Malwarebytes

2021

State of Malware

REPORT

Contents

1 | Executive summary 3

2 | How COVID-19 changed the threat landscape: The four goals of cybercrime during the pandemic 7

- Exploit fear 8
- Gather intel 9
- Upgrade 10
- Attack 11

3 | Windows threat landscape 2020 12

- Categories 13
- Threat families 16
- Breakdown 19
- Upgrades: A deeper analysis of ransomware 22
- Malware snapshots 23
- Spotlight: Egregor ransomware 25
- Windows threat landscape 2020 summary 28

4 | Malware as a business 29

- Victim vetting mechanisms 31

5 | Mac threat landscape 2020 33

- ThiefQuest 37
- PUP removal on macOS 38
- Adware activity 39
- Nation-state and other targeted malware 40

6 | Android threat landscape 2020 41

- Fake ad blocker 41
- Back again: HiddenAds 42
- Bankbot becomes popular 43
- Pre-installed malware only gets worse 43
- Malware gets nastier 44
- Adware 44
- Android threat summary 45

7 | Data privacy in 2020 46

- Stalkerware-type app use spikes 47
- A digital approach to coronavirus 49
- Small legislative gains 51

8 | Regional breakdown of threats in 2020 53

- North America 54
- EMEA 54
- LATAM 55
- APAC 55

9 | Industry threat landscape 2020 58

- Malware in the dentistry sector 61
- Malware in the grocery/supermarket sector 62
- Web skimmers 63

10 | Conclusion 64

1 | Executive summary

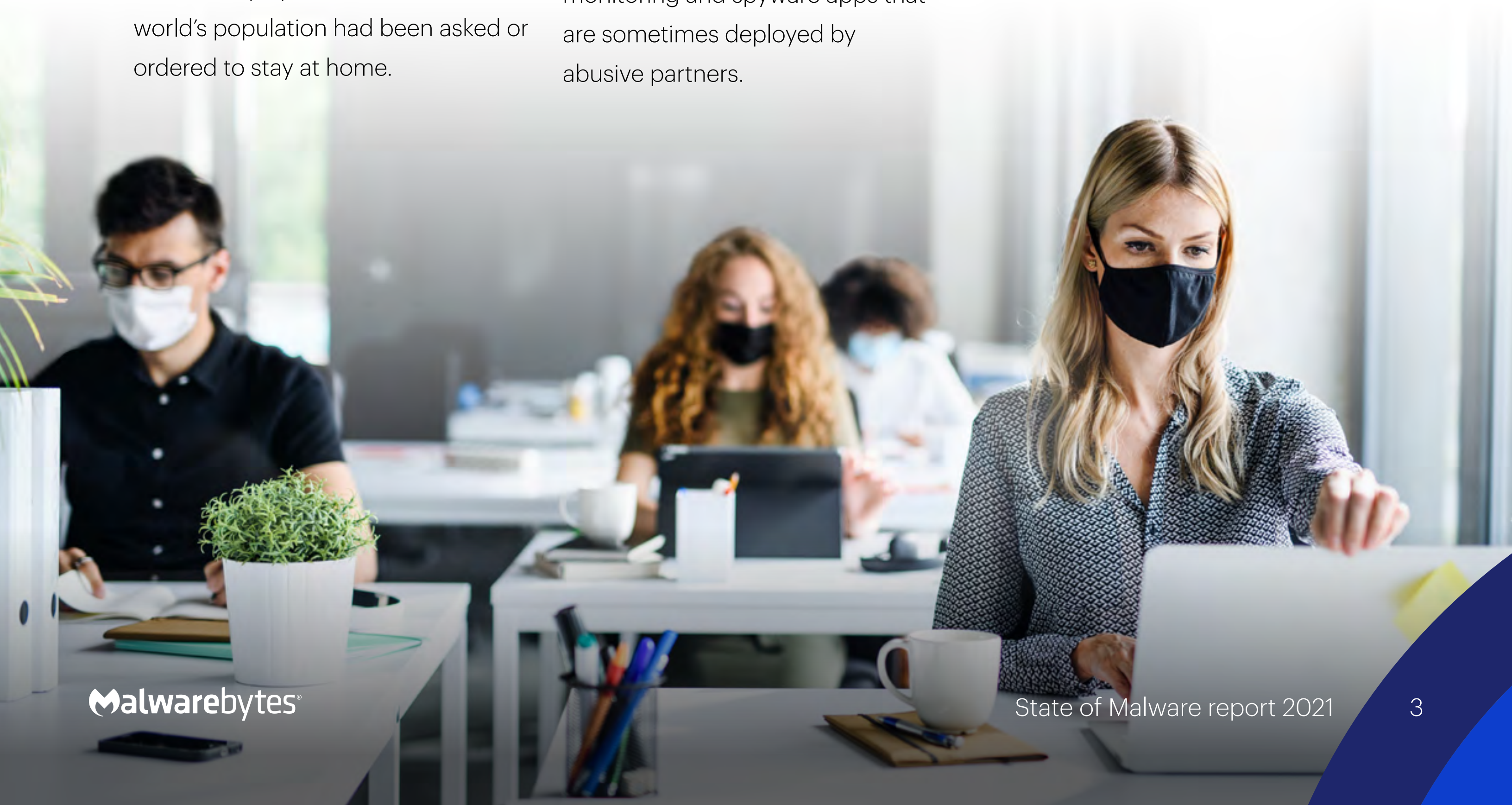
The story of 2020 is of the devastating COVID-19 pandemic, and of how the world adapted. The story of malware in 2020 then, is a story of how the tools and tactics of cybercrime and cybersecurity changed against a backdrop of enormous changes to ordinary life.

The novel coronavirus outbreak that began in the city of Wuhan in China was declared a global pandemic on March 12, 2020. Any thoughts that cybercriminals might be above exploiting the catastrophe were quickly disabused. Instead, they adapted and doubled down. As the world watched in alarm at the outbreak spreading, criminals preyed upon people's fears mercilessly, with an avalanche of coronavirus phishing emails and scams.

Around the world, governments tried to stop their hospitals from being overwhelmed by ordering lockdowns, stay-in-place orders, and school closures. By April 2020, half the world's population had been asked or ordered to stay at home.

As entire businesses switched to remote working, IT teams found themselves trying to fit months-long projects into days, with security an unfortunate but understandable casualty. Faced with a new landscape, cybercriminals ditched some old tactics and placed a new emphasis on gathering intelligence. And as people adapted to their "new normal," scammers exploited their isolation with a resurgence in tech support scams. New adversaries crawled out of the woodwork, too. April's global shutdown was accompanied by a staggering rise in the use of stalkerware, a short-hand term for the type of mobile monitoring and spyware apps that are sometimes deployed by abusive partners.

As entire businesses switched to remote working, IT teams found themselves trying to fit months-long projects into days, with security an unfortunate but understandable casualty.



The pandemic also created new challenges to online privacy. As countries turned to digital contact tracing to contain outbreaks, a stark dichotomy emerged: It is possible for people to have personal privacy or effective contact tracing, but probably not both. Around the world, the progress of privacy-preserving legislation slowed to a crawl.

What began as a global health crisis soon became a global economic crisis too, with almost no business left unscathed.

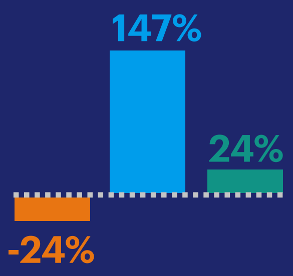
And what began as a global health crisis soon became a global economic crisis too, with almost no business left unscathed. The fate of different industry sectors was mirrored in the number of cyberattacks they suffered. As the manufacturing and automotive sectors contracted, attackers simply turned their faces to agriculture and other essential industries instead. Ransomware gangs reneged on early promises to stay away from hospitals and hit new lows, attacking hospitals and medical facilities in organized campaigns.

Through it all, there is one form of business that seems to have thrived in 2020 though—the creation and operation of malicious software. The pace of innovation picked up in 2020 as many entirely new malware families emerged. Ransomware gangs continued to learn from each other too, with successful tactics spreading quickly between them. Perhaps the most important new tactic that emerged was "double extortion," which saw cybercriminal groups extorting more money with threats to leak sensitive data than from decrypting compromised computers.

If 2020 taught us anything, it's that cybercrime stops for nothing. There are no targets, and no opportunities for exploitation, that are beyond the pale.

Thankfully, the year had another lesson for us too: That there are heroes everywhere. The healthcare professionals, teachers and other essential workers rightly deserve the loudest acclaim, but heroes emerged in all areas of life. So we want to finish with a thank you to the unsung army of sysadmins and security professionals who moved mountains in 2020 to keep millions of people safe online as the world around them was turned on its head.

Here are key takeaways of what we learned in 2020

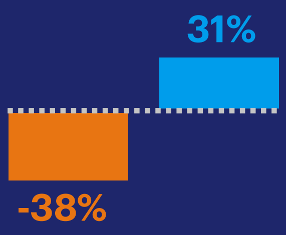


Malware detections on Windows business computers decreased by **24%** overall, but detections for HackTools and Spyware on Windows increased dramatically—by **147%** and **24%**, respectively

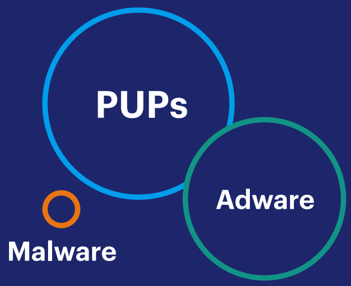
Among the top five threats for both businesses and consumers were the Microsoft Office software cracker KMS, the banking malware Dridex, and BitCoinMiners; business detections for KMS and Dridex rose by **2,251%** and **973%**, respectively

Detections for the most notorious business threats Emotet and Trickbot fell this year by **89%** and **68%** respectively, although the operators behind these threats still pulled off several big attacks in 2020

A new ransomware called **Egregor** came onto the scene in late 2020, deployed in attacks against Ubisoft, K-Mart, Crytek, and Barnes & Noble



Overall Mac detections decreased by **38%**, though Mac detections for businesses increased **31%**

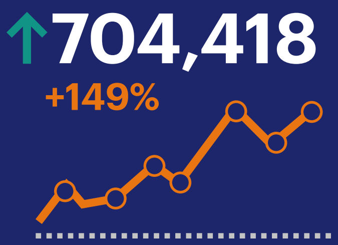


Malware accounted for just **1.5%** of all Mac detections in 2020—the rest can be attributed to Potentially Unwanted Programs (PUPs) and Adware

Here are key takeaways of what we learned in 2020 (cont.)

20K+
Detections

ThiefQuest tricked many researchers into believing it was the first example of ransomware on macOS since 2017, but the malware was hiding its real activity of massive data exfiltration. It accounted for more than **20,000 detections** in 2020



On Android, HiddenAds—which aggressively pushes ads to users—racked up **704,418 detections**, an increase of nearly **149%**

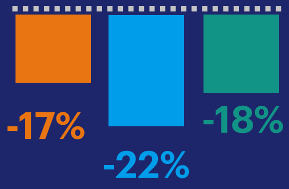
We **twice** uncovered pre-installed malware on phones provided by Assurance Wireless through the US government-funded Lifeline Assistance program

Stalkerware-type app detections—which include detections for Monitor apps and Spyware apps on Android—surged in conjunction with shelter-in-place orders that governments began implementing in February and March: Monitor app detections rose from January to December by **565%**; Spyware app detections rose across the same time period by **1,055%**

↑607%

↑67%

The agriculture industry suffered through a **607%** increase in malware detections, while malware detections in the food and beverage industry increased by **67%**



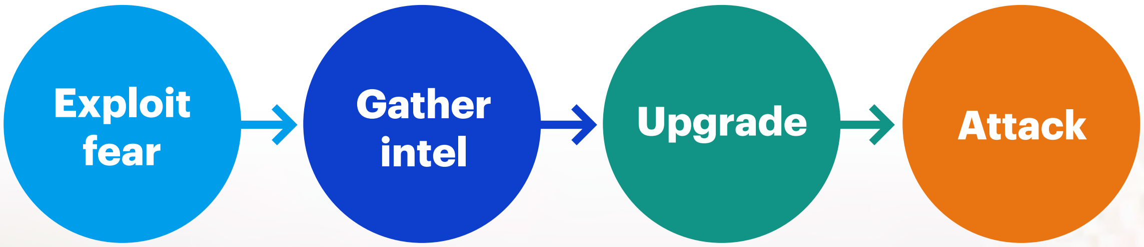
More traditional targets, such as manufacturing, healthcare and medical, and automotive all experienced drops in detections by varying degrees—education fell **17%**, healthcare dropped **22%**, and the automotive industry decreased by **18%**

2 | How COVID-19 changed the threat landscape: The four goals of cybercrime during the pandemic

By observing trends in detections, attacks, and reporting throughout 2020, we identified four primary goals of cybercriminals during the year, and specifically, during the pandemic.

These goals often overlap and are not unique to this situation; however, we do not believe cybercriminals have ever enjoyed as much freedom to accomplish their wants, because in 2020, COVID-19 split the world—cybercriminals pounced, and the rest of the world scrambled.

Briefly, the four cybercrime goals that we found in 2020 were to:



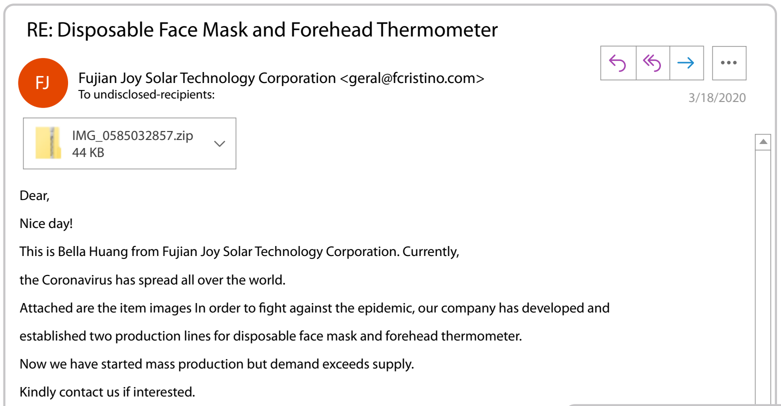
Exploit fear → Gather intel → Upgrade → Attack

Let's look at how these goals played out.

Exploit fear

The first goal involves utilizing fear, confusion, or any high emotion to get potential victims to click on links or open attachments. We've repeatedly seen this with past tragedies or world events, from the Boston bombing of 2013 to the 2016 US Presidential election. 2020 was no different, and COVID-19 made a nice hook for cybercriminals. We saw malicious phishing campaigns that fraudulently posed as health advisories, PPE order forms, and donation requests from charities, including UNICEF.

We saw malicious phishing campaigns that fraudulently posed as health advisories, PPE order forms, and donation requests from charities, including UNICEF.



RE: Disposable Face Mask and Forehead Thermometer

FJ Fujian Joy Solar Technology Corporation <geral@fcristino.com>
To undisclosed-recipients:

3/18/2020

IMG_0585032857.zip
44 KB

Dear,

Nice day!

This is Bella Huang from Fujian Joy Solar Technology Corporation. Currently, the Coronavirus has spread all over the world.

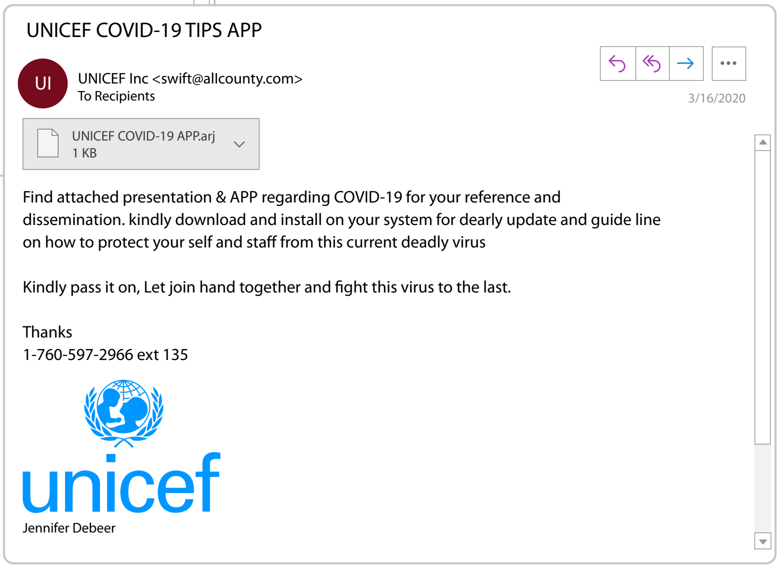
Attached are the item images In order to fight against the epidemic, our company has developed and established two production lines for disposable face mask and forehead thermometer.

Now we have started mass production but demand exceeds supply.

Kindly contact us if interested.

Thanks and best regards,
FRADAH MOHAMED
Customer Service
1-888-3M HELPS (1-888-364-3577)

A COVID-19 themed phishing email that Malwarebytes encountered last year



UNICEF COVID-19 TIPS APP

UI UNICEF Inc <swift@allcounty.com>
To Recipients

3/16/2020

UNICEF COVID-19 APP.arj
1 KB

Find attached presentation & APP regarding COVID-19 for your reference and dissemination. kindly download and install on your system for dearly update and guide line on how to protect your self and staff from this current deadly virus

Kindly pass it on, Let join hand together and fight this virus to the last.

Thanks
1-760-597-2966 ext 135

unicef
Jennifer Debeer

A COIVD-19 themed phishing email impersonating the children's charity organization, UNICEF

In our *Cybercrime tactics and techniques report for Q1 2020*, we analyzed some of these malicious email campaigns spreading malware including AveMaria, a popular Remote Access Trojan, and AZORult, a dangerous information-stealing malware.

Commercial criminals were not the only ones using this tactic. We also observed numerous state-sponsored Advanced Persistent Threat (APT) groups using COVID-19 themed spear phishing emails. Perhaps the goal of these attacks was to not only copy what commercial criminals were doing, but to also mask their intent or origin from researchers.

Gather intel

In tandem with exploiting fear, cybercriminals sought to gather intelligence about targets. That meant deploying various information-gathering tools through malicious phishing attacks. During this time, threat actors leaned heavily on information stealers, Spyware, and tools that collected information about victims' systems.

That intelligence gathering allowed cybercriminals to obtain a better understanding of the tools, types of access, and resources that employees relied on, especially after the shift to working from home (WFH).

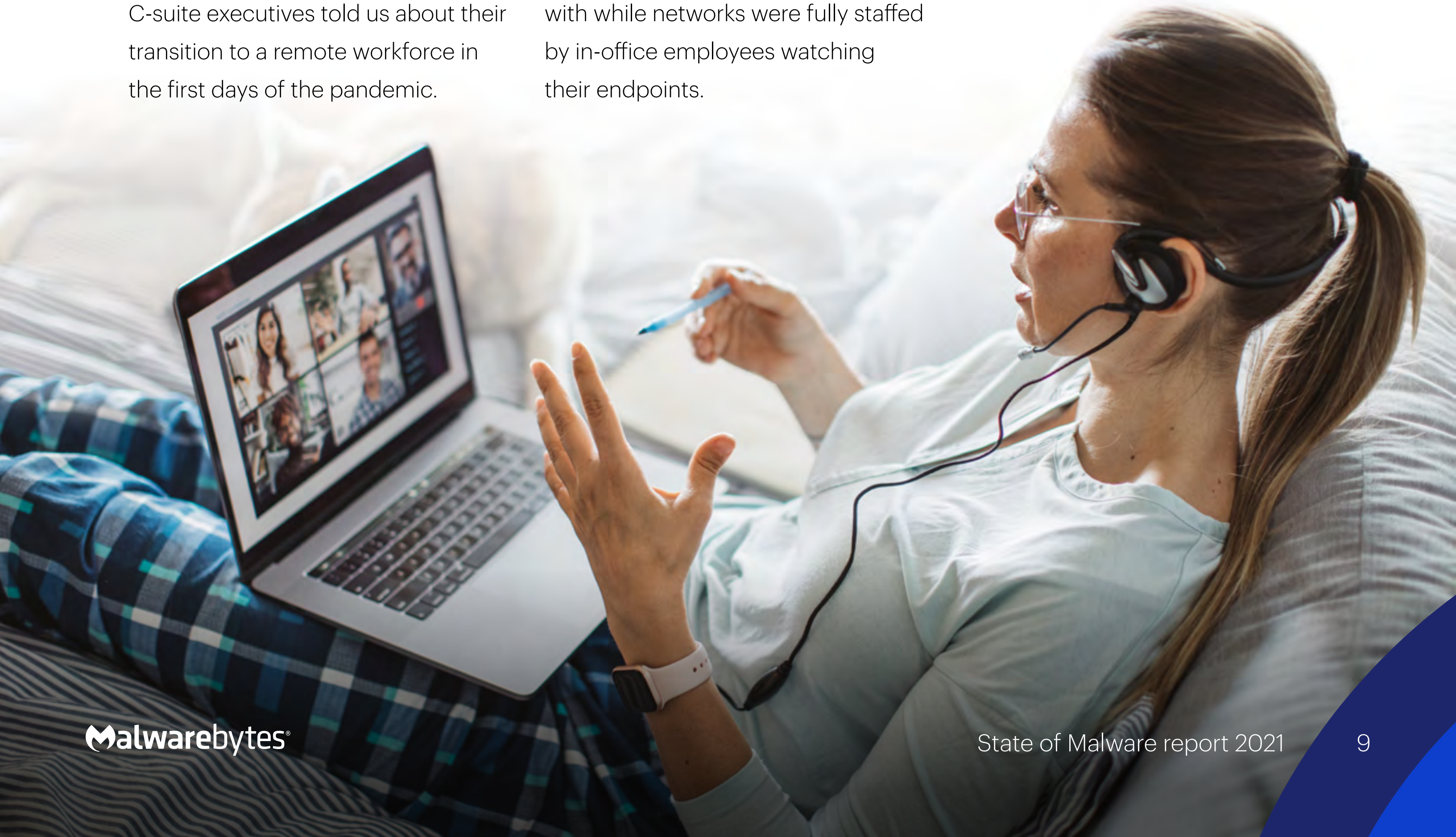
In our report, *Enduring from home: COVID-19's impact on business security*, more than 200 information technology managers, directors and C-suite executives told us about their transition to a remote workforce in the first days of the pandemic.

Their responses showed promise, but something stood out: An immense amount of "security hubris," or an overabundance of trust in an existing or singular security control. For example, not bothering to deploy email security when you have already invested in expensive border security tools.

Information gathering isn't an effort specific to 2020, but it seemed critical in the first few months of the pandemic. In April, Google reported it was blocking 18 million spam emails related to COVID-19 per day!

With reams of better intelligence now in hand, threat actors found new freedom in how they could attack corporate networks. They developed new features which may have been difficult or impossible to experiment with while networks were fully staffed by in-office employees watching their endpoints.

Intelligence gathering allowed cybercriminals to obtain a better understanding of the tools, types of access, and resources that employees relied on, especially after the shift to working from home (WFH).



Upgrade

Every year, malicious tools get updated and upgraded, especially if the groups behind them find success in the cybercrime markets and have extra cash to reinvest in their tools. However, most of these upgrades are small increases in malware capabilities. Rarely do they surprise.

In 2020, that changed, as we saw a waterfall of updates from some of the biggest malware names in the wild today.

Emotet, the popular first-stage infection and malware delivery botnet, started stealing existing email threads from victims. Trickbot, a frequent travel partner with Emotet, launched new upgrades to not only the primary bot malware, but the framework which helps to distribute this threat, too. For example, a new exploit meant to quickly compromise domain controller servers on a corporate network, known as ZeroLogon, was added into Trickbot's functionality. As Trickbot frequently is in charge of spreading laterally to every endpoint, this makes its job much easier.

The upgrades we saw last year also influenced attack methods. In fact, 2020 saw a significant increase in brute force attacks against Remote Desktop Protocol (RDP) clients. Many of the major breaches in 2020 were due to cybercriminals attacking vulnerable systems manually, rather than with automated malware infections, after gaining entry via RDP.

In addition, by mid-year we saw malicious phishing email themes change away from COVID-19 messaging to messaging about the tools found through the information gathering phase. This means that not only did malware get updated, but so did the tactics behind nabbing potential victims. For example, we saw an increase in malicious spam posing as information regarding Zoom, Microsoft Teams, Slack, and other applications that employees began using more frequently.

We saw an increase in malicious spam posing as information regarding Zoom, Microsoft Teams, Slack, and other applications that employees began using more frequently.

Attack

The final goal is likely the goal for every cybercriminal, all the time: Attack.

In 2020, it took on new meaning.

The increase in brute force attacks, combined with the deployment of customized intrusion tools, new exploits, and the use of sometimes commercial tools... allowed attackers to map out and infect networks faster than we have ever seen.

The increase in brute force attacks, combined with the deployment of customized intrusion tools, new exploits, and the use of sometimes commercial tools that are meant for penetration testing or identifying vulnerabilities in a network, allowed attackers to map out and infect networks faster than we have ever seen.

These attacks against businesses—despite new techniques for infection—shared the same goal as most business-focused attacks in 2019, which was to launch network-wide ransomware infections.

But unlike in 2019, we dealt with a far more diverse cast of characters in ransomware. Many threat actors removed their kid gloves and jabbed organizations harder than ever, followed with a right hook of extortion.

Some ransomware families, like Maze, shut down, only for affiliates using them to pick up new ransomware families to distribute, like Egregor. These families also posted victim information online, either to show proof of infection, strong-arm the victim into paying, or hurt the victim's reputation by advertising their breach.

In fact, in 2020, attackers made more money by demanding payment for not posting stolen data than they did from victims who paid the ransom just to decrypt their files! This was true for the ransomware family REvil, or Sodinokibi, who claimed to net $100 million in the last year, much of which came from extortion threats.

Further, companies including Garmin were hit by WastedLocker, the latest ransomware family launched by Evil Corp, which is the same group that created the Dridex banking Trojan. The breach was so significant that it took down GPS and cloud data services for the company's clients, which may indicate that the future of ransomware attacks is operational disruption.

Sadly, despite the public health crisis caused by the pandemic, criminals did not take it easy on the healthcare industry. Instead, we saw a massive campaign by Emotet to focus on healthcare organization compromise, and 250 hospitals attached to the Universal Health Services chain in the US were hit with Ryuk ransomware infections.

As for the cybercrime goals to watch in 2021, expect much of the same. As employees hopefully return to the office and try to find normalcy, attackers will shift their tactics once again in order improve their effectiveness against our defenses and weaknesses.

But those predictions will have to wait until next year to be proven or disproven.

3 | Windows threat landscape 2020

Last year saw a surprising drop in malware detections overall. The COVID-19 pandemic influenced the cybercrime world so much that many campaigns we expected to see either never arrived, arrived with less impact, or were replaced entirely with attacks designed to exploit the pandemic.

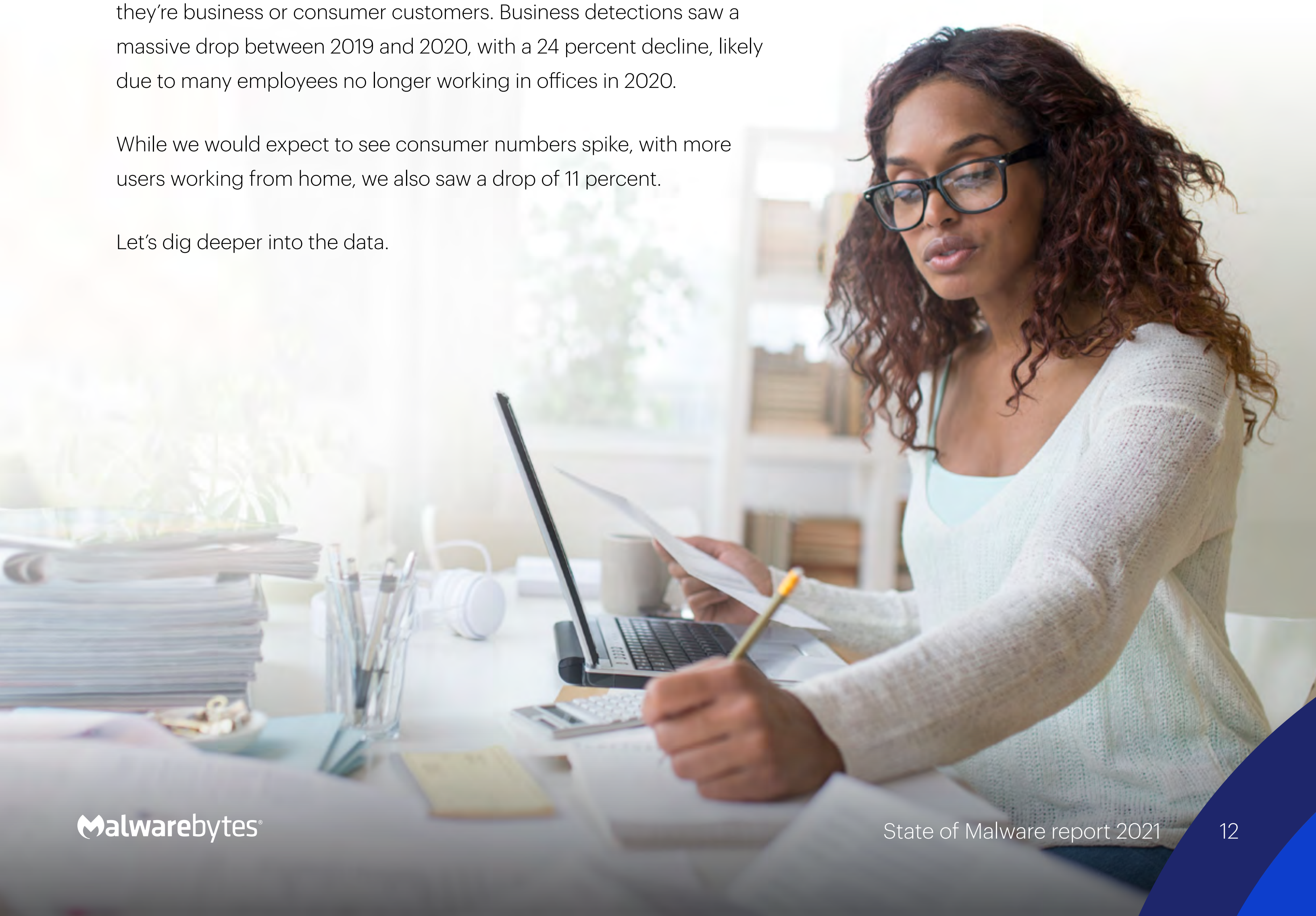
Total Windows malware detections 2020 compared to 2019

	2019	2020	% Change
Business	22,009,793	16,709,936	-24%
Consumer	103,504,287	92,294,406	-11%
Total	**125,522,505**	**111,014,261**	**-12%**

Overall, we saw a decline of 12 percent in detections across the board. That's every operating system and every region, regardless of whether they're business or consumer customers. Business detections saw a massive drop between 2019 and 2020, with a 24 percent decline, likely due to many employees no longer working in offices in 2020.

While we would expect to see consumer numbers spike, with more users working from home, we also saw a drop of 11 percent.

Let's dig deeper into the data.



Categories

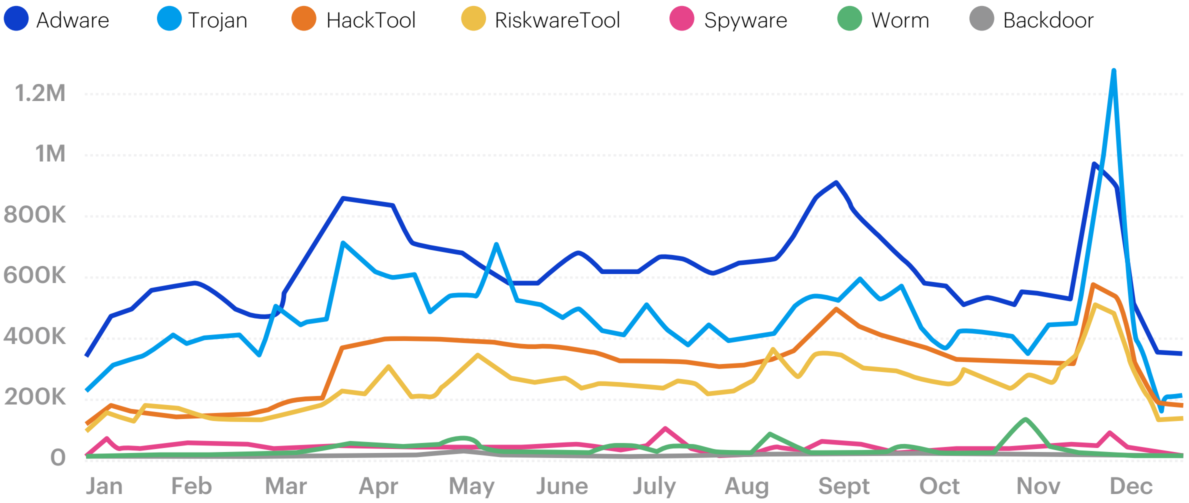
We begin our analysis by looking at overall malware category detections between 2019 and 2020. While no attacker group is limited to the type of malware they choose to use, certain categories represent certain cohorts, for example Adware, while other category changes might represent a shift in attacker trends.

Top 10 consumer malware categories 2020 compared to 2019

	Threats	2019	2020	% Change
1	Adware	41,151,954	31,502,039	-23%
2	Trojan	27,391,382	23,729,868	-13%
3	HackTool	6,437,673	15,882,958	147%
4	RiskwareTool	14,180,159	12,346,354	-13%
5	Spyware	1,960,652	2,434,723	24%
6	Worm	2,284,877	2,075,855	-9%
7	Backdoor	3,614,672	1,819,980	-50%
8	Rogue	501,146	1,050,713	110%
9	CrackTool	1,247,364	843,811	-32%
10	Virus	766,925	581,829	-24%

The usual suspects, like Adware, Trojans, and RiskwareTools (like cryptocurrency miners) experienced a significant decline from the previous year. However, we saw huge spikes in HackTools, Spyware, and other software meant to compromise security and/or collect information on the victim—which represents the second cybercrime goal of 2020.

Top 10 malware category detections for consumers 2020



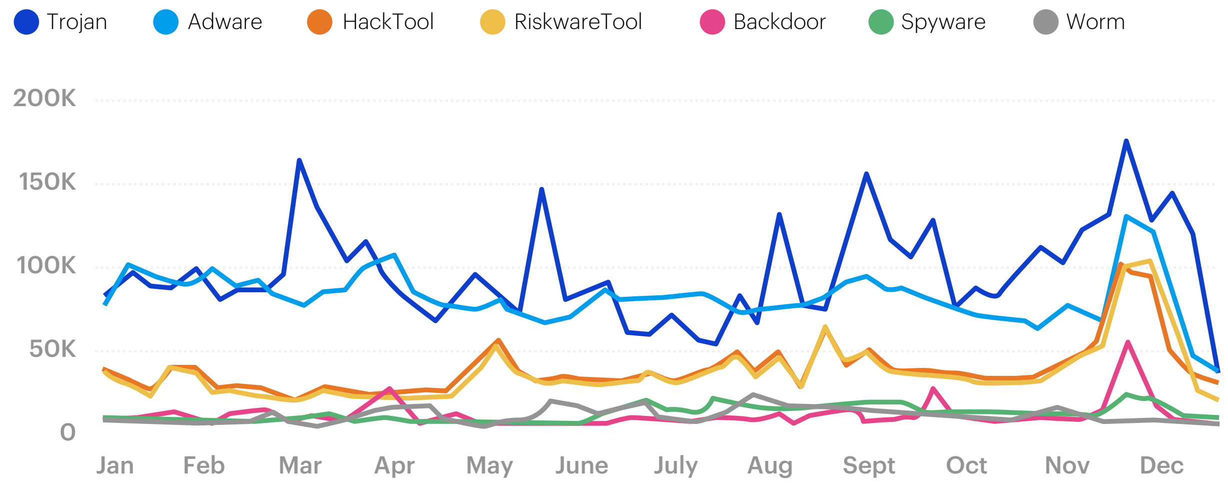
When we looked at these detection changes over time, we saw that Trojans and Adware still dominated. But in April, we began to see a spike in HackTool detections. This "shelf" also showed up in our business detections and, in our opinion, represents the beginning of cybercriminal efforts to brute force unattended corporate networks.

Top 10 business malware categories 2020 compared to 2019

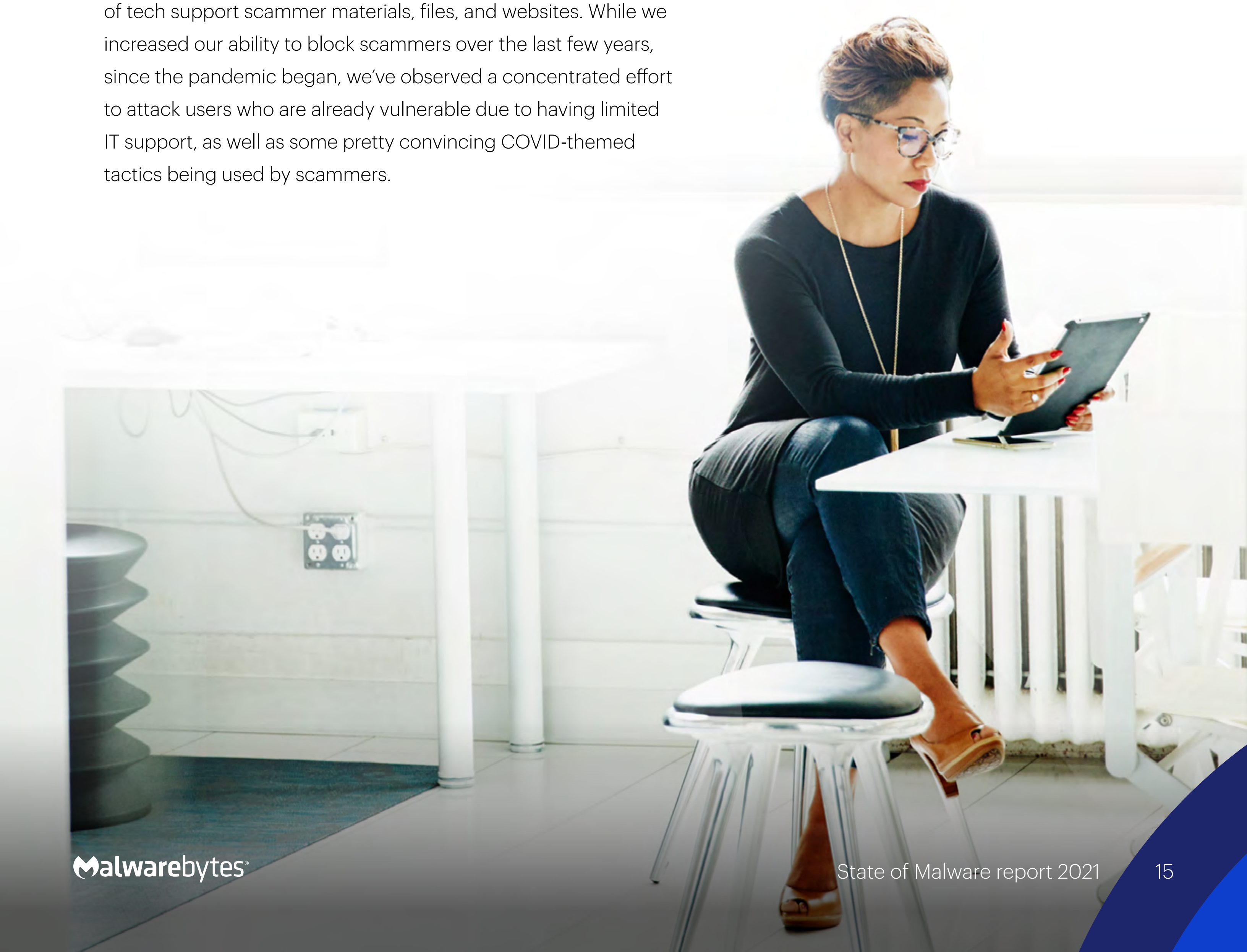
	Threats	2019	2020	% Change
1	Trojan	11,140,084	6,135,219	-45%
2	Adware	4,586,057	3,997,158	-13%
3	HackTool	937,941	2,562,196	173%
4	RiskwareTool	1,715,806	1,763,072	3%
5	Backdoor	1,235,067	490,201	-60%
6	Spyware	291,525	440,368	51%
7	Worm	414,349	391,854	-5%
8	Rogue	94,210	243,208	158%
9	Ransom	704,991	199,838	-72%
10	Hijacker	248,877	167,252	-33%

Looking at business detections we see a similar story, with Trojans, Adware, and even ransomware dropping between 2019 and 2020. HackTools surged in detections against businesses as well, which is represented by the increase in use of commercially developed and offered "hacking tools" to launch attacks or compromise systems.

Top 10 malware category detections for businesses 2020



In addition, Rogue malware also spiked, specifically our detections of tech support scammer materials, files, and websites. While we increased our ability to block scammers over the last few years, since the pandemic began, we've observed a concentrated effort to attack users who are already vulnerable due to having limited IT support, as well as some pretty convincing COVID-themed tactics being used by scammers.



Threat families

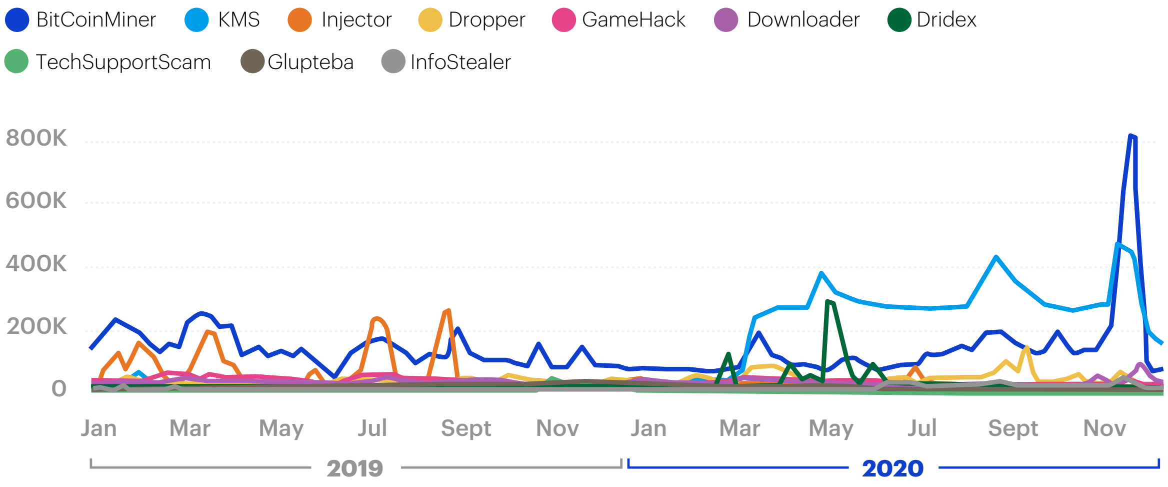
Going deeper, let's look at the specific threat families that were most prominent in 2020 and how that changed from 2019.

Top 10 consumer threats 2020 compared to 2019

	Threat	2019	2020	% Change
1	KMS	511,848	11,350,985	2,118%
2	BitCoinMiner	6,897,365	5,876,303	-15%
3	Dropper	1,192,150	1,919,851	61%
4	Dridex	54,697	1,088,427	1,890%
5	Downloader	999,838	932,564	-7%
6	GameHack	1,467,240	907,455	-38%
7	Tech-SupportScam	210,236	866,561	312%
8	Glupteba	406	840,754	206,982%
9	Injector	2,487,127	820,887	-67%
10	InfoStealer	50,941	759,754	1,391%

Our top detection of the year, almost across the board, was HackTool.KMS, which we will break down later.

Top 10 consumer threats 2019 and 2020



For consumer-focused threats, our next top detection was BitCoinMiner, which is no surprise given that the value of Bitcoin in 2020 shot higher than ever. There was also a campaign pushing the Dridex banking malware in March, May, and into the new year, with detections increasing in December, which was greater than what we saw from other, similar families.

The backdoor Trojan Glupteba was only discovered in late 2019, but it had constant distribution for nearly all of 2020. This malware is commonly distributed through exploit kits and joins the victims' system to a botnet. The capabilities of the Glupteba botnet range from cryptojacking and browser data theft, to attacking routers and utilizing the ETERNALBLUE exploit to distribute itself through an infected network.

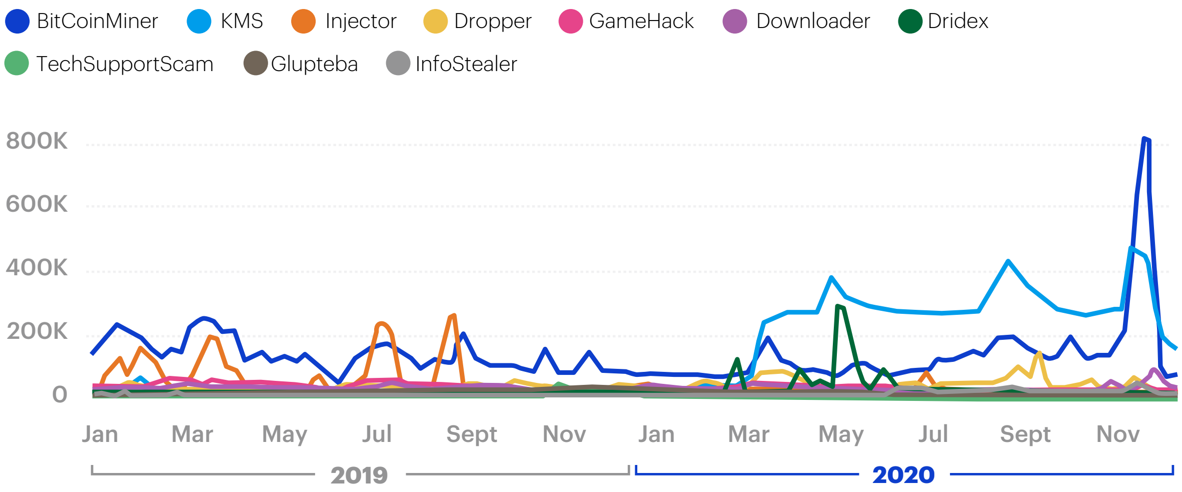
Moving on to notable business detection trends, we saw BitCoinMiner, KMS, and Dridex rank high, but we also saw a huge spike in information-stealing malware and the backdoor Farfli. This suggests, along with the rest of our data, that the disruption from COVID-19 affected both victims and attackers, as many popular forms of malware used in 2019 were benched in favor of either new malware families or re-investment in existing and older malware families.

Top 10 business malware threats 2020 compared to 2019

	Threats	2019	2020	% Change
1	BitCoinMiner	1,352,256	2,769,835	105%
2	KMS	81,356	1,912,628	2,251%
3	Dridex	37,899	406,575	973%
4	Tech-SupportScam	64,097	203,795	218%
5	Injector	4,254,292	187,283	-96%
6	InfoStealer	8,510	183,568	2,057%
7	Dropper	464,464	174,270	-62%
8	Farfli	24,368	162,281	566%
9	Trickbot	455,571	144,993	-68%
10	Emotet	1,235,801	132,326	-89%

Notorious families like Trickbot and Emotet made our Top 10 list this year, even though they both dropped in detections dramatically. This is not necessarily due to a lack of effort from the groups behind Trickbot and Emotet. In fact, this year both families developed new methods of infection, new platforms for malware distribution, and new functionality in an unprecedented season of evolution, followed by a hard push in the second half of the year.

Top 10 business threats 2019 and 2020



What explains the almost 90 percent drop in Emotet detections in 2020 versus 2019, then?

Primarily, we can blame the efforts of these groups in reducing their "waste." In this case, waste is created by using a "wide net" approach to infection, where many potential victims are targeted, usually through email phishing attacks. Most of these widespread attacks won't succeed, and many of them will also end up in the hands of security researchers who have honeypots set up to capture malicious email. The researchers can then quickly create new ways of detecting that malware, which makes it less effective against new victims. What we see with Emotet today is that the groups are pickier about who they target. This should result in a greater success rate, and, as an added bonus for the attacker, if the distribution attack fails, the malware could still be used against another victim without fear of detection.

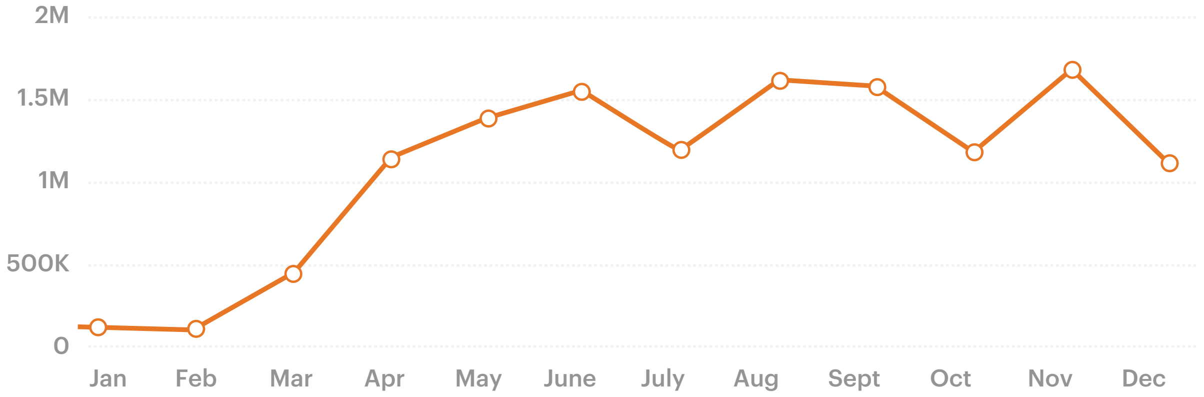
Breakdown

The numbers only tell us so much. Let's see what these attacks actually looked like, and how they sometimes contributed directly to threat actors' 2020 goals.

HackTool.KMS

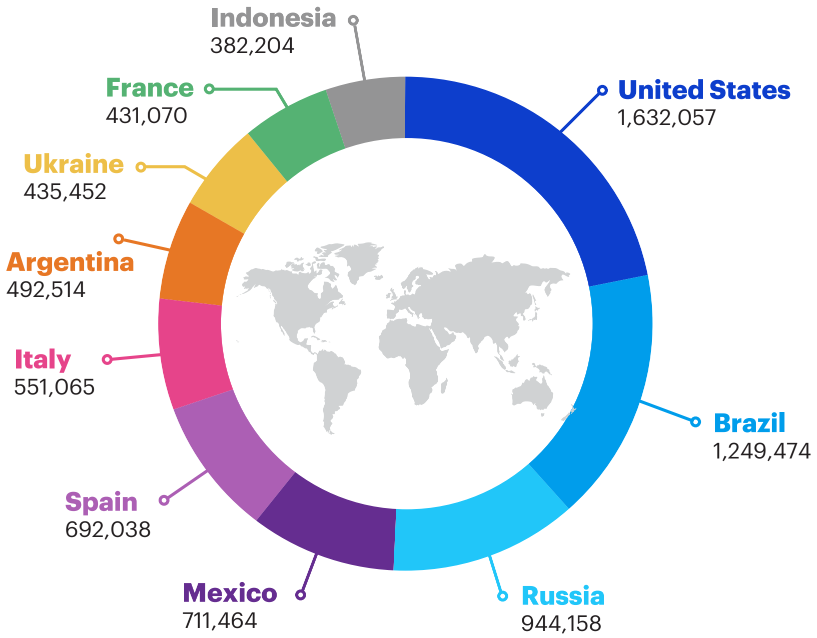
First, let's look at the surge of detections for HackTool.KMS. This detection hasn't been around for a long time, though it's been incredibly prominent in 2020. This detection is meant to identify software that allows users to utilize Microsoft software illegally. With so many users moving to WFH last year, many employees and maybe even employers started using cracked versions of Microsoft applications, like Windows or Microsoft Office.

HackTool.KMS detections 2020



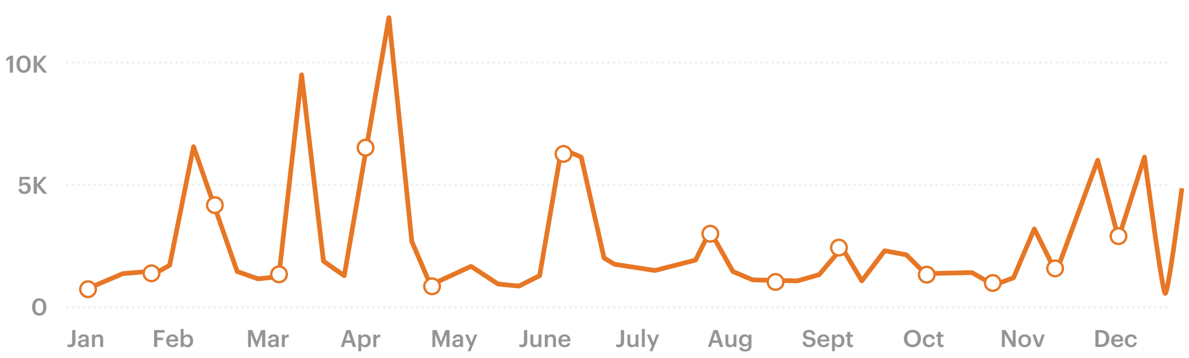
Some threats lean toward one particular country, like the United States, but in the case of HackTool.KMS, we see a somewhat even distribution of this detection across the globe, with the greatest number of detections coming from the US and Brazil, followed shortly by Russia.

HackTool.KMS detections by country

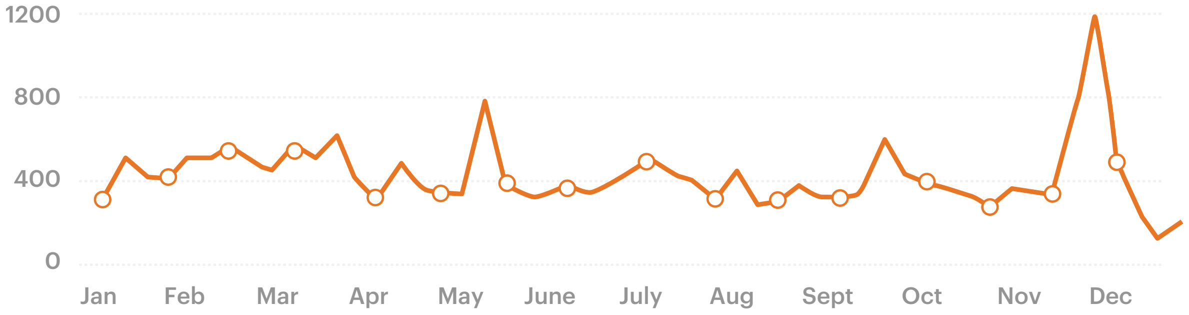


We also saw spikes in the use of NSA hacking tools first leaked in 2017 by the Shadowbrokers group. Two of the detections created from that event were active in 2020.

Trojan.ShadowBrokers detections 2020

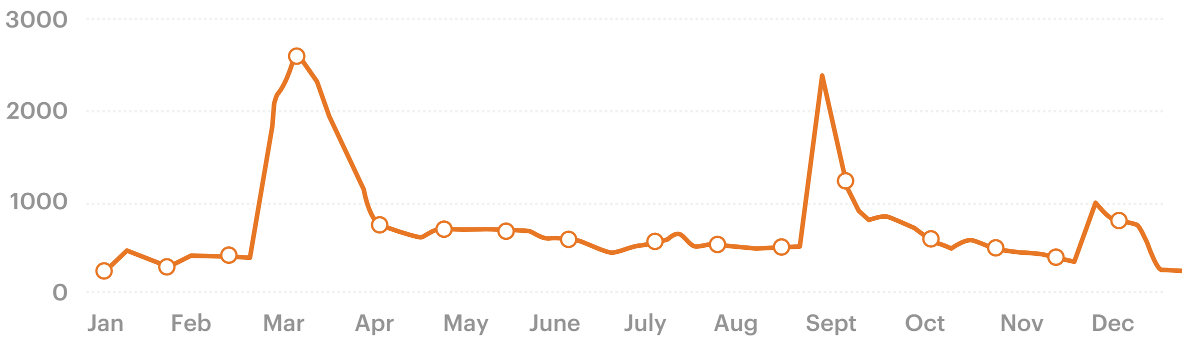


HackTool.Equation detections 2020

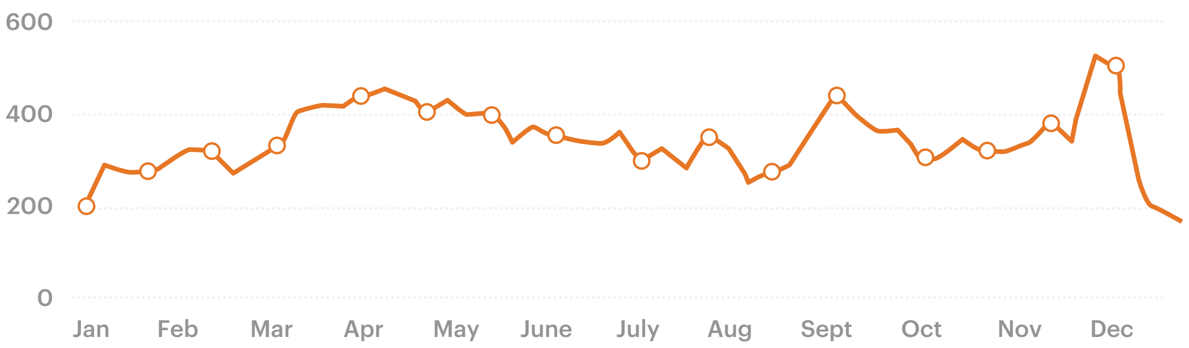


In addition to these tools, which are used to identify vulnerable systems and exploit them using sophisticated code, leading to further compromise, we also saw a spike in tools used to collect or crack passwords.

HackTool.MimiKatz detections 2020



HackTool.Cain detections 2020



MimiKatz is a popular penetration testing tool which allows passwords to be extracted from an infected system, exploiting a flaw in Windows password security. If you have studied hacking at any length, you will likely have heard of the Cain and Abel password cracker. Detections for tools like this have been rising through the pandemic due to the increase in manual attacks for the sake of gathering data that might be used for greater corporate access in the future.

Taken together, we see that last year, attackers increasingly relied on popular, sometimes commercial, penetration testing tools and suites to give them access into more secured corporate networks. These tools require human interaction and control, which also requires a greater focus on a target by a criminal, as opposed to a "spray and pray" approach to attacking victims.

Upgrades: a deeper analysis of ransomware

In addition to the upgrades of families like Emotet and Trickbot, we saw attackers pushing ransomware to give their tools more capability. Notable examples of this are the families of Maze, RagnarLocker, and RegretLocker ransomware.

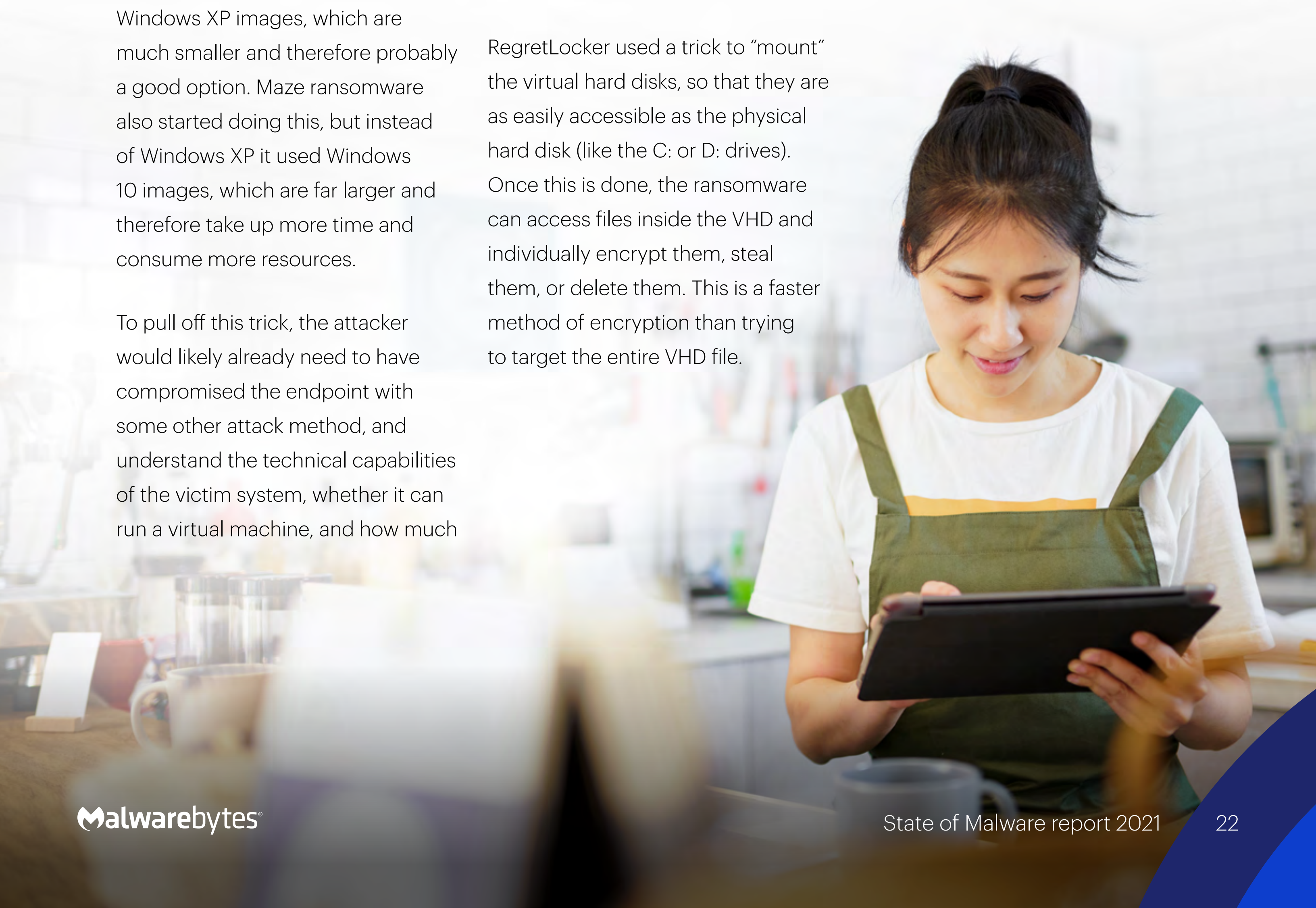
The RagnarLocker ransomware found a new way to encrypt files on an endpoint that might have some kind of ransomware protection on it. It does this by downloading a virtual machine image, loading it silently, and then using that virtual machine (VM) to launch the ransomware, accessing files on the host system through "shared folders." RagnarLocker did this with Windows XP images, which are much smaller and therefore probably a good option. Maze ransomware also started doing this, but instead of Windows XP it used Windows 10 images, which are far larger and therefore take up more time and consume more resources.

To pull off this trick, the attacker would likely already need to have compromised the endpoint with some other attack method, and understand the technical capabilities of the victim system, whether it can run a virtual machine, and how much negative noise that might make on the network.

Along the same lines, RegretLocker ransomware didn't try to run a virtual machine on the victim system, but rather wanted to speed up its ability to encrypt files found on a virtual hard drive file. These files are huge archives that hold the virtual hard disk (VHD) of a virtual machine. If an attacker wanted to encrypt the data inside a VHD, they would endure a painfully slow process because of how large these files are. This might be a common issue if targets include server farms or if the target organization stores their more sensitive data inside VHDs.

RegretLocker used a trick to "mount" the virtual hard disks, so that they are as easily accessible as the physical hard disk (like the C: or D: drives). Once this is done, the ransomware can access files inside the VHD and individually encrypt them, steal them, or delete them. This is a faster method of encryption than trying to target the entire VHD file.

The RagnarLocker ransomware found a new way to encrypt files on an endpoint that might have some kind of ransomware protection on it.



Malware snapshots

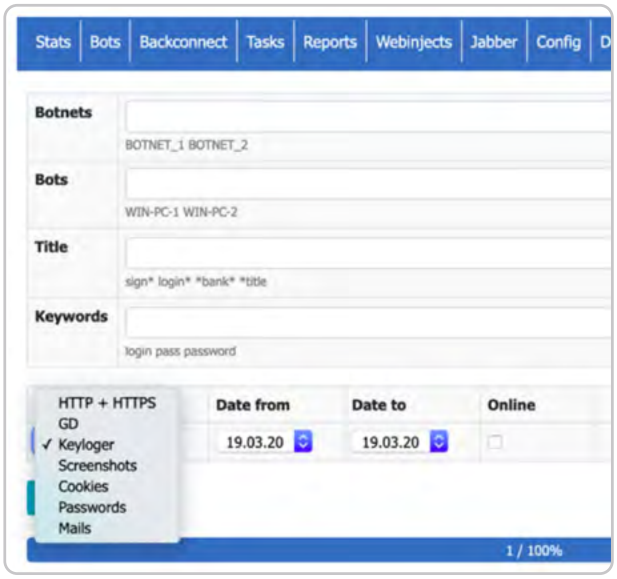
No analysis of 2020 would be complete without looking closely at some of the more nefarious malware that harmed businesses and consumers.

Let's look at last year's activity from Zloader, REvil, and Maze, while also shining a spotlight on something new: Egregor.

Zloader (Silent Night)

Last May, we published a comprehensive paper on a new Zloader variant, a bot reminiscent of the infamous ZeuS, likely the most well-known banking Trojan dating back to 2011. Underground, this malware was known as Silent Night and it was advertised by a threat actor with the username "Axe," who security experts believe developed the Axe Bot.

In comparison to other bots, Silent Night fetches a rather expensive price, at $4,000 a month for unique builds. It boasts a number of features typical of banking Trojans such as web injections, form grabbers, and keylogging.



Botnets	BOTNET_1 BOTNET_2
Bots	WIN-PC-1 WIN-PC-2
Title	sign* login* *bank* *title
Keywords	login pass password

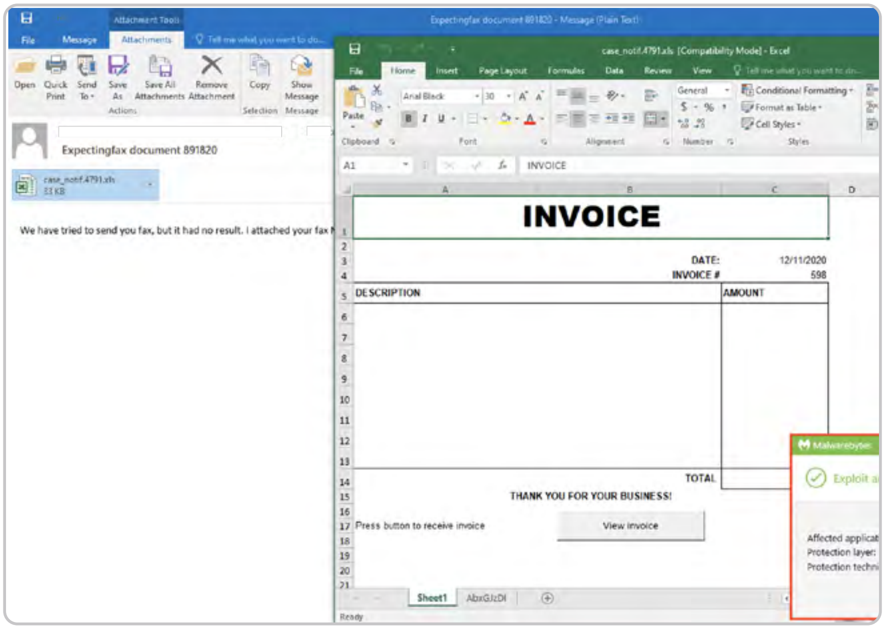
Date from	Date to	Online
19.03.20	19.03.20	□

A screenshot showing Silent Night's capabilities

Zloader was first seen being dropped by the RIG exploit kit but mostly transitioned to malspam as a primary distribution source.

Zloader acts as a downloader for several different modules. Some researchers have observed Zloader downloading specific utilities such as Cobalt Strike, which attackers can leverage to roam within a network before deploying ransomware like Ryuk. This type of collaboration with ransomware gangs mirrors what we have seen with Emotet and TrickBot.

The Zloader botnet will remain a threat to watch for in 2021, especially if it continues to be used as an initial foothold to deploy ransomware.



Expectingfax document 891820 - Message (Plain Text)

Expectingfax document 891820

case_notif.4791.xls
33 KB

We have tried to send you fax, but it had no result. I attached your fax f

INVOICE

DATE: 12/11/2020
INVOICE # 598

DESCRIPTION	AMOUNT
TOTAL	

THANK YOU FOR YOUR BUSINESS!

Press button to receive invoice — View invoice

A fraudulent invoice that attempted to deliver Silent Night

Maze ransomware

Initially discovered by Malwarebytes in May 2019, Maze is a family of ransomware (previously referred to as "ChaCha") often distributed via exploit kits or malicious email document attachments.

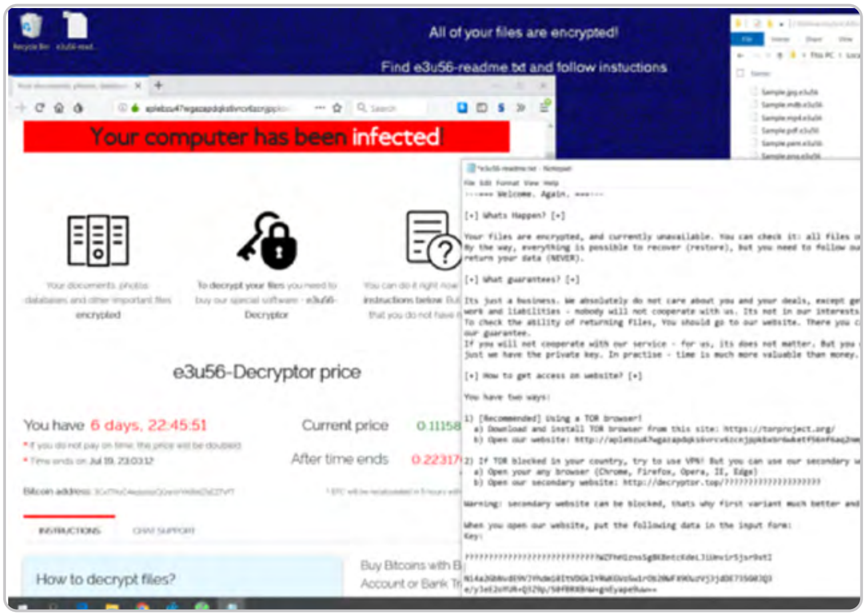
On November 1, 2020, the team responsible for developing Maze announced their official retirement, stating that any further groups claiming their name should be considered fraudulent. However, many analysts suspect the group may resurface, possibly employing new tactics or infection vectors. Some analysts have also speculated about ties between the Maze group and the REvil ransomware group EvilCorp.

While these claims have largely been dismissed as rumor, there is instead evidence that former Maze affiliates have shifted to the Egregor ransomware family, which we discuss below.

As we mentioned earlier in this report, Maze went beyond holding data hostage—it included an additional threat of publicly releasing swiped data if a ransom went unpaid. The Maze group set up an online portal to host the stolen data, publishing after a grace period (typically a few weeks) if their demands were not met.

Although Maze ransomware detections fell significantly after the group's reported retirement, many of the same actors pivoted to other ransomware-as-a-service (RaaS) groups employing similar infection vectors and deployment strategies. As these threats evolve, we expect to see increasing use.

Maze went beyond holding data hostage—it included an additional threat of publicly releasing swiped data if a ransom went unpaid.



Recycle Bin
e3u56-read...
All of your files are encrypted!
Find e3u56-readme.txt and follow instuctions
Your computer has been infected!
Your documents, photos, databases and other important files encrypted
To decrypt your files you need to buy our special software - e3u56-Decryptor
You can do it right now. Follow the instructions below. But remember that you do not have much time
e3u56-Decryptor price
You have 6 days, 22:45:51
Current price 0.11158
After time ends 0.22317
INSTRUCTIONS
CHAT SUPPORT
How to decrypt files?
Buy Bitcoins with Bank Account or Bank Transfer
Sample.jpg.e3u56
Sample.mdb.e3u56
Sample.mp4.e3u56
Sample.pdf.e3u56
Sample.pem.e3u56
Sample.png.e3u56

```
---=== Welcome. Again. ===---

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files o
By the way, everything is possible to recover (restore), but you need to follow ou
return your data (NEVER).

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except ge
work and liabilities - nobody will not cooperate with us. Its not in our interests
To check the ability of returning files, You should go to our website. There you c
our guarantee.
If you will not cooperate with our service - for us, its does not matter. But you
Just we have the private key. In practise - time is much more valuable than money.

[+] How to get access on website? [+]

You have two ways:

1) [Recommended] Using a TOR browser!
  a) Download and install TOR browser from this site: https://torproject.org/
  b) Open our website: http://aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nm

2) If TOR blocked in your country, try to use VPN! But you can use our secondary w
  a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
  b) Open our secondary website: http://decryptor.top/????????????????????

Warning: secondary website can be blocked, thats why first variant much better and

When you open our website, put the following data in the input form:
Key:
```

A ransomware attack from REvil

REvil

REvil is a RaaS business also known as "Sodin" and "Sodinokibi." It made its first appearance in April 2019 shortly before GandCrab, another popular ransomware family that eventually shut down. The timing and similarities led some to believe there was a relationship between the two.

REvil spreads using a number of vectors including malicious spam, drive-by exploits, and RDP attacks, as well as vulnerabilities, such as

CVE-2019-2725 (Oracle WebLogic server), and even managed service providers (MSPs).

Newer REvil variants use the Heaven's Gate technique which consists of executing 64-bit code in the context of a 32-bit process with the goal of going undetected.

The REvil gang is among the most sophisticated, and it regularly boasts about its capabilities and intent to go after large victims, in addition to leaking some of their data publicly. They constantly tweak their code in order to stay ahead of the competition.

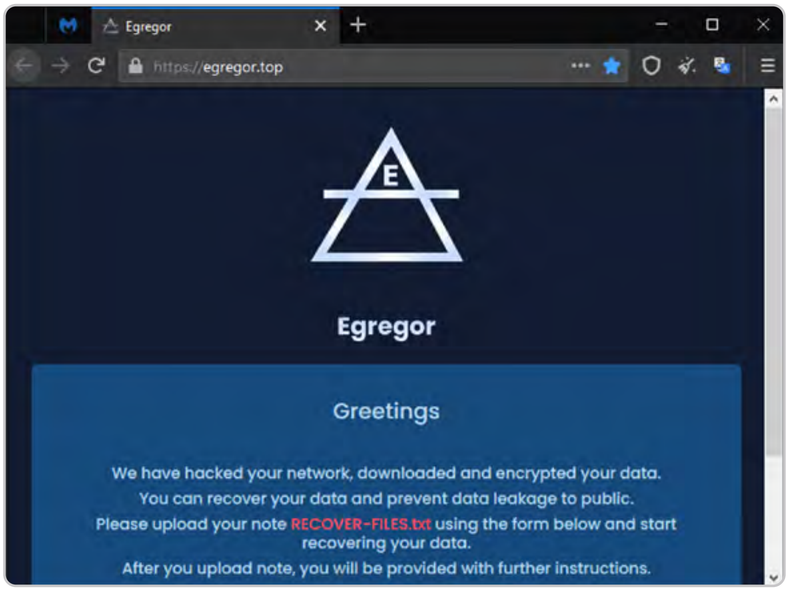
With a successful affiliate model that allegedly earned them $100 million in a year, REvil is poised to make headlines in 2021.

The REvil gang is among the most sophisticated, and it regularly boasts about its capabilities and intent to go after large victims.

SPOTLIGHT

Egregor ransomware

A new ransomware family, first discovered in late 2020, has already exhibited massive, devastating success. Born from the lessons of multiple evolutions of ransomware and the efforts of cybercrime groups to create a powerful tool with which to attack corporate networks, this is Egregor.



Greetings

We have hacked your network, downloaded and encrypted your data.
You can recover your data and prevent data leakage to public.
Please upload your note RECOVER-FILES.txt using the form below and start recovering your data.
After you upload note, you will be provided with further instructions.

A screenshot of the Egregor "welcome" page that greets infected victims

What is Egregor?

Egregor is a new family of ransomware, first spotted in September 2020. It is thought to be the successor of the Maze ransomware family, as many "affiliate" criminals who worked with Maze switched to Egregor around the same time that Maze shut down operations in October 2020.

Egregor follows the RaaS model, meaning the malware's developers focus on creating the best ransomware application possible and then selling it to "affiliates" or other criminals who distribute the ransomware in a variety of ways. Once a ransom infection occurs and payment is made, the affiliate receives 70 percent of the payment and the Egregor actors receive 30 percent. RaaS predates Egregor, back to 2016 when ransom gangs used it to distribute the Cerber ransomware.

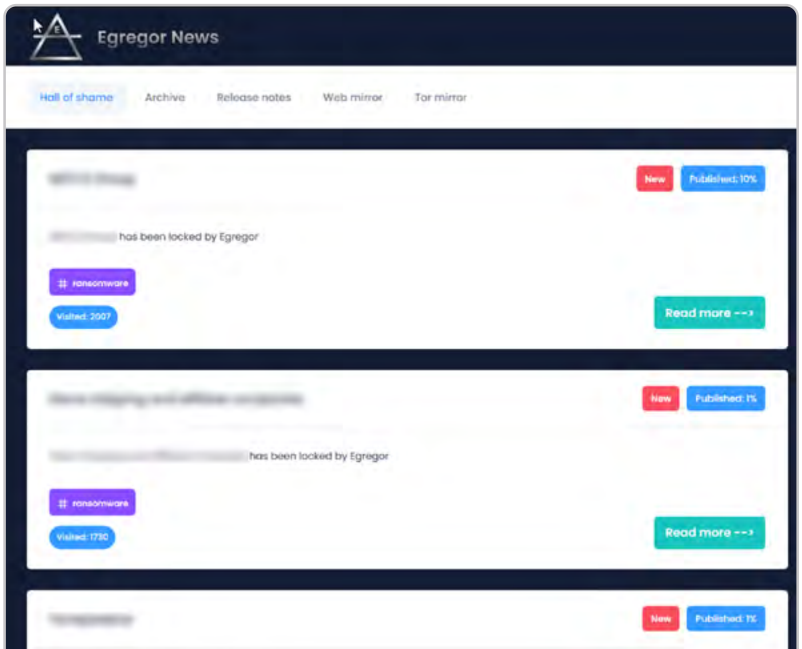
Egregor utilizes a "double extortion" method of attack. Beyond encrypting files, the ransom actors also steal data from the victim and threaten to publish the stolen information online unless the ransom is paid. We've primarily seen this new trick over the last year, which may indicate that, over time, victims have increasingly refused to pay ransom demands, as they are better equipped with backups or other methods of restoring their encrypted files.

What can it do?

Egregor encrypts victim files using the ChaCha and RSA encryption algorithms. Depending on how the malware is installed on the network and what other tools are installed with it, it can spread laterally throughout the network.

As mentioned, Egregor steals victims' data and threatens to post it online or sell it on the black market, if the ransom isn't paid. It does this through its "shame website" called "Egregor News."

This website both publicizes a successful attack against a specific organization, as well as pressures the victim into payment.



[redacted]

New Published: 10%

[redacted] has been locked by Egregor

ransomware

Visited: 2007

Read more -->

[redacted]

New Published: 1%

[redacted] has been locked by Egregor

ransomware

Visited: 1730

Read more -->

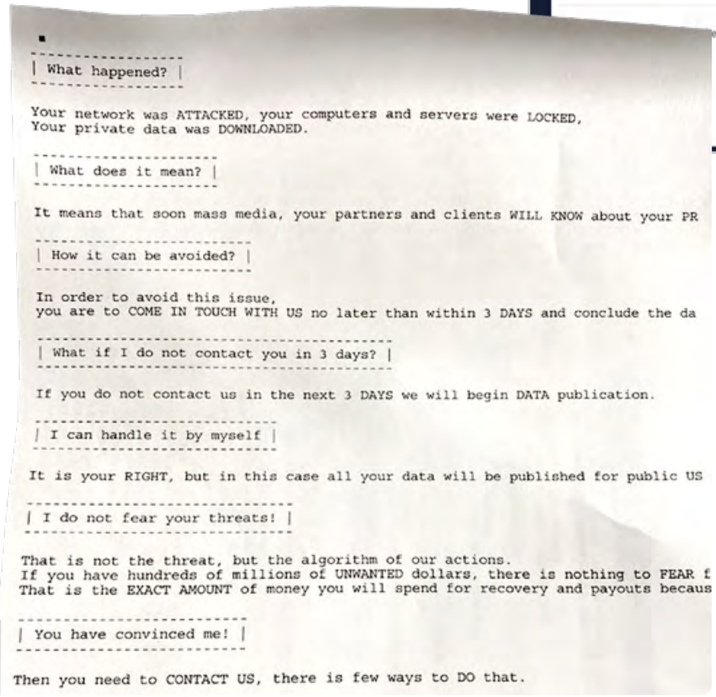
[redacted]

New Published: 1%

ed by Egregor

Read more -->

A screenshot of "Egregor News," a unique addition to cyber-extortion schemes used by threat actors today



```
.
-------------------
| What happened? |
-------------------
Your network was ATTACKED, your computers and servers were LOCKED,
Your private data was DOWNLOADED.

---------------------
| What does it mean? |
---------------------
It means that soon mass media, your partners and clients WILL KNOW about your PR

------------------------
| How it can be avoided? |
------------------------
In order to avoid this issue,
you are to COME IN TOUCH WITH US no later than within 3 DAYS and conclude the da

-------------------------------
| What if I do not contact you in 3 days? |
-------------------------------
If you do not contact us in the next 3 DAYS we will begin DATA publication.

----------------------
| I can handle it by myself |
----------------------
It is your RIGHT, but in this case all your data will be published for public US

--------------------------
| I do not fear your threats! |
--------------------------
That is not the threat, but the algorithm of our actions.
If you have hundreds of millions of UNWANTED dollars, there is nothing to FEAR f
That is the EXACT AMOUNT of money you will spend for recovery and payouts becaus

-----------------------
| You have convinced me! |
-----------------------
Then you need to CONTACT US, there is few ways to DO that.
```

Egregor's ransomware note, physically printed onto a sheet of paper

Egregor has also been seen sending its ransom notes to printers on infected networks. While this hasn't been seen with every infection, one case involved point of sale systems printing ransom notes on receipt paper.

> **The more alarming infection method that we observed, though, was through the use of Cobalt Strike, a popular penetration testing platform.**

How does Egregor spread?

By utilizing the RaaS model, Egregor can reportedly be distributed in a variety of ways. Some reports claim that Egregor is spread along with, or by, the Qakbot/Qbot malware, using malicious phishing attacks. We've also seen a few exploits being used to help spread Egregor, including:

- Microsoft Exchange Exploit (CVE-2020-0688)
- VBScript Engine Exploit (CVE-2018-8174)
- Adobe Flash Player Exploit (CVE-2018-4878/CVE-2018-15982)

The more alarming infection method that we observed, though, was through the use of Cobalt Strike, a popular penetration testing platform which gained notoriety in 2020 as a useful tool for network compromise when used by cybercriminals. The use of Cobalt Strike and other "off the land" and penetration testing tools is usually preceded by an infection through malicious emails or, as more commonly seen this year, brute forcing of vulnerable RDP ports.

Can Egregor defend itself?

Egregor will only launch when provided with the correct command line input, notably a password that the attackers must provide. This hinders security researchers' ability to analyze the malware.

In addition, Egregor shuts down processes related to malware analysis, like process monitor, as well as other applications, like MySQL, Microsoft OneNote, and Microsoft Outlook. Shutting down these applications can both protect Egregor from analysis, and unlock more files for it to encrypt. For example, Office documents opened by their applications may prevent the ransomware from being able to encrypt that file. The same goes for SQL database files that hold relevant and valuable data but are locked as long as the database applications are still running.

Finally, perhaps because this malware likely originated in Eastern Europe, Egregor investigates locale information about victim systems and if any are found to be set to locales in a post-Soviet state, the malware shuts itself down and does not cause any damage. Some of these countries include Armenia, Belarus, Georgia, Kazakhstan, Romania, Russia, and Turkmenistan.

Avoiding victims from certain countries is not new and in fact most ransomware we've seen over the last five years has had this feature embedded in it. The idea is that if the ransomware avoids infecting users in these countries, Russian and other local law enforcement organizations will turn a blind eye to cybercrime. Whether this is the intent of Egregor, or a red herring to throw off the creator's actual nationality, we may never know.

Notable attacks

Despite its late arrival, Egregor was very busy last year and was involved in numerous high-profile attacks. During the last months of 2020, Egregor was used to attack the businesses of Ubisoft, K-Mart, Crytek, and Barnes & Noble, to name a few. The FBI even issued a warning about Egregor and its intent on attacking business networks.

Guidance

In addition to regular guidance on multifactor authentication and utilizing anti-malware software, the FBI recommends that users create backups of their data. When considering how to backup data, make sure you are backing it up, off-site, either to a separate device or the cloud, and utilize as many layers of security as possible to protect those backups from unauthorized access.

In addition, the FBI recommends prioritizing public-facing remote access products and services, like RDP, when it comes to rolling out updates. This will help prevent those ports from being used to break into the network.

Finally, do not pay the ransom. In the past, with ransomware that only encrypted files, paying the ransom was more of an individual choice based on the circumstances of the attacked organization. In some cases, paying the ransom was the understandable, if difficult, decision, as the fallout from not paying might have been more costly. Those days are over.

Ransomware actors today, especially those that employ double extortion, are more likely to take your money, but not delete stolen files or decrypt data, and then return later demanding more money.

When ransomware was mostly focused on consumer victims, customer service was an important part of the attack, because unless the victim had confidence they would have their files returned, they were unlikely to hand over payment. In today's ransomware-filled world, establishing a rapport with the victim is not necessary, as the hijacking of valuable data from companies tends to be seen as much more valuable than consumer family pictures, and in turn means much bigger ransom demands for the attackers. Law enforcement agencies are actually moving to outlaw companies paying ransom actors, because ransom payments fund the attackers' future endeavors and encourage others to follow suit.

We will likely see more Egregor in 2021, and it may become the new poster child for ransomware in the 2020s.

What's next?

Egregor is just another evolution in the world of ransomware attacks. It takes a lot of inspiration (and, in some cases, code) from previous ransomware families like Maze, Cerber, and Sekhmet, and this time next year we might be discussing the ransomware family that is inspired by Egregor. However, it is still incredibly dangerous, having successfully attacked major organizations and enjoying the backing of numerous cybercriminal groups. We will likely see more Egregor in 2021, and it may become the new poster child for ransomware in the 2020s.

Windows threat landscape 2020 summary

2020 was a busy year for malware, with new developments, new targets, and new attackers. All the while, attackers and defenders struggled to fully understand how our world began to change during the pandemic. In 2021, we'll likely see a return to semi-normal, with more targeted attacks against businesses, likely using the tools developed this year for manual breaches that lead to higher potential payouts for threat actors.

Before we look at our Mac data, we must address a specific campaign that verified a malware trend that Malwarebytes has known about for years. This isn't about individual malware capabilities or deployment methods, but about human operations.

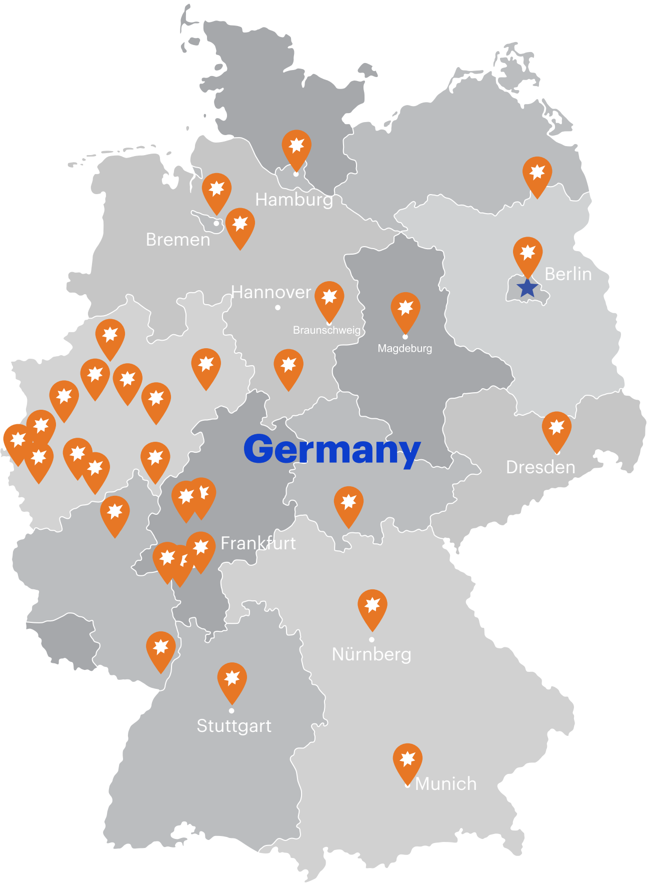
This is malware as a business.

4 | Malware as a business

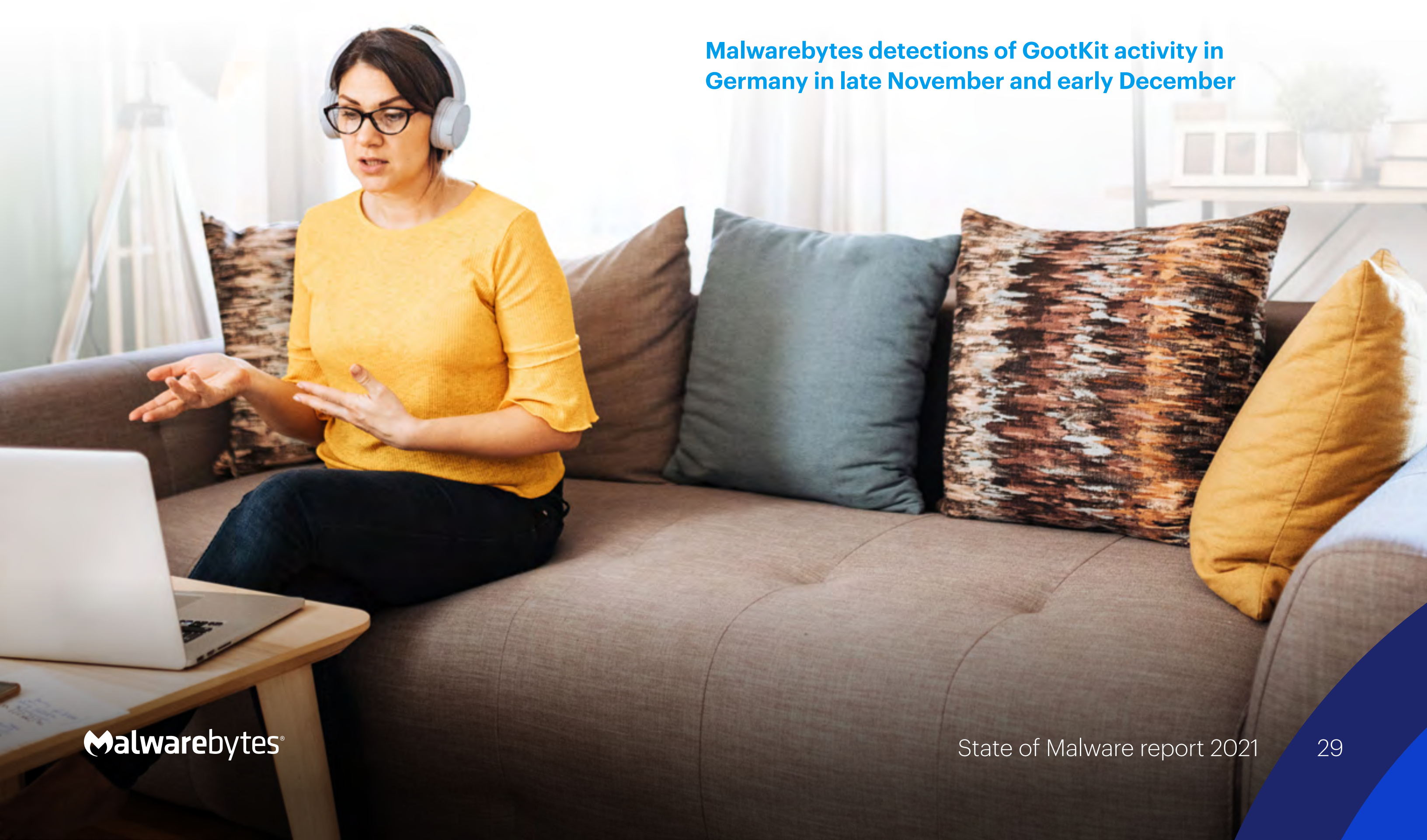
In 2020, we scrutinized one malware campaign that confirmed every piece of a now-proven trend: Malware operations have built up the same type of infrastructure as a small business.

On November 23, Malwarebytes received information about an increase in GootKit infections in Germany. The old banking Trojan, which dates back to at least 2014, can record keystrokes and video as a means of stealing financial information.

When Malwarebytes investigated, we found that a GootKit infection was pushing the REvil ransomware to machines in Germany. Of particular note, though, is that we saw this activity only in Germany.



Malwarebytes detections of GootKit activity in Germany in late November and early December



This is one of the strongest examples that Malwarebytes has seen... of malware-distribution-as-a-service.

This activity could indicate that the GootKit authors had offered granular, focused malware distribution services—able to precisely target certain geographies and nothing beyond them. Further, we saw that GootKit had previously pushed the SunCrypt ransomware, which means that its authors were also capable of changing the final payload in its latest resurgence in Germany.

This is one of the strongest examples that Malwarebytes has seen to prove the ongoing phenomenon of malware-distribution-as-a-service, in which the capability to target and distribute specific malware to one area or one geographic region becomes part of the appeal of that malware itself. Appealing to whom? To other threat actors, of course.

Malware-distribution-as-a-service should not be considered an isolated development, but as an offering from malware authors who are improving single parts of the standard malware attack chain.

Here, malware authors are focusing on the modularization of campaigns, which allows for greater specialization. Malicious actors no longer need to be experts at crafting the whole chain of their attacks. The process can be broken into chunks and these can be refined and perfected.

This leaves malware authors to concentrate on making more effective malware, while malware distributors work to improve their distribution networks, all while still making a profit and running their business.

The campaign that we investigated is simply the latest representation of increased professionalism and business acumen displayed by malware authors in recent years. The move toward marketplace cybercrime is only going to make the threat landscape more dangerous, as the tools we'll likely see being distributed, sold, and launched are going to be more sophisticated than most anything we've seen before.

This is already happening in the world of RaaS, where we continue to see rapid evolution.

Entire teams are collaborating on effective attacks.

Away from raw malware capabilities, threat actors have also bolstered their so-called "workforce"—with entire teams collaborating on effective attacks.

Victim vetting mechanisms

To improve efficiency in how they use their tools, some malware groups scout out a victim before launching their entire arsenal. We call this trend malware "victim vetting mechanisms."

These mechanisms include gathering information about the victim, such as:

- What domain is this endpoint connected to?
- What is the IP address of this endpoint?
- What applications are running on this endpoint?
- Who are the active users of this endpoint?

Then, by using the gathered data, the actors can determine if the target is worth attacking or not. They may launch preliminary attacks, attempt to spread laterally, or utilize RAT tools for additional information gathering.

The point of victim vetting is to reduce the resources spent on a potential victim, evade any traps or honeypots, and reduce the chance that in-use tools and techniques get analyzed or discovered, similar to what we saw with Emotet removing its "waste" last year.

In addition to hiding tools and techniques, malware campaigns that result in a ransomware infection have a better return on investment (ROI) if the victims are not individual consumers. Simply put, a business stands to lose more money from operational downtime and will therefore likely be willing to pay more. Individual consumer infections are just not going to generate as much money.

To pull this off, we've seen actors like Trickbot utilize a new tool they developed called "LightBot." This PowerShell script gathers much of the data referenced earlier and sends it back to the attacker, who can then confirm if they want to attack that target. Perhaps the organization will not be able to pay the desired ransom, or perhaps the target is too well guarded to make it worth attacking them.

In addition, we are seeing more malware samples call home with reports about victim machines which are then put through a manual evaluation. This means there is a team of people manually sorting through reports generated by the malware, prioritizing the more interesting victims, assigning special cases for a deeper dive, and performing manual recon and lateral propagation.

Malware campaigns that result in a ransomware infection have a better return on investment (ROI) if the victims are not individual consumers.

Taking a step back from these operations, we find significant infrastructure. There is the malware campaign itself, in which distribution can be handled by malware distributors who can target specific regions with specific payloads, even while using prior malware that delivered separate payloads in the past. That payload could be a type of ransomware that itself is offered through a RaaS group, which has its own tech support and developers. But before the ransomware is delivered, a group could rely on victim vetting mechanisms to determine which targets are worth attacking.

Malware, then, is not at all an automated process. The threat actors behind many of the attacks we saw last year—and the years before—are not one-person hackers looking to cause a little chaos. Those threat actors belong to criminal businesses, and those businesses have people in seats with roles and responsibilities, and they are becoming more capable as time passes.

This trend of vetting victims before launching attacks isn't new and in fact it's one of the top rules in the state-sponsored, advanced persistent threat (APT) handbook. To see it done by commercially-focused criminals isn't surprising.

However, if new tools and frameworks are created, shared, or sold online, making vetting easier for less sophisticated actors, it will make some attacks less likely (as the ROI might not be worth it) and others very difficult to stop (as they are using tools that few have seen and can stop).

Malware is not at all an automated process. The threat actors behind many of the attacks we saw last year—and the years before—are not one-person hackers looking to cause a little chaos.

5 | Mac threat landscape 2020

Mac detections in 2020 fell a fair bit from the all-time high we previously reported for 2019, with overall detections decreasing by more than 37 percent.

This was primarily due to a drop in detections of Adware and potentially unwanted programs (PUPs), while malware (mostly backdoors, data stealers, and cryptocurrency stealers/miners) increased by more than 61 percent!

Mac detections 2020 compared to 2019

	2019	2020	% Change
Business	4,022,256	5,257,570	31%
Consumer	116,833,049	70,027,857	-40%
Total	**120,855,305**	**75,285,427**	**-38%**

Malwarebytes saw its highest number of Mac detections in the US. This is no surprise, as the US is our largest market. However, malware detections only represented 1 percent of the total Mac detections in the US last year. Similarly, in most of the countries with a large number of detections—Australia, UK, Canada, France, and others—malware made up less than 5 percent of the total detection count. Conversely, a number of countries clustered mostly in Asia and Europe saw a much higher percentage of malware, such as South Korea (18.1 percent), Ukraine (16.3 percent), Norway (15.0 percent), and the Czech Republic (14.9 percent). Other top contenders included Greece, Malaysia, United Arab Emirates, Indonesia, Taiwan, and Austria.

In most countries, PUPs and Adware comprised the majority of the detections, without any discernible patterns. In some countries, Adware ranked as king, while in other countries, PUPs took the crown. In Barbados, for example, 99.9 percent of all nearly 1 million detections were PUPs, while Tanzania saw 95.6 percent of detections in the form of Adware.

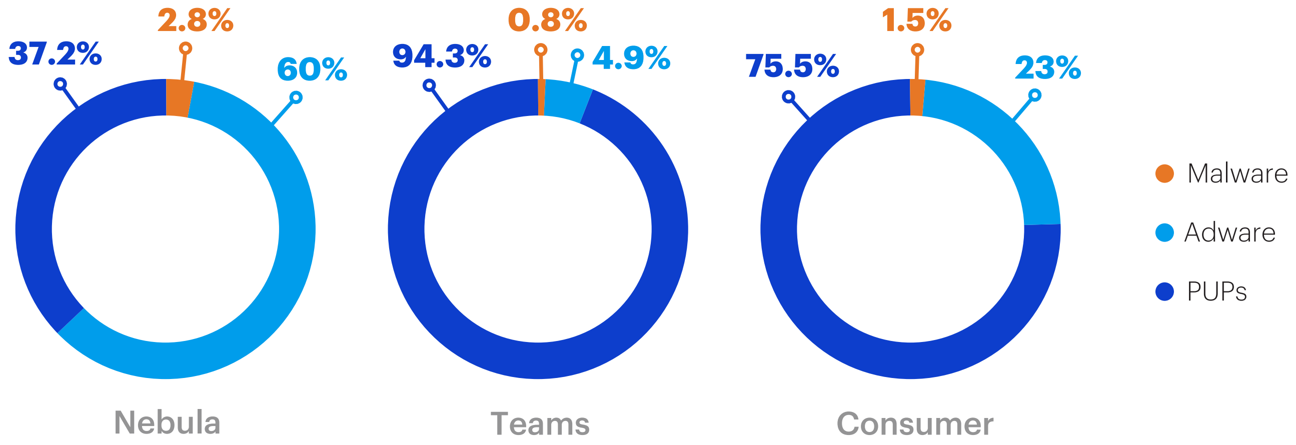
Overall, PUPs represented more than 76 percent of our detections for Mac in 2020, while Adware represented about 22 percent. Malware accounted for only 1.5 percent of the total, skewed heavily by the data from countries with low malware percentages, like the US, which alone made up nearly 70 percent of the data.

Overall, PUPs represented more than 76% of our detections for Mac in 2020, while Adware represented about 22%. Malware accounted for only 1.5% of the total.

When comparing our business telemetry with our consumer telemetry, we found some interesting differences. In consumer products, PUPs accounted for more than three quarters of all detections, with Adware accounting for most of the rest. As we saw with our overall detections for Mac, malware made up only 1.5 percent of the consumer detections.

On the business side, devices with our managed Nebula service, typically used by medium to large businesses with IT that is likely to do device management, we recorded far fewer PUPs, at only around a third of the detections, while Adware accounted for almost two thirds. These business machines saw far more malware, as well.

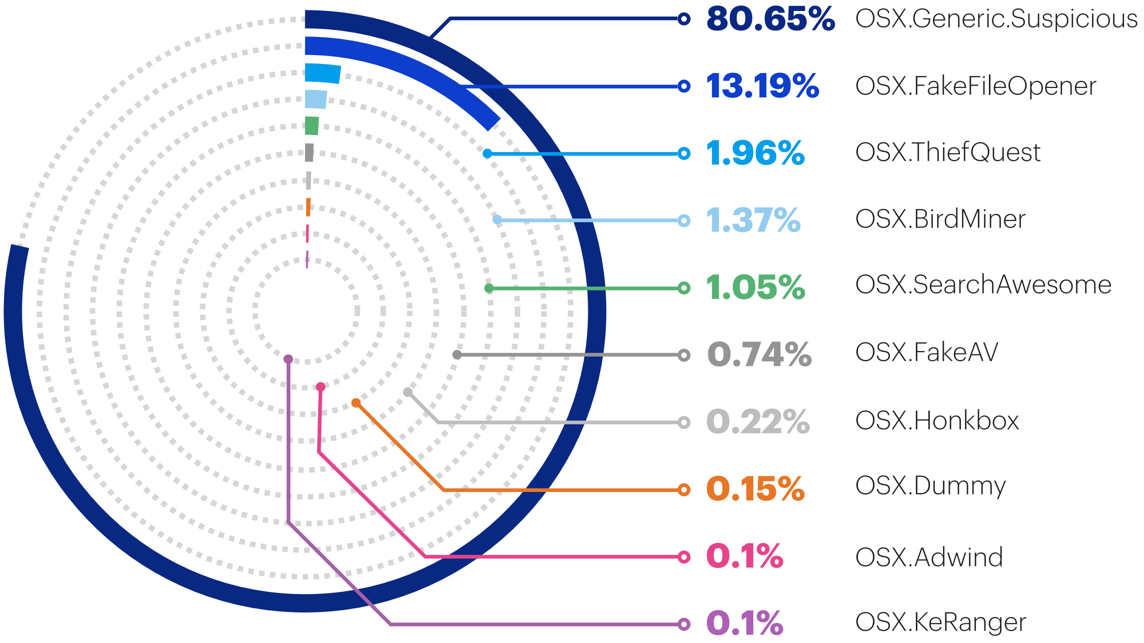
Detections from our Teams product, typically used by small businesses without much—if any—IT support and no central device management, hewed more closely to consumer usage than business. PUPs made up the vast majority with Teams, clocking in at almost 95 percent of all detections!



This data would seem to indicate that in business environments, the main threats are malware and Adware, which are similar in everything except who is targeted: The user of the machine, or an advertising or affiliate program. PUPs are a much smaller issue, likely because of the availability of IT resources that make the user less likely to install rogue antivirus, or questionable "cleaning" software. Why buy such software when you can simply ask IT for help?

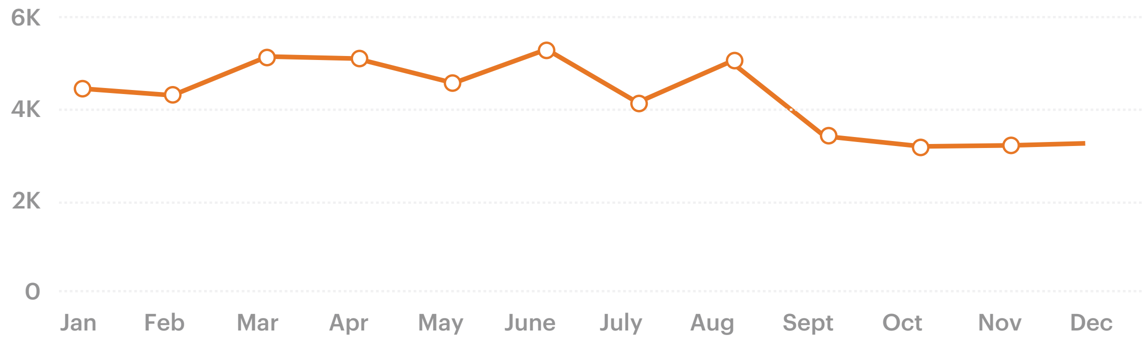
On the other hand, for consumers and small businesses without IT support, PUPs represent a more significant issue, as users seek help for problems and stumble onto the wrong "solutions."

Top 10 Mac malware of 2020



Of all the malware detected on macOS, the top ten malware families accounted for more than 99 percent of the total. The vast majority—80 percent of the overall malware detections—were detected due to suspicious behaviors. These behaviors can include such things as attempting to run obfuscated Python or shell code as a persistent process via launchd, or making a hidden file in the root user's folder run at startup. Coming in second was OSX.FakeFileOpener, a series of malicious apps designed to hijack the process through which macOS determines what app should be used to open a file.

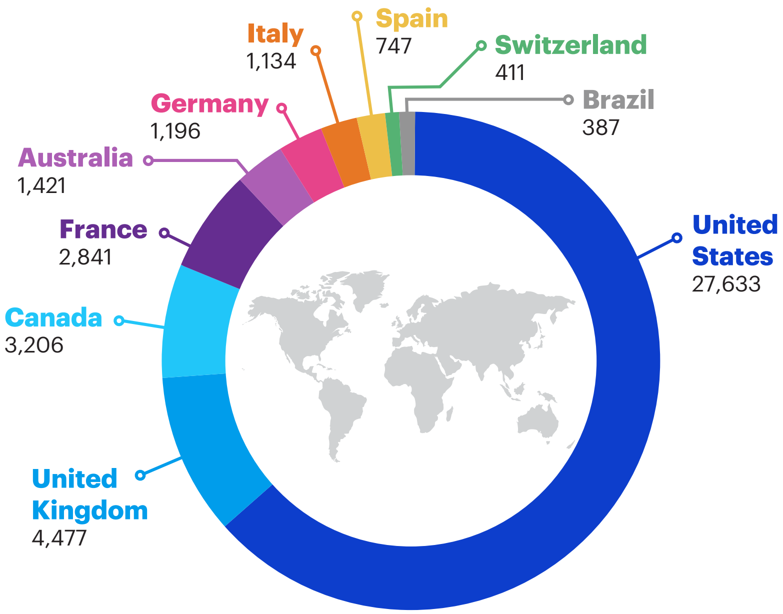
OSX.FakeFileOpener detections 2020



Coming in third was the most interesting piece of Mac malware seen in 2020: ThiefQuest, aka EvilQuest, which we discuss further below.

Interestingly, the KeRanger ransomware came in tenth, just as it did in 2019. This is quite odd, as this malware is extinct and hasn't been capable of encrypting files since not long after its discovery in 2016. This may be an artificial detection, caused by people testing to see if Malwarebytes detects KeRanger. It could also be detections of old, infected versions of the Transmission app, in which the malware is no longer functional but the app itself works normally. Transmission can update itself to a clean version, which removes all traces of the malware, but users would have no idea they're infected and could still be using a version that has not been updated. KeRanger detections at this point are almost entirely inside the US; you could count the detections outside the US on the fingers of both hands.

Mac threat detection count by country

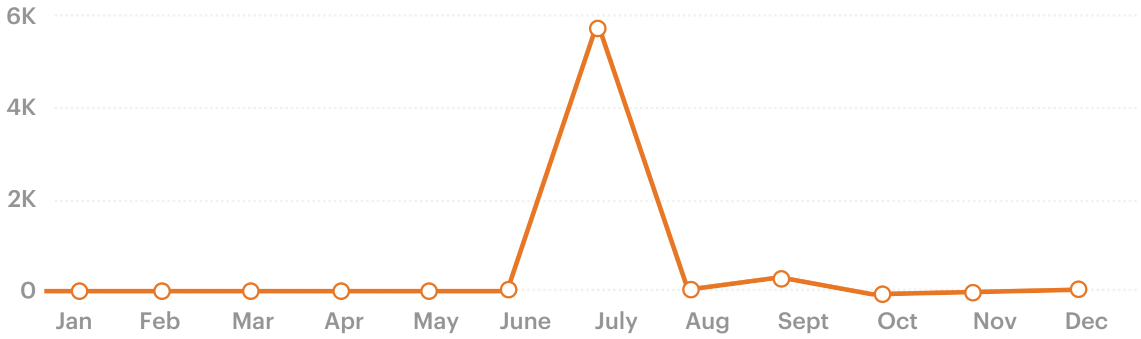


ThiefQuest

ThiefQuest was the most unusual malware seen on macOS in 2020. It spread through apparently legitimate installers found on torrent sites, but those installers dropped an extra bonus of malware in addition to the expected software.

Once infected, Macs would eventually start to see files getting encrypted. If you happened not to notice, the malware would display a pop-up message to let you know, and it would even use text-to-speech to verbally pester you about it. Like most ransomware, it provided a file with instructions. Clearly, all signs pointed to this being the first Mac ransomware since 2017.

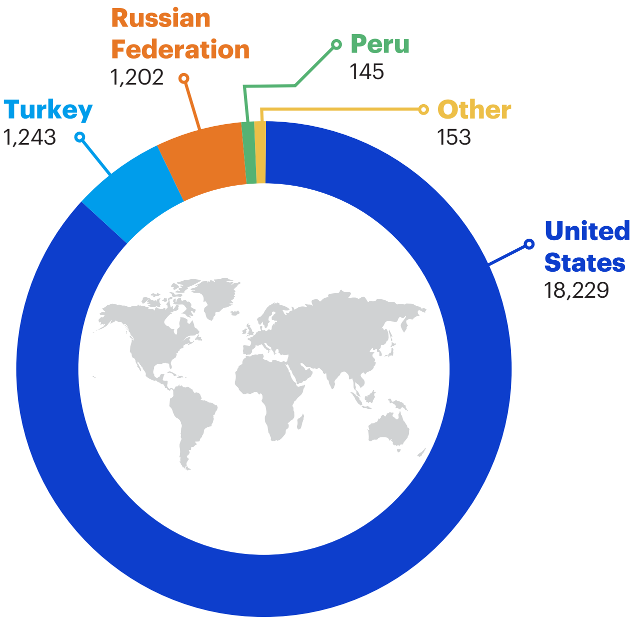
ThiefQuest detections 2020



Except it wasn't. A deeper look revealed oddities. For example, there was no email address offered to use to contact the creator of the malware once you'd paid. Further, the Bitcoin addresses referenced in the instructions on every computer were all the same, meaning there was no way for the attacker to verify you had paid.

Upon further investigation, we learned that the ransomware activity was really a cover for massive data exfiltration, including MS Office and Apple iWork documents, PDF files, images, cryptocurrency wallets, and more. This kind

ThiefQuest detection count by country



of malware, known in the Windows world as a "wiper," had never before been seen on Macs.

Even more interesting, the malware would inject malicious code into executable files found in the Users folder, such as components of Google Software Update, in a virus-like manner, another rarity in the Mac world. The combination of these features made ThiefQuest not only the most unusual Mac malware in 2020, but perhaps the most unusual Mac malware ever.

PUP removal on MacOS

Recently, Apple introduced a new system extension technology for use by security apps. One major advantage of these system extensions is that they're protected against removal by default, by the system. Not even the user can manually remove these without disabling the System Integrity Protection security feature of macOS.

Fortunately, developers must apply to Apple and be granted a special entitlement before they can create and ship a system extension. In theory, this should protect against abuse of system extensions for malicious purposes. Unfortunately, several programs that Malwarebytes and other security products detect as PUPs have managed to get this entitlement.

Apple and the security industry have not always been on the same page about detection of PUPs. (Hardly surprising, considering members of the security industry itself are often not on the same page about what is or isn't a PUP.) It's not that Apple approves of PUPs, necessarily; it's just that it leaves it to others to police PUPs in most cases.

All that changed with macOS 10.15 (Catalina). We've entered a world in which no software in the entire industry can remove all components of these PUPs, because they've come under the protection of Apple.

Apple's days of sitting on the fence are now over. With the protection involved in the system extension entitlement, there is no longer any middle ground. At the time of writing, Apple is implicitly siding with the PUPs, providing them

Recently, Apple introduced a new system extension technology for use by security apps... which are protected against removal by default, by the system.

We've entered a world in which no software in the entire industry can remove all components of PUPs, because they've come under the protection of Apple.

protection against removal. Time will tell if Apple decides to side with those who stand against these PUPs, by revoking their entitlements.

Adware activity

Adware is a type of malware for which the victim is not the user of the computer (not directly, at least). Adware targets advertisers and affiliate programs, generating revenue through ads injected into the browser or through affiliate links. For example, it may redirect your browser's searches to go through an affiliate link on Yahoo or Bing, rather than the search engine you might normally use. At that point, every time you do a search, the criminal behind it gets paid.

On macOS, Adware is by far the most dominant type of malware that we see. Interestingly, it is also some of the most sophisticated malware that we see. This year, a number of interesting Adware techniques appeared, such as phishing for the user's admin password, using synthetic clicks to automate installation of browser extensions, modifying the sudoers file to maintain root permissions indefinitely, and manually editing the Transparency, Consent, and Control (TCC) database to give the Adware additional access to the system.

While none of this was particularly new, some advanced techniques that we spotted were.

For example, one family of Adware installed a Safari extension by duplicating Safari, modifying it to automatically activate a particular extension at launch, and then opening it. This is a highly advanced technique that exploits limitations in how macOS manages code signing.

If an attacker were to modify a code signed app and then distribute it, macOS would prevent that app from running. However, apps already installed on the system can be modified in a variety of ways without triggering macOS security to block them.

We also saw Adware starting to use system configuration profiles and managed preferences to force the browser to use a particular home page and search engine. These things exist to allow IT admins to set defaults, and prevent users from changing them, but Adware is abusing them for malicious purposes.

We've also seen an interesting new pattern in Adware installers. Apple has locked down macOS more and more, requiring not just code signing but also a new "notarization" process. Notarization involves submitting apps to Apple. As part of the process, Apple's automation somehow scans the apps to ensure they don't contain any malware.

Adware developers responded in divergent ways. Some simply stopped signing their Adware, providing the user with instructions on how to bypass macOS security to run the unsigned installer. This means that they don't have to bother with notarization, but they also don't have to worry about Apple revoking their code signing certificate.

On macOS, Adware is by far the most dominant type of malware that we see. Interestingly, it is also some of the most sophisticated malware that we see.

However, other Adware developers went the other way, and actually managed to get their malware notarized! In a number of cases, it appears to have passed the notarization checks without significant modification. Apple can, and does, revoke the notarization and code signing certificates in these cases, but this happens later, once Apple's security researchers have discovered the offending software.

Nation-state and other targeted malware

The bulk of the non-Adware malware activity on macOS has come from targeted attacks. This includes a lot of activity from nation-state threat actors, such as North Korea or China.

North Korea's Lazarus Group was active throughout the year, releasing multiple Mac versions of their Fallchill, GMERA, Yort, and Dacls RAT malware. Vietnam's OceanLotus group was also active, with new variants of their OceanLotus backdoors affecting macOS.

Also last year, according to a report from journalist Zack Whittaker of TechCrunch, a state-backed attack, likely from China, targeted the Uyghur people, a Muslim group that has been the subject of oppression by the Chinese government. The attack reportedly relied on a series of malicious websites that could hack into iOS devices that visited them. (These attacks also involved Android and Windows malware, but no known Mac malware.)

Although there was non-targeted Mac malware in 2020, it was relatively limited. Most of this malware included cryptominers, with some uncommon backdoors, and the unusual ThiefQuest malware mixed in for good measure.

Apple has locked down the system more and more, requiring not just code signing but also a new "notarization" process. Notarization involves submitting apps to Apple.

6 | Android threat landscape 2020

Last year was another big one for Android malware.

Malware that we detected heightened activity on in late 2019 proved more stubborn than expected, as was the case with Android/Trojan.Dropper.xHelper. Recorded detections for some known types of malware grew significantly, including those for Android/Trojan.FakeAdsBlock and Android/Trojan.Bankbot. Old, recognizable threats in this landscape—like Android/Trojan.HiddenAds—became more prevalent. Pre-installed malware continued to cause nightmares for support centers and customers. And, of course, Adware could not be overlooked.

Here's what we saw last year.

Fake ad blocker

Climbing the detection charts in 2020 was a bit of malware that can best be described as "ironic." Posing as a so-called Ads Blocker, Android/Trojan.FakeAdsBlock produces an alarming number of non-stop ads. Because of this malware's "special" ad-blocking capabilities, it asks for extra permissions that other, legitimate ad blockers do not require.

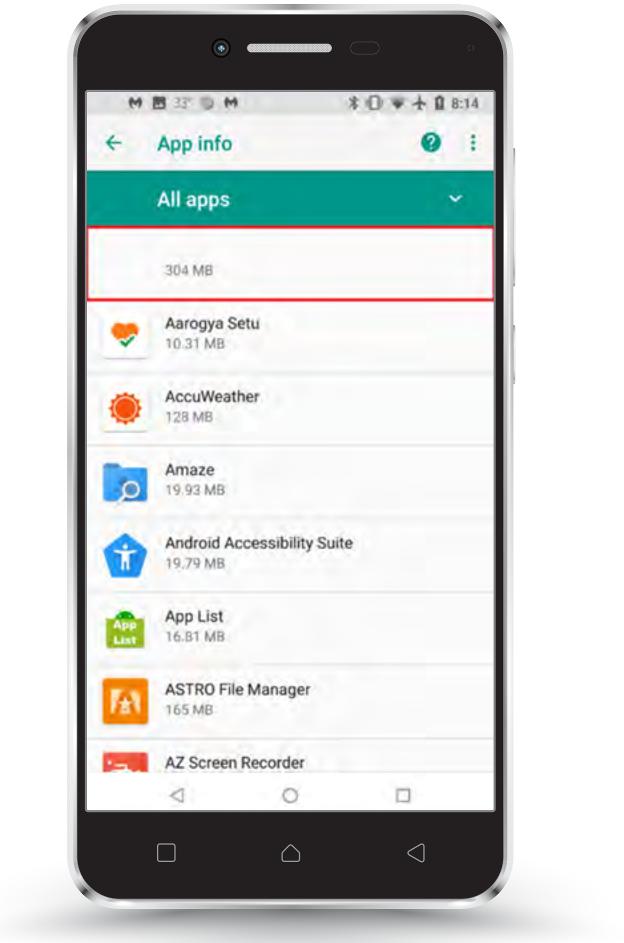
First, it asks for *Display over other apps* permissions. It also asks to be a source of allowing installs of unknown apps from unknown sources. Once these permissions are accepted by a user, Android/Trojan.FakeAdsBlock can then display ads over other apps and install separate, additional malware from non-Google Play Store sources. And that is precisely what it does.

Within minutes of having its permissions granted, raunchy ads come in all forms: Opening the default web browser to ad sites, popping up ads in the notifications, even utilizing a fake Facebook Messenger notification that opens to ads when clicked.

The tricks don't end there: It is extremely difficult to find any trace of Android/Trojan.FakeAdsBlock in the App info list as it has no identifying icon or name—just a blank box at the top of the list.

This blank box tactic has become particularly popular among many forms of malware—most notably Android/Trojan. HiddenAds, a close cousin to FakeAdsBlock.

The malware's dangerous capabilities are matched by its detection numbers. In 2020, FakeAdsBlock accounted for 80,654 detections.



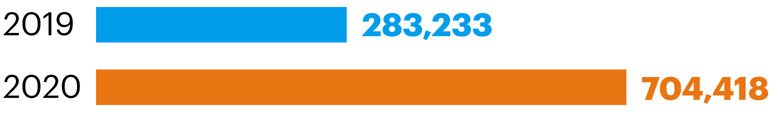
304 MB
Aarogya Setu 10.31 MB
AccuWeather 128 MB
Amaze 19.93 MB
Android Accessibility Suite 19.79 MB
App List 16.81 MB
ASTRO File Manager 165 MB
AZ Screen Recorder

Android/Trojan.FakeAdsBlock hides itself from view, displayed only as a blank box

Back again: HiddenAds

Coming back as the topmost prevalent malware seen on mobile devices is Android/Trojan.HiddenAds. It is the malware that keeps on giving, as it pushes aggressive ads anywhere it can. That includes in the notifications, on the lock screen, displayed as full pop-up screens, in the default browser, and more.

HiddenAds detections 2019/2020

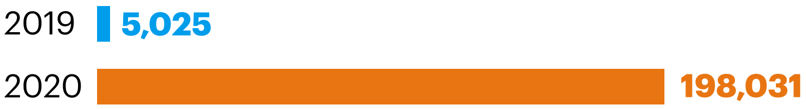


In 2019, Malwarebytes recorded 283,233 detections for HiddenAds. This year, Malwarebytes recorded a massive uptick at 704,418 detections—an increase of 421,185. In fact, this malware's detection numbers proved so high that our threat intelligence team did not even need to look at the data to know about its popularity: Our support team told us this was the mobile malware they most often address.

Bankbot becomes popular

Banking Trojans have existed for a long time in the Android landscape. However, the generic Android/Trojan.Bankbot saw a huge spike in detections in 2020, amassing a staggering 198,031 detections. This is a big jump from the 5,025 detections recorded in 2019.

Android/Trojan.Bankbot detections 2019/2020



This huge jump in detections is concerning for users, as Bankbot steals payment information using fake login screens that ask users to re-enter payment information. This gives users everywhere another reason to be careful when entering their credit card information.

The huge jump in Bankbot detections is concerning for users, as it steals payment information using fake login screens that ask users to re-enter payment information.

Pre-installed malware only gets worse

Once again, pre-installed malware proved to be one of the most painful thorns for customer support workers and customers themselves, as this type of malware comes pre-installed on new mobile devices and remains unremovable, despite many best efforts. While most of these types of malware can be uninstalled using a more advanced technical method, some can't even be uninstalled this way. This is due to the pre-installed malware being coded within system apps that are needed for basic device functionality, such as the Settings app and SystemUI app.

We saw this with the UMX U683CL, a phone provided by Assurance Wireless via the US government-funded Lifeline Assistance program in early 2020. Then again we saw this happen with the ANS UL40 device, yet another phone provided by Assurance Wireless.

The most prevalent pre-installed malware was Android/PUP.Riskware.Autoins.Fota, a variant of Adups. Autoins.Fota was also part of the reason why HiddenAds was so prevalent: It is known to auto-install multiple variants of HiddenAds onto mobile devices without user consent or knowledge.

In 2019, Autoins.Fota accounted for 255,514 detections. Detections decreased to 74,073 this year, but don't be fooled, this pre-installed malware remained just as prevalent—detections just appeared lower because Autoins.Fota had been reclassified as a variant of Android/Trojan.Dropper.

Malware gets nastier

Similar to how pre-installed malware can rebuff basic de-installation attempts, there is another type of malware with an equally dangerous defense mechanism—staying on a mobile device even after a factory reset. We saw this in 2020 with Android/Trojan.Dropper.xHelper. This malware accounted for 9,686 detections in 2020. It most likely also aided in the high volume of HiddenAds malware being dropped onto mobile devices.

Adware

With more aggressive malware displaying ads—such as FakeAdsBlock and HiddenAds—it's easy to overlook the less harmful category of Adware. Although less damaging and aggressive, Adware still ranks high on sheer annoyance.

There were two variants we saw in 2020 that gave everyone headaches.

With a high count of 143,465 detections in 2020, Android/Adware.MobiDash dwells on third-party app stores, hidden within the code of repackaged legitimate apps. If a user has a long list of installed apps, tracking down which app is causing periodic ads could be tough.

The second variant is Android/Adware.AdNote, first seen at the end of 2020. Posing as various office-type apps on the Google Play store, this Adware is known to open the default browser to an ad website. AdNote accounted for 4,483 detections and a lot of frustration in 2020.

Autoins.Fota is part of the reason why HiddenAds is so prevalent: It is known to auto-install multiple variants of HiddenAds onto mobile devices without user consent or knowledge.

Android threat summary

Year over year, Android malware becomes more prevalent, nastier, and takes up even more real estate in the malware threat landscape. This year was no different, and we saw quite a bit of growth from the mobile malware that we selected at the beginning of the year as likely problems.

Our predictions were based on pretty solid ground: As more aggressive malware—categorized as Trojans—infests mobile devices with a barrage of ads in every corner, less aggressive Adware slips through the cracks onto the Google Play store.

As expected, generating ad revenue continued to be the main way that malware developers funded their operations, and in 2020, business boomed.

We predict the same for 2021.

Year over year, Android malware becomes more prevalent, nastier, and takes up even more real estate in the malware threat landscape.

7 | Data privacy in 2020

The story of data privacy is ever evolving.
In 2020, that story proved both global and personal.

One year after the launch of the Coalition Against Stalkerware—the multi-disciplinary group that helps to protect users against apps that can non-consensually invade their personal privacy—the group more than doubled in size, with representation in the United States, Canada, Ireland, India, Uganda, France, Germany, and Greece.

Unfortunately, the Coalition Against Stalkerware met a new obstacle in 2020—the coronavirus. As individual states and countries implemented shelter-in-place orders to limit the spread of the growing pandemic, the use of stalkerware-type apps actually increased. Several cybersecurity vendors, including Malwarebytes, recorded increased detections in these types of apps throughout the entire year.

In tandem with this increase, governments across the world sought digital solutions to the pandemic itself, hoping to launch data tracking systems that could aid the work of contact tracing. Cell phone location data was monitored, credit card purchases were scoured, and Apple and Google focused on Bluetooth capabilities between devices.

Several cybersecurity vendors, including Malwarebytes, recorded increased detections in stalkerware-type apps throughout the entire year.

For years, Malwarebytes has detected and warned users about the potentially dangerous capabilities of stalkerware, an invasive threat that can rob individuals of their expectation of, and right to, privacy.

Along the way, the torrent of data privacy legislation that the US witnessed in 2019 slowed down into more of a trickle. Only a few data privacy bills were introduced into either its House of Representatives or Senate, and a similarly small number of data privacy bills became laws in individual states.

Here's the story of data privacy in 2020.

Stalkerware-type app use spikes

For years, Malwarebytes has detected and warned users about the potentially dangerous capabilities of stalkerware, an invasive threat that can rob individuals of their expectation of, and right to, privacy. Our commitment to this effort helped us launch the Coalition Against Stalkerware in 2019.

Importantly, companies that are not involved in the Coalition Against Stalkerware also took commendable steps to protect users everywhere from these and similar threats. In July, for example, Google announced that it would no longer allow advertising for spyware and stalkerware on its platform, barring some exceptions. Further, in December, Apple published a guide that offered advice on how to revoke account access for previously-approved users, empowering some device owners to, say, prevent an ex-partner from accessing their data after the end of a relationship.

Despite these corporate strides, this year brought with it a global pandemic. And with the pandemic, detections of stalkerware-type apps increased dramatically.

In 2020, Malwarebytes recorded a significant uptick in stalkerware-type app detections on our Android product. Internally, Malwarebytes does not classify anything as "stalkerware." Instead, we have two categories for apps with monitoring capabilities: Monitor and Spyware.

From January 1 to June 30, Monitor detections rose 780 percent, and Spyware detections rose 1,677 percent.

That six-month comparison represents our highest increase when looking across the entire year. Starting in July, detections slightly dropped, and then sustained lowered levels for the rest of the year.

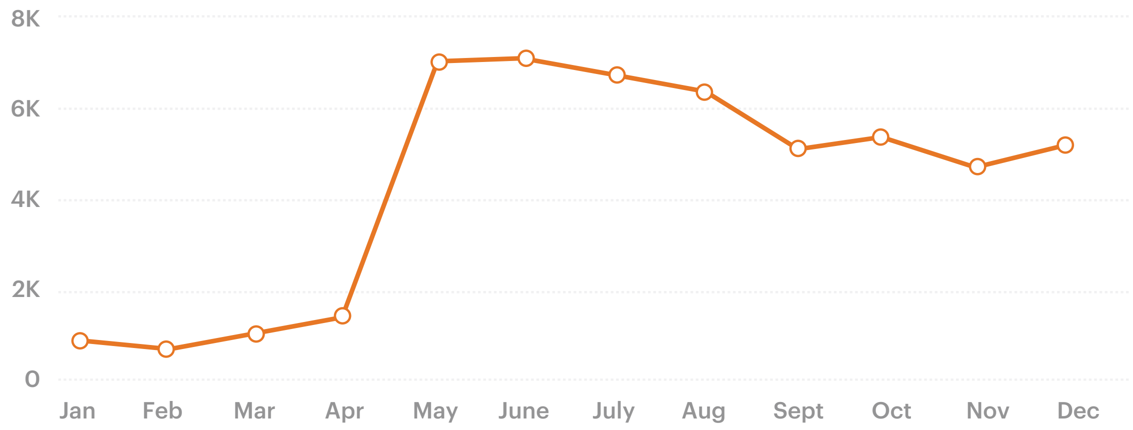
Despite that measured decrease, stalkerware-type detections remained considerably higher at the end of December than the detections recorded in January. When comparing the month of January to the month of December, monitor app detections increased by 565 percent, and spyware app detections increased by 1,055 percent.

+780%

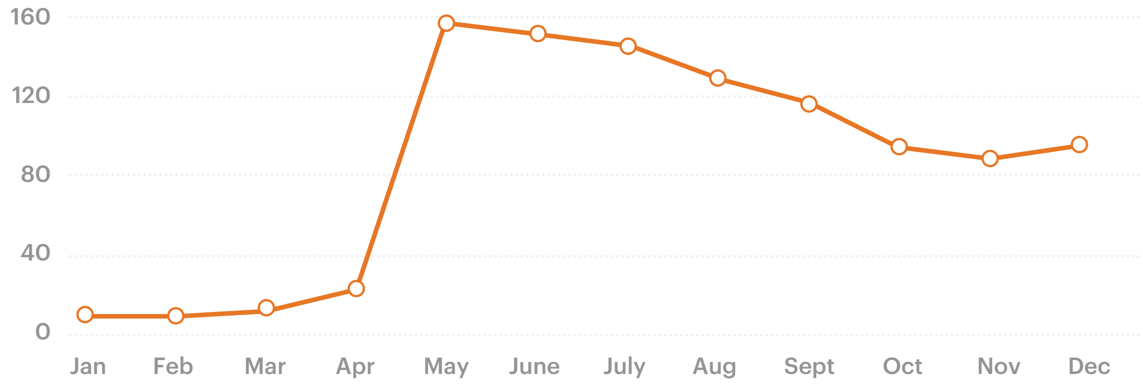
+1,677%

From Jan. 1 to June 30 2020, Monitor detections rose 780%, and Spyware detections rose 1,677%.

Monitor app detections on Android in 2020



Spyware app detections on Android in 2020



Of course, the decline in detections from June to December does not mean that the problem is going away, though, and it’s clear that the threat of stalkerware-type apps continues. As we move into 2021, and as the pandemic continues, we see no reason for this threat to suddenly disappear.

Instead, we will continue to work to protect users against these threats, as we have for years.

A digital approach to coronavirus

In December 2020, countless Californians received the fulfilled promise of a better way to track the spread of coronavirus—state residents could now opt into a Bluetooth-tracking mechanism on either their Apple or Android phones that would inform them if they had come into close contact with an individual who had tested positive for COVID-19.

The program was the latest, broad attempt to manage public health with the aid of technology. It was hardly the first.

In early 2020, as the coronavirus moved about the world in a wildfire-like spread, international governments implemented their own approaches to contact tracing. Contact tracing is the public health detective work that builds a map of where infected patients went, who they visited, when they came into contact, and for how long. It is a critical tool in battling any widespread illness. With the aid of digital tracking, some governments thought, the coronavirus could better be protected against.

But, as many people began to understand, the measures taken by their own governments sometimes placed them in a difficult vice—give up their data privacy for only a minute chance of being better informed.

The methods of digital tracking varied greatly.

Singapore rolled out a voluntary mobile app to provide contact tracing. South Korea focused on tracking credit card transactions, and the country published information on who visited what restaurants and bars and at what time they visited. In Moscow, the government promoted a mobile app that offered its users a sort of digital "passport" to be outside, allowing 30 minutes of approved outdoors time for, say, taking out the garbage, or 60 minutes for taking a walk around the neighborhood.

Other countries probed cell phone location data, with or without users' approval.

Israel shifted a once-secret surveillance program which was previously used for counter-terrorism measures to track the spread of COVID-19. In the Lombardy region of Italy, the government worked with a major telecommunications company to analyze reportedly anonymized cell phone location data to understand whether physical lockdown measures proved effective at fighting the virus. The Austrian government tried the same.

Similarly, the Pakistani government relied on provider-supplied location information to send targeted SMS messages to anyone who came into close, physical contact with confirmed coronavirus patients.

Finally, other countries released mobile apps.

As many people began to understand, the measures taken by their own governments sometimes placed them in a difficult vice—give up their data privacy for only a minute chance of being better informed.

Norway released an app that stored location data for 30 days on a centralized server. Colombia released an app that asked people to provide their data and, strangely, to answer questions about their participation at protests, and their ethnicity. And Argentina released an app which allowed for self-diagnosis but required people to include their National ID, email and phone number.

Before long, this deep digital tracking began to show cracks—both in privacy protection, and in societal impact.

In South Korea, where credit card transactions were tracked, the government disclosed an outbreak of 80 COVID-19 cases tied to one man. Because of the country's expansive surveillance mechanisms, the man could be traced to one night spent at five separate clubs in Seoul's gay district. Many in the LGBTQ community reportedly feared that their own credit card transactions at similar clubs would mandate them to be tested, which could then potentially out their sexuality to employers or colleagues.

Separately, the Dutch government held an open invitation for a contact tracing app this year; 750 proposals were submitted and not a single one was approved, due to privacy and security failings. Relatedly, a cybersecurity company called GuardSquare tested 17 contact tracing apps from 17 different countries and found common privacy failures in many.

As governments continued to implement digital measures to track the coronavirus, multiple digital rights advocates offered advice on what a responsible data collection infrastructure should require.

For example, Privacy International and more than 100 other, similar groups wrote that any government surveillance implemented to curb the spread of the coronavirus must be "necessary and proportionate," must only continue for as long as the pandemic, must only be used to respond to the pandemic, must account for potential discrimination caused by artificial intelligence technologies, and must allow individuals to challenge any data collection, aggregation, retention, and use, among other restrictions.

Before long, this deep digital tracking began to show cracks—both in privacy protection, and in societal impact.

As governments continued to implement digital measures to track the coronavirus, multiple digital rights advocates offered advice on what responsible data collection should require.

Nearly one year after the start of the pandemic, a small number of countries have emerged as leaders in public health, having limited the spread of COVID-19 to just dozens of individuals and then to nearly no persons at all.

One study that investigated the successes in fighting COVID-19 stressed the importance of digital tracking methods in Taiwan and New Zealand, but the study made it abundantly clear that digital tracking methods were not the cure-all to defeating the virus. Instead, a robust public infrastructure that worked in tandem to provide contact tracing, along with a fast, coordinated response and effective methods for quarantining and isolation, all played a role. Also of high priority, said the researchers, was "mass mask use."

Small legislative gains

Compared to 2018 and 2019, the legislative appeal for a US data privacy rehaul slowed down. Far fewer bills were introduced at the Federal level, and one of the only tech-focused bills to actually gain approval from the US Senate focused on improving the cybersecurity protocols for Internet of Things devices purchased by government agencies.

In California, though, one intrepid data privacy advocate utilized the state's ballot proposition procedure to get his law passed not through the state legislature, but through the voting booth. On November 4, Californians voted in favor of Proposition 24, which will amend California's current data privacy law, the California Consumer Privacy Act (CCPA).

Proposition 24's amendments to the CCPA include the creation of a new category of "sensitive personal information," which includes Californians' precise geolocation data, information revealing racial or ethnic origin, religious or philosophical beliefs, or union membership, email and text message content, genetic data, and biometric information that is specifically collected and analyzed "for the purpose of uniquely identifying a customer."

Interestingly, several organizations that typically favor stronger data privacy laws rallied against Proposition 24. Many shared the same worry that Proposition 24 expands the CCPA's current allowance for "pay-for-privacy" schemes, in which the public can be penalized for asserting their data privacy rights. Proposition 24's carveout is small on paper, as it only applies to stores operating "loyalty clubs," but according to American Civil Liberties Union's opposition, any opportunity to amend the CCPA should close known loopholes, not make more exceptions for them.

One study that investigated the successes in fighting COVID-19 stressed the importance of digital tracking methods in Taiwan and New Zealand.

The opposition proved ineffective though. Californians voted in favor of Proposition 24, with a 56.2 percent-43.8 percent split.

Away from local politics, one Senator introduced a data privacy bill that tried to move beyond the current consent model in the US, in which consumers are nearly forced into agreeing to data collection and sharing in exchange for using online platforms.

The Data Accountability and Transparency Act would do away with the complex, hundred-page legal forms that users are expected to read—but likely never do—when signing up for an online service.

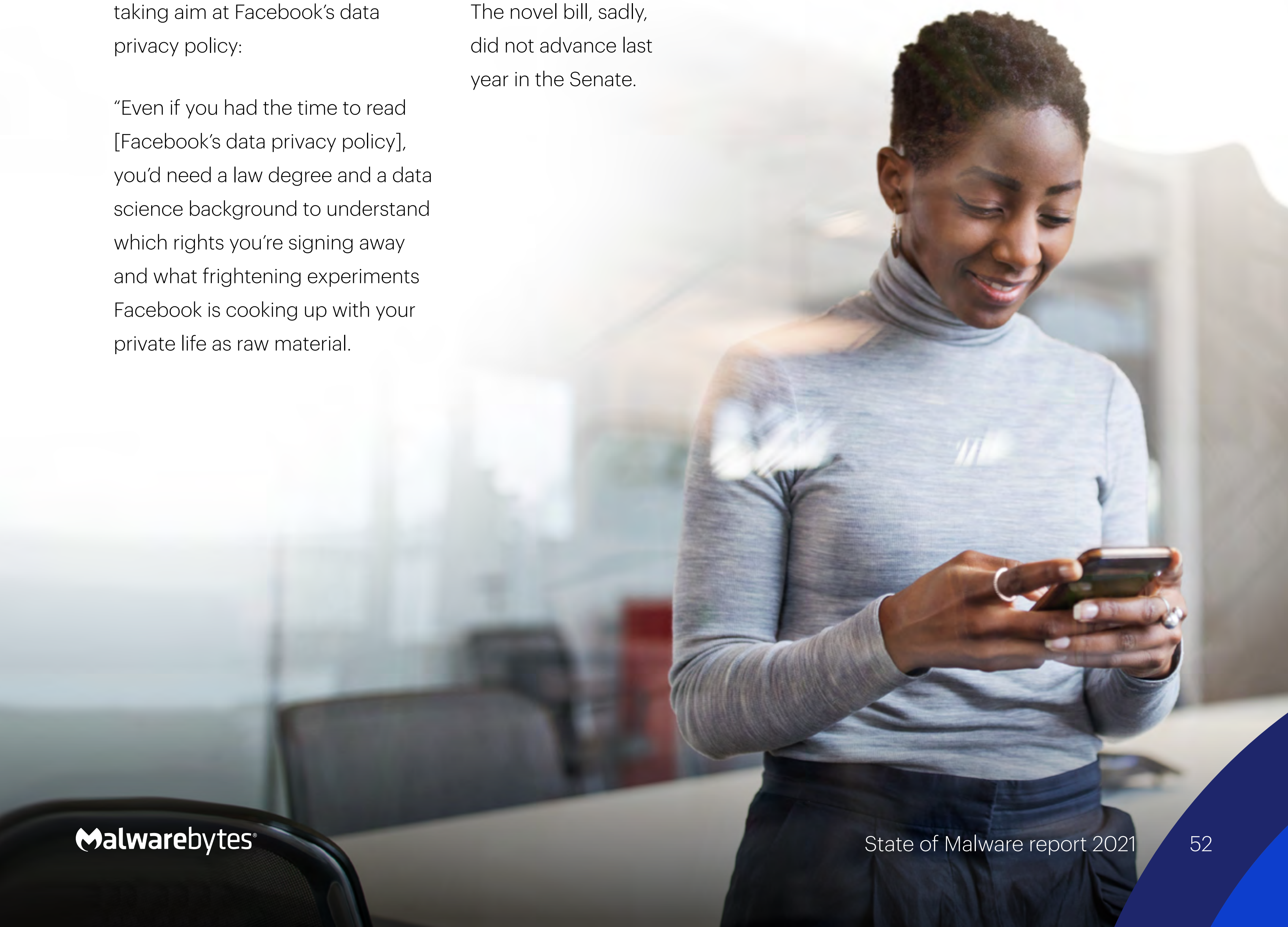
The bill's sponsor, Democratic US Senator Sherrod Brown of Ohio, explained this unfairness in a piece he wrote for Wired, specifically taking aim at Facebook's data privacy policy:

"Even if you had the time to read [Facebook's data privacy policy], you'd need a law degree and a data science background to understand which rights you're signing away and what frightening experiments Facebook is cooking up with your private life as raw material. And even if you do have handfuls of advanced degrees and a superhuman ability to read the hundreds of privacy policies you agree to every year, clicking No isn't a realistic option when you depend on the service. So most of us click Yes and agree to sign away our information, because our credit cards, mortgages, car loans, bank accounts, health apps, smart phones, and email accounts all require us to. It's simply the price of admission.

Privacy is a civil right. But corporations force you to sign it away every day."

The novel bill, sadly, did not advance last year in the Senate.

> **"Privacy is a civil right. But corporations force you to sign it away every day."**
>
> **– US Senator Sherrod Brown of Ohio**

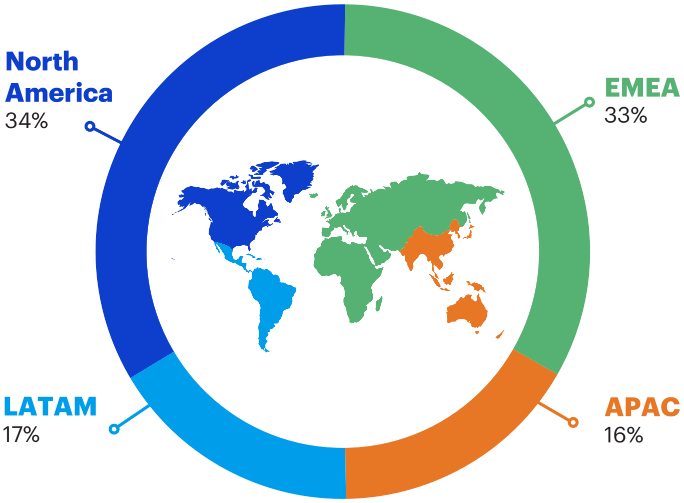


8 | Regional breakdown of threats in 2020

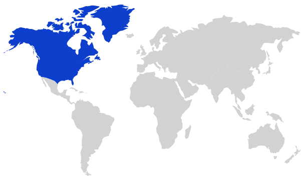
Even though the Internet and cybercrime are more or less without boundaries—aside from the countries that run a state firewall—there are always some regional differences.

These are caused by different factors like the behavior of potential victims, the interests of the criminals, and themes specific for particular regions or countries. For example, we typically see more banking Trojans in Latin America, and a higher use of exploit kits in Asia.

The stats below show the total number of detections by Malwarebytes for all of 2020. We've filtered out PUPs as well as those that are strictly Adware, and then constructed a top five for both consumer and business categories.



Regional detection breakdown 2020



North America

Overall detections in 2020 compared to 2019

2019	2020	% Change
71,241,542	40,937,130	-43%

Consumer threat detections

	Threats	2020
1	KMS	1,834,619
2	BitCoinMiner	1,738,121
3	Genieo	1,234,163
4	Dridex	904,134
5	TechSupportScam	767,845

Business threat detections

	Threats	2020
1	BitCoinMiner	1,311,164
2	KMS	319,752
3	Dridex	223,203
4	TechSupportScam	191,312
5	InfoStealer	168.386

EMEA

Overall detections in 2020 compared to 2019

2019	2020	% Change
43,719,941	40,045,057	-8%

Consumer threat detections

	Threats	2020
1	KMS	4,212,939
2	BitCoinMiner	2,049,179
3	Dropper	556,051
4	GameHack	407,299
5	Genieo	323,626

Business threat detections

	Threats	2020
1	KMS	605,221
2	BitCoinMiner	441,047
3	Dridex	130,569
4	Farfli	121,407
5	SecurityRun	78,726

LATAM

Overall detections in 2020 compared to 2019

2019	2020	% Change
22,355,541	20,375,372	-9%

Consumer threat detections

	Threats	2020
1	KMS	3,065,182
2	Dropper	740,038
3	BitCoinMiner	625,483
4	VBCrypt	384,447
5	WinActivator	217,324

Business threat detections

	Threats	2020
1	KMS	523,025
2	BitCoinMiner	433,299
3	Injector	61,401
4	Dropper	43,350
5	Dridex	40,733

Asia Pacific

Overall detections in 2020 compared to 2019

2019	2020	% Change
30,979,088	19,880,257	-36%

Consumer threat detections

	Threats	2020
1	KMS	1,479,875
2	BitCoinMiner	903,461
3	Glupteba	417,348
4	Dropper	392,619
5	RemoteExec	184,193

Business threat detections

	Threats	2020
1	BitCoinMiner	414,881
2	KMS	227,447
3	RemoteExec	145,728
4	Glupteba	73,066
5	Vools	69,664

Asia Pacific

Without Singapore, Australia or New Zealand

Overall detections in 2020 compared to 2019

2019	2020	% Change
28,342,311	17,469,089	-38%

Consumer threat detections

	Threats	2020
1	KMS	1,277,315
2	BitCoinMiner	760,158
3	Glupteba	410,970
4	Dropper	374,190
5	RemoteExec	184,189

Business threat detections

	Threats	2020
1	BitCoinMiner	312,340
2	KMS	207,930
3	RemoteExec	145,713
4	Glupteba	72,756
5	Vools	59,620

Australia & New Zealand

Overall detections in 2020 compared to 2019

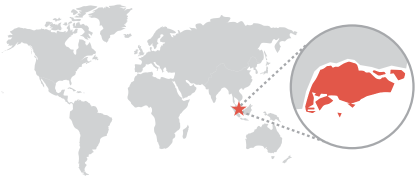
2019	2020	% Change
2,227,704	1,979,592	-11%

Consumer threat detections

	Threats	2020
1	KMS	177,153
2	BitCoinMiner	105,920
3	Genieo	59,148
4	ProxyGate	22,075
5	Vsearch	19,684

Business threat detections

	Threats	2020
1	BitCoinMiner	74,260
2	KMS	17,559
3	Passview	3,869
4	Genieo	3,212
5	Trickbot	2,086



Singapore

Overall detections in 2020 compared to 2019

2019	2020	% Change
409,073	431,576	▨ 6%

Consumer threat detections

	Threats	2020
1	BitCoinMiner	37,383
2	KMS	25,407
3	VBCrypt	5,225
4	Dropper	4,031
5	GameHack	3,560

Business threat detections

	Threats	2020
1	BitCoinMiner	28,281
2	KMS	1,958
3	PasswordStealer	1,500
4	Emotet	1,292
5	Trickbot	1,198

Let's talk about some of the numbers that jumped out at us. The KMS detections are software that's designed to use Microsoft applications without a bought-and-paid-for registration key. This type of software has always been popular with consumers, but in 2020 we saw it in the business stats almost across the board.

In North America and APAC, we saw more Bitcoin miners than KMS detections on business computers. Bitcoin miners have been on the rise, which seems likely to continue so long as the value of Bitcoin and other cryptocurrencies increases.

The regional differences get bigger when we look lower in the top five charts. For the most dominant Trojans, we see Dridex rank high in North America, typical reconnaissance malware show up in EMEA, and information stealers amassing many detections in APAC.

There's been another trend in 2020 that doesn't show up in the stats, or it might be better to say that it stands out by being absent.

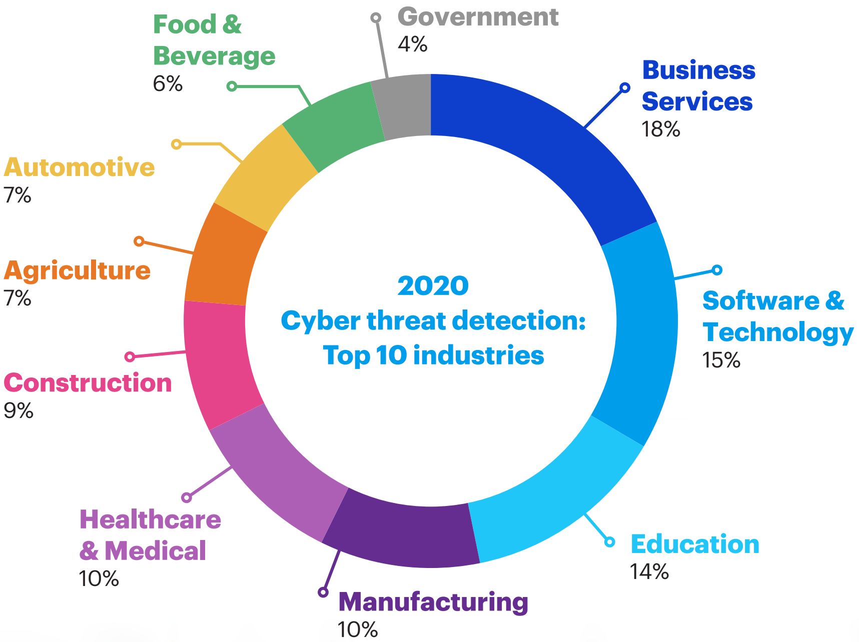
Ransomware became more targeted in 2020, so despite not registering the highest detection numbers, it was still a type of threat to reckon with in every region. There is some indication for this trend if you look at the tools that cyberattackers use to gain and expand their foothold on a network, such as Dropper and RemoteExec. These tools are often used in the initial stages of a ransomware attack or data breach.

9 | Industry threat landscape 2020

Comparing 2019 and 2020 reveals a volatile, shifting situation where some industries experienced big decreases in detections while others suffered spikes in attacks.

The pandemic has likely contributed to swinging figures, as malware developers react to the surge in WFH and potential relocation of primary targets. It's also possible that industries which may not be able to relocate as easily as more standard office work, have become more attractive propositions for hackers seeking out organizations that are still on-site.

When we reviewed the data, we found that the industries that represented the highest share of overall detections in 2020 include business services (18 percent), software and technology (15 percent), and education, which weighed in at 14 percent.



Top 10 industry sectors by detections in 2020 compared to 2019

	Industry	2019	2020	% Change
1	Business services	33,077	42,688	-29%
2	Software & technology	23,648	35,320	49%
3	Education	37,548	31,315	-17%
4	Manufacturing	46,137	24,225	-47%
5	Healthcare & medical	30,884	23,993	-22%
6	Construction	20,519	20,232	-1%
7	Agriculture	2,238	15,815	607%
8	Automotive	18,949	15,605	-18%
9	Food & beverage	8,839	14,790	67%
10	Government	11,352	9,388	-17%

While agriculture may "only" be sitting at 7%, in terms of detection numbers it has experienced something of a sea change. Namely, an increase of 607% from 2019

Further, while agriculture may "only" be sitting at 7 percent, in terms of detection numbers it has experienced something of a sea change. Namely, an increase of 607 percent, soaring from 2,238 detections in 2019 to 15,605 detections in 2020. Tech support scams were non-existent in this industry throughout 2019, with zero detections until November, when we detected around 100 attacks.

In 2020, these scams were scattered throughout the entire year with regular attacks hitting every month, amounting to 499 detections recorded for the whole of 2020 versus the 100 we saw in 2019. In fact, tech support scams were the most commonly used form of attack in this sector for 2020, despite solid numbers for IFEOHijack (a method for intercepting calls to one executable and triggering another instead) which tallied 362 detections in 2020 with a strong showing in May and June. In 2019, it didn't even appear on the radar for this industry.

This could indicate that threat actors were trying new methods to compromise the sector during lockdown, and the sudden emergence of tech support scams could be attackers thinking remote workers are more isolated and therefore more vulnerable to social engineering attempts.

Food and beverage, another essential pandemic service, saw a dramatic increase in attacks. Although this industry was not attacked as often as some others (it accounted for just 6 percent of the attacks in our top ten), attacks rose by 67 percent in 2020. That's 8,839 detections in 2019 versus 14,790 in 2020. With easy availability of food and drink being crucial, it's no surprise attackers gravitated toward the industry. As with agriculture, tech support scams barely featured in this industry in 2019 with 210 cases, versus 1,555 in 2020.

More traditional targets, such as manufacturing, healthcare and medical, and automotive all dropped in detections by varying degrees. Education fell by 17 percent in 2020 versus 2019, healthcare dropped 22 percent, and the automotive industry decreased by 18 percent. With so many forced to home school and (depending on the region) not so many people on the roads, it makes sense those would go down. It's also perhaps possible some groups happy to target medical services in the past found it to be a bridge too far during a global pandemic.

This isn't mere assumption—in March, the news outlet BleepingComputer contacted several ransomware groups to ask about whether they would refrain from targeting hospitals as the coronavirus spread across nearly every country in the world. Several groups responded yes. Unfortunately, that good faith flashed away.

On March 18, the operators behind Maze ransomware issued a press release saying they would not pursue any "activity" against "all kinds of medical organizations until the stabilization of the situation with virus."

By March 23, a medical facility working on the coronavirus vaccine was hit with a Maze ransomware attack.

Looking back at our data for 2020, it makes sense that scammers would strengthen interest in the software and technology industry considering the explosion of WFH and the endless array of tools required for remote work. Detections shot up 49 percent (35,320 detections in 2020 versus 23,648 in 2019), with business services being the biggest slice of detections in 2020 despite a drop of 29 percent from 2019.

Manufacturing experienced a drop of 47 percent, with detections falling from 46,137 in 2019 to 24,225 in 2020. As with so many other industries, tech support scams went from practically nothing to 1,820 detections in 2020 spread throughout the year.

Trickbot reigned supreme in the government vertical in 2019 with 4,122 detections and Emotet achieved a close second with 2,978 detections. In 2020, overall government detections dropped 17 percent from 11,352 to 9,388 and, once more, tech support scams came from nowhere to hit second place with 862 detections across the year. (First place went to Infostealers, with 995 detections.)

It makes sense that scammers would strengthen interest in the software and technology industry considering the explosion of WFH and the endless array of tools required for remote work.

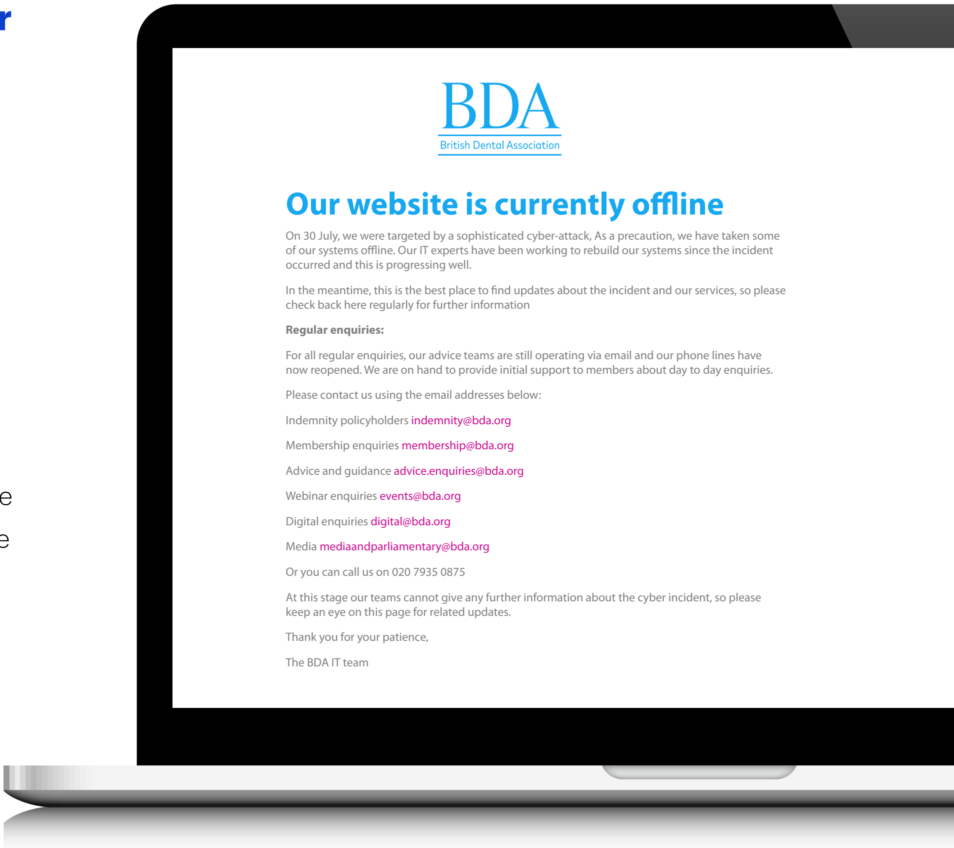
Everywhere you look, tech support scams are back, making it one of the most notable changes to the threat landscape in 2020. However you look at it, the human aspect of furthering attacks into organizations and supply chains is back with a vengeance.

Malware in the dentistry sector

The dentistry sector—which accounts for 5 percent of all ransomware-affected entities in healthcare—has suffered its fair share of online attacks, compromises, and stolen data since at least early 2016.

In August, the BBC reported that the British Dental Association (BDA), the trade union organization for dentists in the UK, confirmed that it had been a victim of a cyberattack. The data breach affected not just UK dentists whose personal data and email correspondences were stolen and leaked online—but also some of the personal details of their patients.

After discovering the breach, the BDA took its website offline to "lower the risk of malware for the cyber incident."



BDA
British Dental Association

Our website is currently offline

On 30 July, we were targeted by a sophisticated cyber-attack, As a precaution, we have taken some of our systems offline. Our IT experts have been working to rebuild our systems since the incident occurred and this is progressing well.

In the meantime, this is the best place to find updates about the incident and our services, so please check back here regularly for further information

Regular enquiries:

For all regular enquiries, our advice teams are still operating via email and our phone lines have now reopened. We are on hand to provide initial support to members about day to day enquiries.

Please contact us using the email addresses below:

Indemnity policyholders indemnity@bda.org

Membership enquiries membership@bda.org

Advice and guidance advice.enquiries@bda.org

Webinar enquiries events@bda.org

Digital enquiries digital@bda.org

Media mediaandparliamentary@bda.org

Or you can call us on 020 7935 0875

At this stage our teams cannot give any further information about the cyber incident, so please keep an eye on this page for related updates.

Thank you for your patience,

The BDA IT team

After discovering the breach, the BDA took its website offline to "lower the risk of malware for the cyber incident"

While some practices exhibit a firm awareness level on how to respond in the event of an attack against their systems, some have yet to catch up. The types of best practices that some organizations may have perfected are not so easily within reach of others, including effectively detecting compromises within their network, the proper procedures of reporting to the authorities, and the delicate process of notifying those affected by such cyberattacks.

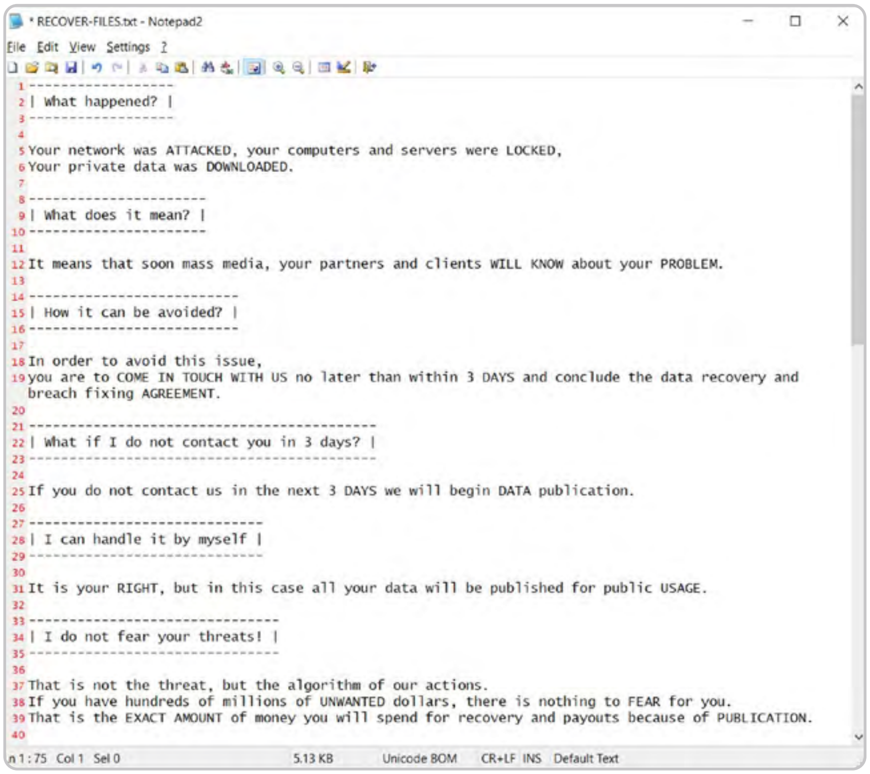
Dyras Dental, a Michigan-based practice, was found to be remiss at notifying its patients about a ransomware attack that compromised and exfiltrated its data. The news of its breach only came to light when DataBreaches.Net, an independent breach reporting website that has been around since 2009, reached out to the dental practice in late September 2020 to let it know it had become a victim of Egregor ransomware.

DataBreaches.Net was able to get a copy of the data dump released by the Egregor threat actors, which was available on both the public Internet and the dark web. Most of the data files appeared to be from Dyras Dental's Dentrix system, and contained employee and patient data, as well as business records.

Malware in the grocery/ supermarket sector

Scams, point-of-sale (PoS) malware, retailer site flaws, and phishing are all cyberattacks that are typically associated with the grocery industry. They are cited as potential causes of massive data breaches and data compromise in general. But now, we can add one more to this roster: ransomware.

Case in point: In mid-November, Cencosud, a Chilean-based multinational retail company and one of the biggest in Latin America, was hit by Egregor ransomware. The Clarín, an Argentinian publisher, further reported that printers in affected retail shops started printing out the ransom note.



```
------------------
| What happened? |
------------------

Your network was ATTACKED, your computers and servers were LOCKED,
Your private data was DOWNLOADED.

----------------------
| What does it mean? |
----------------------

It means that soon mass media, your partners and clients WILL KNOW about your PROBLEM.

--------------------------
| How it can be avoided? |
--------------------------

In order to avoid this issue,
you are to COME IN TOUCH WITH US no later than within 3 DAYS and conclude the data recovery and
breach fixing AGREEMENT.

-------------------------------------------
| What if I do not contact you in 3 days? |
-------------------------------------------

If you do not contact us in the next 3 DAYS we will begin DATA publication.

-----------------------------
| I can handle it by myself |
-----------------------------

It is your RIGHT, but in this case all your data will be published for public USAGE.

-------------------------------
| I do not fear your threats! |
-------------------------------

That is not the threat, but the algorithm of our actions.
If you have hundreds of millions of UNWANTED dollars, there is nothing to FEAR for you.
That is the EXACT AMOUNT of money you will spend for recovery and payouts because of PUBLICATION.
```

The ransom note used in the Cencosud attack

Since COVID-19 ushered us into the pandemic age in the first quarter of 2020, some threat actors have notably increased their attacks on essential businesses, such as healthcare and supply chains, as they recognize how valuable these businesses are. With many shoppers favoring going online, as well as brick-and-mortar shops and retailers pivoting to online sales, cybercriminals have become more tactical and quite sophisticated.

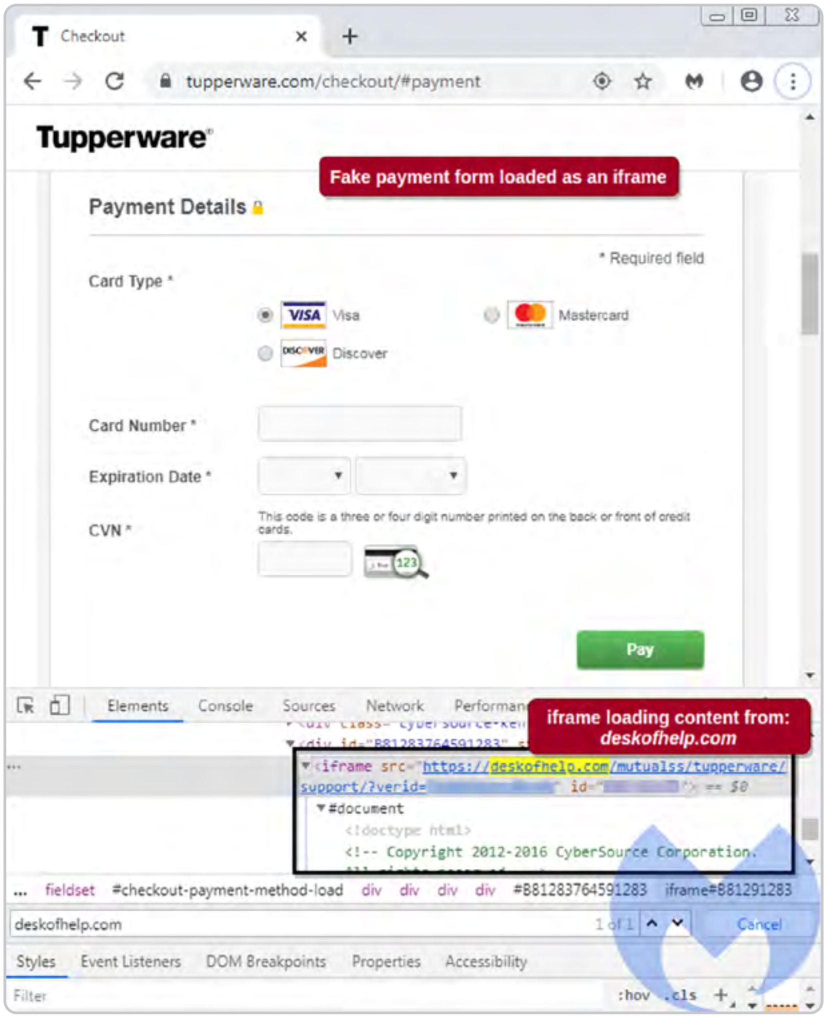
Web skimmers

First showing up in 2016, Magecart is a criminal group widely known for its use of web skimmers, a piece of malicious code that is introduced in web payment pages so cybercriminals can skim card details from shoppers without them knowing. In March 2020, when countries around the world first implemented shelter-in-place and lockdown procedures, online skimming increased by 26 percent.

Web skimmers have been found in both small-sized and enterprise-level websites that allow internet users to shop from their official pages. Tupperware's website, for example, was compromised and found to be hosting a web skimmer in March. Malwarebytes researchers, who were among the first to find this web skimmer, noted that there was "a fair amount of work put into the Tupperware compromise to integrate the credit card skimmer seamlessly and stay undetected for as long as possible."

The Magecart gang is also found to use impersonation tricks as another way to hide their payload. In this case, they made their skimmer appear to be Rocket Loader, a Cloudflare feature that improves the load time of web pages.

The huge successes of Magecart, and possibly other groups who use web skimmers, can probably be attributed to the end of life of Magento 1.x, the version of the open-source ecommerce platform for SMBs first introduced in 2008. This means that developers will no longer support, patch, or provide quality fixes to Magento 1, giving criminals another reason to exploit it, and consequently victimize more organizations who have yet to update to its newest version.



```
▾<iframe src="https://deskofhelp.com/mutualss/tupperware/support/?verid=[redacted]" id="[redacted]"> == $0
  ▾#document
    <!doctype html>
    <!-- Copyright 2012-2016 CyberSource Corporation.
... fieldset #checkout-payment-method-load div div div div #B81283764591283 iframe#B81291283
deskofhelp.com
```

The rogue iframe expertly placed on the compromised payment page of Tupperware's website

10 | Conclusion

2020 was a year of tragedy, upheaval, and adaptation. People and organizations adapted, but so did the cybercriminals who preyed upon them.

Their tactics and targets may have changed but their intentions did not. The amount of Windows malware aimed at businesses decreased, but it wasn't a show of clemency. It was simply a sign that its operators had learned they could do more damage with less.

Data exfiltration became a mainstream tactic for ransomware gangs in 2020, and even made an appearance in a piece of rare Mac malware. The business model of choice for most criminals targeting Apple and Android operating systems remained Adware, though.

But the most unsettling change of behaviour we saw was in the use of Spyware. As the world locked down in April 2020, a tool that was once the preserve of nation states and cybercriminals became something otherwise ordinary people used on each other.

As 2021 begins and the pandemic still rages, more change seems likely, but one trend seems set in stone—the world of work has changed forever. By spring 2021, vast numbers of businesses will have spent an entire year operating remotely. Some, maybe many, will never return to the old ways of working. So, as we enter the new year, it's time to abandon old ideas about security, and long-outdated thoughts of impenetrable corporate perimeters. If the future of work is flexible, adaptable and remote, then the future of security must be too.

By spring 2021, vast numbers of businesses will have spent an entire year operating remotely. Some, maybe many, will never return to the old ways of working.

Contributors

Adam Kujawa
Director of Malwarebytes Labs

Jerome Segura
Director of Threat Intelligence

Thomas Reed
Director of Mac and Mobile

Nathan Collier
Senior Malware Intelligence Analyst, Mobile

JP Taggart
Senior Security Researcher

Hossein Jazi
Senior Threat Intelligence Analyst

Anna Brading
Editor-in-Chief, Malwarebytes Labs

Mark Stockley
Editor-in-Chief, Malwarebytes Labs

David Ruiz
Senior Threat Content Writer, Malwarebytes Labs

Jovi Umawing
Senior Threat Content Writer, Malwarebytes Labs

Chris Boyd
Senior Threat Intelligence Analyst, Malwarebytes Labs

Pieter Arntz
Senior Threat Intelligence Analyst, Malwarebytes Labs

Malwarebytes®

Malwarebytes Inc.

3979 Freedom Circle, 12th Floor

Santa Clara, CA 95054

USA

+1-800-520-2796