White Paper

Bitdefender®

Mid-Year Threat Landscape Report

2019

Contents

Executive summary:

The first half of 2019 brought interesting developments in malware targeting popular operating systems, in hardware and software vulnerabilities affecting consumer and businesses, and in the increased number of attacks aimed at (and even carried out by) IoTs.

With the money motive driving the proliferation of malware, cybercriminals are nothing if not resourceful when developing new malware strands or coming up with more successful attack vectors. The number of malware samples roaming the internet is about to reach the **1 billion**[1] milestone.

"74.23% Ransomware Increase YoY"

The threat landscape has also evolved to the point where some major threat categories, all financially motivated, dominate the market. For example, **ransomware has increased by 74.23 percent**[2] **YoY** (year-over-year), according to a comparison of Bitdefender telemetry reports from H1 2018 with reports from H1 2019.

While popular ransomware families, such as **GandCrab**, have closed shop after generating more than **$2 billion**[3] in about 18 months of activity, spinoff ransomware families seem to have filled in the gap. Sodinokibi (aka REvil or Sodin) is one example that has quickly gained popularity in recent ransomware campaigns, focusing on specific industry verticals. Targeting large organizations, educational institutions and critical infrastructures, with a particular focus on the United States, ransomware remains a lucrative business that constantly adapts its business model, techniques and sophistication.

The fall of GandCrab, which dominated the ransomware market with a share of over 50 percent, has left a power vacuum that various spinoffs are quickly filling. **This fragmentation can only mean the ransomware market will become more powerful and more resilient against combined efforts by law enforcement and the cybersecurity industry to dismantle it.**

Seemingly benign threats that we tag ass **PUA (Potentially Unwanted Applications),** have also made quite an interesting mark on the first half of 2019, accounting for **over 79 percent of the top global Windows threat reports.**

Tagged as grayware, PUA now walks a fine line between malware and legitimate adware services. Recent Bitdefender investigations reveal three advanced adware campaigns that could put some spyware to shame. Zacinlo, Scranos, and IsErIk pack unique features that even enable rootkit capabilities, enabling attackers to fully manage infected systems.

The numbers of both software and hardware vulnerabilities made headlines during the first half of 2019. Over **27.86 percent**[4] **of all reported vulnerabilities were tagged as high or critical**, with a CVE score above 7.0. Impacting Intel chips going back as far as 2012, Bitdefender researchers found new vulnerabilities enabling attackers to exfiltrate information without leaving any traces within the operating system. Businesses and datacenters that run infrastructures based on Intel's vulnerable CPUs have limited mitigation options, and replacing vulnerable hardware or disabling hyperthreading are not options.

"27.86% of reported vulnerabilities tagged as high or critical"

More than **41.6 billion**[5] **connected IoT devices** are estimated to be on the market by 2025, generating over 79.4 zettabytes (ZB) of data. Since more than 22 billion [6] IoTs are currently connected to the internet, most of them sporting vulnerabilities that can be remotely exploited by threat actors to take control over them, a sufficiently large botnet can be amassed and used to take down infrastructures. If Mirai [7] has taught us anything, it's that seemingly benign IoTs can disrupt a country's entire internet infrastructure, potentially inflicting billions in financial losses due to internet connectivity disruptions.

[1] **AV-TEST**. https://www.av-test.org/en/statistics/malware/

[2] **Bitdefender, "Global Mid-Year Threat Landscape Report 2018"**. https://download.bitdefender.com/resources/files/News/CaseStudies/study/235/Bitdefender-2018-Global-Mid-Year-Threat-Landscape-Report.pdf

[3] **ZDNet, "GandCrab ransomware operation says it's shutting down"**. https://www.zdnet.com/article/gandcrab-ransomware-operation-says-its-shutting-down/

[4] **CVE Details**. https://www.cvedetails.com/

[5] **IDC, The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast.** https://www.idc.com/getdoc.jsp?containerId=prUS45213219

[6] **Strategy Analytics, Inc., Connected Home Devices (CHD) service, Global Connected and IoT Device Forecast Update.** https://news.strategyanalytics.com/press-release/iot-ecosystem/strategy-analytics-internet-things-now-numbers-22-billion-devices-where

[7] **Wikipedia**. https://en.wikipedia.org/wiki/Mirai_(malware)

The economic impact of disruptive cyber attacks might be enormous if we take into account, for instance, only the employers' expenses in the service industry caused by a potential Internet connection drop. If all employees in the service sector in the European Union suffer an Internet connection drop for just one working hour, the loss to the EU economy would climb into the billions of euros, according to our estimates.

With an **average hourly labor cost of 27.4 euros**[8] in 2018 in the EU and almost **90 million**[9] **employees** in the service industry in the 28 EU countries, **an hour without Internet would cost the EU economy almost 2.5 billion euros**, while the losses for an eight-hour working day would reach approximately 20 billion euros.

The number of **Android threat reports increased 39.31 percent** in H1 2019 from H1 2018, showing that threat actors are stepping up efforts to compromise Android devices. Since most devices are shared between personal and business tasks and activities, malware infections can endanger not just personal data and information, but also corporate data including sensitive emails and even intellectual property data.

> **"49%**
>
> of information security professionals worry about the readiness of their organization to deal with such attacks"

In light of the evolving threat landscape, malware diversification, and the potential financial impact on business of a data breach or attack, a Bitdefender survey revealed that **49 percent**[10] of information security professionals worry about the readiness of their organization to deal with such attacks.

In this report, Bitdefender covers some of the most common cyber threats in today's digital landscape, while offering and interpreting telemetry and threat intelligence reports from our consumer and enterprise business lines.

Ranging from threats specifically targeting Microsoft's Windows, Apple's Mac (macOS), and Google's Android mobile operating system, to threat intelligence from our honeypots and various IoT sensors, this report aims to offer a comprehensive view of what threats target users and large enterprises.

Key Takeaways

- 74.23 percent increase in ransomware reports YoY
- Ransomware ranks first in YoY threat reports, with 2019 threats diversifying to include exploits, Trojans, Fileless, coin miners and Trojan bankers
- Ransomware market fragmentation leads to new ransomware families, which means they're more resilient to takedowns by law enforcement and cybersecurity vendors.
- Up to 2.5 billion euros an hour in financial losses for the EU economy, should internet infrastructures be taken offline for a single hour by IoT botnets causing DDoS attacks
- 49 percent [11] of security professionals lose sleep worrying about their organization's cybersecurity
- 48 percent average increase in the global volume of spam

[8] **Eurostat, Labour costs annual data - NACE Rev. 2.** https://ec.europa.eu/eurostat/databrowser/view/tps00173/default/table?lang=en

[9] **Eurostat, Employment by A*10 industry breakdowns**. http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=nama_10_a10_e&lang=en

[10] **Bitdefender, "Hacked Off! Study"**. https://www.bitdefender.com/files/News/CaseStudies/study/285/Bitedefender-Hacked-Off-Report.pdf

[11] **Bitdefender, "Hacked Off"**. https://www.bitdefender.com/files/News/CaseStudies/study/285/Bitedefender-Hacked-Off-Report.pdf

Threats Going After the Average User

Scrolling through the cybersecurity headlines of 2019, it's not hard to discern the top threats looming over businesses and consumers alike. While most reports involve ransomware attacks on critical infrastructures – a rapid shift from past-years' spray-and-pray attacks on targets big and small – most malware deployed by cybercriminals globally is of an altogether different nature.

The first half of 2019 saw a considerable spike in deployment of **PUA** (Potentially Unwanted Applications), targeting both Windows and Mac users. In fact, PUA is one of the most prominent threats targeting the latter group. PUAs can compromise privacy or weaken the computer's security in a variety of ways, some more dangerous than others. Shady software developers and distributors may bundle a wanted program download with a wrapper designed to install an unwanted app. In many cases, the user has no clear opt-out mechanism, or the PUA installation isn't expressly stated.

Coin-mining malware used in cryptojacking campaigns remains common. Despite the shutdown of various 'legitimate' mining services like the infamous CoinHive, in 2019 we still encounter many websites rigged with coin-mining code. We also see continued efforts involving internal threat actors – actual employees using the computing power found in their workplace to mine crypto cash. In one such notable incident, workers at a nuclear power plant in Ukraine (including the security guards) were caught mining digital currency using the plant's computing hardware.

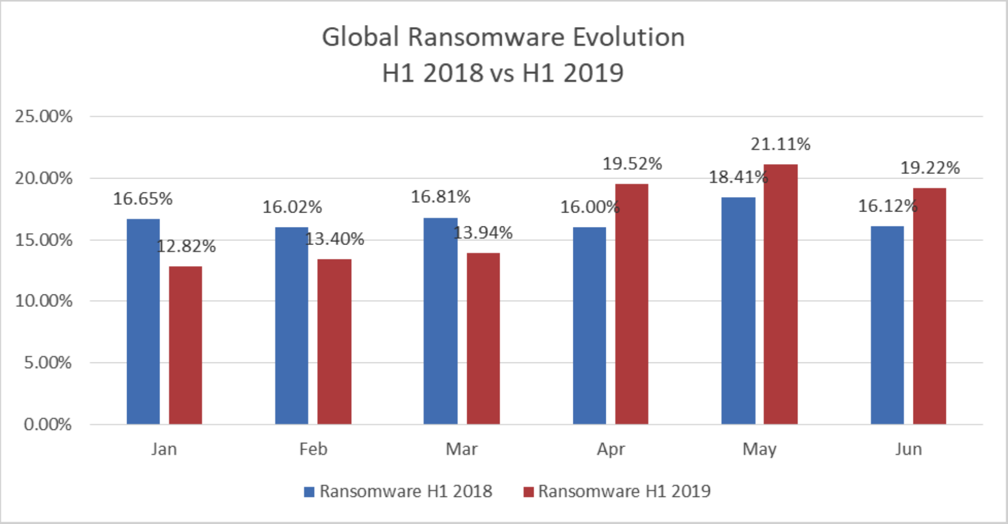
Exploits leveraging unpatched or previously-unknown vulnerabilities remain a top threat in the Windows ecosystem. Unpatched flaws have historically been the go-to vector for hackers, and 2019 is no different.

Fileless attacks and **Banking Trojans** finish last on our top-six threat list, but that doesn't make them any less dangerous: the less attention it gets from security telemetry, the more targeted and profitable the attack for those behind the Command & Control server.

With over 350,000 new threats emerging every day – and that's against just Windows - the number of malware samples is estimated to pass the milestone of 1 billion by the end of 2019. While the number of macOS malware samples may not be nearly as high as that of Windows threats, its sophistication and impact mustn't be underestimated. Password-stealing Trojans, cryptocurrency miners, and even aggressive adware are to be taken seriously, as they can impact not just the performance and usability of your Mac, but also your data and even financial well-being.

Windows Threat Landscape at a Glance

When looking at the global evolution of threats, we've analyzed five categories, ranging from ransomware, coin miners, and fileless to PUA, exploits and banking Trojans. During the first half of 2019, the number of ransomware reports was slightly lower than during the first half of 2018, but this is likely a direct result of GandCrab operators throttling down their operation after announcing their cease and desist.



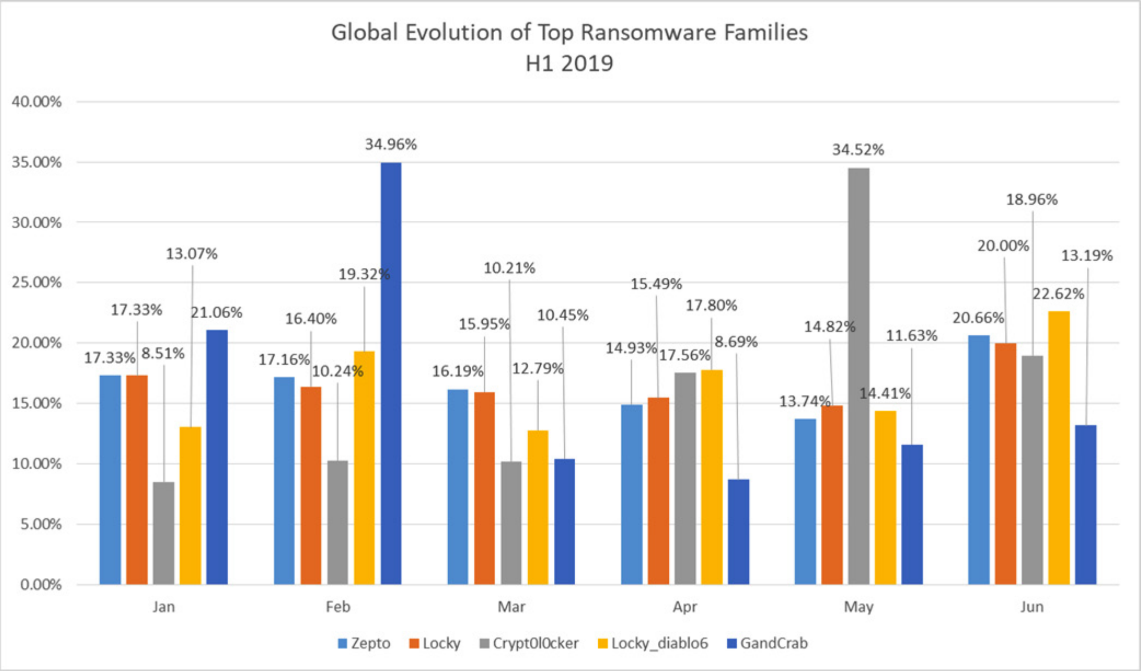
However, during the second of half of 2019, ransomware reports have intensified, potentially as a direct result of new ransomware families that emerged to fill the void left by GandCrab. While new ransomware families, such as Sodinokibi (aka REvil or Sodin), and many others, may have not grown as dominant as CanGrab, they have successfully been adopted by the threat actor community. As a result, the number of ransomware reports increased by 64.66 percent (8.29 percentage points) in May 2019 compared to January 2019, an ascending trend that started in April and is likely to continue through the end of 2019.

However, if we look at the evolution of the top ransomware families on a monthly basis during the first half of 2019, it becomes clear that GandCrab has lost a lot of its huge market share. Interestingly, we can also spot an increase in the number of reports for other ransomware that have picked up on the power void left behind by GandCrab.

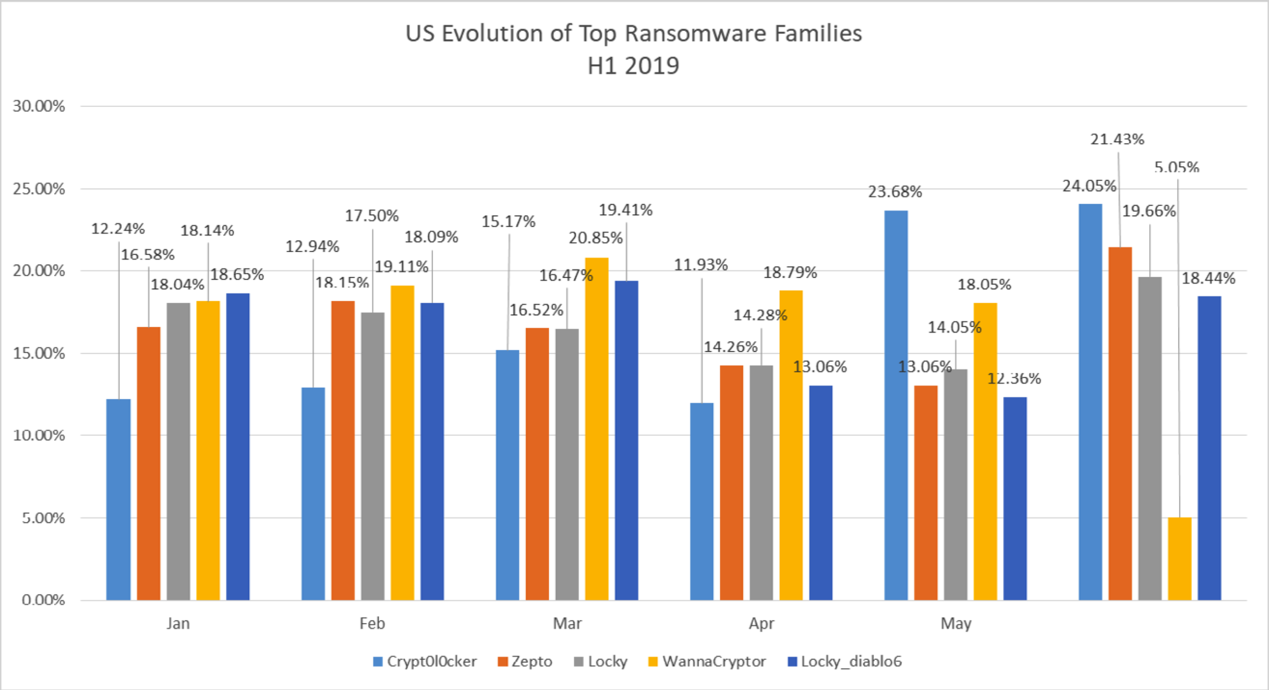
While we limited out telemetry to the 5 most popular ransomware families, the same trend has been spotted with less popular ones. Cybercriminals may have reverted to previously known ransomware families to continue their campaigns as an equally business-oriented and affiliation-based ransomware family fills in the gap left by GandCrab operators.

Evolution of top Ransomware Families

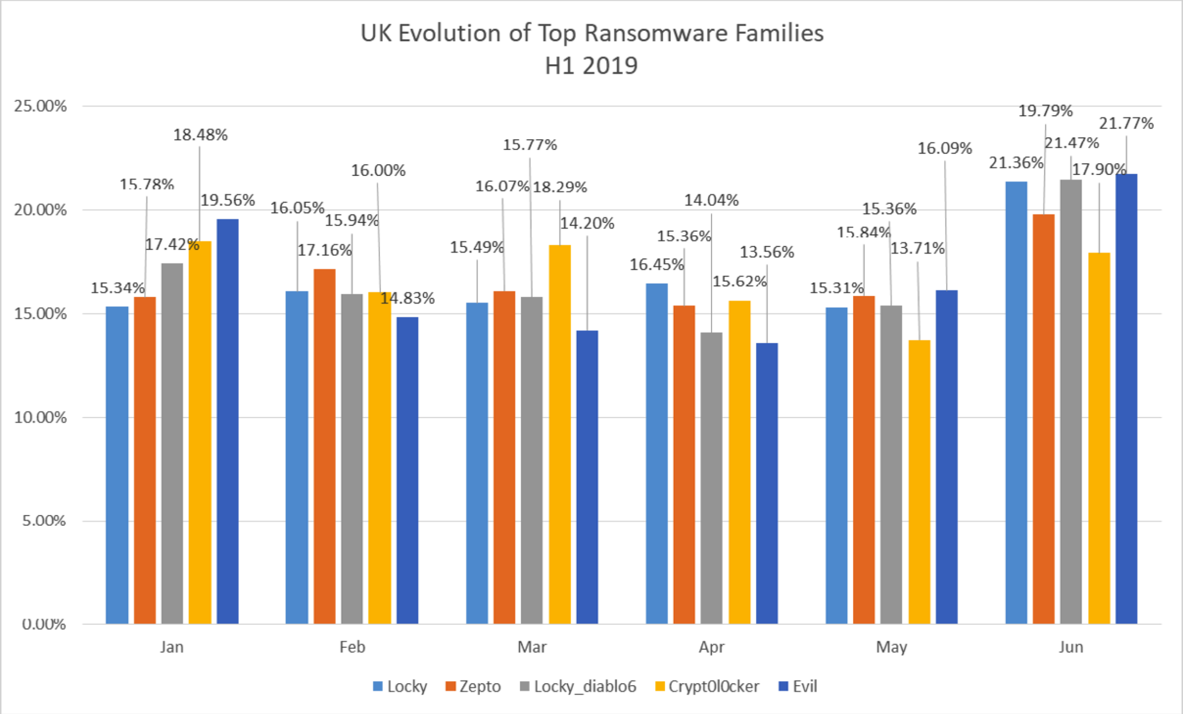
Global



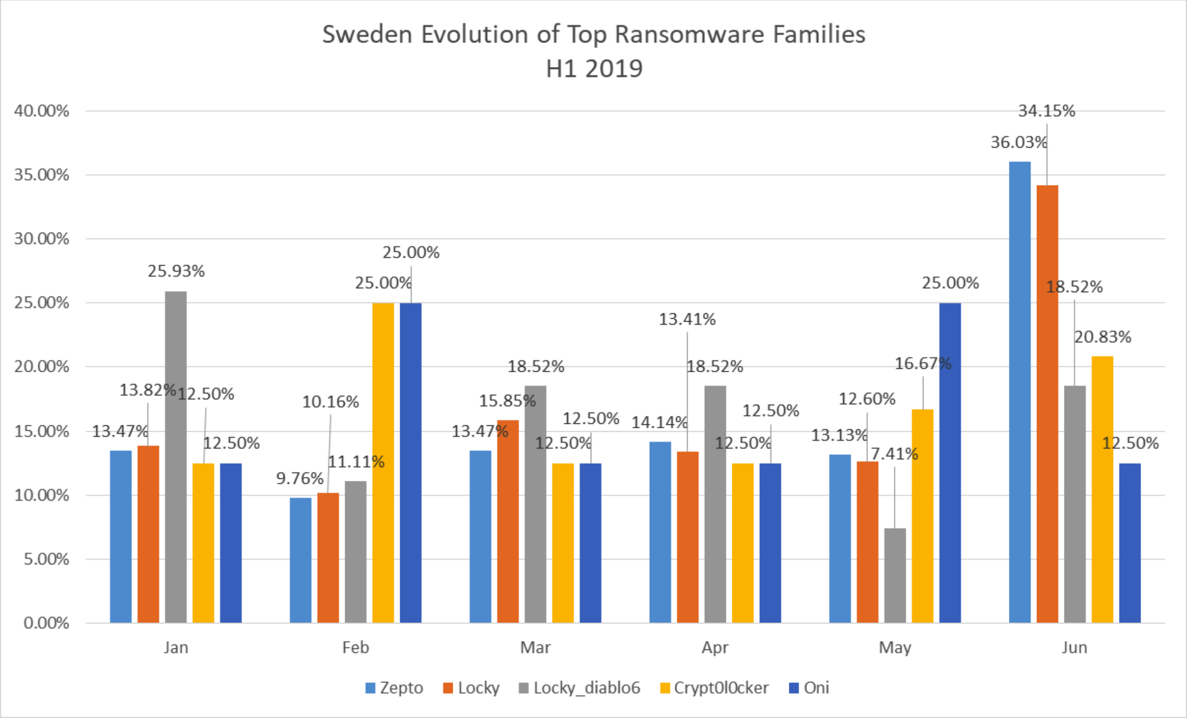
United States



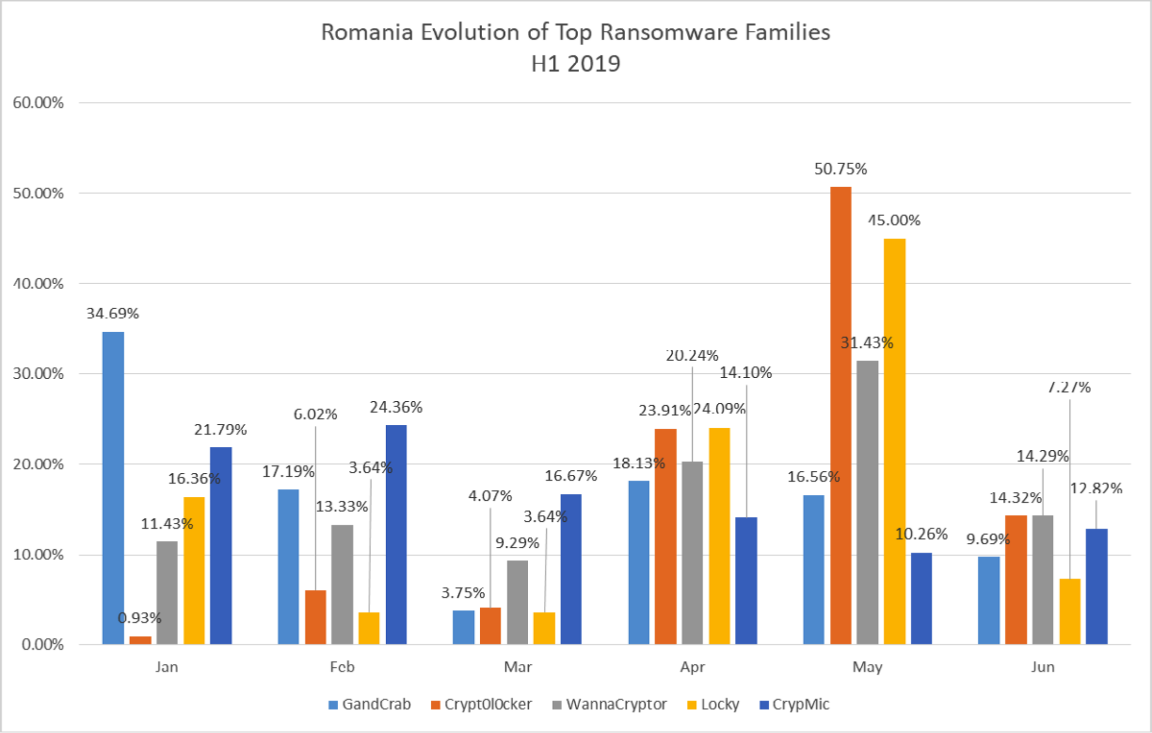
United Kingdom



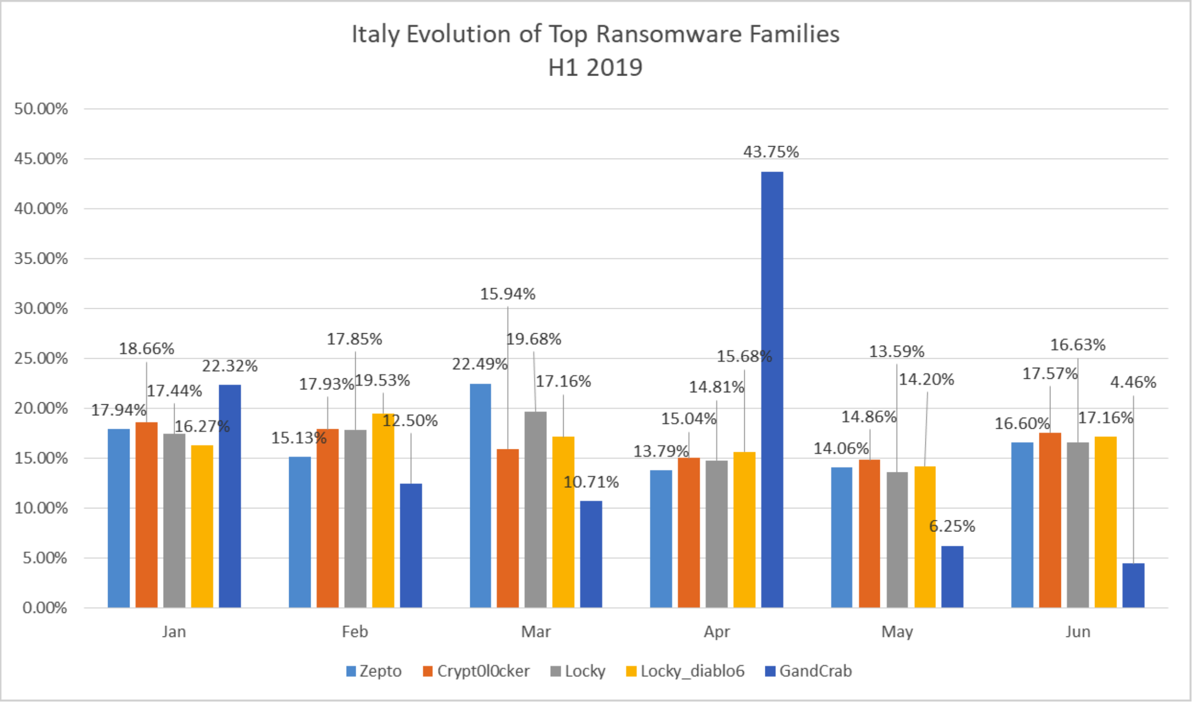
Sweden



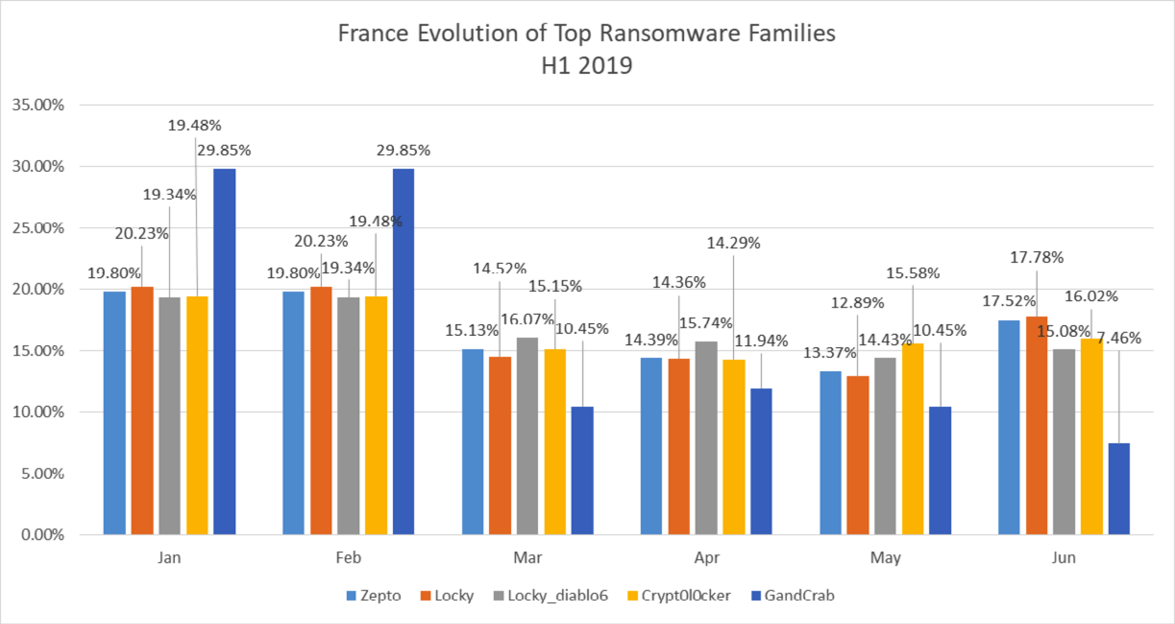
Romania



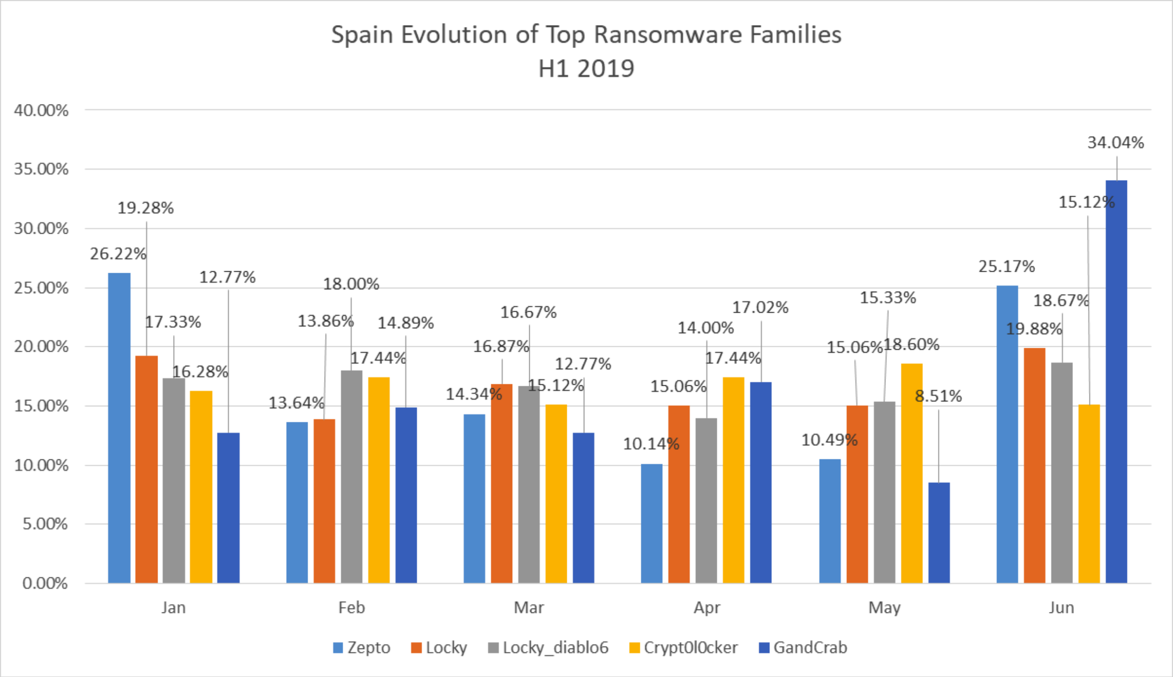
Italy



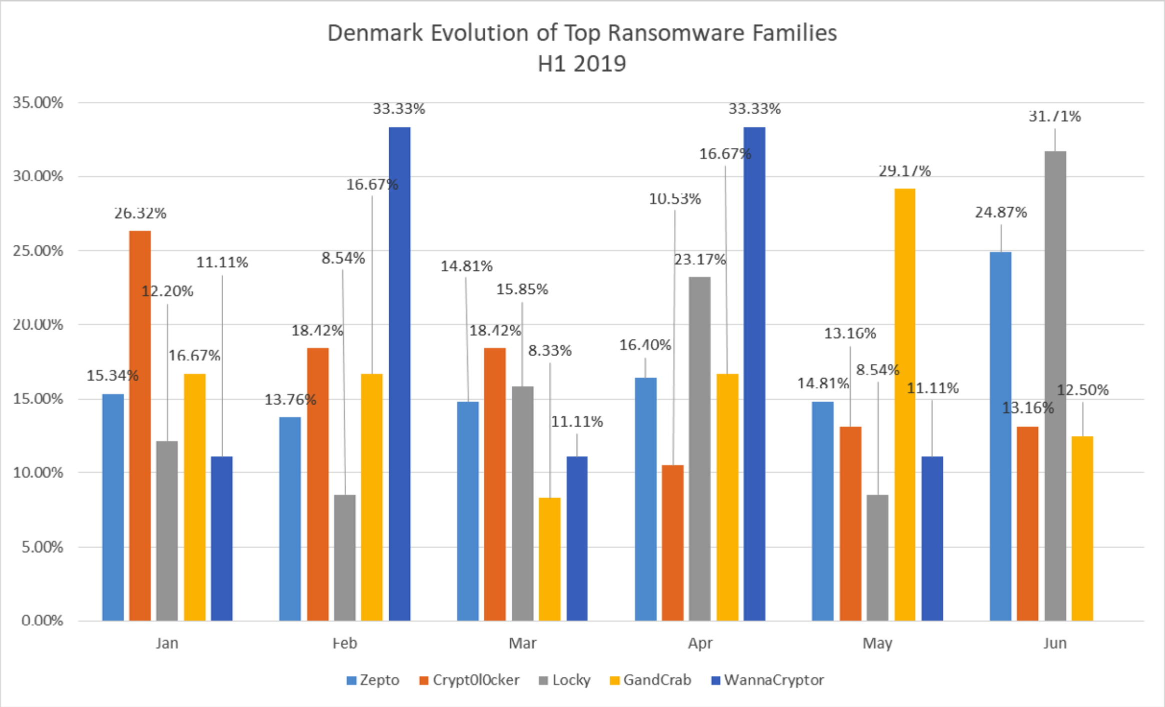
France



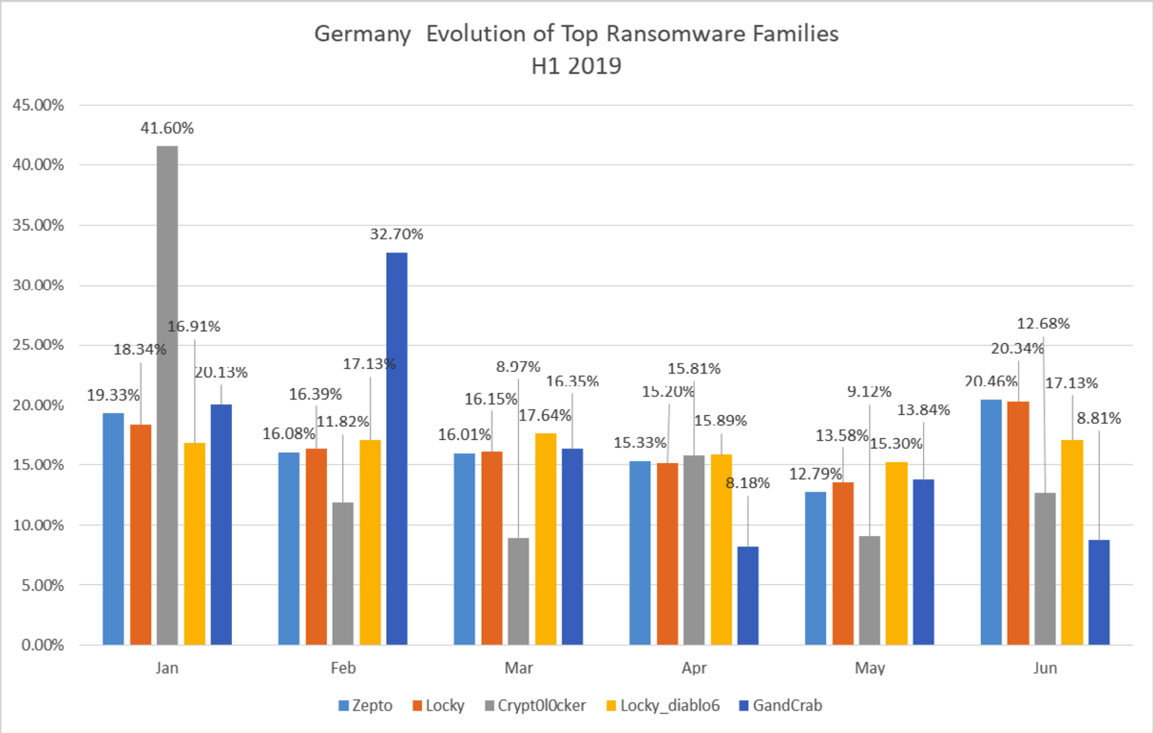
Spain



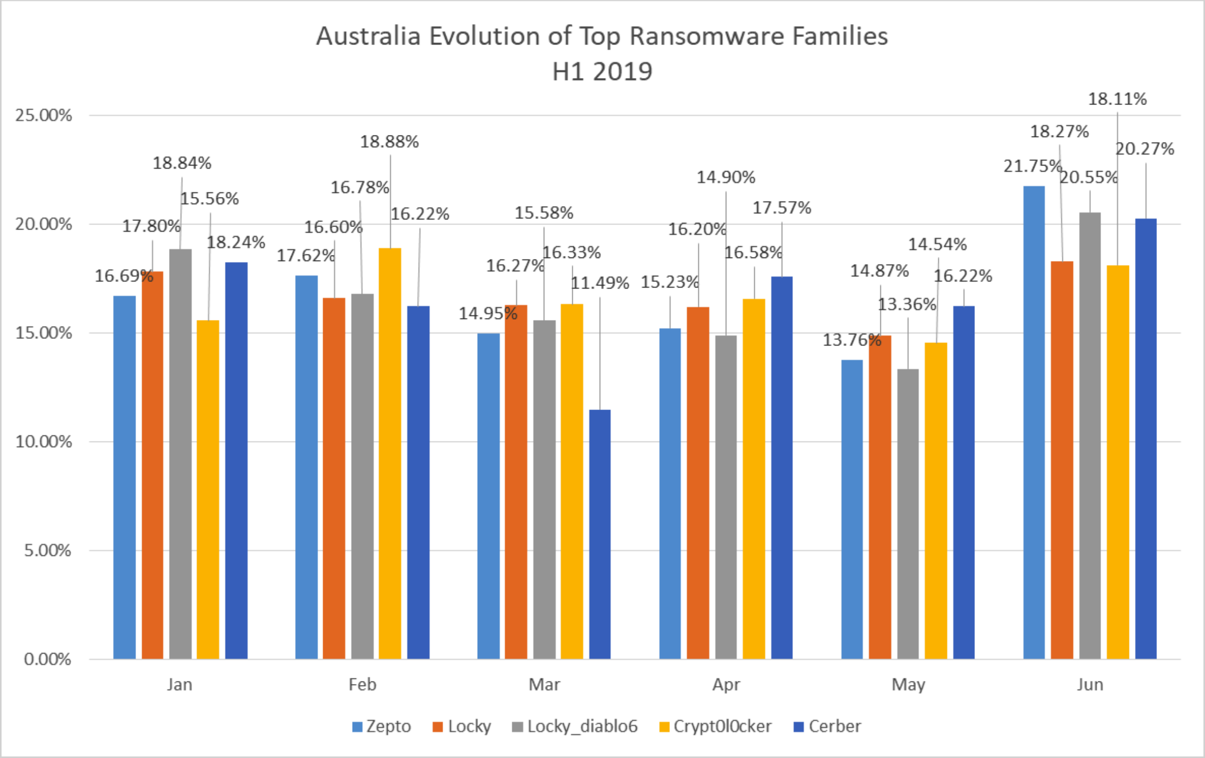
Denmark



Germany

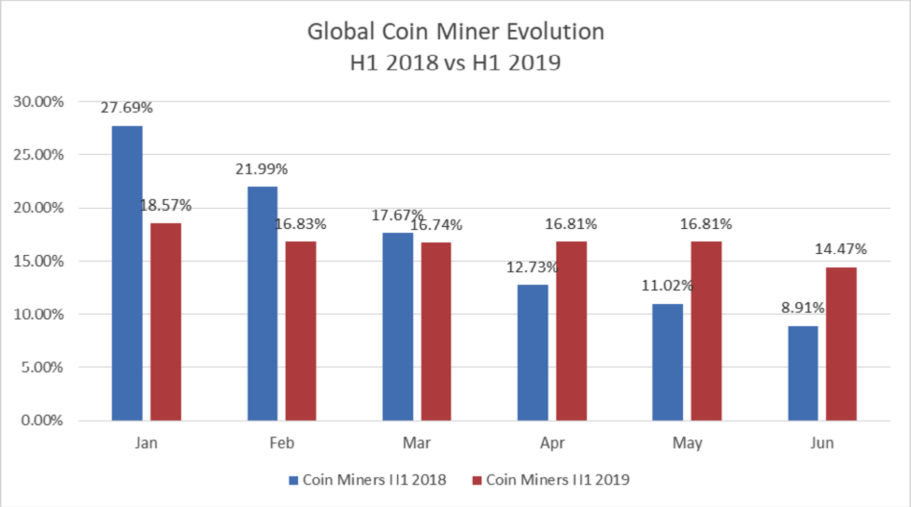


Australia


Australia Evolution of Top Ransomware Families
H1 2019
25.00%
20.00%
15.00%
10.00%
5.00%
0.00%
16.69%
17.80%
18.84%
15.56%
18.24%
17.62%
16.60%
16.78%
18.88%
16.22%
14.95%
16.27%
15.58%
16.33%
11.49%
15.23%
16.20%
14.90%
16.58%
17.57%
13.76%
14.87%
13.36%
14.54%
16.22%
21.75%
18.27%
20.55%
18.11%
20.27%
Jan
Feb
Mar
Apr
May
Jun
Zepto
Locky
Locky_diablo6
Crypt0l0cker
Cerber

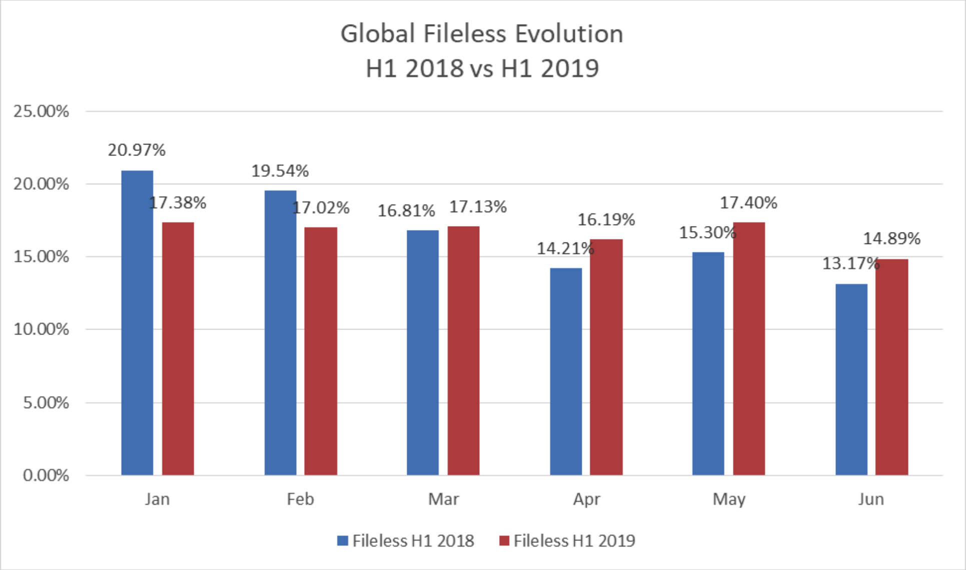
The evolution of coin miners somewhat plateaued during the first half of 2019, potentially pointing to interest from threat actors in using it as an alternative for generating profit. If during the first half of 2018 coin miners were on a descending path, in 2019 coin miner reports showed only slight variations.

Evolution of Coin Miners, Fileless malware, Bankers, and PUA



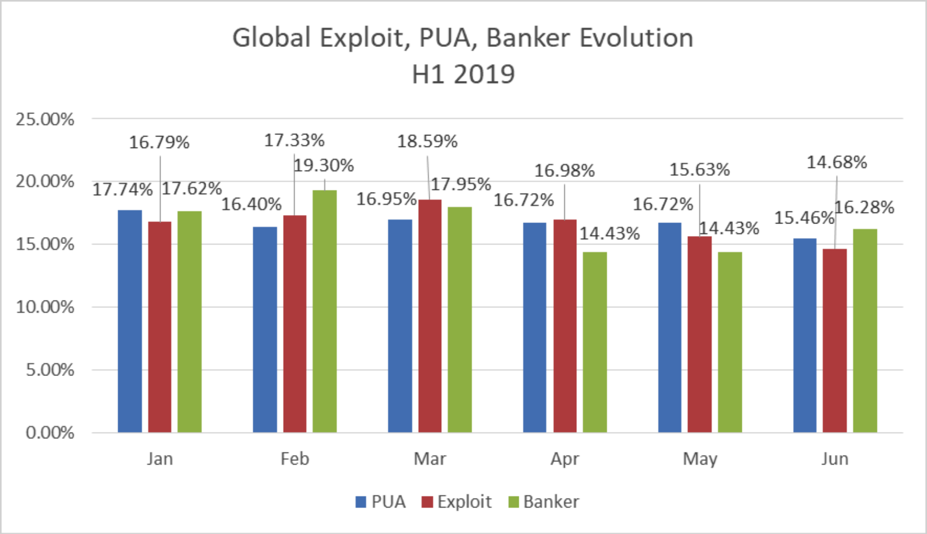
With cybercriminals intrinsically motivated by profit – and as a result investing time and effort in building threats that find alternatives ways of providing that – cryptocurrency miners are not likely to go away any time soon, very much in line with 2019 cybersecurity predictions

.



During the first half of 2018, fileless malware was mostly on a descending trend, but year-over-year reports indicate that that cybercriminals have made better use of it in 2019. Fileless malware reports have been consistent throughout the first half of 2019, registering a slight drop of 2.51 percentage points in June, compared to May.

In 2019, we've also started seeing increased activity among three other threats: exploits, PUA, and banking Trojans. Interestingly, their evolution seems to have been somewhat consistent throughout the first six months of 2019, each showing minimum fluctuations in terms of percentage points.

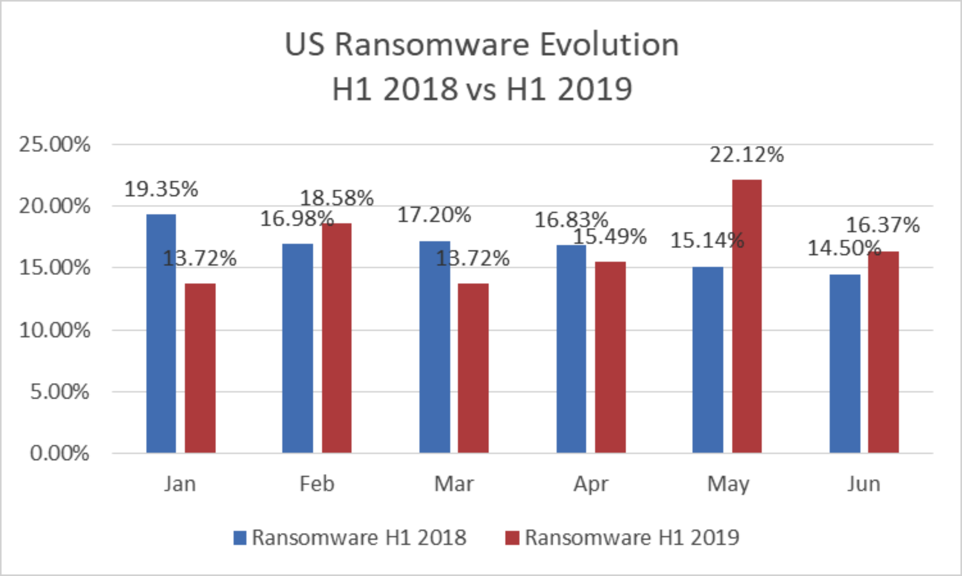


For instance, from 17.74 percent in January - of all PUA reports during H1 2019 – by June it only dropped by 2.28 percentage points. The number of reported exploits seems to have also remained somewhat constant, reaching a peak in March of 18.59 percent – of all exploits reported during 2019 – and a low of 14.86 percent in June.

While banking Trojans may have been around for the better part of a decade, the number of reports seems to suggest that cybercriminals still find it lucrative. With February registering the highest activity in terms of reports (19.30 percent – of all banking Trojan reports during H1 2019), the largest drop in terms of percentage points (4.87 percentage points) was registered during April and May.

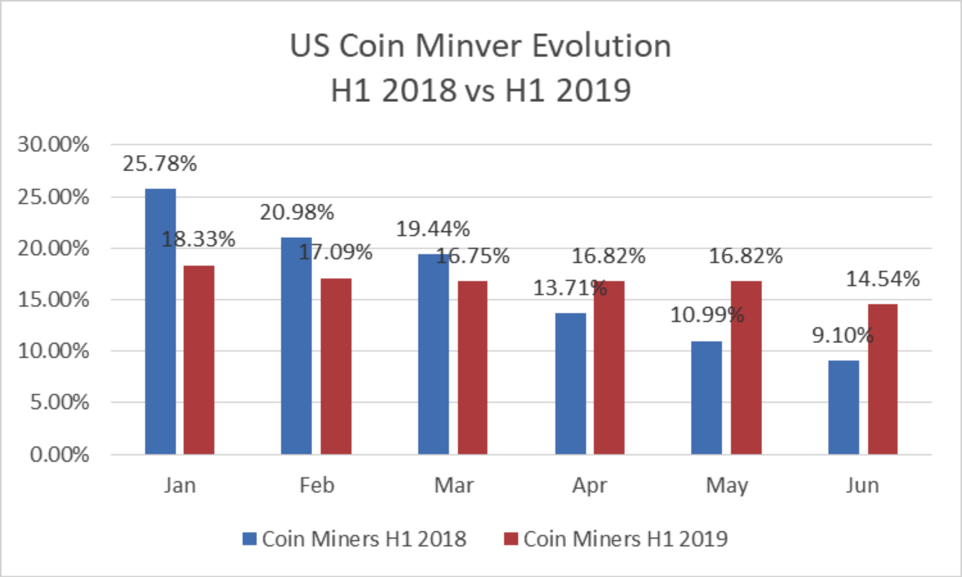
United States

Ransomware evolution in the US follows the global trend, with the first quarter of 2019 showing a drop in the number of reports caused by the GandCrab market fluctuation, only to spike back up again in May. Consequently, 22.12 percent of all ransomware reports in the US within the first half of 2019 were reported in May.



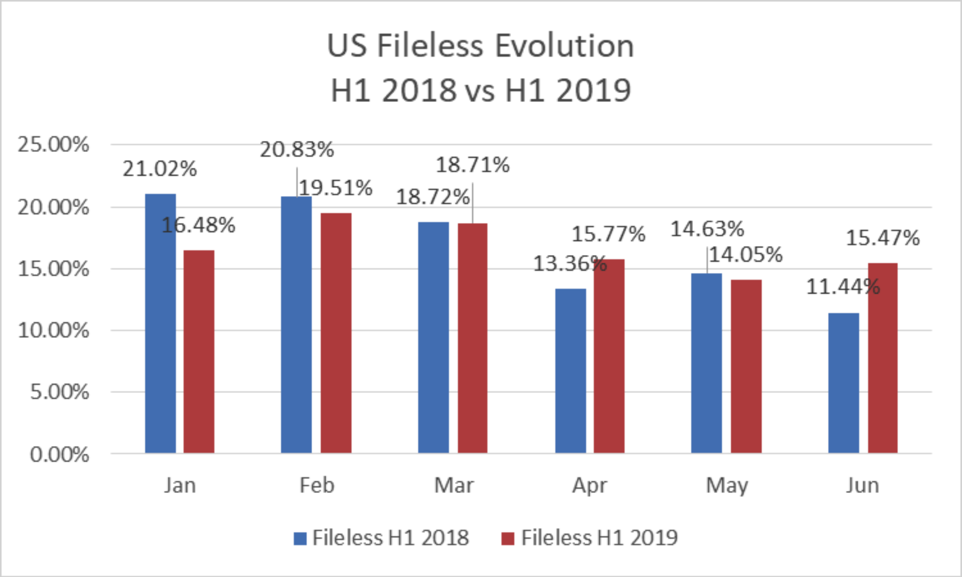
While ransomware reports were also high in February and June of H1 2019, these recent stats only strengthen the conclusion that the ransomware industry took a couple of months to stabilize. With US being one of the countries taking the brunt of ransomware attacks, it's safe to assume that local threat landscape trends will reflect global ones.

Coin miner reports in the United States also plateaued after a descending curve in the first half of 2018. While January registered 18.33 percent of the total number of coin miner reports in H1 2019, reports dropped only by 3.79 percent by June 2018.



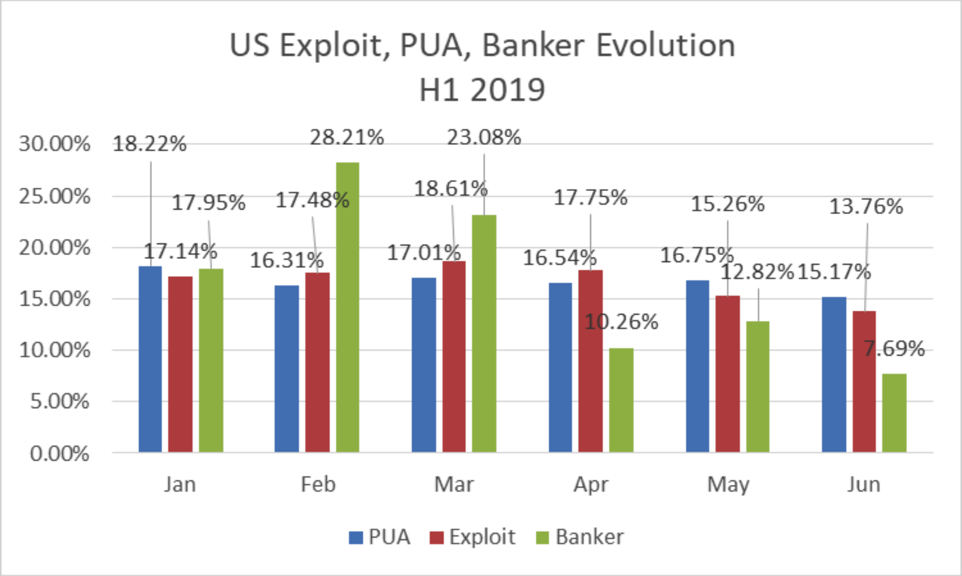
Alternatively, during the same timeframe in 2018, coin miner reports dropped from January's 25.78 percent - of all reports during H1 2018 - to 9.10 percent in June, which translates into a drop of 16.68 percentage points.

Fileless malware, the third most popular threat in 2018, also saw an increase in the number of reports in the US in 2019. During the first half of 2018, fileless reports fluctuated by 9.58 percentage points, but in the same timeframe in 2019 it fluctuated only by 5.46 percentage points.



The stats above also show that fileless reports also picked up during the second quarter of 2019. This was perhaps fueled by the increase of ransomware and coin miner reports, as fileless malware is usually a preferred delivery mechanism.

Exploits, PUA, and banking Trojans were also popular in the United States in the first half of 2019, while the latter seems to have spiked during February and March. Trojan bankers in February accounted for 28.21 percent – of all Trojan banker reports in H1 2019 – while March seems to have been equally prolific, with 23.08 percent.

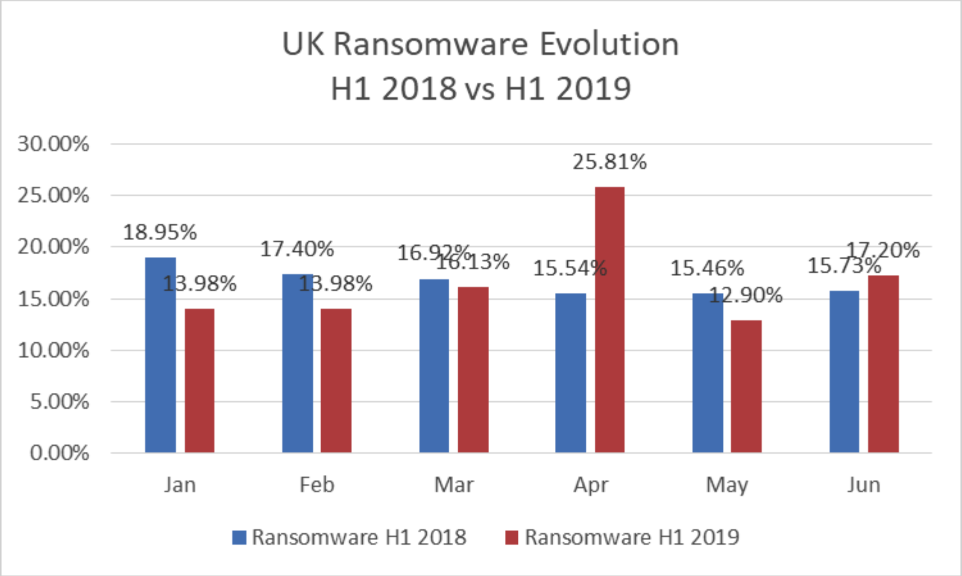


Exploit use via webpages and other delivery mechanisms was also steady throughout the first six months of 2019, with reports fluctuating by only 3.99 percent. As the above stats seem to indicate, web-based exploit kits still seem to remain a popular and serve as low-hanging fruit for cybercriminals. It requires minimal effort to acquire and deploy, while potentially yielding great results on unpatched victims.

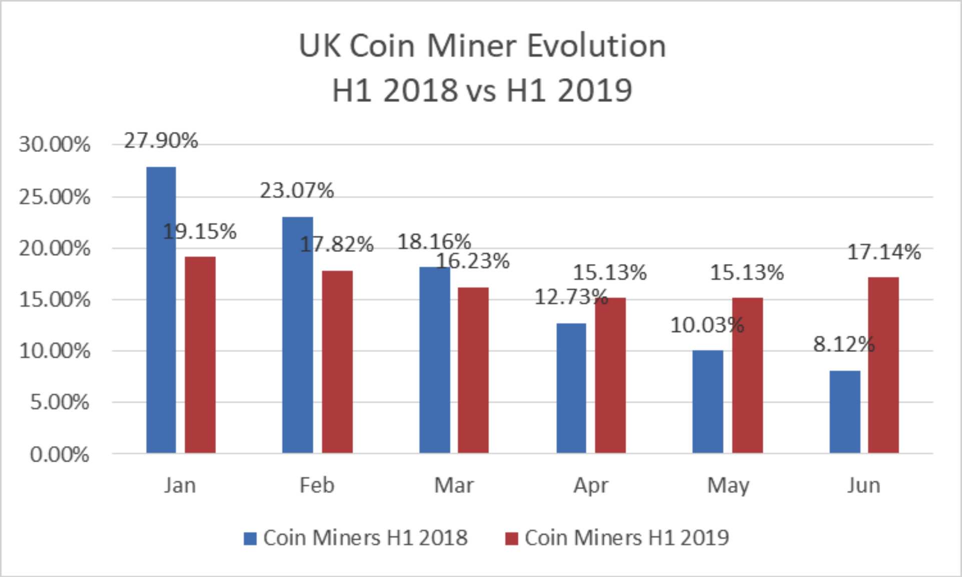
Although potentially unwanted applications walk a fine line between legitimate and malicious, they remain a constant privacy and sometimes even security threat to users. It can collect too much personal information, bombard users with ads, change default search engines, and even sometimes act as backdoors, and the US seems to have its share of it. With reports in the US remaining constant through the first half of 2019, users are strongly advised to carefully read privacy agreements and read EULAs before quickly clicking "Next" while installing new applications on their Windows devices.

The United Kingdom

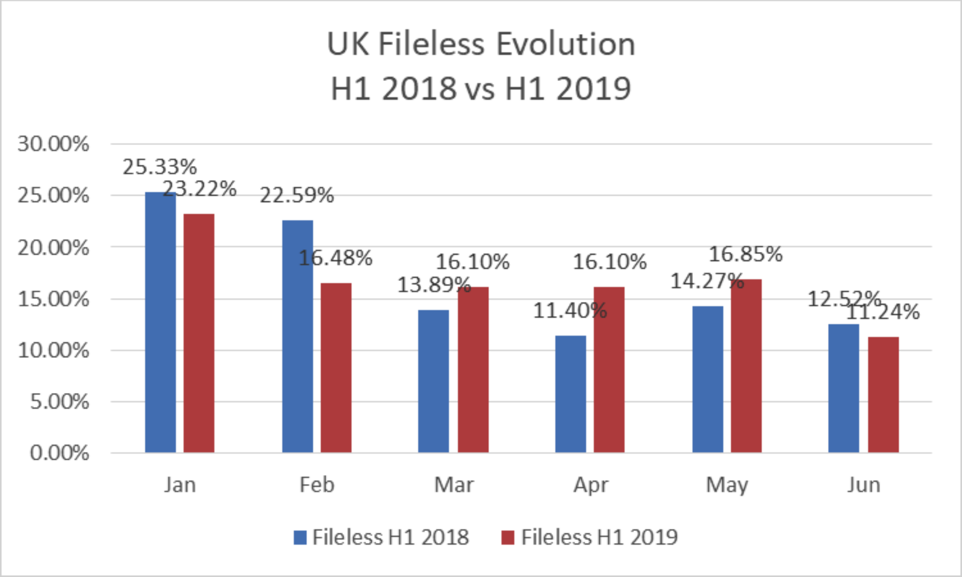
Year-over-year ransomware reports on the United Kingdom seem to follow the same trends, with April 2019 being the only exception. With April clocking in more than 25.81 percent of all ransomware reports in the UK during the first half of 2019, June seems to come in second with 17.20 percent.



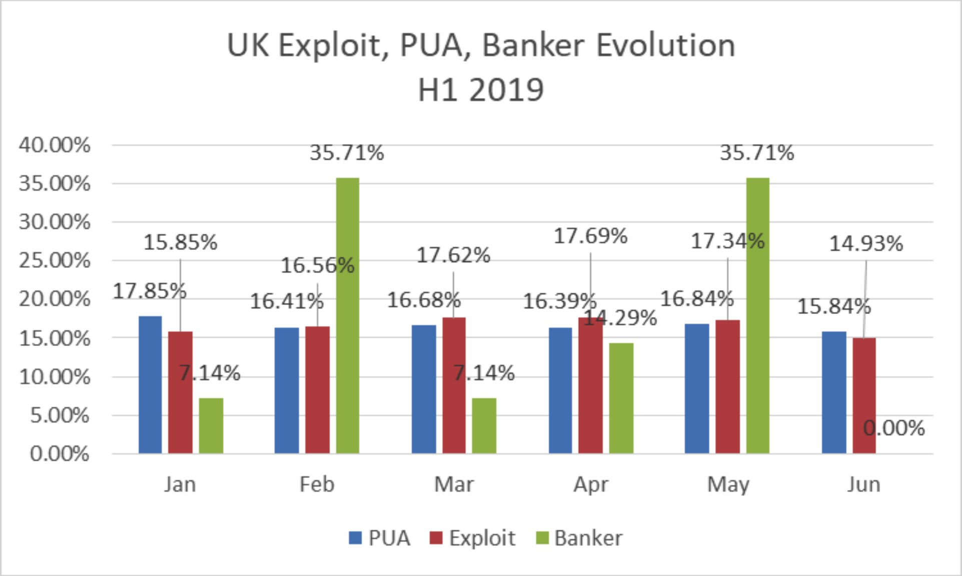
Coin miners in the UK appears to have been more popular with threat actors, as the number of reports from April to June 2019 seem significantly higher than those of 2018. If 2018 showed a steeply descending curve in reports from January towards June, coin miner reports in 2019 remained somewhat constant, with a January high of 19.15 percent – of all coin miner reports in the UK during H1 2019 – and a low of 15.13 percent in both April and May.



Fileless malware reports also showed more consistency during the first half of 2019 in the UK, as reports seem to have fluctuated less wildly than the same timeframe during 2018. With an 11.98 percentage point difference between January and June, cybercriminals seem to have been leveraging fileless malware more frequently in 2019.



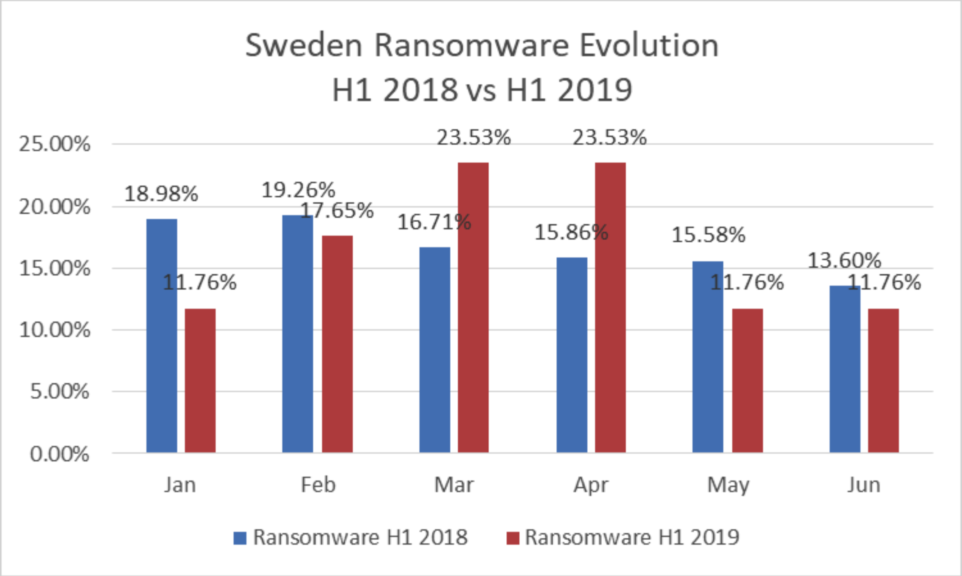
As for the evolution of exploits, PUA, and banking Trojans in the UK, threat actors seem to have been using banking Trojans as a weapon of choice. With February clocking in at 35.71 percent – of the total number of banking Trojans in the UK during H1 2019 – and May at 35.71 percent, this seems to have been one of the most fluctuating threats.



Exploits and potentially unwanted applications in the UK seem to have been following the same trends, as both only fluctuated slightly. Since PUA resides more in the grayware area in terms of threats, it's worth nothing that exploit kits also seem to have been popular in delivering other types of malware.

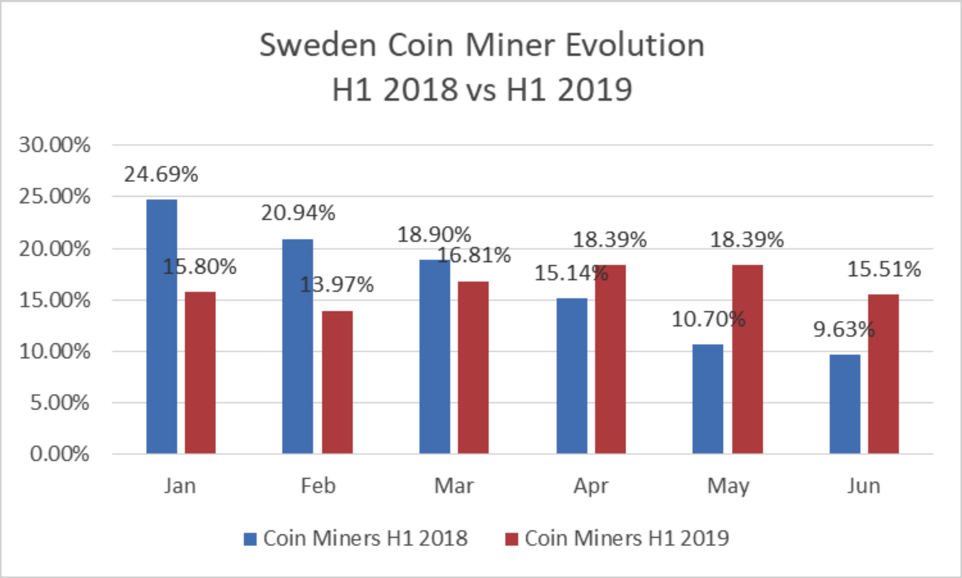
Sweden

Ransomware in Sweden during the first half of 2019 seems to have spiked during March and April, indicating that some campaigns might have been active at the time. While during the first half of 2018 ransomware reports seem to have had the same descending path as in other countries, during 2019 it seems that cybercriminals might have experimented with new ransomware families shortly after the fall of GandCrab.

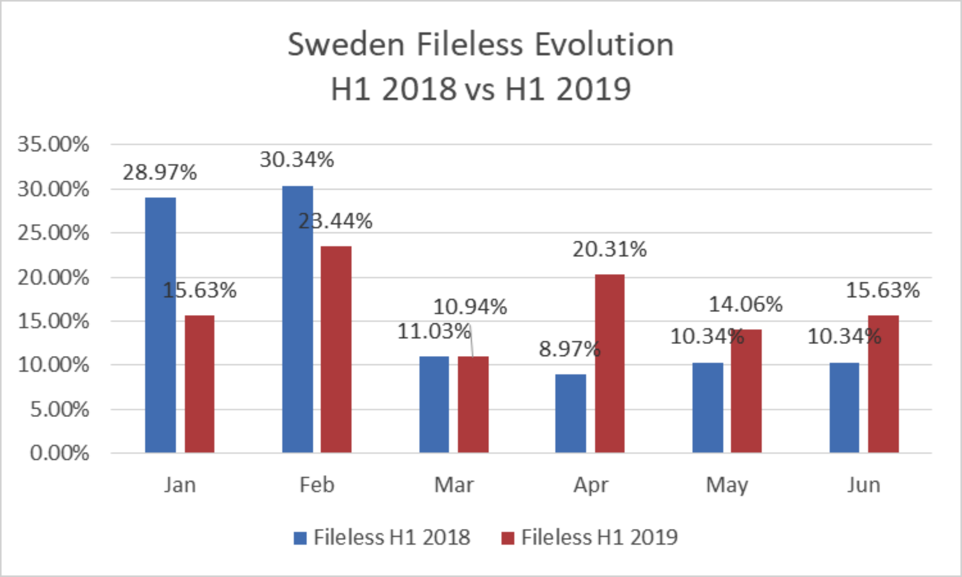


Clocking in at 23.53 percent – of all ransomware reports in Sweden during H1 2019 – both March and April registered the same percentages.

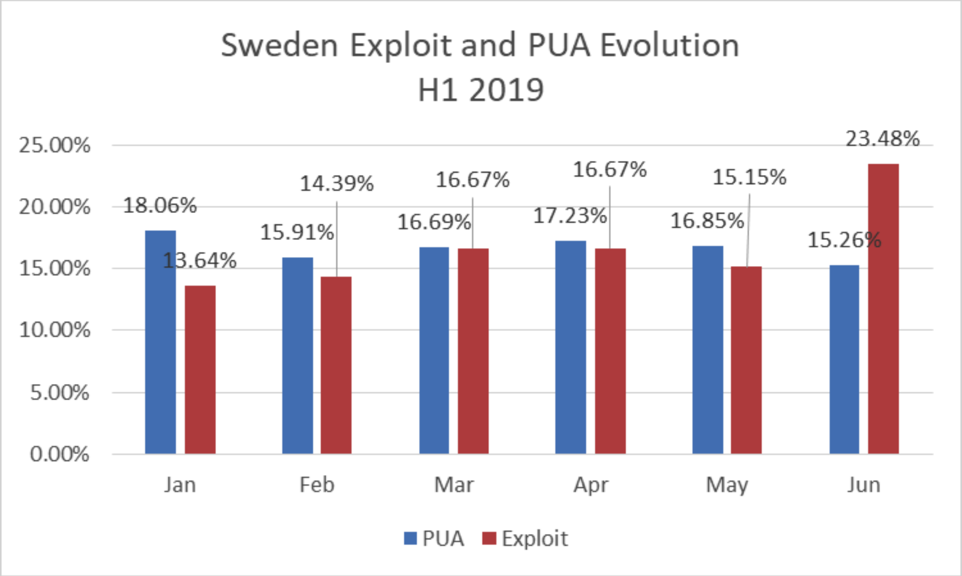
Coin miners on the other hand were more popular during April, May and June, in direct contrast with the H1 2018 trend. Clocking in at 18.39 percent – of all coin miner reports in Sweden during H1 2019 – both April and May seem to have registered peak activity.



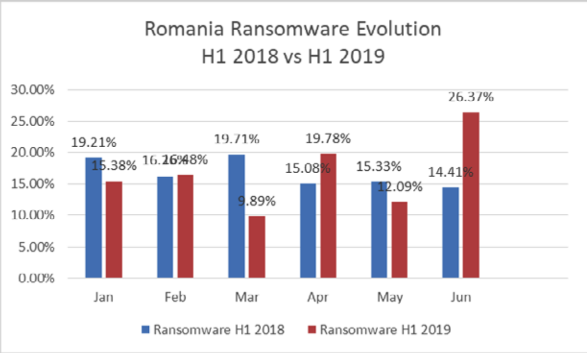
Interestingly, fileless reports in Sweden seem to differ from global trends. Reports during both January and February 2018 and 2019 seem to have been at their highest, while following the same exact evolution trend year-over-year. The only spike in fileless 2019 reports seems to have been registered during April, clocking in at 20.31 percent of all fileless reports during H1 2019.

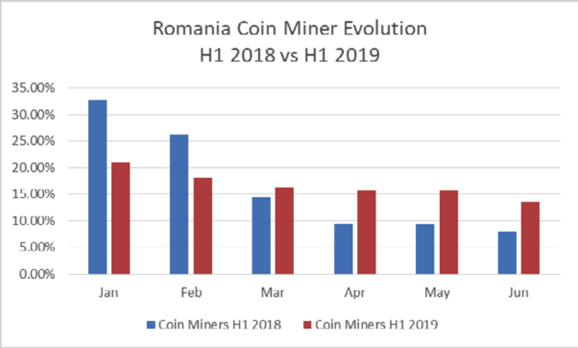


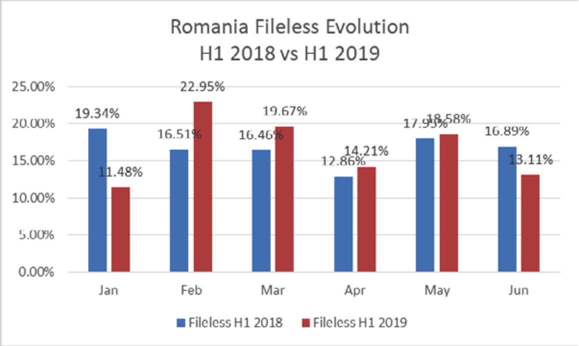
Exploit reports in Sweden remained fairly constant throughout the first half of 2019, with one major spike registered in June, with 23.48 percent of all reports during H1 2019. The steady number of PUA reports also seems to indicate that Swiss users need to pay more attention to reading terms of service, license agreements, or constantly clicking “Next” when installing applications, as they can pack much more than meets the eye.

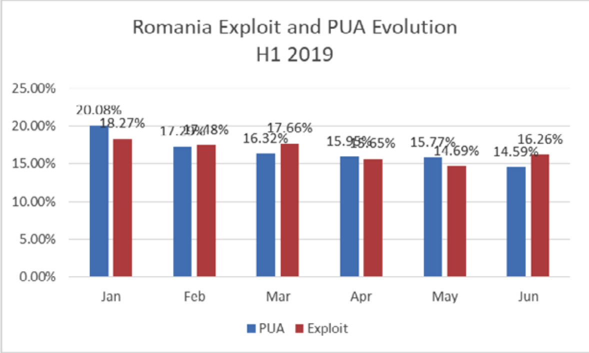


Romania

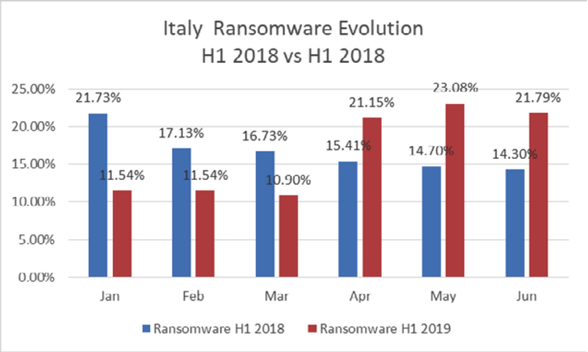


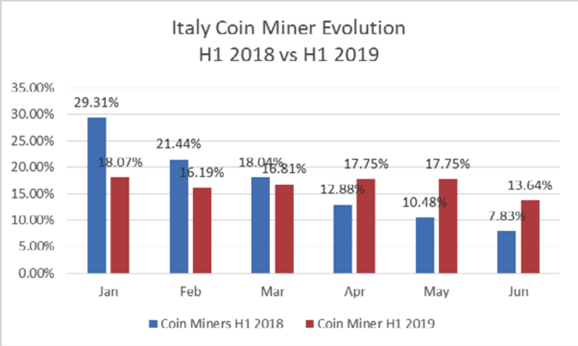


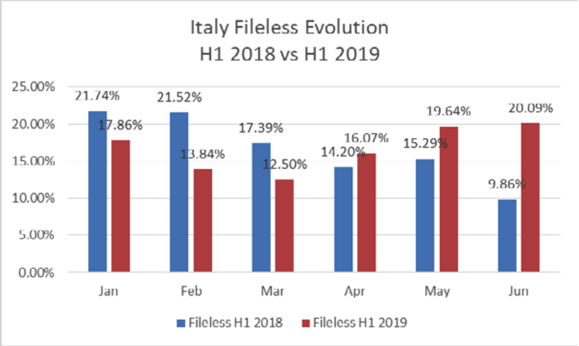


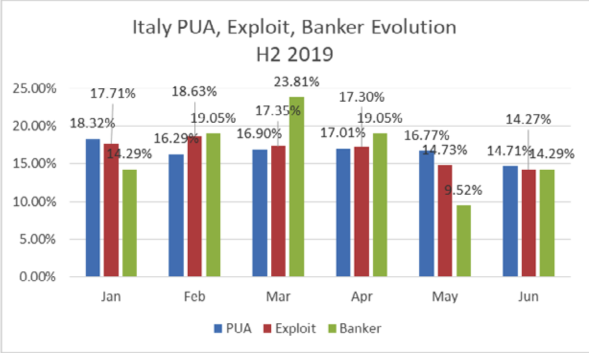


Italy

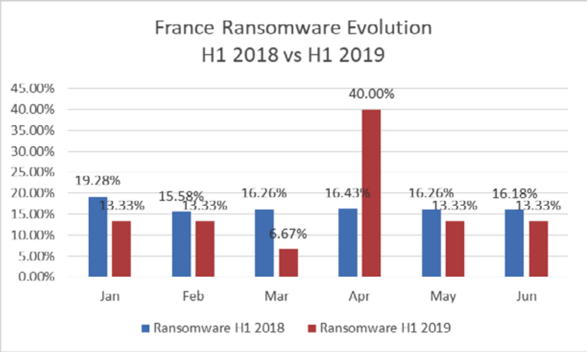


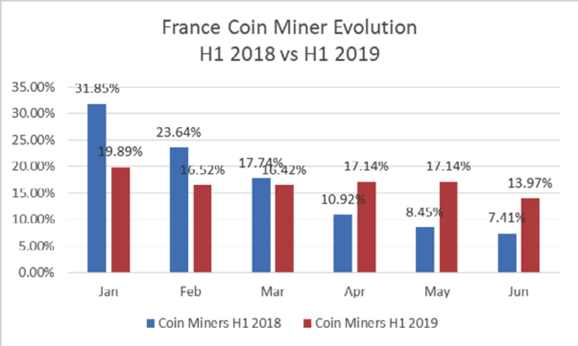


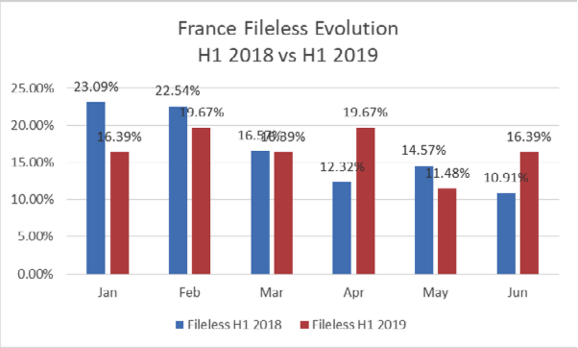


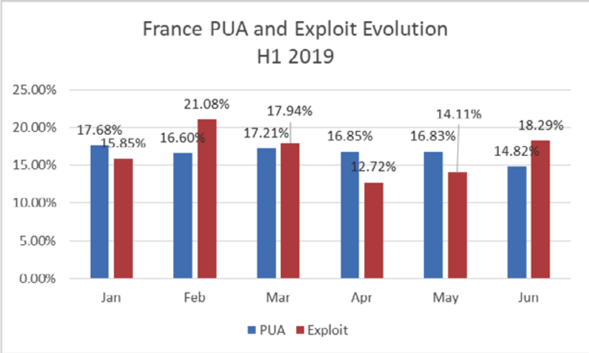


France

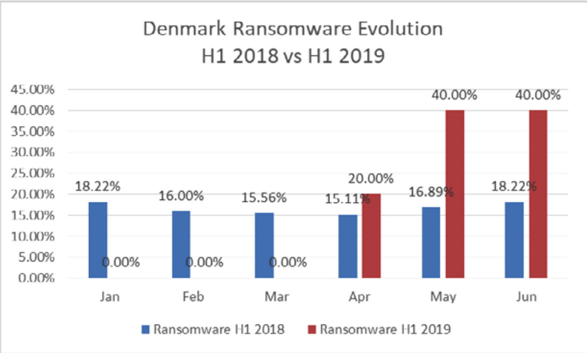

France Ransomware Evolution
H1 2018 vs H1 2019

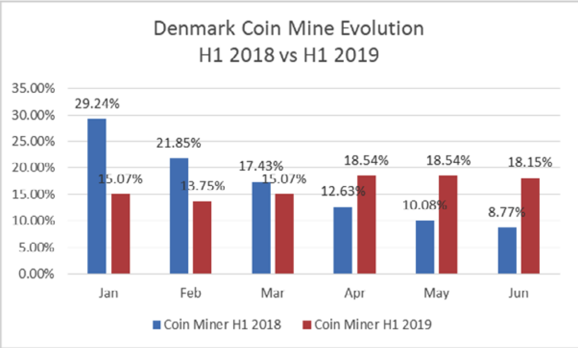

France Coin Miner Evolution
H1 2018 vs H1 2019

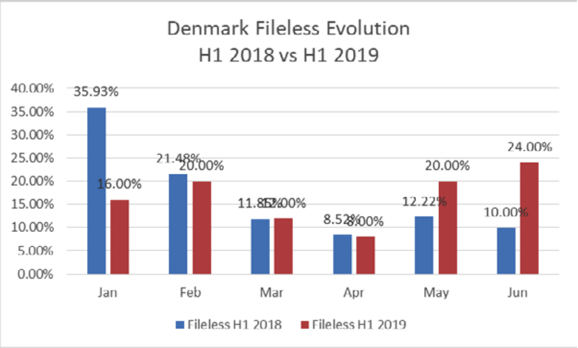

France Fileless Evolution
H1 2018 vs H1 2019

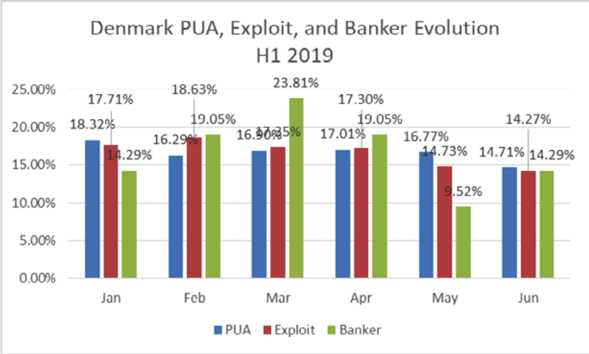

France PUA and Exploit Evolution
H1 2019

Denmark

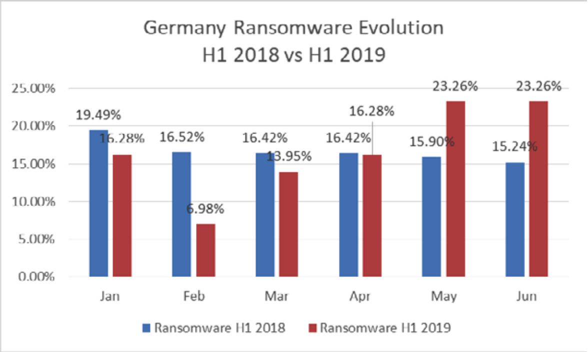

Denmark Ransomware Evolution
H1 2018 vs H1 2019

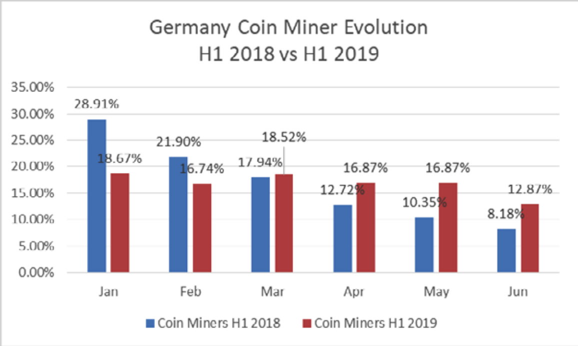

Denmark Coin Mine Evolution
H1 2018 vs H1 2019

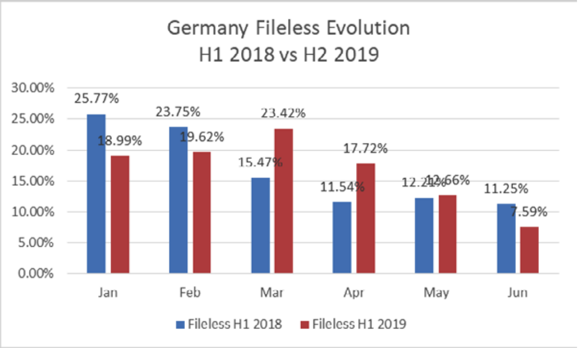

Denmark Fileless Evolution
H1 2018 vs H1 2019

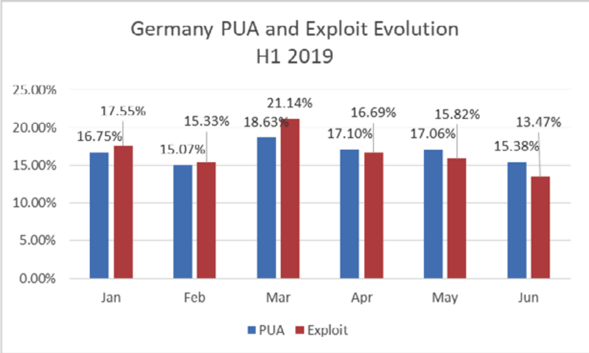

Denmark PUA, Exploit, and Banker Evolution
H1 2019

Germany

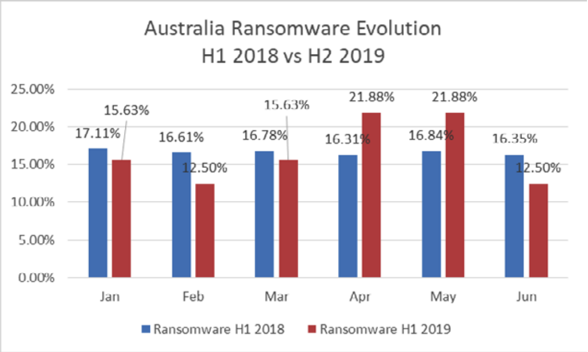


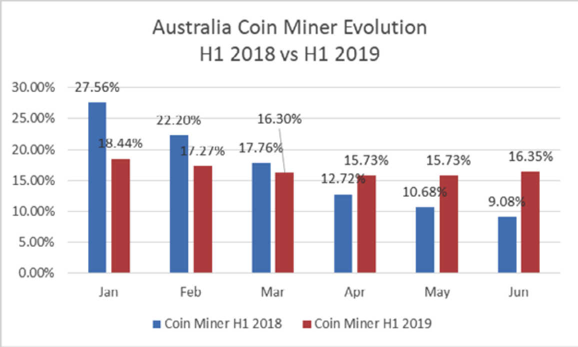


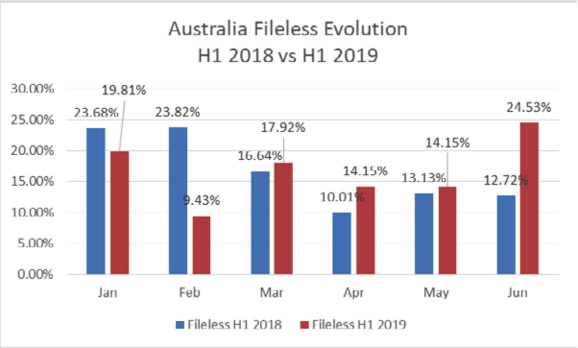


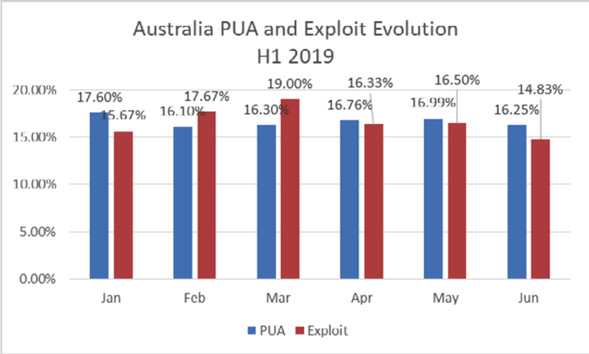


Australia

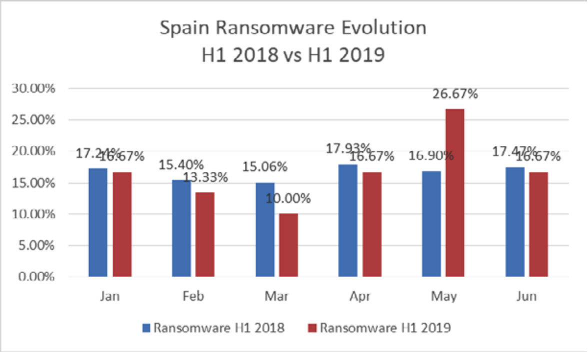


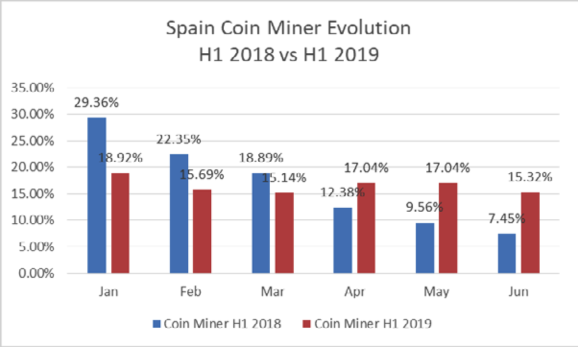


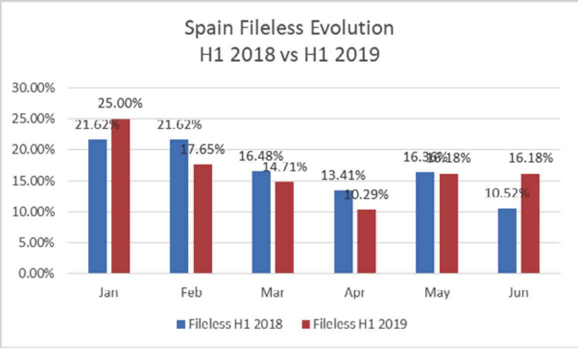


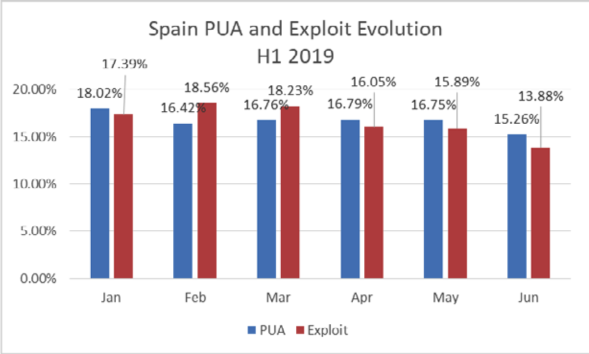


Spain


Spain Ransomware Evolution
H1 2018 vs H1 2019
30.00%
25.00%
20.00%
15.00%
10.00%
5.00%
0.00%
17.24%
16.67%
15.40%
13.33%
15.06%
10.00%
17.93%
16.67%
16.90%
26.67%
17.47%
16.67%
Jan
Feb
Mar
Apr
May
Jun
■ Ransomware H1 2018
■ Ransomware H1 2019


Spain Coin Miner Evolution
H1 2018 vs H1 2019
35.00%
30.00%
25.00%
20.00%
15.00%
10.00%
5.00%
0.00%
29.36%
18.92%
22.35%
15.69%
18.89%
15.14%
12.38%
17.04%
9.56%
17.04%
7.45%
15.32%
Jan
Feb
Mar
Apr
May
Jun
■ Coin Miner H1 2018
■ Coin Miner H1 2019


Spain Fileless Evolution
H1 2018 vs H1 2019
30.00%
25.00%
20.00%
15.00%
10.00%
5.00%
0.00%
21.62%
25.00%
21.62%
17.65%
16.48%
14.71%
13.41%
10.29%
16.36%
16.18%
10.52%
16.18%
Jan
Feb
Mar
Apr
May
Jun
■ Fileless H1 2018
■ Fileless H1 2019


Spain PUA and Exploit Evolution
H1 2019
20.00%
15.00%
10.00%
5.00%
0.00%
18.02%
17.39%
16.42%
18.56%
16.76%
18.23%
16.79%
16.05%
16.75%
15.89%
15.26%
13.88%
Jan
Feb
Mar
Apr
May
Jun
■ PUA
■ Exploit

macOS Threat Landscape

OS-wise, Macs have a 6% market share, while Windows has 36% (avg. last 12 months according to statcounter.com). With Windows remaining a lucrative battlefront, there is little incentive for malware authors to invest time and resources to develop mass-market Mac-centric threats, focusing mostly on advanced and sophisticated threats designed for C-level executives and decision makers.

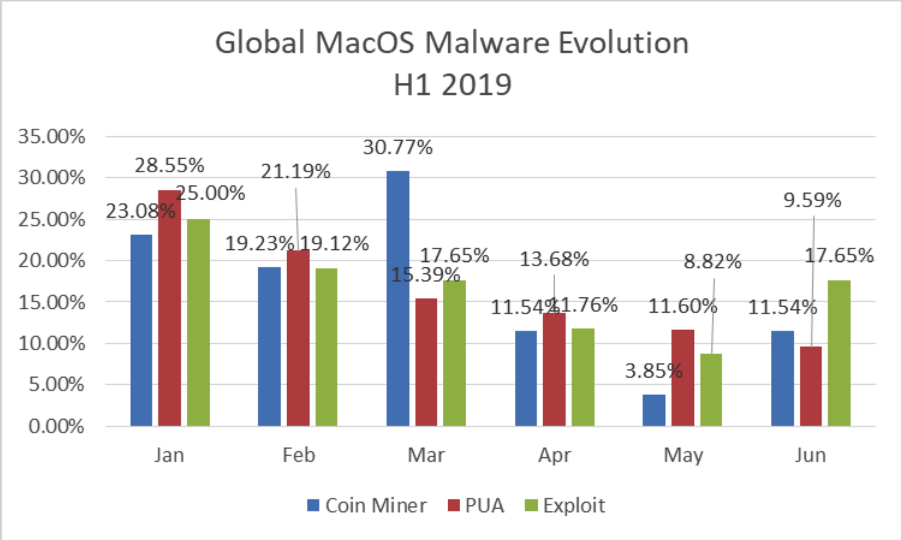
Macs are not immune to threats. While ransomware has been scarce on macOS, it has been easily targeted by cryptojacking (coin mining) operations, exploits leveraging known vulnerabilities, Potentially Unwanted Applications (PUAs) and, of course, run-of-the-mill platform-agnostic online threats like phishing.

In the first half of 2019, some of the most common threats directed at macOS revolve around coin miners, PUA and exploits, according to Bitdefender telemetry. While most threats that involve coin miners leverage compromised legitimate websites that “borrow” computing power from unsuspecting visitors, some threats even target users that have various cryptocurrency wallets.

For instance, instead of stealing computing power, cybercriminals often resort to stealing user cookies that frequently contain login credentials for various cryptocurrency exchanges, such as Coinbase, Binance, Poloniex, and many others. This is far more lucrative, as users suspect nothing while cybercriminals literally cash out their victims’ wallets. Of course, these threats are also versatile enough to steal other cookies and password that can be used for authenticating to a wide range of services, broadening the implications and potential security risks.

Bitdefender telemetry also found many reports coming from vulnerabilities. This might indicate that exploit kits leveraging unpatched vulnerabilities in commonly used browser plugins or macOS applications are constantly probed by malicious websites in an attempt to place various threats.

Like Windows users, Mac users don’t typically install updates as soon as they arrive. Most targeted macOS attacks leveraging exploits were conducted in the first three months of the year. In the April – May time period, exploit-based attacks dropped considerably, as shown in the chart below, only to rise again in June.



One explanation would be that Apple patched hundreds of vulnerabilities in the last two macOS security updates alone (released in the March – June time period). As customers progressively ceded to the update nag, exploit kits leveraging those flaws likely became useless.

Unlike the previous Windows telemetry, ransomware, fileless attacks and banking Trojans are not as prevalent on macOS. While there have been reported incidents in the wild where macOS Trojans have been used to steal banking credentials or even exfiltrate sensitive data, such as user names and passwords by acting as locally installed keyloggers, the number of reports of macOS-installed malware is relatively low.

However, cybercrooks targeting Macs prefer to focus on web-based threats, such as fraud, phishing, and coin-mining software, or even potentially unwanted apps (PUAs).

We can also draw a correlation between PUAs and coin miners, as coin miners sometimes arrive by means of PUAs. **Potentially Unwanted Applications (PUA)**[12] in H1 2019 were the most common threat for macOS users – by a considerable margin. While January clocked in at 28.55 percent of all reported PUAs during H1 2019, the number slightly decreased over the next couple of months.

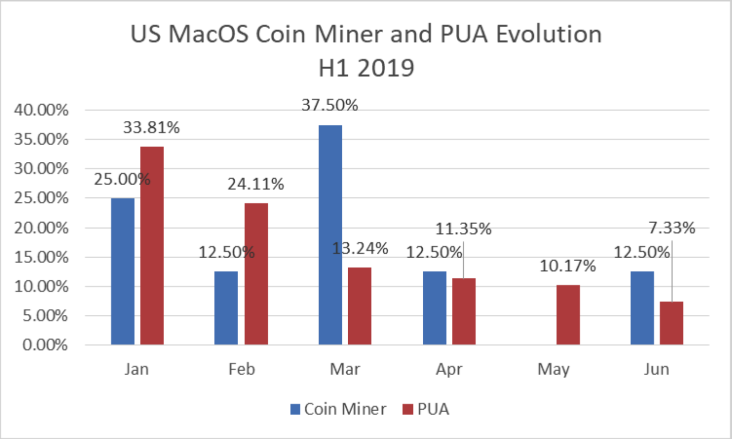
PUA, which border malware, are also called "grayware," because they typically end up on a user's computer either without their express consent or bundled with a seemingly legitimate application. Even when installed with the user's consent, a PUA can have hidden functions that may collect personal data and send it to a server controlled by its authors. That data can later be sold to advertisers without the user knowing it, or monetized in some other way.

PUAs often end up on a user's system as part of a larger bundle that the user intentionally downloaded. A PUA may also be downloaded and installed intentionally by a user who was misled by the author's marketing. Some PUAs are dressed as cleaning utilities, while other may run unwanted processes invisible to the user, such as coin miners.

Exploits, PUAs and coin miners were the most lucrative forms of cybercrime on macOS in H1 2019. Ransomware operators have all but committed themselves fully to the Windows ecosystem, but the occasional fileless threat leverages scripts or macros embedded within Microsoft Office documents running on Macs.

In countries such as the United States, coin miner reports for macOS seemed to jump in March 2019, peaking at 37.50 percent of all reports during H1 2019 in US. January also seems to have been relatively high, peaking at 25 percent, while PUAs took the lead with 33.81 percent of all PUA reports in the US in H1 2019.

Although coin miners might not have dominated the macOS threat landscape report, potentially unwanted applications seem to have had more reports than any other threat.



In terms of reports for individual countries regarding macOS malware evolution, only potentially unwanted applications seem to have had reports of any significance. While web-based exploits delivered via tampered or malicious websites may have sparsely showed up in our telemetry, they're only a fraction of the number of potentially unwanted applications reported.

[12] Wikipedia, "Potentially unwanted program",. https://en.wikipedia.org/wiki/Potentially_unwanted_program

Android Threat Landscape

With **more than 2.5 billion**[13] **active Android devices**, the mobile operating systems has seen its share of malware. Malware developers have been focusing on Android rather than any other mobile OS, mostly because of its market share. With a massive **76.24 percent**[14] **of the mobile OS market**, Android presents a unique opportunity for threat actors as they can potentially affect many more people and compromise their data than with any other mobile OS.

Although most Android applications are downloaded from the official Google Play store, which housed **more than 2.7 million**[15] **apps as of June 2019**, some Android users may not have access to these repositories and hence resort to third-party marketplaces. These marketplaces may pose security challenges as they might not vet applications for malware as diligently as Google. However, Google Play has seen its fair share of malware and **aggressive adware**[16] applications as well. Since the Android user base is extremely large, the more an application bundled with aggressive adware is downloaded, the more revenue it generates for threat actors.

"More than

2.5 billion

active Android devices"

39.31%

YoY increase in Android malware reports

While Google's official marketplace has done a great job of bouncing nasty applications by making Google Play Protect a lot more potent in terms of spotting malicious apps, there have been occasional slipups. Borderline malicious apps that relied on various techniques for dodging security vetting, such as encrypting the main logic of the application and loading it dynamically, hiding code that is triggered remotely by server configurations or commands, or even uploading a clean version of the application and then adding a malicious update, have sometimes proven effective against Google Play Protect. Most apps that exhibit this behavior are taken offline as soon as they're reported, but some manage to remain available for quite a while.

In fact, Bitdefender telemetry shows **a 39.31 percent YoY increase in Android malware reports**, compared to the first half of 2018. While not all reported applications are directly related to malware or spyware, adware has become a lucrative threat that Android malware developers seem to increasingly exploit.

Not all users download apps only from the official marketplace. Some want to simply sideload apps from third-party stores because they might refuse to purchase the legitimate apps – thus exposing themselves to fake apps and malware – or they may simply live in geo-fenced regions that don't allow access to the official store. Most of these free app stores don't have even basic security screenings for submitted apps, meaning that users are more likely to install malware and fake applications rather than something clean.

Android malware can be just as pervasive as Windows malware in terms of capabilities and surveillance options. Since smartphones are equipped with a wide range of sensors, such as cameras, GPS, microphones, gyroscopes, they can easily be turned into spies that monitor, record, and broadcast all activity.

Bitdefender Labs recently uncovered such a **spyware framework, dubbed Triout**[17], that not only hid its presence on the devices, but also packed abilities such as recording phone calls, logging incoming text messages, recoding videos, taking pictures and collecting GPS coordinates, then broadcasting all of that to an attacker-controlled C&C (command and control) server.

The same Android spyware framework was also found on third-party marketplaces impersonating a legitimate privacy-enabling application that promised a means to bypass censored or blocked websites by leveraging a series of proxies. The legitimate application had **over 50 million**[18] **installs** and over 1 million reviews (mostly positive), meaning its popularity could have been abused by threat actors to repackage it with the spyware framework.

[13] **Android**. https://twitter.com/Android/status/1125822326183014401

[14] **Statcounter**. https://gs.statcounter.com/os-market-share/mobile/worldwide

[15] **Statista**. https://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/

[16] **Bitdefender Labs**. https://labs.bitdefender.com/2019/07/adware-packed-fake-apps-still-making-their-way-to-google-play/

[17] **Bitdefender Labs, "Triout – Spyware Framework for Android with Extensive Surveillance Capabilities"**. https://labs.bitdefender.com/2018/08/triout-spyware-framework-for-android-with-extensive-surveillance-capabilities/

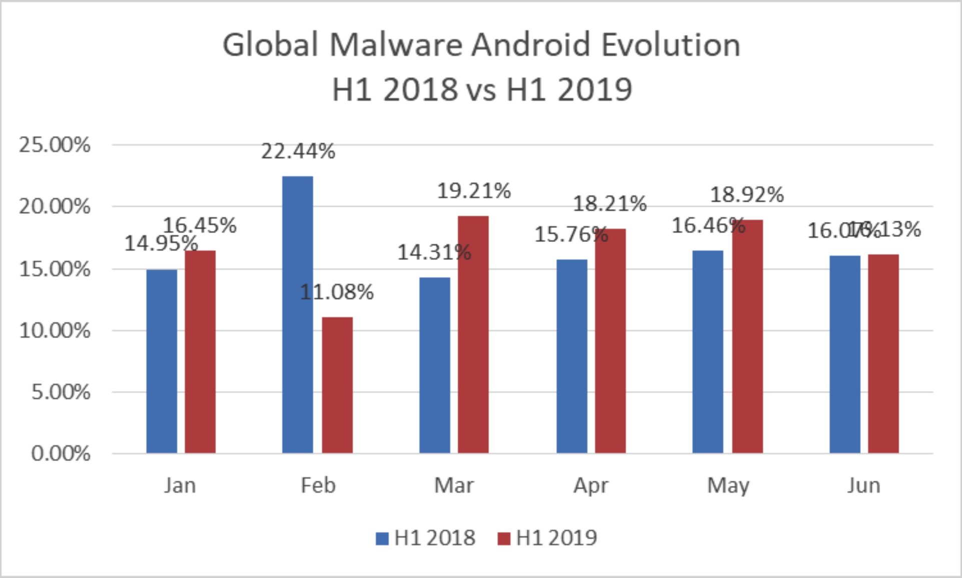
[18] **Bitdefender Labs, "Triout Android Spyware Framework Makes a Comeback, Abusing App with 50 Million Downloads"**. https://labs.bitdefender.com/2019/02/triout-android-spyware-framework-makes-a-comeback-abusing-app-with-50-million-downloads/

While Android malware can come in all shapes and sizes, the main motivation behind developing such threats usually stems from the cybercriminals desire to generate profit by exfiltrating sensitive and valuable data and selling it to the highest bidder, extorting victims, or making money off affiliate ads.

Some of the top threats identified by Bitdefender during the first half of 2019 actually involve malware families that download additional components, malware that tries to gain persistence by using known exploits to root unpatched Android operating systems, as well as applications that bombard users with tons of ads to which the malware developer is affiliated.

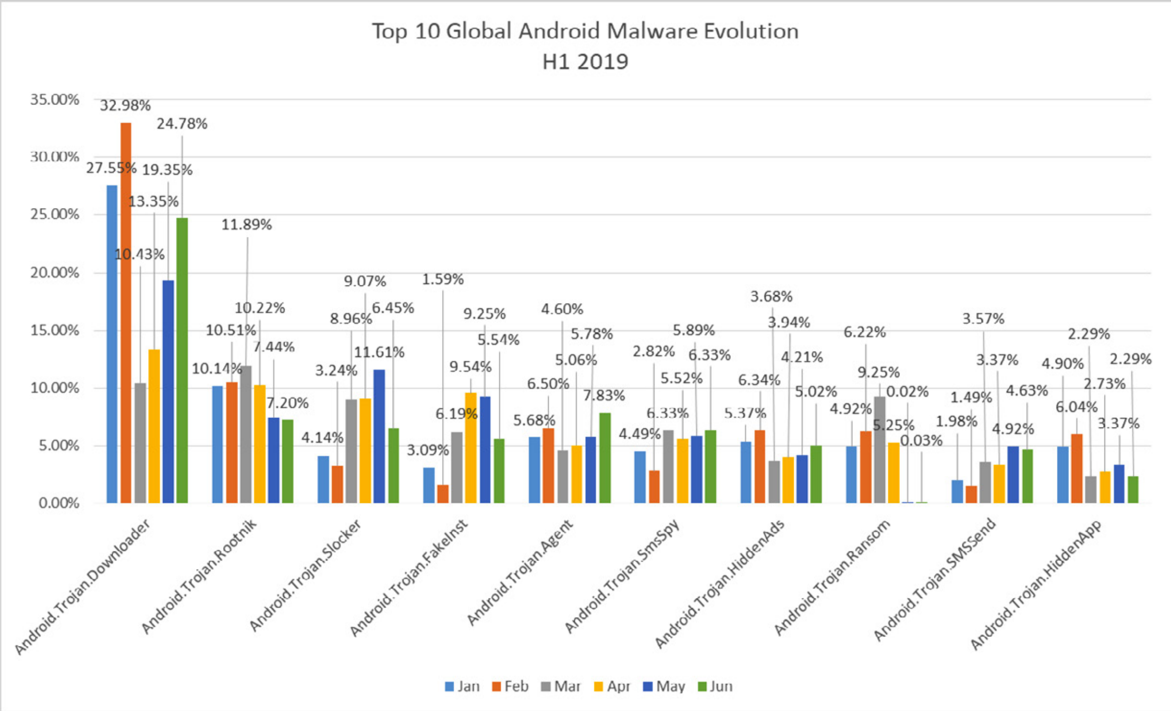
While aggressive adware might seem benign at first glance, as it only shows popups and redirects user searches to various websites, they can do much more than just irk users. They also drain a battery a lot faster and in time contribute to poorer battery performance due to increase recharge cycles.

The evolution of Android malware in the first half of 2019 compared to the first half of 2018 points to the same increase in numbers mentioned in the beginning of this section. On a month-by-month comparison, 2019 has seen a steady increase in Android malware reports, except for February. Clocking in at 11.08 percent of all Android malware reports during the first half of 2019, February 2018 reports were almost double.



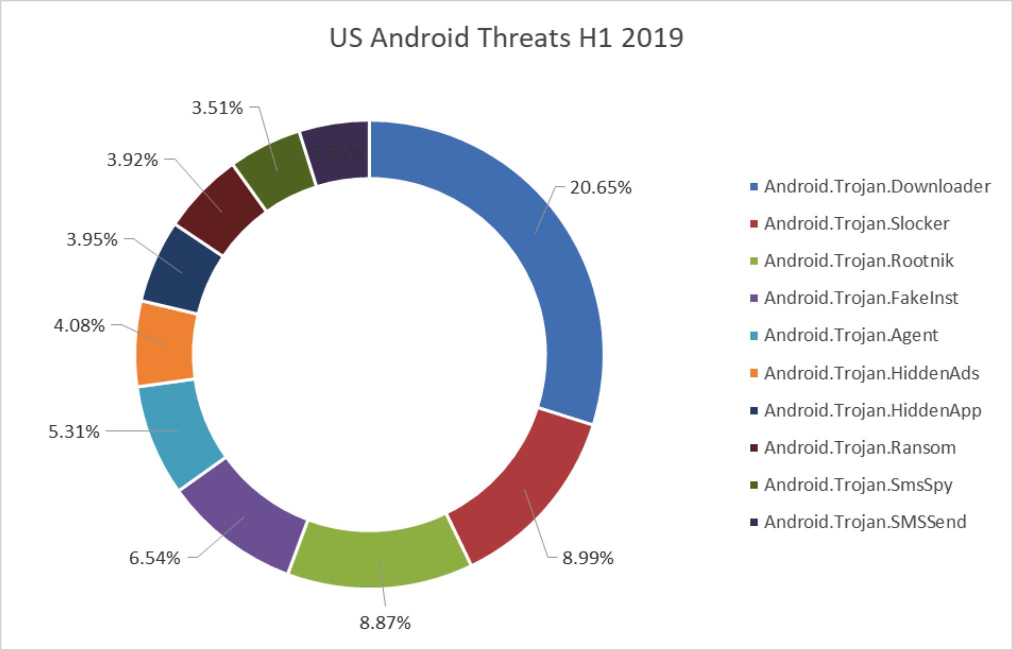
The top 10 global Android malware evolution chart below shows the performance of some of the most prevalent malware families in the first half of 2019. While the most popular involve threats that download additional components or try to root older and unpatched Android distributions, Android.Trojan.HiddenAds, Android.Trojan.HiddenApp, and Android.Trojan.FakeApp exemplify the most common tactics Android malware developers use to infect and monetize Android devices.

Either by displaying aggressive ads, hiding the application under various names to make them difficult for users to find and uninstall, or by posing as legitimate applications, these three malware families can sometimes act as an initial foothold into the device to download and install additional applications.

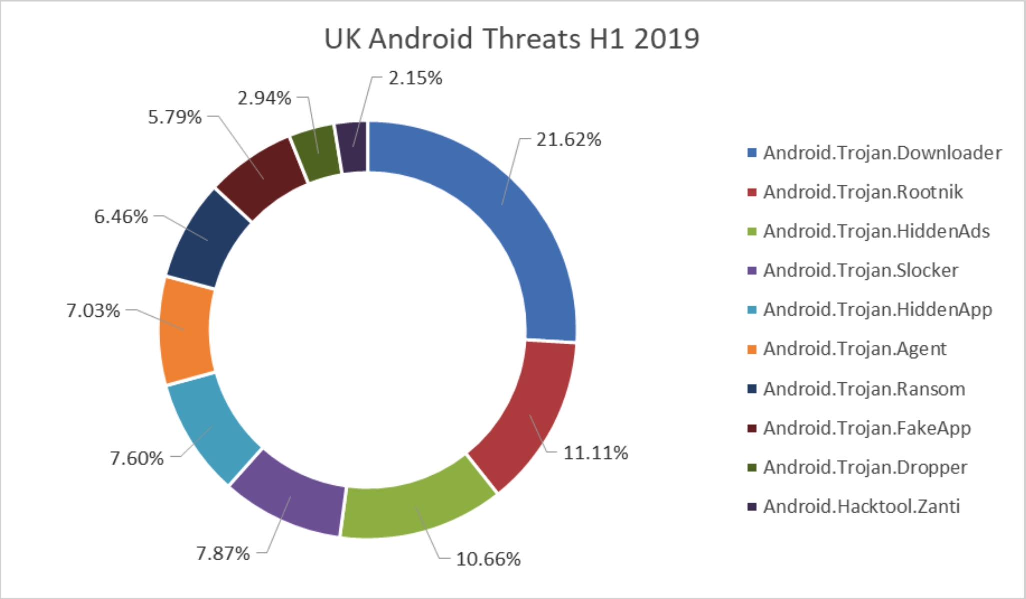


Even ransomware, a threat common to Windows operating systems, has made its way to Android. Two malware families – Android.Trojan.Ransom and Android.Trojan.SLocker – are responsible for preventing users from accessing data stored on their devices. While Android ransomware may not be able to actually encrypt data stored on the device, it can display a nag screen with a PIN lock, preventing users from unlocking their devices unless a ransom note is paid. Removing these threats can be a matter of performing a clean wipe of the device, but that would mean losing all locally stored data, such as documents, photos, videos, and media files, unless they have been backed up in the cloud.

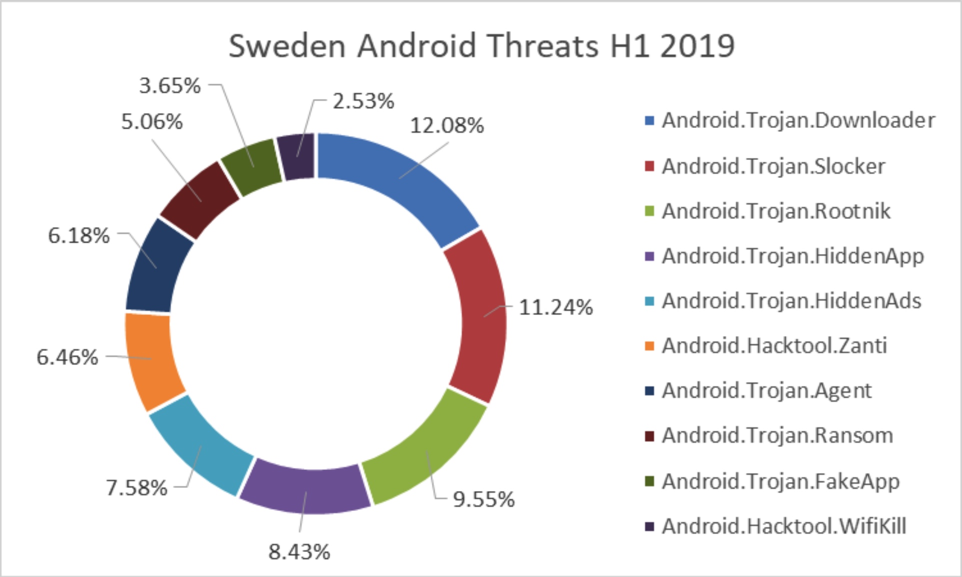
United States



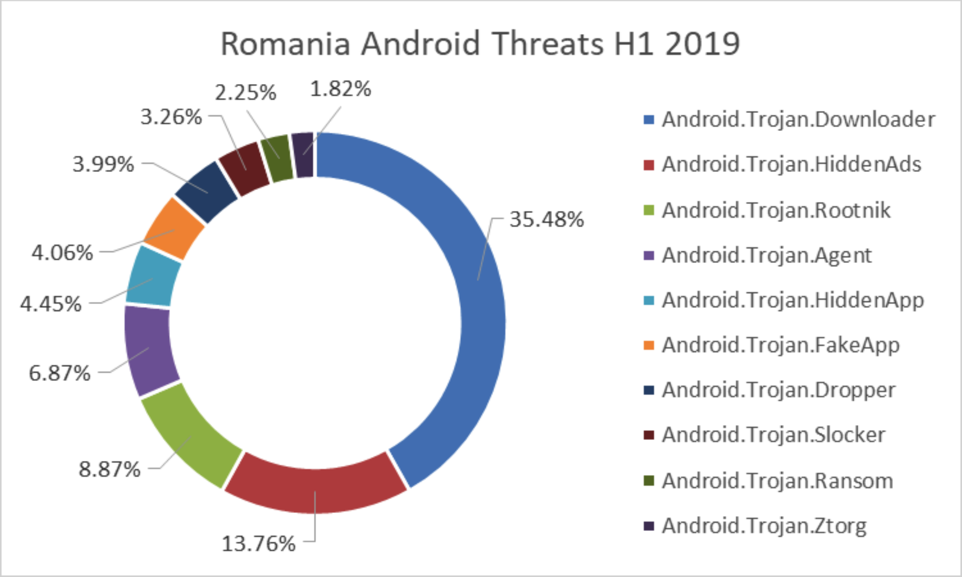
The United Kingdom



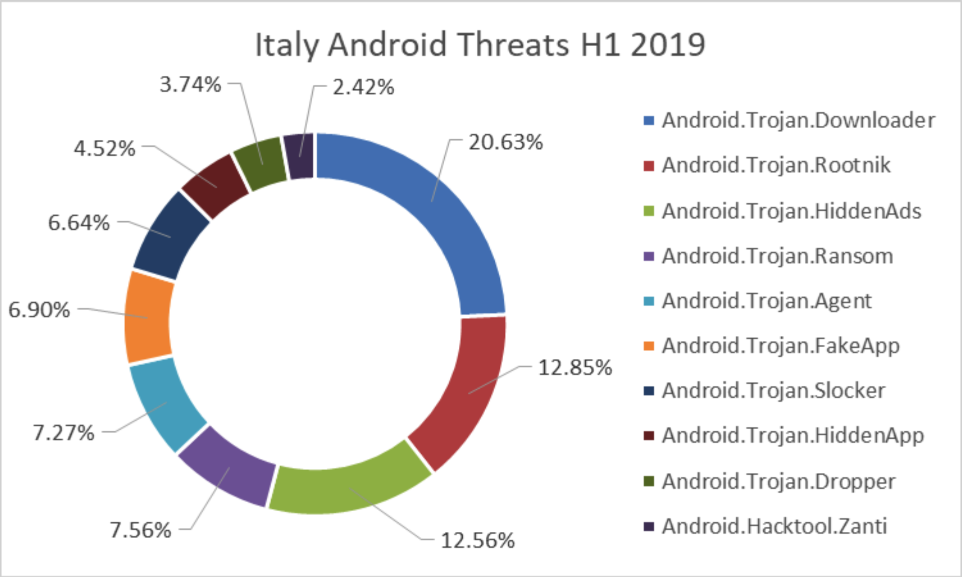
Sweden



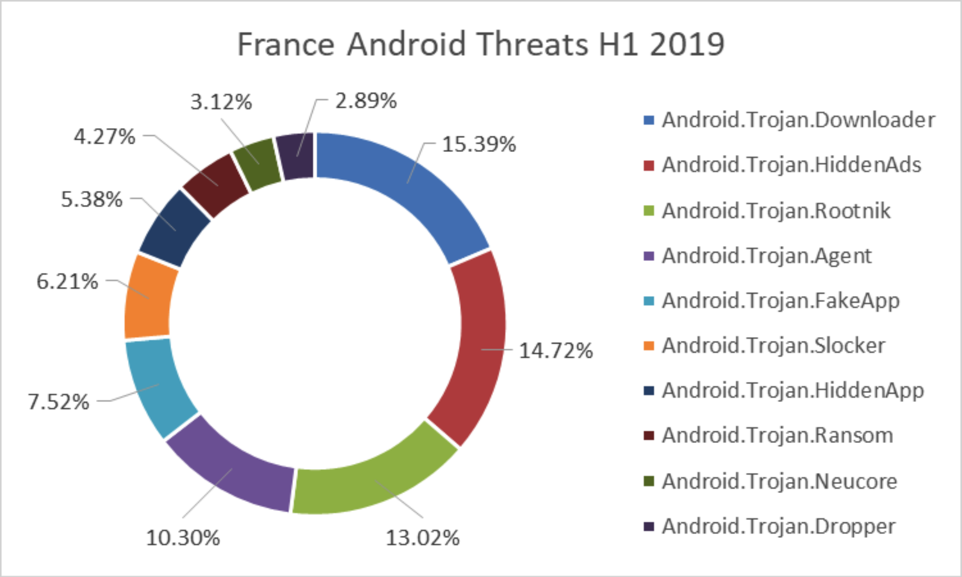
Romania



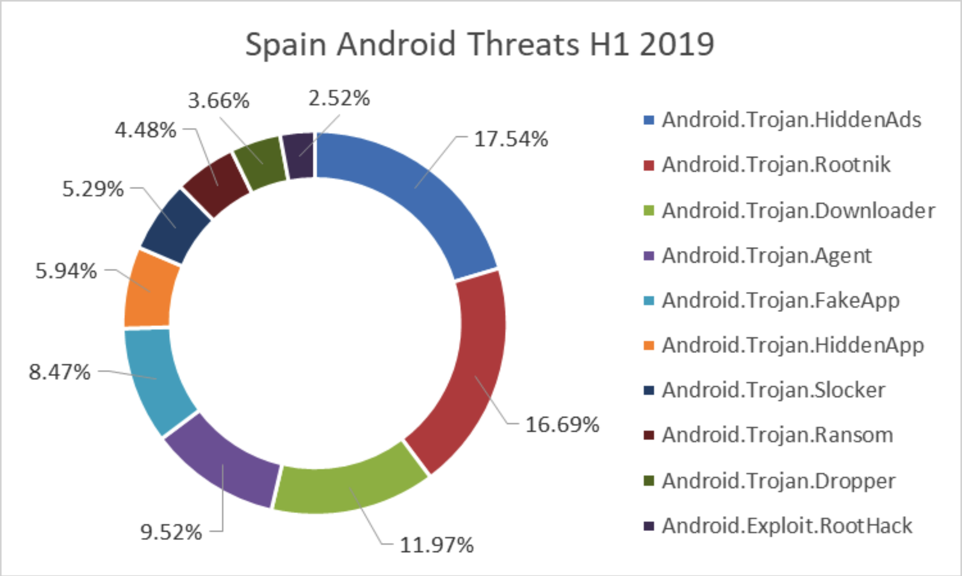
Italy



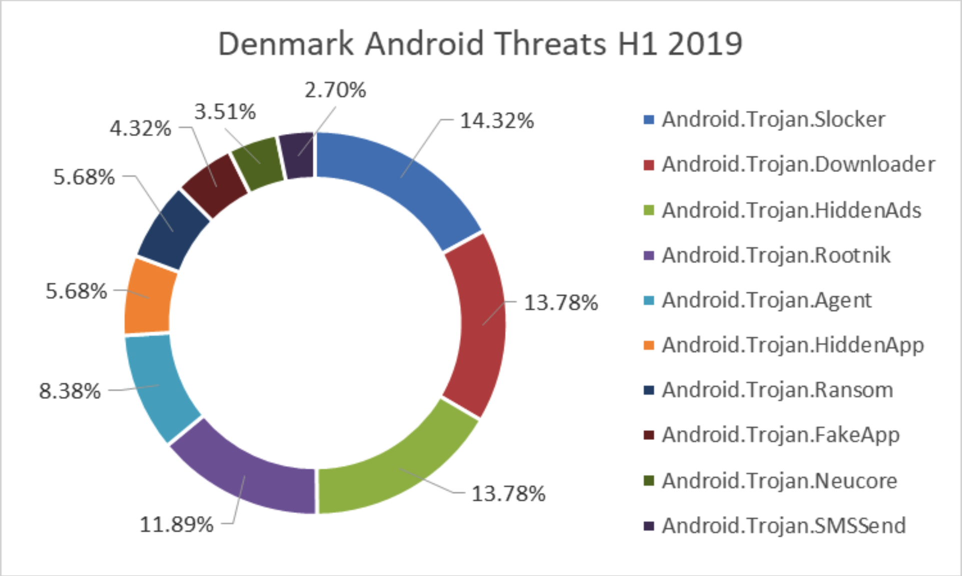
France



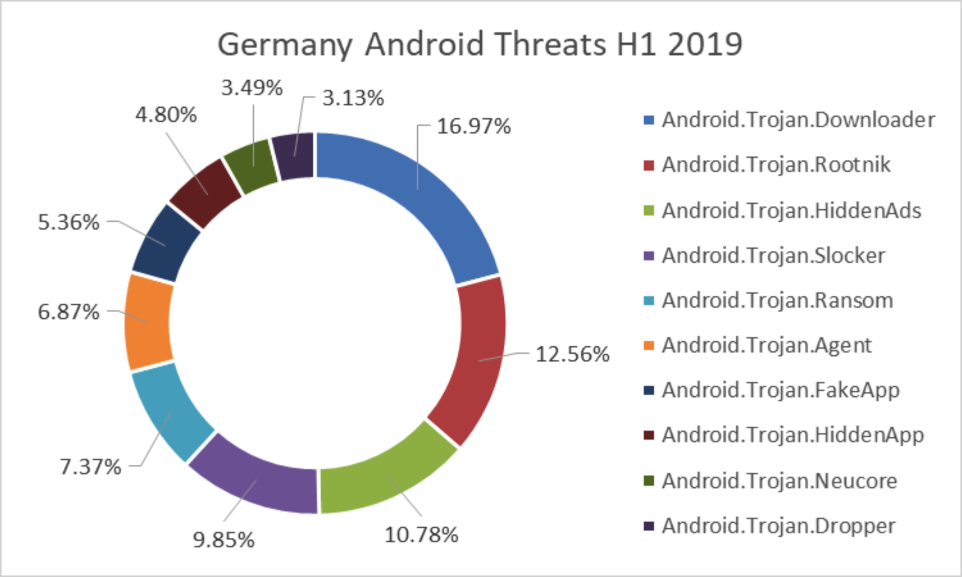
Spain



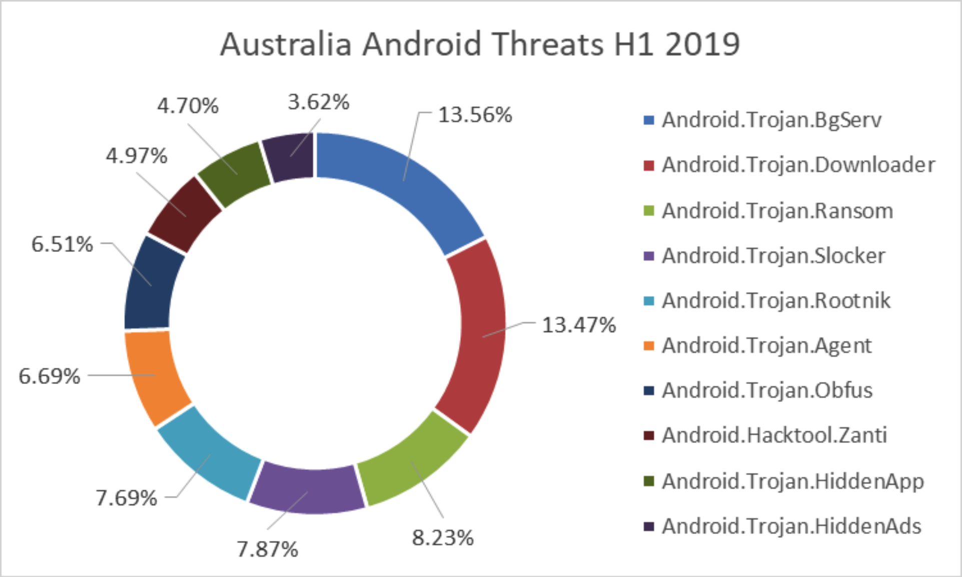
Denmark



Germany



Australia



IoT Threat Landscape

One of the most vulnerable segments of our digital life, the Internet of Things (IoT), continues to grow at a steady pace. More than 22 billion[19] smart / connected devices exist in the world, and the number is projected to reach 41.6 billion by 2025.

While smart devices do a good job of delivering the Internet's promise to make the world a truly connected place, these gizmos often lack safeguards against targeted attacks. Such lax security configurations include:

- default passwords (i.e. 123456 or "password")
- outdated firmware
- legacy OS (i.e. Symbian)
- the inability to install new firmware (in case a vulnerability is discovered)
- unintuitive / cumbersome setup forcing users to skip certain security settings
- can't be fitted with a traditional antivirus solution…

"22 billion

smart / connected devices exist in the world"

… and the list could go on.

IoT gadgets such as voice-activated assistants and baby monitors also have access to highly sensitive and personal data, and there is no shortage of hacking precedents for these types of devices. Cybercriminals also hack IoT devices in bulk to create botnets and conduct massively disruptive[20] DDoS attacks.

After Mirai's source code went public, many IoT botnets started probing for IoT devices in an attempt to compromise and enslave them. Since malware is designed with a financial motive, some IoT botnets are used for extortion. In a large-scale DDoS attack on an online target, such as a retailer or vendor, attackers often contact the target with extortion demands to halt the attack.

While the popular belief is that IoTs are mostly comprised of IP cameras, DVRs, and all sorts of sensors, some IoT botnets often include exploits and vulnerabilities found in mobile devices running Android OS and even mass-market routers.

Bitdefender researchers found a new IoT botnet, Hide and Seek[21], that amassed over 90,000 IoT devices in a large botnet in a matter of days. The first variant performed brute force attacks over the Telnet service to remotely dial into devices, while later updates involved new command injection exploits in a device's web interface, extending the botnet's capabilities to IPTV cameras. New capabilities were later added, even abusing Android Debug Bridge (ADB) over Wi-Fi feature in Android devices, which developers normally use for troubleshooting, to add vulnerable Android-running devices to their botnet. This simple new capability allowed attackers to add at least another 40,000[22] new devices to their zombie network.

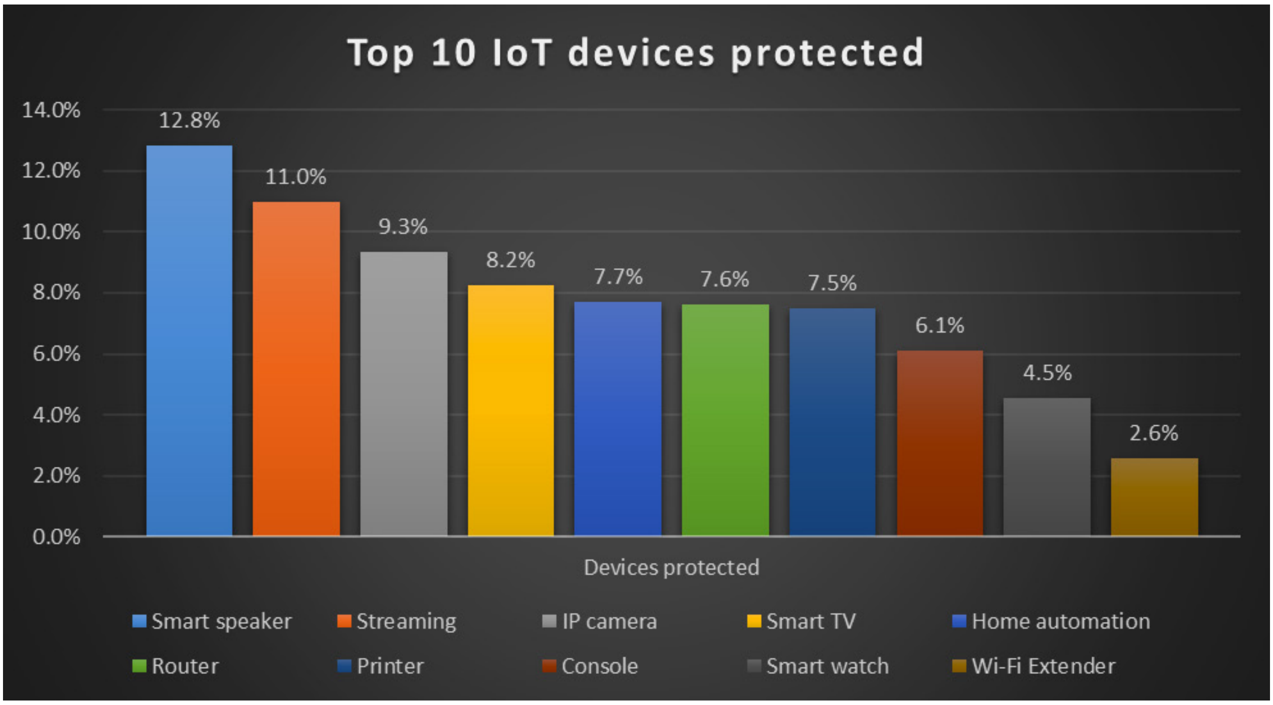
Our internal telemetry shows an increase in blips on the IoT radar, including smart speakers, IP cameras, smart TVs and fridges, home automation gear and smart bulbs. The chart below shows a breakdown of the top 10 smart devices protected by our IoT security solutions.

[19] **IDC, The Growth in Connected IoT Devices Is Expected to Generate 79**.4ZB of Data in 2025, According to a New IDC Forecast, https://www.idc.com/getdoc.jsp?containerId=prUS45213219

[20] **Wikipedia, Mirai (malware), https://en**.wikipedia.org/wiki/Mirai_(malware)

[21] **Bitdefender, "New Hide 'N Seek IoT Botnet using custom-built Peer-to-Peer communication spotted in the wild", https://labs**.bitdefender.com/2018/01/new-hide-n-seek-iot-botnet-using-custom-built-peer-to-peer-communication-spotted-in-the-wild/

[22] **Bitdefender, "Hide and Seek IoT Botnet Learns New Tricks: Uses ADB over Internet to Exploit Thousands of Android Devices"**. https://labs.bitdefender.com/2018/09/hide-and-seek-iot-botnet-learns-new-tricks-uses-adb-over-internet-to-exploit-thousands-of-android-devices/

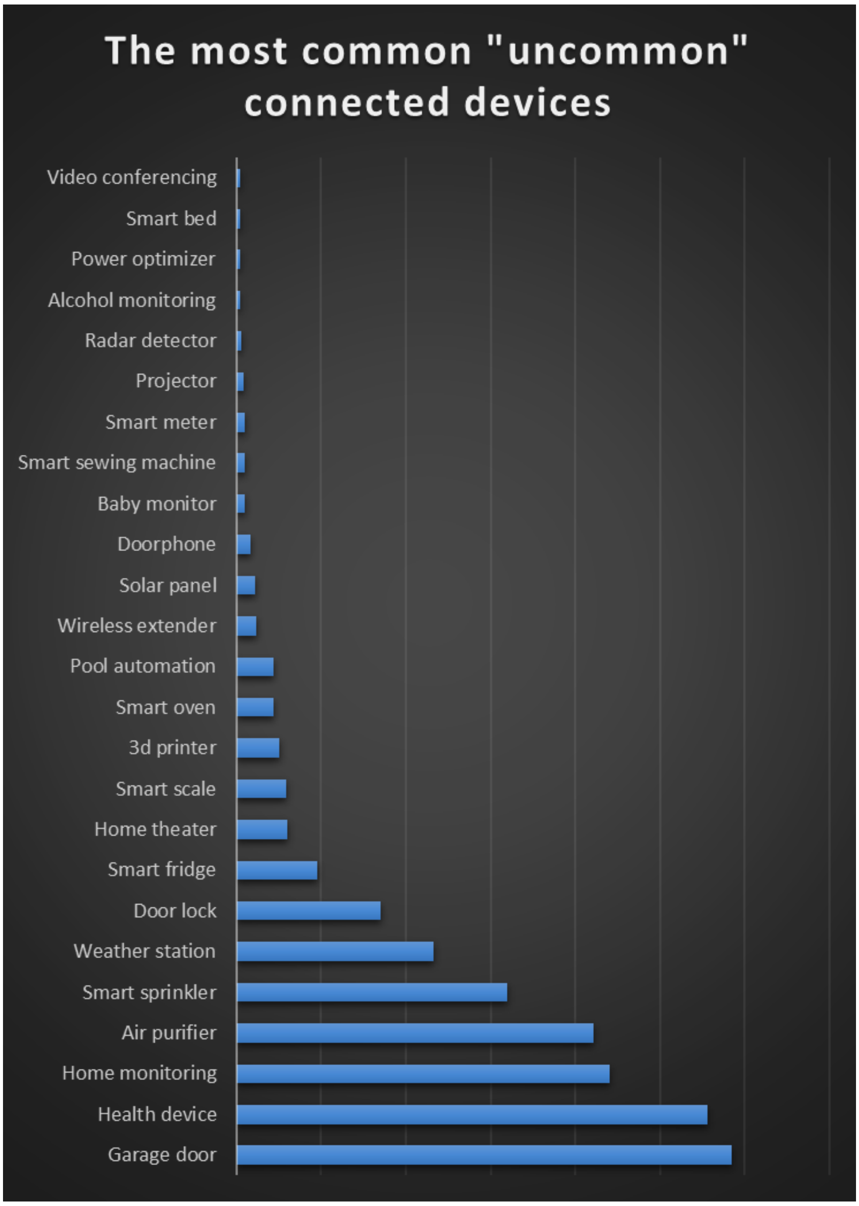


Note: "Streaming" devices include things like the Amazon Fire TV Cube, Roku or Google ChromeCast. "Home automation" includes thermostats, automated lighting fixtures, etc., and "Consoles" include the usual suspects – i.e. Sony PlayStation, Nintendo Switch, Microsoft Xbox.

As shown in the chart above, smart speakers (including those powered by voice assistants like Google Home and Amazon Echo) are the most common IoT gadgets in smart households, followed by streaming devices and IP cameras, smart TVs and home automation products. These top 10 gadgets account for 77% of a much broader fleet of connected devices.

The remaining 23% includes a plethora of other device types, such as smart plugs, smart door locks and doorbells, weather stations, solar panels, animal trackers and feeders (dispensers), smart beds, water sprinklers, smart air conditioning units, air purifiers, and so on. These devices may not be as prevalent as the top ten, but they are out there, in the millions, and require constant protection against bad guys.

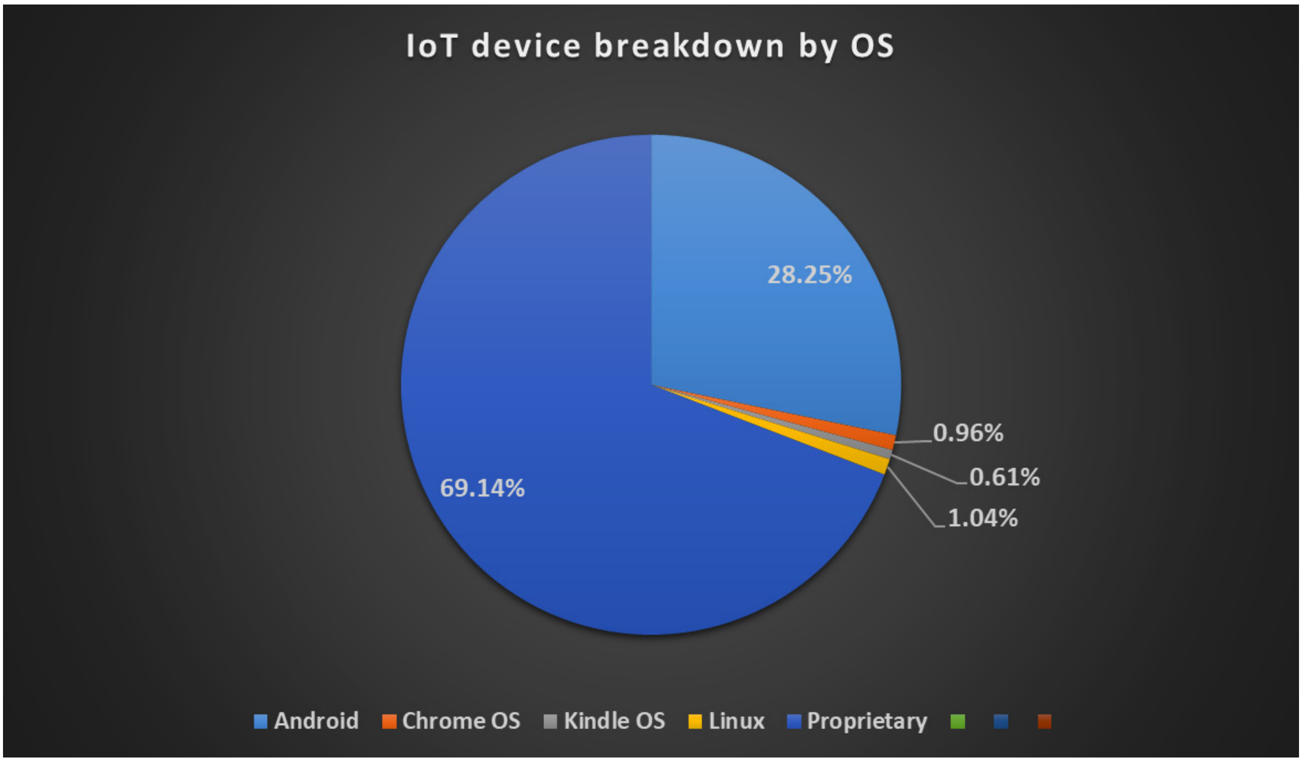
To get an idea of the diversity of the IoT ecosystem, the chart below shows a breakdown of the scarcer variety of smart devices protected by Bitdefender solutions. These are the most common "uncommon" members of the IoT family.



It's also worth noting that many of these devices receive no security updates even if vulnerabilities are found within their firmware or operating system. They might also lack an update mechanism, preventing vendors from fixing a known vulnerability. And their shelf life is often extremely short, meaning vendors stop supporting them after a couple of months.

When we step outside the "traditional" IoT family to include every connected device protected by Bitdefender, things look a lot more interesting. Our IoT solutions also cover gadgets running common household names like Windows, iOS, macOS and Android. Any connected device can be considered a member of the broader IoT family.

However, for the sake of consistency, we will exclude phones and tablets, or things running Windows, keeping a tight focus on gadgets defined as members of the traditional IoT family. A breakdown of the most common operating systems powering smart devices looks a bit like this:



As shown above, not all IoT vendors and manufacturers use open source operating systems, sometimes going for proprietary OSs. This IoT operating system fragmentation and lack of standardization makes it difficult to properly audit devices and enforce consistent policies across the spectrum, as well as properly maintain the code behind the OS to make sure that its audited and updated to resolve known security issues.

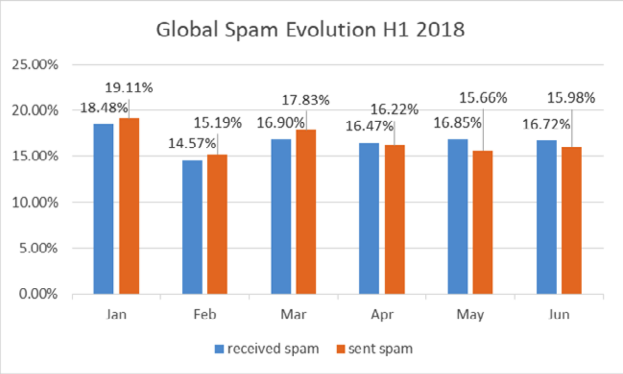
Spam Evolution

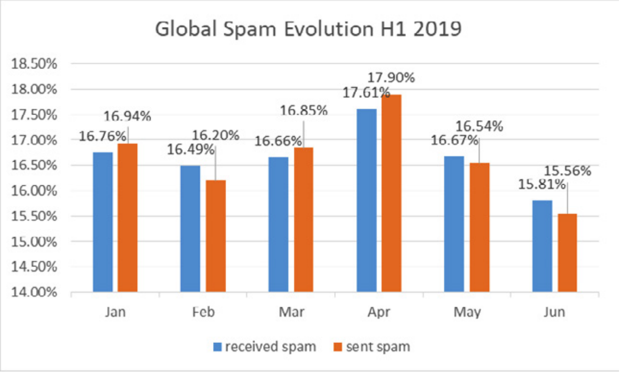
Bitdefender telemetry reports a **45.90 percent increase in the global volume of spam received**, and a **50.11 percent year-over-year increase in the global volume of spam sent**.

“50.11%

year-over-year increase in the global volume of spam sent”

The practice of sending unsolicited emails is as old as the first ever email service provider. While spam is usually associated with marketing materials and promotional offers that expire if you don’t immediately read the email and click the embed link, email remains one of the main communication methods between individual users, between companies, and even between companies and their clients.





However, spam has also remained a key attack vector and delivery mechanisms for malware, ranging from banking Trojans to ransomware. It’s also highly popular for scams like the Nigerian prince, CEO fraud and impersonation. Spam remains a popular cyberweapon because it can effectively exploit social engineering by creating a sense of legitimacy and urgency to perform various actions, such as opening an attachment, clicking a link, or even wiring funds to attacker-controlled accounts.

Some scams heavily leverage social engineering, by researching the victim to make the message more personalized and compelling, while others target users en masse. Cybercriminals also often use victims’ computers as part of a spam botnet to send out infected messages to other victims.

One such example is the TrickBot Trojan [23] that emerged in early 2016 as a spinoff of the older Dyre/Dyreza[24] Trojan, but was constantly updated to include spam-sending capabilities, on top of the original e-banking and Bitcoin Wallet credential-harvesting features. It infected victims via spam campaigns then harvested user email credentials and used their email addresses to send spam, using victims as a spreading mechanism as well.

TrickBot has also on occasion been dropped as a second-stage payload by other malware, as cybercriminals either banded together or rented access to botnet infrastructures to maximize profits. However, one of the most common traits of all recent credential-harvesting Trojans is that they include both some of the latest tools and techniques to steal credentials, such as using the EternalBlue[25] vulnerability or the MimiKatz[26] tool, as well as the ability to use the victim’s system as a self-propagation mechanism through spam-sending campaigns.

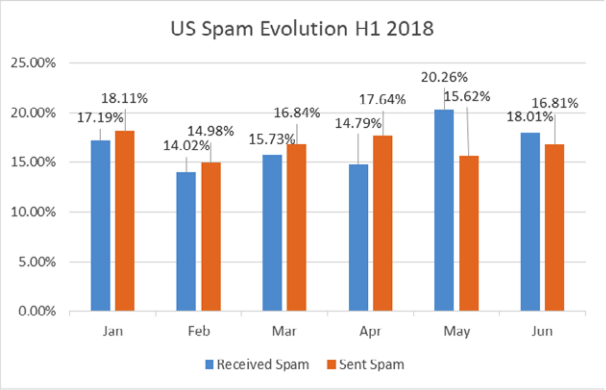
[23] **Bitdefender, “Emotet, Lokibot, TrickBot still impacting enterprise environments globally”**. https://hotforsecurity.bitdefender.com/blog/emotet-lokibot-trickbot-still-impacting-enterprise-environments-globally-20909.html

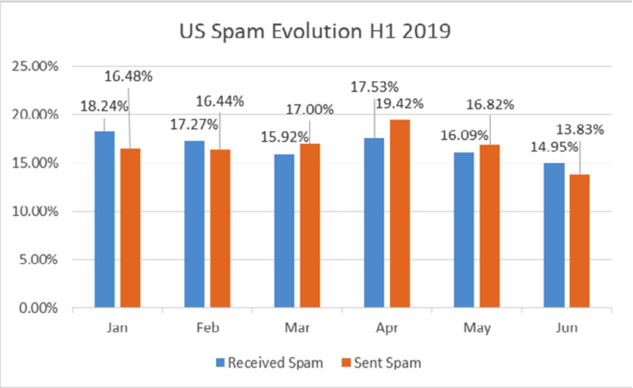
[24] **Bitdefender, “Is Dyre Trojan making a comeback?”**. https://hotforsecurity.bitdefender.com/blog/is-dyre-trojan-making-a-comeback-16952.html

[25] **EternalBlue, Wikipedia**. https://en.wikipedia.org/wiki/EternalBlue

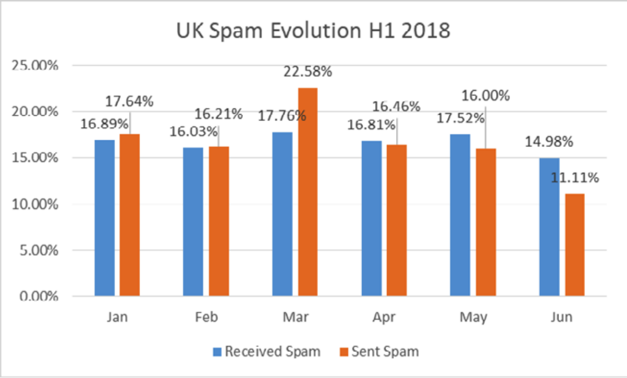
[26] **GitHub, Mimikatz**. https://github.com/gentilkiwi/mimikatz/wiki

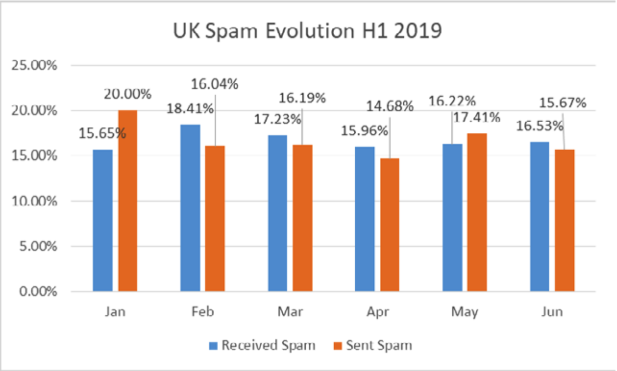
United States


US Spam Evolution H1 2018

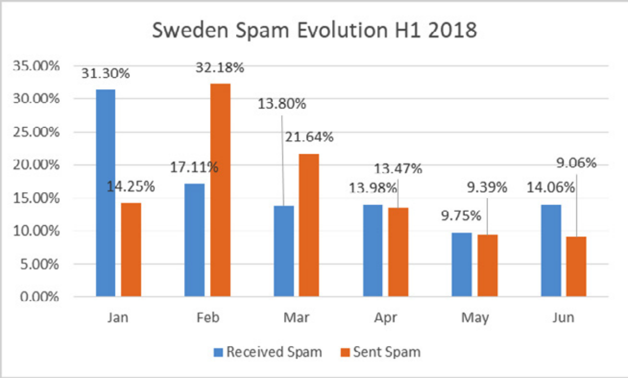

US Spam Evolution H1 2019

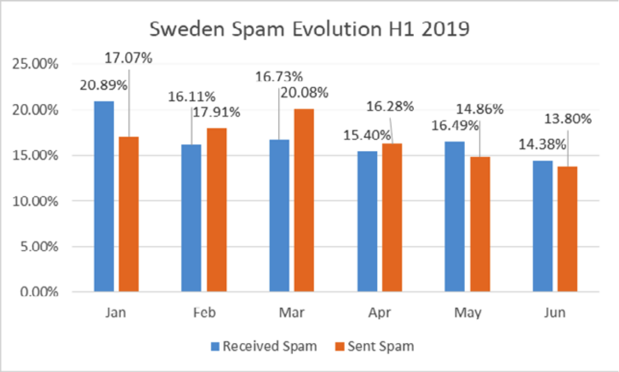
United Kingdom


UK Spam Evolution H1 2018

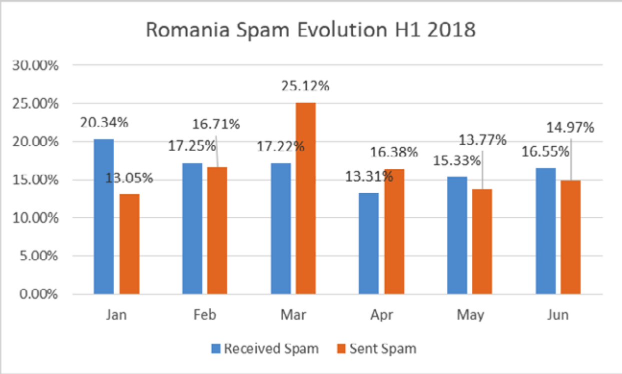

UK Spam Evolution H1 2019

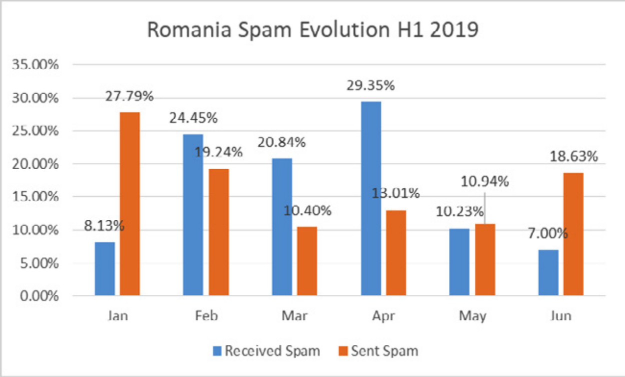
Sweden


Sweden Spam Evolution H1 2018

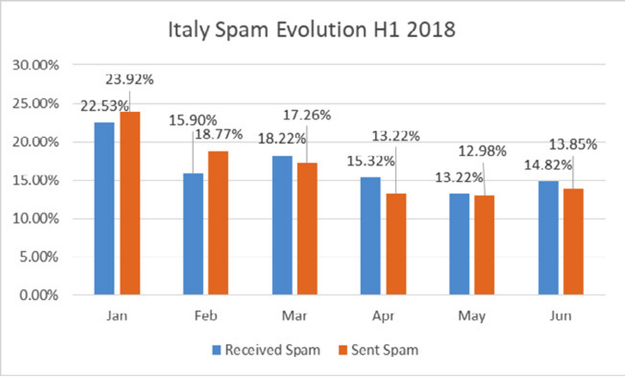

Sweden Spam Evolution H1 2019

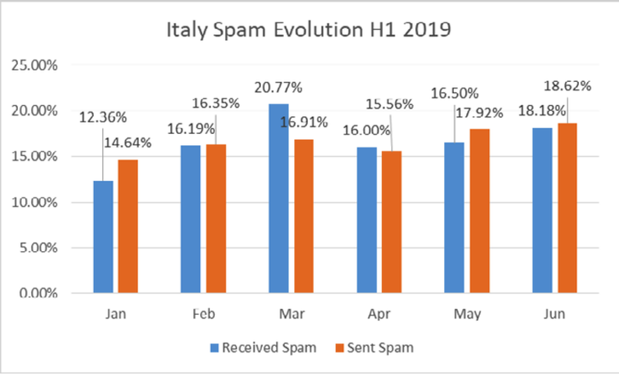
Romania


Romania Spam Evolution H1 2018

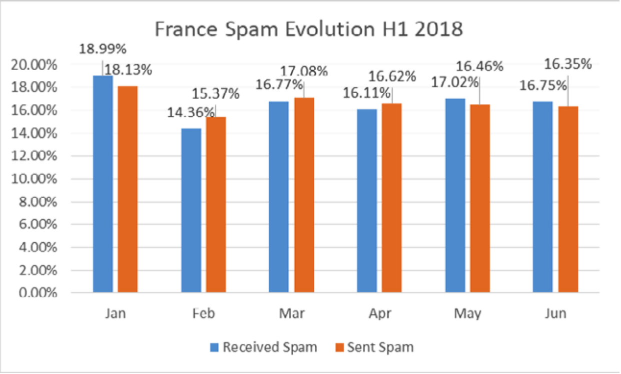

Romania Spam Evolution H1 2019

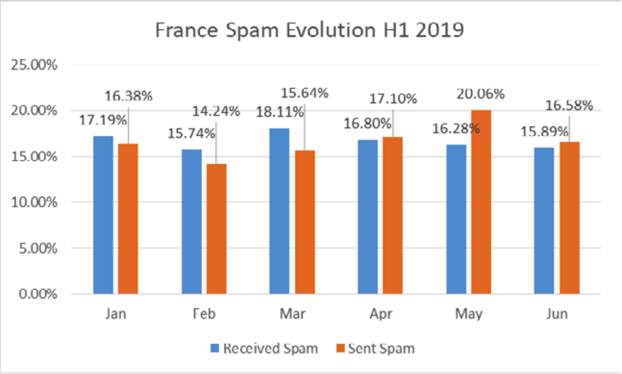
Italy



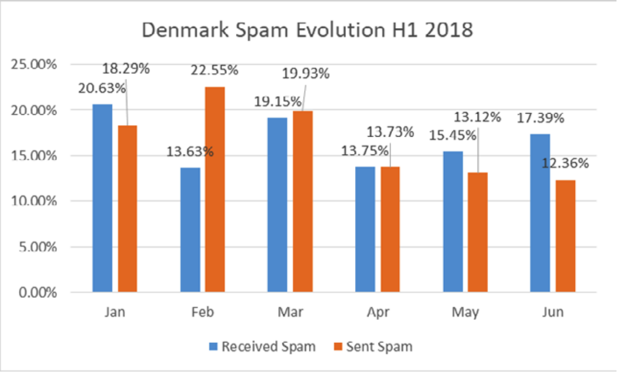


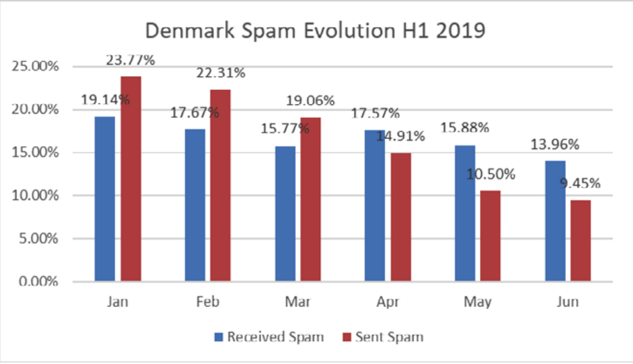
France



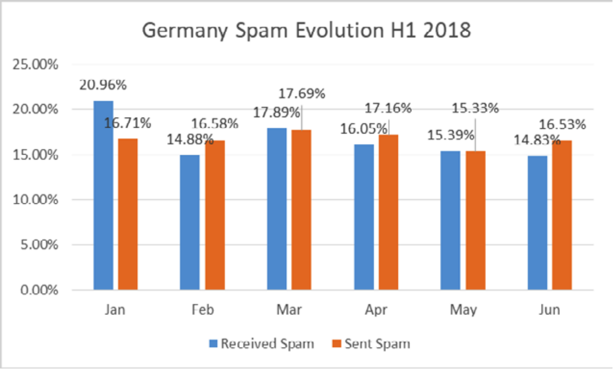


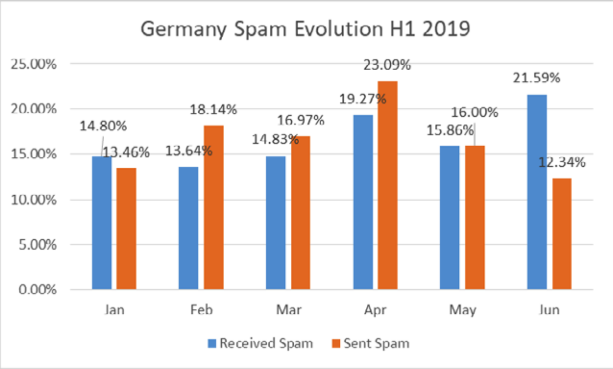
Denmark



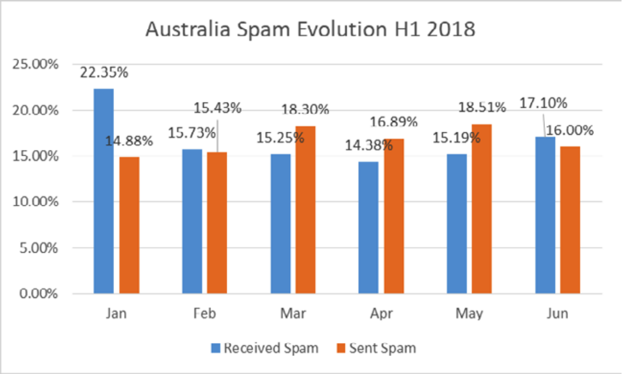


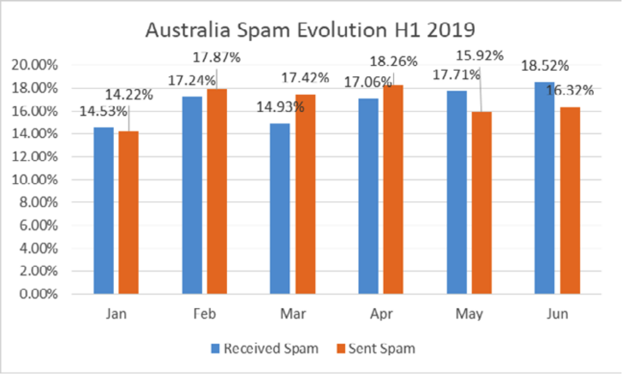
Germany



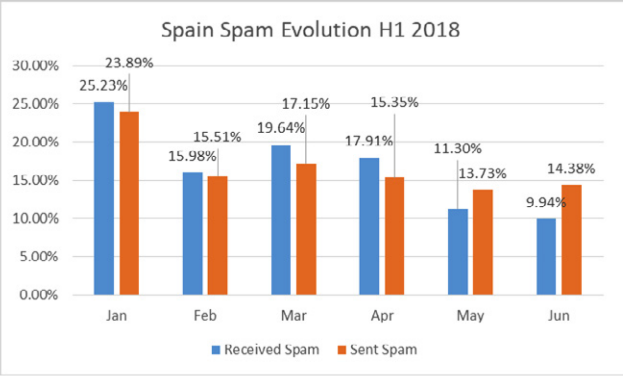


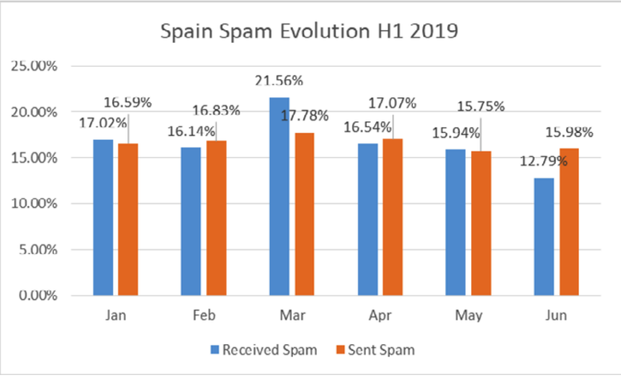
Australia





Spain





Business

Business Threats and Trends

Some **57 percent[27] of companies have experienced a breach** during the past three years and 24 percent already having suffered a breach half way through 2019. Meanwhile, the **36 percent of companies** fortunate enough to have dodged a potential cyberattack **believe it's likely they're currently facing one without knowing about it**.

“57%

of companies have experienced a breach”

As the threat landscape has grown more complex and more diverse, cybersecurity professionals have had to double down on efforts to devise new security strategies and employ new security solutions that can protect their business continuity.

While no organization is impervious to data breaches, the media's constant focus on security blunders that often leave organizations exposed contributes to reputational damage and causes frustration among security professionals. CIOs and CISOs are constantly looking for tools that can help them improve their understanding of cybersecurity, especially because of the ever-growing cybersecurity skills shortage.

“cybersecurity workforce gap is estimated to reach

1.8 million

by 2022”

Recent studies suggest that the **cybersecurity workforce gap is estimated to reach 1.8 million[28]** by 2022 – a 20% increase from 2015 – while 68% of workers in North America believe this shortage is caused by a lack of qualified personnel.

In a growing trend in the realm of ransomware, 2019 saw a spike in attacks targeting critical infrastructures and government institutions. Ransomware operators did not discriminate and ransomware strains like **LockerGoga, Ryuk and REvil (aka Sodinokibi or Sodin)** – spinoffs of the notorious GandCrab – dominated ransomware incident headlines in the first half of 2019. The most targeted verticals range from education, government, critical infrastructures (water distribution, power plants), healthcare, and services, all the way to MSPs (Managed service providers) whose offerings include cybersecurity services for a wide portfolio of clients.

Despite the fall of GandCrab, the number of ransomware reports targeting businesses steadily increased during the first half of 2019, with newer ransomware families filling in the void left behind by GandCrab.

While the extinction of one of the most prolific ransomware families might have been celebrated by both law enforcement and the security industry, the emergence of new families that share some similarities might make **business-targeting ransomware more resilient than ever**. At the same time, this doubling down and refocusing of efforts by the cybercriminal community means that the ransomware market is more mature and more versatile than ever.

Advanced persistent threats developed by nation-state actors or by highly organized cybercriminal groups should also woory organizations, especially those in the financial sector. Threat actors like APT28 and Carbanak have been known to use advanced and sophisticated techniques and malware to infiltrate both the public and private sector, fueled by motives ranging from espionage to financial gains.

While no industry vertical is safe from threats, the healthcare industry is among those most likely to suffer the brunt of attacks, either from ransomware or from vulnerabilities found in medical devices. As connected devices in healthcare become the new norm, with manufacturers rushing to get FDA approval for heart-rate and glucose monitors, some devices are more vulnerable than others and may put patient life and data at risk. In fact, the FDA has issued several safety communication in recent months, warning of vulnerabilities in implantable cardioverter defibrillators (ICDs) and cardiac resynchronization therapy defibrillators (CRT-Ds)[29], as well as insulin pumps[30]. As a result, smart medical devices connected to the internet are just as vulnerable as, if

[27] **Bitdefender, “Hacked off”**.
https://www.bitdefender.com/files/News/CaseStudies/study/285/Bitedefender-Hacked-Off-Report.pdf

[28] **(ISC)^2, “Global Information Security Workforce Study”**.
https://www.isc2.org/News-and-Events/Press-Room/Posts/2017/06/07/2017-06-07-Workforce-Shortage

[29] **FDA, “Cybersecurity Vulnerabilities Affecting Medtronic Implantable Cardiac Devices, Programmers, and Home Monitors: FDA Safety Communication”**.
https://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-affecting-medtronic-implantable-cardiac-devices-programmers-and-home

[30] **FDA, “Certain Medtronic MiniMed Insulin Pumps Have Potential Cybersecurity Risks: FDA Safety Communication”**.

not more vulnerable, regular IoTs, except they have the potential to affect both lives and data if hacked by ill-intended parties.

Windows Threat Landscape for Businesses

The Windows threat landscape for businesses has been largely dominated by ransomware, fileless malware and web-based exploits. While previous Bitdefender reports did not include a split between consumer and business telemetry, this time we focus on how these threats have evolved in the first half of 2019, on a monthly basis.

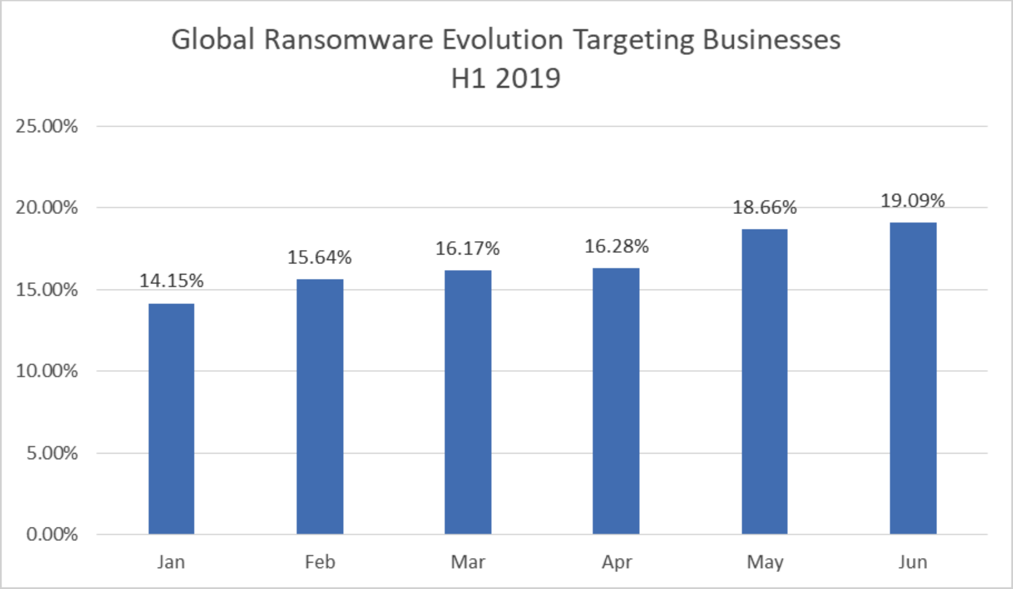
Ransomware

Ransomware has attracted the most media attention by far in news about incidents targeting critical infrastructure. Media reports show that attacks targeting critical infrastructures and government institutions spiked in 2019, with two particular incidents making headlines. The first one involves the city of New Bedford in the state of Massachussetts, which declined to offer attackers for $5.3 million to restore their affected systems. Instead, they made a modest counter-offer of $400,000, which seems to have been declined by attackers, leaving the city scrambling for solutions. Fortunately, IT administrators eventually managed to recover most of the lost data from backups.

The second incident was the attack in March on Norsk Hydro, the Norwegian aluminum and renewable energy company. It's believed operators used LockerGoga, a new strain of ransomware targeting Windows systems that emerged earlier this year. LockerGoga and BitPaymer are two flavors of the same ransomware family, sharing numerous similarities, such as the ransom note, file names and extensions, extortion methods, and more. Soon after hitting Norway, LockerGoga operators set their sights on two chemical companies in the United States: Hexion and Momentive.

Bitdefender reports on the monthly distribution of ransomware targeting organizations show that threat actors have steadily intensified their attacks using new or even revamped ransomware families, in the fall of GandCrab.

https://www.fda.gov/medical-devices/safety-communications/certain-medtronic-minimed-insulin-pumps-have-potential-cybersecurity-risks-fda-safety-communication

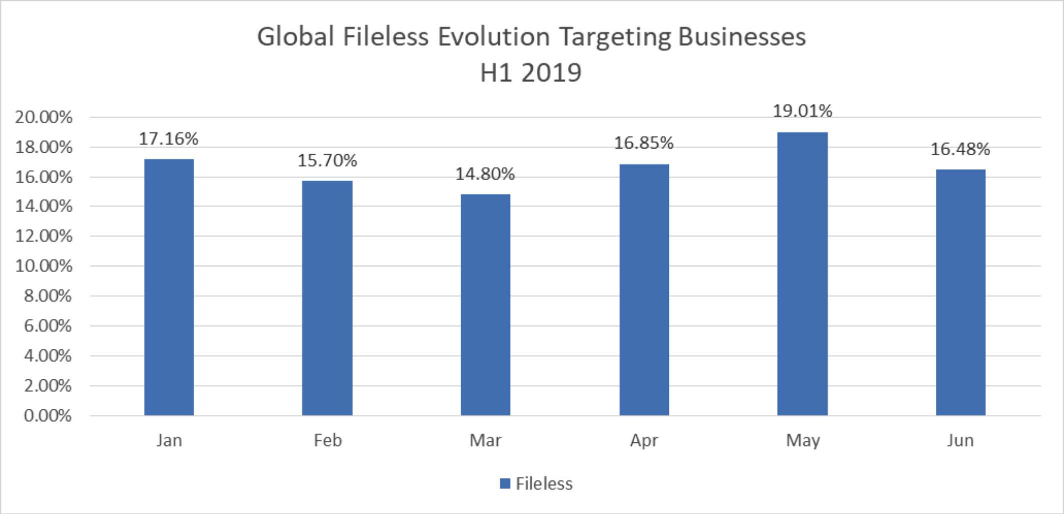


From January through June 2019, popular ransomware families that have proven effective in the past were steadily used against organizations. Everything from Crypt0l0cker, LockerGoga, Ryuk, and REvil (aka Sodinokibi or Sodin) all the way to Zepto, Locky, Cerber, and even WannaCryptor, has been reported by Bitdefender telemetry. With almost 300 ransomware families currently at their disposal, threat actors have constantly used at least 15 of the most popular ones.

Fileless Malware

Fileless malware has become a steady nuisance for organizations, as it's usually the most common attack vector – normally from spam emails – that yields success in infiltrating and deploying malicious payloads while dodging traditional security solutions. As most fileless malware leverages PowerShell or Visual Basic scripts embedded in spear-phishing emails, threat actors mostly use it as a first line of attack, whose purpose is to probe and assess the system for security solutions and then either broadcast specific information to a C&C (Command & Control) server or download additional malicious components.

Because it's so effective and stealthy, it's easy to understand why attackers don't give it up. This in turn causes security concerns for security professionals, who sometimes disable PowerShell or Microsoft Office Macros in an attempt to stop potential threats.

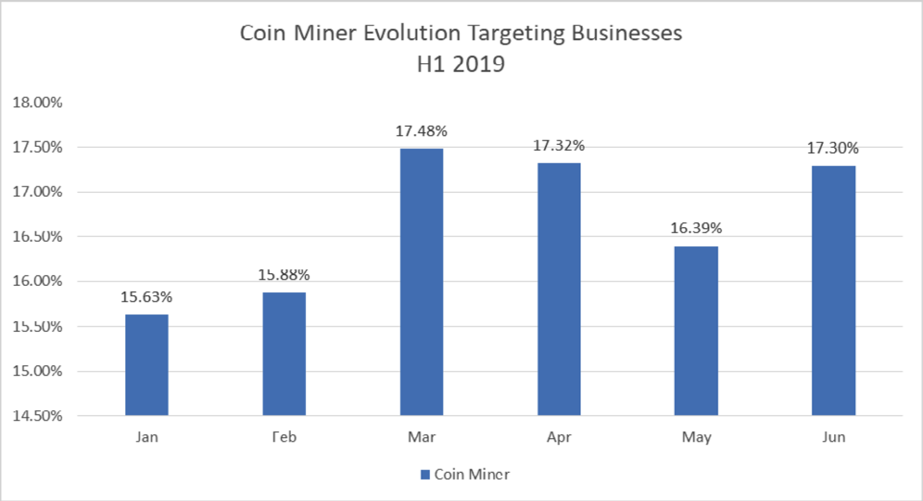


This increase in the number of reports regarding fileless threats targeting businesses in the first half of 2019 basically proves the old adage: "if it ain't broke, don't fix it".

Cryptocurrency miners

Another threat recently developed specifically to generate profit is **crypotojacking**. Cryptocurrency miners may have started as a consumer nuisance, but they ended up affecting businesses as well by going after computing-intensive cloud infrastructures. While a number of businesses and organizations have been affected by cryptocurrency miners being deployed in their cloud, most don't consider it a threat because it's seemingly benign.

However, a cryptojacking infection within an organization should be treated as a data breach -- if attackers managed to stealthily deploy and install a cryptocurrency miner, they could have also had access to other resources.



Bitdefender telemetry in business environments shows cryptocurrency miner reports intensified after seemingly plateauing during the first couple of months of 2019. While most cryptojacking attempts involve a web-based component, such as a compromised websites that an employee visits, some reports involve attempts to install actual cryptocurrency mining clients on endpoints.

IoT/Industrial IoT

Threat actors may abuse vulnerabilities in industrial IoTs and smart things in an organization's network to tamper with critical infrastructure equipment or even use them as gateways into the organization. However, more insidious attacks may involve creating panic by affecting down power grids[31] or by destroying industrial equipment[32]. The Triton[33] malware is one example of a threat designed to inflict physical destruction on industrial safety systems, potentially causing massive damage to oil and gas plants. Because it specifically targeted controllers designed to act as the last line of defense to avoid critical failures in industrial infrastructures, Triton was dubbed as the one of the world's most destructive pieces of malware.

The vast majority of vulnerabilities involving IoTs and industrial IoTs involve the lack of – or poor – authentication when remotely dialing in and controlling them. Industrial IoTs are even worse at this, as they were initially designed to accept parameters and instructions by having engineers directly connecting to them via serial ports, meaning authentication was not necessary if the person was already authorized to be near such devices. All that changed when serial-to-Ethernet adapters were introduced, enabling engineers to remotely configure these devices.

Some of the most common services usually exposed to the internet by these devices involve Telnet (Port 23), SSH (port 22), UPnP, and even UDP ports. Bitdefender has deployed a series of honeypots, mimicking the behavior of such vulnerable ports, and connected them to the internet to be probed by IoT malware and threat actors.

[31] **Wikipedia, Industroyer**.
https://en.wikipedia.org/wiki/Industroyer

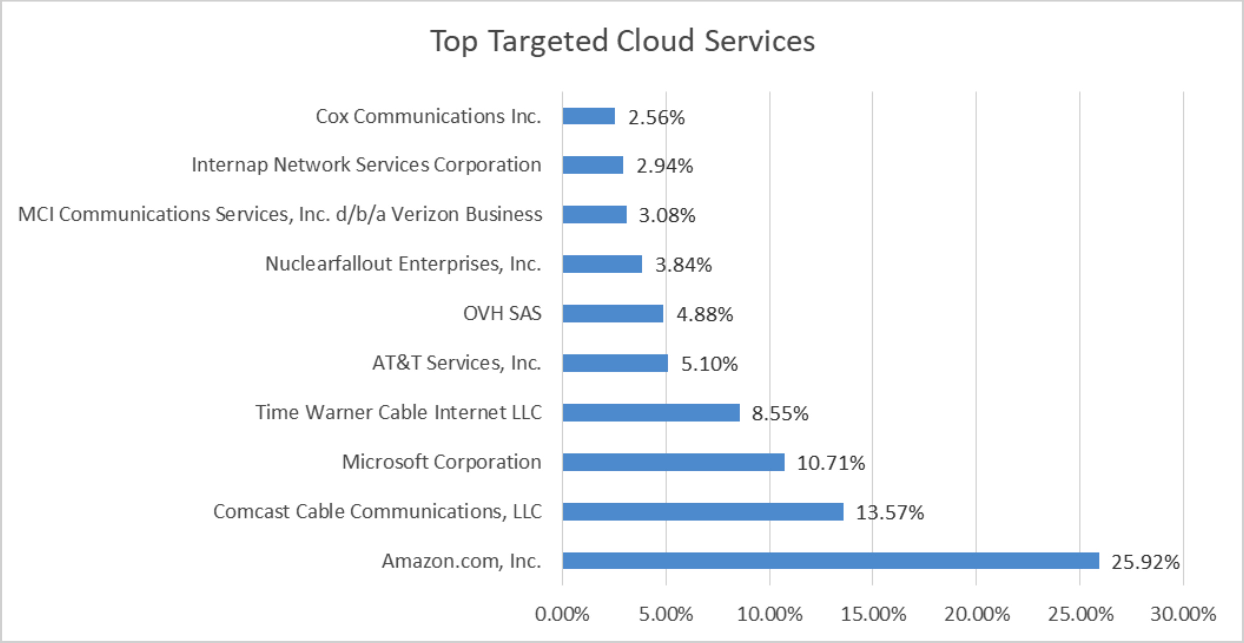
[32] **"A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try."**.
https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html

[33] **Wikipedia, Triton (malware)**.
https://simple.wikipedia.org/wiki/Triton_(malware)

The purpose of deploying honeypots is twofold: it helps security researchers assess the size and scope of a potential botnet that attempts to amass IoT devices by leveraging a specific vulnerability, and at the same time gain access to potentially new malware samples that have not yet been reported in the wild. These valuable pieces of intelligence can help security researchers learn more about the tactics and tools used by cybercriminals when compromising devices, and at the same time understand the motives of their operation.

Bitdefender honeypot telemetry from the first half of 2019 shows that attackers successfully **compromised the Telenet port more than 7.73 million times** using a combination of username and password. While this process is usually automated and left to scripts that either brute-force or try out commonly used usernames and passwords, it does show that the Telnet port is actively scanned for by IoT malware and threat actors.

As a result of successfully compromising our honeypots, they were instructed by C&C servers to perform **over 196,000 attacks on various infrastructures and services**, within the first half of 2019. In fact, some of these attacks' most targeted infrastructures and services were hosted by Amazon, Comcast, and even Microsoft. While our honeypots never participated in actual attacks on those infrastructures, but only received instructions to do so, it was interesting to see who attackers were targeting.



These attacks were likely not intentionally directed at Amazon per-se – 25.92 percent of all attacks reported within the first half of 2019 – but rather towards services hosted by the cloud service provider.

After being infiltrated, Bitdefender honeypots were instructed to download various files, such as scripts, malware, and even executable files, totaling **over 14.34 million artefacts**. This means that threat actors were not only trying to get into devices, but also ensure persistency by deploying tools or malware designed to either ensure a foothold or move laterally across the network to find and compromise other devices.

With the help of these honeypots, we were able to infiltrate hundreds of IoT botnets and see the type of instructions they would receive, where their command and control servers were located, and potentially learn the size of the botnets.

However, since the same IoT vulnerability can easily be exploited by another IoT malware or threat actor, some of these compromised devices can change ownership several times a day. This means that, while some IoT malware can amass a large botnet very quickly, control over that number of devices can fluctuate wildly, as botnet operators compete with each other.

MSP (Managed Service Providers)

“72%

of security professionals believe that a lack of the right tools and knowledge are the main obstacles to rapid incident repose”

While large organizations may be able to flex their cybersecurity budgets and invest in building cybersecurity teams and their own internal SOC (Security Operations Center), SMBs are usually constrained by a lack of budget and qualified personnel. Consequently, **72 percent[34] of security professionals** believe that a lack of the right tools and knowledge are the main obstacles to rapid incident repose.

Outsourcing some **security challenges to MSPs** is now considered an appealing option for businesses, especially since it’s been proven to keep operational costs low while ensuring that incident response and breach detection times are within industry standards. However, this places a huge burden on MSPs, who now need complete visibility into environments ranging from physical and virtual to cloud-based and on premise.

On top of that, MSPs are increasingly targeted by threats and cybercriminals, as they hold the keys to the crown jewels for all their clients, potentially enabling threat actors to access a far wider and more diverse pool of systems and data with the compromise of just one target. Consequently, the compromise of a single MSPs can damage reputation and trust across their entire client portfolio. Even the DHS Cybersecurity and Infrastructure Security Agency (CISA) recently[35] issued cybersecurity guidance for service providers, urging them to take action and improve their cybersecurity capabilities in light of the growth in attacks targeting them.

Another option for organizations facing these cybersecurity challenges is to turn to **MDR (Managed Detection and Response) services**, which is basically an outsourced SOC comprised of experienced security analysts who monitor detailed telemetry to quickly and effectively respond to malicious activities, while actively removing threats and reducing dwell time and limiting any damage to the organization. Besides garden-variety threats, the services also defend against modern threats and advanced attacks.

Ransomware

MSPs have increasingly been targeted by ransomware in the past couple of years, especially by GandCrab. Ransomware-as-a-service operations have found MSPs particularly vulnerable to these threats – and potentially more profitable – as MSPs usually have access remote direct access to client infrastructures.

Either by compromising MSPs via RDP (Remote Desktop Protocol) using stolen or brute-forced credentials or by phishing employees and gaining access to the remote technical support services used to manage client infrastructures, GandCrab operators would use MSPs to launch attacks on dozens of organizations.

Consequently, instead of compromising individual organizations managed by MSPs, they would compromise as many as possible by dialing into them and manually deploying GandCrab ransomware samples and tweaking the ransom note based on the victim’s profile.

While security researchers and law enforcement went to great lengths to offer victims proactive protection against ransomware as well as free decryption[36] tools for various GandCrab versions, new ransomware families have emerged in the fall of GandCrab.

Sodinokibi (aka REvil or Sodin) is a new ransomware-as-a-service that security researchers believe is operated by the group behind GandCrab.

While GandCrab may have had its reputation spotted by successful attempts from law enforcement and the security industry to help victims recover their files, this new and equally potent ransomware family starts with a clean slate.

[34] **Bitdefender, “Hacked off”**. https://www.bitdefender.com/files/News/CaseStudies/study/285/Bitedefender-Hacked-Off-Report.pdf

[35] **CISA, “Chinese Malicious Cyber Activity”**. https://www.us-cert.gov/china

[36] **Bitdefender, “GandCrab Ransomware decryption tool”**. https://labs.bitdefender.com/2018/10/gandcrab-ransomware-decryption-tool-available-for-free/

Consequently, MSPs can’t yet breathe easily in the face of ransomware attacks. Instead, they may actually be more targeted by several spin-offs of GandCrab.

However, the attack methods used to compromise MSPs and their clients may revolve around the same techniques as before, which means everything from spearphishing emails with tainted email attachments, to RDP compromise and the exploitation of various vulnerabilities found in the remote management tools MSPs use to manage client infrastructures.

Spam and BEC

> **“volume of spam increased by an average of**
>
> **48%**
>
> **year-over-year”**

While the **volume of spam increased by an average of 48 percent year-over-year**, according to Bitdefender telemetry, the financial losses caused by BEC (Business Email Compromise)[37] attempts seem to be one of the highest among emails scams. In fact, BEC scams have skyrocketed during the past couple of years.

These types of scams usually target companies by sending deceptive messages to business email addresses in an attempt to convince employees to transfer company funds to attacker-controlled bank accounts.

Also known as man-in-the-email scams, attackers exploit the social engineering to create a sense of urgency and legitimacy surrounding the scam email, usually impersonating the CEO or an executive entitled to authorize wire transfers.

Recent stats published by The Financial Crimes Enforcement Network FinCEN[38] - a bureau of the United States Department of the Treasury – reveal more than 32,000 cases of attempted theft via BEC, totaling **$9 billion, since September 2016**.

The same authority states that the number of BEC reports has increased from just under 500 per month in 2016 to over 1,100 monthly reports in 2018, averaging over $300 million per month in total attempted BEC thefts.

The most common topics range from bogus invoices and CEO impersonation, all the way to actually compromising an executive’s account and using it to send the email, impersonating various attorneys or law firms, and even stealing tax statements of employees and executives to make the emails more personal and compelling.

The manufacturing and construction, commercial services, and real estate sectors account for 59 percent of all BEC scams, and organizations need to start training their employees to spot them, set in place procedures to prevent single-point-of authorization, and invest in email security solutions that can correctly tag these email as scams.

As most of these scams have no attachment that needs to be executed by employees, they usually fly below the radar of traditional email filtering security solutions, eventually ending up in employee inboxes.

SMB

Most SMBs focus on fast growth, aggressive expansion and maximizing profit. These strategic business decisions seldom include an incident response plan to ensure business continuity in the event of a cybersecurity incident that endangers company data regarding their clients or their intellectual property. Recent surveys show that about 60 percent[39] of SMBs lack an incident response plan and that 66 percent of business leaders don’t believe they’ll be hit by a cyberattack.

While the popular belief amongst SMBs is that they’re too small to be targeted by threat actors, they’re more valuable than they think. Because they often deal with sensitive customer data and provide services for larger organizations, SMBs can be far more lucrative targets than large businesses.

[37] **Wikipedia, Business Email Compromise (BEC),** https://en.wikipedia.org/wiki/Business_email_compromise

[38] **FinCEN, “Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business Processes”,** https://www.fincen.gov/sites/default/files/advisory/2019-07-16/Updated%20BEC%20Advisory%20FINAL%20508.pdf

[39] **Keeper Security, “The 2019 SMB Cyberthreat Study”,** https://keepersecurity.com/blog/2019/07/24/cyber-mindset-exposed-keeper-unveils-its-2019-smb-cyberthreat-study/

Cybersecurity may have become a top priority for more than 80 percent[40] of SMBs, but surveys show that around 30 percent spend less than $100,000 on cybersecurity per year. While the cost of a cyberattack on small companies may be non-trivial, about 60 percent[41] of SMBs that have suffered of a cybersecurity incident may end up going out of business within the next six months. Coupled with the lack of understanding, preparedness, and budget allocation for cybersecurity, SMBs may be the most vulnerable to cyberattacks in terms of business continuity.

A continued lack of budget, talent and training often leaves SMB employees vulnerable to cyberattacks ranging from garden-variety malware to ransomware and even sophisticated threat actors that use SMBs and their infrastructure as attack platforms for cyberattacks on larger organizations. This lack of funding even makes it difficult or SMBs to identify and also remediate any attacks that have been targeting them, potentially causing them to turn to MSPs that can deliver security services at a fraction of the costs.

While GandGrab posed serious concerns for SMBs, its fall has opened the market for new contenders in the ransomware-as-a-service business, in the likes of Sodinokiki (aka REvil or Sodin). Security researchers believe the group behind GandCrab may also operate Sodinokibi, and SMBs still face the same risk of compromise.

If anything, the maturity and diversification of ransomware-as-a-service may make it more difficult for SMBs as they have to protect against more than one ransomware family, while the same attack techniques could still be employed in terms of delivery mechanisms and compromise.

Consequently, installing a multi-layered security solution that can identify and prevent ransomware from being deployed, perform constant backups of critical data, as well as maintain a strong patching policy, is a basic security principle for SMBs aiming to minimize potential ransomware infections.

Whether it be GandCrab, Sodinokibi, or any other ransomware-as-a-service family, SMBs will continuously be targeted unless they start increasing the cost of attack for threat actors and proactively deploying security mechanisms that limit or prevent the fallout of a ransomware infection and data loss.

[40] **Untangle, "2019 SMB IT Security Report",** https://www.techrepublic.com/article/budget-constraints-pose-the-highest-threat-to-smb-it-security/

[41] **Hiscox, "2018 HISCOX Small Business Cyber Risk Report ™",** https://www.hiscox.com/documents/2018-Hiscox-Small-Business-Cyber-Risk-Report.pdf

Bitdefender is a global security technology company that delivers solutions in more than 100 countries through a network of value-added alliances, distributors and reseller partners. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a leading security provider in virtualization and cloud technologies. Through R&D, alliances and partnership teams, Bitdefender has elevated the highest standards of security excellence in both its number-one-ranked technology and its strategic alliances with the world's leading virtualization and cloud technology providers.
More information is available at http://www.bitdefender.com/.