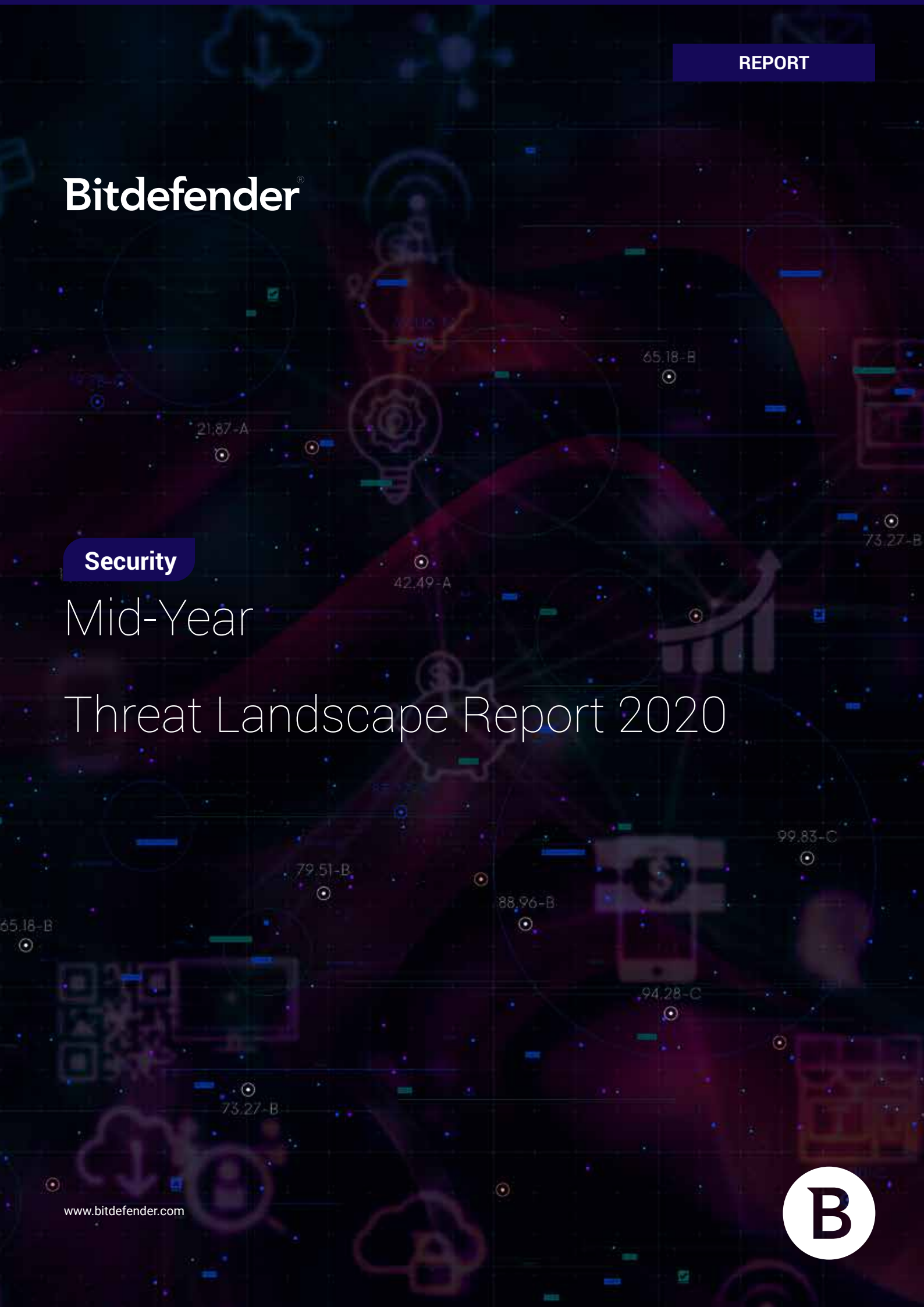
REPORT

Bitdefender



Security

Mid-Year Threat Landscape Report 2020

www.bitdefender.com

Contents

Executive summary

The threat landscape has always been influenced by events and shifts in cybercriminal practices, but the global coronavirus pandemic has caused a significant shift both in how cybercriminals operate and how they hone their skills.

A defining characteristic of the first half of 2020 in terms of threats and malware is that they all played on the same theme: the pandemic. A spike in scams, phishing and malware across all platforms and attack vectors seems to have been a direct result of cybercriminals leveraging issues related toCovid-19 to exploit fear and misinformation.

This catalyst was responsible for a **five-fold increase**[1] **in the number of coronavirus-themed reports** in the first two weeks of March alone. Then, in May and June, an average of **60 percent of all received emails were fraudulent**, according to Bitdefender telemetry. Whether it was phishing scam exploiting the coronavirus, a fundraiser or a jaw-dropping offer you couldn't resist, bad actors have pulled every trick of the trade to fool victims into providing sensitive information, installing malware, or falling prey to scams.

Attack vectors commonly used by attackers to compromise and take control of home networks were being used in conjunction with the panic caused by the pandemic. Bitdefender researchers have found a **DNS hijacking attack**[2] on a popular brand of home routers, used by attackers to redirect victims to malware-serving websites promising applications that offer new and up to date information about the outbreak.

Android malware quickly capitalized on the topic, with malware developers rushing to weaponize popular application, such as the **Zoom**[3] **video conferencing application**, used by employees now working from home. Packing RAT (Remote Access Trojan) capabilities, or bundling[4] them with ransomware[5], banking malware, or even highly aggressive adware, Android malware developers were also fully exploiting the pandemic wave. Some legitimate Android developers even tweaked content on Google Play application webpages to gain better ranking, mostly for applications under the Health and Fitness or Medical categories.

Attacks on home IoT (Internet of Things) devices have also grown, with Bitdefender telemetry picking up an increase of 46 percent from January to June in terms of reported suspicious incidents. Ranking from exploiting unpatched vulnerabilities to bruteforcing attacks, IoT malware[6] has become highly versatile, robust, and is constantly updated. IrcFlu, Dark_Nexus[7] and InterPLanetary Storm are only some of the examples of IoT malware gaining popularity in the first half of 2020.

Windows threats that we've grown used to, such as ransomware, fileless malware, cryptocurrency miners, Trojan bankers and exploits, are still going strong, with several families emerging as the most popular and constantly updated. For example, Emotet, Agent Testla[8], TrickBot[9]and Dridex have become the go-to threats that threat actors used during the pandemic, both because of their long-standing track record for effectiveness, but also because their developers have constantly added new features, making them more resilient against detection from security solution and more feature-packed.

1 "5 Times More Coronavirus-themed Malware Reports during March", Bitdefender, https://labs.bitdefender.com/2020/03/5-times-more-coronavirus-themed-malware-reports-during-march/
2 "New Router DNS Hijacking Attacks Abuse Bitbucket to Host Infostealer", Bitdefender, https://labs.bitdefender.com/2020/03/new-router-dns-hijacking-attacks-abuse-bitbucket-to-host-infostealer/
3 "Who installs Zoom apps outside the Play Store? Well, lots of people", Bitdefender, https://labs.bitdefender.com/2020/04/who-installs-zoom-apps-outside-the-play-store-well-lots-of-people/
4 "Infected Zoom Apps for Android Target Work-From-Home Users", Bitdefender, https://labs.bitdefender.com/2020/03/infected-zoom-apps-for-android-target-work-from-home-users/
5 "Android SLocker Variant Uses Coronavirus Scare to Take Android Hostage", Bitdefender, https://labs.bitdefender.com/2020/05/android-slocker-variant-uses-coronavirus-scare-to-take-android-hostage/
6 "SSH-Targeting Golang Bots Becoming the New Norm", Bitdefender, https://labs.bitdefender.com/2020/06/ssh-targeting-golang-bots-becoming-the-new-norm/
7 "New dark_nexusIoT Botnet Puts Others to Shame", Bitdefender, https://labs.bitdefender.com/2020/04/new-dark_nexus-iot-botnet-puts-others-to-shame/
8 "Oil & Gas Spearphishing Campaigns Drop Agent Tesla Spyware in Advance of Historic OPEC+ Deal", Bitdefender, https://labs.bitdefender.com/2020/04/oil-gas-spearphishing-campaigns-drop-agent-tesla-spyware-in-advance-of-historic-opec-deal/
9 "New TrickBot Module Bruteforces RDP Connections, Targets Select Telecommunication Services in US and Hong Kong", Bitdefender, https://labs.bitdefender.com/2020/03/new-trickbot-module-bruteforces-rdp-connections-targets-select-telecommunication-services-in-us-and-hong-kong/

Key Findings:

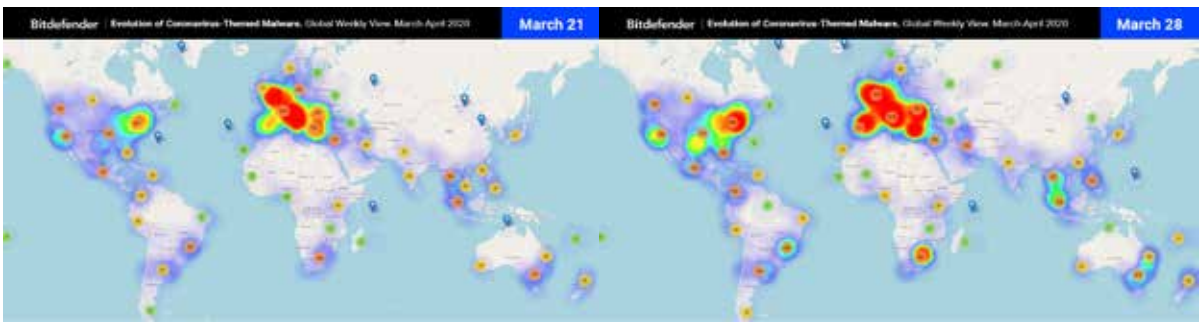
- Seven-fold year-on-year increase in ransomware reports
- 4 out of 10 Covid-themed emails are spam
- 46 percent increase in the number of IoT suspicious incident reports
- 55.73 percent of IoT network threats involve port-scanning attacks
- GoLang becoming a popular programming language for IoT malware
- Coronavirus-themed Android threats leverage the pandemic
- Attackers focus more on social engineering, less on malware sophistication
- Coronavirus-themed threats becoming the new norm

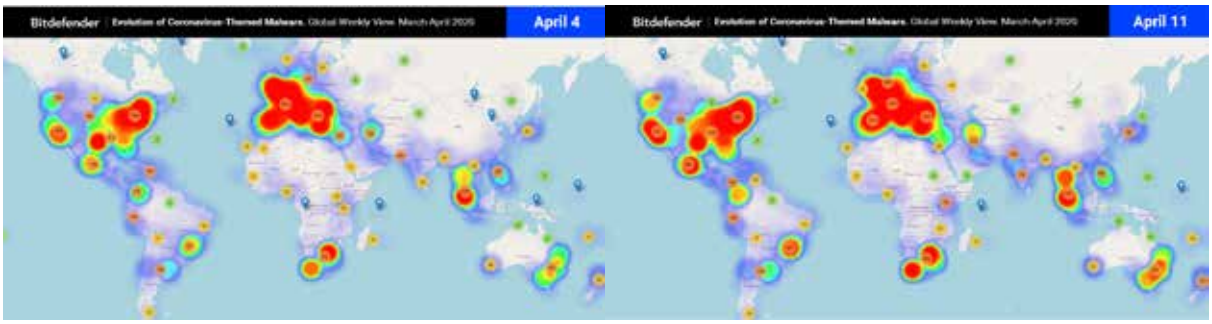
Coronavirus – The New Theme

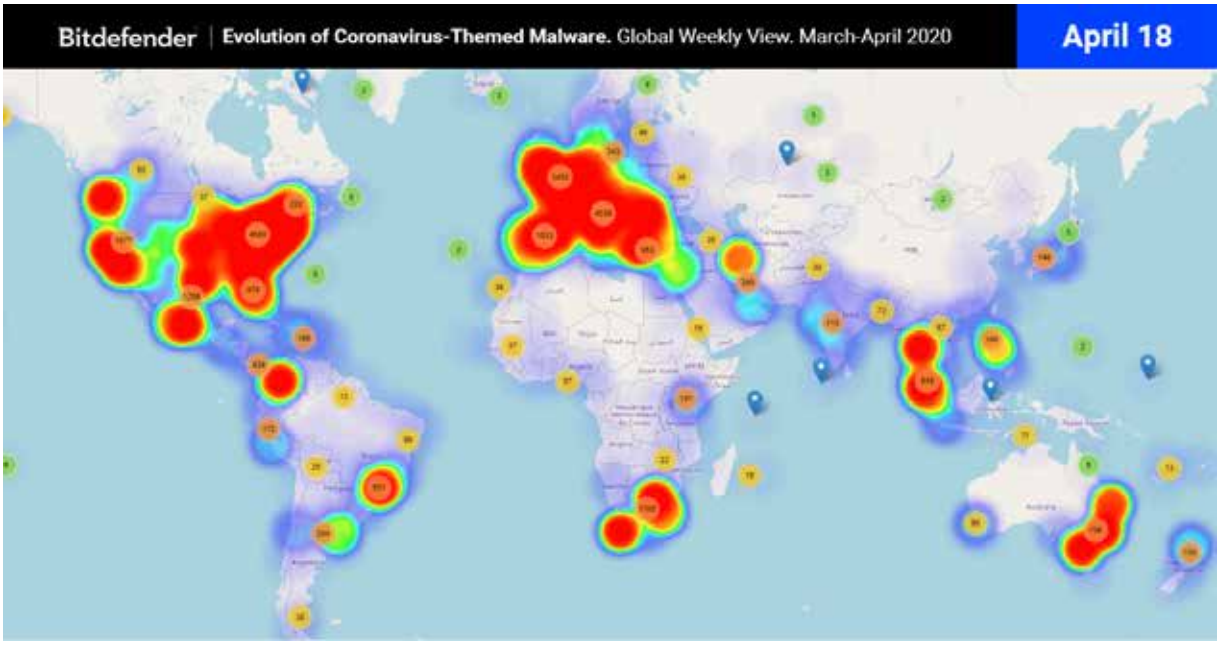
Every year has its own theme with a "soundtrack" we keep hearing on repeat, and this year it's the "coronavirus". If previous years were dominated by ransomware, banking Trojans, and even exploits that wreaked havoc, the global pandemic has been the perfect catalyst for cybercriminals to dress-up their threats with a cloak of panic, fear and information manipulation.

As the year began and the number of affected countries and people peaked in early March, threat actors seized the opportunity to exploit the topic by focusing less on malware sophistication, and more on carefully planning malware-serving campaigns that selectively targeted specific regions and countries.

The weekly evolution of Coronavirus-themed threat reports between March and the first half of April shows that threat actors were aiming their campaigns at the regions affected by the pandemic, at that time.

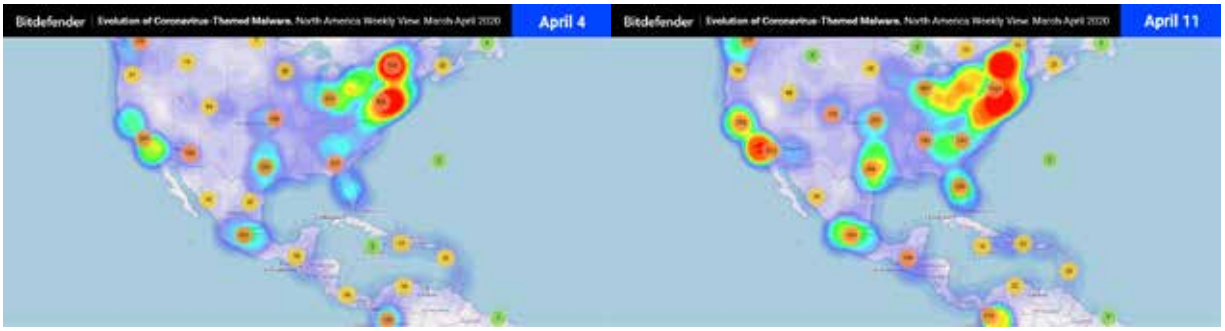


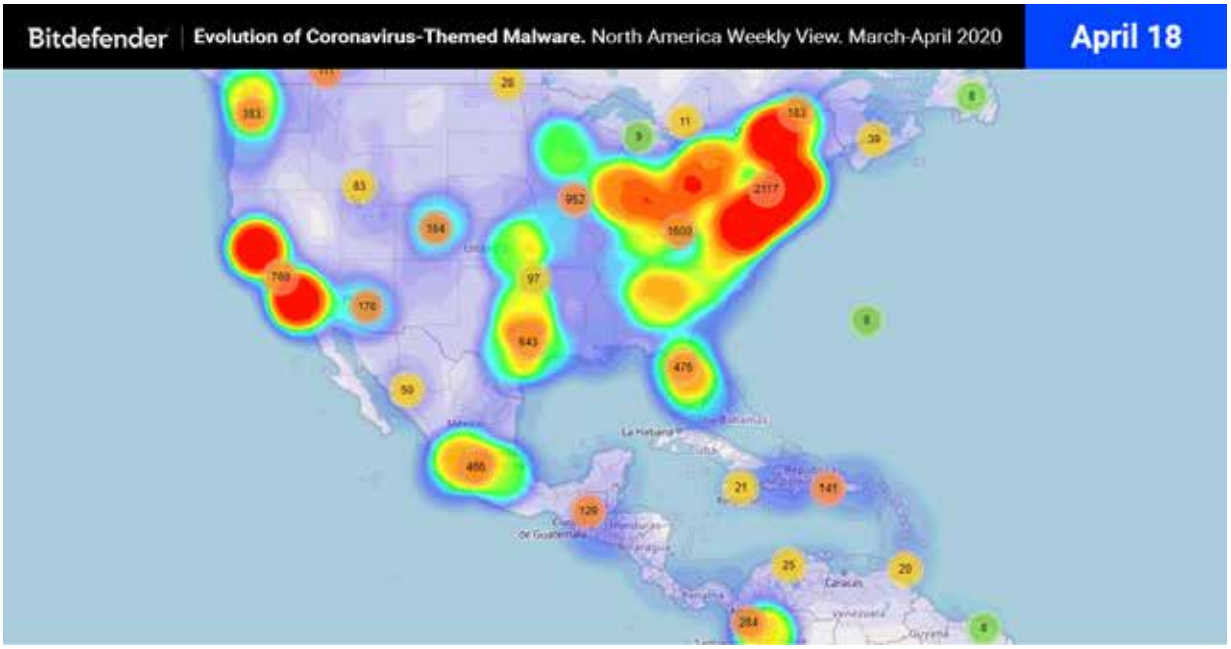




While the number of themed reports has since gone down, starting with a 10 percent drop in May from April, it's unlikely that we've seen the last of this theme in 2020. If anything, as the World Health Organization warns of a potential second wave of infections, cybercriminals are likely to once again seize the opportunity to create fraud campaigns with fictive health products and even send themed spam promising new treatments or cures.

For the United States, things were a bit different, in the sense that coronavirus-themed threat reports started two weeks later than in Europe. However, reports picked as the US started reporting a rapid spike in actual SARS-CoV-2 infection among the population, threat actors quickly ramping up their campaigns to take advantage of the fear, panic, and misinformation caused by the pandemic.





These somewhat limited snapshots into the evolution of coronavirus-themed threats do offer a glimpse into just how opportunistic threat actors have been during the spike of the global pandemic and how quickly they've adapted their messages based on how the infection developed regionally.

Below, is a snapshot of how coronavirus-themed malware reports have evolved in Europe, during the same time span.


Bitdefender
March 7

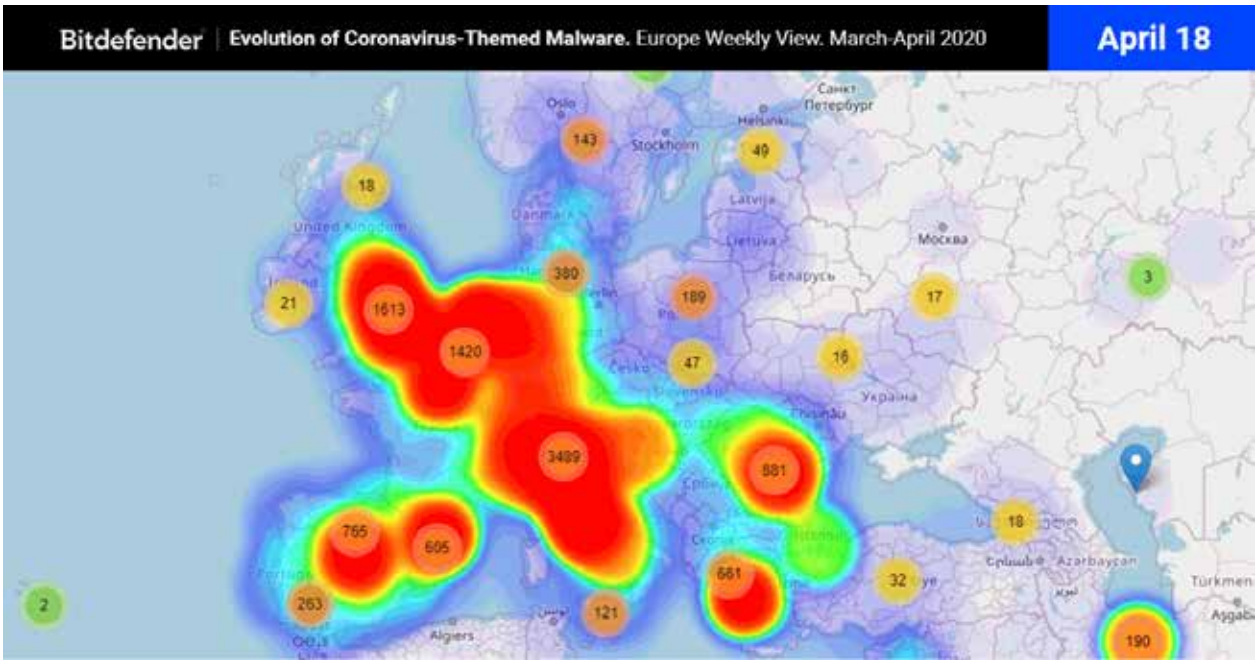

Bitdefender
March 14


Bitdefender
March 21


Bitdefender
March 28


Bitdefender
April 4


Bitdefender
April 11


Bitdefender
Evolution of Coronavirus-Themed Malware. Europe Weekly View. March-April 2020
April 18
Oslo
Stockholm
Санкт-Петербург
Helsinki
Latvija
Lietuva
Беларусь
Москва
Україна
United Kingdom
Danmark
Algiers
143
49
18
380
189
17
3
21
1613
1420
47
16
3489
881
755
605
681
18
263
121
32
190
2

Windows Threat Landscape

When looking at the threat landscape and how it has evolved year-over-year, two factors have to be considered: consistency with previous reports, in order to better illustrate how specific threats have evolved, and also understanding the global evolution of threats. That said, while the first half 2020 has been an interesting year from a threat-evolution perspective, it has also shown that threat actors will double down on using the threats that they know and have proven successful in the past. In times of pandemic, exploiting an opportunistic topic is a matter of launching timely campaigns instead of focusing on malware innovation.

A Primer on Threats

Ransomware remained a popular threat throughout our threat landscape for 2020. Focused on encrypting files, documents, databases, and any other relevant file type, ransomware has become the go-to mechanism for threat actors in terms of generating profit. Restricting access to files and leaving behind a ransom note to the victim, file recovery becomes next to impossible without a backup or a ransomware decryption tool. The third option, paying the ransom note, is never advisable, as it shows threat actors that this type of behavior can be profitable and it fuels them with the financial resources to keep developing new ransomware or other threats. While there are multiple ransomware families, from here on we will refer to them as a whole category of threats, unless discussing specific ransomware families.

If ransomware is an upfront method for demanding money from victims, **coin miners** are stealthy and use the victims' computing power to generate – or mine – cryptocurrency. With somewhere between 4,600 and over 6,000 cryptocurrencies[10] out there – of course, not all are minable –cybercriminals have plenty of options. By sizing the collective computing power of victims, threat actors can create mining pools that silently tax their victim's computing resources. While it may not be as financially enticing as ransomware, it's still a method focused on making money by using the victim instead of asking for direct payment. While there are various cryptocurrency miners, from here on we will refer to them as a general category of threats, unless addressing a specific cryptocurrency miner by name.

Fileless malware is also a popular mechanism used as a first line of attack. While it's not fileless per se, cybercriminals use scripts with various commands that are often executed by existing tools within the operating system. For instance, PowerShell, Visual Basic Scripts and even macros within Microsoft's Office suite can be used to automatically execute instructions when embedded within seemingly legitimate documents. Threat actors usually prefer fileless malware as it allows them to perform an initial reconnaissance of the victim's system before "bringing out the big guns," while at the same time dodge detection from traditional security solutions.

Exploits are usually part of exploit kits that exploit unpatched or unknown vulnerabilities in operating systems, browsers, applications, or any other software running on a victim's machine. They allow attackers to force an application to "misbehave" and run malicious code, either altering the application's functionality and causing unpredictable results or instructing it to run malicious code as if it were part of it. Threat actors mostly use them as a means of covertly planting other threats, in an attempt to dodge detection from traditional security solutions. Addressing exploits is usually a matter of keeping operating systems and applications up to date, or by using a security solution that specifically looks for threats trying to exploit those unpatched vulnerabilities. From here on, we will refer to exploits as a general category encompassing exploits, unless specifically discussing a specific exploit or vulnerability.

Bankers, also known as Trojan Bankers, are used to perform financial heists. Their focus is either on harvesting credit card data when the victim types it into legitimate webpages, or redirecting victims to fraudulent webpage and instructing them to fill in financial and credit card information. A large number of banker Trojans are currently employed by threat actors, some packing more features than others. While the differences between them might revolve around

10 "How Many Cryptocurrencies Are There In 2020?", E-Cryptocurrencynews, https://e-cryptonews.com/how-many-cryptocurrencies-are-there-in-2020/

features and infrastructure, their ultimate goal remains to collect and exfiltrate financial information. From here on, we will refer to bankers as a general category that encompasses all known Trojan bankers, unless specifically discussing a specific Trojan banker threat or family.

In our 2019[11] mid-year threat landscape report, these were also the top threats analyzed. When going through this year's mid-year threat landscape report, we compare some of those figures to this year's telemetry. It's worth noting that, while some percentages might seem similar to last year, the actual number of total reports for 2020 may vary by several orders of magnitude in some instances.

Global Evolution of Windows Threats

When analyzing threat landscape telemetry for the first half of 2020, it's worth noting that year-over-year percentage increases might be the result of intensified cybercriminal activity and a potential increase in the number of protected Bitdefender endpoints or user base. However, the evolutions for some specific threats show a significant evolution in terms of year-over-year reports, which can by far outpace the evolution of Bitdefender's year-over-year user base increase. Before we dive into and analyze how some of the most popular threats have evolved during 2020 compared to 2019, let's take a look at some specific threats that we didn't discuss in our previous 2019 mid-year threat landscape report.

11 "Mid-Year Threat Landscape Report", Bitdefender, https://www.bitdefender.com/files/News/CaseStudies/study/293/Bitdefender-WhitePaper-Mid-Year-Threat-Landscape-Report-2019.pdf

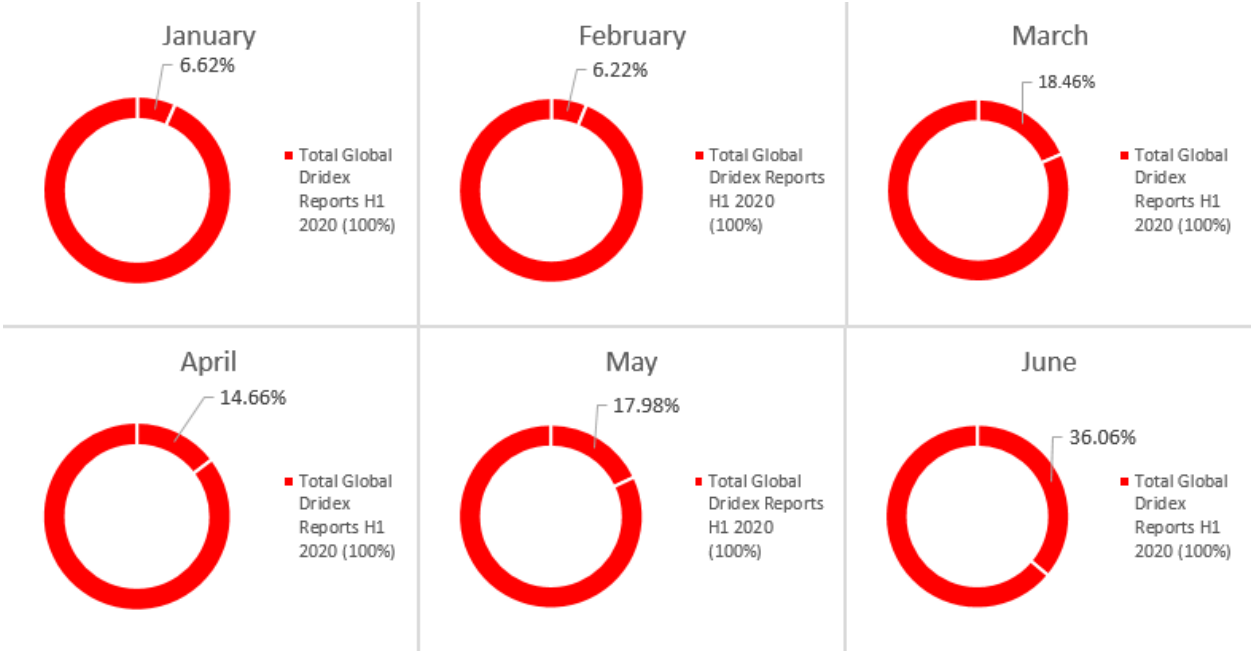
Dridex

This financially motivated banking Trojan was responsible for financial losses estimated[12] at £20 million in the UK and $10 million in the US during 2015 alone. It's far from obsolete, and spam campaigns pushing Dridex are still considered very lucrative.

The malware's diverse capabilities range from capturing screenshots and stealing credentials to incorporating the victim machine into a botnet that's either used to send spam or perform denial of service attacks. Apart from stealing sensitive data, Dridex has been known to operate in conjunction with ransomware operators, delivering ransomware-payloads to Dridex-infected victims. Paid ransom notes would then be split between the Dridex and ransomware operators.

As the malware itself is mostly distributed via spam email campaigns, looking at how the total global number of Dridex reports have evolved during the first half of 2020, it's safe to conclude that Dridex operators have intensified their activity since the global Coronavirus pandemic hit.

In January and February, the number of Dridex reports accounted for only 12.84 percent of all global Dridex reports throughout the first half of 2020, but starting in March attackers redoubled efforts to spread Dridex. While the number of reports remained steady throughout March, April and May, the biggest spike in Dridex reports was registered in June (36.06 percent, of all Dridex reports for H1 2020).



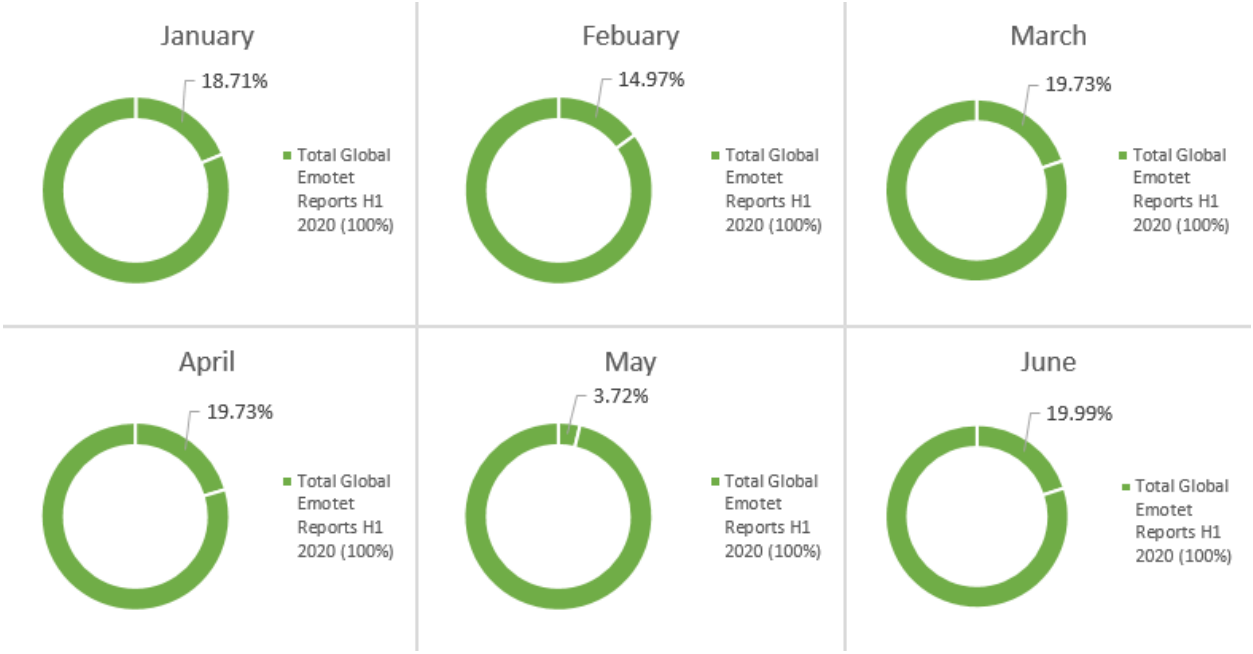
It's safe to guess that, if the pandemic proved an excellent catalyst for new Dridex campaigns in March, as pandemic restrictions eased and the holiday season kicked in, attackers likely exploited not just the Coronavirus topic in their emails, but also travel and financial subjects.

12 "Dridex", Wikipedia, https://en.wikipedia.org/wiki/Dridex

Emotet

Emotet[13] is also an advanced banking Trojan that's highly sophisticated in terms of dodging detection from security solutions. Although first identified in 2014, it has constantly been under development, with new modules added over time. While its primary purpose was to steal banking credentials and financial data, it was later used as a loader for other types of malware. Emotet operators have been known to work with other cybercriminal gangs by renting access to their botnet, also known as Infrastructure-as-a-service (IaaS), or by working with Ryuk ransomware operators.

Emotet plays an important role in the cybercrime ecosystem, as it features one of the biggest networks of compromised systems (botnets[14]). Whether it's sending out spam or performing on-demand denial of service attacks, Emotet is one of the most dangerous botnets to date.



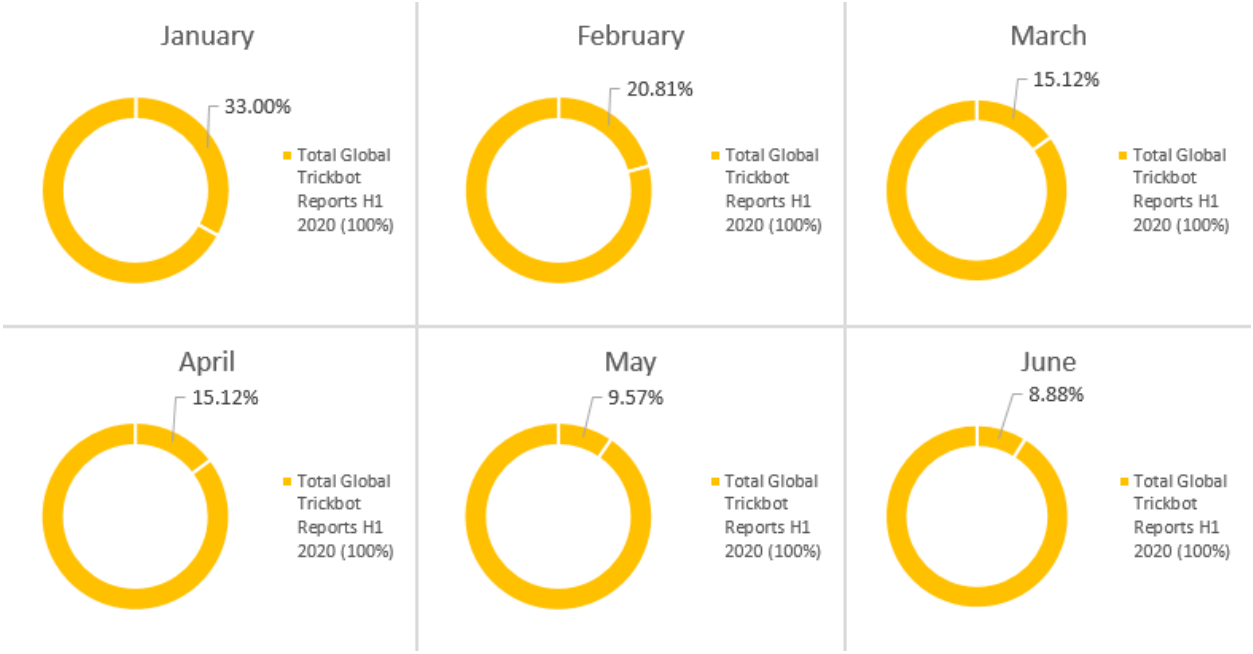
Looking at Bitdefender's telemetry on Emotet, it becomes immediately apparent that reports throughout the first half of 2020 were relatively consistent each month. While May seems to have registered the lowest number of reports – from the total number of global Emotet reports during the first half of 2020 – March, April and June registered over 19 percent each.

13 "Emotet", Wikipedia, https://en.wikipedia.org/wiki/Emotet
14 "Botnet", Wikipedia, https://en.wikipedia.org/wiki/Botnet

TrickBot

Also considered a banking Trojan, TrickBot was discovered in 2016 and was mostly distributed via email spam campaigns, embedded within seemingly legitimate attachments. While its primary purpose was to steal sensitive information, such as data and e-banking credentials, it was later updated with new modules meant for lateral movement across networks, and even the ability to exploit unpatched vulnerabilities, such as the infamous EternalBlue[15].

What sets it apart from other Trojans is its modular architecture. This allows cybercriminals to simply add new capabilities as modules, which can work with the Trojan's existing core functions. Bitdefender researchers recently[16] stumbled on such a new module designed to bruteforce RDP connections belonging to select telecommunication services in the US and Hong Kong. TrickBot has also been distributed both via spam campaigns and by other similar banking Trojans, such as Emotet. While some core functionalities of the two Trojans overlap, TrickBot's modular architecture makes it a highly versatile threat that threat actors can use to both move laterally across infected networks and deploy any new malicious payload on victims' machines.



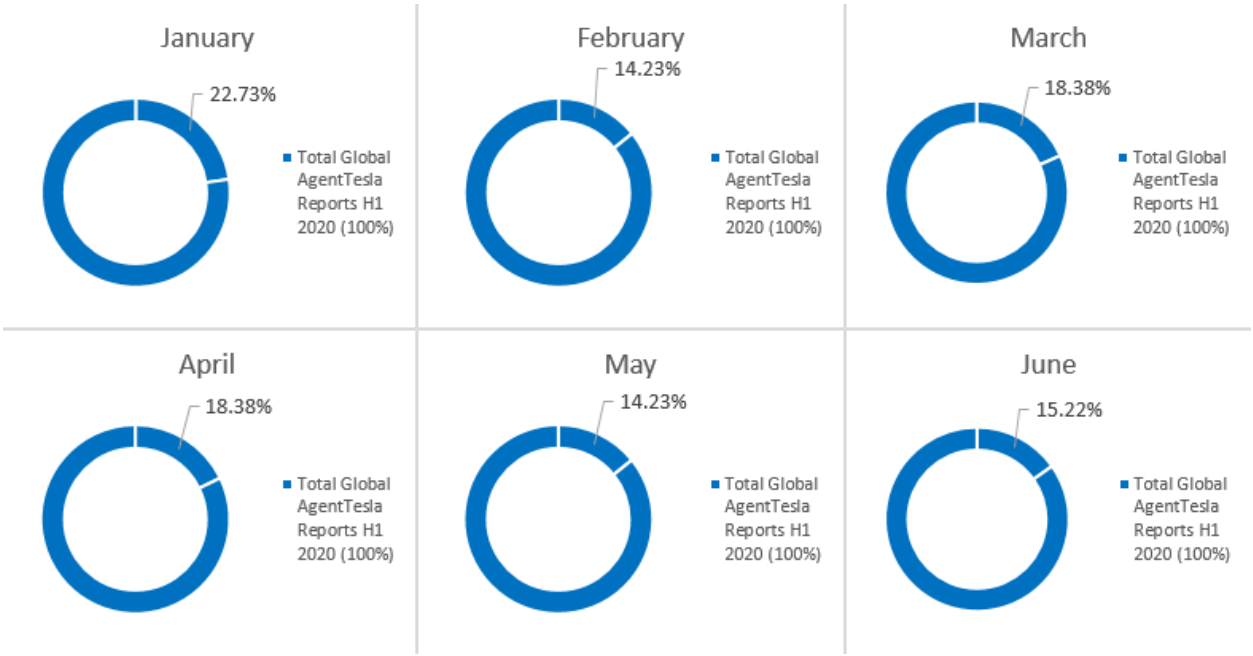
Looking at how the number of global TrickBot reports during the first half of 2020, most seem to have occurred during the first four months, accounting for 84.05 percent of the total number of reports in H1 2020.

15 "EternalBlue, Wikipedia, https://en.wikipedia.org/wiki/EternalBlue
16 "New TrickBot Module Bruteforces RDP Connections, Targets Select Telecommunication Services in US and Hong Kong", Bitdefender, https://labs.bitdefender.com/2020/03/new-trickbot-module-bruteforces-rdp-connections-targets-select-telecommunication-services-in-us-and-hong-kong/

AgentTesla

Known since 2014, the password-stealing AgentTesla Trojan has become popular mostly because of it's As-a-Service business model and easy-to-use interface. Featuring a wide range of surveillance, data-stealing and security-dodging features, malware developers have been distributing AgentTesla using various business models, including subscription-based. Malware-as-a-service is not new, but it does allow malware developers to focus on improving the capabilities of the Trojan, while others use it to steal information or amass massive botnets.

Since AgentTesla can be bought on obscure forums by anyone interested, it could also be used in sophisticated spearphishing campaigns operated by advanced cybercriminals to cover their tracks in case of detection and make it seem like a traditional infection. Bitdefender researchers have recently[17] found a highly targeted spearphishing campaign going after companies in oil & gas, just days in advance of the historic OPEC+ deal following the oil crisis caused by the Coronavirus pandemic.



Looking at how AgentTesla reports evolved during the first half of 2020, it becomes clear that it's popular among cybercriminals and that it's something we'll be seeing for a long time. Although reports peaked in January at 22.73 percent – of all AgentTesla reports in H1– reports remained relatively constant during the first half of 2020. While it might not be as versatile or as mainstream as Emotet or TrickBot, the AgentTesla Trojan still packs enough spyware features to turn it into a very potent espionage threat.

17 "Oil & Gas Spearphishing Campaigns Drop Agent Tesla Spyware in Advance of Historic OPEC+ Deal", Bitdefender, https://labs.bitdefender.com/2020/04/oil-gas-spearphishing-campaigns-drop-agent-tesla-spyware-in-advance-of-historic-opec-deal/

Ransomware

Compared to the first half of 2019, the Windows threat landscape for the first half of 2020 saw some interesting developments when looking at some of the most popular threats. For example, if during the first half of 2019 **ransomware reports** were at their lowest in January (12.82 percent) of all ransomware reports during the first half of 2019, during the same time span in 2020 ransomware reports peaked during January (19.20 percent), of all ransomware reports during the first half of 2020.

Interestingly, the total number of **global ransomware reports increased by 715.08 percent YoY**, potentially suggesting that threat actors upped their ransomware campaigns to capitalize on both the pandemic and the work-from-home context and the commoditization of ransomware-as-a-service. However, looking at the monthly evolution of ransomware, other interesting patterns emerge. For example, if during the first half of 2019 ransomware reports were relatively low, only to peak in May, during the first half of 2020 global ransomware reports have somewhat remained constant throughout the first six months, with no notable spikes or drops.

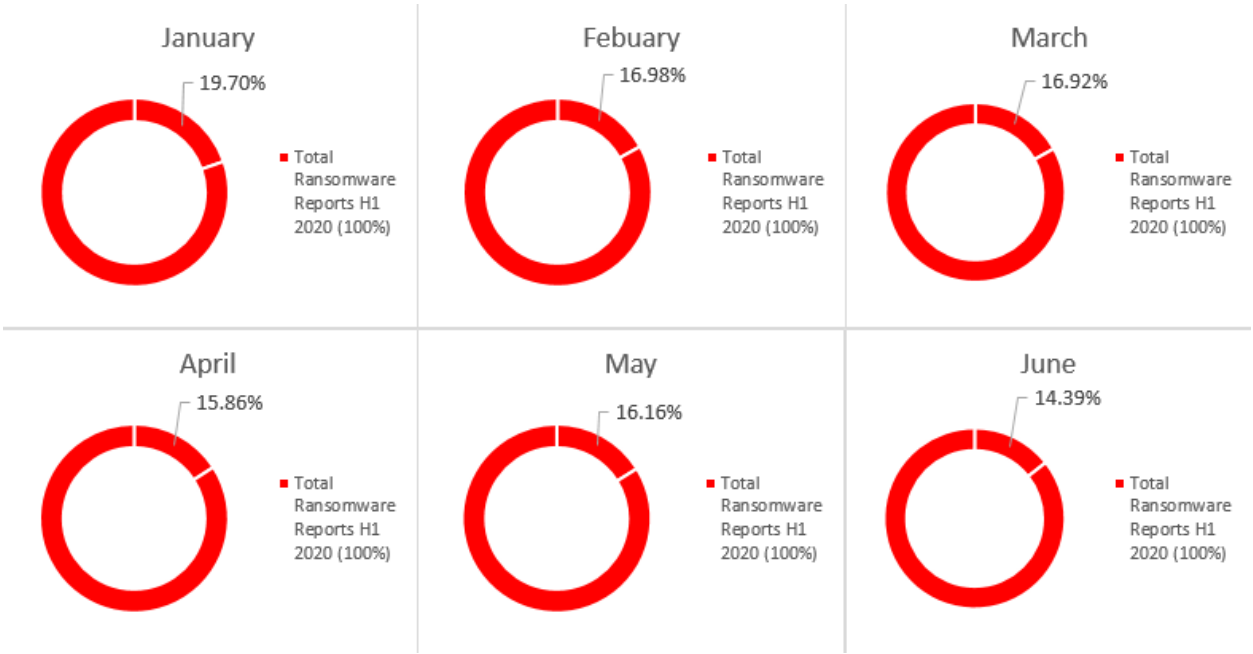


Fig. 1 – Global ransomware evolution H1 2020

Coin miners, fileless malware and exploit reports have also seen a steady increase in the number of reports during the first half of 2020 when compared to 2019. However, if reports spiked during 2019 in particular months, this year their reports barely fluctuated.

Coin Miners

For instance, **coin miner reports** held steady throughout the first half of 2019, with reports relatively constant from one month to the next. During the same time span in 2020, February recorded the highest spike, with 33.75 percent of all coin miner reports for the first half of 2020.

While the number of reports seem to have followed a descending path throughout the next couple of months of 2020, **the total number of coin miner reports during H1 2020 increased by 20.32 percent compared to first half of 2019.** While the increase in reports might not be as significant as the spike in ransomware reports, it does reveal continued interest in coin miners.

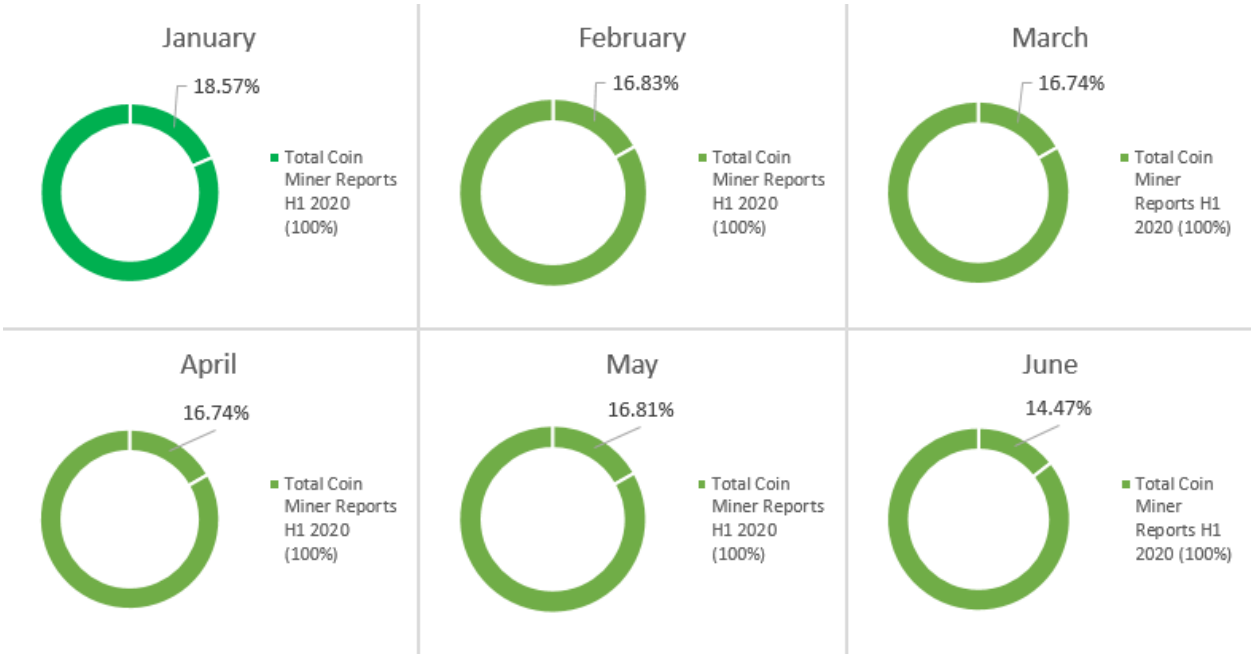


Fig. 2 – Global Coin Miner Evolution H1 2020

Exploits

Exploits have also had an interesting evolution throughout the first half of 2020, as the global number of exploit reports have **increased by 405.79 percent** compared to the global number of exploit reports during the first half of 2019. However, in terms of distribution, things are relatively similar to how coin miners have evolved. Exploits also peaked in **February, accounting for 29.11 percent of all exploit reports during the first half of 2020**.

If throughout the first half of 2019 exploit reports were relatively equally distributed from January until June, during the first half of 2020, only February showed a spike, with reports plateauing from March until June. However, it is worth pointing out that overall, the total number of exploit reports throughout H1 2020 was four times higher than in the first half of 2019.

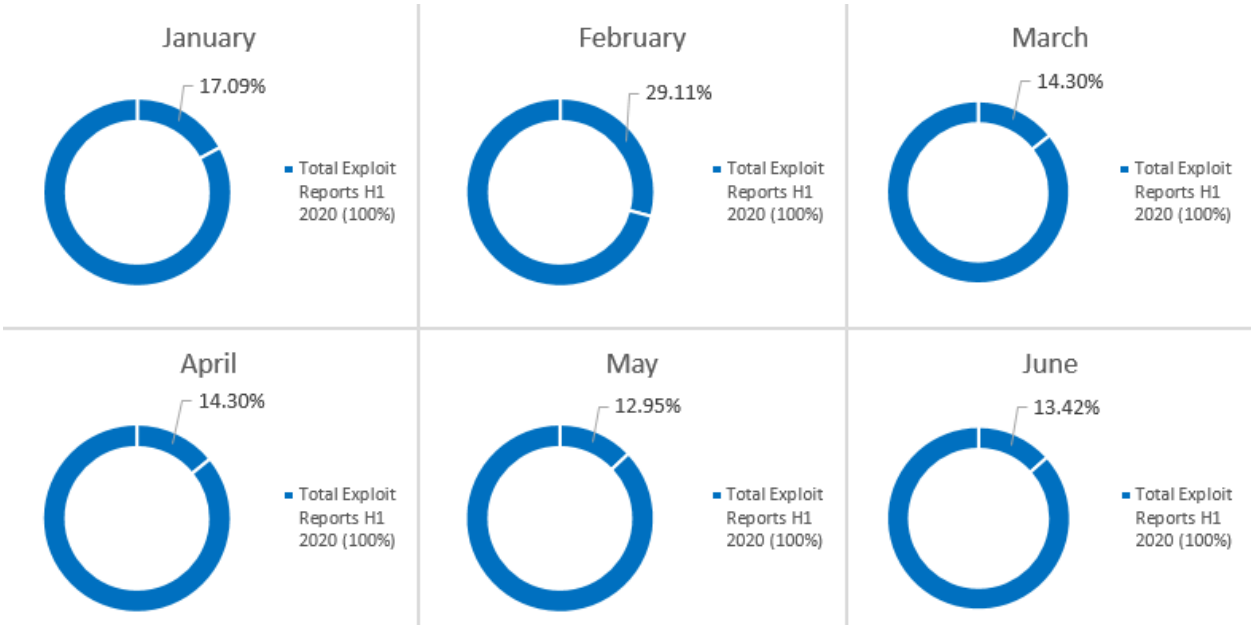


Fig. 3 – Global Exploit Evolution H1 2020

Fileless Malware

Fileless malware reports in the first half of 2019 were relatively constant from January until May, registering minor fluctuations. The lowest number of reports was registered in June 2019, with 14.89 percent of all fileless malware reports throughout the first half of 2019. However, during the same time span in 2020, fileless malware reports peaked during **January (20.69 percent) and March (23.56)**, both accounting for 44.25 percent of all fileless malware reports throughout the first half of 2020. While reports may have fluctuated during the next three months, it is worth nothing that that fileless malware is still popular with threat actors.

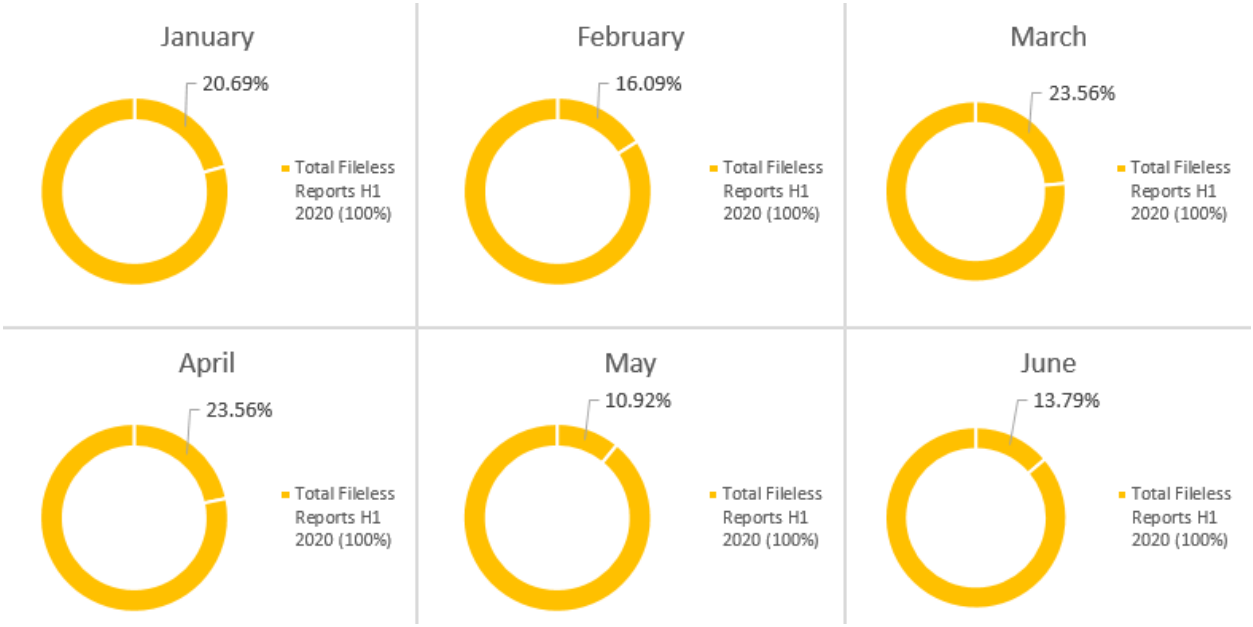


Fig. 4 – Global Fileless malware evolution H1 2020

Bankers

Looking at the **global evolution of bankers**, reports **during the first half of 2020 increased seven-fold compared to the first half of 2019**. While bankers have become extremely popular and versatile in terms of dodging security solutions and bundling in new features, during the first half of 2019 banker reports were evenly distributed from January through June.

This **banker distribution changed during H1 2020**, as banker reports started to spike throughout April, May and June 2020, accounting for 64.52 percent of all banker reports during the first half of 2020. If during the first three months of 2020 threat actors were mostly focused on ransomware and other traditional threats, it wasn't until April that banker campaigns started to pick up steam.

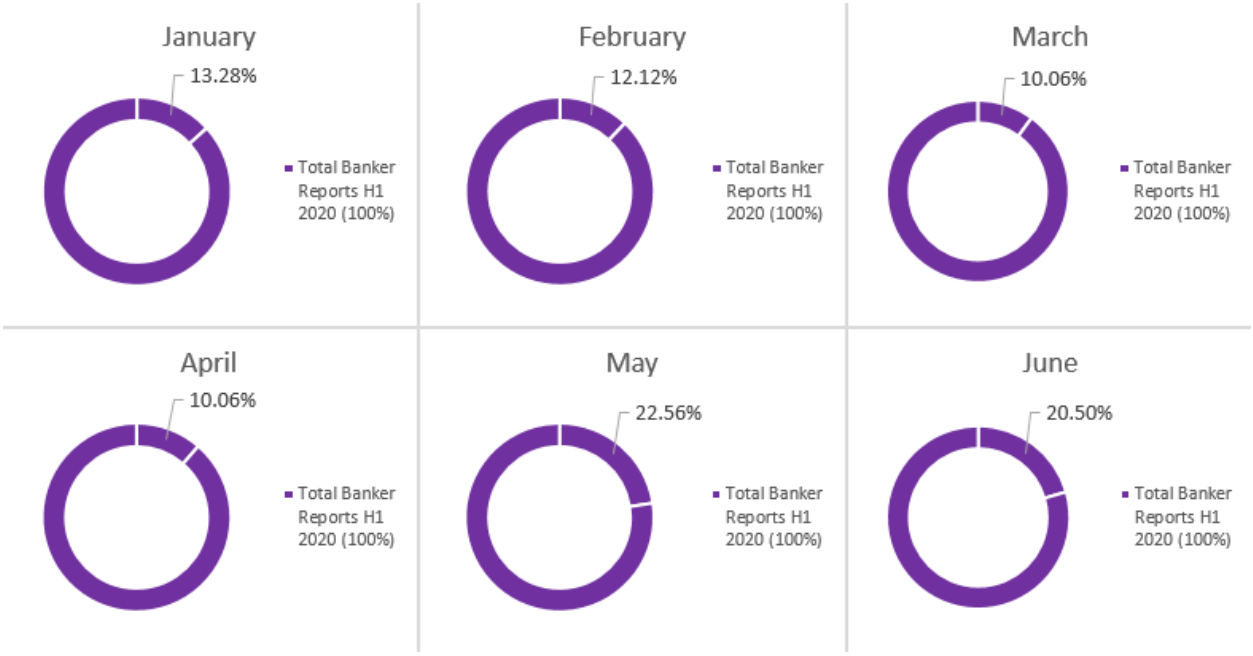


Fig. 5 – Global Bankers evolution H1 2019 vs H1 2020

Potentially Unwanted Applications (PUA)

While it's not considered a threat or malware per se, but more of a nuisance, Potentially Unwanted Applications (PUAs) can cause serious usability and performance issues and are generally irksome if they end up on Windows or macOS-running machines. While the number of **PUA reports increased by 332.5 percent during the first half of 2020 compared to the first half of 2019**, the monthly evolution of PUA reports differed significantly.

If **during the first half of 2019 the number of PUA reports spiked in January (17.74 percent** of all PUA reports during the first half of 2019), during the next five months it registered minor fluctuations. During the first half of 2020, PUA reports were at their lowest in January (11.28 percent of all PUA reports during H1 2020), only to steadily increase throughout the next four months, peaking in May (20.23 percent of the total number of PUA reports during H1 2020). It's obvious when comparing the year-over-year PUA reports that, while during the first half of 2019 PUA reports followed a descending path from January until June, during the same time span in 2020 PUA reports followed an ascending path from January until June, in terms of reports.

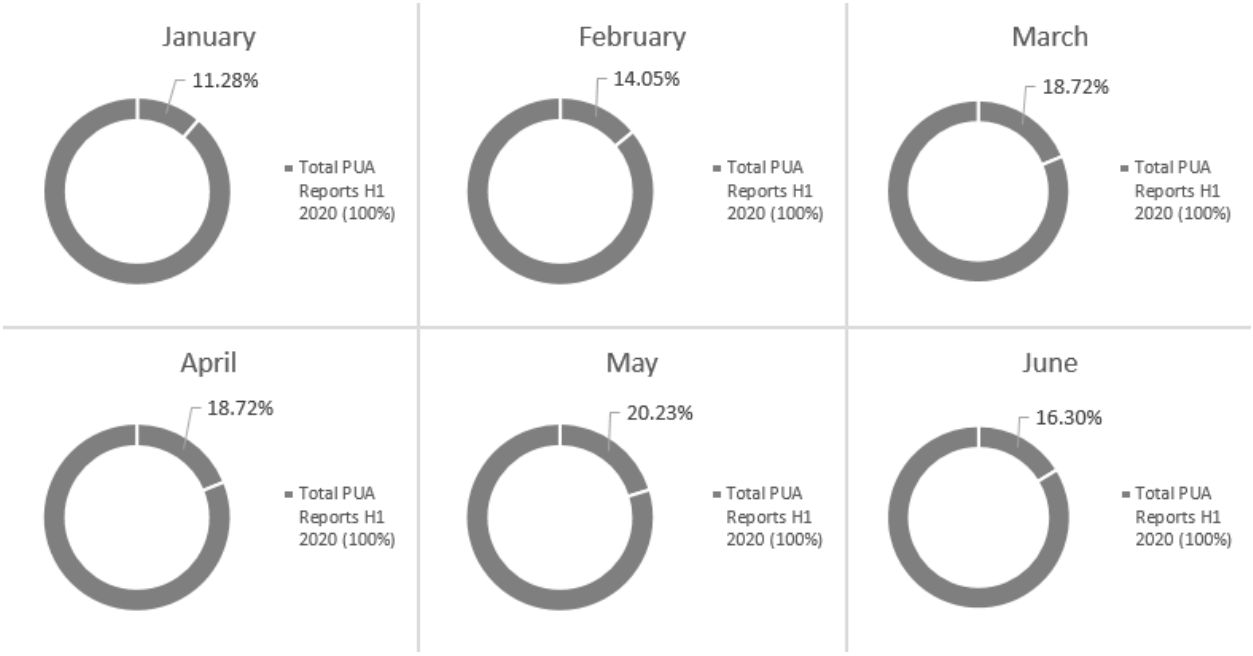


Fig. 6 – Global PUA evolution H1 2020

Evolution of Top Ransomware Families

In our previous mid-year threat landscape report for 2019 we analyzed the evolution of some of the most popular ransomware families at the time. Looking at how the same ransomware families have evolved throughout the first half of 2020, it's safe to conclude that, apart from some minor spikes, they're still going strong.

Attempts to infect users with ransomware in 2020 have not slowed down. In fact, it's anything but, supporting the notion that all schools of malicious actors have ramped up their efforts to capitalize on vulnerable remote workers and worried members of the public seeking information related to the pandemic.

The end of 2019 marked a notable new trend in the ransomware business, with operators not only holding data for ransom, but also copying it and threatening to make it public, coercing victims to cave in and pay. The infamous Maze Team presumably started the trend as the world edged closer to 2020. Rival ransomware gangs soon took notice of their success and adopted their modus operandi to spur their own operations. Despite gripping headlines about ransomware strains like REvil, Maze, DoppelPaymer, Nemty and others, there are plenty of ransomware families out there that offer their services to the highest bidder.

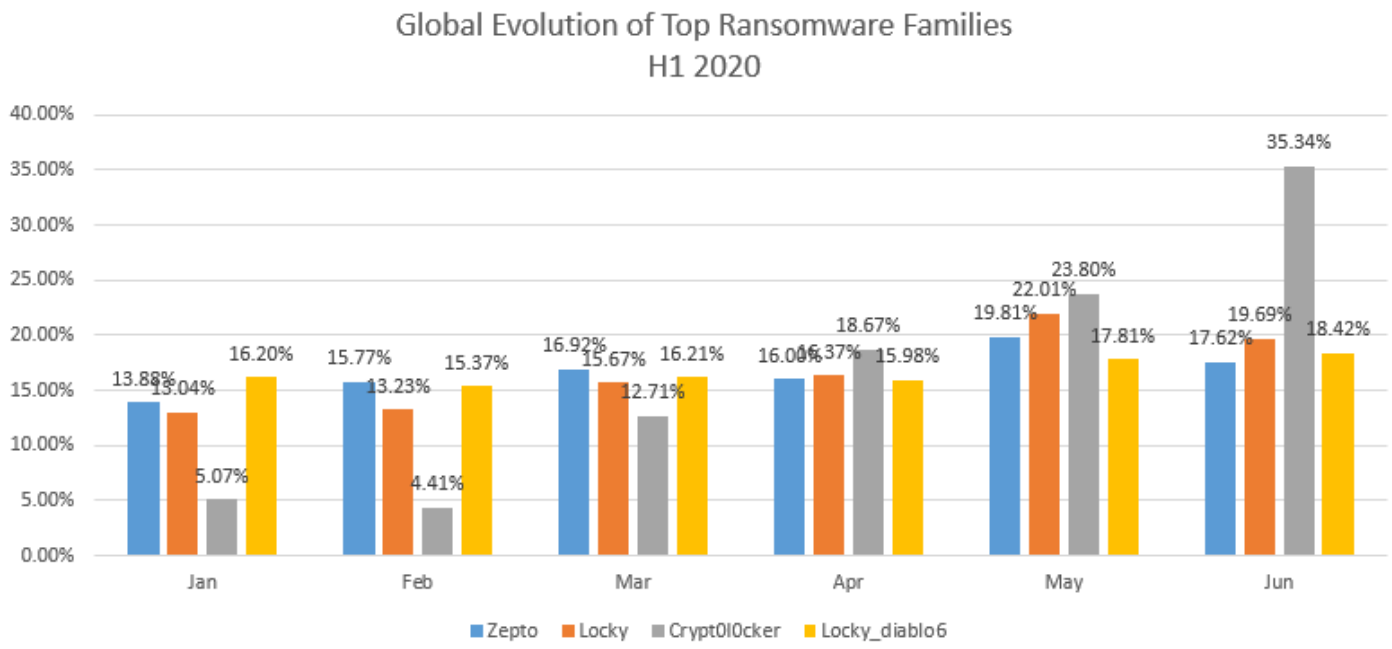


Fig. 7 - Global Evolution of Top Ransomware Families H1 2020

Some new families showed up during the first half of 2020, such as Sodinokibi (aka REvil or Sodin), known to focus on specific industry verticals by targeting various organizations and industrial infrastructures. If during the first half of 2019 it barely registered in our global telemetry, during the first half of 2020 this particular ransomware family seems to have become more popular. For instance, April, May and June accounted for **75.98 percent** of all Sodinokibi reports during the first half of 2020.

United States

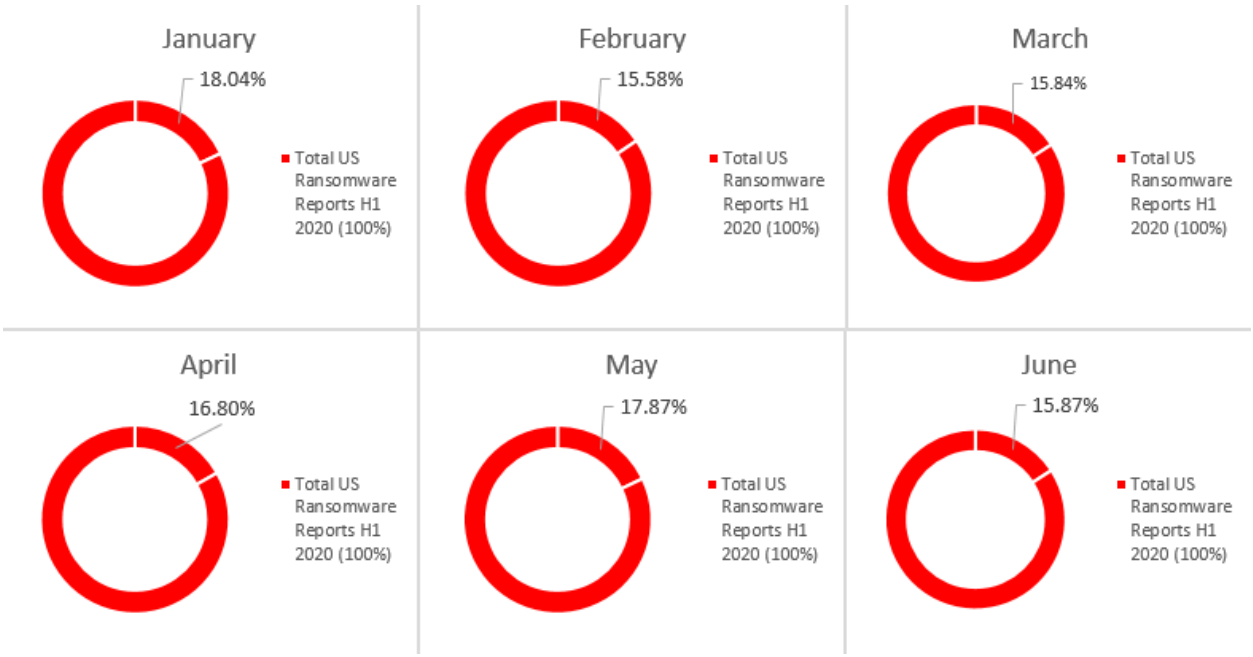


Fig. 8 –US Ransomware Evolution H1 2020

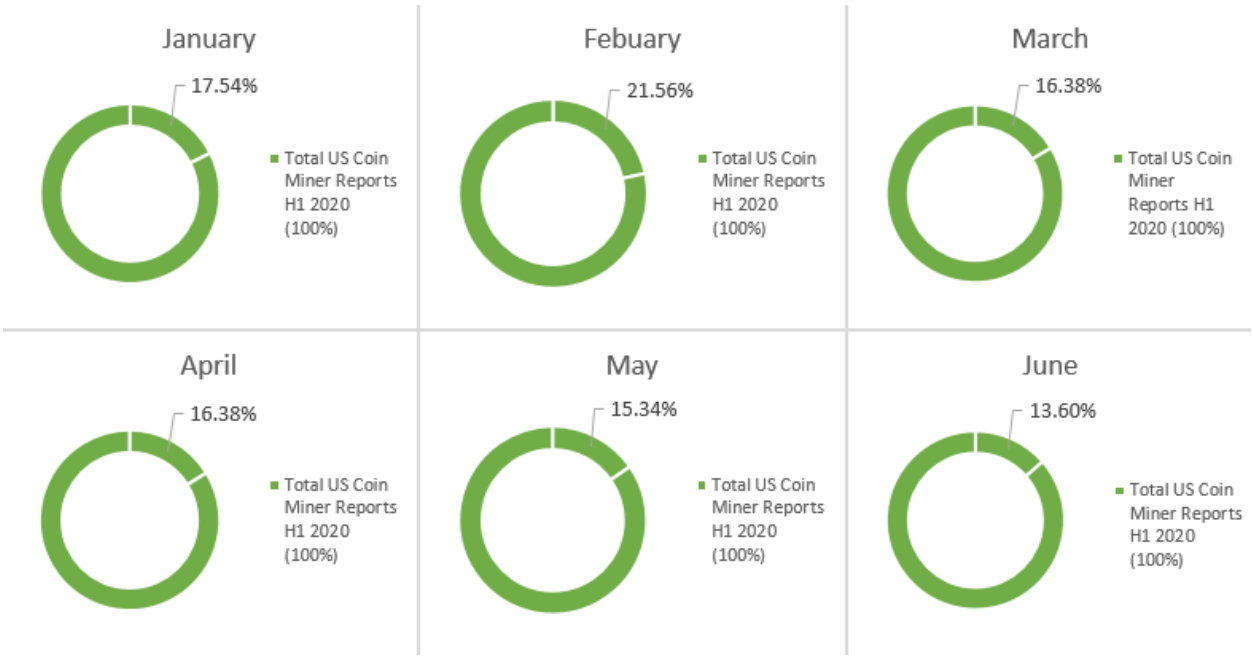


Fig. 9 –US Coin Miner Evolution H1 2020

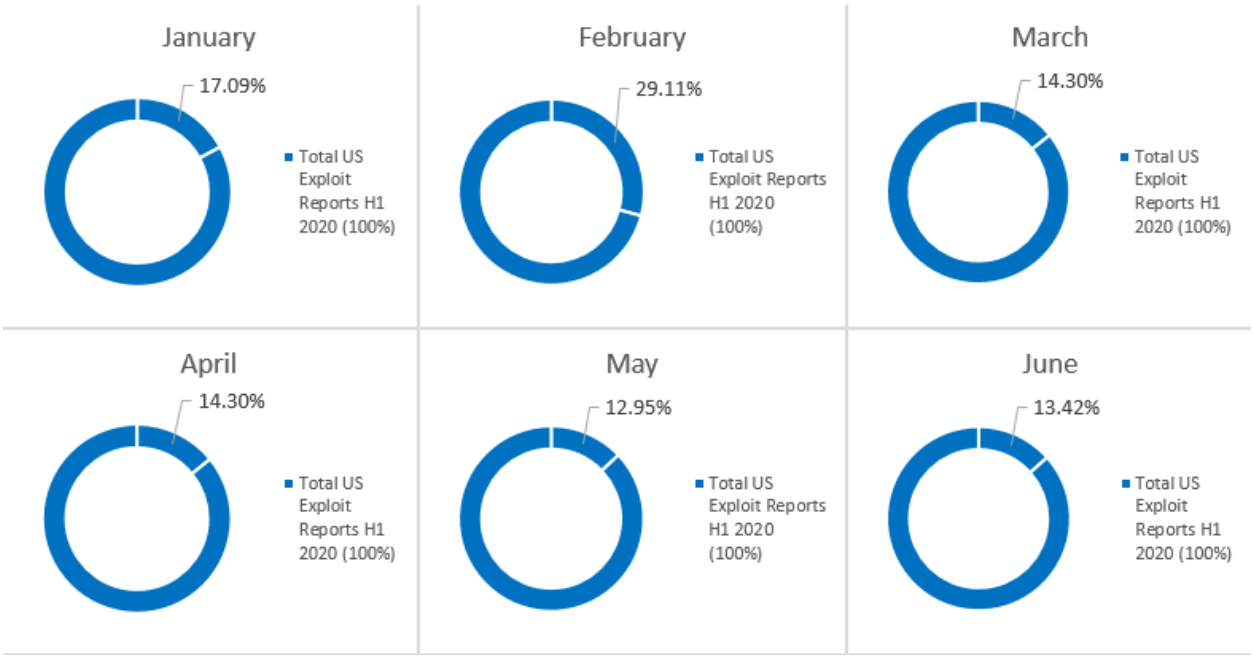


Fig. 10 –US Exploit Evolution H1 2020

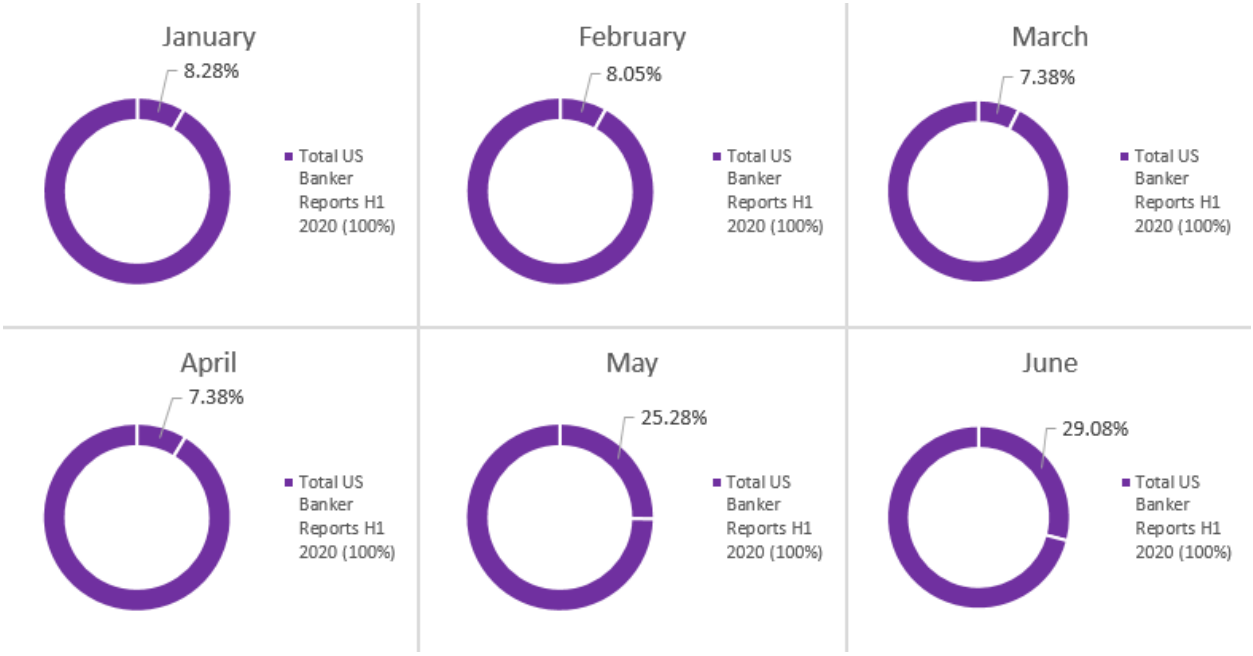


Fig. 11 –US Banker Evolution H1 2020

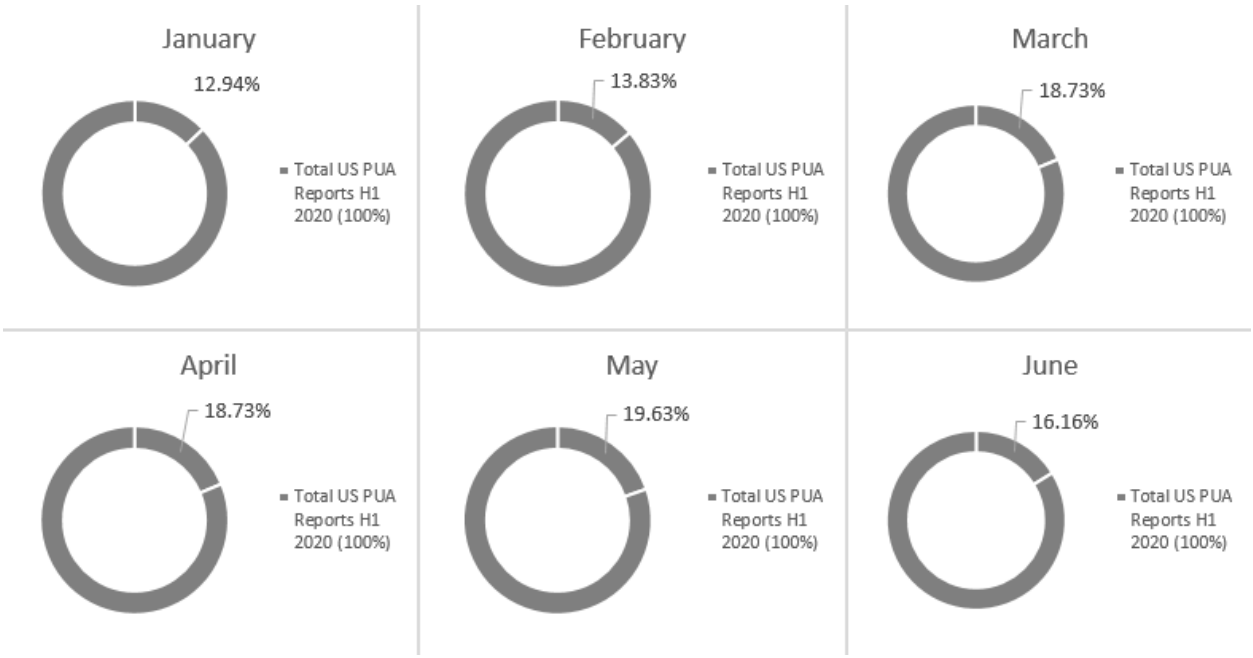


Fig. 12 –US PUA Evolution H1 2020

The United Kingdom

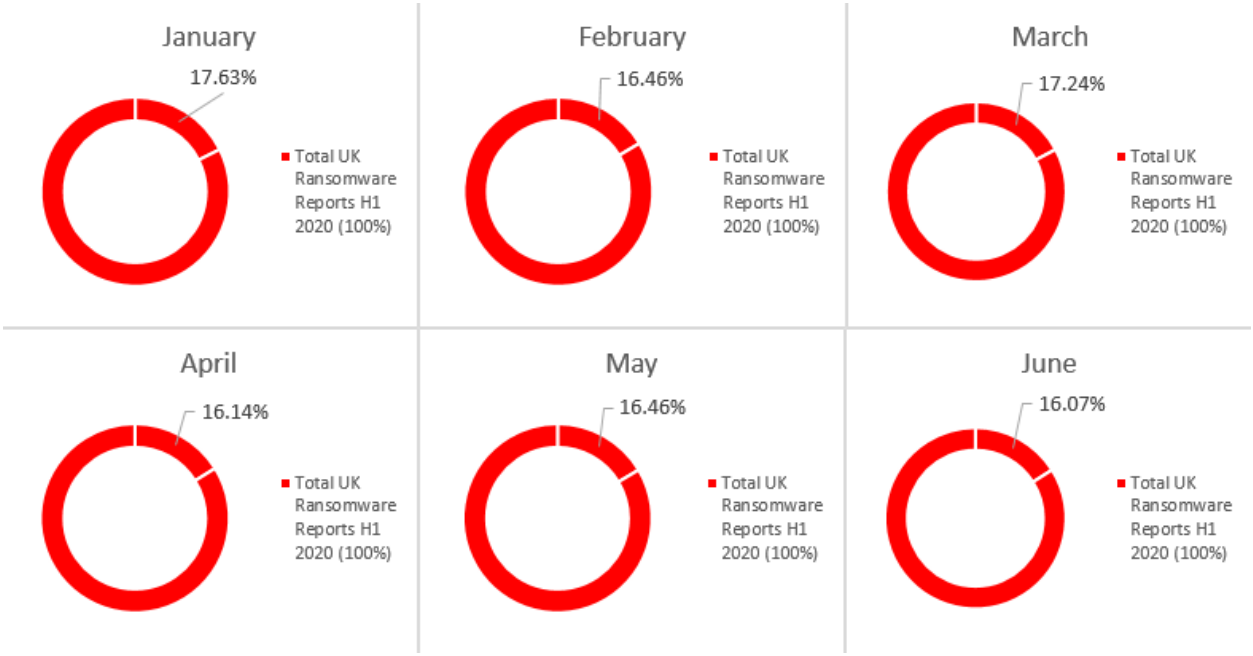


Fig. 13 –UK Ransomware Evolution H1 2020

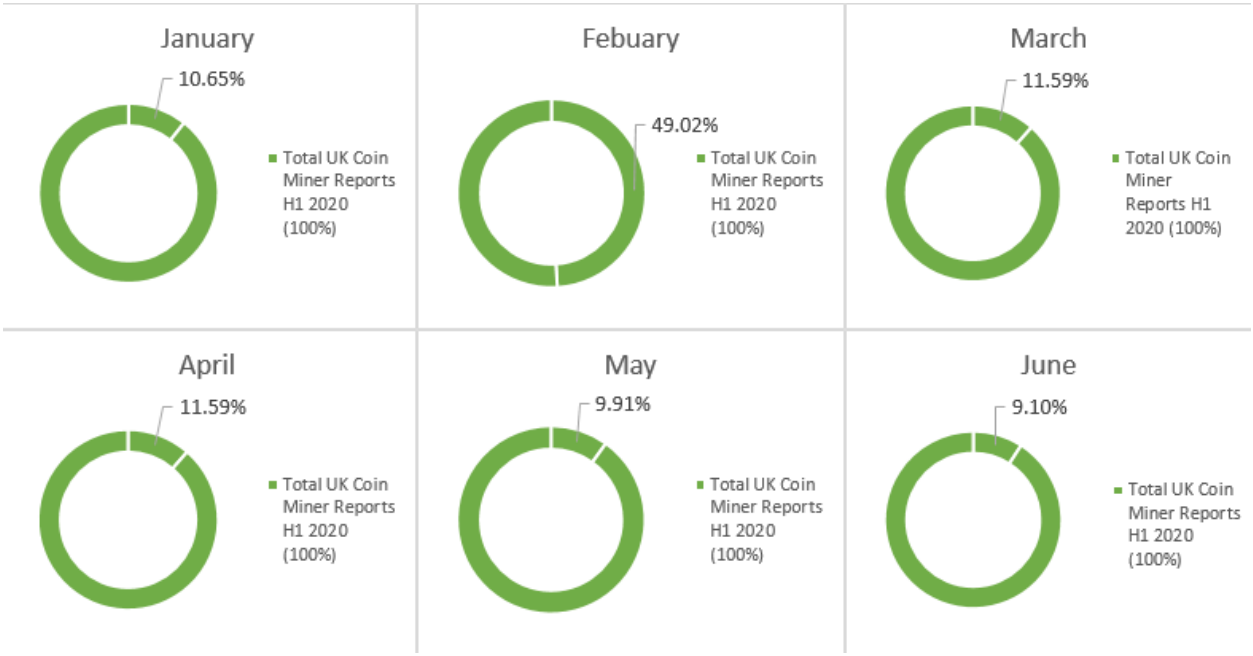


Fig. 14 –UK Coin Miner Evolution H1 2020

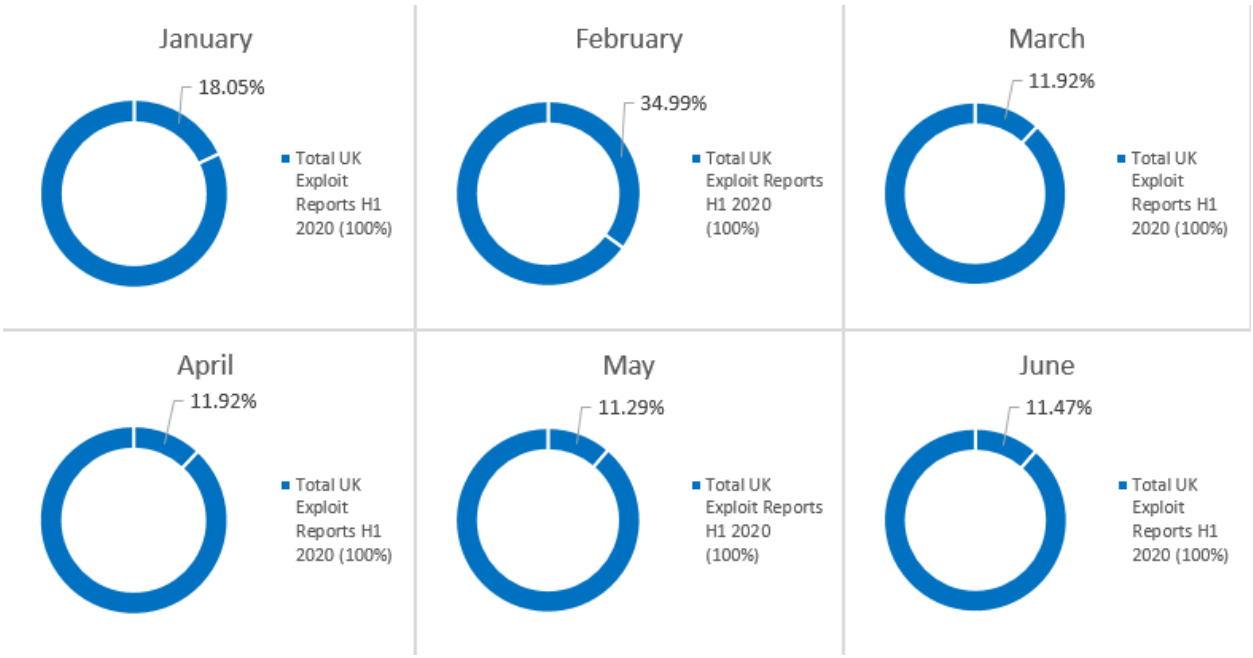


Fig. 15 –UK Exploit Evolution H1 2020

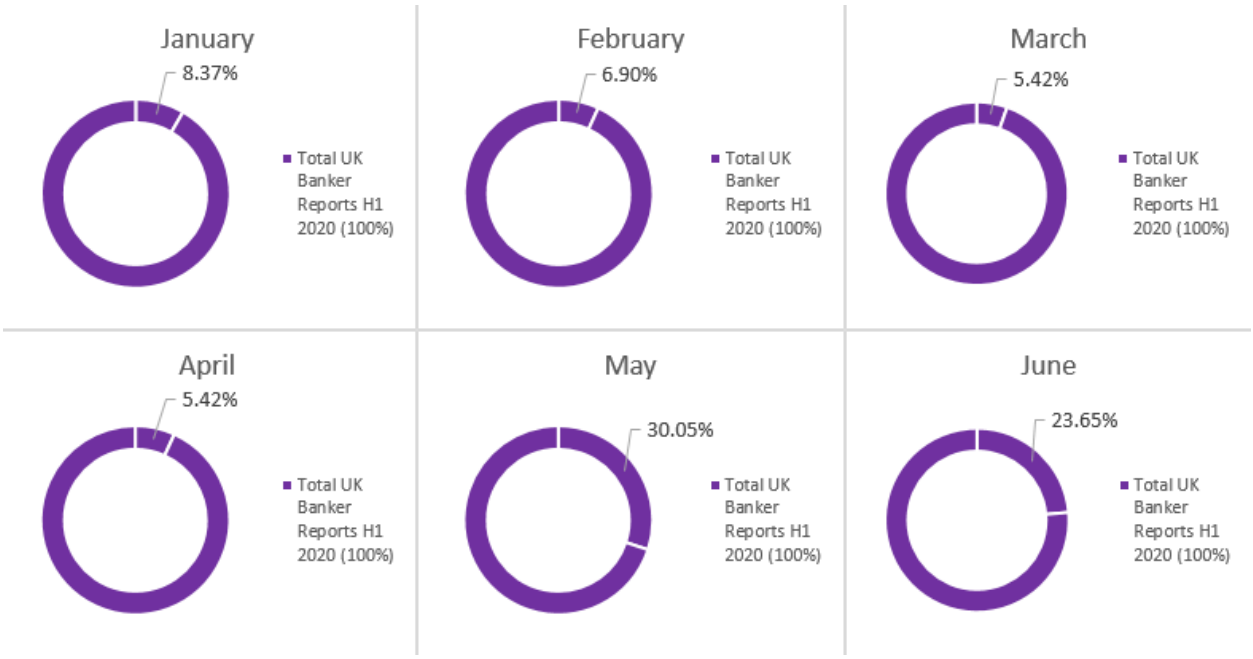


Fig. 16 –UK Banker Evolution H1 2020

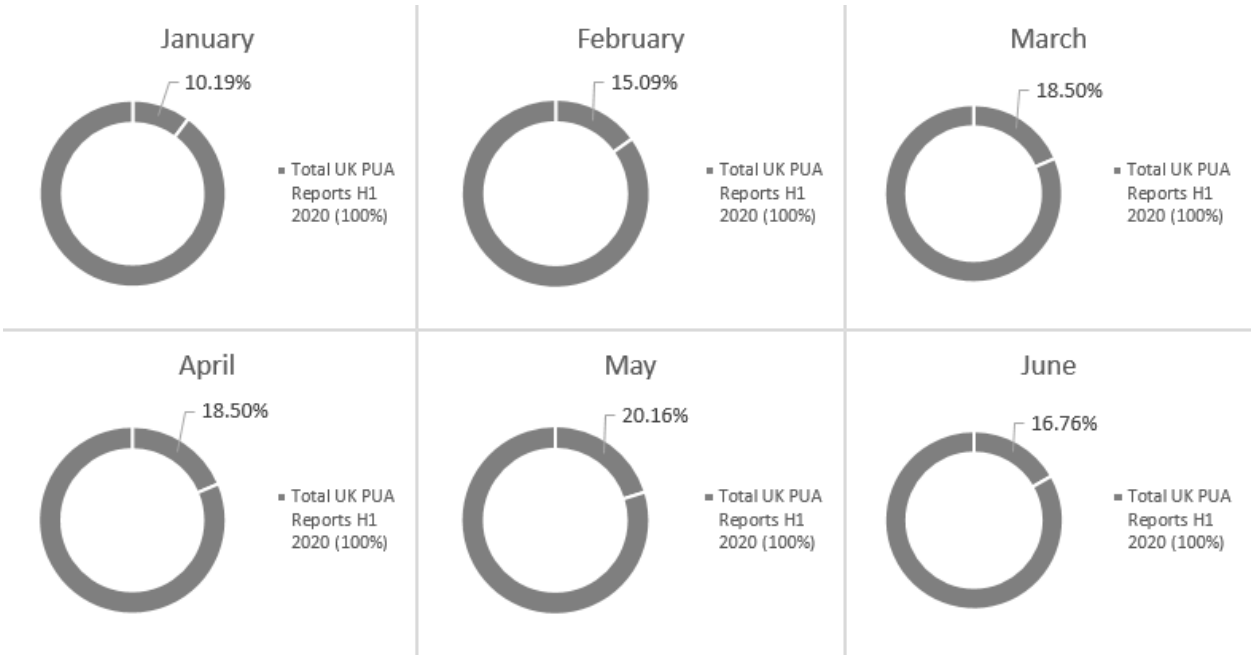


Fig. 17 –UK PUA Evolution H1 2020

Sweden

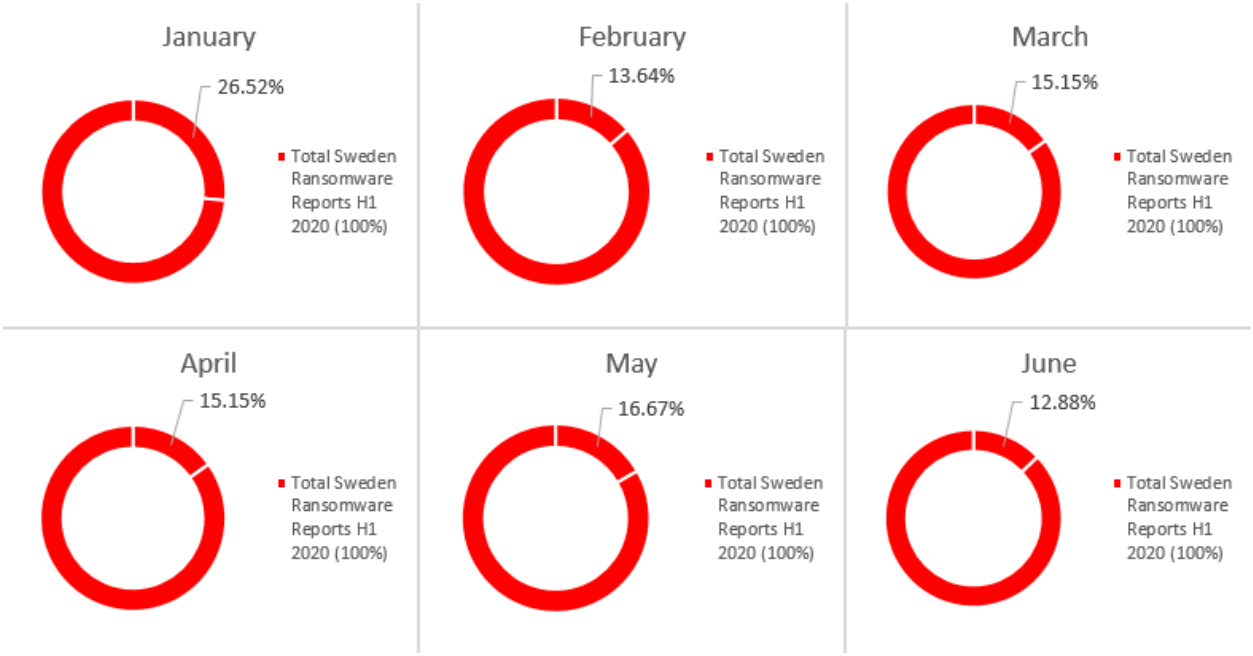


Fig. 18 –Sweden Ransomware Evolution H1 2020

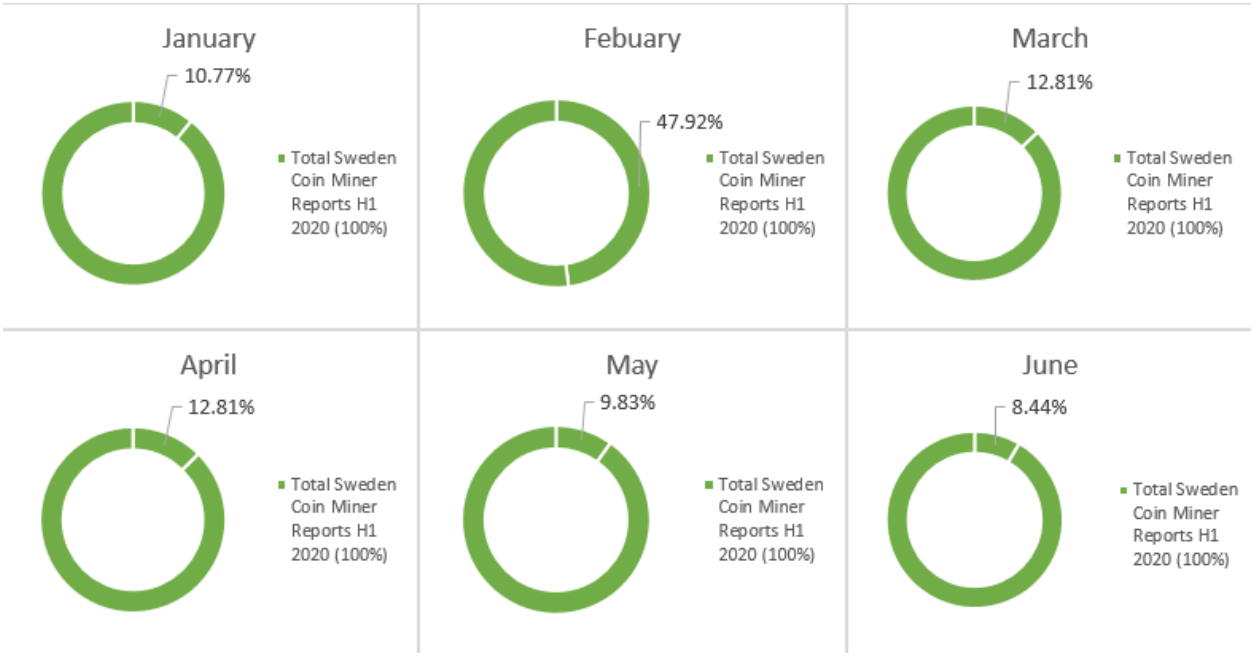


Fig. 19 –Sweden Coin Miner Evolution H1 2020

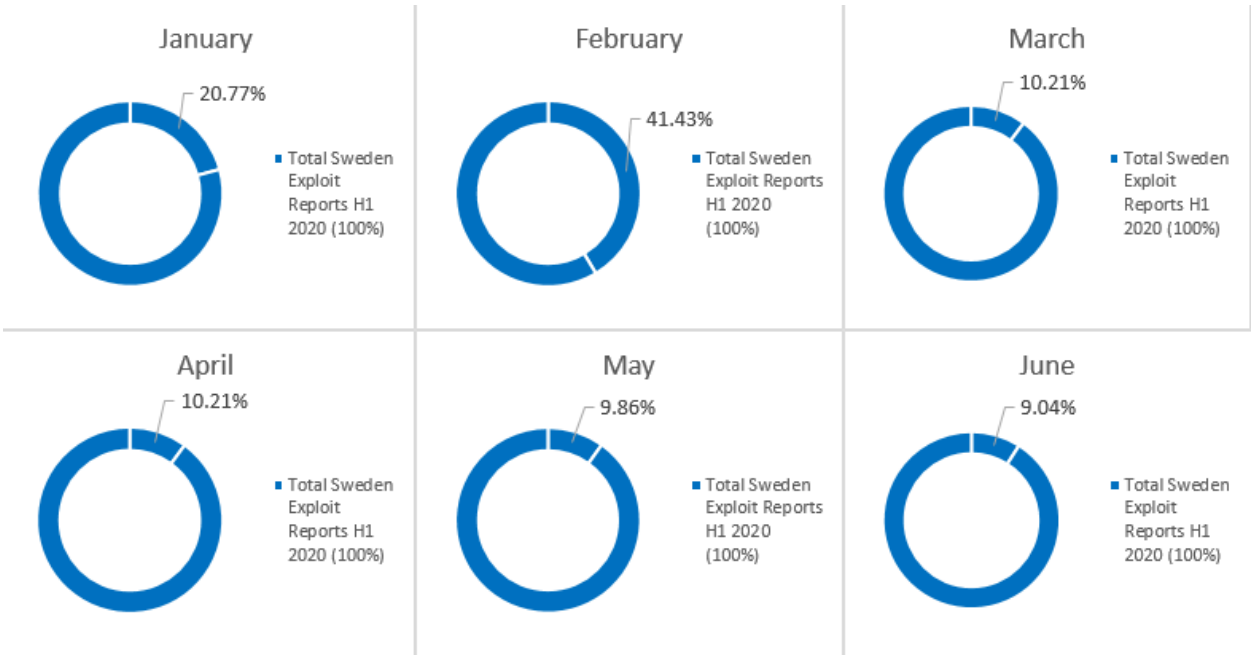


Fig. 120 –Sweden Exploit Evolution H1 2020

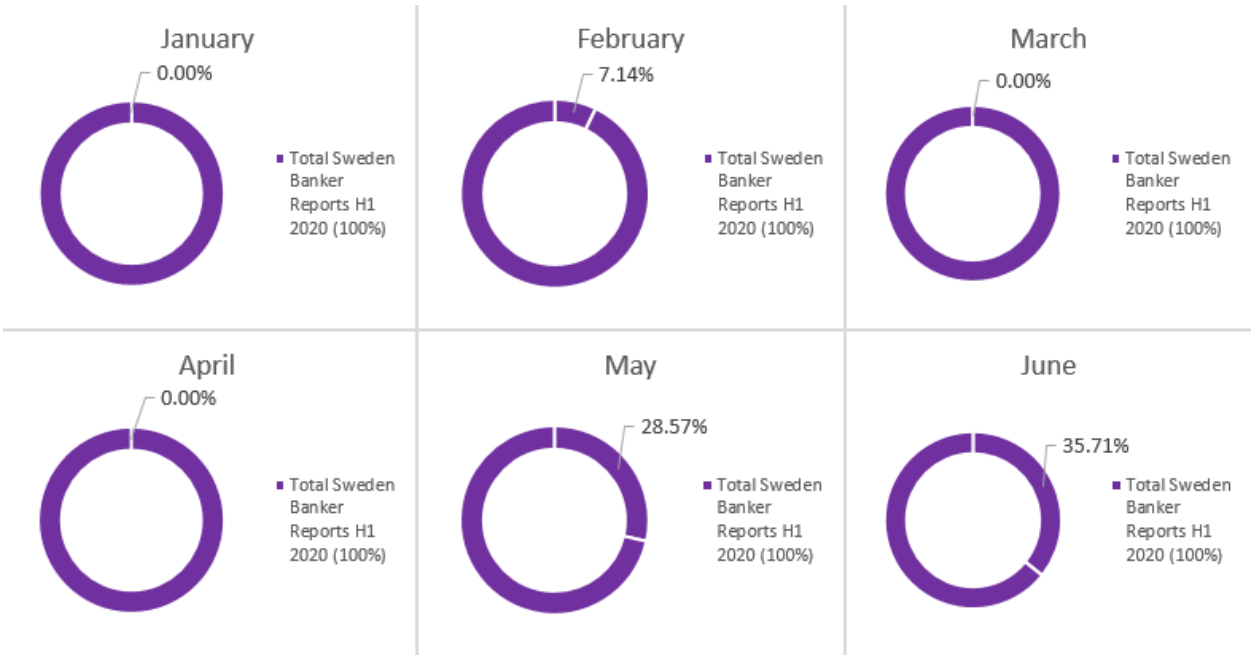


Fig. 21 –Sweden Banker Evolution H1 2020

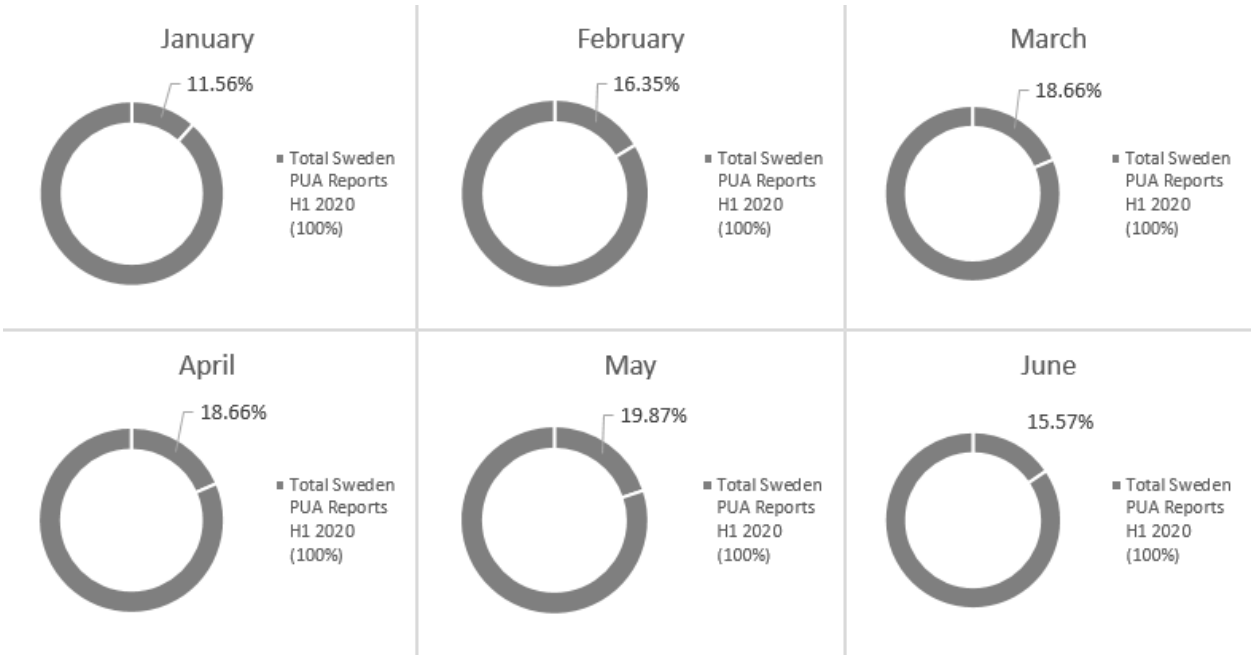


Fig. 22 –Sweden PUA Evolution H1 2020

Romania

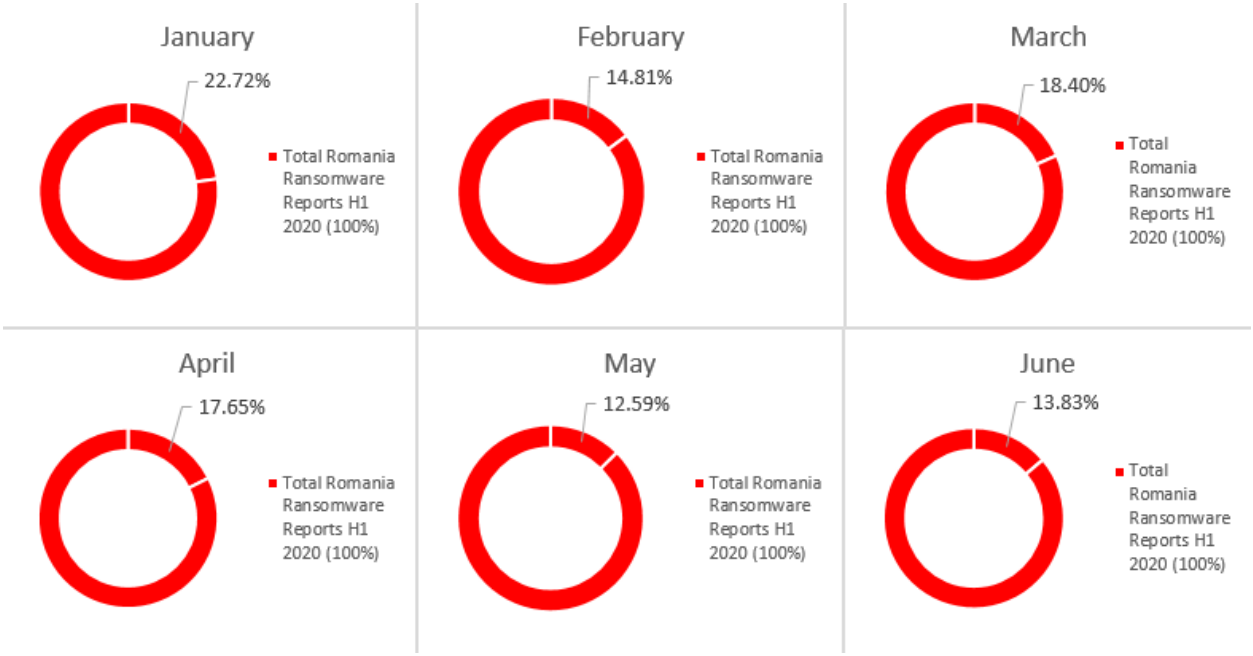


Fig. 23 –Romania Ransomware Evolution H1 2020

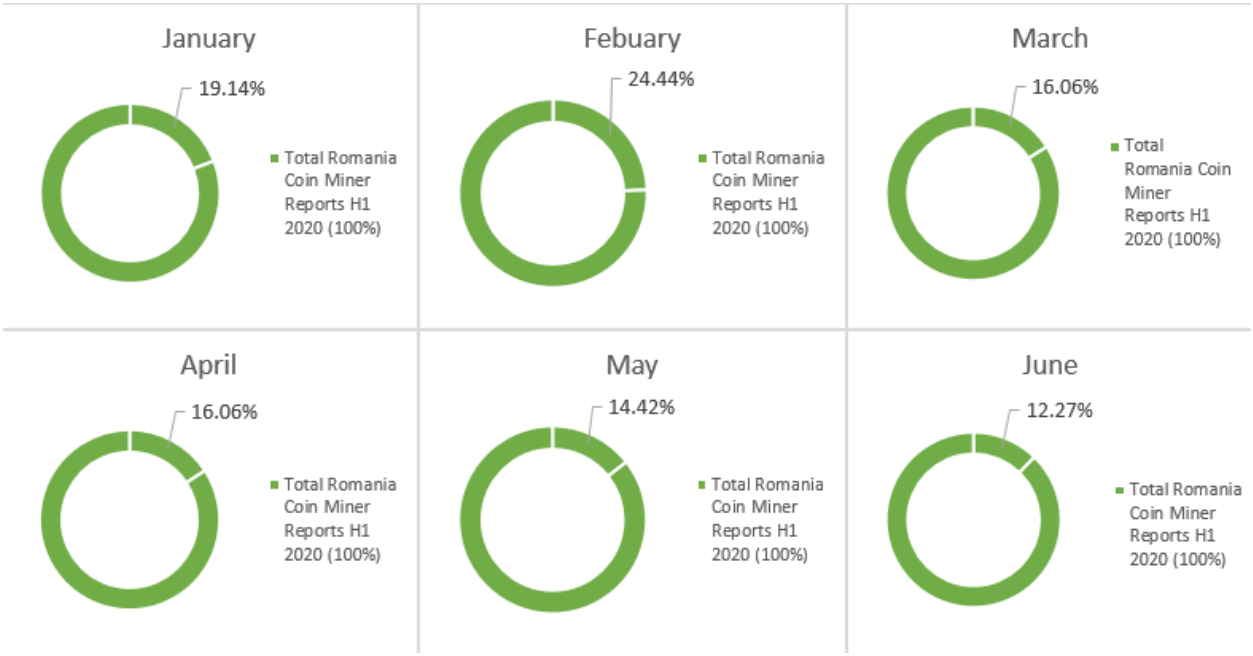


Fig. 24 –Romania Coin Miner Evolution H1 2020

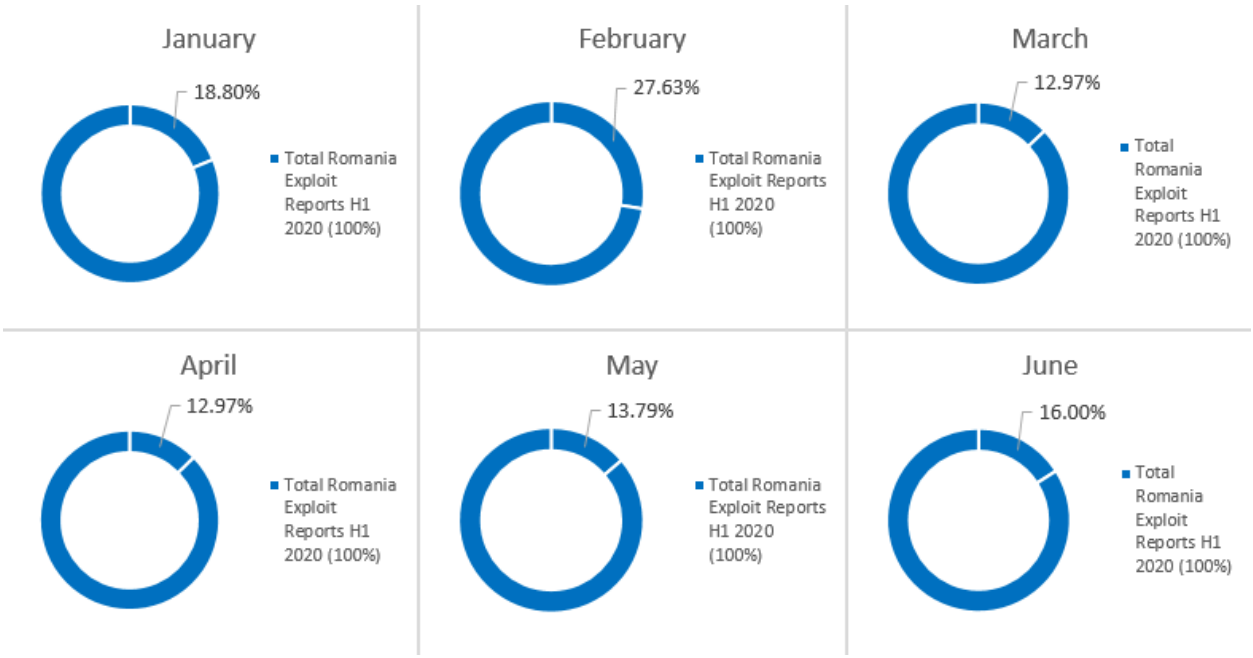


Fig. 25 –Romania Exploit Evolution H1 2020

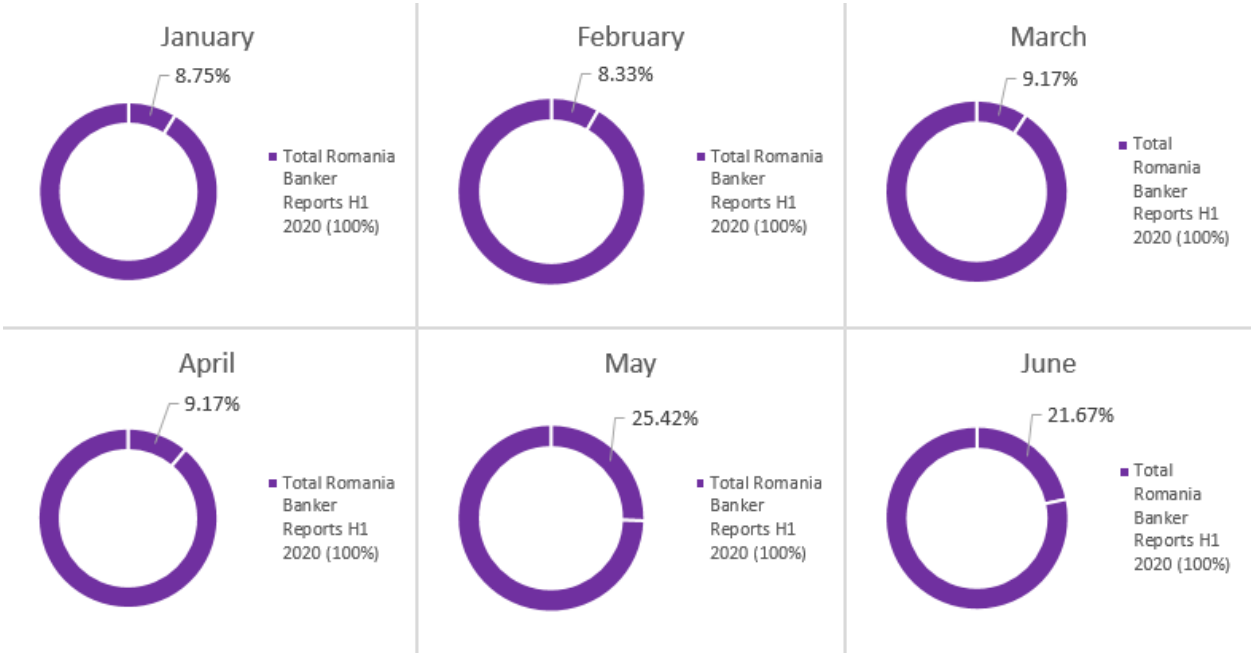


Fig. 26 –Romania Banker Evolution H1 2020

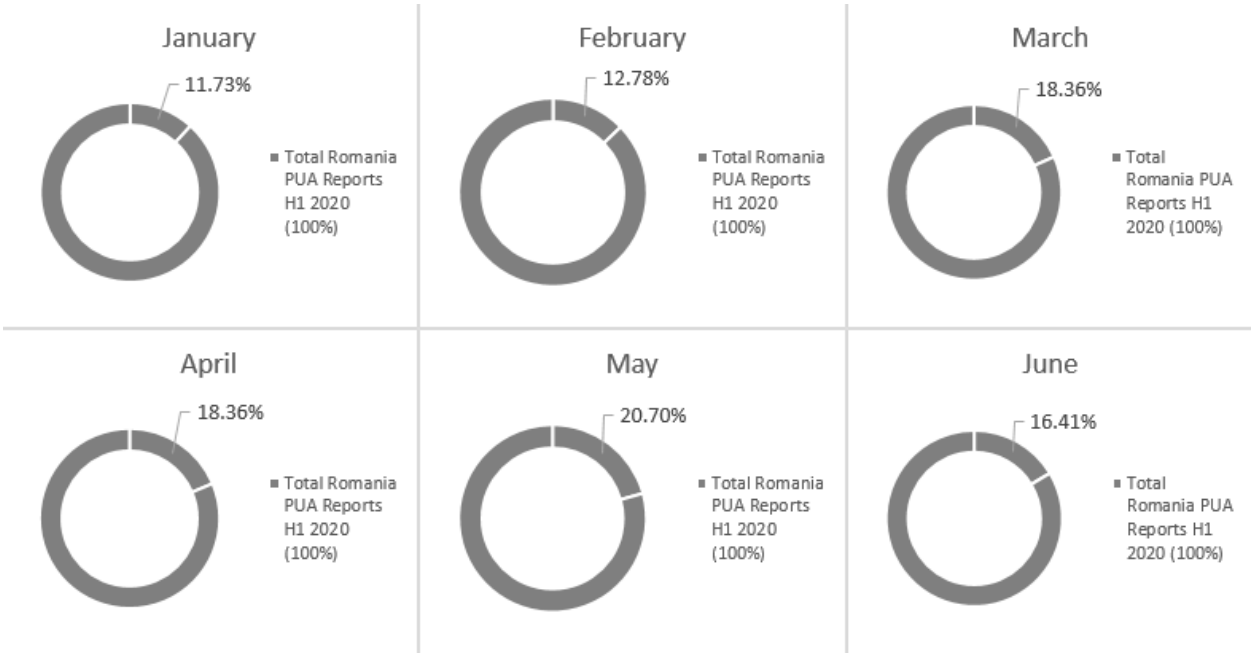


Fig. 27 –Romania PUA Evolution H1 2020

Italy

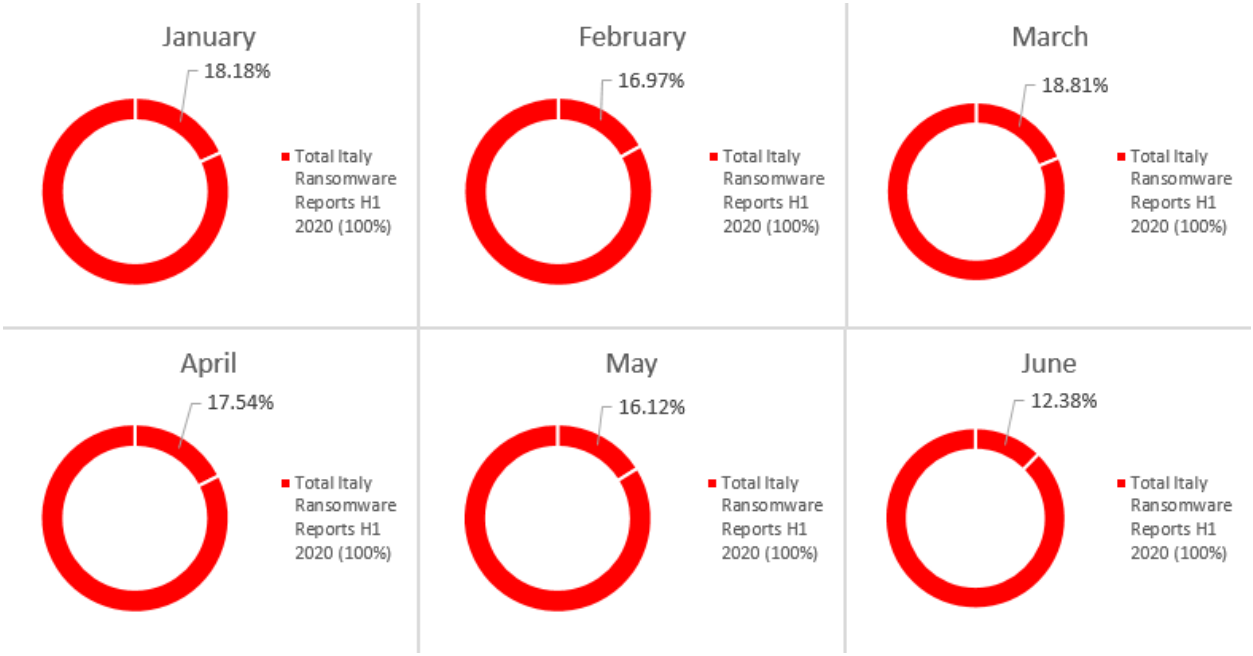


Fig. 28 –Italy Ransomware Evolution H1 2020

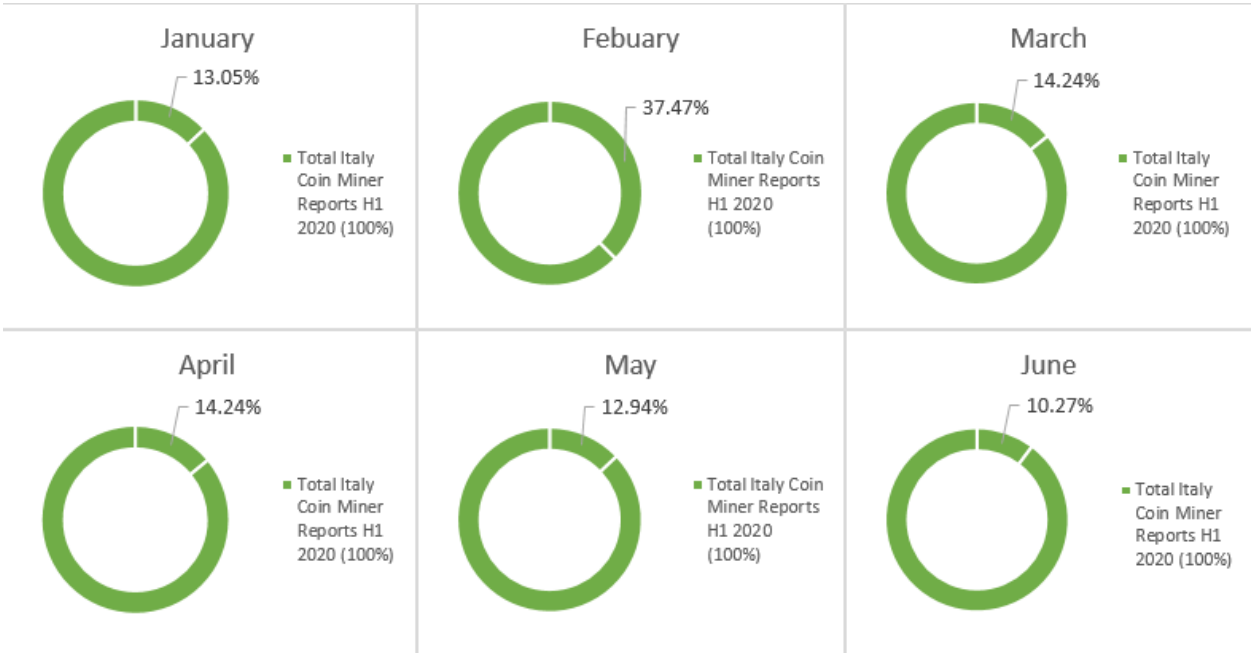


Fig. 29 –Italy Coin Miner Evolution H1 2020

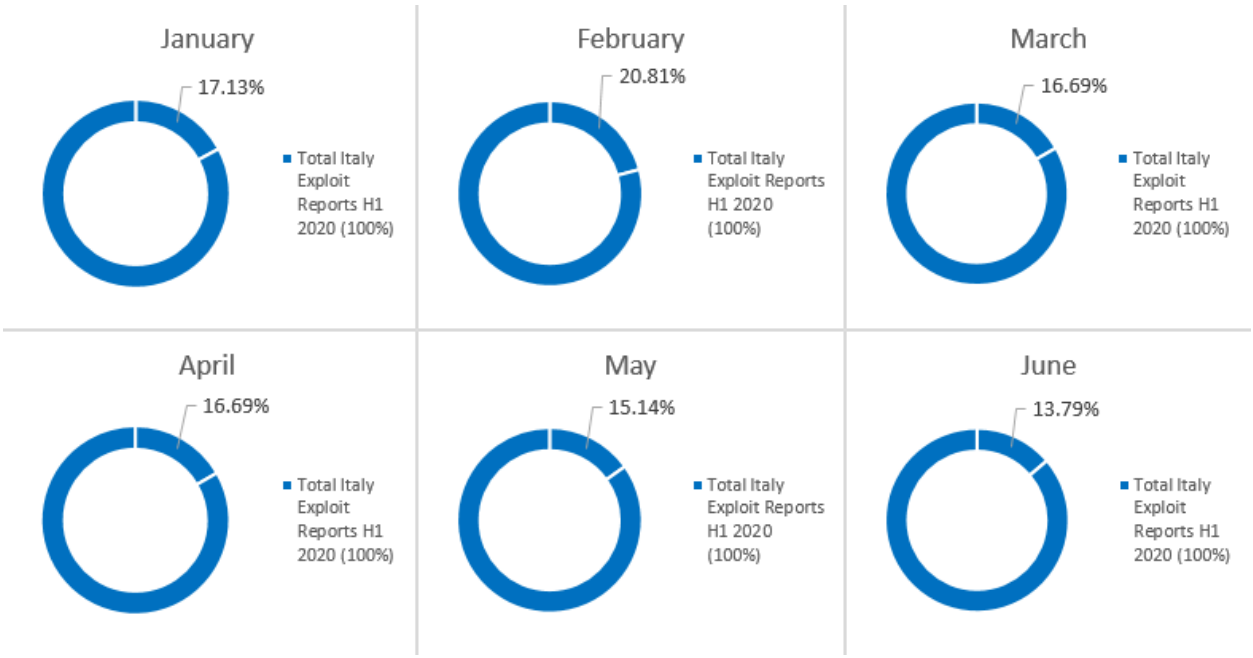


Fig. 30 –Italy Exploit Evolution H1 2020

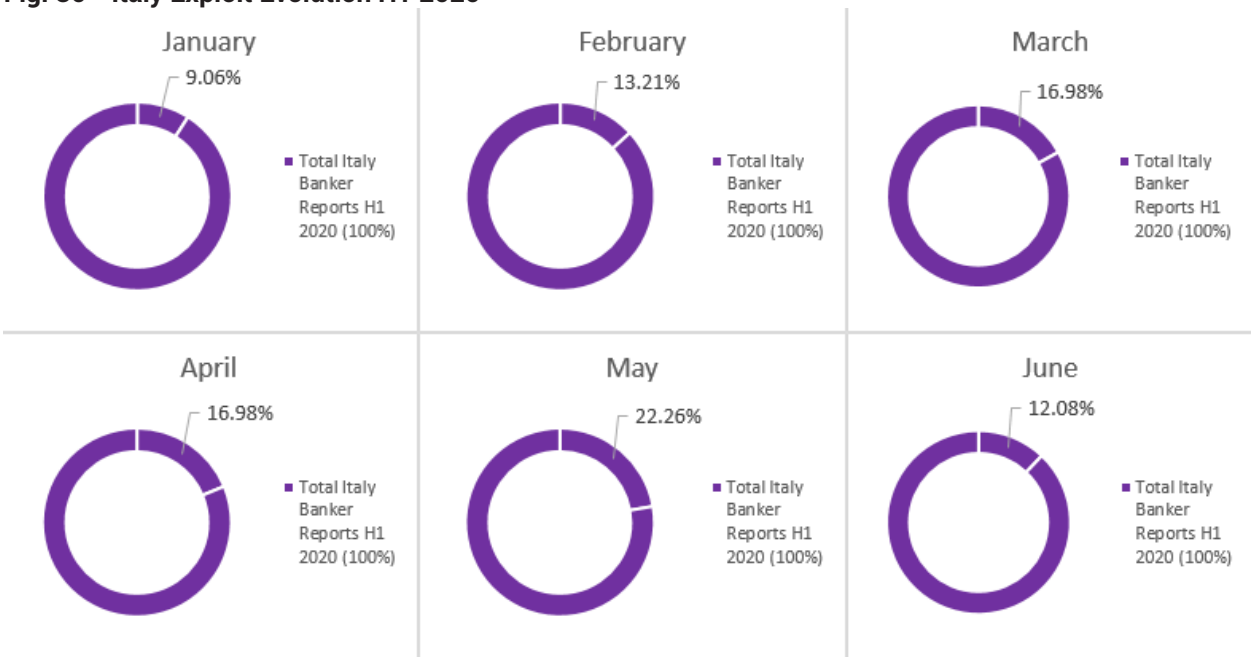


Fig. 31 –Italy Banker Evolution H1 2020

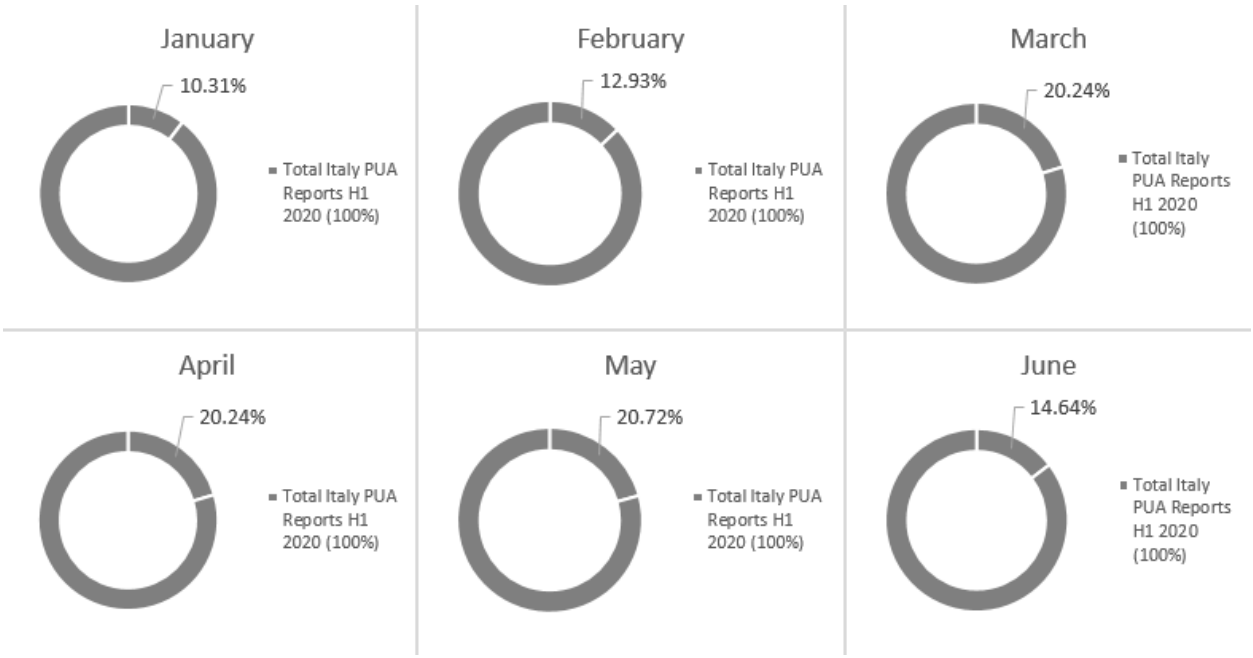


Fig. 32 –Italy PUA Evolution H1 2020

France

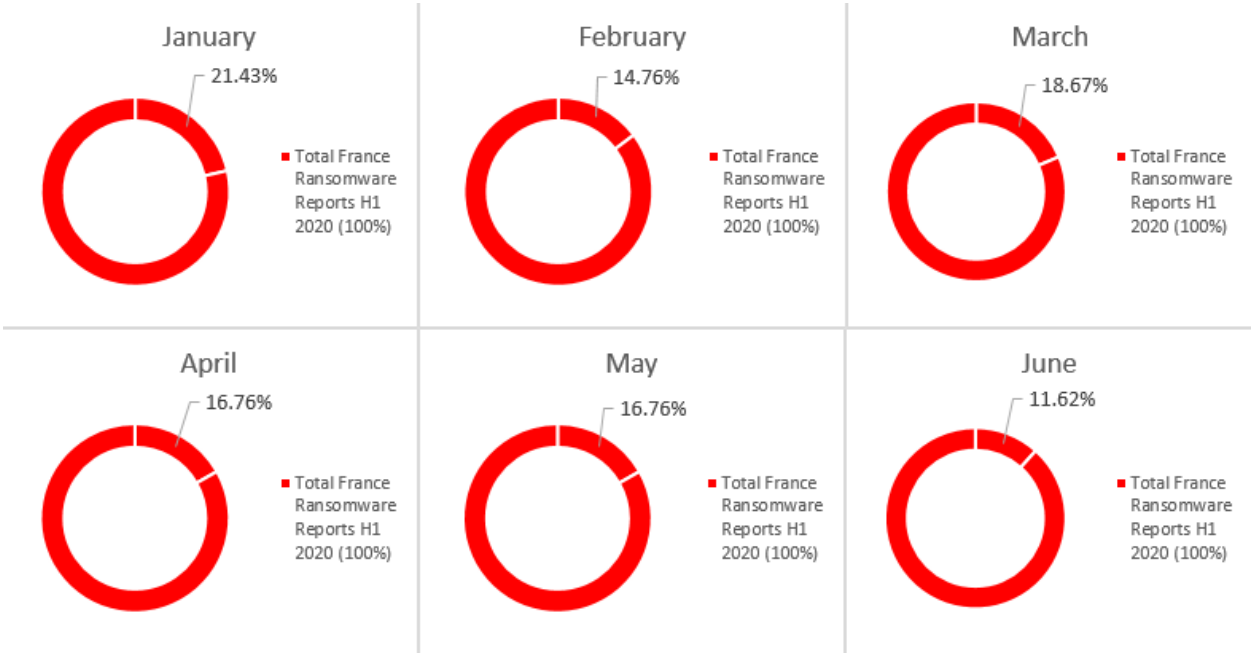


Fig. 33 –France Ransomware Evolution H1 2020

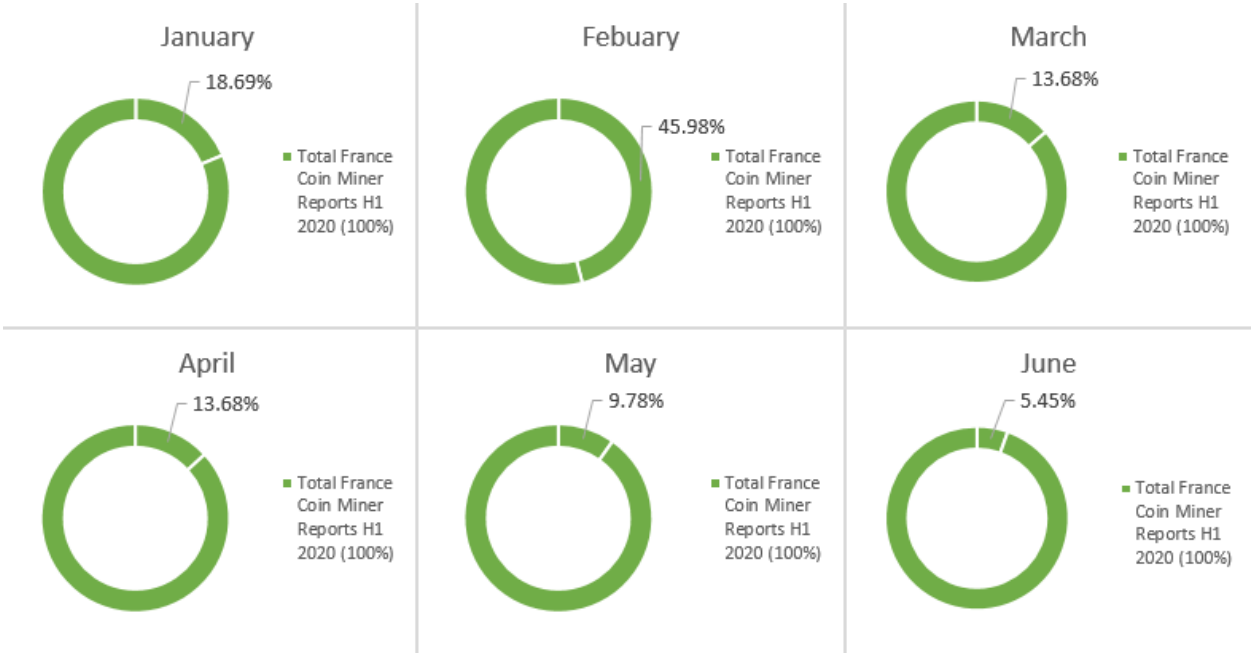


Fig. 34 –France Coin Miner Evolution H1 2020

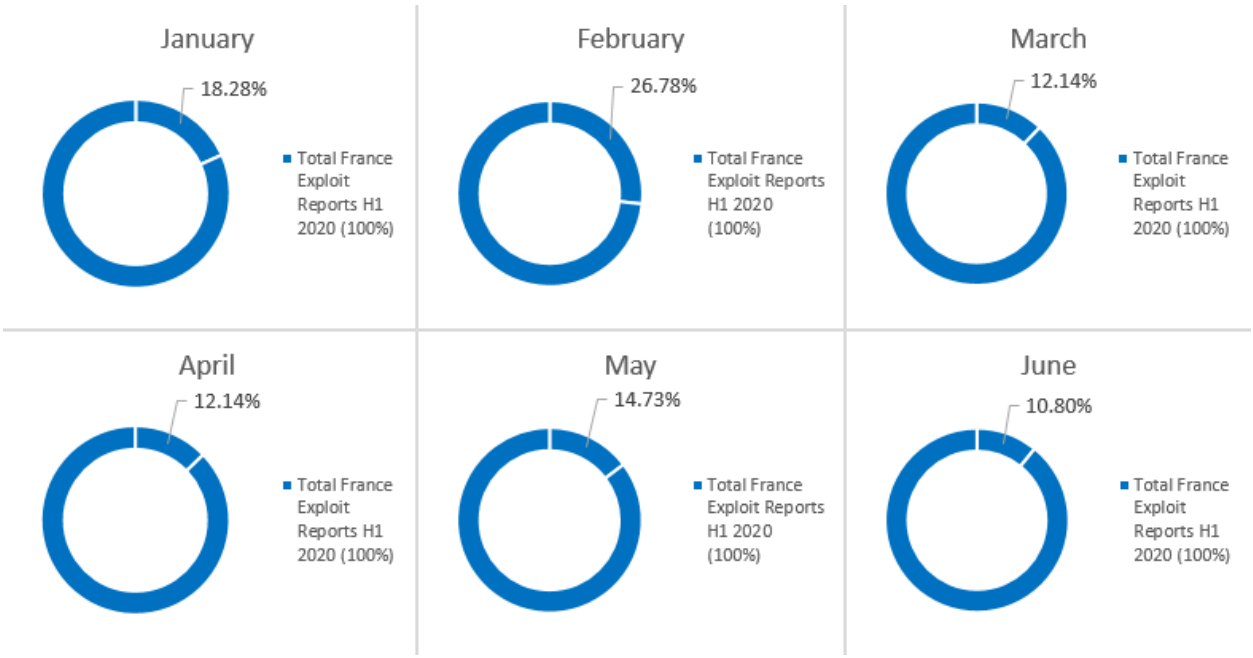


Fig. 35 –France Exploit Evolution H1 2020

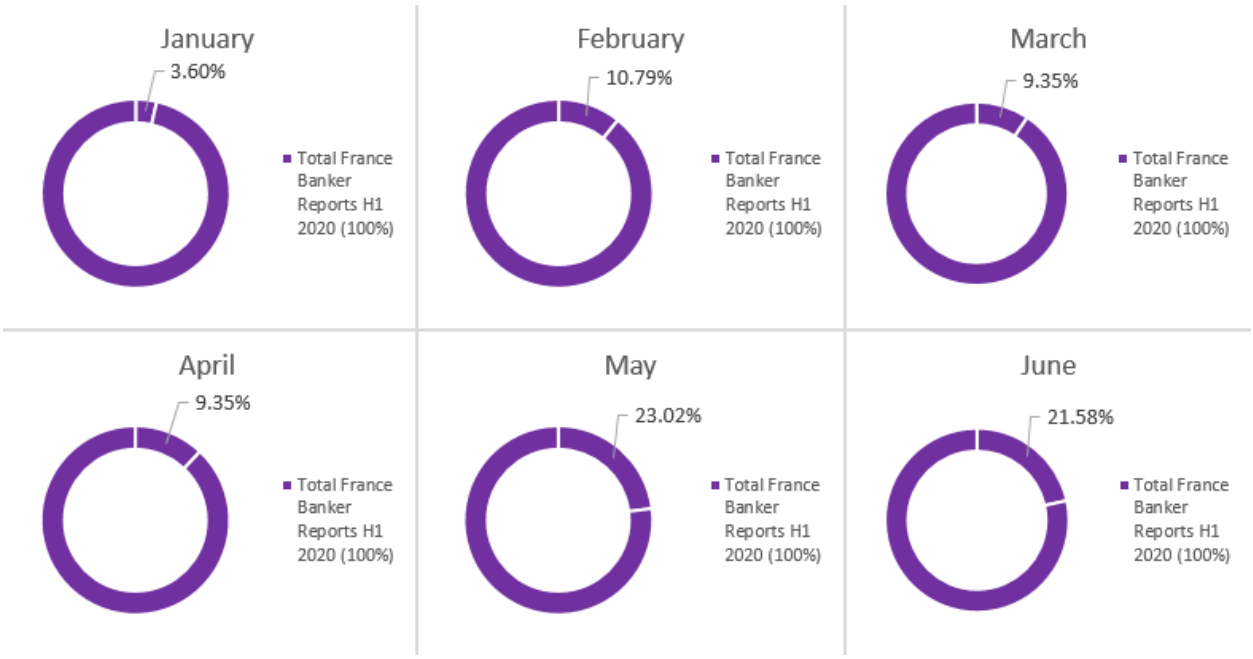


Fig. 36 –France Banker Evolution H1 2020

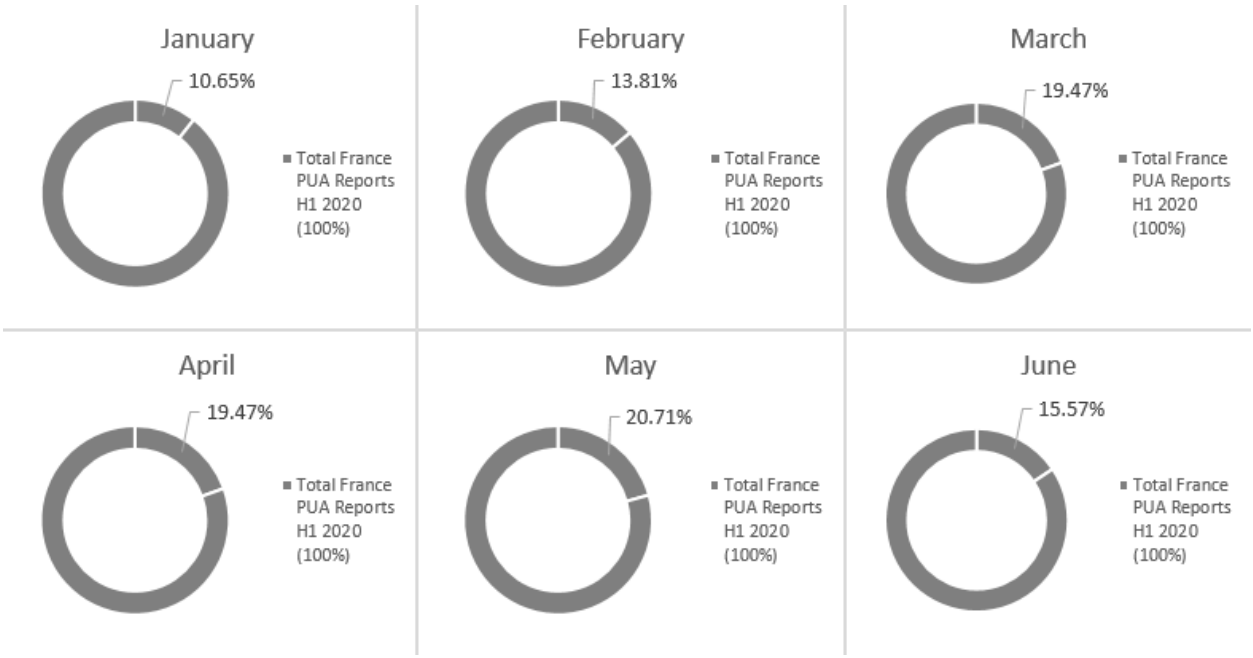


Fig. 37 –France PUA Evolution H1 2020

Spain

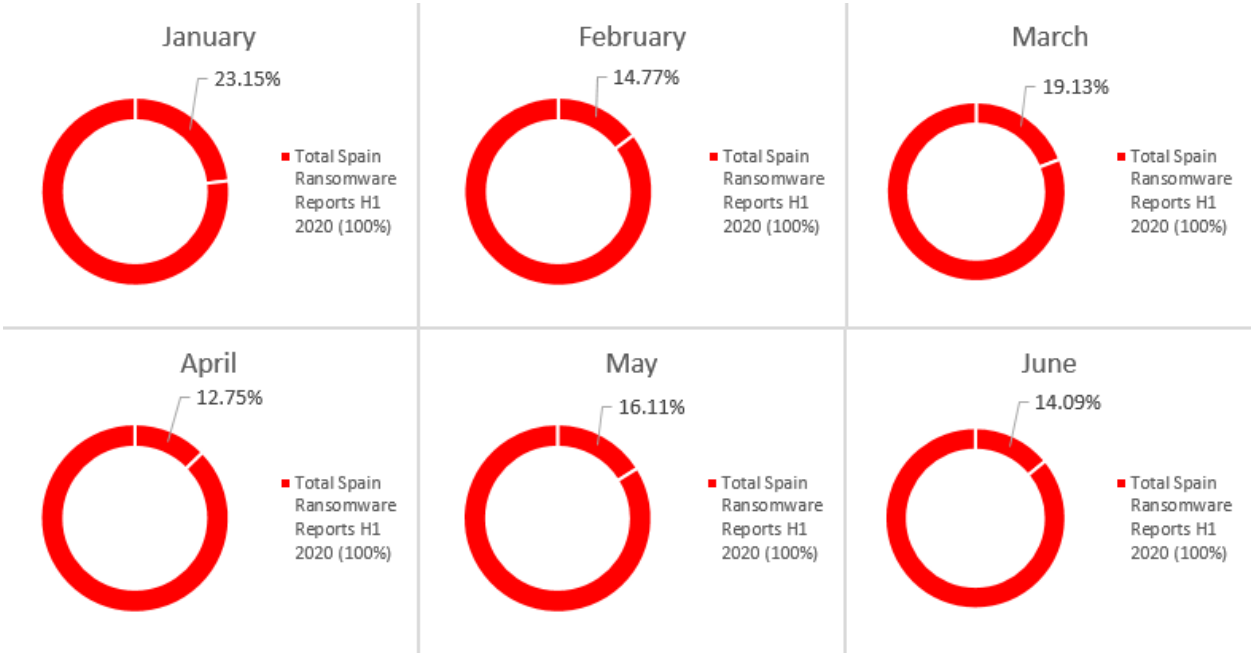


Fig. 38 –Spain Ransomare Evolution H1 2020

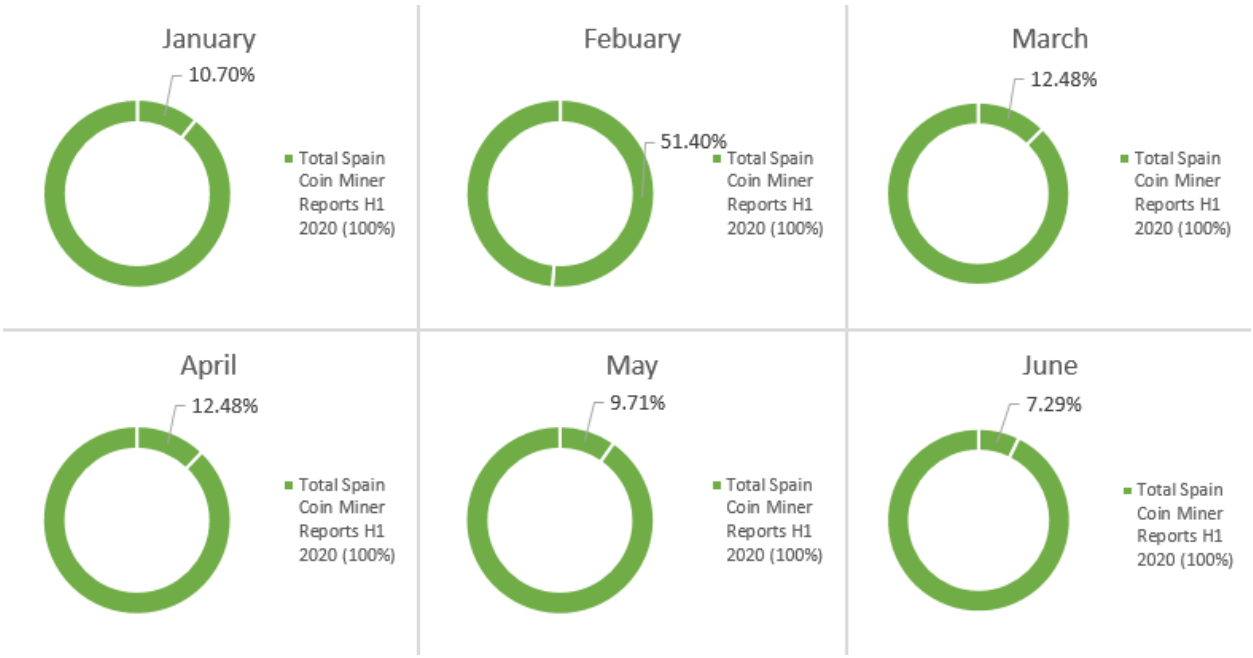


Fig. 39 –Spain Coin Miner Evolution H1 2020

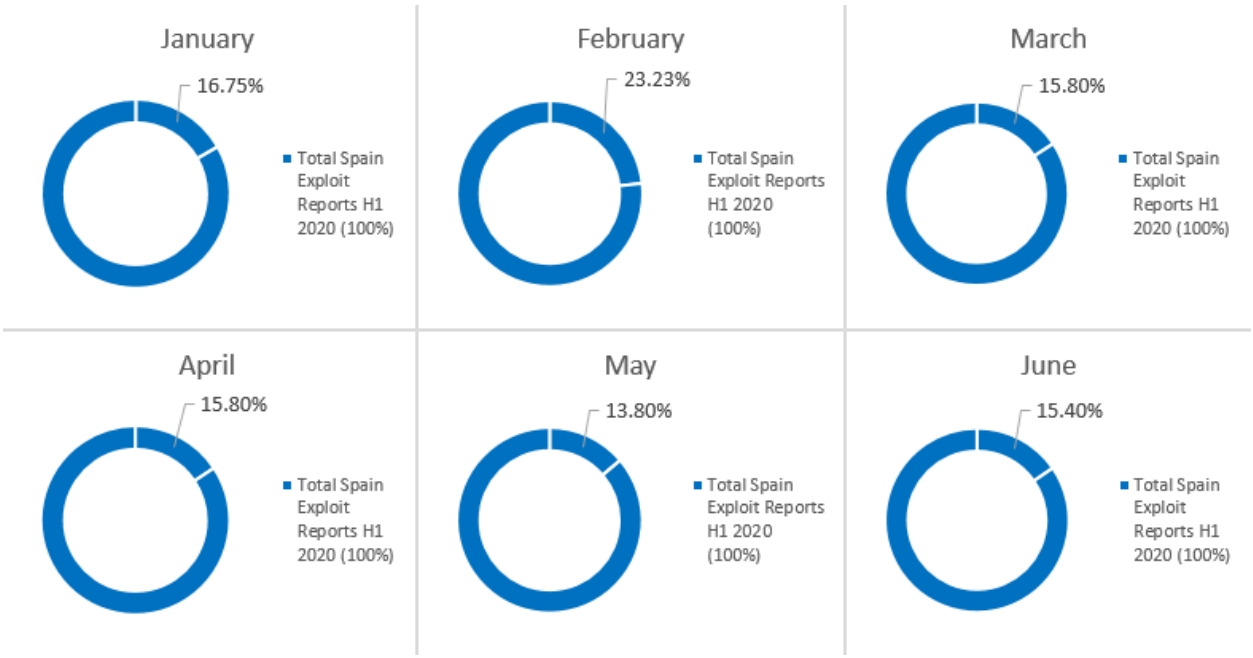


Fig. 40 –Spain Exploit Evolution H1 2020

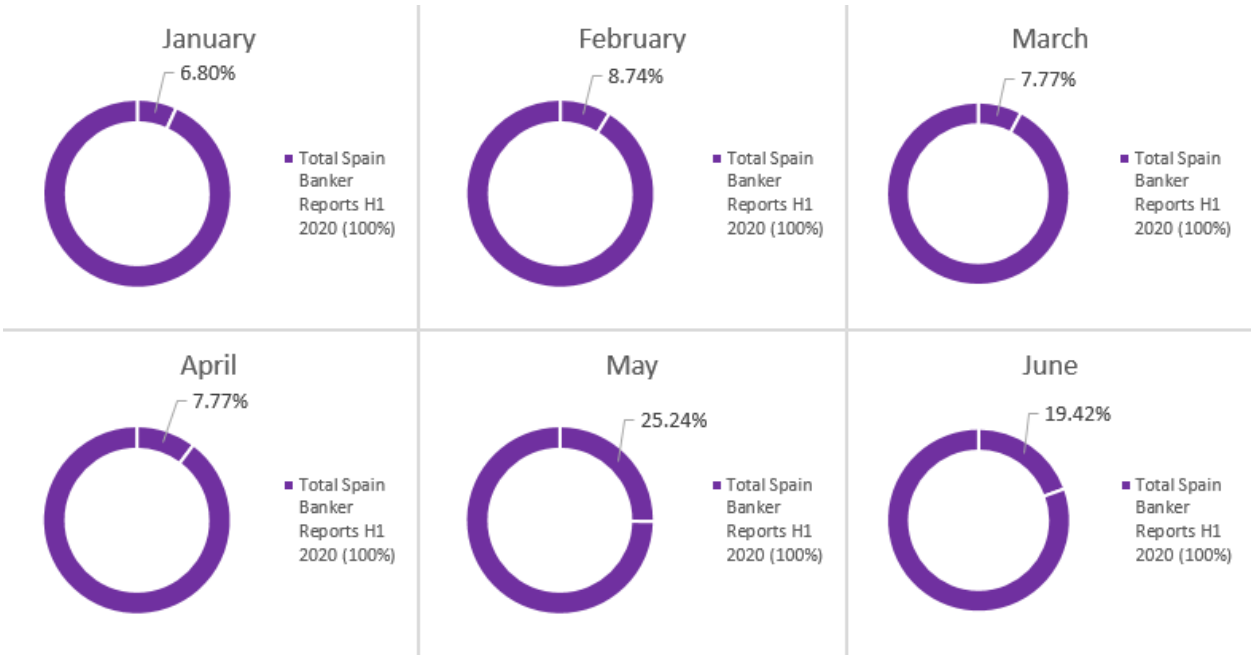


Fig. 41 –Spain Banker Evolution H1 2020

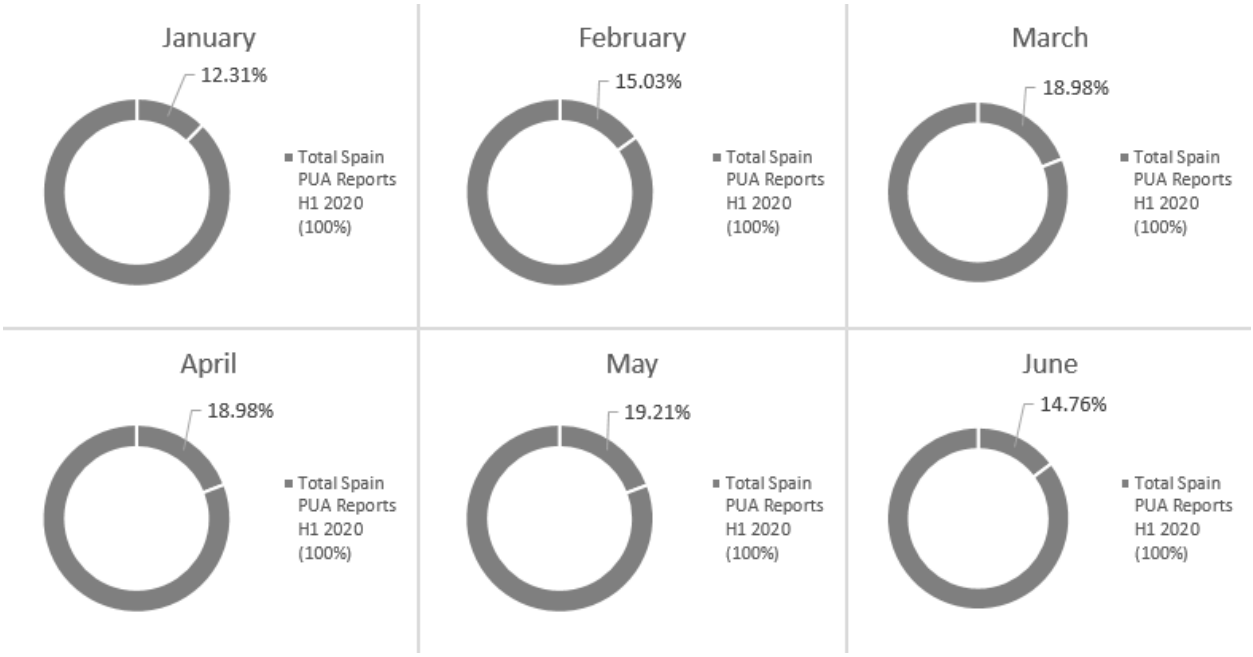


Fig. 42 –Spain PUA Evolution H1 2020

Denmark

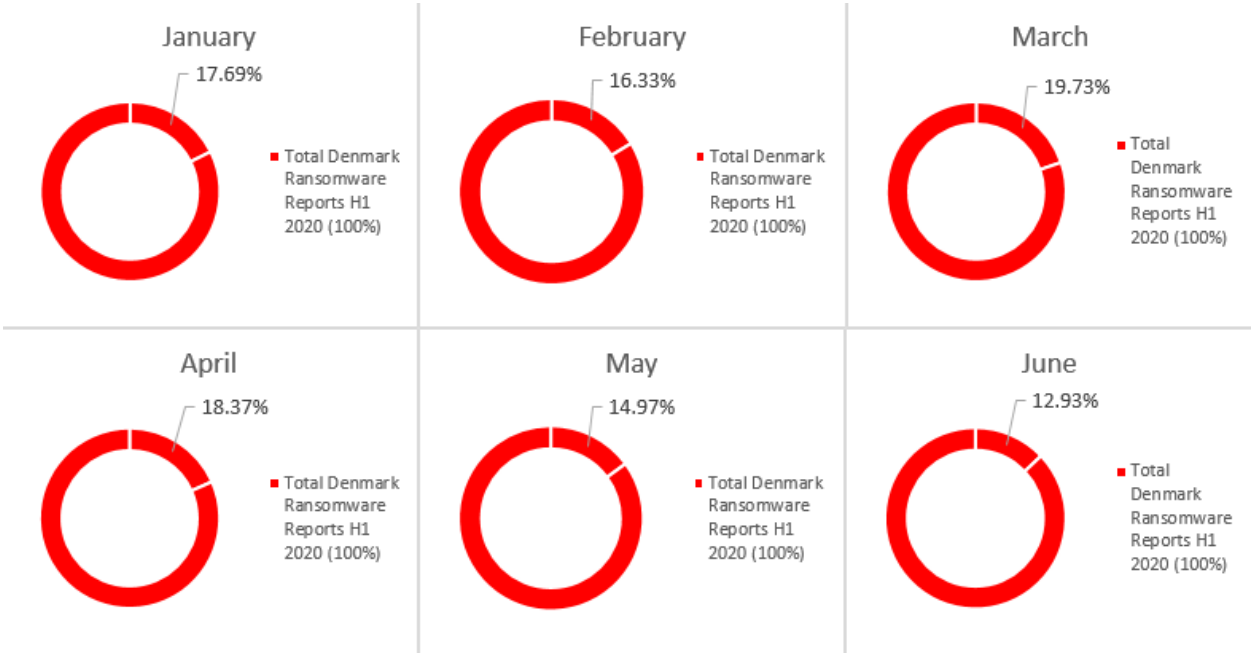


Fig. 43 –Denmark Ransomware Evolution H1 2020

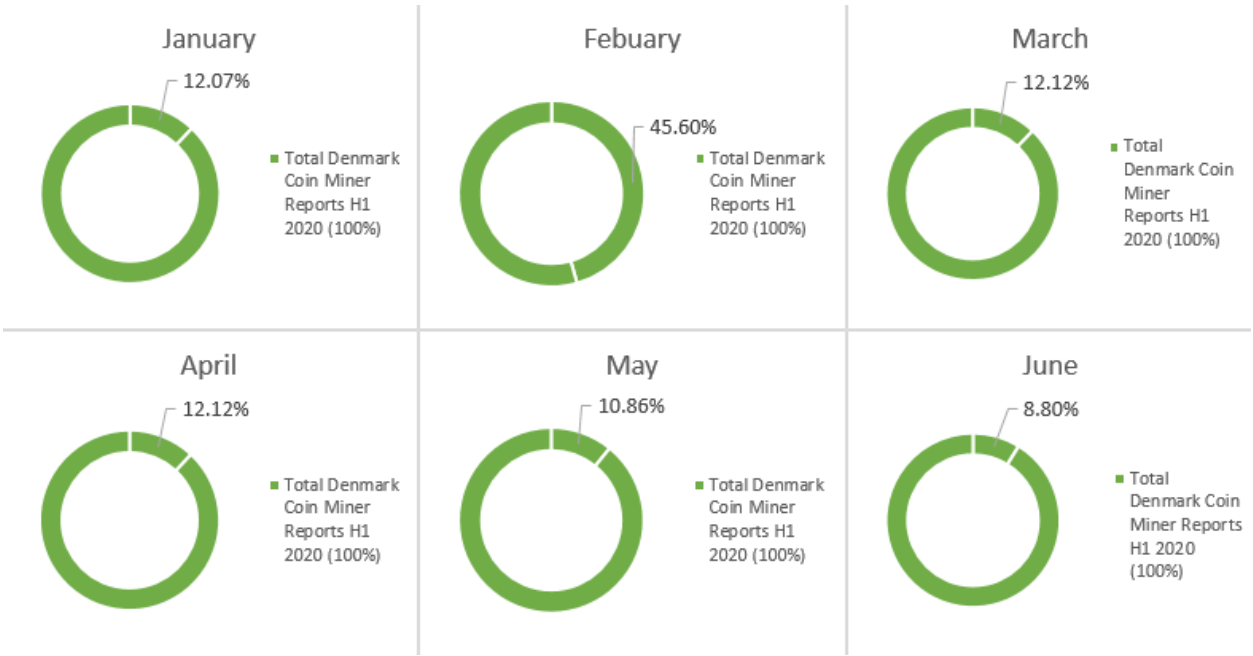


Fig. 44 –Denmark Coin Miner Evolution H1 2020

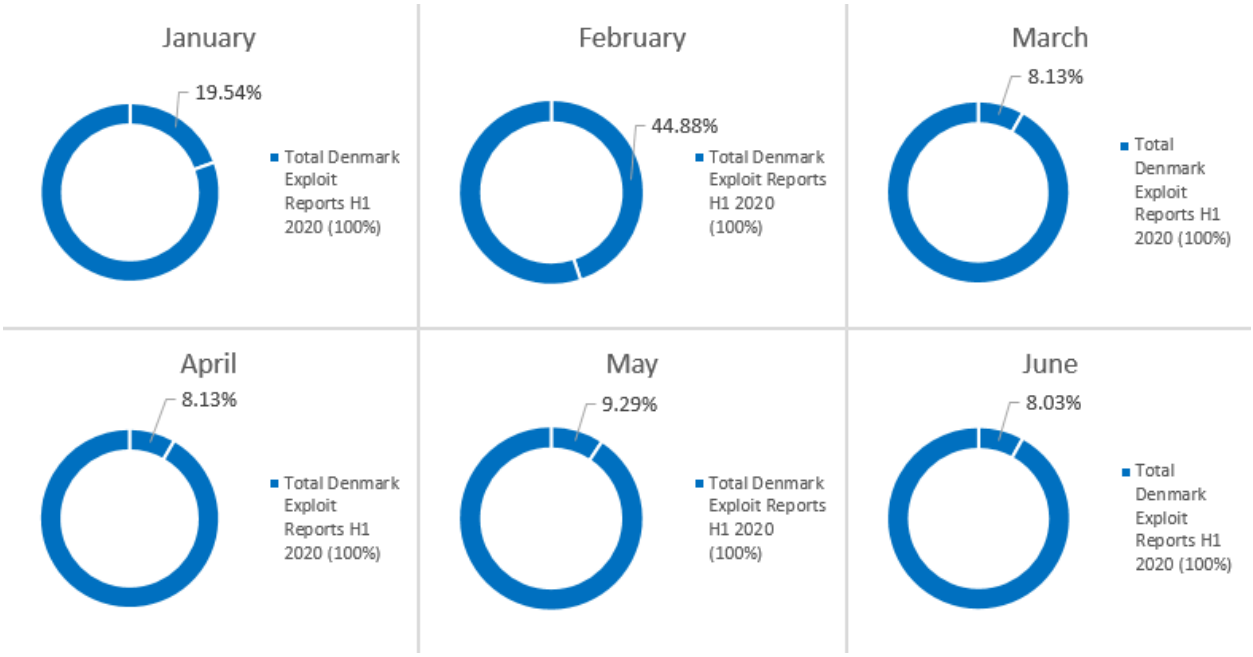


Fig. 45 –Denmark Exploit Evolution H1 2020

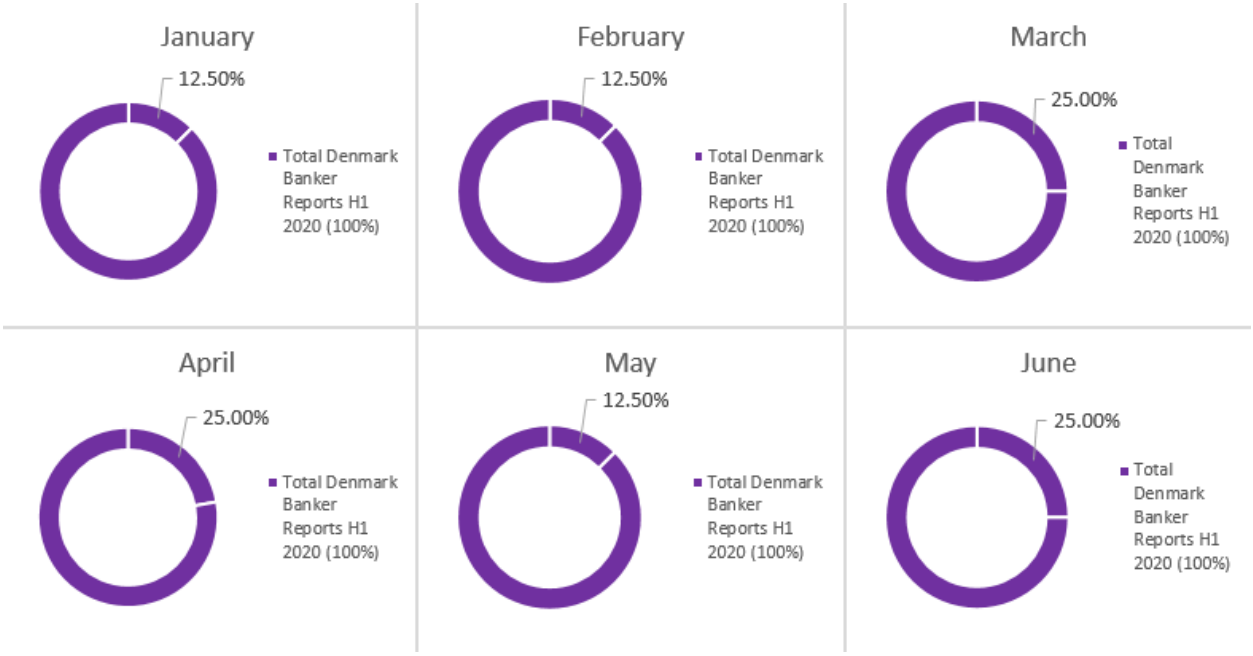


Fig. 46 –Denmark Banker Evolution H1 2020

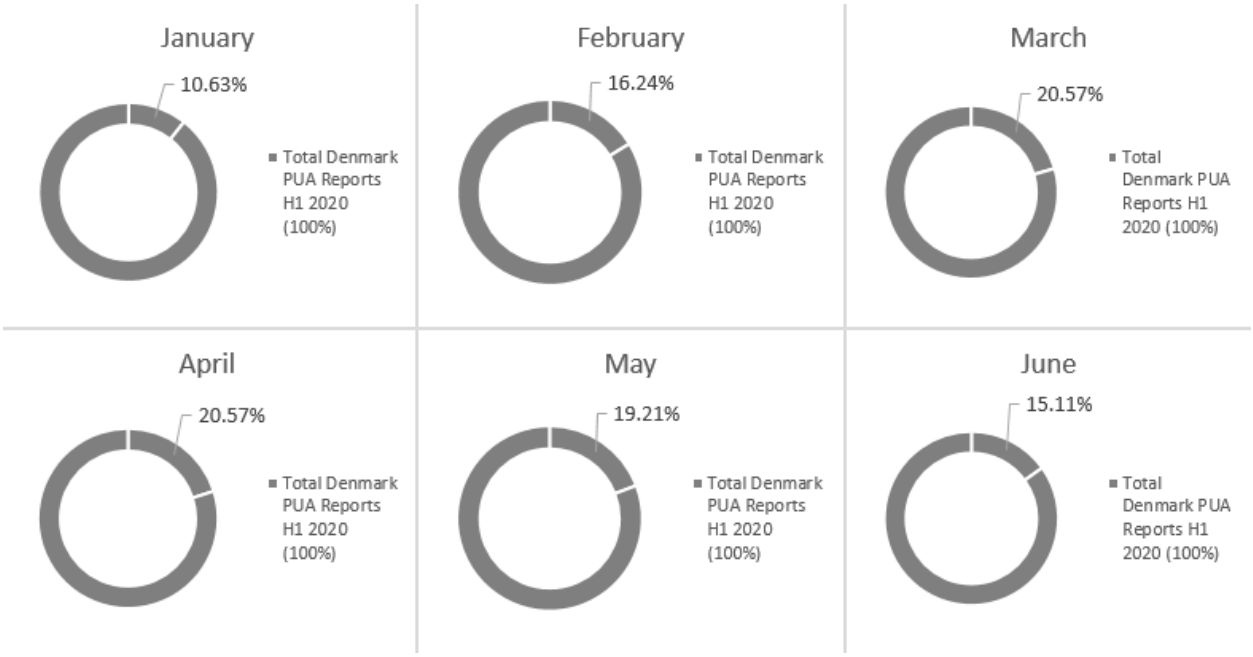


Fig. 47 –Denmark PUA Evolution H1 2020

Germany

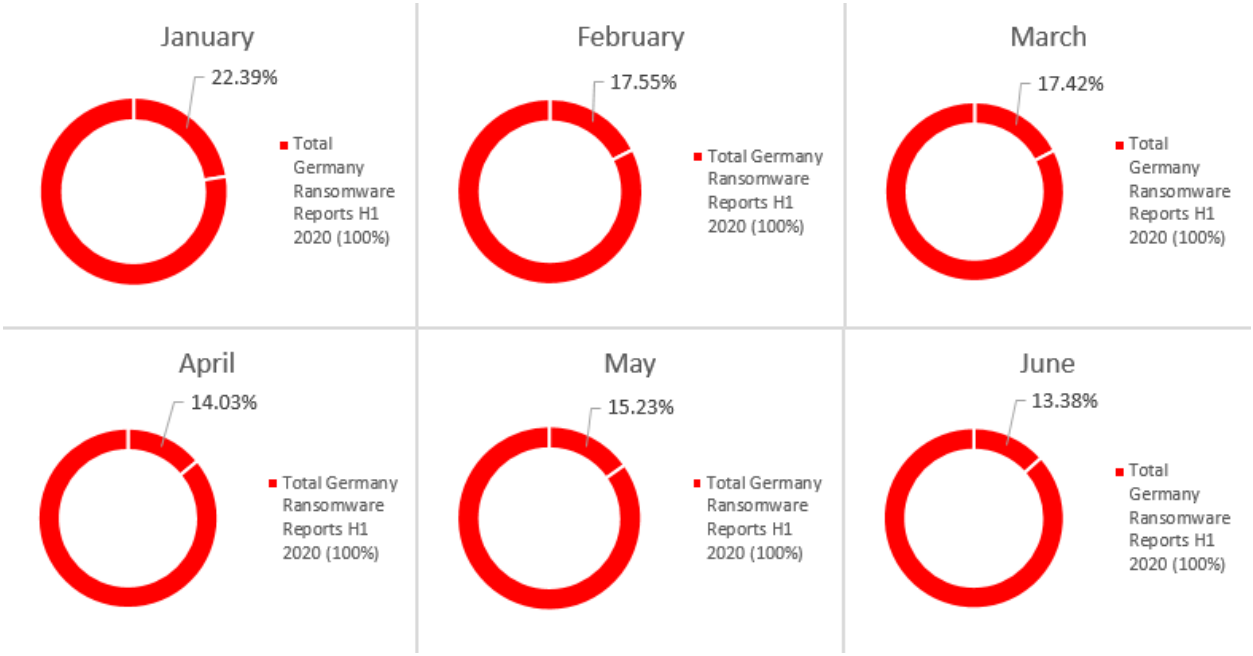


Fig. 48 –Germany Ransomware Evolution H1 2020

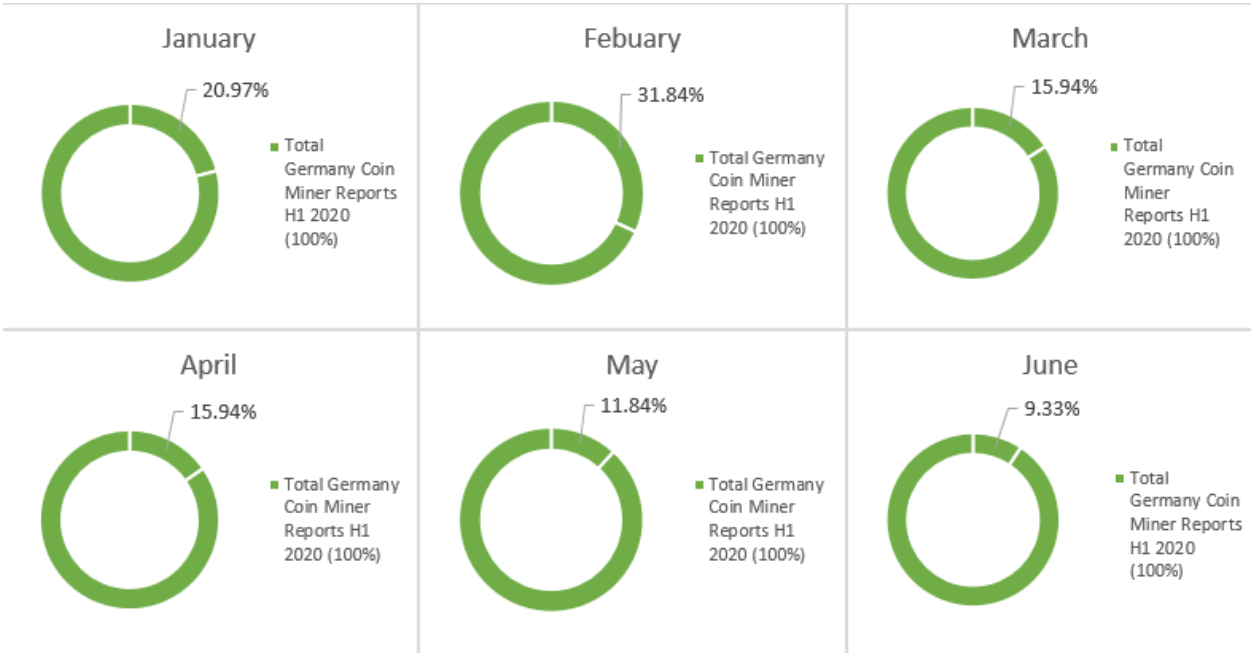


Fig. 49 –Germany Coin Miner Evolution H1 2020

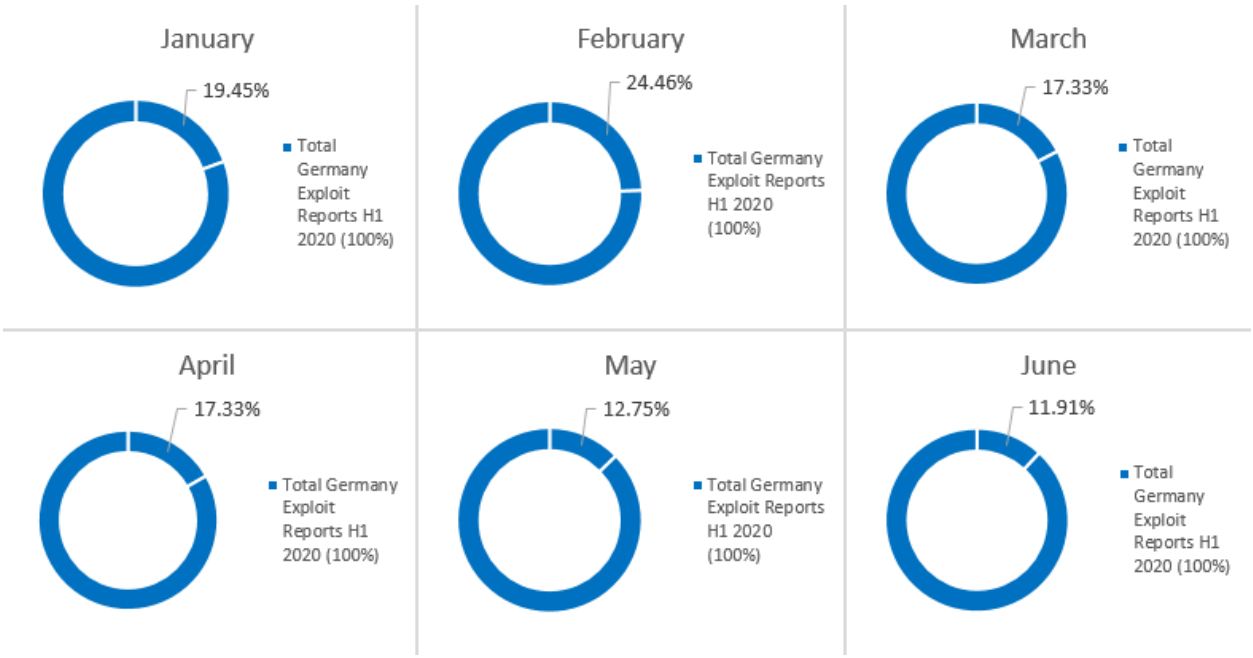


Fig. 50 –Germany Explout Evolution H1 2020

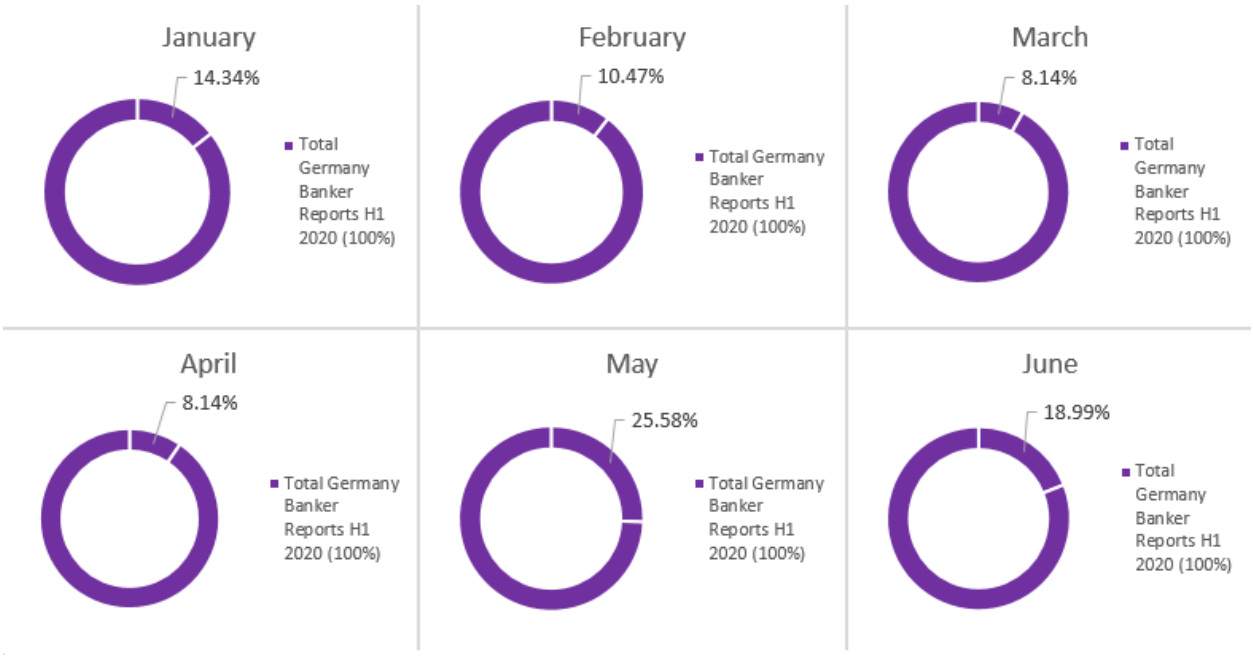


Fig. 51 –Germany Banker Evolution H1 2020

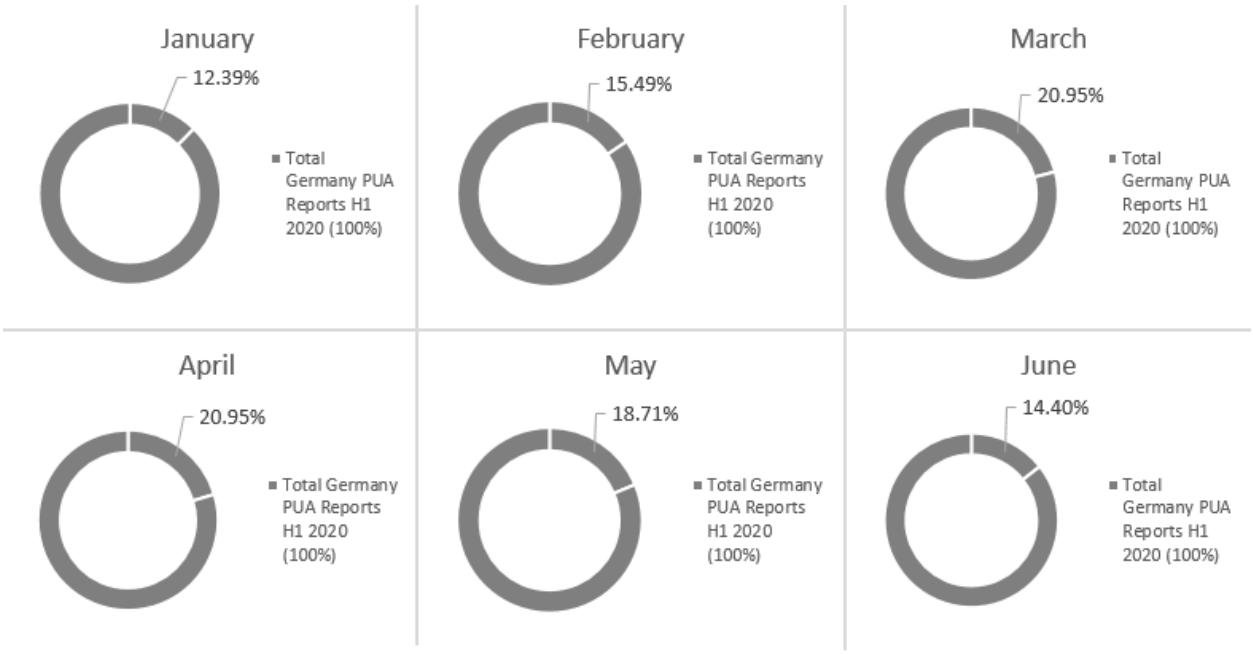


Fig. 52 –Germany PUA Evolution H1 2020

Australia

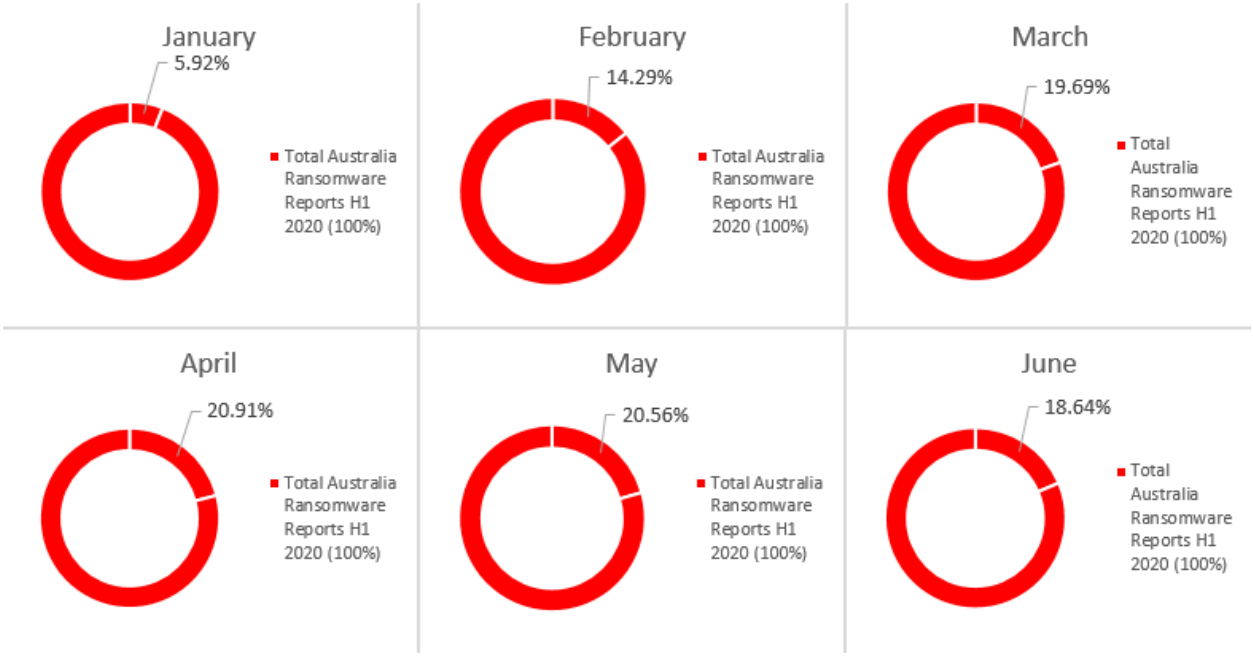


Fig. 53 –Australia Ransomware Evolution H1 2020

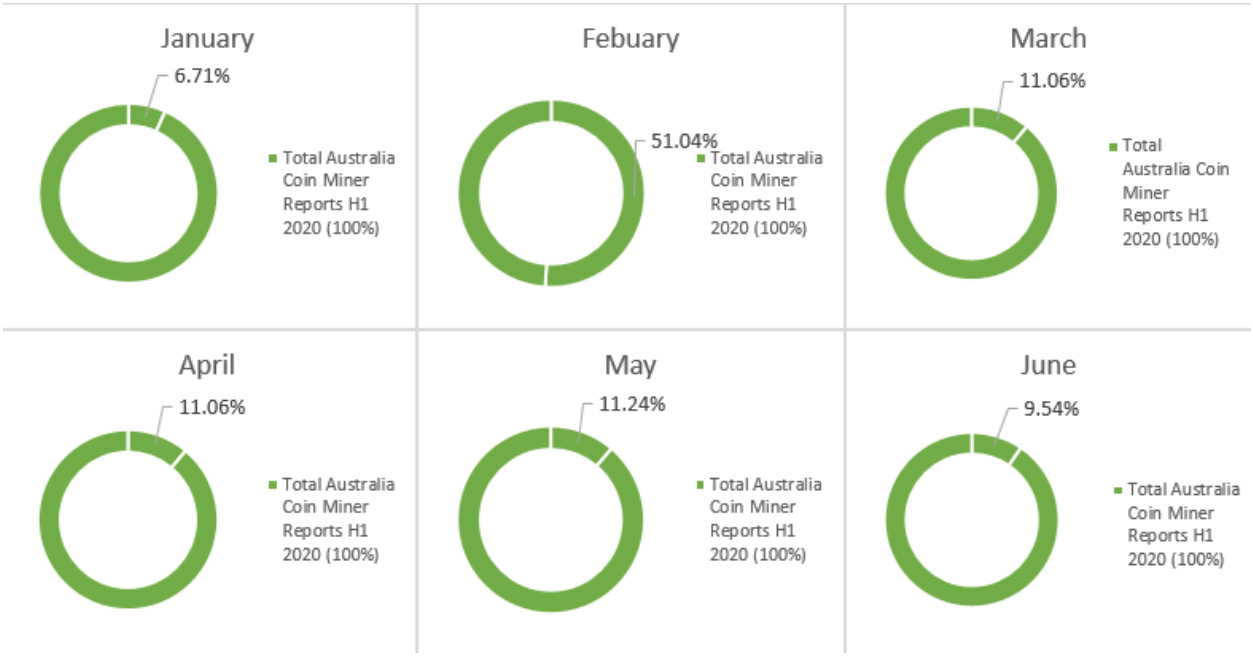


Fig. 54 –Australia Coin Miner Evolution H1 2020

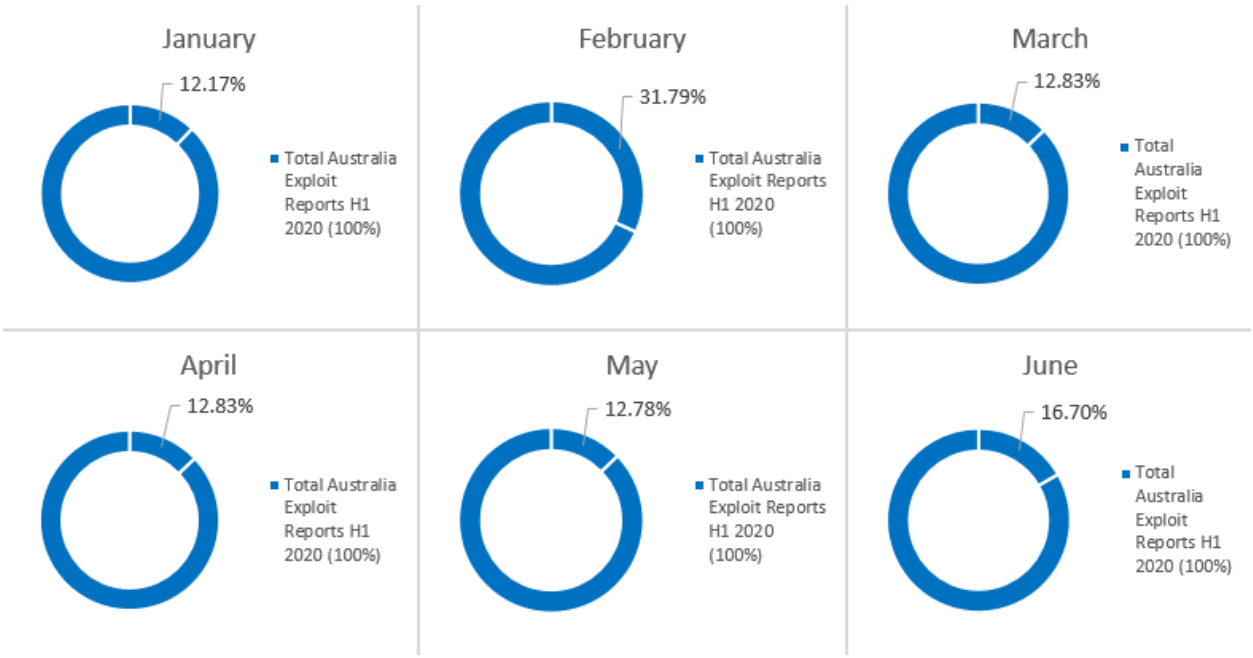


Fig. 55 –Australia Exploit Evolution H1 2020

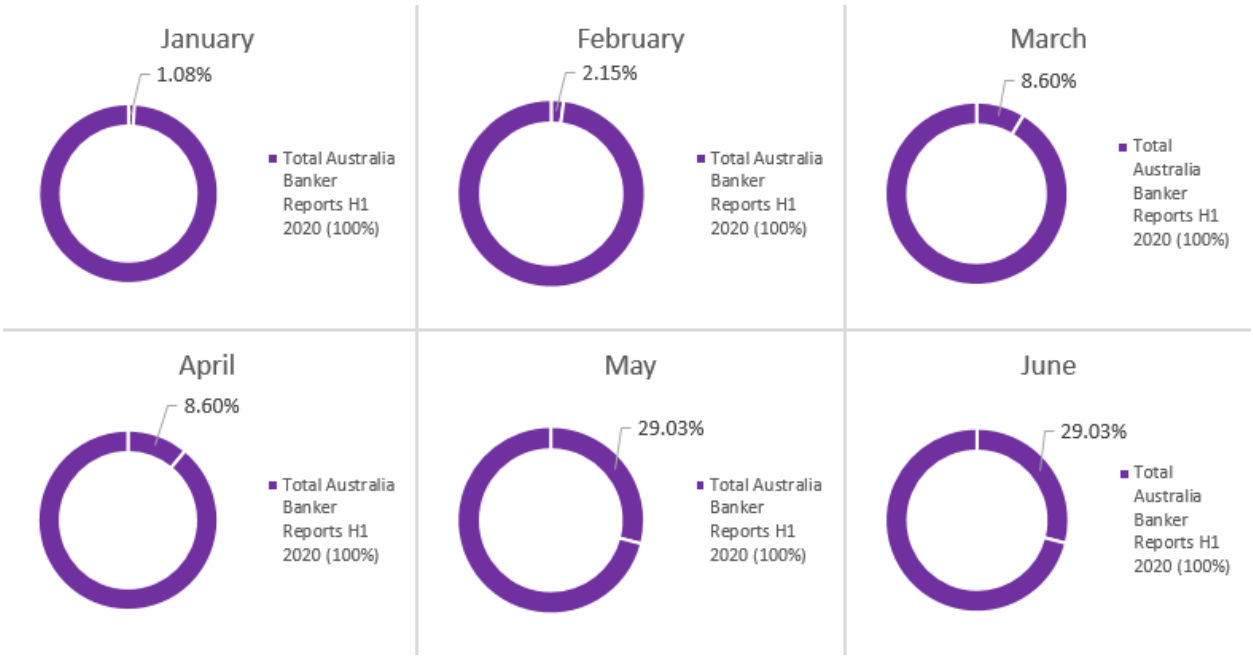


Fig. 56 –Australia Banker Evolution H1 2020

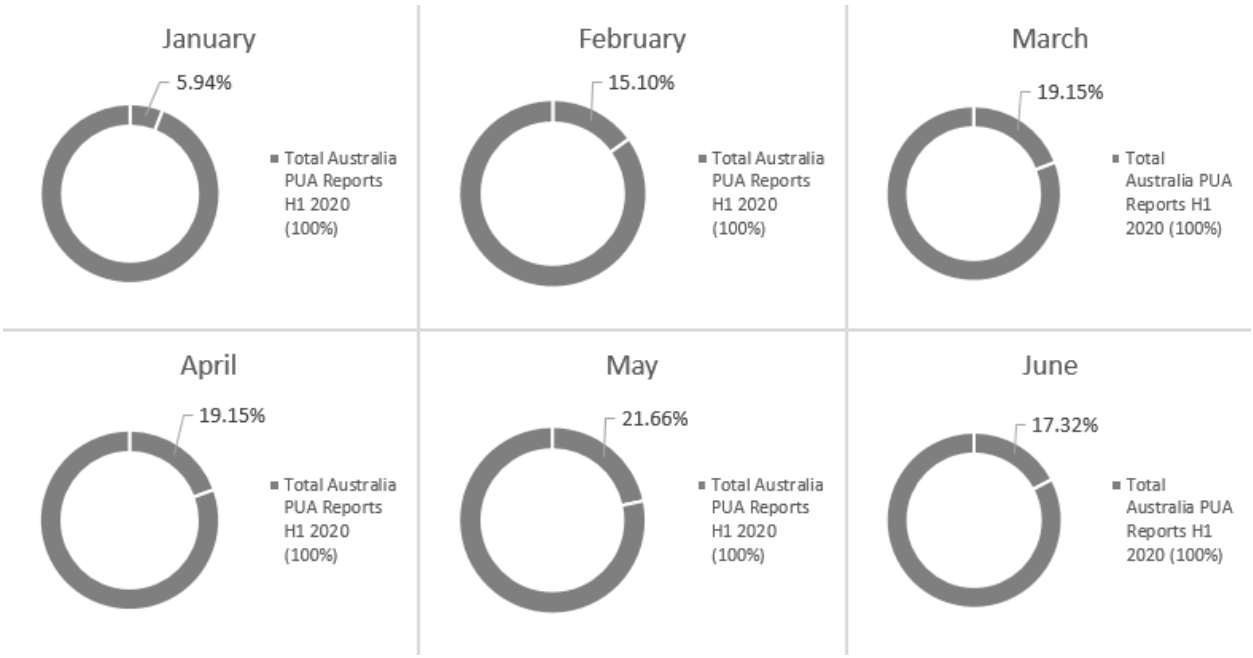


Fig. 57 –Australia PUA Evolution H1 2020

Netherlands

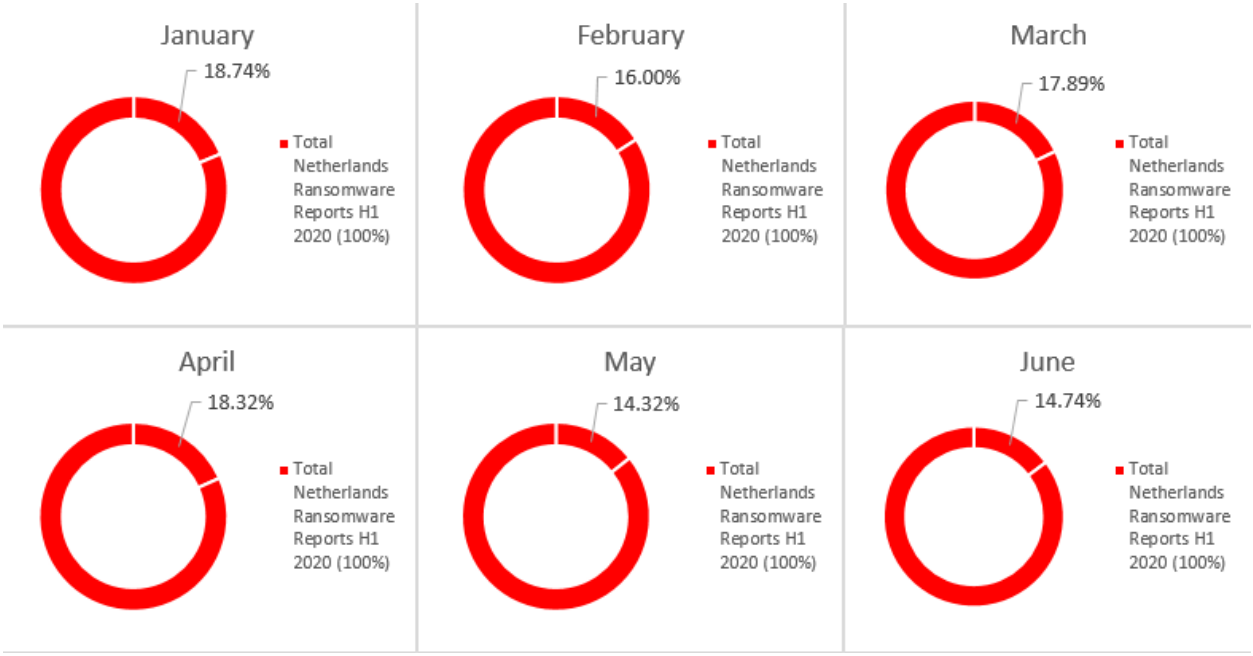


Fig. 58 –Netherlands Ransomware Evolution H1 2020

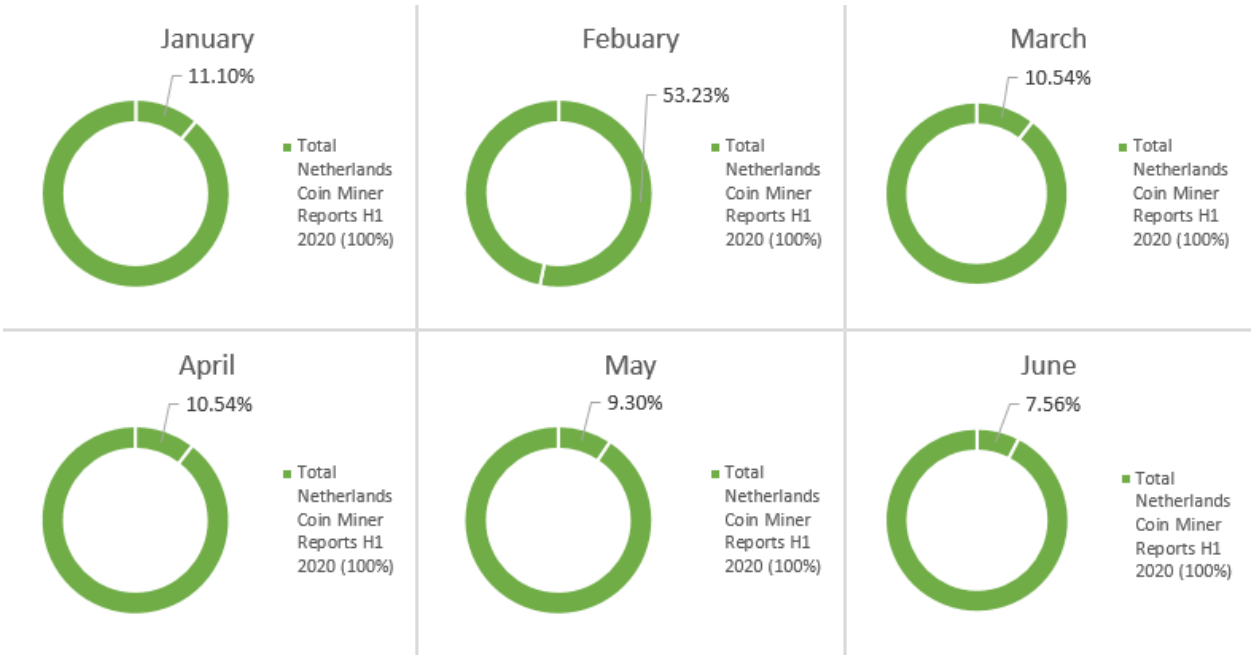


Fig. 59 –Netherlands Coin Miner Evolution H1 2020

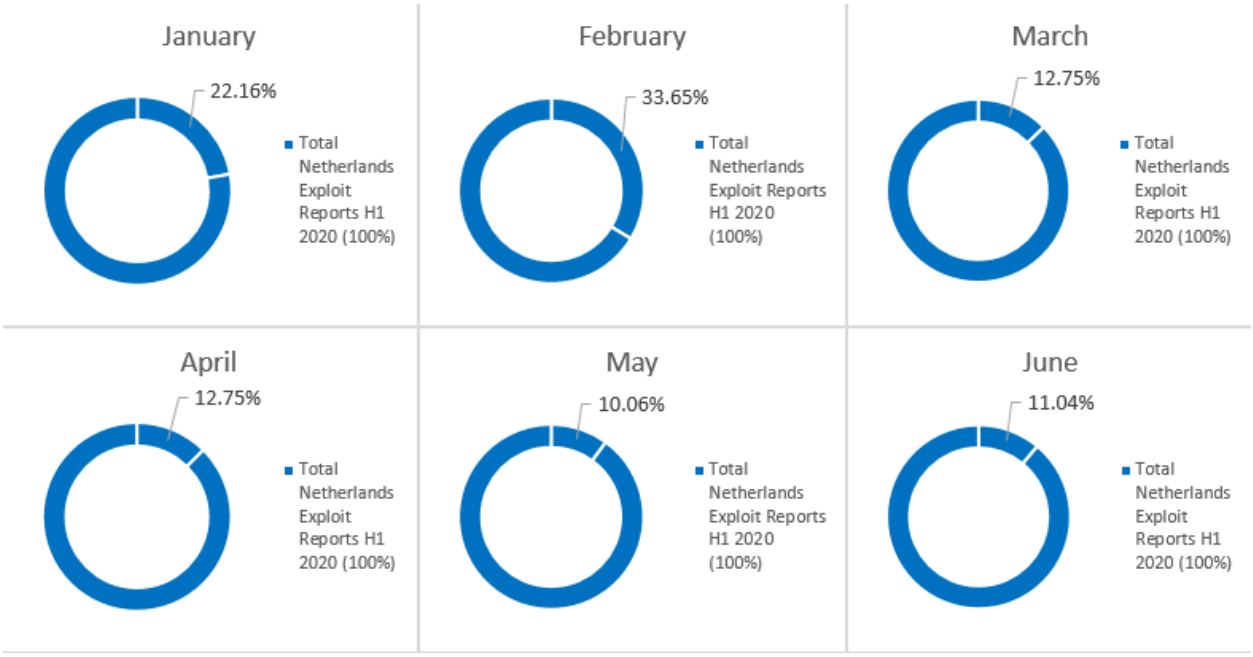


Fig. 60 –Netherlands Exploit Evolution H1 2020

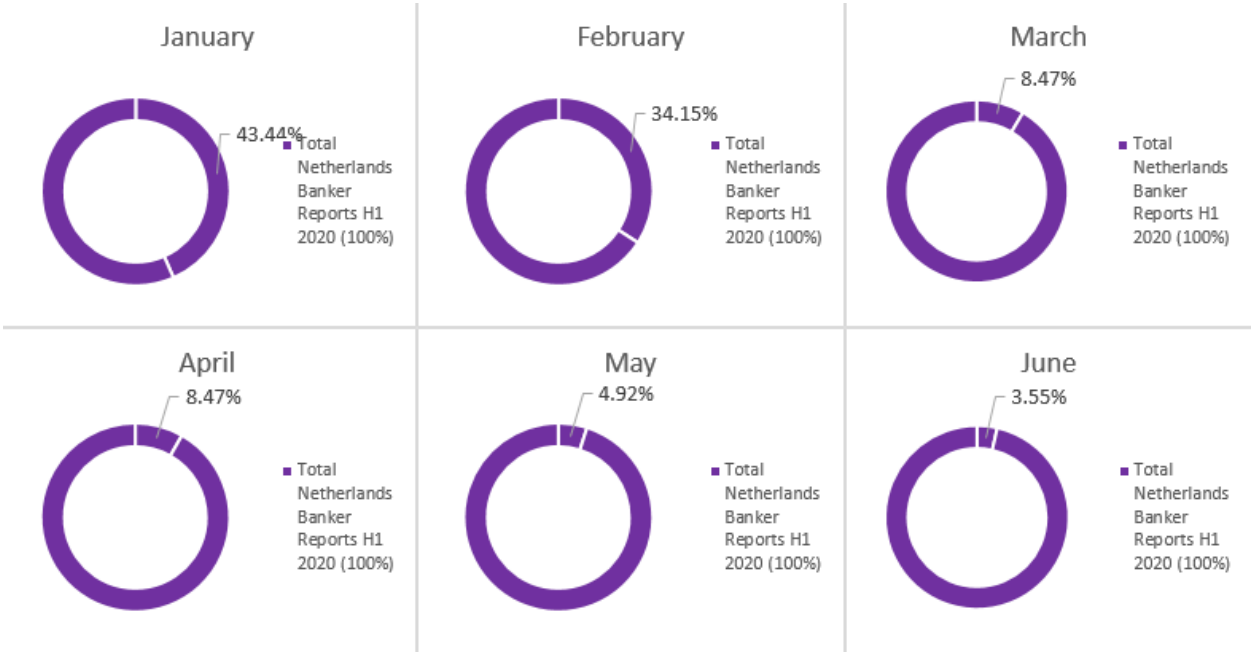


Fig. 61 –Netherlands Banker Evolution H1 2020

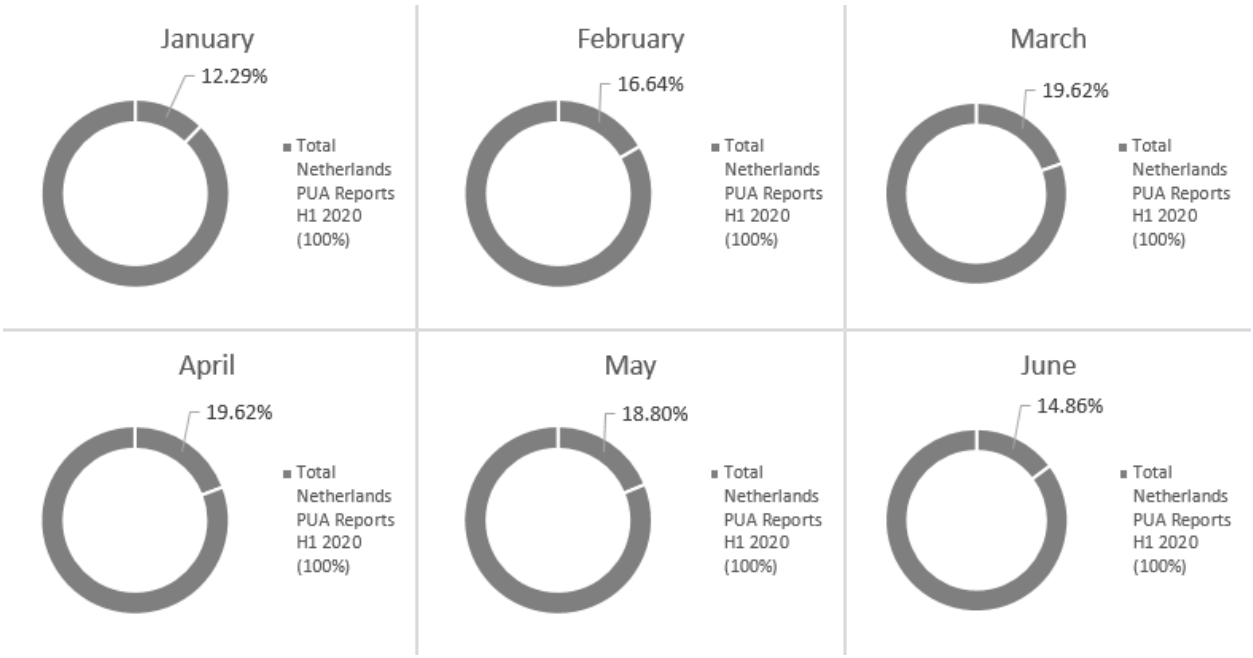


Fig. 61 –Netherlands PUA Evolution H1 2020

MacOS Threat Landscape

In the first half of last year, the most common threats directed at macOS users were coin miners, potentially unwanted applications (PUAs) and exploits. The threat landscape remains virtually unchanged for Mac users in 2020 from the first half of 2019.

From coin miners to PUA and exploits, macOS users seem to have been targeted by the same threats as in the first half of 2019. However, when comparing their monthly YOY evolution, it seems that during the first half of 2020 they evolved quite differently.

Coin miners have evolved completely differently than a year earlier, with the number of reports increasing during March, April, and May 2020. If anything, while previously the number of reports were higher as the year started, it seems that during 2020 coin miner reports started slow, only to spike in February (24.02 percent) and March (31.55 percent) 2020.

Coin miners continue to have a presence on Apple computers in 2020. Stealing computing power to make a slow but sure buck doesn't seem like the most attractive business model, but the untraceable nature of cryptocurrency provides a safe haven for some lucrative actors.

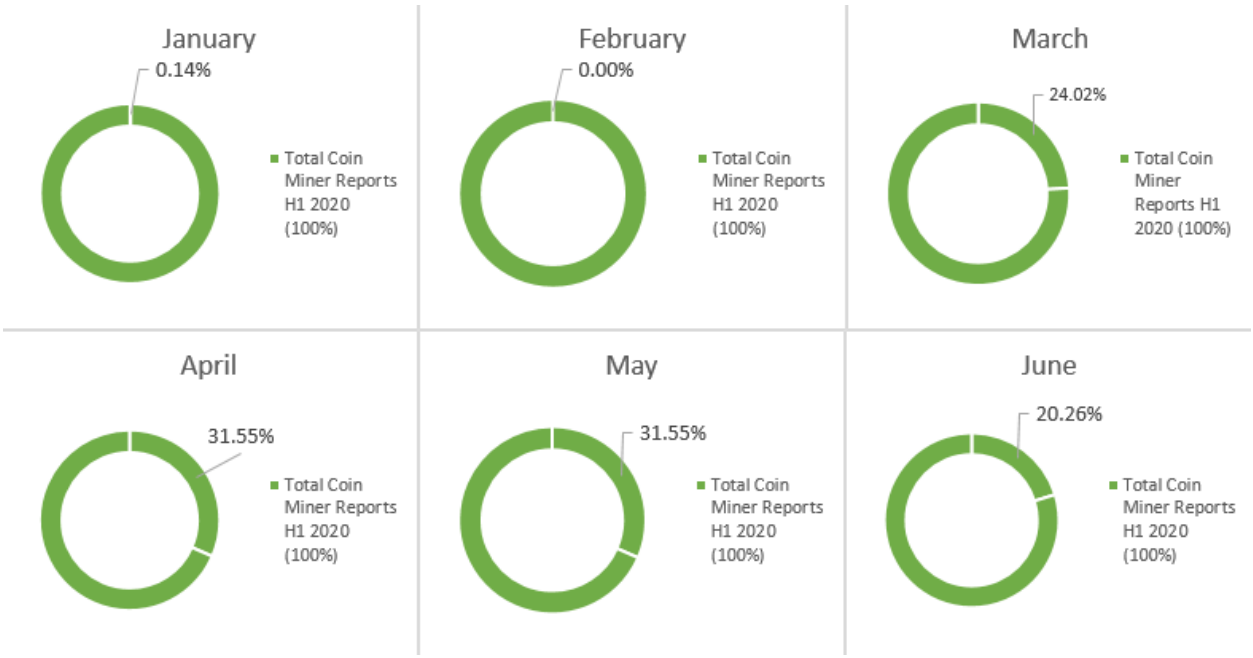


Fig. 63 - Global Coin Miner evolution on macOS H1 2020

Exploit reports followed the same trend as coin miners during the first half of 2020, starting with a low number of reports during January and February, then peaking in March (23.55 percent) and June (38.73 percent) of all exploits reported during the first six months. In contrast, during 2019, exploit reports started with a peak in January, only to constantly drop throughout the next months.

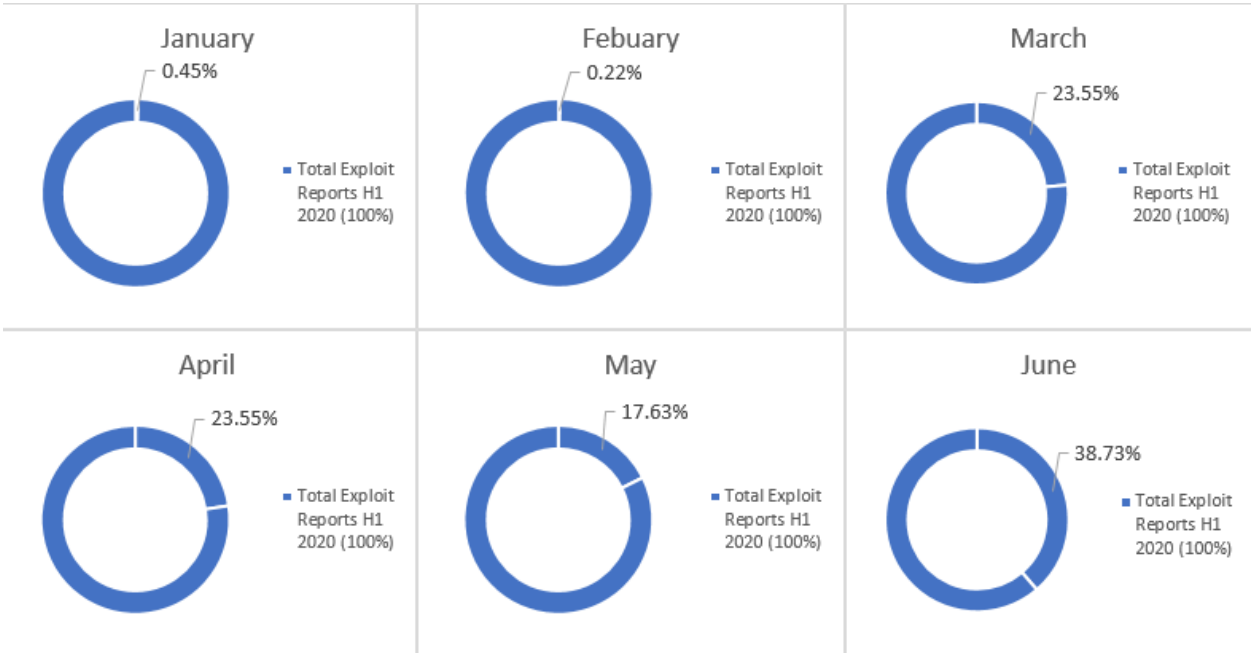


Fig. 64 - Global Exploit evolution on macOS H1 2020

Potentially Unwanted Applications (PUA) on macOS are also a pain, as some applications tend to bundle other unrelated software that sometimes makes for an unpleasant user experience when interacting with your operating system and applications. Following the YoY trends set by the previous threat charts, PUA reports also peaked in March (24.04 percent) and April 2020 (31.55 percent), after last year registering the highest peak in January (28.55 percent).

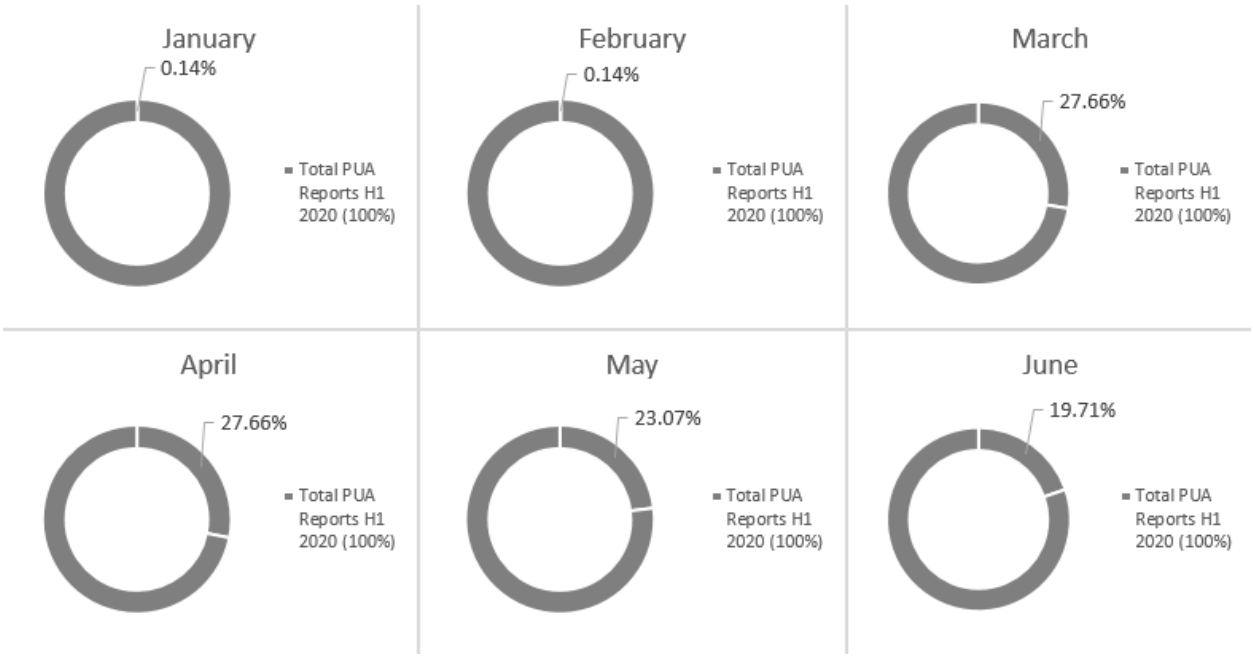


Fig. 65 - Global PUA evolution on macOS H1 2019 vs H1 2020

Android Threat Landscape

There are around 1.6 billion[18] Android users in the world right now and around 2.5 billion active Android devices, at last count in 2019. It's not really a surprise that malware developers focus almost all of their efforts on compromising that platform. With a market share[19] that surpasses 80%, the number and sophistication of attacks will only increase.

The term malware has a slightly different definition on Android, as attackers are not necessarily looking to steal data or compromise devices, although that is part of their activity. In many situations, the deployed apps are only looking to implement aggressive adware that has only one purpose, to generate funds for bad actors.

You might be inclined to think that nothing bad can happen if you download your Android apps from the Google Play Store, but you would be wrong. Some apps fall through the cracks as app developers find new ways to circumvent security.

In fact, Google routinely removes apps from its store after finding they violate disruptive ads policy and disallowed interstitial policy. In one purge, the company removed[20] more than 600 apps in one swoop and banned them from the monetization platform. Users were served full-screen ads when trying to make a phone call or when using GPS apps while driving.

The main problem with malware stems from third-party stores or from shady websites that provide already-infected files. In some situations, users have no choice but to use other solutions because the official Google Play Store is not available in their region. The malware is usually persistent, and it isn't easy to get rid of.

It's important to mention that these infections usually are part of larger campaigns, with bad actors controlling their applications from command and control centers (C&C). While most C&C operations are shut down as soon as they are discovered, some are sheltered enough to remain operational.

What makes Android malware even more dangerous than its counterparts on other operating systems is the range of data that attackers can access. A compromised phone means access to the gallery, contacts, GPS location, banking apps, and much more.

If, in 2019 we had the Triout[21] spyware network, 2020 brought on the discovery of a malware that operated below the radar in the past four years called Mandrake[22]. What makes this malware interesting and scary at the same time is that its operators intentionally stayed hidden by not infecting too many devices.

Unlike other malware campaigns in which criminals try to infect as many devices as possible, hoping that something will eventually stick, the exact opposite happens with Mandrake. Since it's considered a spying platform, its operation is a bit different. The malware would kick in only after a monitoring period, giving hackers time to figure out if the target is worth it. This method allowed them to stay under the radar for a very long time.

The usual motivation of cybercriminals on Android is to make money, by any means necessary. Sometimes they are just looking to exploit the existing ads frameworks, but the more aggressive malware campaigns will go after people's data, which they sell on the dark web.

But 2020 has proven a unique year because of the COVID-19 pandemic that changed cybercriminal behavior. If, until now, they struggled to find some hook to trick people into installing their corrupt apps, the pandemic gave them a foothold.

18 "Global number of internet users 2012-2019, by operating system", Statista, https://www.statista.com/statistics/543185/worldwide-internet-connected-operating-system-population/
19 "Smartphone Market Share", IDC, https://www.idc.com/promo/smartphone-market-share/os
20 "Disruptive ads enforcement and our new approach", Google, https://security.googleblog.com/2020/02/disruptive-ads-enforcement-and-our-new.html
21 "Triout Android Spyware Framework Makes a Comeback, Abusing App with 50 Million Downloads", Bitdefender, https://labs.bitdefender.com/2019/02/triout-android-spyware-framework-makes-a-comeback-abusing-app-with-50-million-downloads/
22 "Mandrake – owning Android devices since 2016", Bitdefender, https://labs.bitdefender.com/2020/05/mandrake-owning-android-devices-since-2016/

Bitdefender analyzed Android telemetry[23] from Google Play and several other marketplaces, looking for coronavirus-themed legitimate apps and malware in Europe, and we observed a significant increase in interest in downloading and installing medical applications. Criminals are using the Coronavirus to deploy aggressive adware, and bundle apps with banking Trojans, SMS-sending malware, and even the money-siphoning Android malware named Joker Trojan.

Some of the more common types of Android malware discovered in 2020 include various families, such as Android.Trojan.Downloader Total, Android.Trojan.HiddenApp Total, Android.Trojan.Agent Total, Android.Trojan.Adrd Total, Android.Trojan.FakeInst Total, and Android.Trojan.Obfus Total.

As is obvious, most of the malware is either geared toward the hidden installation of aggressive adware, or to hide the installation of other packages, like banking Trojans.

Looking at the YoY evolution of global Android threat reports, it's interesting to spot that each year as a unique fingerprint in terms of the number of malicious reports registered each month. If during the first half of 2018 the highest number of Android threats were reported in February, during the first half of 2019 Android malware reports were somewhat constant throughout all six months. However, during the first half of 2020, April (31.72 percent) and May (27.65 percent) had the highest number of reports.

Interestingly, January and February 2020 had the lowest number of reports, potentially because as the world moved to a work-from-home condition, users started downloading more applications from untrusted sources. For instance, Bitdefender researchers found numerous instances in which popular video conferencing, such as Zoom[24], or other Android applications, were tainted[25] by malware developers and spread through third-party marketplaces to infect users with ransomware[26], Trojans and information stealers.

It's likely no surprise that, during the first half of 2020, the number of reported Android threats started to increase from March, as threat actors potentially capitalized on the fear, panic and misinformation caused by the pandemic to bundle malware with seemingly legitimate Android apps.

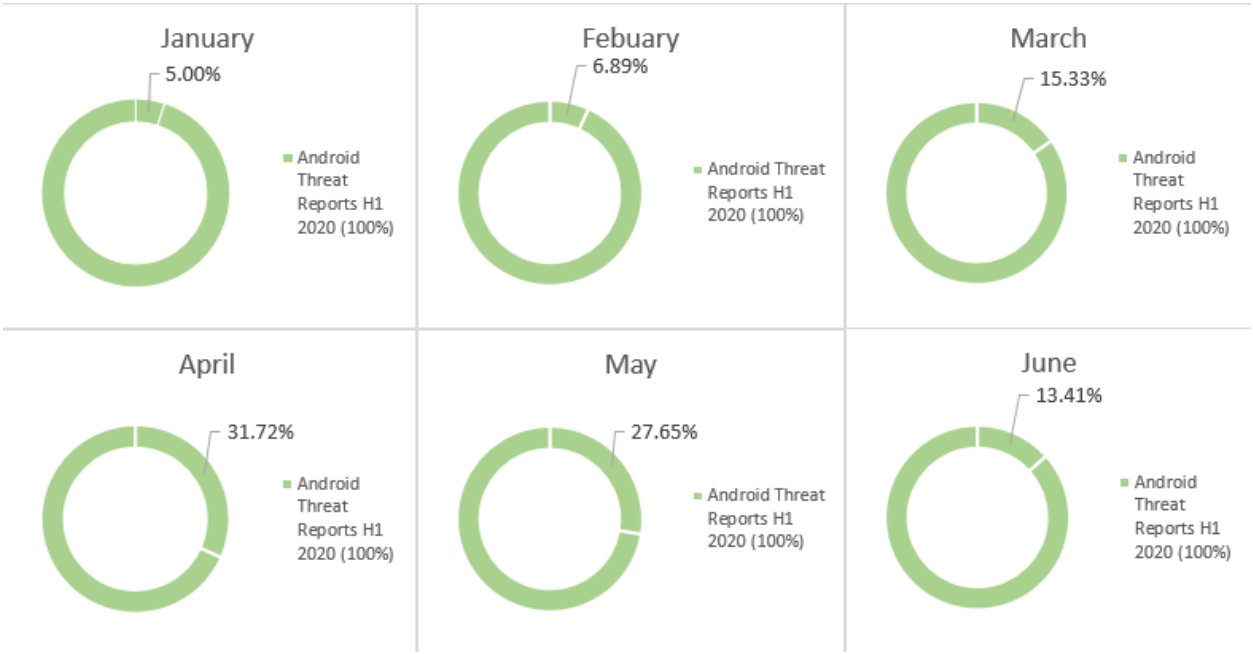


Fig. 66 - Global Evolution of Android Threat Reports H1 2020

23 "Android Apps and Malware Capitalize on Coronavirus", Bitdefender, https://labs.bitdefender.com/2020/03/android-apps-and-malware-capitalize-on-coronavirus/
24 "Who installs Zoom apps outside the Play Store? Well, lots of people", Bitdefender, https://labs.bitdefender.com/2020/04/who-installs-zoom-apps-outside-the-play-store-well-lots-of-people/
25 "Infected Zoom Apps for Android Target Work-From-Home Users", Bitdefender, https://labs.bitdefender.com/2020/03/infected-zoom-apps-for-android-target-work-from-home-users/
26 "Android SLocker Variant Uses Coronavirus Scare to Take Android Hostage", Bitdefender, https://labs.bitdefender.com/2020/05/android-slocker-variant-uses-coronavirus-scare-to-take-android-hostage/

Looking at the top Android malware families during the first half of 2020, we have everything from information stealers to fake installers and ransomware. While the Android.Trojan.Adrd Android malware family ranks first (11.97 percent of the total number of malicious Android reports during the first half of 2020), it's closely followed by the Android.Trojan.FakeInst (10.57 percent) and Android.Trojan.FakeInst (10.08 percent) malware families.

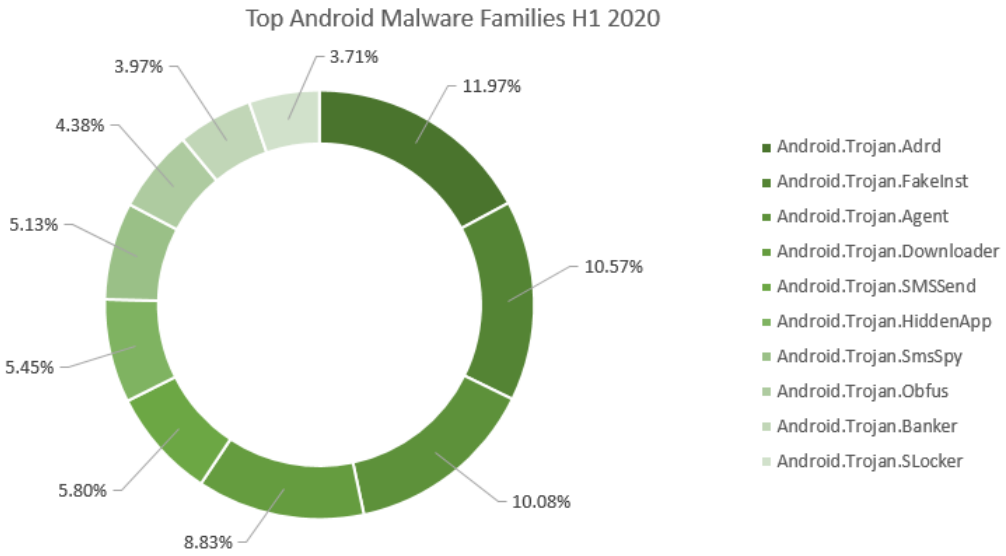


Fig. 67 – Top Android malware families H1 2020

Interestingly, while these are focused on installing additional malware by posing as legitimate apps or by being bundled with truly legitimate applications, ransomware also makes it to our list of the top 10 threat. While SMS-sending Trojans and Android Bankers are somewhat more lucrative for threat actors, the Android.Trojan.SLocker ransomware family still manages to account for 3.71 percent of all Android malware reports during the first half of 2020.

While these remain the top global malware families for Android-running devices, variations to this Top 10 list may occur depending on the country.

United States

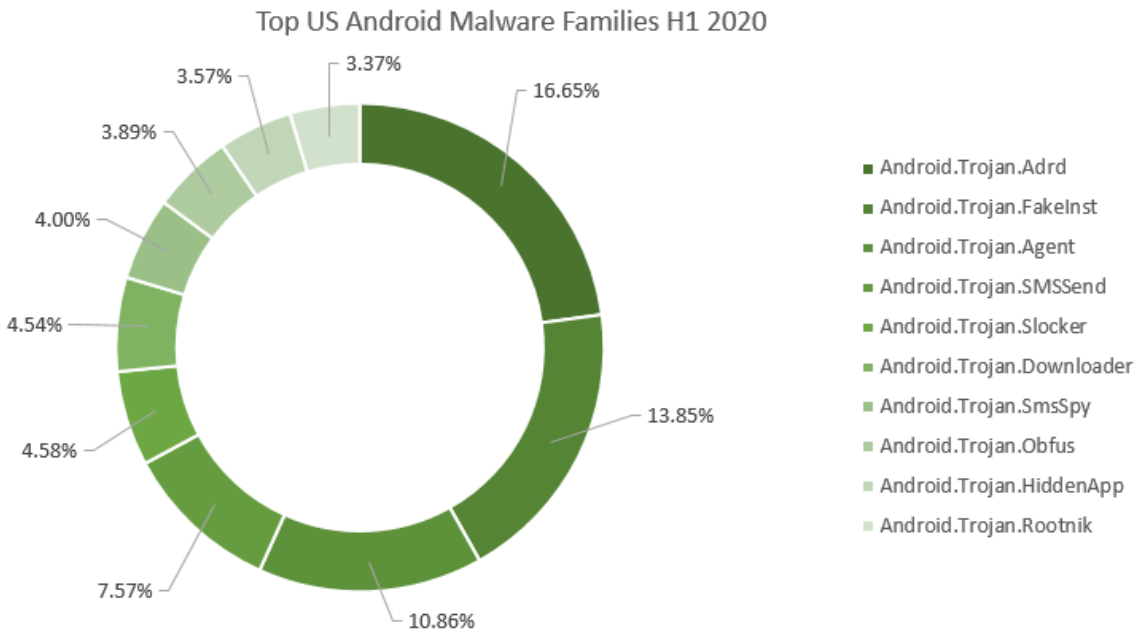


Fig. 68 – Top US Android malware families H1 2020

United Kingdom

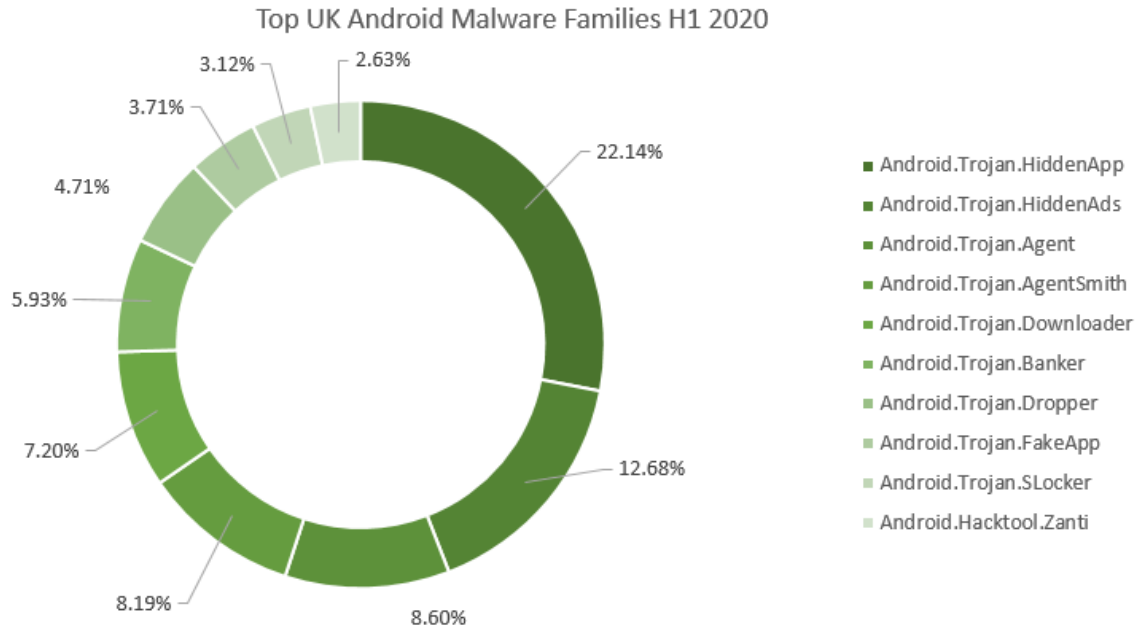


Fig. 69 – Top UK Android malware families H1 2020

Sweden

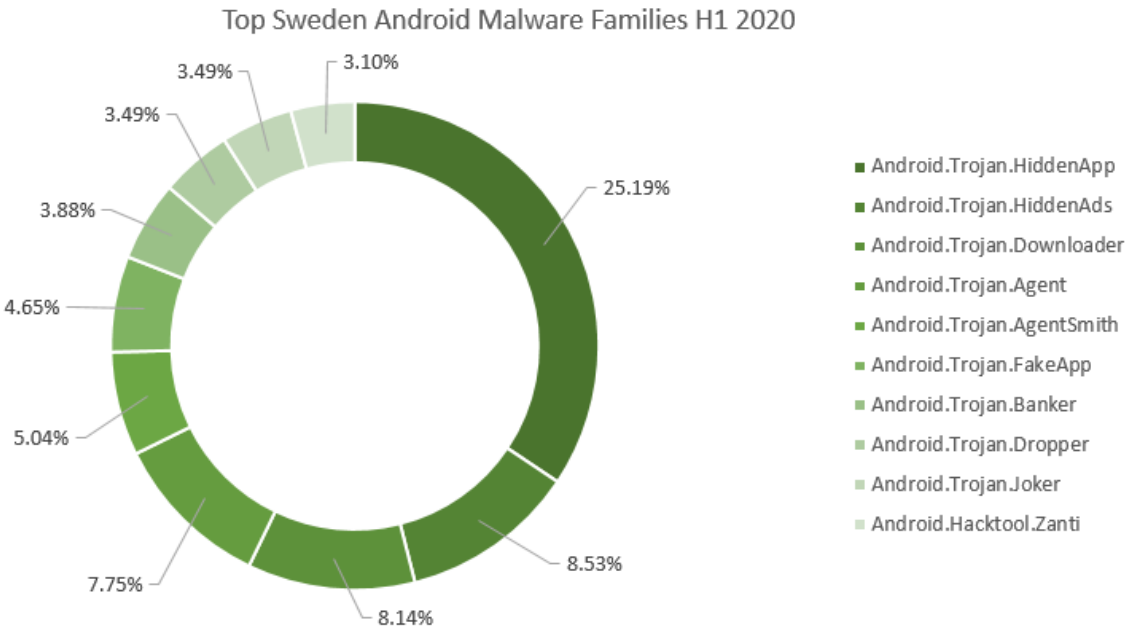


Fig. 70 – Top Sweden Android malware families H1 2020

Romania

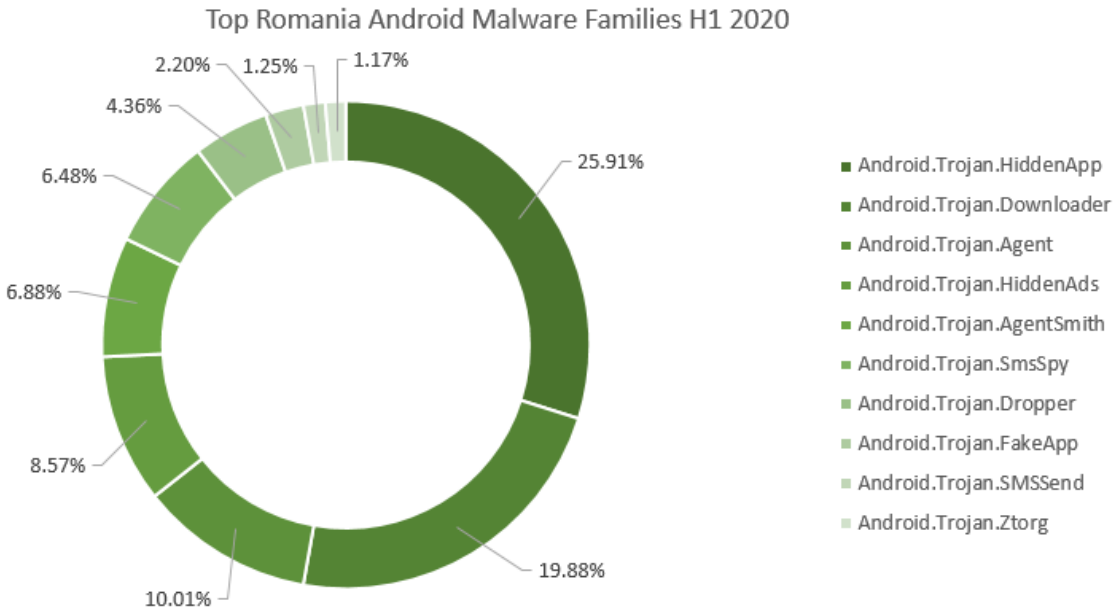


Fig. 71 – Top Romania Android malware families H1 2020

Italy

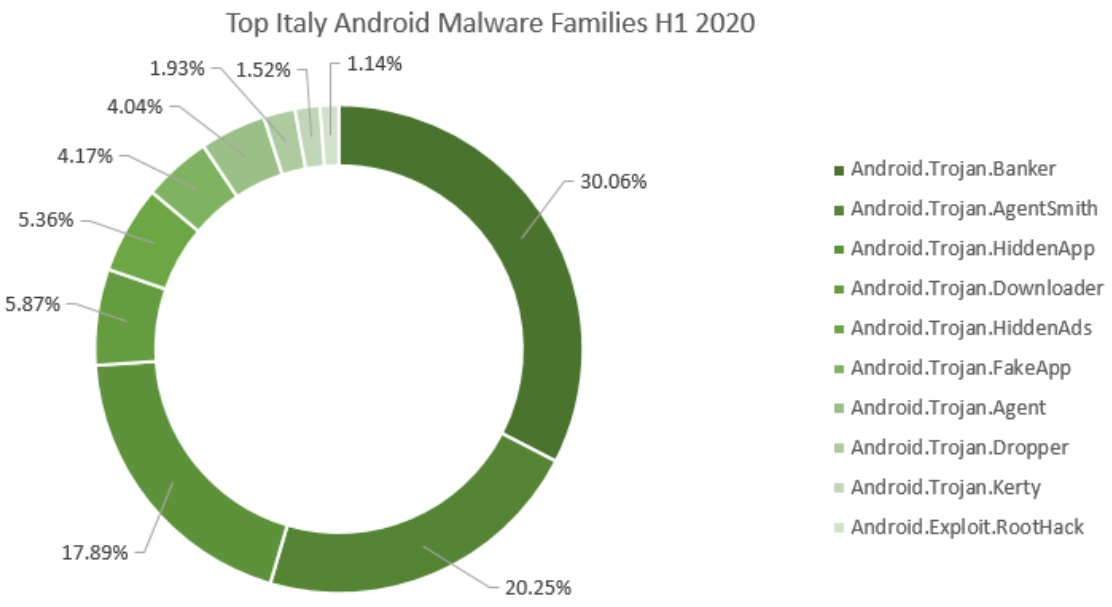


Fig. 72 – Top Italy Android malware families H1 2020

France

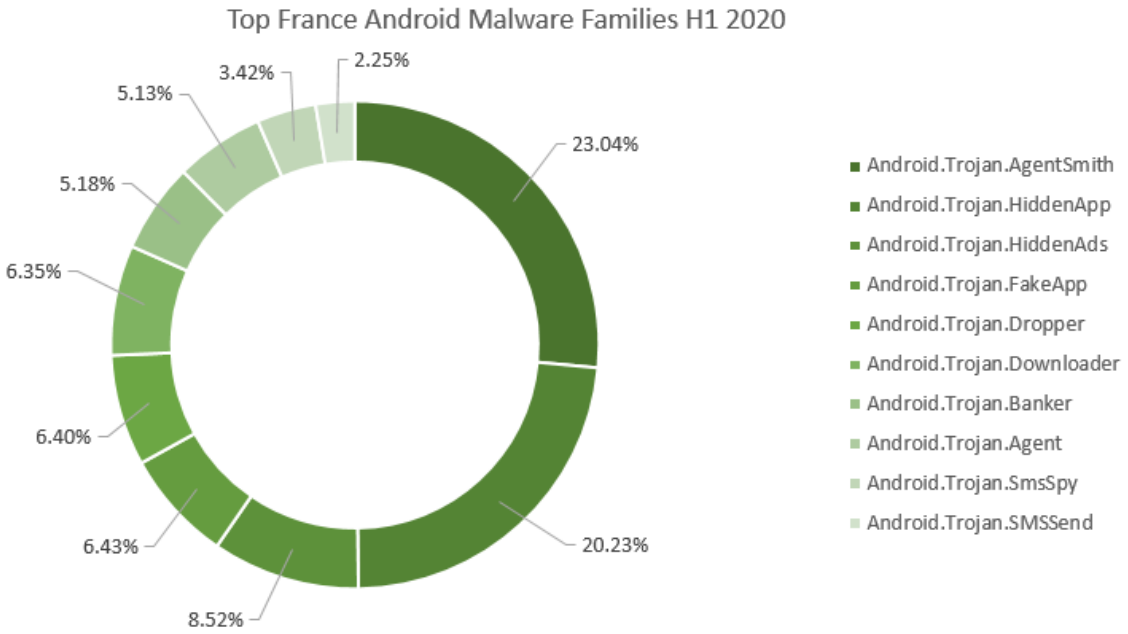


Fig. 73 – Top France Android malware families H1 2020

Spain

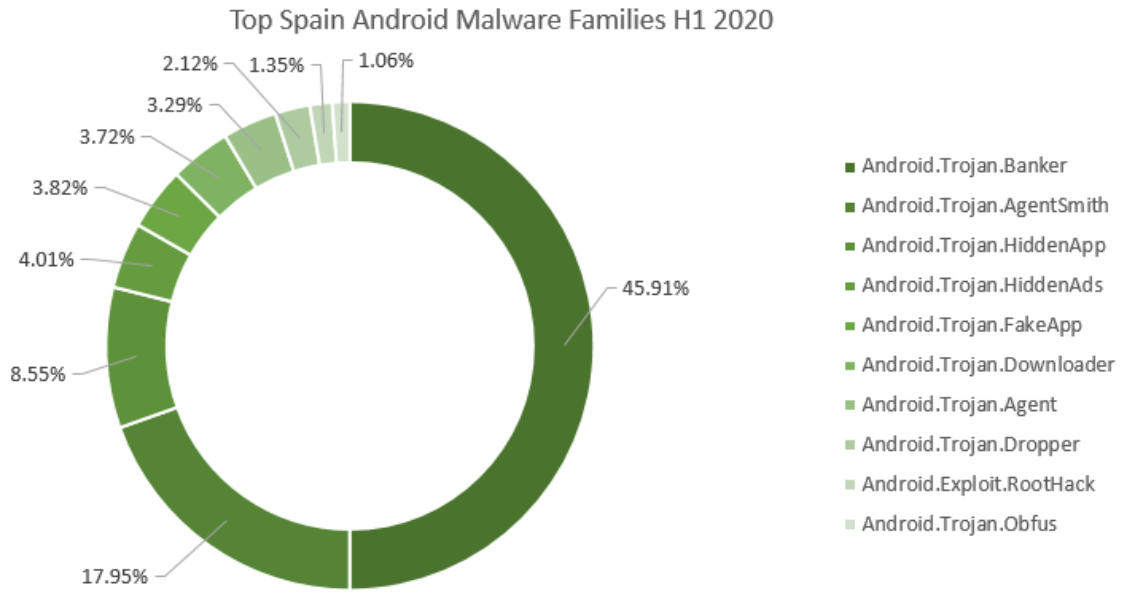


Fig. 74 – Top Spain Android malware families H1 2020

Denmark

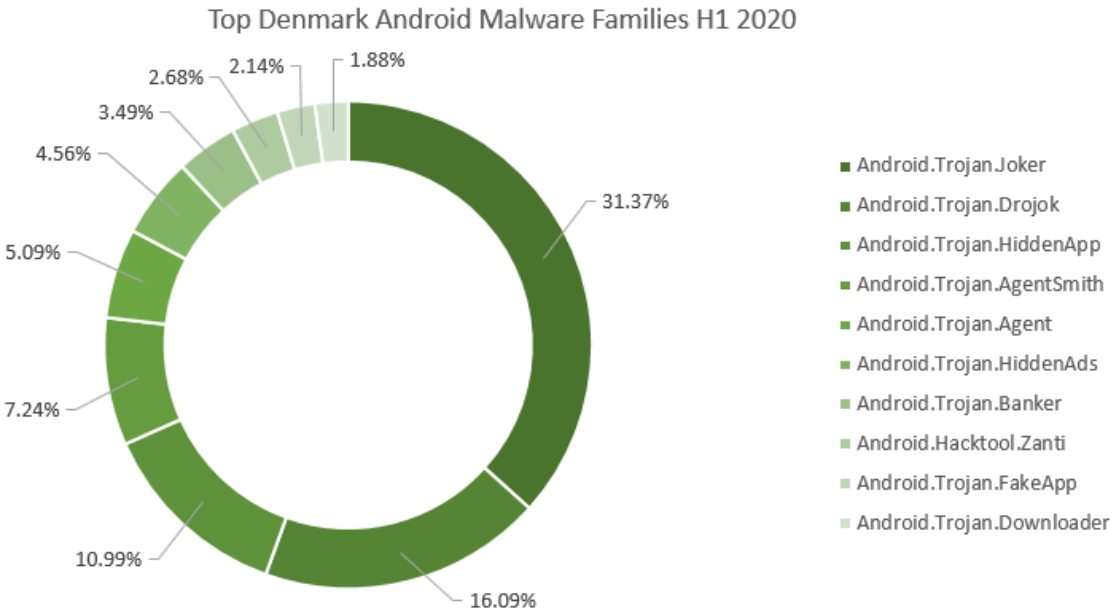


Fig. 75 – Top Denmark Android malware families H1 2020

Germany

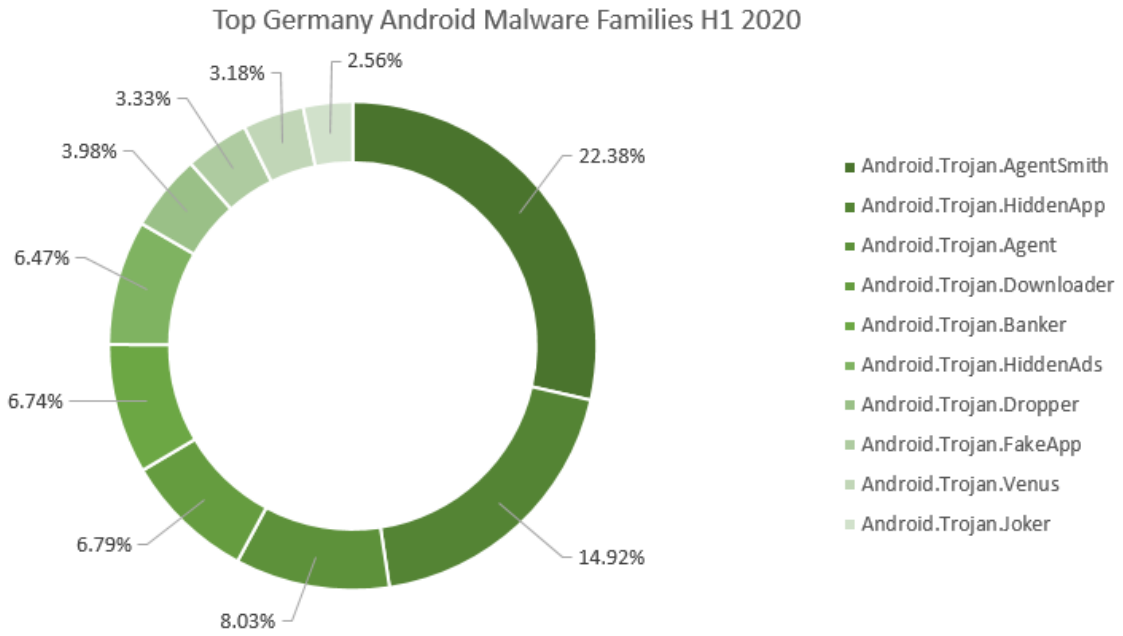


Fig. 76 – Top Germany Android malware families H1 2020

Australia

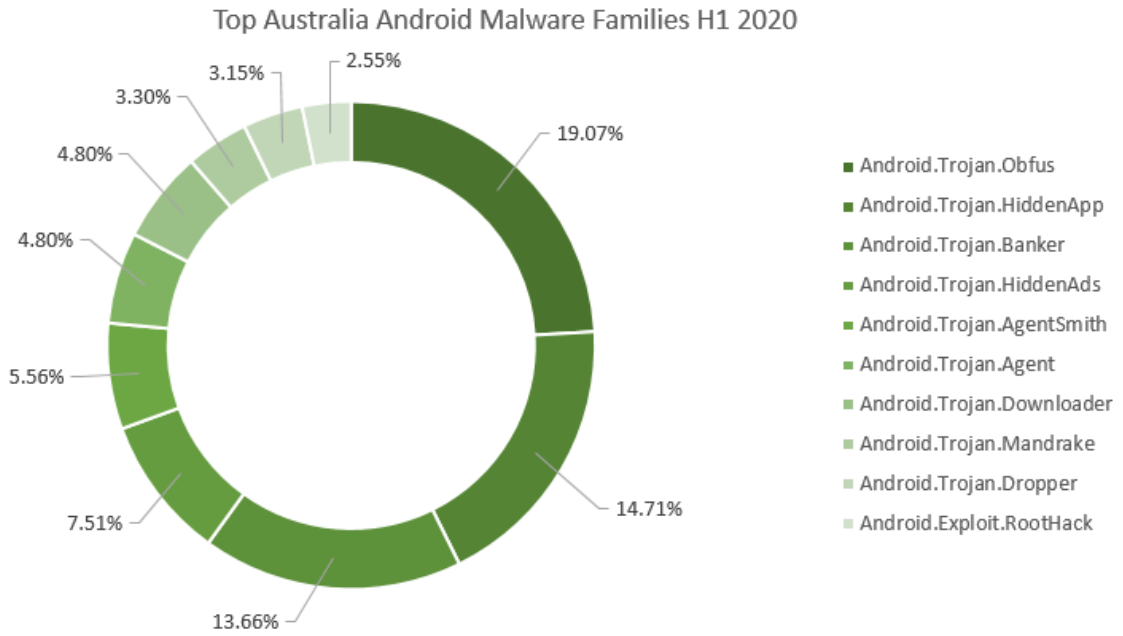


Fig. 77 – Top Australia Android malware families H1 2020

Netherlands

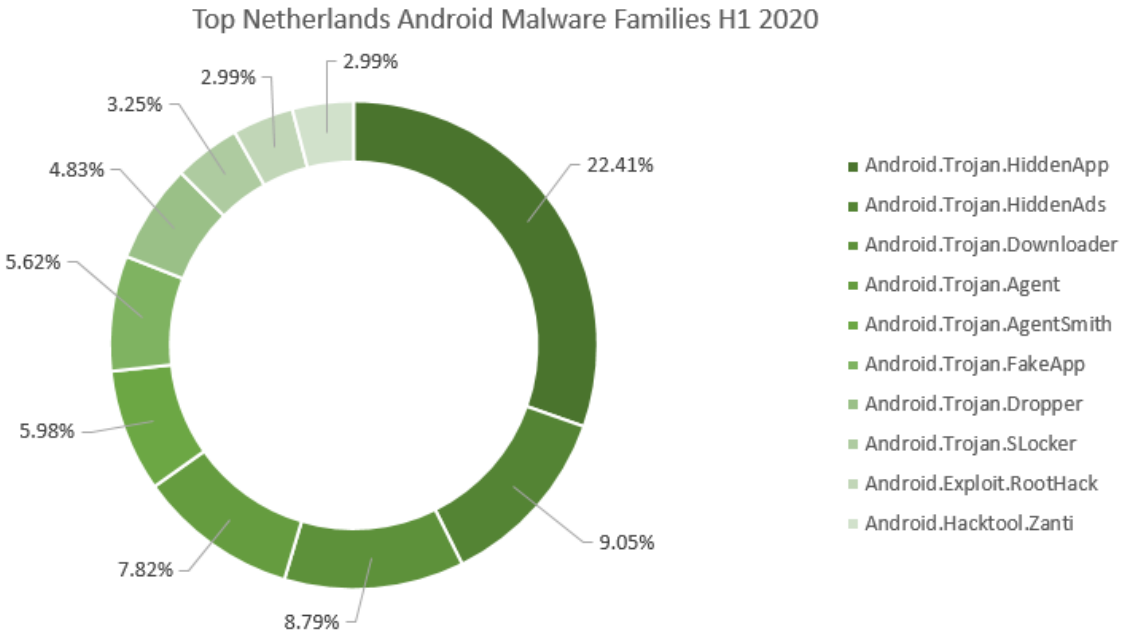


Fig. 78 – Top Netherlands Android malware families H1 2020

Internet of Things (IoT) Threat Landscape

The digital world is full of Internet of Things (IoT) devices, seen and unseen. Despite the economic problems brought on by the pandemic and the inevitable slowdown in innovation and deployment, IoT spending is expected to return to double-digit growth[27] rates in 2021 and on track to reach the projected 41.6 billion[28] units by 2025.

The expected growth is only matched by the security aspect of the IoT world, or the lack thereof, in terms of significance. For all the incredible features that IoT brings into our lives, both from commercial and industrial points of view, this technology branch is fraught with security issues, ranging from lack of support from manufacturers to vulnerabilities that affect billions of devices at once.

One of the more serious problems often overlooked is that people don't realize they own IoT devices and are not worried about issues. But people own routers, smartwatches, smart fridges, personal assistants, smart cars, and much more. Some of the most prominent issues include:

- Weak or default passwords that were never changed by users
- Vulnerabilities never addressed by manufacturers
- Companies that abandon support quickly after launch
- Old devices that reached end of life (EOL)
- Much, much more

Hackers are usually after one of two things. They either want to compromise IoT devices and steal personal data, or extend their botnets, allowing them to launch DDoS attacks or rent those services to third parties. Either way, using a vulnerable IoT device is a risk for the customer and others.

The Mirai[29] botnet casts its shadow to this day. Since its developers released the source code online four years ago, new variants have been released, and there's always something new in the making. While Mirai continues to show its ugly head here and there, we also see quite a few new botnets, written from scratch, usually in GoLang.

Spinoffs of the popular botnet have popped in and out of existence, with one of the latest dubbed LiquorBot. A reimplementation of Mirai written in GoLang, LiquorBot[30] was spotted in early 2020 incorporating cryptocurrency-mining features and propagating through SSH brute-forcing and exploitation of unpatched vulnerabilities in select router models.

Other recent examples[31] include IRCflu, which uses a legitimate open-source IRC bot (IRCflu) as a backdoor into compromised SSH servers, or InterPlanetary Storm, a bot designed to infect Windows machines.

The one that recently garnered the most attention was dark_nexus[32], an IoT botnet with new features and capabilities compared to other similar malware. What makes it interesting is that it's designed for 12 different CPU architectures. Bitdefender spotted it during development, allowing us to trace its source more quickly and mark its evolution.

Our internal telemetry shows that the number of **IoT suspicious incidents** has been growing steadily from January to June, with a total **increase of 46% in just six months**. As for devices commonly present in households**, 61.56 percent of all traditional internet-connected devices** within households consist of smartphones, computers, tablets, laptops, consoles and routers, according to Bitdefender telemetry, with IoTs making up the rest.

27 "Worldwide Spending on the Internet of Things Will Slow in 2020 Then Return to Double-Digit Growth, According to a New IDC Spending Guide", IDC, https://www.idc.com/getdoc.jsp?containerId=prUS46609320
28 "The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast", IDC, https://www.idc.com/getdoc.jsp?containerId=prUS45213219
29 Mirai (malware), Wikipedia, https://en.wikipedia.org/wiki/Mirai_(malware)
30 "Hold My Beer Mirai – Spinoff Named 'LiquorBot' Incorporates Cryptomining", Bitdefender, https://labs.bitdefender.com/2020/01/hold-my-beer-mirai-spinoff-named-liquorbot-incorporates-cryptomining/
31 "SSH-Targeting Golang Bots Becoming the New Norm", Bitdefender, https://labs.bitdefender.com/2020/06/ssh-targeting-golang-bots-becoming-the-new-norm/
32 "New dark_nexusIoT Botnet Puts Others to Shame", Bitdefender, https://labs.bitdefender.com/2020/04/new-dark_nexus-iot-botnet-puts-others-to-shame/

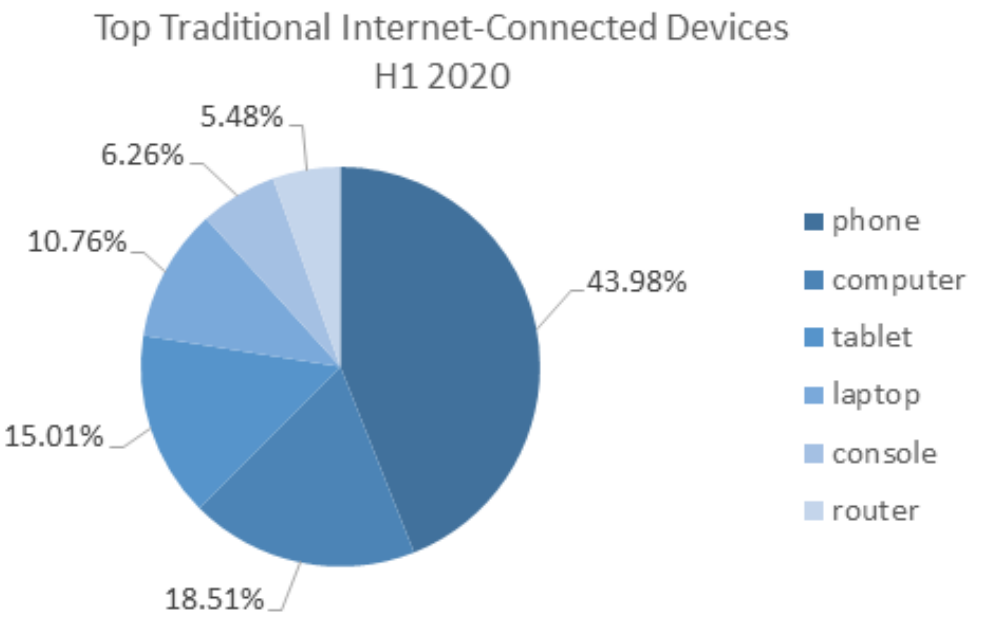


Fig. 79 – Top Traditional internet-connected devices

Interestingly, among the most popular IoT devices in households are streaming devices, such as Roku and Apple TV to Amazon Fire TV Stick, Google Chromecast, and others. This particular category makes up for about **14.65 percent of all IoT devices within households**, according to Bitdefender telemetry.

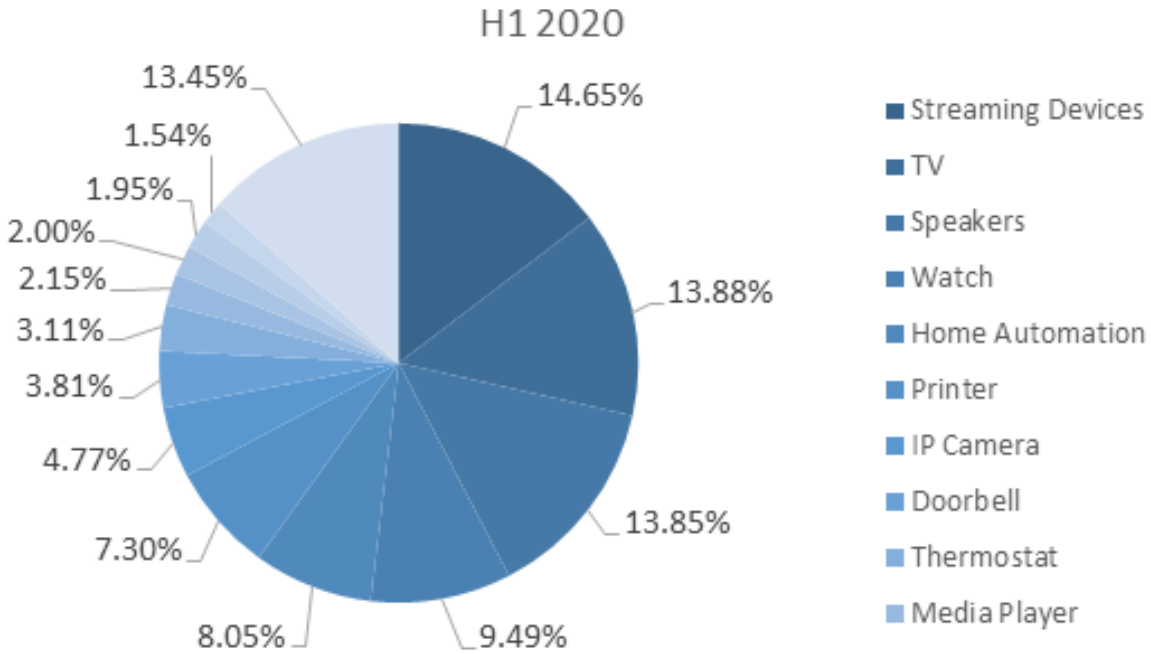


Fig. 80 – Top household IoT Devices H1 2020

Naturally, smart TVs (13.88 percent) and smart speakers (13.85 percent) are next, followed by smartwatches (9.49 percent), home automation systems (8.05 percent), printers (7.30 percent), IP cameras (4.77 percent), smart doorbells (3.81 percent) and smart thermostats (3.11 percent). We often say that people don't know when they have IoT devices in their households, and they are easy to neglect. Some of the more "exotic" examples of IoT devices include VOIP phones, smart bulbs, smart vacuums, air purifiers, solar panels, baby monitors, cooking robots, motion sensors and many others.

Routers are a particularly interesting range of devices that are often extremely vulnerable. A recent study found that most commercial routers[33] haven't been updated in more than a year, are riddled with hundreds of vulnerabilities and are running ancients OSs and EOL Linux kernels.

Another interesting aspect is the OS spread among connected IoT devices, and anyone trying to guess the distribution would probably be wrong. Around 46% of the IoT hardware runs proprietary software, followed by iOS with 27%. Windows, Android, and Mac OS X finish last, by far.

In terms of threats going after household IoT devices, Bitdefender network threat protection technologies reported that **55.73 percent** of all identified network incidents represent port **scanning attacks**. This means threat actors are constantly scanning for open ports on internet-connected smart devices to identify potentially vulnerable devices and remotely dial into them. **Password stealing attempts via HTTP account for 22.62 percent** of all household network incidents, suggesting that, once attackers identify a potential internet-connected device, they will attempt to probe for plaintext credentials sent over unencrypted connections or services.

With more and more IoT devices going online every minute, the risks increase. And if we also consider that many of the IoT devices we used yesterday are no longer supported today, it's easy to see why hackers are increasingly focusing their efforts on this part of the tech world.

33 "Home Router Security Report 2020", Fraunhofer Institute for Communication, Information Processing and Ergonomics FKIE, https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/HomeRouter/HomeRouterSecurity_2020_Bericht.pdf

Spam Evolution

The first half of 2020 was nobody's cup of tea. Amid the chaos surrounding the spread of COVID-19, cyber-crime flourished, with bad actors constantly adapting to changing political and economic conditions across the globe.

Email reigns as the number one threat vector that cybercriminals employ to enable a successful cyberattack or scam to collect sensitive information from users.

Most notably, spammers have sharpened their skills over the past year, developing emails that often evade spam-filtering algorithms and individual analysis. Even though many e-mails have become more personalized and convincing, with fewer grammar mistakes, the content itself has not necessarily changed.

As the world struggled to cope with the difficulties brought on by the pandemic, cybercriminals managed to thrive, going all out to exploit the fears, financial distress and overwhelming need for information exhibited by the general population.

We're six month into adjusting to the effects of the coronavirus pandemic, and while one should think that scammers have exhausted the subject, coronavirus-related spam and malspam[34] are here to stay.

Whether it's a phishing scam exploiting the coronavirus, a fundraiser or a jaw-dropping offer you can't resist, bad actors have pulled off every trick of the trade to fool victims into providing sensitive information to spread malware.

The strain of social distancing and the shift to remote work have also played a crucial role in the enablement of cyber-crime and malicious emails. As a result of stay-at-home orders, consumers spent more time online to virtually connect with coworkers, friends and family, stream entertainment, shop and peruse emails.

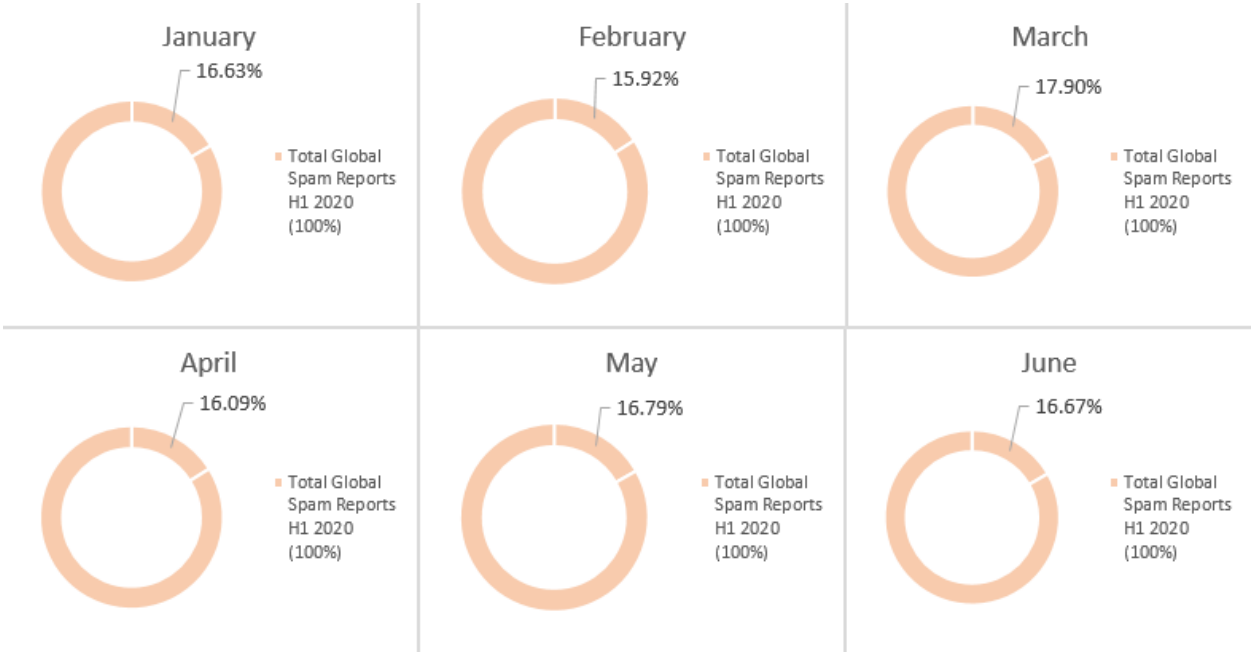


Fig. 81 – Global evolution of received spam H1 2020

When comparing the evolution of received spam during the first half of 2019 with the first half of 2020, it's interesting to spot that significantly more spam was received in March 2020 than any other month. In fact, if during the first half of 2019 Bitdefender telemetry only registered a single spike in telemetry during April (17.61 percent), in 2020 our

34 "Malicious Spam Is Adapting to the Pandemic, Bitdefender Telemetry Shows", Bitdefender, https://hotforsecurity.bitdefender.com/blog/malicious-spam-is-adapting-to-the-pandemic-bitdefender-telemetry-shows-22917.html

telemetry picked two spikes, in March (17.90 percent) and May (16.79 percent).

It's likely that the uptick in received spam during these two months of 2020 is a result of the global pandemic that cybercriminals leveraged to send out more spam and scams. Since March was when the pandemic quickly made its way through Europe, with countries forced to implement a state of emergency, cybercriminals likely seized the opportunity to exploit fear, misinformation and the general panic caused by the outbreak.

More often than not, malicious actors seek financial gain from their swindles, and the economic Coronavirus Aid, Relief, and Economic Security (CARES) Act, along with the extended tax filing date made the United States a more desirable target.

In Europe, the UK and Germany were also prime targets, as both countries were overwhelmed by the outbreak, and implemented stable relief programs and financial assistance measures for businesses and employees.

Oh, Corona!

Covid-19-related spam has been the hallmark of the past six months, and the fear surrounding the virus continues to fuel malware and spam. On average, during the first half of 2020, **four out of 10 Coronavirus-themed emails were tagged as spam**.

As millions of consumers look for updates and information regarding the spread and containment of the pandemic, scammers obliged, spreading misinformation[35], fake cures and offers for protective gear.

Most frequently, fraudsters have impersonated government, health and financial institutions, with various scam emails purporting to be from the World Health Organization requesting detailed information or funds from individuals.

Just another case of malware

Malware-laden e-mails are not exempt from this year's threat landscape. A series of malspam campaigns were noticed this spring, with attackers sending out emails with malicious attachments. For example, out of the total global emails scanned during **April 24, 45 percent were tagged as containing malware**.

Another spike showed up on April 24, when 41.5 percent of all scanned emails within that day had some form of malicious attachment, and again on May 4 (42.69 percent). The beginning of June was also interesting, as a malspam campaign seems to have spread across four days, from **May 31st until June 3rd. On average, four out of 10 emails send throughout each day within that time spam was tagged as containing malware**.

Travel

Amid the pandemic, tourism and transport services were halted, with serious social and economic effects. However, as governments gradually lifted travel restrictions, individuals have started planning their much anticipated city breaks or getaways.

Fraudsters have made the most of the news, deploying a campaign targeting travel and vacation enthusiasts at the end of May. Although it may have started out innocently enough on May 25, it first peaked on **May 31. On that day, from all the scanned spam emails, around three out of 10 were travel-themed.** While the campaign did slow down for a couple of days, it peaked once more on **June 7, with four out of 10 spam emails scanned that day being tagged as travel-themed**.

These peaks in travel scams might have to do with an ease on restrictions in countries hit hardest by the pandemic.

35 "Coronavirus Phishing Scams Exploit Misinformation", Bitdefender, https://hotforsecurity.bitdefender.com/blog/coronavirus-phishing-scams-exploit-misinformation-22599.html

As the holiday season approached and pandemic restrictions were lifted, attackers may have seized the opportunity and prayed on everyone's interest in taking a break and planning their vacations. Consequently, these spikes in travel-themed spam once again prove that threat actors are tuned in to their victims' needs and interests, planning their messages and campaigns to maximize their effectiveness.

The old Nigerian prince swindle and advance-fee scams

Social engineering at its finest has kept this old ruse up and running for nearly three decades now. While one might assume that the scam would have withered amid the crisis, think again. Bitdefender telemetry picked up a flood of Nigerian prince and similar advance-fee scams in May. In **May, Nigerian prince scams accounted for 30% of incoming spam** scanned during that day.

Advance-fee scams accounted for **one out of four emails on May 14**, with no particular other surges following. While these two scams are similar, both requiring some form of advance payment, nuances separate them. For example, while Nigerian scams usually promise a large sum of money in exchange for some "small" tax fees, advance-fee scams revolve around investments, loans, inheritances or even gifts.

Extortion and online dating scams

Two significant extortions campaigns were noticed on **April 27 and May 19**, when **37.34% and 30.13%** of all incoming emails (scanned within those days) concerned individuals attempting to blackmail recipients. While no evidence links these campaigns to previous data breaches of a sensitive nature, such as Ashley Madison or the more recent MobiFriends[36] dating app leak, the classic "I know about the secret you are keeping from your wife and everyone else" is still around.

Cyber-criminals have been diligently leveraging the social distancing measures and loneliness of citizens in isolation, with noticeable spikes in online dating scams flagged between May and June 2020. Dating scams accounted for **more than six out of 10** of all incoming unsolicited emails on **May 10 and May 11**, spiking the same way again on **June 14 and June 15**.

However, extortion emails have adapted to suit the ongoing health crisis. An original blackmailing campaign[37] was detected by Bitdefender in March, when bad actors were threatening to infect recipients and their families with Covid-19 unless victims transfer money to the blackmailers' bitcoin wallet.

Now let's take a close look at how received spam has evolved throughout the first half of 2020 compared to the first half of 2019, within specific countries.

36 "Personal Information of 3.6 Million MobiFriends is Up for Grabs, Free Download Included", Bitdefender, https://hotforsecurity.bitdefender.com/blog/personal-information-of-3-6-million-mobifriends-is-up-for-grabs-free-download-included-23234.html
37 "Pay me or I'll cough: Bad actors bully email recipients with new Covid-19 extortion scam", Bitdefender, https://hotforsecurity.bitdefender.com/blog/pay-me-or-ill-cough-bad-actors-bully-email-recipients-with-new-covid-19-extortion-scam-22768.html

United States

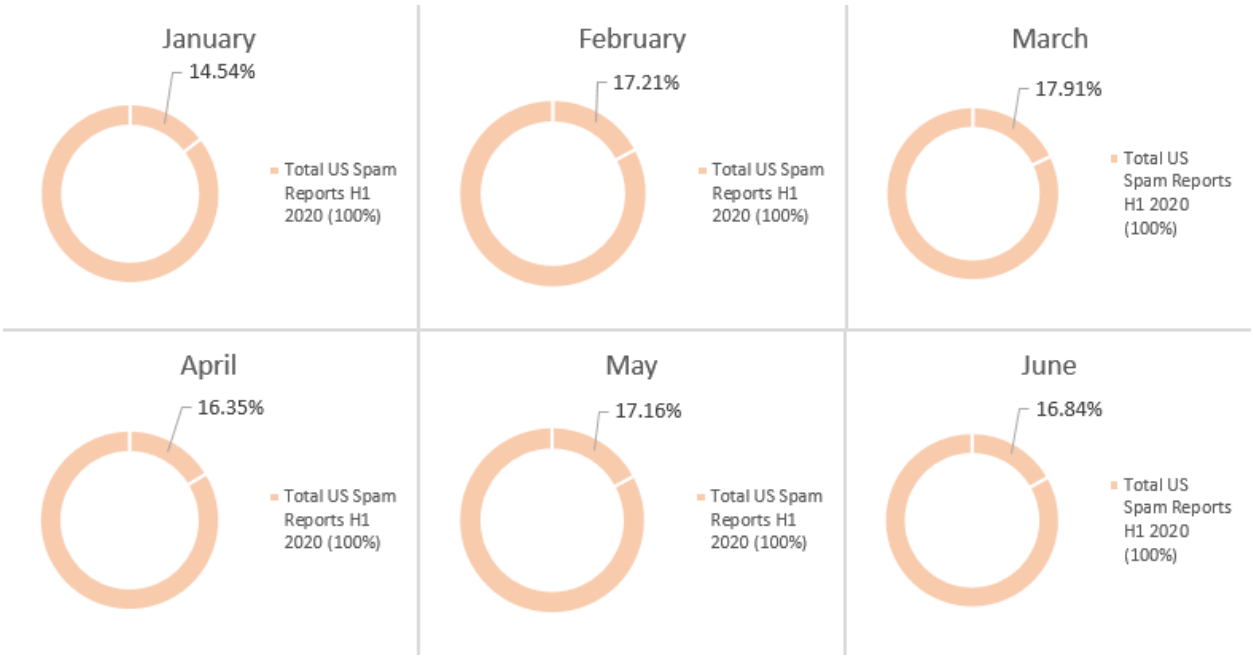


Fig. 82 – US evolution of received spam H1 2020

United Kingdom

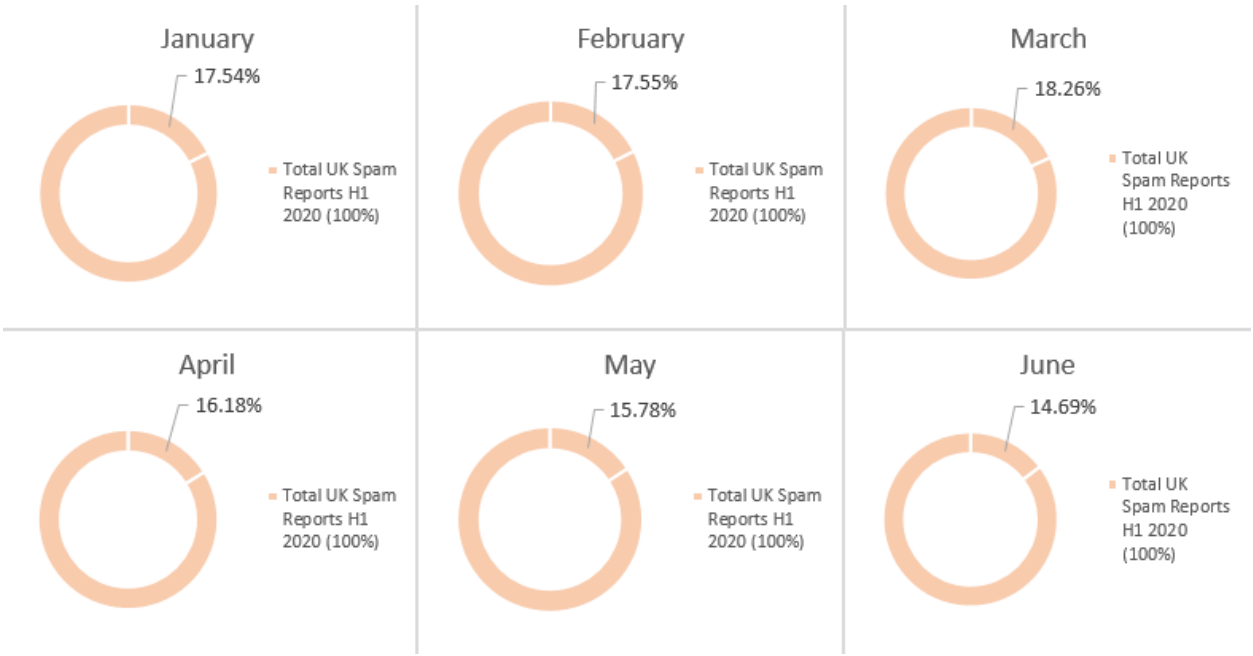


Fig. 83 – UK evolution of received spam H1 2020

Sweden

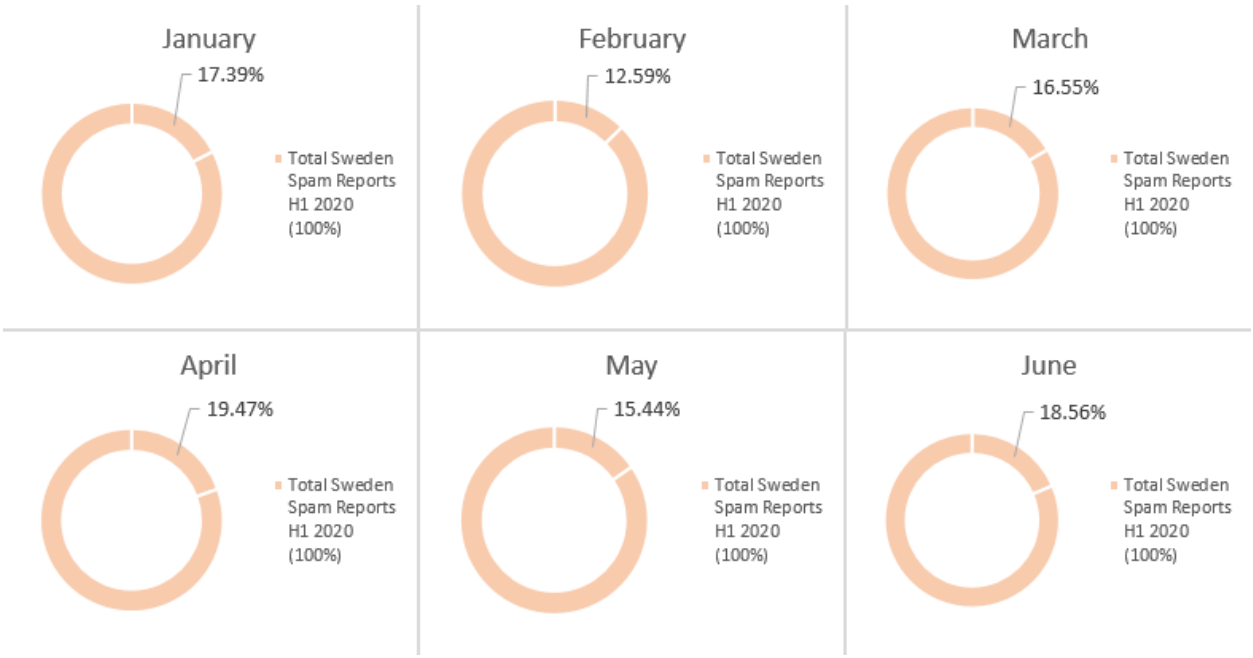


Fig. 84 – Sweden evolution of received spam H1 2020

Romania

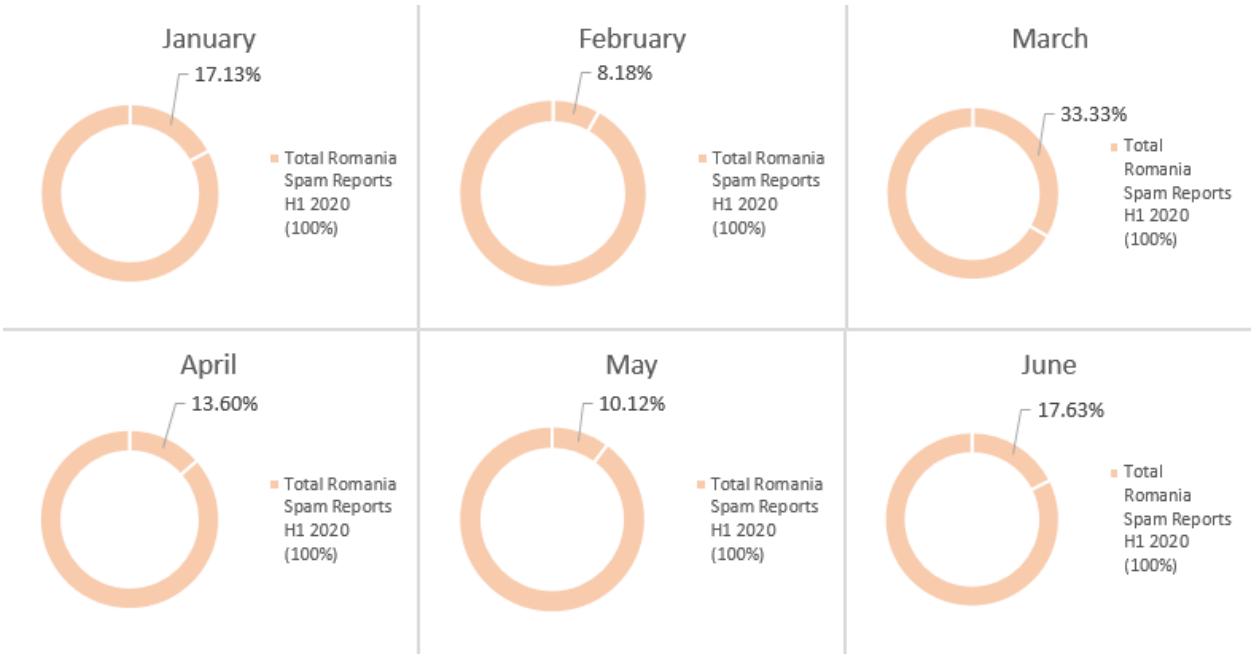


Fig. 85 – Romania evolution of received spam H1 2020

Italy

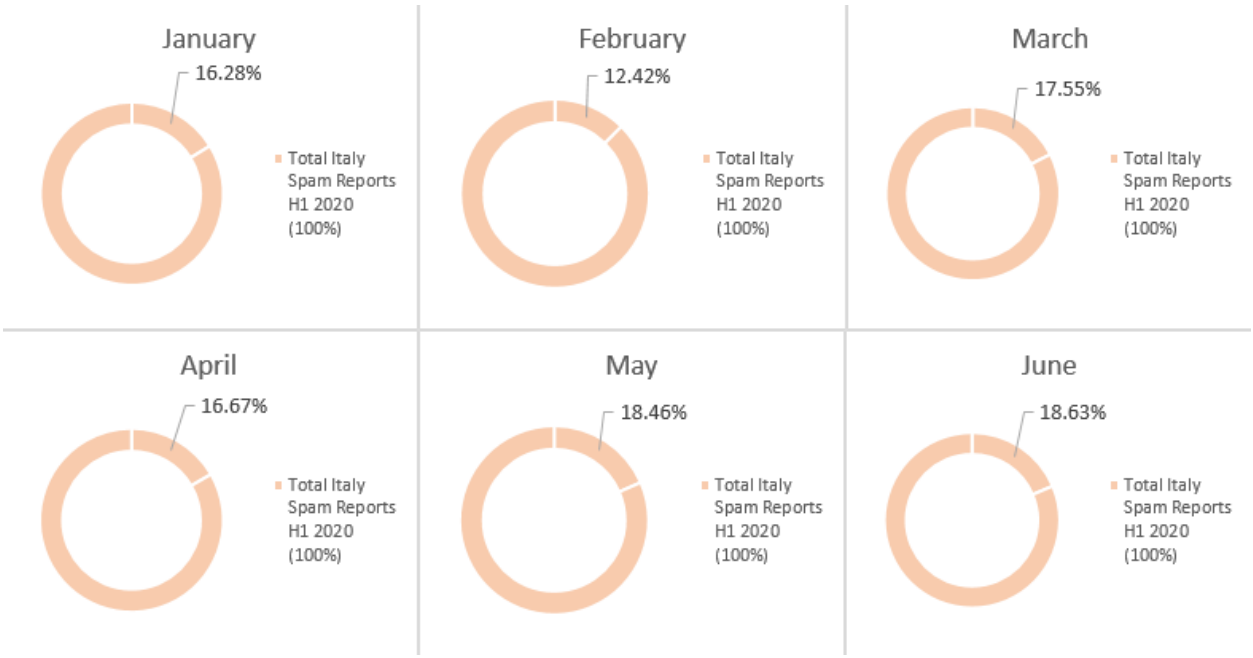


Fig. 86 – Italy evolution of received spam H1 2020

France

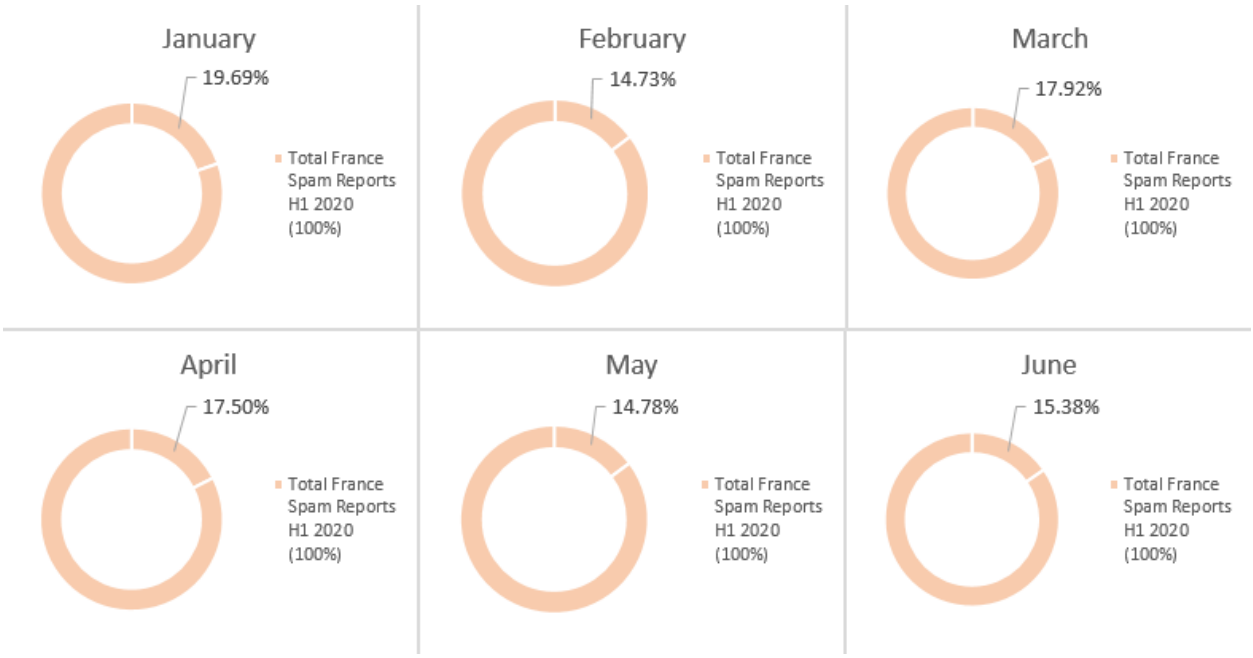


Fig. 87 – France evolution of received spam H1 2020

Denmark

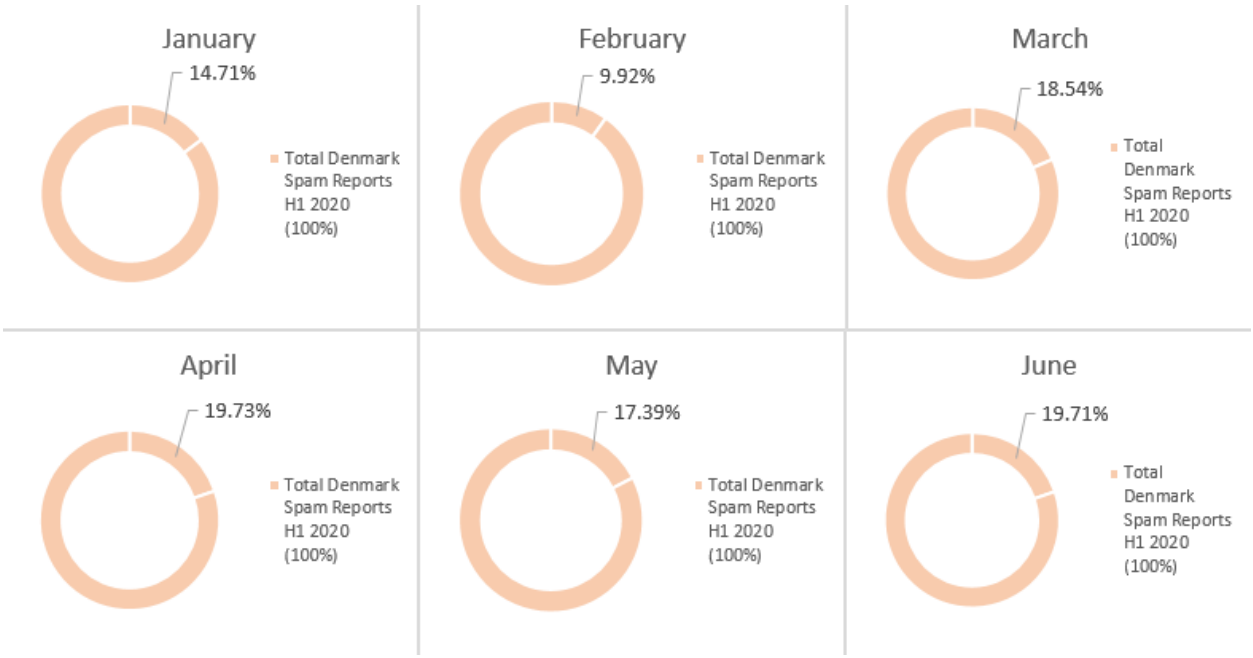


Fig. 88 – Denmark evolution of received spam H1 2020

Germany

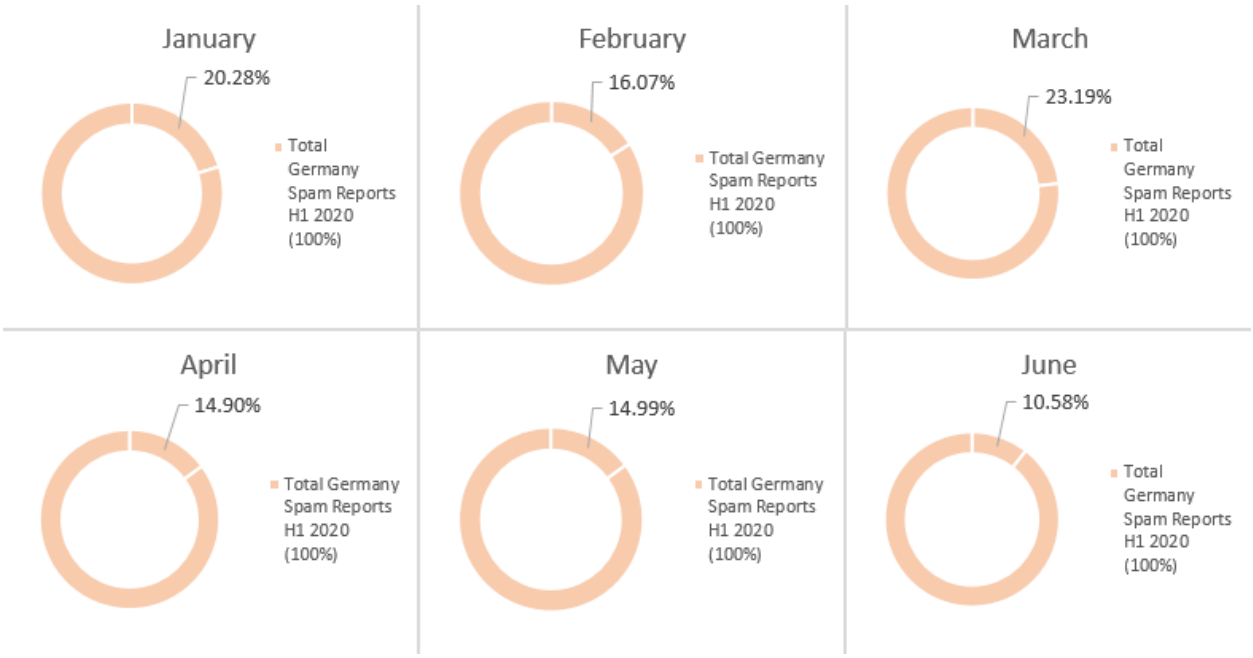


Fig. 89 – Germany evolution of received spam H1 2020

Australia

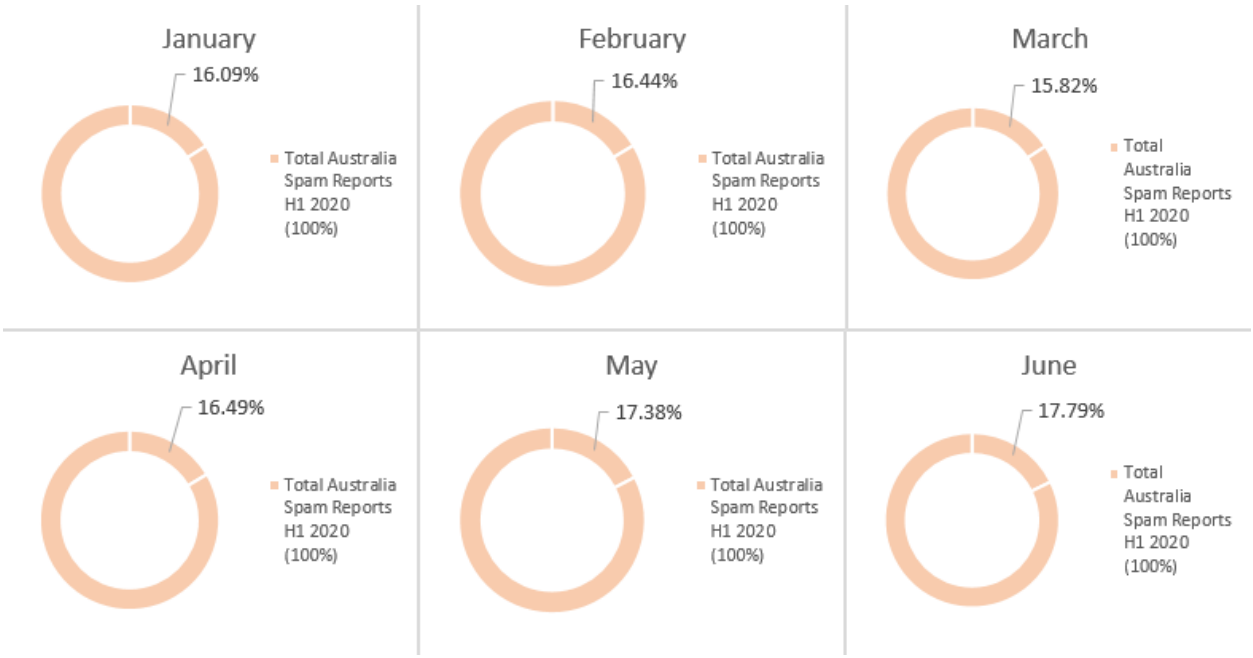


Fig. 90 – Australia evolution of received spam H1 2020

Spain

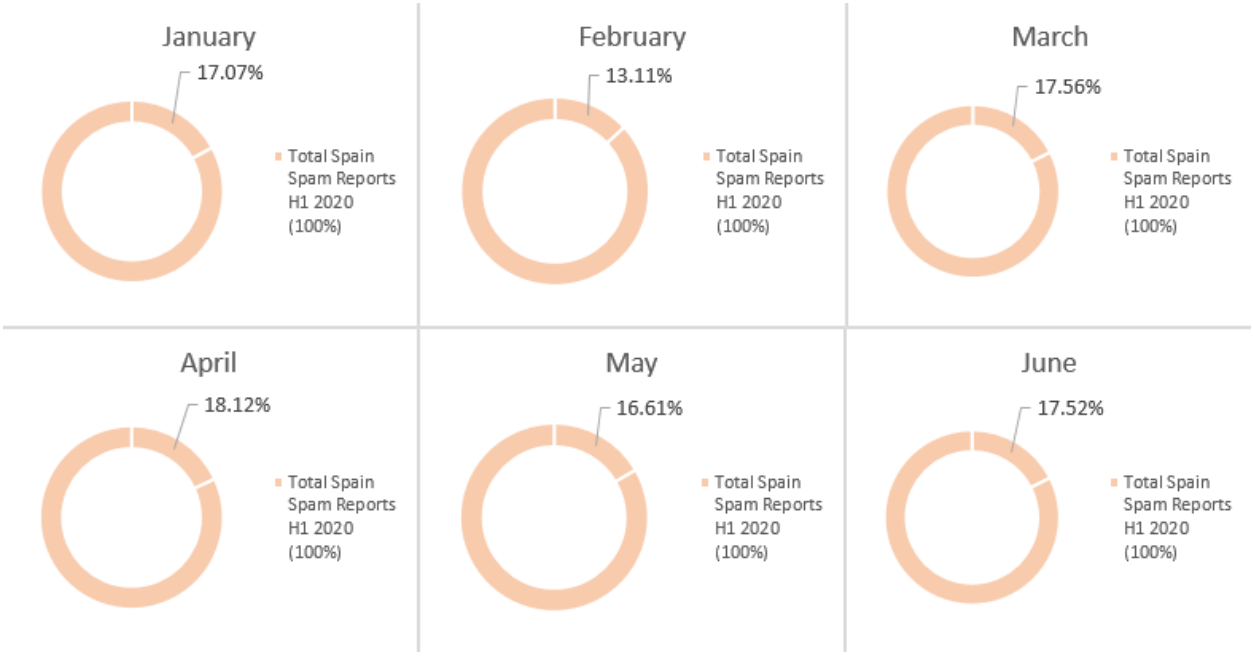


Fig. 91 – Spain evolution of received spam H1 2020

NOTE: THIS REPORT IS BASED ON TECHNICAL INFORMATION PROVIDED COURTESY OF BITDEFENDER LABS TEAMS.

Why Bitdefender

Proudly Serving Our Customers

Bitdefender provides solutions and services for small business and medium enterprises, service providers and technology integrators. We take pride in the trust that enterprises such as **Mentor, Honeywell, Yamaha, Speedway, Esurance or Safe Systems** place in us.

Leader in Forrester's inaugural Wave™ for Cloud Workload Security
NSS Labs "Recommended" Rating in the NSS Labs AEP Group Test
SC Media Industry Innovator Award for Hypervisor Introspection, 2nd Year in a Row
Gartner® Representative Vendor of Cloud-Workload Protection Platforms

Dedicated To Our +20.000 Worldwide Partners

A channel-exclusive vendor, Bitdefender is proud to share success with tens of thousands of resellers and distributors worldwide.

CRN 5-Star Partner, 4th Year in a Row. Recognized on CRN's Security 100 List. CRN Cloud Partner, 2nd year in a Row
More MSP-integrated solutions than any other security vendor
3 Bitdefender Partner Programs - to enable all our partners – resellers, service providers and hybrid partners – to focus on selling Bitdefender solutions that match their own specializations

Trusted Security Authority

Bitdefender is a proud technology alliance partner to major virtualization vendors, directly contributing to the development of secure ecosystems with **VMware, Nutanix, Citrix, Linux Foundation, Microsoft, AWS, and Pivotal.**
Through its leading forensics team, Bitdefender is also actively engaged in countering international cybercrime together with major law enforcement agencies such as FBI and Europol, in initiatives such as NoMoreRansom and TechAccord, as well as the takedown of black markets such as Hansa. Starting in 2019, Bitdefender is also a proudly appointed CVE Numbering Authority in MITRE Partnership.

RECOGNIZED BY LEADING ANALYSTS AND INDEPENDENT TESTING ORGANIZATIONS

TECHNOLOGY ALLIANCES

Bitdefender®

Founded 2001, Romania
Number of employees 1800+

Headquarters
Enterprise HQ – Santa Clara, CA, United States
Technology HQ – Bucharest, Romania

WORLDWIDE OFFICES
USA & Canada: Ft. Lauderdale, FL | Santa Clara, CA | San Antonio, TX | Toronto, CA
Europe: Copenhagen, DENMARK | Paris, FRANCE | München, GERMANY | Milan, ITALY | Bucharest, Iasi, Cluj, Timisoara, ROMANIA | Barcelona, SPAIN | Dubai, UAE | London, UK | Hague, NETHERLANDS
Australia: Sydney, Melbourne

UNDER THE SIGN OF THE WOLF

A trade of brilliance, data security is an industry where only the clearest view, sharpest mind and deepest insight can win — a game with zero margin of error. Our job is to win every single time, one thousand times out of one thousand, and one million times out of one million.

And we do. We outsmart the industry not only by having the clearest view, the sharpest mind and the deepest insight, but by staying one step ahead of everybody else, be they black hats or fellow security experts. The brilliance of our collective mind is like a **luminous Dragon-Wolf** on your side, powered by engineered intuition, created to guard against all dangers hidden in the arcane intricacies of the digital realm.

This brilliance is our superpower and we put it at the core of all our game-changing products and solutions.

Bitdefender-PR-Report-Mid2020-crisp14740-en_EN
08/19/20August 20, 2020 2:46 pm08/20/20