KASPERSKY lab

Kaspersky Security Bulletin:

PREDICCIONES DE AMENAZAS PARA 2019

Vicente Díaz

CONTENIDO

No hay nada más difícil que hacer predicciones. Entonces, en lugar de recurrir a una bola de cristal, aquí la idea es hacer pronósticos basados en hechos recientes y en las tendencias que podrían ser usadas en los próximos meses.

Tras consultar a las personas más inteligentes que conozco y basando nuestro escenario en los ataques APT, que son los que suelen mostrar una mayor innovación cuando se trata de violar la seguridad, presentamos aquí nuestras principales "predicciones" de lo que podría suceder en los próximos meses.

NO MÁS ATAQUES APTS DE GRANDES DIMENSIONES

¿Qué? ¿Cómo es posible que en un mundo donde a diario descubrimos cada vez más actores de ataques, la primera predicción parezca apuntar en la dirección opuesta?

La razón es que la industria de la seguridad ha ido descubriendo, de forma consistente, operaciones altamente sofisticadas patrocinadas por gobiernos y cuya preparación llevó años. Una posible reacción lógica de un atacante ante esa situación sería explorar nuevas técnicas mucho más sofisticadas y difíciles de descubrir y de atribuir a agentes específicos.

De hecho, hay muchas maneras diferentes de hacerlo. El único requisito es comprender las técnicas utilizadas por la industria para identificar a los autores de los ataques y las similitudes entre distintos tipos de ataques, como también los artefactos utilizados en ellos, algo que no parece ser un gran secreto. Con los recursos suficientes, lo más simple para un atacante sería llevar a cabo diferentes conjuntos de operaciones muy difíciles de relacionar con el mismo actor u operación. Los atacantes con más y mejores recursos podrían iniciar operaciones innovadoras, mientras mantienen vigentes sus operaciones más antiguas. Por supuesto, hay una buena posibilidad de que se descubran las operaciones más antiguas, pero descubrir las nuevas operaciones supondría un mayor desafío.

En lugar de crear campañas más sofisticadas, en algunos casos parecería más eficaz para algunos actores muy específicos que tienen la capacidad de hacerlo, apuntar directamente a la infraestructura y a las empresas donde se puedan encontrar víctimas, como los proveedores de Internet. A veces esto puede lograrse a través de la regulación, prescindiendo del malware.

Algunas operaciones simplemente se externalizan a diferentes grupos y empresas que utilizan diversas herramientas y técnicas, lo que hace muy difícil dar con el actor intelectual original. Vale la pena tener en cuenta que, en el caso de operaciones patrocinadas por gobiernos, esta "centrifugación" de recursos y talento podría afectar el futuro de dichas campañas. En este escenario, las capacidades técnicas y las herramientas pertenecen a la industria privada y están al alcance de cualquier cliente que, en muchos casos, no comprende del todo los detalles técnicos y las consecuencias que pueden provocar.

Todo esto sugiere que es improbable que descubramos nuevas operaciones altamente sofisticadas: lo más probable es que los atacantes bien preparados y que poseen los recursos necesarios simplemente cambien a nuevos paradigmas.

HARDWARE DE RED E IOT

Parecía lógico que en algún momento cada actor desplegaría capacidades y herramientas diseñadas que apunten al hardware de red. Campañas como VPNFilter son un ejemplo perfecto de cómo los atacantes ya han comenzado a implementar sus programas maliciosos para crear 'botnets' multipropósito. En este caso en particular, a pesar de que el malware estaba muy difundido, tomó cierto tiempo detectar el ataque, lo que es preocupante, considerando lo que podría suceder en operaciones con blancos más específicos.

En realidad, esta idea puede ir aún más lejos para los actores con los recursos suficientes: ¿por qué no apuntar directamente a una infraestructura aún más elemental en lugar de sólo atacar a una organización? No hemos alcanzado ese nivel de riesgo (hasta donde sabemos), pero ejemplos pasados (como Regin) muestran lo tentador que resulta ese nivel de control para cualquier atacante.

Las vulnerabilidades en el hardware de red permiten que un atacante siga direcciones diferentes. Podría optar por crear botnets masivas para después usarlas con diferentes objetivos, o podría apuntar a blancos seleccionados para lanzar ataques más clandestinos. En este segundo grupo, podríamos considerar ataques sin malware, en los que basta abrir un túnel VPN para reflejar o redirigir el tráfico para que el atacante obtenga toda la información que busca.

Todos estos elementos de red también podrían ser parte del poderoso Internet de las cosas (IoT), donde las botnets siguen creciendo a un ritmo aparentemente imparable. Estas botnets podrían ser increíblemente poderosas en manos equivocadas, por ejemplo si se las usa para interrumpir el funcionamiento de una infraestructura crítica. Los actores con muchos recursos podrían abusar de este instrumento, posiblemente utilizando un grupo de cobertura o en algún tipo de ataque terrorista.

Un ejemplo de cómo se pueden usar estas versátiles botnets, además de los ataques destructivos, es realizar las comunicaciones maliciosas mediante el salto de frecuencia de corto alcance, como una forma de evadir las herramientas de monitorización al omitir los canales de exfiltración convencionales.

Si bien esta parece ser una advertencia recurrente año tras año, nunca debemos subestimar las botnets en el IoT, ya que se están haciendo cada vez más fuertes.

REPRESALIA PÚBLICA

Una de las preguntas más importantes en términos de diplomacia y geopolítica era cómo lidiar con un ataque cibernético activo. La respuesta no es simple y entre muchas otras consideraciones depende en gran medida de cuán malo y flagrante ha sido el ataque. Sin embargo, parece que después de ataques como el lanzado contra el Comité Nacional Demócrata, las cosas se han puesto más serias.

Las investigaciones sobre ataques recientes de alto perfil, como los lanzados contra Sony Entertainment Network o DNC, culminaron que se sometiera a proceso a una lista de sospechosos. Esto no sólo llevó a que se enjuicie a los responsables, sino que también se los expuso públicamente. Esto puede usarse para inducir una ola de opiniones que podrían provocar consecuencias diplomáticas más serias.

Es así que hemos visto que Rusia sufrió tales consecuencias como resultado de su supuesta interferencia en procesos democráticos. Esto podría hacer que otros lo piensen bien antes de emprender futuras operaciones de este tipo.

Sin embargo, el mayor logro de los atacantes fue provocar miedo a que pase algo así, o llevar a pensar de que ya podría haber ocurrido. Ahora pueden aprovecharse de ese miedo, de la incertidumbre y de la duda de maneras diferentes y más sutiles, algo que se vio en operaciones notables, como Shadowbrokers. Y creemos que más cosas de este tipo están por venir.

¿Qué veremos en el futuro? Es probable que las operaciones pasadas solo estuvieran probando el terreno de la propaganda. Creemos que esto solo es el comienzo y que este campo será objeto de diversas formas de abuso, por ejemplo, en incidentes con banderas falsas, como Olympic Destroyer, cuyo objetivo final aún no está claro, ni tampoco se sabe a ciencia cierta cómo se la llevó a cabo.

APARICIÓN DE RECIÉN LLEGADOS

Simplificando un poco, el mundo de los ataques APT parece estar dividiéndose en dos grupos: los actores más avanzados con los recursos tradicionales (que predecimos que se desvanecerán) y otro grupo de recién llegados, llenos de energía, que quieren entrar en el juego.

La cuestión es que la barrera de entrada nunca ha sido tan baja, con cientos de herramientas muy efectivas, exploits reutilizados filtrados y frameworks de todo tipo disponibles para que cualquiera los use. Como ventaja adicional, estas herramientas hacen que la atribución sea casi imposible y pueden ser fácilmente personalizadas si es necesario.

Hay dos regiones en el mundo donde estos grupos son cada vez más frecuentes: el Sudeste Asiático y el Medio Oriente. Hemos observado el rápido avance de grupos sospechosos que operan en estas regiones, tradicionalmente mediante la ingeniería social para sus blancos locales, aprovechando su poca protección y la carencia de una cultura de seguridad. Sin embargo, a medida que los blancos aumentan sus defensas, los atacantes hacen lo mismo con sus capacidades ofensivas, lo que les permite extender sus operaciones a otras regiones a medida que mejoran el nivel técnico de sus herramientas. En este escenario de herramientas basadas en scripts también podemos encontrar compañías emergentes que brindan servicios regionales que, a pesar de las fallas de OPSEC, continúan mejorando sus operaciones.

Un aspecto interesante que vale la pena considerar desde un ángulo más técnico es cómo las herramientas de post-explotación de JavaScript pueden encontrar una nueva vida a corto plazo, dada la dificultad de limitar su funcionalidad por parte de un administrador (a diferencia de PowerShell), su falta de registros de sistema y su capacidad para ejecutarse en sistemas operativos más antiguos.

LOS ANILLOS NEGATIVOS

El año de Meltdown/Spectre/AMDFlaws y todas las vulnerabilidades asociadas (y las que vendrán) nos hizo replantearnos dónde reside el malware más peligroso. Y aunque en el mundo real no hemos visto casi nada que abuse las vulnerabilidades debajo del Anillo 0, la mera posibilidad de que suceda es realmente aterradora, ya que sería invisible para casi todos los mecanismos de seguridad con que contamos.

Por ejemplo, en el caso de SMM, ha habido al menos una prueba de concepto (PoC) accesible al público desde 2015. SMM es una característica de la CPU que efectivamente podrá dar acceso completo remoto a un equipo sin siquiera permitir que los procesos de Anillo 0 tengan acceso a su espacio de memoria. Eso hace que nos preguntemos si el que no hayamos encontrado ningún malware que abuse dicha vulnerabilidad es simplemente porque es muy difícil de detectar. Abusar de esta vulnerabilidad parece ser una oportunidad demasiado buena para ignorarla, así que estamos seguros de que varios grupos han intentado explotar, quizás con éxito, tales mecanismos durante años.

Vemos una situación similar con el malware de virtualización o hipervisor, o con el malware para UEFI. Hemos visto pruebas de concepto de ambos, e incluso HackingTeam reveló un módulo de persistencia UEFI que ha estado disponible desde al menos 2014, pero, una vez más, aún no se han descubierto ejemplares en el mundo real.

¿Encontraremos alguna vez este tipo de raros ejemplares? ¿O es que no han sido explotados todavía? Lo último parece poco probable.

TU VECTOR FAVORITO DE INFECCIÓN

En la predicción quizás menos sorprendente de este artículo, nos gustaría decir algunas palabras sobre el spear-phishing. Creemos que el vector de infección más exitoso adquirirá aún más importancia en el futuro más cercano. La clave de su éxito sigue siendo su capacidad para despertar la curiosidad de la víctima, y las recientes fugas masivas de datos de varias plataformas de redes sociales podrían ayudar a los atacantes a mejorar esta estrategia.

Los datos obtenidos de los ataques contra gigantes de las redes sociales como Facebook, Instagram, LinkedIn y Twitter están ahora en el mercado, al alcance del público. En algunos casos, aún no está claro qué tipo de datos buscaban los atacantes, pero entre ellos podrían estar los mensajes privados o hasta las credenciales. Esto es un tesoro para los ingenieros sociales y podría dar lugar, por ejemplo, a que un atacante utilice las credenciales robadas de algún contacto cercano para compartir en las redes sociales algo que ya se discutió en privado, lo que mejorará considerablemente las posibilidades de éxito del ataque.

A esto se pueden agregar técnicas de exploración tradicionales en las que los atacantes comprueban dos veces el blanco para asegurarse de que se trata de la víctima correcta, minimizando así la distribución de malware y su detección. En cuanto a los archivos adjuntos, es práctica común asegurarse de que haya interacción humana antes de lanzar cualquier actividad maliciosa, para así esquivar los sistemas de detección automática.

De hecho, hay varias iniciativas que utilizan el aprendizaje automático para mejorar la efectividad del phishing. Aún se desconoce cuáles serían sus efectos en la vida real, pero lo que parece claro es que la combinación de todos estos factores mantendrá en los próximos meses al spear-phishing como un vector de infección muy efectivo, sobre todo en las redes sociales.

DESTRUCTOR DESTRUCTIVO

Olympic Destroyer fue uno de los casos más famosos de malware potencialmente destructivo durante el año pasado, pero muchos atacantes están incorporando de forma regular dichas capacidades en sus campañas. Los ataques destructivos tienen varias ventajas para los atacantes, especialmente en términos de desviar la atención y eliminar cualquier registro o evidencia después del ataque. O simplemente como una desagradable sorpresa para la víctima.

Algunos de estos ataques destructivos tienen blancos geoestratégicos relacionados con conflictos actuales, como hemos visto en Ucrania, o con intereses políticos, como los ataques que afectaron a varias compañías petroleras en Arabia Saudita. En otros casos, pueden ser el resultado de un hacktivismo, o actividad de un grupo subsidiario utilizado por una entidad más poderosa que prefiere permanecer en las sombras.

De todos modos, la clave de todos estos ataques es que son "demasiado buenos" para no usarlos. En términos de represalias, por ejemplo, los gobiernos podrían usarlos como una respuesta equidistante entre una respuesta diplomática y un acto de guerra; de hecho, algunos gobiernos están experimentando con ellos. La mayoría de estos ataques se planifican por adelantado, lo que implica una etapa inicial de reconocimiento e intrusión. No sabemos cuántas víctimas potenciales ya están en situaciones vulnerables, cuando todo el ataque ya está listo y solo falta que se apriete el gatillo, o qué otras armas tienen los atacantes en su arsenal esperando la orden de ataque.

Los entornos de ICS y la infraestructura crítica son especialmente vulnerables a tales ataques y aunque la industria y los gobiernos han hecho un gran esfuerzo en los últimos años para mejorar la situación, las cosas están lejos de ser ideales. Por eso creemos que, aunque tales ataques nunca se generalizarán, el próximo año ocurrirán algunos, especialmente como represalias a decisiones políticas.

CADENA DE SUMINISTRO AVANZADA

Este es uno de los vectores de ataque más preocupantes que se ha explotado con éxito en los últimos dos años y que ha hecho que todos piensen en cuántos proveedores tienen y qué tan seguros son. La cuestión es que no hay una respuesta fácil para este tipo de ataque.

A pesar de que se trata de un vector fantástico para apuntar a toda una industria (similar a los ataques watering hole) o incluso a todo un país (como se vió con NotPetya), no es tan bueno cuando se trata de ataques más selectivos, ya que el riesgo de detección es mayor. También hemos visto intentos más indiscriminados, como inyectar códigos maliciosos en repositorios públicos de bibliotecas comunes. La última técnica podría ser útil en ataques cronometrados muy cuidadosamente, cuando estas bibliotecas se usan en un proyecto muy particular, con la subsiguiente eliminación del código malicioso del repositorio.

Ahora, ¿es posible usar este tipo de ataque de una manera más específica? Parece ser difícil en el caso del software, porque dejaría rastros en todas partes y el malware podría distribuirse a varios clientes. Es más realista en los casos en que el proveedor trabaja exclusivamente para un cliente específico.

¿Y qué pasa con los implantes de hardware? ¿Son una posibilidad real? Últimamente esto ha generado alguna controversia. Aunque las filtraciones de Snowden revelaron cómo se puede manipular el hardware en su camino hacia el cliente, esto no parece ser algo que la mayoría de los actores pueda hacer, excepto aquellos muy poderosos. Pero hasta éstos se verán limitados por varios factores.

Sin embargo, en los casos en que se conoce al comprador de un pedido en particular, podría ser más factible que un actor intente manipular el hardware en el origen, en lugar de hacerlo mientras está en camino al cliente.

Es difícil imaginar cómo se podrían eludir todos los controles técnicos en una línea de montaje industrial y cómo se podría llevar a cabo tal manipulación. No queremos descartar esta posibilidad, pero probablemente implicaría la colaboración del fabricante.

En general, los ataques a la cadena de suministro son un vector de infección efectivo que continuaremos viendo. En términos de implantes de hardware, creemos que es extremadamente improbable que ocurra, y si lo hace, probablemente nunca lo sepamos...

Y MÓVIL

Esto figura en las predicciones de cada año. No se espera nada innovador, pero siempre es interesante pensar en las dos velocidades para esta lenta ola de infecciones. No hace falta decir que todos los actores tienen componentes móviles en sus campañas; no tiene sentido dedicarse sólo a las computadoras personales. La realidad es que podemos encontrar muchos ejemplos de artefactos para Android, pero también algunas mejoras en términos de ataques contra iOS.

Si bien las infecciones exitosas para iPhone requieren concatenar varias vulnerabilidades de días cero, siempre hay que recordar que los actores con recursos gigantescos pueden pagar por dicha tecnología y usarla en ataques críticos. Algunas empresas privadas afirman que pueden acceder a cualquier iPhone que posean físicamente. Otros grupos menos pudientes pueden encontrar algunas formas creativas para eludir la seguridad en tales dispositivos, por ejemplo, utilizando servidores de MDM fraudulentos e ingeniería social para pedir a sus blancos que los utilicen en sus dispositivos, lo que permite a los atacantes instalar aplicaciones maliciosas.

Será interesante ver si el código de arranque de iOS filtrado a principios de año proporcionará alguna ventaja a los atacantes, o si encontrarán nuevas formas de explotarlo.

En cualquier caso, no esperamos ningún gran brote de malware dirigido a dispositivos móviles, pero esperamos ver una actividad continua por parte de atacantes avanzados para encontrar formas de acceder a los dispositivos de sus blancos.

LAS OTRAS COSAS

¿En qué estarán pensando los atacantes en términos más futuristas? Una de las ideas, especialmente en el campo militar, podría ser dejar de usar seres humanos, que son débiles y propensos a cometer errores, y reemplazarlos por algo más mecánico. Teniendo esto en cuenta, y también pensando en el ejemplo de los presuntos agentes de GRU expulsados de Holanda el pasado abril después de intentar piratear la red Wi-Fi de la OPCW, surge la pregunta: ¿qué tal si se usan drones en lugar de agentes humanos para hackear a corta distancia?

¿O qué pasa si se utilizan puertas traseras en algunos de los cientos de proyectos de criptomonedas para la recopilación de datos, o incluso para obtener ganancias financieras?

¿Se utilizarán dispositivos digitales para el blanqueo de dinero? ¿Y si se hacen compras en juegos y después se venden esas cuentas en el mercado?

Son tantas las posibilidades, que las predicciones siempre estarán por debajo de la realidad. El entorno es tan complejo que ya no somos capaces de entenderlo en su totalidad, lo que aumenta las posibilidades de ataques especializados en diferentes áreas. ¿Cómo se puede abusar del sistema interno interbancario de una bolsa de valores para cometer fraudes? No tengo ni idea, ni siquiera sé si existe tal sistema. Este es solo un ejemplo de cuán abiertos a la imaginación están los atacantes detrás de estas campañas.

Estamos aquí para intentar anticiparnos, para comprender los ataques que no entendemos y para evitar que ocurran en el futuro.