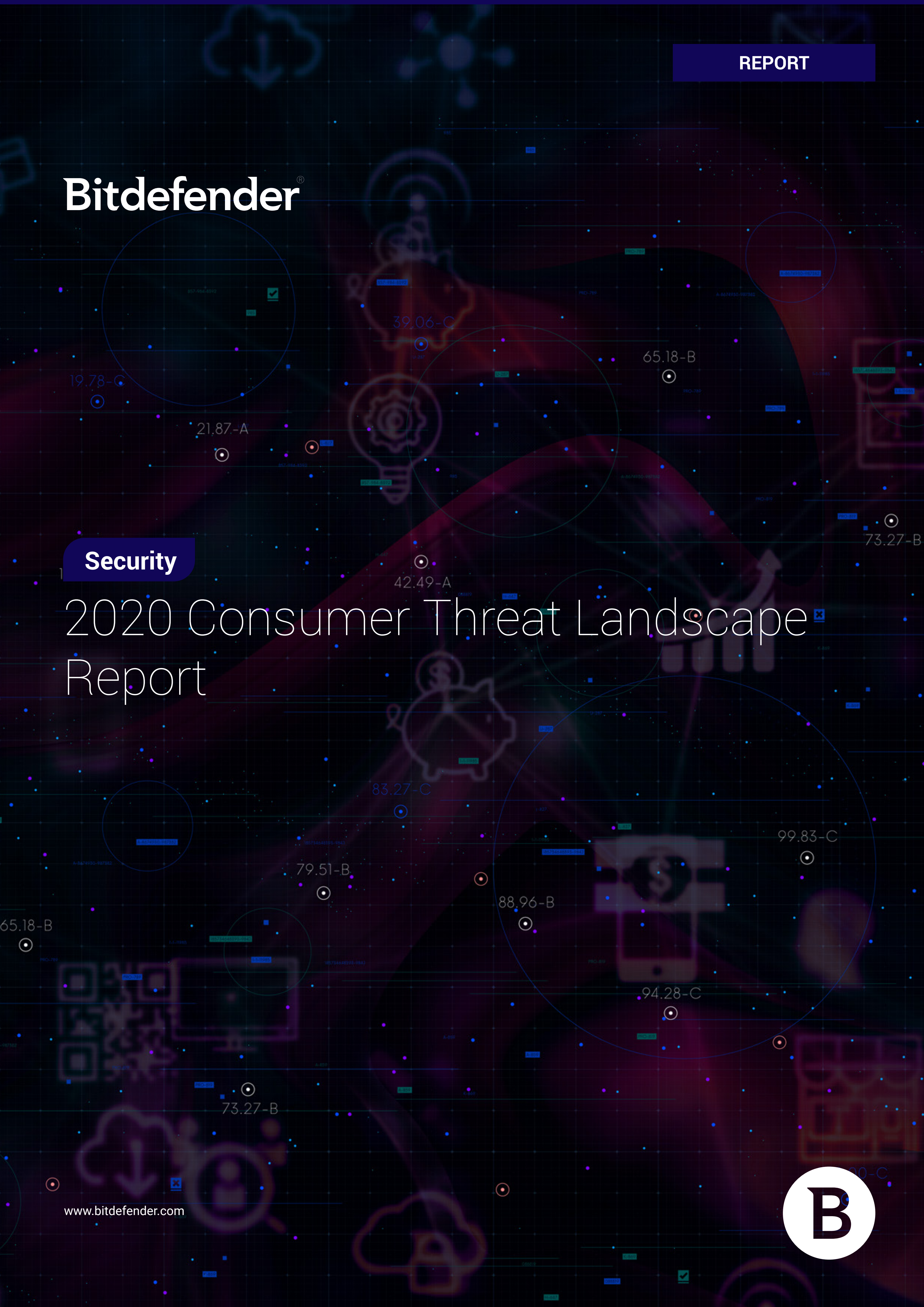
REPORT

Bitdefender®



Security

2020 Consumer Threat Landscape Report

www.bitdefender.com

Contents

Executive Summary:

While 2020 was not a typical year for average users or organizations, threat actors and threats thrived and even evolved in light of the global pandemic caused by the COVID-19 virus. The consumer threat landscape report for 2020 is meant as an overview of the evolution of threats year-over-year and on a quarterly basis, in an attempt to highlight trends that will likely spill into 2021. From how ransomware has evolved both globally and in specific countries, to Android threats, IoT and spam, Bitdefender consumer telemetry aims to capture a snapshot of what threats targeted the average user and how to best protect against them. With a 485 percent increase in year-over-year (YoY) global ransomware reports in 2020 compared to 2019, according to Bitdefender telemetry, threat actors have doubled down on what was already a very lucrative business. Potentially unwanted applications (PUAs) might not be malicious per se, but they can irritate the average user by behaving in a way that may cause system slowdowns, display unexpected ads, or even install additional software. With a 320 percent increase in YoY global PUA reports, it's likely that more users encountered these types of applications last year than during 2019.

However, while the increase might be significant, the overall distribution of PUA reports throughout both 2019 and 2020 is similar, suggesting a consistent and sustained growth throughout the year. The evolution of some popular Trojans throughout 2020 was sometimes wildly inconsistent. While some popular Trojans like TrickBot and Emotet were immensely popular throughout the year, they evolved differently in each quarter in terms of reports. During the first half of 2020, TrickBot reports accounted for 68 percent of all TrickBot reports throughout the year, but the second half of 2020 saw a dramatic decrease in reports, potentially due to kneecapping1 operations performed by law enforcement in an attempt limit the potential damage TrickBot operators could have caused ahead of the U.S. elections. While Emotet was often used in conjunction with Trickbot, its popularity among threat actors seems to have skyrocketed in the second half of 2020 compared to the first half. The second half accounted for 84 percent of all Emotet reports throughout the year. With TrickBot quietly trying to rebuild2 its infrastructure, cybercriminals likely turned to Emotet operators in an attempt to continue their operations.

Since the world had to adapt to remote work, and staying at home became the new normal, threat actors have also updated their spam-sending tactics by focusing more on delivering seemingly legitimate emails, in an attempt to maximize their chances of infecting users. With fewer typos, more jargon, and the use of legitimate logos when impersonating companies and organizations, cybercriminals fully used their social engineering skills to create believable spam messages. Either capitalizing on their recipients' curiosity or exploiting that users and service providers have started interacting more online, cybercriminals often deployed themed spam campaigns Android was also plagued by fake applications impersonating popular video conferencing software and medical applications, with significant spikes during April and May, which accounted for 14 percent and 12 percent, respectively, of the total number of reports in 2020, according to Bitdefender telemetry. However, strictly looking at the year-over-year evolution of the second half of 2020 compared to the same period a year earlier, the number of reported Android threats rose 32 percent.

As the pandemic pushed employees to work from home, work devices most likely started sharing a network with other potentially vulnerable internet-connected devices, raising security concerns for organizations. However, this shift in workforce might have also affected IoT buying decisions, as it's likely more people started thinking of purchasing new routers, new or additional smart TVs, network attached storage devices, and even smart media players. When analyzing Bitdefender IoT telemetry for the second half of 2020, we found a 220 percent YoY increase in the number of reported media player devices. The number of reported network attached storage devices (NAT) during the second half of 2020 also increased by 81 percent compared to the second half of 2019. These spikes could indicate users became more interested in consuming and storing content, potentially caused by travel restrictions imposed by the pandemic.

[1] "New action to combat ransomware ahead of U.S. elections", Microsoft, https://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-elections/
[2] "TrickBot is Dead. Long Live TrickBot!", Bitdefender, https://labs.bitdefender.com/2020/11/trickbot-is-dead-long-live-trickbot/

Key Findings:

- 485 percent increase YoY in global ransomware reports
- 53 percent drop in TrickBot reports during the second half of 2020
- 449 percent increase in Emotet reports during the second half of 2020
- 320 percent increase YoY in global PUA reports
- 32 percent increase in reported Android threats during second half of 2020 compared to second half of 2019

Challenges Brought by the New Normal

Without a doubt, while 2020 was an atypical year for everyone, it was more so from a cybersecurity or cyber threats perspective. From a spam and phishing perspective, attackers would focus on creating simple and generic messages aimed at being as vague as possible in an attempt to trick victims into clicking on a link or opening an embedded attachment. However, the pandemic proved to be a new opportunity for exploiting a highly popular topic and increasing the success rate of spam and phishing by focusing more on the content and social engineering aspect of the message. As reported[3] in our mid-year threat landscape report, spam messages dropped typos in favor of adequate jargon, legitimate logos, and even impersonating real figures.

This trend was repeated successfully throughout 2020, with cybercriminals creating campaigns aimed at exploiting every aspect that changed in our way of interacting with service providers from banking institutions to delivery services. Distinguishing spam from legitimate messages has become more difficult amid a shift from increasing the volume of spam sent to increasing the success rate of campaigns. While spam messages mostly delivered the same banking Trojans or ransomware families we've seen in the past, cybercriminals seemingly opted for better open rates by focusing more on quality than quantity.

Coronavirus-themed spam messages might have been the theme for the first half of 2020, but banking services, delivery services, and even travel services were among the most popular themes during the second half. For example, a series of phishing campaigns impersonating online banking[4] services were spotted during specific days in September, October and November.

As for more traditional threats that have plagued both users and organizations, ransomware also had an interesting 2020. Adding double extortion to its features in an attempt to further pressure the victim into paying, ransomware also started being delivered by two of the most popular botnet infrastructures -- TrickBot and Emotet. The affiliate model, also known as the –as-a-service model, had ransomware groups working with botnet operators and selling access to those package services in an attempt to maximize shared profits. This strategic approach between ransomware and botnet operators has led to ransomware families like Maze, Egregor and Ryuk making more headlines in the media than before, and potentially boosting profits for cybercriminals.

While this cooperation between threat actors might trigger a new trend in terms of organized cybercrime, ransomware was also augmented with an additional extortion component. Threatening victims with publishing the stolen data accessed before the encryption, ransomware operators add more pressure on their victims to pay, otherwise risking public shaming and reputational damages.

Remote work may have also affected not just organizations but also employees as their home networks featuring personal devices and IoTs now started accommodating enterprise-grade devices. With most security researchers

[3] "Mid-Year Threat Landscape Report 2020", Bitdefender, https://www.bitdefender.com/files/News/CaseStudies/study/366/Bitdefender-Mid-Year-Threat-Landscape-Report-2020.pdf
[4] "Spammers Get Better at Impersonating Banking Services, Use Lingo and Legit Layouts to Con Victims", Bitdefender, https://hotforsecurity.bitdefender.com/blog/spammers-get-better-at-impersonating-banking-services-use-lingo-and-legit-layouts-to-con-victims-24805.html

deeming internet-connected smart devices prone to vulnerabilities, devices such as smart IP camera surveillance devices[5], smart light bulbs[6], smart locks[7], baby monitors[8], and even smart doorbells[9] could pose security risks that attackers may exploit to compromise other devices sharing the same network.

However, remote work may have also influenced shopping habits, as it's likely that IoT purchases increased. Bitdefender's IoT telemetry alone revealed that, during the second half of 2020, one of the most commonly reported household devices was network attached storage devices (NAS), accounting for 22 percent of all reported IoTs during the second half of 2020. Media players, IP cameras, TVs and routers are next, suggesting that they are the most common smart devices in households.

These new changes and trends in the threat landscape will likely spill over into 2021. Cybercriminals will likely reuse everything they learned and that proved successful during 2020 and users will also have to adapt to better identifying and mitigating potential threats. Whether its IoTs, ransomware, spam, phishing, or Android threats, the 2020 threat landscape proved that cybercriminals are fast to adapt and highly opportunistic, and that panic, fear and misinformation can become powerful tools in the hands of threat actors.

Windows Threat Landscape

To remain consistent with previous Bitdefender threat landscape reports, when analyzing the Windows threat landscape for the entire 2020 we considered the same type of threats and compared their YoY evolution on a quarterly basis. While some threats have experienced significant spikes in terms of number of YoY reports, in some instances their quarterly evolution was consistent across the entire year.

Interestingly, individually analyzing telemetry from specific countries has revealed that threat actors may sometimes lean on very specific threats when planning their campaigns, potentially in an attempt to maximize their efforts.

Throughout the following threat landscape we'll be taking a closer look at telemetry for ransomware, coin miners, fileless malware, exploits and bankers, analyzing both their global and regional evolution.

Global Evolution of Windows Threats

Throughout 2020 there were numerous incidents involving massive botnets distributing ransomware infections or spam and spearphishing campaigns that were executed with great attention to detail in an attempt to net as many victims as possible without arousing suspicion.

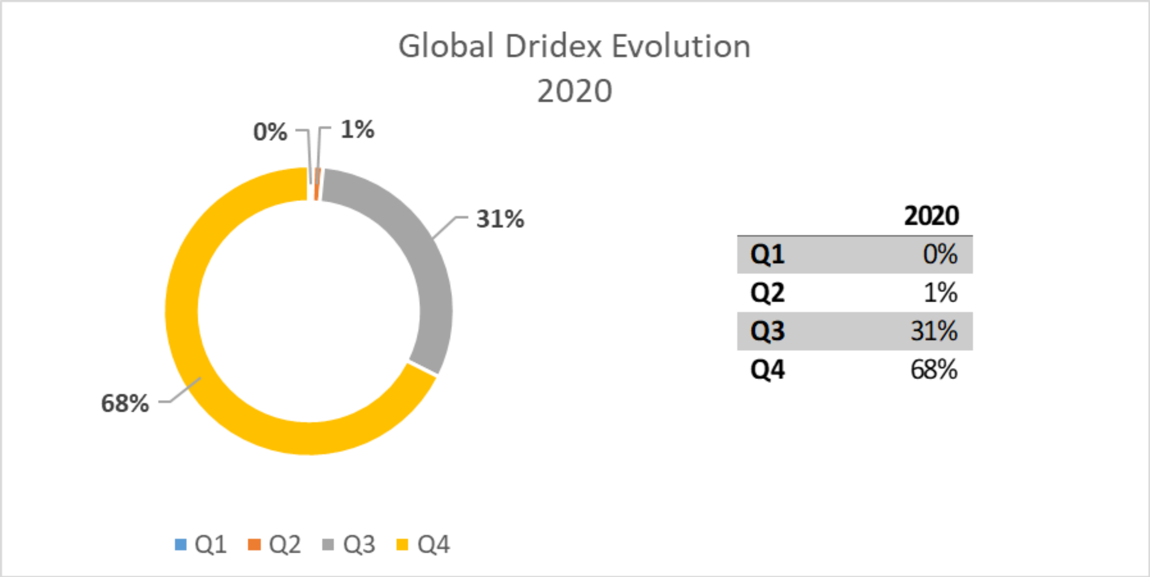
Popular banking Trojans like Dridex, Emotet, Trickbot and AgentTesla were also quite popular among cybercriminals in 2020. While some of these Trojans focused on individually collecting personal or financial data from victims, others were used as a means to deliver ransomware or even additional Trojans.

[5] "Cracking the LifeShield: Unauthorized Live-Streaming in your Home", Bitdefender, https://labs.bitdefender.com/2021/01/cracking-the-lifeshield-unauthorized-live-streaming-in-your-home/
[6] "When the Lights Go Out: Cracking the Sonoff / eWeLink Platforms", Bitdefender, https://labs.bitdefender.com/2020/12/when-the-lights-go-out-cracking-the-sonoff-ewelink-platforms/
[7] "Smart Locks Not So Smart with Wi-Fi Security", Bitdefender, https://labs.bitdefender.com/2020/08/smart-locks-not-so-smart-with-wi-fi-security/
[8] "Severe Vulnerability in iBaby Monitor M6S Camera Leads to Remote Access to Video Storage Bucket", Bitdefender, https://labs.bitdefender.com/2020/02/severe-vulnerability-in-ibaby-monitor-m6s-camera-leads-to-remote-access-to-video-storage-bucket/
[9] "Ring Video Doorbell Pro Under the Scope", Bitdefender, https://labs.bitdefender.com/2019/11/ring-video-doorbell-pro-under-the-scope/

Dridex

The Dridex financial Trojan has been known to be quite versatile when used by cybercriminals, as it can take screenshots from victims' systems, steal credentials and even perform distributed denial of service attacks if operators have a sufficiently massive botnet of compromised systems.

Looking at the global evolution of Dridex reports, our telemetry revealed that the second half of 2020 was the most active for Dridex operators. **The last quarter of 2020 alone reported 68 percent of all global Dridex reports from the entire year.** Dridex activity did start to pick up in the third quarter of 2020, and the second half was the most active for Dridex operators.



	2020
Q1	0%
Q2	1%
Q3	31%
Q4	68%

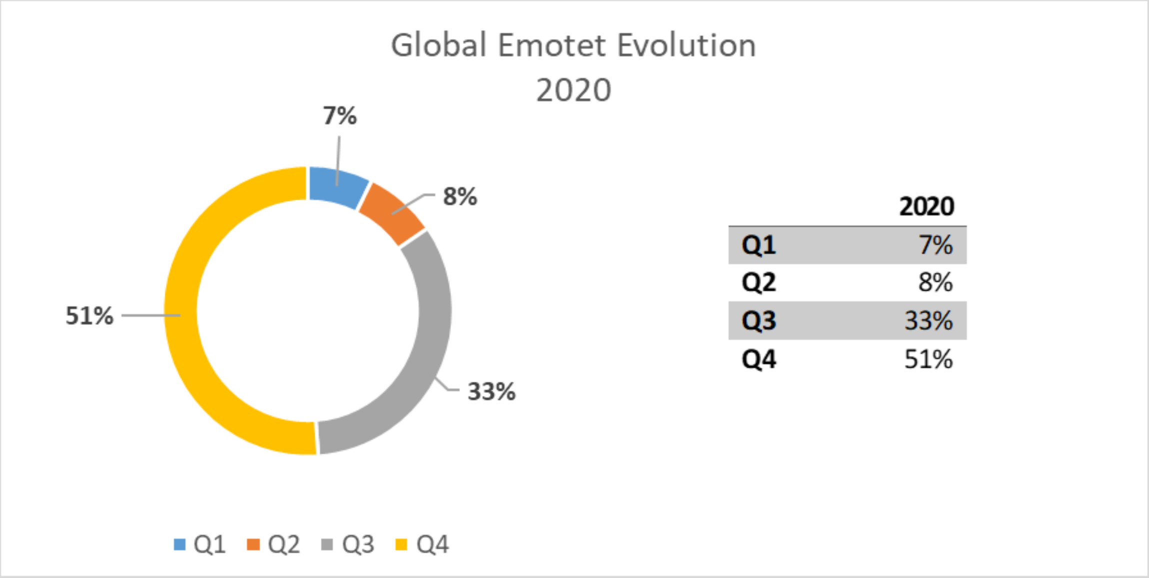
Fig. 1 - Global Dridex Evolution 2020

Emotet

Emotet and Trickbot have frequently been spotted together, usually one delivering the other. However, their massive botnet infrastructures were also used to deliver various strains of ransomware, with operators and potentially splitting profit.

Looking at how global **Emotet** reports evolved throughout the year, the second half of 2020 seems to have been extremely busy for Emotet operators. With the **last quarter of 2020 registering 51 percent of all global Emotet reports throughout the year**, it's likely cybercriminals turned to this particular botnet in light of recent operations[10] from law enforcement that crippled a large part of TrickBot's infrastructure.

[10] "New action to combat ransomware ahead of U.S. elections", Microsoft, https://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-elections/



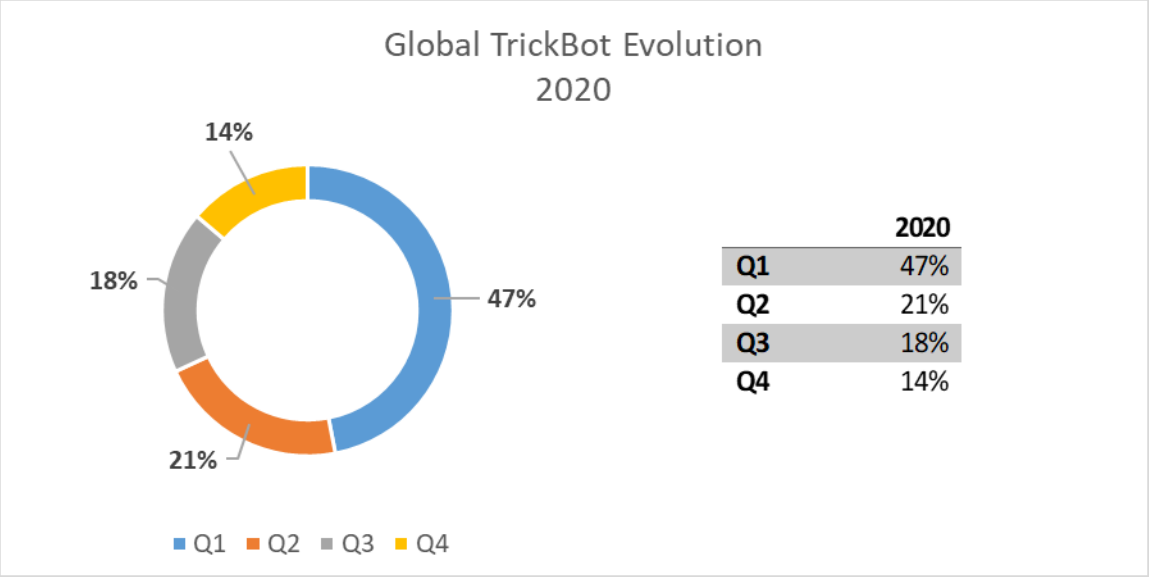
	2020
Q1	7%
Q2	8%
Q3	33%
Q4	51%

Fig. 2– Global Emotet Evolution 2020

TrickBot

This particular banking Trojan has been notoriously popular amongst cybercriminals because, apart from its primary purpose of collecting sensitive data and harvesting credentials from victims, it also packed features designed to move laterally across compromised networks and compromise other machines. This particular feature turned TrickBot into a powerful weapon as it made it highly resilient to cleanups and enabled ransomware operators to deliver payloads on high-value targets.

While TrickBot's operations might have been disrupted during the second half of 2020, Bitdefender telemetry shows that **TrickBot was at its peak during the first quarter, with 47 percent of all global TrickBot reports throughout the year**. Potentially capitalizing on the pandemic and being distributed via spam campaigns, TrickBot's popularity amongst cybercriminals seems to have been really high during the first half of 2020.



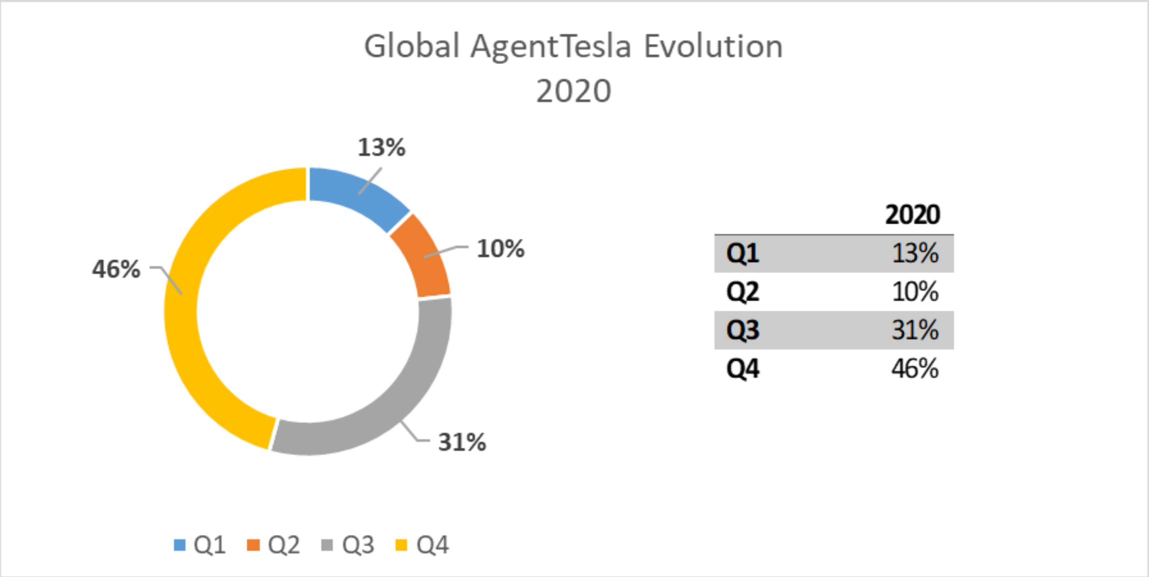
	2020
Q1	47%
Q2	21%
Q3	18%
Q4	14%

Fig. 3– Global TrickBot Evolution 2020

AgentTesla

This Trojan has been known since 2014 for its password-stealing capabilities, and the adoption of an as-a-service business model has also turned it into a go-to choice for cybercriminals either seeking a botnet or a data-stealing Trojan.

Much like Emotet's evolution throughout 2020, AgentTesla's popularity seems to have peaked during the second half of 2020. With **Q4 accounting for 46 percent of all global AgentTesla reports throughout the year**, it's likely that cybercriminals turned to this particular Trojan after TrickBot's kneecapping operations. However, AgentTesla is mostly known for being distributed via spam campaigns and having a wide range of surveillance, data-stealing and security-dodging features.



	2020
Q1	13%
Q2	10%
Q3	31%
Q4	46%

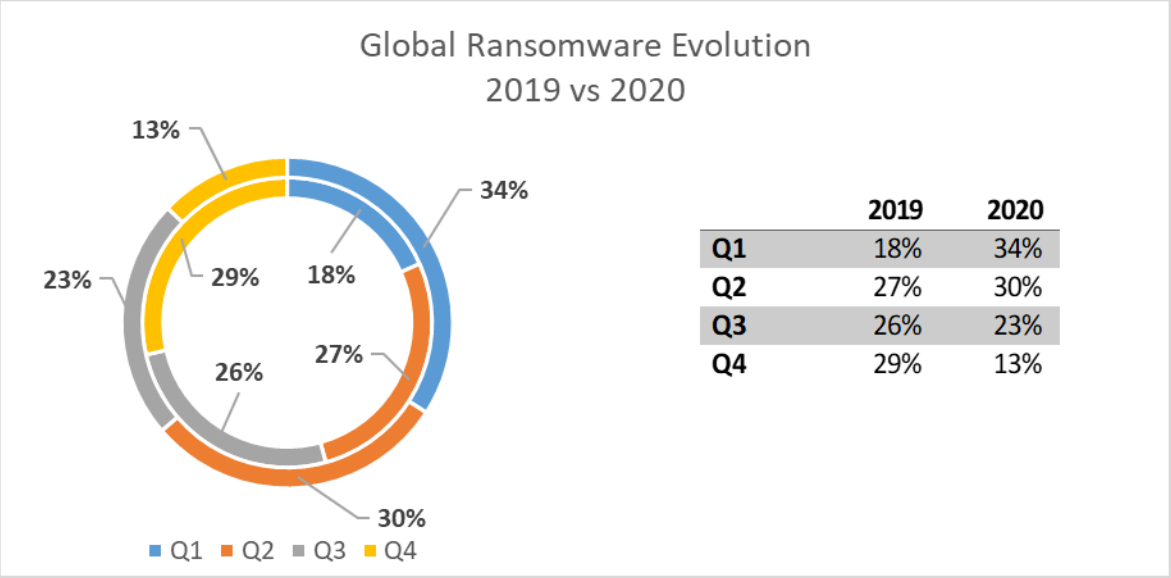
Fig. 4 – Global AgentTesla Evolution 2020

Ransomware

When looking at the year-over-year evolution of global ransomware reports, during 2020 we saw a 485 percent YoY increase. While this might not sound like the dramatic jump that we've grown accustom to seeing, it's likely because ransomware attacks have been more focused on maximizing profits by going after big targets.

"Big game hunting" is a tactic that ransomware operators seem to have adopted throughout 2020, to which they've added an extortion component, threatening to openly publish the stolen data if the ransom note is not paid. This additional extortion pressure is meant as a deterrent for companies to treat a ransomware infection as a hardware failure and outright refuse to give in to ransom demands. Threatening to go public with the stolen sensitive data is an additional guarantee that even if the victim can recover from backups, it will at least be willing to pay to avoid reputational damages or even financial damages resulting from data breach fines.

The year-over-year quarterly evolution of global ransomware reports suggests that ransomware was more active during the first half of 2020 than in the first half of 2019.



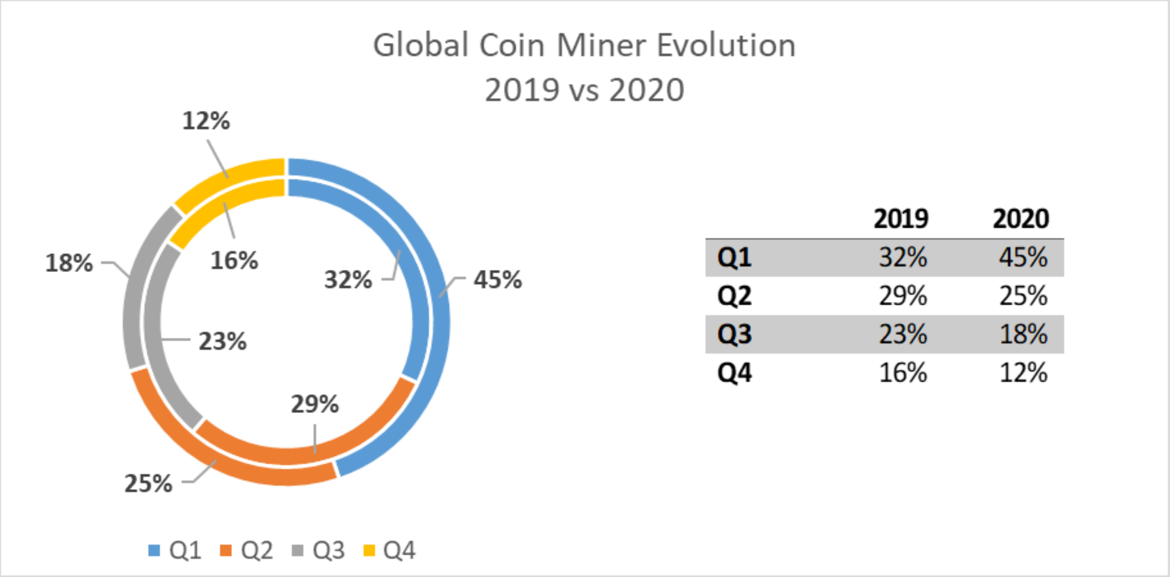
	2019	2020
Q1	18%	34%
Q2	27%	30%
Q3	26%	23%
Q4	29%	13%

Fig. 5 – Global Ransomware Evolution 2019 vs 2020

Coin Miners

Coin miner reports throughout the first half of 2020 were also higher that in the second half, clocking in at 70 percent of all global coin miner reports. Looking at both the 2019 and 2020 quarterly evolution of global coin miner reports, there seems to be continuous interest from cybercriminals to continue using and deploying it, in an attempt to generate profit by leveraging the computing power of their victims.

If in 2020, coin miner reports start off strong and the reports start to slowly dim down, suggesting that cybercriminals might have also capitalized on the pandemic during the first half of the year. During 2019, reports were somewhat more balanced, as they did not fluctuate more than a couple of percentage points each quarter.



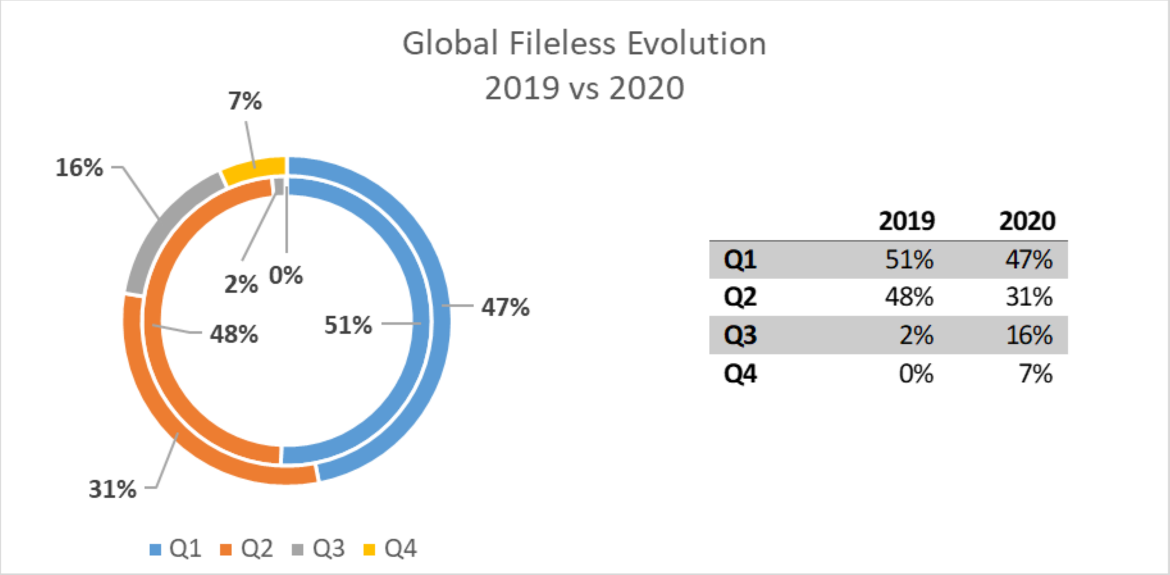
	2019	2020
Q1	32%	45%
Q2	29%	25%
Q3	23%	18%
Q4	16%	12%

Fig. 6 – Global CoinMiner Evolution 2019 vs 2020

Fileless Malware

Looking at the evolution of global fileless malware reports both during 2019 and 2020, the highest number of reports seems to occur during the first half of each year. The quarterly evolution of fileless malware reports throughout 2020 suggests that threat actors have also capitalized on the early panic caused by the pandemic in order to maximize their efforts of delivering fileless threats.

With 78 percent of global fileless malware reports during 2020 reported in the first half of 2020, its likely threat actors focused on other threats throughout the second half of the year.



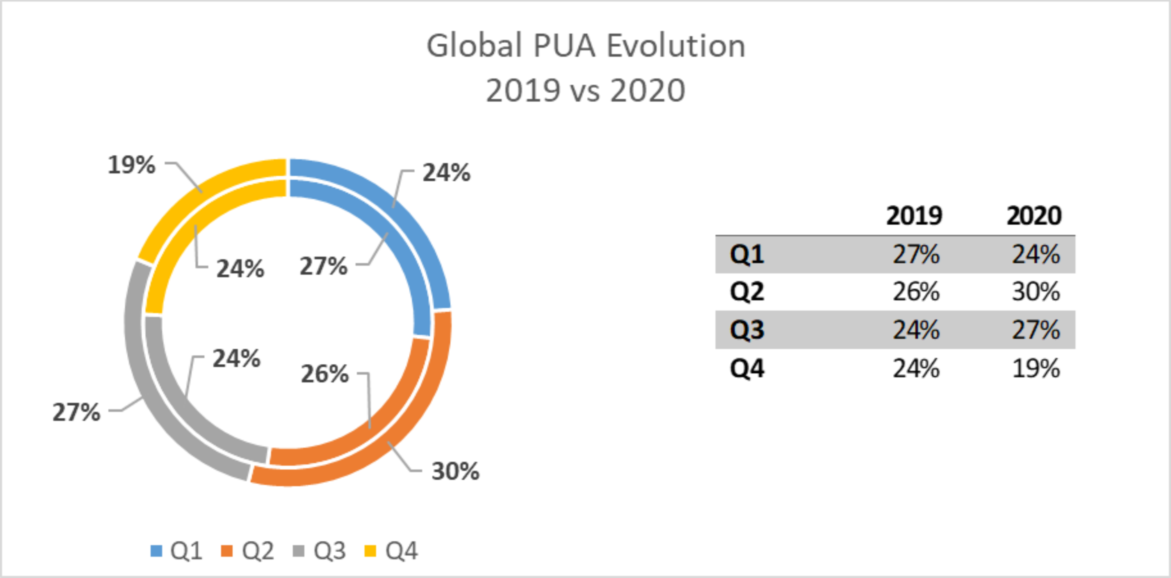
	2019	2020
Q1	51%	47%
Q2	48%	31%
Q3	2%	16%
Q4	0%	7%

Fig. 7 – Global Fileless Evolution 2019 vs 2020

Potentially Unwanted Applications (PUA)

While it’s true that potentially unwanted applications may not be harmful per se, they do have a reputation for sometimes causing usability and performance issues by installing additional applications and even displaying aggressive ads.

While **the number of global PUA reports increased by 320 percent in 2020 compared to 2019**, the quarterly distribution of reports seems to have remained somewhat similar across both years. The same pattern reported above where reports seem to increase during the first half of the year and then decrease towards the fourth quarter, seems to hold true for PUA as well.



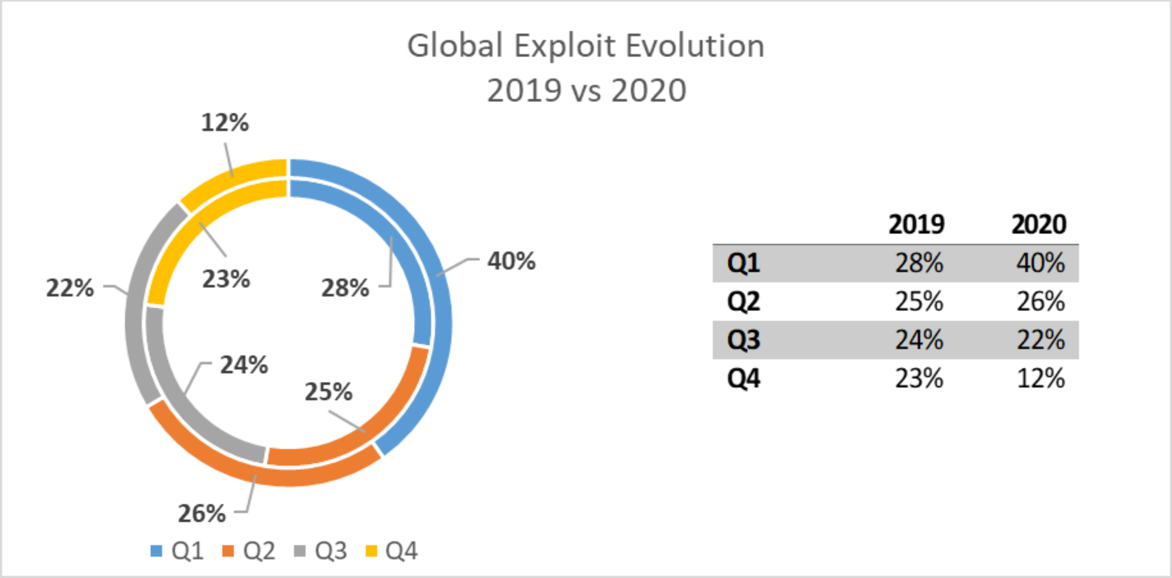
	2019	2020
Q1	27%	24%
Q2	26%	30%
Q3	24%	27%
Q4	24%	19%

Fig. 8 – Global PUA Evolution 2019 vs 2020

Exploits

The number of reported exploits throughout 2020 has also followed the same trend as previous threats, in the sense that we saw an increase in reports during the first half of 2020 and a decrease towards the end of the year. Although we noticed a 3**00 percent increase in global exploit report during 2020 compared to 2019, around 66 percent of all global exploit reports were registered during the first half of 2020**.

If during 2019 exploit reports were somewhat constant across all four quarters, during 2020 there's a significant decrease in reports when comparing the first and the fourth quarter. From 40 percent in Q1 2020 to 12 percent in Q4 2020, the descending number of reports is in line with previous trends observed for other threats.



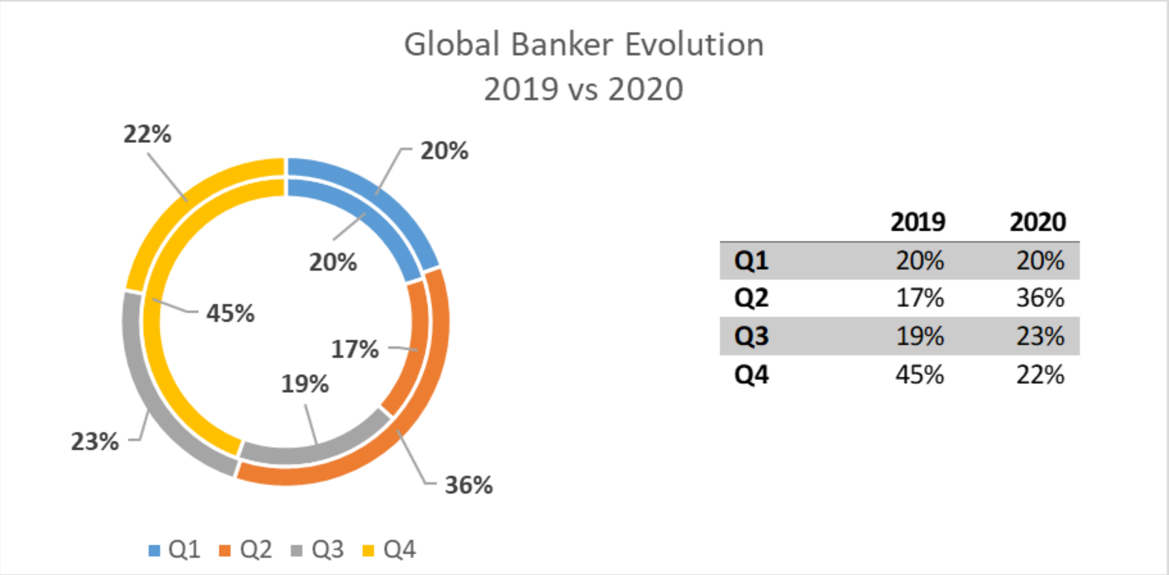
	2019	2020
Q1	28%	40%
Q2	25%	26%
Q3	24%	22%
Q4	23%	12%

Fig. 9 – Global Exploit Evolution 2019 vs 2020

Bankers

If in 2019 around 45 percent of all reported banker Trojans occurred in Q4, 2020 saw a relatively even distribution of reports. The only significant spike was registered in the second quarter of 2020, with 36 percent of the total global banker reports from 2020.

However, if during 2019 the second half of the year accounted for 64 percent of all banker reports, during 2020 the first half of the year seems to have been slightly more favorable for cybercriminals using bankers, clocking in 56 percent of all global banker reports during 2020.



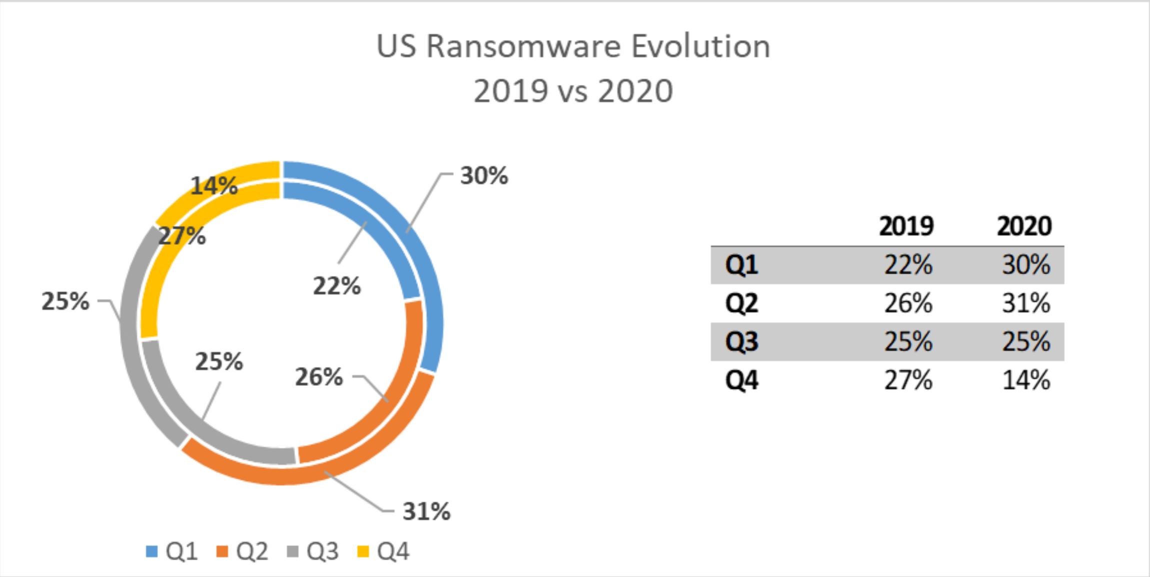
	2019	2020
Q1	20%	20%
Q2	17%	36%
Q3	19%	23%
Q4	45%	22%

Fig. 10 – Global Banker Evolution 2019 vs 2020

Threats Evolution per Country

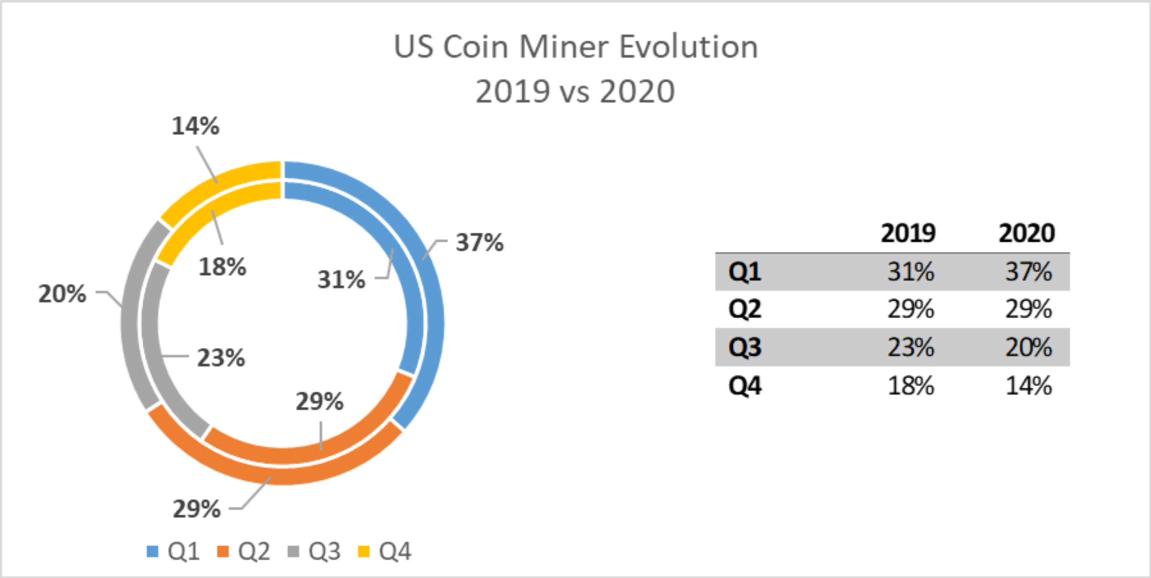
While the global evolution of ransomware, coin miner, fileless, PUA, exploit and banker reports provides both a general overview of how cybercriminals have operated as well as an insight into how popular they've become, analyzing their local evolution in specific countries can provide a better view into how cybercriminals plan and execute their campaigns in each specific region.

United States



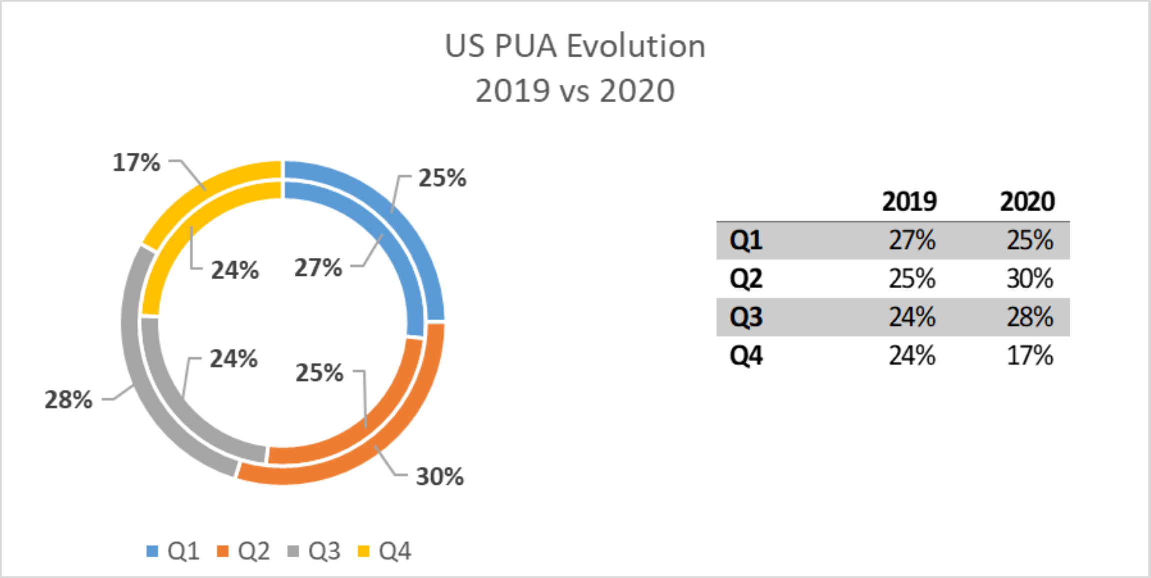
	2019	2020
Q1	22%	30%
Q2	26%	31%
Q3	25%	25%
Q4	27%	14%

Fig. 11 – US Ransomware Evolution 2019 vs 2020



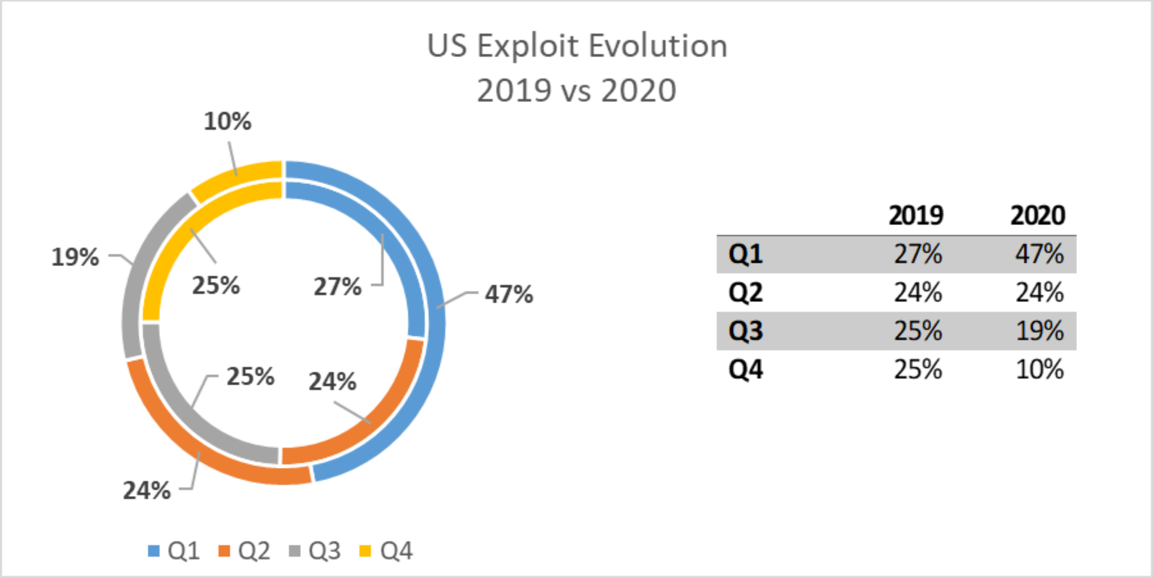
	2019	2020
Q1	31%	37%
Q2	29%	29%
Q3	23%	20%
Q4	18%	14%

Fig. 12 – US Coin Miner Evolution 2019 vs 2020



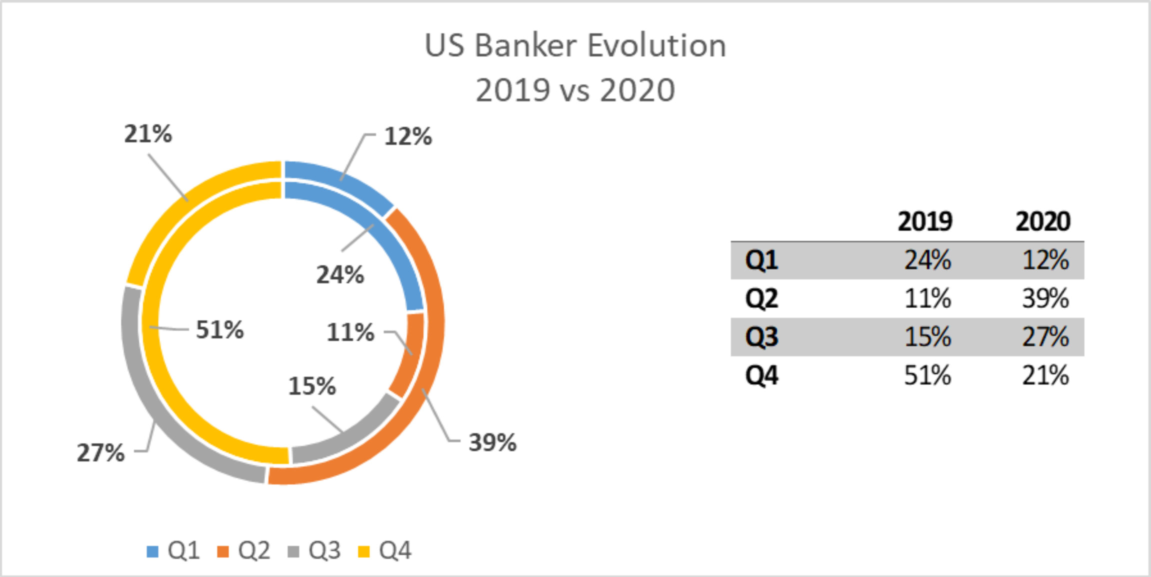
	2019	2020
Q1	27%	25%
Q2	25%	30%
Q3	24%	28%
Q4	24%	17%

Fig. 13 – US PUA Evolution 2019 vs 2020



	2019	2020
Q1	27%	47%
Q2	24%	24%
Q3	25%	19%
Q4	25%	10%

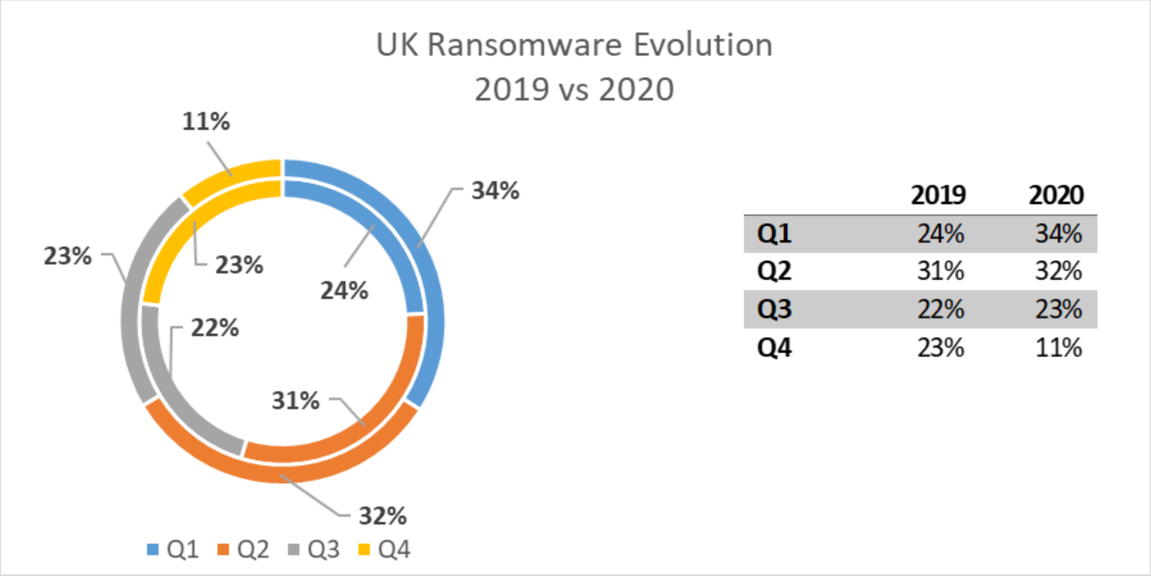
Fig. 14 – US Exploit Evolution 2019 vs 2020



	2019	2020
Q1	24%	12%
Q2	11%	39%
Q3	15%	27%
Q4	51%	21%

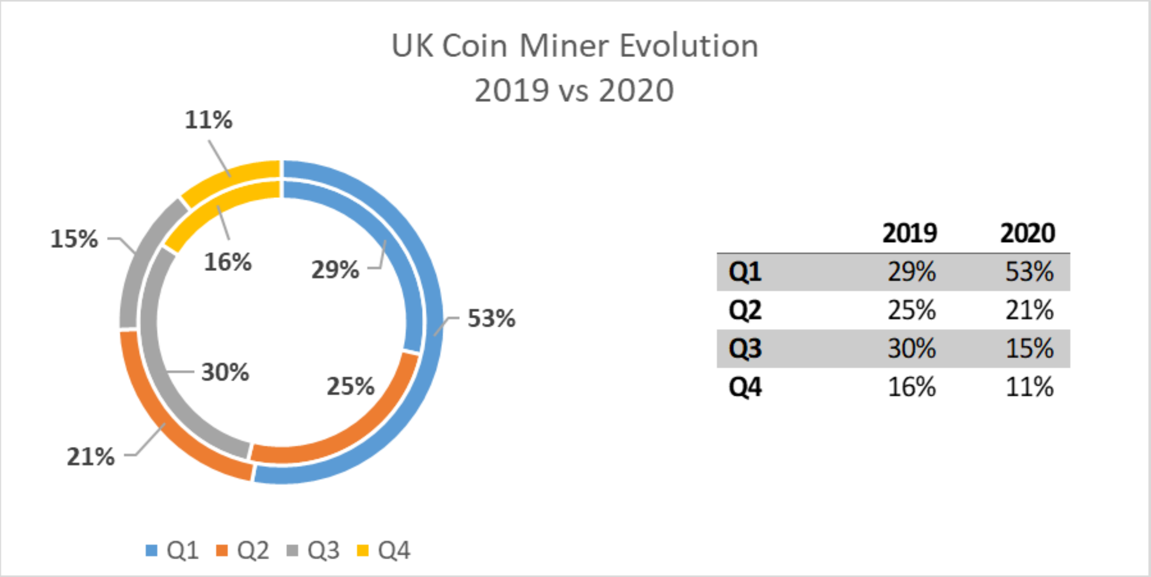
Fig. 15 – US Banker Evolution 2019 vs 2020

United Kingdom



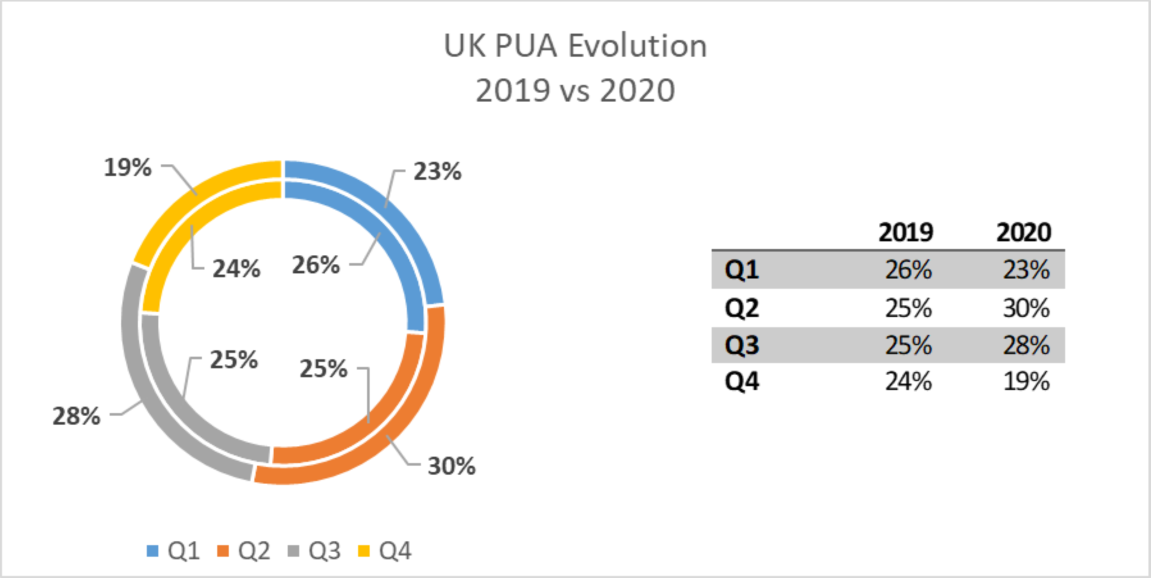
	2019	2020
Q1	24%	34%
Q2	31%	32%
Q3	22%	23%
Q4	23%	11%

Fig. 16 – UK Ransomware Evolution 2019 vs 2020



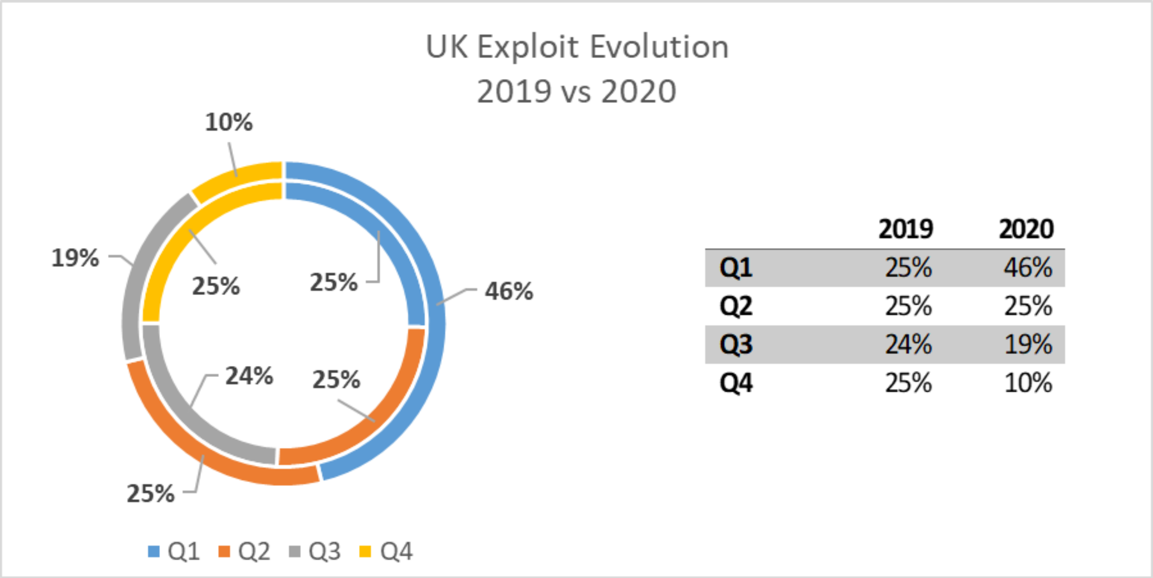
	2019	2020
Q1	29%	53%
Q2	25%	21%
Q3	30%	15%
Q4	16%	11%

Fig. 17 – UK Coin Miner Evolution 2019 vs 2020



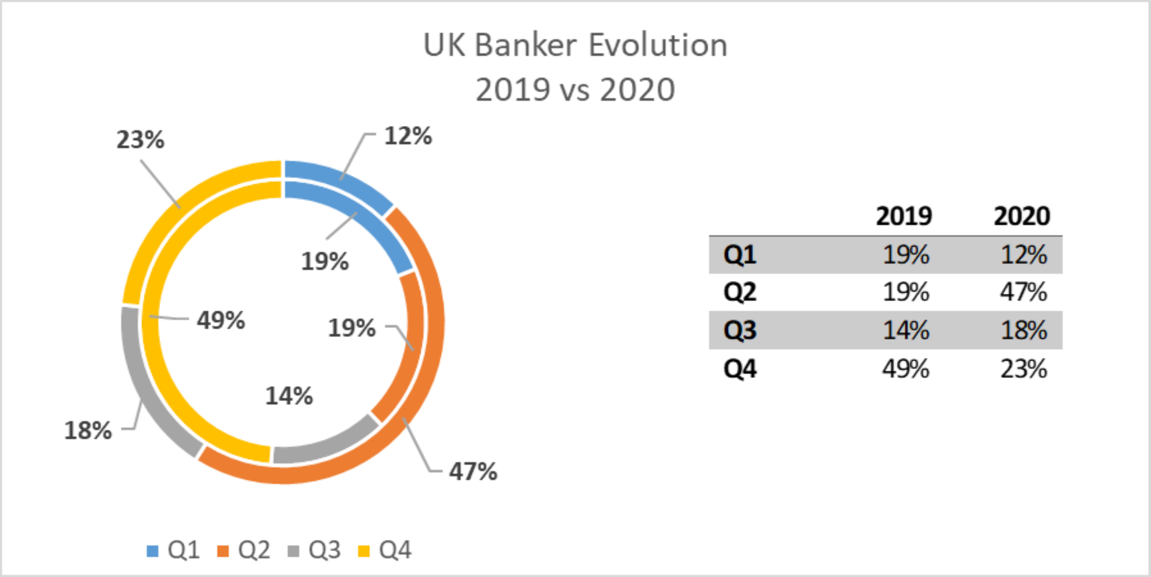
	2019	2020
Q1	26%	23%
Q2	25%	30%
Q3	25%	28%
Q4	24%	19%

Fig. 18 – UK PUA Evolution 2019 vs 2020



	2019	2020
Q1	25%	46%
Q2	25%	25%
Q3	24%	19%
Q4	25%	10%

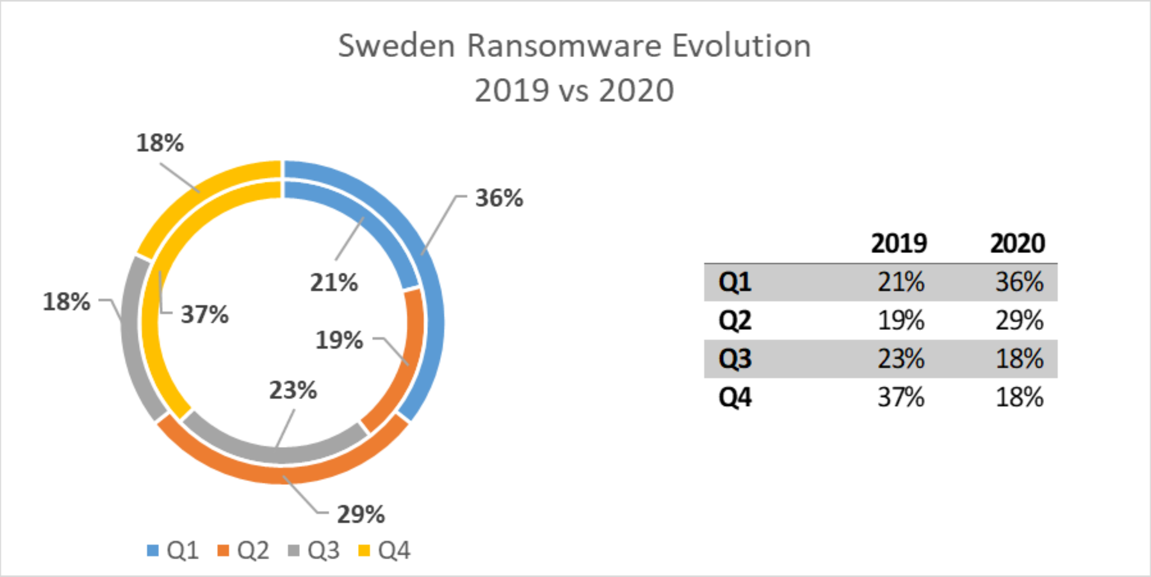
Fig. 19 – UK Exploit Evolution 2019 vs 2020



	2019	2020
Q1	19%	12%
Q2	19%	47%
Q3	14%	18%
Q4	49%	23%

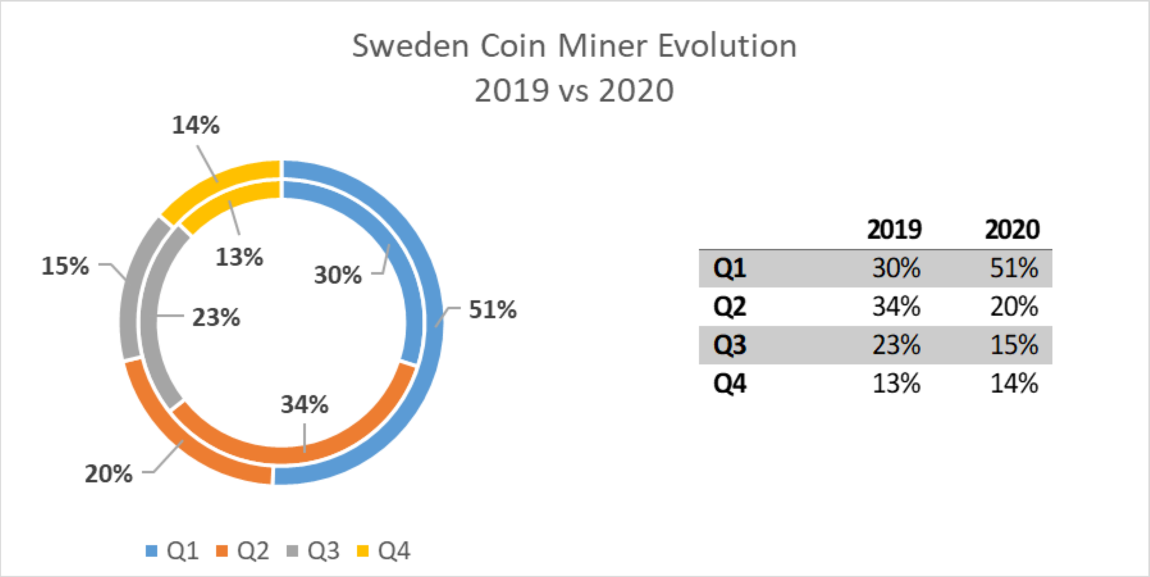
Fig. 20 – UK Banker Evolution 2019 vs 2020

Sweden



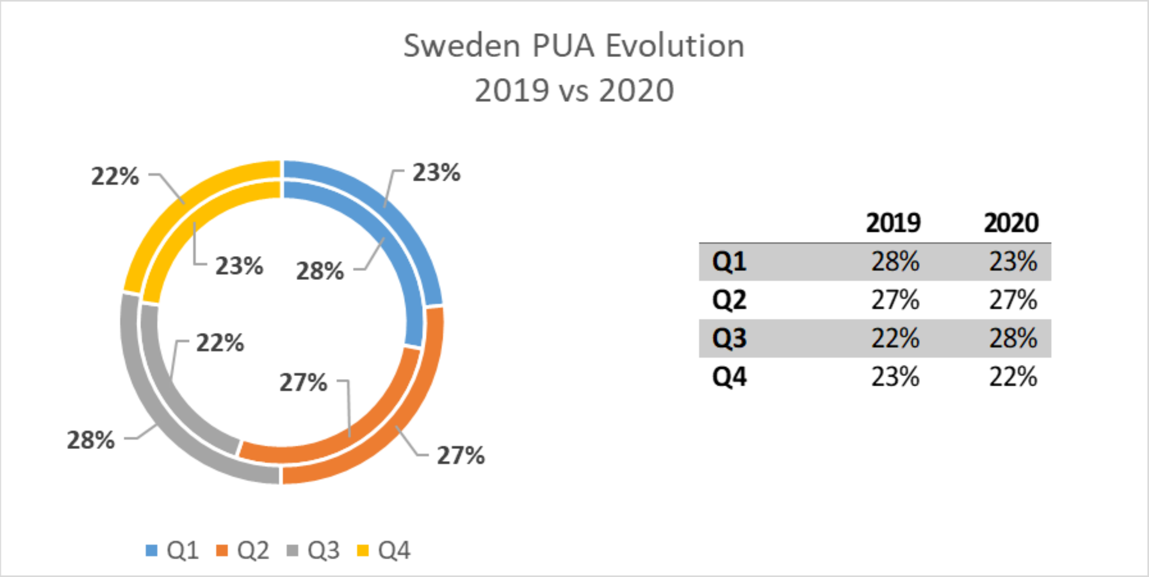
	2019	2020
Q1	21%	36%
Q2	19%	29%
Q3	23%	18%
Q4	37%	18%

Fig. 21 – Sweden Ransomware Evolution 2019 vs 2020



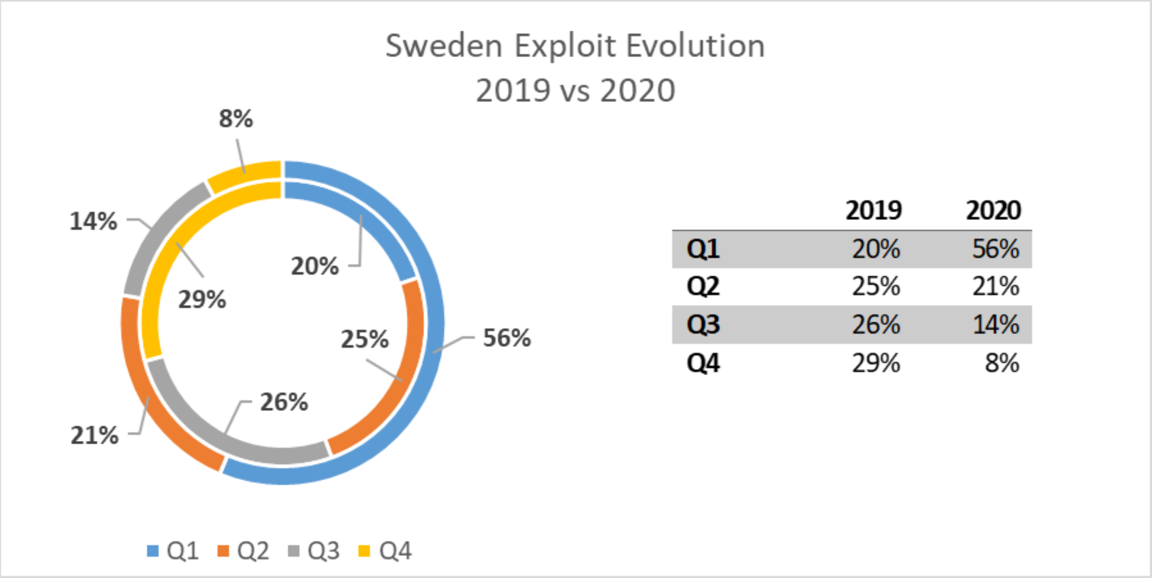
	2019	2020
Q1	30%	51%
Q2	34%	20%
Q3	23%	15%
Q4	13%	14%

Fig. 22 – Sweden Coin Miner Evolution 2019 vs 2020



	2019	2020
Q1	28%	23%
Q2	27%	27%
Q3	22%	28%
Q4	23%	22%

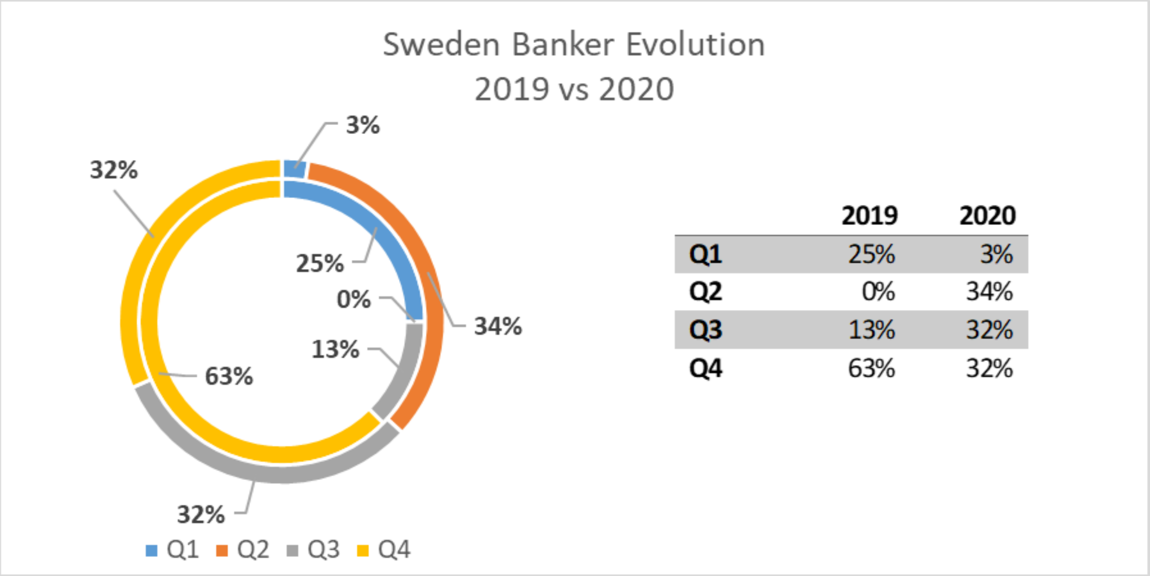
Fig. 23 – Sweden PUA Evolution 2019 vs 2020



Sweden Exploit Evolution
2019 vs 2020

	2019	2020
Q1	20%	56%
Q2	25%	21%
Q3	26%	14%
Q4	29%	8%

Fig. 24 – Sweden Exploit Evolution 2019 vs 2020

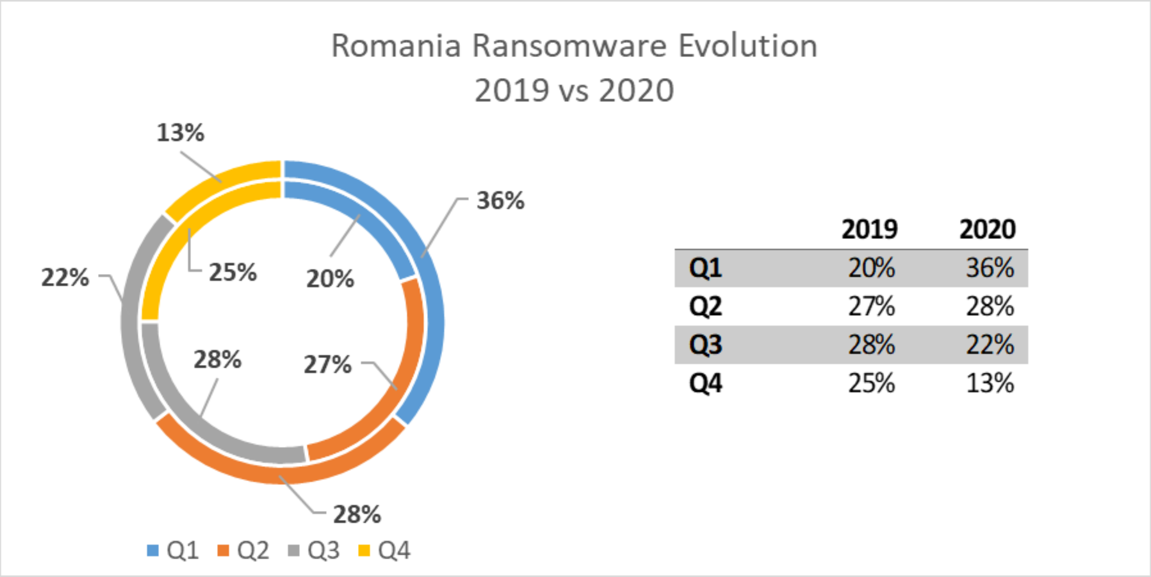


Sweden Banker Evolution
2019 vs 2020

	2019	2020
Q1	25%	3%
Q2	0%	34%
Q3	13%	32%
Q4	63%	32%

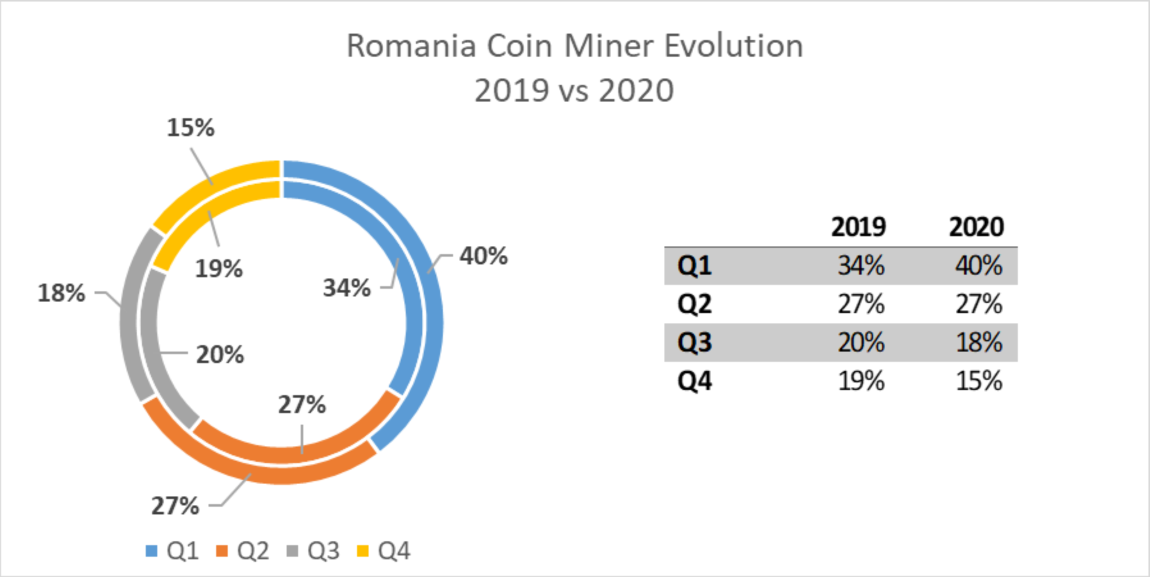
Fig. 25 – Sweden Banker Evolution 2019 vs 2020

Romania



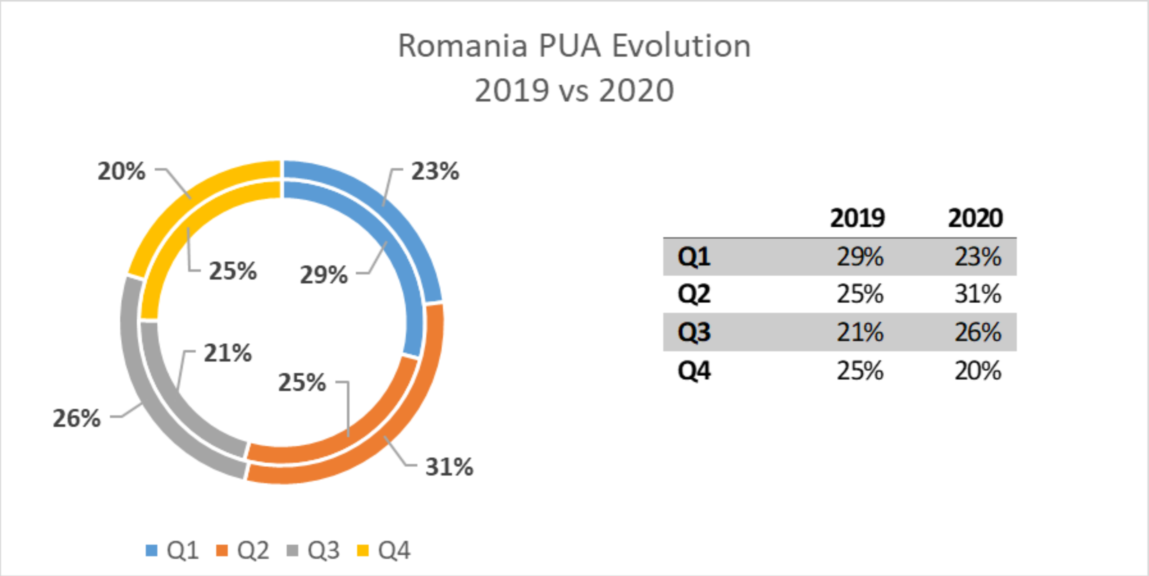
	2019	2020
Q1	20%	36%
Q2	27%	28%
Q3	28%	22%
Q4	25%	13%

Fig. 26 – Romania Ransomware Evolution 2019 vs 2020



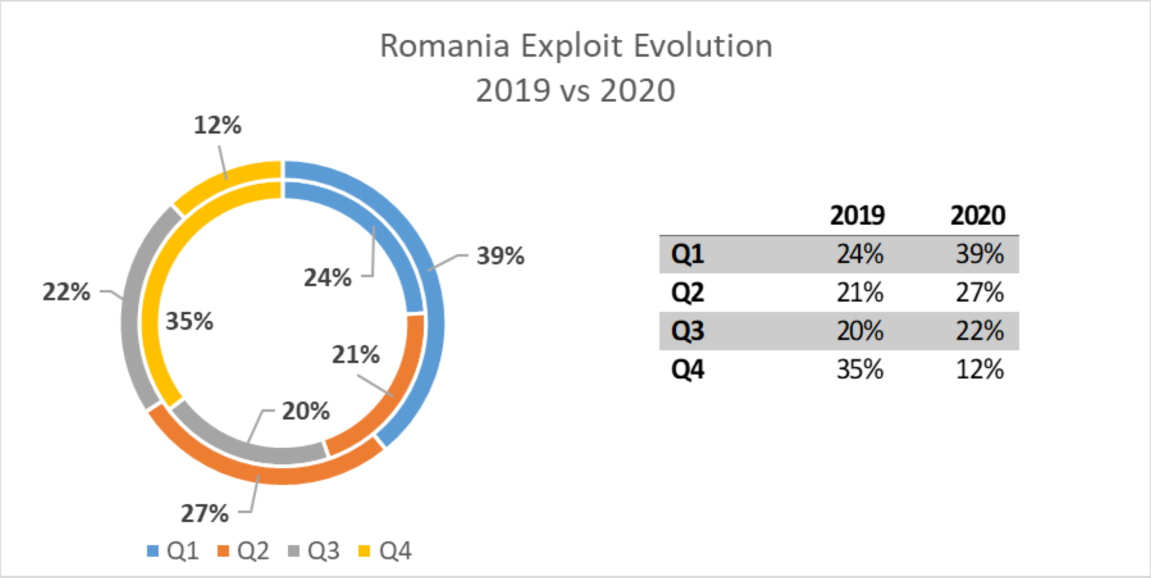
	2019	2020
Q1	34%	40%
Q2	27%	27%
Q3	20%	18%
Q4	19%	15%

Fig. 27 – Romania Coin Miner Evolution 2019 vs 2020



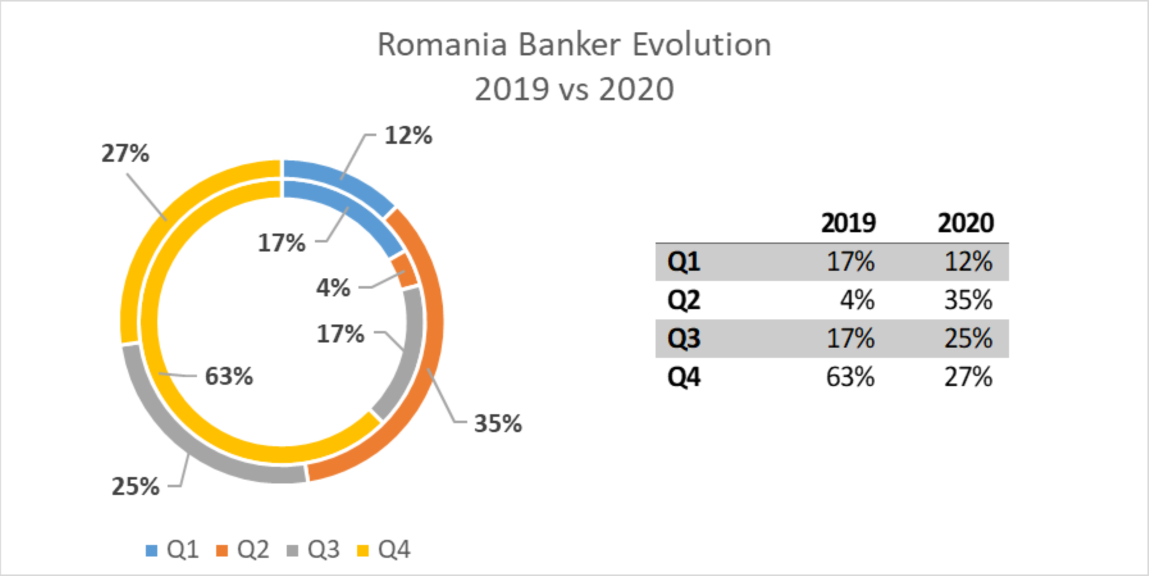
	2019	2020
Q1	29%	23%
Q2	25%	31%
Q3	21%	26%
Q4	25%	20%

Fig. 28 – Romania PUA Miner Evolution 2019 vs 2020



	2019	2020
Q1	24%	39%
Q2	21%	27%
Q3	20%	22%
Q4	35%	12%

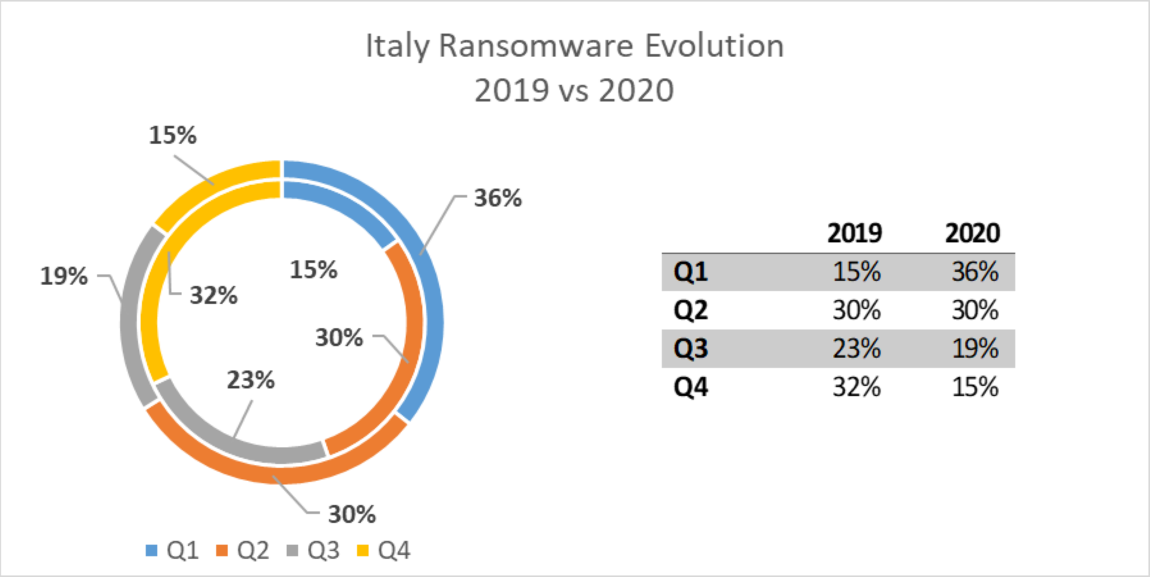
Fig. 29 – Romania Exploit Evolution 2019 vs 2020



	2019	2020
Q1	17%	12%
Q2	4%	35%
Q3	17%	25%
Q4	63%	27%

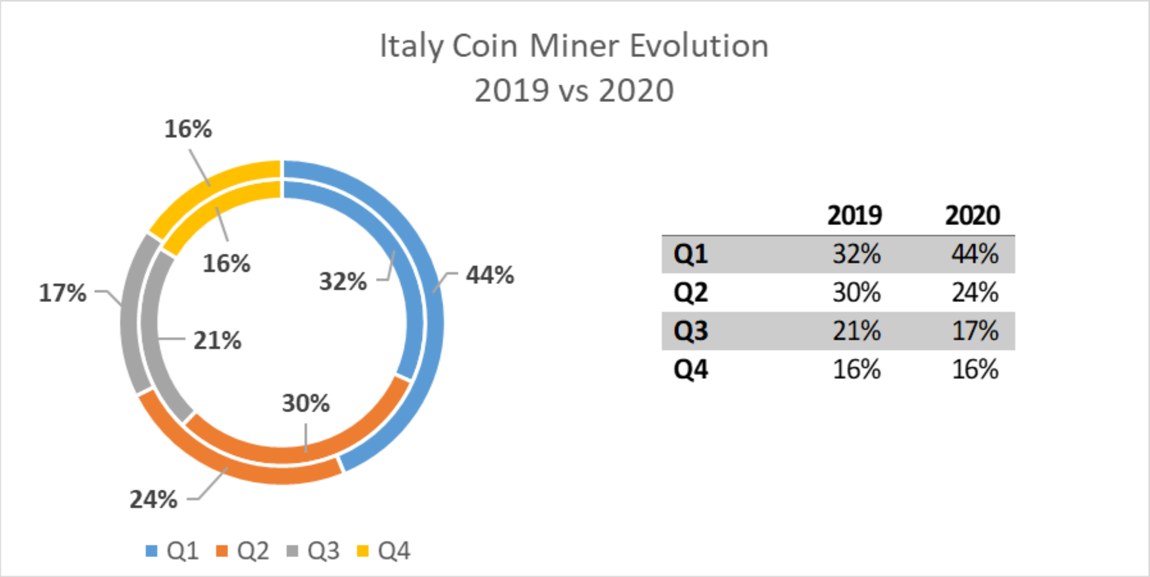
Fig. 30 – Romania Banker Evolution 2019 vs 2020

Italy



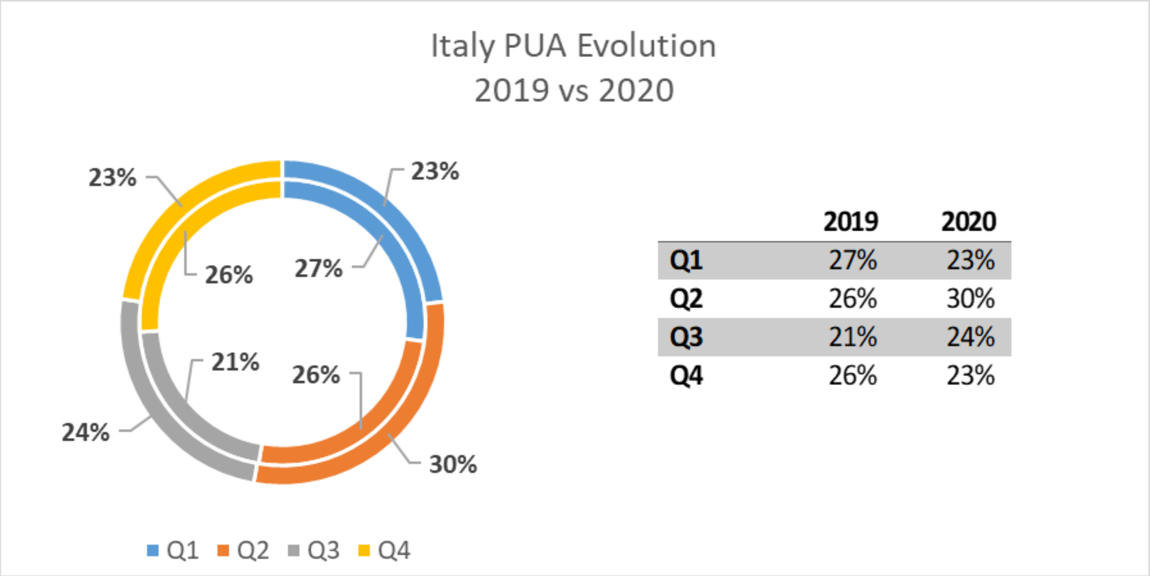
	2019	2020
Q1	15%	36%
Q2	30%	30%
Q3	23%	19%
Q4	32%	15%

Fig. 31 – Italy Ransomware Evolution 2019 vs 2020



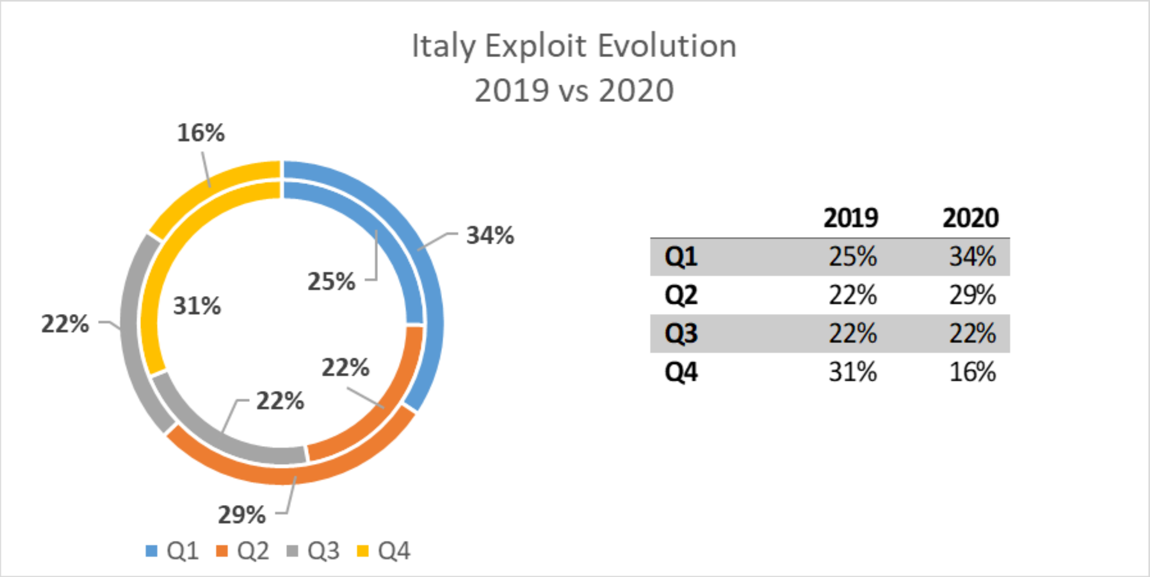
	2019	2020
Q1	32%	44%
Q2	30%	24%
Q3	21%	17%
Q4	16%	16%

Fig. 32 – Italy Coin Miner Evolution 2019 vs 2020



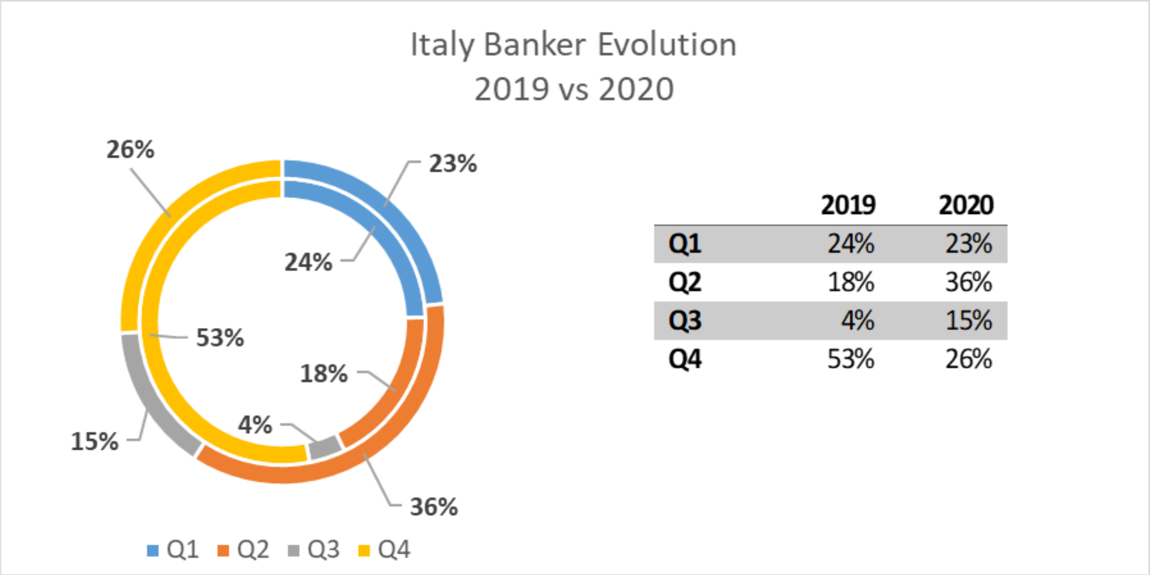
	2019	2020
Q1	27%	23%
Q2	26%	30%
Q3	21%	24%
Q4	26%	23%

Fig. 33 – Italy PUA Evolution 2019 vs 2020



	2019	2020
Q1	25%	34%
Q2	22%	29%
Q3	22%	22%
Q4	31%	16%

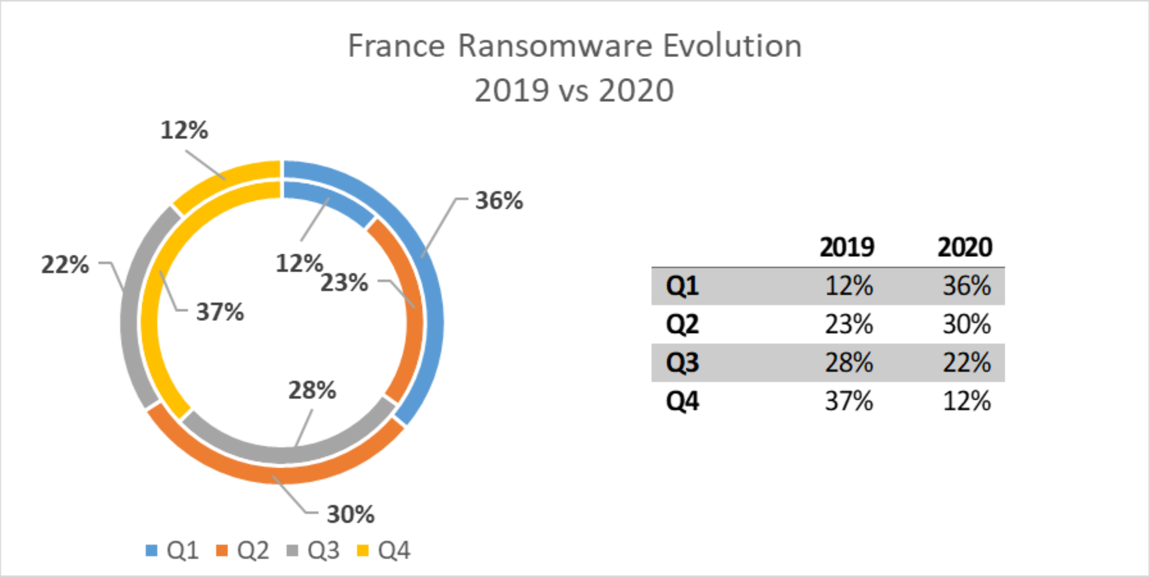
Fig. 34 – Italy Exploit Evolution 2019 vs 2020



	2019	2020
Q1	24%	23%
Q2	18%	36%
Q3	4%	15%
Q4	53%	26%

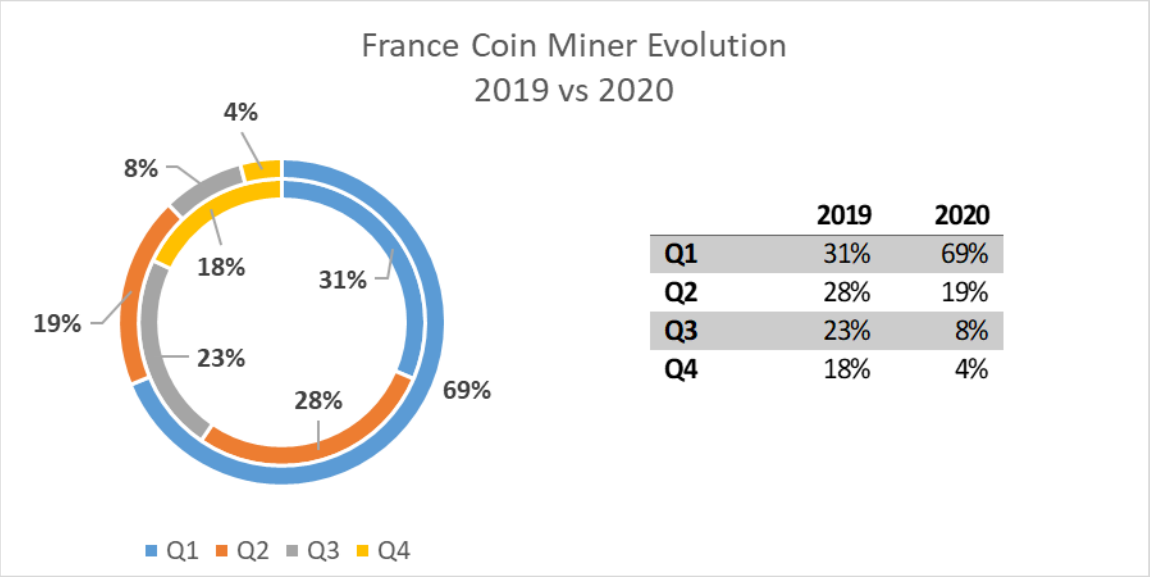
Fig. 35 – Italy Banker Evolution 2019 vs 2020

France



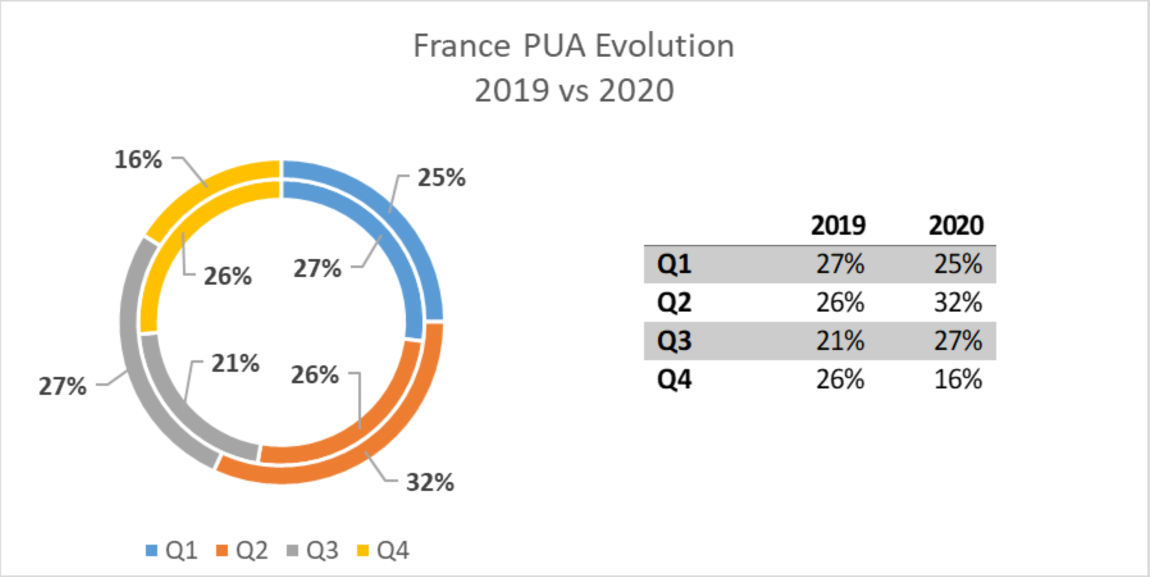
	2019	2020
Q1	12%	36%
Q2	23%	30%
Q3	28%	22%
Q4	37%	12%

Fig. 36 – France Ransomware Evolution 2019 vs 2020



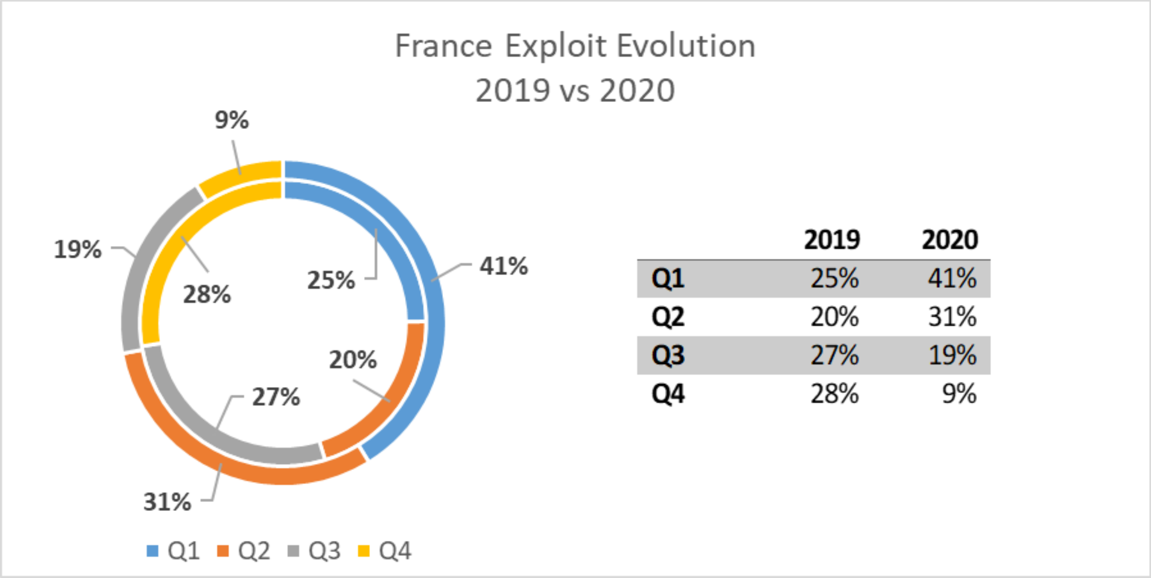
	2019	2020
Q1	31%	69%
Q2	28%	19%
Q3	23%	8%
Q4	18%	4%

Fig. 37 – France Coin Miner Evolution 2019 vs 2020



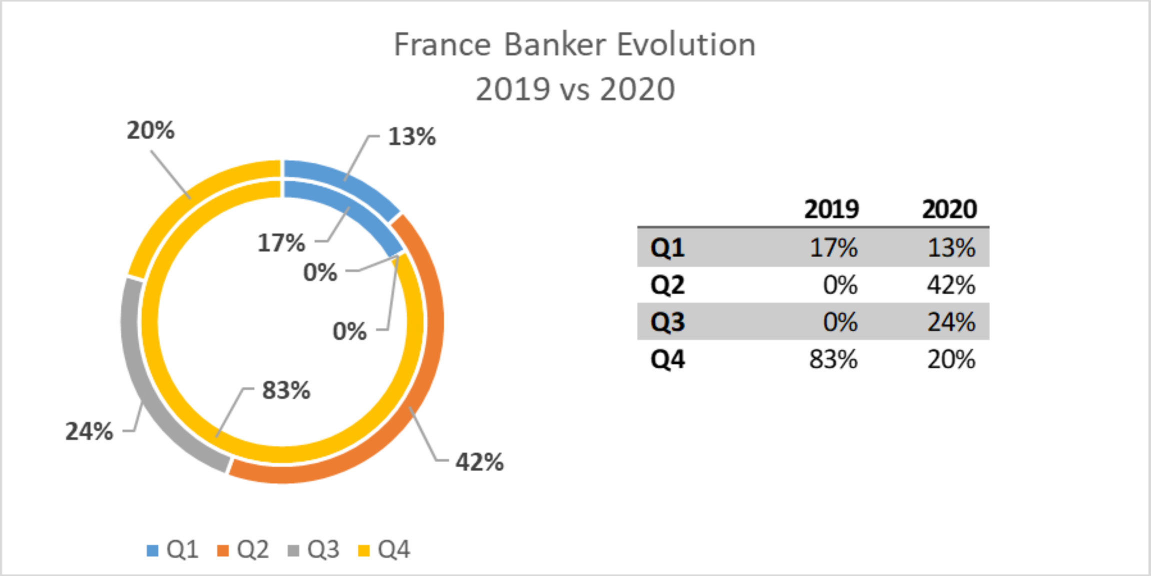
	2019	2020
Q1	27%	25%
Q2	26%	32%
Q3	21%	27%
Q4	26%	16%

Fig. 38 – France PUA Evolution 2019 vs 2020



	2019	2020
Q1	25%	41%
Q2	20%	31%
Q3	27%	19%
Q4	28%	9%

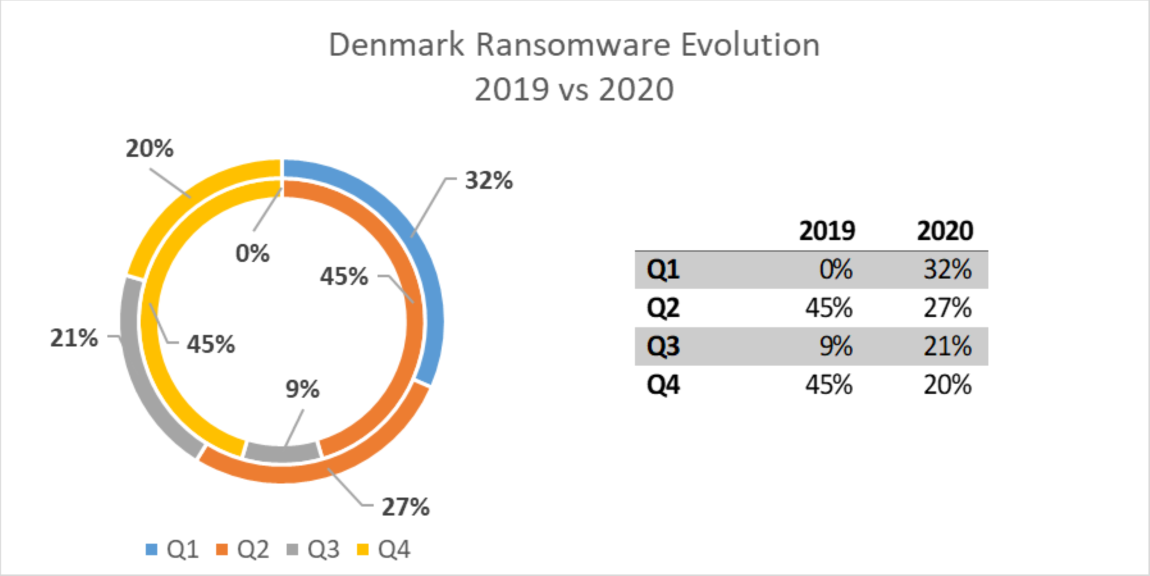
Fig. 39 – France Exploit Evolution 2019 vs 2020



	2019	2020
Q1	17%	13%
Q2	0%	42%
Q3	0%	24%
Q4	83%	20%

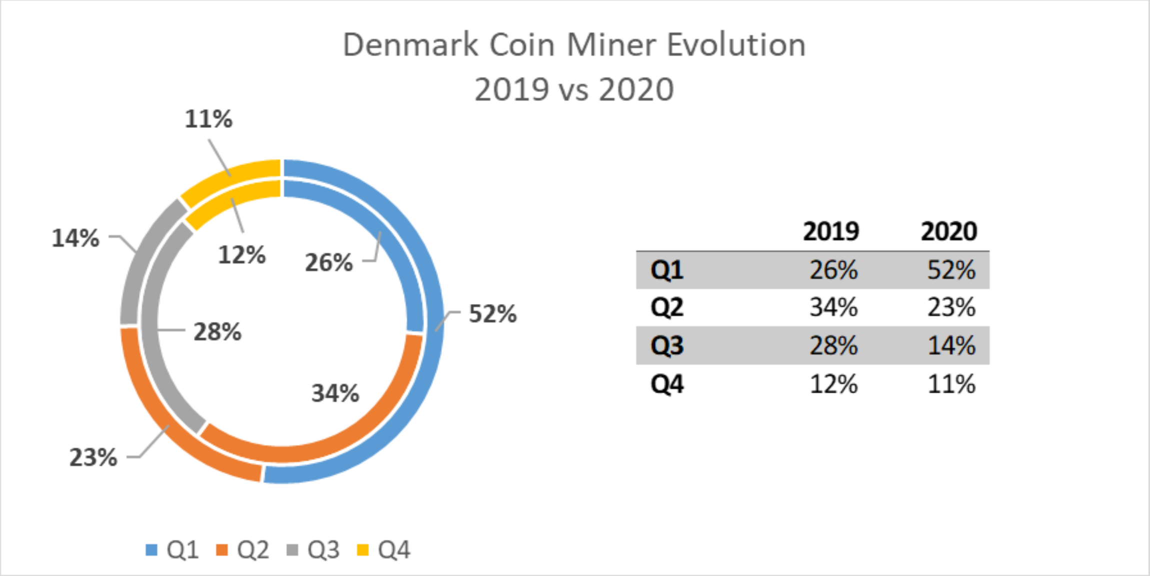
Fig. 40 – France Banker Evolution 2019 vs 2020

Denmark



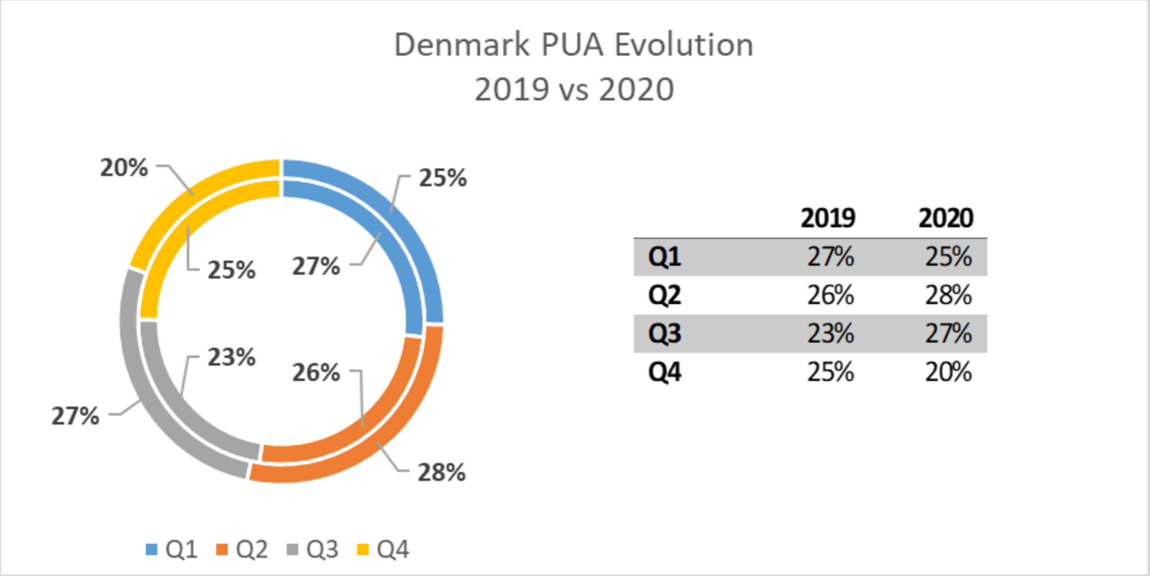
	2019	2020
Q1	0%	32%
Q2	45%	27%
Q3	9%	21%
Q4	45%	20%

Fig. 41 – Denmark Ransomware Evolution 2019 vs 2020



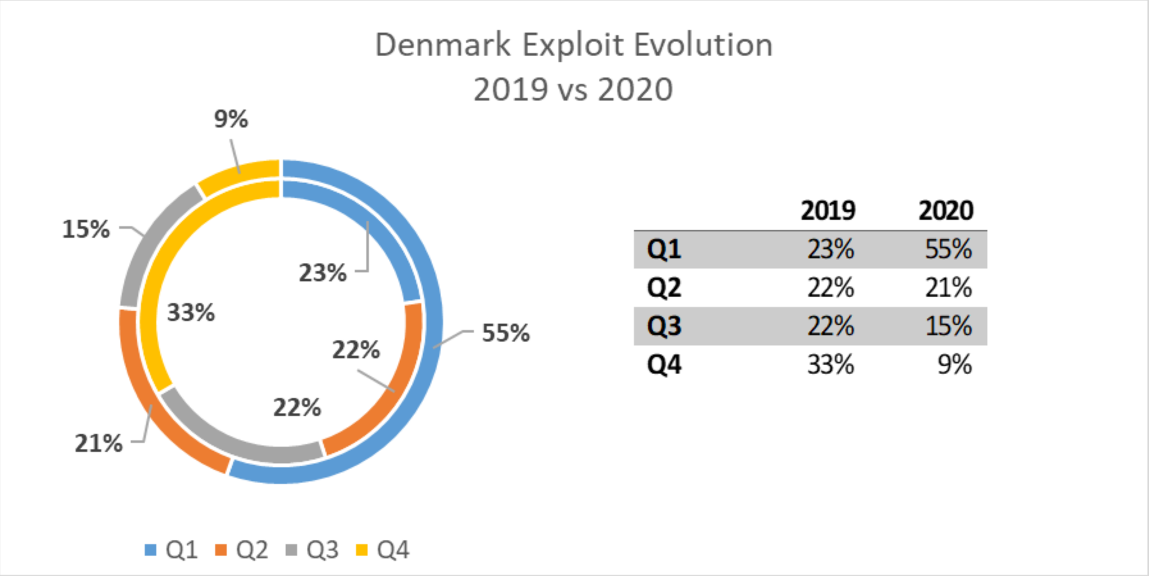
	2019	2020
Q1	26%	52%
Q2	34%	23%
Q3	28%	14%
Q4	12%	11%

Fig. 42 – Denmark Coin Miner Evolution 2019 vs 2020



	2019	2020
Q1	27%	25%
Q2	26%	28%
Q3	23%	27%
Q4	25%	20%

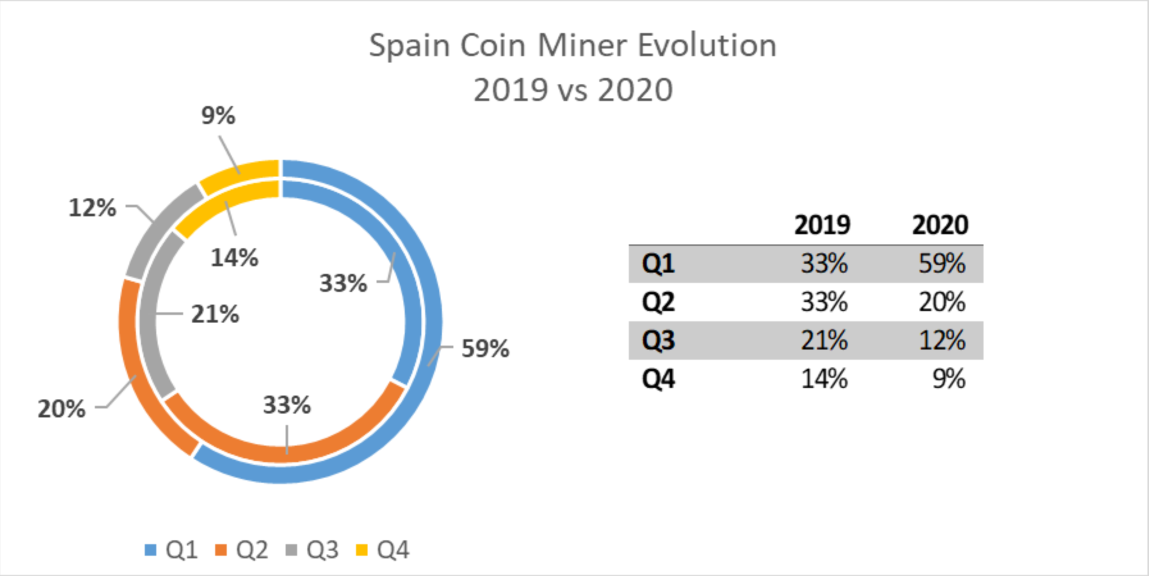
Fig. 43 – Denmark PUA Evolution 2019 vs 2020



	2019	2020
Q1	23%	55%
Q2	22%	21%
Q3	22%	15%
Q4	33%	9%

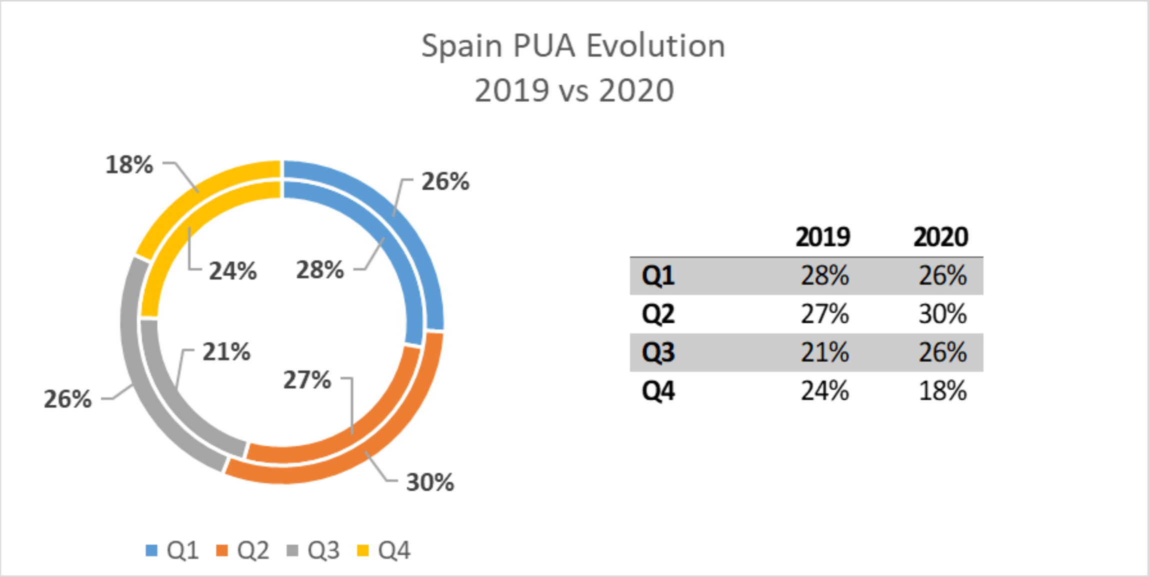
Fig. 44 – Denmark Exploit Evolution 2019 vs 2020

Spain



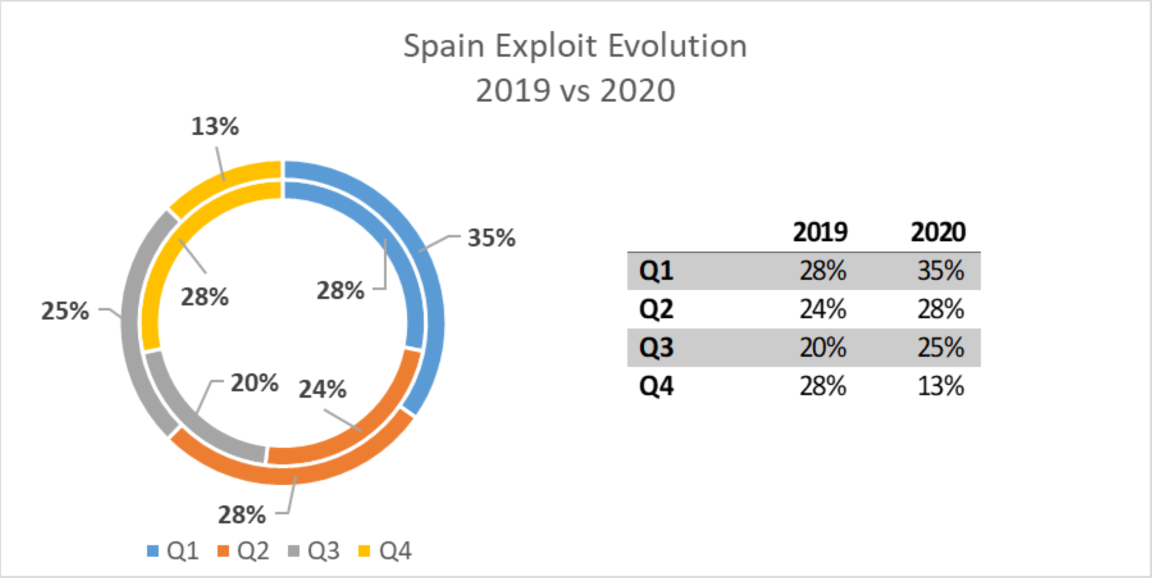
	2019	2020
Q1	33%	59%
Q2	33%	20%
Q3	21%	12%
Q4	14%	9%

Fig. 45 – Spain Coin Miner Evolution 2019 vs 2020



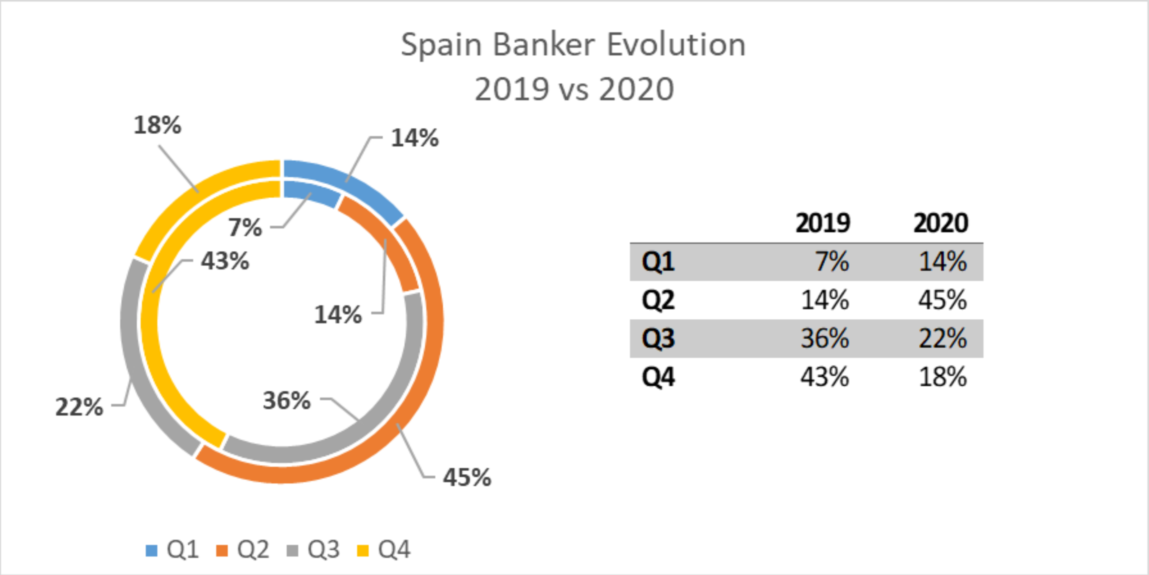
	2019	2020
Q1	28%	26%
Q2	27%	30%
Q3	21%	26%
Q4	24%	18%

Fig. 46 – Spain PUA Evolution 2019 vs 2020



	2019	2020
Q1	28%	35%
Q2	24%	28%
Q3	20%	25%
Q4	28%	13%

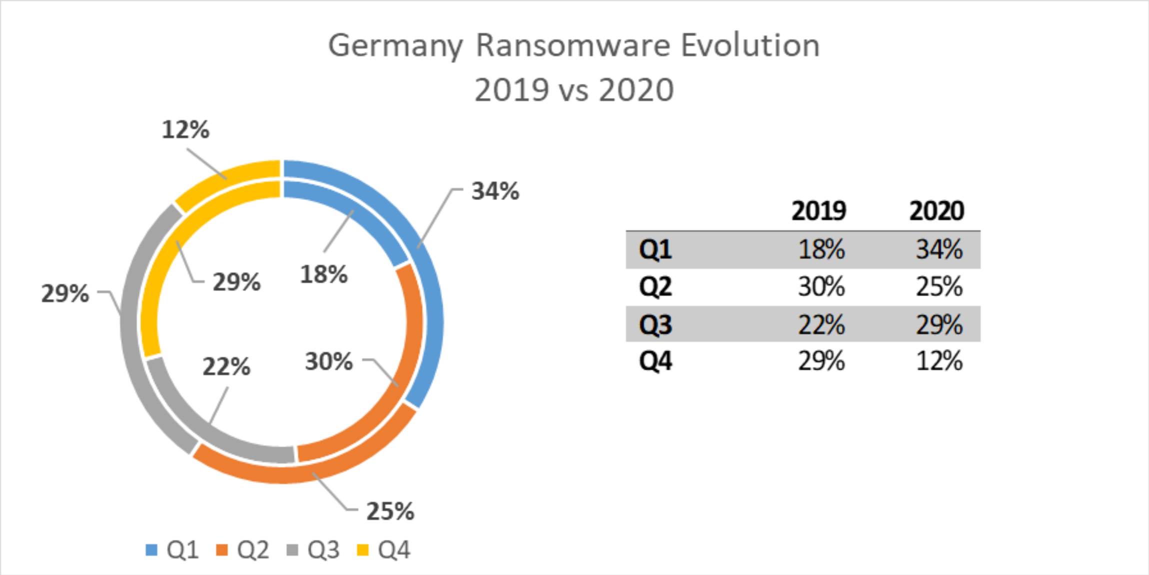
Fig. 47 – Spain Exploit Evolution 2019 vs 2020



	2019	2020
Q1	7%	14%
Q2	14%	45%
Q3	36%	22%
Q4	43%	18%

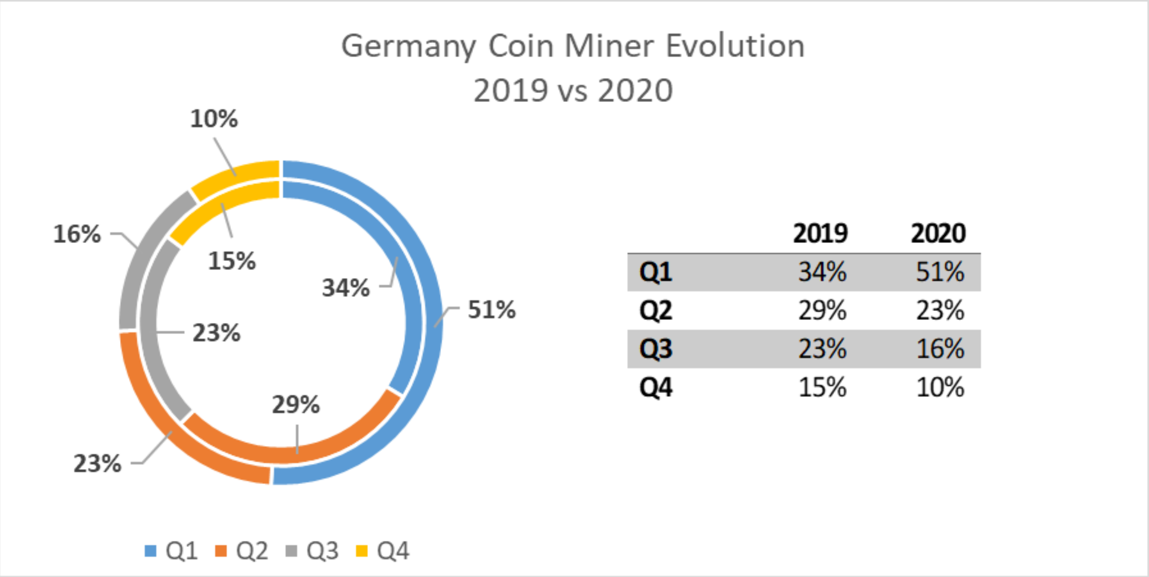
Fig. 48 – Spain Banker Evolution 2019 vs 2020

Germany



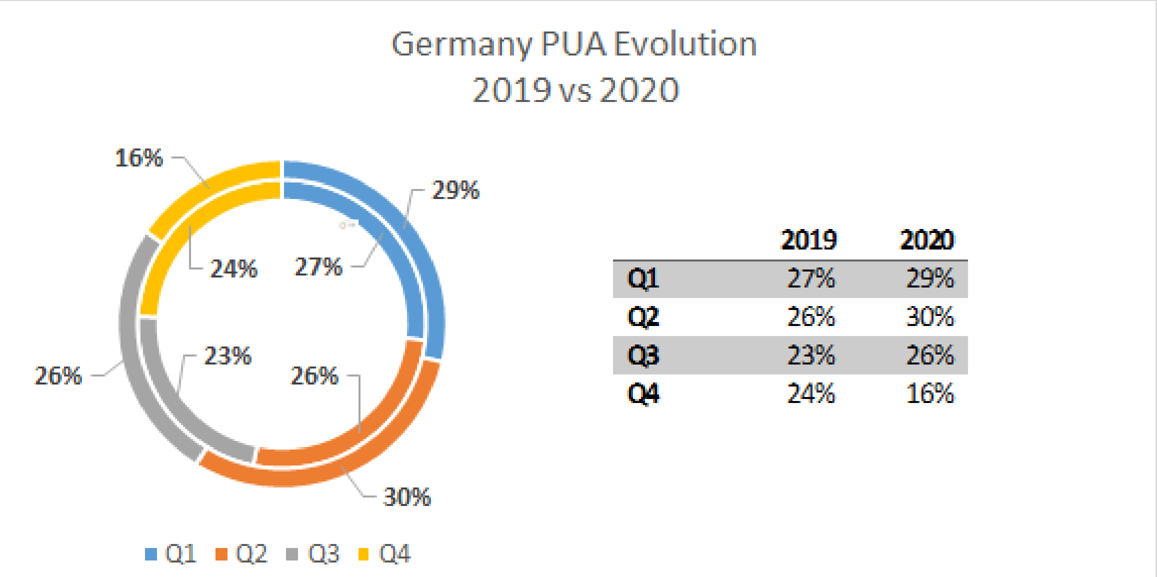
	2019	2020
Q1	18%	34%
Q2	30%	25%
Q3	22%	29%
Q4	29%	12%

Fig. 49 – Germany Ransomware Evolution 2019 vs 2020



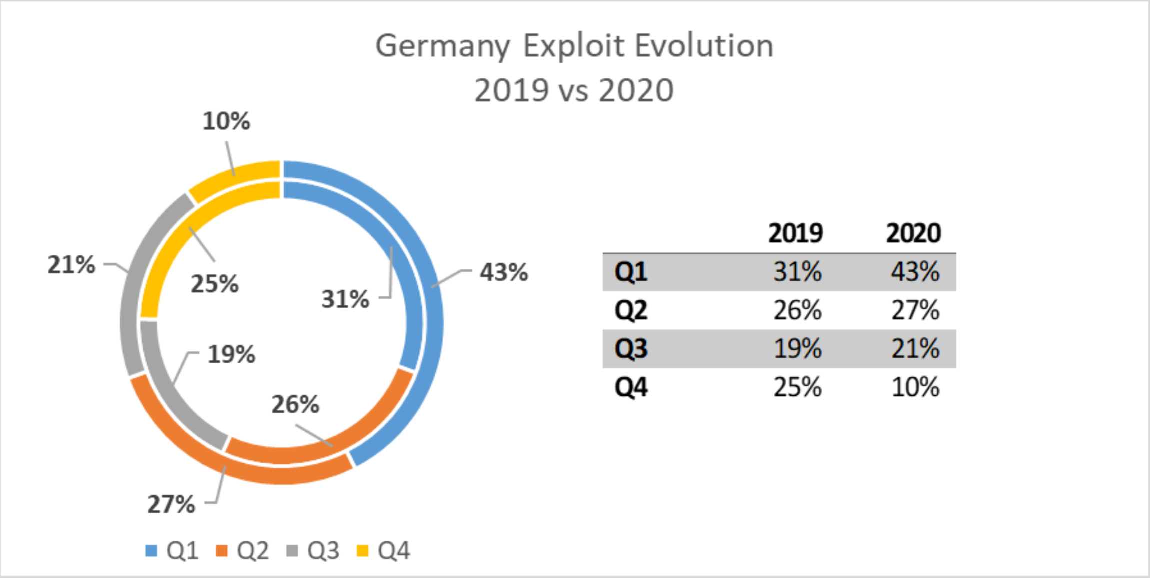
	2019	2020
Q1	34%	51%
Q2	29%	23%
Q3	23%	16%
Q4	15%	10%

Fig. 50 – Germany Coin Miner Evolution 2019 vs 2020



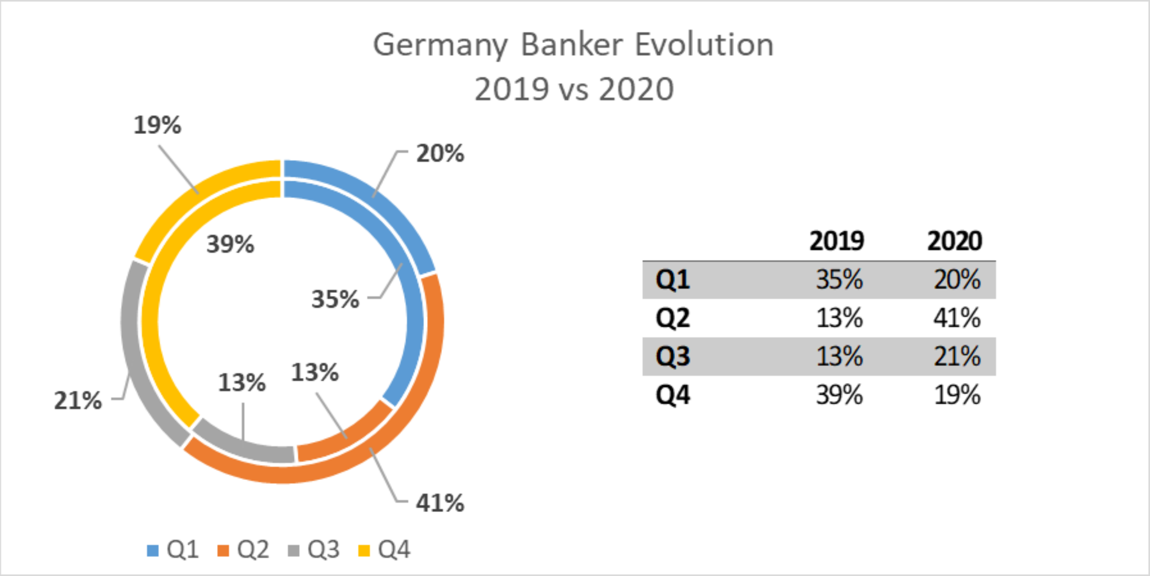
	2019	2020
Q1	27%	29%
Q2	26%	30%
Q3	23%	26%
Q4	24%	16%

Fig. 51 – Germany PUA Evolution 2019 vs 2020



	2019	2020
Q1	31%	43%
Q2	26%	27%
Q3	19%	21%
Q4	25%	10%

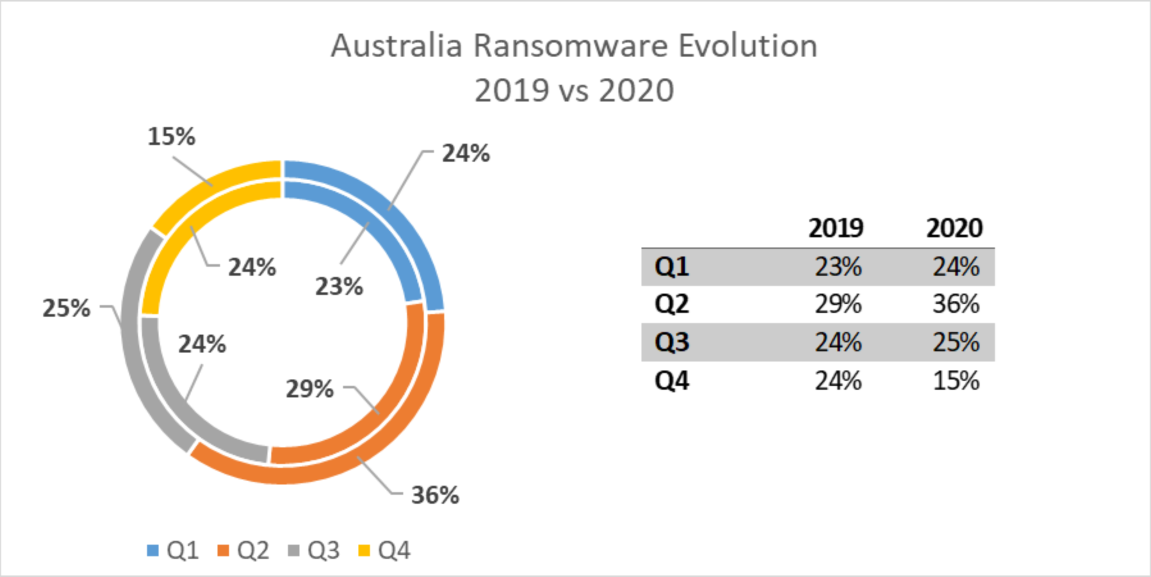
Fig. 52 – Germany Exploit Evolution 2019 vs 2020



	2019	2020
Q1	35%	20%
Q2	13%	41%
Q3	13%	21%
Q4	39%	19%

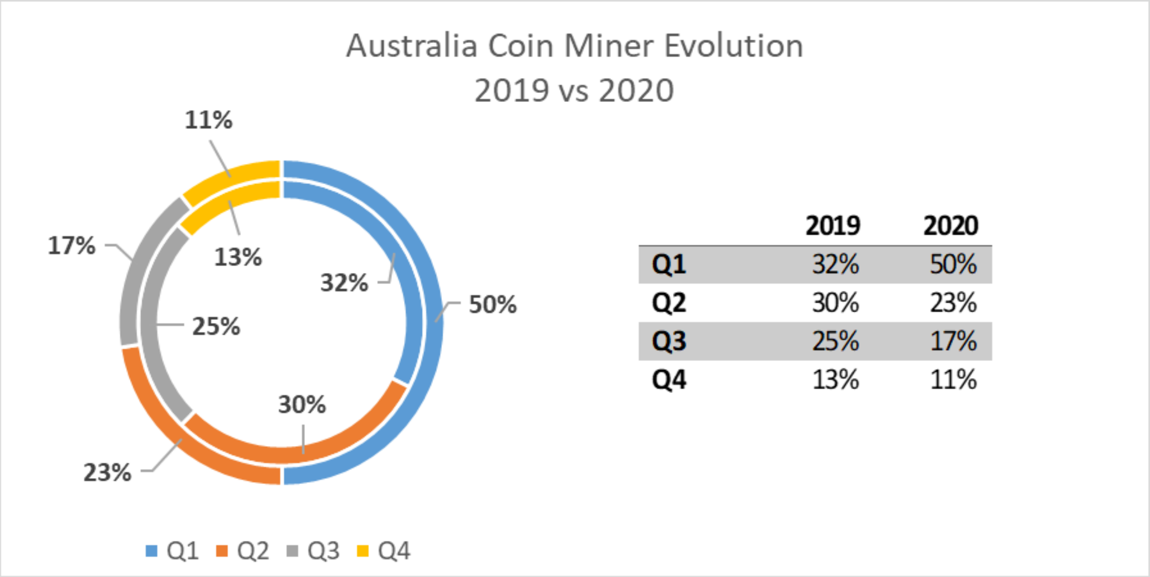
Fig. 53 – Germany Banker Evolution 2019 vs 2020

Australia



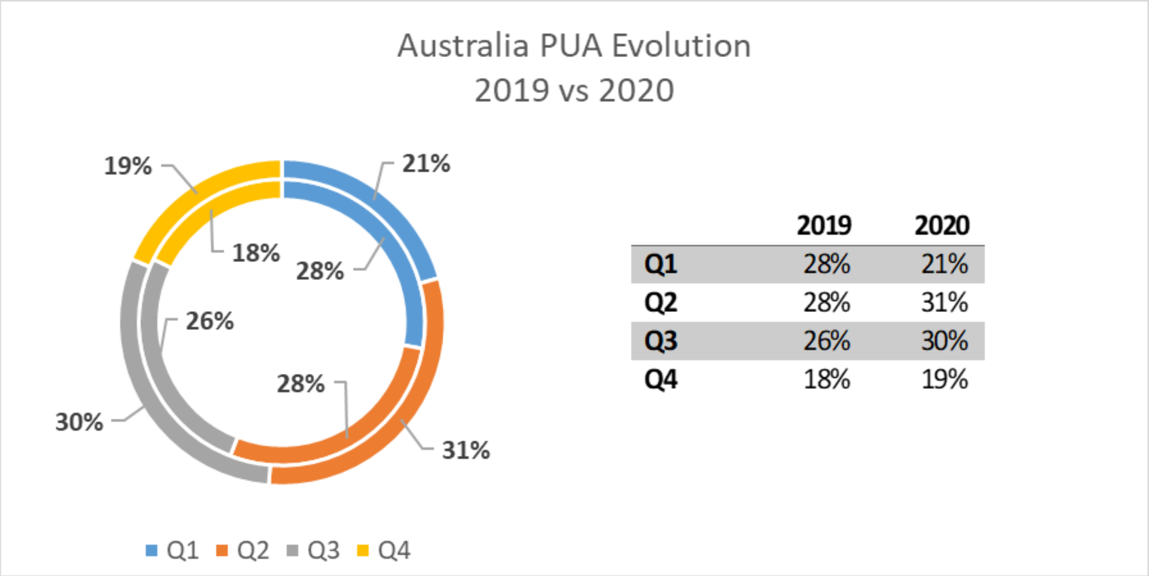
	2019	2020
Q1	23%	24%
Q2	29%	36%
Q3	24%	25%
Q4	24%	15%

Fig. 54 – Australia Ransomware Evolution 2019 vs 2020



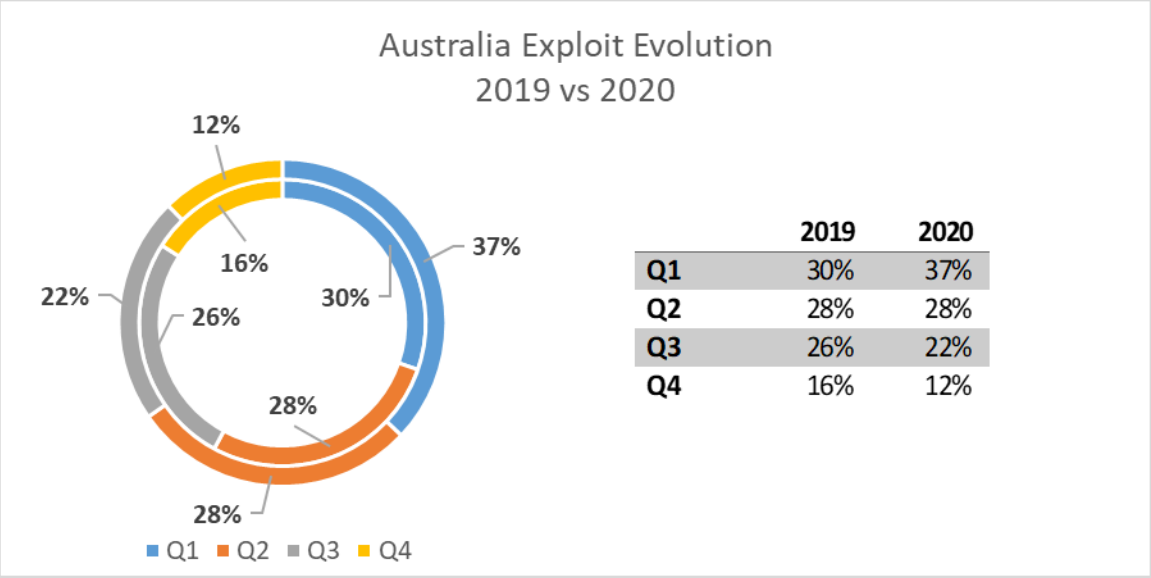
	2019	2020
Q1	32%	50%
Q2	30%	23%
Q3	25%	17%
Q4	13%	11%

Fig. 55 – Australia Coin Miner Evolution 2019 vs 2020



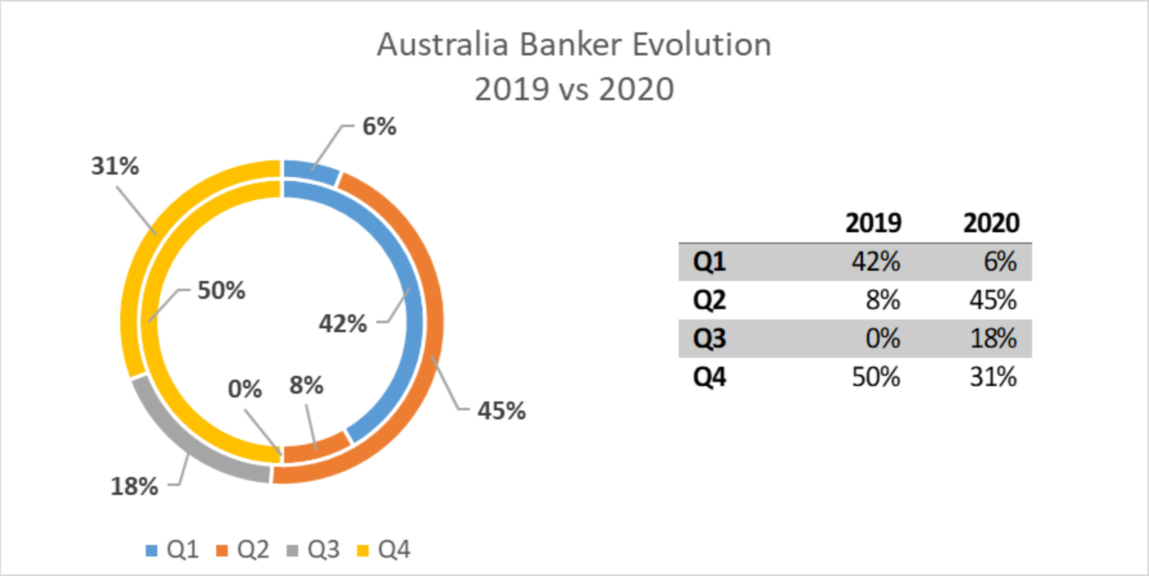
	2019	2020
Q1	28%	21%
Q2	28%	31%
Q3	26%	30%
Q4	18%	19%

Fig. 56 – Australia PUA Evolution 2019 vs 2020



	2019	2020
Q1	30%	37%
Q2	28%	28%
Q3	26%	22%
Q4	16%	12%

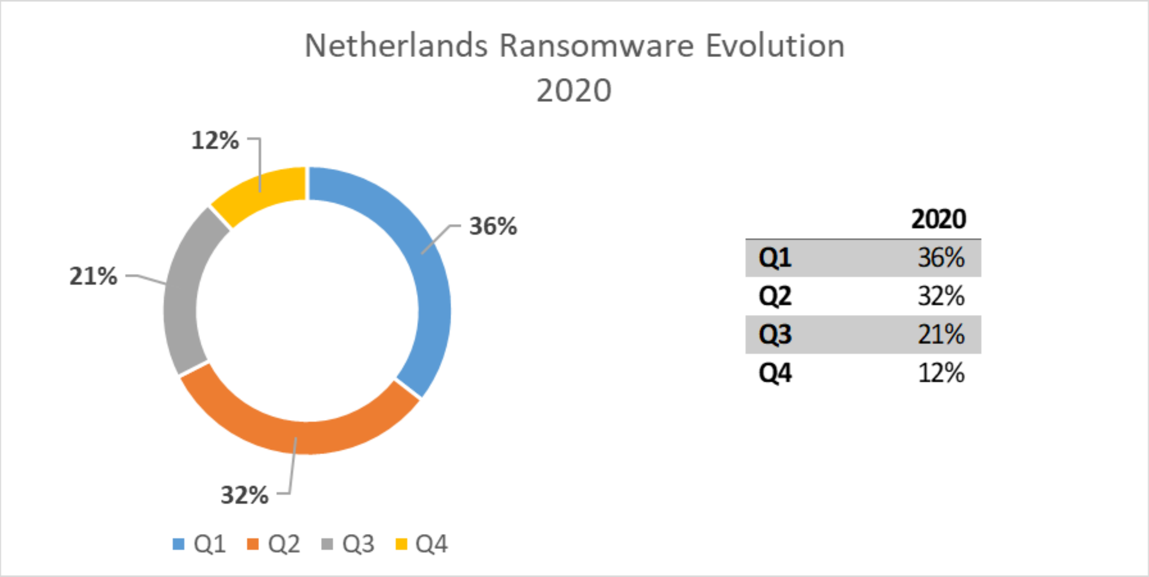
Fig. 57 – Australia Exploit Evolution 2019 vs 2020



	2019	2020
Q1	42%	6%
Q2	8%	45%
Q3	0%	18%
Q4	50%	31%

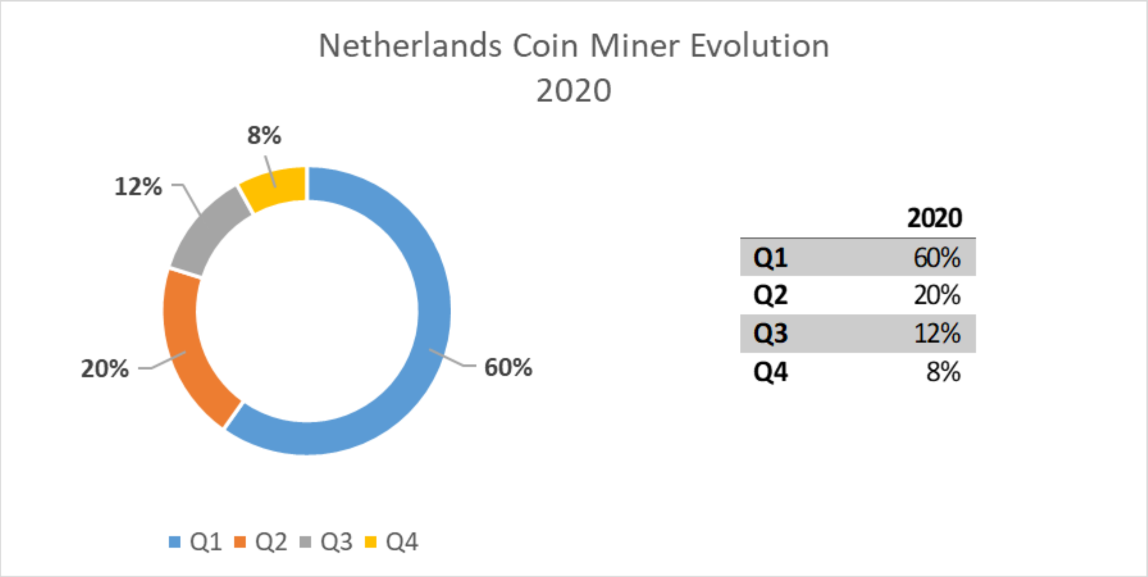
Fig. 58 – Australia Banker Evolution 2019 vs 2020

Netherlands



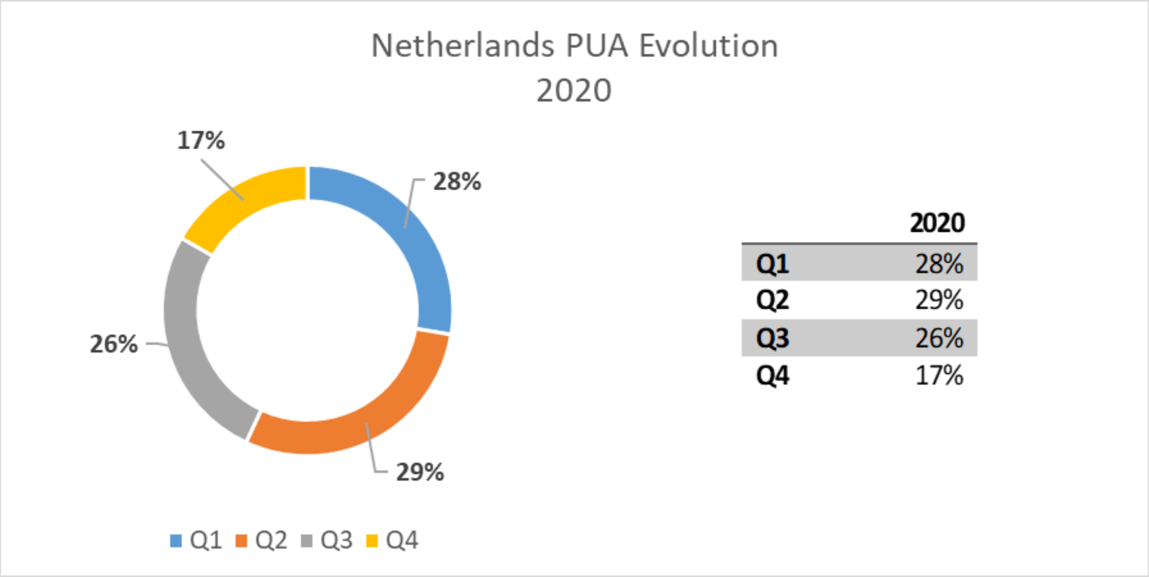
	2020
Q1	36%
Q2	32%
Q3	21%
Q4	12%

Fig. 59 – Netherlands Ransomware Evolution 2019 vs 2020



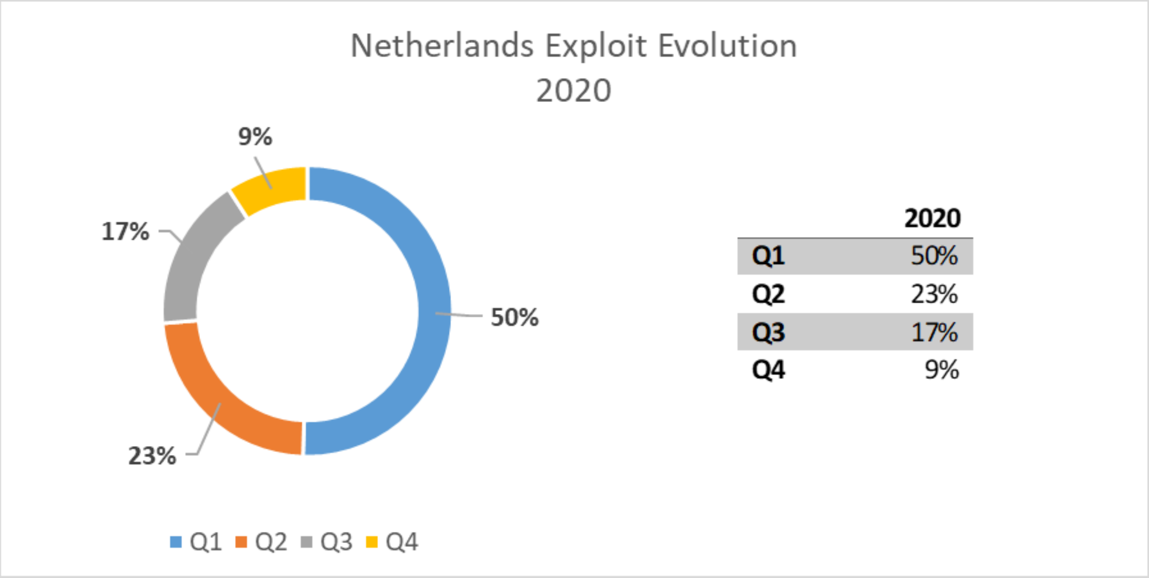
	2020
Q1	60%
Q2	20%
Q3	12%
Q4	8%

Fig. 60 – Netherlands Coin Miner Evolution 2019 vs 2020



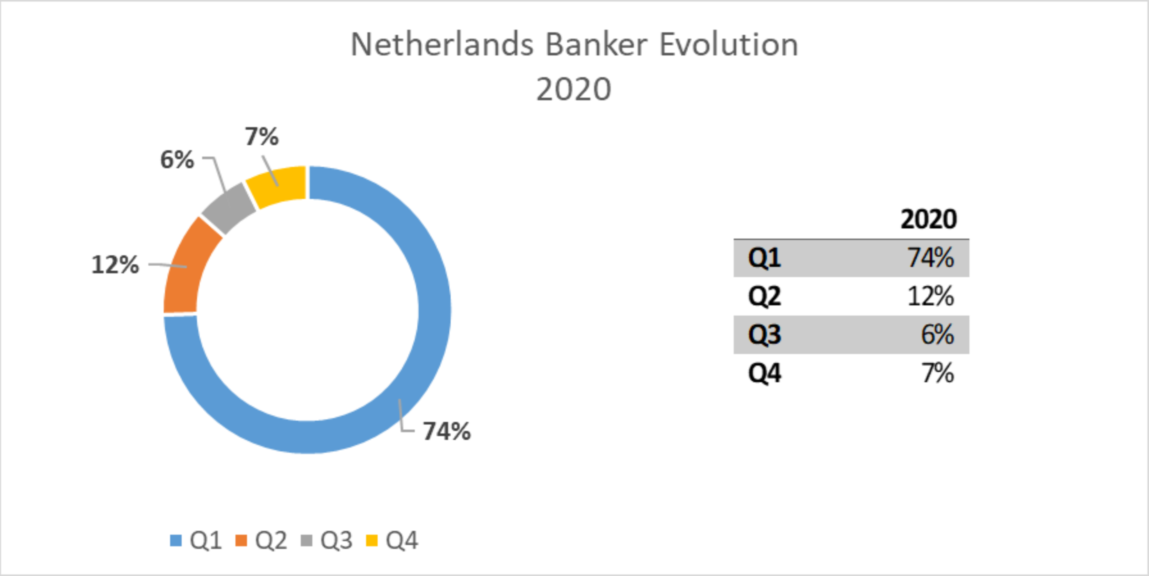
	2020
Q1	28%
Q2	29%
Q3	26%
Q4	17%

Fig. 61 – Netherlands PUA Evolution 2019 vs 2020



	2020
Q1	50%
Q2	23%
Q3	17%
Q4	9%

Fig. 62– Netherlands Exploit Evolution 2019 vs 2020

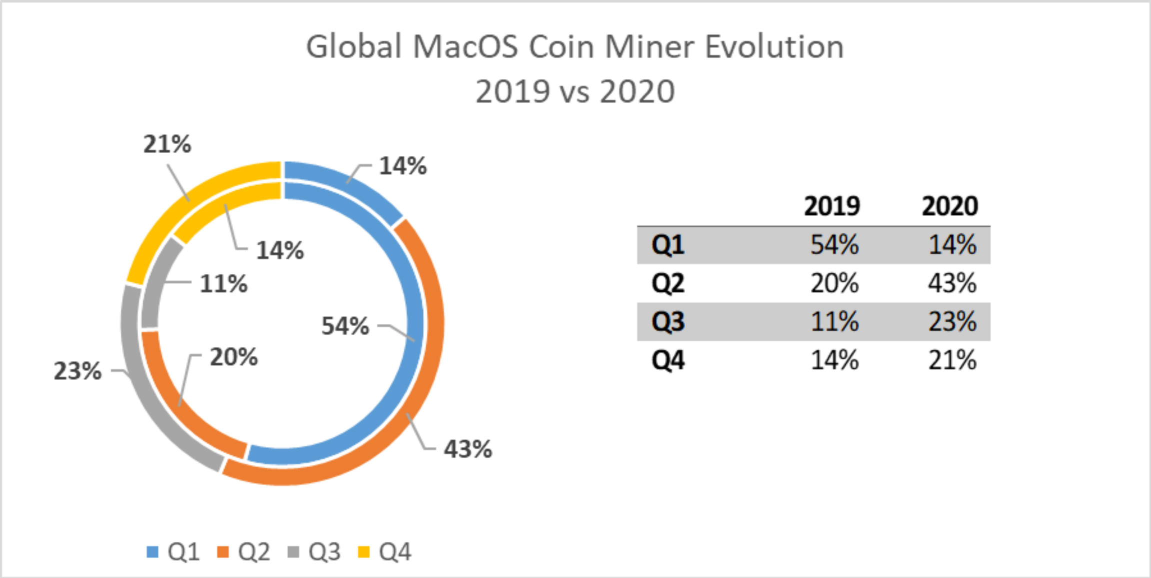


	2020
Q1	74%
Q2	12%
Q3	6%
Q4	7%

Fig. 63 – Netherlands Banker Evolution 2019 vs 2020

macOS Threat Landscape

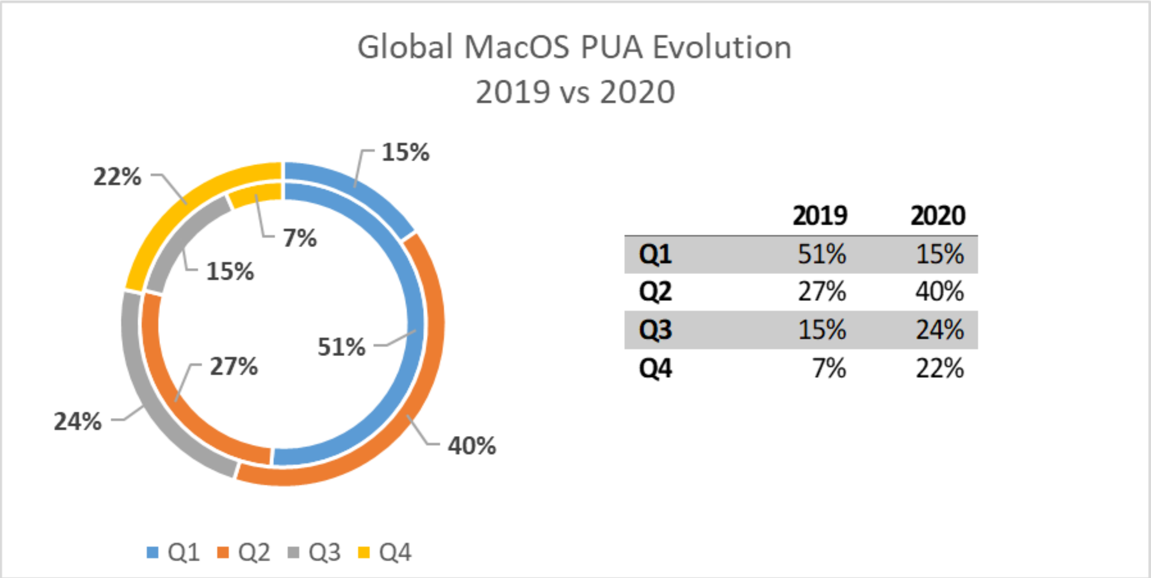
The threat landscape for MacOS, when comparing how threats have evolved in 2020 compared to 2019, saw some interesting shifts. Coin miners, PUAs and exploits evolved somewhat differently throughout 2020 than they did within 2019. If 74 percent of coin miner reports in 2019 were reported during the first half of the year, only 57 percent of coin miner reports in 2020 were reported during the first half of 2020.



	2019	2020
Q1	54%	14%
Q2	20%	43%
Q3	11%	23%
Q4	14%	21%

Fig. 64 – Global MacOS Coin Miner Evolution 2019 vs 2020

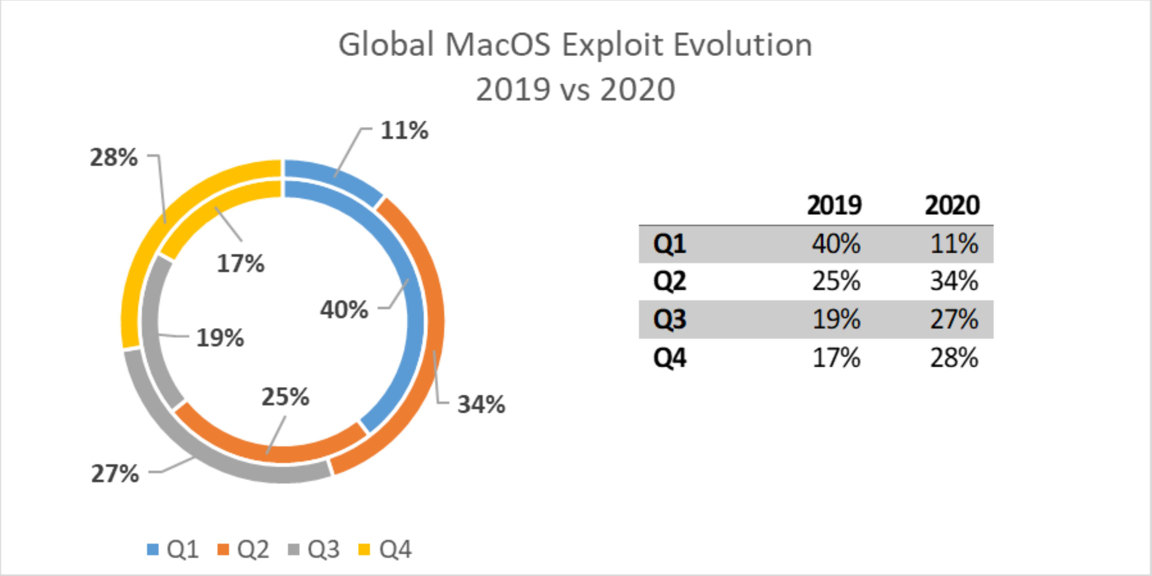
Potentially unwanted applications may be a nuisance for Windows-running users, but they also affect MacOS. The highest number of Potentially Unwanted Applications reports for MacOS during 2020 was registered during the second quarter, with 40 percent of all PUA reports for MacOS during the year. While in 2019 the first quarter accounted for the highest number of reports throughout the year, during 2020 MacOS PUA reports were more even across all four quarters.



	2019	2020
Q1	51%	15%
Q2	27%	40%
Q3	15%	24%
Q4	7%	22%

Fig. 65 – Global MacOS PUA Evolution 2019 vs 2020

Exploit reports for MacOS in 2020 seem to have followed the same trend as potentially unwanted applications. The highest number of exploit reports for MacOS was reported during the second quarter of 2020, following a slow decline throughout the rest of the year. This trend is somewhat in line with how reports evolved in the previous year. During 2019 the highest number of MacOS exploits was reported in the first quarter, with 40 percent of the total number of reports throughout the year.



	2019	2020
Q1	40%	11%
Q2	25%	34%
Q3	19%	27%
Q4	17%	28%

Fig. 66 – Global MacOS Exploit Evolution 2019 vs 2020

Android Threat Landscape

Even if Android seems like a similar ecosystem to the rest of the platforms, most threats don't follow a similar pattern and are very specific to this operating system, closely emulating the general profile of regular phone users.

2020 was anything but a regular year for any industry, so it's easy to understand why Android threats evolved in an interesting pattern as well. The new work-from-home paradigm changed how we viewed the importance of an office setting, but it also changed how criminals found new avenues for attack, quickly adapting to a unique situation.

The advent of video conferencing solutions in the wake of the massive demand due to the COVID-19 pandemic opened the door for opportunistic threat actors. For example, our telemetry detected a very unusual trend in which a relatively large number of users started installing Zoom apps from sources other than the official ones[11]. This, of course, opened up their devices to potential infections with malware posing as Zoom installers.

Of course, the use of COVID-19 as a platform to spread malware was both foreseeable and preventable, but it happened anyway. We also detected Android apps[12] that promised valuable information about the pandemic at a time when such data was scarce. Using these malicious apps, mostly available through third-party marketplaces, attackers could potentially steal personal data, SMS messages, contacts, and much more.

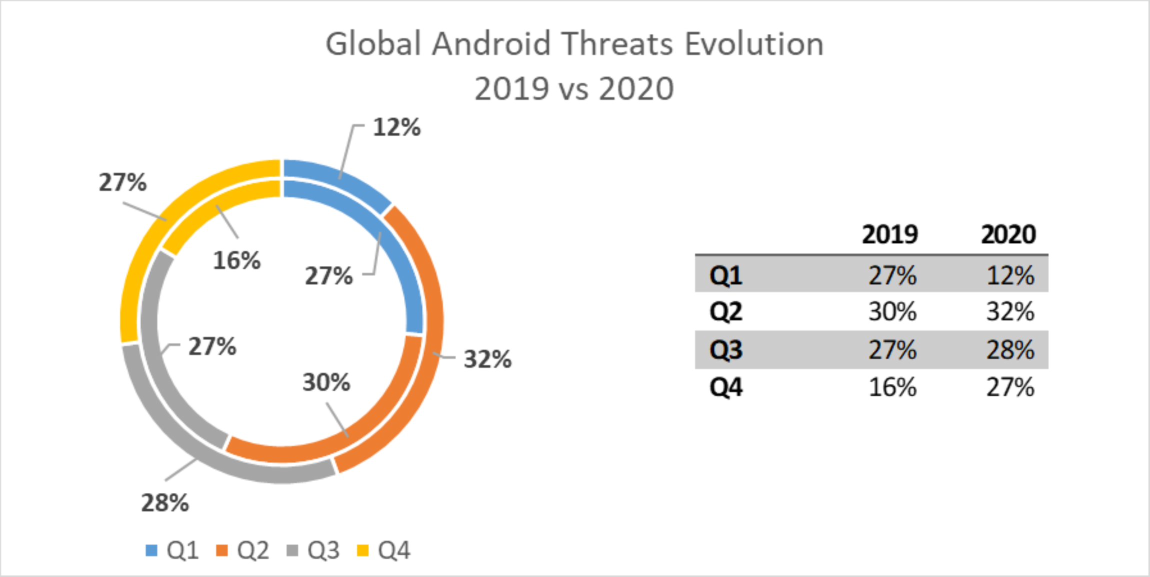
Pandemic-related apps were not the only ones to garner attention in 2020. We also discovered apps available through Google Play tainted with the Cerberus[13] Banker malware. Interestingly, these apps also delivered on their promised functionalities, with malware served as a side dish.

[11] "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/
[12] "Android Malware in COVID-19 Clothes Steals SMS and Contacts", Bitdefender, https://labs.bitdefender.com/2020/05/android-malware-in-covid-19-clothes-steals-sms-and-contacts/
[13] "Apps on Google Play Tainted with Cerberus Banker Malware", Bitdefender, https://labs.bitdefender.com/2020/09/apps-on-google-play-tainted-with-cerberus-banker-malware/

One of the more interesting pieces of malware found in 2020 was Mandrake[14]. Its developers went through a lot of trouble to infect only specific devices. Attackers were interested in very particular targets, avoiding countries that would not bring them any return of interest. The infection itself was triggered when the users apparently accepted the EULA, but actually granted criminals extremely powerful permissions.

We can also observe that Android is becoming a much more targeted platform for spying campaigns deployed by APTs. One of these campaigns made headlines in 2020. Dubbed Bitter[15], the Advanced Persistent Threat group (also known as APT-C-08) has been active both in desktop and mobile malware campaigns for quite a long time, as their activity seems to date back to 2014.

Overall, 2020 differed a lot from 2019, with attackers focusing more on capitalizing on popular topics such as the coronavirus pandemic or the increase adoption of productivity or video conferencing tools.



	2019	2020
Q1	27%	12%
Q2	30%	32%
Q3	27%	28%
Q4	16%	27%

Fig. 67 – Global Android Threats Evolution 2019 vs 2020

In terms of the global evolution of top Android malware families, it's worth noting that Android.Trojan.Agent Android malware family ranked first, with 35 percent of the total global number of Android malware reports during the second half of 2020. Android malware in this category tends to run in the background and not reveal its presence on the victim's device. Used either for information exfiltration or to amass compromised devices into DDoS-performing botnets, this Android malware category contains a wide range of threats, with different capabilities.

[14] "Mandrake – owning Android devices since 2016", Bitdefender, https://labs.bitdefender.com/2020/05/mandrake-owning-android-devices-since-2016/
[15] "BitterAPT Revisited: the Untold Evolution of an Android Espionage Tool", Bitdefender, https://labs.bitdefender.com/2020/06/bitterapt-revisited-the-untold-evolution-of-an-android-espionage-tool/

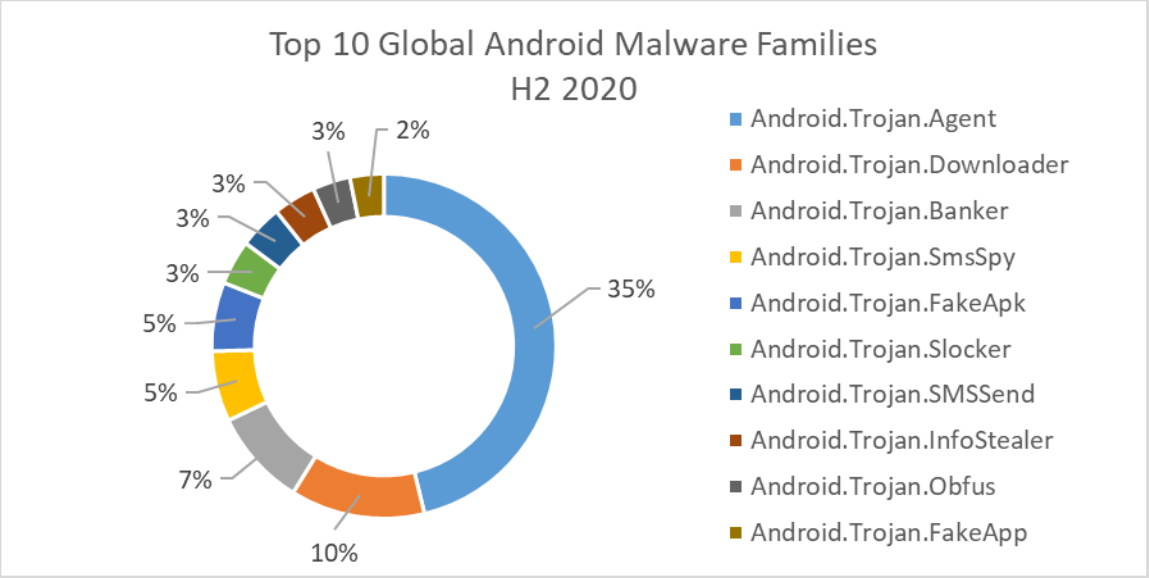
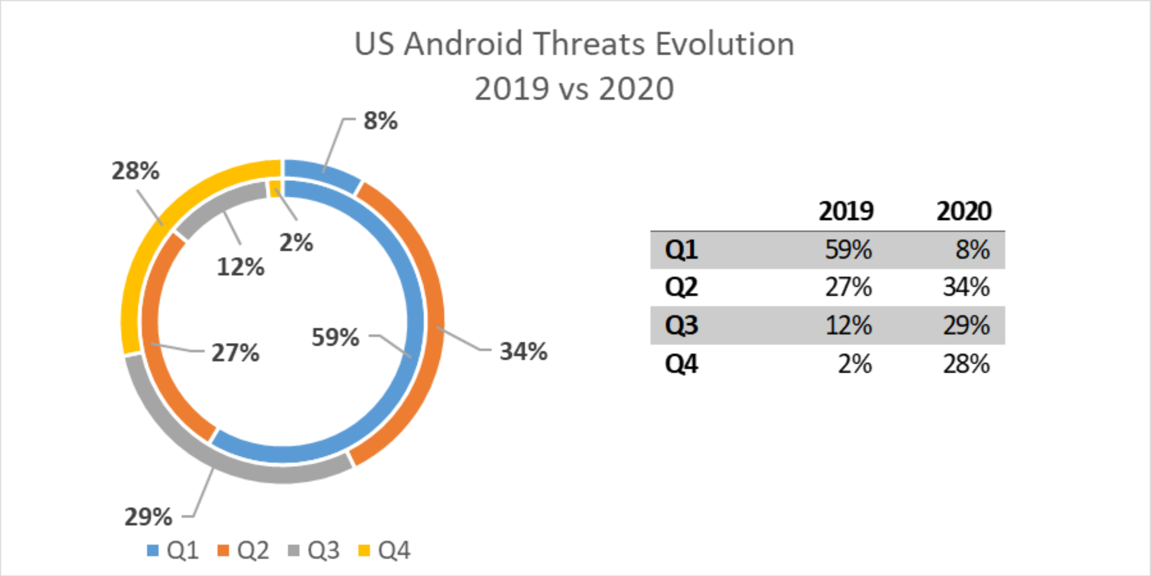


Fig. 68 – Top 10 Global Android Malware Families H2 2020

The Android.Trojan.Downloader Android malware family came second, with 10 percent of the total global number of Android malware reports during the second half of 2020. Mainly used to install additional malicious apps, most threats in this category act as first-stage downloaders, just as the category name implies.

The global evolution of Android malware families continues to feature Android Bankers Trojans, SMS-sending malware, fake applications, and even various ransom-demanding screen lockers (ransomware-like threats), which suggest that the Android threat landscape is also very diverse.

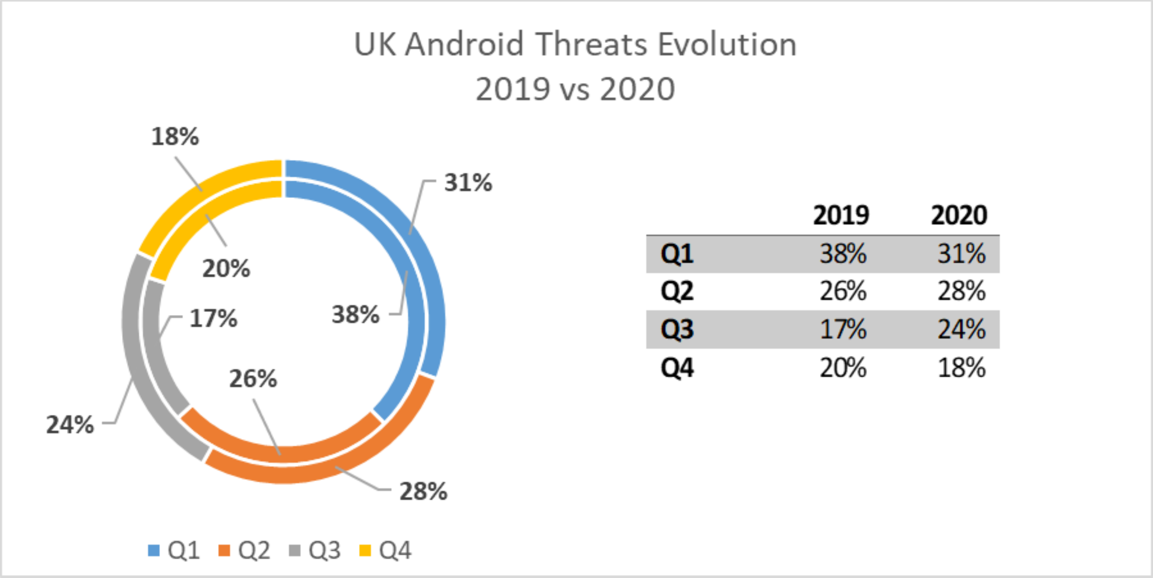
United States



	2019	2020
Q1	59%	8%
Q2	27%	34%
Q3	12%	29%
Q4	2%	28%

Fig. 69 – US Android Threats Evolution 2019 vs 2020

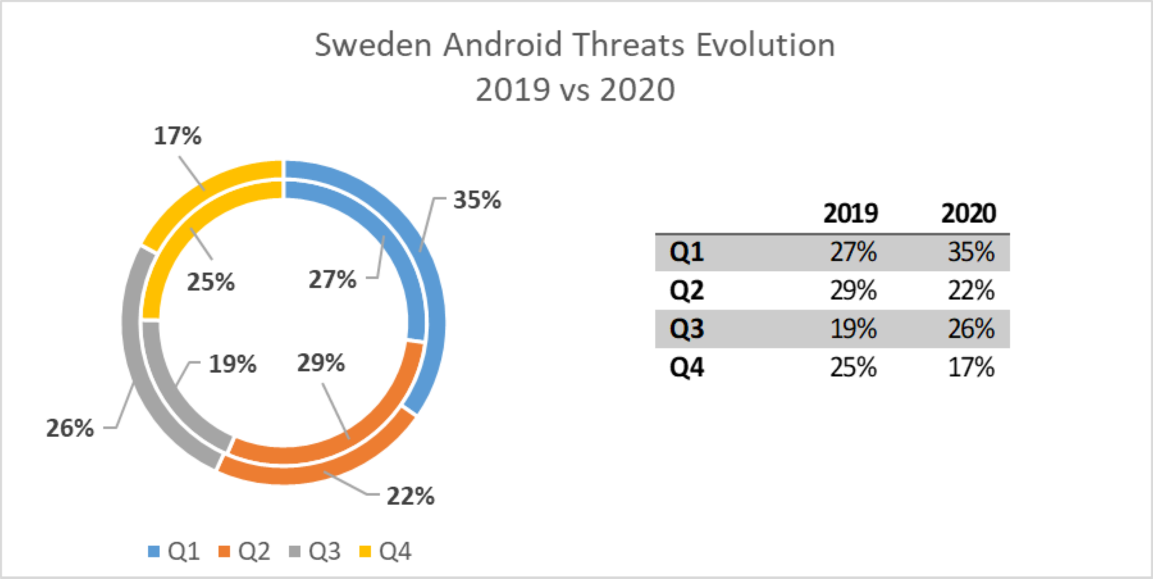
United Kingdom



	2019	2020
Q1	38%	31%
Q2	26%	28%
Q3	17%	24%
Q4	20%	18%

Fig. 70 – UK Android Threats Evolution 2019 vs 2020

Sweden

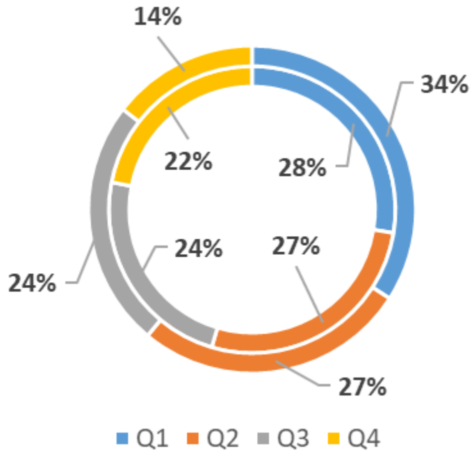


	2019	2020
Q1	27%	35%
Q2	29%	22%
Q3	19%	26%
Q4	25%	17%

Fig. 71 – Sweden Android Threats Evolution 2019 vs 2020

Romania

Romania Android Threats Evolution
2019 vs 2020

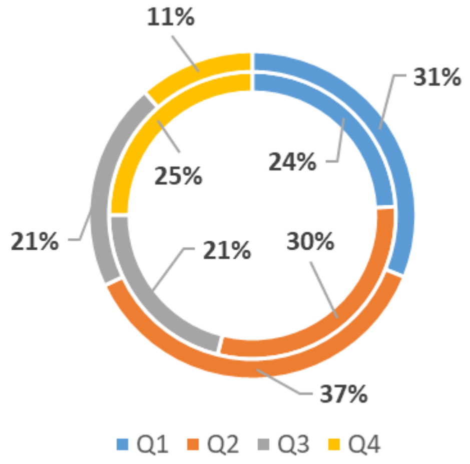


	2019	2020
Q1	28%	34%
Q2	27%	27%
Q3	24%	24%
Q4	22%	14%

Fig. 72– Romania Android Threats Evolution 2019 vs 2020

Italy

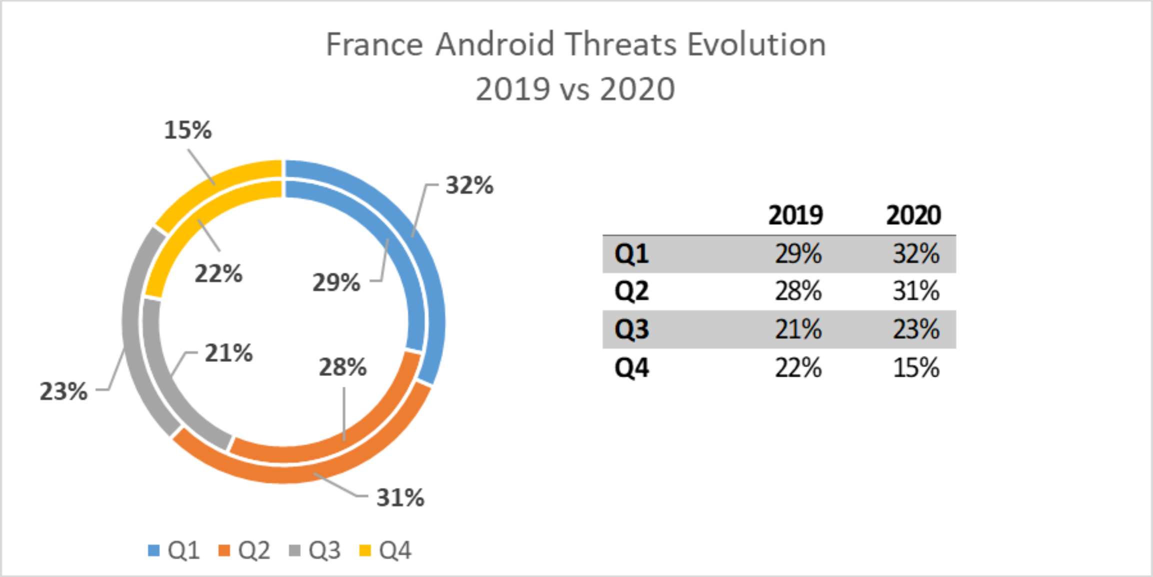
Italy Android Threats Evolution
2019 vs 2020



	2019	2020
Q1	24%	31%
Q2	30%	37%
Q3	21%	21%
Q4	25%	11%

Fig. 73 – Italy Android Threats Evolution 2019 vs 2020

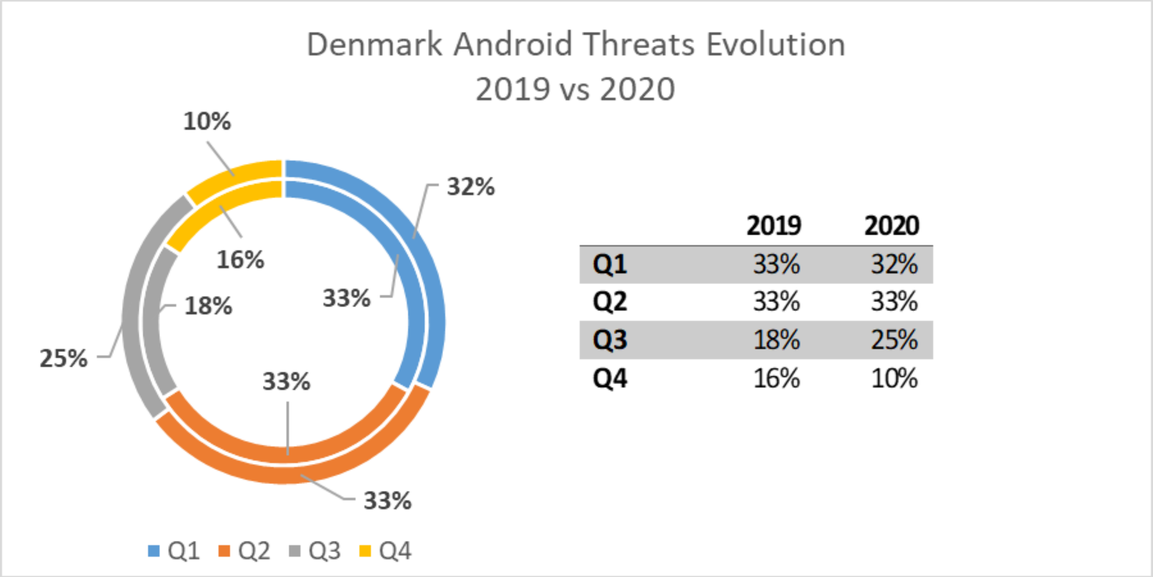
France



	2019	2020
Q1	29%	32%
Q2	28%	31%
Q3	21%	23%
Q4	22%	15%

Fig. 74 – France Android Threats Evolution 2019 vs 2020

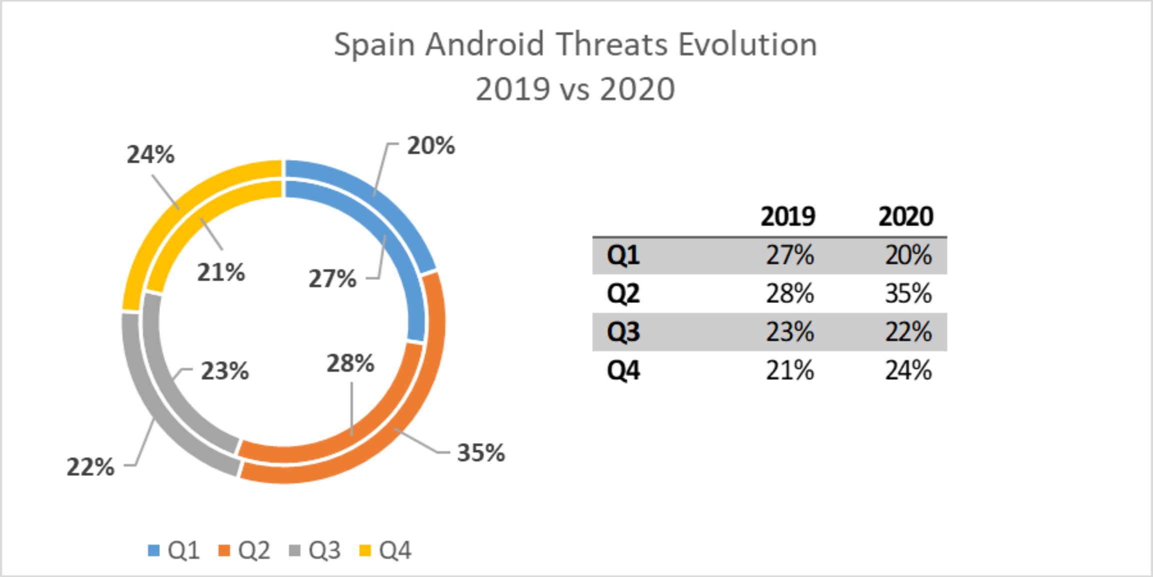
Denmark



	2019	2020
Q1	33%	32%
Q2	33%	33%
Q3	18%	25%
Q4	16%	10%

Fig. 75 – Denmark Android Threats Evolution 2019 vs 2020

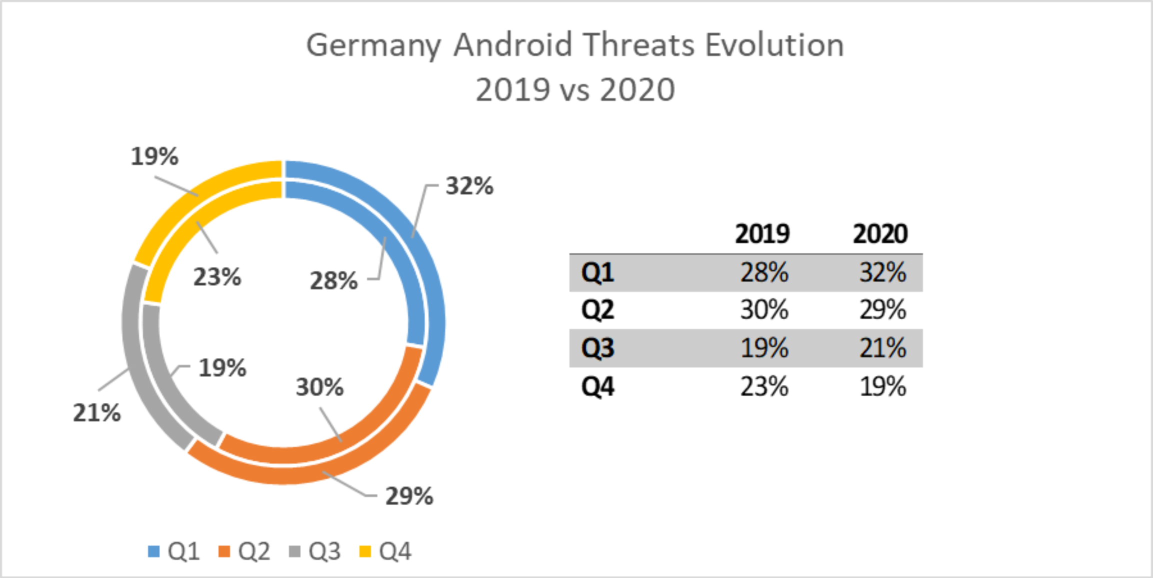
Spain



	2019	2020
Q1	27%	20%
Q2	28%	35%
Q3	23%	22%
Q4	21%	24%

Fig. 76 – Spain Android Threats Evolution 2019 vs 2020

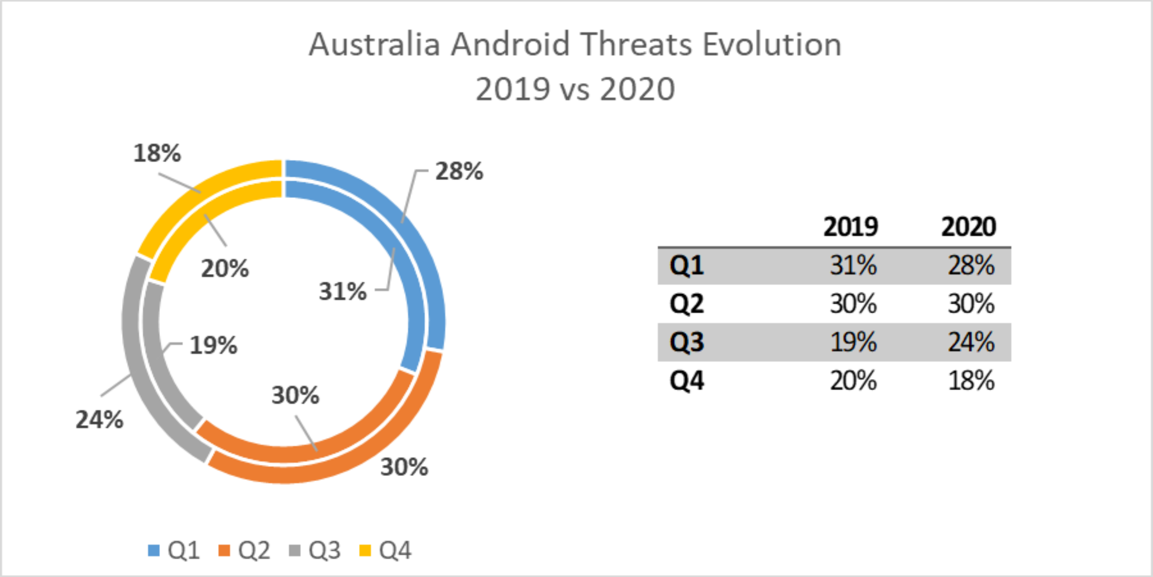
Germany



	2019	2020
Q1	28%	32%
Q2	30%	29%
Q3	19%	21%
Q4	23%	19%

Fig. 77 – Germany Android Threats Evolution 2019 vs 2020

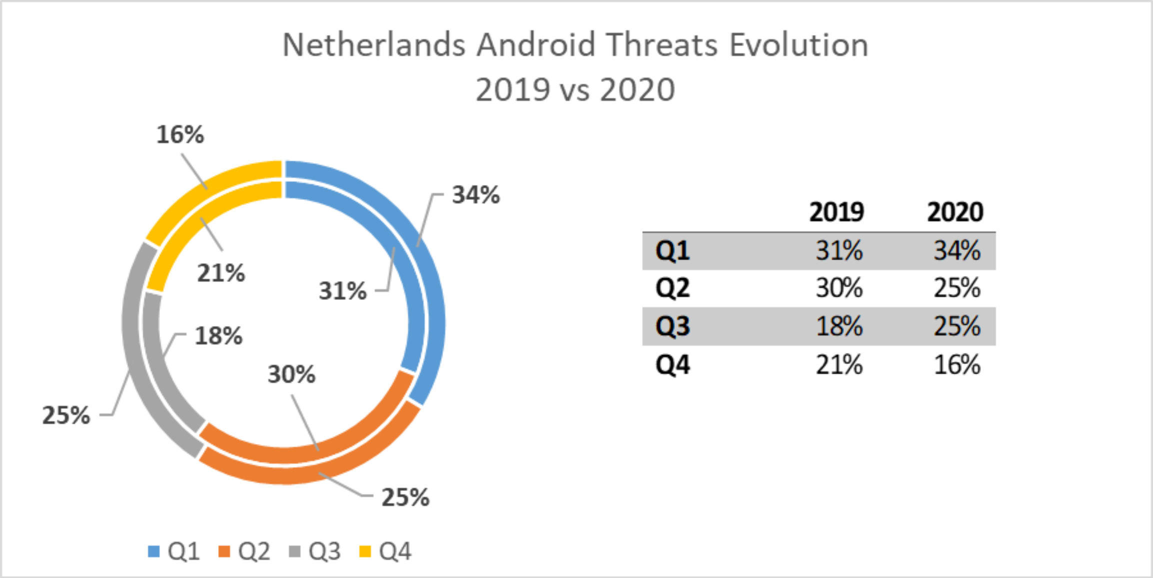
Australia



	2019	2020
Q1	31%	28%
Q2	30%	30%
Q3	19%	24%
Q4	20%	18%

Fig. 78 – Australia Android Threats Evolution 2019 vs 2020

Netherlands



	2019	2020
Q1	31%	34%
Q2	30%	25%
Q3	18%	25%
Q4	21%	16%

Fig. 79 – Netherlands Android Threats Evolution 2019 vs 2020

Internet of Things (IoT) Threat Landscape

The expansion of the Internet of Things (IoT) ecosystem is one of the few constants in the technology market, and it's only rivaled by another certainty. More IoT devices deployed in the wild directly translates into a larger attack surface and, with the number of smart homes expected to grow at a compound annual growth rate (CAGR) of 12.5 percent in North America and 20.2 percent in Europe[16], there's no shortage of potential problems.

When it comes to IoT devices, there's something else that doesn't seem to be impacted by the industry's continuous evolution, and that's a poor security track record. Regardless of how many new IoT devices arrive onto the market or how many features they've been bundled with over the years, they still pack security challenges.

One reason for this lack of security hardening may revolve around poor design from manufacturers, lack of meaningful support after launch, and even abandonment. It's a multifaceted problem because sometimes the average user is also part of the issue when they don't change default credentials or use weak ones, they don't update the devices' firmware and software or they don't replace the IoT when it reaches end of life (EOL).

There's one trend we noticed in 2020, and it's likely linked to the COVID-19 pandemic and the fact that people got stuck indoors and begun to look for more IoT niches to fill in their already smart homes. Many of the vulnerabilities and security issues we found are in everyday items that are now smart.

For example, we analyzed the August Smart Lock[17], an Internet-connected device that, in theory, has a very extensive market for landlords, allowing them to issue and revoke access by electronically sharing a token or pin code during booking. What we found was a vulnerability that, if exploited, could allow attackers to intercept the Wi-Fi password.

Another potential security issue involved the ITEAD Sonoff / eWeLink platform-as-a-service that manages remote control and connectivity between smart switches, relays or outlets and the software applications controlling them. The vulnerability identified by Bitdefender could let attackers gain control of random devices.

Apart from our own research, an avalanche of vulnerabilities have been found in the TCP/IP stack, like the Amnesia:33 collection of security issues[18] or the similar Ripple20[19]. Combining both, there is a potential to affect hundreds of millions of IoT devices.

Looking at our telemetry, we noticed an increase in the number of vulnerable devices in people's homes. For example, **network-attached devices** may not be in the top 20 most common IoT devices, but they **rank first in the number of identified vulnerabilities**. That number **increased by 189 percent YoY from 2019 to 2020**.

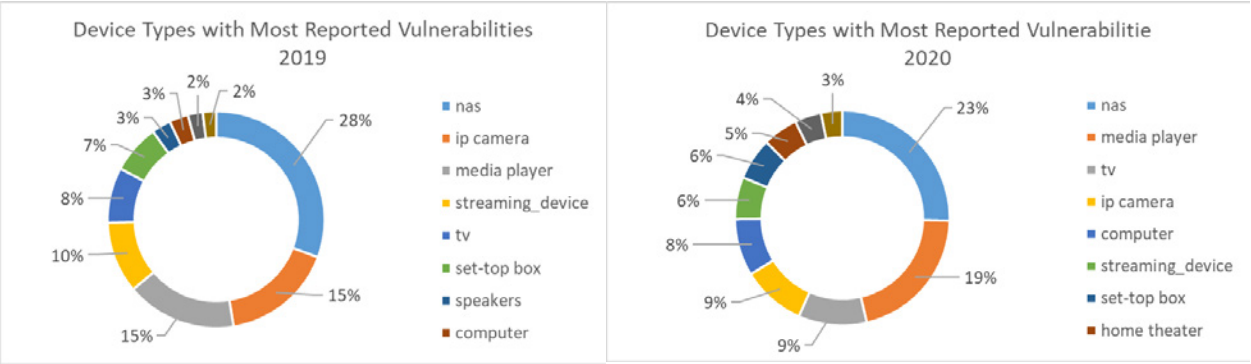


Fig. 80 – Device Types with Most Reported Vulnerabilities 2019 vs 2020

[16] "Smart Homes and Home Automation", BERG Insight, http://www.berginsight.com/ReportPDF/ProductSheet/bi-sh8-ps.pdf
[17] "Cracking the August SmartLock: WiFi Password Eavesdropping Made Easy", Bitdefender, https://www.bitdefender.com/files/News/CaseStudies/study/363/Bitdefender-PR-Whitepaper-AugustConnect-creat4699-en-EN-GenericUse.pdf
[18] "AMNESIA:33 How TCP/IP Stacks Breed Critical Vulnerabilities in IoT, OT and IT Devices", Forescout, https://www.forescout.com/company/resources/amnesia33-how-tcp-ip-stacks-breed-critical-vulnerabilities-in-iot-ot-and-it-devices/
[19] "Ripple20", JSOF, https://www.jsof-tech.com/disclosures/ripple20/

IP cameras are another sore spot in the IoT ecosystem because of the nature of the data they capture. Their presence in the top 10 most vulnerable IoT devices could be cause for concern. The LifeShield[20] Bitdefender research demonstrates, again, why using IP cameras in your home is not a clear-cut proposition that comes with little to no risk for the users.

IP cameras are among the most vulnerable IoT devices, according to Bitdefender telemetry, and they also **registered a 99 percent YoY increase in the number of vulnerabilities in 2020, compared to 2019**.

Smart TVs are also becoming more popular, meaning more users now have powerful hardware in their homes that could attract cybercriminals. Compounded with the **335 percent YoY increase in the number of vulnerabilities found in Smart TV** by our technologies, it something to consider when evaluating your home network security.

Finally, we would be remiss not to mention the smart home theater. There seems to have been a rise in popularity of these types of devices, according to our telemetry, clocking in at eight place in our top most vulnerable devices in 2020.

We looked at the most used operating systems of devices monitored by Bitdefender's IoT technologies. We compared them with the data we had on the most vulnerable devices. To say that the results are surprising is an understatement.

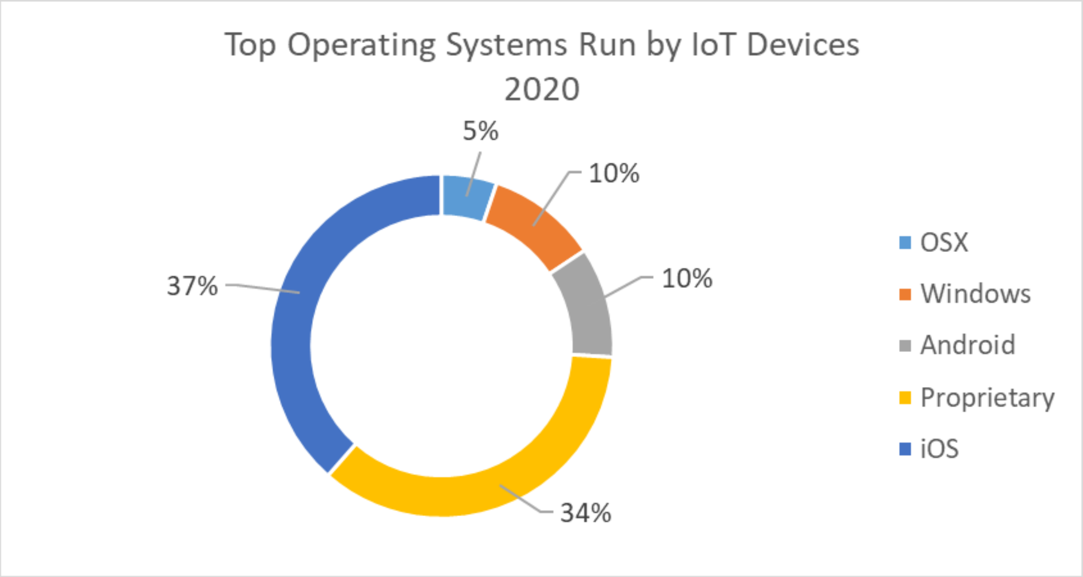


Fig. 81 – Top Operating Systems Run by IoT Devices 2020

It turns out that while devices with proprietary operating systems make up 34 percent of what people usually own, they are responsible for 92 percent of all detected vulnerabilities. It's a worrying statistic that's unlikely to change anytime soon.

[20] "Cracking the LifeShield: Unauthorized Live-Streaming in your Home", Bitdefender, https://labs.bitdefender.com/2021/01/cracking-the-lifeshield-unauthorized-live-streaming-in-your-home/

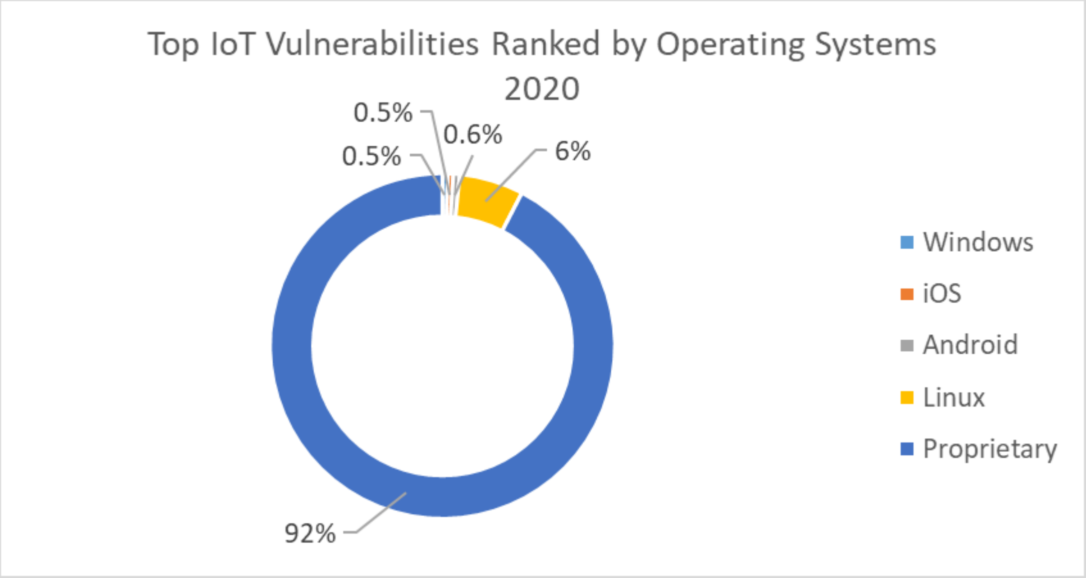


Fig. 82 – Top IoT Vulnerabilities Ranked by Operating Systems 2020

Spam Evolution

Throughout 2020, bad actors have exploited the ongoing stream of news, events and changes in economic and social agendas, consistent with the increased digitalization and overall growth in internet use due to the health crisis.

Spam emails continued to reign among the most-adopted cyber weapons deployed by cybercriminals during the second half of 2020. Spammers sought to trick recipients into revealing their financial information or installing credential-stealing Trojans and ransomware on their device.

In the first half of 2020, we saw a jump in phishing and malware campaigns surrounding the pandemic, as financial hardship and confusion created the perfect storm for cybercriminals and fraudsters seeking to capitalize on global lockdowns.

Despite these favorable conditions, the global email spam rate has decreased since 2019, dropping 3.88 percentage points in 2020.

Throughout 2020, Americans received the largest share of unsolicited spam emails, consisting of 38 percent of global spam volume, increasing by 4.51 percentage points since 2019 (34 percent), according to Bitdefender spam telemetry. The United States may have provided the most profitable opportunities for scammers to rip off the population as they continued to exploit government-issued stimulus payments. The economic fallout from COVID-19 sent shockwaves around the US, as millions of workers were laid off during the first half of 2020. The trend is likely to pick up again with an expected second round of stimulus payments underway.

The UK comes in second place, receiving 7 percent of global spam by volume, gaining 1.31 percentage points compared to 2019 (6 percent), according to Bitdefender spam telemetry. In contrast to 2019, Sweden dropped 1.49 percentage points, earning the third spot in the global rundown of received spam with 5 percent. Similarly, Germany shed 0.89 percentage points, taking fourth place with 5 percent of the received global spam volume of 2020.

Overall, significantly more spam email was received in March 2020 (9 percent) than in any other month in 2020.

However, in the second half of 2020, it’s interesting to spot that most unsolicited emails were received in July (18 percent, from the total amount of spam reported in the second half of 2020) than in any other month.

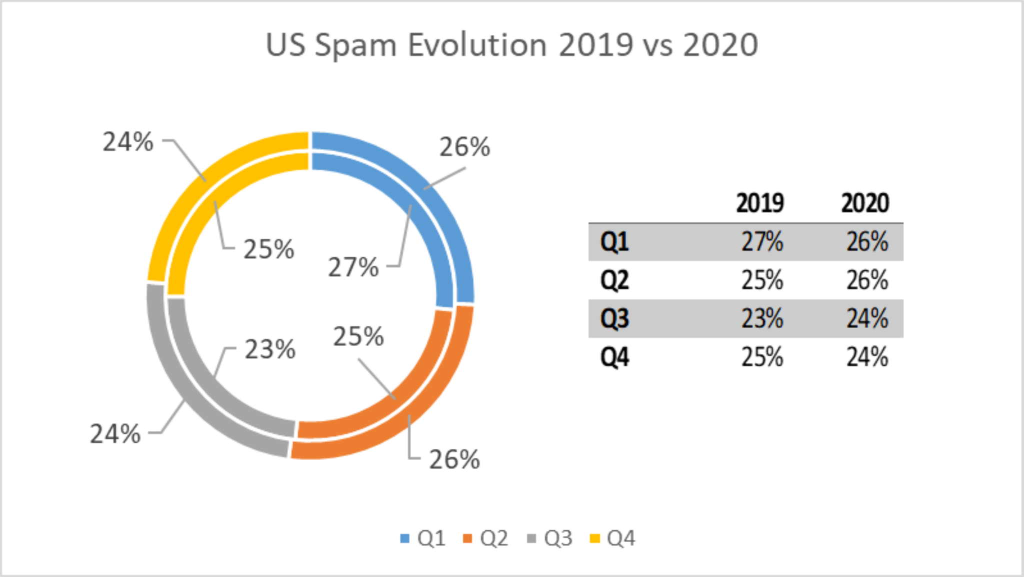
In the second half of 2019, Bitdefender telemetry picked up three globally significant spikes in received spam during August (17 percent), September (17 percent), and October (19 percent), but our telemetry only registered two globally significant spikes in received spam in 2020, in July and October (17 percent).

In 2019, spammers were keen on exploiting highly anticipated releases of Hollywood movies, TV shows and gadgets, baiting recipients with "free" streaming and discount opportunities to steal personal and financial information. Additionally, on top of billions of generally harmless promotional emails clogging inboxes daily, scams and phishing emails are the second-biggest categories of spam targeting recipients in 2020.

Bypassing spam filters was the hallmark of 2020, as attackers developed new means of delivering unsolicited emails, tailoring fraudulent correspondence to the ongoing health crisis and pandemic-induced boom in e-commerce. Last year, spammers spent their energy improving old ruses, concentrating on quality rather than quantity and highlighting their creativity and ability to adapt to social and economic changes. From get-rich-quick schemes, fake lottery scams and Black Friday discounts, cybercriminals have managed to set up a profitable business throughout 2020.

A constant recurrence in the spam and malspam campaigns of 2020 remains COVID-19. As the coronavirus filled headlines, scammers and fraudsters used the pandemic as a lure to trick recipients into installing malware or providing personally identifiable information. Unlike the first half of 2020, when spam tactics involved spreading fake news, COVID-19 updates and medical supplies, in the third and fourth quarter of 2020, cybercriminals shifted their focus to the economic struggle.

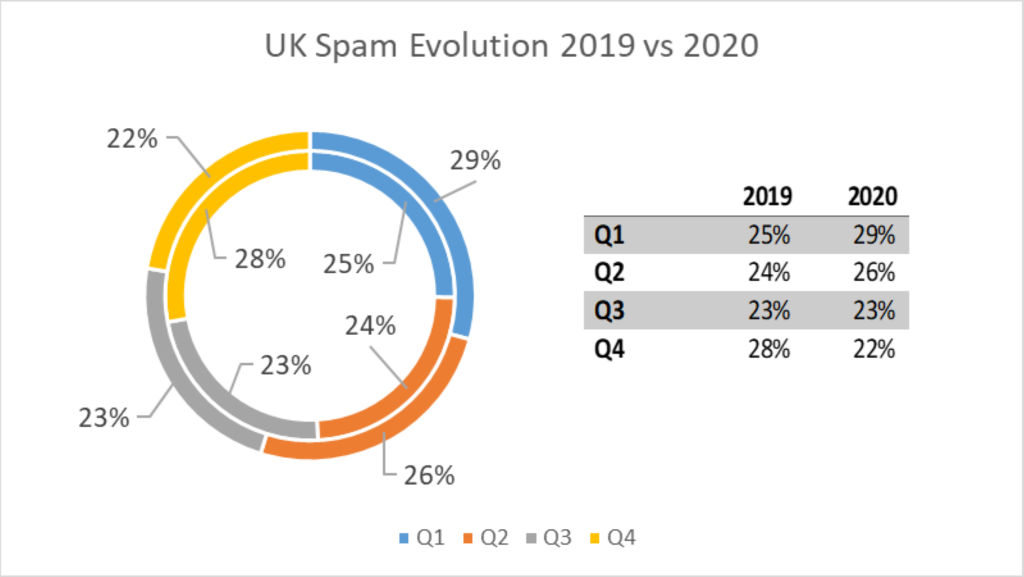
United States



	2019	2020
Q1	27%	26%
Q2	25%	26%
Q3	23%	24%
Q4	25%	24%

Fig. 83 – US Spam Evolution 2019 vs 2020

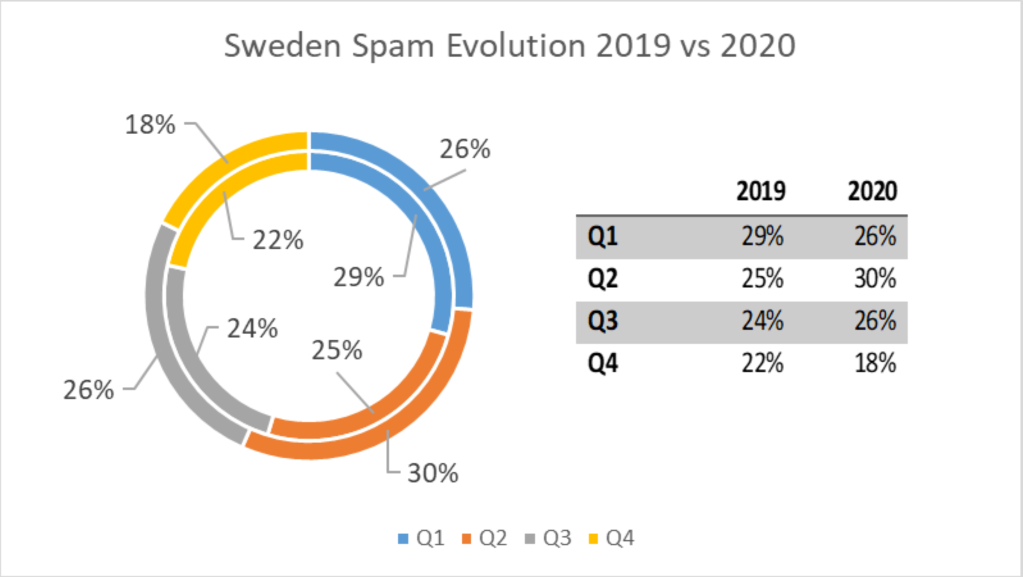
United Kingdom



	2019	2020
Q1	25%	29%
Q2	24%	26%
Q3	23%	23%
Q4	28%	22%

Fig. 84 – UK Spam Evolution 2019 vs 2020

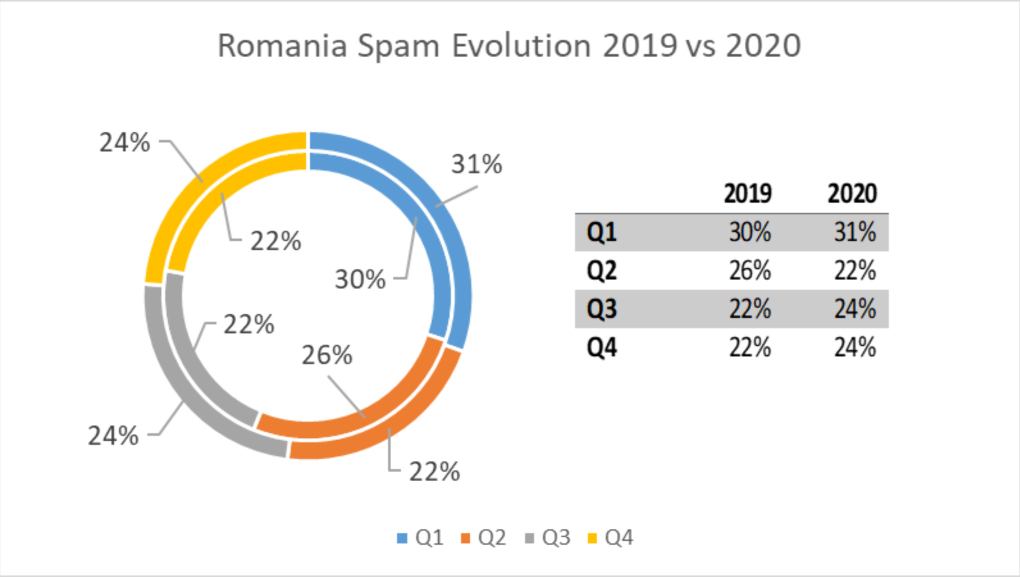
Sweden



	2019	2020
Q1	29%	26%
Q2	25%	30%
Q3	24%	26%
Q4	22%	18%

Fig. 85 – Sweden Spam Evolution 2019 vs 2020

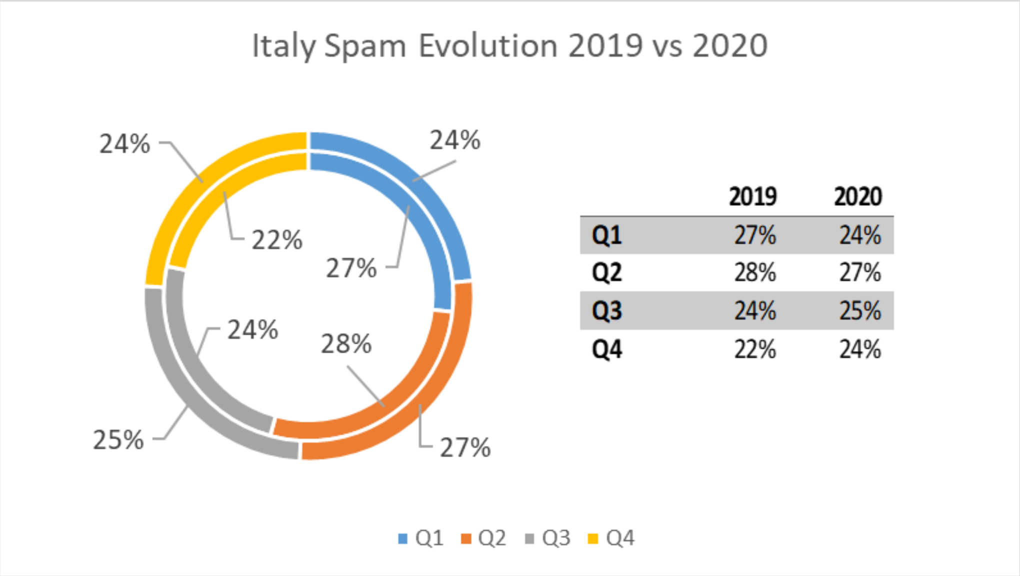
Romania



	2019	2020
Q1	30%	31%
Q2	26%	22%
Q3	22%	24%
Q4	22%	24%

Fig. 86 – Romania Spam Evolution 2019 vs 2020

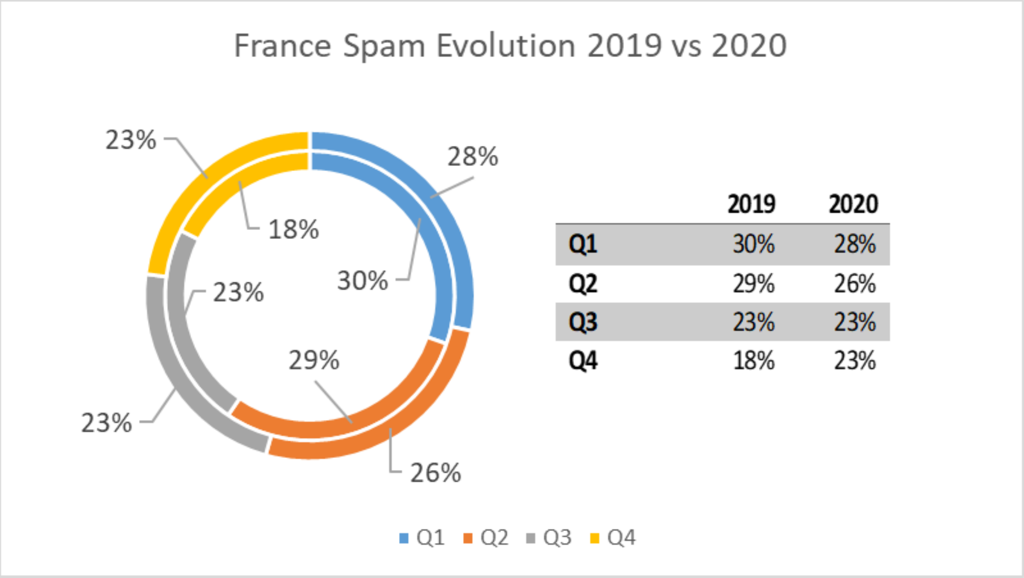
Italy



	2019	2020
Q1	27%	24%
Q2	28%	27%
Q3	24%	25%
Q4	22%	24%

Fig. 87 – Italy Spam Evolution 2019 vs 2020

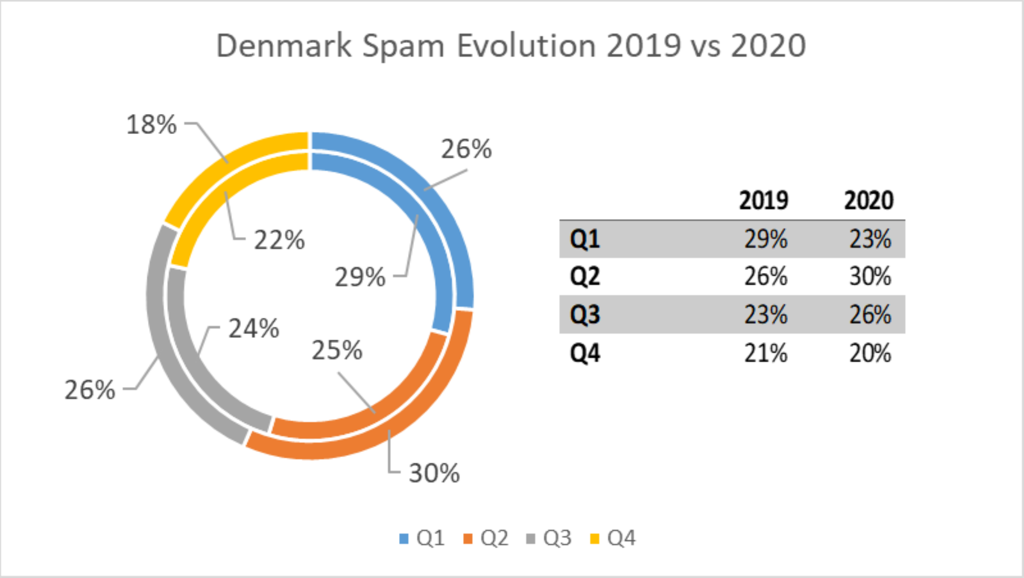
France



	2019	2020
Q1	30%	28%
Q2	29%	26%
Q3	23%	23%
Q4	18%	23%

Fig. 88 – France Spam Evolution 2019 vs 2020

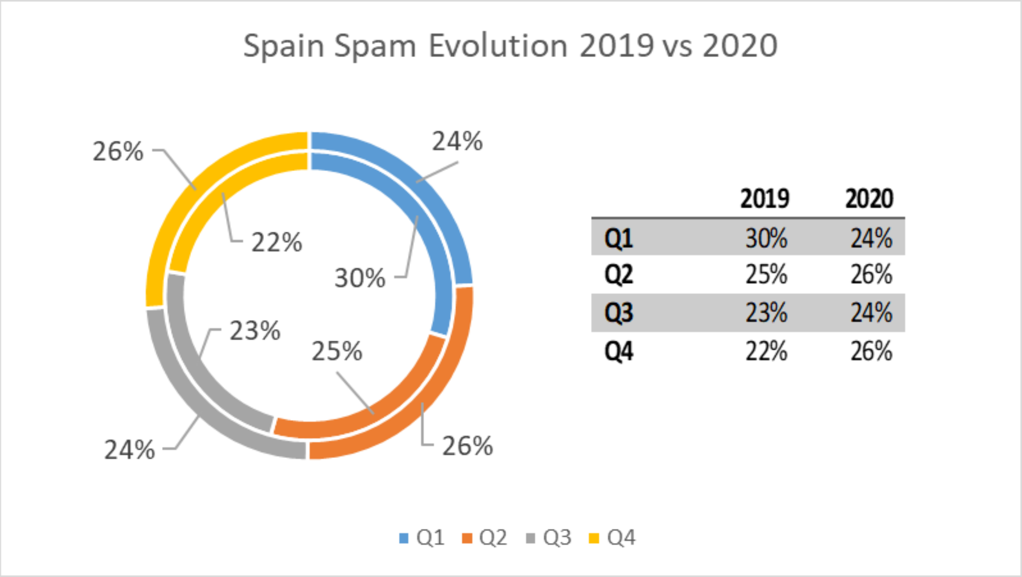
Denmark



	2019	2020
Q1	29%	23%
Q2	26%	30%
Q3	23%	26%
Q4	21%	20%

Fig. 89 – Denmark Spam Evolution 2019 vs 2020

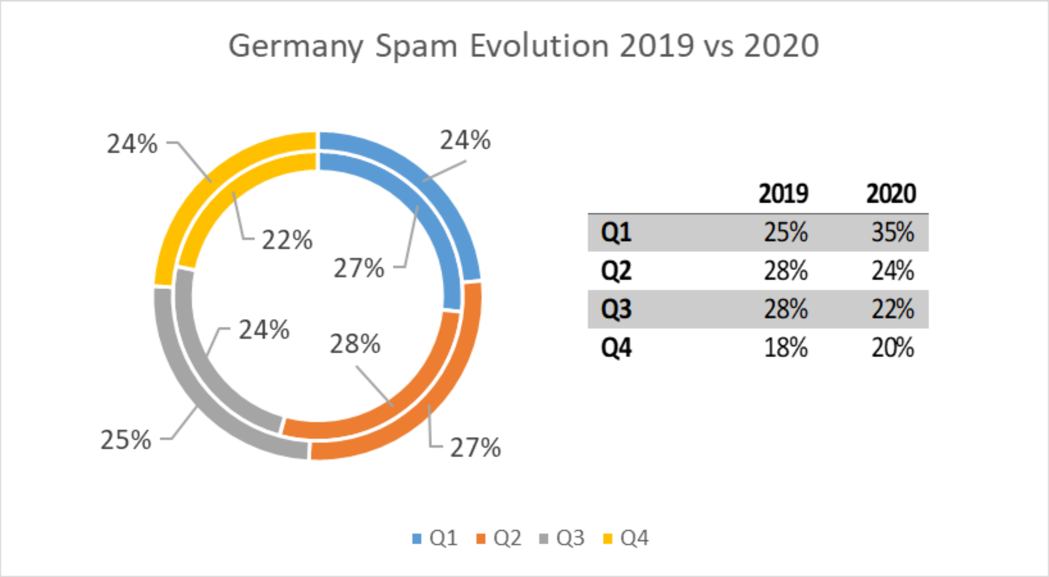
Spain



	2019	2020
Q1	30%	24%
Q2	25%	26%
Q3	23%	24%
Q4	22%	26%

Fig. 90 – Spain Spam Evolution 2019 vs 2020

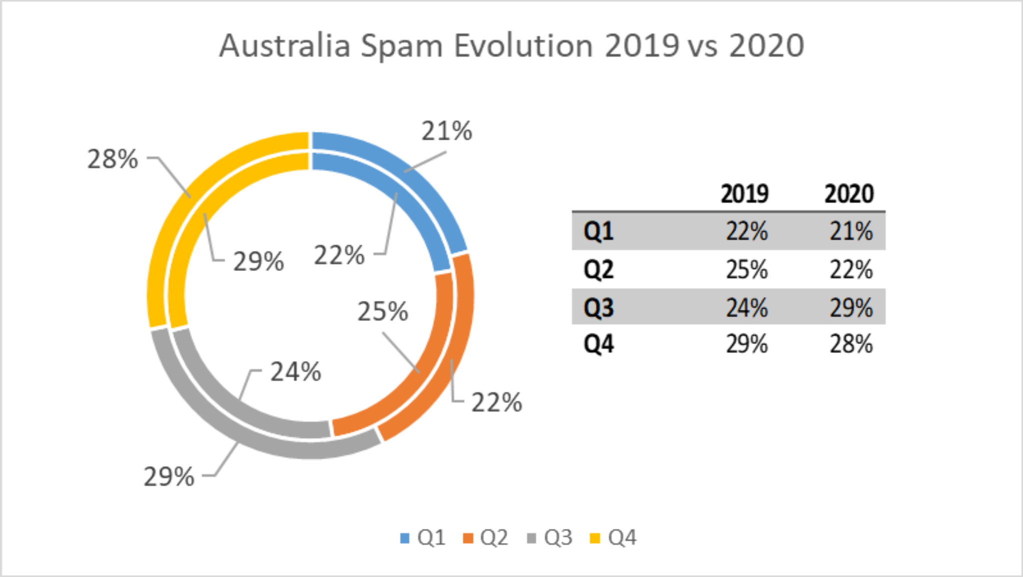
Germany



	2019	2020
Q1	25%	35%
Q2	28%	24%
Q3	28%	22%
Q4	18%	20%

Fig. 91 – Germany Spam Evolution 2019 vs 2020

Australia



	2019	2020
Q1	22%	21%
Q2	25%	22%
Q3	24%	29%
Q4	29%	28%

Fig. 92 – Australia Spam Evolution 2019 vs 2020

Scammers impersonate popular banks and financial services

Armed with six months of practicing on a remote-working population, some malicious actors have improved their social engineering skills and spoofing techniques to deliver seemingly trustworthy correspondence, intended to fool recipients with various degrees of cybersecurity expertise.

For example, the surge in digital transactions and increased usage of online banking services birthed a wave of phishing campaigns impersonating popular financial institutions and banks from across the globe, including Bank of America, HSBC Bank, Standard Bank, Wells Fargo, New Zealand Banking Group Limited and National Australia Bank.

Between September and November 2020, Bitdefender Antispam Lab picked up three notable phishing campaigns highlighting fraudsters' skillfulness in attempting to mimic legitimate emails sent out by financial entities[21].

On September 20, 38 percent of all incoming correspondence relating to banks on that day, were marked as spam. The most significant phishing campaign was spotted on October 25, with nearly six in 10 bank-related emails (59 percent) marked as spam, on that day. On November 29, some 30 percent of all incoming email traffic appearing to be sent from well-known financial institutions was fraudulent.

Coronavirus-related spam is here to stay

Throughout the summer months, coronavirus-related spam remained a constant reminder of how malicious actors continue to exploit the ongoing pandemic.

No significant spikes in spam or malspam campaigns were noticed between July and August. Bitdefender telemetry did pick up two significant spikes in coronavirus spam, on October 25 and December 16, when 67 percent and 79 percent of all received coronavirus-related emails, respectively,were marked as spam.

The most recent coronavirus-fueled mass mailing campaigns were most likely the work of botnets springing back to life at the hands of their operators exploiting COVID-19 vaccine efforts.

[21] "Spammers get better at Impersonating banking services, use lingo and legit layouts to con victims," Bitdefender, https://hotforsecurity.bitdefender.com/blog/spammers-get-better-at-impersonating-banking-services-use-lingo-and-legit-layouts-to-con-victims-24805.html

Last year, the coronavirus also made its debut in lottery and advance-fee scams. Bogus lottery winnings are probably one of the oldest tactics scammers use. Although sweepstakes scams may not seem very practical in 2020, scammers piggybacked on the COVID-19 crisis to push mass-market spam campaigns[22] impersonating popular brands and existing lottery names.

Presidential election phishing

Weeks ahead of the US presidential election, spam groups targeted citizens with voter registration-related schemes to trick them into accessing spoofed government websites to input their personal information.

Multiple spam campaigns targeting voters were noticed starting in mid-October. The peak in election spam was on November 8, when 73 percent of all presidential election email traffic received on that day was marked as spam. On November 13, related spam traffic dropped down to 57 percent of all spam on that day, with a second major uptick on November 22 of 70 percent of all spam reported on that specific date.

Pay me, or else

Extortionists also took advantage of the increased number of remote workers and social distancing measures to build up their repertoire of threatening correspondence.

As internet users adapted to new work environments, cybercriminals have, too, by strengthening their creative side. Increased use of video-conference platforms such as Zoom was a stepping-stone to successful extortion campaigns.

If in the first months of 2020, blackmailers would bully email recipients into making Bitcoin transactions to avoid getting family members infected with COVID-19[23], cybercriminals quickly adapted their methods during the second half of the year.

On October 20, Bitdefender Antispam Lab picked up a fresh take on cyber-extortion campaigns targeting US users. A quarter-million inboxes were hit by scammers claiming to have recorded sensitive material through a security vulnerability on Zoom[24].

A substantial extortion campaign was also observed before Christmas. On December 21, 57 percent of all incoming spam traffic on that day was flagged as an extortion attempt.

[22] "Feeling Lucky This Holiday Season? COVID-19, Google and Microsoft 'Lotteries' are Out for Your Info and Money," Bitdefender, https://hotforsecurity.bitdefender.com/blog/feeling-lucky-this-holiday-season-covid-19-google-and-microsoft-lotteries-are-out-for-your-info-and-money-24915.html

[23] "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

[24] "COVID-19, Zoom and Bedroom Lewdness Make for Sly (S)extortion Tactic," Bitdefender, https://hotforsecurity.bitdefender.com/blog/covid-19-zoom-and-bedroom-lewdness-make-for-sly-sextortion-tactic-24436.html

Final Thoughts

To say that 2020 was a peculiar year in terms of threats is a massive understatement. From coronavirus-themed threats that stretched from phishing to Android threats, and spam emails that have become increasingly more sophisticated and legitimate-looking, 2020 acted as a catalyst for cybercriminals in terms of quickly adapting to popular topics and increasing the success rate of their campaigns.

Any tactics or malware that proved successful for cybercriminals in 2020 will likely spill over into 2021, potentially becoming the new standard. In light of this, everyone is strongly encouraged to always use a security solution, regardless of what device they use, to constantly use strong and unique passwords for their accounts and devices, update applications and operating systems with the latest patches, and always be vigilant when reading any information online.

This page is intentionally left blank

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.

About Bitdefender

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, business, and government environments, Bitdefender is the industry's trusted expert* for eliminating threats, protecting privacy and data, and enabling cyber resiliency. With deep investments in research and development, Bitdefender Labs discovers 400 new threats each minute and validates 30 billion threat queries daily. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioral analytics, and artificial intelligence and its technology is licensed by more than 150 of the world's most recognized technology brands. Founded in 2001, Bitdefender has customers in 170 countries with offices around the world. For more information, visit https://www.bitdefender.com.

*Bitdefender has ranked #1 in 54% of all tests by AV-Comparatives 2018-2021 for real-world protection, performance, malware protection & advanced threat protection.

RECOGNIZED BY LEADING ANALYSTS AND INDEPENDENT TESTING ORGANIZATIONS

CRN AV-TEST AV Gartner 451 Research FORRESTER IDC GLOBAL

TECHNOLOGY ALLIANCES

Microsoft NUTANIX aws Pivotal Cloud Foundry CITRIX

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-2020-creat5258-en_EN
03/12/21March 25, 2021 4:30 pm03/25/21