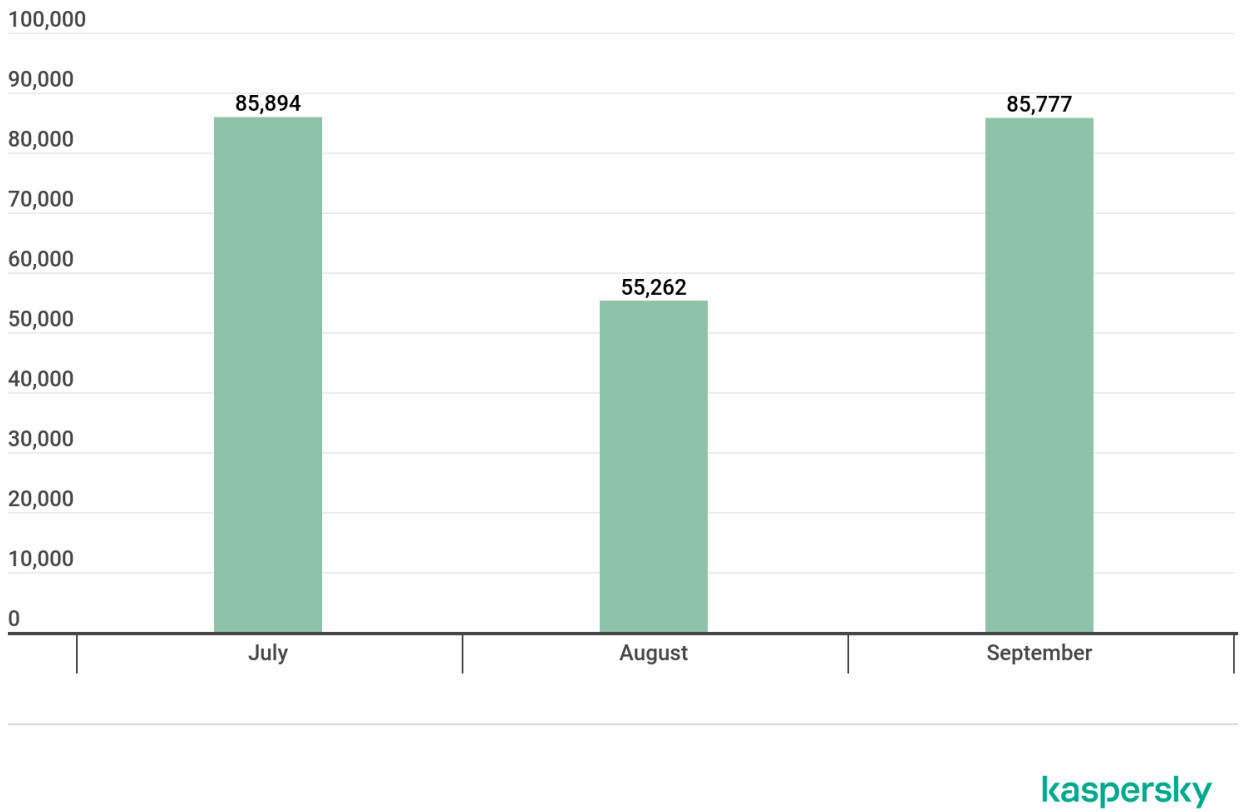
حفاظت سیستم های کامپیوتری در حوزه سلامت

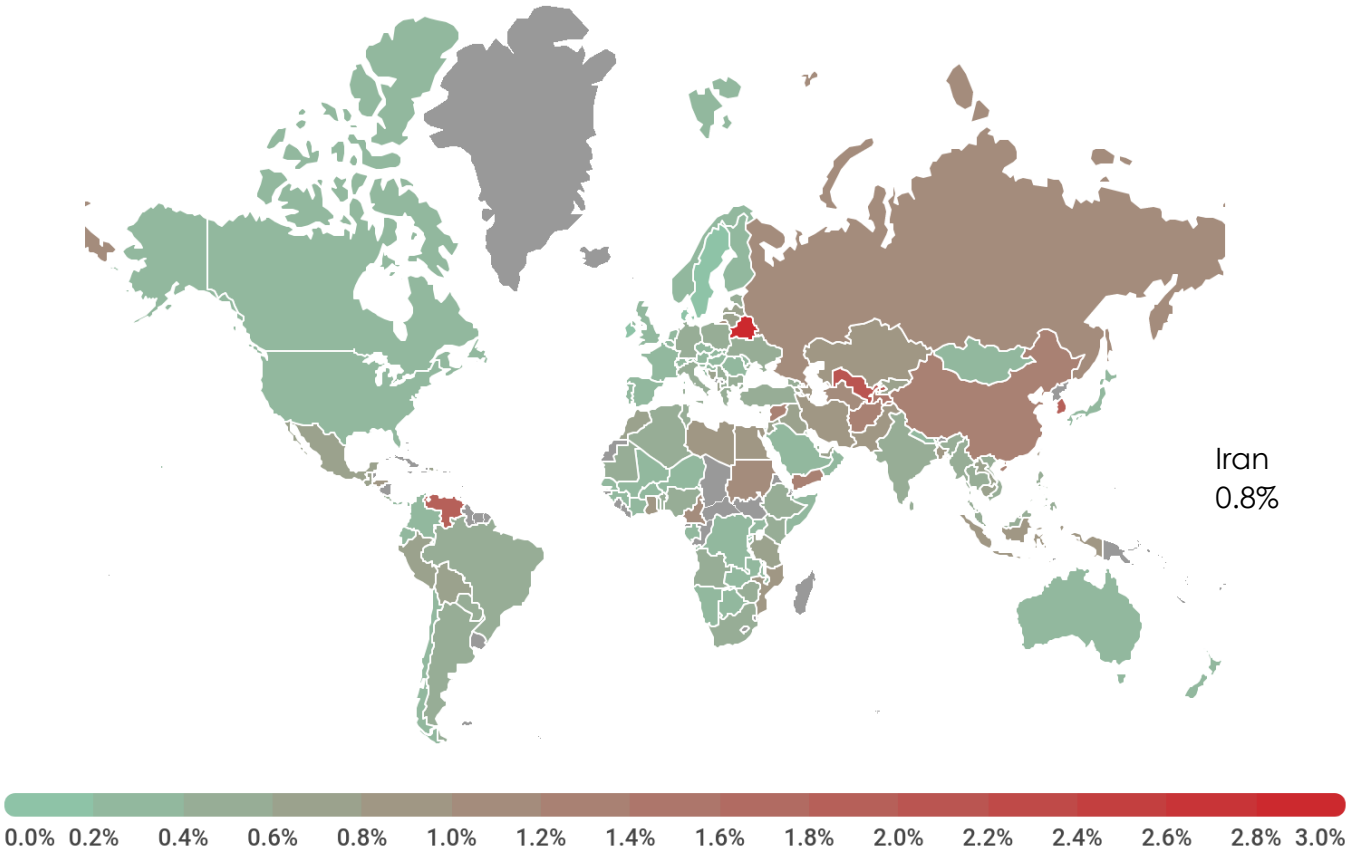
آمار تهدیدات موجود در سه ماهه سوم ۲۰۱۹

Financial threats

- کسپرسکی ۱۹۷،۵۵۹ بد افزار که برای سرقت پول از طریق دسترسی آنلاین به حساب های بانکی روی رایانه ها طراحی شده اند را مسدود کرده است.



Number of unique users attacked by financial malware, Q3 2019



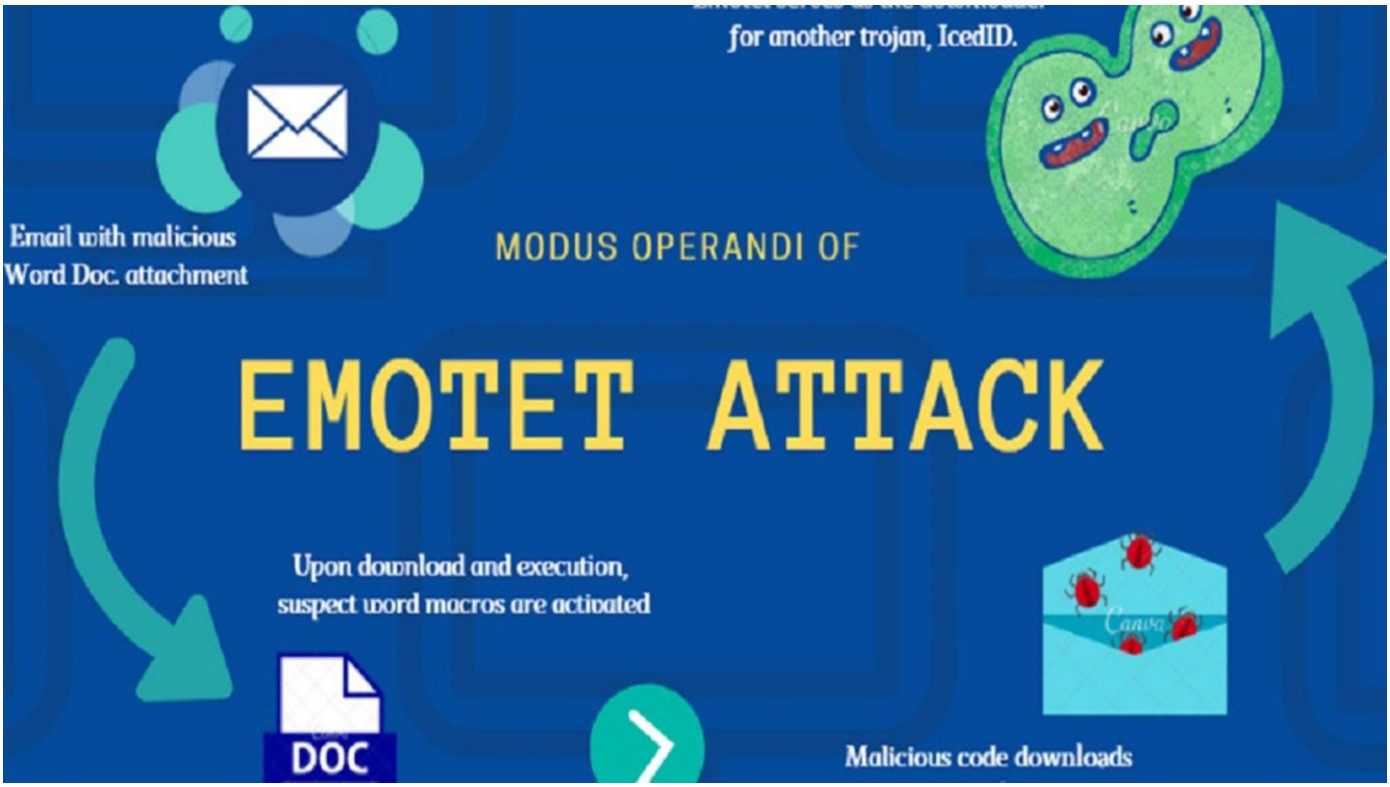
kaspersky

Geography of banking malware attacks, Q3 2019

	Name	Verdicts	%*
1	Zbot	Trojan.Win32.Zbot	26.7
2	Emotet	Backdoor.Win32.Emotet	23.9
3	RTM	Trojan-Banker.Win32.RTM	19.3
4	Nimnul	Virus.Win32.Nimnul	6.6
5	Trickster	Trojan.Win32.Trickster	5.8
6	CliptoShuffler	Trojan-Banker.Win32.CliptoShuffler	5.4
7	Nymaim	Trojan.Win32.Nymaim	3.6
8	SpyEye	Trojan-Spy.Win32.SpyEye	3.4
9	Danabot	Trojan-Banker.Win32.Danabot	3.3
10	Neurevt	Trojan.Win32.Neurevt	1.8

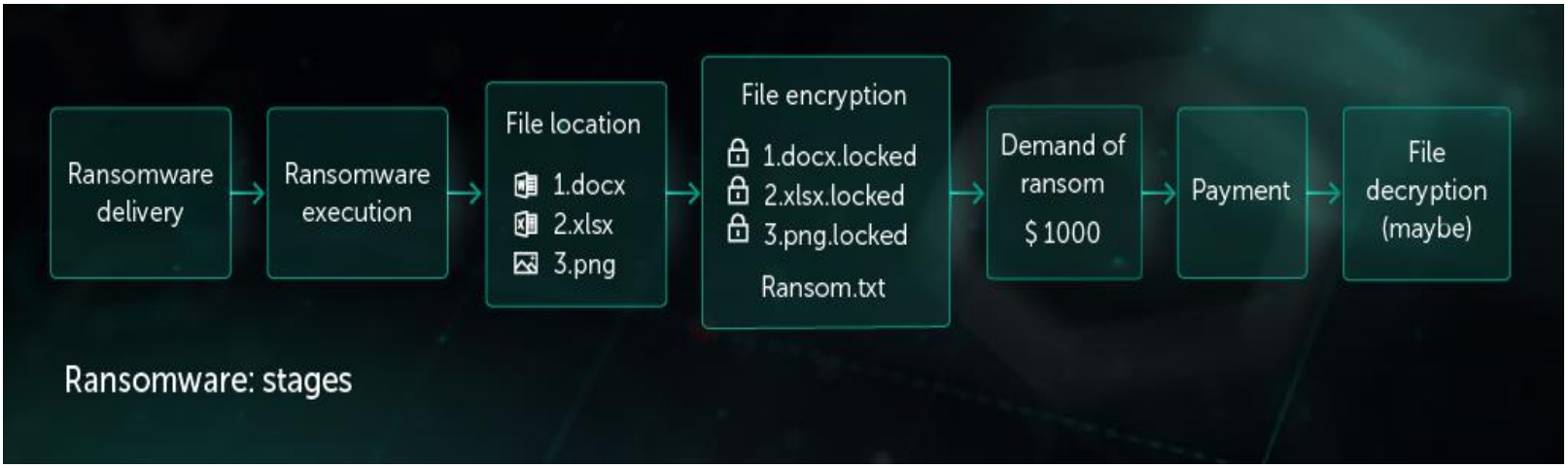
*** Unique users attacked by this malware as a percentage of all users attacked by financial malware.*

بـد افزار Emotet توســـط هکرهـا برای آلوده کردن اهـداف قربـانی، از طریقspam ایمیل، و به منظور دزدیدن اطلاعات مالی مانند اطلاعات ورود به حســـاب بانک یا کیف ارز دیجیتالی (cryptocurrency) اســـتفاده می‌شود.

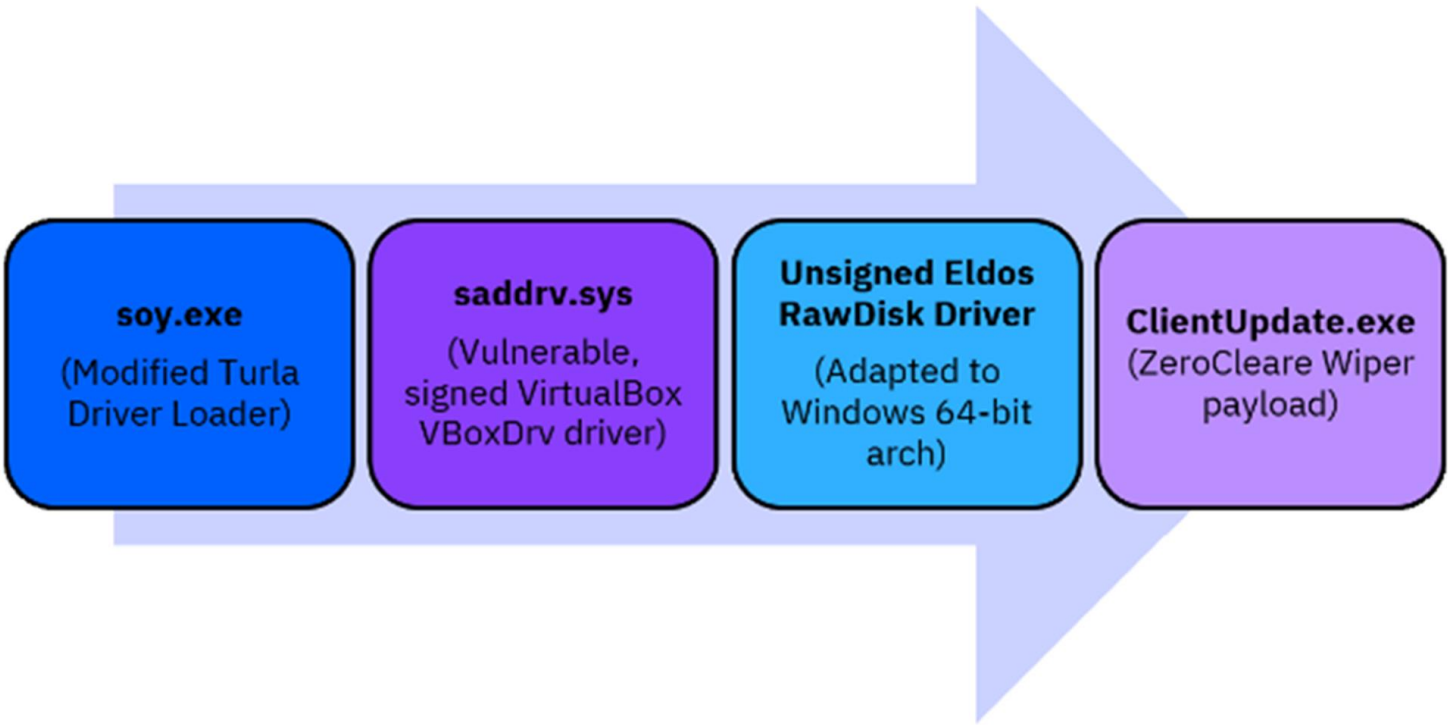


Ransomware programs

خنثی سازی حملات باج افزارها روی ۲۲۹،۶۴۳ کاربر منحصر به فرد

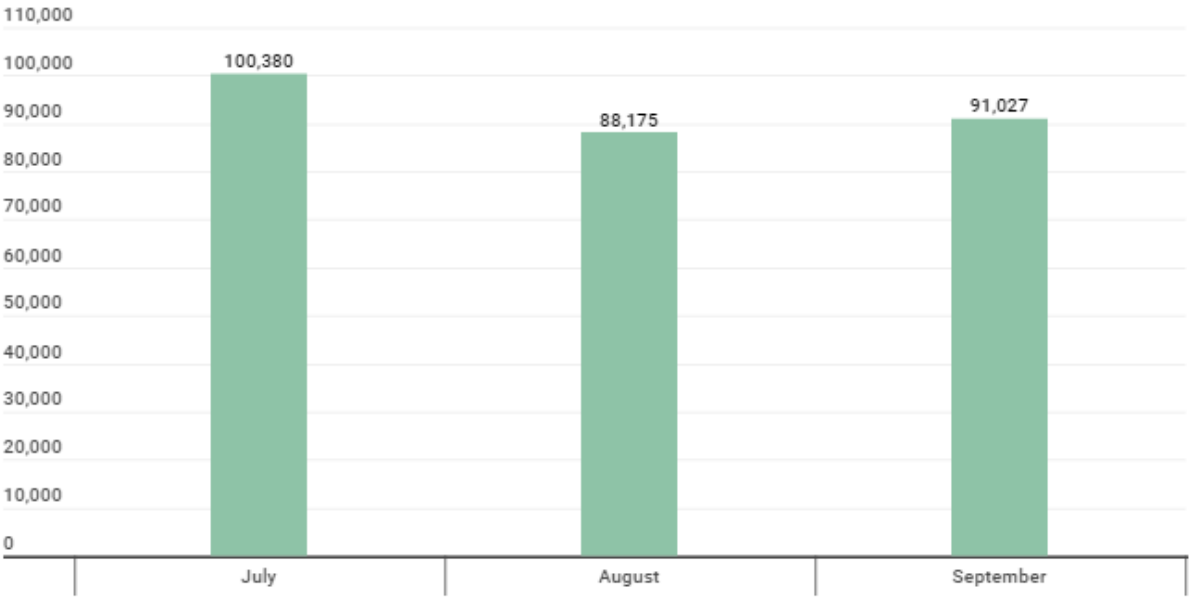


نـوع دیگـری از بـدافزارها کـه درکنـار بـاج افزارهـا در حـال توسـعه و رشـد هسـتند Wiper نـام دارنـد عملکـرد آن هـا در ظـاهر همچـون بـاج افزارهـا با تغییر نام فایل ها و درخواست باج همـراه اسـت امـا ایـن تروجـان بـه طـور برگشت ناپذیری محتوای فایل هـا را خـراب مـی کنـد(با صـفر کـردن بایتهـا و تغییر تصادفی آن ها)



Number of users attacked by ransomware Trojans

In Q3 2019, Kaspersky products defeated ransomware attacks against 229,643 unique KSN users. This is slightly fewer than the previous quarter.



kaspersky

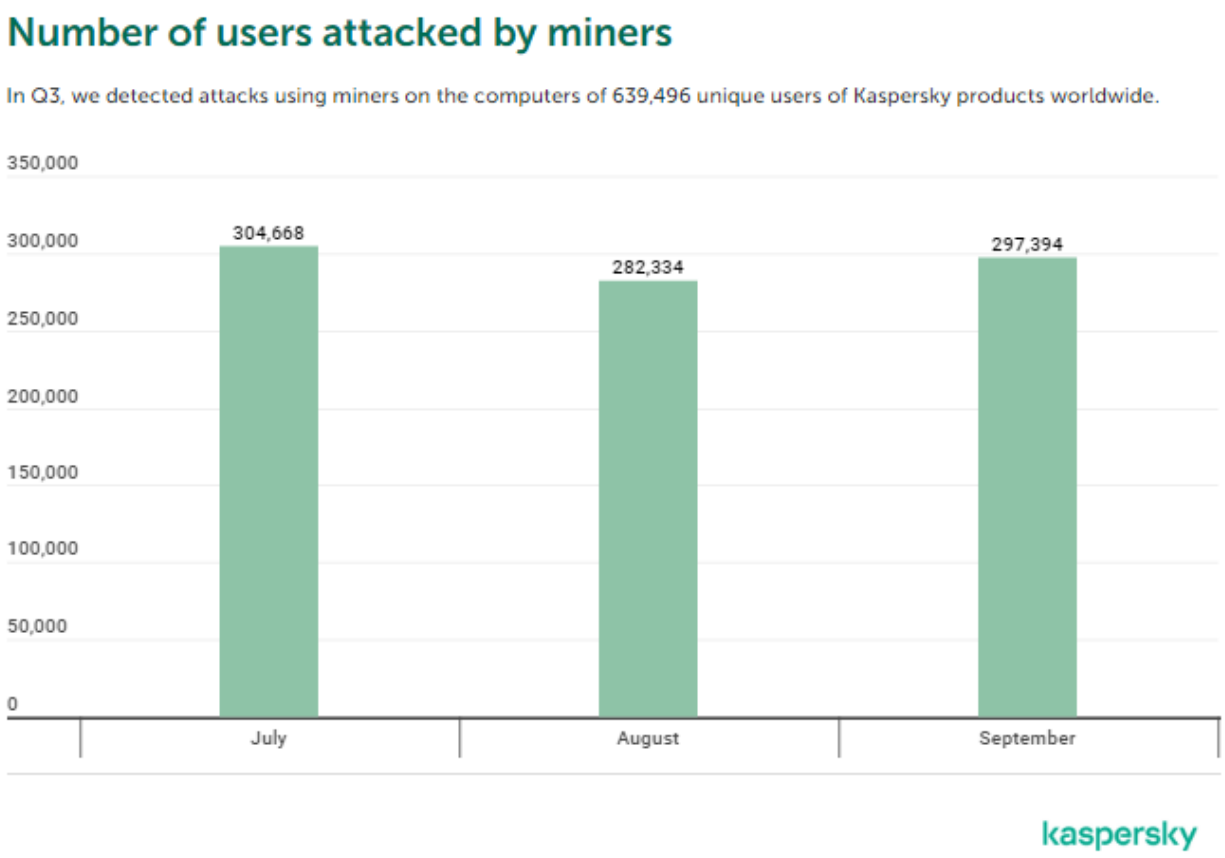
TOP 10 most common families of ransomware Trojans

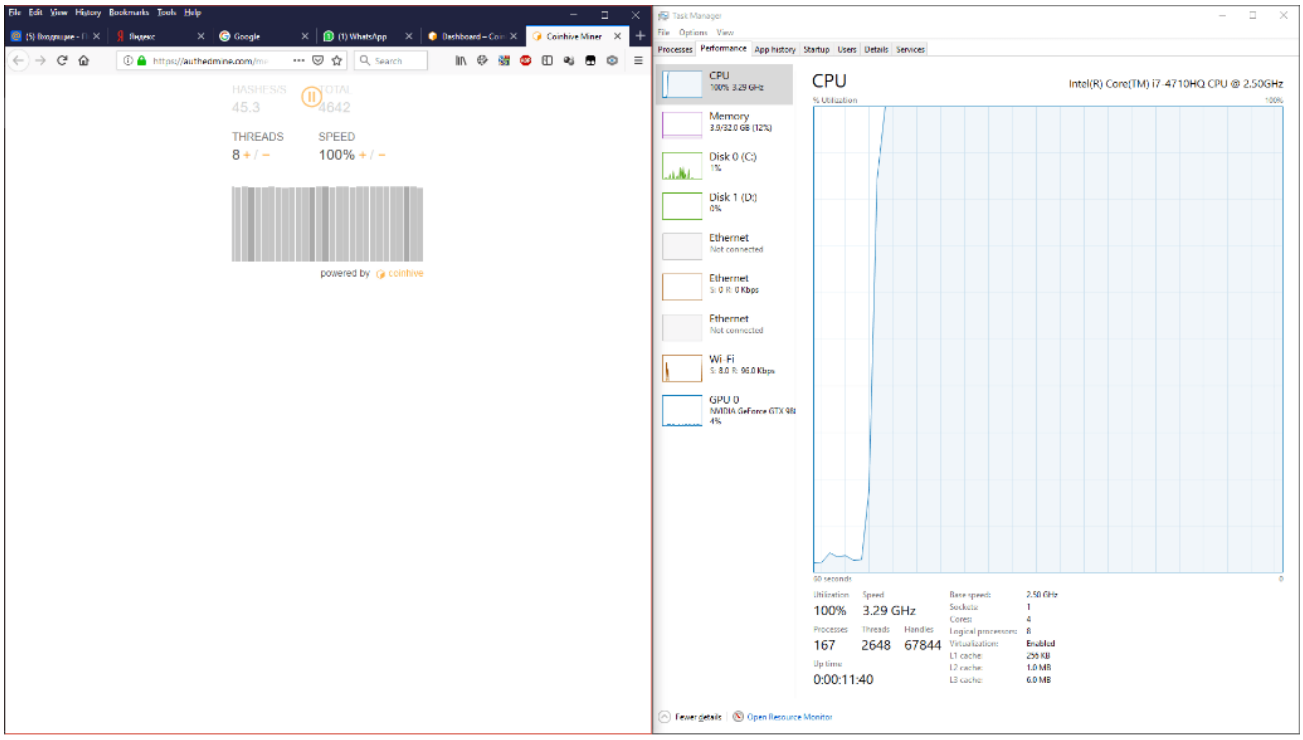
	Name	Verdicts	% of attacked users*
1	WannaCry	Trojan-Ransom.Win32.Wanna	20.96
2	(generic verdict)	Trojan-Ransom.Win32.Phny	20.01
3	GandCrab	Trojan-Ransom.Win32.GandCrypt	8.58
4	(generic verdict)	Trojan-Ransom.Win32.Gen	8.36
5	(generic verdict)	Trojan-Ransom.Win32.Encoder	6.56
6	(generic verdict)	Trojan-Ransom.Win32.Crypren	5.08
7	Stop	Trojan-Ransom.Win32.Stop	4.63
8	Rakhni	Trojan-Ransom.Win32.Rakhni	3.97
9	(generic verdict)	Trojan-Ransom.Win32.Crypmod	2.77
10	PolyRansom/VirLock	Virus.Win32.PolyRansom Trojan-Ransom.Win32. PolyRansom	2.50

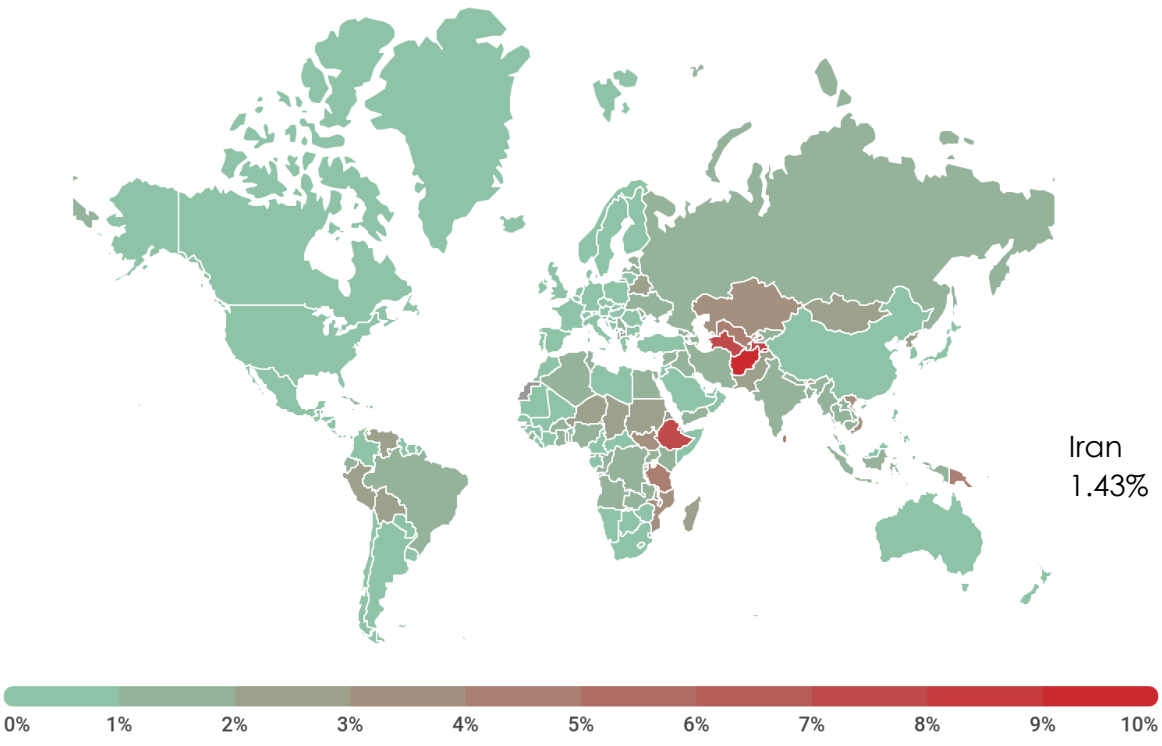
** Unique Kaspersky users attacked by the specified family of ransomware Trojans as a percentage of all users attacked by ransomware Trojans.*

Miners

در سه ماهه سوم سال ۲۰۱۹ تعداد ۶۳۹،۴۹۶ حمله که ماهیت ماینری داشته اند توسط محصولات کسپرسکی شناسایی و مسدود شده اند.




File Edit View History Bookmarks Tools Help
Coinhive Miner
https://authedmine.com/mi
Search
HASHES/S
45.3
TOTAL
4642
THREADS
8 + / −
SPEED
100% + / −
powered by coinhive
Task Manager
File Options View
Processes Performance App history Startup Users Details Services
CPU
100% 3.29 GHz
Memory
3.9/32.0 GB (12%)
Disk 0 (C:)
1%
Disk 1 (D:)
0%
Ethernet
Not connected
Ethernet
S: 0 R: 0 Kbps
Ethernet
Not connected
Wi-Fi
S: 8.0 R: 96.0 Kbps
GPU 0
NVIDIA GeForce GTX 9M
4%
CPU
Intel(R) Core(TM) i7-4710HQ CPU @ 2.50GHz
% Utilization
100%
60 seconds
0
Utilization
100%
Speed
3.29 GHz
Processes
167
Threads
2648
Handles
67844
Up time
0:00:11:40
Base speed: 2.50 GHz
Sockets: 1
Cores: 4
Logical processors: 8
Virtualization: Enabled
L1 cache: 256 KB
L2 cache: 1.0 MB
L3 cache: 6.0 MB
Fewer details
Open Resource Monitor



Geographical spread of countries by share of users attacked by miners, Q3 2019

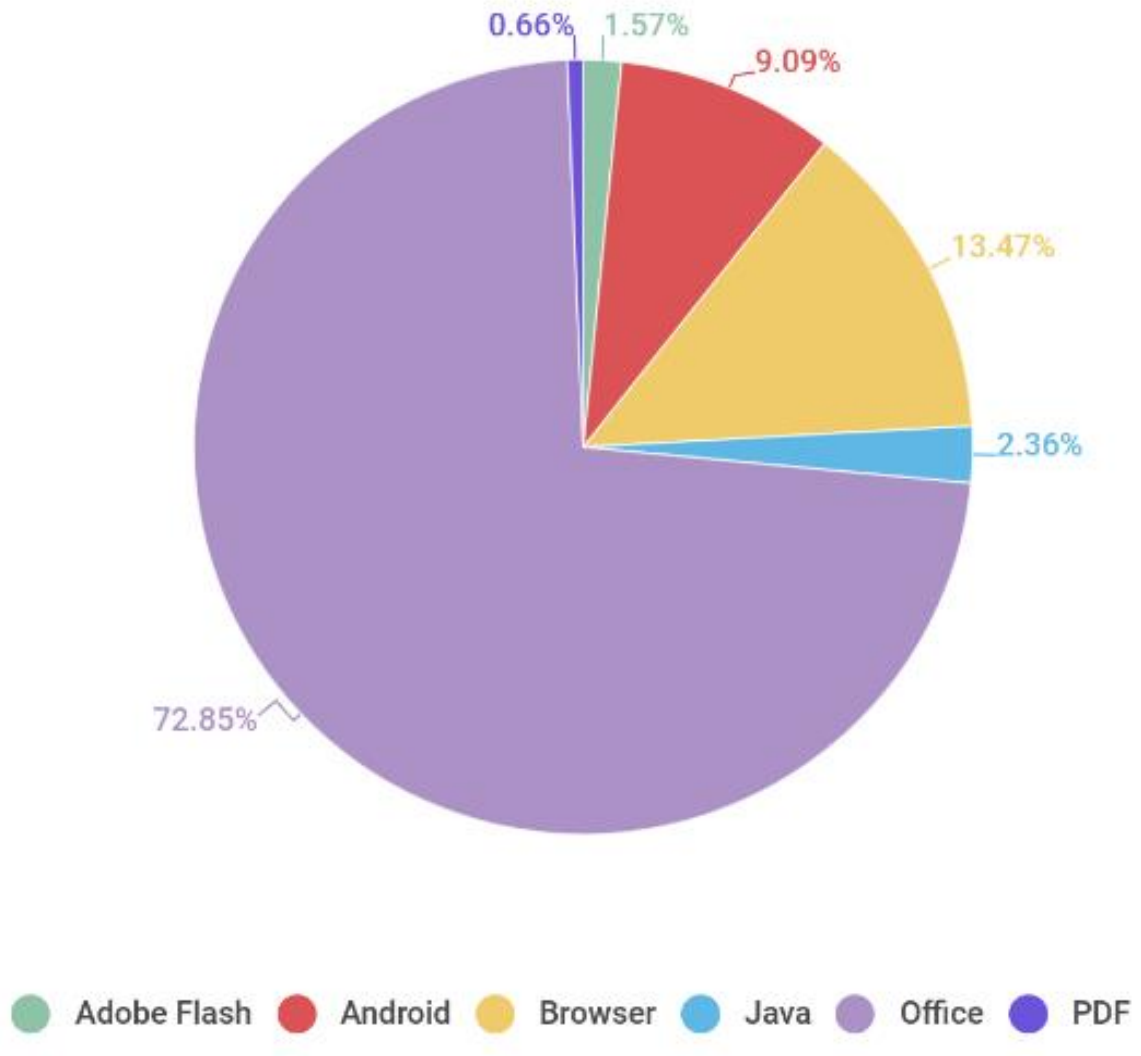
استفاده از آسیب پذیری برنامه ها توسط مهاجمان در حملات سایبری

- مجموعه مایکروسافت آفیس
- مرورگرها

Internet Explorer CVE-2019-1367

Google Chrome

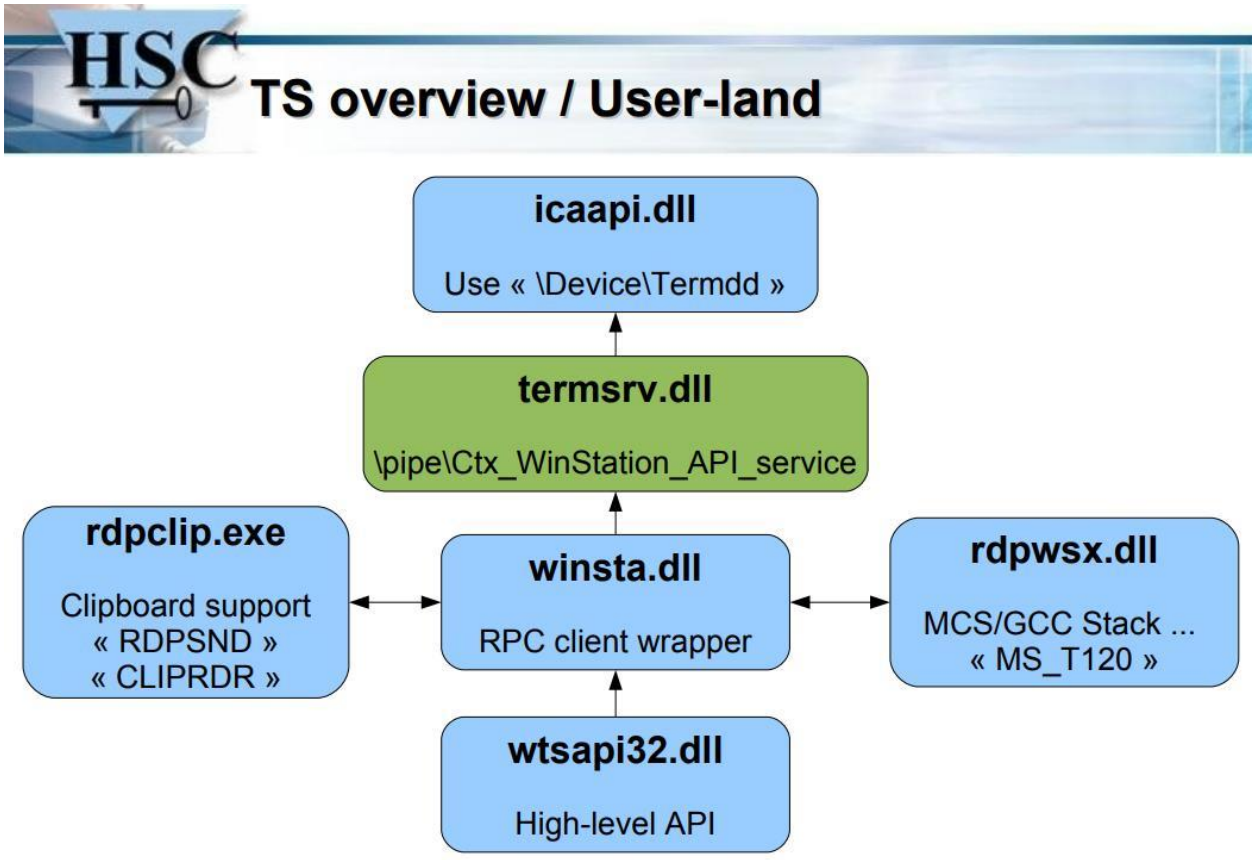
- Privilege escalation vulnerabilities



حملات تحت شبکه

- آسیب پذیری در پروتکلSMB
- Bruteforce روی سرویس هایی همچون RDP

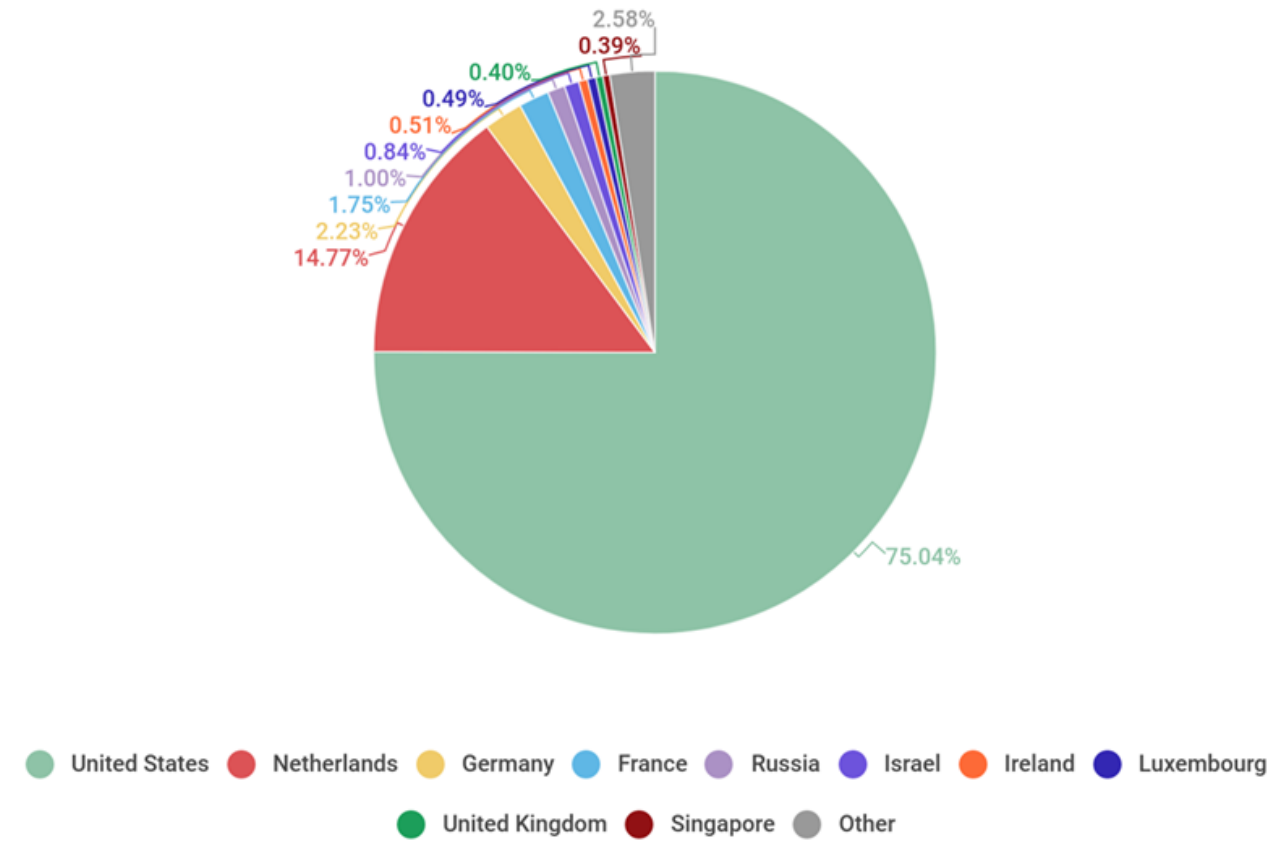
DejaBlue: New BlueKeep-Style Bugs Renew the Risk of a Windows Worm



Attacks via web resources

در سه ماهه سوم سال ۲۰۱۹ آمار زیر از طریق KSN بدست آمده است:

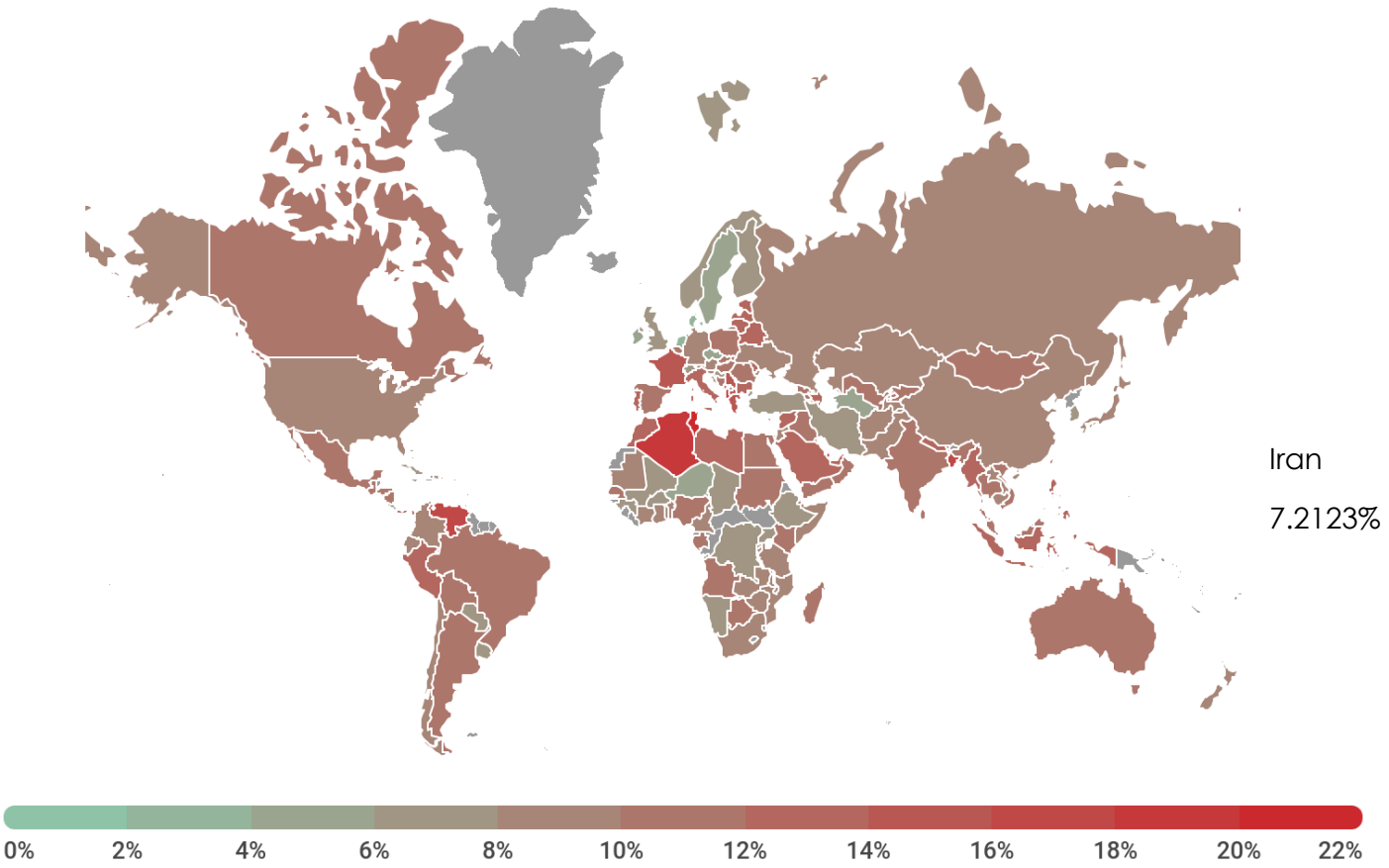
- مسدود سازی ۹۸۹،۴۳۲،۴۰۳ حمله که از منابع آنلاین در ۲۰۳ کشور دنیا انجام می شد.
- شناسایی ۵۶۰،۰۲۵،۳۱۶ لینک آلوده منحصر به فرد توسط ماژول Web-Anti Virus



kaspersky

Distribution of web-based attack sources by country, Q3 2019

به طور متوسط ۱۰,۹۷٪ از رایانه های کاربران اینترنت در سطح جهان حداقل یکبار مورد حمله بدافزارهای تحت وب قرار گرفته امد.



Geography of malicious web-based attacks, Q3 2019

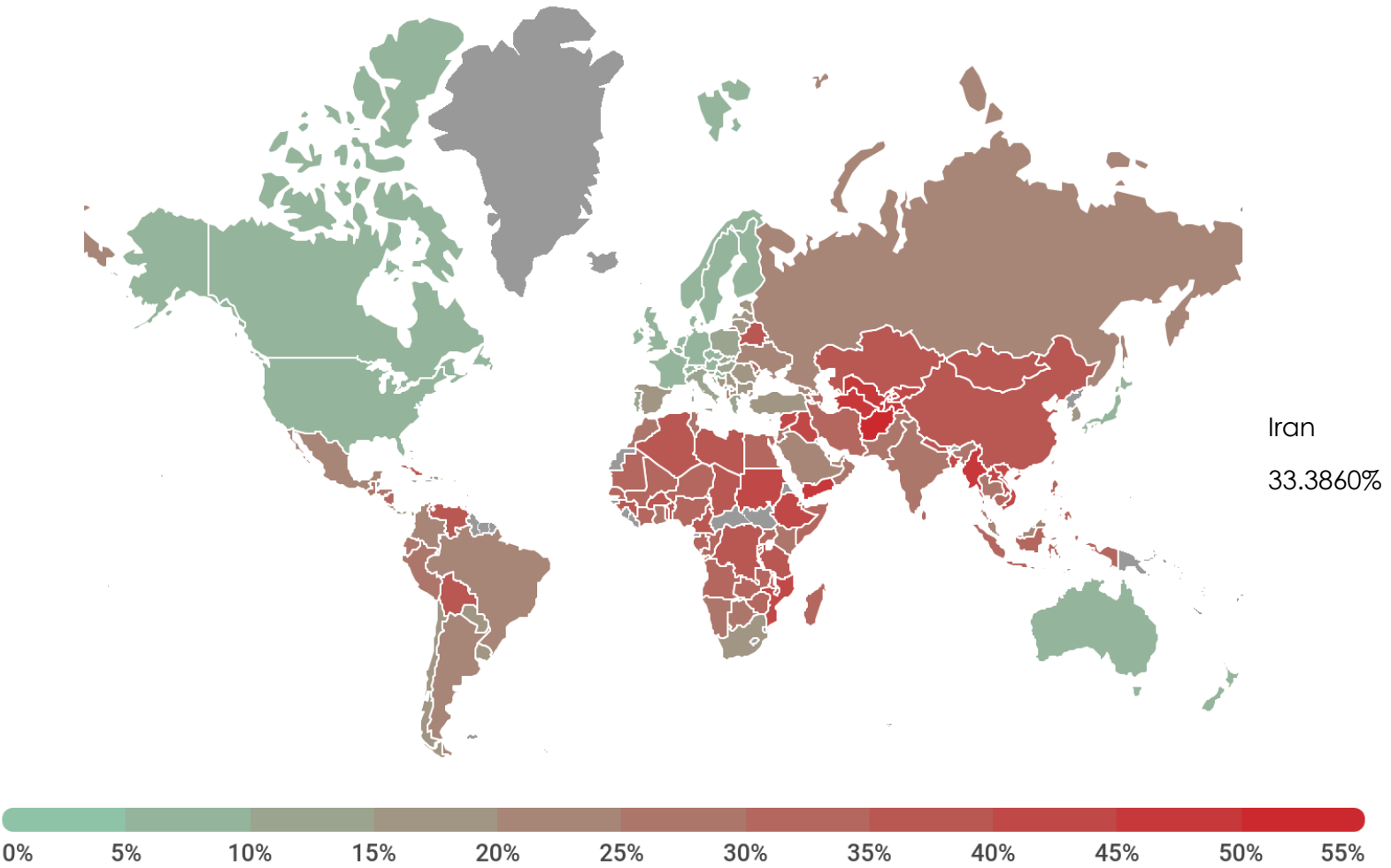
Local threats

- فایل های متنی
- مدیا (عکس و فیلم و موسیقی)
- Removable Drives
- Installer

آمار زیر از تجزیه و تحلیل نتایج Anti-Virus Scan ها و اسکن های Removable Drive ها تولید شده است.

در سه ماهه سوم ۲۰۱۹ تعداد ۲۳۰،۰۵۱،۰۵۴ آبجکت آلوده منحصربفرد توسط ماژول File-Anti Virus شناسایی شده است.

	Country*	% of attacked users**
1	Afghanistan	53.45
2	Tajikistan	48.43
3	Yemen	48.39
4	Uzbekistan	48.38
5	Turkmenistan	45.95
6	Myanmar	45.27
7	Ethiopia	44.18
8	Laos	43.24
9	Bangladesh	42.96
10	Mozambique	41.58
11	Syria	41.15
12	Vietnam	41.11
13	Iraq	41.09
14	Sudan	40.18
15	Kyrgyzstan	40.06
16	China	39.94
17	Rwanda	39.49
18	Venezuela	39.18
19	Malawi	38.81
20	Nepal	38.38



Geography of local infection attempts, Q3 2019

پیش بینی های سال ۲۰۲۰

- موج جدیدی برای بدست آوردن سوابق پزشکی در Darkweb وجود دارد به طوریکه گاهی هزینه بدست آوردن آن ها از اطلاعات کارت های اعتباری هم بیشتر است. اینکار باعث باز شدن راهی برای کلاهبرداری های جدید از بیمار و نزدیکانش است.
- دسترسی به اطلاعات بیمار نه تنها زمینه را برای سرقت اطلاعات بلکه زمینه را برای دستکاری و تغییر اطلاعات فراهم می کند. این امر می تواند منجر به حملات هدفمند به افراد شود تا تشخیص صحیح را از بین برده و آسیب های جانی به فرد را بوجود آورد. اشتباهات تشخیصی آمار بالایی در علت مرگ و میر افراد دارد.
- تعداد حملات به دستگاههای تأسیسات پزشکی در کشورهایی که تازه فرآیند دیجیتالی شدن را در زمینه خدمات پزشکی آغاز کرده اند ، سال آینده به طور قابل توجهی رشد خواهد کرد. انتظار داریم شاهد بروز حملات باج افزار هدفمند علیه بیمارستان ها در کشورهای در حال

توسعه باشیم. موسسات پزشکی در حال تبدیل شدن به زیرساخت های صنعتی هستند. عدم دسترسی به داده های داخلی (به عنوان مثال سوابق دیجیتال بیمار) یا منابع داخلی (مانند تجهیزات پزشکی متصل در بیمارستان) می تواند تشخیص بیمار را متوقف کرده و حتی کمکهای اضطراری را مختل کند

- در سال آینده شاهد افزایش حملات هدفمند علیه مؤسسات تحقیقات پزشکی و شرکتهای دارویی به منظور سرقت مالکیت معنوی تحقیقات پرهزینه ی آن ها خواهیم بود.
- خوشبختانه ، تا به حال هرگز شاهد حمله به وسایل پزشکی کاشته شده (مانند محرک های عصبی) در بدن انسان نبودیم. اما این واقعیت که آسیب پذیری های امنیتی بی شماری در چنین دستگاه هایی وجود دارد به معنای این است که فقط محتاج به زمان است. در آینده با ایجاد شبکه های متمرکز دستگاههای پزشکی پوشیدنی و کاشته شده (مانند تحریک کننده های قلبی) شاهد به وجود آمدن موجی از حملات برای از کارانداختن و تغییر این دستگاهها در بدن بیماران خواهیم بود.