Boletín de seguridad Kaspersky, 2019

Estadísticas

kaspersky

Contenido

Todos los datos estadísticos utilizados en este informe se obtuvieron de la red de nube global Kaspersky Security Network (KSN), que recibe información enviada por varios de los componentes de nuestras soluciones de seguridad. Dichos datos provienen de los usuarios que dieron su consentimiento para transferirlos a KSN. Millones de usuarios de productos Kaspersky en 203 países y territorios de todo el mundo participan en este intercambio global de información sobre actividades maliciosas. Las estadísticas recopiladas cubren el período comprendido entre noviembre de 2018 y octubre de 2019 inclusive.

Cifras del año

- Durante el año, el 19,8% 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 neutralizaron **975 491 360** ataques lanzados desde recursos de Internet ubicados en diversos países del mundo.
- Se registraron **273 782 113** URL únicas que provocaron reacciones del antivirus web.
- Nuestro antivirus web registró **24 610 126** objetos maliciosos únicos.
- Los ataques de cifrado se reflejan en **755 485** equipos de usuarios únicos.
- Durante el período abarcado por este informe, los criptomineros atacaron a **2 259 038** usuarios únicos.
- En **766 728** equipos de los usuarios se neutralizaron intentos de ejecución de programas maliciosos diseñados para robar dinero mediante el acceso en línea a cuentas bancarias.

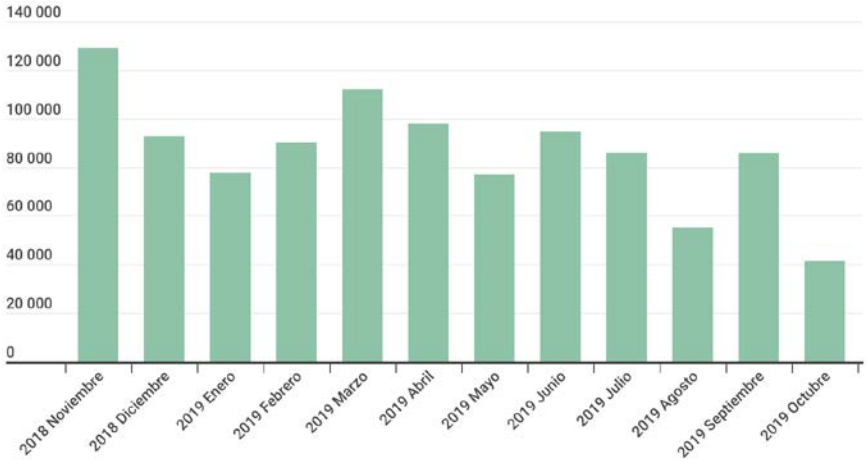
Las estadísticas sobre amenazas móviles se presentarán en el informe "Virología móvil 2019"

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 el periodo abarcado por este informe, las soluciones de Kaspersky neutralizaron intentos de ataques de uno o más programas maliciosos diseñados para robar dinero de cuentas bancarias en **766 728** equipos de usuarios.

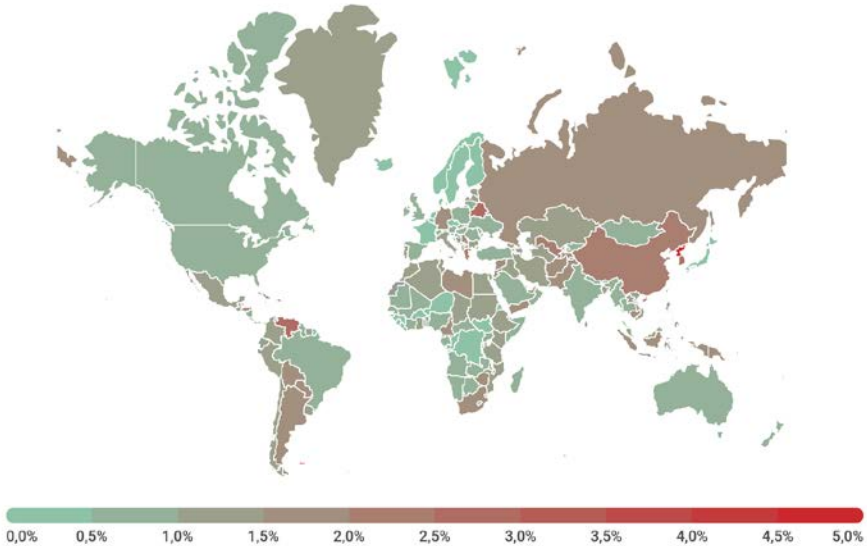


Número de usuarios atacados por malware financiero, noviembre de 2018 – octubre de 2019

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 que se vieron afectados por esta amenaza durante el trimestre, del total de usuarios de nuestros productos en ese país.

kaspersky



Geografía de los ataques de malware bancario, noviembre de 2018 – octubre de 2019

TOP 10 de países por el porcentaje de usuarios atacados

	País*	%**
1	Bielorrusia	2,8
2	Corea del Sur	2,6
3	Venezuela	2,6
4	China	2,4
5	Grecia	2,1
6	Islas Maldivas	2,0
7	Uzbekistán	2,0
8	Camerún	1,9
9	Serbia	1,9
10	Afganistán	1,8

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

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

TOP 10 de familias de malware bancario

TOP 10 de familias de malware utilizado para atacar a clientes de banca en línea.

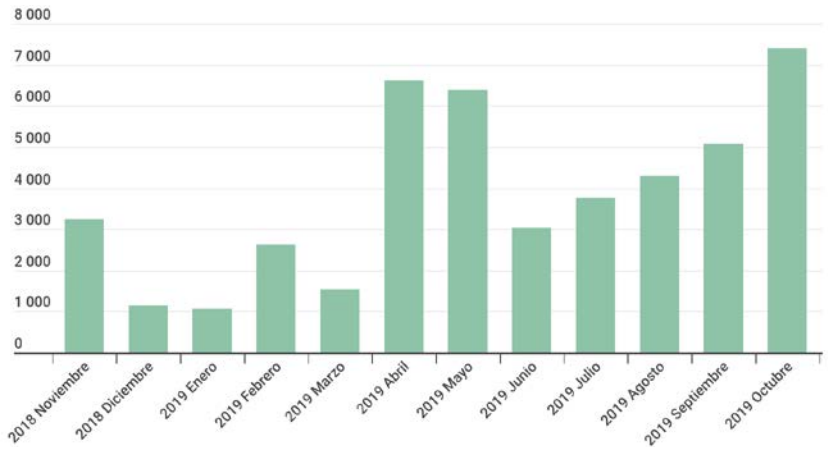
	Nombre	%*
1	Trojan.Win32.Zbot	23,10
2	Trojan-Banker.Win32.RTM	21,60
3	Backdoor.Win32.Emotet	12,30
4	Backdoor.Win32.SpyEye	7,10
5	Trojan.Win32.Nymaim	5,80
6	Trojan-Banker.Win32.Trickster	4,80
7	Trojan-Banker.Win32.Ramnit	4,40
8	Trojan.Win32. Neurevt	3,10
9	Trojan-Banker.Win32.CliptoShuffler	1,90
10	Trojan-Banker.Win32.Danabot	1,30

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

kaspersky

Programas cifradores maliciosos

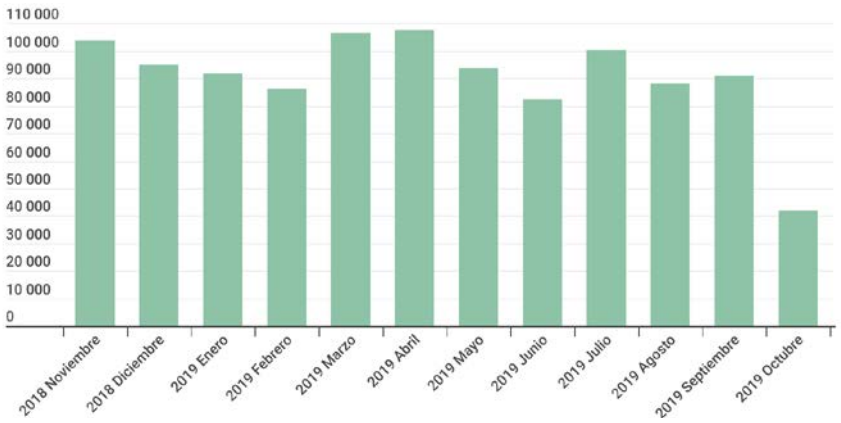
Durante el período del informe, identificamos más de **46 156** modificaciones criptográficas y descubrimos **22** nuevas familias Cabe destacar que no hemos creado una nueva familia para cada nuevo cifrador. Por el contrario, a la mayoría de las amenazas de este tipo les asignamos un veredicto genérico, que utilizamos cuando encontramos ejemplares nuevos y desconocidos.



Número de nuevas modificaciones de cifradores, noviembre de 2018 – octubre de 2019

Número de usuarios atacados por troyanos cifradores

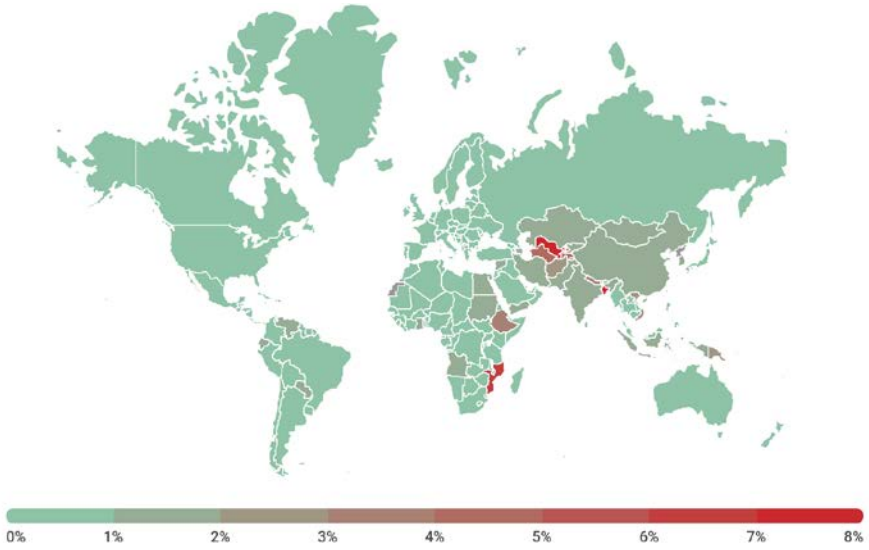
Durante el período abarcado por el informe, los troyanos cifradores atacaron a **755 485** equipos de usuarios únicos, de los cuales 209 679 son corporativos (excluyendo PYMES) y 22 440 son PYMES.



Número de usuarios atacados por troyanos cifradores, noviembre de 2018 – octubre de 2019

kaspersky

Geografía de los ataques



Geografía de los ataques de troyanos cifradores, noviembre de 2018 – octubre de 2019

TOP 10 de países afectados por ataques de troyanos cifradores

	País*	%**
1	Bangladesh	13,78
2	Uzbekistán	7,20
3	Mozambique	6,08
4	Turkmenistán	4,23
5	Etiopía	3,97
6	Nepal	3,86
7	Afganistán	2,45
8	Vietnam	2,34
9	China	1,94
10	India	1,91

* Hemos excluido de los cálculos a los países donde el número de usuarios de Kaspersky es relativamente bajo (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 en el país.

TOP 10 de las familias más difundidas de troyanos cifradores

	Nombre	Veredicto	%*
1	WannaCry	Trojan-Ransom.Win32.Wanna	23,56
2	(generic verdict)	Trojan-Ransom.Win32.Phny	16,81
3	GandCrab	Trojan-Ransom.Win32.GandCrypt	12,17
4	(generic verdict)	Trojan-Ransom.Win32.Gen	6,26
5	(generic verdict)	Trojan-Ransom.Win32.Crypmod	5,08
6	(generic verdict)	Trojan-Ransom.Win32.Encoder	4,65
7	Shade	Trojan-Ransom.Win32.Shade	2,66
8	PolyRansom/ VirLock	Virus.Win32.PolyRansom Trojan-Ransom.Win32.Win32.PolyRansom	2,43
9	(generic verdict)	Trojan-Ransom.Win32.Crypren	2,28
10	Stop	Trojan-Ransom.Win32.Stop	1,94

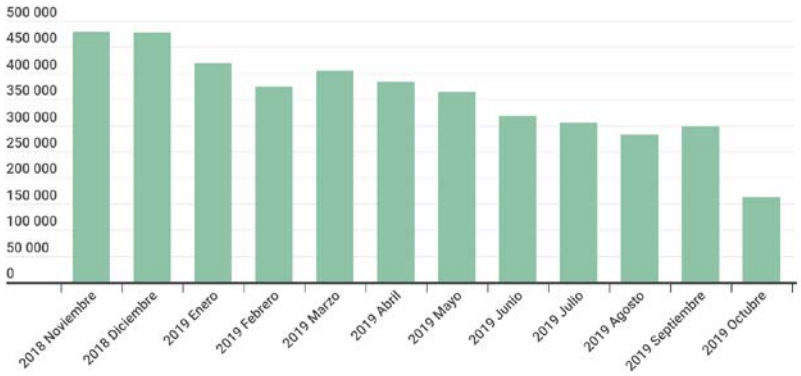
* Porcentaje de usuarios únicos de Kaspersky que sufrieron ataques de una familia específica de troyanos extorsionadores, del total de usuarios víctimas de ataques lanzados por troyanos extorsionadores.

kaspersky

Criptomineros

Número de usuarios atacados por malware de criptominería

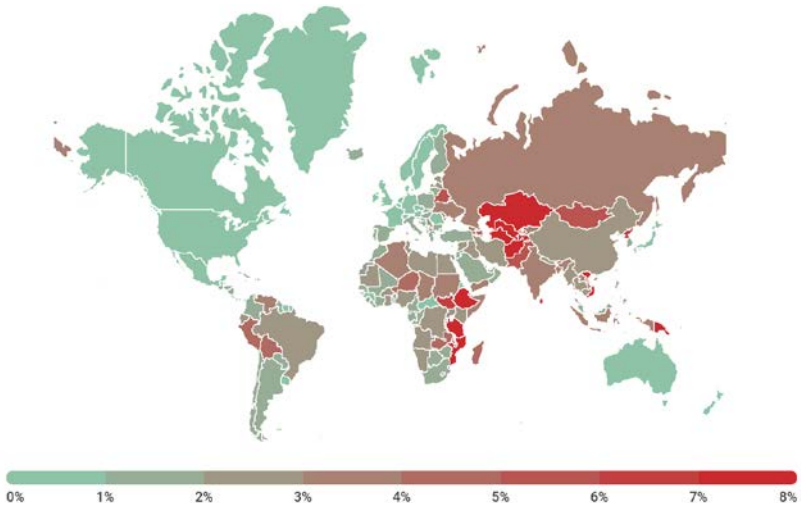
Durante el período cubierto por este informe, registramos intentos de instalar criptomineros en los equipos de **2 259 038** usuarios únicos. En el volumen total de ataques, la proporción de criptomineros fue del 3,64%, y entre los programas del tipo Risktool, del 6,94%.



Número de usuarios atacados por los criptomineros, noviembre de 2018 – octubre de 2019

Los productos de Kaspersky detectaron con mayor frecuencia Trojan.Win32.Miner.bbb: que representó el 13,45% del número total de usuarios atacados por mineros. Le siguen Trojan.Win32.Miner.ays (11,35%), Trojan.JS.Miner.m (11,12%) y Trojan.Win32.Miner.gen (9,32%).

Geografía de los ataques



Geography of miners attacks, November 2018 – October 2019

kaspersky

Aplicaciones vulnerables utilizadas por los ciberdelincuentes en sus ataques

El período descrito en este informe se caracterizó por una gran cantidad de ataques selectivos que utilizaban exploits para vulnerabilidades de día cero. A lo largo del año, los expertos de Kaspersky hicieron los siguientes descubrimientos:

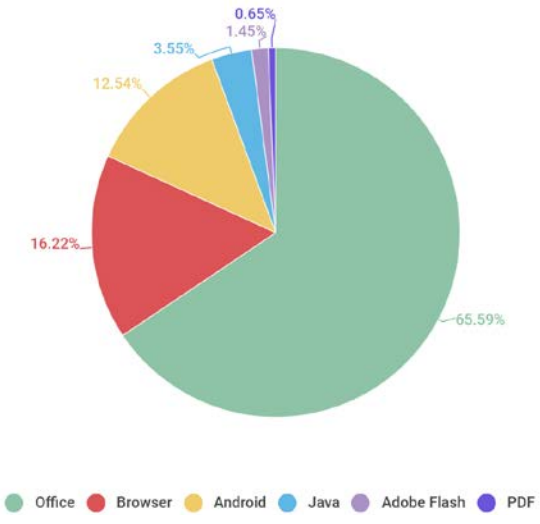
- La vulnerabilidad CVE-2018-8611, corregida en el parche de diciembre, que fue utilizada por varios grupos de hackers, como FruityArmor y SandCat. En el momento en que se descubrió el exploit para esta vulnerabilidad, FruityArmor ya era un grupo bastante conocido, con un historial de uso de exploits de día cero; SandCat, por el contrario, era un grupo relativamente nuevo. La vulnerabilidad encontrada era muy grave, porque permitía obtener privilegios de sistema y ejecutar códigos a nivel de núcleo en todas las versiones de los sistemas operativos Windows, incluso la última versión de Windows 10 RS4 en el momento del descubrimiento. Además, la vulnerabilidad se encontraba en el controlador Kernel Transaction Manager, que permitía que el exploit evadiera los entornos de ejecución aislada de los navegadores web.
- La vulnerabilidad CVE-2019-0797 se descubrió en febrero y se corrigió en el parche de marzo. Al igual que la anterior vulnerabilidad CVE-2018-8611, la nueva vulnerabilidad podría haber sido explotada por varios grupos, entre ellos FruityArmor y SandCat. Esta vulnerabilidad ocupó el cuarto lugar entre las vulnerabilidades de día cero más explotadas descubiertas por Kaspersky durante el primer semestre del año. Al igual que las vulnerabilidades descubiertas anteriormente, se la utilizaba para elevar los derechos del usuario en el sistema operativo Windows, pero a diferencia de CVE-2018-8611, el componente vulnerable era el controlador win32k.sys responsable de los gráficos y la interfaz.
- En marzo, se descubrió la vulnerabilidad CVE-2019-0859, que fue explotada activamente y que permite elevar los derechos de Windows debido a otro error en el controlador win32k.sys. Una carga útil bastante específica provista con el código shell es indicio de que el exploit fue utilizado por uno de los grupos cibercriminales que tienen como blanco al sector financiero.
- La vulnerabilidad CVE-2019-13720 se descubrió a fines de octubre después de una serie de ataques contra las nuevas versiones de Google Chrome. Después de que informamos a Google sobre esta vulnerabilidad explotada activamente, la compañía lanzó la versión actualizada del navegador Chrome 78.0.3904.87. Dimos a estos ataques el nombre Operation WizardOpium, ya que, a pesar de haber notado algunas similitudes en el código, no pudimos establecer una conexión exacta con otros grupos.

El número total de exploits de día cero utilizados activamente en 2019, y que descubrimos junto con colegas de otras compañías antivirus, fue mayor que el año anterior.

Durante el período cubierto por este informe, observamos una disminución en el número de exploits para las vulnerabilidades de Adobe Flash Player, cuya fecha de finalización de soporte está fijada para fines del próximo año. La proporción de exploits para navegadores web también ha disminuido ligeramente, a pesar de la aparición de varias vulnerabilidades de día cero explotadas públicamente. Lo mismo puede decirse de la proporción de exploits para Android en este período: disminuyó hasta alcanzar el 12%. Por el contrario, la proporción de exploits para PDF ha aumentado ligeramente.

Durante el último período del informe, vimos un rápido aumento del número de usuarios atacados por exploits para Microsoft Office: al llegar el cuarto trimestre de 2018, los exploits para esta suite de aplicaciones se han convertido en líderes por el número de ataques. Durante el periodo de estudio, Microsoft Office sigue siendo el líder entre las aplicaciones atacadas con mayor frecuencia. Pero a diferencia de años anteriores, este año el arsenal de los atacantes no sufrió grandes cambios, y las vulnerabilidades más utilizadas siguen siendo CVE-2017-11882, CVE-2018-0802, CVE-2017-8570 y CVE-2017-0199. A pesar de la ausencia de cambios notables en el arsenal de exploits, los atacantes siguen encontrando nuevas técnicas para ofuscar documentos y eludir las técnicas de detección estática, pero este tema en su integridad está detallado en un artículo aparte en Securelist.

La clasificación de las aplicaciones vulnerables se basa en los veredictos asignados por los productos de Kaspersky 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.



Distribución de exploits utilizados en los ataques lanzados por los ciberdelincuentes, por tipo de aplicaciones atacadas, noviembre de 2018 – noviembre de 2019

kaspersky

En el periodo en cuestión, los ataques de red siguieron siendo uno de los tipos de ataques más comunes. Podemos decir con certeza que 2019 será recordado por el descubrimiento de múltiples vulnerabilidades en el subsistema de escritorio remoto para varias de las versiones de sistemas operativos Windows. A estas vulnerabilidades se les ha asignado los nombres BlueKeep y DejaBlue. Por el momento, no observamos que estas vulnerabilidades se estén explotando de forma generalizada, lo que puede explicarse por la complejidad de este proceso. Entre los primeros lugares de los ataques de red, como en años anteriores, hay diversas variaciones de exploits para vulnerabilidades en el protocolo SMB, conocidas como EternalBlue, EternalRomance, etc. Tampoco podemos dejar de mencionar que una gran parte del tráfico de red malicioso se compone de solicitudes destinadas a averiguar contraseñas de servidores y servicios de red populares, como el Protocolo de escritorio remoto y el Microsoft SQL Server, respectivamente.

Ataques a través de recursos web

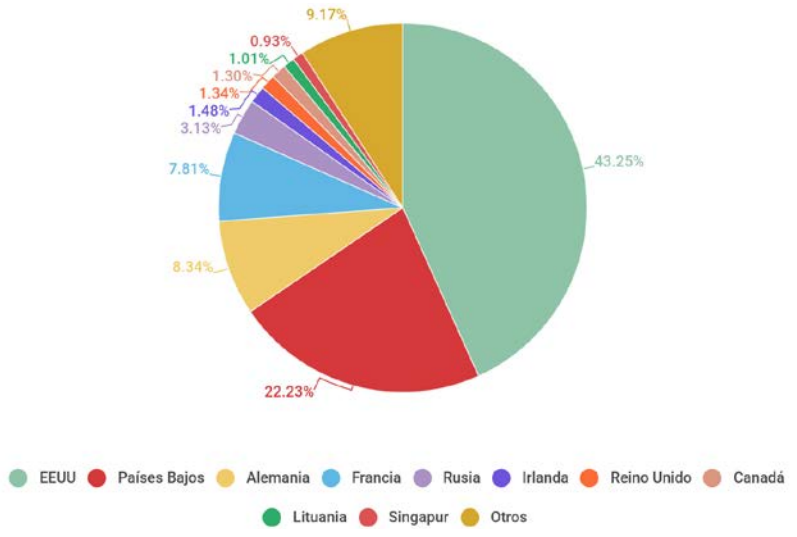
Los datos estadísticos de este capítulo han sido recopilados por el antivirus web, que impide que los usuarios descarguen objetos maliciosos de una página web maliciosa o infectada. Los delincuentes crean sitios maliciosos a propósito, pero también los sitios legítimos se pueden infectar cuando son los 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. 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).

Durante el periodo cubierto por este informe, las soluciones de Kaspersky neutralizaron **975 491 360** ataques lanzados desde recursos de Internet ubicados en diversos países del mundo. Al mismo tiempo, el 90,83% del número total de estos recursos de Internet se concentra en solo 10 países.



Distribución de fuentes de ataques web por países, noviembre 2018 – octubre 2019

kaspersky

En comparación con los resultados del año anterior, la distribución de las fuentes de ataques web no ha cambiado mucho. En primer lugar se ubica Estados Unidos (43,25%), seguido de Países Bajos (22,23%) y Alemania (8,34%).

Países donde los usuarios estuvieron bajo mayor riesgo de infección 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 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 solo 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, 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 **78%** de los equipos de usuarios en los que se activó el antivirus web.

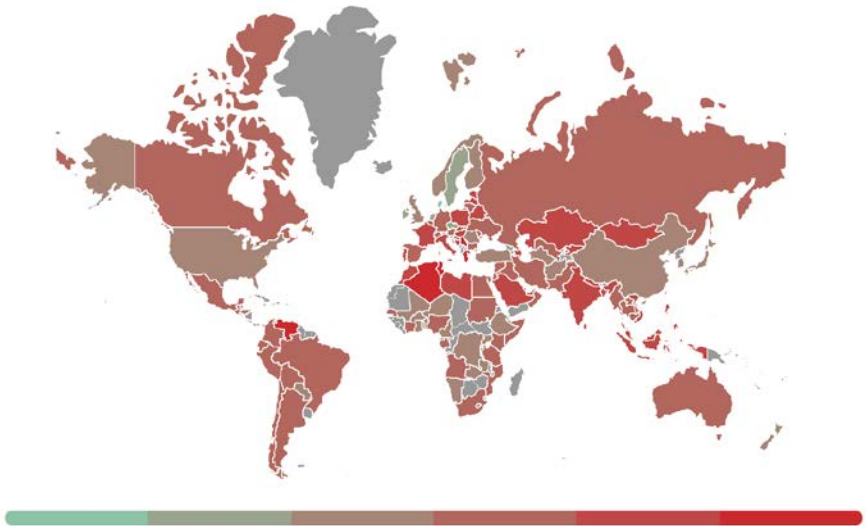
TOP 20 de países donde los usuarios han estado bajo mayor riesgo de infectarse mediante Internet

	País*	%**
1	Argelia	33,02
2	Venezuela	30,25
3	Túnez	29,50
4	Grecia	26,07
5	Serbia	25,80
6	Bangladesh	24,95
7	Moldavia	24,78
8	Azerbaiyán	24,74
9	Bielorrusia	24,52
10	Polonia	24,13
11	Mongolia	24,05
12	Filipinas	23,89
13	Marruecos	23,87
14	Letonia	23,22
15	Catar	22,94
16	Vietnam	22,57
17	Taiwán, Provincia de China	22,13
18	Francia	21,99
19	Portugal	21,97
20	Italia	21,96

* En los cálculos hemos excluido a los países en los que la cantidad de usuarios de Kaspersky 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 en el país

En promedio, en el periodo de este informe el **19,8%** de los equipos de los usuarios de Internet en el mundo al menos una vez fueron objeto de un ataque web mediante software de clase Malware.



Geografía de los ataques de malware web, noviembre de 2018 – octubre de 2019

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

Durante el período cubierto por este informe, el antivirus web de Kaspersky detectó **24 610 126** objetos maliciosos únicos (scripts, exploits, archivos ejecutables, etc.) y **273 782 113** URL maliciosas únicas que activaron 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	Malicious URL	85,40
2	Trojan.Script.Generic	5,89
3	Trojan.Script.Miner.gen	3,89
4	Trojan-Clicker.HTML.Iframe.dg	0,65
5	Trojan.BAT.Miner.gen	0,26
6	Trojan-Downloader.JS.Inor.a	0,22
7	Trojan.PDF.Badur.gen	0,21
8	DangerousObject.Multi.Generic	0,21
9	Trojan-Downloader.Script.Generic	0,17
10	Trojan-PSW.Script.Generic	0,15
11	Trojan.Script.Agent.gen	0,15
12	Hoax.HTML.FraudLoad.m	0,13
13	Exploit.Script.Generic	0,08

	Veredicto	%*
14	Trojan.Script.Agent.bg	0,07
15	Trojan.Multi.Preqw.gen	0,06
16	Exploit.MSOffice.CVE-2017-11882.gen	0,06
17	Trojan-Downloader.JS.SLoad.gen	0,05
18	Hoax.Script.Loss.gen	0,05
19	Trojan.JS.Miner.m	0,05
20	Trojan-Downloader.VBS.SLoad.gen	0,04

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

A pesar de que en el TOP 20 hay algunos veredictos relacionados con los criptomineros para páginas web, la cantidad de detecciones de criptomineros escritos en JavaScript y de intentos de conectarse a sitios de criptominería web ha disminuido bastante en comparación con 2018. Esto se reflejó en el número total de detecciones web y en el porcentaje de veredictos del tipo Malicious URL. Este veredicto se basa en el contenido de nuestra lista negra, que contiene enlaces a páginas web que desvían al usuario hacia exploits, sitios con exploits y otros programas maliciosos, centros de control de botnets, etc.

Amenazas locales

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

En esta sección, analizamos 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 se detectaron con mayor frecuencia en los equipos de los usuarios en el periodo abarcado por este informe Esta clasificación no incluye programas del tipo Riskware ni programas publicitarios.

	Veredicto	%*
1	DangerousObject.Multi.Generic	26,43
2	Trojan.Multi.BroSubsc.gen	9,48
3	Trojan.Script.Generic	6,19
4	Trojan.Multi.GenAutorunReg.a	5,94
5	HackTool.Win64.HackKMS.b	4,40
6	HackTool.MSIL.KMSAuto.by	3,69
7	HackTool.Win32.KMSAuto.bu	3,54
8	Trojan.WinLNK.Agent.gen	3,45
9	HackTool.MSIL.KMSAuto.a	3,43
10	Trojan.WinLNK.Starter.gen	3,42
11	HackTool.MSIL.KMSAuto.dh	2,83
12	HackTool.Win32.KMSAuto.c	2,75
13	HackTool.MSIL.KMSAuto.di	2,65
14	Trojan.Win32.Generic	2,53
15	HackTool.Win32.KMSAuto.cb	2,50
16	HackTool.Win64.HackKMS.c	2,47
17	HackTool.MSIL.KMSAuto.bx	2,18
18	Trojan.Win32.AutoRun.gen	1,93
19	Virus.Win32.Sality.gen	1,90
20	HackTool.Win32.KMSAuto.m	1,90

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

El primer lugar en nuestro TOP 20, como ya es tradición, lo ocupa el veredicto DangerousObject.Multi.Generic (26,43%), 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.

El segundo lugar fue ocupado por una amenaza relativamente nueva que se generalizó este año, Trojan.Multi.BroSubsc.gen (9,48%). El malware de esta familia se instala de forma encubierta en el navegador después de que la víctima ingresa a un sitio malicioso o publicitario. La tarea de Trojan.Multi.BroSubsc.gen es mostrar mensajes publicitarios incluso cuando el navegador de la víctima no se está ejecutando.

En general, durante el período del informe, notamos una disminución en la popularidad de los criptomineros, que hizo que este tipo de malware quedara fuera del TOP 20 de amenazas.

Países en que los equipos de los usuarios estuvieron expuestos a 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.

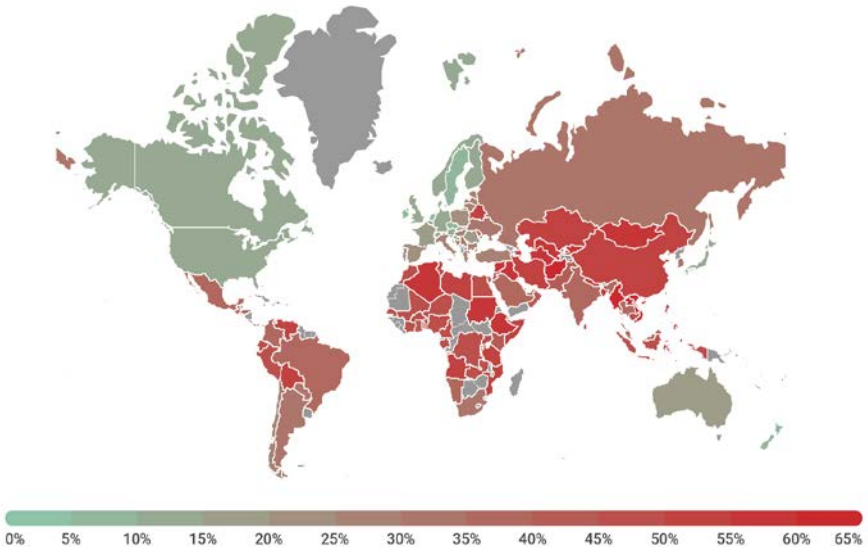
TOP 20 países según el riesgo de infección local

	País*	%**
1	Afganistán	65,55
2	Vietnam	61,84
3	Laos	61,95
4	Myanmar	60,80
5	Bangladesh	59,51
6	Mongolia	59,41
7	Uzbekistán	58,06
8	Turkmenistán	57,57
9	Argelia	57,50
10	Irak	57,33
11	Siria	57,04
12	Sudán	55,41
13	Kirguistán	55,15

* En los cálculos hemos excluido a los países donde la cantidad de usuarios de Kaspersky 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 en el país.

	País*	%**
14	Etiopía	55,08
15	Bolivia	54,85
16	China	54,64
17	Nepal	54,57
18	Mozambique	54,52
19	Libia	54,36
20	Ruanda	54,14



Geografía de infecciones provocadas por malware local, noviembre de 2018 – octubre de 2019

En el periodo de este informe, 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.

kaspersky