Digital Security
Progress. Protected.

Threat Report

H2 2023

June 2023 – November 2023

(eset):research

Contents

Executive summary

Android

SpinOk spinning the definition of Android spyware

SDK or spyware? A significant number of legitimate Android apps started to behave as spyware; the reason is a third-party software development kit.

IoT Botnets

Who killed Mozi?

ESET researchers discovered and analyzed a kill switch that had taken down one of the most prolific IoT botnets.

Web threats AI

Abusing the ChatGPT name for malicious domains

A new economy has arisen around OpenAI API keys and the ChatGPT name, luring legitimate participants and cybercriminals alike.

Cryptocurrency threats Infostealers Malware-as-a-Service

Lumma Stealer takes the cryptostealer threat landscape by storm

Illicit cryptomining may be on its way out, but Lumma Stealer's success shows that cryptowallets remain in the sights of cybercriminals.

IoT Android Botnets

Android TV boxes under fire: Pandora builds a botnet for DDoS attacks

A new Mirai-based threat uses malicious streaming apps to enslave devices in Latin America.

Infostealers Web threats

Magecart, the ever-present phantom haunting e-commerce

It seems there is never a prolonged period without notable Magecart attacks and H2 2023 was no exception.

Web threats

Website visitors under siege by malicious scripts

The rise in JS/Agent detections reveals that almost 45,000 websites have fallen victim to malicious JavaScript code.

Ransomware

Cl0p and its MOVEit hack: A mass-spreading yet targeted attack

How exploitation of a two-year-old zero day by one actor caused a global cybersecurity nightmare.

Foreword

Welcome to the H2 2023 issue of the ESET Threat Report!

The second half of 2023 witnessed significant cybersecurity incidents. Cl0p, a notorious cybercriminal group known for carrying out ransomware attacks on a major scale, garnered attention through its extensive "MOVEit hack", which surprisingly did not involve ransomware deployment. The attack targeted numerous organizations, including global corporations and US governmental agencies. A key shift in Cl0p's strategy was its move to leak stolen information to open worldwide web sites in cases where the ransom was not paid, a trend also seen with the ALPHV ransomware gang. Other new strategies in the ransomware scene, according to the FBI, have included the simultaneous deployment of multiple ransomware variants and the use of wipers following data theft and encryption.

In the IoT landscape, our researchers have made a notable discovery. They have identified a kill switch that had been used to successfully render the Mozi IoT botnet nonfunctional. It is worth mentioning that the Mozi botnet is one of the largest of its kind we have monitored over the past three years. The nature of Mozi's sudden downfall raises the question of whether the kill switch was used by the botnet creators or Chinese law enforcement. A new threat, Android/Pandora, surfaced in the same landscape, compromising Android devices – including smart TVs, TV boxes, and mobile devices – and utilizing them for DDoS attacks.

Amidst the prevalent discussion regarding AI-enabled attacks, we have identified specific campaigns targeting users of tools like ChatGPT. We also noticed a considerable number of attempts to access malicious domains with names resembling "chapgpt", seemingly in reference to the ChatGPT chatbot. Threats encountered via these domains also include web apps that insecurely handle OpenAI API keys, emphasizing the importance of protecting the privacy of your OpenAI API keys.

We have also observed a significant increase in Android spyware cases, mainly attributed to the presence of the SpinOk spyware. This malicious software is distributed as a software development kit and is found within various legitimate Android applications. On a different front, one of the most recorded threats in H2 2023 is three-year-old malicious JavaScript code detected as JS/Agent, which continues to be loaded by compromised websites.

Similarly, Magecart, a threat that goes after credit card data, has continued to grow for two years by targeting myriads of unpatched websites. In all three of these cases, the attacks could have been prevented if developers and admins had implemented appropriate security measures.

Lastly, the increasing value of bitcoin has not been accompanied by a corresponding increase in cryptocurrency threats, diverging from past trends. However, cryptostealers have seen a notable increase, caused by the rise of the malware-as-a-service (MaaS) infostealer Lumma Stealer, which targets cryptocurrency wallets. These developments show an ever-evolving cybersecurity landscape, with threat actors using a wide range of tactics.

I wish you an insightful read.

Jiří Kropáč
ESET Director of Threat Detection

Threat landscape trends

Android

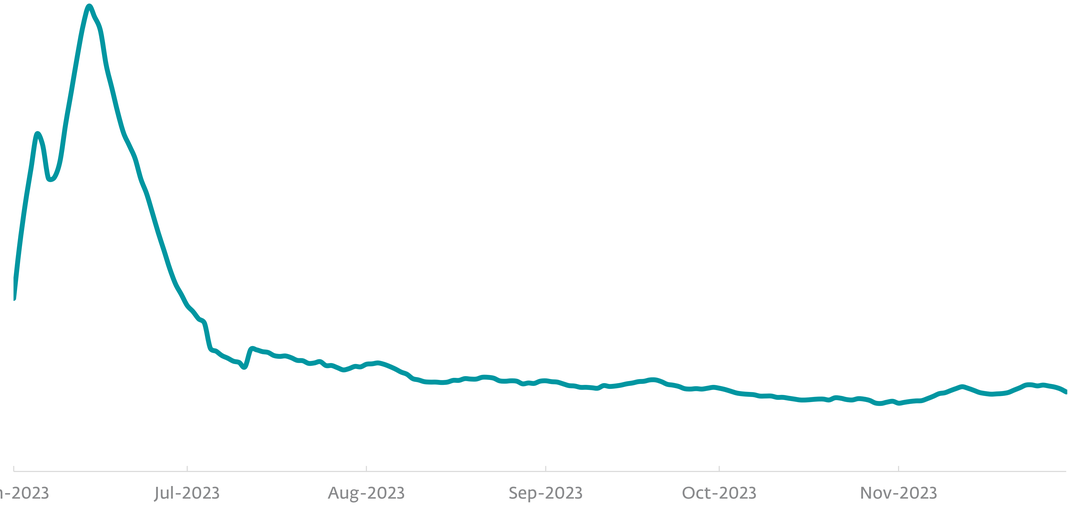
SpinOk spinning the definition of Android spyware

SDK or spyware? A significant number of legitimate Android apps started to behave as spyware; the reason is a third-party software development kit.

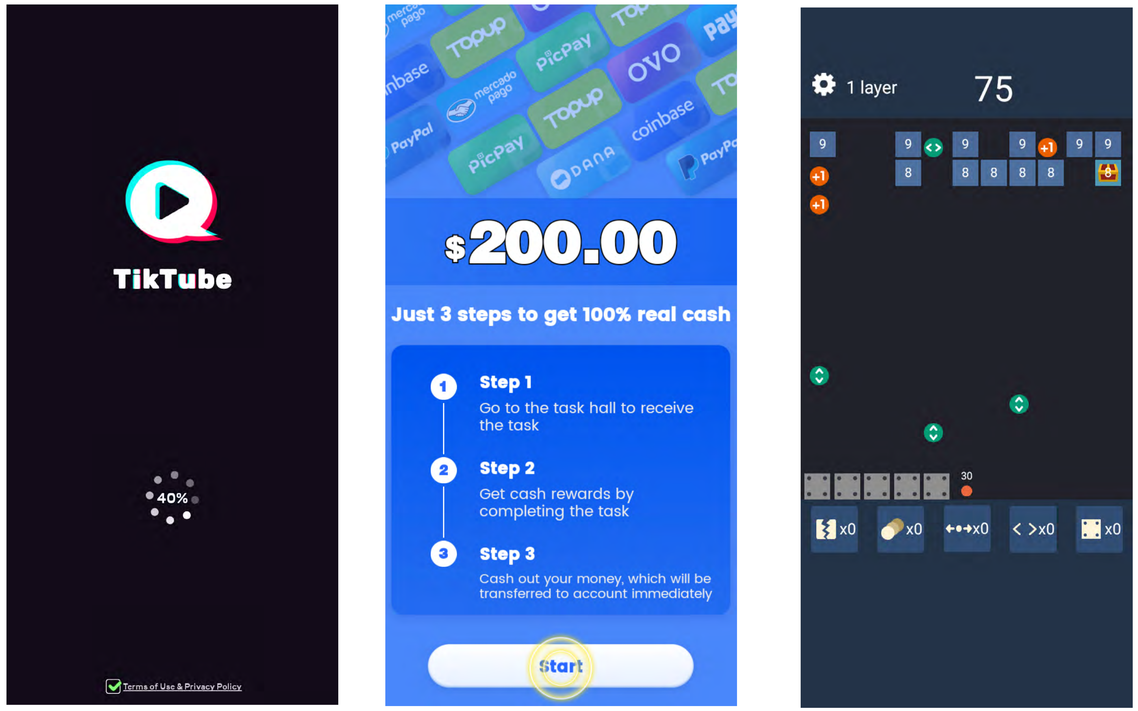
During the second half of 2023, ESET telemetry reported a significant surge in Android Spyware detections, rising by 89%. This increase was primarily due to a mobile marketing software development kit (SDK), identified as SpinOk Spyware by ESET. Surprisingly, this SDK was incorporated into numerous legitimate Android applications, including many available on official app marketplaces. As a result, SpinOk Spyware climbed to seventh place in the Top 10 Android detections for H2 2023, becoming the most prevalent type of Spyware for the period – almost a third of all Spyware detections seen by ESET telemetry consisted of SpinOk.

Apps in which ESET and other cybersecurity vendors detect the SpinOk spyware contain a specific version of a mobile marketing SDK provided by a company named OKSpin. SDKs can be integrated into mobile apps to aid developers and marketers in collecting user data, analyzing user behavior, delivering personalized content, and executing other marketing strategies. In this instance, the OKSpin SDK offered app developers a gaming platform intended to monetize app traffic. Developers could embed it into a wide variety of apps and games, including those on official Android marketplaces. However, once an app with that OKSpin SDK is installed, it operates like spyware, connecting to a command-and-control server and extracting a range of data from the device, including potentially sensitive clipboard contents.

SpinOk also identifies emulated environments: it does so by analyzing data collected from the device's gyroscope and magnetometer. If it determines that it is



Android/SpinOK detection trend in H2 2023, seven-day moving average



Examples of various apps containing the SDK that behaves as spyware

in a virtualized environment, it changes its behavior to avoid detection by sandboxes and researchers.

Cybersecurity company **Doctor Web** identified 101 apps containing the SpinOk Spyware on Google Play, and although all of them were taken down from this platform, ESET telemetry continued to detect a significant number of such apps installed on Android devices worldwide. After Doctor Web's findings were published, OKSpin updated its module.

The question remains, how did an SDK behaving as spyware find its way into so many apps, installed over 421 million times? Despite its significant presence in the mobile marketing sphere, OKSpin maintains a low-profile online presence. The company does not offer any contact details on its website, but we were able to find it **registered in Hong Kong**. Its given address is shared by a multitude of other companies, all claiming to occupy the same room within the **same office building** in Hong Kong. This suggests that OKSpin operates as a **letterbox company** and its address is used only for receiving mail and creating a semblance of physical presence in Hong Kong, while the actual business operations may be conducted elsewhere. Adding to the intrigue, in the **Offshore Leaks report**, which exposed international tax fraud, there is a company registered in a room adjacent to OKSpin's claimed location.

A **representative** from an app that used the SDK provided by OKSpin shared their experience, shedding light on how the SDK found its way into numerous applications. According to the representative, their initial contact with OKSpin was through a business development agent who proposed a "revenue growth program". The app developer confessed to failing to conduct thorough due diligence: they did not properly assess the third-party SDK before incorporating it into their app, which led to their legitimate app being removed from Google Play. Following the removal of the SDK, they then had to navigate a protracted process to have their app reinstated on the platform.

The case of SpinOk highlights a prevalent issue where a typical user downloading an app from an official store may not be able to discern whether the app contains malware or potentially unwanted elements. In such scenarios, a cybersecurity app is a valuable tool for detecting potential threats. Furthermore, this case serves as a cautionary tale for app developers, underscoring the risks associated with hasty and uninformed integration of third-party technology, which can disrupt their revenue stream and potentially lead to complications with their standing on official app stores.

The described surge of detections in the Spyware category, driven by SpinOk, stood out against the backdrop of a general decline in the detection of other Android threats, and is responsible for the overall rise of Android detections in H2 2023 by 22%. Adware, a constant threat in the Android environment, contributed to 36% of total detections in H2. This enduring prevalence of Adware can be traced to the pervasive use of free mobile games, which are often laden with intrusive ads. Clickers exhibited a significant upward trend, with an increase of 63% in detections. The rise in Clickers can also be linked to the growing distribution of apps loaded with ads, a strategy proving to be lucrative for cybercriminals. Nonetheless, HiddenApps remained the most widespread Android detection, even though there was a small decline of 3% in their detection rate. The only other category that recorded an increase in detections was Stalkerware, by 5%.

Adware, Clickers, and HiddenApps represent distinct Android detection types, each exploiting advertisements in unique ways. Adware primarily functions by displaying unsolicited ads on a user's device. In contrast, HiddenApps cleverly conceal themselves on a device post installation and can execute various malicious – or at least unwanted – activities, including the display of intrusive ads. Clickers, on the other hand, are designed to fraudulently generate ad revenue through automated ad-clicking, unbeknownst to the user. This differentiation explains the distinction between Hiddad trojan and Hiddad PUA, both listed in the Top 10 Android detections in H2 2023. While Hiddad trojan falls under the HiddenApps category, Hiddad PUA is classified as a potentially unwanted application (PUA). Despite their similarities, these two detections exhibit slightly different behaviors on Android devices.

Financial threats, which encompass Banking malware and Cryptostealers, recorded a 14% decrease, thus continuing their downward trajectory from H1 2023. The second half of 2023 also saw a considerable decrease in detections of SMS threats (23%), Ransomware (22%), Cryptominers (10%), and ScamApps (9%).

EXPERT COMMENT

The SpinOk case serves as a reminder for app developers about the need for caution when deciding to incorporate third-party technology into their apps. It's common for developers to be approached by third-party tech providers, but it's crucial to evaluate these technologies thoroughly to ensure that they are secure and suitable for their apps.

Ensuring the security of an SDK involves a series of steps, starting with a comprehensive investigation of the provider's reliability. This involves understanding the SDK's functionality, examining its documentation, and, if feasible, scrutinizing the source code for any anomalies. Developers should utilize static analysis tools to unearth unwanted behavior and potential vulnerabilities, and keep an eye on network traffic to spot any unexpected data transfers. They can also scan their own apps with reputable security products after a test integration with the third-party SDK under consideration. It's advantageous to verify whether the SDK or its provider has any security certifications or audits, and feedback from developer forums or groups should be considered. Prior to integrating an SDK into apps, we advise developers to conduct a test in a safe environment to assess its behavior and performance. Remember, integrating an SDK into your app gives it access to all of your app's data, so if resources for such evaluations are lacking, it's best to avoid using third-party SDKs.

Lukáš Štefanko, ESET Senior Malware Researcher

IoT Botnets

Who killed Mozi?

ESET researchers discovered and analyzed a kill switch that had taken down one of the most prolific IoT botnets.

For over two years, we've been writing in ESET Threat Reports about the Mozi IoT botnet, reporting mostly on its gradual descent on autopilot. In August 2023, the botnet experienced an unanticipated nosedive in activity. First, it vanished from the radar in India (on August 8, 2023) and then a week later in China (August 16) – countries that hosted the lion's share of the enslaved devices. Our deeper analysis showed that this was a deliberate takedown that could have been done by only two entities.

The originators of the Mozi botnet were **apprehended** by Chinese law enforcement in July 2021. Since then, the botnet continued exploiting vulnerabilities and infesting hundreds of thousands of new IoT devices each year but, unsurprisingly, there was no apparent use of the aggregated network and no updates to the Mozi bot code being propagated across it.

Mozi mostly compromises vulnerable Netgear DGN devices (**EDB-25978**), DASAN Networks GPON home routers (**CVE-2018-10562**), D-Link routers (**CVE-2015-2051**), and Jaws web servers (**EDB-41471**), but its spreading powers eroded over time. Between January and April 2022, the botnet added almost 500,000 new and unique minions, mostly from China and India. In the following four months that number already dropped to 383,000 and in the last third of 2022, it slid again to just 289,000 new bots.

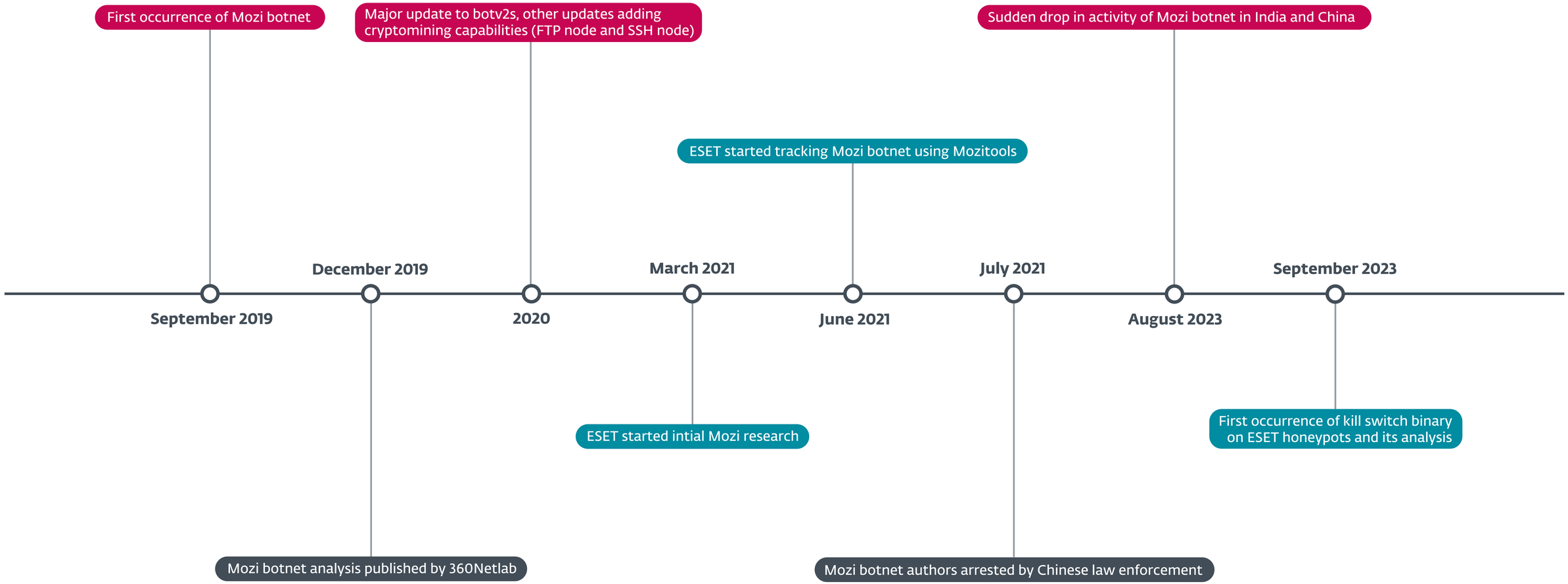
This trend could theoretically continue until Mozi couldn't find any more devices to compromise. But it's downfall came much faster. In August 2023, Mozi bots unexpectedly stopped propagating and the number of unique IPs seen within our honeypots had nosedived by 89% within a few days.

Our investigation into the sudden collapse led us to the discovery of a control payload (a configuration file) that worked as a kill switch. Upon delivery, it stopped all attempts to propagate the malware further and stripped Mozi bots of most of their functionality.

```
int __fastcall recursive_dir_crawler_sub_EA24(const char *a1, int a2)
{
  int v4; // r6
  int v6; // r0
  int v7; // r4
  int v8; // r5
  int v9; // r0
  int v10; // r0
  _BYTE v11[1024]; // [sp+0h] [bp-818h] BYREF
  char v12[1048]; // [sp+400h] [bp-418h] BYREF

  v4 = _GI_opendir();
  if ( !v4 )
    return 0;
  while ( 1 )
  {
    v6 = _GI_readdir(v4);
    v7 = v6;
    if ( !v6 )
      break;
    v8 = v6 + 11;
    if ( strcmp(v6 + 11, ".") && strcmp(v7 + 11, "..") )
    {
      v9 = *(unsigned __int8 *)(v7 + 10);
      if ( v9 == 8 )
      {
        v10 = _GI_strrchr(v7 + 11, 46);
        if ( v10 )
        {
          if ( !strcmp(v10, ".sh") )
          {
            memset(v11, 0, sizeof(v11));
            _GI_sprintf(v11, "%s/%s", a1, (const char *)(v7 + 11));
            processSHfile_sub_E848(v11, a2);

          }
        }
      }
      else if ( v9 == 4 )
      {
        memset(v12, 0, 1024);
        _GI_strcpy(v12, a1);
        strcat(v12, "/");
        _GI_strcat(v12, v8);
        if ( !_GI_strstr(v12, "/proc/")
          && !_GI_strstr(v12, "/tmp/")
          && !_GI_strstr(v12, "/var/")
          && !_GI_strstr(v12, "/lib/")
          && !_GI_strstr(v12, "/dev/")
          && !_GI_strstr(v12, "/sys/") )
        {
          recursive_dir_crawler_sub_EA24(v12, a2);
        }
      }
    }
  }
  _GI_closedir(v4);
  return 1;
}
```

```
int __fastcall recursive_dir_crawler_sub_8A60(const char *a1, int a2)
{
  int v4; // r6
  int v6; // r0
  int v7; // r4
  int v8; // r5
  int v9; // r0
  int v10; // r0
  _BYTE v11[1024]; // [sp+0h] [bp-818h] BYREF
  char v12[1048]; // [sp+400h] [bp-418h] BYREF

  v4 = _GI_opendir();
  if ( !v4 )
    return 0;
  while ( 1 )
  {
    v6 = _GI_readdir(v4);
    v7 = v6;
    if ( !v6 )
      break;
    v8 = v6 + 11;
    if ( strcmp(v6 + 11, ".") && strcmp(v7 + 11, "..") )
    {
      v9 = *(unsigned __int8 *)(v7 + 10);
      if ( v9 == 8 )
      {
        v10 = _GI_strrchr(v7 + 11, 46);
        if ( v10 )
        {
          if ( !strcmp(v10, ".sh") )
          {
            memset(v11, 0, sizeof(v11));
            _GI_sprintf(v11, "%s/%s", a1, (const char *)(v7 + 11));
            if ( !access(v11, 2) )
            {
              if ( !sub_898C() )
              {
                sub_83E0(v11, a2);
                sub_F3E4(0);
              }
              sub_101B4(1);
            }
          }
        }
      }
      else if ( v9 == 4 )
      {
        memset(v12, 0, 1024);
        _GI_strcpy(v12, a1);
        strcat(v12, "/");
        _GI_strcat(v12, v8);
        if ( !_GI_strstr(v12, "/proc")
          && !_GI_strstr(v12, "/haha")
          && !_GI_strstr(v12, "/tmp")
          && !_GI_strstr(v12, "/var")
          && !_GI_strstr(v12, "/lib")
          && !_GI_strstr(v12, "/dev")
          && !_GI_strstr(v12, "/sys") )
        {
          recursive_dir_crawler_sub_8A60(v12, a2);
        }
      }
    }
  }
  _GI_closedir(v4);
  return 1;
}
```

Code snippets of the original Mozi sample (left) vs kill switch sample seen in 2023 (right)



Mozi timeline

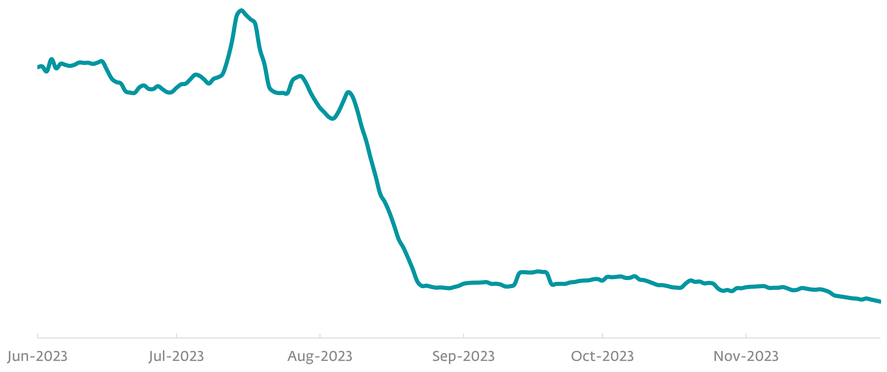
ESET researchers first spotted the kill switch inside a user datagram protocol (UDP) message, which was missing the typical encapsulation of BitTorrent's distributed sloppy hash table (BT-DHT) protocol. The person behind the takedown sent the control payload eight times to each available bot, always instructing the device to download and install an update of itself via HTTP.

The control payload also demonstrated several other functions such as killing the parent process and replacing the original Mozi file with itself, disabling system services such as sshd and Dropbear, executing router/device configuration commands and disabling access to a specific set of ports.

Despite the drastic reduction in functionality, Mozi bots have maintained persistence. They also pinged a remote server, probably for statistical purposes. Both these actions indicate that Mozi's sudden demise was in fact a deliberate and calculated takedown. Upon closer inspection, the kill switch shows a strong connection to the botnet's original source code and use of correct private keys to sign the binaries.

Based on these facts, we hypothesize about two potential actors, who could stand behind the castration of the botnet: the original botnet creators, or Chinese law enforcement forcing the cooperation of the creators.

The demise of one of the most prolific IoT botnets provided a wealth of cyberforensic and technical information on how such botnets are created, operated, and dismantled. In the coming months, ESET researchers will publish a detailed analysis on WeLiveSecurity.com.



Sudden drop in Mozi activity globally in H2 2023, seven-day moving average

EXPERT COMMENT

In recent years, IoT malware has slipped to the periphery of concern given its difficult detection, monitoring, and often unattainable mitigation. Still, threats like Mirai and its offspring represent a significant risk, as smart devices can easily be exploited to create large DDoS networks, anonymization networks, or be used for targeted tracking of VIP users.

Adequate security measures and standards for IoT protection are available, but not all manufacturers are willing to implement them – be the reason the costs, negligence, or anything else. Also, one cannot expect end users to be the force of change, because they are mostly indifferent to whether their router or security camera recorder is conducting some illicit activity, since it doesn't affect their experience.

Meanwhile, attackers keep pace with vulnerabilities, exploiting an ever-growing number of weaknesses and types of devices and all that with alarming proficiency. The significance of honeypots in monitoring such actions is therefore crucial, having been instrumental in observing occurrences like the shutdown of Mozi. Ultimately, understanding and addressing these and all the emerging potential cyberthreats will be critical to help increase the digital security of the future internet.

Milan Fránik, ESET malware researcher

Web threats AI

Abusing the ChatGPT name for malicious domains

A new economy has arisen around OpenAI API keys and the ChatGPT name, luring legitimate participants and cybercriminals alike.

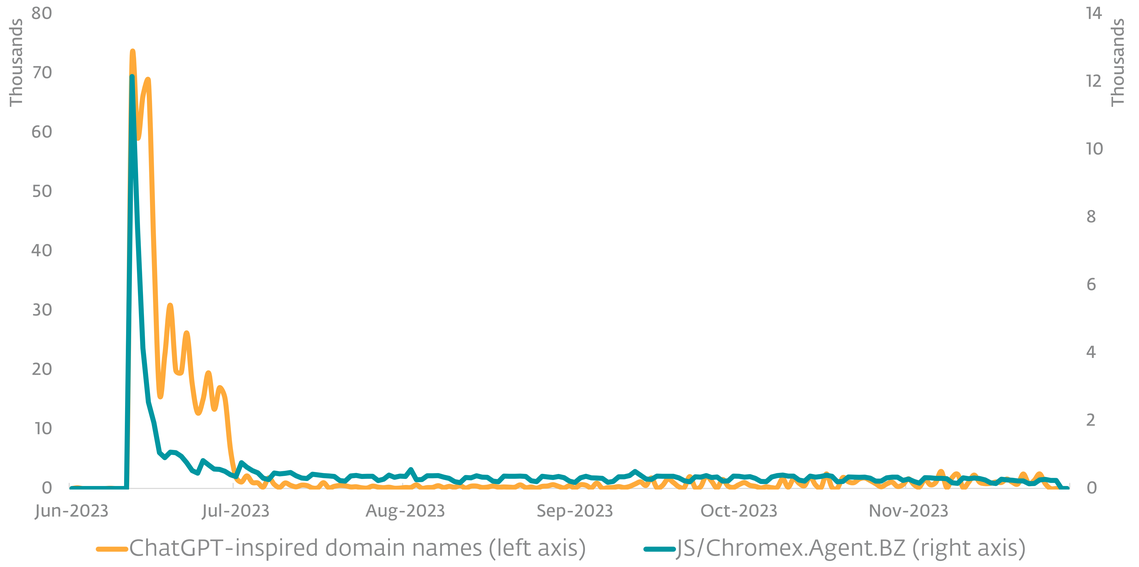
ESET telemetry in H2 2023 recorded blocking over 650,000 attempts to access malicious domains whose names include the string `chapgpt` or similar text in apparent reference to the ChatGPT chatbot. While most blocks happened in June, the succeeding months saw website visitors encountering a steady stream of malicious domains superficially offering OpenAI services.

Threats encountered via these domains include web apps that insecurely handle OpenAI API keys, and malicious Google Chrome browser extensions for ChatGPT.

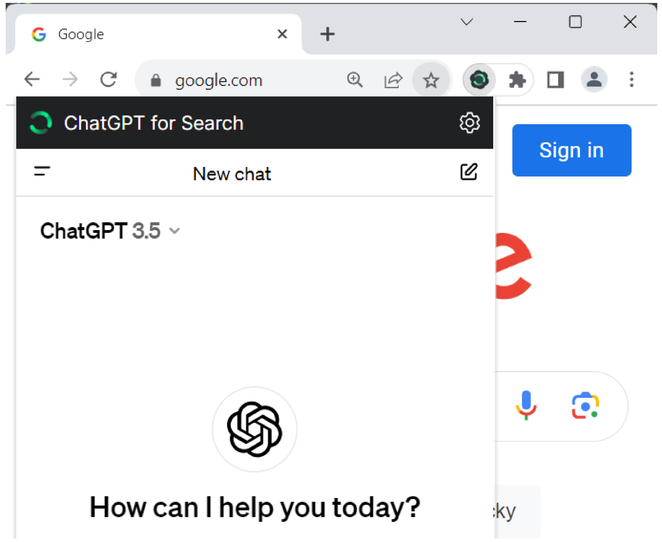
OpenAI offers an API that grants access to **AI models trained by OpenAI**, such as GPT, DALL·E, and Whisper. Using the API requires obtaining a key from OpenAI and sending it in an **HTTP Authoirzation header** to an `api.openai.com` endpoint. OpenAI then bills each API key user according to the number of tokens used.

Protecting the privacy of your API key is thus critical to ensuring that your API use stays within budget. However, some developers have built bring-your-own-key apps that request your OpenAI API key, purportedly to make calls to `api.openai.com` on your behalf. If the app sends your key to the developer's server, there may be little to no guarantee that your key will not be leaked or misused, even if the call to the OpenAI API is also made. This is why OpenAI strongly **exhorts**: "**Remember that your API key is a secret!** Do not share it with others or expose it in any client-side code (browsers, apps)."

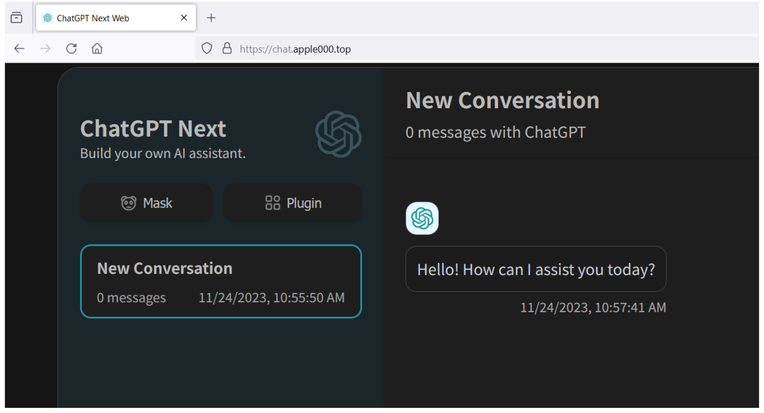
In one case, we noticed that a ChatGPT web app on `chat.apple000[.]top` asks users for their OpenAI API keys and sends them to its own server.



Detections of malicious ChatGPT-inspired domain names and JS/Chromex.Agent.BZ in H2 2023



ChatGPT for Search Chrome browser extension detected as JS/Chromex.Agent.BZ



A ChatGPT web app that sends OpenAI API keys to its own server

This web app links to the **open-source code in GitHub** from which it was built. A **Censys query** for HTML web pages that use the title "ChatGPT Next Web" suggests that over 7,000 servers host a copy of this web app. Whether these copies were created as a part of campaigns phishing for OpenAI API keys or were exposed on the internet for another reason cannot be determined with certainty; however, we strongly discourage entering your OpenAI API key into any app that sends it to an untrusted server.

Apart from such web apps, almost all blocks of malicious ChatGPT-inspired domain names in the second half of 2023 were related to Chrome extensions detected as JS/Chromex.Agent.BZ – a detection first seen in June.

For example, we saw `gptforchrome[.]com` leading to the malicious extension **ChatGPT for Search - Support GPT-4** in the Chrome Web Store, which we have reported to Google. In June, a developer also **reported** that this extension was potentially malicious.

This Chrome extension uses an **extension service worker** to import JavaScript from a file called `tracker.js`, which periodically sends the following information to the `gptforchrome[.]com` server:

- extension ID,
- extension version,
- unique user ID assigned by the extension, and
- current timestamp.

If the server sends a URL in response, the extension can display it in a new browser tab. This functionality, undisclosed by the developer, could be a conduit to malicious web pages.

EXPERT COMMENT

Deleting malicious browser extensions may not be enough to prevent attempts at re-compromise if you have turned on sync in your browser. Whenever the sync process runs, it attempts to make browser data – such as extensions – from other devices available in the browser on your current device. Make sure to delete malicious browser extensions on all your devices, especially if you have enabled sync. Even better is to carefully vet browser extensions before installing them and to use a reliable, multilayered security solution that can detect them.

Jiří Kropáč, ESET Director of Threat Detection

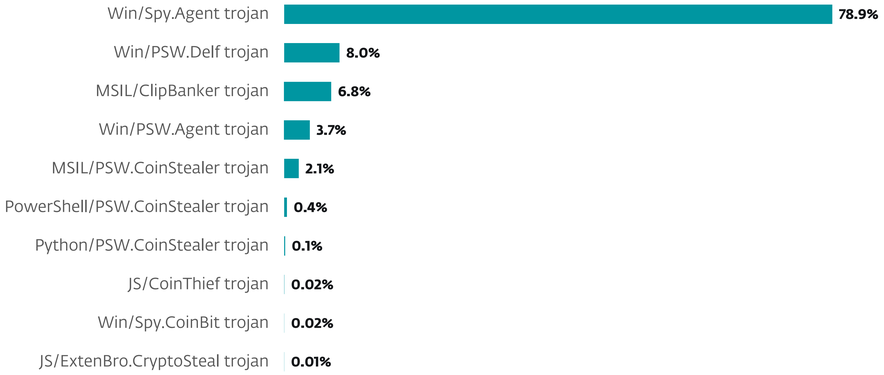
Cryptocurrency threats Infostealers Malware-as-a-service

Lumma Stealer takes the cryptostealer threat landscape by storm

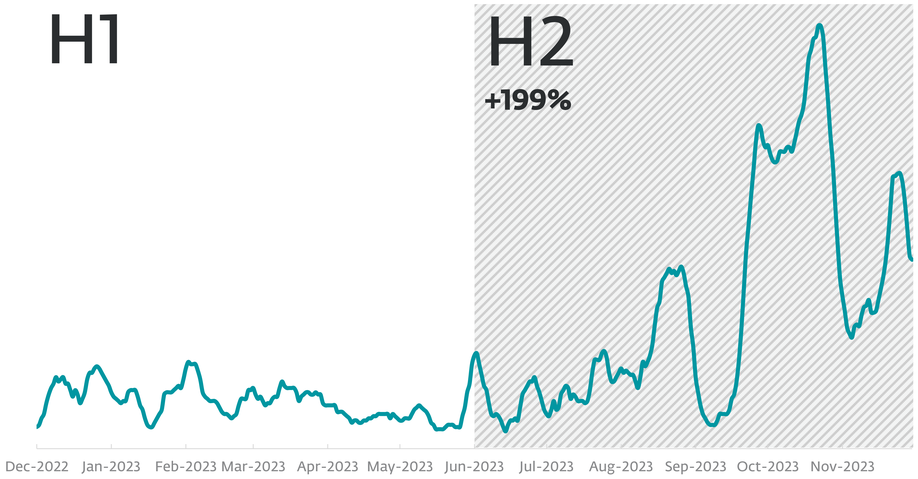
Illicit cryptomining may be on its way out, but Lumma Stealer's success shows that cryptowallets remain in the sights of cybercriminals.

H2 2023 continued the phenomenon described in the previous **Threat Report**: the exchange rate of bitcoin kept going up, yet cryptocurrency threats failed to match this trend. However, while cryptominers – which make up the majority of cryptocurrency threats detected by ESET – experienced yet another steep decline (down by 21%), cryptostealers were on the rise. In H2 2023, these threats grew by more than 68%. Thankfully, we cannot speak of a cryptostealing renaissance just yet, as this sudden increase was caused by just one specific threat, which accounted for almost 80% of detections in this category – the Win/Spy.Agent.PRG trojan.

By matching the samples registered in ESET telemetry data and the samples found on VirusTotal, we determined that Win/Spy.Agent.PRG is a malware-as-a-service (MaaS) infostealer called **Lumma Stealer**. Also known as LummaC2 Stealer, this malware is written in C and targets cryptocurrency wallets, user credentials, and two-factor authentication browser extensions. It also exfiltrates information from compromised machines. Between H1 and H2 2023, the



Top 10 cryptostealer families in H2 2023 (% of Cryptostealer detections)



Lumma Stealer detection trend in H1 and H2 2023, seven-day moving average

number of Lumma Stealer detections tripled. We registered the highest rate of Win/Spy.Agent.PRG detections in the latter half of H2, peaking in October.

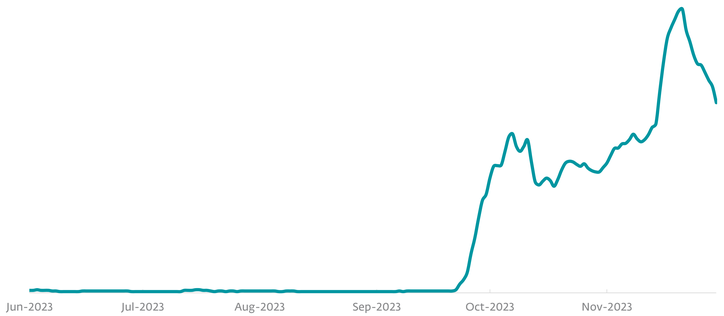
This up-and-coming MaaS first appeared in the wild in August 2022 and is available for sale on underground forums and on Telegram. Multiple tiers are **offered**, with prices ranging from USD 250 up to USD 20,000; the highest tier even gives buyers access to the infostealer's source code and allows them to sell the malware themselves.

Interestingly, there are ESET detections of Win/Spy.Agent.PRG from before 2022. Based on the information shared on X (formerly Twitter) by the cybersecurity company **Sekoia.io** and the user **Fumik0_**, we conclude that the detections prior to 2022 belong to Mars, Arkei, and Vidar infostealers, whose common code base was later repurposed to create Lumma Stealer.

Being available for sale and not focusing purely on cryptostealing are very likely the main factors behind Lumma Stealer's popularity among cybercriminals. As we discussed in the RedLine Stealer section of the H1 2023 ESET Threat Report, ready-made malware solutions contribute to the proliferation of malicious campaigns because they make the malware available even to potentially less technically skilled threat actors. Offering a broader range of functions then serves to render Lumma Stealer even more attractive as a product.

Although this infostealer spreads mainly through cracked installations of software such as VLC and ChatGPT, it has been seen utilizing other distribution vectors as well. For example, in February 2023, a Korean YouTuber was **targeted** via a spearphishing email impersonating the video game company Bandai Namco. Threat actors have also been spreading it via the **content delivery network** of the popular chat platform Discord. Furthermore, Lumma Stealer is one of the possible payloads of a recent **fake browser update** campaign, in which a compromised website is made to display an overlay telling the victim that a browser update is necessary to access the site. Clicking the update button then delivers malware such as RedLine, Amadey, or the titular Lumma Stealer to the victim's machine.

At ESET, we have also seen Lumma Stealer being distributed by the Win/TrojanDownloader.Rugmi trojan. This malware is a loader with three types of components: a downloader that downloads an encrypted payload, a loader that runs the payload from internal resources, and another loader that runs the payload from an external file on the disk. Apart from Lumma Stealer, Win/TrojanDownloader.Rugmi is also used to deliver other infostealers, among them Vidar, Rescoms, and RecordBreaker. The detections of this loader skyrocketed in H2, going from single digit daily numbers to hundreds per day.



Win/TrojanDownloader.Rugmi detection trend in H2 2023, seven-day moving average

CRYPTOCURRENCY HEISTS AND SCAMS

Malware that targets cryptocurrencies may not be as common as before, but H2 2023 saw no lack of high-profile cryptocurrency-related cybercrime.

Cryptoscammers posing as NFT developers

The FBI issued a **warning** about criminals posing as legitimate NFT developers in order to steal the cryptocurrency funds of their victims. These scammers make posts claiming to offer limited NFT opportunities that lead to spoofed websites. Once victims try to make purchases via the website, the threat actors can steal the funds contained within their cryptocurrency wallets.

Lazarus linked to theft of roughly USD 900 million in cryptocurrency

Between July 2022 and July 2023, the Lazarus APT group **laundered** around USD 900 million in cryptocurrency through cross-chain crime: when criminals convert cryptocurrency assets from one token or blockchain to another, often in quick succession, to obfuscate the assets' origin.

Elon Musk cryptocurrency scams find a new platform

Scams posing as cryptocurrency giveaways by Elon Musk have for some time been quite notorious on X and Instagram. Now, they are finding a new audience on the video-sharing platform **TikTok**, using deep fakes of Musk interviews. In order to receive the advertised reward, users are asked to make activation deposits into scam sites, which then steal the payments.

USD 4.4 million in cryptocurrency stolen due to LastPass breach

In October, hackers used private keys and passphrases from leaked LastPass databases to **steal** USD 4.4 million in cryptocurrency. LastPass was breached twice in 2022, giving threat actors access to the company's customer data.

IoT Android Botnets

Android TV boxes under fire: Pandora builds a botnet for DDoS attacks

A new Mirai-based threat uses malicious streaming apps to enslave devices in Latin America.

Any device connected to the internet could become a target for cybercriminals. Smart TVs with their peripherals are no exception. In September 2023, a new IoT botnet sprang to life, which ESET detects as Android/Pandora. First described by **Doctor Web**, the threat compromises Android devices – most prominently Android TV boxes – with Mirai-based malware. The enslaved devices are then used by the botnet operators to run DDoS attacks.

According to ESET telemetry, Android/Pandora attempted to compromise tens of thousands of Android devices, with approximately a fifth of instances detected and blocked directly on victims' television sets by ESET Smart TV Security.

The biggest spike of activity was observed on September 8, with over two thousand attacks. After the initial wave, the activity dropped to about five hundred attacks daily. The most targeted region is Latin America, with Brazil leading the pack (20%), followed by Mexico (13%) and Peru (11%).

There are two possible delivery methods for the Android/Pandora malware. First is via malicious firmware updates that were preinstalled on the Android TV box by the reseller or downloaded and installed by an unaware victim.

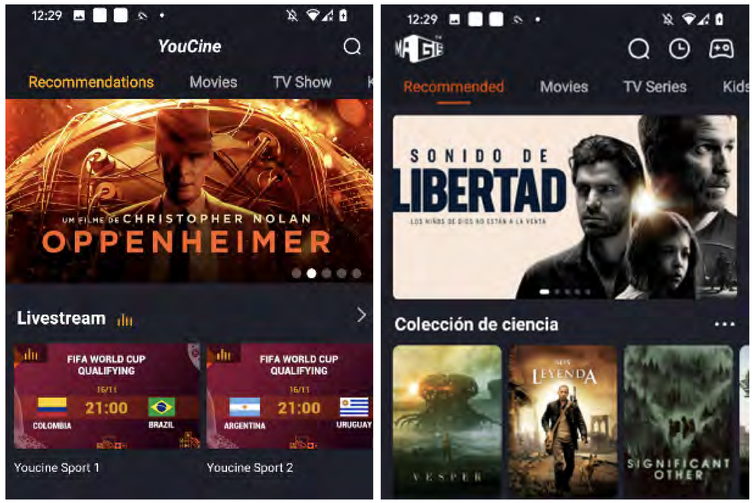
However, the main distribution channel seems to be websites spreading malicious apps with names such as MagisTV, Tele Latino, and YouCine. These are offered not only for TVs, smartphones, tablets and Android TV boxes, but also for TV sticks from Amazon and Xiaomi.

Upon installation, these apps offer streaming services and pirated content that can be accessed for free, on trial, or with a premium account. From the user's perspective, the app provides all the promised features and content without any obvious signs of malicious activity. Moreover, paying for the premium subscription lowers the willingness of a victim to voluntarily remove the malware from the device.

Android/Pandora detection trend from September 2023 to November 2023

ANDROID TV BOX

It's an IoT peripheral device – typically a box or a dongle – that users plug into their TV to gain access to a variety of streaming apps, or content, that is not natively supported by their television set.



User interface of the malicious apps

Although the list of app permissions doesn't seem to be intrusive or to hint at spyware functionality, if installed on a Smart TV, Pandora requests superuser or root rights for the application. For this to work, however, the device already needs to be rooted at the point of installation; the app does not try to root the device itself.

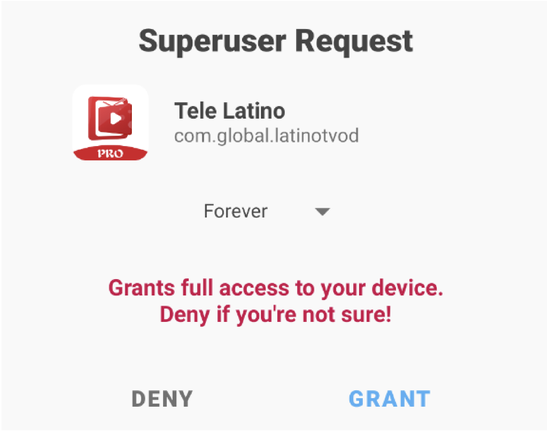
(Other) Mirai-based botnets

While the Pandora botnet was on the rise, other Mirai-based botnets tracked by ESET – including Gafgyt, BotenaGo, Dofloo, Tsunami, Zero, and others – seemed to lose steam. According to our telemetry, these networks of enslaved IoT devices caused "only" 7.5 million attacks in H2 2023, a notable 59% decrease compared to H1 2023. The highest number of those attacks were directed at the US (22%), Germany (7%), and the United Kingdom (7%).

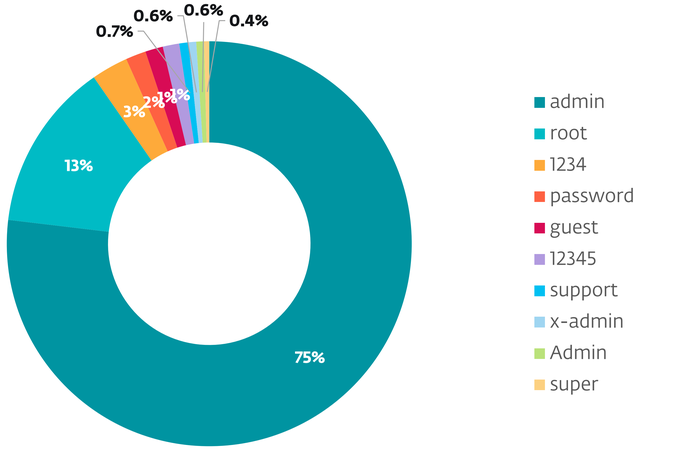
Somewhat counterintuitively, the number of servers delivering modified Mirai payloads for these botnets dropped by only 3% – just a few dozen machines – and the Mirai-based IoT armies have grown by 58% from 106,000 to over 168,000 between the first and second halves of 2023.

The largest share of that increase came from Egypt, which hosted close to 110,000 (65%) of all the detected compromised devices – a 164% jump compared to 42,000 (39%) seen in the first half of 2023. Looking at the other side of that equation, the greatest percentage of unique devices facing Mirai-based bot attacks were in Germany (16%), the US (9%), and Mexico (7%).

Mirai-based botnets have refreshed the list of exploited flaws in H2 2023 by adding CVE-2023-26801: this recently reported command injection vulnerability in several LB-LINK routers was the second most abused in the last six months and accounted for 10% of all detected attack attempts.



Pandora request for superuser (root) rights on an Android Smart TV



Top 10 most common weak IoT device passwords in 2023

Infostealers Web threats

Magecart, the ever-present phantom haunting e-commerce

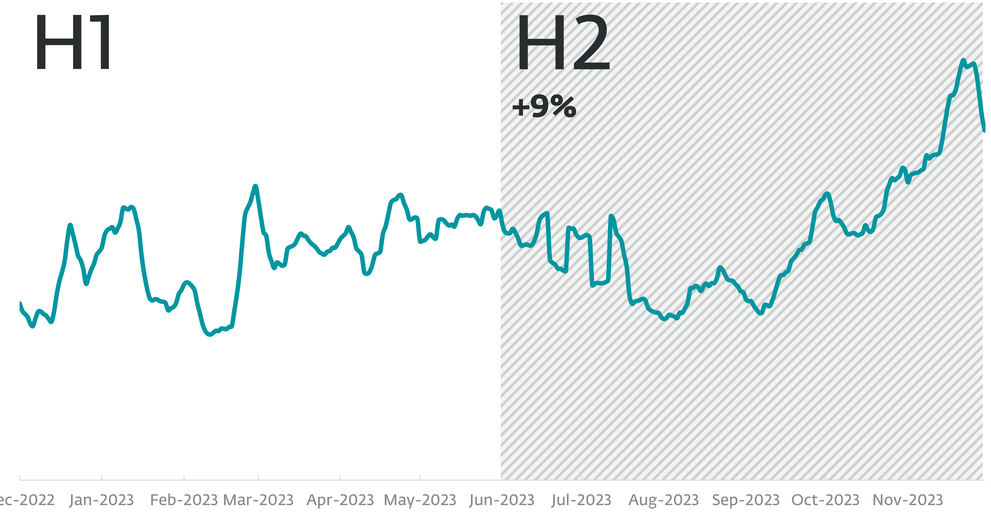
It seems there is never a prolonged period without notable Magecart attacks and H2 2023 was no exception.

Magecart has been successfully targeting online shopping and hospitality platforms since 2015 and shows no signs of stopping. On the contrary, based on ESET data, H2 2023 marks the second year of continuous growth for this malware. But what makes Magecart such a pervasive threat?

In ESET telemetry, Magecart detections fall under JS/Spy.Banker, which is categorized as a web skimmer – i.e., a malicious online script injected into the code of hacked or unpatched websites with the goal of stealing information from those who browse these websites. Magecart mostly goes after credit card data and targets websites hosted on Magento and WordPress platforms. There is no single threat actor behind Magecart attacks; ESET tracks under the one label the activity of the several groups that use Magecart.

This malware family consistently ranks in the top positions in our most-detected Infostealer statistics. In H2 2023, it was in second place, with detections counting in tens of thousands, the only threat with more detected activity being Agent Tesla. Still, it should be mentioned that since JS/Spy.Banker detections are based on the number of unique visits to a website, it will have a generally higher number of detections than threats distributed as email attachments or downloader payloads.

Nevertheless, there is little doubt that Magecart is a very prolific threat. Looking at our data, JS/Spy.Banker has been growing in numbers since the end of 2021 – the overall increase of its detections between 2021 and 2023 amounts to 343%. Zooming in on H2 2023, we can see that while the malware family did not grow dramatically this period (+9%), there was still an uptick

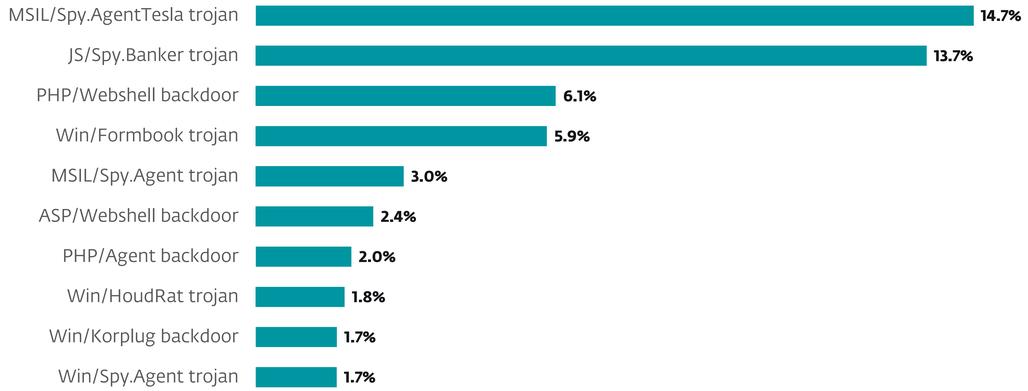


JS/Spy.Banker detection trend in H1 and H2 2023, seven-day moving average

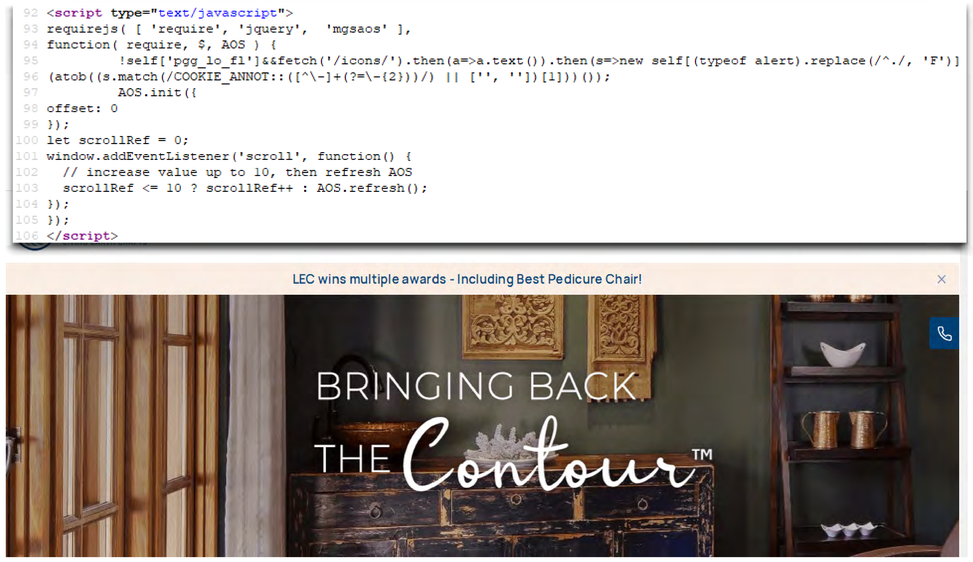
in detections starting in October and accelerating throughout November. Since the end of the year is also the time when people generally do a lot more online shopping due to the approaching holiday season, it comes as no surprise that Magecart rates would increase as well.

While Magecart attacks are not the most flashy or sophisticated forms of cybercrime out there, they have been successfully used by cybercriminals for years. Their simplicity works in their favor, using scripts that are relatively straightforward to code, while the myriads of unpatched websites make for easy prey. It also seems that the ongoing AI boom might be a boon to Magecart: researchers have **shown** that ChatGPT can be abused to write web-skimming scripts, which would make this type of malware accessible to a broader range of cybercriminal actors.

Apart from the obvious impact on the customers of a compromised website whose money and personal information gets into the hands of cybercriminals, Magecart attacks can be quite devastating to the targeted companies. Due to the loss of confidence of their clients, these businesses face monetary consequences, since fewer customers equals less revenue. There can also be legal ramifications: for example, in the EU, these companies can find themselves in violation of GDPR due to data leaks, which can lead to significant fines. In a recent **report**, IBM estimated that the average cost of a data breach in 2023 was USD 4.45 million.



Top 10 infostealer families in H2 2023 (% of Infostealer detections)



Website compromised by JS/Spy.Banker and the malicious code linked to the page

It is, however, very much possible to protect a business against Magecart skimmers. If you want to prevent your website from being compromised, we recommend that you make sure that your website servers and CMS are running up-to-date software, and that the accounts administering those resources are protected by strong authentication mechanisms (i.e., using strong passwords and two-factor authentication).

In H2 2023, there have also been some notable evolutions in the threat actors' approach towards compromising e-commerce websites. This is another reason why Magecart is, at least for now, here to stay – it does not remain stagnant.

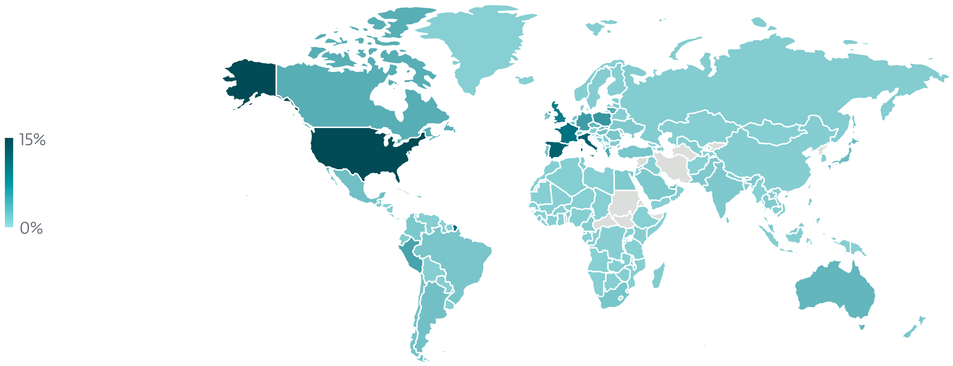
Analysts at Akamai published two research pieces on these more sophisticated attacks. **One** of them describes how cybercriminals leverage legitimate websites to attack others. First, they inject Magecart code into a vulnerable site, using it to host the code, then they attack their actual target by employing malicious JavaScript code snippets as loaders that get the full code from the previously compromised vulnerable website.

We have also been encountering scripts that function similarly to the ones described in the linked article – if a skimmer is not located directly on the targeted website, ESET products usually detect the script leading to it. These scripts often belong to the JS/Redirector or JS/Agent families.

The other research piece talks about hiding Magecart scripts in 404 error pages: once a victim wants to pay for the goods they're buying, a malicious piece of code calls the 404 page with the skimmer script, which then overlays a lookalike payment form on the checkout page to capture the user data. At ESET, we detect the code snippet loader hidden within the 404 pages as JS/Spy.Banker.MC.

The abuse of HTML error pages is an established cybercriminal technique. For example, the now-defunct TeslaCrypt ransomware used to hide C&C commands in HTML tags. Luckily, Magecart scripts are usually easily recognized by cybersecurity products even though the threat actors try to hide them in creative ways: in case of an encounter with a compromised site, it would be detected and blocked by the ESET detection engine.

Magecart attacks are the most prevalent in the US, which registered almost 15% of JS/Spy.Banker attack attempts. This threat is actually the most detected infostealer in the United States, accounting for a third of all Infostealer detections in the country. This is also the case in Italy, the country with the second highest numbers of JS/Spy.Banker detections globally (11%). This threat represents 42% of Infostealer detections ESET telemetry registered there



Geographic distribution of JS/Spy.Banker detections in H2 2023

OTHER INFOSTEALER INSIGHTS

macOS password stealers on the rise

The macOS platform is generally targeted by adware and Potentially Unwanted Applications (PUAs); however, ESET telemetry has detected a worrying trend in H2 2023, where Password Stealing Ware (PSW) on macOS experienced a staggering 290% increase. PSWs, which are just one subset of infostealers detected on the macOS platform by ESET, are a type of malware designed to steal sensitive data from users' systems. Working quietly in the background, PSWs can record keystrokes, capture screenshots, or directly steal saved passwords from the users' browsers or other applications.

Fueling this surge are numerous new PSWs discovered by security researchers in H2 2023, such as **Metastealer**, **Pureland**, **Realst Infostealer**, **ShadowVault macOS Stealer**, **MacStealer**, and **AMOS**. Posing as specific files or useful apps, these infostealers spread via malicious websites, malvertising, and phishing. In addition to stealing passwords and exfiltrating various file types, they can also extract credit card information and target cryptocurrency wallets. Despite the sharp rise in PSWs, even though the total numbers are rather low, it's worth noting that the overall category of Infostealers on macOS has increased only slightly in H2 2023 by 10%.

Qbot operations disrupted

In August 2023, the notorious Qbot malware (also known as Qakbot) was **taken down** thanks to a coordinated international operation conducted by several national law enforcement agencies, and organizations such as Europol and the FBI. In the process, the authorities seized nearly EUR 8 million in cryptocurrencies. The examination of Qbot infrastructure revealed over 700,000 compromised computers worldwide.

Looking at ESET telemetry data, the malware was already mostly inactive by that time. We have not seen much Qbot activity since the middle of the year – the last campaign we tracked occurred in the latter half of June. We have occasionally noticed some Qbot C&C server detections since the takedown took place, but some of the servers in question had already been neutralized by the authorities.

Web threats

Website visitors under siege by malicious scripts

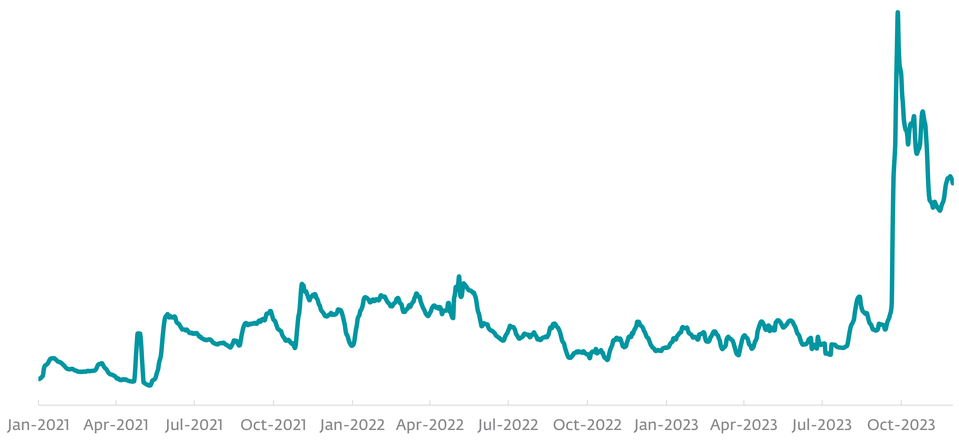
The rise in JS/Agent detections reveals that almost 45,000 websites have fallen victim to malicious JavaScript code.

A threat contender has risen 111% to take second place among all threats recorded by ESET telemetry in H2 2023: JS/Agent. This detection name refers to malicious JavaScript code loaded by compromised web pages. From September 2023, we have observed a massive wave of JS/Agent detections – the likes of which have not been seen in the past three years.

As can be seen in the **Magecart** section, threat actors are known to attempt to exploit website vulnerabilities that may allow them to inject malicious JavaScript code into web pages. Such code is typically the beginning of a chain of scripts that allows attackers to download further malicious scripts, which can take over admin access to the site, install malicious web plugins, or deliver payloads such as backdoors.

Most of the increase in JS/Agent detections was due to the 136% growth of the JS/Agent.PHC variant and the appearance of the .RAN and .RAW variants. The .PHC variant includes the ndsj malware Sucuri reported on in June 2022. This malware consists of lightly obfuscated JavaScript that executes the next stage, usually a malicious PHP script already present on the compromised web server and whose job is to fetch a JavaScript payload from a C&C server.

The most prevalent detections of JS/Agent.PHC were in Japan (10%), Spain (8%), and the US (6%). From September to November, ESET telemetry recorded 14,500 websites compromised with the .PHC variant.



JS/Agent detection trend from January 2021 to November 2023, seven-day moving average

EXPERT COMMENT

Website admins should be wary of which plugins they install, especially for WordPress, as this dramatically increases the attack surface. Make sure to put in place a patching policy that requires admins to apply updates as soon as they are available. Teach your web developers about secure coding practices such as data sanitization, secure HTTP headers, and a Content Security Policy to prevent multiple types of script injection attacks.

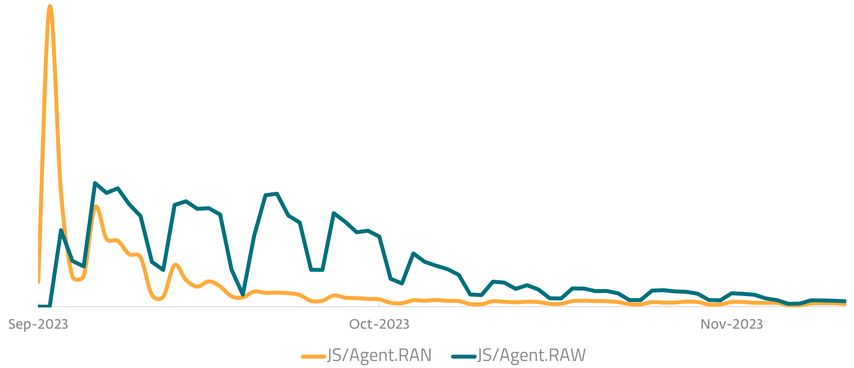
Ján Adámek, ESET Senior Detection Engineer

The .RAN and .RAW variants include malicious JavaScript detected as part of a **Balada Injector campaign** reported by Sucuri in October 2023. Both these variants are distinct, lightly obfuscated scripts but with a similar purpose: downloading the next-stage JavaScript code from a C&C server. For example, some .RAN samples download a script from `stay.decentralappps[.]com`, and some .RAW samples reach out to `cdn.statisticscripts[.]com`.

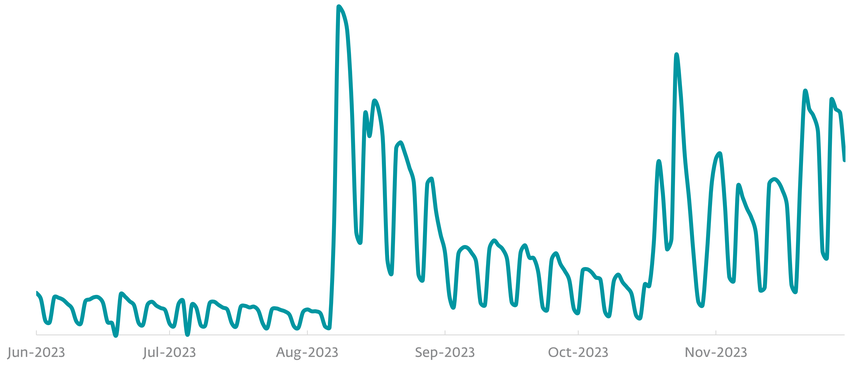
The .RAN variant accounts for the spike on September 21, the largest one seen in the past three years. Successive waves of detections are mainly due to the RAW variant.

The .RAN and .RAW variants and 37 other related JS/Agent variants add up to over 900,000 detections in the second half of 2023. This indicates that many websites have been compromised in this period, probably due to attackers exploiting website vulnerabilities such as **CVE-2023-3169**, which affects specific versions of the **tagDiv Composer** plugin for WordPress, as reported in our **ESET Security Forum**.

The most prevalent detections of these 39 variants were in Italy (10%), Czechia (7%), and Poland (7%). From September to November, ESET telemetry recorded 6,700 websites compromised with the .RAN variant, and 23,500 with the .RAW variant.



JS/Agent.RAN and JS/Agent.RAW detection trends from September 2023 to November 2023



JS/Agent.PHC detection trend in H2 2023

Ransomware

Cl0p and its MOVEit hack: A mass-spreading yet targeted attack

How exploitation of a two-year-old zero day vulnerability by one actor caused a global cybersecurity nightmare.

The biggest ransomware story of H2 2023 doesn't even include ransomware per se. What qualifies the so-called "MOVEit hack" for this chapter is that it was carried out by a cybercriminal group known as Cl0p (aka Lace Tempest, FIN11, TA505, or Evil Corp) infamous for using ransomware in large-scale hacks. However, its latest campaign reached such proportions that encrypting every victim was probably too laborious even for this group.

It all started on May 27, the first day of the US Memorial Day long weekend, when the cybercriminals launched a massive exploitation of a zero-day vulnerability (CVE-2023-34362) in the widely used managed transfer app MOVEit. The flaw, which the attackers probably sat on since 2021, allowed them to escalate their privileges and gain unauthorized access to stored and transferred data.

About a week later, the range of impact started to become apparent as information about high-profile victims – such as the BBC, British Airways, and Aer Lingus – started rolling in. It was about the same time that Microsoft first attributed the attack to the Cl0p gang, which in turn confirmed it via media and bragged that the number of compromised companies was in the hundreds.

Six months later, the number of affected organizations has surpassed 2,600 – at least according to Emsisoft's monitoring. The list of victims includes US governmental agencies, schools and universities, healthcare institutions, and also global corporations such as Sony, EY, and PricewaterhouseCoopers. If the 83 million records of individuals that were leaked are multiplied by IBM's average cost of USD 165 per breached record, that puts the estimated financial

EXPERT COMMENT

Looking back at 2023, we can safely say that ransomware was more active than in 2022. Based on published information and the incidents we investigated, the ransom demands grew also, although it is difficult to assess whether this was due to the greed of the attackers; victims being less willing to pay, which in turn forced attackers to look for revenue in masses; or if the adjustment was influenced by high inflation.

The story that stood out most to us was surely the MOVEit hack. However, it wasn't just the size of the campaign that made it so prominent, but also the technical proficiency of the Cl0p gang that was behind the attack. These threat actors demonstrated they can find a new zero-day vulnerability, weaponize it, and wait for the opportune moment to deploy it.

In 2024, we expect most of the outlined trends to continue, with current major players focusing on expansion of their affiliate programs. By employing other cybercriminals within their schemes, notable families will limit the space for emergence of new competitors.

Jakub Souček, ESET Senior Malware Researcher

damage of the hack close to USD 14 billion. That's more than the USD 10 billion damage caused by the infamous **NotPetya incident**.

Early estimates say Cl0p could pull in as much as **USD 75–100 million** from its victims. Due to severity of the incident – and probably its heavy focus on the US and Canada – the US Department of State has **issued a USD 10 million bounty** for any information leading to the arrest and conviction of the perpetrators.

The MOVEit hack could also point to a new trend in the ransomware scene, as Cl0p started using the **clear web** to leak the stolen information. This move was first seen in June 2023 with the ALPHV ransomware gang (aka BlackCat) and makes this kind of cyberincident much more visible, increasing pressure on the victim. In an attempt to avoid takedowns, Cl0p also leaked part of the information via **torrents** due to the sheer volume of data stolen.

Two other new trends in H2 have been highlighted by the **FBI**. First was the deployment of two or more ransomware variants during the same incident, usually a choice of the AvosLocker, Diamond, Hive, Karakurt, LockBit, Quantum, and Royal families. Second was the use of wipers on top of data theft and ransomware encryption. This way attackers can corrupt data in compromised systems after a set time and thus further increase pressure on the victim.

CosmicBeetle replaces Scarab ransomware with its own ScRansom

In H2 2023, ESET researchers took a closer look at CosmicBeetle – a Turkish-speaking threat actor that uses the small Spacecolon (Sc) toolset to deploy ransomware all over the world.

ESET researchers also discovered a new ransomware strain in development, naming it ScRansom and attributing it with high confidence to the same threat actor. While at the time of our initial **publication** we haven't observed any in-the-wild attacks using ScRansom, the situation changed shortly afterwards and this variant is now the preferred ransomware deployed by the CosmicBeetle group, replacing it's former main payload choice - Scarab ransomware.

In some of its recent attacks, the threat actor modified the ransom note to impersonate LockBit and even set up a surface web leak site, mimicking LockBit's. There, they copied a few of the most recent LockBit victims and added some of their own. CosmicBeetle is likely abusing LockBit's well-known name in order increase pressure on its own victims.

To gain an initial foothold, CosmicBeetle uses several attack avenues, including RDP brute forcing and exploitation of the ZeroLogon vulnerability (**CVE-2020-1472**). With low confidence, ESET researchers also assess that CosmicBeetle may be abusing a vulnerability in FortiOS, based on a "Forti" string found in the code and the fact that the vast majority of its victims have devices running FortiOS in their environment.

The Spacecolon toolset consists of three tools: the main orchestrator called ScHackTool, used to deploy a small component ScInstaller, which in turn installs CosmicBeetle's backdoor ScService. The latter allows the attacker to execute commands, retrieve information about victims' systems and download and execute payloads – for details refer to our **original analysis**.

NOTABLE NEW PLAYERS AND REBRANDS

3AM

A new Rust-based ransomware made headlines in September, attracting researchers' attention mostly by being deployed as a backup variant after a failed attempt to run LockBit ransomware. Since then, 3AM has been used to attack more than a dozen other victims, spilling their information via a newly set up Tor leak site.

LostTrust

LostTrust ransomware is a likely rebrand of the MetaEncryptor ransomware used by the same cybercriminal actors.

SophosEncrypt

It is not uncommon for cybercriminals to try to pin their activity on cybersecurity researchers and organizations. SophosEncrypt is an example of ransomware where threat actors are trying to "sell" their product as if it came from a known security company, Sophos.

NoEscape

A new ransomware family called NoEscape has caught attention of researchers and media in July 2023. Based on code similarity in its encryptor, experts suggest it could be a rebrand of a once prominent ransomware strain, known as Avaddon, whose operators closed shop in 2021. According to the list on NoEscape's darkweb leak site, the NoEscape group has already compromised at least a hundred companies in H2 2023.

Hunters International

Is Hive back? In H2 2023, the new ransomware as a service operation named Hunters International was launched. Upon analyzing its encryptor, several security researchers found major code overlap with Hive – a criminal service that was **infiltrated and then dismantled** by law enforcement early in H1 2023. The threat actors behind the new Hunters International deny any relationship to Hive and claim they've bought and fixed the old code from the previous operators. As for victims, Hunters' leak site lists dozens of compromised organizations, mostly from the United States and Europe.

ARRESTED/CLOSED SHOP/DECRYPTED:

HACKED: **Trigona**

The Trigona ransomware gang saw their servers **infiltrated and wiped** by Ukrainian cyberactivists. The Ukrainian Cyber Alliance (UCA) also claimed that they exfiltrated source code, internal communication, database records, and other data from Trigona's systems. This might include decryption keys; however, UCA didn't provide any further updates.

ARRESTED: **Ragnar Locker**

In late October, law enforcement agents **took action** against the Ragnar Locker ransomware family, interviewing five suspects and arresting one key individual. Physical raids were conducted in Czechia, Spain, and Latvia; seizure of infrastructure took place in the Netherlands, Germany, and Sweden. The dark web site was also taken down, and replaced with information about the operation. Ragnar Locker had been active since 2019, attacking critical infrastructure including the Portuguese national carrier and a hospital in Israel.

LEAKED CODE: **HelloKitty**

Source code for more ransomware has been **leaked**, this time it seems by the malicious actors behind the HelloKitty family themselves. The code for the first version of their malware appeared on a Russian-speaking forum accompanied by claims of work on a new, more powerful encryptor. This leaked code can – and probably will – lead to a series of newcomers who will try to utilize the information.

ARRESTED: **LockBit (affiliate)**

While the **arrest** of a LockBit affiliate took place early in 2023, US authorities only unveiled the charges and expected penalty in June 2023. The US Department of Justice is asking the courts to send the Russian Ruslan Magomedovich Astamirov to jail for up to 25 years.

DECRYPTOR: **Key Group**

Based on flaws in its encryption scheme, researchers **created** a decryptor for the Key Group ransomware. The free tool helps victims hit by the early versions of the ransomware. Key Group has been active since 2023, and is labeled as a Russian-speaking actor.

DECRYPTOR: **Akira**

A decryption tool is also **available** for the Akira ransomware, which has been active since 2023 attacking various sectors across the globe.

BOUNTY: **Cl0p**

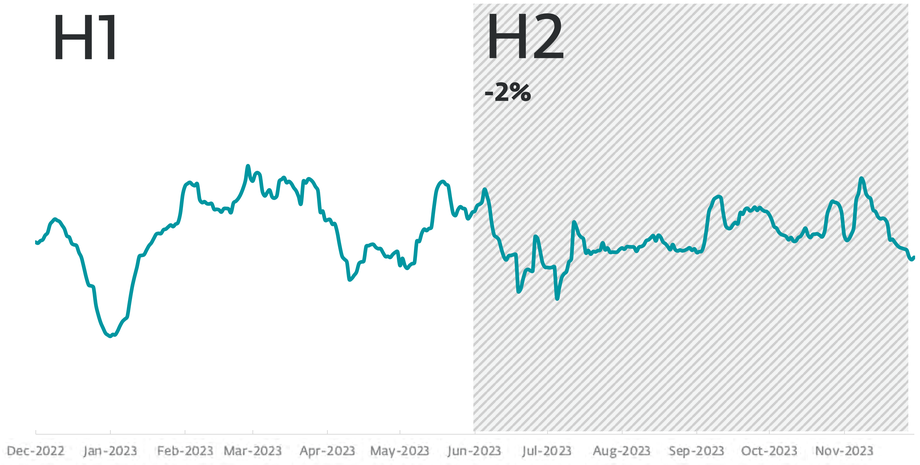
Due to the severity of the MOVEit hack the US Department of State has **issued** a USD 10 million bounty for any information leading to the arrest and conviction of the perpetrators known as the Cl0p gang.

ARRESTED: **MegaCortex, HIVE, LockerGoga, Dharma**

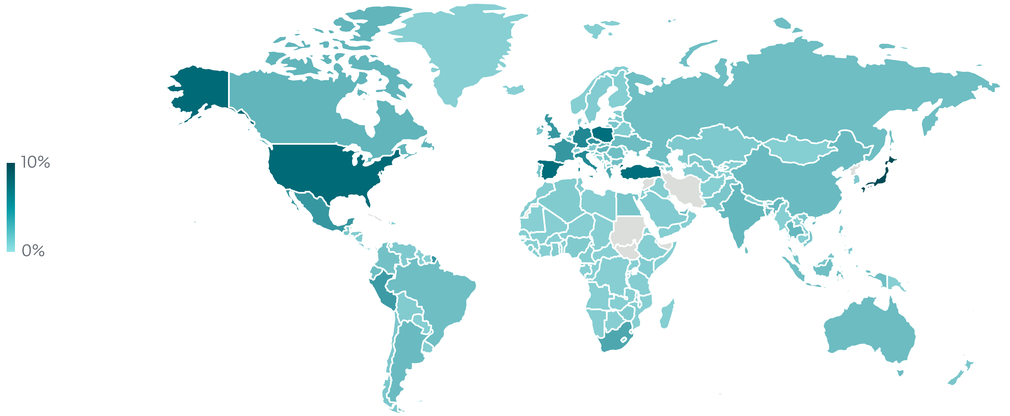
Europol, Eurojust, and agencies from seven countries have **dismantled** an organized group of ransomware actors whose attacks affected more than 1,800 victims in 71 countries. All five suspects were taken into custody in Ukraine, including a 32-year-old ringleader. A total of 30 locations were searched. This action followed a first round of arrests from **2021**.

Threat telemetry

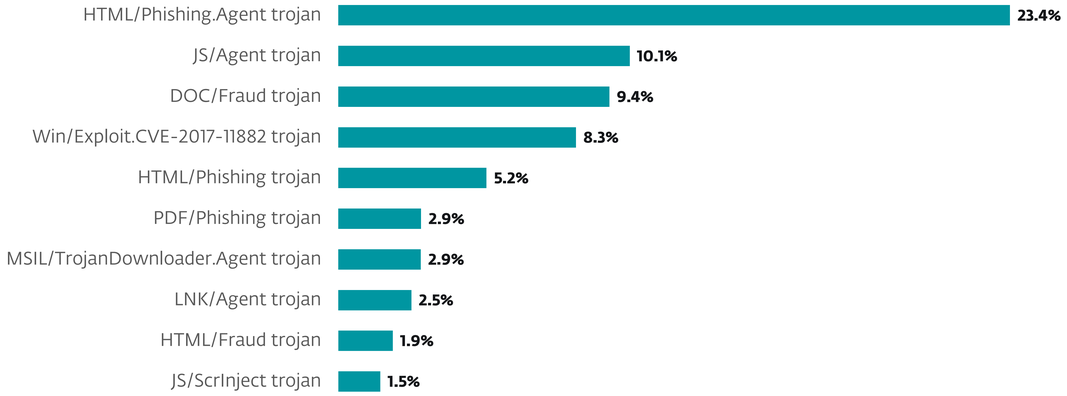
All threats



Overall threat detection trend in H1 2023 and H2 2023, seven-day moving average

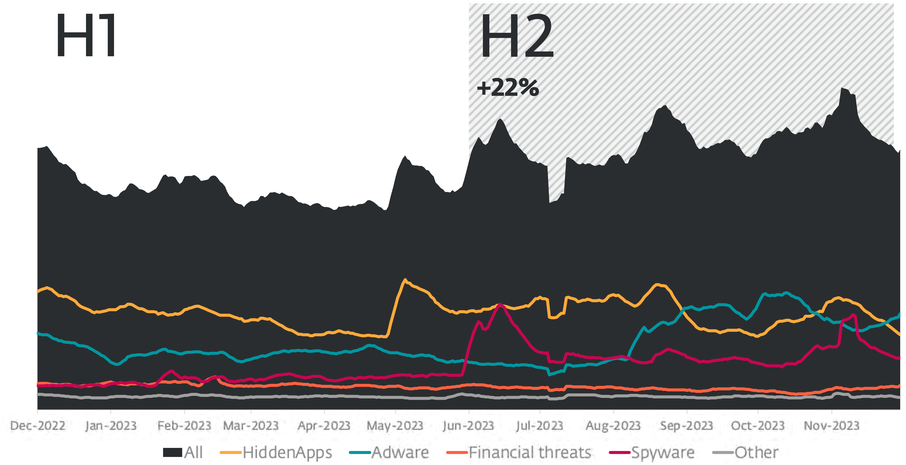


Geographic distribution of malware detections in H2 2023

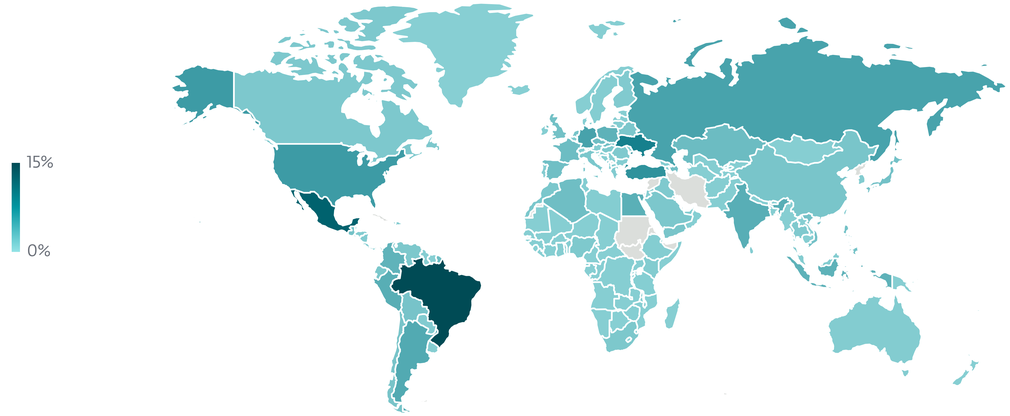


Top 10 malware detections in H2 2023 (% of malware detections)

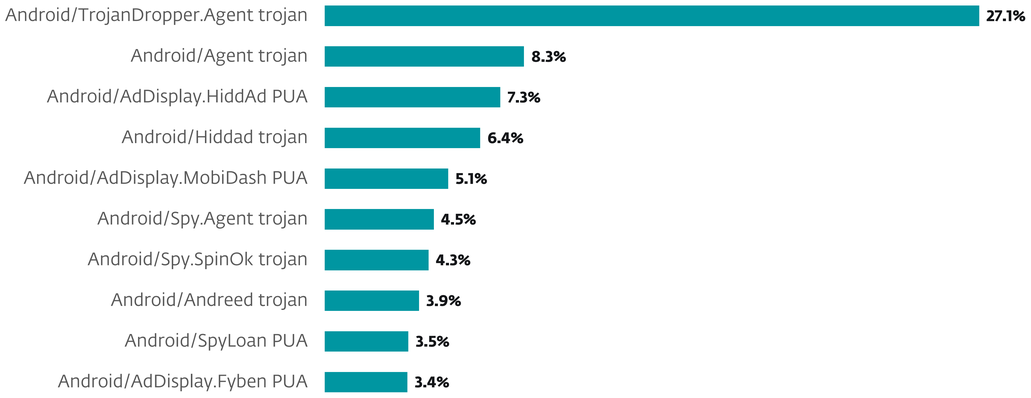
Android



Detection trends of selected Android detection categories in H1 2023 and H2 2023, seven-day moving average (trends of Clickers, Cryptominers, Ransomware, Scam apps, SMS trojans, and Stalkerware are combined in the trendline Other)

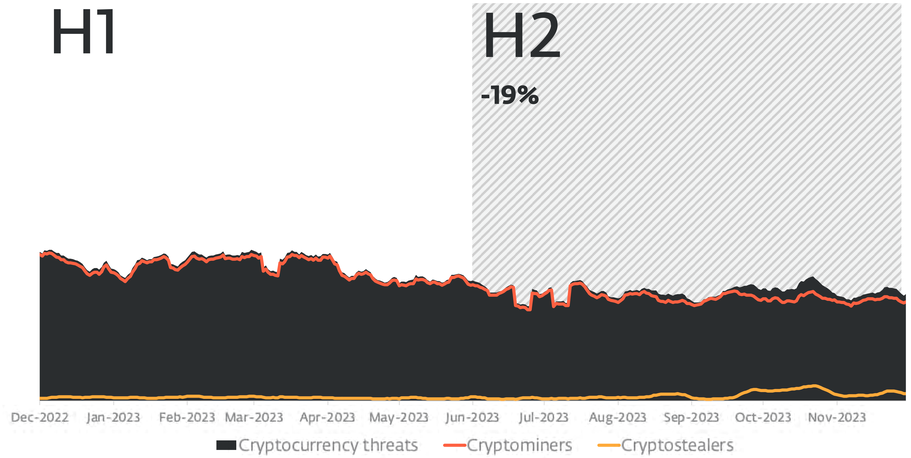


Geographic distribution of Android detections in H2 2023

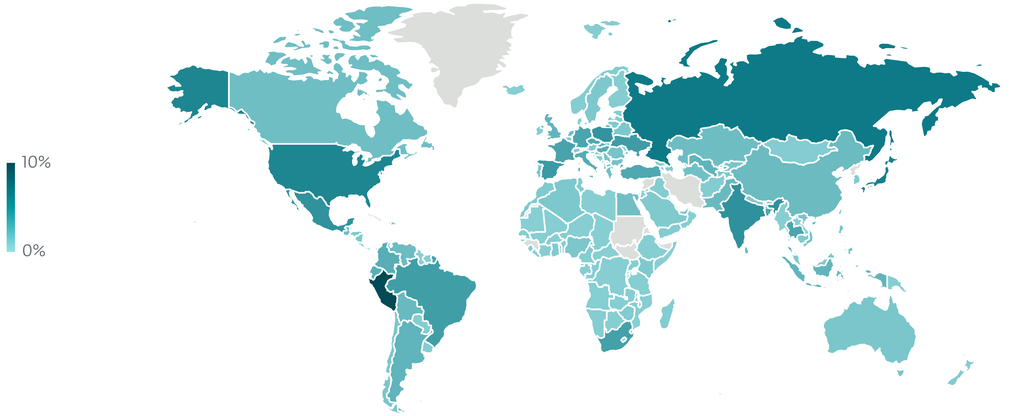


Top 10 Android detections in H2 2023 (% of malware detections)

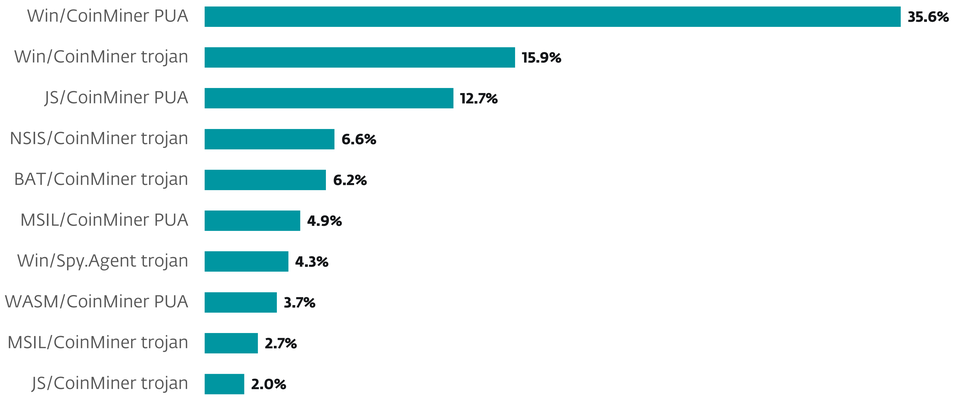
Cryptocurrency threats



Cryptocurrency threat detection trend in H1 2023 and H2 2023, seven-day moving average

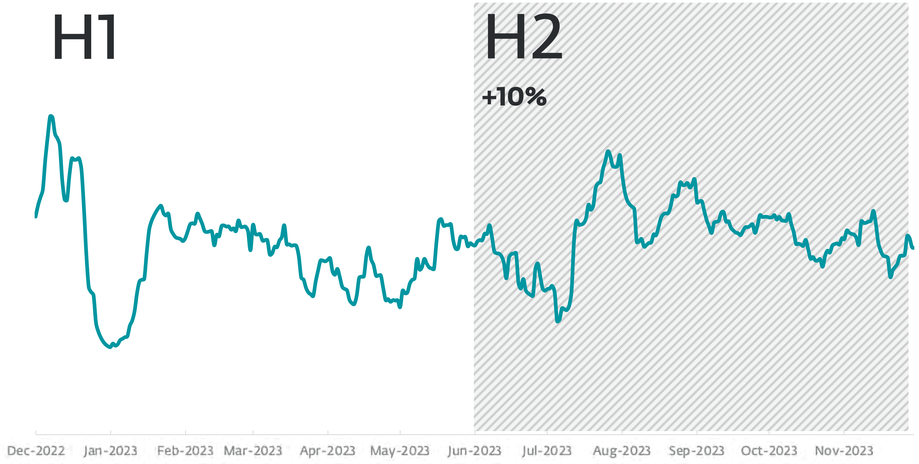


Geographic distribution of Cryptocurency threat detections in H2 2023

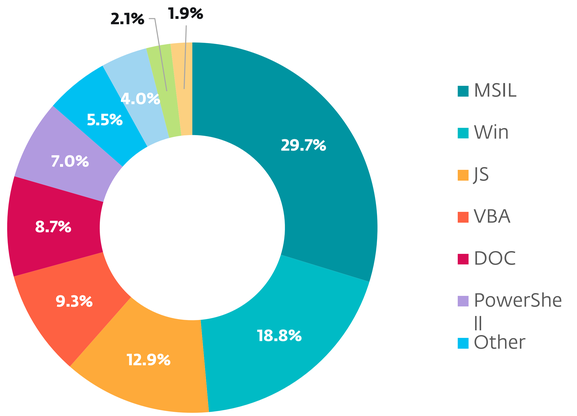


Top 10 Cryptocurrency threat detections in H2 2023 (% of malware detections)

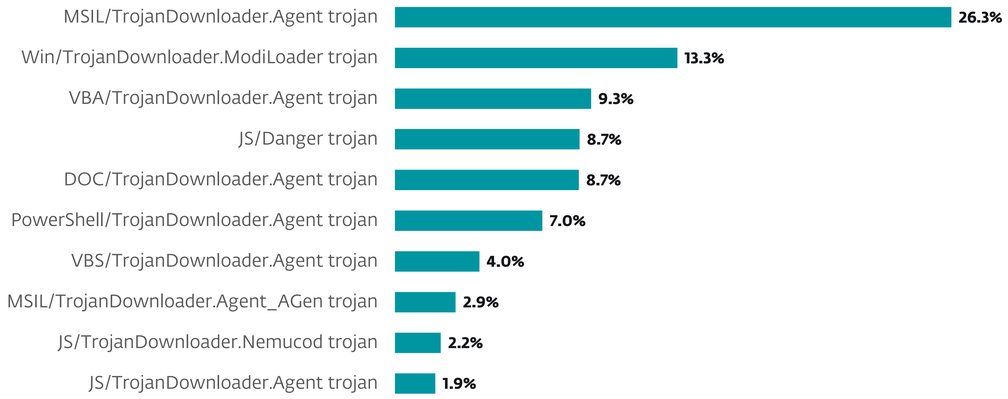
Downloaders



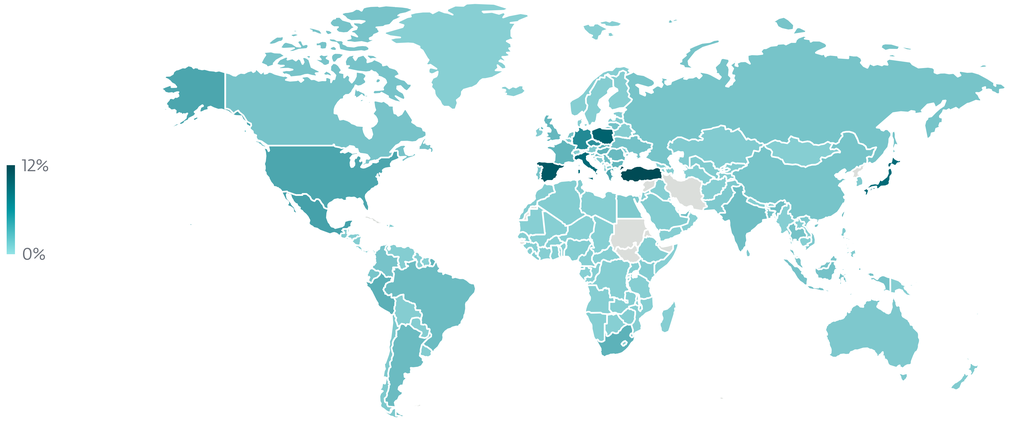
Downloader detection trend in H1 2023 and H2 2023, seven-day moving average



Downloader detections per detection type in H2 2023

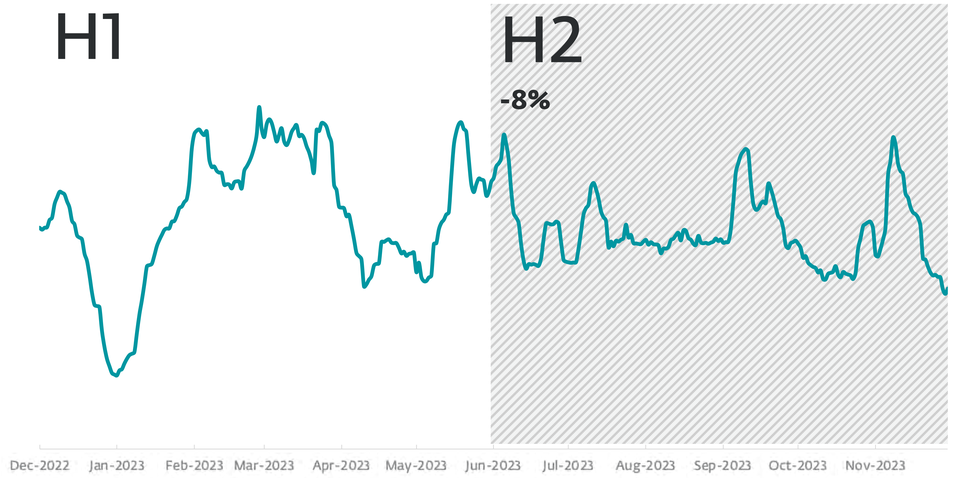


Top 10 Downloader detections in H2 2023 (% of malware detections)

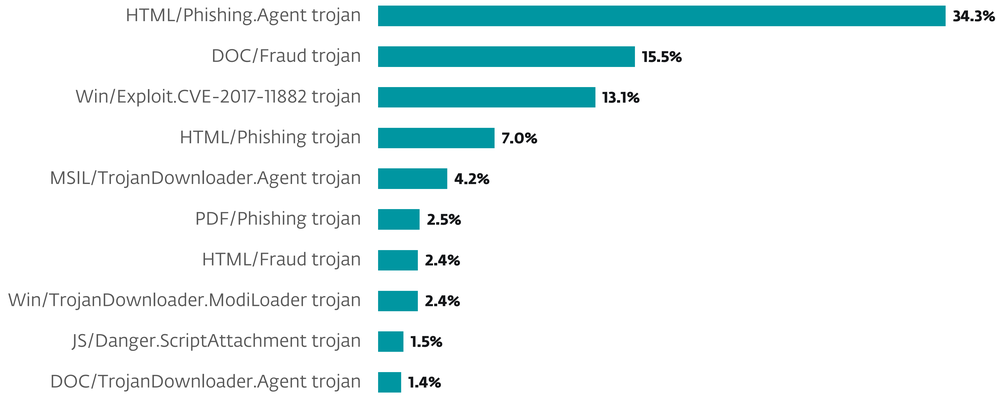


Geographic distribution of Downloader detections in H2 2023

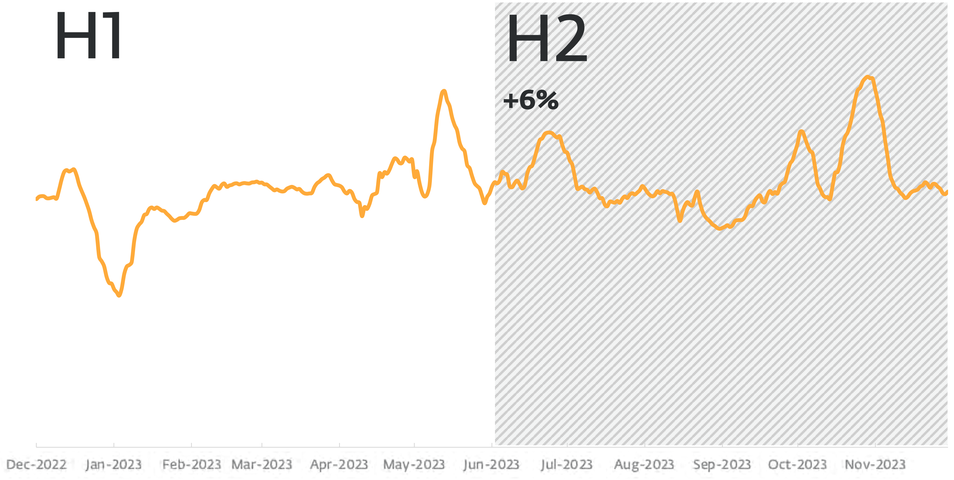
Email threats



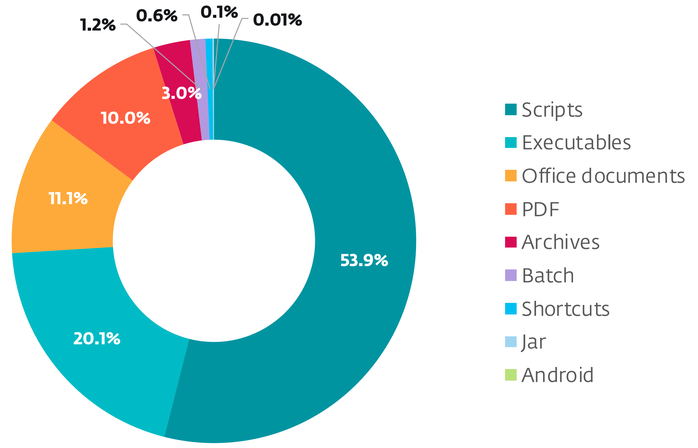
Malicious email detection trend in H1 2023 and H2 2023, seven-day moving average



Top 10 threats detected in emails in H2 2023

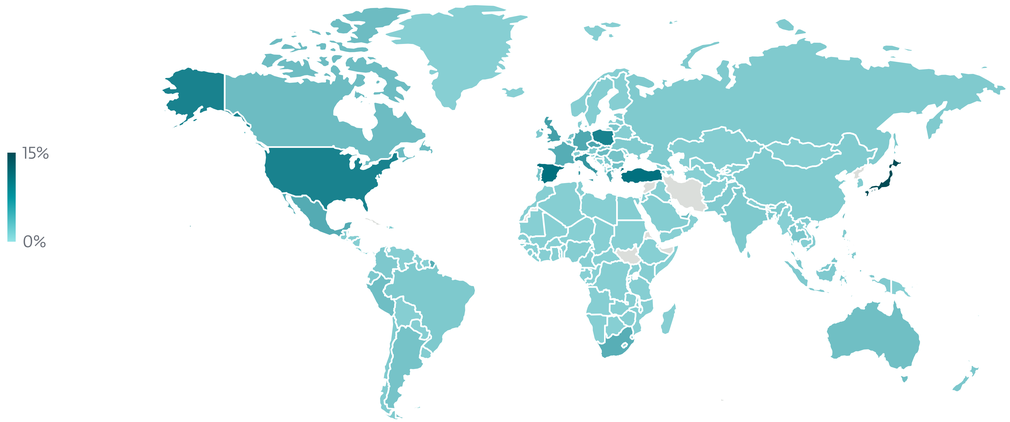


Spam detection trend in H1 2023 and H2 2023, seven-day moving average



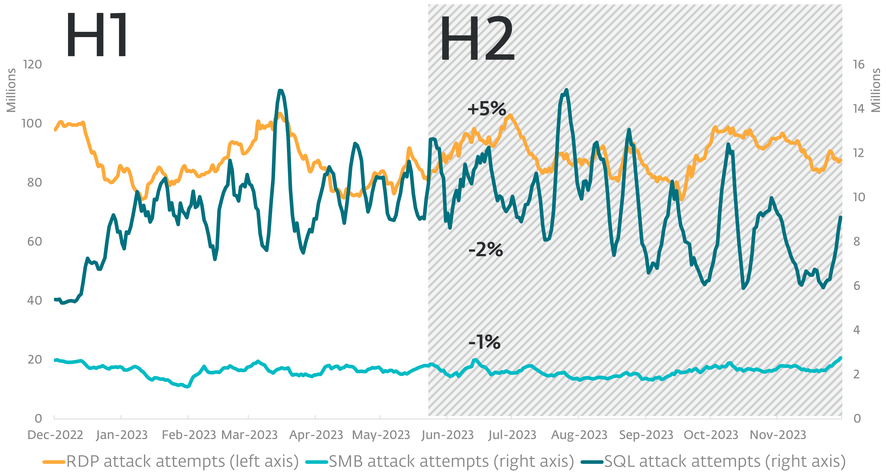
Top malicious email attachment types in H2 2023

Email threats

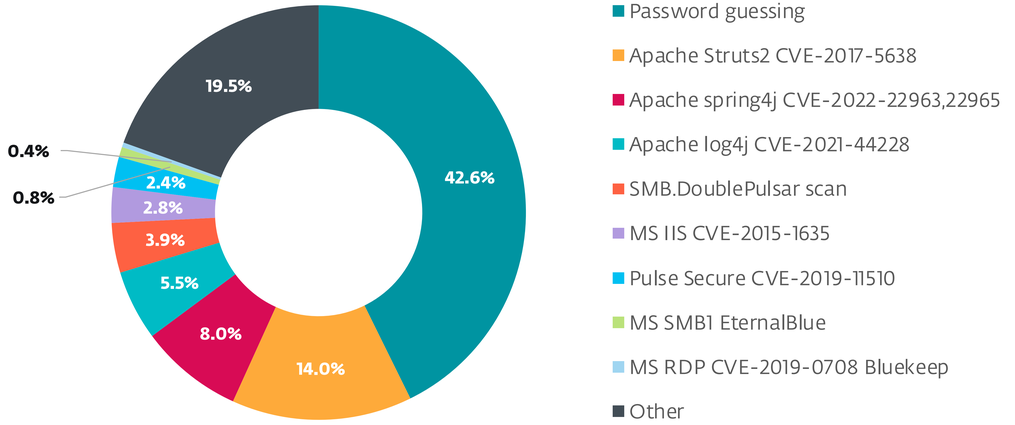


Geographic distribution of Email threat detections in H2 2023

Exploits

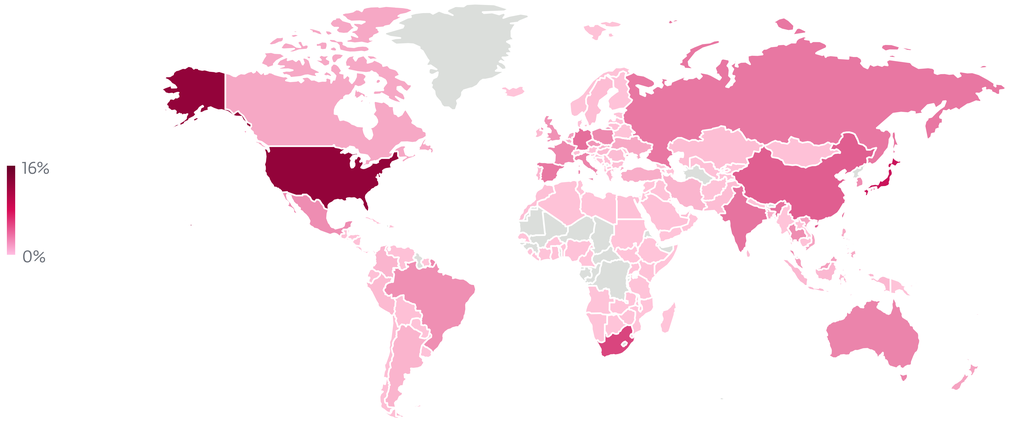


Trends of RDP, SMB and SQL attack attempts in H1 2023 and H2 2023, seven-day moving average

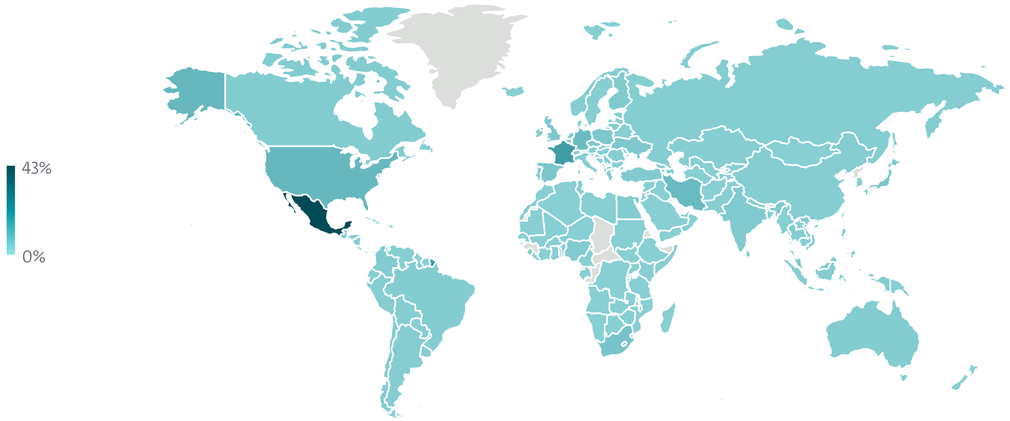


External network intrusion vectors reported by unique clients in H2 2023

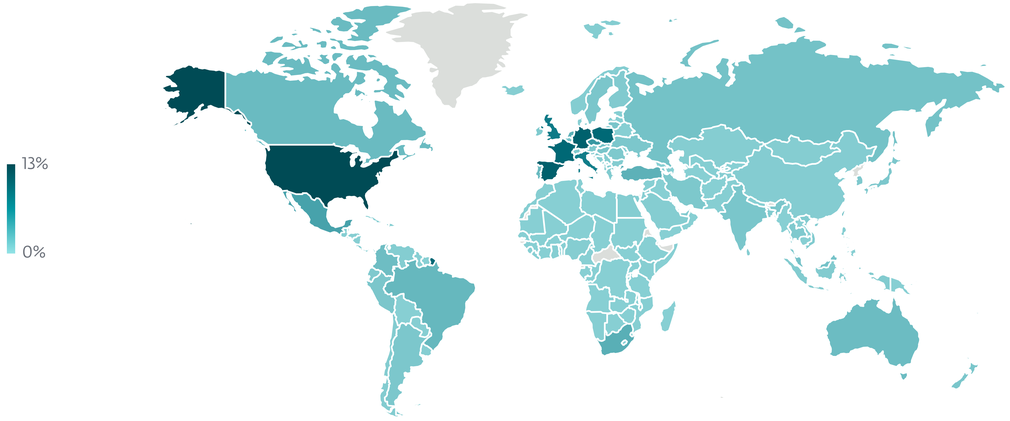
Exploits



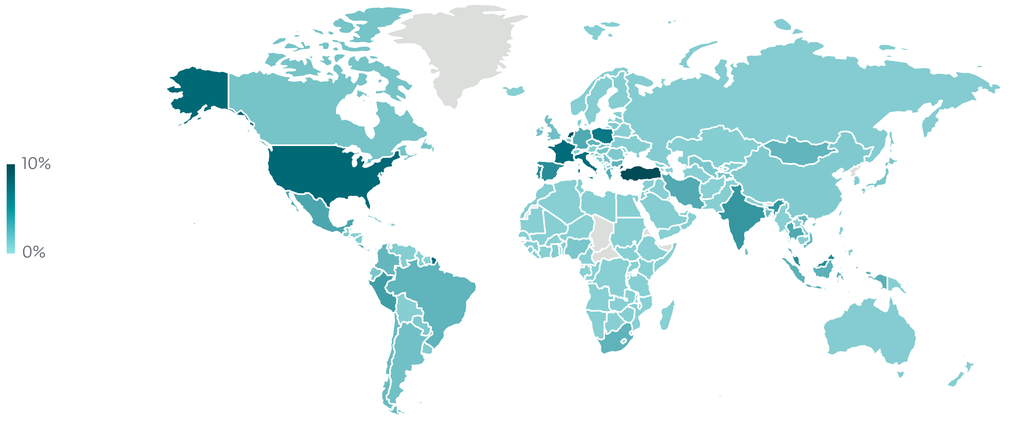
Geographic distribution of RDP password guessing attack attempt sources in H2 2023



Geographic distribution of SMB password guessing attack attempt targets in H2 2023

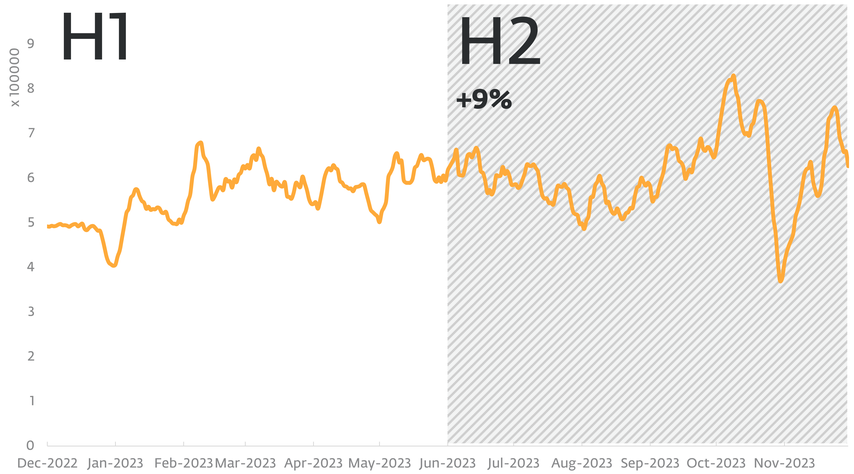


Geographic distribution of RDP password guessing attack attempt targets in H2 2023

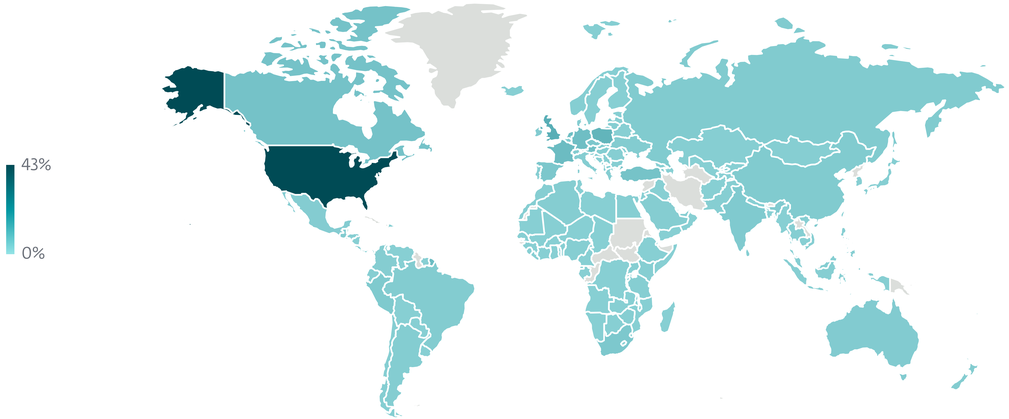


Geographic distribution of SQL password guessing attack attempt targets in H2 2023

Exploits

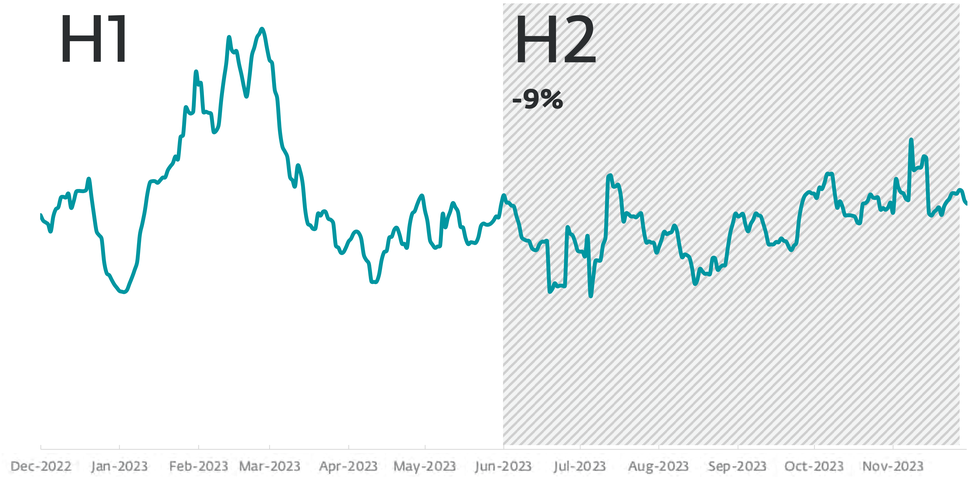


Detection trend of Log4Shell exploitation attempts in H1 2023 and H2 2023, seven-day moving average

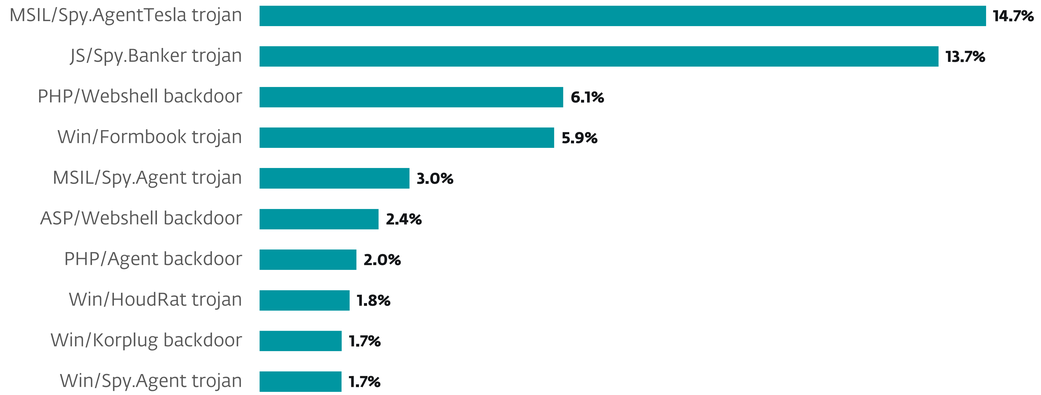


Geographic distribution of Log4Shell exploitation attempts in H2 2023

Infostealers

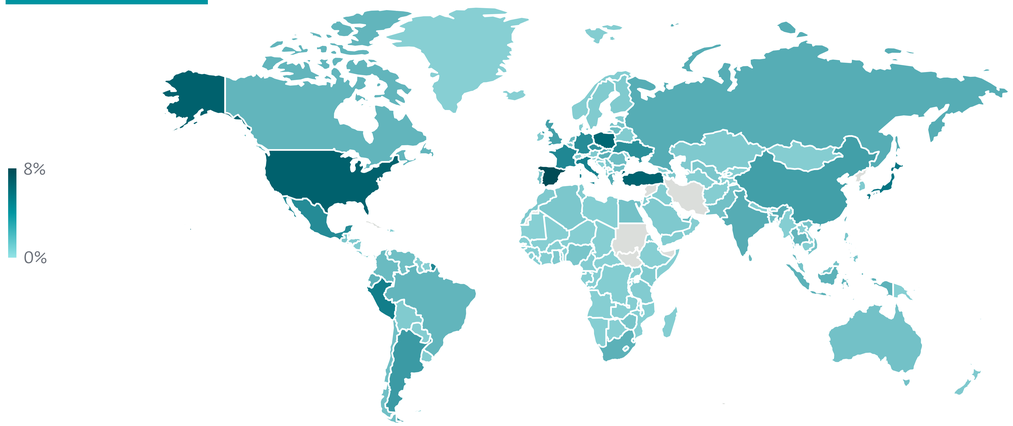


Infostealer detection trend in H1 2023 and H2 2023, seven-day moving average



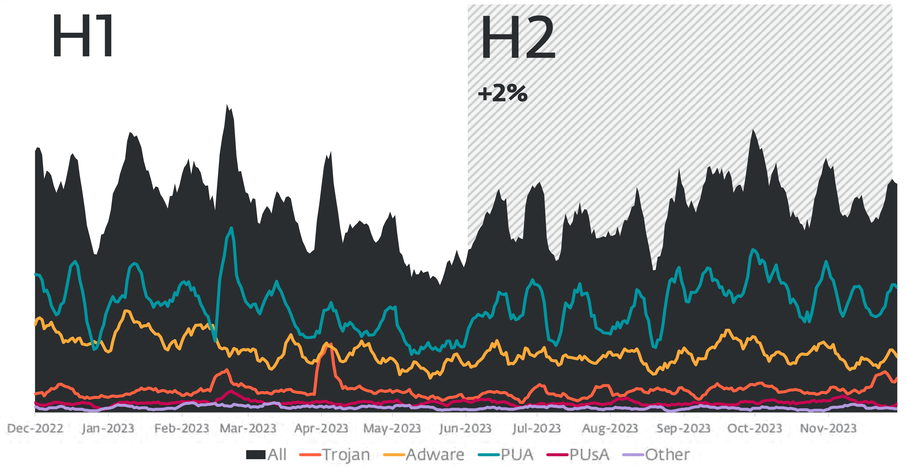
Top 10 Infostealer families in H2 2023 (% of Infostealer detections)

Infostealers

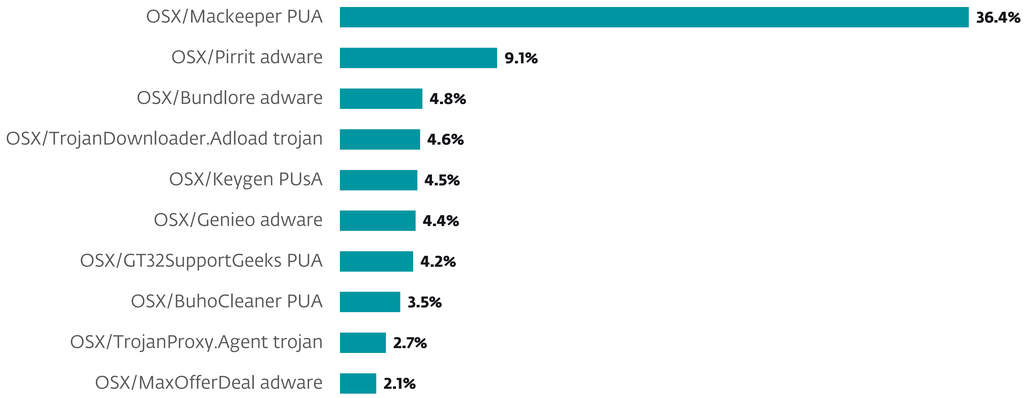


Geographic distribution of Infostealer detections in H1 2023

macOS

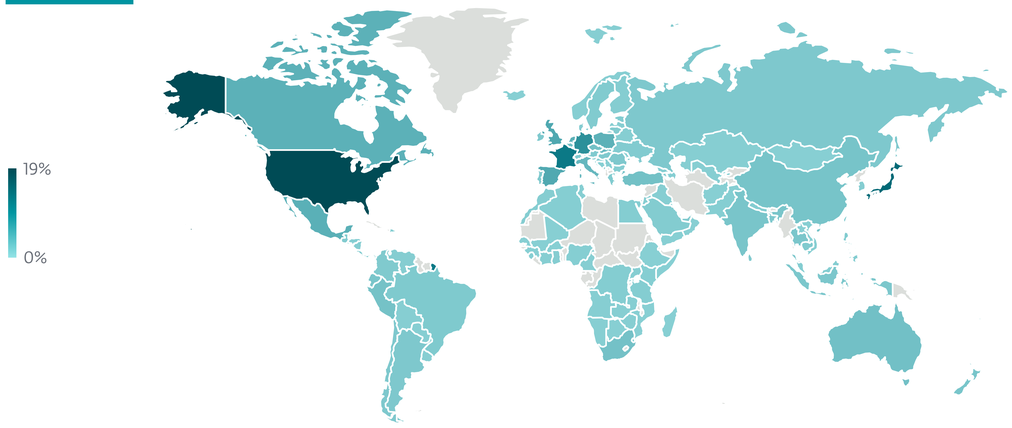


macOS detection trend in H1 2023 and H2 2023, seven-day moving average



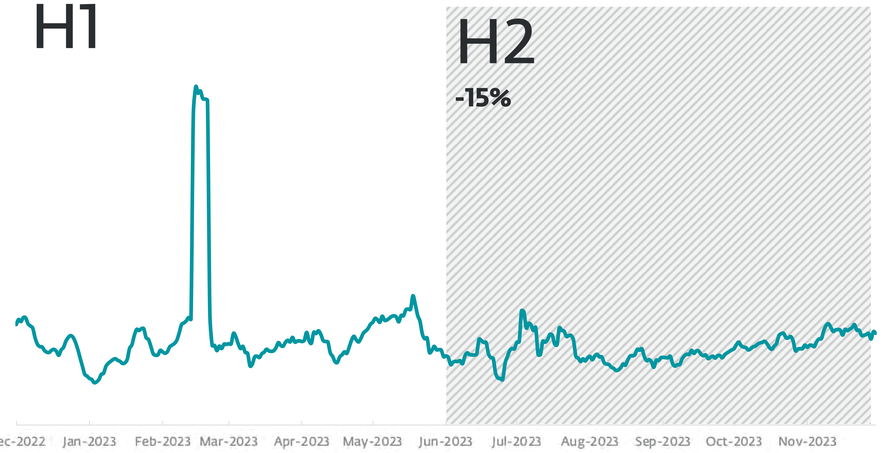
Top 10 macOS detections in H2 2023 (% of macOS detections)

macOS

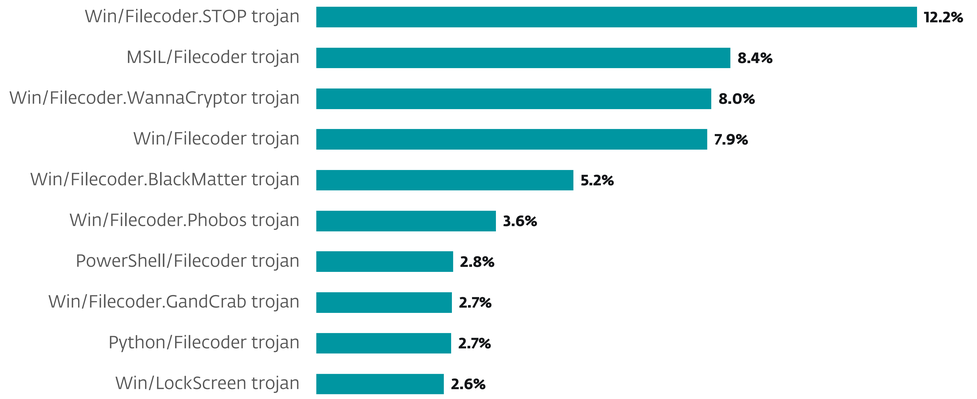


Geographic distribution of macOS detections in H2 2023

Ransomware

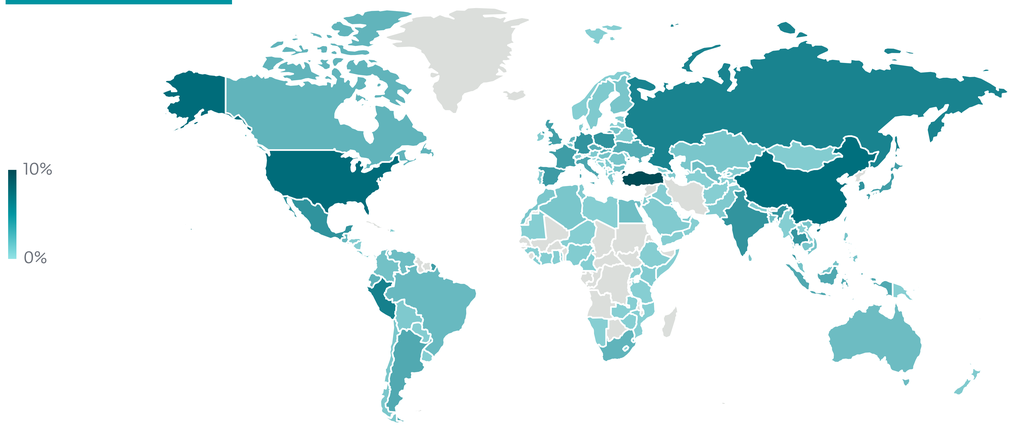


Ransomware detection trend in H1 2023 and H2 2023, seven-day moving average



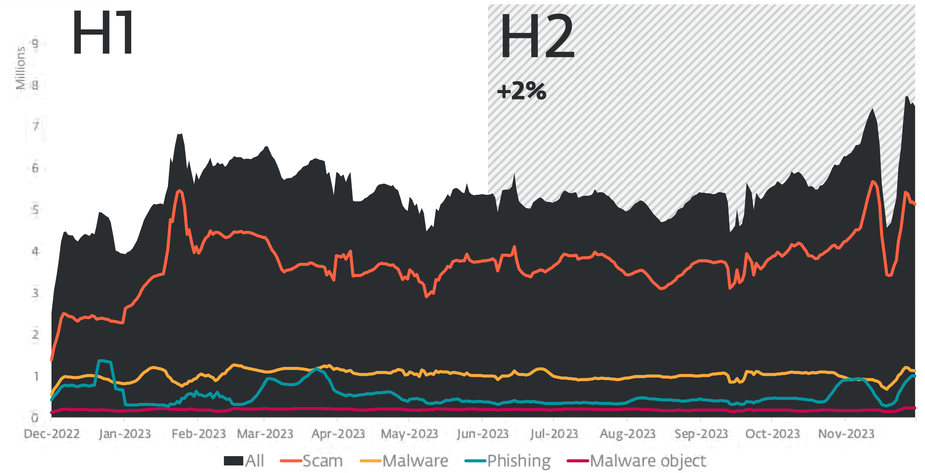
Top 10 Ransomware detections in H2 2023 (% of Ransomware detections)

Ransomware

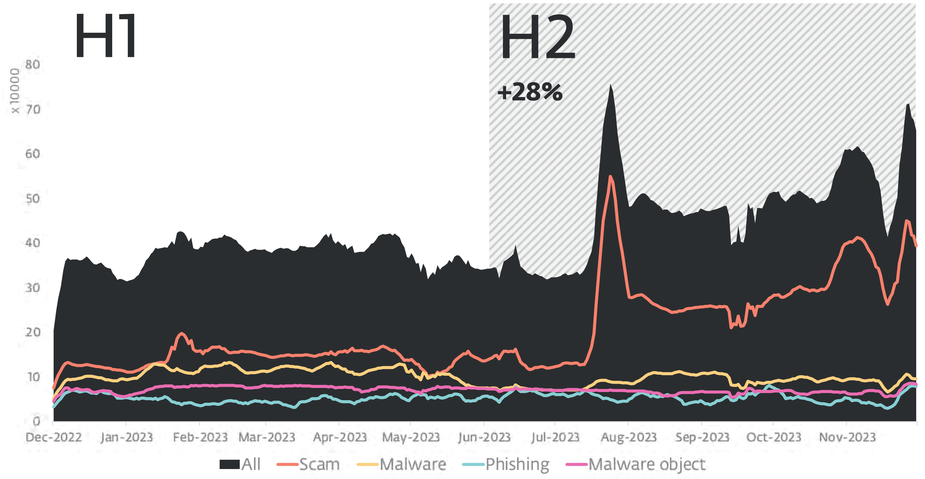


Geographic distribution of Ransomware detections in H2 2023

Web threats

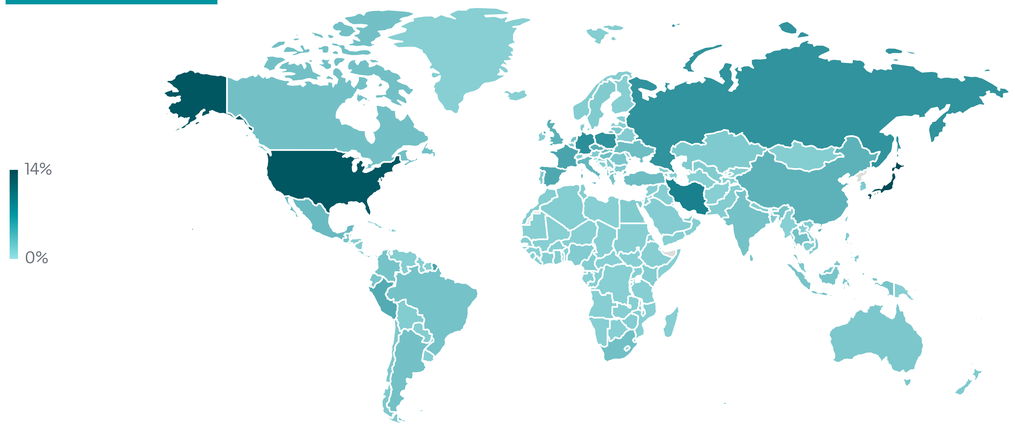


Web threat block trend in H1 2023 and H2 2023, seven-day moving average

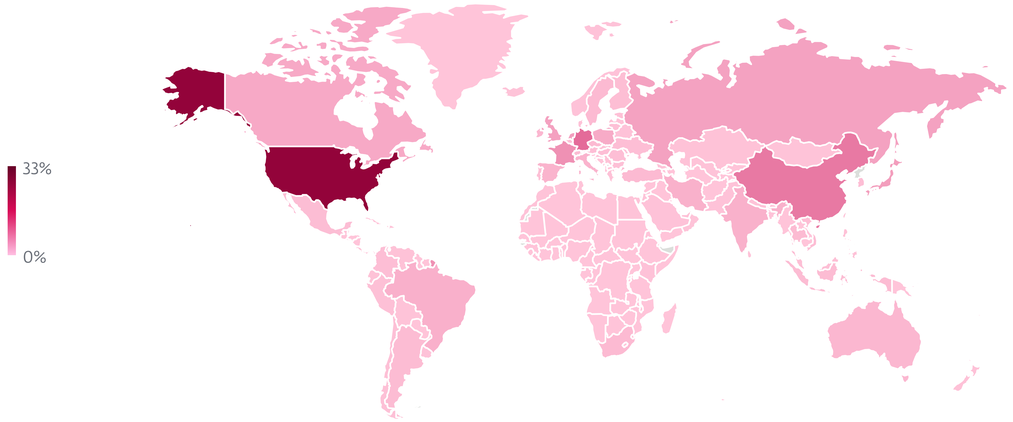


Unique URL block trend in H1 2023 and H2 2023, seven-day moving average

Web threats



Global distribution of Web threat blocks in H2 2023



Global distribution of blocked domain hosting in H2 2023

Research publications

Asylum Ambuscade: Crimeware or cyberespionage?

A curious case of a threat actor at the border between crimeware and cyberespionage

Android GravityRAT goes after WhatsApp backups

ESET researchers analyzed an updated version of Android GravityRAT spyware that steals WhatsApp backup files and can receive commands to delete files

What's up with Emotet?

A brief summary of what happened with Emotet since its comeback in November 2021

ESET Research Podcast: Finding the mythical BlackLotus bootkit

Here's a story of how an analysis of a supposed game cheat turned into the discovery of a powerful UEFI threat

MoustachedBouncer: Espionage against foreign diplomats in Belarus

Long-term espionage against diplomats, leveraging email-based C&C protocols, C++ modular backdoors, and adversary-in-the-middle (AitM) attacks... Sounds like the infamous Turla? Think again!

ESET Research Podcast: Unmasking MoustachedBouncer

Listen as ESET's Director of Threat Research Jean-Ian Boutin unravels the tactics, techniques and procedures of MoustachedBouncer, an APT group taking aim at foreign embassies in Belarus

Mass-spreading campaign targeting Zimbra users

ESET researchers have observed a new phishing campaign targeting users of the Zimbra Collaboration email server.

Scarabs colon-izing vulnerable servers

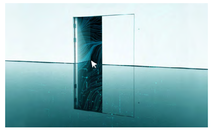
Analysis of Spacecolon, a toolset used to deploy Scarab ransomware on vulnerable servers, and its operators, CosmicBeetle

Telekopye: Hunting Mammoths using Telegram bot

Analysis of Telegram bot that helps cybercriminals scam people on online marketplaces

BadBazaar espionage tool targets Android users via trojanized Signal and Telegram apps

ESET researchers have discovered active campaigns linked to the China-aligned APT group known as GREF, distributing espionage code that has previously targeted Uyghurs



Sponsor with batch-filed whiskers: Ballistic Bobcat's scan and strike backdoor

ESET Research uncovers the Sponsoring Access campaign, which utilizes an undocumented Ballistic Bobcat backdoor we have named Sponsor

ESET Research Podcast: Sextortion, digital usury and SQL brute-force

Closing intrusion vectors force cybercriminals to revisit old attack avenues, but also to look for new ways to attack their victims

OilRig's Outer Space and Juicy Mix: Same ol' rig, new drill pipes

ESET researchers document OilRig's Outer Space and Juicy Mix campaigns, targeting Israeli organizations in 2021 and 2022

Stealth Falcon preying over Middle Eastern skies with Deadglyph

ESET researchers have discovered Deadglyph, a sophisticated backdoor used by the infamous Stealth Falcon group for espionage in the Middle East

Lazarus luring employees with trojanized coding challenges: The case of a Spanish aerospace company

While analyzing a Lazarus attack luring employees of an aerospace company, ESET researchers discovered a publicly undocumented backdoor

Operation Jacana: Foundling hobbits in Guyana

ESET researchers discovered a cyberespionage campaign against a governmental entity in Guyana

Operation King TUT: The universe of threats in LATAM

ESET researchers reveal a growing sophistication in threats affecting the LATAM region by employing evasion techniques and high-value targeting

Winter Vivern exploits zero-day vulnerability in Roundcube Webmail servers

ESET Research recommends updating Roundcube Webmail to the latest available version as soon as possible

Who killed Mozi? Finally putting the IoT zombie botnet in its grave

How ESET Research found a kill switch that had been used to take down one of the most prolific botnets out there

Unlucky Kamran: Android malware spying on Urdu-speaking residents of Gilgit-Baltistan

ESET researchers discovered Kamran, previously unknown malware, which spies on Urdu-speaking readers of Hunza News

Telekopye: Chamber of Neanderthals' secrets

Insight into groups operating Telekopye bots that scam people in online marketplaces

ESET APT Activity Report Q2–Q3 2023

An overview of the activities of selected APT groups investigated and analyzed by ESET Research in Q2 and Q3 2023

Credits

Team

Peter Stančík, Team Lead
Hana Matušková, Managing Editor

Aryeh Goretsky
Branislav Ondrášik
Bruce P. Burrell
Klára Kobáková
Nick FitzGerald
Ondrej Kubovič
Rene Holt
Zuzana Pardubská

Contributors

Anton Mäčko
Dušan Lacika
Igor Kabina
Ivan Bešina
Jakub Souček
Ján Adámek
Ján Šugarek
Jiří Kropáč
Ladislav Janko
Lukáš Štefanko
Martin Červeň
Michal Kopera
Michal Malík
Michal Škuta
Milan Fránik
Miloš Čermák
Patrik Sučanský
Vladimír Šimčák
Witold Gerstendorf

About the data in this report

The threat statistics and trends presented in this report are based on global telemetry data from ESET. Unless explicitly stated otherwise, the data includes detections regardless of the targeted platform.

Further, the data excludes detections of potentially unwanted applications, potentially unsafe applications and adware, except where noted in the more detailed, platform-specific sections and in the Cryptocurrency threats section.

This data was processed with the honest intention to mitigate all known biases, in an effort to maximize the value of the information provided.

Most of the charts in this report show detection trends rather than provide absolute numbers. This is because the data can be prone to various misinterpretations, especially when directly compared to other telemetry data. However, absolute values or orders of magnitude are provided where deemed beneficial.

About ESET

For more than 30 years, ESET has been developing industry-leading IT security software and services to deliver comprehensive, multilayered protection against cybersecurity threats for businesses and consumers worldwide. ESET has long pioneered machine learning and cloud technologies that prevent, detect and respond to malware. ESET is a privately owned company that promotes scientific research and development worldwide.

WeLiveSecurity.com

@ESETresearch

ESET GitHub

ESET Threat Reports and APT Activity Reports