Telefónica

INSIDE ELECTIONS_

Amenazas al proceso electoral alemán

21.09.2017

CYBER SECURED BY ElevenPaths

elevenpaths.com

Amenazas al proceso electoral alemán

Visión del analista

En los últimos meses, distintas instituciones gubernamentales de Alemania habrían sido objetivo de diferentes tipos de ciberataques perpetrados por actores como APT28. En este sentido, se habría identificado un repunte durante los meses de agosto y septiembre de las sesiones activas del *malware* asociados a las herramientas utilizadas por este grupo entre las que se ha encontrado al menos una cuyo objetivo concreto eran instituciones gubernamentales de Alemania. Dada la naturaleza de las evidencias encontradas, existe riesgo real de que la información potencialmente sustraída a actores políticos en Alemania puede ser utilizada en el marco de las próximas elecciones. Por otro lado, se han detectado otras muestras genéricas con capacidades de robo de información, control de los sistemas infectados y diferentes implementaciones para atacar plataformas Windows, Mac y Android. Según el grupo de trabajo desarrollado por East StratCom de la Unión Europea, también se han reportado operaciones de desinformación por la gestión de la crisis de los refugiados, así como contra soldados alemanes durante su estacionamiento en Lituania como parte de la OTAN presuntamente vinculadas a acciones del gobierno ruso en el ciberespacio.

Principales claves del país

Nombre oficial	República Federal de Alemania
Capital	Berlín
Idioma oficial	Alemán
Religión	Estado aconfesional
Forma de Estado	**Estado federal Democrático Social y de Derecho.** El Presidente Federal es el jefe del Estado, elegido durante 5 años. El **Bundestag** (Cámara baja) representa al pueblo alemán. El **Bundesrat** (Consejo Federal) es la cámara de representación de los Estados Federados.
Principales temas de actualidad	Negociación sobre el programa «Diseñar el futuro de Alemania». Cuestiones en materia de energía. Construcción del proyecto europeo en el que Alemania es uno de los principales actores. Crisis de los refugiados.

Las referencias regionales para Alemania se centran en:

La relación con **Estados Unidos** es uno de sus pilares de su política exterior, especialmente en el aspecto de la seguridad y la defensa.

Alemania es considerado un interlocutor válido en las relaciones con Rusia. Sin embargo, ha sido criticada por Moscú por la crisis de Ucrania.

Se han intensificado las inversiones con **Brasil** y **México**, así como con **China**.

Alemania desempeña un papel cada vez más relevante en el continente africano. Su influencia es cada vez más creciente en la zona del **Mashrek** y en el **Magreb**.

Tipos de amenazas identificadas

Amenazas atribuidas a agentes externos

Alemania ha sufrido con anterioridad ataques a diversas infraestructuras políticas, principalmente atribuidas al grupo APT28 (también denominado Pawn Storm, Fancy Bear, Sofacy Group y Strontium). En este sentido, en junio de 2015, la Oficina Federal Alemana para la Seguridad en las Tecnologías de la Información (BSI, por sus siglas en alemán) confirmó que varios partidos políticos habían sido objetivo de ataques de *phishing*. De la misma manera, el jefe de la agencia de inteligencia doméstica atribuyó también el compromiso en ese mismo mes de las redes del Bundestag a este grupo [1].

Paralelamente, investigadores de TrendMicro identificaron en abril y mayo de 2016 que este mismo grupo habría creado servidores de correo falsos para lanzar campañas de *phishing* contra miembros del partido político Unión Demócrata Cristiana (CDU, por sus siglas en alemán) y así obtener credenciales y acceso a sus cuentas [2]. A pesar de que las autoridades alemanas confirmaran que el ataque había sido realizado por Pawn Storm, se desconoce si llegaron a tener éxito ya que hasta la fecha no se han filtrado correos electrónicos. Algunos expertos afirman que la información potencialmente sustraída podría tener un objetivo concreto como influenciar las elecciones alemanas del próximo 24 de septiembre, de forma similar a como se trató de hacer con las estadounidenses.

Por otro lado, la compañía de ciberseguridad Fireeye ya habría publicado a principios de este año un informe donde resaltaba la *suite* de *malware* utilizada por dicho grupo, entre las que se encuentran las siguientes herramientas: Chopstick, Eviltoss, Gamefish, Sourface, Oldbait y Coreshell. Según las bases de datos de amenazas de las que dispone ElevenPaths, se habría identificado en los meses de agosto y septiembre de 2017 un repute en el número de sesiones activas vinculadas a estas amenazas (1 476 y 7 825 sesiones, respectivamente), tal y como se muestra en la Figura 1.

Entre todas las muestras de *malware*, una de ellas estaría utilizando Coreshell y habría afectado a organizaciones gubernamentales en Alemania.

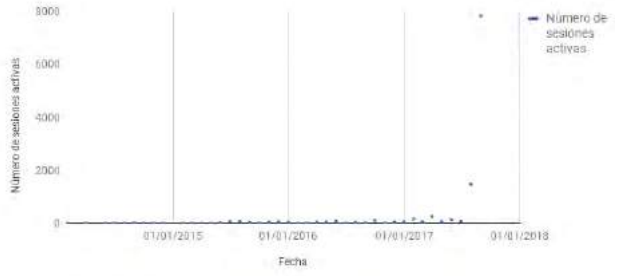

Figura 1. Número de sesiones activas de las piezas de *malware* vinculadas a la suite de herramientas utilizadas por APT28

Coreshell es un *downloader* que descarga en una segunda fase un *backdoor* desde un C2. Este *downloader*, con el tiempo ha evolucionado desde Sourface a versiones más recientes de Coreshell, normalmente compiladas en una DLL (coreshell.dll).

Utiliza dos subprocesos para comunicarse con su C2. El primero envía *beacons* que contienen la lista de procesos del *host* comprometido y el segundo es responsable de descargar y ejecutar dos *payloads*. Los mensajes son enviados utilizando peticiones HTTP POST cuya información se encuentra codificada en Base64 y además cifrada. En cuanto al método utilizado, usa un algoritmo de flujo personalizado con una clave de seis bytes. Los comandos desde el C2 hasta los *implants* de Coreshell usan otro tipo de cifrado de flujo, pero esta vez utilizan una clave de ocho bytes.

Coreshell ha usado el mismo *user-agent string* ("MSIE 8.0") que Sourface utilizó anteriormente, pero en muestras más recientes Coreshell utiliza el *user-agent string* de Internet Explorer.

Desde otro punto de vista, también se han identificado otras familias de *malware* más genérico y no asociado a grupos conocidos o al menos no atribuidos a ellos como parte de su arsenal de herramientas actual. Entre ellas se han encontrado distintos tipos de *malware* con capacidades de robo de información, control de los sistemas infectados y diferentes implementaciones para atacar plataformas Windows, Mac y Android.

También se han identificado ficheros ejecutables, documentos de texto y ficheros .pdf con *exploits* embebidos, *exploit kits*, Flash y aplicaciones

desarrolladas en Java. A continuación se enumeran algunas muestras que estarían afectando a sedes gubernamentales alemanas son las siguientes:

- NetWireRAT. Herramienta de administración remota (RAT) que es utilizada comúnmente por muchos tipos de atacantes para tomar el control remoto sobre un sistema.
- DarkComet. RAT utilizado por muchos tipos de atacantes proporcionando control completo sobre el sistema infectado.
- Adwind. RAT en Java que se ha distribuido como servicio.
- GearInformer. Se trata de una versión actualizada y renombrada del *keylogger* iSpy.
- H1N1. *Downloder* que afecta a Windows. Este *malware* envía información del sistema y acepta los comandos de un servidor de control. Los comandos compatibles permitirían descargar y ejecutar archivos en el sistema infectado. El *malware* inyecta sus *payloads* en procesos legítimos para ocultar sus actividades.
- KeyBase. *Keylogger* que también viene equipado con robo de credenciales y funcionalidad de visualización de sitios web.
- MagnitudeEKFlashContainer. Muestra provista por el *exploit kit* Magnitude que explota versiones de Adobe Flash Player.
- Matsnu. Un *infector* x86 que actúa como *backdoor* una vez que se tiene acceso al sistema con capacidad de cargar y ejecutar cualquier código en el sistema pudiendo cifrar archivos o robar datos confidenciales.
- NanoCoreRAT. Troyano que abre una puerta trasera y roba información del equipo comprometido. También permitiría a un atacante ejecutar varios comandos en el sistema infectado.
- NeutrinoEKExploitsFlashContainer. Archivos de Flash utilizados como parte del *exploit kit* Neutrino.
- PredatorPain. Troyano destinado al robo de información capaz de capturar contraseñas, pulsaciones de teclado, capturas de pantalla y otra información sensible.
- Recslurp. Troyano con capacidad para sustraer credenciales FTP y exfiltrar a un servidor remoto.
- SundownEKFlashContainer. Archivos de Flash que descargan *malware* en el equipo de la víctima como parte del *exploit kit* Sundown.
- Ursnif. *Stealer* y *downloader* con capacidades de robar información de navegadores y otras aplicaciones como Microsoft Outlook. También tiene la capacidad de descargar componentes maliciosos adicionales de servidores de C2 del atacante y cargarlos dinámicamente en memoria.
- Zincite. *Backdoor* instalado comúnmente por el gusano Mydoom.
- RTF-OLE-Exploit. Técnica multiexplotación que suele verse en *exploits* de HTML o JavaScript, pero rara vez en *exploits* de RTF o de Office. Las vulnerabilidades que explota son las siguientes: CVE-2012-0158, CVE-2012-2539, CVE-2014-1761 y CVE-2015-1641.

El rango temporal en la que se sitúan estas amenazas es desde enero del 2015 hasta las más recientes detectadas durante el desarrollo de esta investigación en septiembre de 2017. Por su parte, los vectores de infección han sido el correo electrónico, la navegación web, Flash, FTP, Owncloud y Mediafire.

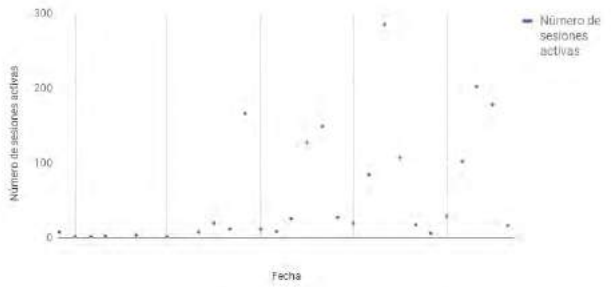

Figura 2. Número de sesiones activas de piezas de *malware* genérico con impacto en instituciones gubernamentales alemanas.

Por otro lado, según el gobierno alemán, también se han detectado operaciones de propaganda y desinformación procedentes de medios de comunicación rusos similares a los identificados en las elecciones de Estados Unidos y de Francia. En este sentido, el grupo de trabajo East StratCom de la Unión Europea, creado en 2015 para combatir las campañas de desinformación del gobierno ruso, descubrió que la canciller Angela Merkel estaba siendo objetivo constante de este tipo de ataques debido a su política hacia los refugiados [3]. Otro caso estaría relacionado con unos correos electrónicos enviados a medios de comunicación sobre el «Caso Lisa» en donde soldados alemanes habrían sido acusados de violación durante

su estacionamiento en Lituania como parte de las fuerzas militares de la OTAN [4].

Amenazas atribuidas a agentes internos

A finales de 2011, se publicó en la Chaos Computer Club [5], una de las conferencias más importantes de seguridad a nivel internacional, el troyano R2D2 (denominado también como Ozapftis o Bundestrojaner) que estarían utilizando las fuerzas y cuerpos de seguridad alemanas para interceptar las comunicaciones. Entre las capacidades de esta herramienta se incluyen las de interceptar las comunicaciones de Skype, MSN Messenger y Yahoo Messenger, registrar las pulsaciones del teclado en Firefox, Opera, Internet Explorer y SeaMonkey, tomar capturas de pantalla de las pantallas de los usuarios y comunicarse con un sitio web de forma remota [6]. No se han podido identificar apariciones más recientes de amenazas similares.

Bibliografía

[1] «APT28: At the Center of the Storm « Threat Research Blog», *FireEye*, 11-ene-2017. [En línea]. Disponible en: https://www.fireeye.com/blog/threat-research/2017/01/apt28_at_the_center.html. [Accedido: 18-sep-2017].

[2] Trend Micro, «Two Years of Pawn Storm. Examining an Increasingly Relevant Threat», Research Paper, 2017.

[3] AFP, «Merkel faces more Russian disinformation ahead of poll: source», *Yahoo News*, 23-ene-2017. [En línea]. Disponible en: https://www.yahoo.com/news/merkel-faces-more-russian-disinformation-ahead-poll-source-201147963.html. [Accedido: 18-sep-2017].

[4] D. Welle (www.dw.com), «Why the "fake rape" story against German NATO forces fell flat in Lithuania | Europe DW | 23.02.2017», *DW.COM*, 23-feb-2017. [En línea]. Disponible en: http://www.dw.com/en/why-the-fake-rape-story-against-german-nato-forces-fell-flat-in-lithuania/a-37694870. [Accedido: 18-sep-2017].

[5] «CCC | Chaos Computer Club analyzes government malware». [En línea]. Disponible en: https://ccc.de/en/updates/2011/staatstrojaner. [Accedido: 18-sep-2017].

[6] «'Government' backdoor R2D2 Trojan discovered by Chaos Computer Club», *Naked Security*, 09-oct-2011. .

Acerca de ElevenPaths

En ElevenPaths creemos en la idea de desafiar el estado actual de la seguridad, característica que debe estar siempre presente en la tecnología. Nos replanteamos continuamente la relación entre la seguridad y las personas con el objetivo de crear productos innovadores capaces de transformar el concepto de seguridad y de esta manera, ir un paso por delante de nuestros atacantes, cada vez más presentes en nuestra vida digital.

Más información

www.elevenpaths.com

@ElevenPaths

blog.elevenpaths.com