
# Boletín de seguridad Kaspersky 2020. Estadísticas

kaspersky

# Contenido





kaspersky

# Cifras del año

- Durante el año, el 10,18% 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 **666 809 967** ataques lanzados desde recursos de Internet ubicados en diversos países del mundo.
- Registramos **173 335 902** URL maliciosas únicas en las que se activó el antivirus web.
- Nuestro antivirus web bloqueó **33 412 568** objetos maliciosos únicos.
- En los equipos de **549 301** usuarios se neutralizaron ataques de cifradores.
- Durante el período abarcado por el informe, los criptomineros atacaron a **1 523 148** usuarios únicos.
- En **668 619** 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 2020"**

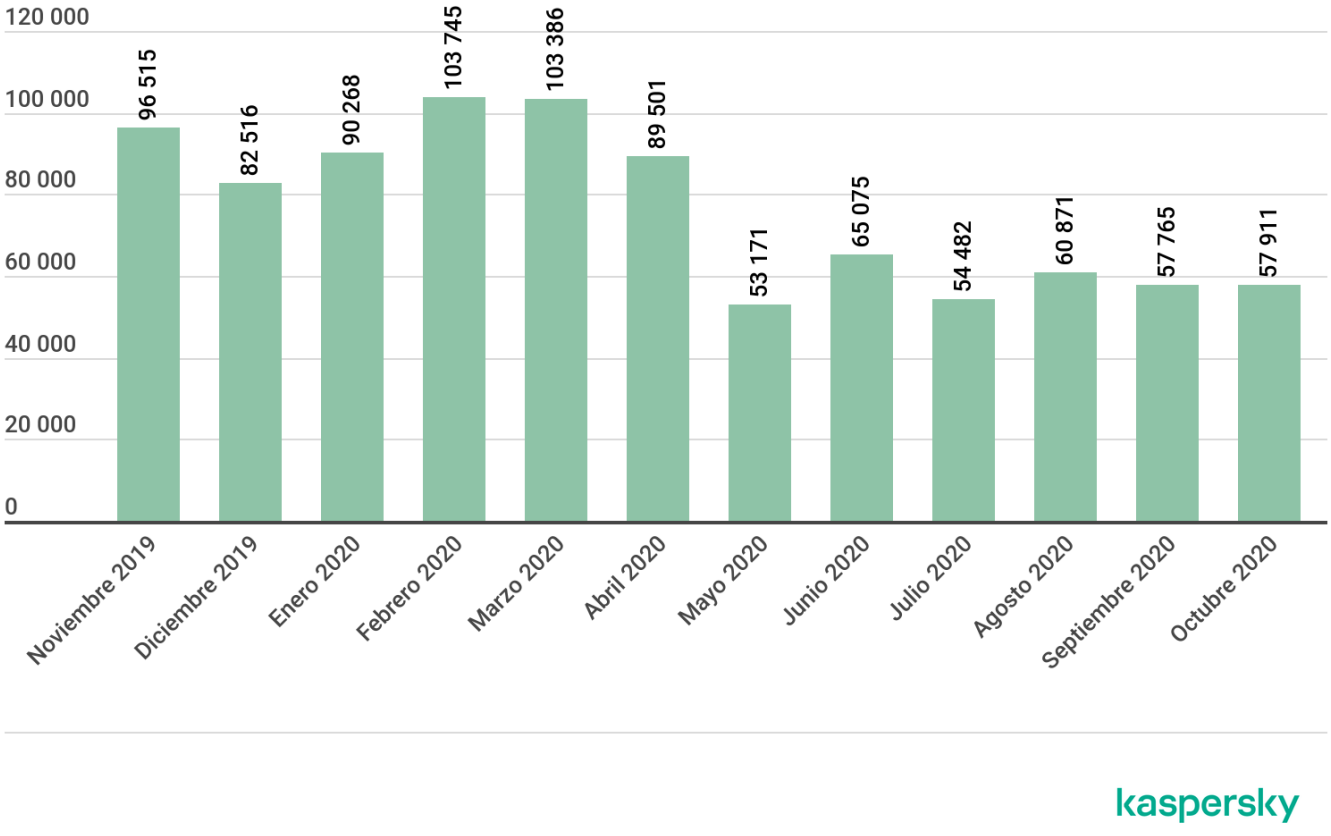
**Todos los datos estadísticos utilizados en este informe se obtuvieron de la red de nube global Kaspersky Security Network (KSN), que recibe información enviada por varios de los componentes de nuestras soluciones de seguridad. Dichos datos provienen de los usuarios que dieron su consentimiento para transferirlos a KSN. Millones de usuarios de productos Kaspersky de todo el mundo participan en el intercambio global de información sobre actividades maliciosas. Las estadísticas recopiladas cubren el período comprendido entre noviembre de 2019 y octubre de 2020, inclusive.**

# Amenazas financieras

**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 **668 619** equipos de los usuarios.



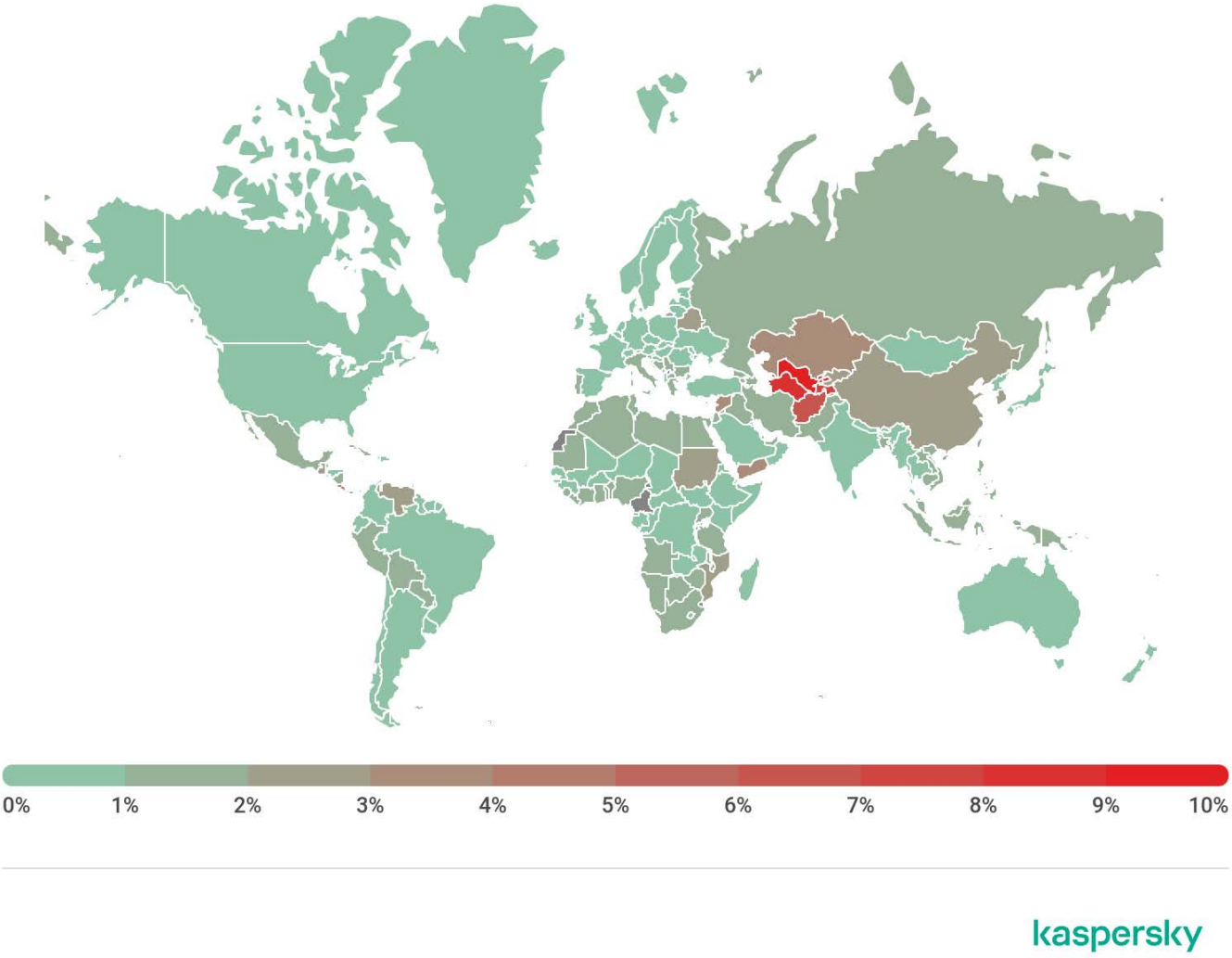

Número de usuarios atacados por malware financiero,
noviembre de 2019 - octubre de 2020



kaspersky

## Geografía de los ataques

Para evaluar y comparar el riesgo de infección con troyanos bancarios y programas maliciosos para cajeros automáticos y terminales de pago al que están expuestos los equipos de los usuarios en diferentes países del mundo, para cada uno de ellos hemos calculado el porcentaje de usuarios de productos de Kaspersky que se vieron afectados por amenazas financieras durante el trimestre, respecto al total de usuarios de nuestros productos en ese país.




**Geografía de los ataques de malware bancario, noviembre de 2019 - octubre de 2020**



kaspersky

### TOP 10 de países por el porcentaje de usuarios atacados

| | País* | %** |
|---|---|---|
| **1** | Uzbekistán | 10,4 |
| **2** | Turkmenistán | 8,6 |
| **3** | Tayikistán | 7,5 |
| **4** | Afganistán | 6,6 |
| **5** | Costa Rica | 4,0 |
| **6** | Yemén | 3,9 |
| **7** | Kazajistán | 3,5 |
| **8** | Siria | 3,3 |
| **9** | Guatemala | 2,8 |
| **10** | Corea del Sur | 2.7 |

* 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 financiero, del total de usuarios atacados por todos los tipos de malware.

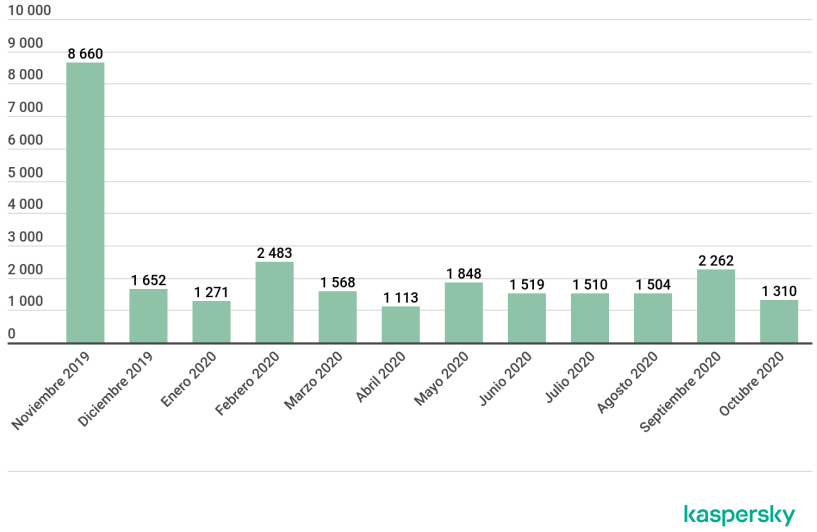
## TOP 10 familias de malware financiero

| | Nombre | %* |
|---|---|---|
| **1** | Zbot | 21,6 |
| **2** | Emotet | 15,1 |
| **3** | CliptoShuffler | 15 |
| **4** | RTM | 11,1 |
| **5** | Trickster | 5,1 |
| **6** | Nimnul | 4,2 |
| **7** | Neurevt | 3,3 |
| **8** | Danabot | 3,2 |
| **9** | SpyEye | 3,2 |
| **10** | Nymaim | 2,1 |

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

# Programas cifradores maliciosos

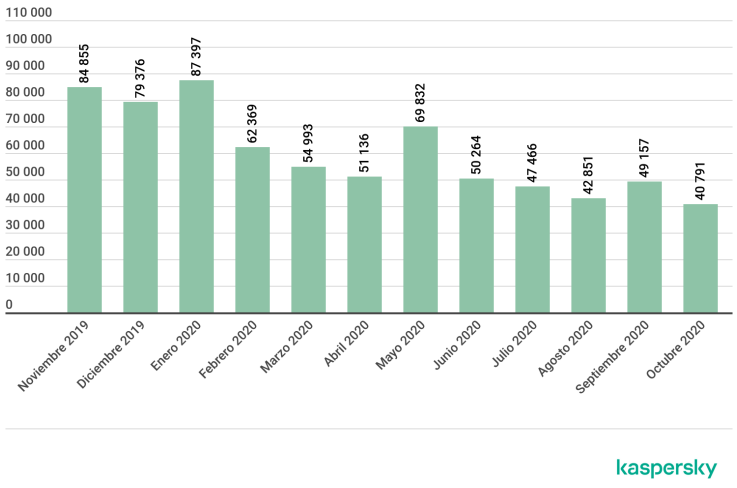
Durante el período del informe, identificamos más **26 700** modificaciones de ransomware y descubrimos **21** nuevas familias. Aquí vale la pena mencionar que no creamos una familia separada para cada nuevo ransomware. Por el contrario, a la mayoría de las amenazas de este tipo les asignamos un veredicto genérico, que utilizamos cuando encontramos ejemplares nuevos y desconocidos.




**Número de nuevas modificaciones de ransomware, noviembre de 2019 - octubre de 2020**

## Número de usuarios atacados por troyanos cifradores

Durante el período cubierto por el informe, los troyanos cifradores atacaron **549 301** usuarios únicos, entre ellos 123 630 usuarios corporativos, sin contar las PYMES, y 15 940 usuarios asociados con PYMES.

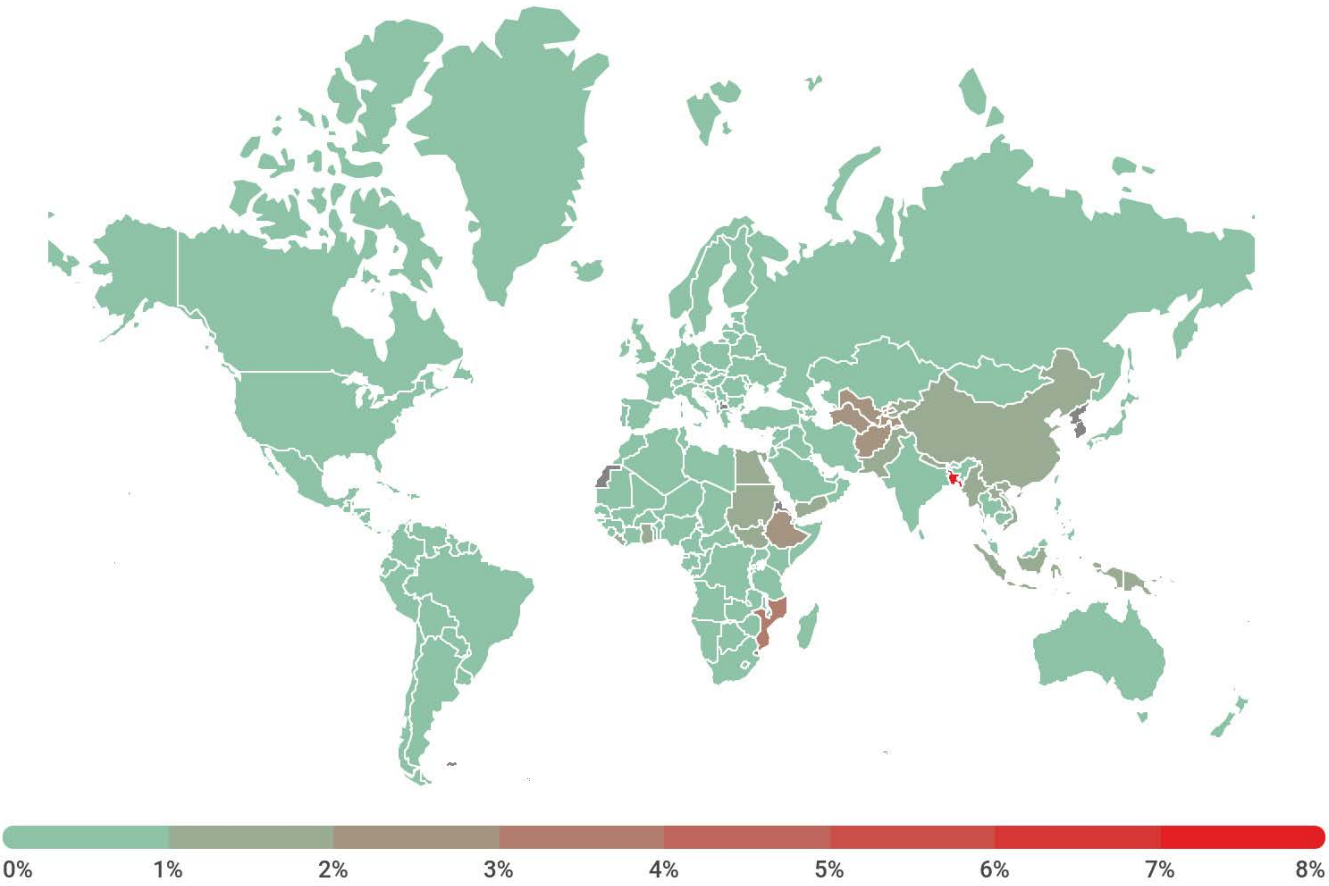



**Número de usuarios atacados por troyanos cifradores, noviembre de 2019 - octubre de 2020**



kaspersky

## Geografía de los ataques




Geografía de los ataques de troyanos cifradores,
noviembre de 2019 - octubre de 2020



kaspersky

### TOP 10 de países afectados por ataques de troyanos cifradores

| | País* | %** |
|---|---|---|
| 1 | Bangladesh | 8,12 |
| 2 | Mozambique | 3,13 |
| 3 | Turkmenistán | 2,65 |
| 4 | Haití | 2,47 |
| 5 | Uzbekistán | 2,39 |
| 6 | Etiopía | 2,10 |
| 7 | Afganistán | 2,06 |
| 8 | Nepal | 1,97 |
| 9 | Sudán | 1,92 |
| 10 | Kirguistán | 1,77 |

* 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

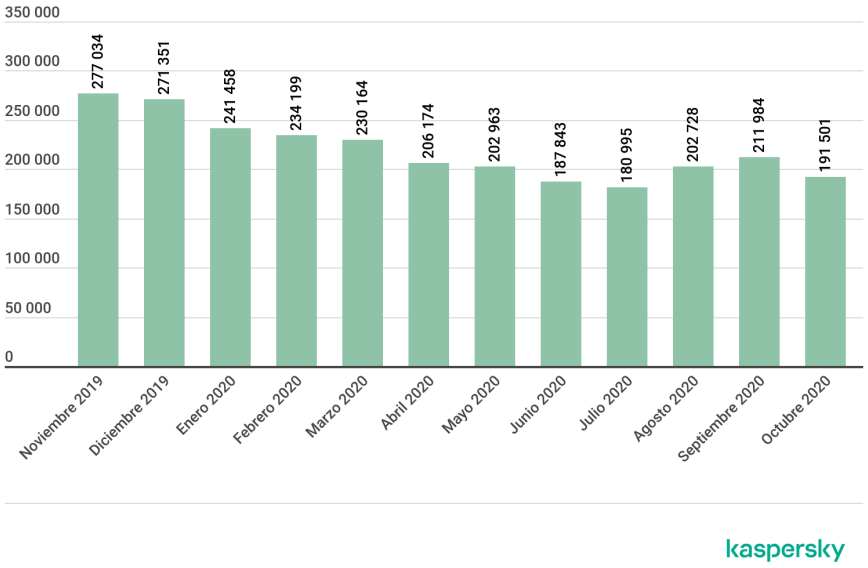
| | Nombre | Veredicto | %* |
|---|---|---|---|
| 1 | WannaCry | Trojan-Ransom.Win32.Wanna | 16,56 |
| 2 | (veredicto genérico) | Trojan-Ransom.Win32.Phny | 11,56 |
| 3 | (veredicto genérico) | Trojan-Ransom.Win32.Gen | 11,37 |
| 4 | Stop | Trojan-Ransom.Win32.Stop | 7,76 |
| 5 | (veredicto genérico) | Trojan-Ransom.Win32.Encoder | 6,66 |
| 6 | (veredicto genérico) | Trojan-Ransom.Win32.Generic | 4,77 |
| 7 | (veredicto genérico) | Trojan-Ransom.Win32.Crypren | 4,07 |
| 8 | PolyRansom/VirLock | Virus.Win32.PolyRansom<br>Trojan-Ransom.Win32.PolyRansom | 2,54 |
| 9 | Crysis/Dharma | Trojan-Ransom.Win32.Crusis | 2,21 |
| 10 | (veredicto genérico) | Trojan-Ransom.Win32.Crypmod | 1,83 |

* 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.

# Criptomineros

## Número de usuarios atacados por criptomineros

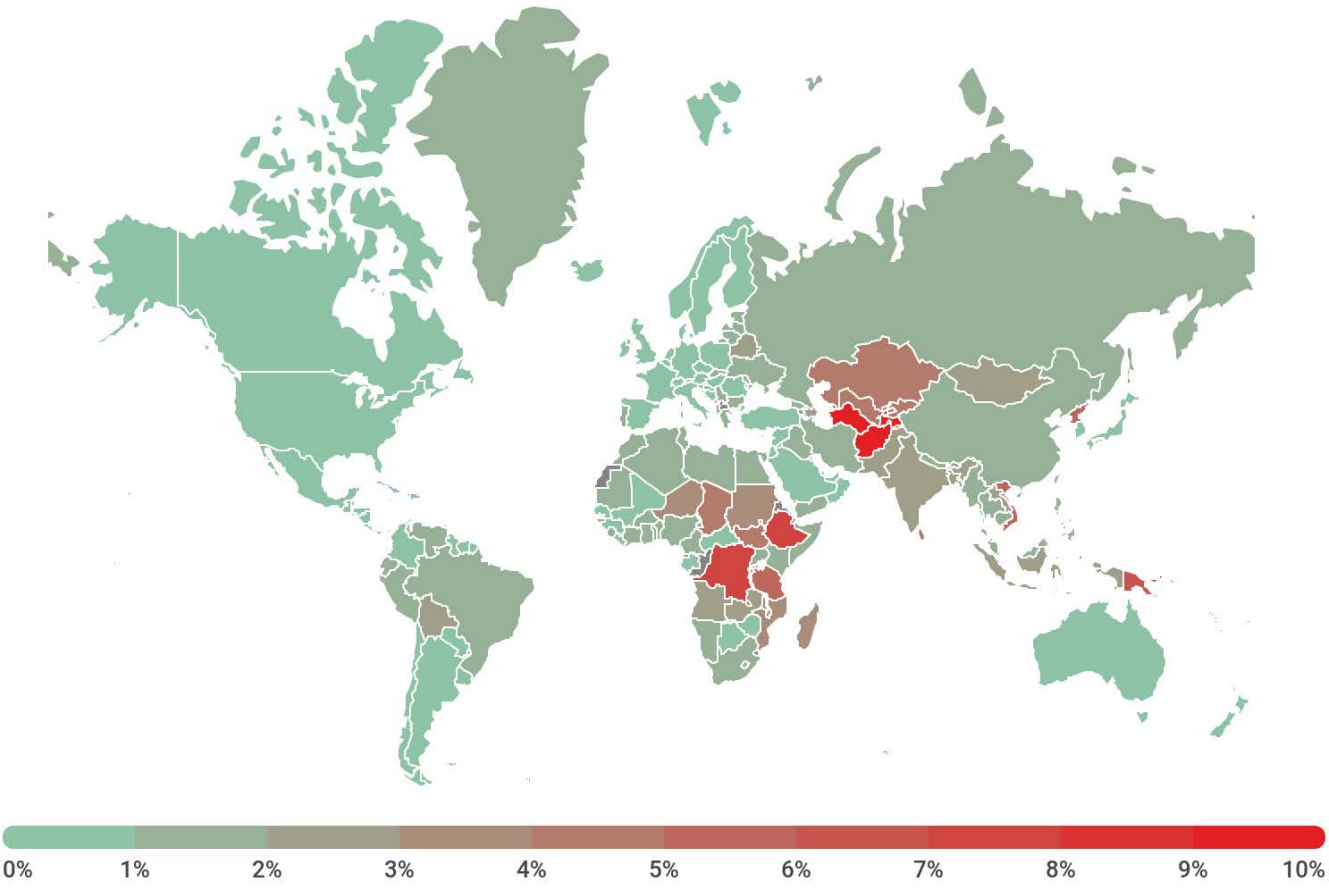
Durante el período del informe, detectamos intentos de instalar criptomineros en los equipos de **1 523 148** usuarios únicos. La participación de los criptomineros en el volumen total de ataques fue del 2,49%, y entre todos los programas del tipo Risktool, fue del 13,82%.




**Número de usuarios atacados por criptomineros, noviembre de 2019 - octubre de 2020**

Los productos de Kaspersky detectaron con mayor frecuencia a Trojan.Win32.Miner.bbb, que representó el 17,53% del número total de usuarios atacados por mineros. Le siguen Trojan.Win32.Miner.ays (10,86%), Trojan.JS.Miner.m (10,28%) y Trojan.Win32.Miner.gen (8,00%).

## Geografía de los ataques




Geografía de los ataques que involucran a criptomineros,
noviembre de 2019 - octubre de 2020



kaspersky

# Aplicaciones vulnerables utilizadas por los ciberdelincuentes en sus ataques

En 2020, los investigadores encontraron la mayoría de las vulnerabilidades antes de que los atacantes pudieran explotarlas. Sin embargo, el año no estuvo exento de vulnerabilidades de día cero. En particular, los expertos de Kaspersky descubrieron:

- La vulnerabilidad CVE-2020-1380, que es un posible escenario "use-after-free" en el componente Jscript9 del navegador Microsoft Internet Explorer, causado por controles insuficientes durante la generación del código JIT optimizado. Es probable que esta vulnerabilidad haya sido aprovechada por el grupo de APT DarkHotel en la primera etapa de irrupción en los sistemas, mientras que en las etapas siguientes, la carga útil estaba a cargo de un exploit adicional que aumentaba los privilegios en el sistema.
- La vulnerabilidad CVE-2020-0986 en el componente GDI Print/Print Spooler del sistema operativo Microsoft Windows, que permite manipular la memoria de un proceso para permitir la ejecución de códigos arbitrarios en el contexto de un proceso de servicio del sistema. La explotación de esta vulnerabilidad le da al atacante la capacidad de eludir el sandbox, por ejemplo, en el navegador.

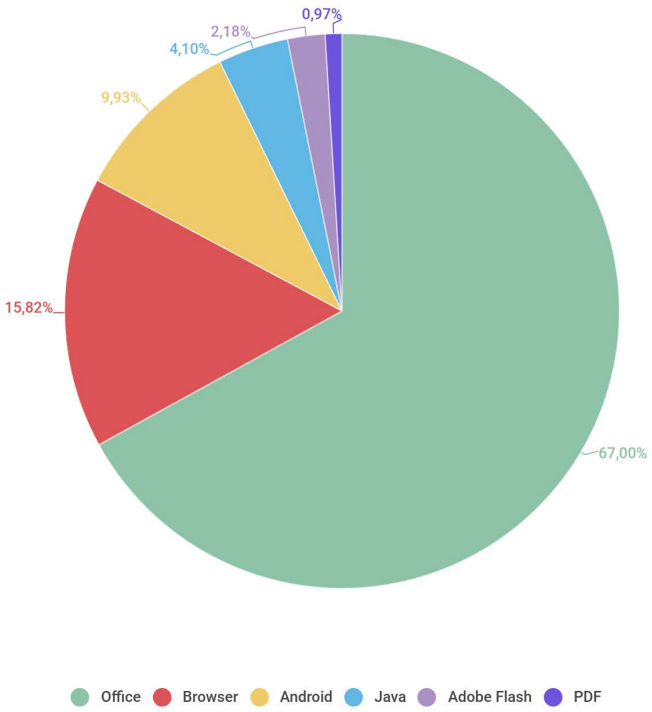
También vale la pena mencionar las vulnerabilidades encontradas por nuestros socios:

- Cuatro vulnerabilidades de día cero en Google Chrome: CVE-2020-16010, CVE-2020-16009, CVE-2020-15999 y CVE-2020-6418. Todas ellas se utilizaron para infectar sistemas y permitieron a los atacantes ejecutar códigos en el sistema de destino. Por ejemplo, la vulnerabilidad CVE-2020-15999 es un error en la popular biblioteca libfreetype2 que ocurre al procesar imágenes PNG incrustadas dentro de fuentes TrueType. En teoría, la explotación de la vulnerabilidad es posible en otros productos que utilizan esta biblioteca.
- Tres vulnerabilidades de día cero en Mozilla Firefox (CVE-2020-6820, CVE-2020-6819, CVE-2019-17026), que también permiten infectar los sistemas de los usuarios.
- Una vulnerabilidad de día cero en Microsoft Internet Explorer (CVE-2020-0674) supuestamente explotada por el grupo de APT DarkHotel. Consiste en un posible escenario "use-after-free", cuando el recolector de basura, en una situación determinada, dejaba de rastrear objetos pasados como argumentos a la función de devolución de llamada al usar la operación de clasificación de vectores.
- Cuatro vulnerabilidades de día cero en Microsoft Windows (CVE-2020-0938, CVE-2020-1020, CVE-2020-1027, CVE-2020-17087). CVE-2020-17087: un error en el controlador criptográfico del kernel, arraigado en una validación de entrada insuficiente al usar llamadas IOCTL desde el nivel de usuario, permitió a los atacantes pasar por alto el sandbox de Google Chrome e infiltrarse en el sistema.

Es probable que el próximo año tengamos noticias sobre los posibles autores y los instrumentos que explotaron estas vulnerabilidades.

Durante el período del informe, observamos una ligera disminución del número de ataques contra aplicaciones de Microsoft Office, pero esto no impidió que ocuparan el primer lugar en popularidad. Los atacantes siguieron modificando y ofuscando las vulnerabilidades CVE-2017-11882, CVE-2018-0802, CVE-2017-8570 y CVE-2017-0199 ya conocidas y por un tiempo eludieron los mecanismos de seguridad de algunas soluciones antivirus.

Este año es el final de la vida útil de Adobe Flash, pero nuestros datos muestran que el interés de los ciberdelincuentes no ha disminuido: el número de ataques que aprovechan los errores de Flash ha aumentado en 0,7 p.p. En el período del informe, los navegadores web se mantienen en el 11% y siguen siendo uno de los principales métodos para infectar los sistemas de usuarios desprotegidos. Los ataques a Android (9,93%) que utilizan vulnerabilidades se redujeron en 2,6 p.p. El número de exploits que explotan vulnerabilidades en la plataforma Java (4,10%) y vulnerabilidades en PDF (0,97%) ha cambiado ligeramente.




**Distribución de exploits utilizados en los ataques lanzados por los ciberdelincuentes, por tipo de aplicaciones atacadas, noviembre de 2019 - noviembre de 2020**

**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.**

Al igual que antes, los ataques de red fueron el método más extendido para penetrar sistemas en 2020. Una parte significativa son los ataques de fuerza bruta para varios servicios de red: RDP, MSSQL, etc. Además, el periodo cubierto por este informe nos mostró que en el sistema operativo Windows todo es cíclico y la mayoría de las vulnerabilidades descubiertas existen en los mismos servicios, por ejemplo, en los controladores de los protocolos de red SMB (SMBGhost, SMBBleed), DNS (SigRed) y ICMPv6 (BadNeighbor). Se encontraron dos vulnerabilidades críticas (CVE-2020-0609 y CVE-2020-0610) en el servicio Remote Desktop Gateway. También se descubrió una vulnerabilidad interesante en el servicio de red NetLogon, que recibió el nombre de Zerologon. Y para finalizar, a pesar de que los exploits de las familias EternalBlue y EternalRomance son ya antiguas, los ciberdelincuentes las siguen utilizando.

# Ataques a macOS

Durante el período del informe, no solo detectamos la ausencia de modificaciones de malware ya conocido para macOS, sino también varias amenazas nuevas. Entre ellos hay dos puertas traseras: Capip y Lador. Este último es particularmente digno de mención porque está escrito en el lenguaje Go y su tamaño es de 5,5 megabytes, muchas veces más grande que un malware similar escrito en Objective C. También es de interés el ransomware autorreplicante Virus.OSX.ThifQseut.a, también conocido como EvilQuest.

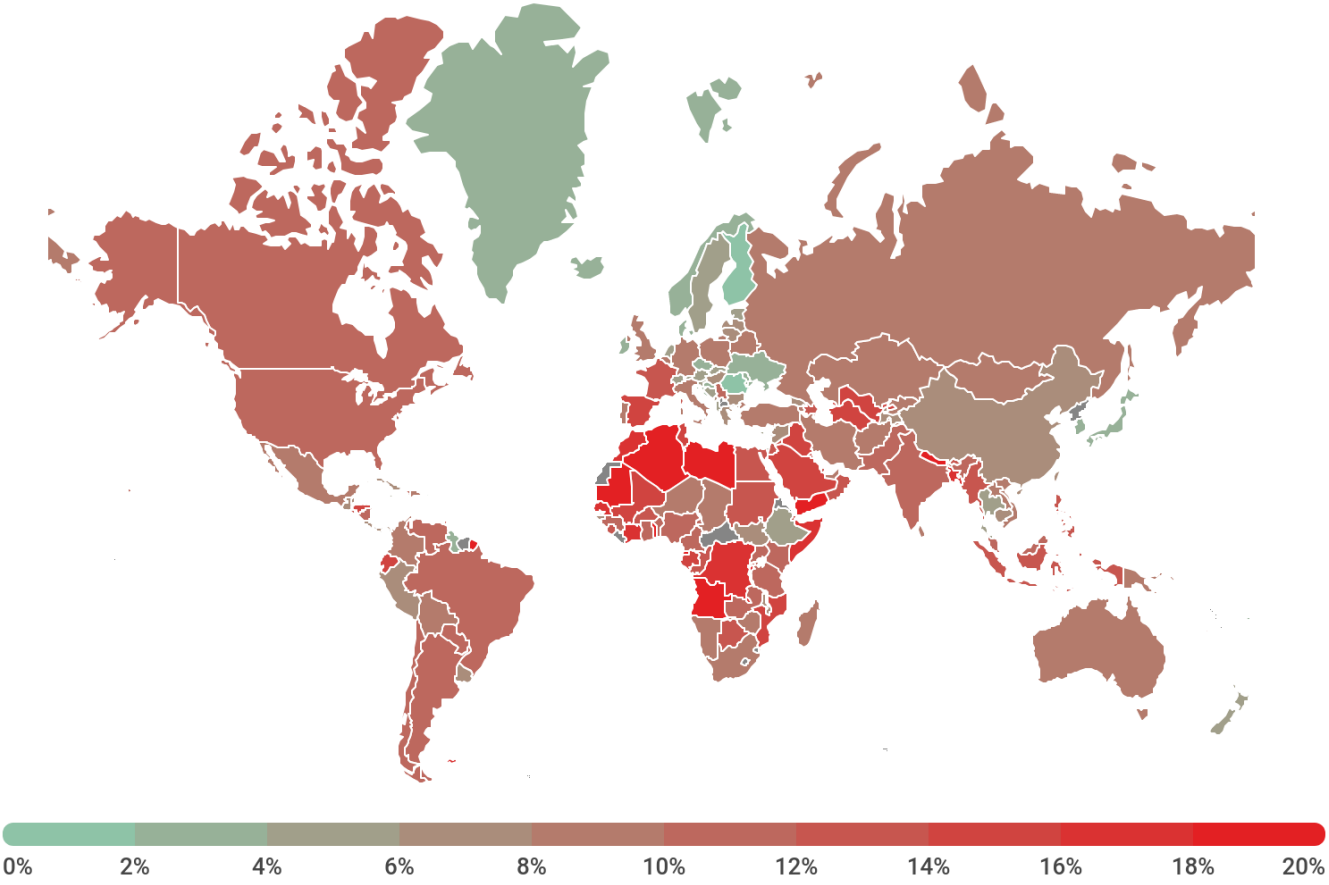
**TOP 20 de amenazas para macOS**

| | Veredicto | %* |
|---|---|---|
| **1** | Trojan-Downloader.OSX.Shlayer.a | 17,27 |
| **2** | Monitor.OSX.HistGrabber.b | 9,10 |
| **3** | AdWare.OSX.Pirrit.j | 8,08 |
| **4** | AdWare.OSX.Cimpli.k | 6,99 |
| **5** | AdWare.OSX.Pirrit.x | 6,93 |
| **6** | AdWare.OSX.Bnodlero.at | 6,33 |
| **7** | AdWare.OSX.Pirrit.o | 5,41 |
| **8** | AdWare.OSX.Ketin.h | 5,33 |
| **9** | AdWare.OSX.Bnodlero.t | 5,14 |
| **10** | AdWare.OSX.Spc.a | 4,95% |

* Porcentaje de usuarios únicos que se toparon con este programa malicioso, del total de los usuarios de las soluciones de protección de Kaspersky para macOS.

La mayor parte de nuestro TOP 10 durante el período del informe lo ocupan programas publicitarios. Sin embargo, el primer lugar lo ocupó el troyano Shlayer, sobre el que escribimos a principios de 2020.

## Geografía de las amenazas




Geografía de las amenazas para macOS,
noviembre de 2019 - octubre de 2020



kaspersky

### TOP 10 de países por el porcentaje de usuarios atacados

| | País* | %** |
|---|---|---|
| **1** | España | 14,03 |
| **2** | Francia | 13,54 |
| **3** | Canadá | 11,35 |
| **4** | Estados Unidos | 10,76 |
| **5** | India | 10,53 |
| **6** | Brasil | 10,22 |
| **7** | México | 9,86 |
| **8** | Italia | 9,80 |
| **9** | Australia | 9,09 |
| **10** | Inglaterra | 8,99 |

* Hemos excluido de la clasificación a los países donde el número de usuarios de las soluciones de Kaspersky para macOS es relativamente pequeño (menos de 5000).

** Proporción de usuarios atacados únicos en el país, del total de los usuarios de las soluciones de seguridad de Kaspersky para macOS en el mismo país.

# Ataques contra el Internet de las cosas (IoT)

## Estadísticas de amenazas para IoT

Durante el período del informe, más del 80% de los ataques a las trampas de Kaspersky se llevaron a cabo mediante el protocolo Telnet.

| | |
|---|---|
| Telnet | 81,02% |
| SSH | 18,98% |

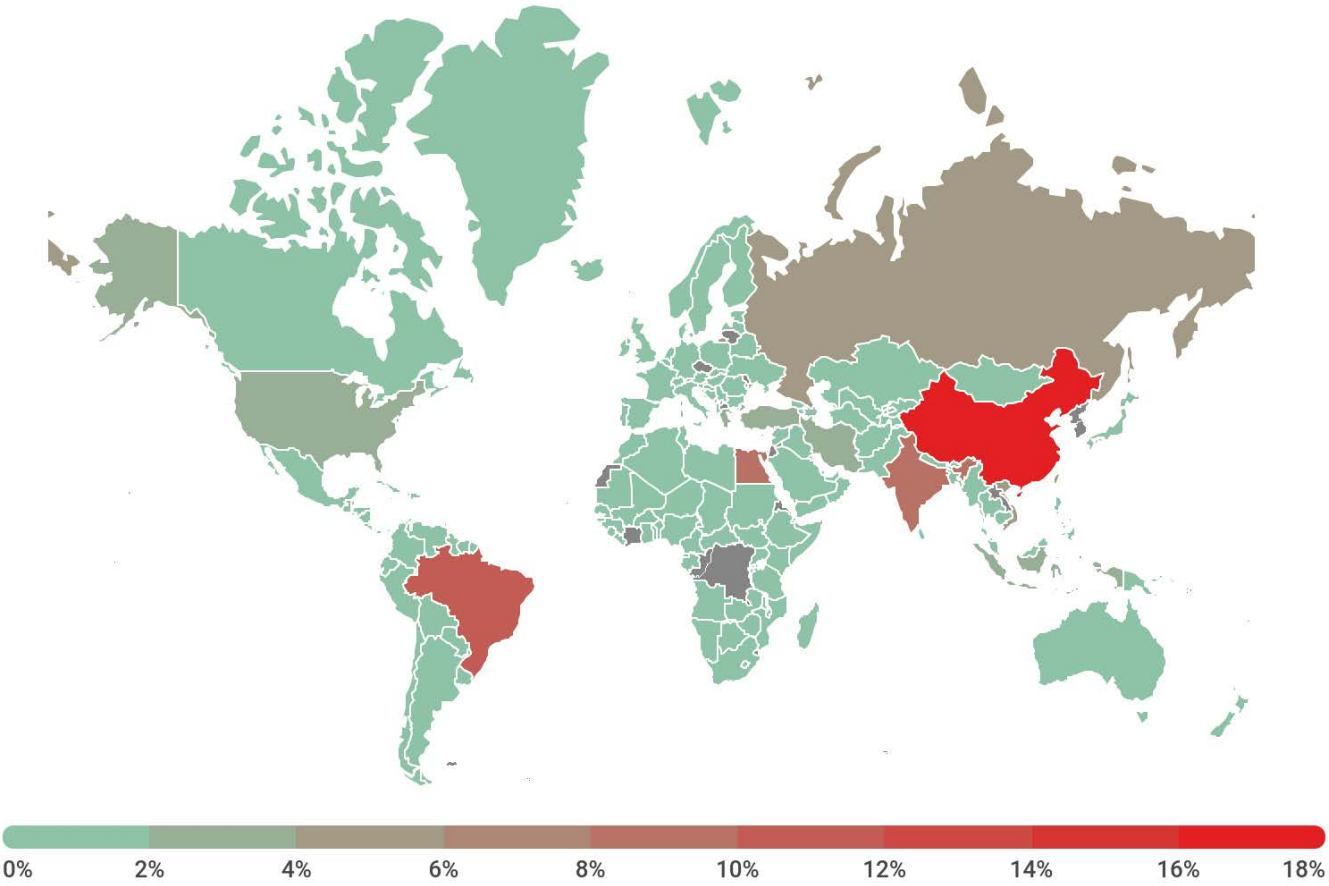
**Tabla de distribución de servicios atacados, por cantidad de direcciones IP únicas de dispositivos que llevaron a cabo ataques, noviembre de 2019 - octubre de 2020**

En cuanto a la distribución del número de sesiones, aquí también prevalece Telnet, ya que dos tercios de todas las sesiones de trabajo se realizaron con este protocolo.

| | |
|---|---|
| Telnet | 67,60% |
| SSH | 32,40% |

**Tabla de distribución de sesiones de trabajo de ciberdelincuentes con trampas de Kaspersky, noviembre 2019 - octubre 2020**

Como resultado, elegimos los dispositivos que llevaron a cabo ataques utilizando el protocolo Telnet para construir el mapa de distribución de direcciones IP de los atacantes.




Geografía de las direcciones IP de los dispositivos desde los que se llevaron a cabo los ataques a las trampas Telnet de Kaspersky, noviembre de 2019 - octubre de 2020

**TOP 10 de países donde se ubicaron los dispositivos desde los cuales se llevaron a cabo ataques a las trampas Telnet de Kaspersky**

| | País* | %** |
|---|---|---|
| **1** | China | 17,95 |
| **2** | Brasil | 10,35 |
| **3** | Egipto | 9,26 |
| **4** | India | 8,51 |
| **5** | Taiwán, Provincia de China | 5,11 |
| **6** | Vietnam | 4,94 |
| **7** | Rusia | 4,00 |
| **8** | Irán | 3,96 |
| **9** | Turquía | 2,46 |
| **10** | Estados Unidos | 2,42 |

* Proporción de dispositivos desde los que se llevaron a cabo ataques en un país específico, del número total de dispositivos.

## Amenazas cargadas en las trampas

| | Veredicto | %* |
|---|---|---|
| **1** | Trojan-Downloader.Linux.NyaDrop.b | 42,43 |
| **2** | Backdoor.Linux.Mirai.b | 27,01 |
| **3** | Backdoor.Linux.Mirai.ba | 10,09 |
| **4** | Backdoor.Linux.Gafgyt.a | 7,46 |
| **5** | Backdoor.Linux.Gafgyt.bj | 1,54 |
| **6** | Trojan-Downloader.Shell.Agent.p | 0,83 |
| **7** | Backdoor.Linux.Mirai.cn | 0,73 |
| **8** | Backdoor.Linux.Mirai.cw | 0,64 |
| **9** | Backdoor.Linux.Mirai.h | 0,53 |
| **10** | Backdoor.Linux.Mirai.c | 0,51 |

* Proporción de un malware específico, del número total de malware cargado en dispositivos de IoT como resultado de un ataque exitoso.

# Ataques a través de recursos web

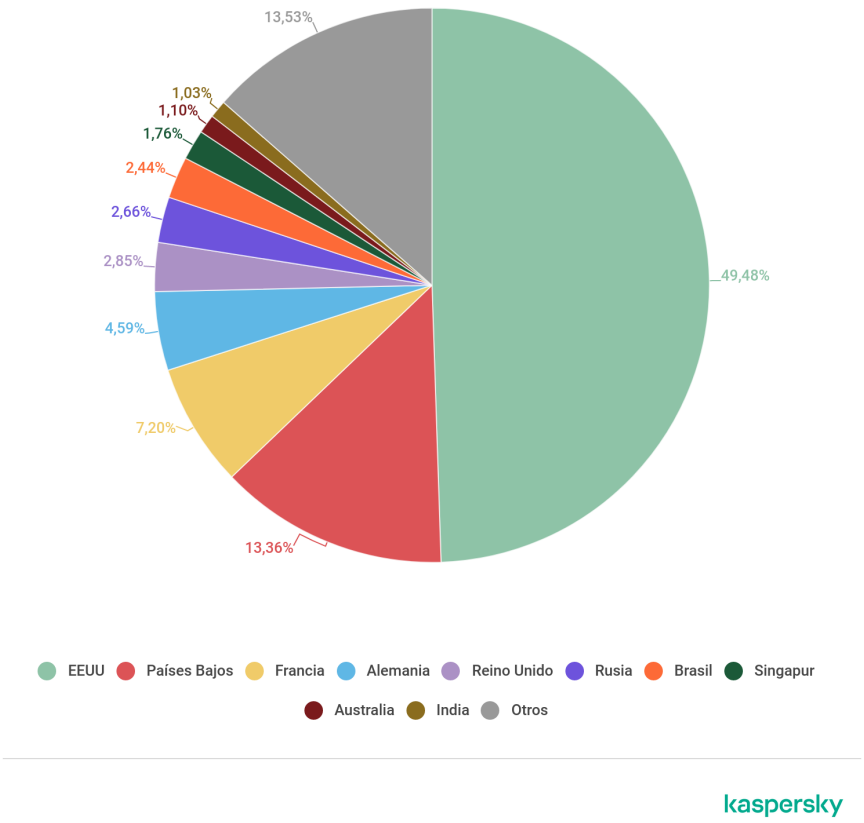
**Los datos estadísticos de este capítulo han sido recopilados por el antivirus web, que protege a los usuarios cuando descargan objetos maliciosos de una página web maliciosa o infectada. Los delincuentes crean estos sitios maliciosos a propósito, pero también los sitios legítimos se pueden infectar 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 por Internet bloqueados por los productos de Kaspersky en los equipos de los usuarios (páginas web con desvíos hacia exploits, sitios con exploits y otros programas maliciosos, centros de administración de botnets, etc.). Destacamos que cada host único puede ser fuente de uno o más ataques web.**

**Para detectar 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 en cuestión y la detección de la ubicación geográfica de esta dirección IP (GEOIP).**

Durante el periodo cubierto por este informe, las soluciones de Kaspersky neutralizaron **666 809 967** ataques lanzados desde recursos de Internet ubicados en diversos países del mundo. Además, el 86,47% del monto total de estos recursos se ubicaron en solo 10 países.




**Distribución de fuentes de ataques web por países, noviembre 2019 - octubre 2020**

Al igual que en 2019, Estados Unidos ocupa el primer lugar entre los países de origen de los ataques web (49,48%); su participación aumentó en 6 p.p. Alemania (4,59%) pasó de la tercera a la cuarta posición y Francia (7,20%) el lugar que dejó vacante.

## 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.**

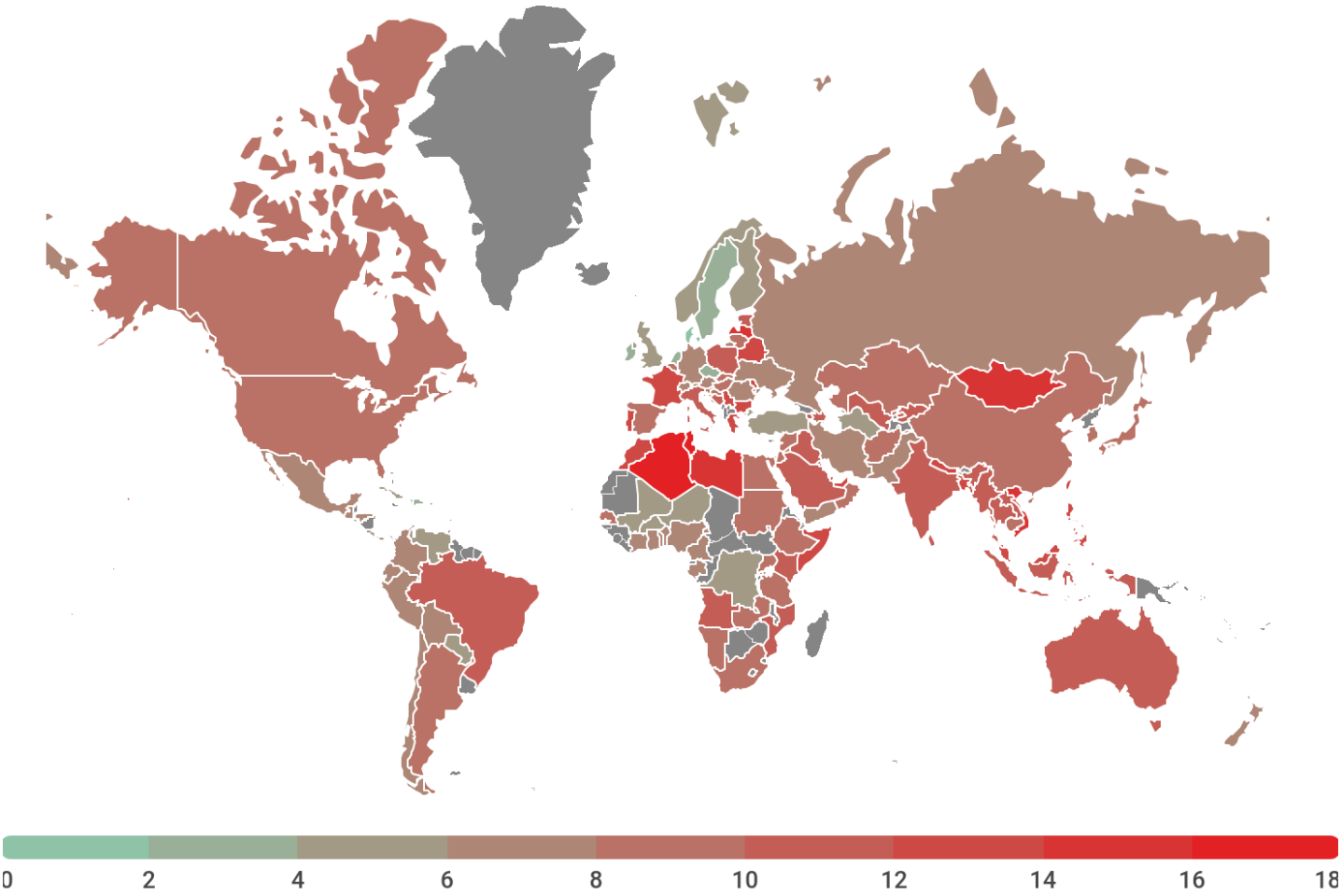
Recordamos al lector que esta calificación toma en cuenta solo los ataques realizados por objetos maliciosos de la clase Malware. En los cálculos no tomamos en cuenta las reacciones del antivirus web ante los programas potencialmente peligrosos y no deseados, como RiskTool y programas publicitarios. 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** | Túnez | 18,27 |
| **2** | Argelia | 16,42 |
| **3** | Mongolia | 15,94 |
| **4** | Vietnam | 15,61 |
| **5** | Letonia | 14,73 |
| **6** | Libia | 14,25 |
| **7** | Grecia | 13,96 |
| **8** | Bangladesh | 13,75 |
| **9** | Taiwán, Provincia de China | 13,62 |
| **10** | Francia | 13,58 |
| **11** | Bulgaria | 13,37 |
| **12** | Nepal | 13,15 |
| **13** | Filipinas | 12,99 |
| **14** | Portugal | 12,79 |
| **15** | Catar | 12,75 |
| **16** | Marruecos | 12,71 |
| **17** | Malasia | 12,55 |
| **18** | República de Moldavia | 12,55 |
| **19** | Bielorrusia | 12,54 |
| **20** | Somalia | 12,45 |

* 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 cubierto por este informe el **10,18%** 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.




kaspersky

Geografía de los ataques web de malware,
noviembre de 2019 - octubre de 2020

## 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 **33 412 568** objetos maliciosos únicos (scripts, exploits, archivos ejecutables, etc.) y **173 335 902** 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.



kaspersky

| | Veredicto* | %** |
|---|---|---|
| **1** | URL malicioso | 66,07 |
| **2** | Trojan.Script.Generic | 9,25 |
| **3** | Trojan.Multi.Preqw.gen | 6,10 |
| **4** | Trojan.BAT.Miner.gen | 3,57 |
| **5** | Trojan.Script.Miner.gen | 3,43 |
| **6** | Hoax.HTML.FraudLoad.m | 1,38 |
| **7** | Trojan.PDF.Badur.gen | 1,12 |
| **8** | Backdoor.HTTP.TeviRat.gen | 0,51 |
| **9** | Trojan-Downloader.Script.Generic | 0,50 |
| **10** | Trojan-PSW.Script.Generic | 0,47 |
| **11** | Exploit.MSOffice.CVE-2017-11882.gen | 0,38 |
| **12** | DangerousObject.Multi.Generic | 0,36 |
| **13** | Trojan-Clicker.HTML.Iframe.dg | 0,23 |
| **14** | Trojan.Script.Redirector.gen | 0,22 |
| **15** | Hoax.Script.Loss.gen | 0,19 |
| **16** | Exploit.Script.Generic | 0,17 |
| **17** | Trojan.MSOffice.SAgent.gen | 0,13 |
| **18** | Trojan.Script.Agent.bg | 0,13 |
| **19** | Trojan-Downloader.JS.SLoad.gen | 0,12 |
| **20** | Trojan-Downloader.MSOffice.SLoad.gen | 0,12 |

* Se excluyen de la lista amenazas del tipo HackTool
** Porcentaje de ataques de este programa malicioso, del total de ataques web de la clase Malware registrados en los equipos de usuarios únicos de los productos de Kaspersky.

En el período del informe, el primer lugar lo ocupó el tradicional veredicto Malicious URL (66,07%). Los usuarios lo ven cuando nuestras soluciones bloquean los intentos de seguir enlaces peligrosos ya conocidos que conducen a recursos con exploits y otro malware, servidores de administración de botnets, sitios de ransomware, etc.

Algunos mineros web como Trojan.Script.Miner.gen todavía se encuentran en nuestro TOP 20, pero la criptominería oculta no es tan popular como lo era hace un par de años.

Las detecciones de nuestro TOP 20 que contienen MS Office o PDF en sus nombres son varios documentos maliciosos que se utilizan en los envíos masivos de spam. Como regla, su tarea es transportar a su destino la carga útil, por ejemplo el troyano bancario Emotet, y es precisamente su descarga lo que bloquea nuestro antivirus web.

# 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 por medio de la infección de archivos o memorias extraíbles, o aquellos que inicialmente entraron en forma velada (por ejemplo, los 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 | 26,59 |
| **2** | Trojan.Multi.BroSubsc.gen | 20,44 |
| **3** | Trojan.Multi.GenAutorunReg.a | 7,99 |
| **4** | Trojan.Multi.Misslink.a | 7,47 |
| **5** | Trojan.Script.Generic | 6,45 |
| **6** | Trojan.WinLNK.Agent.gen | 3,00 |
| **7** | Trojan.Win32.SEPEH.gen | 2,88 |
| **8** | Trojan.Win32.Generic | 2,53 |
| **9** | Trojan.WinLNK.Starter.gen | 2,45 |
| **10** | Trojan.Multi.Agent.gen | 2,12 |
| **11** | Trojan.WinLNK.Runner.jo | 2,02 |
| **12** | Trojan.Win32.AutoRun.gen | 1,91 |
| **13** | Trojan.Multi.GenAutorunTask.c | 1,91 |
| **14** | Virus.Win32.Sality.gen | 1,84 |
| **15** | Trojan.Multi.GenAutorunTask.a | 1,76 |
| **16** | Trojan.Multi.GenAutorunTaskFile.a | 1,73 |
| **17** | Trojan-Downloader.Script.Generic | 1,64 |
| **18** | Trojan.AndroidOS.Boogr.gsh | 1,59 |

| | Veredicto* | %** |
|---|---|---|
| **19** | Trojan.Multi.GenBadur.gen | 1,52 |
| **20** | Virus.Win32.Pioneer.cz | 1,51 |

* Se excluyen de la lista las amenazas del tipo HackTool
** 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 el período del informe lo ocupó el veredicto DangerousObject.Multi.Generic (26,59%), que utilizamos para el malware detectado mediante tecnologías de nube. Estas tecnologías se aplican cuando en las bases antivirus todavía no hay datos que ayuden a detectar el programa malicioso, pero en la nube de la compañía antivirus ya hay información sobre el objeto. En esencia, así es como se detectan los programas maliciosos más nuevos.

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

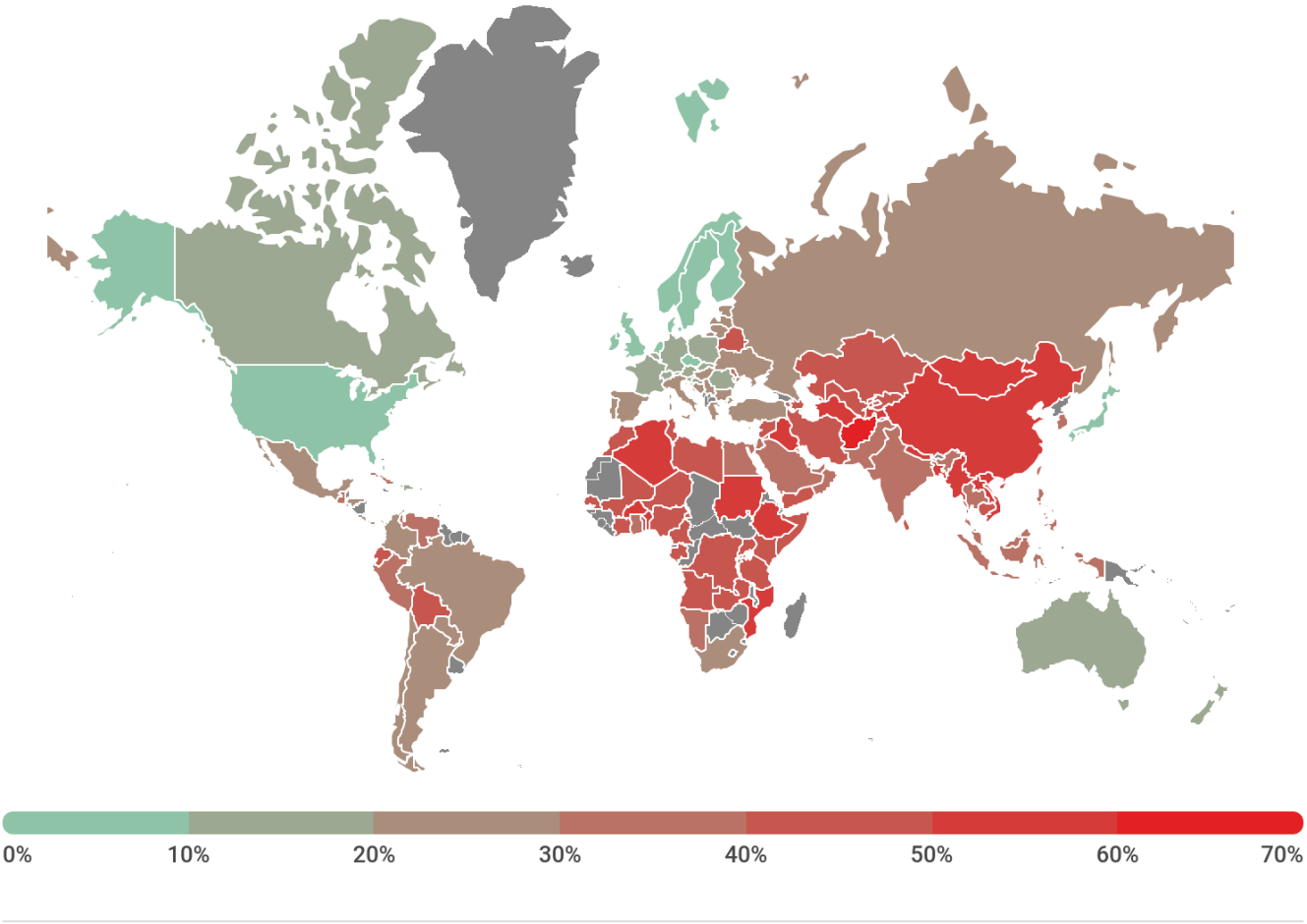
**Para cada uno de los países calculamos con qué frecuencia durante el año los usuarios se toparon con las reacciones del antivirus de archivos. Se tuvieron en cuenta los objetos detectados que se encuentran directamente en las computadoras de los usuarios o en los medios extraíbles conectados (unidades 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 | 63,52 |
| **2** | Myanmar | 59,89 |
| **3** | Laos | 57,40 |
| **4** | Vietnam | 56,84 |
| **5** | Mongolia | 55,11 |
| **6** | China | 54,81 |
| **7** | Bangladesh | 54,74 |
| **8** | Etiopía | 54,67 |
| **9** | Ruanda | 53,22 |
| **10** | Burkina Faso | 52,57 |
| **11** | Turkmenistán | 52,47 |
| **12** | Benín | 52,43 |
| **13** | Tayikistán | 52,29 |
| **14** | Argelia | 51,85 |
| **15** | Irak | 51,73 |

| | País* | %** |
|---|---|---|
| **16** | Mozambique | 50,98 |
| **17** | Sudán | 50,88 |
| **18** | Nepal | 50,07 |
| **19** | Tanzania | 49,34 |
| **20** | Costa de Marfil | 49,31 |

* 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.




**Geografía de las infecciones locales de malware, noviembre de 2019 - octubre de 2020**

En el periodo cubierto por este informe, se detectó un promedio de al menos un programa malicioso en el **28,65%** de los equipos, discos duros o medios extraíbles pertenecientes a los usuarios de KSN.



kaspersky