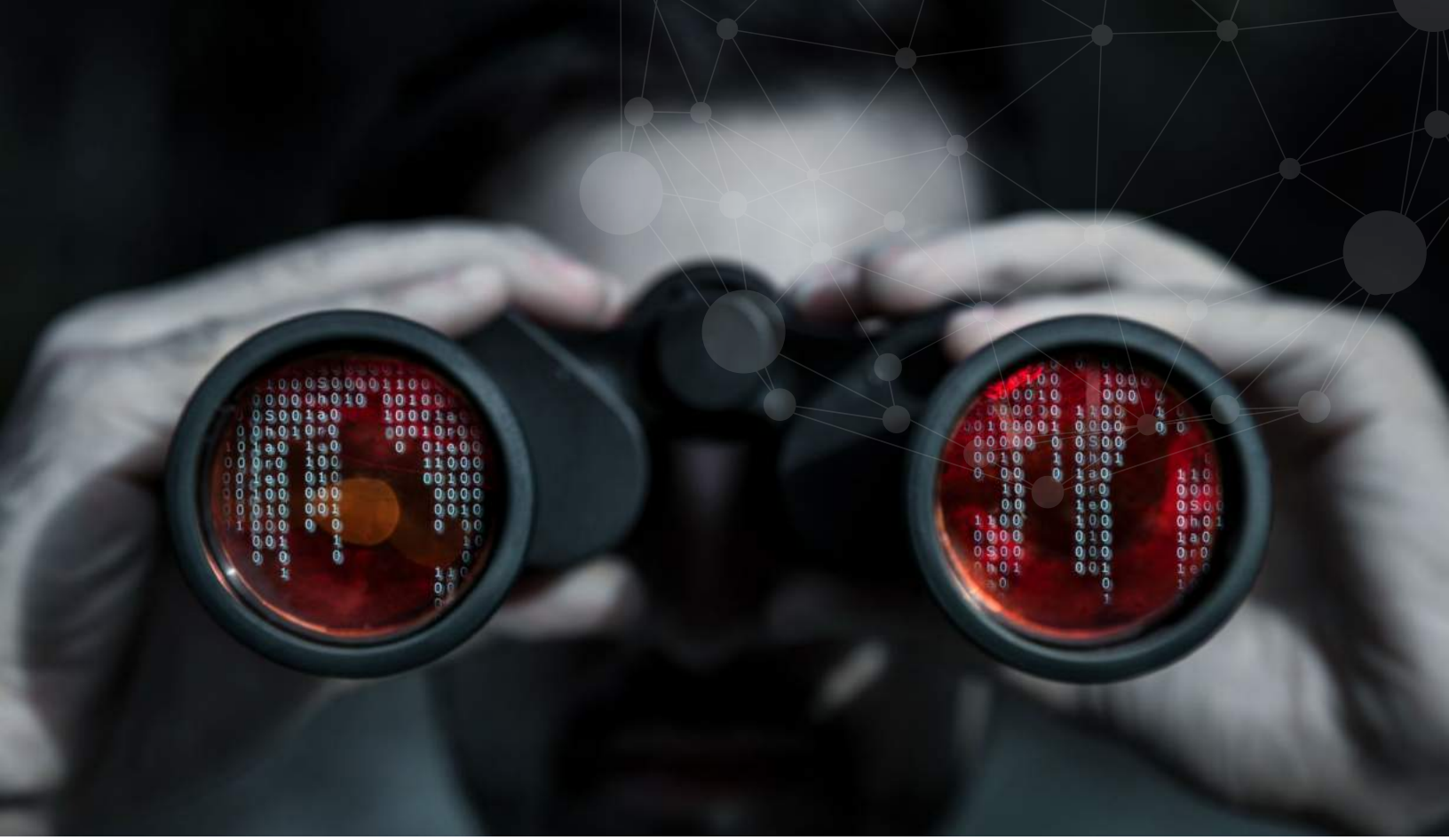
ALEF

INFINIDAD DE SOLUCIONES

RESUMEN DE SEGURIDAD 2017: EL AÑO DE LOS LLAMADOS DE ATENCIÓN

PARTE I



2017 EL AÑO DE LOS LLAMADOS DE ATENCIÓN

Recién terminados de ver en nuestra bola de cristal y destacar algunas de las tendencias que esperamos dominen el panorama cibernético en el año entrante, vamos a ofrecer una imagen de lo que fue 2017. En cierta manera, este puede ser considerado el "año de los llamados de atención". Las alarmas apenas han dejado de sonar a medida que seguíamos despertando a la realidad de un estallido de nuevos incidentes cibernéticos. Golpeando a lo largo y a lo ancho, dichas incursiones proveyeron a todo aquel que se acerca a la Web con el material suficiente para reflexionar acerca de qué tan inseguros pueden ser nuestros mundos en línea. Más que 'siéntate y relájate', es hoy más común 'levántate y toma nota'.

Como parte de nuestra narrativa, centraremos la atención en eventos clave y destacaremos características en común, fundamentando las principales tendencias y temas que han definido a este año. Además, revisaremos algunas de las predicciones para 2017 que nuestros líderes en la materia han hecho un año atrás.

CAYENDO EN LA MADRIGUERA CON EL RANSOMWARE

La cantidad de atención alcanzada por el ransomware o ataques del estilo (como wipers y algunas estafas de soporte técnico) este año, también nos tienta a concluir que 2017 será recordado como 'el año del ransomware'. De hecho, probablemente hayas oído esa frase anteriormente, incluida con precaución en nuestra reseña 2016. Sin embargo, la imagen puede no ser tan clara. Para no ser opacadas por el simple malware, las brechas de seguridad a gran escala abundaron – e incluso llegaron a su máximo – este año, demostrando que el ser afectado por una brecha de seguridad ya no es una cuestión de 'y si…' sino de 'cuándo'. El Ransomware y las brechas de seguridad se mantienen como grandes espinas que rodean a usuarios y organizaciones alrededor del mundo, y suelen pinchar sus defensas sin demasiado esfuerzo. De hecho, a veces ambas amenazas se entrelazan, dando como resultado una combinación de ingredientes de inseguridad cibernética altamente volátil.

Mientras el problema que el ransomware representa ha estado descendiendo hacia sus más bajos niveles en los últimos años, las ganancias – y por lo tanto las demandas de ellas – han llegado a picos en la dirección opuesta. Tanto es así que el incentivo por obtener ganancias cada vez más grandes ha continuado incentivando el florecimiento de kits de 'Ransomware como servicio' (RaaS, por sus siglas en inglés), permitiendo a atacantes no necesariamente expertos en tecnología golpear fuertemente a sus objetivos. En pocas palabras, todo lo que se necesita es tener intenciones maliciosas y algo de dinero. Contrasta esos gastos insignificantes con las ganancias potenciales: El FBI estima que la cantidad total de pagos hechos por rescates cibernéticos se acerca al billón de dólares anuales.

En un nuevo cambio de paradigma del ransomware, muchos ataques son ahora sofisticadas, e incluso personalizadas, campañas que involucran sectores y víctimas deliberadamente seleccionados, y ya no intentos generales por obtener cualquier monto de dinero de víctimas aleatorias.

RANSOMWARE, BRECHAS DE SEGURIDAD Y DDOS... ¿SE ACERCAN LAS GRANDES BRECHAS EN IOT?

El Ransomware también ha estado evolucionando de muchas otras maneras, dando como resultado amenazas híbridas. La rentabilidad del 'modelo de negocio' basado en la extorsión cibernética también se evidencia por el hecho de que éstas tácticas fueron trasladadas a otras plataformas (Android) hace ya cierto tiempo, y son también la columna de los ataques seguidos de amenazas extorsivas bajo la pena de hacer públicos los datos robados.

La red de televisión HBO y la plataforma de streaming Netflix, estuvieron en el centro de la cuestión a comienzos de año por las filtraciones consecuentes del conflicto de Sony en 2014, en lo que efectivamente iguala la militarización de sus propios datos.

Los desarrollos durante los últimos años también han validado algunas de nuestras preocupaciones respecto a cierto grado de hibridación entre extorsión, DDoS (denegación de servicio, por sus siglas en inglés) y/o la explotación de vulnerabilidades del IoT, ya que futuras amenazas se apoyan sobre el ya probado ransomware criptográfico. En un poco sorpresivo avance de esta evolución, una desagradable combinación de extorsión y DDoS ha tenido a los criminales aún más expectantes este año, y ha ganado mayor tracción, especialmente tras una exitosa campaña extorsiva que concedió a sus organizadores sumas por el valor de $1 millón en bitcoins en junio.

En el gran plan de cosas, el hambre por intimidar a las víctimas a pagar bajo la amenaza de un ataque DDoS también está impulsado por la disponibilidad de ambos 'servicios' – RaaS y DDoS para alquilar. Mientras que estos pagos junto con las amenazas DDoS suelen ser mucha palabra pero poca acción, la prevalencia de DDoS hace de estos asaltos una de las principales amenazas que enfrentan las organizaciones. Para empeorar las cosas, dichos ataques suelen presentarse como una cortina de humo para lograr otros objetivos, principalmente ataques de malware o robo de información.

Para sumar a los conflictos está la proliferación de dispositivos IoT (Internet de las Cosas). Dejando de lado las pruebas de concepto, aún nos queda

por ver un ataque plenamente desarrollado que involucre demandas aleatorias a cambio de liberar las "cosas inteligentes" secuestradas. Sin embargo, las pistas no suelen ser tan claras. Mientras dicho secuestro no es necesariamente tan simple como a veces muestran los medios, no podemos dejar de replicar nuestras frecuentes preocupaciones sobre qué podría suceder si/cuando un método de ataque de moda, como el ransomware, se une con incontables dispositivos del IoT no asegurados listos para ser explotados.

Los ataques DDoS – como aquel que causó una interrupción extendida de la actividad de Internet en Estados Unidos hace poco más de un año – suelen ser conducidos por máquinas reclutadas por botnets. Los desarrollos en el ámbito de las botnet marcaron un hito hace unas pocas semanas, cuando una operación internacional de desmantelamiento destruyó cientos de botnets que operan hace tiempo manejadas por una familia de malware llamados Wauchos (también conocidos como Gamarue o Andromeda) siguiendo un esfuerzo que duró más de un año e involuró asistencia técnica de investigadores de ESET.

WANNACRYPTOR COMO CANARIO EN UNA MINA DE CARBÓN

El 12 de mayo de 2017 era un viernes normal, hasta que empezaron a reportarse miles de bloqueos en computados alrededor del mundo, que sólo serían liberadas a cambio del valor de $300 en bitcoin. La infección sin precedentes – el ransomware llamado WannaCryptor (detectado por ESET como WannaCryptor.D y llamado también WannaCry y Wcrypt) – se expandió de manera vertiginosa, afectando alrededor de 300.000 computadoras en aproximadamente 150 países. En contraste, los pagos no fueron considerables si se considera su alcance epidémico.

Mientras las víctimas trataban de encontrar un sentido en medio del caos e intentaban recuperar su información – que de hecho se asemejaba a una broma tonta – el estallido pronto fue frenado en seco luego de que un investigador en seguridad registrara un dominio para desactivar el ataque,

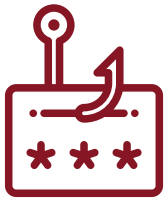
poniendo fin al desarrollo del ransomware. En poco tiempo, el dominio fue puesto en alerta máxima, sin embargo, dado que algunos atacantes buscaban resucitar a WannaCryptor mediante ataques DDoS que apuntaban a derribar el dominio y dejarlo fuera de línea, utilizando versiones exactamente iguales a la botnet Mirai en el proceso. Wannacryptor se propagó explotando vulnerabilidades en la implementación de Windows del protocolo Server Message Block (SMB), utilizando las herramientas EternalBlue y DoublePulsar desarrolladas por la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés). En la actualidad, Microsoft ha presentado una actualización de seguridad para que las versiones compatibles con Windows pongan parches a los huecos explotados por EternalBlie dos meses antes de la explosión y un mes antes de que un grupo de atacantes conocido como Shadow Brokers liberara las dos herramientas en la web. Con el objetivo de prevenir posteriores repeticiones del ataque, Microsoft decidió emitir parches de emergencias para sistemas ya no soportados, como Windows XP. A diferencia de los reportes iniciales, se descubrió que prácticamente todas las víctimas de WannaCryptor utilizaban sistemas de Windows 7 (obviamente sin parches).

OTRO ATAQUE GLOBAL

Unas seis semanas después, con la nota de rescate en rojo y blanco de Wannacryptor aún fresca en la memoria, todas las miradas se dirigieron hacia otra amenaza virulenta con sus particularidades. El 27 de junio, el ransomware detectado por ESET como Diskcoder.C también llamado ExPetr, PetrWrap o Not-Petya) comenzó a circular y, mientras atacaba a organizaciones alrededor del mundo, la mayoría de las compañías abatidas tenían base en Ucrania.

El malware Diskcoder.C ejemplificó lo decepcionante que pueden ser las apariciones en el mercado cibercriminal. Partiendo de las tendencias previas y contrario a las creencias iniciales, este malware resultó ser un limpiador destructivo, más que un ransomware que debería, al menos en teoría, ser capaz de revertir sus propios cambios.

Diskcoder.C utilizó una versión modificada del exploit EternalBlue, al igual que WannaCryptor, pero fue más allá dentro de los sistemas de las víctimas. En vez de cifrar archivos individuales, su payload sobrescribió el Master Boot Record (MBR) del disco duro e impulsó un reinicio. En consecuencia, si bien la nota de rescate y demanda por una llave de desbloqueo aparecieron en la pantalla, era sólo el malware lo que se iniciaba una vez terminado el reinicio de la máquina, y no existía manera de recuperar los archivos.



En la raíz de esta epidemia global había un compromiso exitoso del software contable M.E.Doc, popular en varias industrias en Ucrania. Un número de organizaciones ejecutaron una actualización troyanizada de M.E.Doc y sufrieron la infección, con el malware luego propagándose en sistemas globales mediante negocios interconectados con sus socios ucranianos. Las multinacionales globales registraron daños de cientos de millones de dólares estadounidenses. Mientras ese daño puede ser considerado como colateral, dejó al descubierto la magnitud de la amenaza que los ataques de malware representan para las infraestructuras y cadenas de suministros.

EN LA MADRIGUERA DE BAD RABBIT

Avanzando al 24 de octubre, una variante de la familia Diskcoder con capacidades similares a las de un gusano, trajo consigo otro colapso en ciberseguridad, aun si la infección se confinó principalmente a Rusia y Ucrania. Denominado Diskcoder.D y también llamado Bad Rabbit, se propagó con el aspecto de una falsa actualización de Flash mostrado como un pop-up en sitios de noticias legítimos – pero infectados. Aparte de forzar su camino por las redes, también hizo uso de EternalRomance, otro exploit SMB filtrado por Shadow Brokers.

LOS DISPOSITIVOS MÓVILES NO QUEDAN FUERA

La plataforma Android, con casi una década de antigüedad, permanece como el principal objetivo de los criminales que atacan dispositivos móviles, y específicamente, el ransomware móvil ha ido creciendo de manera continua como amenaza mundial durante ya un buen tiempo. Los troyanos bancarios se mantienen como otro pilar en el espacio Android. De hecho, ambas funcionalidades podrían unirse, como halló a comienzos de este año Lukáš Štefanko, malware researcher de ESET.

Štefanko descubrió un tipo de ransomware de Android con dos puntas. Por un lado, DoubleLocker no sólo cifra los archivos del usuario, sino que también bloquea el dispositivo modificando el PIN. A su vez, es también el primer ransomware que se conoce que se haya difundido haciendo uso incorrecto de los servicios de accesibilidad de la plataforma.

DoubleLocker deriva de una familia de malware bancarios ya establecida y puede convertirse en lo que Štefanko llama 'ransom-bancario', capaz de limpiar la cuenta bancaria o de PayPal del usuario antes de bloquear el dispositivo y los datos y demandar un rescate. Una prueba de este 'ransom-banker' fue detectada en mayo de 2017.

En la segunda parte de nuestra Ciberseguridad en 2017, el foco estará puesto sobre la (in)seguridad de los datos, las vulnerabilidades y los peligros de enfrentarse a infraestructura crítica.