DNS identificó llamadas telefónicas, notificaciones en la facturación y redireccionamiento de usuarios a páginas web configuradas a medida entre los métodos más efectivos para notificar a los clientes que sus sistemas estaban infectados. Los investigadores Wei Meng y Ruian Duan, trabajando bajo la supervisión del profesor de la Facultad de Ciencias de Computación de Georgia Tech, Wenke Lee, determinaron también que las advertencias "activas" en las redes sociales eran útiles para posibilitar la remediación. Con este enfoque, sitios como Google informaron directamente a los usuarios que sus máquinas habían sido infectadas a través de las ventanas de los navegadores, una táctica que demostró ser más efectiva para motivar a los usuarios a que sanearan sus sistemas que las advertencias pasivas emitidas en mensajes generales o nuevos artículos en plataformas de redes sociales.

"Las redes sociales pueden tener un rol importante en alertar a los usuarios sobre infecciones en sus sistemas y en detener brotes de malware. Creemos en la importancia de implementar notificaciones activas y directas en una etapa temprana del proceso", indicó Lee.

Los investigadores observaron tanto a diversos tipos de alertas a usuarios finales como a los esfuerzos de los operadores de red para ayudar a los clientes a sanear sus sistemas, incluyendo el uso de jardines vallados (walled gardens), redireccionamiento de DNS, programas anti-virus y herramientas para eliminar malware. Parte del desafío que enfrenta la industria con los programas bot radica en determinar cómo notificar a los usuarios de una manera oportuna y creíble que sus sistemas han sido comprometidos, para luego ayudar a los clientes que carecen de formación técnica a que saneen sus máquinas, de acuerdo con el presidente conjunto del M3AAWG, Michael O'Reirdan.

O'Reirdan indicó, "La respuesta de la industria al malware cambiador de DNS mostró claramente cuán bien los competidores y proveedores pueden trabajar en conjunto cuando la seguridad de los usuarios está en juego. Fue también una oportunidad extraordinaria para estudiar objetivamente los distintos enfoques que han desarrollado las empresas a fin de ayudar a los clientes y entender el importante rol que cada uno de nosotros desempeña en salvaguardar la experiencia de navegar en internet. La participación activa de proveedores de anti-malware y de herramientas de seguridad, agencias del cumplimiento de la ley, proveedores de sistemas operativos y de tecnología de redes para el hogar ha demostrado ser crucial. En última instancia, se requiere del trabajo conjunto de todo el ecosistema de internet para proteger a los usuarios finales.

Los datos utilizados en el estudio para determinar los índices de infección y limpieza los suministraron de forma anónima los principales ISP de alrededor del mundo a través de Grupo de Trabajo del Cambiador DNS (DCWG) al equipo de investigación en el Centro de Seguridad de la Información en Georgia Tech (GTISC). A fin de identificar los distintos tipos de técnicas de notificación y mediación utilizados, los investigadores enviaron cuestionarios donde

preguntaban cómo habían alertado a los usuarios que habían sido infectados con el malware cambiador de DNS y los detalles específicos sobre los esfuerzos de remediación empleados por cada ISP para ayudar a los clientes a limpiar sus máquinas. Un ISP que no tomó ninguna acción en respuesta al malware se convirtió en el punto de referencia para medir la efectividad de los otros enfoques, de acuerdo con Lee.

Desde 2007 hasta 2011, el troyano cambiador de DNS secuestró búsquedas en internet y reencaminó los navegadores de Web de computadoras infectadas hacia sitios fraudulentos utilizando los servidores DNS ilegales operados por Rove Digital. No obstante, si los servidores de DNS ilegales se hubiesen apagado cuando fueron arrestados los estonios supuestamente responsables, los usuarios finales infectados no habrían podido acceder a la Web. El DCWG fue un grupo formado para ayudar al organismo encargado del cumplimiento de la ley a tratar con los problemas potenciales de los usuarios finales que surgirían de las acciones tomadas por este cuerpo de seguridad. El DCWG también ayudó a operar y monitorear los servidores DNS "limpios" que fueron operados legalmente por el Internet Systems Consortium (ISC) de conformidad con una orden judicial desde noviembre de 2011 a julio de 2012. Como resultado, en lugar de perder repentinamente el acceso a internet, millones de usuarios fueron notificados que sus máquinas habían sido infectadas y que era necesario sanearlas.

El Estudio completo de remediación del cambiador DNS está disponible en el sitio web del M³AAWG en https://www.maawg.org/sites/maawg/files/news/GeorgiaTech_DNSChanger_Study-2013-02-19.pdf.

Acerca del Grupo de Trabajo Anti-Abuso de Mensajes, Malware y Móvil (M³AAWG)

El Grupo de Trabajo Anti-Abuso de Mensajes, Malware y Móvil (M³AAWG) es donde se une la industria para trabajar contra los bots, malware, spam, virus, ataques de rechazo de servicios y otras formas de explotación en línea. M³AAWG (www.M3AAWG.org) representa más de mil millones de casillas de mensajes de algunos de los principales operadores de redes en el mundo. Aprovecha el alcance y experiencia de sus socios globales para abordar el abuso en las redes existentes y nuevos servicios emergentes a través de tecnología, colaboración y políticas públicas. También trabaja para educar a los formuladores de políticas globales sobre los asuntos técnicos y operacionales relacionados con el abuso y mensajes en línea. M³AAWG con sede en San Francisco, California, es un foro abierto impulsado por las necesidades del mercado y respaldado por los principales operadores de redes y proveedores de mensajes.

Directorio de M³AAWG: AT&T (NYSE: [T](#)); Cloudmark, Inc.; Comcast (NASDAQ: [CMCSA](#)); Constant Contact (NASDAQ: [CTCT](#)); Cox Communications; Damballa, Inc.; Eloqua; Facebook; France Telecom (NYSE y Euronext: FTE); Google; PayPal; Return Path; Symantec; Time Warner Cable; Verizon Communications y Yahoo! Inc.

Socios plenos de M³AAWG: 1&1 Internet AG; Adaptive Mobile Security LTD; Adobe Systems Inc.; AOL; BAE Systems Detica; Cisco Systems, Inc.; Dynamic Network Services Inc.; Email Sender and Provider Coalition; Genius; iContact; Internet Initiative Japan (IJI NASDAQ: [IJIJ](#)); Mailchimp; McAfee Inc.; Message Systems; Mimecast; Nominum, Inc.; Proofpoint; Scality; Spamhaus; Sprint; y Twitter.

La lista completa de los socios está disponible en <http://www.m3aawg.org/about/roster>.

Contacto con los medios:

Linda Marcus, APR. 1+714-974-6356, LMarcus@astra.cc, Astra Communications
