KASPERSKY lab

Kaspersky: Boletín
De Seguridad

ESTADÍSTICAS GENERALES DE 2017

CONTENTS

El año en cifras 4

Aplicaciones vulnerables utilizadas en ciberataques 5

Amenazas en línea (ataques desde Internet) 9

Los 10 principales países con recursos infectados en Internet 11

Los 20 principales veredictos detectados en Internet 12

Programas ransomware cifradores 14

Amenazas en línea en el sector financiero 18

Países en los que los usuarios enfrentan el mayor riesgo de infecciones en Internet 22

Amenazas locales 25

TOP 20 de objetos maliciosos detectados en los equipos de los usuarios 26

Países en los que los usuarios enfrentan el mayor riesgo de infecciones locales 28

Todas las estadísticas mencionadas en este informe se obtuvieron a través de Kaspersky Security Network (KSN), una red antivirus que funciona con varios componentes de protección antimalware. Los datos fueron voluntariamente proporcionados por los usuarios de KSN. Millones de usuarios de los productos de Kaspersky Lab en 213 países y territorios en todo el mundo participan en este intercambio mundial de información sobre actividades maliciosas.

EL AÑO EN CIFRAS

El **29,4%** de los equipos de los usuarios sufrieron al menos un ataque de programas maliciosos a través de Internet en el año.

Las soluciones de Kaspersky Lab neutralizaron **1 188 728 338** ataques lanzados desde recursos en Internet distribuidos por todo el mundo.

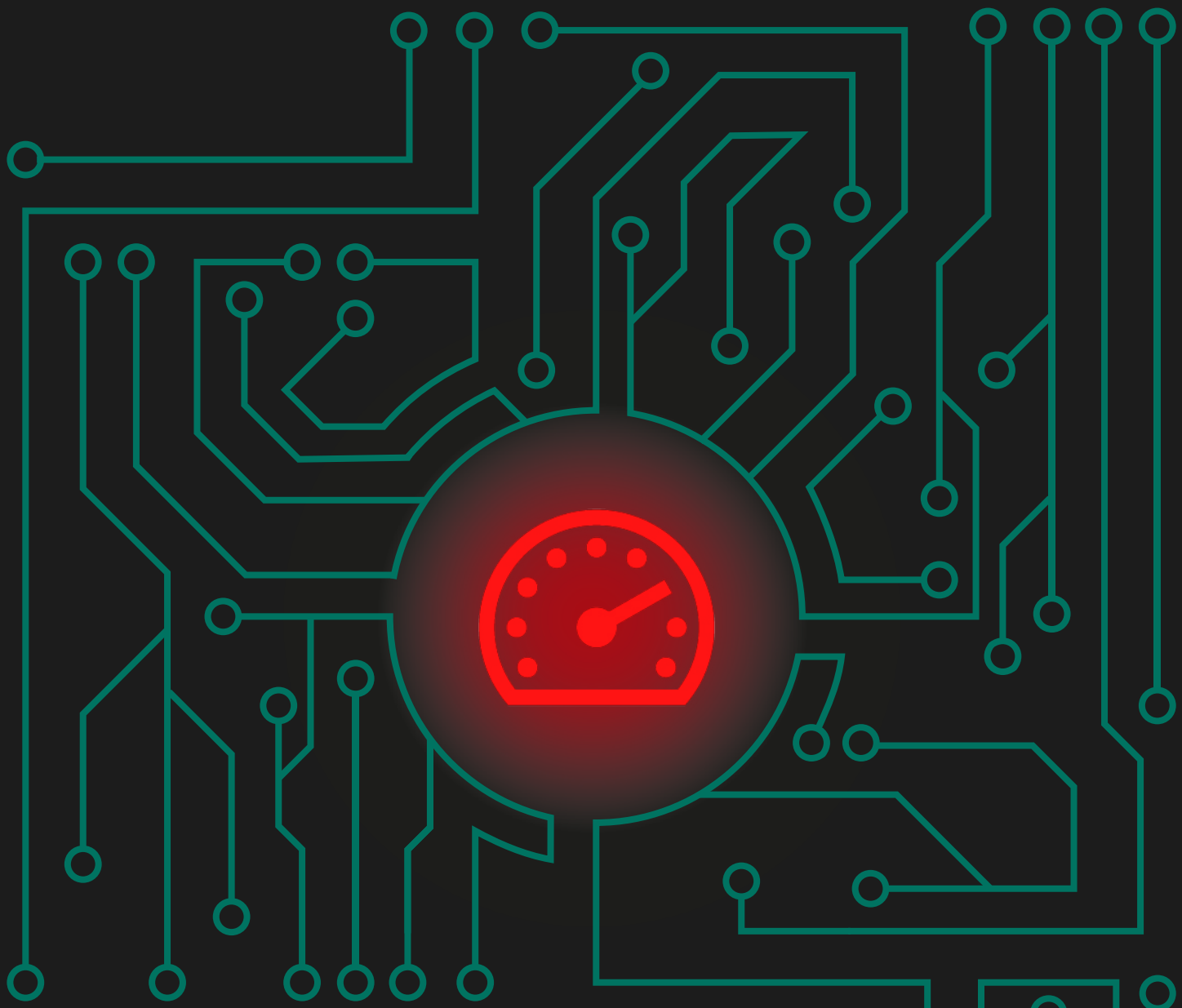
Los componentes antivirus web reconocieron **199 455 606** URLs únicas como maliciosas.

Los antivirus web de Kaspersky Lab detectaron **15 714 700** objetos maliciosos únicos.

939 722 equipos de usuarios únicos fueron atacados por programas maliciosos cifradores.

Las soluciones de Kaspersky Lab bloquearon **1 126 701** intentos de ataques de malware diseñado para robar dinero mediante la banca online.

Las estadísticas sobre amenazas móviles se encuentran en el informe "Evolución del malware móvil en 2017".



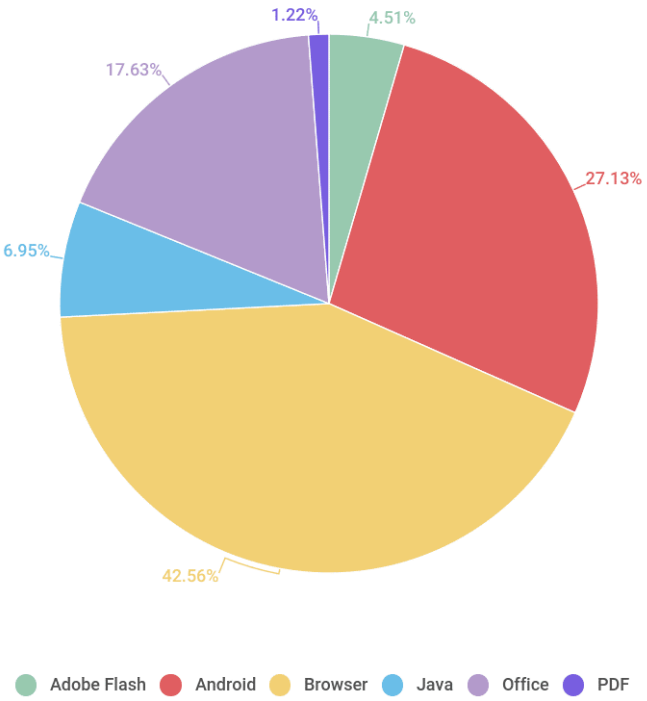
APLICACIONES VULNERABLES UTILIZADAS EN CIBERATAQUES

En 2017 se vieron muchas vulnerabilidades de día cero activamente explotadas no sólo en ataques selectivos, sino también de forma masiva. A diferencia de las estadísticas del año pasado, los exploits para vulnerabilidades en Adobe Flash Player e Internet Explorer han ido disminuyendo, siendo reemplazados por exploits para Microsoft Office. La creación de exploits confiables para Flash Player se ha convertido en un proceso que consume mucho tiempo y dinero para el ciberpirata promedio. No se trata sólo de encontrar y explotar una vulnerabilidad en Flash Player, sino que también hay que superar las medidas de seguridad en los modernos navegadores web. Y como todos los principales actores de kits de exploits se retiraron del mercado en 2017, sólo los atacantes altamente sofisticados son capaces de desarrollar un exploit para Flash Player.

Debido a que el mercado de kits de exploits, tradicionalmente dominado por los exploits para navegadores y Flash Player, está decayendo, estamos ante un crecimiento sustancial de ataques contra usuarios de Microsoft Office: un 4% en este año o un escalofriante 14% en los dos últimos años. La principal razón para este aumento radica en las numerosas vulnerabilidades día cero descubiertas en Office en los últimos 12 meses. Las vulnerabilidades de corrupción de memoria binaria CVE-2017-0261, CVE-2017-0262, CVE-2017-11826 se utilizaron en ataques APT, aunque no fueron más ampliamente usadas en campañas de spam malicioso debido a la complejidad y baja confiabilidad de los exploits. Los exploits para tres vulnerabilidades 'lógicas' (CVE-2017-0199, CVE-2017-8570, y CVE-2017-8759) han sido utilizadas este año en la mayoría de los ataques tipo spear-phishing. Según las estadísticas de KSN, más del 90% de los documentos de Microsoft Office con exploits detectados contenían exploits para las vulnerabilidades CVE-2017-0199 o CVE-2017-8759, lo que los coloca muy por encima de otros exploits. Resulta interesante que muchos de los documentos con un exploit para Microsoft Office en 2017 también contenían un componente phishing, en caso de que la víctima ya hubiese parchado la vulnerabilidad.

Los exploits para Android también mostraron un alza anual del 6%, sumando el 27% de todos los exploits. El rápido crecimiento del año pasado aún continúa, principalmente debido a un aumento en la cantidad de exploits que facilitan el escalamiento de privilegios de raíz en dispositivos móviles Android.

Sin embargo, el principal suceso - no sólo del segundo trimestre, sino de todo el año 2017 - fue la publicación del archivo comprimido 'Lost in Translation' por parte del grupo de hackers Shadow Brokers. Este archivo comprimido contenía múltiples exploits de red para varias versiones de Windows. E incluso a pesar de que la mayoría de esas vulnerabilidades no eran en realidad del tipo día cero y que Microsoft las había parchado con la actualización MS17 - 010 un mes antes, la publicación tuvo graves consecuencias. Los daños causados por los gusanos de red, troyanos y programas ransomware cifradores que se propagaron a través de la red con la ayuda de

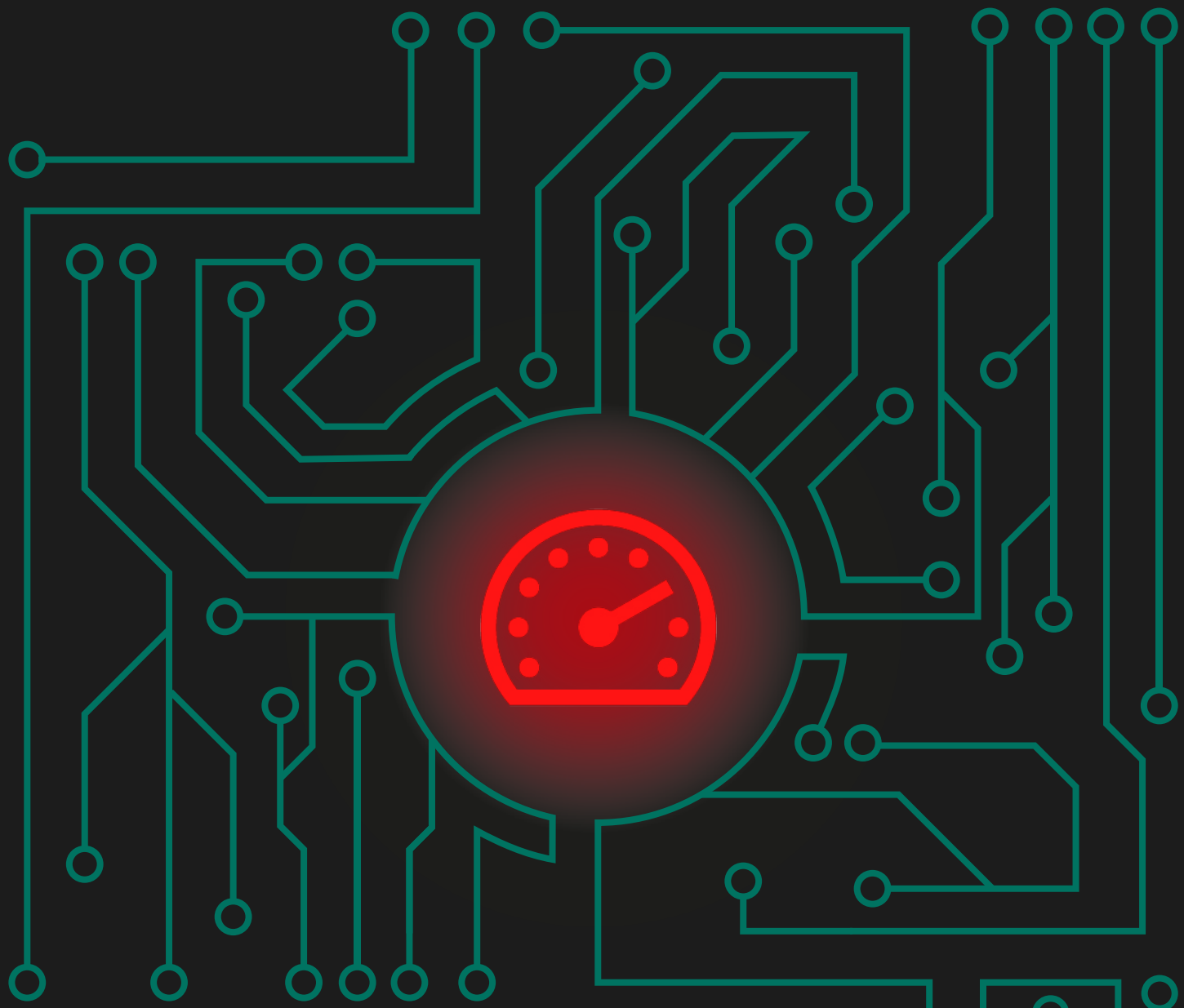


Distribución de los exploits usados en ciberataques, por tipo de aplicación atacada. Noviembre de 2016 – Octubre de 2017

los exploits EternalBlue y Eternal Romance SMB, así como a través de los usuarios infectados, son incalculables. En las estadísticas anuales sobre los ataques de red bloqueados por nuestro componente IDS, vimos que el veredicto Intrusion.Win.MS17-010.* fue una de las vulnerabilidades de red más explotadas durante varios meses.

Las aplicaciones vulnerables se clasifican según los informes de los productos de Kaspersky Lab sobre la neutralización de los exploits utilizados por los ciberdelincuentes tanto en ataques desde Internet, como en aplicaciones locales infectadas, incluyendo las instaladas en los dispositivos móviles de los usuarios.

En resumen, 2017 significó la interrupción de una larga tendencia en el mercado de kits de exploits, que dejó de lado a Internet Explorer y Adobe Flash Player para concentrarse en Microsoft Office. Cada vez es más común que los ciberpiratas recurran a técnicas de ingeniería social, ya que es un recurso barato y a veces hasta más confiable que el uso de exploits 'tradicionales'. Los ataques globales de los programas extorsionadores WannaCry y ExPetr demostraron lo peligroso y desastroso que puede ser un gusano de red, incluso si utiliza una vulnerabilidad que ya estaba parchada.



AMENAZAS EN LÍNEA (ATAQUES DESDE INTERNET)

Las estadísticas se basan en los veredictos de los componentes Web Antivirus que protegen a los usuarios contra intentos de descarga de objetos maliciosos desde un sitio web malicioso o infectado. Los ciberpiratas crean deliberadamente sitios web maliciosos. Entre los sitios infectados se encuentran aquellos con contenidos provistos por los usuarios (como los foros), así como recursos legítimos infectados.

En 2017, el antivirus web de Kaspersky Lab detectó **15 714 700** objetos maliciosos únicos (scripts, exploits, archivos ejecutables, etc.) y **199 455 606** URLs únicas. Las soluciones de Kaspersky Lab detectaron y neutralizaron **1 188 728 338** ataques maliciosos lanzados desde recursos en línea localizados en 206 países en todo el mundo.

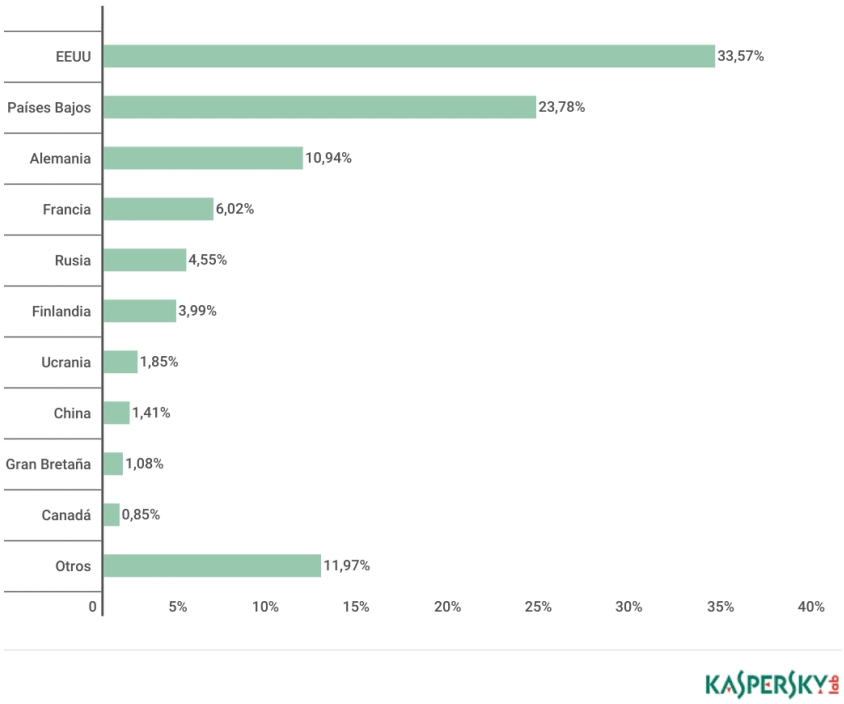
LOS 10 PRINCIPALES PAÍSES CON RECURSOS INFECTADOS EN INTERNET

Las siguientes estadísticas se basan en la ubicación física de los recursos en línea utilizados en ataques y bloqueados por nuestros componentes antivirus (páginas web con desvíos a exploits, sitios con exploits y otros programas maliciosos, centros de comando de redes zombis, etc.). Cualquier host único podría ser el origen de uno o más ataques desde Internet.

Para determinar el origen geográfico de los ataques desde Internet, se comparan los nombres de dominio con sus verdaderas direcciones IP de dominio, y luego se establece el origen geográfico de una dirección IP específica (GEOIP).

En 2017, las soluciones de Kaspersky Lab neutralizaron 1 188 728 338 ataques lanzados desde recursos web localizados en varios países en todo el mundo.

Un 88,03% de notificaciones sobre ataques bloqueados por los componentes antivirus provinieron de recursos en línea localizados en 10 países.



Distribución de fuentes de ataques web por país. Noviembre de 2016 - Octubre de 2017

Se mantuvieron los primeros tres países de la lista: EE.UU. (33,57%), Holanda (23,78%) y Alemania (10,94%). Francia (6,02%) desplazó a Rusia (4,5 5%) y ocupó la cuarta posición. Las Islas Vírgenes y Bulgaria abandonaron el TOP 10, mientras que Finlandia (3,99%) y Canadá (0,85%) hiciero su debut.

LOS 20 PRINCIPALES VEREDICTOS DETECTADOS EN INTERNET

En 2017, los componentes antivirus web de Kaspersky Lab detectaron **15 714 700** objetos maliciosos únicos: scripts, exploits, archivos ejecutables, etc.

Durante el año, los programas publicitarios y sus componentes se encontraron en el 22% de los equipos de los usuarios donde nuestro componente antivirus web detectó amenazas.

En 2017, identificamos los 20 programas maliciosos más activos en ataques por Internet lanzados contra computadoras.

	Nombre*	% de todos los ataques**
1	URLs maliciosas	**87,75%**
2	Trojan.Script.Generic	**6,69%**
3	Trojan.JS.Small.ci	**1,66%**
4	Trojan-Clicker.HTML.Iframe.dg	**1,44%**
5	Trojan.JS.Miner.d	**0,31%**
6	Trojan-Downloader.JS.Agent.npe	**0,25%**
7	Packed.Multi.MultiPacked.gen	**0,16%**
8	Trojan-Downloader.Script.Generic	**0,14%**
9	Trojan-Dropper.VBS.Agent.bp	**0,09%**
10	Exploit.Script.Generic	**0,07%**
11	Trojan.JS.Agent.dvu	**0,07%**
12	Trojan-Clicker.Script.Generic	**0,06%**
13	Trojan.JS.Agent.sileof	**0,05%**
14	Trojan-Downloader.JS.SLoad.gen	**0,05%**
15	Trojan-Downloader.JS.Redirector.a	**0,04%**
16	Hoax.HTML.FraudLoad.m	**0,03%**

	Nombre*	% de todos los ataques**
17	Trojan.Script.Iframer.a	**0,03%**
18	Trojan.JS.AdInject.a	**0,03%**
19	Trojan.JS.Agent.ckf	**0,02%**
20	Trojan.Win32.Cometer.aj	**0,02%**

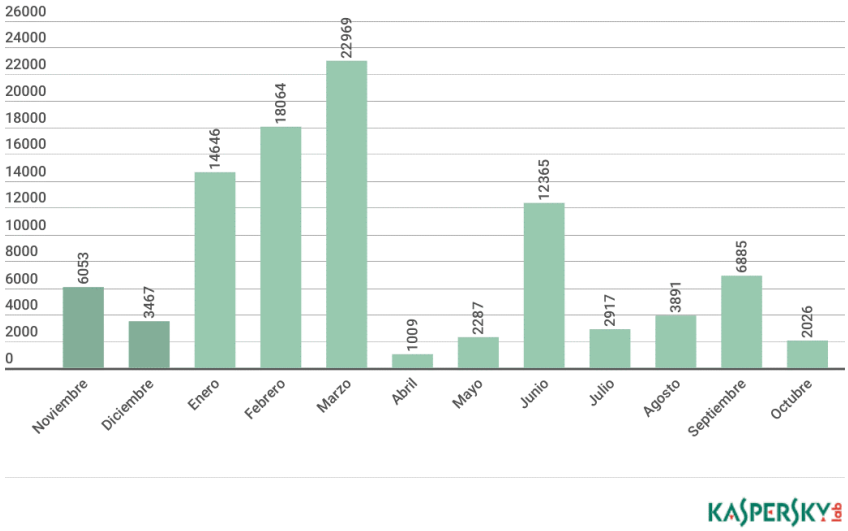
Hoy en día, los exploits web ya no son tan populares, pero todavía podemos ver el veredicto Exploit.Script.Generic en la décima posición de esta clasificación.

Otros scripts realizan diferentes actividades maliciosas. Por ejemplo, Trojan.JS.Small.ci inyecta agresivamente anuncios de terceras partes en el tráfico, Trojan.JS.Miner.d es un minero web, Trojan.JS.Agent.sileof avisa sobre la detección de recursos fraudulentos que bloquean los navegadores al generar de forma constante mensajes falsos sobre infecciones.

*Estas estadísticas representan los veredictos de detección de nuestro módulo Web Antivirus. La información fue proporcionada por los usuarios de los productos de Kaspersky Lab que aceptaron compartir sus datos locales.
** Porcentaje de todos los ataques en línea con programas maliciosos registrados en los equipos de usuarios únicos.

PROGRAMAS RANSOMWARE CIFRADORES

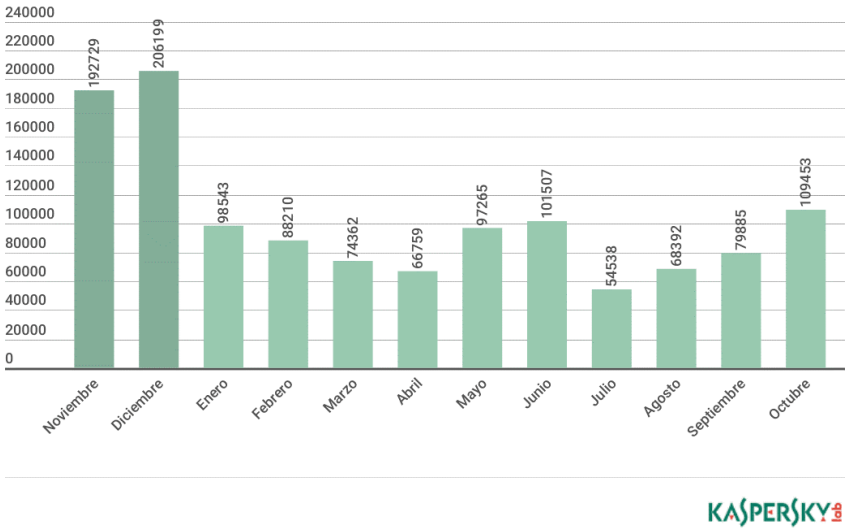
En 2017, detectamos más de **96 000 modificaciones** de programas ransomware cifradores y descubrimos **38 familias nuevas**.



Número de nuevas modificaciones en programas ransomware cifradores.
Noviembre 2016 – Octubre 2017

Número de usuarios atacados por cifradores

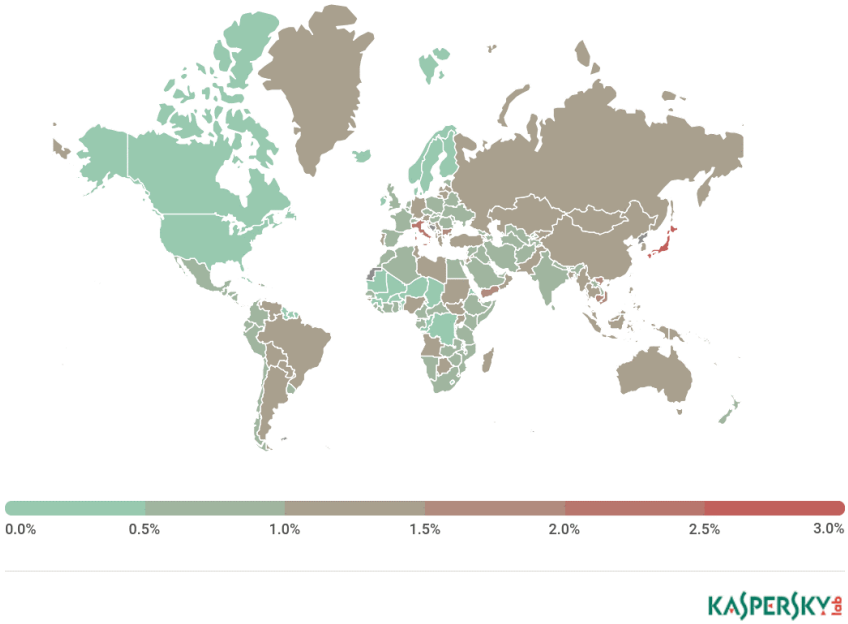
En 2017, **939 722 usuarios únicos de KSN** fueron atacados por cifradores, entre ellos **240 000** usuarios corporativos.



Número de usuarios atacados por programas ransomware cifradores.
Noviembre de 2016 – Octubre de 2017

Es importante recordar que la cantidad real de incidentes es mayor, pues las estadísticas sólo reflejan los resultados de detecciones por firmas y heurísticas, mientras que en el caso de muestras de programas maliciosos nuevos y desconocidos, los productos de Kaspersky Lab detectan troyanos cifradores en base a modelos de reconocimiento de comportamiento.

Geografía de los ataques



Geografía de los ataques con programas ransomware cifradores en 2017 (porcentaje de usuarios atacados)

TOP10 de países atacados por programas cifradores

	País*	% de usuarios atacados por cifradores**
1	Japón	2,83
2	Italia	2,37
3	Vietnam	1,95
4	Bulgaria	1,68
5	Taiwán	1,59
6	Camboya	1,53
7	Croacia	1,48
8	Líbano	1,44
9	Brasil	1,42
10	Indonesia	1,35

*Se han excluido aquellos países en los que el número de usuarios de los productos de Kaspersky Lab es relativamente pequeño (menos de 50 000).
** Usuarios únicos cuyos equipos han sido atacados por programas ransomware cifradores en relación porcentual a todos los usuarios únicos de los productos de Kaspersky Lab en el país.

TOP 10 de las principales familias de cifradores más propagadas

	Nombre	Veredicto*	% de usuarios atacados**
1	WannaCry	Trojan - Ransom.Win32.Wanna	**7,71**
2	Locky	Trojan - Ransom.Win32.Locky	**6,70**
3	Cerber	Trojan - Ransom.Win32.Zerber	**5,89**
4	Jaff	Trojan - Ransom.Win32.Jaff	**2,58**
5	Cryrar/ACCDFISA	Trojan - Ransom.Win32.Cryrar	**2,20**
6	Spora	Trojan - Ransom.Win32.Spora	**2,19**
7	Purgen/GlobeImposter	Trojan - Ransom.Win32.Purgen	**2,11**
8	Shade	Trojan - Ransom.Win32.Shade	**2,06**
9	Crysis	Trojan - Ransom.Win32.Crusis	**1,25**
10	CryptoWall	Trojan - Ransom.Win32.Cryptodef	**1,13**

La epidemia de WannaCry afectó a cientos de miles de equipos en todo el mundo. No resulta sorprendente que haya sido la familia de cifradores más expandida en 2017.

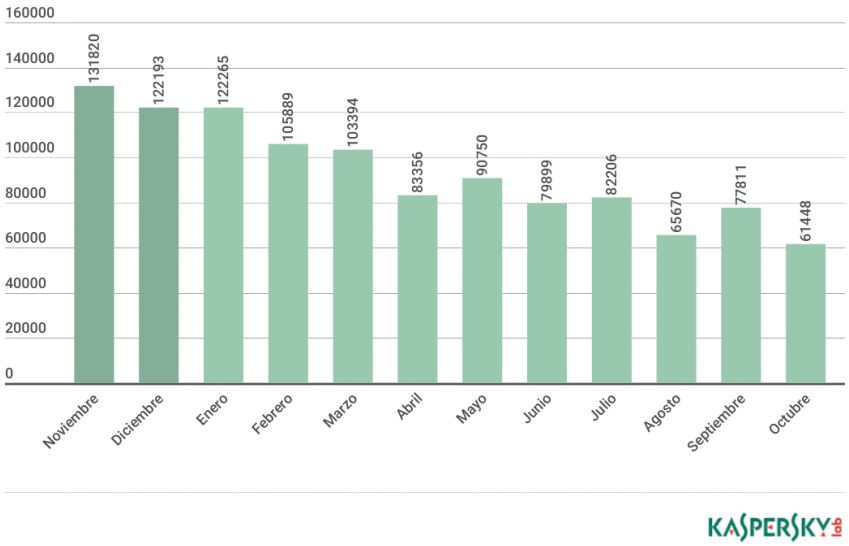
Puede encontrar más información sobre la situación del ransomware en: Kaspersky Security Bulletin – 2017: Historia del año.

*Estas estadísticas se basan en los veredictos de detección recibidos de los usuarios de los productos de Kaspersky Lab que aceptaron proporcionar sus datos estadísticos.
** Usuarios únicos cuyos equipos han sido atacados por una determinada familia de programas ransomware cifradores en relación porcentual a todos los usuarios de los productos de Kaspersky Lab atacados por programas ransomware cifradores.

AMENAZAS EN LÍNEA EN EL SECTOR FINANCIERO

Estas estadísticas se basan en los veredictos de detección de los productos de Kaspersky Lab, recibidos con el consentimiento de los usuarios de los productos de Kaspersky Lab. Las estadísticas anuales de 2017 se basan en datos recibidos entre noviembre de 2016 y octubre de 2017 e incluyen los programas maliciosos para terminales PoS y cajeros automáticos, pero no incluyen las amenazas móviles.

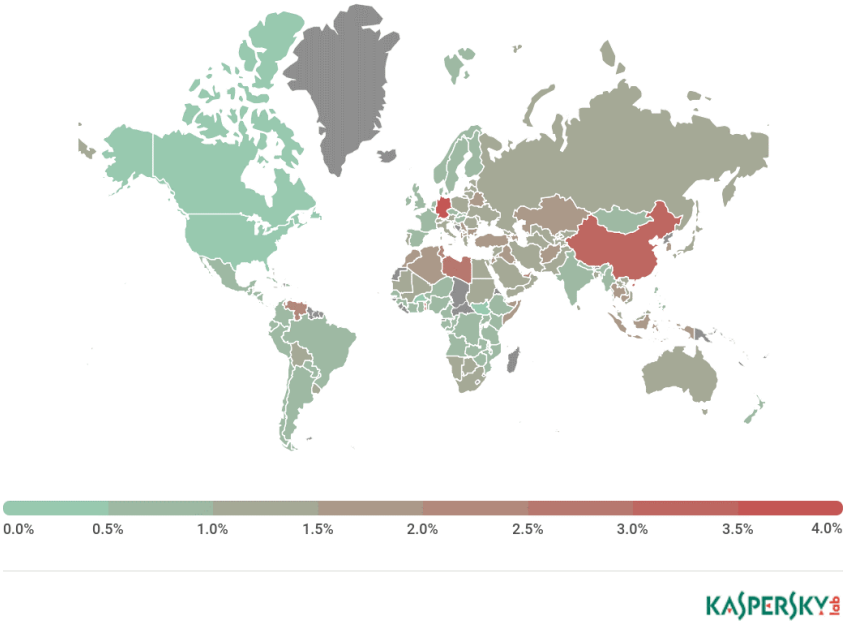
En 2017, las soluciones de Kaspersky Lab bloquearon intentos de ataque de uno o más programas maliciosos diseñados para robar dinero mediante la banca en línea en **1 126 701** equipos.



Cantidad de usuarios atacados por malware financiero. Noviembre de 2016 – Octubre de 2017

Geografía de los ataques

Para evaluar y comparar el riesgo de contraer infecciones por troyanos bancarios y programas maliciosos para PoS y cajeros automáticos en todo el mundo, calculamos el porcentaje de usuarios de los productos de Kaspersky Lab en el país en el que se encontró este tipo de amenaza durante el periodo de investigación, en relación a todos los usuarios de nuestros productos en dicho país.



Geografía de los ataques de malware financiero en 2017

TOP 10 de países por porcentaje de usuarios atacados

	País*	% de usuarios atacados**
1	Alemania	**4,44**
2	Togo	**3,17**
3	China	**3,05**
4	Libia	**2,81**
5	Líbano	**2,45**
6	Túnez	**2,21**
7	Taiwán	**2,15**
8	Emiratos Árabes Unidos	**2,12**
9	Venezuela	**2,06**
10	Jordania	**1,88**

*Se excluyeron aquellos países en los que la cantidad de usuarios de los productos de Kaspersky Lab es relativamente pequeña (menos de 50 000 y menos de 7000 notificaciones sobre malware bancario).
**Usuarios únicos cuyos equipos fueron atacados por malware financiero en relación porcentual a todos los usuarios atacados por todos los tipos de malware

Las 10 principales familias de malware bancario

La siguiente tabla muestra las 10 familias de programas maliciosos más usados en 2017 para atacar a usuarios de banca en línea (en relación porcentual a los usuarios atacados):

	Nombre*	% de usuarios atacados**
1	Trojan - Spy.Win32.Zbot	**39,2**
2	Trojan.Win32.Nymaim	**26,2**
3	Trojan.Win32.Neurevt	**5,9**
4	SpyEye	**5,8**
5	Trojan - Banker.Win32.Gozi	**4,3**
6	Emotet	**3,1**
7	Caphaw	**3,0**
8	Trickster	**2,8**
9	Cridex/Dridex	**2,7**
10	Backdoor.Win32.Shiz	**2,4**

* Estas estadísticas se basan en los veredictos de detección generados por los productos de Kaspersky Lab y recibidos de los usuarios de los productos de Kaspersky Lab que aceptaron compartir sus datos estadísticos.
** Usuarios únicos cuyos equipos fueron atacados por el programa malicioso, en relación porcentual a todos los usuarios únicos atacados por programas maliciosos financieros.

PAÍSES EN LOS QUE LOS USUARIOS ENFRENTAN EL MAYOR RIESGO DE INFECCIONES EN INTERNET

Para evaluar los países en los que los usuarios enfrentan ciberamenazas con mayor frecuencia, calculamos cuántas veces los usuarios de Kaspersky Lab encontraron veredictos de detección en sus equipos en cada país. Los datos resultantes muestran el riesgo de infección al que están expuestos los equipos en diferentes países en el mundo, y constituyen un indicador de la agresividad del entorno al que se enfrentan los usuarios en distintas partes del mundo.

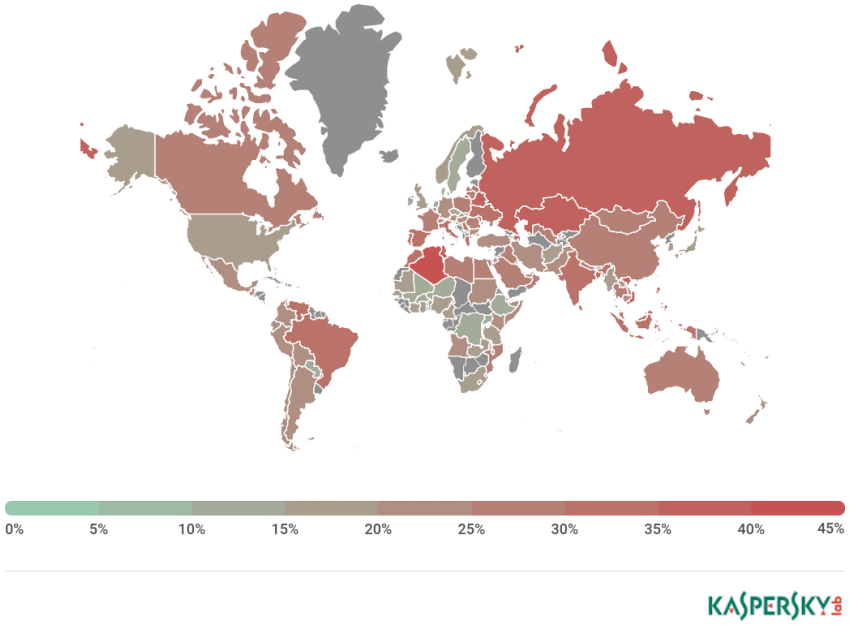
Esta clasificación sólo incluye a los ataques de programas maliciosos que pertenecen al tipo Malware. Esta clasificación no incluye las detecciones del módulo Web Antivirus de programas potencialmente peligrosos o no deseados, como Risk Tool o Adware.

TOP 20 de países cuyos usuarios enfrentan el mayor riesgo de infecciones en línea

	País*	% de usuarios únicos**
1	Argelia	**44,06**
2	Bielorrusia	**38,39**
3	Rusia	**36,91**
4	Kazajistán	**36,57**
5	Túnez	**36,51**
6	Vietnam	**35,01**
7	Azerbaiyán	**34,70**
8	Catar	**34,20**
9	Portugal	**33,01**
10	Grecia	**32,80**
11	Brasil	**32,66**
12	Moldavia	**32,42**
13	India	**32,34**
14	Marruecos	**31,72**
15	Venezuela	**31,52**
16	España	**31,20**
17	Sri Lanka	**30,75**
18	Malasia	**30,52**
19	Bangladesh	**30,37**
20	Ucrania	**30,27**

Estas estadísticas se basan en los veredictos de detecciones producidos por el módulo Web Antivirus, enviados por los usuarios de los productos de Kaspersky Lab que aceptaron compartir sus datos estadísticos.

*Se excluyeron aquellos países en los que la cantidad de usuarios de los productos de Kaspersky Lab es relativamente pequeña (menos de 50.000).
**Usuarios únicos cuyos equipos fueron atacados por programas Malware en relación porcentual a todos los usuarios únicos de ciertos productos de Kaspersky Lab en dicho país.



Geografía de ataques maliciosos desde Internet en 2017 (clasificados por el porcentaje de usuarios atacados)

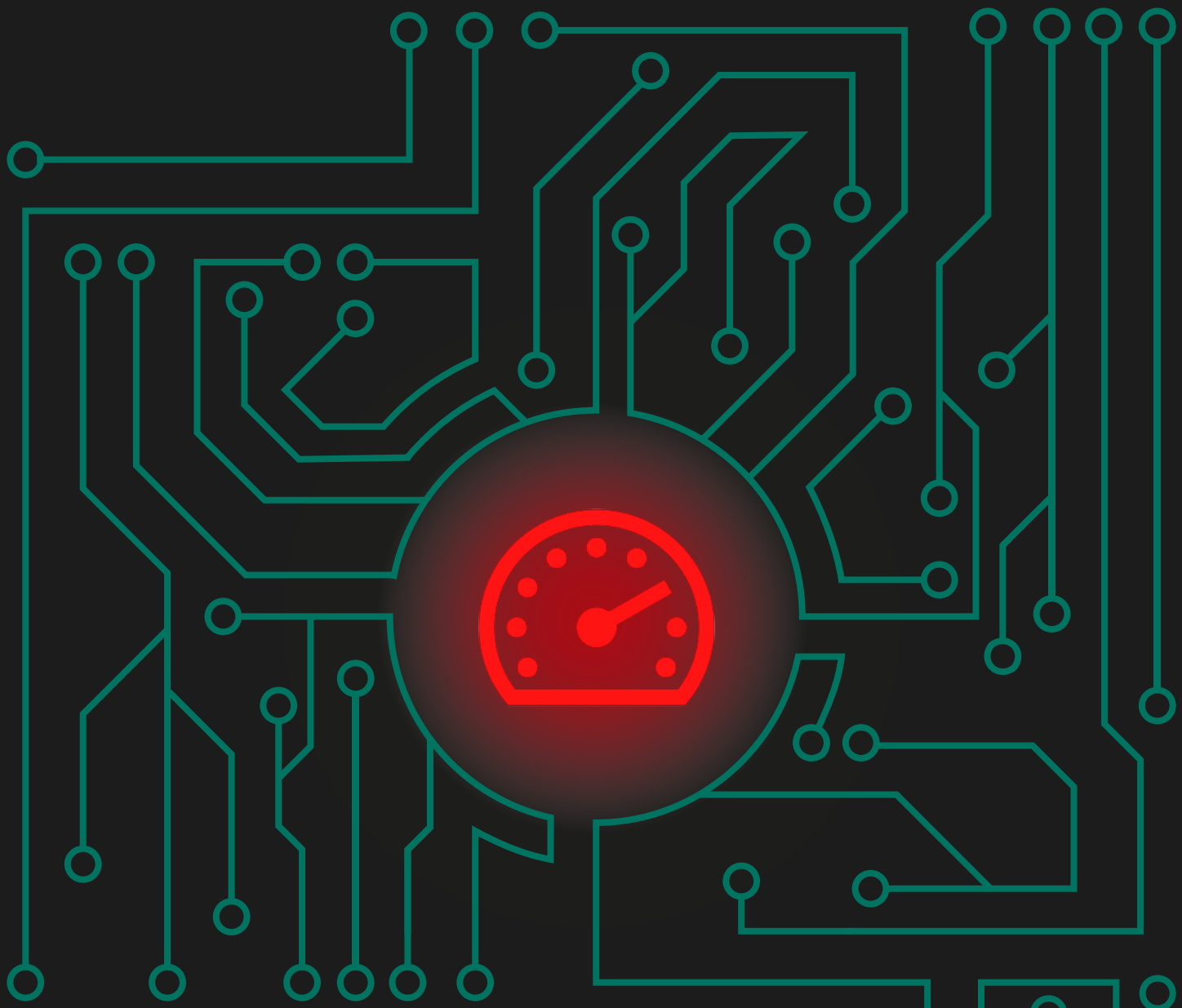
Los países pueden dividirse en tres grupos que reflejan los diferentes niveles de riesgo de infección.

El grupo de alto riesgo (más del 40%).
En 2017, este grupo incluyó un solo país: Argelia.

El grupo de riesgo medio (20%-39,9%).
Este grupo incluye 75 países, entre los cuales sobresalen: Bielorrusia (38,39%), Rusia (36,91%), Kazajistán (36,57%), Vietnam (35,01%), España (31,19%), Rumania (29,5%), Irak (26,85%), Angola (24,22%), Alemania (22,82%), Suiza (21,55%), Kenia (20,6%), Bolivia (20,15%).

El grupo de bajo riesgo (0-19,9%).
Los países con los entornos de Internet más seguros incluyen: Afganistán (19,55%), EE.UU. (19,4%), Reino Unido (19,22%), Japón (15,41%), Uganda (13,49%), Irlanda (12,15%).

En 2017, el **29,4%** de los equipos detectaron al menos un ataque de **Malware** mientras estaban conectados a Internet.



AMENAZAS LOCALES

TOP 20 DE OBJETOS MALICIOSOS DETECTADOS EN LOS EQUIPOS DE LOS USUARIOS

Las estadísticas de infecciones locales para los equipos de los usuarios son un indicador muy importante, pues reflejan las amenazas que han penetrado sistemas mediante la infección de archivos o de dispositivos extraíbles, o que inicialmente entraron al equipo en formato codificado (por ejemplo, programas integrados en instaladores complejos, archivos codificados, etc.). Además, estas estadísticas incluyen los objetos detectados en los equipos de los usuarios después de que el componente Antivirus de archivos de Kaspersky Lab realizara el primer análisis del sistema.

Esta sección contiene un análisis de los datos estadísticos obtenidos de los análisis antivirus de archivos en el disco duro en el momento en que se crearon o fueron abiertos, y los resultados de los análisis de varios dispositivos extraíbles de almacenamiento de datos.

Para esta clasificación, identificamos las 20 amenazas detectadas con más frecuencia en los equipos de los usuarios en 2017. Esta clasificación no incluye los programas Adware ni Riskware.

	Nombre*	% de usuarios únicos atacados**
1	DangerousObject.Multi.Generic	35,87%
2	Trojan.Script.Generic	9,47%
3	Trojan.Multi.GenAutorunReg.a	8,48%
4	HackTool.Win32.KMSAuto.i	8,39%
5	Trojan.WinLNK.Runner.jo	5,57%
6	Trojan.WinLNK.Agent.gen	4,89%
7	Trojan.WinLNK.StartPage.gena	4,14%
8	Trojan-Downloader.Script.Generic	3,64%
9	Trojan.Win32.AutoRun.gen	3,46%
10	HackTool.Win32.KMSAuto.c	3,21%
11	Virus.Win32.Sality.gen	3,16%
12	Trojan.Multi.Powecod.a	2,59%
13	Trojan.Win32.Starter.yy	2,21%
14	Worm.VBS.Dinihou.r	2,18%
15	Trojan.WinLNK.Agent.ew	2,14%
16	Trojan.Multi.StartPageTask.a	2,02%
17	Trojan.Multi.StartPageTask.b	1,94%
18	Trojan.Win32.Generic	1,94%
19	HackTool.Win32.Kiser.fnawf	1,69%
20	Trojan.Win32.Agentb.bqyr	1,58%

Estas estadísticas se basan en los veredictos de detección generados por los módulos de análisis durante acceso y a pedido en los equipos de usuarios de los productos de Kaspersky Lab que aceptaron compartir sus datos estadísticos.

El veredicto DangerousObject.Multi.Generic, que se refiere a malware detectado con la ayuda de tecnologías en la nube, ocupa el primer lugar (35,87%). Las tecnologías en la nube funcionan cuando las bases de datos antivirus todavía no contienen las firmas o heurísticas para detectar un programa malicioso, pero la base de datos en la nube de la compañía ya tiene información sobre el objeto. De hecho, los más recientes programas maliciosos se detectan de esta manera.

La proporción total del malware para Win32 disminuyó debido al correspondiente incremento de detecciones de otras plataformas de scripts.

Trojan.Script.Generic ocupó el segundo lugar. Su porcentaje disminuyó debido a que este año algunos representantes de esta detección se clasificaron como menos genéricos.

Existen variantes propagadas del malware WinLNK, que ocupan las posiciones 5°, 7° y 15° en nuestro TOP 20. Este programa malicioso está diseñado para cambiar la configuración del navegador o para descargar las siguientes etapas de la infección.

El 12° lugar le corresponde a un debutante: Trojan.Multi.Powecod.a (2,59%). Este programa malicioso usa PowerShell en una variedad de acciones maliciosas.

*Veredictos de detección de programas maliciosos generados por los módulos de análisis al acceso y a pedido en los equipos de usuarios de los productos de Kaspersky Lab que aceptaron compartir sus datos estadísticos.
** Proporción de usuarios individuales en cuyos equipos el módulo File Antivirus detectó estos programas en relación a todos los usuarios individuales de los productos de Kaspersky Lab en cuyos equipos se detectaron programas maliciosos.

PAÍSES EN LOS QUE LOS USUARIOS ENFRENTAN EL MAYOR RIESGO DE INFECCIONES LOCALES.

Para cada país, calculamos la cantidad de detecciones del componente file antivirus que los usuarios enfrentaron durante el año. Los datos incluyen programas maliciosos localizados en los equipos de los usuarios o en medios extraíbles conectados a equipos, como unidades USB, tarjetas de memoria de cámaras o teléfono, y unidades de disco duro externas. Estas estadísticas reflejan la proporción de equipos infectados en países de todo el mundo.

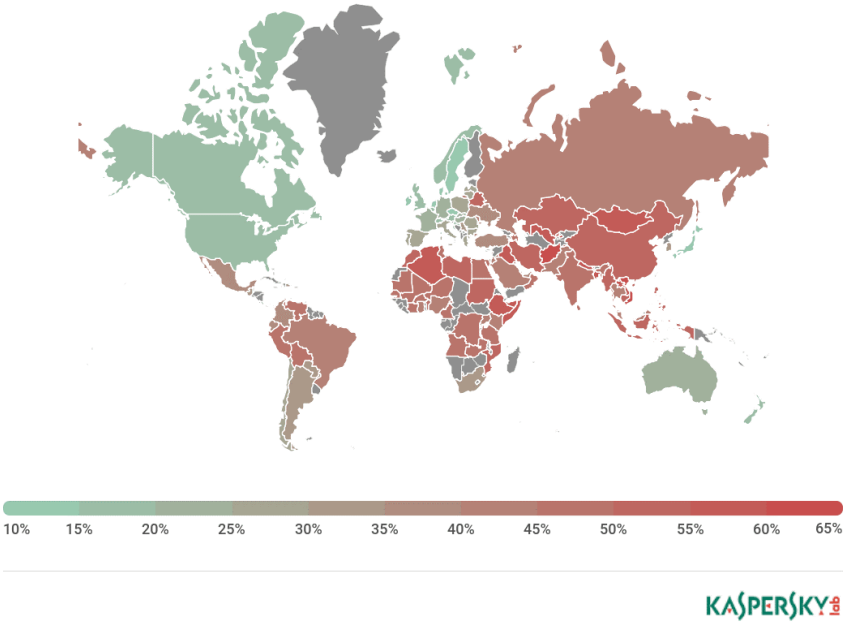
TOP 20 de países con mayor nivel de infección

	País*	% de usuarios únicos**
1	Vietnam	**67,41**
2	Afganistán	**63,03**
3	Argelia	**61,36**
4	Laos	**61,08**
5	Mongolia	**60,67**
6	Uzbekistán	**58,86**
7	Ruanda	**58,42**
8	Irak	**58,39**
9	Etiopía	**58,35**
10	Bangladesh	**58,09**
11	Somalia	**57,78**
12	Nepal	**57,60**
13	Mozambique	**56,12**
14	Libia	**55,85**
15	Camboya	**55,79**

	País*	% de usuarios únicos**
16	Kazajistán	**54,87**
17	Sudán	**54,76**
18	Birmania	**54,73**
19	Indonesia	**53,92**
20	Marruecos	**53,48**

Estas estadísticas se basan en los veredictos de detección generados por el antivirus de archivos, recibidos con el consentimiento de los usuarios de los productos de Kaspersky Lab.

* En los cálculos se han excluido los países con un número reducido de usuarios (menos de 50 000) de los productos de Kaspersky Lab.
** Porcentaje de usuarios únicos en el país con equipos que bloquearon amenazas locales de programas maliciosos en relación porcentual a determinados usuarios únicos de los productos de Kaspersky Lab.



Geografía de infecciones locales en 2017 (clasificadas según el porcentaje de usuarios atacados)

Los países pueden dividirse en varias categorías de riesgo que reflejan el nivel de las amenazas locales.

Riesgo máximo (más del 60%): cinco países entre los 20 principales.

Entre los países con **alto riesgo (40%-59,99%):** sobresalen: Uzbekistán (58,87%), Camboya (55,79%), Camerún (50,87%), Egipto (49,12%), Uganda (45,12%), Rusia (42,26%), Brasil (41,94%).

Entre los países con **riesgo moderado de infecciones (20%–39,99%)** figuran: Ucrania (39,84%), México (36,52%), Turquía (35,91%), Serbia (32,02%), Chile (28,67%), Grecia (26%), Israel (24,4%), Hungría (21,96%).

El grupo de bajo riesgo (0-19,9%): Australia (19,55%), Singapur (15,5%), Japón (12,5%), Irlanda (10,25), Dinamarca (8,88%).

En 2017, al menos un programa malicioso se encontró en el 36,8% de equipos, unidades de disco duro o unidades extraíbles de los usuarios de KSN.

KASPERSKY lab