KASPERSKY lab

Boletín de seguridad Kaspersky 2018

LA HISTORIA DEL AÑO: EL MALWARE DE CRIPTOMINERÍA

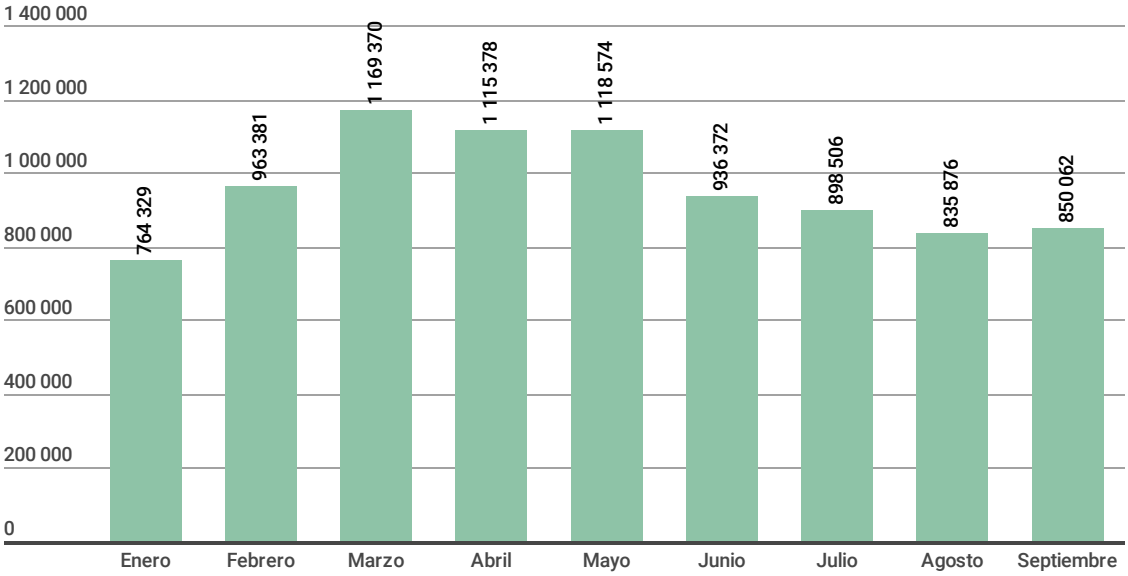
CONTENTS

El malware de criptominería que infecta los equipos de los desprevenidos usuarios funciona con el mismo modelo de negocios que los programas de ransomware: la potencia de procesamiento del equipo de la víctima se utiliza para enriquecer a los delincuentes. En el caso de los criptomineros, el usuario puede no darse cuenta durante mucho tiempo que el 70-80 % de la potencia del procesador central o gráfico de su equipo se utiliza para generar monedas virtuales. En cambio, los documentos cifrados y los mensajes de los extorsionadores son mucho más difíciles de ignorar.

Por lo general, el malware de criptominería se instala en los equipos de los usuarios y de las empresas junto con programas publicitarios, juegos hackeados y otro contenido pirateado. Al mismo tiempo, el "umbral de entrada" (el proceso de creación del criptominero en sí) es ahora bastante bajo: los atacantes cuentan con la ayuda de programas de afiliados, grupos de minería abiertos y constructores de mineros listos para usar. Además, existe otro método para el robo de recursos informáticos, que consiste en incrustar en una página web un script de minería de datos, que se lanza cuando el usuario abre el sitio en su navegador. En un grupo aparte están los delincuentes que no tienen como objetivo los equipos privados, sino los servidores de grandes compañías, cuya infección es un proceso que requiere más trabajo.

TENDENCIAS

2018 comenzó con un aumento en el número de ataques relacionados con los mineros. Sin embargo, después de la caída del precio de las principales criptomonedas, que tuvo lugar de enero a febrero, se pudo observar que las infecciones tendían a disminuir, proceso que iba a la par con la pérdida general de interés en las criptomonedas. No obstante, en el gráfico de abajo es patente que, aunque el número de ataques de criptomineros ha disminuido, la amenaza que representan sigue siendo relevante. El tiempo dirá en cuánto disminuirá el número de infecciones después del colapso de la tasa de Bitcoin ocurrido en noviembre.



Número de usuarios únicos atacados por malware de minería, del primer al tercer trimestre de 2018

El software de minería clandestino fue muy popular entre los propietarios de botnets, como lo confirman las estadísticas de archivos descargados por botnets: el auge de los criptomineros tuvo lugar el primer trimestre de 2018, y la proporción de este malware en la primera mitad del año fue del 4,6 % del total de archivos descargados por botnets. En comparación, el segundo semestre de 2017 esta cifra estaba por debajo del tres por ciento (2,9 %). De esto se deduce que ahora los atacantes son más propensos a considerar las botnets como un medio de difusión de software para extraer criptomonedas.

	Segundo semestre de 2017		Primer trimestre de 2017	
1	Lethic	17.0%	njRAT	5.2%
2	Neutrino.POS	4.6%	Lethic	5.0%
3	njRAT	3.7%	Khalesi	4.9%
4	Emotet	3.5%	Malware de criptominería	4.6%
5	Malware de criptominería	2.9%	Neutrino.POS	2.2%
6	Smoke	1.8%	Edur	1.3%
7	Cutwail	0.7%	PassView	1.3%
8	Extorsionistas	0.7%	Jimmy	1.1%
9	SpyEye	0.5%	Gandcrab	1.1%
10	Snojan	0.3%	Cutwail	1.1%

Amenazas más descargadas, segundo semestre de 2017 – primer trimestre de 2018

Continuando con el tema de las botnets, es imposible no mencionar que en el tercer trimestre de 2018, registramos una disminución en el número de ataques DDoS y, según nuestros expertos, lo más probable es que se deba a la "conversión" de la potencia de las botnets, que pasó de los ataques DDoS a la minería de criptomonedas. Esto no solo se vio influenciado por la alta popularidad de éstas últimas, sino también por la alta competencia en el "mercado de DDoS". Esto llevó a que los ataques sean más baratos para los clientes, pero no para los dueños de botnets, sobre cuyos hombros todavía pesan muchos "aspectos organizacionales" no muy lícitos.

La minería se diferencia favorablemente en que, con ciertos enfoques en su organización, puede ser imperceptible para el propietario del equipo infectado y, por lo tanto, las posibilidades de que el atacante tenga que vérselas con la policía cibernética son mucho menores. Y la conversión de la potencia de servidor disponible hace que su propietario sea invisible a las agencias policiales. Hay evidencias indirectas de que los propietarios de muchas botnets famosas cambiaron su vector de actividades, pasándose a la minería. Por ejemplo, las actividades DDoS de la exitosa botnet Yoyo han disminuido mucho, aunque no contamos con información que confirme su desaparición.

Además, la minería comenzó a acaparar tanta (o más) atención que los cifradores: este año conocimos varios ejemplos de malware reprocesado que ahora posee funciones adicionales de extracción de criptomonedas. Y las técnicas utilizadas por los autores de los mineros también se están haciendo cada vez más sofisticadas.

Así, en julio de este año apareció en nuestro campo de visión una implementación interesante del minero, que llamamos PowerGhost. Este software malicioso sabe afianzarse en el sistema y propagarse en grandes redes corporativas, infectando tanto las estaciones de trabajo como los servidores. Para que el usuario y las soluciones de protección no se den cuenta de su presencia durante el mayor tiempo posible, el criptominero utiliza muchas técnicas que no suponen el uso de archivos. La infección se produce a distancia mediante exploits o herramientas de administración remota (Windows Management Instrumentation). Durante la infección, se inicia un script powershell de una sola línea que descarga el cuerpo principal del malware y lo lanza inmediatamente, sin escribirlo en el disco duro.

Otro ejemplo de reconversión es el troyano extorsionador Trojan-Ransom.Win32.Rakhni, cuyas primeras muestras fueron descubiertas por Kaspersky Lab en 2013. Sus funciones de minería son una novedad introducida en 2018. La decisión de usarlas depende de la presencia de la carpeta %AppData %\Bitcoin en la máquina infectada. Si existe, el gestor de arranque descarga la herramienta de cifrado. Si la carpeta no existe y el equipo tiene más de dos procesadores lógicos, se descarga un criptominero. Para que el malware permanezca desapercibido en el sistema, los desarrolladores hicieron que se parezca a los productos de Adobe. Esto se refleja en el icono y el nombre del archivo ejecutable, así como en una firma digital falsa, que utiliza el nombre de la compañía Adobe Systems Incorporated.

PBot, que antes era un programa exclusivamente publicitario, aprendió a instalar utilidades de extracción de criptomonedas en los equipos. Este malware se propaga a través de sitios de afiliados que inyectan scripts en sus páginas, los que a su vez remiten al usuario a los enlaces patrocinados. Un esquema de distribución típico es el siguiente:

1. El usuario visita uno de los sitios de la red de afiliados;
2. Al hacer clic en cualquier lugar de la página, aparece una nueva ventana del navegador en la que se abre el enlace intermedio;
3. El enlace envía al usuario a la página de descarga de PBot, cuya tarea es engañar al usuario para inducirlo a descargar e iniciar el malware.

La moneda más común entre todas las criptomonedas extraídas ilegalmente es monero (xmr). Esto se debe a que su algoritmo presupone el anonimato, su precio es relativamente alto en el mercado y es fácil de vender, ya que es aceptado por la mayoría de las grandes bolsas de intercambio de criptomonedas. Para una red de bots que extrae esta moneda ilegalmente, es importante poder extraerla utilizando la CPU. Según algunas fuentes, cerca del 5 % de la extracción total de criptomonedas, por un valor de 175 millones de dólares, se extrajo de forma ilegal.

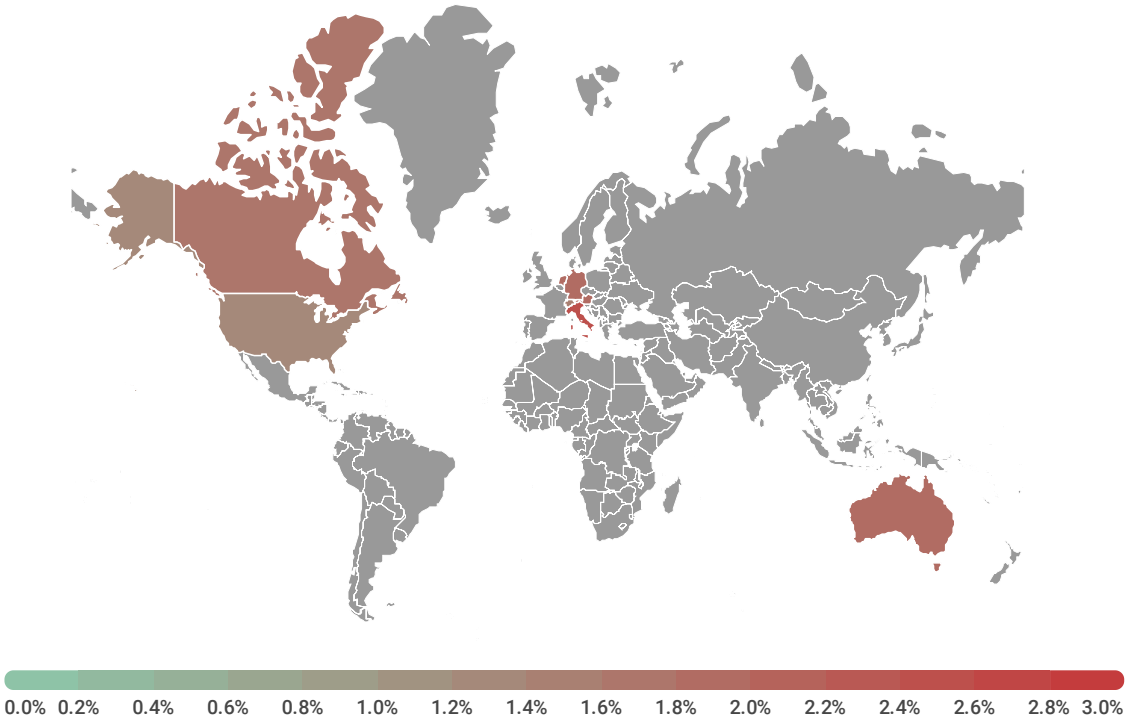
FACTORES QUE AFECTAN LA DISTRIBUCIÓN DE LOS CRIPTOMINEROS

The conclusion based on data we obtained from various sources is that legislative control over cryptocurrencies has little impact on the spread of hidden mining. For example, in Algeria and Vietnam cryptocurrencies are either prohibited or severely restricted under domestic law. Yet Vietnam is third in the ranking of leading countries by number of miner attacks, and Algeria is sixth. Meanwhile, Iran, which is presently drafting legislation to govern cryptocurrency and developing plans to issue its own "coins," is in seventh place.

País	Estado de las criptomonedas	% de ataques
Kazajistán	Ni prohibidas, ni legalizadas.	16,5 %
Vietnam	Prohíbida su emisión (minería)	13,00 %
Indonesia	Reconocida como producto básico	12,87 %
Ucrania	Circulación regida por la ley	11,19 %
Rusia	Se está considerando legislarlas	10,71 %
Argelia	Prohibidas	9,03 %
Irán	Está preparando el reglamento legislativo, tiene previsto crear su propia criptomoneda	7,21 %
India	Piensa prohibirlas, se están discutiendo en audiencias	7,20 %
Tailandia	Circulación regida por la ley	6,76 %
Taiwán	No están prohibidas	5,81 %

Top 10 de países con la mayor proporción de ataques de criptomineros, enero a octubre de 2018 (solo se incluyen los países con más de 500 000 clientes de Kaspersky Lab)

En comparación, los usuarios de EE. UU. fueron los menos afectados por los criptomineros, con un 1,33 % del total de ataques. En Suiza solo el 1,56 % de los usuarios se toparon con este tipo de malware. Inglaterra, donde los ataques representaron el 1,66 %, ocupa el tercer puesto.



Mapa de países con la menor proporción de ataques de criptomineros, enero a octubre de 2018 (solo se incluyen los países con más de 500 000 clientes de Kaspersky Lab)

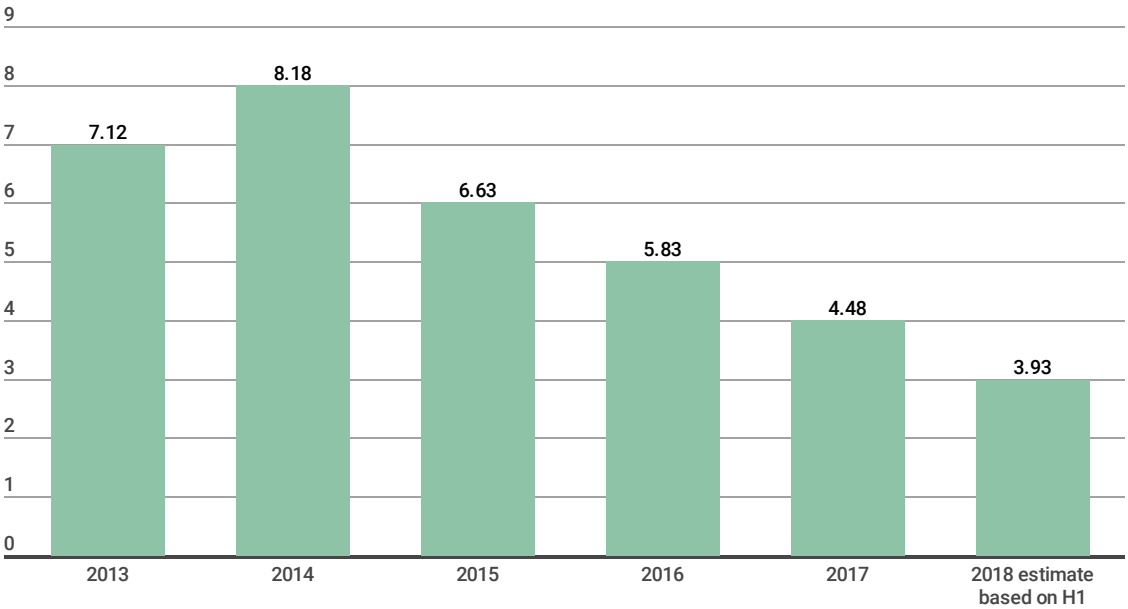
La difusión de los criptomineros no se ve afectada por el costo de la electricidad, que varía mucho de un país a otro. Además, este factor carece de importancia para un delincuente que explota los recursos de otras personas.

MODOS DE DIFUSIÓN

Si damos un vistazo al nivel de propagación del software pirateado en los países con la mayor cantidad de ataques de mineros, podemos notar una clara correlación: cuanto más software sin licencia se distribuye, mayor es el número de criptomineros. Esto lo confirman nuestras estadísticas, que muestran que la mayoría de las veces los criptomineros llegan a los equipos de las víctimas junto con software pirateado.

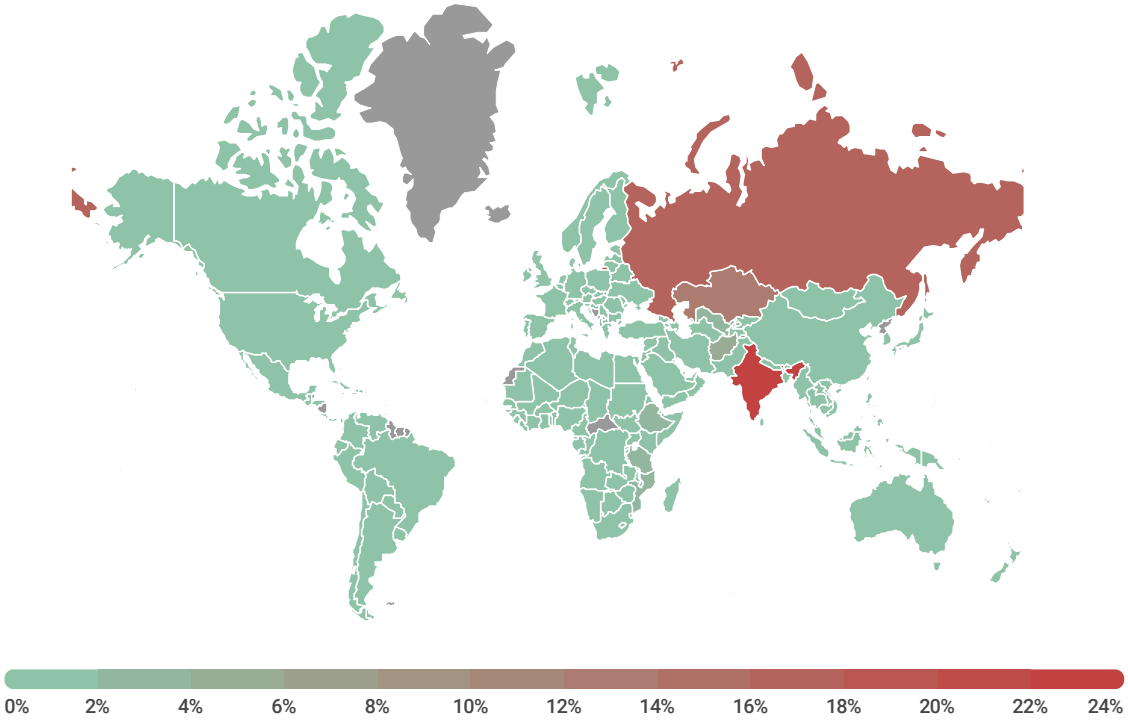
Otro vector de la penetración de criptomineros en las computadoras son los instaladores de adware que se distribuyen por medio de ingeniería social. Las opciones más sofisticadas, como la propagación a través de vulnerabilidades como EternalBlue, tienen como blanco la potencia de servidores y son menos comunes.

Además, no hay que olvidar que las unidades USB se vienen utilizando para distribuir software de criptominería desde al menos 2015. El porcentaje de detecciones del popular minero de Bitcoin Trojan.Win64.Miner.all en dispositivos extraíbles crece cada año en aproximadamente 1/6. En 2018, uno de cada diez usuarios afectados por malware propagado a través de "unidades flash" fue víctima de este minero (aproximadamente el 9,22 %). En comparación, en 2017 esta cifra fue del 6,7 % y en 2016, del 4,2 %.



Número de usuarios únicos (en millones) en cuyos equipos se encontró malware en los directorios raíz, que es el principal signo de infección a través de medios extraíbles, 2013-2018. Fuente: KSN.

Trojan.Win32.Miner.ays/Trojan.Win.64.Miner.all se detectó en India (23,7 %), Rusia (18,45 %) y Kazajstán (14,38 %), pero algunos casos aislados también se registraron en países de Asia y África, en Europa (en el Reino Unido, Alemania, los Países Bajos, Suiza, España, Bélgica, Austria, Italia, Dinamarca y Suecia), Estados Unidos, Canadá y Japón.



Porcentaje de usuarios afectados por los mineros de bitcoin en medios extraíbles, 2018.
Fuente: KSN (solo se incluyen los países con más de 10 000 clientes de Kaspersky Lab)

CONCLUSIÓN

Si resumimos los resultados del año pasado, podemos destacar las siguientes tesis:

1. La creciente popularidad y el precio de las criptomonedas han convencido a los ciberdelincuentes de la necesidad de invertir recursos en el desarrollo de nuevas técnicas para los criptomineros que, según nuestros datos, están reemplazando gradualmente a los troyanos extorsionadores.
2. Las actividades de la criptominería clandestina disminuyen en los periodos de caída de precios de las criptomonedas.
3. La expansión de la criptominería clandestina no se ve afectada por factores como la regulación legislativa de las criptomonedas o el costo de la electricidad en la región.
4. A menudo, los mineros entran en las computadoras de las víctimas cuando descargan contenido sin licencia o instalan software pirateado. En consecuencia, este tipo de amenaza es más frecuente en los países que tienen un bajo nivel de regulación del mercado de software sin licencia y donde la educación digital general de los usuarios es insuficiente.