Check Point
SOFTWARE TECHNOLOGIES LTD

YA ESTÁ AQUÍ LA 5ª GENERACIÓN DE CIBERATAQUES, Y LA MAYORÍA DE LAS EMPRESAS ESTAN REZAGADAS

Un nuevo modelo para evaluar y planificar la seguridad

GEN V

TABLA DE CONTENIDO

CONTEXTO

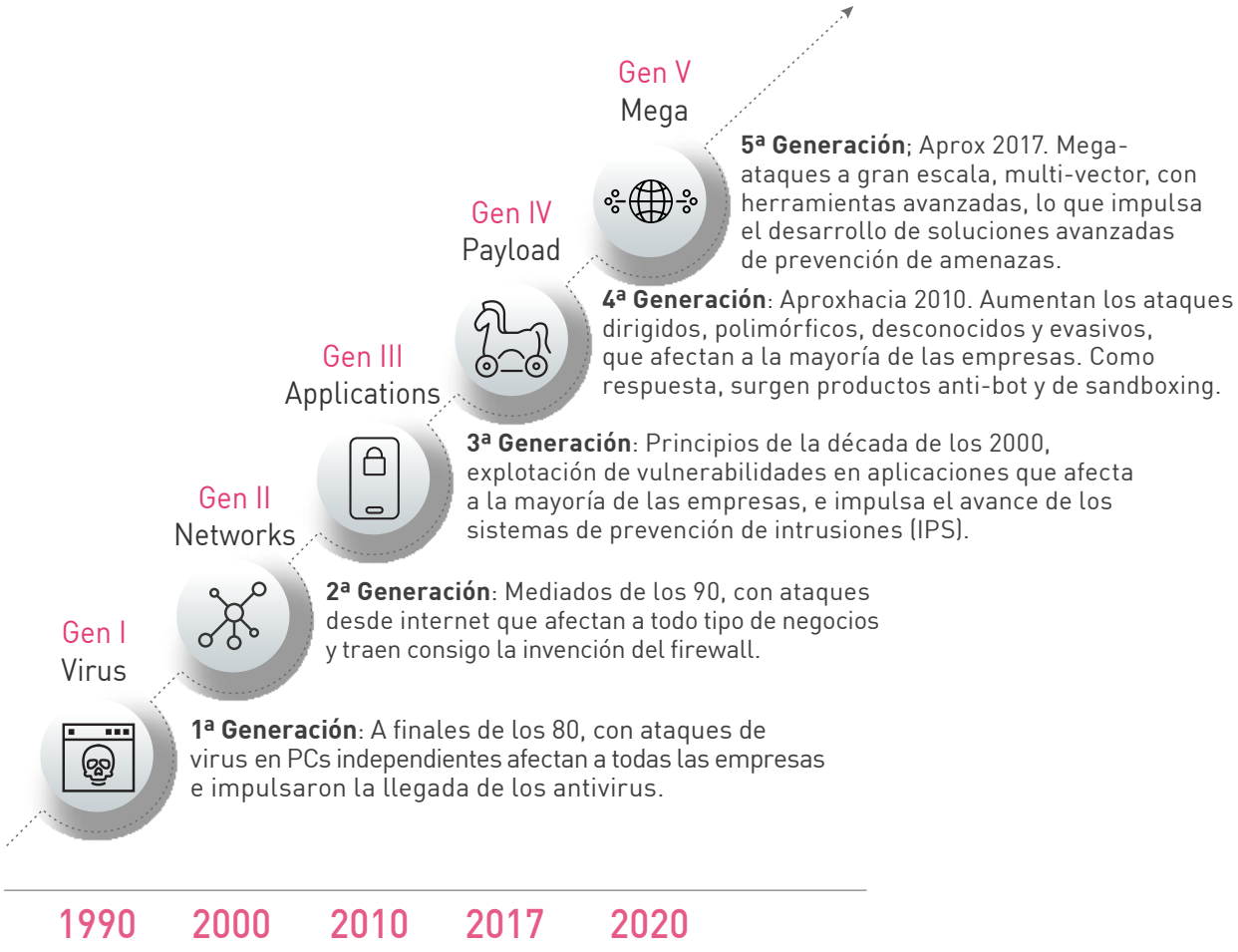
En los últimos 25 años, los ciberataques y la ciberseguridad han avanzado rápidamente. Mirando atrás, es fácil identificar diferentes generaciones de ataques y de soluciones de seguridad para protegerse de ellos. Sin embargo en la actualidad la velocidad de la evolución de los ataques es mucho mayor que el nivel de seguridad que han desarrollado las empresas. Esto es un problema. El nivel de seguridad implementado por las empresas no puede estar rezagado con respecto al nivel de los ataques que las amenazan. Los ataques actuales son los más avanzados y de mayor impacto que hemos visto, y sin embargo la seguridad implementada por la mayoría de las empresas es obsoleta e incapaz de proteger contra dichos ataques.

Hay muchas razones por las que las infraestructuras de seguridad se han quedado atrás a medida que el nivel de los ataques ha ido aumentando. La más obvia es que los atacantes no tienen restricciones. Pueden definir y empujar los límites, incluso romper las reglas, en el desarrollo de técnicas nuevas y más avanzadas. Las empresas, por supuesto, tienen procesos de control de cambios, restricciones presupuestarias, reglas de cumplimiento y otras muchas limitaciones operativas a las que deben adaptarse, lo que restringe el avance de la seguridad. Otra razón es el método tradicional de construir una infraestructura de seguridad donde una tecnología específica es desplegada para defenderse de un tipo de ataque específico, o para proteger un tipo concreto de aplicación. Este enfoque binario, mono-visión, también conocido como “de soluciones puntuales”, fue efectivo en generaciones anteriores, cuando los ataques eran unidimensionales, pero los ataques actuales son multi-todo: multi-dimensionales, multi-escenario, multi-vector y polimórficos... Proteger adecuadamente las operaciones de TI de una empresa actualmente requiere un enfoque nuevo, integral, para evaluar y diseñar la seguridad en función de una infraestructura integrada y unificada que prevenga los ataques en tiempo real.

El marco generacional descrito en este documento es una herramienta nueva y muy importante para las organizaciones de cara a evaluar su seguridad actual en relación al nivel de los ataques que están sucediendo a diario. Esta es una forma nueva y muy efectiva de evaluar su postura general de seguridad. Para la mayoría de las empresas, esta evaluación revelará la cruda realidad de que, a pesar de todos sus esfuerzos, su nivel de protección está generaciones por debajo del nivel de los ataques que a los que habrán de hacer frente.

Las generaciones de los ciberataques y la ciberseguridad

Es la aparición –y más tarde el avance continuo– de los ataques lo que ha llevado a la creación y posterior avance de los productos de seguridad. Mirando atrás, se pueden ver diferentes líneas generacionales en los avances de los ataques y de las soluciones de protección, cada una de ellas más sofisticada que la anterior. Primero las redes, y luego Internet, han conectado a personas, empresas y gobiernos como nunca antes en la historia humana. Esta conectividad también ha creado una nueva gran frontera, que también supone un nuevo escenario rico en objetivos para el crimen y las actividades ilícitas. Desde curiosos hackers hasta espionaje patrocinado por empresas y estados o el cibercrimen organizado, el nuevo mundo conectado ha proporcionado acceso casi sin limitaciones a todo tipo de activos y datos privados... ¡con casi total anonimato! Como no podía ser de otro modo, cada avance con éxito de la actividad maliciosa ha impulsado el correspondiente avance en la ciberseguridad. Esta evolución cíclica, sin duda, continuará.



"Solo el 5% de las empresas está utilizando ciberseguridad de 5ª generación"

1ª GENERACIÓN

INTRODUCCIÓN

La 1ª generación comenzó en la década de los 80, coincidiendo con la llegada de los ordenadores personales y su uso masivo por parte del público. Pronto aparecieron los primeros ataques de virus, que eran programas de software malicioso que se auto-replicaban en otros ordenadores. Estos ataques de virus afectaban a todo tipo de negocios y usuarios de computadores personales. El impacto de estos ataques de virus fue lo suficientemente grande y disruptivo y entonces comenzaron a desarrollarse productos antivirus para protegerse contra ellos.

Proliferación

Ordenadores personales operados como dispositivos autónomos (stand-alone). Para compartir ficheros entre usuarios y ordenadores se utilizaban disquetes floppy. De este modo, también, comenzaron a proliferar los virus.

Los atacantes

Es en esta era donde surgieron los "hackers desde el sótano de sus padres". El término "hackeo informático", y finalmente "hackeo" se hizo común en los 80 para referirse a aquellos que escribían programas de software para inhabilitar o atacar ordenadores. Estos hackers eran sobre todo adolescentes curiosos que actuaban por pura diversión, y por el reto de penetrar las defensas de los sistemas. Muchos escribían virus, también, buscando reconocimiento y para crearse una reputación personal como creadores de programas inteligentes. Trascendiendo el ámbito particular, los hackers avanzaron y se organizaron a través de redes de "boletines electrónicos" (BBS, por sus siglas en inglés) que les otorgaban anonimato y libertad para compartir conocimientos y logros entre sus colegas.

Ejemplos de ataques conocidos de 1ª Generación

Elk Cloner

Elk Cloner es conocido como el primer virus escrito y publicado para infectar ordenadores personales. Codificado como una broma por Richard Skrenta, por entonces de 15 años, era sobre todo una molestia, que ocasionalmente mostraba un poema en el ordenador "infectado".

> *"Cuando Rich Skrenta creó Elk Cloner como una broma en febrero de 1982, era un estudiante de secundaria de 15 años con una precoz habilidad para la programación y un interés desmedido por los ordenadores. Este virus boot sector (que afectaba al arranque de los ordenadores) se escribió para sistemas Apple II, que eran los ordenadores domésticos predominantes en aquella época, a través de disquetes infectados.*
>
> *Si se arrancaba un Apple II desde un disquete infectado, Elk Cloner se convertía en un fichero residente en la memoria del ordenador. Los discos que se insertaban en este ordenador recibían una dosis del malware en el momento en que el usuario escribía en el catálogo de comandos para obtener una lista de archivos.*

> *Los ordenadores infectados mostraban un poema breve, escrito también por Skrenta, cada 15 arranques desde un disco infectado:*
>
> *Elk Cloner: El programa con personalidad*
>
> *¡Se adueñará de tus discos, se infiltrará en tus procesadores! ¡Sí, es Cloner!*
>
> *¡Se pegará a ti como la cola! ¡Modificará la memoria! ¡Es Cloner! ¡Pásalo!"* [1]

Brain

Brain es considerado el primer virus a nivel mundial. Fue creado por error en 1988, cuando dos hermanos, Basit y Amjad Farooq Alvi, escribieron lo que creyeron que sería un mecanismo para evitar la copia ilegal de sus productos de software. Sin embargo, su diseño era defectuoso, y su herramienta se convirtió en un virus real que se copiaba y replicaba.

> *"Considerado como el primer virus de PC a nivel mundial, Brain se activaba al cambiar el sector de arranque de un disquete. Cuando el disquete infectado se insertaba en un ordenador, instalaba Brain en su memoria, desde donde infectaba otros nuevos disquetes cuando se insertaban".* [2]

Tecnologías de seguridad desarrolladas como resultado de los ataques de 1ª generación

En respuesta al creciente número de virus y software malicioso, se desarrollaron muchas herramientas y, finalmente, productos comerciales para combatirlos, concretamente productos antivirus. Dos ejemplos tempranos son:

- En 1985, G Data Software lanzaba su primer producto antivirus para la plataforma Atari ST. [3]
- En 1987, John McAfee fundaba McAfee y lanzaba su primer antivirus, VirusScan.

> *A modo de profecía, en 1987 Fred Cohen escribió: "... no hay algoritmo que pueda detectar todos los posibles virus para ordenadores."* [4]

Implicaciones a nivel de infraestructura de seguridad

Si bien había controles a nivel de contraseña para acceder a los PC, e incluso controles adicionales para acceder a los archivos, la única "infraestructura de ciberseguridad" en esta generación eran los productos antivirus.

1. Referencia: *https://www.theregister.co.uk/2012/12/14/first_virus_elk_cloner_creator_interviewed/*
2. Referencia: http://www.zdnet.com/pictures/ten-computer-viruses-that-changed-the-world/
3. Referencia: *https://en.wikipedia.org/wiki/Antivirus_software*
4. Referencia: *https://antivirussw.weebly.com/history.html*

2ª GENERACIÓN

INTRODUCCIÓN

La 2ª Generación surge en los 90, con la llegada de las redes e Internet. Todo el mundo quería "conectarse" Con las redes conectando ordenadores e Internet conectando gobiernos, empresas y público en general, se abrían las puertas a una amplia y rápida propagación de software malicioso y volátil. Este acceso sin restricciones a todo aquello que estuviera conectado, llevó al desarrollo del firewall de red.

Proliferación

La conectividad de red permitió compartir información pasando de la velocidad de los disquetes a la velocidad de los ordenadores conectados a redes. Por supuesto, la velocidad y la propagación de los ataques crecieron de igual modo.

Los atacantes

La llegada de las redes puso fin a las "BBS piratas" a medida que los hackers comenzaron a movilizarse, organizarse y comunicarse a través de la World Wide Web y los sitios web. Este aumento en la conectividad, a su vez, hizo aumentar la propagación y el daño desde aquellos bromistas iniciales para dar comienzo las primeras etapas, aún incipientes, del cibercrimen.

Ejemplos de ataques conocidos de 2ª Generación

Morris

El "gusano" Morris fue lanzado en los primeros días de Internet, en noviembre de 1988. Robert Morris, un estudiante de la Universidad de Cornell, creó el gusano Morris con intenciones aparentemente inocentes. Él afirma que desarrollo este gusano con el objetivo de medir el tamaño de Internet. Desafortunadamente, el gusano contenía un error que causaba que infectara repetidamente los ordenadores consumiendo sus recursos y creando condiciones de denegación de servicio. Se estima que Morris infectó hasta 60.000 sistemas host a través de Internet, y puso de manifiesto que la seguridad en las redes y en Internet era muy necesaria.

> *"El código fuente muestra que Morris intentó mantener la propagación del gusano bajo control, pero confió en su código más de lo que debía". Los errores en el código provocaron el bloqueo de muchos sistemas (básicamente todos los sistemas SunOS), y que se ejecutara mas de una vezen muchos otros sistemas, devorando sus recursos".* [5]
>
> *"Todo el mundo se dio cuenta entonces que la seguridad de los ordenadores ya no era sólo teoría, sino algo que había que tomar muy en serio."* [6]

5. Referencia: *http://www.zdnet.com/article/the-morris-worm-internet-malware-turns-25/*
6. Referencia: *http://www.zdnet.com/article/the-morris-worm-internet-malware-turns-25/*

¿El primer ciber-robo?

El artículo "*The First Great Cyber Crime: 1994 Attack Against Citibank*", publicado en CTOVision.com, señala que éste es posiblemente el primer robo económico ejecutado mediante un ciberataque. Está descrito también por el FBI:

> *"Las dimensiones globales del cibercrimen se hicieron claramente visibles ya en 1994. En el verano de ese año, desde el corazón de Rusia, un joven informático llamado Vladimir Levin robaba un banco estadounidense sin ni siquiera levantarse de su silla. Durante dos meses, Levin, con la ayuda de otros muchos conspiradores, penetró en los sistemas de Citibank y logró transferir más de 10 millones de dólares a cuentas de todo el mundo utilizando un servicio de transferencia por teléfono. Trabajando con Citibank y las autoridades rusas, los agentes del FBI pudieron rastrear el robo, lo que les llevó de vuelta a Levin en San Petersburgo. Levin pronto fue trasladado a Londres y arrestado".*

Virus Melissa

En 1999, David Smith, un programador de redes, lanzó el Virus "Melissa" en Internet. Estaba contenido en una macro de Microsoft Word que cuando se abría, se enviaba por correo electrónico a las primeras 50 direcciones de email del archivo de direcciones MAPI del ordenador. Aparentemente, la motivación principal de Smith era la curiosidad. Melissa dejó 100.000 servidores de email fuera de servicio y causó más de 80 millones de dólares en daños y perjuicios.

> *'Melissa.A' utilizaba en cierto modo técnicas de ingeniería social, ya que venía con el mensaje "Aquí está el documento que me pidió... no se lo muestre a nadie". En solo unos días, el virus protagonizó uno de los casos más importantes de infección masiva de la historia, causando daños de más de 80 millones de dólares a compañías estadounidenses. Compañías como Microsoft, Intel y Lucent Technologies tuvieron que bloquear sus conexiones de Internet debido a él".* [7]

Tecnologías de seguridad desarrolladas como resultado de los ciberataques de 2ª generación

En respuesta al "Salvaje Oeste" de acceso libre y abierto a todo aquello que estuviese conectado, una serie de innovadores y emprendedores desarrollaron el primer firewall de red para controlar el acceso a redes privadas desde la internet pública. Básicamente, el firewall de red es una barrera entre dos redes a través de la cual debe pasar todo el tráfico y que establece reglas para determinar qué parte del tráfico se permite y qué parte del tráfico se bloquea. Ejemplos de los primeros firewalls son:

En 1991, Digital Equipment Corporation lanza el firewall DEC SEAL.

7. Referencia: *https://www.pandasecurity.com/mediacenter/malware/most-famous-virus-history-melissa/*

En 1994, Trusted Information Systems presenta un Firewall Toolkit (FWTK) de código abierto con el nombre de Gauntlet.

También in 1994, Check Point lanza el Firewall-1, el primer firewall con "stateful inspection", que le permite rastrear el estado operativo de la red y evaluar cada paquete dentro del contexto de su conexión.

Implicaciones para la infraestructura de seguridad

El firewall y los productos antivirus son esenciales para la protección de cualquier empresa o entidad que tenga conectadas sus redes internas a Internet. Se puede afirmar que el firewall y el antivirus son la primera "infraestructura de ciberseguridad" real. Esta era marca también el comienzo del modelo de seguridad basado en "soluciones puntales" para seleccionar e implementar productos ad hoc para proteger contra amenazas específicas o para proteger servicios concretos.

3ª GENERACIÓN

INTRODUCCIÓN

La 3ª Generación surge a principios de siglo, cuando los atacantes aprenden a aprovechar vulnerabilidades en todos los componentes de las infraestructuras de TI. IETF RFC 2828 define "**vulnerabilidad**" como "*defecto o debilidad en el diseño, implementación u operación de un sistema que podría ser explotado para violar las políticas de seguridad de dicho sistema*."

Y las vulnerabilidades eran cada vez más numerosas En un momento dado, había muchas de ellas en sistemas operativos, aplicaciones... cualquier elemento de cualquier infraestructura de TI presentaba vulnerabilidades de las que un avezado atacante podría sacar partido para obtener acceso a una red privada. Los ataques dirigidos contra vulnerabilidades no podían ser detenidos de manera efectiva por firewalls, antivirus o sistemas de detección de intrusos (IDS). De modo que los productos de IDS avanzaron para dar paso a los sistemas de prevención de intrusiones (IPS), que tenían capacidad no sólo de detectar, sino también de prevenir atraques contra las diferentes vulnerabilidades.

Proliferación

"Sofisticación" es una palabra muy utilizada en la actualidad para describir algunos ciberataques. Esta 3ª generación mostraba ya los primeros indicios de sofisticación en el ataque. En lugar de escribir virus o gusanos que luego podían propagarse erróneamente, en esta era los atacantes comenzaron a analizar las redes y los productos de software para identificar debilidades y vulnerabilidades específicas contra las que diseñar ataques para penetrar e interrumpir las operaciones y/o para robar activos. Y en ocasiones los ataques eran encubiertos en un velo blanco de "ingeniería social" que invitaba a los usuarios a hacer clic, lo que iniciaba la infección.

Los atacantes

La industria de TI está en auge en estos momentos, creando nuevos productos, herramientas, aplicaciones y servicios para satisfacer las necesidades de un mercado hambriento que se mueve activa y agresivamente hacia el mundo online y los atacantes comienzan a entender el botín que les espera. Se hicieron más organizados y sofisticados, menos interesados en la notoriedad y ´mucho más en hacer dinero rápido a través de medios ilícitos: el cyber hacking.

Ejemplos de ataques conocidos de 3ª Generación

ILOVEYOU

El virus ILOVEYOU fue lanzado el 4 de mayo de 2000, y en cuestión de minutos había infectado miles de ordenadores. Fue tal su alcance y su impacto que ese mes fue portada en la *revista* TIME . Las empresas y proveedores de antivirus optaron por filtrar todos los emails con el título "ILOVEYOU", pero los atacantes, simplemente, cambiaron el título para continuar con su propagación.

> *"El virus ILOVEYOU viene oculto en mensajes de email con el asunto "I LOVE YOU" y contiene un adjunto que, cuando se abre, hace que el mensaje se reenvíe a todos los contactos de la lista de direcciones de Microsoft Outlook, y quizá , lo que es más grave, la pérdida de todos los archivos JPEG, MP3 y de algunos otros formatos del disco duro del destinatario. Dado que Outlook está ampliamente instalado como sistema de correo electrónico mayoritario en las redes corporativas, el virus ILOVEYOU puede propagarse rápidamente de usuario a usuario dentro de cualquier organización. El 4 de mayo de 2000, el virus se propagó tan rápidamente que algunas grandes empresas, como Ford Motor Company, tuvieron que apagar sus sistemas de correo electrónico. El virus llegó´, en un solo día, a unos 45 millones de usuarios".* [8]

SQLSlammer

SQLSlammer, también conocido como "Sapphire", entre otros nombres, atacó vulnerabilidades en Microsoft SQL Server y MSDE, y se convirtió en el gusano de más rápida propagación de todos los tiempos.

> *"A medida que comenzó a propagarse por Internet, su tamaño se duplicaba cada 8,5 segundos. Consiguió infectar a más del 90 por ciento de los hosts vulnerables en sólo 10 minutos." ... El gusano "comenzó a infectar hosts poco antes de las 05:30 UTC el sábado 25 de enero. Sapphire explotaba una vulnerabilidad que provocaba la saturación del búfer en ordenadores conectados a Internet que ejecutaban Microsoft SQL Server o MSDE 2000 (su motor de escritorio). Esta debilidad, localizada en un servicio de indexación subyacente, fue descubierta en julio de 2002; Microsoft lanzó un parche para la vulnerabilidad antes de que está fuera anunciada. El gusano afectó, al menos, a 75.000 hosts, quizá muchos más, y causo caídas en redes y consecuencias tan imprevistas como vuelos cancelados e interferencias en elecciones y fallas en cajeros automáticos."* [9]

8. Referencia: http://searchsecurity.techtarget.com/definition/ILOVEYOU-virus
9. Referencia: https://www.caida.org/publications/papers/2003/sapphire/sapphire.html

Estonia

El 27 de abril de 2007, la Unión Europea y Estonia, país miembro de la OTAN, fueron víctimas de ciberataques masivos contra sus infraestructuras.

> Estos ataques *"... inundaron sitios web de organizaciones en Estonias, incluidos el Parlamento del país, bancos, ministerios, periódicos y emisoras de radio, en medio del desacuerdo con Rusia sobre el traslado del "Soldado de Bronce" de Tallin, una estatua-mausoleo de la era soviética, y otras tumbas de guerra emplazadas en esta localidad. La mayoría de los ataques que impactaron al público en general se distribuyeron como ataques de denegación de servicio, desde individuos particulares usando varios métodos (por ejemplo, inundaciones de pings), hasta costosos alquileres de botnets usualmente utilizadas para la distribución de spam. También se produjeron ataques de spam contra los principales portales de noticias a través de comentarios y desfiguración de sitios web incluyendo el que sufrido por la web del Partido Reformista de Estonia."* [10]

Tecnologías de seguridad desarrolladas como resultado de los ataques de 3ª Generación

La industria de la seguridad, con emprendedores muy jóvenes pero muy brillantes, respondió a esta explosión en las vulnerabilidades y en los ataques contra las mismas con los sistemas de detección de intrusos, que pronto evolucionaron para dar lugar a los productos de prevención de intrusiones. Después de todo, si puedes detectar un ataque... ¿por qué no prevenirlo?
La protección principal que ofrecen los productos IPS es que protegen la explotación de vulnerabilidades conocidas. Son productos basados en firmas, lo que significa que se escribe una firma para cada una de las vulnerabilidades conocidas y de alto nivel, con objeto de detectar aquellas actividades que podrían estar intentando aprovechar alguna de estas vulnerabilidades. Los productos IPS son realmente un avance más allá del antivirus y el firewall, porque inspeccionan el tráfico de la red, paquete por paquete, buscando coincidencias de firmas o actividades anómalas o sospechosas. Cuando se registra una coincidencia, el ataque es bloqueado. Sin embargo, la precisión en la prevención es un desafío, ya que los "falsos positivos" son un obstáculo que dificulta la adopción de sistemas IPS.

Implicaciones en la infraestructura de seguridad

En esta era se produce una explosión en el número y diversidad de las tecnologías y servicios, y al mismo tiempo una explosión de proveedores de seguridad y productos para protegerlos. Las startups y los proveedores de seguridad crean rápidamente nuevos productos, especializados en diferentes "segmentos" de seguridad, desde firewalls hasta antivirus, detección de intrusos, aplicaciones web, sistemas peer-to-peer, telefonía por Internet, y muchos más.

Esta es también la época en la que comienzan a ganar peso los modelos de "soluciones puntuales" de cara a la construcción de infraestructuras de seguridad. Para cada nuevo tipo de ataque y cada nuevo tipo de servicio o aplicación de TI, las empresas agregarían un nuevo producto de seguridad para protegerse contra ese ataque o para proteger ese servicio. En casi todos los casos, el nuevo producto sería de un proveedor de seguridad diferente, especializado en el área de seguridad que hay que cubrir. Esto lleva a infraestructuras de seguridad compuestas por múltiples productos, de múltiples proveedores, cada uno con su propia interfaz de usuario y su consola de gestión, lo que pronto comenzaría a ser complejo e ineficiente desde el punto de vista operativo. Y, lo que es más importante: el nivel de protección comenzó a caer por debajo del nivel de los ataques que se estaban ejecutando.

10.Reference: *https://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia*

4ª GENERACIÓN

INTRODUCCIÓN

La 4ª Generación emerge aproximadamente en el año 2010, cuando los atacantes alcanzan nuevos niveles de sofisticación. De hecho, los atacantes y sus métodos pueden considerarse ya como profesionales. Los ataques iban desde el espionaje internacional hasta brechas masivas de información personal o interrupciones de Internet a gran escala. Los ataques de esta generación llenarán titulares en los principales diarios, simplemente por el impacto a gran escala y la relevancia para el público en general. Los ataques llegaron hasta las juntas directivas, hasta los CEOs, y motivaron investigaciones gubernamentales.

Si bien la seguridad de 2ª y 3ª generación proporcionaba control de accesos e inspeccionaba todo el tráfico de red, presentaba importantes carencias a la hora de validar el contenido real recibido por los usuarios a través de emails, descargas de archivos u otros medios. Los ataques se ocultaban en todo tipo de archivos, desde currículums hasta archivos de imágenes, con un sofisticado código listo para activarse y propagarse, y en ocasiones soportados por enormes ejércitos de bots listos para quebrar las defensas. Todo lo que se necesitaba era que el usuario, sin saberlo, hiciera lo que se esperaba de él —por ejemplo, abrir un archivo adjunto en un email aparentemente oficial que llega a su buzón de correo, o descargar un archivo comercial de Internet, o insertar un pen drive USB en su portátil— y el ataque, silenciosamente, ya estaba en marcha. El objetivo podía ser una base de datos de clientes para filtrar información personal, o comunicarse con los servidores de Comando y Control (C & C) para iniciar un ataque masivo de denegación de servicio mediante bots con fines de interrupción, o como señuelo para un ataque real entre muchas otras opciones.

Proliferación

La sofisticación aumenta drásticamente en esta generación, y es una clara indicación de lo que está por venir. Las brechas principales fueron resultado de ataques específicamente diseñados y programados para comprometer al objetivo y exfiltrar información que luego venderían en el mercado negro y/o para causar grandes interrupciones. En esta generación, la proliferación es diferente y más peligrosa que en generaciones anteriores. Debido a la filtración involuntaria de sofisticadas herramientas de ataque más allá de sus objetivos originales, el mundo de los hackers obtuvo nuevo conocimiento y así aumentó aún más su sofisticación a nivel general. Por ejemplo, el gusano Stuxnet se extendió más allá de su objetivo original, y algunos de sus elementos se encontraron más tarde en otros ataques. Hoy puede ser descargado por cualquier persona.

Atacantes
En esta generación, los "atacantes" genéricos evolucionan hasta adquirir una fuerza mucho más organizada y formidable. Van a convertirse en entidades criminales, realmente profesionales. Los estados aprovechan sus propias fuerzas (sobre todo, como un brazo de sus fuerzas armadas) para fabricar ciberataques por motivos económicos,para causar disrupciones, o para ambas cosas.

Ejemplos de ataques conocidos de 4ª Generación

Descubierto en el otoño de 2010, el gusano Stuxnet atacó las instalaciones nucleares de Natanz, en Irán. Descrito por algunos como el ataque más avanzado jamás diseñado, Stuxnet buscaba los controladores de Siemens que administraban las centrifugadoras nucleares de las instalaciones y, una vez infectadas, cautelosamente tomaba su control, para en última instancia causarles daños físicos.

> *"Pero en 2010, Stuxnet escapa de Natanz, probablemente en el portátil de alguien; una vez conectado a la Internet pública, hizo algo para lo que no estaba diseñado: propagarse a nivel masivo".* [11]

Más tarde se supo que Stuxnet había sido creado en un esfuerzo conjunto entre Estados Unidos e Israel con el objetivo de impedir las ambiciones nucleares de Irán.

Target
En diciembre de 2013, Target, el tercer minorista más grande de EEUU, copaba los titulares con motivo de un ciberataque que instaló malware en sus terminales de punto de venta (POS) y comprometió más de 40 millones de tarjetas bancarias, así como información privada de hasta 110 millones de clientes (los informes hablan de entre de 70 y 110 millones). Según se informó, los atacantes violaron primero la red del proveedor de aire acondicionado de Target, que a su vez tenía acceso remoto a la red de Target para propósitos de servicio en algunas tiendas del grupo. Desde allí, los atacantes pudieron implantar el malware en los terminales de Target para capturar y exportar números de tarjetas y otros datos personales antes de que fueran cifrados y enviados al sistema de proceso de transacciones de Target. Se supone que el impacto financiero de la brecha fue de cientos de millones de dólares, si bien algunas estimaciones llegan hasta los 1.000 millones [12]. Asímismo, el CEO y presidente de la junta directciva de Target, Gregg Steinhafel, presentó su renuncia. [13]

Como indicador de esta generación de ataques, a continuación se muestran varios puntos reveladores sobre este ataque y la brecha que provocó:

- El acceso a la red corporativa por parte del proveedor de aire acondicionado debería haber sido debidamente segmentado del resto de la red corporativa. Algo que también es un requisito para cumplir con el estándar de la PCI (Payment Card Industry) para negocios que gestionan transacciones con tarjeta bancaria. [14]

- Hay informes que dicen que uno de los productos puntuales de seguridad de Target consiguió detectar el ataque, pero al estar orientado únicamente a la detección, no lo bloqueó, y, a pesar de las múltiples alertas sobre su detección, el equipo de Target paso por alto el ataque en sus inicios.

11. Referencia: *https://www.forbes.com/sites/christopherskroupa/2017/04/19/the-cost-of-cyber-breach-how-much-your-company-should-budget/#1a4c8926ce74*
12. Referencia: https://www.forbes.com/sites/christopherskroupa/2017/04/19/the-cost-of-cyber-breach-how-much-your-company-should-budget/#1a4c8926ce74
13. Referencia: *http://www.zdnet.com/article/target-ceo-out-after-massive-cyberattack-cfo-to-replace*
14. Referencia: *https://www.computerworld.com/article/2487425/cybercrime-hacking/target-breach-happened-because-of-a-basic-network-segmentation-error.html*

> *" 53,7 millones: los ingresos que presuntamente habrían obtenido los hackers por la venta de los 2 millones de tarjetas robadas a Target, vendidas a un precio medio de 26,85 dólares (precio medio entre 18.00 y 35.70 dólares)".* [15]

DYN

El viernes 21 de octubre de 2016, la ciberseguridad alcanzaba un nuevo nivel de conocimiento público, cuando el mundo supo que un ejército de bots, infiltrado en cámaras conectadas a Internet, fue capaz de causar caídas en servicios online de primer orden como Twitter, Amazon, Spotify y Netflix. El ataque global de denegación de servicio (DDoS) contra DYN, una gran empresa dedicada a infraestructuras DNS, provocó la caída. Puede que no dejara en shock a los profesionales de la seguridad en Internet, pero era una nueva demostración de la fragilidad de la red. Afortunadamente, no fue tan dañino como podría haber sido. [16]

> *"Durante un ataque de DDoS que utiliza el protocolo DNS, puede ser difícil distinguir el tráfico legítimo del tráfico del ataque. Por ejemplo, el impacto del ataque generó una tormenta de actividad legítima de reintento cuando los servidores intentaron actualizar sus memorias caché, creando un volumen de tráfico entre 10 y 20 veces superior a lo normal en una gran cantidad de direcciones IP. Cuando se produce una congestión del tráfico DNS, los intentos de acciones legítimas contribuyen aún más al volumen del tráfico. Pudimos ver tráfico de ataque y tráfico legítimo procedente de millones de IP en todas las geografías. Parece que los ataques maliciosos provenían de al menos una botnet, y la tormenta de reintentos aportó un indicador falso sobre un numero de endpoints mucho mayor de lo que ahora suponemos que es. Todavía estamos trabajando en el análisis de los datos, pero la estimación en el momento de este informe es de unos 100.000 endpoints maliciosos. Podemos confirmar que un volumen significativo de tráfico de ataque se originó a partir de botnets basadas en Mirai".* [17]

Tecnologías de seguridad desarrolladas como resultado de los ataques de 4ª Generación

Esta generación marca claramente el punto donde se asume que la seguridad basada en firmas ya no es suficiente. Estos productos detectan ataques basados en "firmas" que se crean DESPUÉS de descubrir, analizar y comunicar al mercado los ataques. La ventana de exposición para las empresas es de días, e incluso de meses, hasta que se desarrolla un "parche" para corregir la vulnerabilidad. Entonces, ante la existencia de un malware más sofisticado, un malware nuevo (porque existen firmas para detectarlo) y mucho más avanzado que los modelos seguridad basados en firmas, se desarrollaron nuevas tecnologías para defenderse contra ataques desconocidos y "de día cero". Concretamente, se crearon tecnologías para protegerse contra ataques de redes bot y para inspeccionar todas las entradas de archivos antes de que los usuarios accedieran a ellos. Estas tecnologías son comúnmente conocidas como tecnologías anti-bot y de sandboxing. Y con su aparición, algunas empresas añadieron a sus entornos dos nuevos productos "puntuales", lo que vendría a complicar aún más sus infraestructuras de seguridad.

15. Referencia: https://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/
16. Referencia: http://blog.checkpoint.com/2016/11/08/denied-dealing-global-distributed-denial-service/
17. Referencia: https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

5ª GENERACIÓN

INTRODUCCIÓN

La 5ª Generación surge aproximadamente en 2017, cuando la filtración de una serie de herramientas avanzadas resulta en numerosos mega-ataques multi-vector a gran escala que generarán ingresos e interrupciones para los delincuentes y causando un enorme impacto. Esto condujo a un malware mucho más sofisticado y personalizado, que puede infiltrarse y propagarse desde prácticamente cualquier vector de las infraestructuras de TI, incluidas las redes de una empresa, instancias de nube, oficinas remotas, dispositivos móviles, sistemas de terceros y mucho más. Esta 5ª y última generación de ataques está bien descrita en ***The Global Risks Report 2018, 13th Edition***: "*... Incidentes que un día bien pudieron ser considerados extraordinarios, se están convirtiendo en algo cada vez más habitual.*" Y el informe cita más adelante dos ejemplos de ataques durante 2017 diciendo: "*...el ataque WannaCry, que afectó 300.000 ordenadores en 150 países, y NotPetya, que causó pérdidas trimestrales por valor de 300 millones de dólares para varias empresas afectadas.*"

Proliferación

Los ataques de 5ª Generación se mueven muy rápido, y en solo unas horas pueden infectar a una enorme cantidad de empresas y entidades en numerosas geografías. Sí, los virus de generaciones anteriores también se movieron rápidamente, pero estos ataques de 5ª generación son rápidos y altamente sofisticados, son furtivos y casi siempre tienen éxito. Por ejemplo, el ataque de WannaCry aprovechó una herramienta llamada EternalBlue, desarrollada por la Agencia de Seguridad Nacional (NSA) de Estados Unidos, y que supuestamente fue filtrada involuntariamente. La herramienta aprovechaba vulnerabilidades en Windows XP para muchos tipos de ataque, desde ransomware hasta interrupciones. Los ataques de 5ª generación son una amenaza que ha escalado respecto a las generaciones anteriores, porque son mega-ataques multi-vectoriales que pueden infiltrarse y proliferar rápida y silenciosamente desde y hacia cualquier elemento de una infraestructura de TI, incluidas redes, instancias de nube, oficinas remotas, endpoints, dispositivos móviles y soluciones de terceros, entre otros.

Los atacantes

Si aún no está usted seguro de la gravedad y las capacidades de los ataques de 5ª generación, considere estas apreciaciones de https://www.knowbe4.com/resources/five-generations-of-cybercrime/

- El cibercrimen tiene sus propias redes sociales, con sus propios servicios de custodia
- Ahora, el malware se puede adquirir por licencias e incluso recibir soporte técnico
- Usted puede alquilar botnets por horas, para lanzar su propia ola de crímenes
- Servicios de infección de malware en modo "pago por uso" que crea botnets rápidamente
- Un mercado en vivo para exploits de día cero (vulnerabilidades desconocidas)

Es obvio que, en el momento de la redacción de este documento, durante el 1º trimestre de 2018, los cibercriminales están muy organizados, incluso industrializados, como debería estarlo cualquier negocio diseñado para el éxito. Los atacantes tienen conocimiento técnico y, a medida que surgen nuevas tecnologías en el mercado, rápidamente las explotan para sus propósitos y en detrimento de sus objetivos.

Ejemplos de ataques conocidos de 5ª Generación

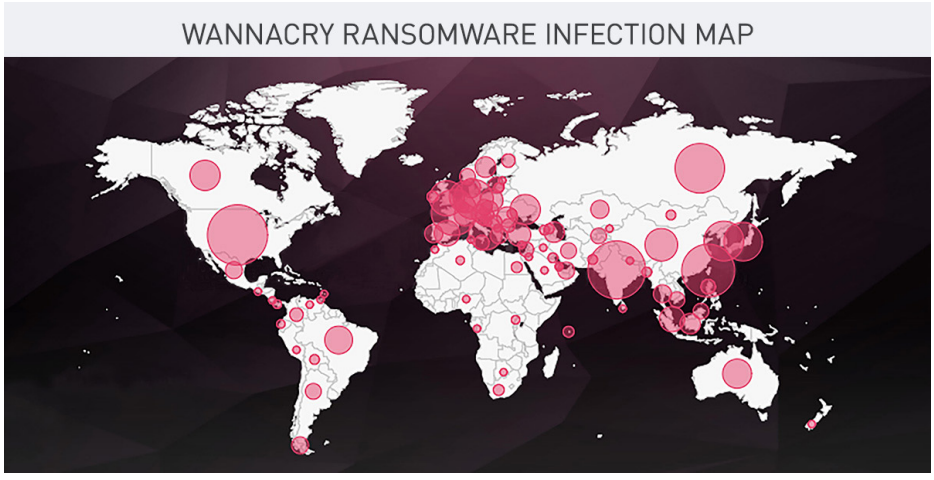
WannaCry

En mayo de 2017, el ataque ransomware WannaCry golpeó y atacó a ordenadores con sistema operativo Windows XP en todo el mundo. El ataque cifró los datos y luego exigió que se realizara el pago de un rescate en bitcoins. WannaCry aprovechó una herramienta llamada EternalBlue, desarrollada por la Agencia de Seguridad Nacional de Estados Unidos, y que supuestamente se filtró involuntariamente.

Irónicamente, el parche necesario para prevenir las infecciones por WannaCry estaba disponible antes de que comenzara el ataque: El boletín de seguridad de Microsoft MS17-010, publicado el 14 de marzo de 2017, actualizaba la implementación del protocolo SMB de Windows para evitar infecciones a través de EternalBlue. Sin embargo, a pesar del hecho de que Microsoft había marcado el parche como crítico, muchos sistemas aún no se habían reparado en mayo de 2017, cuando WannaCry comenzó su rápida propagación.[18]

Una serie de factores hizo que la proliferación inicial de WannaCry fuera especialmente elevada: alcanzó varios sistemas importantes y de alto perfil, incluidos muchos del Servicio Nacional de Salud de Gran Bretaña; explotó una vulnerabilidad de Windows que se sospechaba que había sido descubierta por primera vez por la NSA; y fue provisionalmente vinculado por Symantec y otros investigadores de seguridad al Grupo Lazarus, una organización cibercriminal posiblemente conectada con el gobierno de Corea del Norte.[19]

El ataque fue detenido a los pocos días de descubrirse gracias a los parches de emergencia lanzados por Microsoft, y al descubrimiento de un mecanismo de seguridad kill switch que evitó que los ordenadores infectados propagaran aún más el ransomware. Se estima que el ataque afectó a más de 200.000 ordenadores de 150 países, con unos daños totales que se estiman entre cientos y miles de millones de dólares. [20]



17 de mayo de 2017, Fuente: Blog de Check Point Software Technologies, http://blog.checkpoint.com/2017/05/17/check-point-reveals-global-wannacry-ransomware-infection-map-cpx-europe-2017/

18. Referencia: *https://www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html*
19. Referencia: *https://www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html*
20. Referencia: *https://en.wikipedia.org/wiki/WannaCry_ransomware_attack*

NotPetya

En marzo de 2016 apareció un nuevo ransomware, Petya. Encriptaba discos duros y exigía un rescate a cambio de la clave para descifrar los archivos. Más tarde, en junio de 2017, un ataque que inicialmente se pensó que también era Petya atacó bancos, aeropuertos y compañías eléctricas en Ucrania, Rusia y algunos países europeos. Tras un análisis más profundo, se le denominó NotPetya, porque realmente no lo era...

> *El Petya original requería que la víctima lo descargara desde un correo electrónico, lo ejecutara y le diera permisos de administrador. NotPetya, sin embargo, explotaba varios métodos diferentes para propagarse sin intervención humana. El vector de infección original parecía ser una "puerta trasera" implantada en M.E.Doc, un paquete de software de contabilidad que utilizan casi todas las empresas en Ucrania. Tras infectar los servidores de Medoc, NotPetya utilizó una amplia variedad de técnicas para propagarse a otros ordenadores, incluyendo EternalBlue y EternalRomance, dos exploits desarrollados por la NSA para aprovechar un error en la implementación del protocolo SMB de Windows. También podía aprovechar una herramienta llamada Mimi Katz para localizar credenciales de administración de red en la memoria de las máquinas infectadas, y luego utilizar las herramientas PsExec y WMIC, integradas en Windows, para acceder de forma remota a otros ordenadores de la red local e infectarlos también.* [21]

El ataque de Petya cifraba archivos y mostraba un proceso para pagar un rescate y obtener la clave para descifrarlos. NotPetya también cifraba los archivos, pero solo aparentaba ofrecer un medio para adquirir la clave de descifrado: La ficha en su pantalla de rescate era simplemente un número sin sentido generado al azar.

> *Entonces, ¿cuál era el verdadero propósito de NotPetya? El hecho de que hubiera sido mejorado radicalmente en su eficiencia respecto a su antecesor, Petya, hace pensar en un autor con muchos recursos: por ejemplo, una agencia de inteligencia estatal, o un departamento de ciberguerra. Todo ello, combinado con el enfoque del ataque de 2017 en Ucrania, hizo que muchos señalaran a Rusia, con quien aquel país había estado involucrado en un conflicto desde la ocupación de Crimea en 2014. Esta acusación fue hecha suya por el propio gobierno ucraniano, y muchas fuentes occidentales coinciden, incluyendo EEUU y Reino Unido. Rusia, por su parte, lo niega, señalando que NotPetya infectó también muchos ordenadores rusos.* [22]

Sin embargo, entre las empresas más afectadas por el ataque se encuentra una de las navieras más grandes del mundo, A.P. Moller-Maersk. Con sede en Copenhague, el ataque causó retrasos e interrupciones en los envíos durante semanas, y un impacto financiero estimado entre 200 y 300 millones de dólares. [23]

21. Referencia: https://www.csoonline.com/article/3233210/ransomware/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html
22. Referencia: https://www.csoonline.com/article/3233210/ransomware/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html
23. Referencia: https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/#16ab49f84f9a

Tecnologías de seguridad desarrolladas como resultado de los ataques de 5ª Generación

La 5ª generación de ataques resalta la necesidad de unas infraestructuras de seguridad integradas y unificadas. De hecho, hablamos de "arquitecturas" de seguridad. Los vectores de ataque y vías de proliferación incluyen todo aquello que esté conectado a Internet, ya sea en las instalaciones, en remoto o dispositivos móviles, o con conexiones compartidas con terceros. Tal como se supo después, los ataques de 5ª generación están diseñados para ser exitosos con el objetivo, moverse rápido por los diferentes elementos de las infraestructuras de TI y opera con un sigilo increíble. Las generaciones de seguridad anteriores no estaban integradas, sino basadas en soluciones puntuales, basadas sobre todo en tecnologías de detección desconectadas entre sí y sin capacidad de proteger contra los ataques "anteriormente considerados extraordinarios y ahora de lo más común" de 5ª generación.

Por ejemplo, los sistemas de sandboxing de 4ª generación permiten al primer ataque infectar a un "paciente cero" y por tanto a la red, mientras el sandbox analiza y construye indicadores para detectar reiteraciones del mismo ataque. Esto no es suficientemente efectivo y está claramente por detrás de las capacidades de los ataques de 5ª generación. Los ataques de 5ª generación, como WannaCry o NotPetya, combinados con los nuevos servicios de TI dinámicos que permiten los accesos móviles y los servicios elásticos y por demanda de la nube, requieren nuevos modelos para evaluar y construir infraestructuras de seguridad. Este es el modelo de 5ª generación para la seguridad de TI y es una arquitectura integrada y unificada que comparte inteligencia de amenazas en tiempo real para una prevención rápida, en tiempo real, desde que se produce el ataque.

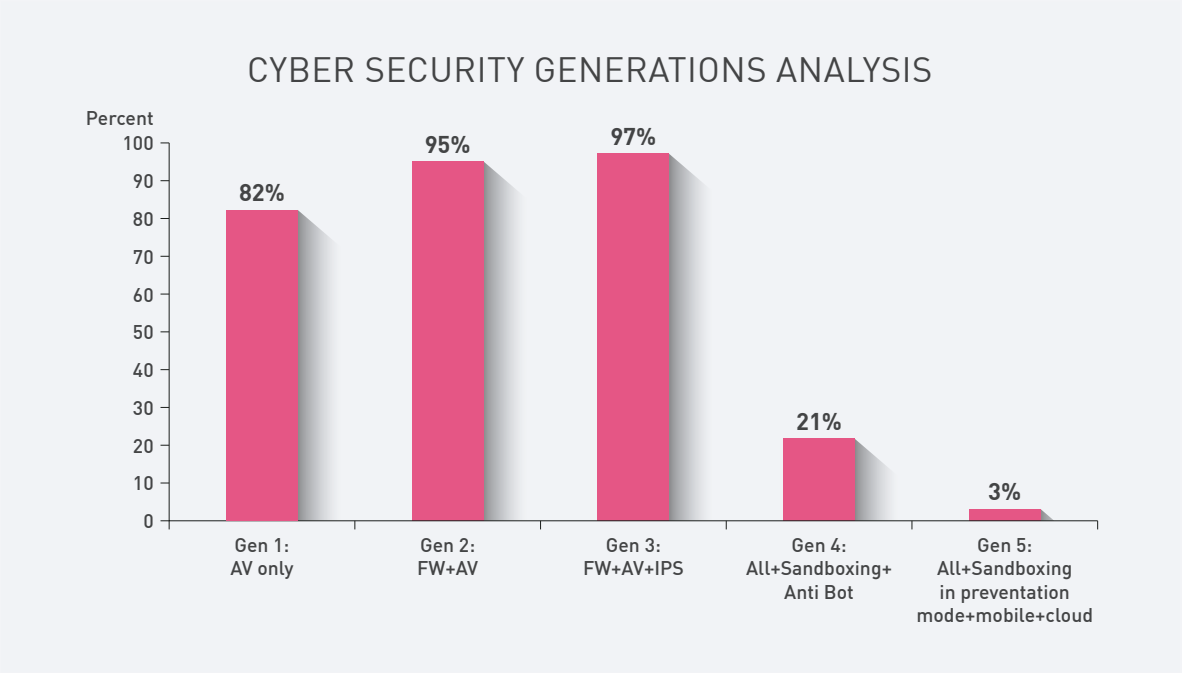
Los ciberataques de 5ª generación están diseñados para el éxitose mueven muy rápido y operan con un increíble sigilo.

PERSPECTIVA

Evaluar y visualizar la seguridad desde este punto de vista generacional aporta una perspectiva nueva y muy reveladora. De hecho, este nuevo modelo y esta nueva perspectiva son necesarios para la seguridad de TI, porque los viejos métodos tradicionales están fallando. Ver y evaluar la seguridad de TI a través de un prisma generacional revela algunas ideas urgentes, incluso sorprendentes.

1. Los niveles seguridad de las empresas están por debajo del nivel de los ataques a los que se enfrentan.

Concretamente, la mayoría de los negocios se encuentran en un en una 2ª o 3ª generación de seguridad, y ello a pesar de que, como hemos leído, los ataques actuales ya están en esta 5ª generación, mucho más avanzada y dañina. Durante el primer trimestre de 2018, Check Point encuestó a 443 profesionales de seguridad de todo el mundo sobre sus infraestructuras de seguridad, y los resultados validan que estas infraestructuras, en su mayoría, están generacionalmente por debajo del nivel de los ataques contra los que han de protegerse. La situación, desde luego, es realmente urgente y alarmante.

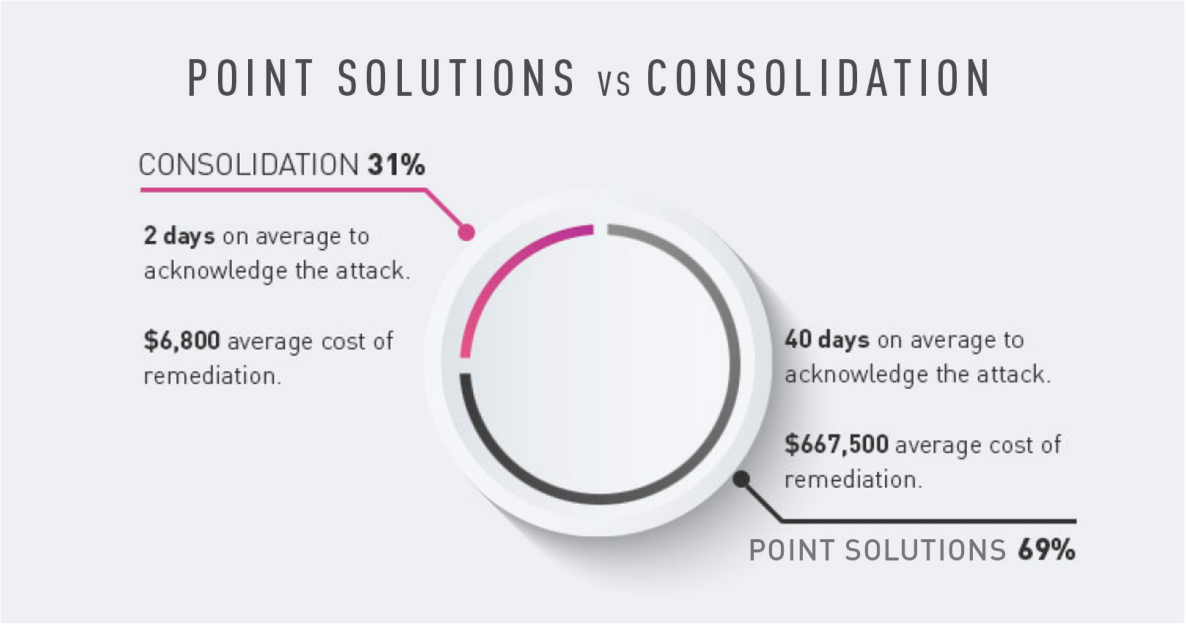


¿Por qué y cómo puede suceder esto? La velocidad de avance del ataque es mucho más rápida que la capacidad del negocio de para evaluar, seleccionar y desplegar las nuevas tecnologías de seguridad necesarias para protegerse contra los nuevos ataques. Mientras los atacantes operan libremente y avanzan sin obstáculos, las empresas se ven cohibidas por requisitos de disponibilidad del servicio, gestión del cambio, controles de cumplimiento, escasez de personal, restricciones presupuestarias y unas infraestructuras de seguridad basadas en soluciones puntuales. Es difícil continuar añadiendo más productos a una infraestructura de seguridad ya saturada. La conclusión es que las empresas no pueden mantenerse al día.

2. Se necesita un nuevo modelo para evaluar las amenazas y la seguridad.

En generaciones anteriores, era eficaz agregar nuevos productos de seguridad para cada nuevo tipo de ataque o aplicación. Sin embargo, este modelo de tipo "hay un nuevo ataque; despliega un nuevo producto" ya no funciona. Este enfoque conlleva infraestructuras de seguridad basadas en soluciones puntuales, con productos no integrados sin una distribución y una gestión de amenazas centralizadas. Y, al no estar integrados y no poder compartir información sobre ataques en tiempo real, sacrifican la precisión y, por tanto, la mayoría sólo están habilitados para la detección. Estos despliegues de "soluciones puntuales" son ineficientes desde el punto de vista operativo, ya que pueden estar compuestos por 20, 30 o más productos de seguridad. La gestión de todos estos productos requiere más personal de seguridad, precisamente en un momento en que escasean los conocimientos de seguridad. Por tanto, a pesar de los mejores esfuerzos de las empresas, las infraestructuras de seguridad de TI de hoy están "rezagadas generacionalmente" y son incapaces de protegerse de los ataques que se están lanzando.

Como prueba de ello, en una reciente encuesta a ejecutivos se les hicieron varias preguntas sobre sus requisitos de ciberseguridad, así como sus desafíos e inquietudes cotidianos. Una de las preguntas fue: ¿cuál le parece el mejor enfoque? De forma abrumadora, los ejecutivos declararon que estaban satisfechos con su estrategia de soluciones puntuales, y que la habían promovido dentro de su organización. Sin embargo, una vez que se les hicieron más preguntas respecto a su posición de seguridad, se hizo obvio que su idea de lo que era mejor para su organización era una falsa sensación de seguridad, mostrando una significativa diferencia en los procesos de recuperación de ataques:



Como demuestran los resultados de la mencionada encuesta, el uso del modelo generacional para evaluar las amenazas y la infraestructura de seguridad generan una perspectiva nueva muy diferente, y muy valiosa. También impulsan una mejor seguridad, con operaciones más eficientes y a menores costos.

3. Se requiere una seguridad de 5ª Generación.

Como hemos visto, la mayoría de los negocios están sólo en la 2ª y 3ª generación de la seguridad, mientras que los ataques están en la 5ª generación. Y, por supuesto, los cibercriminales y los ciberataques solo pueden seguir avanzando en organización, sofisticación y velocidad. Las empresas necesitan construir un plan para moverse desde su seguridad basada en soluciones puntuales hacia infraestructuras de seguridad de 5ª generación. La seguridad de 5ª generación consiste en una prevención de amenazas avanzada que previene de manera uniforme los ataques en toda la infraestructura de TI y las redes de la empresa, así como en instancias virtuales, entornos de nube, endpoints, oficinas remotas y dispositivos móviles, con una única gestión central para administración, monitorización y respuesta. Es una base que no solo protege contra los ataques de 5ª generación, sino que también es una arquitectura sobre la cual las empresas pueden añadir capacidades de seguridad de manera fácil y eficiente a medida que las amenazas avanzan y los entornos de TI evolucionan.

¿Qué es la seguridad de 5ª Generación? La seguridad de 5ª Generación incorpora los siguientes avances sobre la seguridad de 4ª generación:

- **Consolida** la seguridad de la anterior generación -la de los firewalls de nueva generación (NGFW), el sandboxing, la protección contra bots, la seguridad para endpoints, etc.- en un único sistema de seguridad unificado .
- **Comparte** información sobre amenazas en tiempo real en todo el sistema.
- **Previene** los nuevos ataques avanzados de 5ª generación y que ocurren por primera vez, con lo que impide las infecciones a "pacientes cero".
- **Amplía** la prevención desde ataques avanzados a implementaciones en la nube y dispositivos móviles como parte de un sistema de seguridad único y consolidado.
- Previene **uniformemente** los ataques en toda la infraestructura de redes de la empresa, instancias virtuales, implementaciones de nube, endpoints, oficinas remotas y dispositivos móviles.
- Gestiona, supervisa y responde **centralizadamente** a todas las actividades y eventos de seguridad como un único sistema de seguridad unificado.

Así es la seguridad de 5ª generación, y eso es Check Point Infinity: la única arquitectura de ciberseguridad totalmente consolidada, que protegerá su empresa y su infraestructura de TI contra los mega-ciberataques de 5ª generación en todo tipo de redes, endpoints, entornos de nube y dispositivos móviles.

Una arquitectura diseñada para resolver las complejidades de una conectividad creciente y una seguridad ineficiente. Con prevención de amenazas en tiempo real contra amenazas conocidas y desconocidas, aprovechando la tecnología más avanzada y soluciones de día cero. Además, el intercambio automático de inteligencia de amenazas en todas las redes, endpoints, entornos de nube y dispositivos móviles ofrece una seguridad consistente a lo largo de todos los componentes de Check Point y sella las brechas de seguridad.

La arquitectura Check Point Infinity consolida la gestión de múltiples capas de seguridad, aportando una mayor eficiencia en las políticas y la capacidad de administrar la seguridad a través de un único dashboard. La gestión unificada correlaciona centralizadamente todo tipo de eventos en todos los entornos de red, servicios en la nube e infraestructuras móviles.

RESUMEN

El progreso y los beneficios sociales que ha traído la tecnología son realmente deslumbrantes. Cuando me gradué en 1980, nunca había tocado un "ordenador". Obtuve mi título universitario en un entorno de mainframes IBM Virtual Machine (VM), y algunos de mis primeros proyectos fueron desarrollados en tarjetas perforadas. Hoy puedo comunicarme con mi familia, amigos y colegas, acceder a las redes de mi empresa y a información y recursos hasta hace poco impensables desde prácticamente cualquier parte del mundo, con un teléfono inteligente increíblemente pequeño y portátil. El avance es realmente notable. Y sin embargo, si como individuo me resisto a unirme al mundo de la tecnología, o simplemente me quedo rezagado, estoy en desventaja social, porque estaré menos conectado y sin la riqueza de información y eficiencia que me brindan como individuo los smartphones y la informática.

La evolución de los ciberataques y de la ciberseguridad es igualmente sorprendente. Lo que comenzó a principios de los 80 por curiosidad, diversión o notoriedad, es hoy una industria multimillonaria para el crimen organizado. De igual modo, nacida también en la década de los 80, la industria de seguridad de TI es en la actualidad una industria multimillonaria que es, de hecho, absolutamente esencial para proteger las operaciones diarias de todo en la vida moderna, desde actividades de negocio básicas hasta entornos críticos como hospitales o infraestructuras críticas de naciones y países industrializados.

Cada gran avance en los ataques y en la seguridad ha definido claras generaciones evolutivas. La seguridad de TI desplegada en la actualidad por las empresas se encuentra en un punto de inflexión muy preocupante, porque la mayoría de las infraestructuras de seguridad de TI solo están en su 2ª o 3ª generación, mientras que los ataques actuales han avanzado mucho más, hasta llegar a su 5ª generación. En pocas palabras, la seguridad de las empresas está por rezagada, mal equipada para protegerse contra el nivel de ataques que se están lanzando. Tras muchas generaciones y muchos productos, el modelo de seguridad de "soluciones puntuales" es operacionalmente complejo y más frágil, y no puede avanzar al mismo ritmo que los ataques. Este es un problema alarmante, que primero ha de ser reconocido y luego resuelto. Este nuevo modelo generacional revela deficiencias obvias en la seguridad actual con respecto a los ataques. Así que, junto con “la regla de oro” de seguridad de proteger cada activo de acuerdo con su valor, este estado de cosas exige también otra regla de oro: que la generación de seguridad implementada debe al menos ser igual a la generación de los ataques lanzados.

Concretamente, para protegerse contra los ataques de 5ª generación, las empresas deben desplegar una seguridad de 5ª generación. La seguridad de 5ª generación consiste en una prevención avanzada de amenazas que de manera uniforme previene ataques en toda la infraestructura de TI de una empresa, incluyendo redes, instancias virtuales, entornos de nube, endpoints, oficinas remotas y dispositivos móviles, con una única gestión centralizada para administración, monitorización y respuesta. Es una base que no solo protege contra ataques de 5ª generación, sino que también es una arquitectura sobre la cual las empresas pueden añadir capacidades de seguridad de manera sencilla y eficiente a medida que avanzan los ataques y evolucionan los entornos de TI.

Eso es Check Point Infinity. Check Point Infinity es una arquitectura de seguridad que ofrece prevención de amenazas avanzada para proteger toda la infraestructura de TI de las empresas, incluidas redes, instancias de nube y dispositivos móviles, contra los ataques más avanzados de hoy en día. La arquitectura Infinity soporta integración real con productos de terceros y, a través del programa de partners Check Point OpSec, Check Point ofrece un rico ecosistema de productos compatibles. Por último, como acabamos de leer, las empresas no pueden continuar añadiendo productos para mantenerse al día con el nivel de avance de los ataques. Check Point Infinity soluciona esto también, porque fue diseñada y construida específicamente para adaptarse a las nuevas tecnologías y formas de ataque.

Esto es una seguridad de 5ª generación: Check Point Infinity, la solución para proteger a las empresas ahora y en el futuro.

Sede central

5 Ha'Solelim Street, Tel Aviv 67897, Israel

Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

Sede en España

Vía de las Dos Castillas, 33, 28224 Pozuelo de Alarcón (Madrid)

Tel: +34 91 799 27 14 | Fax: +34 91 457 20 79