KASPERSKY lab

Kaspersky boletín de seguridad 2018

ESTADÍSTICAS

CONTENIDO

Todos los datos estadísticos utilizados en este informe se obtuvieron utilizando la red de nube global Kaspersky Security Network (KSN), que recibe información enviada por varios de los componentes de nuestras soluciones de seguridad. Los datos provienen de los usuarios que dieron su consentimiento para transferir esta información a KSN. Millones de usuarios de productos Kaspersky Lab de 213 países y territorios de todo el mundo participan en el intercambio global de información sobre actividades maliciosas. Las estadísticas 2018 abarcan el período comprendido entre noviembre de 2017 y octubre de 2018.

CIFRAS DEL AÑO

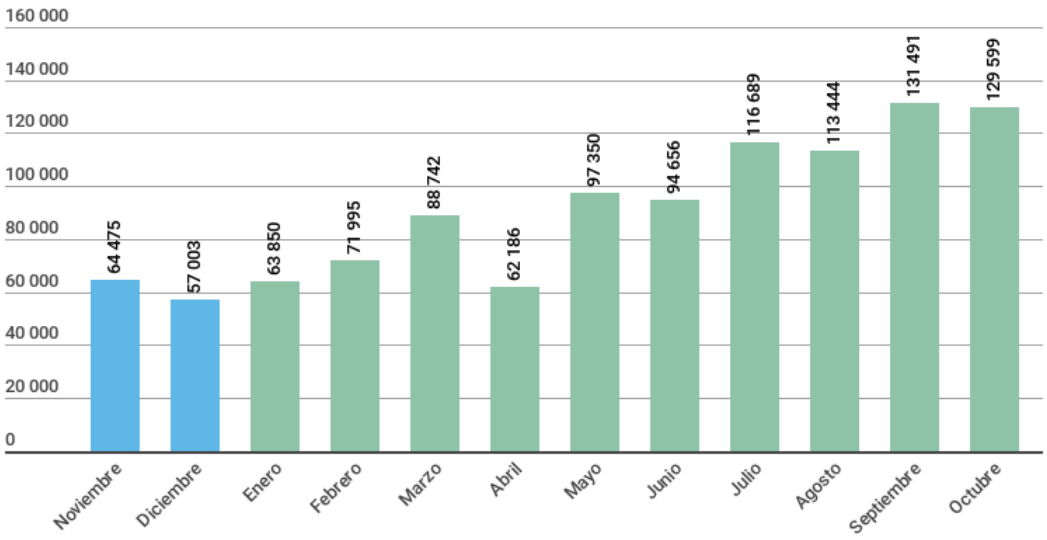
- Durante el año, el 30,01% de los equipos de los usuarios de Internet en el mundo sufrieron al menos una vez un ataque web de la **clase Malware**.
- Las soluciones de Kaspersky Lab neutralizaron **1 876 998 691** ataques lanzados desde recursos de Internet ubicados en diversos países del mundo.
- Se registraron **554 159 621** URL únicas que provocaron respuestas del antivirus web.
- Nuestro antivirus web registró **21 643 946** objetos maliciosos únicos.
- Se neutralizaron ataques de cifradores en los equipos de **765 538** usuarios únicos.
- Durante el período abarcado por este informe, los criptomineros atacaron a **5 638 828** usuarios únicos.
- En los equipos de **830 135** usuarios se neutralizaron intentos de ejecución de programas maliciosos diseñados para robar dinero mediante el acceso en línea a cuentas bancarias.

MALWARE BANCARIO

Las estadísticas presentadas no solo incluyen datos sobre amenazas bancarias, sino también sobre malware para cajeros automáticos y terminales de pago. Las estadísticas de las amenazas móviles similares se presentan en un informe aparte.

Número de usuarios atacados por malware bancario

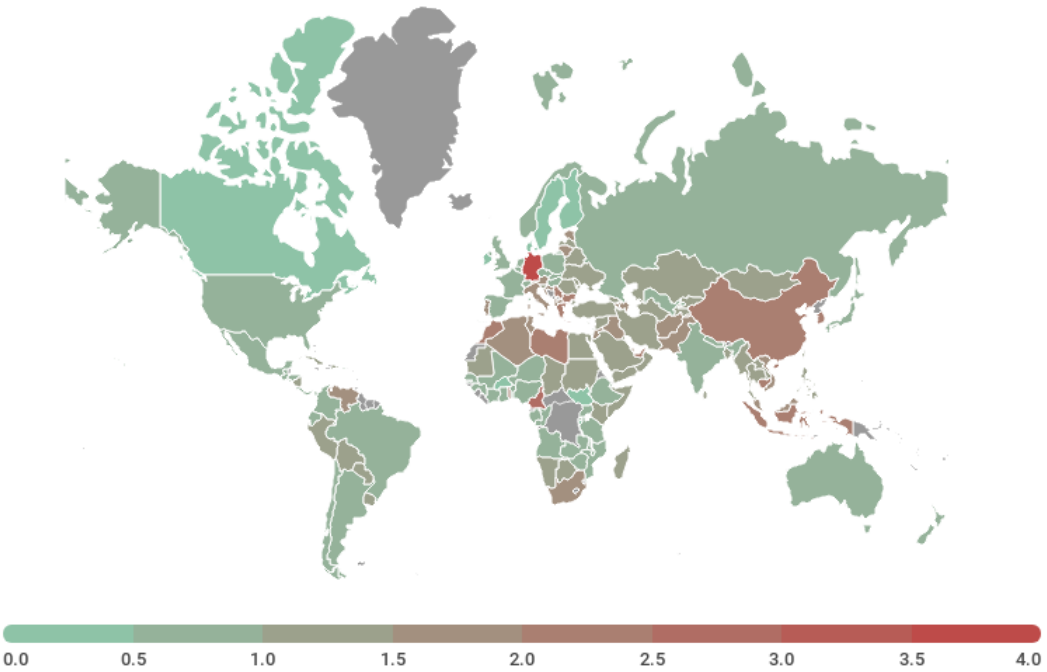
En 2018, las soluciones de Kaspersky Lab neutralizaron intentos de lanzar uno o más programas maliciosos diseñados para robar dinero de cuentas bancarias en los equipos de **830 135** usuarios.



Número de usuarios atacados por malware financiero, noviembre de 2017 – octubre de 2018

Geografía de los ataques

Para evaluar y comparar el riesgo de infección por malware bancario al que están expuestos los equipos de los usuarios en diferentes países del mundo, hemos calculado para cada país el porcentaje de usuarios de productos de Kaspersky Lab que se vieron afectados por esta amenaza durante el trimestre, del total de usuarios de nuestros productos en ese país.



Geografía de los ataques de malware bancario, noviembre de 2017 – octubre de 2018

TOP 10 de países según el porcentaje de usuarios atacados

	País*	%**
1	Alemania	4,0
2	Camerún	2,6
3	Corea del Sur	2,4
4	Maldivas	2,4
5	República de Togo	2,3
6	Indonesia	2,2
7	Libia	2,2
8	Emiratos Árabes Unidos	2,1
9	Grecia	2,1
10	China	2,0

** En los cálculos hemos excluido a los países en los que la cantidad de usuarios de Kaspersky Lab es relativamente baja (menos de 10 000).*

*** Proporción de usuarios únicos cuyos equipos fueron atacadas por malware bancario, del total de usuarios atacados por todos los tipos de malware.*

TOP 10 de familias de malware bancario

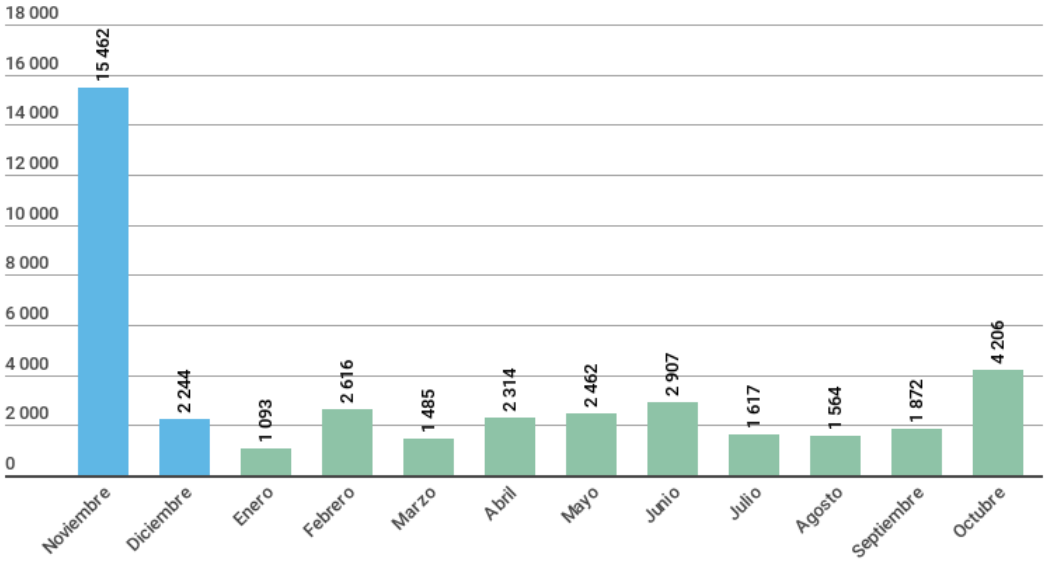
10 TOP de familias de malware utilizado para atacar a los clientes de banca en línea en 2018:

	Nombre	%*
1	Trojan.Win32.Zbot	26,3
2	Trojan.Win32.Nymaim	19,8
3	Backdoor.Win32.SpyEye	14,7
4	Backdoor.Win32.Caphaw	5,2
5	Trojan-Banker.Win32.RTM	5,2
6	Backdoor.Win32.Emotet	4,9
7	Trojan.Win32. Neurevt	3,9
8	Trojan-Banker.Win32.Tinba	1,9
9	Trojan.Win32.Gozi	1,8
10	Trojan-Banker.Win32.Trickster	1,5

** Porcentaje de usuarios atacados por este programa malicioso, del total de los usuarios atacados por malware bancario.*

PROGRAMAS CIFRADORES MALICIOSOS

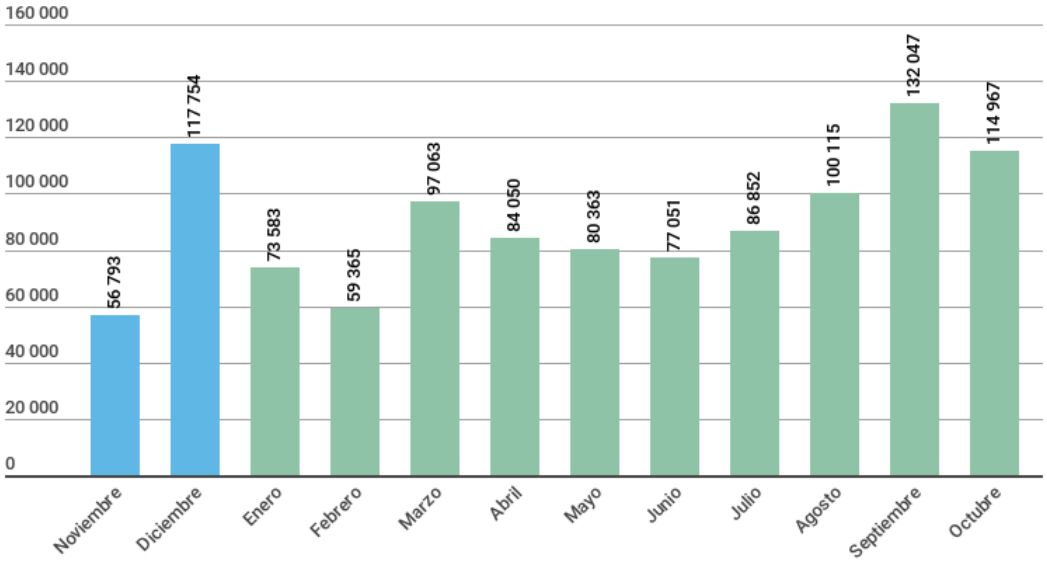
En 2018, identificamos más de **39 842** modificaciones de cifradores y descubrimos **11** nuevas familias. Cabe destacar que no creamos una nueva familia para cada nuevo cifrador. Por el contrario, a la mayoría de las amenazas de este tipo les asignamos el veredicto genérico que utilizamos cuando detectamos ejemplares nuevos y desconocidos.



Número de nuevas modificaciones cifradas, noviembre 2017 – octubre 2018

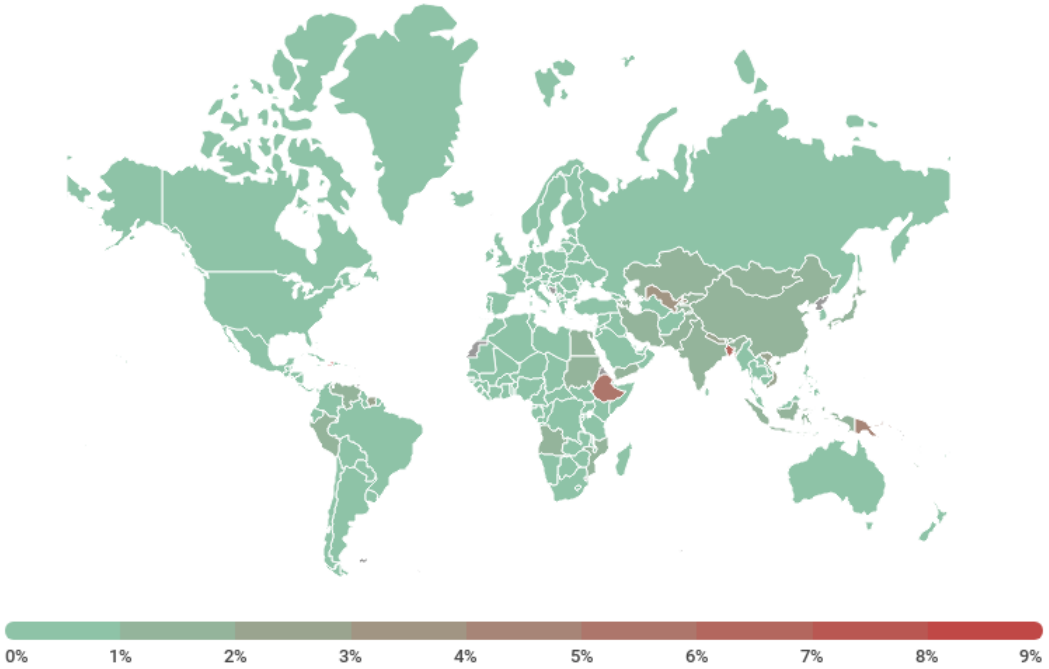
Número de usuarios atacados por troyanos cifradores

En 2018, los troyanos cifradores lanzaron ataques contra **765 538** usuarios únicos. Entre ellos había más de 220 mil usuarios corporativos y más de 27 mil empresas, entre pequeñas y medianas.



Número de usuarios atacados por troyanos cifradores, noviembre de 2017 – octubre de 2018

Geografía de los ataques



Geografía de los ataques lanzados por troyanos cifradores, noviembre de 2017 – octubre de 2018

TOP 10 de países afectados por ataques de troyanos cifradores

	País*	%**
1	Bangladesh	6,65
2	Etiopía	5,25
3	Uzbekistán	3,50
4	Nepal	2,79
5	Vietnam	2,12
6	Indonesia	1,95

	País*	%**
7	India	1,87
8	Angola	1,84
9	Pakistán	1,78
10	China	1,72

** Hemos excluido de los cálculos a los países donde el número de usuarios de Kaspersky Lab es relativamente baja (menos de 50 000).*

*** Porcentaje de usuarios únicos cuyos equipos fueron atacados por troyanos cifradores, de la cantidad total de usuarios de productos de Kaspersky Lab en el país.*

TOP 10 de las familias más difundidas de troyanos cifradores

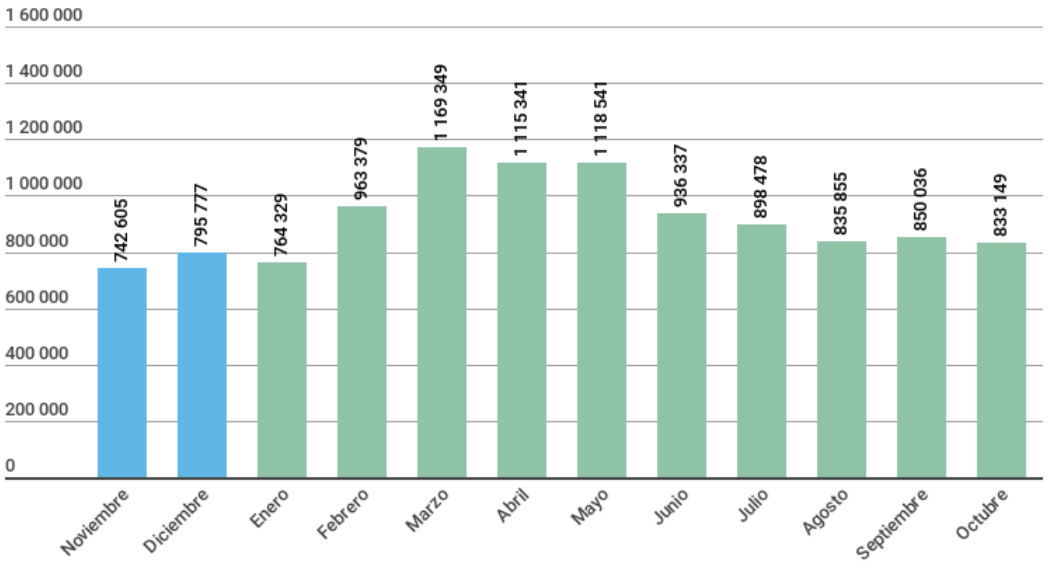
	Nombre	Veredicto	%*
1	WannaCry	Trojan-Ransom.Win32.Wanna	29,32
2	(veredicto genérico)	Trojan-Ransom.Win32.Phny	11,43
3	GandCrab	Trojan-Ransom.Win32.GandCrypt	6,67
4	Cryakl	Trojan-Ransom.Win32.Cryakl	4,59
5	PolyRansom/VirLock	Virus.Win32.PolyRansom	2,86
6	(veredicto genérico)	Trojan-Ransom.Win32.Gen	2,40
7	Shade	Trojan-Ransom.Win32.Shade	2,29
8	Cerber	Trojan-Ransom.Win32.Zerber	2,20
9	Purgen/GlobeImposter	Trojan-Ransom.Win32.Purgen	1,82
10	Crysis/Dharma	Trojan-Ransom.Win32.Crusis	1,72

** Porcentaje de usuarios únicos de Kaspersky Lab que sufrieron ataques de una familia específica de troyanos extorsionadores, del total de usuarios víctimas de ataques lanzados por troyanos extorsionadores.*

CRIPTOMINEROS

Número de usuarios atacados por criptomineros

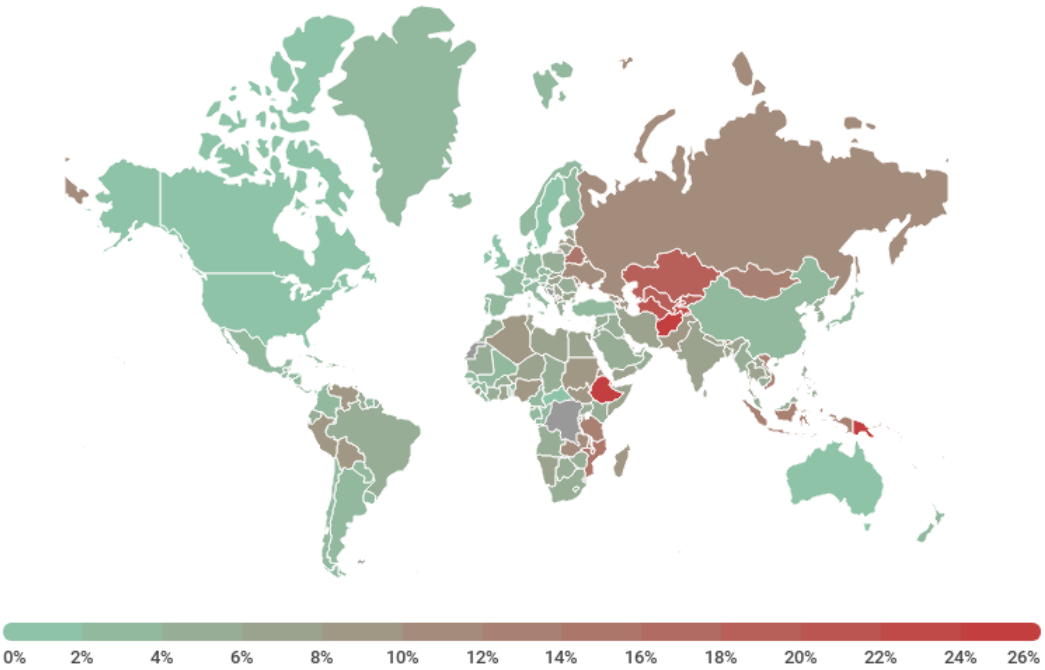
Durante el período cubierto por este informe, registramos intentos de instalar criptomineros en los equipos de **5 638 828** usuarios únicos. En el volumen total de ataques, la proporción de criptomineros fue del 8,50%, y entre todos los programas del tipo Risktool, del 16,88%.



Número de usuarios atacados por los criptomineros, noviembre de 2017 – octubre de 2018

La mayoría de las veces, los productos de Kaspersky Lab detectaron al malware Trojan.JS.Miner.m, que representó casi el 22% del total de usuarios atacados por los criptomineros. A una distancia significativa le siguen los representantes de la familia Trojan.Win32.Miner: Miner.gen (9,44%), Miner.ays (5,30%) y Miner.bbb (2,71%).

Geografía de los ataques



Geografía de los ataques lanzados con la participación de criptomineros, noviembre 2017 – octubre 2018

APLICACIONES VULNERABLES UTILIZADAS POR LOS CIBERDELINCUENTES DURANTE LOS ATAQUES CIBERNÉTICOS

El período cubierto por este informe se caracterizó por una gran cantidad de ataques selectivos que utilizaban exploits para vulnerabilidades de día cero. Detectamos:

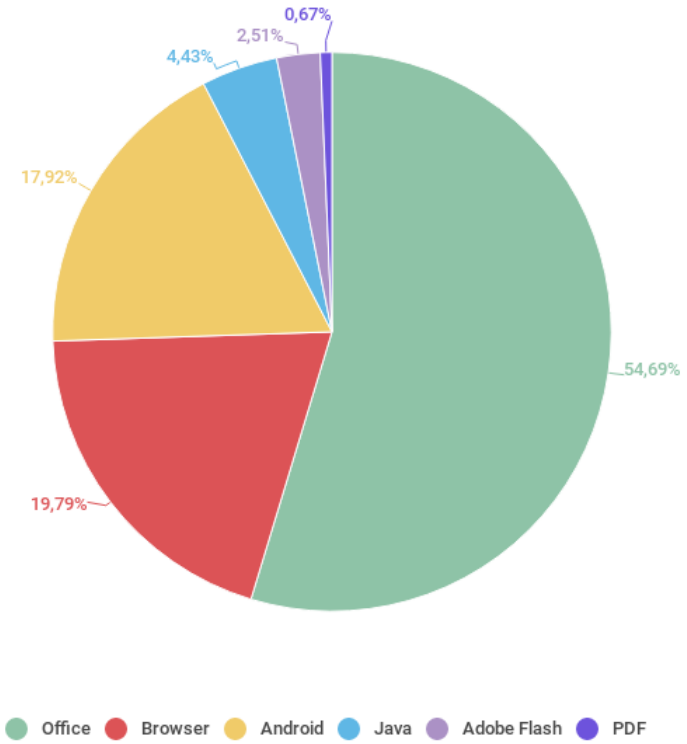
- Vulnerabilidades para Adobe Flash (software que está llegando al final de su ciclo vital) explotadas por los delincuentes (CVE-2018-4878, CVE-2018-5002);
- Una vulnerabilidad explotada de Acrobat Reader, la primera que vemos desde hace mucho tiempo (CVE-2018-4990);
- Vulnerabilidades de VBScript, uno de los motores de scripts de Windows (CVE-2018-8174, CVE-2018-8373), que se utiliza en el navegador Internet Explorer (entre otros);
- Varias vulnerabilidades en el controlador del subsistema de gráficos de Windows win32k.sys, que fueron utilizadas por delincuentes tanto para aumentar privilegios en el sistema operativo, como en conjunto con otras vulnerabilidades para eludir la "caja de arena" (CVE-2018-8120, CVE-2018-8453, CVE-2018 -8589).

Al igual que en el último año, la cantidad de usuarios atacados por exploits para vulnerabilidad de Adobe Flash Player e Internet Explorer ha disminuido, a pesar de que en ambos productos han aparecido varias nuevas vulnerabilidades de días cero explotadas públicamente. Por ejemplo, la vulnerabilidad CVE-2018-4878 de Adobe Flash Player, cuya prueba de concepto fue hecha pública por el investigador que la descubrió, se integró en muchos paquetes de exploits populares menos de dos meses después de la publicación del parche. Pero aún así, la participación de las plataformas mencionadas en las estadísticas anuales se ha reducido a menos de la mitad.

La participación de la plataforma Android en nuestro gráfico de distribución de exploits se redujo al 18 % (-9 puntos porcentuales en comparación con el año pasado), lo que nos lleva a la conclusión de que la seguridad del sistema operativo de Google está aumentando. En parte, el motivo fue la política más agresiva de actualización de dispositivos a las últimas versiones del sistema operativo. Por ejemplo, según los datos de octubre de 2018, el sistema operativo Android 8.0+ Oreo está instalado en los dispositivos del 22 % de los usuarios de Android. A modo de comparación, en octubre de 2017, se instaló la última versión de Android 7.0+ Nougat disponible en ese momento en solo el 16 % de los usuarios.

Al mismo tiempo, observamos un fuerte aumento en el número de usuarios atacados por exploits para vulnerabilidades de Microsoft Office, que se cuadruplicó en comparación con el promedio de 2017. Esto llevó a un aumento en la proporción de la suite Office en nuestras estadísticas, del 17,63% al 55 %, un porcentaje aparentemente increíble. La razón de este crecimiento fue el envío masivo de correos no deseados que propagan documentos con exploits para las vulnerabilidades CVE-2017-11882 y CVE-2018-0802. Estas vulnerabilidades han ganado popularidad entre los ciberdelincuentes debido a la estabilidad de su funcionamiento y facilidad de uso: es suficiente modificar el script del generador de exploits puesto a disposición del público. La posibilidad de utilizar ofuscaciones para que las soluciones de seguridad no las detecten y la amplia cobertura de varias versiones de Microsoft Office ha desempeñado un papel importante: sin el parche correspondiente, todas las versiones de la suite ofimática lanzadas en los últimos 18 años son vulnerables.

Los exploits para otras vulnerabilidades populares (CVE-2017-8570, CVE-2018-4878, CVE-2018-8174), distribuidas a través de documentos de MS Office, también jugaron un papel en el aumento de la participación de este paquete en nuestras estadísticas.



Distribución de exploits utilizados en los ataques lanzados por los delincuentes, por tipo de aplicaciones atacadas, noviembre de 2017 – octubre de 2018

El ranking de las aplicaciones vulnerables se basa en los veredictos asignados por los productos de Kaspersky Lab a los exploits bloqueados utilizados por los ciberdelincuentes tanto en ataques de red como en aplicaciones locales vulnerables, entre ellos los dispositivos móviles de los usuarios.

En 2018, no hubo incidentes como el del año pasado, cuando el grupo de hackers **Shadow Brokers** publicó el archivo **Lost In Translation**, que contenía una gran cantidad de exploits de red. Sin embargo, el número de archivos maliciosos que sacan provecho de los exploits de este archivo, así como el número de ataques que los utilizan, siguieron creciendo: en comparación con el año pasado, nuestro componente de detección de intrusos bloqueó muchos más intentos de explotación del exploit para SMS EternalBlue.

ATAQUES A TRAVÉS DE RECURSOS WEB

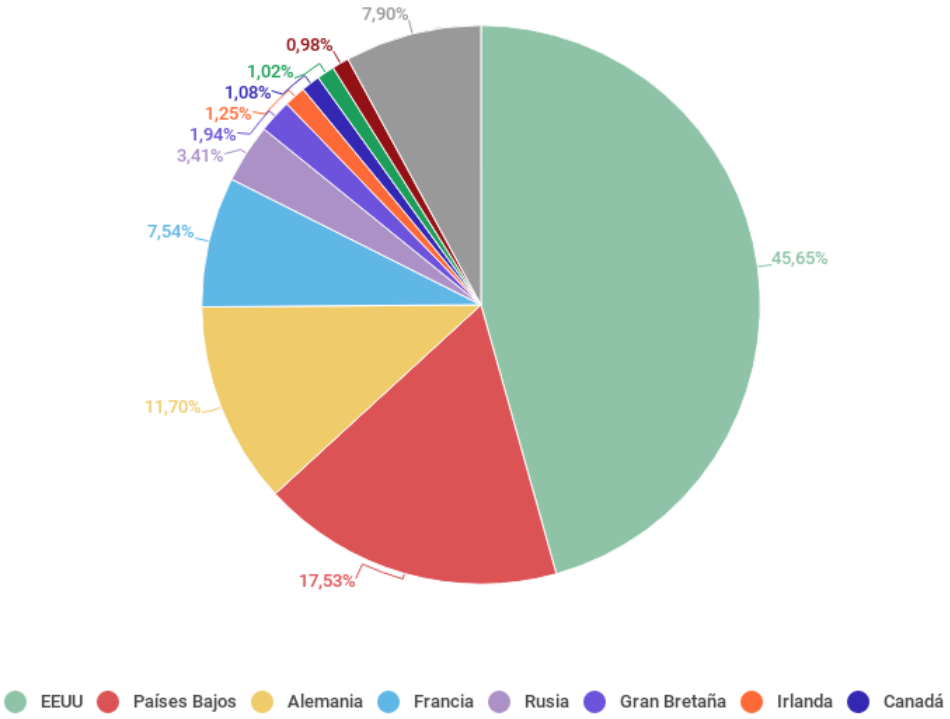
Los datos estadísticos de este capítulo han sido recopilados por el antivirus web, que impide que los usuarios descarguen objetos maliciosos de una página web maliciosa o infectada. Los delincuentes crean sitios maliciosos a propósito, pero también los sitios legítimos se pueden infectar cuando son los usuarios quienes crean su contenido (como en el caso de los foros), o si son víctimas de hackeo.

Países fuente de ataques web

Esta estadística muestra la distribución por país de las fuentes de ataques en línea contra los equipos de los usuarios (páginas web con redireccionamientos a exploits, sitios con exploits y otros programas maliciosos, centros de control de botnets, etc.) bloqueados por los productos de Kaspersky Lab. Cada host único puede ser fuente de uno o más ataques web.

Para determinar el origen geográfico de los ataques web se usó el método de comparación del nombre de dominio con la dirección IP real donde se encuentra el dominio dado y la definición de la ubicación geográfica de la dirección IP (GEOIP).

Las soluciones de Kaspersky Lab neutralizaron **1 876 998 691** ataques lanzados desde recursos de Internet ubicados en diversos países del mundo. Al mismo tiempo, el 92,1 % del total de notificaciones de ataques bloqueados por los componentes antivirus provino de recursos en línea ubicados en solo 10 países.



Distribución de fuentes de ataques web por países. Noviembre 2017 – octubre 2018

En comparación con los resultados del año anterior, la distribución de las fuentes de ataques web no ha cambiado mucho. En el primer lugar sigue Estados Unidos (45,65%), seguido de Holanda (17,53%) y Alemania (11,70%). Abandonaron el TOP10 Finlandia, Ucrania y China. Sus lugares fueron ocupados por Irlanda (1,25%), Luxemburgo (1,02%) y Singapur (0,98%).

Países donde los usuarios han estado bajo mayor riesgo de infectarse mediante Internet

Para evaluar el riesgo de infección con malware a través de Internet al que están expuestos los equipos de los usuarios en diferentes países del mundo, hemos calculado con qué frecuencia durante el año los usuarios de los productos de Kaspersky Lab en cada país se toparon con la reacción del antivirus web. Los datos obtenidos reflejan el índice de la agresividad del entorno en el que funcionan los equipos en diferentes países.

Recordamos al lector que esta calificación toma en cuenta sólo los ataques realizados por objetos maliciosos de la clase Malware. En los cálculos no tomamos en cuenta las reacciones del antivirus web ante los programas potencialmente peligrosos y no deseados, tales como RiskTool y programas publicitarios. En general, durante el período que abarca el informe, los programas de publicidad y sus componentes se registraron en el **53%** de los equipos de usuarios en las que se activó el antivirus web.

TOP20 de países donde los usuarios han estado bajo mayor riesgo de infectarse mediante Internet

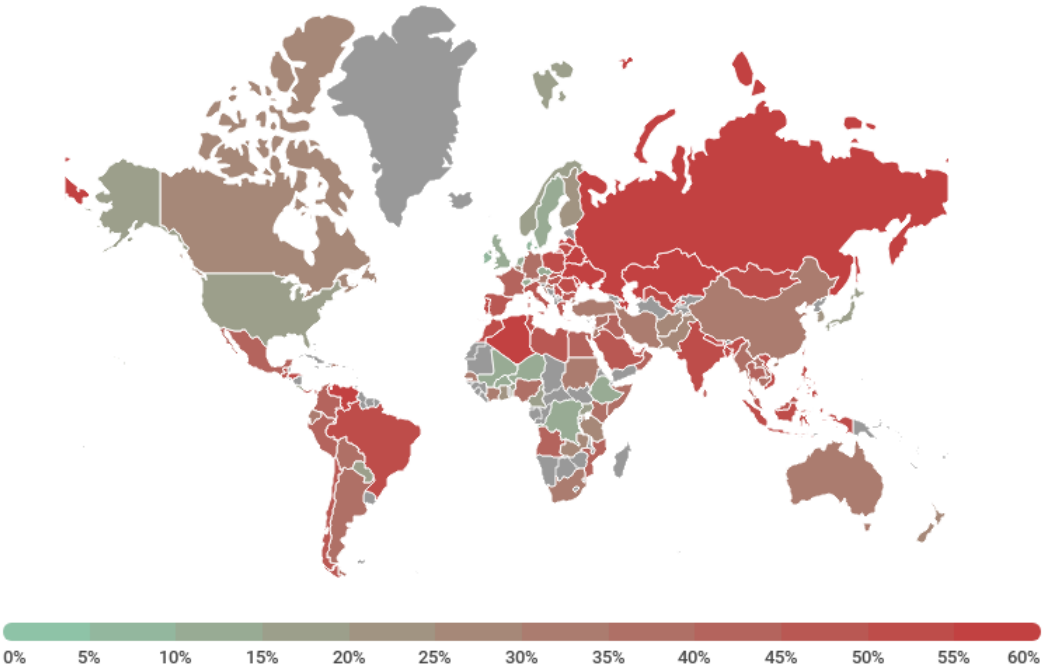
	País*	%**
1	Argelia	43,31
2	Bielorrusia	43,0
3	Venezuela	39,48
4	Kazajistán	37,76
5	República de Moldova	37,39
6	Azerbaiyán	36,82
7	Rusia	36,22
8	Ucrania	35,52
9	Letonia	34,63
10	Serbia	34,62
11	Vietnam	34,45
12	Catar	34,37
13	Túnez	34,35
14	Indonesia	33,69
15	Rumania	33,09
16	Mongolia	32,88

	País*	%**
17	Filipinas	32,81
18	Marruecos	32,7
19	Brasil	31,0
20	Nepal	31,90

** En los cálculos hemos excluido a los países en los que la cantidad de usuarios de Kaspersky Lab es relativamente baja (menos de 50 000).*

*** Porcentaje de usuarios únicos que fueron víctimas de ataques web realizados por malware, del total de los usuarios únicos de los productos de Kaspersky Lab en el país.*

En promedio, durante el año el **30,01%** de los equipos de los usuarios de Internet en el mundo al menos una vez enfrentaron un ataque web que involucraba software de la clase Malware.



Geografía de los ataques de malware web, noviembre de 2017 – octubre de 2018

Top 20 de los programas maliciosos más utilizados en ataques en línea

En 2018, el antivirus web de Kaspersky Lab detectó **21 643 946** objetos maliciosos únicos (scripts, exploits, archivos ejecutables, etc.) y **554 159 621** URL únicas donde se activó el antivirus web. Basándonos en los datos recopilados, identificamos los 20 programas maliciosos más utilizados en los ataques en línea contra los equipos de los usuarios.

	Veredicto	%*
1	URL malicioso	89,50
2	Trojan.Script.Generic	6,19
3	Trojan.Script.Miner.gen	1,95
4	Trojan.Script.Agent.gen	0,38
5	Trojan.JS.Miner.m	0,27
6	Trojan-Clicker.HTML.Iframe.dg	0,26
7	Trojan.JS.Agent.eak	0,13
8	Trojan.JS.Miner.d	0,12
9	Hoax.HTML.FraudLoad.m	0,11
10	Trojan.Win32.Miner.ays	0,06
11	Trojan-Dropper.VBS.Agent.bp	0,05
12	Trojan-Downloader.Script.Generic	0,05
13	Trojan.Win64.Shelma.a	0,04
14	Packed.Multi.MultiPacked.gen	0,04
15	Trojan.JS.Miner.x	0,04
16	Trojan.JS.Miner.y	0,04

	Veredicto	%*
17	Hoax.Script.Generic	0,03
18	DangerousObject.Multi.Generic	0,03
19	Trojan.Script.Iframer	0,03
20	Trojan.JS.Agent.ecp	0,02

** Porcentaje de todos los ataques web de la clase malware registrados en los equipos de usuarios únicos de los productos de Kaspersky Lab.*

Este año, el TOP20 incluyó a muchos criptomineros web, en su mayoría representantes de la familia Trojan.JS.Miner que ocuparon cuatro de los veinte puestos. Al mismo tiempo, las vulnerabilidades web reunidas bajo el veredicto Exploit.Script.Generic y que se ubicaron en el décimo lugar el año pasado, esta vez no lograron entrar en el TOP 20.

AMENAZAS LOCALES

Las estadísticas de infecciones locales de los equipos de los usuarios son un indicador importante. En ella se enumeran los objetos que entraron en el equipo mediante la infección de archivos o memorias extraíbles, o aquellos que inicialmente entraron en forma velada (por ejemplo, programas incluidos en los instaladores complejos, archivos cifrados, etc.). Además, estas estadísticas incluyen los objetos detectados en los equipos de los usuarios después del primer análisis del sistema realizado con el software antivirus Kaspersky Lab.

En esta sección, evaluamos los datos estadísticos resultantes del análisis antivirus de archivos en el disco duro en el momento de su creación o acceso, y los datos del análisis de varios medios de almacenamiento extraíbles.

TOP 20 de malware detectado en los equipos de los usuarios

Hemos identificado las veinte amenazas que en 2018 se detectaron con mayor frecuencia en los equipos de los usuarios. Esta calificación no incluye programas del tipo Riskware y programas publicitarios.

	Veredicto	%*
1	DangerousObject.Multi.Generic	32,15
2	Trojan.Script.Generic	14,46
3	Trojan.Multi.GenAutorunReg.a	5,76
4	Trojan.WinLNK.Agent.gen	4,56
5	Trojan.WinLNK.Starter.gen	3,47
6	HackTool.Win32.KMSAuto.c	3,14
7	HackTool.Win64.HackKMS.b	2,69
8	Trojan.Win32.Generic	2,56
9	Trojan.Script.Miner.gen	2,44
10	Trojan.Win32.AutoRun.gen	2,43
11	Trojan-Downloader.Script.Generic	2,33
12	Virus.Win32.Sality.gen	2,30
13	HackTool.Win32.KMSAuto.m	2,05

	Veredicto	%*
14	Trojan.AndroidOS.Boogr.gsh	1,96
15	Trojan.Win32.Agentb.bqyr	1,48
16	Trojan.Win32.Miner.gen	1,41
17	Trojan.Multi.GenAutorunBITS.a	1,28
18	Trojan.Multi.Babits.genw	1,19
19	Virus.Win32.Nimnul.a	1,18
20	HackTool.MSIL.KMSAuto.ba	1,13

** Porcentaje de usuarios únicos, en cuyos equipos el antivirus de archivos detectó este objeto, del total de usuarios únicos de los productos de Kaspersky Lab en los que los programas maliciosos provocaron la reacción del antivirus.*

El primer lugar en nuestro TOP20, como ya es tradición, lo ocupa el veredicto DangerousObject.Multi.Generic (32,15%), que utilizamos para los programas maliciosos detectados con la ayuda de las tecnologías de nube. Estas tecnologías se activan cuando en las bases antivirus todavía no existen ni firmas, ni métodos heurísticos que detecten el programa malicioso, pero la base de datos de nube de la compañía ya tiene información sobre este objeto. Así es como se detecta el malware más reciente.

Múltiples variaciones del malware WinLNK siguen siendo comunes: Trojan.WinLNK.Agent.gen (4,56%) está en el cuarto lugar, y Trojan.WinLNK.Starter.gen (3,47%) está justo detrás de él. Este malware puede cambiar la configuración del navegador de la víctima o usarse para descargar otro malware.

En el puesto 14 se ubica Trojan Trojan.AndroidOS.Boogr.gsh (1,96%), un malware que se detecta utilizando tecnologías de aprendizaje automático para programas maliciosos que funcionan en el sistema operativo Android.

Trojan.Multi.GenAutorunBITS.a (1,28%) y Trojan.Multi.Babits.genw (1,19%) ocupan los lugares 17 y 18 respectivamente. Estos programas maliciosos, como muchos otros, utilizan el componente. Background Intelligent Transfer Service para afianzarse en el sistema.

Países en que los equipos de los usuarios estuvieron expuestos al mayor riesgo de infección local

Para cada uno de los países calculamos con qué frecuencia durante el año los usuarios se toparon con las reacciones del antivirus de archivos. Se tuvieron en cuenta los objetos detectados que se encuentran directamente en las computadoras de los usuarios o en los medios extraíbles conectados (unidades flash, tarjetas de memoria de cámaras y teléfonos, discos duros externos). La presente estadística refleja el nivel de infección de los equipos personales en diferentes países del mundo.

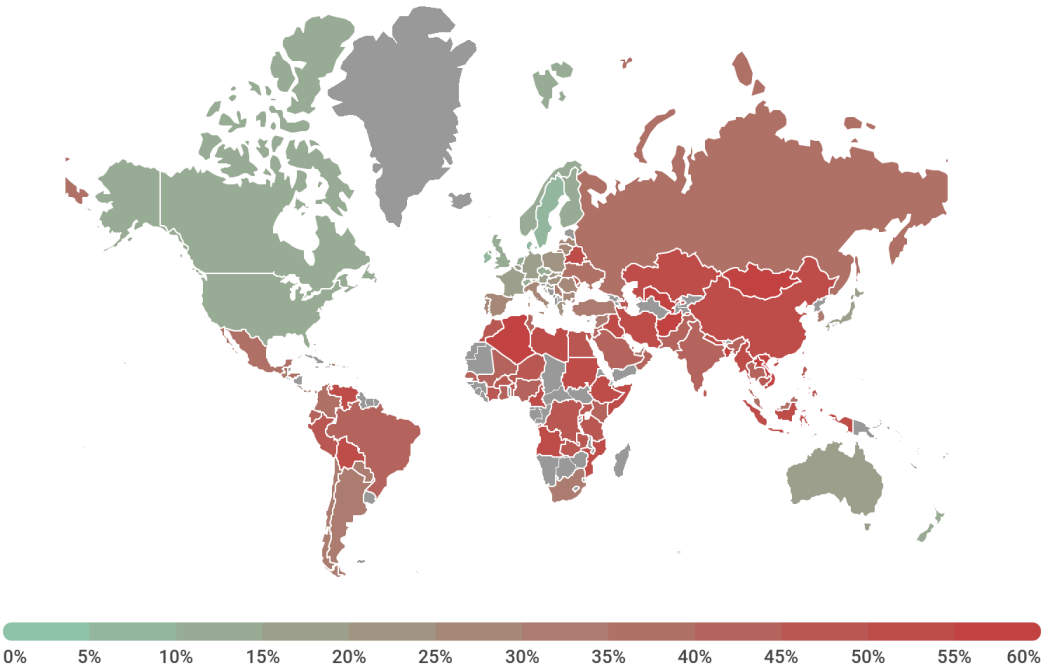
TOP 20 países según el riesgo de infección local

	País*	%**
1	Vietnam	62,29
2	Afganistán	61,93
3	Uzbekistán	60,22
4	Laos	58,94
5	Mongolia	58,35
6	Argelia	58,13
7	Bangladesh	56,58
8	Ruanda	54,88
9	Siria	54,76
10	Myanmar	54,03
11	Sudán	53,77
12	Etiopía	53,69
13	Irak	53,50
14	Mozambique	53,31
15	Kazajistán	53,15
16	Nepal	53,14

	País*	%**
17	Bielorrusia	52,38
18	Libia	51,92
19	Venezuela	51,18
20	China	51,17

** En los cálculos hemos excluido a los países donde la cantidad de usuarios de Kaspersky Lab es relativamente baja (menos de 50 000).*

*** Porcentaje de usuarios únicos en cuyos equipos se bloquearon amenazas locales de la clase Malware, del total de usuarios de productos de Kaspersky Lab en el país.*



Geografía de infecciones provocadas por malware local, noviembre de 2017 – octubre de 2018

En 2018, se detectó un promedio de al menos un programa malicioso en el **35,06%** de los equipos, discos duros o medios extraíbles pertenecientes a los usuarios de KSN.