Telefónica

Del hacking a la delincuencia informática actual

Marta Villén Sotomayor
Directora de Seguridad Lógica y Prevención del Fraude en la Red

1. Evolución del Hacking

Nada queda de los ataques tradicionales a los equipos informáticos y a los activos de información de las grandes organizaciones gubernamentales y de las empresas ejecutados por adolescentes solo como reto intelectual.

La mayor diferencia de la delincuencia informática actual y los ataques tradicionales de los primeros hackers es la intencionalidad que hay detrás de dichos ataques. El objetivo actual es obtener datos valiosos sobre una organización gubernamental, los ciudadanos las empresa y sus clientes, para después utilizarlos para obtener un beneficio económico.

En el pasado los atacantes buscaban la notoriedad que proporciona el ser el primero en conseguir un ataque exitoso, mientras que los ataques de la delincuencia actual están específicamente diseñados para evitar su detección ejecutándolo de una forma sigilosa y los actores buscan el beneficio económico en lugar de la fama.

El cambio en la intención de los grupos delictivos frente a los anteriores hackers requiere que los actores que se dedican a la lucha contra esta delincuencia se adapten a este cambio.

La proliferación de información valiosa transmitida, almacenada o procesada en línea y el incremento de las transacciones económicas del comercio electrónico ha despertado el interés de los grupos criminales que quieren aprovechar esta oportunidad para obtener beneficios económicos.

La amenaza del cibercrimen es particularmente preocupante en la actualidad, pues los grupos criminales se están volviendo cada vez mejor organizados y más expertos

Durante la pasada década, el crimen organizado ha comprendido las oportunidades que ofrece la sociedad de la información, las nuevas tecnologías y la red de redes (Internet); la explotación de un mercado online mediante el comercio electrónico , posibilidad de operar globalmente sin existir fronteras y una capacidad de persecución limitada dada la apariencia de anonimato que crea una sensación de impunidad.

El cibercrimen es el tipo de crimen con mayor tasa de crecimiento, y el Tesoro de los EEUU ya consideraba en 2006 que había rebasado en beneficios a la venta ilegal de drogas. Así pues, en 2009 creció en un 345% el número de enlaces a sitios web con contenido malicioso según refleja el último informe sobre seguridad -IBM X-Force ® 2009 Trend and Risk Report- que elabora anualmente el equipo de investigación y desarrollo de IBM Internet Security Systems (NYSE:IBM).

La delincuencia informática es percibida por las empresas como uno de los riesgos emergentes más preocupantes y con mayor impacto que el crimen convencional. La pérdida de beneficios, las horas del personal perdidas en la gestión de los ataques de seguridad en las tecnologías de la información y los daños de reputación e imagen están considerados como problemas más importantes que los ocasionados por el crimen convencional.

Los impactos en el negocio incluyen además de las perdidas económicas directas, las derivadas del lucro cesante por cierres temporales de las operaciones para limitar los efectos de un ataque y el intangible derivado del impacto en la reputación e imagen por el incremento de la publicidad negativa en los medios.

Para la sociedad los ataques contra las infraestructuras criticas tanto energéticas, sanitarias, transportes, telecomunicaciones etc son objetivos estratégicos capaces de afectar a un porcentaje altísimo de la población e impedir el suministro de los servicios esenciales.

Además, los delitos informáticos están generando grandes beneficios económicos para los implicados. Y en el futuro es muy posible que las organizaciones sufran un mayor impacto en su negocio según los grupos delictivos se van haciendo más ambiciosos y expertos.

2. Delincuencia informática actual

Los ataques informáticos son cada vez más sofisticados, por tratarse de un tipo de amenazas que están bien gestionadas y orquestadas por diferentes grupos delictivos que utilizan una red de actores operando en diferentes regiones del mundo y están muy poco conectado.

El otro gran cambio que se ha producido es que el delito es cometido por partes mediante una división y especialización de las actividades que son ejecutadas por fases y la suma de las fases es la que produce el delito completo, los actores de cada una de las partes no se conocen entre si y solo tienen en común el reparto del dinero que se produce por adelantado.

En lugar de ser ejecutados por un solo individuo, por una asociación o grupo organizado, los ataques se trocean y se encargan a diferentes actores en muchos casos sin ningún nexo de unión, que están especializados y sacan partido únicamente de su participación en cada una de las fases en que se divide el ataque.

Los ataques delictivos actuales se trocean y son delegadas a diferentes "actores" (individuos que se especializan en ejecutar un conjunto específico de acciones) a menudo en diferentes partes del mundo, y sacan partido únicamente de su participación. Esto crea un proceso descentralizado y muy poco conectado.

Cada una de las cinco fases clave en las que se dividen estos ataques son:

1. *Reconocimiento* – Investigar los posibles objetivos del ataque.
2. *Desarrollo* – Construir el o los ataques que tendrán mayor probabilidad de éxito.
3. *Extracción* – Ejecutar el ataque contra el objetivo y extraer los datos.
4. *Explotación* – Utilizar productos o servicios de cibercrimen para realizar actos delictivos.
5. *Blanqueo (Lavado)* – Esconder el origen del dinero, moviéndolo por una red compleja de cuentas bancarias.

Parte de los beneficios económicos de cada fase de un ataque rentable puede utilizarse para desarrollar métodos de ataque más sofisticados (p.ej. virus y troyanos polimórficos y disimulados, kits automáticos de ataque), para infiltrar un mayor número de "durmientes" en organizaciones haciéndose pasar por empleados honestos, o para involucrar a las comunidades de "hackers" para que identifiquen objetivos de alto valor a atacar.

2.1. Reconocimiento

El objetivo de la *fase inicial de Reconocimiento* es llevar a cabo investigaciones que ayudan a los delincuentes a identificar posibles objetivos a atacar

Cualquier delito informático comienza con una investigación preliminar para identificar a las organizaciones gubernamentales o empresariales y/o a los individuos que ofrecen la mejor oportunidad para poder ser atacados y extraer de ellos datos valiosos.

Mediante un proceso de rastreo y de eliminación, los "exploradores" y/o "durmientes" empiezan por identificar los posibles objetivos que tienen datos valiosos y, a continuación, determinan la probabilidad de ejecutar un ataque con éxito evaluando las vulnerabilidades o debilidades de seguridad del objetivo.

El objetivo preferente para los delincuentes informáticos son aquellas instituciones que publican detalles de los sistemas operativos, tienen puertos y servicios abiertos en sus maquinas y presentan vulnerabilidades conocidas y explotables, además de aquellas con un bajo grado de concienciación de seguridad del personal y que además publican los nombres de empleados.

Las técnicas utilizadas en esta fase es el escaneo de IPs, interceptación de tráfico en claro, detección de vulnerabilidades de seguridad para explotar con los exploits o suplantación de un empleado para acceder a un edificio o a un sistema.

2.2. Desarrollo

El objetivo de la *fase de Desarrollo* consiste en construir kits de ataque que tengan alta probabilidad de éxito.

El conocimiento del objetivo obtenido en la fase de Reconocimiento permite a los desarrolladores de malware diseñar el ataque para que pueda tener una alta probabilidad de éxito.

Esta fase se suele llevar a cabo por las comunidades de hacking de Internet y creadores de malware.

Los desarrolladores de malware más expertos normalmente comprobaran el ataque en un entorno "estéril" para verificar su efectividad. Cuando una vez probado se considere que ha pasado las pruebas y esta listo para la distribución, el desarrollador venderá por Internet el kit de ataque y en muchos casos los compradores pueden probar y tienen garantías del producto en cuanto al buen funcionamiento y su capacidad de ocultación "garantía de no detección"..

Algunos métodos de llevar a cabo ataques informáticos no hacen uso de kits de ataque que tengan que ser desarrollados, en los casos de ataques por ingeniería social, divulgación de la información por cómplices introducidos con función de topo, revisión de basura. En este caso la fase de Desarrollo no es muy importante y solo se limita a planificar la siguiente fase de Extracción.

Los kits de ataque más sofisticados se pueden comprar online sin necesidad de estar introducido ni conocer las comunidades de hackers y operarlos con escasos conocimientos técnicos.

2.3. Extracción

El objetivo de la *fase de Extracción* es ejecutar el ataque contra el objetivo y extraer los datos relevantes.

La extracción implica la ejecución del ataque para obtener los datos valiosos de la organización objetivo (p.ej. detalles personales de una agencia de pasaportes, detalles de tarjetas de crédito de un banco, detalles sobre nuevas medicinas de una compañía farmacéutica).

El objetivo preferente para los delincuentes informáticos son identificadores oficiales como números de seguridad social o de documentos nacionales de identidad, detalles de tarjetas de crédito y números PIN, información de clientes, direcciones de correo electrónico, contraseñas, información de patentes, información sobre cuentas bancarias, y nombres de empleados, grado de concienciación de seguridad del personal

El lanzamiento de un ataque se ejecuta por un actor denominado comúnmente como "minero", a menudo desde una región del mundo con leyes laxas para la lucha contra las actividades del cibercrimen. Una vez "cosechados", los datos se anuncian y venden por Internet.

Cuando el ataque persigue una denegación de servicio que consiste en interrumpir servicios de negocio a cambio de un rescate, en vez de extraer los datos en estos casos, los actores involucrados en esta fase obtienen el beneficio de proporcionar los medios para ejecutar este tipo de ataque como por ejemplo alquilar "botnets" constituidos por un conjunto de ordenadores zombies dispuestos a ejecutar las ordenes de ataque.

Normalmente los actores de esta fase se dedican a anunciar y vender los datos robados (en el mercado negro).

El rango de precios de los servicios de extracción o los "entregables" varían dependiendo de la oferta y la demanda en el mercado negro. La tabla adjunta muestra ejemplos de precios online para diferentes tipos de datos que pueden ser comprados a las comunidades de hackers.

Overall Rank 2009	Overall Rank 2008	Item	Percentage 2009	Percentage 2008	Range of Prices
1	1	Credit card information	19%	32%	$0.85–$30
2	2	Bank account credentials	19%	19%	$15–$850
3	3	Email accounts	7%	5%	$1–$20
4	4	Email addresses	7%	5%	$1.70/MB–$15/MB
5	9	Shell scripts	6%	3%	$2–$5
6	6	Full identities	5%	4%	$0.70–$20
7	13	Credit card dumps	5%	2%	$4–$150
8	7	Mailers	4%	3%	$4–$10
9	8	Cash-out services	4%	3%	$0–$600 plus 50%–60%
10	12	Website administration credentials	4%	3%	$2–$30

Fuente: SYMANTEC

2.4. Explotación

El objetivo de la *fase de Explotación* es utilizar los datos comprados en la fase de extracción para cometer otros crímenes financieros.

Los participantes en la fase de Explotación hacen uso de los frutos del trabajo de la fase de Extracción y dependiendo del tipo de datos extraído se usan bien para perpetrar el delitos financieros como fraude con tarjeta de crédito, fraude en solicitud de hipotecas, fraude en pagos en terminales puntos de venta (TPV), falsificación de efectos; o bien para otros tipos de actividad criminal como robo de identidad, extorsión o espionaje industrial.

Pero para enmascarar a los actores de esta fase se utilizan los actores de la siguiente fase que son los encargados de efectuar las transacciones económicas a su nombre.

2.5. Blanqueo (Lavado)

El objetivo de la *fase de Blanqueo (Lavado)* es ocultar la identidad, la fuente y/o el destino del dinero, típicamente moviéndolo a través de una compleja red de cuentas bancarias

La fase final de los ataques rentables implica la transferencia por parte de los grupos criminales del dinero obtenido de la venta de los datos, y/o los kits de ataque, a través de una compleja red de cuentas bancarias para evitar la detección del origen, destino y titulares de las cuentas.

A los actores involucrados en esta fase denominados la "mula" o el "blanqueador" se les retribuye por permitir el uso de sus cuentas bancarias para recibir y posteriormente transferir el dinero a la dirección del grupo criminal.

A la mula o blanqueador se le contrata a través de anuncios de ofertas de trabajo en Internet y normalmente no conocen la identidad de quien les contrata.