KASPERSKY lab

Kaspersky: Boletín de seguridad

PRINCIPALES HISTORIAS DE SEGURIDAD EN 2018

David Emm, Victor Chebyshev

CONTENTS

INTRODUCCIÓN

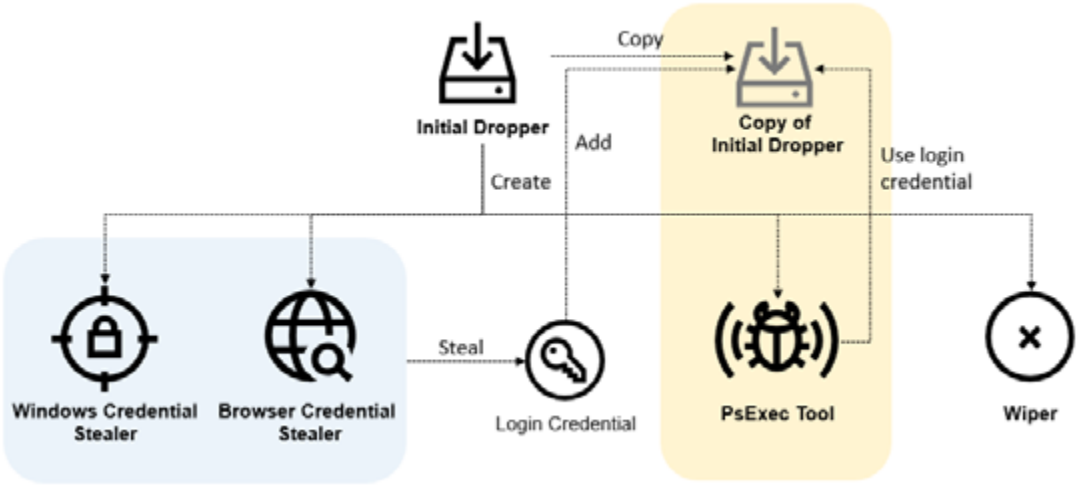
Internet está presente en cada aspecto de nuestra vida cotidiana. Mucha gente realiza sus transacciones bancarias, sus compras y socializa de forma virtual: Internet es la savia de las organizaciones comerciales. La dependencia tecnológica que tienen los gobiernos, empresas y consumidores otorga una amplia superficie de ataques con todo tipo de motivaciones: robos de dinero y de datos, trastornos, daños, daños a la reputación, o simplemente "por diversión". El resultado es un panorama de ciberamenazas que va desde ataques selectivos ultra sofisticados hasta la ciberdelincuencia oportunista. Con demasiada frecuencia, ambas formas se basan en la manipulación sicológica de los usuarios para infectar computadoras personales o sistemas enteros. Cada vez más, entre los dispositivos atacados figuran aquellos que no consideramos como computadoras: desde juguetes para niños hasta cámaras de seguridad. Este es nuestro resumen anual de los principales incidentes y las principales tendencias en 2018.

CAMPAÑAS DE ATAQUES SELECTIVOS

En la Cumbre de Analistas de Seguridad de Kaspersky, llevada a cabo este año, informamos sobre Slingshor, una sofisticada plataforma de ciberespionaje que desde 2012 se cobra víctimas en Medio Oriente y África. Descubrimos esta amenaza, que compite con Regin y ProjectSauron por su complejidad, durante la investigación de un incidente. Slingshot emplea un inusual (y hasta donde sabemos, único) vector de ataque: muchas de sus víctimas fueron atacadas mediante enrutadores MikroTik infectados. Aún no está claro el método exacto que se usó para infectar los enrutadores, pero los atacantes han encontrado una manera de agregar una DLL maliciosa a estos dispositivos: se trata de una DLL que descarga otros archivos maliciosos que luego se guardan en el enrutador. Cuando un administrador del sistema inicia sesión para configurar el enrutador, el software de administración del enrutador descarga y ejecuta un módulo malicioso en la computadora del administrador. Slingshot carga varios módulos en la computadora de la víctima, pero los más notables son Cahnadr, un módulo de modo kernel, y GollumApp, un módulo de modo de usuario. Juntos, permiten mantener persistencia, administrar el sistema de archivos, extraer datos y comunicarse con un servidor de comando y control (C&C). Las muestras que observamos estaban marcadas como 'version 6.x', lo que sugiere que la amenaza ha estado activa por bastante tiempo. El tiempo, la habilidad y el costo necesarios para la creación de Slingshot indican que es muy probable que se trate de un grupo altamente organizado y profesional, quizás patrocinado por algún gobierno.

Poco después del inicio de los Juegos Olímpicos de Invierno en Pyeongchang, comenzamos a recibir informes de ataques de malware contra infraestructuras relacionadas con este evento. Olympic Destroyer apagó los monitores de pantalla, anuló el Wi-Fi y eliminó el sitio web de las Olimpiadas, lo que impidió que los visitantes imprimieran sus boletos. El ataque también afectó a otras organizaciones en la región; por ejemplo, las puertas de esquí y los telesquís se desactivaron en varias estaciones de esquí de Corea del Sur. Olympic Destroyer es un gusano de red, cuyo principal objetivo es destruir los archivos de sus víctimas en recursos compartidos de red remotos. En los días posteriores al ataque, los equipos de investigación y los medios de prensa de todo el mundo atribuyeron el ataque a Rusia, China y Corea del Norte, basándose en una serie de características previamente atribuidas a los grupos de ciberespionaje y sabotaje supuestamente asentados en estos países o que trabajan para los gobiernos de estos países. Nuestros propios investigadores también intentaban entender qué grupo estaba detrás del ataque.

En un momento de nuestra investigación, descubrimos algo que parecía indicar que el grupo Lazarus estaba detrás del ataque. Encontramos un rastro único dejado por los atacantes que coincidía exactamente con un componente de malware de Lazarus que ya conocíamos. Sin embargo, la falta de motivos obvios y las inconsistencias con los TTP (tácticas, técnicas y procedimientos) conocidos de Lazarus -que encontramos durante nuestra investigación in situ en una instalación comprometida en Corea del Sur- nos llevaron a estudiar de nuevo este artefacto. Cuando lo hicimos, descubrimos que el conjunto de características no coincidía con el código y que se la había forjado para que coincidiera perfectamente con la huella dactilar utilizada por Lazarus. Así que llegamos a la conclusión de que la "huella dactilar" era una bandera falsa muy sofisticada, colocada intencionalmente dentro del malware para dar a los cazadores de amenazas la impresión de que habían encontrado una evidencia indiscutible y desviarlos de una atribución más precisa.

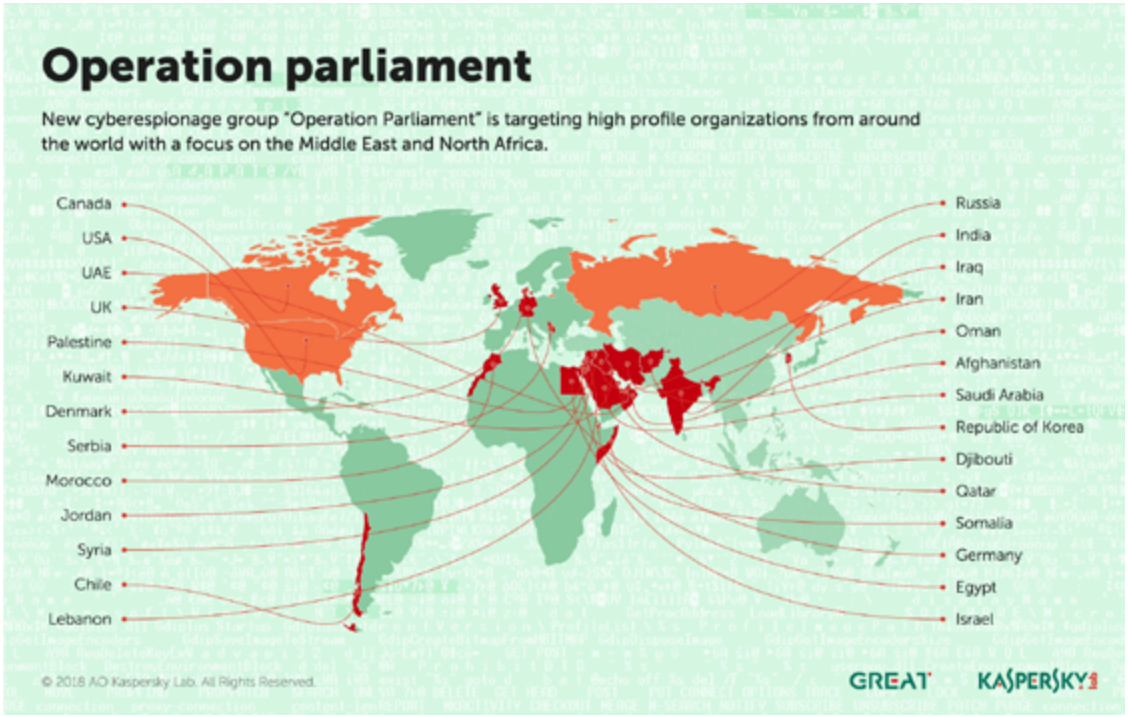


Relaciones de los componentes de OlympicDestroyer

Seguíamos la pista de las actividades de este grupo de APT cuando en junio notamos que habían lanzado una nueva campaña con una distribución geográfica distinta y con nuevos temas. Nuestra telemetría y las características de los archivos de spear-phishing que analizamos indicaban que el grupo detrás de OlympicDestroyer atacaba ahora a organizaciones financieras y relacionadas con la biotecnología con sede en Europa, específicamente en Rusia, Holanda, Alemania, Suiza y Ucrania. A los ataques iniciales de Olympic Destroyer, diseñados

para destruir y paralizar la infraestructura de los Juegos Olímpicos de invierno, así como las cadenas de aprovisionamiento, socios y sedes relacionados con el evento, les precedía una operación de reconocimiento. Esto nos llevó a pensar que estas nuevas actividades eran parte de otra etapa de reconocimiento a la que le seguiría una ola de ataques destructivos con nuevas motivaciones. La variedad de los blancos financieros y no financieros podría ser un indicio de que varios grupos con intereses diferentes estaban utilizando el mismo malware. También podría ser el resultado de la subcontratación de los ciberataques, lo cual no es inusual entre los actores de amenazas patrocinadas por gobiernos. Sin embargo, también es posible que los blancos financieros sean otra operación de bandera falsa a cargo de un actor de amenazas que ya ha demostrado su maestría en esto.

En abril informamos sobre las actividades de Operation Parliament, una campaña de ciberespionaje que tenía como blanco organizaciones judiciales, ejecutivas y legislativas de alto perfil en todo el mundo, concentrándose en Medio Oriente y el norte de África, en particular Palestina. Estos ataques, que empezaron a principios de 2017, apuntaban a parlamentos, senados, agencias y funcionarios gubernamentales de alto nivel, académicos en ciencias políticas, agencias militares y de inteligencia, ministerios, medios de comunicación, centros de investigación, comités electorales, organizaciones olímpicas, grandes compañías comerciales, y otros. La selección de víctimas, distinta a la de anteriores campañas en la región (Gaza Cybergang o Desert Falcons), sugiere un elaborado ejercicio de recopilación de información realizado antes de los ataques (físico y/o digital). Los atacantes han demostrado sumo cuidado en la verificación de los dispositivos de sus víctimas antes de proceder a infectarlos, a fin de proteger sus servidores C&C. Los ataques disminuyeron después de iniciado 2018, quizás debido a que los atacantes lograron sus objetivos.



Hemos continuado con el seguimiento a las actividades de Crouching Yeti (o Energetic Bear), un grupo de ATP activo al menos desde 2010, que apunta particularmente a compañías energéticas e industriales. Este grupo ataca a organizaciones en todo el mundo, pero concentra sus víctimas en Europa, EE.UU. y Turquía. Este último país se añadió a los intereses del grupo durante 2016-2017. Entre las principales tácticas del grupo están el envío de mensajes de correo tipo phishing con adjuntos maliciosos y la infección de servidores con diferentes propósitos, entre ellos, el de alojar herramientas, registros y ataques del tipo watering-hole. US-CERT y el Centro de Ciberseguridad Nacional del Reino Unido (NCSC) han hecho públicas las actividades de Crouching Yeti contra blancos en EE.UU. En abril, ICS CERT de Kaspersky Lab aportó datos sobre los servidores infectados identificados que Crouching Yeti utilizaba y presentó las conclusiones de un análisis de varios servidores web que este grupo infectó durante 2016 y principios de 2017. Puede leer el informe completo aquí. A continuación ofrecemos un resumen de nuestros hallazgos.

1. Con raras excepciones, los miembros del grupo se las arreglan con herramientas disponibles en el mercado. El uso de estas herramientas disponibles en el mercado para lanzar los ataques dificulta en gran medida los esfuerzos de atribución al no contar con 'marcadores' de grupo adicionales.
2. Potencialmente, cualquier servidor vulnerable en Internet interesa a los atacantes cuando quieren establecer un punto de apoyo para después lanzar ataques contra instalaciones.
3. En la mayoría de los casos que hemos observado, el grupo realizó tareas relacionadas con la búsqueda de vulnerabilidades, ganó persistencia en varios hosts y robó datos de autenticación.
4. La diversidad de las víctimas puede ser un indicio de la diversidad de los intereses de los atacantes.
5. Podemos asumir con cierto grado de certeza que el grupo opera sirviendo los intereses o siguiendo las órdenes de clientes externos al grupo, realizando la recopilación inicial de datos, robando datos de autenticación y ganando persistencia en recursos apropiados para posteriores lanzamientos de ataques.

En mayo, los investigadores de Cisco Talos publicaron los resultados de su investigación sobre VPNFilter, un malware utilizado para infectar distintas marcas de enrutadores, especialmente en Ucrania, aunque llegaron a afectar enrutadores en 54 países. Puede leer los respectivos análisis aquí y aquí. En un principio, se creía que este malware había infectado a unos 500 000 enrutadores, entre ellos equipos de red Linksys, MikroTik, Netgear y TP-Link en el sector de empresas pequeñas o domésticas, y los dispositivos de almacenamiento adjuntos a la red (NAS) de QNAP. Sin embargo, después se supo que la lista de enrutadores infectados era mucho más extensa: 75 en total, incluyendo equipos ASUS, D-Link, Huawei, Ubiquiti, UPVEL y ZTE. Este malware es capaz de bloquear el dispositivo infectado, ejecutar instrucciones de shell para su posterior manipulación, crear una configuración TOR para el acceso anónimo al dispositivo, y configurar el puerto proxy y URL proxy del enrutador para manipular las sesiones de navegación. Sin embargo, también se propaga en las redes que dependen de este dispositivo, ampliando así el alcance del ataque. Los investigadores de Global Research and Analysis Team (GReAT) de Kaspersky Lab observaron en profundidad el mecanismo del C&C que utiliza VPNFilter. Una pregunta interesante es: ¿quién está detrás de este malware? Cisco Talos indicó que el responsable es un actor de amenazas patrocinado por o afiliado a un gobierno. En su declaración para drenar el C&C, el FBI sugiere que el responsable es Sofacy (también conocido como APT28, Pawn Storm, Sednit, STRONTIUM o Tsar Team). Hay alguna superposición

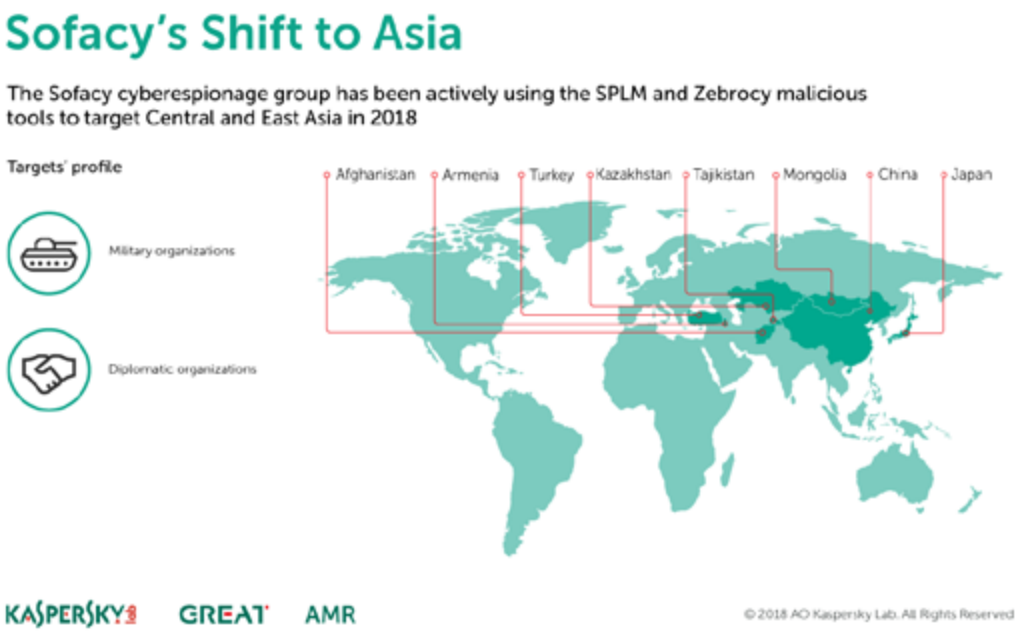
de códigos con el malware BlackEnergy utilizado en ataques anteriores en Ucrania (la declaración del FBI remarca que consideran a BlackEnergy -conocido también como Sandworm- como un subgrupo de Sofacy).

Sofacy es un grupo de ciberespionaje muy activo y prolífico que Kaspersky Lab ha estado rastreando durante muchos años. En febrero publicamos un resumen de las actividades de Sofacy en 2017, que revelan un alejamiento gradual de blancos relacionados con la OTAN a comienzos de 2017, hacia blancos en Medio Oriente, Asia Central y otras regiones. Sofacy utiliza ataques del tipo spear-phishing y water-hole para robar información, como credenciales de cuentas, comunicaciones confidenciales y documentos. Este actor de amenazas también utiliza vulnerabilidades de día cero para implementar su malware.

Sofacy usa diferentes herramientas para diferentes perfiles de blancos. A principios de 2017, la campaña del grupo Dealer's Choice se utilizó para atacar a organizaciones militares y diplomáticas (principalmente en países de la OTAN y Ucrania). Más adelante ese año, el grupo utilizó otras herramientas de su arsenal: Zebrocy y SPLM para atacar a una gama más amplia de organizaciones, incluyendo centros de ciencia e ingeniería, y servicios de prensa, con un enfoque más centrado en Asia Central y el Lejano Oriente. Al igual que otros actores de amenazas sofisticados, Sofacy mantiene un alto nivel de seguridad operativa y se esfuerza para que su malware sea difícil de detectar. Una vez que en una red se han encontrado signos de actividad de actores de amenazas avanzados como Sofacy, es importante revisar los inicios de sesión y accesos de administrador inusuales en los sistemas, escanear minuciosamente los archivos adjuntos entrantes y mantener la autenticación de dos factores para servicios como correo electrónico y acceso VPN. El uso de Informes de inteligencia sobre APTs, de herramientas de búsqueda de amenazas como YARA y de soluciones de detección avanzada como KATA (Kaspersky Anti-Targeted Attack Platform) ayuda a comprender su orientación y a proporcionar formas efectivas de detectar sus actividades.

Nuestra investigación muestra que Sofacy no es el único actor de amenazas que opera en el Lejano Oriente y esto a veces resulta en una superposición de blancos de actores de amenazas muy diferentes. Hemos visto casos en los que el malware Zebracy de Sofacy compitió por el acceso a las computadoras de las víctimas con los clústeres Mosquito Turla de habla rusa; y en los que su puerta trasera SPLM ha competido con los tradicionales ataques Danti de habla turca y china. Los objetivos compartidos incluyen organizaciones gubernamentales de

administración, tecnológicas y científicas relacionadas con el ejército en o desde Asia Central. La superposición más intrigante es probablemente la que existe entre Sofacy y el actor de amenazas de habla inglesa detrás de la familia Lamberts. Esta conexión se descubrió después de que los investigadores detectaran la presencia de Sofacy en un servidor que la inteligencia de amenazas había identificado previamente como infectada por el malware Gray Lambert. El servidor pertenece a un conglomerado chino que diseña y fabrica tecnologías aeroespaciales y de defensa aérea. Sin embargo, en este caso, el vector original de entrega de SPLM permanece desconocido. Esto plantea una serie de posibilidades hipotéticas, incluyendo el hecho de que Sofacy podría estar utilizando un exploit nuevo y aún no detectado o una nueva derivación de su puerta trasera, o que Sofacy de algún modo logró aprovechar los canales de comunicación de Gray Lambert para descargar su malware. Incluso podría ser una bandera falsa, plantada durante la infección anterior de Lambert. Creemos que la respuesta más probable es que una nueva secuencia de instrucciones desconocida de PowerShell o una aplicación web legítima pero vulnerable fue explotada para cargar y ejecutar el código SPLM.



En junio se informó sobre una campaña en curso que apuntaba a un centro nacional de datos en Asia Central. La elección de este blanco tuvo un particular significado: indica que los atacantes lograron acceder a una amplia serie de recursos gubernamentales en una sola redada. Creemos que hicieron esto mediante la inserción de una rutina en los sitios web oficiales del país para lanzar ataques del tipo watering-hole. Atribuimos esta campaña al actor de amenazas de habla china LuckyMouse (también conocido como EmissaryPanda y APT27) debido a las herramientas y tácticas utilizadas en la campaña y a que el dominio del C&C ('update.iaacstudio[.]com') fue utilizado anteriormente por este grupo y a que ya habían atacado a organizaciones gubernamentales, incluyendo aquellas en Asia Central. El vector de infección inicial utilizado en el ataque contra el centro de datos sigue siendo desconocido. Incluso cuando observamos que LuckyMouse utilizaba archivos armados con la vulnerabilidad CVE-2017-118822 (Microsoft Office Equation Editor, ampliamente usada por actores de habla china desde diciembre de 2017), no logramos probar que estaban relacionados con este ataque en particular. Es posible que los atacantes hayan utilizado un ataque del tipo watering-hole para infectar los equipos de los empleados del centro de datos.

En septiembre informamos sobre otra campaña de LuckyMouse. Desde marzo venimos encontrando varias infecciones donde un troyano anteriormente desconocido fue inyectado en la memoria de proceso del sistema 'lsass.exe'. Estos implantes fueron inyectados por el controlador NDISProxy de filtro de red 32- y 64-bitque tiene firma digital. Curiosamente, este controlador está firmado con un certificado digital que pertenece a la compañía china LeagSoft, un desarrollador de software de seguridad informática que tiene su sede en Shenzen, Guandong. Procedimos a informar a la compañía sobre este problema a través de CN-CERT. Esta campaña atacó a organizaciones gubernamentales de Asia central y creemos que el ataque estaba relacionado con una reunión de alto nivel celebrada en la región. Se estima que el tamaño del tunelizador Earthworm usado en el ataque es típico de los actores de amenazas habla china. Asimismo, una de las instrucciones que usaron los atacantes ('-s rssocks -d 103.75.190[.]28 -e 443') crea un túnel hacia un servidor C&C anteriormente conocido de LuckyMouse. La selección de las víctimas en esta campaña también se alinea con los intereses anteriormente demostrados por este actor de amenazas. No vimos ninguna indicación de actividades del tipo spear-phishing o watering-hole; creemos que los atacantes propagaron sus infecciones a través de redes que ya estaban infectadas.

Lazarus es un actor de amenazas bien establecido que ha estado lanzando campañas de ciberespionaje y cibersabotaje desde, al menos, 2009. En los últimos años, este grupo ha lanzado campañas contra organizaciones financieras en todo el mundo. En agosto informamos que este grupo había logrado infectar los sistemas de varios bancos y que se había infiltrado en varias compañías de cambio de criptomonedas y de tecnología financiera en todo el mundo. Mientras ayudábamos en la operación de respuesta a un incidente, descubrimos que la víctima había sido infectada con la ayuda de una aplicación de cambio de criptomonedas troyanizada que mediante un correo electrónico le habían recomendado a la compañía. Un desprevenido empleado había descargado una aplicación de terceros desde un sitio web aparentemente legítimo, infectando así su computadora con el malware conocido como Fallchill, una antigua herramienta que Lazarus recientemente ha vuelto a utilizar. Al parecer, Lazarus ha encontrado una forma elaborada de crear un sitio con apariencia legítima e inyectar una carga maliciosa dentro de un mecanismo "aparentemente legítimo" de actualización de software: en este caso, crear una cadena de aprovisionamiento fraudulenta en lugar de infectar una legítima. De todas maneras, el éxito del grupo Lazarus en infectar cadenas de aprovisionamiento sugiere que seguirán explotando este método de ataque. Los atacantes se esforzaron y desarrollaron malware para otras plataformas además de Windows, incluyendo una versión para Mac OS y, según el sitio web, la versión para Linux está en camino. Es probablemente la primera vez que vemos que este grupo de APT usa malware para Mac OS. Al parecer, en su búsqueda de blancos avanzados, como desarrolladores de software de cadenas de aprovisionamiento y de blancos de alto perfil, los actores de amenazas se ven obligados a desarrollar herramientas de malware para Mac OS. El hecho de que el grupo Lazarus haya ampliado su lista de sistemas operativos atacados debería alarmar a los usuarios de plataformas distintas a Windows. Puede leer nuestro informe sobre la operación AppleJeus aquí.

Turla (también conocido como Venomous Bear, Waterbug o Uroboros) adquirió fama por lo que, en ese momento fue, un rootkit Snake ultra complejo para atacar blancos relacionados con la OTAN. Sin embargo, las actividades de este actor de amenazas van mucho más allá. En octubre informamos sobre las actividades recientes del grupo Turla que revelaban una combinación llamativa de un código antiguo con uno nuevo, y surgieron nuevas especulaciones sobre cuál sería su próximo blanco y qué propagarían. Gran parte de nuestro informe de 2018 se enfocó en la puerta trasera KopiLuwak, basada en JavaScript de este grupo, en las nuevas variantes de la plataforma Carbon y en las técnicas de distribución

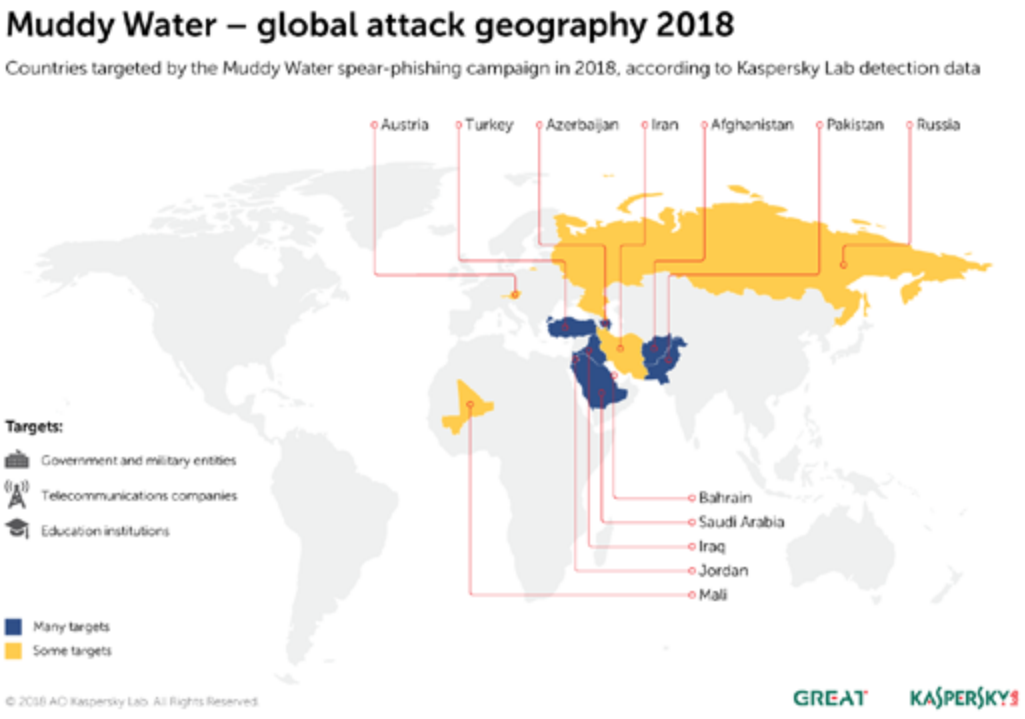
de Meterpreter. Otros aspectos llamativos fueron las dinámicas técnicas de distribución de Mosquito, el uso personalizado de PowerShell de código abierto de PoshSec-Mod, y un código inyector prestado. Relacionamos parte de estas actividades con la infraestructura y puntos de datos de la infraestructura de WhiteBear y la infraestructura de Mosquito y sus actividades en 2017 y 2018. Un aspecto interesante de nuestra investigación fue notar la ausencia de blancos superpuestos con otras actividades de APTs en curso. Turla no se hizo presente en el evento de hackeo DNC, donde Sofacy y CozyDuke sí estuvieron, pero el grupo se mantenía silenciosamente activo en otros proyectos alrededor del mundo. Esto da un indicio sobre las motivaciones y ambiciones de este grupo. Resulta interesante que los datos relacionados con estas organizaciones no se hayan convertido en armas de ataque y que no se las haya detectado en Internet a medida que Turla lleva a cabo sus actividades fuera del radar. Tanto Mosquito como Carbon apuntan principalmente a blancos diplomáticos y de asuntos exteriores, al mismo tiempo que las actividades de WhiteAtlas y WhiteBear se extendieron por el mundo incluyendo a organizaciones relacionadas con los asuntos exteriores; sin embargo, no todos los ataques tienen este perfil: el grupo también ha atacado a centros científicos y técnicos, así como a organizaciones fuera del ámbito político. Las actividades del grupo KopiLuwak no necesariamente se enfocan en blancos diplomáticos o de asuntos exteriores. En lugar de ello, sus actividades en 2018 apuntaron a organizaciones científicas y de investigación gubernamentales y a una organización de comunicación gubernamental en Afganistán. Es probable que esta alta selectividad de blancos, pero más amplia, continúe en 2019.

En octubre informamos sobre las actividades recientes del grupo de APT MuddyWater. Nuestra telemetría indicaba que este actor de amenazas relativamente nuevo que apareció en 2017 se había enfocado principalmente en blancos gubernamentales en Irak y Arabia Saudita. Sin embargo, el grupo detrás de MuddyWater se hizo conocido por atacar a otros países en Medio Oriente, Europa y EE.UU. Recientemente observamos una gran cantidad de archivos del tipo spear-phishing que aparentemente apuntaban a agencias gubernamentales, organizaciones militares, compañías de telecomunicación e instituciones educativas en Jordania, Turquía, Azerbaiyán y Paquistán, además de sus ataques contra blancos en Irak y Arabia Saudita. Se detectaron otras víctimas en Malí, Austria, Rusia, Irán y Baréin. Estos nuevos archivos aparecieron durante 2018 y sus actividades escalaron desde mayo. Estos nuevos archivos del tipo spear-phishing se basan en ingeniería social

para persuadir a sus víctimas a que habiliten los macros. Los atacantes dependen de una serie de hosts infectados para lanzar sus ataques. En las etapas avanzadas de nuestra investigación logramos no sólo observar archivos y herramientas adicionales del arsenal de este grupo, sino también algunos errores OPSEC que cometieron. Para protegernos contra los ataques con malware, desearíamos formular las siguientes recomendaciones:

- Eduque a todo el personal para que sean capaces de identificar comportamientos sospechosos, como los enlaces tipo phishing.
- Eduque al personal de seguridad informática para asegurarse de que posean las habilidades necesarias para configurar, investigar y cazar.
- Use una solución de seguridad corporativa probada junto a soluciones contra ataques selectivos capaces de detectar ataques mediante el análisis de anomalías en la red.
- Asegúrese de que su personal de seguridad cibernética pueda acceder a datos actualizados sobre inteligencia de amenazas, que les proporcionarán las herramientas necesarias para descubrir y prevenir ataques, como los indicadores de compromiso (IoCs) y las normas YARA.
- Establezca procesos de gestión de parches a nivel corporativo.

Las organizaciones de alto perfil deberían adoptar niveles elevados de ciberseguridad, ya que los ataques en su contra son inevitables y no hay perspectivas de que cesen.



DustSquad es otro actor de amenazas que ha atacado a organizaciones en Asia Central. Kaspersky Lab ha estado siguiendo las actividades de este grupo de ciberespionaje de habla rusa durante los dos últimos años, y hemos proporcionado a nuestros clientes informes de inteligencia sobre cuatro de sus campañas con malware para Android y Windows. Recientemente describimos un programa malicioso llamado Octopus, usado por DustSquad para atacar a entidades diplomáticas en la región; el nombre fue acuñado por ESET en 2017 después de que la rutina 0ct0pus3.php fuera usada por este actor en sus antiguos servidores C&C. Mediante el motor de atribución Kaspersky Attribution Engine, basado en algoritmos similares, descubrimos que Octopus está relacionado con DustSquad. Nuestra telemetría hizo seguimiento de esta campaña en 2014 en las repúblicas ex soviéticas en Asia Central (aún ampliamente de habla rusa) y en Afganistán. En abril descubrimos una nueva muestra de Octopus camuflada como Telegram Messenger con una interfaz rusa. No encontramos el software legítimo que este malware imita; de hecho, no creemos que exista. Sin embargo, los atacantes usaron la posible prohibición de Telegram en Kazajistán para introducir este descargador como un software de comunicación alternativo para la oposición

política. Al suscribirse a nuestros informes de inteligencia sobre ATPs, usted accede a nuestras investigaciones y descubrimientos de forma inmediata, incluyendo datos técnicos completos.

En octubre publicamos nuestro análisis sobre Dark Pulsar. Nuestra investigación comenzó en marzo de 2017, cuando Shadow Brokers publicó datos robados que incluían dos plataformas: DanderSpritz y FuzzBunch. DanderSpritz contiene varios tipos de complementos diseñados para analizar a las víctimas, explotar vulnerabilidades, programar tareas, etc. La plataforma DanderSpritz está diseñada para analizar los equipos ya controlados y obtener inteligencia. Juntas, conforman una súper plataforma para ciberespionaje. La fuga no incluía la puerta trasera Dark Pulsar; lo que contenía era un módulo administrativo para controlar la puerta trasera. Sin embargo, al crear firmas especiales en base a algunas constantes mágicas en el módulo administrativo, logramos atrapar el implante. Este implante permite que los atacantes controlen de forma remota los dispositivos infectados. Detectamos 50 víctimas, todas en Rusia, Irán y Egipto, pero creemos que es probable que sean muchas más. Para comenzar, la interfaz de DanderSpritz es capaz de manejar una gran cantidad de víctimas al mismo tiempo. Además, los atacantes suelen borrar su malware una vez finalizada la campaña. Creemos que la campaña cesó después de la fuga 'Lost in Translation' por parte de Shadow Brokers en abril de 2017. Puede leer nuestras estrategias de mitigación sugeridas para amenazas complejas como Dark Pulsar aquí.

CAMPAÑAS DE APTS MÓVILES

El segmento de amenzas de APTs móviles fue testigo de tres eventos relevantes: la detección de las campañas de ciberespionaje Zoopark, BusyGasper y Skygofree.

Técnicamente, las tres están bien diseñadas y comparten su objetivo primario: espiar a sus víctimas. Su principal meta es robar todos los datos personales posibles desde dispositivos móviles: intercepción de llamadas, mensajes, ubicación geográfica, etc. Poseen incluso una función para espionaje mediante el micrófono del dispositivo: el teléfono es usado como un 'error' que ni siquiera necesita ocultarse de un blanco desprevenido.

Los ciberdelincuentes se concentraron en el robo de mensajes desde aplicaciones populares de mensajería instantánea, las cuales han desbancado a los medios de comunicación tradicionales. En varios casos, los atacantes utilizaron exploits capaces de escalar los privilegios locales de los troyanos en el dispositivo, obteniendo así acceso prácticamente ilimitado al control remoto y, frecuentemente, a su manipulación.

También implementaron keyloggers en dos de los tres programas maliciosos, a fin de registrar toda la actividad de la víctima en el teclado del dispositivo capturado. Vale la pena notar que para interceptar las pulsaciones, los atacantes ni siquiera necesitaron privilegios elevados.

Geográficamente, las víctimas se encontraron en varios países: Skygofree apuntó a usuarios en Italia, BusyGasper lo hizo en Rusia, mientras que Zoopark operó en Medio Oriente.

También vale la pena notar que los ciberespías muestran una preferencia notable y creciente por las plataformas móviles: les ofrecen muchos más datos personales.

VULNERABILIDADES

La explotación de vulnerabilidades en el software y el hardware sigue siendo un medio importante para infectar dispositivos de todo tipo.

EA principios de este año se reportó sobre dos vulnerabilidades críticas en los CPUs de Intel: Meltdown y Spectre, que permiten que un atacante lea la memoria de cualquier proceso y de su propio proceso. Estas vulnerabilidades existen desde al menos 2011. Meltdown (CVE-2017-5754) afecta a los CPUs de Intel y permite que el atacante lea los datos de cualquier proceso en el sistema host. Si bien se requiere la ejecución del código, esto se puede lograr de varias maneras: por ejemplo, a través de un error de software o visitando un sitio web malicioso que carga un código JavaScript que ejecuta el ataque Meltdown. Esto significa que todos los datos que residen en la memoria (contraseñas, claves de cifrado, PINs, etc.) podrían leerse si la vulnerabilidad se explota correctamente. Los fabricantes publicaron rápidamente los parches para los sistemas operativos más populares. La actualización de Microsoft, publicada el 3 de enero, no era compatible con todos los programas antivirus, lo que posiblemente originó una Pantalla azul de la muerte (BSoD) en sistemas incompatibles. Por lo tanto, las actualizaciones sólo se podían instalar si un producto antivirus primero había establecido una clave de registro específica para indicar que no había problemas de compatibilidad. Spectre (CVE-2017-5753 y CVE-2017-5715) es ligeramente diferente. A diferencia de Meltdown, este ataque también funciona en otras arquitecturas (como AMD y ARM). Además, Specter sólo puede leer el espacio de memoria del proceso explotado, pero no el de cualquier proceso. Más importante aún, aparte de algunas contramedidas en algunos navegadores, Specter no cuenta con una solución universal. En las semanas posteriores a los informes de las vulnerabilidades, se hizo evidente que no son fáciles de reparar. La mayoría de los parches publicados han reducido la superficie de ataque, mitigando las formas conocidas de explotar las vulnerabilidades, pero no las erradican por completo. Dado que el problema es fundamental para el funcionamiento de las CPUs vulnerables, es probable que los fabricantes tengan que lidiar con nuevas formas de exploits en los próximos años. De hecho, no tardó años. En julio, Intel pagó una recompensa de USD 100.000 por nuevas vulnerabilidades en el procesador relacionadas con la variante uno de Spectre (CVE-2017-5753). Spectre 1.1 (CVE-2018-3693) puede usarse para crear desbordamientos de búfer especulativos. Spectre 1.2 permite que el atacante reescriba datos de sólo lectura y punteros de códigos para vulnerar

las cajas de arena en CPUs que no cuentan con protección para lectoescritura. Estas nuevas vulnerabilidades fueron descubiertas por el investigador Vladimir Kiriansky del MIT y por el investigador independiente Carl Waldspurger.

El 18 de abril alguién cargó un llamativo exploit a VirusTotal. Esto fue detectado por varios proveedores de seguridad, incluyendo Kaspersky Lab, mediante nuestra lógica heurística genérica para archivos antiguos de Microsoft Word. Resultó ser una nueva vulnerabilidad día cero para Internet Explorer (CVE-2018-8174) que Microsoft parchó el 8 de mayo de 2018. Después de procesar la muestra en nuestro sistema de caja de arena, notamos que lograba explotar una versión completamente parchada de Microsoft Word. Esto nos llevó a analizar esta vulnerabilidad con mayor profundidad. La cadena de infección se divide en las siguientes etapas: La víctima recibe un documento malicioso de Microsoft Word Después de abrirlo, la segunda etapa del exploit es su descarga: una página HTML con el código VBScript, la cual activa una vulnerabilidad UAF (Use After Free) y ejecuta el shellcode. Aunque el vector inicial de ataque es un documento de Word, en realidad la vulnerabilidad está en VBScript. Esta es la primera vez que hemos visto que se use una URL Moniker para cargar un exploit para IE en Word: creemos que los atacantes usarán ampliamente esta técnica en el futuro: les permite forzar a la víctima a descargar IE y pasar por alto la configuración predeterminada del navegador. Es probable que los autores de kits de exploits comiencen a usarla en ataques del tipo drive-by (mediante el navegador) y en campañas de spear-phishing (mediante un documento). Para protegerse contra esta técnica, recomendamos aplicar las últimas actualizaciones de seguridad y usar una solución de seguridad capaz de detectar comportamientos.

En agosto, nuestra tecnología AEP (prevención automática de exploits) detectó un nuevo tipo de ciberataque que usaba una vulnerabilidad día cero en el archivo controlador de Windows 'win32k.sys'. Informamos a Microsoft sobre este problema y el 9 de octubre descubrieron la vulnerabilidad (CVE-2018-8453) y publicaron una actualización. Es una vulnerabilidad muy peligrosa que les otorga a los atacantes el control de la computadora infectada. Esta vulnerabilidad se utilizó en una campaña de ataques muy selectivos contra organizaciones en Medio Oriente, donde encontramos menos de una docena de víctimas. Creemos que estos ataques fueron llevados a cabo por el actor de amenazas FruityArmor.

A fines de octubre informamos a Microsoft sobre otra vulnerabilidad día cero que elevaba los privilegios en 'win32k.sys', que permite que un atacante la use para obtener los privilegios necesarios para lograr persistencia en el sistema atacado. Esta vulnerabilidad también fue explotada en un muy limitado número de ataques contra organizaciones en Medio Oriente. El 13 de noviembre Microsoft publicó una actualización para esta vulnerabilidad (CVE-2018-8589). Esta amenaza también fue detectada por nuestras tecnologías proactivas: la avanzada caja de arena y el motor anti-malware de nuestra Plataforma anti-ataques selectivos, y nuestra tecnología AEP.

COMPLEMENTOS PARA EL NAVEGADOR: AMPLIANDO EL ALCANCE DE LOS CIBERDELINCUENTES

Los complementos para el navegador pueden facilitarnos la navegación, ocultando publicidad invasiva, traduciendo textos, ayudándonos a elegir los artículos que queremos comprar en tiendas en línea, y mucho más. Desafortunadamente, también hay complementos indeseables que nos bombardean con publicidad o que recopilan información sobre nuestras actividades. También hay complementos diseñados para robar dinero. A principios de este año, uno de ellos llamó nuestra atención: se comunicaba con un dominio sospechoso. Este complemento malicioso, llamado *Desbloquear Conteúdo*, atacaba a usuarios de servicios de banca en línea en Brasil, recopilando nombres de usuario y contraseñas para luego acceder a las cuentas bancarias de las víctimas.

En septiembre unos hackers publicaron los mensajes privados en al menos 81.000 cuentas de Facebook, proclamando que se trataba sólo de una pequeña fracción de un ataque mucho mayor contra 120 millones de cuentas. En un aviso de Dark Web, los atacantes ofrecieron los mensajes por 10 centavos por cuenta. El ataque estaba siendo investigado por el Servicio ruso BBC y por la compañía de ciberseguridad Digital Shadows. Descubrieron que de 81.000 cuentas, la mayoría eran de Ucrania y Rusia, y algunas de otros países, como Reino Unido, EE.UU. y Brasil. Facebook sugirió que los mensajes fueron robados mediante un complemento maliciosos para el navegador.

Los complementos maliciosos son bastante inusuales, pero debemos tomarlos en serio por los potenciales daños que son capaces de causar. Le recomendamos que instale sólo complementos verificados que tengan grandes cantidades de descargas, además de comentarios, en Chrome Web Store u otro servicio oficial. Incluso así, a pesar de las medidas de protección implementadas por los propietarios de estos servicios, los complementos maliciosos pueden terminar publicados. Entonces, es una buena idea utilizar una solución de seguridad para Internet que le advierta cuando un complemento se comporte de forma sospechosa.

EL MUNDIAL DEL FRAUDE

La ingeniería social sigue siendo una herramienta importante en el arsenal de los ciberatacantes de toda laya. Los estafadores siempre están en busca de oportunidades para ganar dinero aprovechando los principales eventos deportivos, y el Mundial de la FIFA no fue la excepción. Mucho antes del inicio de este evento, los ciberdelincuentes habían comenzado a crear sitios web tipo phishing y a enviar mensajes explotando el tema del Mundial. Estos mensajes del tipo phishing incluían notificaciones fraudulentas de haber ganado una lotería, o un mensaje que ofrecía boletos para alguno de los partidos. Los estafadores esforzaron para imitar los sitios legítimos de los socios de la FIFA, llegando a crear páginas web bien diseñadas que hasta contenía certificados SSL que les daba credibilidad. Los ciberdelincuentes también robaron datos imitando comunicaciones oficiales de la FIFA: la víctima recibía un mensaje anunciándole que el sistema de seguridad había sido actualizado y que debía volver a introducir todos sus datos personales para evitar que la bloqueen. Estos mensajes contenían una un enlace a un sitio web fraudulento donde los estafadores recopilaban la información personal de sus víctimas.

Puede leer aquí nuestro informe sobre las formas en los ciberdelincuentes explotaron el Mundial para lucrar. También ofrecimos algunos consejos para evitar los fraudes del tipo phishing: estos consejos son válidos para cualquier fraude del tipo phishing, no sólo para los relacionados con el Mundial.

Previo a la inauguración del evento, también analizamos los puntos de acceso inalámbrico en las 11 ciudades que albergaron los partidos del Mundial: casi 32.000 puntos de Wi-Fi en total. Mientras verificábamos los algoritmos de cifrado y autenticación, contamos la cantidad de redes WPA2 y abiertas, así como su proporción respecto a todos los puntos de acceso. Más de un quinto de los puntos de acceso a Wi-Fi utilizaban redes poco confiables. Esto significaba que los ciberdelincuentes sólo tenían que encontrarse cerca de un punto de acceso para interceptar el tráfico y robar los datos de los usuarios. Unos tres cuartos de todos los puntos de acceso usaban el cifrado WPA/WPA2, considerado entre los más seguros. El nivel de protección depende en gran medida de la configuración, como la fortaleza de la contraseña fijada por el propietario del punto de acceso. El descifrado de una contraseña con cifrado sólido puede tardar años. Sin embargo, incluso las redes confiables, como WPA2, no pueden considerarse automáticamente totalmente seguras. Aún son susceptibles a los ataques del tipo fuerza bruta, de diccionario y de reinstalación de claves: cuentan con innumerables tutoriales

y herramientas de código abierto disponibles en Internet. Cualquier intento de intercepción de tráfico desde una red WPA en puntos de acceso a Wi-Fi puede realizarse penetrando la brecha que existe en el inicio de sesión entre el punto de acceso y el dispositivo.

Puede leer nuestro informe aquí, así como nuestras recomendaciones para el uso seguro de puntos de acceso a Wi-Fi: estos consejos son válidos donde sea que usted se encuentre, no sólo en el Mundial.

FRAUDES FINANCIEROS A ESCALA INDUSTRIAL

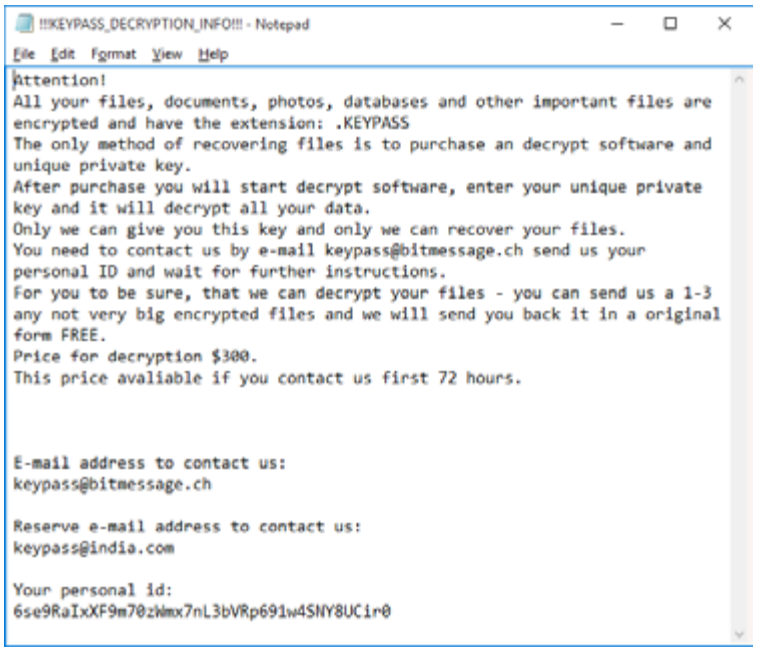
En agosto, ICS-CERT de Kaspersky Lab informó sobre una campaña de phishing diseñada para robar dinero a empresas, especialmente fabricantes. Los atacantes usaron técnicas comunes de phishing para inducir a sus víctimas a pulsar en adjuntos infectados en mensajes de correo que imitaban ofertas comerciales y otros documentos financieros. Los ciberdelincuentes usaron aplicaciones legítimas de administración remota: TeamViewer o RMS (sistema de manipulación remota). Se usaron estos programas para acceder al dispositivo, analizar la información sobre compras actuales y detalles del software financiero y contable utilizado por las víctimas. Después, los atacantes utilizaron diferentes estrategias para robar dinero a la compañía, como remplazar los datos bancarios en las transacciones. Para cuando publicamos nuestro informe, el 1 de agosto, habíamos detectado unas 800 computadoras infectadas en al menos 400 organizaciones en una variedad de industrias: fabricantes, petróleo y gas, metalurgia, ingeniería, energía, construcción, minería y logística. Esta campaña había estado activa desde octubre de 2017.

Nuestra investigación subraya que, incluso cuando los actores de amenazas utilizan técnicas sencillas y malware conocido, pueden tener éxito en sus ataques contra compañías industriales con trucos de ingeniería social y ocultando sus códigos en los sistemas atacados mediante software legítimo de administración remota para evadir la detección de las soluciones antivirus.

Puede leer más sobre la manera en que los atacantes utilizan las herramientas de administración remota para infectar a sus víctimas aquí, así como un resumen de los ataques contra sistemas ICS en el primer semestre de 2018 aquí.

EL RANSOMWARE SIGUE SIENDO UNA AMENAZA

La disminución del número de ataques con ransomware en el último año ha sido bien documentado. Sin embargo, este tipo de malware sigue siendo un gran problema y seguimos viendo el desarrollo de nuevas familias de ransomware. A principios de agosto nuestro módulo anti-ransomware comenzó a detectar al troyano KeyPass. En apenas dos días detectamos este malware en más de 20 países: Brasil y Vietnam fueron muy afectados, pero también encontramos víctimas en Europa, África y el Lejano Oriente. KeyPass cifra todos los archivos, cualquiera sea su extensión, en las unidades locales y los recursos compartidos en red accesibles desde la computadora infectada. Ignora algunos archivos ubicados en directorios que se cifran en el malware. A los archivos cifrados se les asigna la extensión adicional 'KEYPASS' y las notas de rescate llamadas '!!!KEYPASS_DECRYPTION_INFO!!!.txt' que se guardan en los directorios que contienen archivos cifrados. Los desarrolladores de este troyano implementaron un esquema muy simplista. El malware utiliza el algoritmo simétrico AES-256 en modo CFB con Zero IV y la misma clave de 32 bytes para todos los archivos. El troyano cifra un máximo de 0x500000 bytes (unos 5 MB) de datos al comienzo de cada archivo. Poco después de su ejecución, el malware se conecta con su servidor C&C y recibe la clave de cifrado y la identificación de infección de la víctima actual. Los datos se transfieren por HTTP simple en forma de JSON. Si el C&C es inaccesible (por ejemplo, si el equipo infectado no está conectado a Internet o el servidor está inactivo), el malware usa una clave e identificación cifradas. Como resultado, en el caso del cifrado fuera de línea, el descifrado de los archivos de la víctima será intrascendente.



La característica más interesante del troyano KeyPass es la capacidad de tomar el "control manual". El troyano contiene un formulario que está oculto por defecto, pero que se puede mostrar después de presionar un botón especial en el teclado. Este formulario permite que los atacantes personalicen el proceso de cifrado cambiando algunos parámetros, como la llave de cifrado, el nombre de la nota de rescate, el texto de la nota de rescate, la identidad de la víctima, la extensión de los archivos cifrados y la lista de directorios que no se cifrarán. Esta capacidad sugiere que los delincuentes que están detrás del troyano podrían usarlo en ataques manuales.

Sin embargo, no son sólo las nuevas familias de ransomware que están causando problemas. Un año y medio después de la epidemia de WannaCry, este malware sigue encabezando la lista de las familias cifradoras más propagadas: hemos visto 74.621 ataques únicos en todo el mundo. Estos ataques significaron el 28,72% de todos los ataques selectivos con cifradores en el tercer trimestre de 2018. Este porcentaje se ha incrementado en dos tercios durante el año pasado. Esto resulta particularmente alarmante considerando que antes del inicio de la epidemia en mayo de 2017, ya existía un parche para el exploit EternalBlue que WannaCry utilizaba.

ASACUB Y LOS TROYANOS BANCARIOS

2018 arrojó cifras impresionantes de la cantidad de ataques con troyanos bancarios móviles. Al principio del año, este tipo de amenaza parecía haberse estabilizado en términos de la cantidad de muestras únicas detectadas y de la cantidad de usuarios atacados.

Sin embargo, en el segundo trimestre hubo un cambio dramático negativo: aparecieron cifras récord de troyanos bancarios móviles detectados y de usuarios atacados. La causa primaria de este significativo aumento no está clara, aunque los principales culpables fueron los creadores de Asacub y Hqwar. Una característica llamativa de Asacub es su longevidad: según nuestros datos, el grupo responsable ha estado operando por más de tres años.

Asacub se desarrolló a partir de un troyano SMS y desde un principio contó con técnicas para evitar su eliminación y para interceptar llamadas y SMSs entrantes. Posteriormente, sus creadores complicaron la lógica del programa y comenzaron la distribución masiva del malware. El vector elegido fue el mismo que utilizaron al principio: ingeniería social por SMS. Sin embargo, esta vez los números telefónicos válidos se obtuvieron en conocidos tableros de avisos, cuyos propietarios a menudo esperaban mensajes de suscriptores desconocidos.

Posteriormente esta técnica se convirtió en una bola de nieve cuando los dispositivos que el troyano había infectado comenzaron a propagar la infección: Asacub se autopropagaba mediante la lista completa de contactos de la víctima.

INTELIGENTE NO SIGNIFICA SEGURO

Hoy en día vivimos rodeados de dispositivos inteligentes. Esto incluye objetos domésticos cotidianos como televisores, medidores inteligentes, termostatos, monitores para bebés y juguetes para niños. Pero también incluye automóviles, dispositivos médicos, cámaras de CCTV y parquímetros. Incluso estamos viendo el surgimiento de ciudades inteligentes. Sin embargo, esto ofrece una mayor superficie de ataque a cualquiera que busque aprovechar las debilidades de seguridad, para cualquier propósito. Es difícil proteger las computadoras tradicionales. Pero las cosas se ponen más difíciles con el Internet de las cosas (IoT), donde la falta de estandarización permite que los desarrolladores pasen por alto la seguridad o que la consideren como algo secundario. Hay muchos ejemplos que ilustran esto.

En febrero exploramos la posibilidad de que un smart hub podría ser vulnerable a ataques. Un smart hub permite al usuario controlar el funcionamiento de otros dispositivos inteligentes en el hogar, recibir información y enviar instrucciones. Los smart hubs pueden controlarse a través de una pantalla táctil o a través de una aplicación móvil o una interfaz web. Si es vulnerable, podría convertirse en un único punto de falla. Si bien el smart hub que nuestros expertos investigaron no contenía vulnerabilidades significativas, sí contenía errores lógicos que fueron suficientes para que obtuvieran acceso remoto.

Los investigadores del ICS -CERT de Kaspersky Lab recientemente revisaron una cámara inteligente popular para ver qué tan bien protegida estaba de los piratas informáticos. Las cámaras inteligentes son ahora parte de la vida cotidiana. Hoy en día muchos usuarios se conectan a la nube, lo que permite que alguien controle lo que sucede en un lugar remoto: para controlar a las mascotas, para la vigilancia de seguridad, etc. El modelo que nuestros expertos investigaron se comercializa como una herramienta para todo uso, adecuada para usarse como monitor de bebé o como parte de un sistema de seguridad. La cámara puede ver en la oscuridad, seguir un objeto en movimiento, reproducir secuencias de video en un teléfono inteligente o tableta, y reproducir sonido a través de un altavoz incorporado. Desafortunadamente, la cámara resultó tener 13 vulnerabilidades, casi tantas como sus características, que podrían permitirle a un atacante cambiar la contraseña de administrador, ejecutar códigos arbitrarios en el dispositivo, crear una red zombi de cámaras comprometidas o dejar de funcionar completamente.

Los posibles problemas no se limitan a los dispositivos de consumo. A principios de este año, Ido Naor, investigador de nuestro Equipo Global de Investigación y Análisis, y Amihai Neiderman de Azimuth Security, descubrieron una vulnerabilidad en un dispositivo de automatización para una estación de servicio. Este dispositivo estaba conectado directamente a Internet y era responsable de administrar todos los componentes de la estación, incluidos los dispensadores de combustible y los terminales de pago. Más alarmante aún: la interfaz web para el dispositivo era accesible con credenciales predeterminadas. Investigaciones posteriores revelaron que era posible apagar todos los sistemas de combustible, provocar fugas de combustible, cambiar los precios, eludir el terminal de pago (para robar dinero), capturar matrículas de vehículos e identidades de los conductores, ejecutar códigos en la unidad controladora e incluso moverse libremente a través de la red de estaciones de servicio.

La tecnología impulsa mejoras en el cuidado de la salud. Tiene el poder de transformar la calidad y reducir el costo de los servicios de salud. También puede brindar a los pacientes y a los ciudadanos mayor control sobre su atención, empoderar a los cuidadores y apoyar el desarrollo de nuevos medicamentos y tratamientos. Sin embargo, las nuevas tecnologías de atención médica y las prácticas de trabajo móvil están produciendo más datos que nunca, al mismo tiempo que brindan más oportunidades para la pérdida o el robo de datos. Hemos remarcado estos problemas reiteradamente durante los últimos años (puede leer más aquí, aquí y aquí). Seguimos rastreando las actividades de los ciberdelincuentes, observando cómo penetran en las redes médicas, cómo encuentran datos sobre los recursos médicos disponibles públicamente y cómo los extraen. En septiembre analizamos la seguridad en la atención de la salud. Más del 60 por ciento de las organizaciones médicas tenían algún tipo de malware en sus computadoras. Además, los ataques siguen aumentando en la industria farmacéutica: Es vital que las instalaciones médicas eliminen todos los nodos que procesan datos médicos personales, que actualicen el software y eliminen las aplicaciones que ya no se necesitan, y que no conecten equipos médicos costosos a la LAN principal. Puede leer nuestros consejos detallados aquí.

Este año también investigamos los dispositivos inteligentes para animales, específicamente los localizadores de mascotas. Estos dispositivos son capaces de acceder a la red doméstica y al teléfono del dueño de la mascota, así como

a la ubicación de ésta. Queríamos averiguar cuán seguros eran. Nuestros investigadores observaron varios localizadores populares en busca de posibles vulnerabilidades. Cuatro de estos aparatos usaban tecnología Bluetooth LE para comunicarse con el teléfono del propietario. Pero solamente uno lo hacía correctamente. Los otros podían recibir y procesar instrucciones de cualquiera. También podían desactivarse u ocultarse al dueño: todo lo que se necesitaba era estar cerca del dispositivo. Sólo una de las aplicaciones para Android probadas verifica el certificado de su servidor: no depende solamente del sistema. En consecuencia, son vulnerables a los ataques del tipo man-in-the-middle (MitM): los atacantes pueden interceptar datos 'persuadiendo' a sus víctimas para que instalen su certificado.

Algunos de nuestros investigadores también analizaron los dispositivos de vestir, en particular los relojes inteligentes y los rastreadores de ejercicios físicos. Nos interesaba el escenario en el que una aplicación espía instalada en un teléfono pudiera enviar datos desde los sensores de movimientos incorporados (acelerómetro y giroscopio) a un servidor remoto y usar los datos para reconstruir las acciones del usuario: cuándo camina, se sienta, escribe en su teléfono, etc. Comenzamos con un teléfono Android, creamos una aplicación sencilla para procesar y transmitir datos, y luego vimos qué podíamos conseguir a partir de estos datos. No sólo fue posible saber si el usuario estaba sentado o caminando, sino que también logramos saber si estaba de paseo o cambiando de trenes subterráneos, porque los patrones del acelerómetro apenas difieren: así es como los rastreadores de ejercicios físicos distinguen entre caminar y manejar bicicleta. También es fácil saber cuando alguien está escribiendo en su teléfono. Sin embargo, sería difícil saber lo que está escribiendo y se necesitaría repetir los textos ingresados. Nuestros investigadores lograron recuperar una contraseña de computadora con un 96 por ciento de precisión, así como un código PIN introducido en un cajero automático con un 87 por ciento de precisión. Sin embargo, debido la falta de predictibilidad sobre cuándo la víctima los introduce, sería mucho más difícil obtener otros datos, como el número de una tarjeta de crédito o el código CVC. En realidad, la dificultad para obtener estos datos significa que un atacante tendría que tener una poderosa motivación para atacar a alguien en particular. Por supuesto, hay situaciones en las que esto puede valer la pena para los atacantes.

En los últimos años ha habido un crecimiento de los servicios de automóviles compartidos. Estos servicios claramente proporcionan flexibilidad a la gente que necesita circular por las ciudades grandes. Sin embargo, surge esta pregunta sobre seguridad: ¿Cuán protegida está la información personal de los usuarios de estos servicios? En julio probamos 13 aplicaciones para ver si sus desarrolladores habían tenido en cuenta la seguridad. Los resultados no fueron alentadores. Quedó claro que los desarrolladores de estas aplicaciones no comprendían cabalmente las modernas amenazas contra las plataformas móviles: esto se evidenció tanto en la etapa de diseño como en la creación de la infraestructura. Una primera medida sería ampliar la función de notificación a los usuarios sobre actividades sospechosas: actualmente sólo un servicio envía notificaciones a los usuarios sobre intentos de acceso a sus cuentas desde diferentes dispositivos. La mayoría de las aplicaciones analizadas estaban mal diseñadas desde el punto de vista de la seguridad y necesitaban mejorar. Además, muchos de los programas no sólo son muy similares entre sí, sino que hasta se basan en el mismo código. Puede leer nuestro informe aquí, así como nuestras recomendaciones para los usuarios de servicios de automóviles compartidos, y nuestras recomendaciones para los desarrolladores de las respectivas aplicaciones.

Aumenta el uso de dispositivos inteligentes. Algunos pronósticos sugieren que hasta el 2020 la cantidad de dispositivos inteligentes superará la población del mundo en varias veces. Sin embargo, para los fabricantes la seguridad aún no es una prioridad: no hay recordatorios para que el usuario cambie la contraseña por defecto durante la configuración inicial, ni notificaciones sobre la publicación de versiones del firmware. Y el proceso de actualización puede ser complejo para el consumidor promedio. Gracias a esto, los dispositivos del IoT son un blanco codiciado de los ciberpiratas. Más fáciles de infectar que las computadoras, tienen un papel importante en la infraestructura del hogar: algunos controlan el tráfico de Internet, otros toman fotos y videos, otros controlan algunos electrodomésticos, como el aire acondicionado. El malware para dispositivos inteligentes aumenta tanto en cantidad como en calidad. Cada vez más exploits son convertidos en armas de ataque por los ciberdelincuentes, y los dispositivos infectados son usados para lanzar ataques DDoS, para robar datos personales y para la minería de criptomonedas. En septiembre publicamos un informe sobre las amenazas para el IoT, y este año hemos comenzado a incluir información sobre ataques contra el IoT en nuestros informes trimestrales y de fin de año.

Es vital que los proveedores mejoren su enfoque de seguridad y la incorporen en el diseño de sus productos. Algunos gobiernos están elaborando guías en un esfuerzo para alentar a los fabricantes a que incluyan la seguridad en sus dispositivos inteligentes. En octubre, el gobierno británico publicó su código de prácticas para la seguridad del consumidor de dispositivos del IoT. Recientemente, el gobierno alemán publicó sugerencias para normas mínimas para los enrutadores de banda ancha.

Antes de comprar cualquier dispositivo conectado, es importante que los consumidores tengan en cuenta la seguridad.

- Considere si realmente necesita el dispositivo. Si lo necesita, verifique las funciones disponibles y desactive cualquiera que no necesite para reducir su superficie de ataque.
- Busque información en Internet sobre vulnerabilidades reportadas
- Verifique si es posible actualizar el firmware en el dispositivo.
- Siempre cambie la contraseña predeterminada y remplácela con una contraseña única y compleja.
- No comparta en línea los números de serie, direcciones IP y otros datos confidenciales relacionados con el dispositivo.

NUESTROS DATOS EN SUS MANOS

Su información personal es un bien valioso. Esto se evidencia a partir del flujo constante de casos de fugas de seguridad reportados en las noticias: Under Armour, FIFA, Adidas, Ticketmaster, T-Mobile, Reddit, British Airways y Cathay Pacific.

El escándalo que implica el uso, por parte de Cambridge Analytica, de datos de Facebook es un recordatorio de que la información personal no sólo es valiosa para los ciberdelincuentes. En muchos casos, los datos personales son el precio que las personas pagan para obtener un producto o servicio: navegadores "gratuitos", cuentas de correo electrónico "gratuitas", cuentas de redes sociales "gratuitas", etc. Pero no siempre. Cada vez más, estamos rodeados de dispositivos inteligentes que son capaces de reunir detalles sobre las minucias de nuestras vidas. A principios de este año, uno periodista convirtió su departamento en una casa inteligente para medir la cantidad de datos que estaban recopilando las empresas que fabricaban los dispositivos. Dado que generalmente pagamos por tales dispositivos, la recolección de datos difícilmente puede verse como el precio que pagamos por los beneficios que brindan en estos casos.

Algunas fugas de información han sido castigadas con multas para las compañías afectadas (por ejemplo, la Oficina de información del comisionado del Reino Unido multó a Equifax y facebook). Sin embargo, hasta ahora las multas impuestas han sido por fugas que ocurrieron antes de que el Reglamento general de protección de datos (GDPR) de la UE entrará en vigor en mayo. Con seguridad, las penas por fugas de información graves que ocurran en el futuro serán más severas.

No existe la seguridad al 100 %, por supuesto. Pero toda compañía que posea datos personales tiene el deber de protegerlos de la mejor manera posible. Y si alguna fuga resultara en el robo de información personal, las compañías deberían alertar a sus clientes de forma oportuna, permitiéndoles así tomar medidas para limitar los posibles daños que pudiesen ocurrir.

Si bien no hay nada que como individuos podamos hacer para evitar el robo de nuestra información personal de parte de un proveedor de Internet, es importante que tomemos medidas para proteger nuestras cuentas en línea y minimizar el impacto de cualquier fuga, en particular usando contraseñas únicas para cada sitio, así como la autenticación de dos factores.