Estudios CEEAG

Julio 2017 Número 19

CIBERSEGURIDAD
¿POR QUÉ NOS ESTAMOS PONIENDO VULNERABLES?

GDB (R) René Leiva Villagra[1]

Respecto a los ciberataques de Junio del 2017, Brad Smith, presidente y director jurídico de Microsoft escribió: "Un escenario equivalente con armas convencionales sería que al Ejército estadounidense le roben algunos de sus misiles Tomahawk".

Resumen

Este artículo orienta a una visión de la forma como los sistemas cibernéticos han ido avanzando en el tiempo en capacidad de transmisión y proceso, como también han ido exponiéndose a diferentes amenazas que los han hecho más vulnerables.

Sostiene en ello que la masificación de instrumentos con capacidad computacional o de automatización ha aumentado el universo existente, por ende ha crecido el número de dispositivos que pueden ser víctimas o victimarios.

Palabras claves

Ciberguerra, cibernética, ciberespacio, ciberdefensa, malware, software malicioso.

[1] René Leiva es General de Brigada (r) Ejército de Chile. Licenciado en Ciencias Militares y Magister en Ciencias Militares con mención en Planificación y Gestión Estratégica en la Academia de Guerra del Ejército de Chile. Diplomado de la Pontificia Universidad Católica de Chile en Gestión en Educación. Especialista en Inteligencia y Guerra Electrónica. Investigador del Centro de Estudios Estratégicos de la Academia de Guerra del Ejército de Chile. Email: rene.leiva@acague.cl leivarene@yahoo.com

Introducción.

El martes 27 de junio del 2017, algo que ya era esperable se hizo realidad. Una nueva oleada de agresiones cibernéticas atacaba varios objetivos multinacionales. El agente agresor nuevamente se presentaba como un malware tipo 'Ransomware' (que genera una suerte de "secuestro virtual" de los archivos al capturarlos en su origen, encriptarlos y solo devolverlos a su normalidad previo pago de un rescate monetario). Esta nueva agresión habría sido perpetrada mediante un virus denominado "Petrwrap", que corresponde a una variante "Ransomware Petya" usado en ataques anteriores, con una cercana similitud al Wannacry, de triste memoria en su mega bloqueo del 12 de mayo del 2017, que afectó a más de 150 países, con efectos aun no cuantificados en su totalidad.

Una visión del origen del problema.

Vamos al origen de esto. En 1948 aparece la cibernética, aportando con ello un enorme mejoramiento a las capacidades de procesos, tanto como en la amplitud de las aplicaciones desarrolladas. Así los requerimientos de velocidad en la transmisión y necesidades de almacenamiento de datos fueron en constante ascenso, demandando mayores avances tecnológicos. Rapidez y memoria eran los factores iniciales de cada "armatoste cibernético", caracterizados en sus inicios por sus grandes dimensiones volumétricas y consumos de energía.

La conformación de grandes bases de datos aisladas, desconectadas unas de otras, contenidas en un computador aislado de su entorno, acumulando enormes cantidades de información que no podían salir de él, pasó a constituir un problema tecnológico que había que solucionar, por lo que la aparición en enero de 1983 de ARPANET y el protocolo TCP/IP vino a abrir los ojos respecto a que los próximos desafíos irían más allá de la capacidad de proceso y almacenamiento, marchando decididamente a lograr mayor y mejor conectividad.

Por ello, en el pasado, los sistemas informáticos eran relativamente seguros, por encontrarse conectados a una reducida cantidad de subsistemas externos y por constituir elementos de gran valor monetario y dimensión volumétrica, lo que los hacía escasos. Hoy en día, el vertiginoso avance tecnológico ha transformado los antiguos dinosaurios computacionales en dispositivos que han mutado a aparatos con reducción de sus tamaños y costos, por lo tanto mucho más masivos, junto a ser diseñados como dispositivos de arquitecturas abiertas, fácilmente portables y con amplia conectividad a sistemas locales, regionales e incluso internacionales, de transferencia de información de gran velocidad y compleja identificación de su punto de origen.

Lo anterior incide en tener una percepción de disminución en los niveles de seguridad si los contrastamos con los inicios de la informática, donde los eventos de vulnerabilidad eran menores o casi inexistentes, precisamente porque los computadores eran cajas autárquicas, con circuitos de información cerrados, sin conexión externa, por lo tanto aislados de amenazas y distantes de los riesgos.

¿Por qué estamos siendo más vulnerables?

Pero un análisis más detallado de lo antiguo con lo moderno en sistemas computacionales nos lleva a una contrastación de los protocolos de transmisión, verificación, encriptación y proceso, donde se presenta una calidad actual que es exponencialmente superior. Entonces, si las medidas de seguridad presentes son mayores que las del pasado, ¿por qué se da una cantidad mayor de eventos de vulnerabilidad o intrusión informática? La respuesta implica varios factores:

Uno es la cantidad mayor de dispositivos computacionales existentes. Como ya se dijo, los antiguos eran muy grandes de tamaño, de alto consumo eléctrico y de alto costo, lo que solo permitía a escasas instituciones y muy pocos privados contar con un ordenador. En contraste, los nuevos aparatos son de presencia masiva, de costo alcanzable para gran parte de la población, lo que sumado no solamente a computadores, sino que a dispositivos con características informáticas como móviles telefónicos, aparatos "inteligentes", tablets y otros, que hacen mucho mayor el número de elementos conectados a la red. Sumemos a ello el impacto que ya está teniendo el Internet de las Cosas (IoT), lo que agrega un universo enorme de dispositivos enlazados vía WEB, tanto para actividades domésticas, industriales, comerciales, personales y financieras, entre otras. Buena parte de estos dispositivos no están lo suficientemente protegidos, tal como lo afirma el reporte técnico de McAfee Labs[2].

La masificación de instrumentos con capacidad computacional o de automatización ha aumentado el universo existente, por ende el número de dispositivos que pueden ser víctimas o victimarios.

Otro factor que ha aumentado el grado de incidencia de los eventos maliciosos es el desarrollo de nuevas formas de optimización de la plataforma de comunicación. Luego, al estar disponible una mayor capacidad de conectividad, las aplicaciones a disposición del usuario han crecido en número y en demanda de ancho de banda (antes no disponible). Por ello, claramente la cantidad de dispositivos móviles con acceso a Internet ha crecido enormemente, superando la de computadores fijos. Junto a ello, la mayoría de estos dispositivos emulan capacidades GPS (localización terrestre), con una tendencia cada vez

[2] McAfee Labs, Informe sobre Amenazas, Abril 2017.

mayor de contar con LBS (Land Base Systems) que proveen a los usuarios de información en tiempo real, con datos como información de viaje, traslados, navegación, tráfico, meteorológica, turismo, ofertas de retail, emergencias en la ruta, ayuda en accidentes, pagos en línea, entre muchas otras a nombrar. Eso hace a los usuarios tener una necesidad de permanencia conectados a la web, lo que también aumenta los tiempos de riesgo, al estar expuestos permanentemente a amenazas.

La restricción ahora parece haberse volcado más al hardware, donde las limitaciones de capacidad de carga de la batería están marcando el límite de la portabilidad a horas de autonomía de energía.

Otro desarrollo va por la vía de los lugares donde se realiza el proceso y el almacenamiento. Cisco estima que para el 2019 los data centers "en la nube" van a procesar el 86% de toda la data que es necesaria de transferir. Esa tendencia es motivada porque los servidores en la nube son dinámicamente escalables en tecnología, tienden a la automatización de muchos de sus procesos de mantención y respaldo. Por ello, muchos softwares operan virtualizadamente en la red, sin habitar en el dispositivo usuario, el cual va a buscar la aplicación a un servidor en la nube cada vez que la necesite y la va a operar remotamente, con el necesario traspaso de data que ese efecto implica. En ese ambiente de nubes, aplicaciones virtuales y flujos de data, que se conecta por un entramado que no es necesariamente vertical ni jerarquizado, sino que transversal y funcional, corre un estimado 80% de tráfico, bajo el riesgo de operar en bypass de las interfaces de ciberprotección. Acá se remarca el riesgo existente ya que lo que es una ventaja, la multiconectividad, pasa a ser una amenaza al abrir la red a una variedad de dispositivos, aplicaciones, conexiones en la nube, accesos externos dinámicos, todos ellos representando blancos que un ciberagresor va a dimensionar en su valor de disponibilidad de ingresar archivos o programas maliciosos al sistema.

Muchos de estos agentes maliciosos se ocultan en la forma de tráfico de red legítimo o archivos adjuntos, a la vez que explotan funciones de control de acceso a la red e impactan repetidamente en las corazas que tiene el sistema, explorando y buscando las vulnerabilidades que pueda tener, muchas veces encontrándolas. En ello, lo usual es que los atacantes usen sucesiva y/o simultáneamente variados medios y vectores de entrada, para asegurar su éxito.

Independiente del modo de intrusión, los archivos maliciosos pueden clasificarse en tres tipos, siguiendo la norma de Check Point Security Report, en malware conocido, desconocido y de Día Cero (Zero-Day)[3].

[3] Check Point, Security Report 2016, The Attack Arsenal.

Malware conocido corresponde a un elemento completo o segmentado de software malicioso, que cuenta con una huella o firma que es reconocible. Muchas de las herramientas de seguridad usan esta huella cuando analizan la red, para de ahí aplicar técnicas de bloqueo como solución. En ello, la mantención al día de los antivirus y firewalls es un requerimiento fundamental.

El malware desconocido obedece a un software no identificado, que no cuenta con una firma que sea reconocible o identificable. Muchas veces un malware desconocido es creado mediante una simple modificación a un software maligno identificado o generando una alteración al tren de data. Así la nueva versión es “disfrazada” y pasa sin ser detectada por las defensas basadas en identificación de huellas.

Los virus de Día Cero (Zero Day) explotan una vulnerabilidad del sistema, para ingresar en él, alojarse y esperar la instrucción técnica de ejecución, tal como podría ser una bomba a control remoto.

Hacia algunas soluciones

Las soluciones a lo anterior no son simples y se vislumbran en variados niveles:

En lo que es el usuario, se presenta el desafío de hacer aún más amigable la adopción de trabajo en la nube para el operador convencional, decreciendo las exigencias de dominio de destrezas en ciberseguridad, llevándolas a un ambiente más automatizado pero sin perder las prestaciones de protección que el sistema debe proveer para que sea confiable.

En el nivel de la estructura, se requerirá de un segmento de administradores de red de conocimientos más avanzados, con un plan auditable y satisfactorio de respuesta a incidentes, con capacidad de detectar, contener el daño, y minimizar el riesgo.

Junto a ello, debe ser revocada la tendencia a encapsular en el secreto la detección de estos eventos anómalos, abriéndose a notificarlos a los organismos externos que corresponda.

La acción futura debe ser colaborativa, coordinada y célere. De no serlo, el malware se instalará cual maleza en sembradío, con los altos costos que ello implicará.

BIBLIOGRAFÍA

Check Point, Security Report 2016, The Attack Arsenal.

McAfee Labs, Informe sobre Amenazas, Abril 2017.

Sánchez Cordero Pedro, Ciberguerra y Ciberdefensa, Conexión Inversa, España.