GUÍA PARA LA DETECCIÓN Y RESPUESTA

REPLANTEE SU ESTRATEGIA DE RESILIENCIA DE CIBERSEGURIDAD E-BOOK

F-Secure

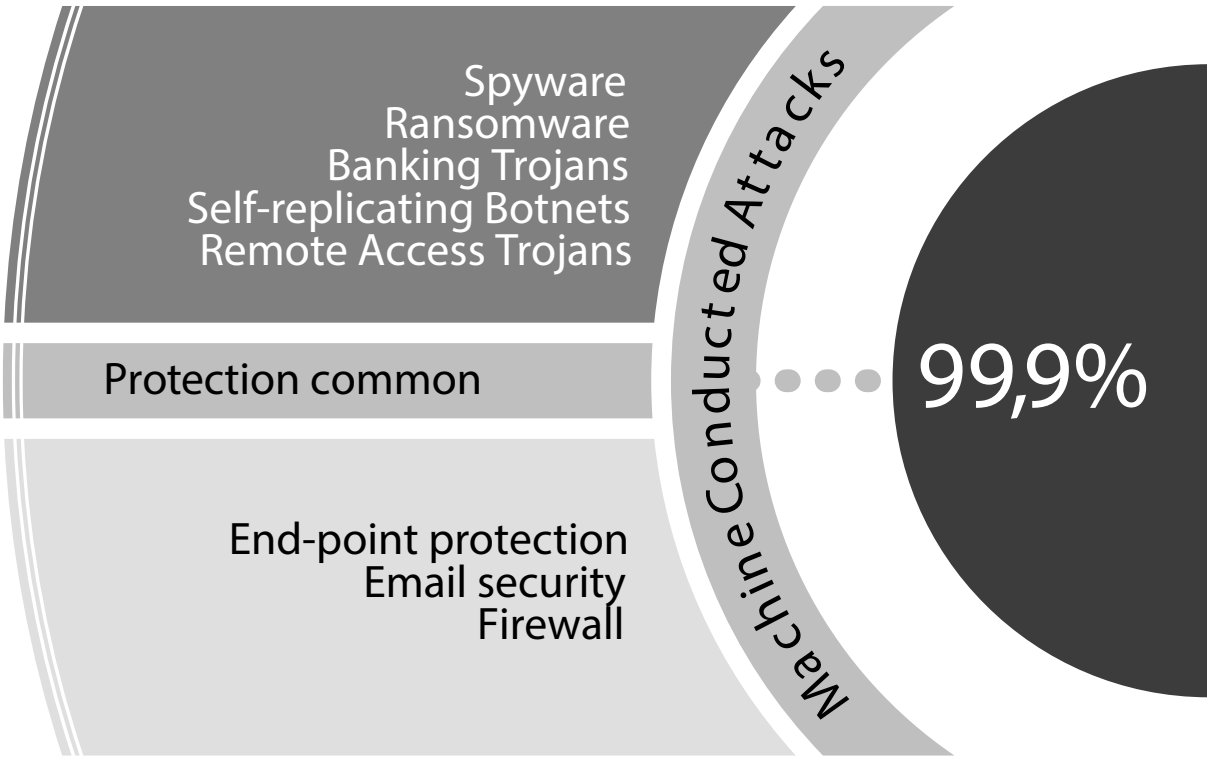
GUIA PARA LA DETECCIÓN Y RESPUESTA

Acerca del campo

En los últimos años, probablemente ha escuchado frases tales como "las tácticas, técnicas y procedimientos elaborados por los actores de la amenaza con muchos recursos caen en manos de adversarios menos habilidosos". Eso es mucho hablar "Espera muchos más guiones para que comiencen a escribir tu sistemas". Como señaló recientemente el Dr. Ian Levy de GCHQ. Muchos de los ataques que estamos viendo hoy en día no son "Amenazas persistentes avanzadas", son simples trucos Realizados por "Toerags Perniciosos Adecuados".

Nada ilustra mejor este fenómeno que el grupo al que hemos denominado "El subterráneo rumano". Este es un grupo con el que hemos tenido experiencia de primera mano en varias ocasiones mientras realizábamos trabajos de respuesta a incidentes y trabajos forenses.

El Subterráneo Romano son, en pocas palabras, un grupo de amigos de la sala de chat de IRC que decidieron que sería genial dedicarse al hobby de "hackear". La mayoría de estos niños, al unirse al colectivo, tienen pocas o ninguna habilidad de Unix para hablar. Probablemente conocen unos cinco comandos en total. Los recién llegados son llevados bajo el ala de un mentor que les proporciona herramientas simples y capacitación para que comiencen con su nuevo pasatiempo. Estos mentores son casi tan inexpertos como los recién llegados: probablemente conozcan cinco comandos de Unix más que sus aprendices.
Pero ya han estado en el juego durante algunas semanas y tienen una gran experiencia.
A medida que los recién llegados aprenden las cuerdas (lo que generalmente implica que han aprendido a configurar y usar un par de herramientas), son promovidos a mentores y contratan a sus propios aprendices. Este modelo jerárquico se asemeja mucho a los esquemas populares de venta de pirámide. que podría haber tenido la desgracia de encontrar. Por supuesto, los individuos involucrados en El Subterráneo Romano no buscan convertirse en millonarios vendiendo jabón. El esquema piramidal es una forma de gamificación, donde el objetivo es recopilar la mayor cantidad posible de sistemas y ascender de rango.



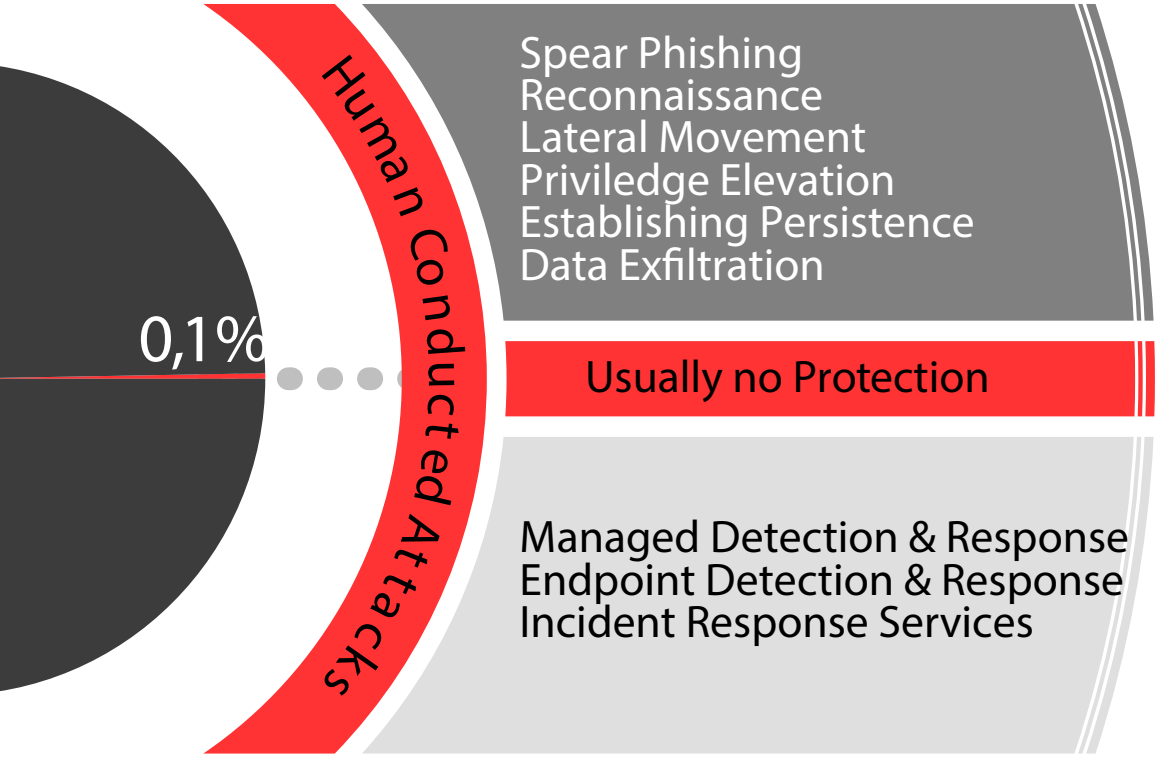
Commodity threats, and the solutions that protect against them are commonplace...

"ESO NO QUIERE DECIR QUE LOS ATACANTES HÁBILES NO ESTÁN TAMBIÉN POR AHÍ". PERO, COMO UNA EMPRESA QUE SE HA IMPLICADO EN MÁS INVESTIGACIONES DE CRIMEN CIBERNÉTICO EUROPEAS QUE CUALQUIER OTRA EN EL MUNDO, PODEMOS DECIRLE QUE NO HAY RAZON DE PREOCUPACIÓN SOBRE LA NSA O EL APT28 HASTA QUE USTED SEPA QUE PUEDE DETENER A ESTOS TIPOS

Naturalmente, son los chicos en la cima de la pirámide quienes realmente se benefician de todo esto. Ellos son los que proporcionan las herramientas y al empujar todo su trabajo manual hacia abajo, obtienen acceso a miles de sistemas comprometidos. Mientras tanto, los recién llegados se complacen en identificarse con orgullo como "piratas informáticos" en sus páginas de Facebook (junto con otros pasatiempos no relacionados, como el wind-surf o el snowboard).

Los kits de herramientas que se empujan hacia abajo en la pirámide generalmente están diseñados para explotar o forzar por fuerza bruta los servicios comunes tales como los servidores SSH y webmail. Lo que podría sorprenderle (o no) es que estos kits de herramientas, en manos de novatos completamente no calificados, se están utilizando para comprometer incluso a las organi-zaciones compatibles con PCI-DSS de todo el mundo. El Subterráneo Rumano representa solo uno de los muchos grupos que forman parte de una tendencia creciente de piratas informáticos y delincuentes cibernéticos poco calificados. Los motivos de los autores intelectuales detrás de estos grupos son, usted lo adivinó, ganancia financiera. Adquirir acceso a un gran número de redes comprometidas de empresas, les permite elegir objetivos principales para la extorsión cibernética y la extracción de datos. Y cualquier empresa es un objetivo potencial.

El hecho de que estos grupos puedan comprometer a las organizaciones compatibles con PCI-DSS es un testamento al hecho de que las soluciones de seguridad cibernética puramente preventivas simplemente ya no lo están deteniendo. Y la razón por la cual tantas compañías ahora son propiedad de este estilo se debe al hecho de que simplemente no tienen una onza de visibilidad en las actividades posteriores a la violación en sus redes.
Eso no quiere decir que los atacantes expertos no estén ahí también. Pero, como una empresa que ha estado involucrada en más investigaciones de delitos cibernéticos en Europa que cualquier otra compañía en el mundo, podemos decirle que no tiene sentido preocuparse por la NSA o el APT28 hasta que sepa que al menos puede detener a estos tipos.



... But targeted attacks have the potential to be a lot more damaging. And most orga nizations aren't protected against those at all. Read on to learn more.

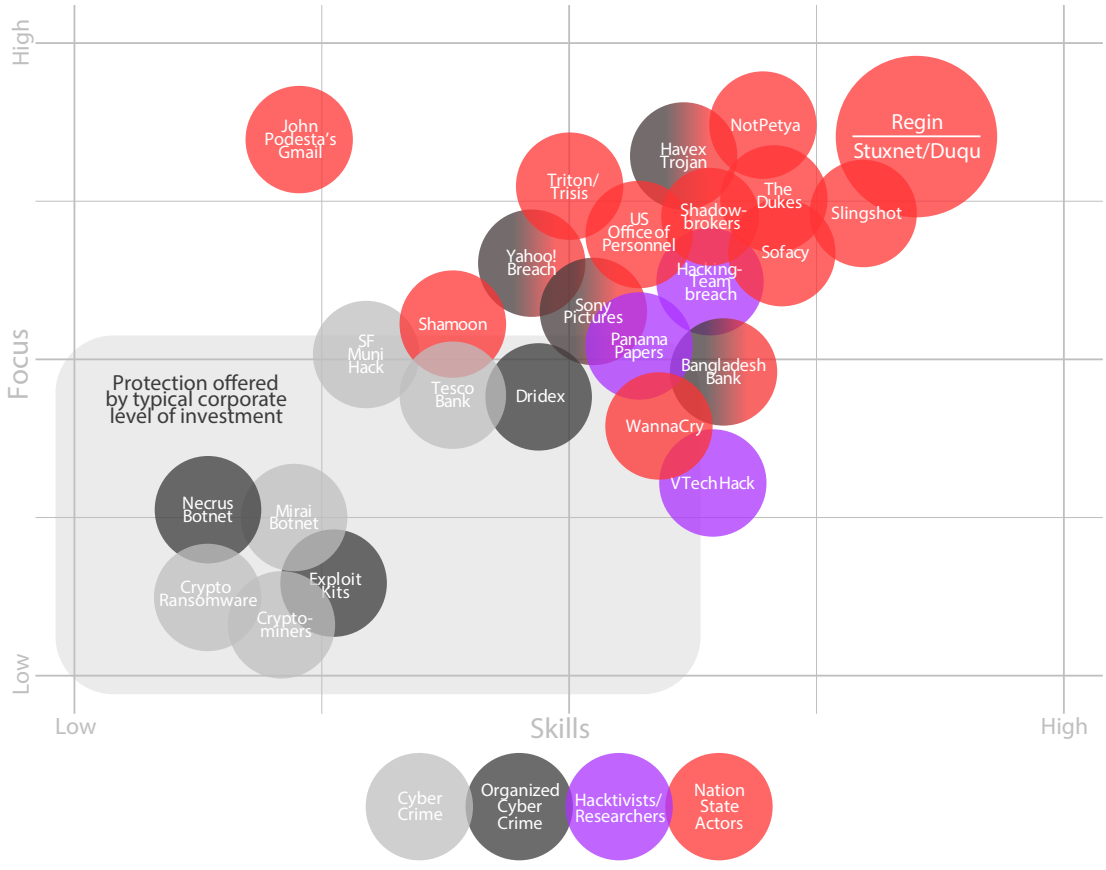
LA ANATOMIA DE UN ATAQUE

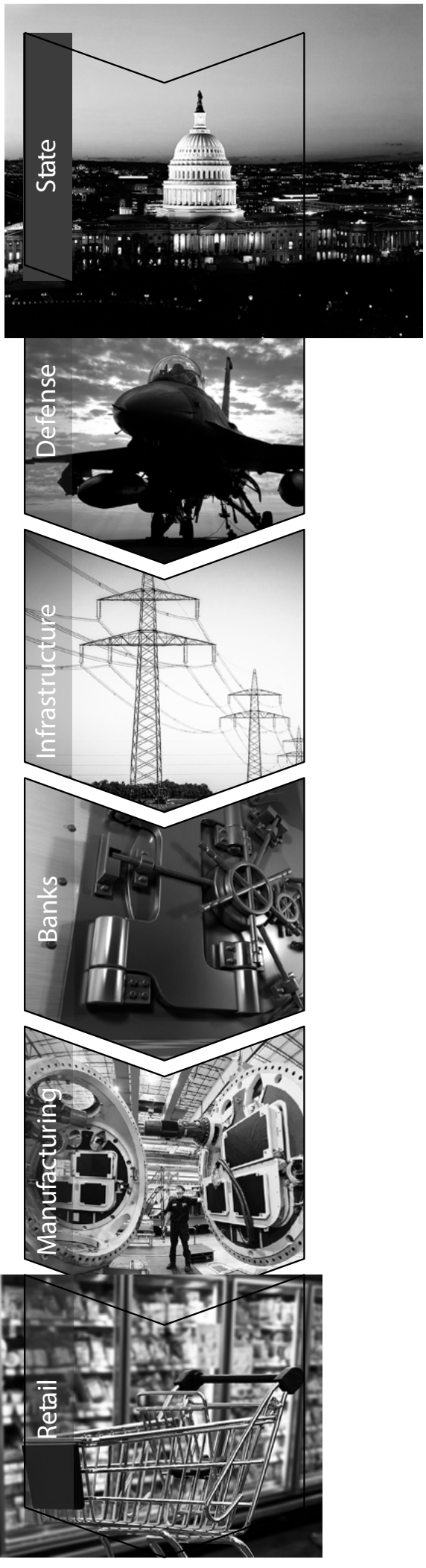
Según nuestra experiencia, la mayoría de las empresas solo analizan la seguridad cibernética en relación con el tema más amplio de la gestión de riesgos. Al realizar el análisis de riesgo, las compañías identifican amenazas o riesgos relevantes para su organización y luego les dan prioridad en función de la probabilidad, el impacto y el costo para mitigar. Al abordar las amenazas cibernéticas, hemos notado una desconexión potencial entre el riesgo que perciben las empresas y la realidad de la situación. Nos gustaría ayudar a aclarar eso.

Los ataques cibernéticos sofisticados tienden a comenzar en la parte superior y se abren camino hacia abajo. Es lo opuesto a la "fruta de baja altura". Cuando se descubren nuevos tipos de ataques, generalmente son atribuibles a actores de amenazas con muchos recursos (es decir, estados nacionales). Estos adversarios, por defecto, van tras los objetivos de mayor valor primero. A medida que las tácticas, técnicas y procedimientos (TTP) utilizados en tales ataques se convierten en conocimiento público, caen en manos de ciberdelincuentes menos organizados. Las nuevas TTP primero se utilizan contra gobiernos, objetivos militares y contratistas de defensa. Los siguientes en la escalera suelen ser Bancos y proveedores de infraestructura crítica (como empresas energéticas). Los mismos TTP luego se utilizan contra la industria pesada y finalmente, todos los demás (fabricación, venta al por menor, PYME, etc).

Las amenazas a una organización no se limitan a ataques desde el exterior. Las fugas accidentales e intencionales pueden originarse y se originan en personas con información privilegiada de la compañía que tienen suficiente acceso a activos críticos o confidenciales. Los ataques ascendentes, donde un socio, proveedor o contratista se ven comprometidos por un atacante que busca establecer una cabeza de playa en una organización adyacente también son muy comunes. En varios casos de respuesta a incidentes en los que hemos estado involucrados, incluso la intrusión física de las instalaciones de una empresa se usó como parte del vector de ataque.

Los ataques cibernéticos vienen en muchas formas, desde malware de productos básicos (como ransomware) hasta ataques altamente calificados realizados por actores de estados nacionales. Hemos dividido estas amenazas en categorías separadas.





"CUANDO LAS REGLAMENTACIONES DE GDPR Y NIS SEAN EFECTIVAS, SERÁ OBLIGATORIO QUE LAS ORGANIZACIONES TENGAN UNA RESPUESTA A LAS VULNERACIONES DE INFORMACIÓN".

Amenazas de productos básicos

Las amenazas de productos básicos son muy frecuentes y lo han sido durante décadas. La posibilidad de una empresa de encontrar amenazas a los productos básicos es, por lo tanto, extremadamente alta. Sin embargo, debido a su prevalencia y larga historia, hay muchas soluciones de software disponibles diseñadas para protegerse contra estas amenazas. Y estas soluciones funcionan según lo previsto. Si una empresa se ve afectada por una amenaza de productos básicos (como crypto-ransomware), el impacto suele ser bastante bajo. La mayoría de las veces estará bloqueado por el software de protección del endpoint. Si se logra filtrar, hay dos opciones: pagar el rescate o solucionar el problema. No pague el rescate y un puñado de empleados perderá un tiempo de trabajo productivo. Pague y la mayoría de las veces, recuperará los datos. Los montos de rescate son bajos para los estándares de la compañía. Por lo tanto, la probabilidad de ver una amenaza de productos básicos es alta, el impacto tiende a ser bajo y el costo de mitigación es básicamente gratuito (asumimos que ya es lo suficientemente inteligente como para ejecutar una solución de protección para endpoint).

Cyber crime

El ciber crimen representa la siguiente catergoría en nuestra escala de evaluación. Esta categoría se mueve hacia el reino de las amenazas malware de las mercancías y hacia ataques dirigidos. Las empresas son seleccionadas como objetivos por varias razones. En algunos casos, una víctima es elegida debido a que ellos mismos se están anunciando via una infraestructura débil o vulnerable. Otros objetivos son seleccionados simple-mente debido a que el atacante está interesado en una organización por una razón u otra.

Los ataques ciber criminales a menudo son oportunistas – el atacante tiene un fácil acceso, ve una oportunidad para hacer dinero y la toma. Los ciberataques son motivados financieramente de manera muy grande.

Una vez que el adversario ha vulnerado la red del objetivo, los sistemas o información será retenidos para pedir rescate. Nos referimos a este fenómeno como “ciber extorsión”. Este tipo de ataques están mucho a la alza y pueden tener como objetivos a organizaciones de cualquier tipo desde PYMES hasta grandes empresas.

Predecimos que la introducción de las reglamentaciones de NIS y GDPR animará a los cibercriminales y los esquemas de ciber extorsión. Una vez que tales reglamentaciones tomen efecto las empresas tendrán mayor voluntad de pagar un rescate para eliminar las noticias de una vulneración bajo la alfombra más que enfrentar la costosa tarea de responder a y reportar el incidente

El crimen cibernético se puede dividir en aproximadamente dos categorías: organizadas y no organizadas. Los grupos organizados de delitos cibernéticos son muy cercanos, en términos de sofisticación, a los actores del estado-nación. Los ataques bancarios de Bangladesh de 2016 son un buen ejemplo de crimen cibernético organizado. Los delincuentes cibernéticos no organizados a menudo corren como lobos solitarios. Tienen menos recursos y su habilidad puede variar.
El metro rumano cae en esta categoría.
Hace dos años, habríamos considerado que la probabilidad de ser presa de los delincuentes cibernéticos era baja. Hoy en día, la probabilidad es media, y en aumento. El impacto financiero y comercial de un ataque dirigido de delitos cibernéticos puede variar. En muchos de los casos a los que hemos respondido, los rescates exigidos por los extorsionadores cibernéticos no organizados solo alcanzaron las decenas de miles de euros, no una suma considerable para la mayoría de las organizaciones. Pero no imaginamos que ninguna organización simplemente pagaría el rescate y se ocuparía de sus asuntos. El conocimiento de que un intruso está en su red será suficiente para llamar a un equipo de respuesta a incidentes para resolver la situación.

Si un adversario logra exfiltrar datos importantes, los costos de un incidente de delito cibernético realmente pueden comenzar a dispararse. Esto es especialmente cierto si los datos del cliente estaban involucrados. Pase lo que pase, lo más probable es que una infracción incurra en costos de reputación, legales, relaciones públicas, negocios y productividad interna. Y las consideraciones ya no se limitan a proteger su negocio y sus datos confidenciales, sino que los organismos reguladores como la Unión Europea han establecido nuevos requisitos. Por ejemplo, el Reglamento de protección de datos general (GDPR) de la UE exige que las organizaciones estén adecuadamente preparadas para detectar, responder e informar sobre violaciones de datos personales dentro de las 72 horas.

Estado nacional

Las compañías que se preocupan por ser blanco de ataques de estado-nación generalmente saben quiénes son. También saben que defenderse contra un ataque de estado-nación es casi imposible. En cualquier caso, se ven obligados a intentarlo (ya que no pueden darse el lujo de no hacerlo). El impacto de los ataques de estado-nación puede variar desde que la propiedad intelectual de alto secreto sea robada por competidores o gobiernos extranjeros hasta que se detenga su enriquecimiento nuclear o cibernético.

Informe especial de Gartner
La ciberseguridad a la velocidad de los negocios digitales
Paul E. Proctor, Ray Wagner, 30 de agosto de 2016, actualizado en diciembre de 2017

"LOS ATAQUES DIRIGIDOS NO SE PREOCUPAN POR SU PRODUCTO" PRÓXIMO ", NO IMPORTA CUÁNTO EL CONCURRENTE DEL VENDEDOR LO RECLAMA A SER. PARA SER BLUNTOS, LAS SOLUCIONES QUE ESTÁN VENDIENDO ESTÁN FIJANDO LOS PROBLEMAS INCORRECTOS ".

NO CREAS EN EL HYPE

Llegando al punto de por qué presentamos este análisis de riesgos, hemos notado que todavía hay un fuerte impulso de marketing hacia las soluciones de protección de puntos finales. Hemos visto a los proveedores de "próxima generación" afirmar que sus soluciones pueden prevenir ataques dirigidos. Algunos incluso afirman tontamente que la detección de infracciones es irrelevante, ya que ya es un "juego terminado" si una amenaza atraviesa las defensas del perímetro.

Estado nacional

Los ataques dirigidos no se preocupan por su producto de "próxima generación", sin importar qué tan brillante sea el proveedor. Para ser franco, las soluciones que están vendiendo son arreglar el problemas incorrectos
Debido a este gran impulso de marketing de la "próxima generación", no estamos realmente sorprendidos de ver que muy pocas empresas con las que hemos hablado son conscientes de la necesidad de detectar fallas.

y capacidades de respuesta. Y ahí radica el problema. Las organizaciones están demasiado distraídas como para darse cuenta de que deberían comenzar a invertir en la detección y respuesta de brechas, en lugar de otra capa de protección contra las amenazas de los productos básicos (aunque a los adversarios les encantaría que lo hiciera). Pongámoslo de esta manera: ¿preferiría que su próximo incidente implique limpiar el malware de una computadora portátil en su departamento de ventas o lidiar con una violación de datos en toda regla.

Pero no solo tome nuestra palabra por ello. Gartner predice que "para 2020, el 60 por ciento de los presupuestos de seguridad de la información empresarial se asignarán a los enfoques de detección y respuesta rápidos, lo que representa un aumento de menos del 30% en 2016". Entonces, pregúntese lo siguiente: cuánto de su presupuesto ¿Ha asignado la detección y respuesta de violación en este momento? Suponemos que no está cerca del 60 por ciento. Según nuestra experiencia, solo el 10% de las empresas con las que hemos hablado pensaban en ello.

PARA 2020, EL 60 POR CIENTO DE LOS PRESUPUESTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA SE ASIGNARÁN A ENFOQUES DE DETECCIÓN Y RESPUESTA RÁPIDOS, LO QUE REPRESENTA UN AUMENTO DE MENOS DEL 30% EN 2016

Informe especial de Gartner
`La ciberseguridad a la velocidad de los negocios digitales
Paul E. Proctor, Ray Wagner, 30 de agosto de 2016, actualizado en diciembre de 2017

"CUALQUIER ORGANIZACIÓN QUE NO CORRE UNA SOLUCIÓN DE DETECCIÓN DE INCUMPLIMIENTO (O QUE NO HA REALIZADO UNA INVESTIGACIÓN RECIENTE) DEBE EN ESTE DÍA Y EDAD, ASUMIR QUE ESTÁ EN UN ESTADO POST-INCUMPLIMIENTO".

DEL DILEMA DE UN DEFENSOR A UN IMPASSE DE INTRUSO

Las amenazas cibernéticas son de naturaleza asimétrica. Un atacante solo necesita tener éxito una vez para obtener acceso a una red. Los defensores deben tener éxito el cien por ciento del tiempo si quieren mantenerlos fuera. No puedes confiar en tener éxito todo el tiempo.

Y sin embargo, esto es lo que la mayoría de las empresas están haciendo. Las tecnologías de defensa perimetral tradicionales, como los firewalls y el software de protección de puntos finales, hacen un buen trabajo en lo que deben hacer, es decir, detectar y bloquear amenazas del mundo real y de los productos básicos. Pero no se puede esperar que estas soluciones detengan a los adversarios avanzados. Cualquier adversario que valga la pena hará un ataque diseñado para eludir esas defensas. Y ni siquiera necesitarán usar malware para ganarse la vida en la organización (al contrario de lo que se podría haber dicho, los atacantes expertos rara vez, si es que alguna vez, usan malware).

Los ataques cibernéticos suelen seguir el mismo patrón. Los atacantes comienzan rompiendo el perímetro de una organización con spear-phishing, abrevadero o ataques de hombre en el medio. A veces, los atacantes pueden ingresar al explotar una vulnerabilidad en un sistema público, o incluso al comprar acceso a un sistema ya comprometido. Una vez dentro del perímetro, los adversarios realizan reconocimientos, elevan los privilegios (mediante la explotación de sistemas mal configurados o vulnerables), buscan contraseñas de administrador de dominio (utilizando herramientas de raspado de memoria como Mimikatz) y pasan lateralmente a sistemas interesantes. A menudo, establecerán la persistencia mediante el uso de RAT estándar, como Orcus, Litemanager o luminocityLink.

Luego, exfiltrarán los datos utilizando métodos sutiles diseñados para imitar el comportamiento normal del usuario.

La mayoría de las herramientas que necesita un atacante están integradas en el propio sistema operativo. Y los atacantes son expertos en esconderse de los sistemas IDS basados en la red al ocultarse en el comando y controlar el tráfico. Es casi imposible detectar técnicas modernas de ataque simplemente analizando el tráfico de red. De hecho, hay muchas formas de ocultarse para un atacante. Todas estas técnicas vuelan bajo el radar de las defensas tradicionales del perímetro, como los cortafuegos, la protección de puntos finales y el filtrado de correo no deseado.

En la mayoría de los casos, una vez que una empresa ha sido violada, los adversarios pueden actuar con impunidad durante el tiempo que deseen. No es raro que una empresa descubra que ha sido comprometida por un tercero (como una organización cert). En nuestra experiencia en el campo, en promedio, el tiempo entre una violación y el descubrimiento es de 200 días. Piense en eso: la mayoría de las organizaciones tarda meses o incluso años en darse cuenta de que han sido pirateados.
Cualquier organización que no ejecute una solución de detección de infracciones (o que no haya realizado una investigación reciente) debe, en la actualidad, asumir que se encuentra en un estado posterior a la infracción.
Las infracciones son cada vez más comunes. Y esto se debe a que los publicistas saben que sus objetivos no tienen idea

están siendo hackeados Para muchos atacantes, comprometer los sistemas es tan fácil como un ladrón entrando a una casa con la puerta delantera completamente abierta.

Pero aquí hay algo interesante: los adversarios en realidad odian la idea de ser atrapados. Y odian operar en un entorno donde existe la posibilidad de que estén siendo monitoreados. Es por eso que la mayoría de los buenos atacantes ejercerán precaución. Una vez dentro de la red de la víctima, un intruso profesional pisará a la ligera, mientras está constantemente buscando señales de que ha sido detectado.

Los atacantes saben que un buen defensor no reaccionará ante los signos de una intrusión en un pánico: observarán al intruso, reunirán información y luego actuarán sobre la situación cuando estén listos y listos. Como defensor, la detección exitosa y la respuesta efectiva constituirán, a los ojos del adversario, una violación de su misión.

Si bien parece que los atacantes tienen la ventaja, en realidad hay mucho que los defensores pueden hacer para voltear las mesas. Todo lo que hace el atacante está obligado a dejar un rastro de evidencia detrás de ellos. Y mientras que un sistema comprometido puede no ser capaz de decirle cuándo es "propiedad", existe la posibilidad de que registre alguna evidencia. Esa evidencia se puede usar para detectar al intruso, o incluso viajar en el tiempo para reconstruir los movimientos del adversario.

Imagínese la frustración cuando un atacante se da cuenta de que se ha monitoreado cada movimiento que han realizado, que han expuesto toda su cadena de herramientas y que efectivamente se los ha enviado de vuelta al punto de partida. No es un gran sentimiento para el atacante. Y una gran victoria para el defensor.

Este es, en nuestra opinión, el mejor enfoque para la defensa cibernética. Vamos a profundizar en cómo lograr ese objetivo.

¿QUÉ ESTRATEGIA ES CORRECTA PARA USTED?

De todos los desafíos que enfrentan las organizaciones mientras desarrollan capacidades de detección y respuesta de violaciones, nada realmente se compara con la dificultad que enfrentan cuando intentan contratar y retener una buena experiencia en seguridad
cibernética. Se estima que, en este momento, hay al menos dos trabajos de seguridad cibernética por cada persona que trabaja en el campo. Se espera que este problema se agudice aún más en el futuro. La única forma de obtener datos válidos de un sistema interno de detección de intrusos (IDS) es contar con expertos en el personal. Lo mismo ocurre con mantenerse al día con la inteligencia de amenazas, configurar sistemas, formar equipos rojos y responder a incidentes correctamente. Por lo tanto, probablemente necesitará más de uno o dos expertos en su nómina.

Y aunque eventualmente podría desarrollar su propio equipo interno, sistemas y experiencia, en la mayoría de los casos significa asumir un proyecto largo y costoso. Finalmente, operar su propio Centro de Operaciones de Seguridad (SOC) 24/7 con recursos adecuadamente capacitados puede llevar el costo total de propiedad al nivel que solo las empresas más grandes están preparadas para invertir.

Con la falta de defensores hábiles de su lado, y con las dificultades y los costos asociados con la creación de sus propias capacidades de detección y respuesta de incumplimiento, las empresas están luchando contra los ataques cibernéticos y perdiendo. Esta es la razón por la cual F-Secure ha pasado los últimos años desarrollando y perfeccionando los servicios de detección y respuesta administrados para las diferentes necesidades de las empresas, para poner nuestra experiencia de seguridad cibernética de clase mundial al alcance de cada organización.

Sin embargo, nuestros servicios no solo proporcionan experiencia humana. Se construyen sobre inteligencia de amenazas, análisis de muestras y tecnologías de toma de decisiones que se han desarrollado internamente durante más de una década. Y si bien una organización podría desarrollar sus propios sistemas internos y experiencia a los niveles que hemos alcanzado, les llevaría mucho tiempo.

Nuestros servicios de detección y respuesta administrados están disponibles con diferentes niveles de servicio y modelos para adaptarse a las necesidades de una organización, ya sea empresarial o de tamaño mediano. Le invitamos a considerar las siguientes tres alternativas.

OPCIÓN 1

Hazlo tú mismo (con opción de aumentar tu equipo)

Muchas organizaciones tienen los recursos para invertir mucho en sus propios equipos de seguridad e infraestructura. Pero incluso las empresas bien invertidas con su propio SOC pueden encontrar valor en aumentar su propio equipo con un proveedor que proporciona exclusivamente servicios de seguridad cibernética. Un equipo extendido que trabaje junto con su equipo de TI puede ayudarlo a superar el problema de contratar y retener un equipo de seguridad de TI lo suficientemente grande.

No todas las empresas que manejan la detección y la respuesta en la empresa necesariamente tienen personal que trabaja 24/7para proteger sus operaciones. A estas organizaciones les puede resultar útil invertir en una solución de detección y respuesta de Endpoints que ayude a su equipo de TI a identificar los ataques durante el horario comercial y también proporcione cobertura fuera del horario comercial con respuesta automática para aislar a los atacantes. Tal enfoque puede ser suficiente para determinar rápidamente el alcance de un ataque, identificar si algún dato personal fue afectado o no, y ser capaz de cumplir con los requisitos reglamentarios para reportar vulneraciones de datos dentro de las 72 horas, según lo requiere el GDPR.

OPCIÓN 2

Gestión de la Detección y Respuesta con F- Secure para 24/7

Para superar la dificultad de tratar de contratar y retener experiencia en seguridad cibernética calificada, F-Secure ofrece servicios de detección y respuesta completamente administrados (MDR). Lo que entendemos por "administrado" es que hay un proceso de instalación mínimo para que las cosas se pongan en marcha, y después de eso, nosotros manejamos todo, desde la detección de vulnerabilidades hasta la respuesta. Nuestros equipos de cazadores de amenazas, personal de respuesta a incidentes y expertos forenses están disponibles las 24 horas del día para un servicio de detección y respuesta de infracciones totalmente administrado que llamamos Servicio de Detección y Respuesta Rápida (RDS).

Con el servicio de detección y respuesta rápida, tendrá la ventaja de que los expertos en seguridad cibernética de clase mundial de F-Secure monitorean su red 24/7. Revisarán todas las detecciones en minutos y determinarán la severidad antes de alertar a su equipo. Las falsas detecciones positivas se marcan de inmediato para garantizar que su equipo solo dedique tiempo a las amenazas reales. Trabajar con nuestros expertos en seguridad cibernética significa que todas las detecciones vienen con orientación y, si es necesario, mayores aclaraciones. La disponibilidad de experiencia humana significa que su equipo pasará mucho menos tiempo en detecciones.

Sin embargo, el Servicio de Detección y Respuesta Rápida no solo proporciona experiencia humana. Es un servicio que se basa en la inteligencia de amenazas, análisis de muestras y sistemas de toma de decisiones con capacidades de aprendizaje automático e inteligencia artificial que se han desarrollado internamente durante más de una década. Y si bien una organización podría eventualmente desarrollar sus propios sistemas internos y experiencia a los niveles que hemos alcanzado, les tomaría mucho tiempo.
Aumentar la disponibilidad y las habilidades de su propio equipo con la ayuda del Servicio de detección y respuesta rápida de F-Secure ayuda para alcanzar fácilmente la disponibilidad 24/7 con un nivel de servicio de 30 minutos y recibir orientación experta para responder en caso de ataque.

OPCIÓN 3

Detección y Respuesta para Endpoint Administrado con un Proveedor Local de Servicio

Un enfoque alternativo para la detección y respuesta administrada es una solución de detección y respuesta de Endpoints (EDR) como F-Secure Rapid Detection & Response, que es suministrada por socios proveedores de servicios certificados y capacitados.
F-Secure capacita a nuestros proveedores de servicios administrados locales para apoyarlo en todo, desde la supervisión del estado de la salud y la seguridad de su entorno de TI, hasta la detección y la orientación de las acciones de respuesta en caso de vulnerabilidades. El proveedor de servicios local está respaldado por la automatización que puede utilizarse para ampliar su disponibilidad más allá de las horas de oficina y también está respaldado por los expertos de F-Secure para manejar incluso los casos más complejos. Muchas compañías encuentran que un proveedor local de servicios administrados es la opción más adecuada para ayudar a mantener bajos sus costos operativos. Según nuestra experiencia, estas tienden a ser organizaciones pequeñas y medianas.
Incluso si su empresa cuenta con una buena inversión de su propio SOC, puede considerar la posibilidad de aumentar su propio equipo con un servicio de detección y respuesta administrados para alcanzar la disponibilidad 24/7 y de menos de 30 minutos para el tiempo de una detección respuesta.

CONSTRUIR LAS CAPACIDADES INTERNAS DE DETECCIÓN Y RESPUESTA DE VULNERABILIDADES ES DIFÍCIL

Nos hemos dado cuenta de que, para la mayoría de las organizaciones, la configuración de las capacidades internas de detección y respuesta de vulnerabilidades tiende a ser una tarea complicada, lenta y costosa. Hay varios componentes que necesitan implementación y configuración. Todos ellos son caros, por lo que las decisiones de compra requieren tiempo e investigación. Los diferentes componentes pueden o no interoperar bien, por lo que también tiene que darse cuenta de eso. Luego debe seleccionar las fuentes de inteligencia de amenazas, y hay docenas, si no cientos, de ellas disponibles. Implementar y configurar estos sistemas es un trabajo complicado. Y al final de todo esto, te quedarás preguntándote si tienes todo cubierto y si todas las piezas se están hablando entre sí correctamente o no. Y eso es sólo la instalación inicial. Después de eso los sistemas, las reglas y alimentación de datos deben mejorarse y modificarse constantemente a medida que el mundo cambia.

Responder a una vulneración también suele ser un proceso largo y costoso que requiere datos forenses de expertos y un trabajo de respuesta a incidentes. Un escenario de respuesta típico incluye eliminar al adversario de la red, limpiar o restaurar los sistemas afectados, restablecer las cuentas comprometidas, determinar dónde ha estado el intruso y determinar qué ha hecho el intruso. La mayoría de las compañías no tienen la experiencia o las capacidades internas para realizar este tipo de actividades, por lo que deben solicitar ayuda a un tercero para auxiliarse.

DEL HÁGALO USTED MISMO AL RETORNO DE INVERSIÓN (DIY TO ROI)

Dado que la experiencia, monitoreo, la búsqueda de amenazas y capacidades de respuestas están cubiertas por F-Secure o por nuestros proveedores, una vez que se ha decidido a implementar el servicio en su organización, todo lo que necesita hacer es instalar unos sencillos sensores en los Endpoints de su organización. El tiempo que transcurre desde la implementación y configuración inicial hasta las capacidades reales de detección y respuesta de vulneraciones es inferior a una semana. De hecho, varios clientes nos han dicho que tenemos el sistema más fácil con el que hayan trabajado.

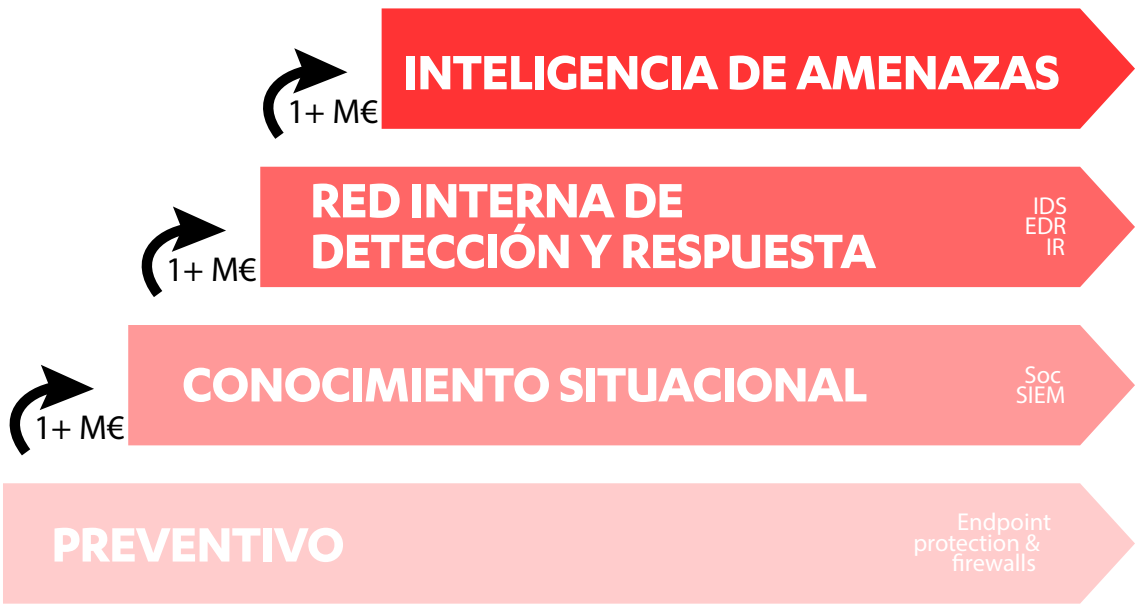
La alternativa a implementar un servicio administrado de detección y respuesta de vulnerabilidades es un proyecto largo (en la mayoría de los casos de 3 a 5 años) y costoso (miles de millones de euros) para la compra, implementación y configuración de sistemas dedicados, y la contratación y capacitación de un personal considerable.

Pero un enfoque administrado para la detección y respuesta no se trata solo de un rápido retorno de la inversión. Hemos visto a muchas compañías tomarse la molestia de crear un SOC y establecer un IDS y SIEM, solo para aun así no detectar amenazas.

Esto se debe a que, según nuestra experiencia, encontrar amenazas reales es como buscar una aguja en un pajar.

Para ilustrar con un ejemplo reciente del mundo real, en una instalación de un cliente de 1000 nodos, nuestros sensores recolectaron alrededor de 2,000,000,000 de eventos durante un período de un mes. El análisis de datos sin procesar en nuestros sistemas de back-end filtró ese número hasta 900,000. Nuestros sistemas de aprendizaje automático y los mecanismos de Detección de contexto amplio ™ redujeron ese número a 25. Finalmente, se analizaron esos 25 eventos, donde se descubrieron 15 amenazas reales (y el cliente las verificó).

La cuestión es que, si elige su propia solución IDS / SIEM, su organización necesitará procesar esos 900,000 eventos. Y es por eso que hemos visitado innumerables sitios de clientes y hemos encontrado amenazas en sus redes, a pesar de que los clientes ya tienen soluciones IDS muy conocidas. Combinar el ruido y los falsos positivos es difícil y puede causar fatiga incluso en los analistas más diligentes.



Para procesar este volumen de eventos, también necesita una inteligencia de amenazas actualizada y confiable. En F-Secure tenemos nuestras propias fuentes internas. Y después de más de 30 años en el negocio también tenemos una colección enorme de muestras históricas que incluso nos da la capacidad de encontrar amenazas relevantes que aún no han sido descubiertas por los actores de amenazas actualmente activos. Nuestros investigadores realizan investigaciones de inteligencia de amenazas e ingeniería inversa. Esto nos brinda un conocimiento de alto nivel del panorama de amenazas globales y un conocimiento técnico profundo de las amenazas en sí. En lugar de estudiar cada amenaza de forma independiente, identificamos las relaciones entre las amenazas, lo que nos permite comprender las capacidades y los motivos de un adversario. Nos enfocamos en el rompecabezas completo y no solo en las piezas individuales.

CENTRO DE DETECCIÓN Y RESPUESTA RAPIDOS

En el núcleo del enfoque de F-Secure para la protección avanzada de amenazas está nuestro Centro de Respuesta y Detección Rápida (RDC), que es la base de operaciones de todos nuestros servicios de respuesta y detección. En RDC, los expertos en seguridad cibernética trabajan las 24 horas del día, los 7 días de la semana, donde buscan amenazas, monitorean los datos y alertas directamente desde los entornos del Servicio de detección y respuesta rápida, de nuestros clientes identifican anomalías y señales de vulnerabilidades y luego trabajan con nuestros clientes para responder a incidentes reales a medida que se producen. También respaldan a nuestros proveedores de servicios certificados de F-Secure Rapid Detection & Response cuando se necesita su experiencia para resolver los casos más exigentes.

El personal de RDC tiene acceso a nuestras propias herramientas de búsqueda de amenazas y analíticas internas, de clase mundial, todos nuestros datos de inteligencia de amenazas, y una gran cantidad de información y conocimiento de nuestros Servicios de Seguridad Cibernética y las organizaciones F-Secure Labs. De hecho, todos estos equipos colaboran estrechamente entre sí.

El personal de nuestro Centro de Respuesta y Detección Rápida está capacitado para manejar una variedad de tareas. También capacitamos a nuestros proveedores de servicios administrados en muchas de estas tareas. Las tareas principales se dividen en aproximadamente tres roles diferentes: cazadores de amenazas, personal de respuesta a incidentes y expertos forenses

Cazadores de amenazas

Los cazadores de amenazas son los primeros en responder por parte nuestra. Ellos monitorean el servicio y buscan amenazas. Cuando un cazador de amenazas descubre algo sospechoso, se reúnen pruebas para verificar el incidente. Si se descubre un incidente real, se le da una prioridad. Las alertas de alta prioridad se generan cuando hay un fuerte indicio de una vulneración en curso y en estos casos, se contacta al cliente de inmediato por teléfono. Para casos no críticos, la guía se envía al cliente por correo electrónico. Los cazadores de amenazas también mantienen al cliente actualizado sobre cualquier investigación en curso.

Personal de respuesta a incidentes

Se asignan los casos complejos al personal de respuesta a incidentes que los clientes no pueden manejar por sí mismos y pueden ayudar al cliente de forma remota o in situ. El personal de respuesta a incidentes puede ayudarlo con una variedad de actividades de respuesta técnica y no técnica, según las necesidades del cliente. También estamos familiarizados con la recopilación de pruebas para fines de aplicación de la ley, en caso de requerirse.

Expertos forenses

Los expertos forenses son especialistas encargados de los casos más difíciles. F-Secure es una de las pocas organizaciones a nivel mundial que puede manejar una amplia gama de tareas forenses, desde la selección interna de la red hasta la ingeniería inversa profunda de muestras de malware únicas. Esto nos permite manejar incluso los ataques más complicados originados en estados nacionales.

EQUIPO ROJO

Las capacidades de seguridad del servicio de detección y respuesta se desarrollan principalmente utilizando un enfoque interactivo de equipo rojo. En resumen, ponemos a nuestros tipos de sistemas de ataque, a averiguar lo que el servicio no pudo detectar y a realizar mejoras. Algunas mejoras se hacen a mano. Otros son aprendidos por nuestros sistemas backend durante los ejercicios de equipo rojo. Como parte de este proceso, documentamos y visualizamos las diversas cadenas de ataque utilizadas, lo que permite a los miembros del equipo rojo crear nuevos métodos de ataque más tortuosos.

Nuestra primera recomendación para los clientes que acaban de comprar el servicio de detección y respuesta de F-Secure es traer a un tercero y realizar un ejercicio de equipo rojo contra nuestro servicio. No solo le ayuda a verificar que todo se haya configurado correctamente, sino que también le permite ver el proceso en acción, lo cual es un agradable camino para practicar para un incidente real.

En el tema de la formación de equipos rojos, hemos desafiado a terceros a que pasen por alto los servicios de detección y respuesta de F-Secure, pero ninguno lo ha logrado todavía. Pero hay más. Hay al menos setenta empresas que afirman que pueden detectar y remediar cualquier ataque dirigido. En nuestra experiencia, hay muy pocos que realmente pueden. ¿Como lo sabemos? Bueno, hasta ahora, tenemos una tasa de éxito impecable en las asignaciones de exposición corporativa (donde un cliente ordenó un ataque dirigido a nosotros). En todos los casos, hemos violado exitosamente a las organizaciones que manejan los productos de nuestros competidores. Y ninguno de esos productos detectó nuestros ataques. No vamos a mencionar ningún nombre.

HOMBRE Y MÁQUINA

En F-Secure hemos reconocido que proteger a nuestros clientes de amenazas avanzadas requiere más que tecnologías de clase mundial basadas en inteligencia artificial. La mejor manera de proporcionar una capacidad de respuesta y detección de violaciones sin igual no es construir una herramienta avanzada de búsqueda de amenazas, sino combinar equipos y máquinas con sistemas de aprendizaje automático y experiencia en seguridad cibernética. Desde el principio, reconocimos las dificultades que otras compañías tenían para desarrollar sus propias capacidades de detección y respuesta de fallas con un enfoque de Hágalo Usted Mismo y decidimos tomar la ruta del servicio administrado.

También reconocemos las diferentes necesidades que tienen varias organizaciones, por lo que diseñamos nuestros servicios administrados para que estén disponibles con diferentes niveles de servicio y modelos para entregar el servicio. El equipo de F-Secure está disponible 24/7 y puede proporcionar servicios de clase mundial con un tiempo de respuesta de 30 minutos después de detectar una amenaza real. Nuestros proveedores de servicios administrados certificados también tienen diferentes niveles de servicio, como la disponibilidad solo durante el horario comercial local respaldado por la automatización las 24 horas.

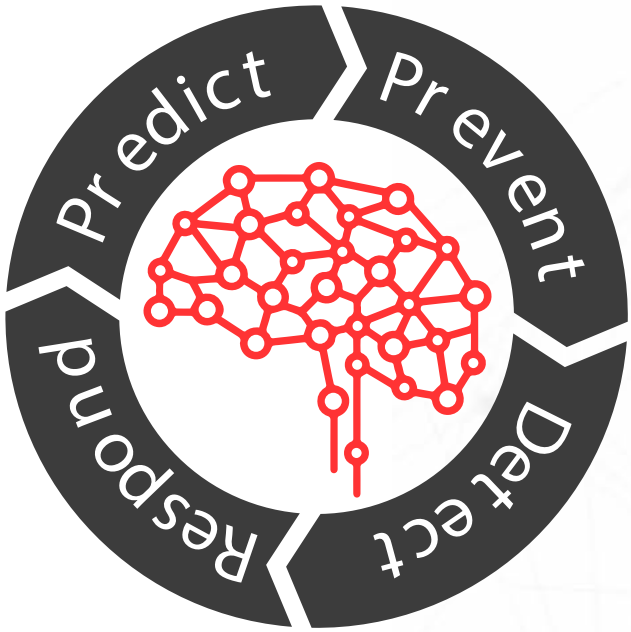
Recomendamos que las organizaciones calculen su retorno de la inversión (ROI) con enfoques alternativos antes de simplemente comprar una pieza de tecnología o contratar un equipo importante para operar la tecnología. Puede ser difícil alcanzar un ROI positivo para desarrollar sus propias capacidades, especialmente después de que también se haya considerado la experiencia humana necesaria.

DETECTANDO EL CONTEXTO MÁS AMPLIO

Cuando se produce un ataque dirigido, necesitará una imagen más amplia de la que puede proporcionar la detección de un host afectado. Para comprender completamente la verdadera gravedad de cada ataque, deberá discernir el contexto más amplio y hacerlo rápidamente.

Para superar el problema de tener demasiados eventos de datos sin procesar para que un humano los procese, F-Secure ha desarrollado un análisis de datos de comportamiento para reducir los datos, junto con los mecanismos de Detección de contexto amplio ™ para construir un contexto alrededor de todos los eventos relevantes en los hosts afectados. La Detección de Contexto Amplio ayuda a las personas a entender fácilmente el ataque dirigido mediante la visualización del conjunto de circunstancias en torno a un ataque e incluso proporciona acciones recomendadas sobre cómo responder. La Detección de Contexto Amplio es un excelente ejemplo del enfoque "hombre y máquina" de F-Secure que permite a las personas detener el ataque rápidamente o incluso definir acciones de respuesta automatizadas cuando el equipo no está trabajando.

ADMINISTRACIÓN DE INCIDENTES E INVESTIGACIONES



Cuando se descubre una infracción, tener acceso a los datos históricos es la clave para crear una línea de tiempo detallada del evento posterior a la infracción. Dado que los adversarios casi invariablemente borran los datos para cubrir sus huellas durante un ataque, tener acceso a los datos que se almacenan fuera de las instalaciones significa tener prácticamente una garantía.

Se presentó una fuente de evidencia a prueba de manipulación indebida para la respuesta a incidentes y los investigadores forenses. En el caso de un incidente, ayudamos al cliente a preservar cualquier evidencia que sea esencial en las acciones de respuesta a incidentes posteriores.

Los servicios de detección y respuesta de F-Secure también están diseñados para buscar la existencia de amenazas recientemente descubiertas en los datos históricos. La búsqueda retrospectiva de amenazas se logra cuando se ejecutan nuevos algoritmos de detección con los datos históricos recopilados de cada uno de nuestros clientes. Este mecanismo es especialmente útil cuando se trata de ataques de adversarios más avanzados (que pueden haber estado ocultos durante algún tiempo).

La solución de F-Secure se puede implementar durante el trabajo continuo de respuesta a incidentes, y se utiliza como un servicio de búsqueda de amenazas que puede ganar rápidamente visibilidad en una red que ya ha sido violada.

Finalmente, los servicios continúan trabajando fuera de la red corporativa. En un mundo donde el perímetro de seguridad clásico se está desmoronando, los enfoques tradicionales de IDS se han vuelto ineficaces (ya que normalmente solo funcionan en el borde de la red). Estos enfoques tradicionales no pueden rastrear amenazas cuando los dispositivos están fuera de la red corporativa o cuando las personas utilizan servicios basados en la nube. Nuestro enfoque de sensor de punto final resuelve este problema de manera bastante efectiva. Además, hemos estado trabajando para extender las capacidades del servicio a servicios en la nube, como Salesforce.

CAZA DE AMENAZAS Y CIENCIA DE DATOS

A diferencia del enfoque tradicional de crear y aplicar un conjunto de detecciones basadas en el comportamiento "malo" conocido, ejecutamos ataques reales contra nuestros sistemas y los entrenamos sobre cómo se ve el comportamiento "bueno". Luego marcamos todo lo demás para un análisis más a fondo y un filtrado de falsos positivos. Creemos que este es el enfoque que la mayoría de los otros proveedores de detección de infracciones también tomarán en cuenta en el futuro.

Los sistemas de caza de amenazas deben poder adaptarse a los cambios rápidamente. Todo en un ambiente monitoreado está en flujo. La gente y los dispositivos van y vienen. Los sistemas operativos y el software son parcheados. Surgen nuevas amenazas y TTPs. Debido a la naturaleza de este flujo, las soluciones tradicionales de IDS tienden a ser “ruidosas” y propensas a falsas alarmas. Estas mismas soluciones tradicionales también son siempre un paso detrás del panorama de amenazas.

Para abordar este problema, nuestros científicos de datos, trabajando junto con los expertos de RDC, han diseñado y desarrollado una serie de análisis estadísticos de fondo, aprendizaje automático y sistemas expertos para respaldar a nuestros analistas. El núcleo del backend de F-Secure es muy simple, y toda la complejidad está integrada en los algoritmos circundantes. Este enfoque permite tiempos de despliegue muy rápidos para nuevos algoritmos de detección (en minutos) y nos permite adaptarnos a los cambios rápidamente. Con el servicio de detección y respuesta de F-Secure en funcionamiento, nunca es necesario esperar a que los sistemas implementados en sus propias instalaciones reciban actualizaciones; toda la lógica está en nuestros sistemas backend.

Nuestros sistemas de análisis realizan una serie de tareas, desde analizar y aprender comportamientos en entornos monitoreados hasta reducir falsos positivos. Diferentes técnicas de análisis son más adecuadas para diferentes tareas. Por ejemplo, un sistema experto es el más adecuado para encontrar el tipo de comportamiento causado por las herramientas comunes de ataque y por los TTP empleados por los ciberdelincuentes. Estos incluyen comandos de PowerShell y direcciones URL maliciosas y direcciones IP. Los sistemas de aprendizaje automático están diseñados para detectar malos comportamientos previamente desconocidos, como secuestros DHCP, falsificaciones y otras tácticas de evasión sigilosa. También utilizamos diferentes combinaciones multinivel de sistemas expertos, análisis estadístico y aprendizaje automático.
Hemos encontrado que los análisis estadísticos simples son los más adecuados para eliminar los falsos positivos, y al aplicar estos métodos, actualmente eliminamos aproximadamente el 80% de todas las alertas irrelevantes. La forma en que construimos estos sistemas y la forma en que interactúan entre sí es bastante única, y es algo que no hemos visto en ninguna otra parte de la industria.

Esta combinación de especialistas en inteligencia artificial y seguridad cibernética es la configuración más eficiente y precisa que podemos crear para trabajar con los datos de eventos que recibimos. Y nos permite detectar ataques antes de que tengan la oportunidad de dañar o acceder a datos críticos para el negocio.

RESUMEN

Esperamos que este documento le haya dado una idea de cómo vemos el panorama de amenazas hoy. Como lo vemos, estas viñetas resumen bastante la situación:

- La mayoría de las organizaciones simplemente no saben si han sido violadas o no.
- Las defensas estáticas se consideran exitosas al 100% contra los atacantes.
- Los atacantes son demasiado cautelosos al ser atrapados.
- Construir buenas capacidades de detección y respuesta de violaciones es difícil.
- Red-teaming es la única manera de probar adecuadamente sus defensas.

Lo que hemos visto en los últimos años refleja una nueva realidad. Y en este momento, construir capacidades de detección y respuesta es una tarea compleja que involucra muchos componentes separados y partes móviles. Y mucho trabajo manual.

Esperamos que en el futuro, los componentes y las tecnologías se unan para crear sistemas automáticos autoadaptativos que puedan aprender de cualquier estímulo nuevo que encuentren. Dichos sistemas ejecutarán automáticamente el descubrimiento de redes, la evaluación de vulnerabilidades y la aplicación de parches, y realizarán actividades de respuesta y remediación posteriores a la violación. Cuando se descubren TTP de intrusión o posteriores a la infracción, estos sistemas se reconfigurarán automáticamente para evitar que ese mecanismo se utilice en el futuro.

En el caso de una infracción, los sistemas afectados, las cuentas y los controles de acceso serán remediados automáticamente.
Por ahora, sin embargo, si le preocupa si lo están pirateando (y creemos que probablemente debería hacerlo), le recomendamos encarecidamente que hable con nosotros o con uno de nuestros proveedores de servicios certificados sobre la detección y respuesta de F-Secure servicios. Porque creemos que una solución administrada es el camino a seguir.
Y he aquí por qué:

- Tendrá todas las capacidades de detección y respuesta en funcionamiento a los pocos días de iniciar la implementación.
- No es necesario que hagas tus propios expertos en seguridad cibernética, construyes tus propios sistemas o ejecutes tus propias operaciones de respuesta, eso lo tenemos cubierto.
- Después de detectar cualquier incidente real en su red, comuníquese con nosotros.

Si está interesado en leer más, tenemos una serie de libros electrónicos en tres partes que aborda las consecuencias de una infracción con más detalle, cómo las empresas están construyendo sus propias capacidades de detección y respuesta, y nuestros consejos. en hacer esto ustedes mismos. También tenemos numerosas publicaciones de blog sobre temas que incluyen delitos cibernéticos, detección y respuesta, y detalles sobre las tecnologías y los procesos que utiliza F-Se-cure. Todo esto se puede encontrar a través del sitio web de F-Secure.