Malwarebytes LABS

PRESENTS

2020 State of Malware Report

February 2020

Table of contents

Table of contents

Malware**bytes**

Executive summary

Global Windows malware detections increased by 13% on business endpoints

Rise in pre-installed malware and adware on Android devices

For the first time ever, Macs outpaced Windows PCs in number of threats detected per endpoint

It was the last year of the 2010s, and cybercriminals let the world know they meant business. From an increase in enterprise-focused threats to diversification of sophisticated hacking, evasion, and stealth techniques to aggressive adware aimed at Androids, the 2019 threat landscape was shaped by a cybercrime industry that was all grown up.

While Malwarebytes observed a relative plateau in the overall volume of threat detections in 2019, our telemetry showed a clear trend toward industrialization. Global Windows malware detections on business endpoints increased by 13 percent, and a bifurcation of attack techniques split threat categories neatly between those targeting consumers and those affecting organizations' networks. The Trojan-turned-botnets Emotet and TrickBot made a return in 2019 to terrorize organizations alongside new ransomware families, such as Ryuk, Sodinokibi, and Phobos. In addition, a flood of hack tools and registry key disablers made a splashy debut in our top detections, a reflection of the greater sophistication used by today's business-focused attackers.

Meanwhile, the 2019 mobile threat landscape fared no better. While Malwarebytes launched a massive drive to combat stalkerware—apps that enable users to monitor their partners' every digital move—which led to an increase in our detections, other nefarious threats lingered on the horizon, with increases in their detections not being helped along by our own research efforts. We observed a rise in pre-installed malware and adware on the devices of our Android customers, with the goal to either steal data or steal attention.

In fact, adware reigned supreme for consumers and businesses on Windows, Mac, and Android devices, pulling ever more aggressive techniques for serving

Malwarebytes

up advertisements, hijacking browsers, redirecting web traffic, and proving stubbornly difficult to uninstall. And for the first time ever, Macs outpaced Windows PCs in number of threats detected per endpoint. Even exploits, malvertising, and web skimmers had a banner year. Outside of cryptominers and leftover WannaCry infections, it seemed there were few cybercrime tactics being outright abandoned or on the decline.

With an increase in impact and reach, then, came an increase in public awareness and scrutiny. And in no area was this more apparent than data privacy. On the heels of the Global Data Privacy Regulation (GDPR) in Europe and several public social media failures, a tsunami of data privacy legislation, proposals, fines, controversies, and public policies came forward in 2019. **After a decade marked by seemingly hundreds of high-profile data breaches, the fallout from all that personally identifiable information (PII) floating around on the dark web finally arrived.**

Methodology

The State of Malware report features data sets collected from product telemetry, honey pots, intelligence, and other research conducted by Malwarebytes threat analysts and reporters from January 1 through December 31, 2019. Data from the previous year is used to demonstrate year-over-year change.

Our telemetry is derived from Malwarebytes customers, both consumer and business, limited to only real-time detections from active, professional, and premium accounts. This selection reduces outlier data that may skew trends. For example, a user installing Malwarebytes for the first time may have hundreds or thousands of detections from existing infections that weren't actively spread during the timeframe of our study. These detections could then muddy data on the distribution or prominence of a particular threat.

In addition, we focus on named threats rather than generic detections gathered by heuristics (i.e. anomalous behavior detections), as they provide little-to-no intelligence value. To that end, the numbers presented in this report represent a percentage of our total collected telemetry, however, this percentage tells the most accurate story about the global threat landscape in 2019.

Key takeaways

› There's been an increasing move over the last two years to organizations over consumers. Overall consumer threat detections are down by 2 percent from 2018, but business detections increased by 13 percent in 2019. This resulted in a mere 1 percent increase in threat volume year-over-year.

› The sophistication of threat capabilities in 2019 increased, with many using exploits, credential-stealing tools, and multi-stage attacks involving mass infections of a target. While seven of 10 top consumer threat categories decreased in volume, HackTools—a threat category for tools used to hack into systems and computers—increased against consumers by 42 percent year-over-year, bolstered by families such as MimiKatz, which also targeted businesses.

› Organizations were once again hammered with Emotet and TrickBot in 2019, two Trojan families that started out as simple bankers/info-stealers then evolved into downloaders and botnets. This was reflected in global business detections, as well as regional and vertical-focused telemetry, where TrickBot and Emotet surfaced in the top five threats for nearly every region of the globe, and in top threat detections for the services, retail, and education industries. Emotet was Malwarebytes' overall second most-detected threat against organizations, increasing by 6 percent over 2018. However, TrickBot's growth in 2019 has been much greater than Emotet's. At fourth place in our top business detections, TrickBot rose by 52 percent from last year.

› Ransomware detections have slightly declined from 2018, however, this is due to a lower rate of WannaCry detections leftover from 2017. Net new ransomware activity against organizations remains higher than we've ever seen before, with families such as Ryuk, Phobos, and Sodinokibi making waves against cities, schools, and hospitals. In fact, Ryuk detections

increased by 543 percent over Q4 2018, and since its introduction in May 2019, detections of Sodinokibi have increased by 820 percent.

› Adware has become much more aggressive in 2019, heavily targeting consumer and business endpoints on Windows, Mac, and Android devices. A new team of the most active adware families have replaced the top adware family detections of 2018. In total, we saw approximately 24 million Windows adware detections and 30 million Mac detections. The top three consumer threat detections belonged to adware families and the number one business detection was also adware. The number one Mac detection, an adware family called NewTab, brought in 28 million detections itself.

› We saw a significant rise in the overall prevalence of Mac threats in 2019, with an increase of over 400 percent from 2018. However, part of that increase can be attributed to an increase in our Malwarebytes for Mac userbase. To see if that increase reflects the reality of the Mac threat landscape, we examined threats per endpoint on both Macs and Windows PCs. In 2019, we detected an average of 11 threats per Mac endpoint—nearly double the average of 5.8 threats per endpoint on Windows.

› Of the four global regions, North America (NORAM) was responsible for 48 percent of our detections, with Europe, the Middle East, and Africa (EMEA) in second place at 26 percent. Latin America (LATAM) and Asia Pacific (APAC) brought up the rear, with 14 and 12

percent, respectively. Two regions saw decreases in overall threats: EMEA detections dropped by 2 percent and APAC, outside of Australia, New Zealand, and Singapore, decreased by 11 percent. In Australia and New Zealand, the dip was more prominent at 14 percent. North America was at the receiving end of more than 24 million threats, up 10 percent from 2018. But LATAM saw the most growth in 2019, up to 7.2 million detections, an increase of 26 percent.

❯ On the web threats front, a shift by browser developers to rely more on the Chromium platform gave us concern for the discovery and development of new exploits against today and tomorrow's browser applications, and not just for the aging and dwindling Internet Explorer. Meanwhile, web skimmer activity was at an all-time high in 2019, with groups like MageCart aggressively modifying payment processor sites to steal financial information without the need for malware to be installed on the endpoint.

❯ Finally, data privacy was heavy on the public mind in 2019, post-GDPR. Several new pieces of legislation were passed in the United States, including laws in Maine, Nevada, and California that may serve as the backbone for future federal regulation. In addition, tech companies such as Apple, Malwarebytes, ProtonMail, and Mozilla launched privacy-forward products in 2019, including tracking blockers, tracking-free browsers, and encrypted calendar tools. On the flip side, many privacy blunders were made by tech juggernauts, such as Google, Amazon, and Facebook, who shipped products with secret microphone features and vulnerabilities enabling customer data to be viewed by employees, sold user data to third-party companies without express permission, and committed other manhandlings of user PII. While the companies publicly pledged to do better on privacy, their revenue models are largely dependent on advertising dollars—meaning user data is their most valuable asset.

Windows threat landscape 2019

Global detections 2018-2019			
	2018	**2019**	**% Change**
Overall	50,170,502	50,510,960	**1%**
Business	8,498,934	9,599,305	**13%**
Consumer	41,671,568	40,911,655	**-2%**

Figure 1. Total number of consumer and business detections in 2019 vs. 2018

Welcome to 2020, stats fans! It's time for us to observe the 2019 threat landscape through the rearview mirror and take note of the interesting developments that happened throughout the year. To begin, we'll examine the total number of business and consumer detections in 2019 compared with 2018.

According to our product telemetry, overall detections of malware have increased year-over-year by only 1 percent, from 50,170,502 to 50,510,960. However, when we separate business and consumer detections, we can see that while consumer threats declined by 2 percent, business detections increased by nearly 1 million, or 13 percent, from 2018 to 2019.

The volume of consumer detections still far outweighs that of businesses, but this trend has been reversing since 2018, when many threat actors began to shift focus to development of malware families and campaigns aimed at organizations where they could profit from larger payouts.

Consumer threat categories

To get a sense of the types of malware consumers across the globe faced in 2019, we first looked at the top threat categories detected on endpoints running Malwarebytes Premium.

Adware is once again the dominant threat category for consumers, as it was in 2018. Detections of adware remained steady throughout the year, with just a slight dip during the summer months. We expect to see adware detections holding on strong for consumers through 2020.

Trojan activity, however, has been on the decline for consumers for most of the year, slipping in volume by 7 percent from 2018. As Trojan families such as Emotet moved away from targeting consumers, we saw the

## Top 10 consumer category detections 2019
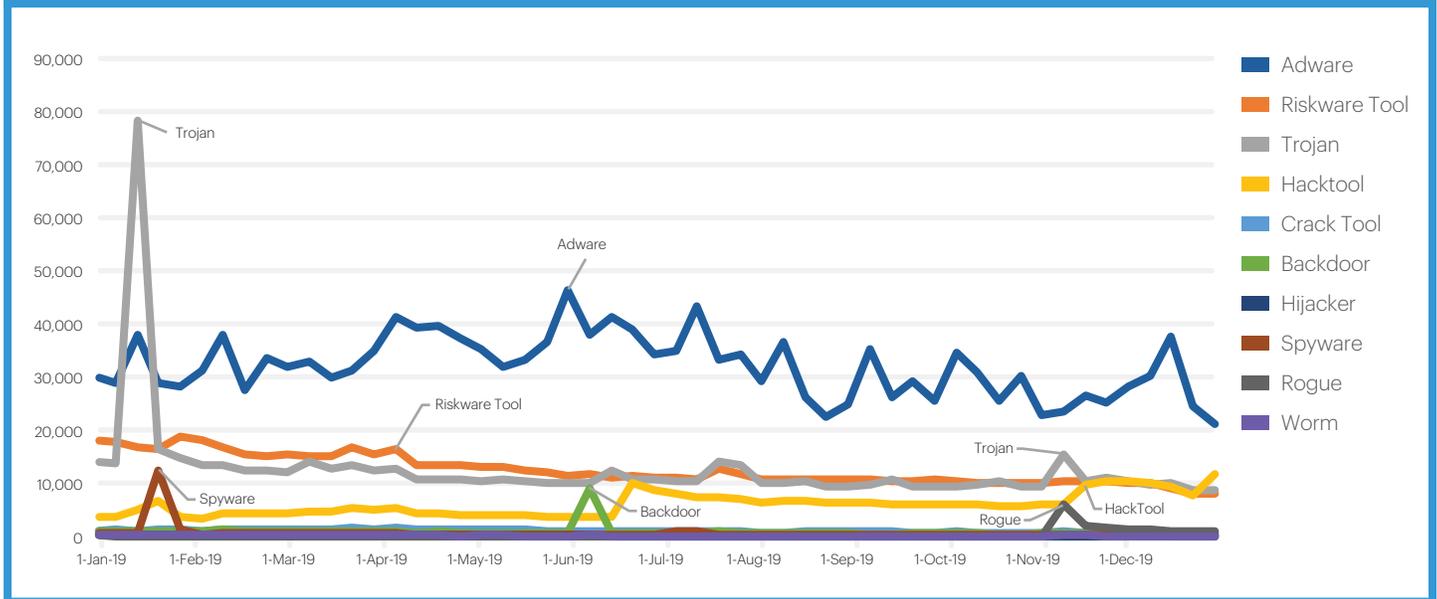
Figure 2. Top 10 consumer threat categories in 2019

overall category drop as a result. In fact, the dramatic spike in Trojan detections at the beginning of the year was due to an Emotet campaign, but we saw no other such drastic increases in Trojan activity against consumers this year. We expect to see Trojan malware continue to be a problem for consumers in 2020, but less so than other threats, and especially less than in previous years.

Meanwhile, riskware (detected as RiskwareTools), which contains most of our cryptominer detections, has been on a steady downward slope, with 4 million fewer detections in 2019 than in 2018—a 35 percent decrease. It's been more than two years since the "CryptoRush" first enamored cybercriminals with dreams of striking it rich via GPU, and reality has begun to sink in. While fluctuations of both cryptocurrency value and spikes of miner detections are common, threat actors are recognizing that the return on investment opportunities for cryptomining have mostly dried up—for now.

While the decline in riskware is one of the most statistically significant decreases (alongside a steep

73 percent dive in hijacker detections), it follows the same pattern as seven of the top 10 consumer threat categories: diminishing importance. Cybercriminals are losing interest in consumer targets, at least by way of the usual threat suspects. Trojans, cryptominers, ransomware, hijackers, backdoors, worms, and more are either being reserved for organizations or ditched altogether.

On the flip side, one threat category saw a surge in 2019 consumer detections: hack tools (detected as HackTools). Increasing by 42 percent over 2018, hack tools moved up in the rankings from fifth to fourth place with nearly 1 million more detections. Hack tools are a category of threats that are frequently used for hacking into a computer or network. These tools may not be malicious themselves, but they are capable of additional intrusion, data collection, and dropping other malware payloads. The sharp increase in hack tools detections on consumer endpoints is concerning, and we'll be keeping a close watch on this category in early 2020 and beyond.

Malwarebytes

Top 10 global consumer categories 2018-2019

	Category	2018	2019	% Change
1	Adware	14,261,896	16,917,174	**13%**
2	Trojan	7,161,012	6,637,893	**-7%**
3	RiskwareTool	10,215,837	6,632,817	**-35%**
4	HackTool	2,319,847	3,287,326	**42%**
5	CrackTool	843,986	641,142	**-24%**
6	Backdoor	601,658	577,679	**-4%**
7	Spyware	448,026	465,284	**4%**
8	Rogue	309,823	270,493	**-13%**
9	Hijacker	745,742	201,785	**-73%**
10	Worm	273,801	196,332	**-28%**

Figure 3. Top 10 consumer threat category rankings

Business threat categories

Moving on to telemetry gathered from organizations running Malwarebytes business products, we saw a greater amount of diversity in threat types and distribution than on the consumer side.

While normally a constant thorn in the side of consumers, adware detections spiked for organizations during the first half of the year, dropping to a manageable level by early summer. Adware was thrown out of the top spot at various periods of the year by

Trojans, backdoors, and riskware, but remained our number one threat category for businesses overall, increasing by 463 percent over its 2018 levels.

Trojan malware, meanwhile, slipped to the second-highest category of business detections in 2019, dethroned from its first-place ranking in 2018. Trojan threats decreased by 25 percent this year, dropping significantly in May and never recovering to its Q1 and Q2 levels. Despite this dip, we still saw 2.8 million detections of Trojan malware in 2019.

## Top 10 business category detections 2018-2019
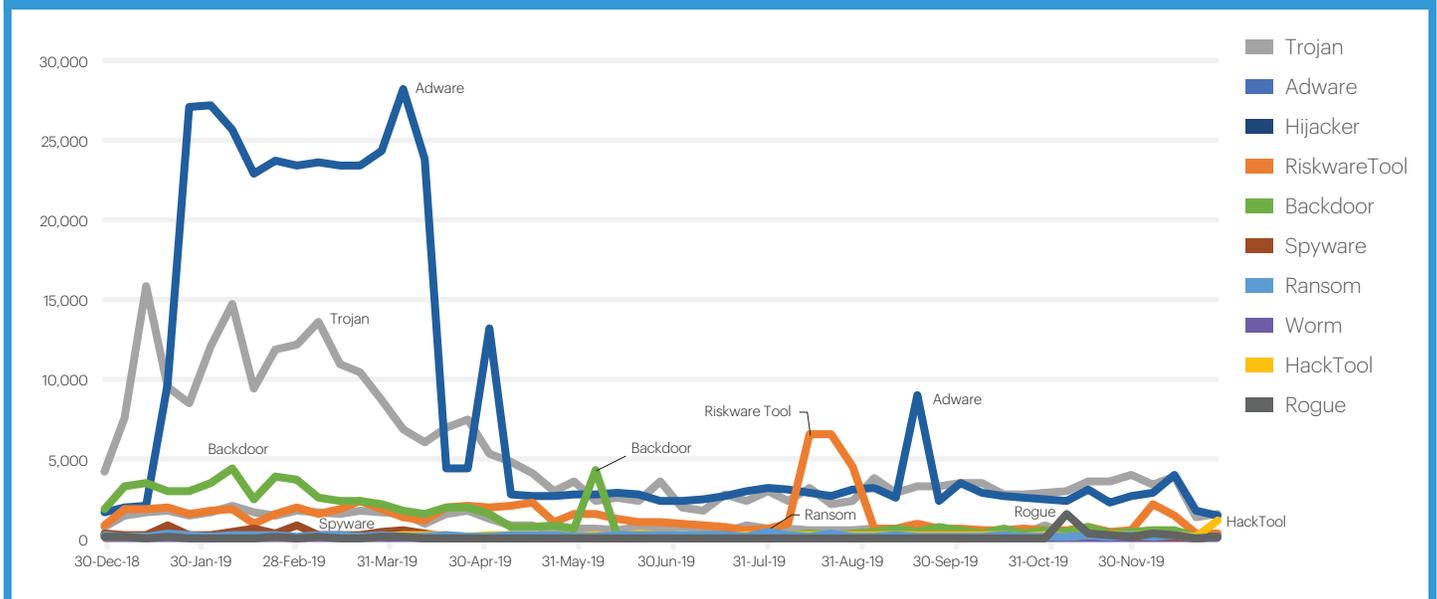
Figure 4. Top 10 business threat categories in 2019

We've observed a heavy volume of backdoor malware aimed at organizations over the years, thanks to families like Vools. This year, backdoor detections increased by 14 percent for organizations. However, the rate of infection declined throughout 2019, starting off the year stronger than ending it.

Meanwhile, riskware detections on business endpoints increased by 52 percent this year, a striking difference from the 35 percent decline on the consumer side. This tells us that threat actors are trying to squeeze the last juice out of the crypto-lemon, looking for higher returns on investment by targeting businesses with fatter crypto wallets or more endpoints to generate CPU.

The 224 percent increase in hack tools detections reinforces what we already know about an attack vector gaining in popularity with cybercriminals—the manual infection of business networks through misconfigured ports or unpatched vulnerabilities. There are also many families of malware, like Mimikatz, that use hacker tools as part of their regular operations, and this probably

contributed to the category's rise through the rankings from position 10 in 2018 to 7 in 2019. In fact, business detections of hack tools more than tripled in number this year. Combining both consumer and business data, there were over 1 million more hack tools detections in 2019 than in 2018. It's clear this threat category meant business.

And then there's the omnipresent ransomware. Despite being dwarfed by other threat categories in volume, ransomware detections in 2019 were both noticeable and concerning. Many of the most high-profile cyberattacks of the year involved ransomware, so we're none too surprised to see it poking its head through the pile of adware and Trojan detections. Year-over-year volume of ransomware detections declined by 6 percent, but the numbers don't tell the full story. The ransomware families most popular with threat actors in 2019 were far more advanced than what we saw in 2018 and the years before.

Top 10 global business categories 2018-2019

	Category	2018	2019	% Change
1	Adware	771,006	4,337,987	**463%**
2	Trojan	3,745,473	2,809,198	**-25%**
3	RiskwareTool	514,020	780,154	**52%**
4	Backdoor	591,903	672,495	**14%**
5	Hijacker	2,259,644	470,878	**-79%**
6	Spyware	246,156	110,805	**-55%**
7	Hacktool	31,835	103,102	**224%**
8	Ransom	101,624	95,523	**-6%**
9	Rogue	61,195	49,504	**-19%**
10	Worm	113,149	44,552	**-61%**

Figure 5. Top 10 business threat category rankings

Consumer threat families

Switching gears to discuss specific families of malware, which live under the umbrella of threat categories, we have identifed the top 10 families that plagued consumers over the last year.

Much of the top threats dealt with by consumers in 2019 were some form of adware. Adware is the perfect type of threat to attack a consumer. Rather than investing in sophisticated forms of malware that can infiltrate entire networks or ransom files, cybercriminals choose inexpensive adware to assist in social engineering tricks, technical support scams, page redirections, or system hijacks meant to sell something to users, inflate views of ads, or scam people out of their money.

Adware families took seven of the top 10 spots, with SearchEncrypt, IronCore, FusionCore, CrossRider, and Spigot joining the list for the first time in 2019. Mindspark and InstallCore are two adware mainstays that experienced 497 and 367 percent increases in 2019, respectively. SearchEncrypt saw an astounding 1,730 percent increase year-over-year. Even if the family didn't make our top 10 for global consumer detections, many other adware families are living large in specific regions and against businesses.

Malwarebytes

Other notable changes include a 375 percent increase of Emotet infections in 2019, which is likely due to an especially active campaign launched at the beginning of the year. In addition, BitCoinMiner detections dropped by 46 percent, which follows the slow decline of the riskware category we witnessed throughout the year.

Top 10 global consumer families 2018-2019

	Threat family	2018	2019	% Change
1	Adware.MindSpark	318,447	1,901,539	**497%**
2	Adware.InstallCore	348,705	1,626,722	**367%**
3	Adware.SearchEncrypt	59,383	1,086,446	**1730%**
4	RiskWare.BitCoinminer	1,380,981	7,403,066	**-46%**
5	Trojan.Emotet	154,941	736,335	**375%**
6	Adware.IronCore	220,221	661,883	**201%**
7	HackTool.FilePatch	615,910	551,861	**-10%**
8	Adware.FusionCore	100,718	516,644	**413%**
9	Adware.Crossrider	251,810	41,089	**64%**
10	Adware.Spigot	214,891	40,965	**88%**

Figure 6. Top 10 consumer threat family rankings

Business threat families

Business endpoints running Malwarebytes in 2019 detected and blocked an enormous number of threats, with several new families observed in the top 10 ranking—more than half of which experienced triple digit percentage increases in 2019. In fact, every single business threat family listed in the top 10 experienced growth this year, with the exception of a single family.

While the adware family Yontoo dropped out of consumer rankings this year, it's now the top threat lodged against businesses, increasing by more than 6,000 percent year-over-year—a clear sign that the threat actors pushing this family have an interest in business victims.

Malwarebytes

Top 10 global business families 2018-2019

	Threat family	2018	2019	% Change
1	Adware.Yontoo	48,922	3,022,523	**6069%**
2	Trojan.Emotet	708,009	750,193	**6%**
3	Hijack.SecurityRun	368,747	443,519	**20%**
4	Trojan.Trickbot	204,313	309,902	**52%**
5	Adware.Mindspark	25,224	182,935	**625%**
6	Trojan.BrowserAssistant.PowerShell	N/A	109,758	N/A
7	Adware.Sogou	26,835	108,381	**304%**
8	Adware.FusionCore	84,414	84,414	**550%**
9	Backdoor.Qbot	11,213	41,089	**465%**
10	Adware.Spigot	14,761	51,184	**247%**

Figure 7. Top 10 business threat family rankings

We saw the ever-popular Trojan Emotet land in our number two spot, having increased by a marginal 6 percent. Bringing up the rear as our fourth most-detected business threat family is TrickBot, another dangerous Trojan that experienced a 52 percent incline over the previous year. In 2018, TrickBot was most often seen pairing with other malware families, such as Emotet, acting as a secondary payload. In 2019, however, we saw a near steady flow of TrickBot detections, regardless if Emotet was active or not.

A fascinating and alarming family that made our top 10 business threats this year is the malware we detect as Trojan.BrowserAssistant.PowerShell. We observed over 100,000 instances of this threat, which is a massive

amount for a detection that didn't even exist in 2018. While known for pushing advertisements to users' browsers by injecting code, we can easily see this same method of infection being used to redirect users to drive-by exploits or phishing pages.

Finally, at number 9 on our list is the backdoor known as QBot or QakBot, a lesser known but nonetheless dangerous threat that increased by 465 percent this year. QBot has historically been known as a banking Trojan, meaning that it steals financial data from systems, but it has also been seen using PowerShell scripts to summon credential theft tools like Mimikatz to self-propagate.

Family deep dive

While we have seen a wide variety of threats throughout 2019, these next five families have had a significant impact on the Windows threat landscape. First, we'll talk about some old buddies of ours, Emotet and TrickBot. After a quick check-in with those chuckleheads, we'll delve into two ransomware families making waves: Ryuk and Sodinokibi. Finally, we'll take a look at a little-known but fairly crafty threat: a hijacker called SecurityRun.

Emotet

Nearly every report we've released over the last two years has mentioned the notorious Emotet Trojan. As much as it would be nice to say, "We're just fans," the reality is that we can't seem to get away from this malware family.
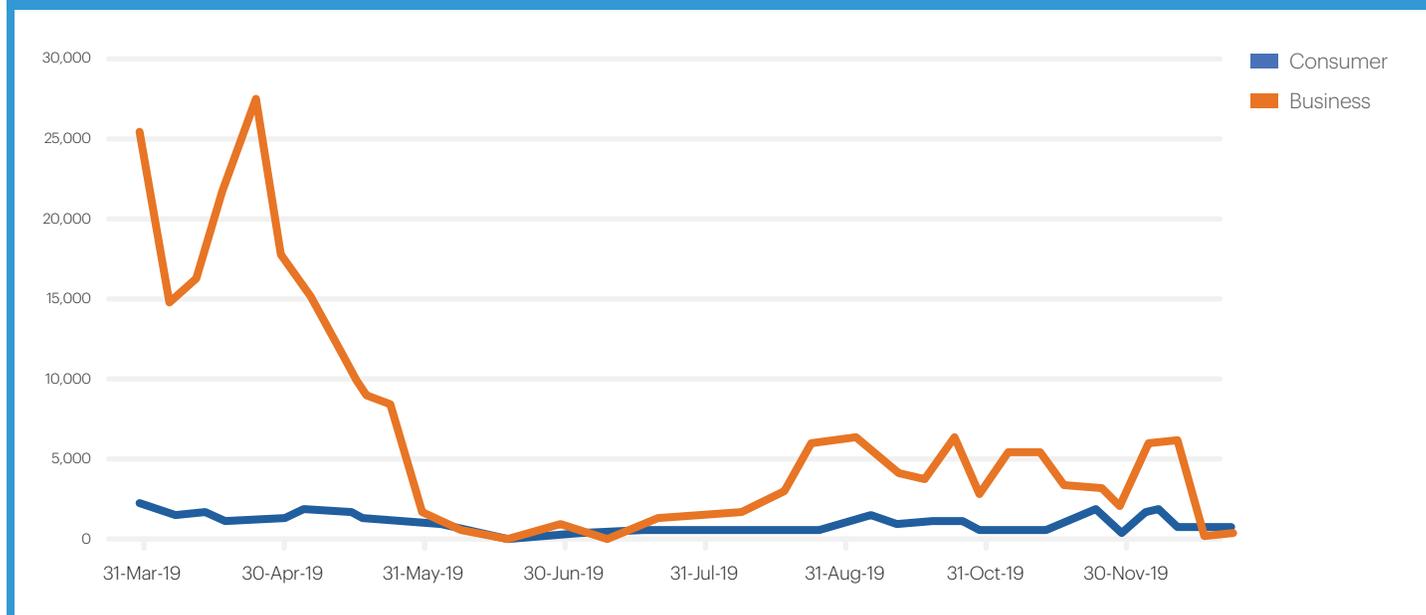
Figure 8. Emotet in the second half of 2019

In 2019, we observed an overall increase of 73 percent in Emotet detections (between both consumer and business customers), much of it coming from a massive campaign in early 2019. Figure 8 expresses the trend in Emotet detections from April to the end of the year, specifically so we can observe what happened after Emotet "went back to sleep" over the summer.

As we expected, Emotet picked back up its campaigns in the fall, targeting businesses over consumers and creating a niche for themselves in selling secondary

payload access to other criminals through their existing infections. The motivation of the actors behind Emotet seems to be expansion of their botnet and offerings to other threat actors.

Emotet seems to focus on Western countries as its primary target, however we've seen increases in Emotet detections all over the world in 2019, from Singapore to the United Arab Emirates to Mexico.

2019 Global Emotet detections by country

Philippines 0.26%

Brazil 0.29%

Australia 0.29%

France 0.29%

Argentina 0.45%

Mexico 0.96%

Canada 1.02%

Germany 1.23%

United Kingdom
23.63%

United States
71.58%
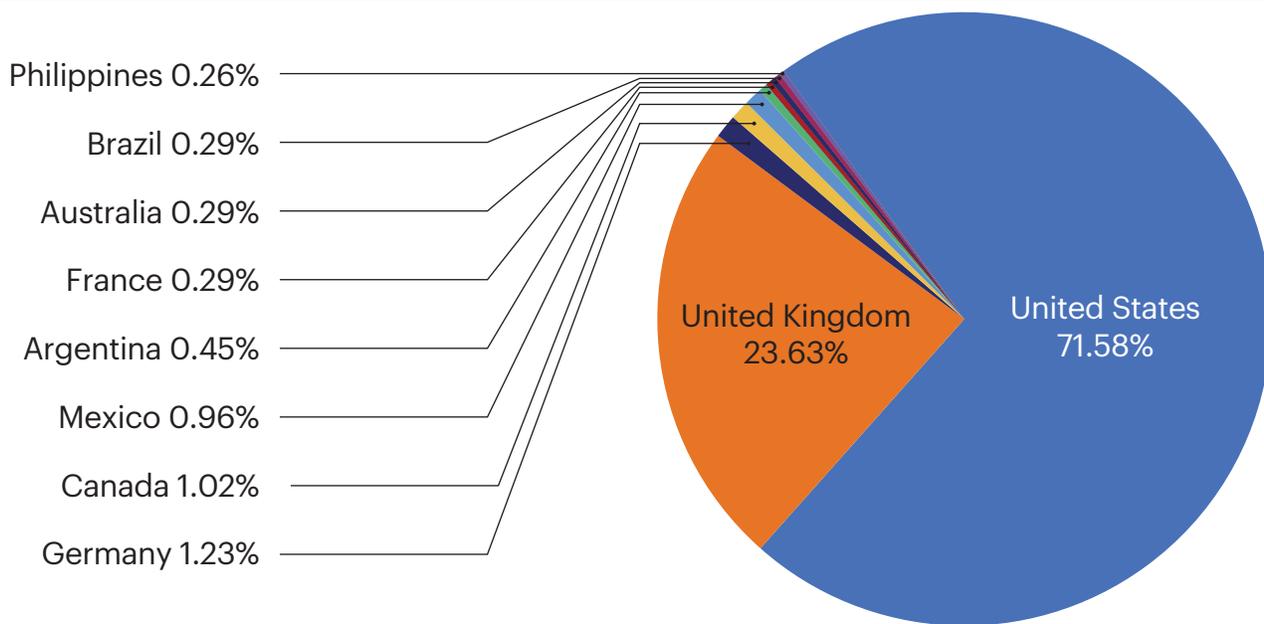
Figure 9. Emotet's top 10 national targets

Distribution of Emotet relies on malicious phishing emails spread by the malware and its controllers. In 2019, we observed campaigns pushing Emotet that used the names of controversial public figures to ensnare users into opening emails and malicious attachments. For example, Emotet was the "prize" for opening up attachments from the following phishes:

❱ Emails claiming they had Edward Snowden's new book, Permanent Record, as a Word attachment

❱ Emails with Word attachments urging users to "support Greta Thunberg," Time Magazine's Person of the Year

In addition, we saw Emotet emails delivered in a variety of languages, including English, Italian, Spanish, German, and French.

As you may remember, one of the capabilities of Emotet includes establishing an affected system as a spam sender. The malware scrapes the users' contacts and

sends out malspam similar to the phishes mentioned here, but further disguised as coming from the infected user.

Combine its spam module functions with frequently-seen secondary payloads of families that can move laterally throughout a network, such as Trickbot or QBot, and you've got the perfect toolkit for infecting an entire corporate network.

TrickBot

Speak of the devil. While mostly associated as a secondary payload for Emotet in the second half of 2018, TrickBot had a steady amount of detections throughout 2019, thanks in part to its own infection efforts.

In 2019, TrickBot was spread in multiple ways, including as a secondary payload, via connected, infected systems (typically, a corporate network), or through good old-fashioned phishing. To get into a corporate

Malwarebytes

Trickbot global activity 2019
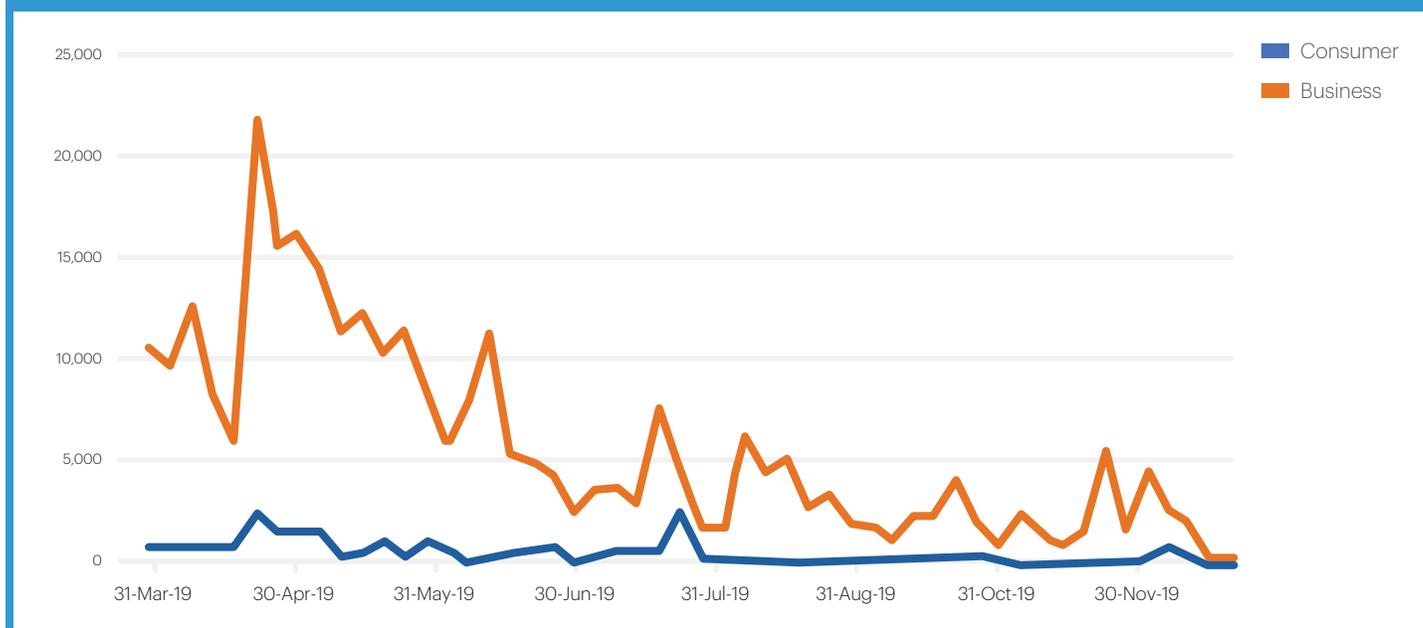
Figure 10. Consumer and business detections of TrickBot in 2019

network on its own, TrickBot harvests and brute-forces network credentials, using Eternal exploits (those stolen by Shadow Brokers from the NSA) to spread laterally through the network. In addition, TrickBot added a new feature to defeat multi-factor authentication, as well as its own spam module called TrickBooster, which was found to have compromised over 250 million accounts.

In 2019, we've observed TrickBot phishing emails disguised as:

❱ Scanned documents from a Xerox printer

❱ Legislation on tax bills

❱ Harassment complaints

Once on the network, besides stealing personally identifiable information from organizations and individuals, TrickBot was observed attempting to steal tax documents so the actors behind the malware could file fraudulent returns.

TrickBot's distribution is slightly more varied and widespread than that of Emotet, though the US and UK are still its top targets. The actors behind this family have made existing infections of TrickBot available to nation-state actors, as well as to other cybercriminals.

We find it interesting that both TrickBot and Emotet evolved from being regular banking Trojans to first-stage infection vendors and botnets. As much we we'd like to bid farewell to both of these families, our guess is we'll be seeing them again in 2020.

2019 Global TrickBot detections by country

Belgium 0.19%
India 0.19%
Italy 0.28%
Spain 0.34%
Australia 0.36%
Mexico 0.36%
Germany 1.27%
Canada 2.01%

United States
59.48%

United Kingdom
35.52%
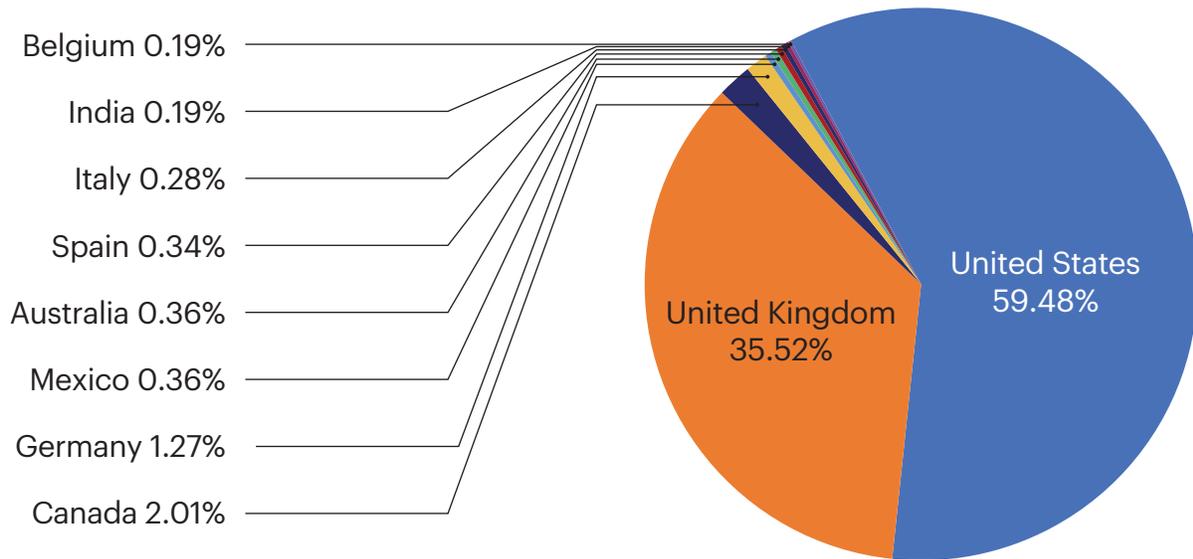
Figure 11. TrickBot national targets in 2019

Ryuk

These next two ransomware families didn't pull down the same numbers as their Trojan brothers, but the damage they caused made their impact in 2019 monumental. The days of seeing massive, year-long ransomware campaigns are over. Instead, ransomware attacks this year relied on more covert and specialized infection methods, such as existing infections of Emotet or TrickBot, to make their presence known.

Ransomware operations in 2019 haven't so much slowed down as their targeting has become more precise. Instead of spraying a wide cross-section of potential victims, ransomware authors sniped the most vulnerable rich targets they could find.

We'll start the story with Ryuk. First discovered in mid-August 2018, Ryuk immediately turned heads after disrupting operations of Tribune Publishing newspapers over the Christmas holiday heading into 2019. It was quarantined eventually; however, Ryuk re-infected and spread onto connected systems in the network because

the security patches failed to hold when tech teams brought the servers back. Detections of Ryuk increased by more than 500 percent in Q1 2019 over the previous quarter, and by Q4 2019, they were up another 43 percent.

There was a time when Ryuk ransomware arrived on clean systems to wreak havoc. But most strains observed in 2019, especially in the second half of the year, belonged to multi-attack campaigns involving Emotet and TrickBot. As such, Ryuk variants arrive on systems pre-infected with other malware—a "triple threat" attack methodology. Once threat actors confirm the systems they've infected with Emotet and TrickBot are in the correct sector, and that they've reached endpoints on which valuable assets are stored, they check for and establish a connection with the target's live servers via remote desktop protocol (RDP). From there, they drop Ryuk.

Ryuk had been seen targeting various enterprise organizations worldwide in 2019, asking ransom payments ranging from 15 to 50 Bitcoins (BTC), which

Ryuk ransomware business detections 2019
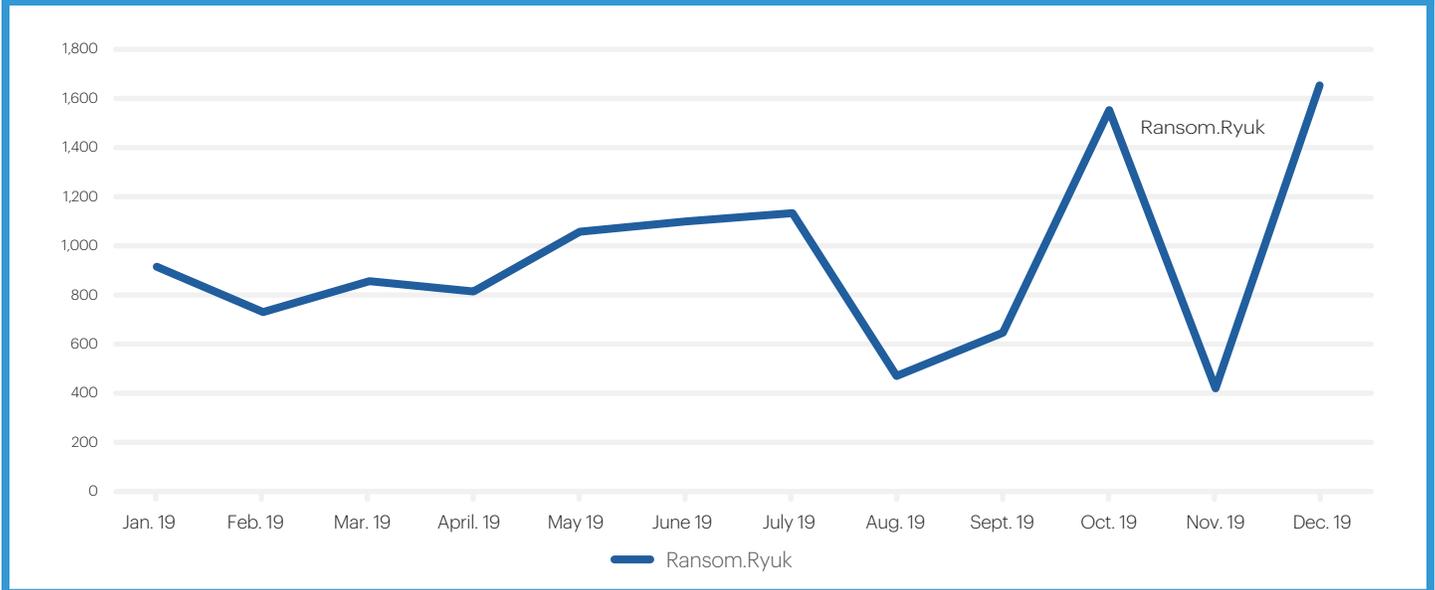
Figure 12. Ryuk detections on business endpoints in 2019

translates to between US$97,000 and $320,000 at time of valuation. This method of exclusively targeting large organizations with critical assets for a high ROI is called "big game hunting." To date, Ryuk ransomware is hailed as the costliest among its peers. According to a report by Coveware, Ryuk's asking price is 10 times the average, though they claim that their ransoms are highly negotiable. The varying ways adversaries work out ransom payments suggests that there may be more than one criminal group behind Ryuk ransomware. As detections spiked heading into 2020, we realized we'd be seeing more of this dangerous and expensive ransomware in the year to come.

Sodinokibi

Sodinokibi is a ransomware-as-a-service threat model that first appeared on the scene in May 2019, curiously congruent with the time that the infamous GandCrab's authors publicly called it quits. Our telemetry lends weight to the theories that Sodinokibi is actually run by GandCrab's authors, who many researchers say simply tweaked some of GandCrab's old features, gave it a new

name, and found new "affiliates" for distribution. Looking at the downturn in GandCrab detections at the end of May and subsequent spike in Sodinokibi detections in June, we'd be hard-pressed to argue otherwise.

Sodinokibi attack methods include:

❱ Active exploitation of a vulnerability in Oracle WebLogic, officially named CVE-2019-2725

❱ Malicious spam or phishing campaigns with links or attachments

❱ Malvertising campaigns that lead to the RIG exploit kit, an avenue that GandCrab used before

❱ Compromised or infiltrated managed service providers (MSPs) to push the ransomware en-masse. This is done by accessing networks via a remote desktop protocol (RDP) and then using the MSP console to deploy the ransomware.

❱ Evading detection through the "Heaven's Gate" technique used to execute 64-bit code on a 32-bit process, which allows malware to run

Top active ransomware family business detections 2019
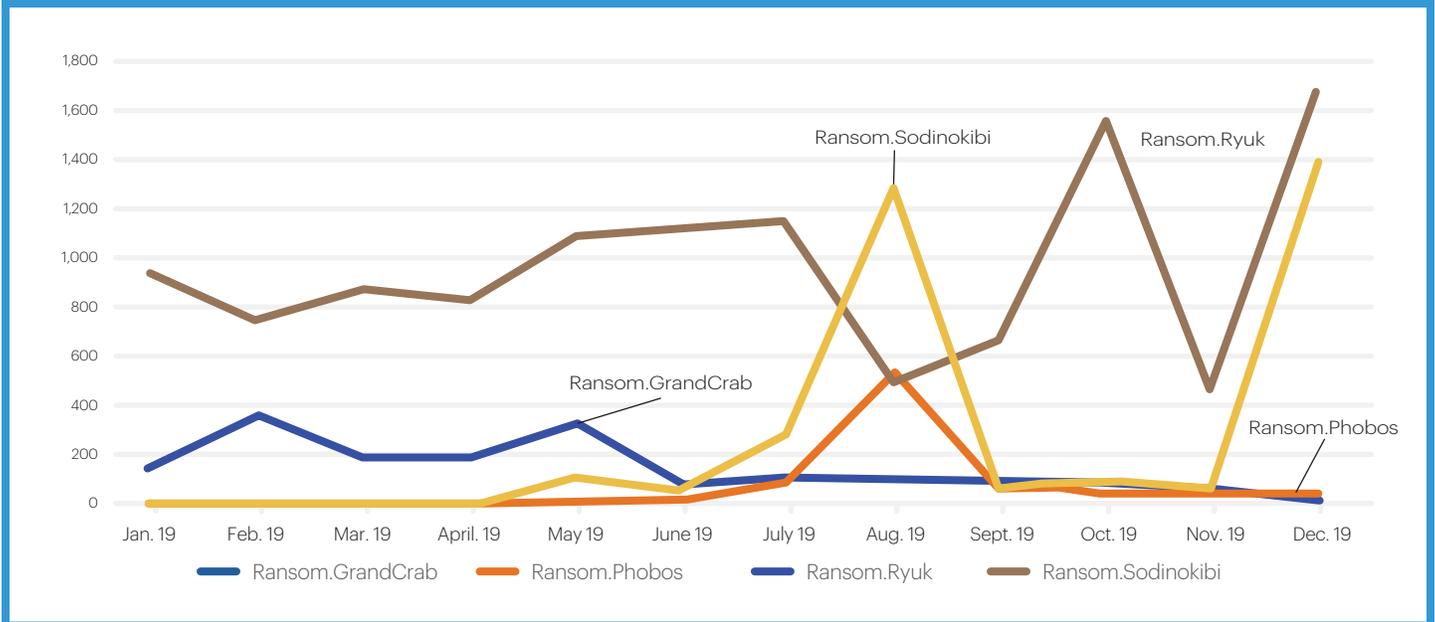
Figure 13. Sodinokibi spikes as GandCrab makes its exit

Although affiliates used many of these tactics to push GandCrab, many cybercriminals—nation-state actors included—have done the same to run their own malware campaigns.

Sodinokibi has shown to be nearly as much of a threat as Ryuk, with high spikes of detections that outweigh what

we've seen with other business-focused ransomware families in 2019, such as Phobos or SamSam. Since its introduction, detections of this family have increased by 820 percent, a foreboding number as we look ahead. We'll likely see both Ryuk and Sodinokibi as the primary families being distributed in the first half of 2020, heralding back to the days of Cerber and Locky.

Sodinokibi ransomware business detections 2019
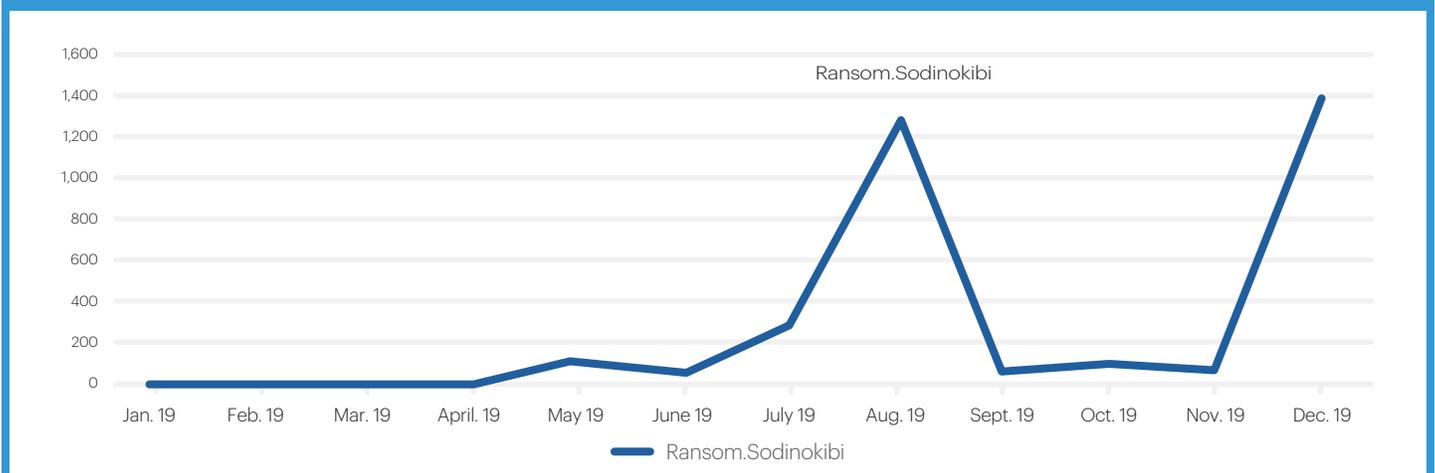
Figure 14. Detections of Sodinokibi on business endpoints in 2019

Malwarebytes

SecurityRun

In a world where malware doesn't merely exist to infect, but to disable security tools, it's no surprise we've seen an increase of threats attempting to do the latter in 2019. One of these threats is a hijacker known as SecurityRun.

This detection is simple: There is a registry key in your system that can be set to prevent certain applications

We thought it prudent to highlight this threat because it was able to achieve such high distribution almost exclusively against business victims.

Another interesting note about this threat: is It's overwhelmingly found in the United Kingdom.

Hijack.SecurityRun global activity 2019
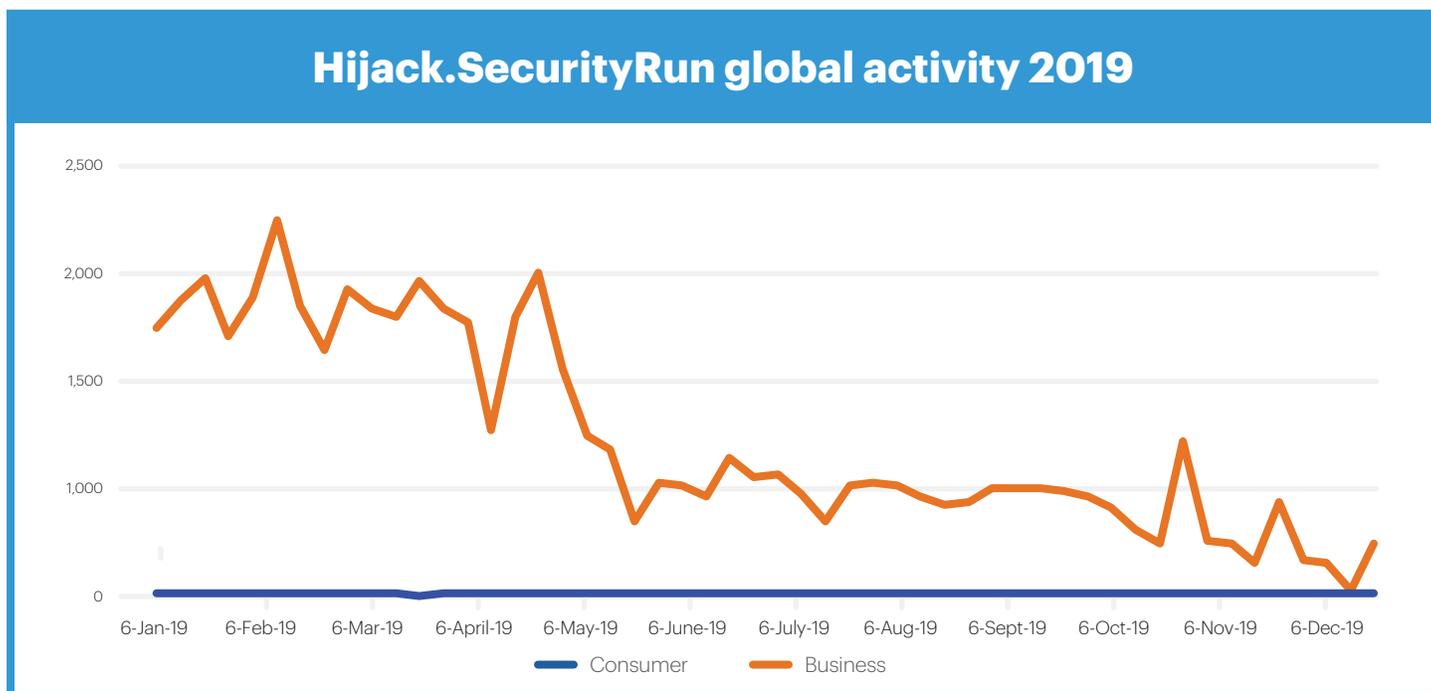
Figure 15. SecurityRun global detections in 2019

from running, including security software. If our product identifies one of these modifications and it wasn't made by the user, that means there's a high probability that the software disabling it doesn't want you running your security tools. Any program quietly disconnecting your security services without your knowledge is likely up to no good.

The registry key altered in this attack is:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\ Windows\safer\codeidentifiers\0\Paths

However, we started seeing an increase in US detections over the UK at the end of October 2019, meaning this threat may soon turn its focus westward. Regardless of the target, these modifications can be made manually by an attacker or automatically by malware, and their discovery should raise some alarms. Best to treat any system with SecurityRun detections as though it's likely been infected, and conduct further investigation.

Malwarebytes

2019 Global SecurityRun detections by country

Canada 0.09%

Brazil 0.12%

Ireland 0.17%

United Kingdom 16.69%
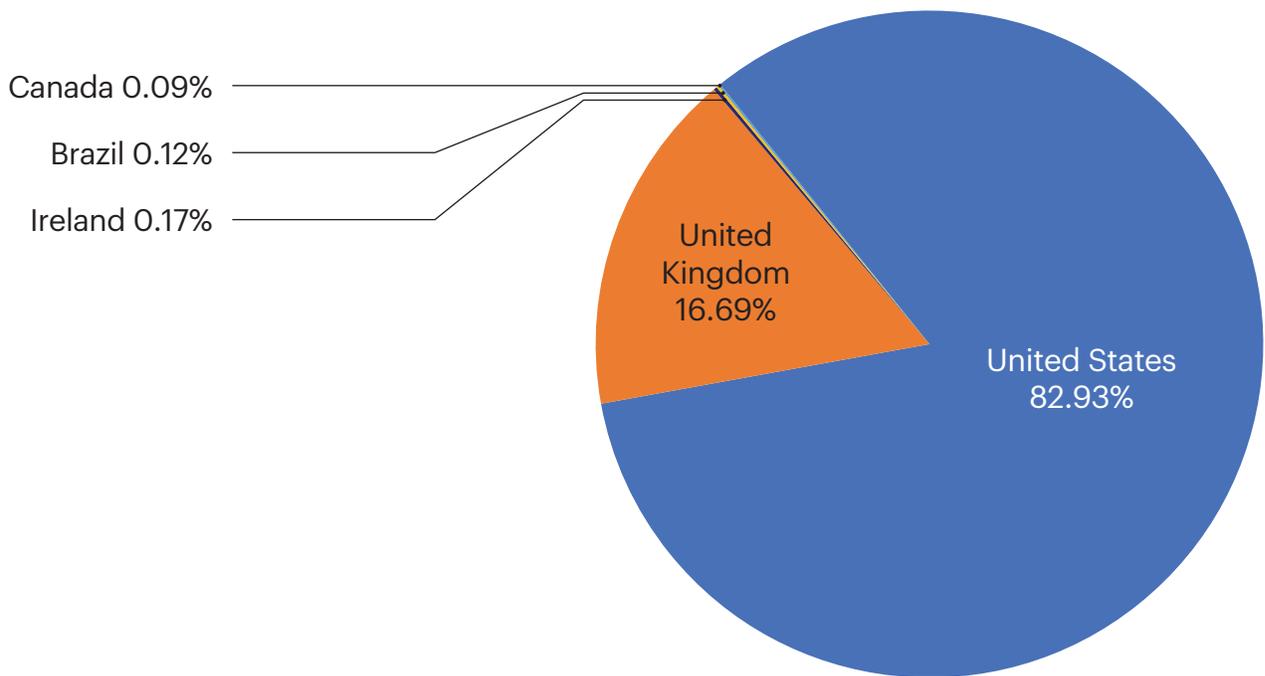
United States 82.93%

Figure 16. Countries targeted by SecurityRun in 2019

2019 US/UK SecurityRun detections

Consumer   Business
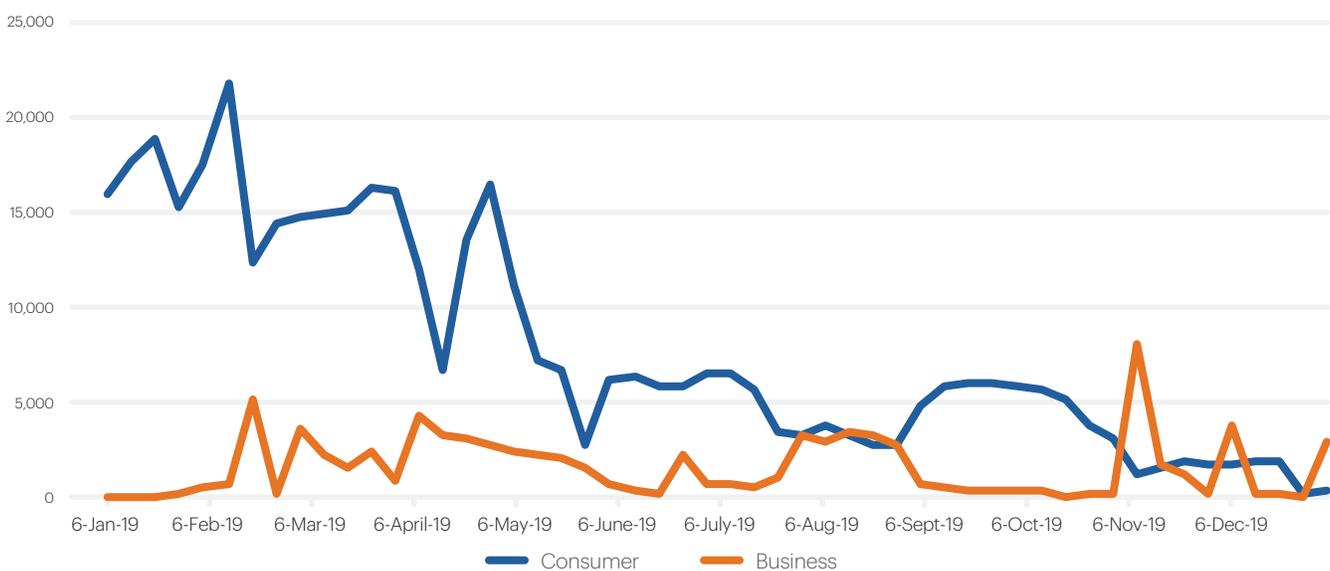
Figure 17. SecurityRun switched targets by October 2019 to the United States.

Windows threats summary

As we examine the trends for Windows users in 2019 and look ahead to 2020, we see that the threat landscape is becoming increasingly divided between consumer and business targets. The major malware threat for consumers on the horizon will be new and more intrusive forms of adware. As the primary pusher of consumer threats in 2019, adware creators in 2020 will count on a more relaxed stance from security providers on detecting threats seen as "diet malware" to continue exploiting humans for their attention, their individual systems, and some of their personal information.

From a business standpoint, however, we're seeing much more diverse malware coming out of the woodwork, not just Emotet and TrickBot, but QBot, SecurityRun, and numerous ransomware families, including Ryuk, Sodinokibi, and Phobos, which have caused significant disruption across the world in 2019. Greater detections of threats such as SecurityRun or hacking tools like Mimikatz show that criminals are doing as much as they can to attack organizations from all angles, using code and tools made available to penetration testers and network administrators to not only infiltrate our space and steal our data, but become more and more proficient at hiding from us.

As detections on organizations ramp up and cybercriminals become more adept at targeting high ROI victims, we expect to see even more diversification and sophistication in 2020 for global Windows business-focused malware.

But that's a lot of racket for only a 1 percent increase in overall malware detections, no? Considering that we're coming down from a cryptocurrency craze, which had covered almost the entire threat landscape in miners, and are dispatching of errant WannaCry detections wandering the net, that 1 percent actually reflects a healthy and growing cybercrime industry. Drastic drops in consumer detections and reasonable increases in business detections mean that we may continue to see overall malware volume decline. However, the financial and operational impact of businesses losing millions, insurance prices spiking, cities and schools halting because of ransomware attacks, and critical infrastructure being exposed and targeted may make it feel as though the Windows threat landscape has indeed become much harsher.

Perhaps the grass is greener, then, on the Mac side? If only.

Malwarebytes

Mac threat landscape 2019

We saw a significant rise in the overall prevalence of Mac threats in 2019, with an increase of over 400 percent from 2018. However, since you could argue—validly—that part of this was due to a corresponding increase in the total number of Mac endpoints running Malwarebytes software, it's more interesting to look at the change in the number of detections per endpoint. Mac detections per endpoint increased from 4.8 in 2018 to a whopping 11.0 in 2019, a figure that is nearly double the same statistic for Windows.

This means that the average number of threats detected on a Mac is not only on the rise, but has surpassed Windows—by a great deal. This is likely because, with increasing market share in 2019, Macs became more attractive targets to cybercriminals. In addition, macOS' built-in security systems have not cracked down on adware and PUPs to the same degree that they have malware, leaving the door open for these borderline programs to infiltrate.

Further, for the first time ever, Mac threats appeared at the top of Malwarebytes' overall threat detections. Two Mac threats—NewTab and PCVARK—showed up in second and third place in our list of the most prevalent detections across all platforms.

Detections per endpoint 2018-2019
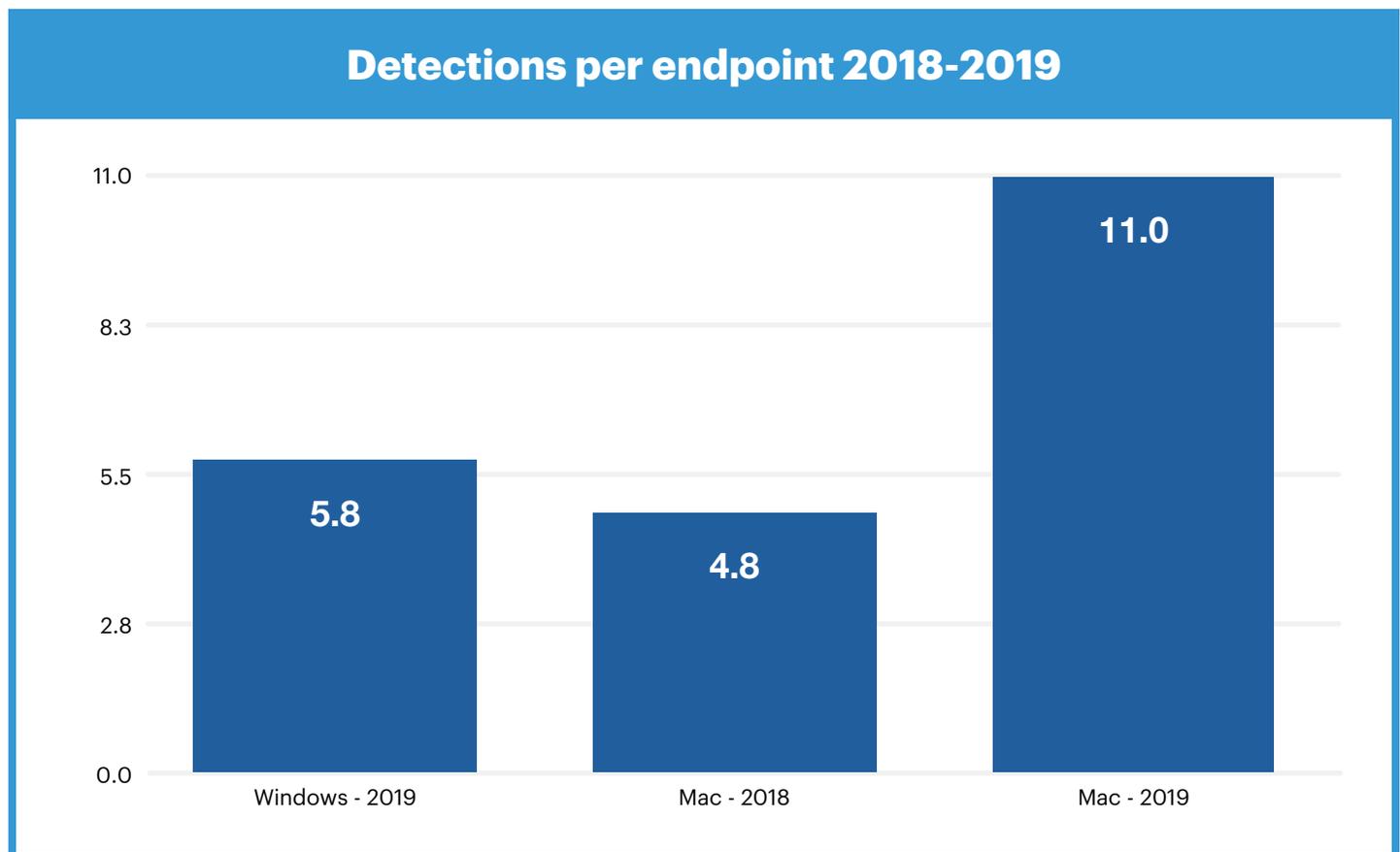
Figure 18. Mac threats per endpoint vs. Windows threats per endpoint

Malwarebytes

Top Mac threats

Macs differ drastically from Windows in terms of the types of threats seen. Where we found several different categories and families in our top detections of Windows threats that classify as traditional malware , especially those aimed at businesses, most Mac threats, and certainly the most prevalent ones of 2019, are families of adware and potentially unwanted programs (PUPs). The most common Mac malware family, OSX.Generic. Suspicious, fell well down the list at 30th place in Mac-specific detections, and hundreds of spots down on a cross-platform threat list.

 Among the top 10 Mac threats (for both consumers and businesses) are a mix of PUPs and adware. The PUPs are a variety of mostly "cleaning" apps that have been determined as unwanted not just by Malwarebytes, but by the Mac user community at large. PUPs MacKeeper and MacBooster, previously first and third on the list in 2018, fell to third and fifth place in 2019. This is likely due to the reliance of the companies behind these PUPs on a single app, each with a known bad reputation in the Mac community.

In contrast, the PCVARK and JDI PUPs have seen a rise in 2019 to second and fourth place, with PCVARK taking third place on cross-platform detections. In 2018, PCVARK was only at 31st place on the list, and JDI was ranked sixth. These detections flag a number of different "cloned" apps, which provide identical functionality under different names. It is likely this strategy of spreading wide under many different names that had launched these apps to the top of our detections.

---

[1] We define "traditional malware" as malicious software such as backdoors, Trojans, and spyware. As mentioned previously, adware is often considered "malware light," as it can run the gamut from legitimate, advertising-supported software to malicious code.
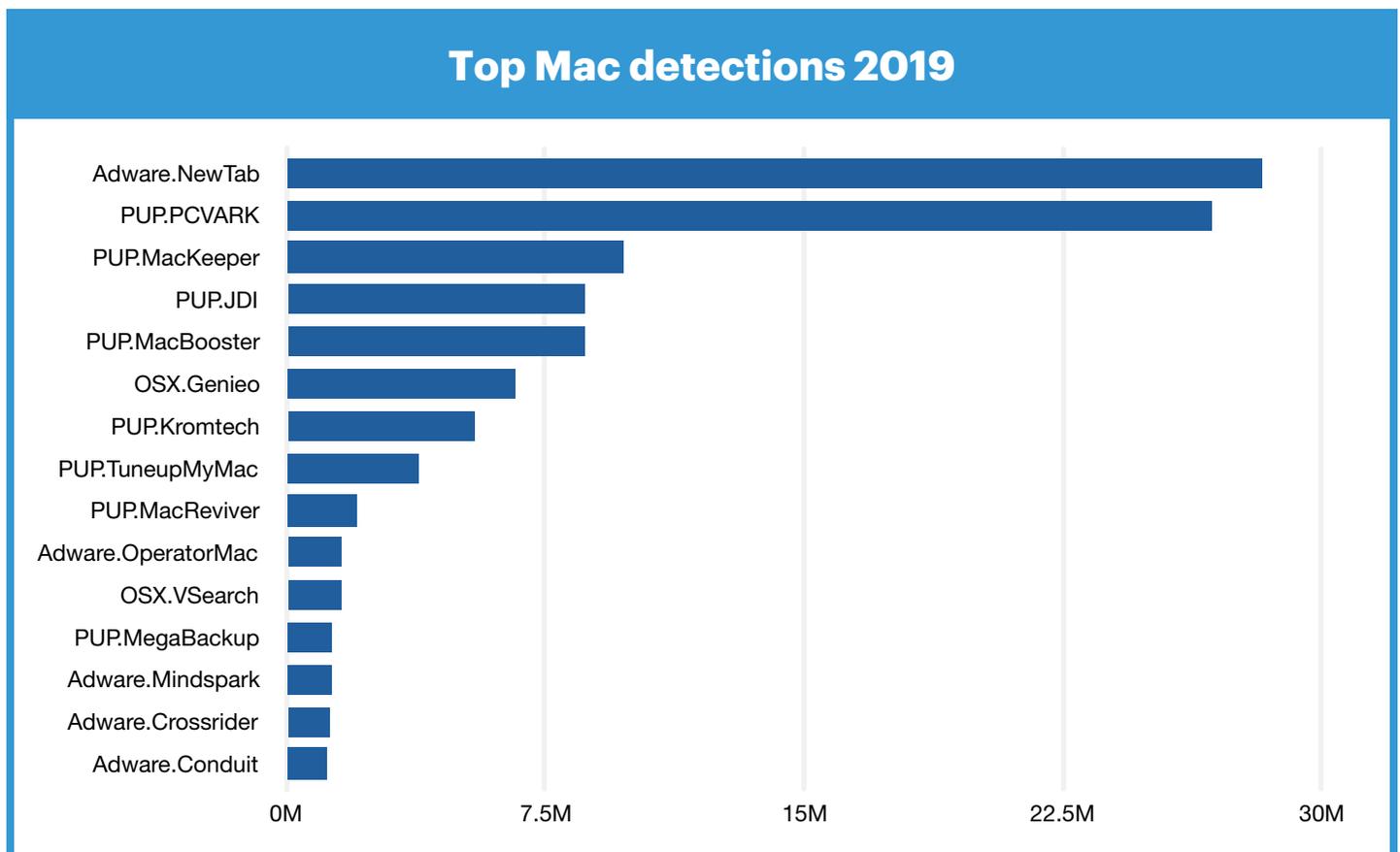
Figure 19. Top Mac detections in 2019

Family deep dive: Mac edition

The most noteworthy cyberthreats of the year aren't always the most voluminous. While that's not true for a couple adware families that topped our list of Mac threats, it's certainly the case for Mac malware detections. The top two Mac malware detections, with healthy numbers exceeding 300,000, are still dwarfed by the number one overall Mac detection, the adware NewTab, which was detected nearly 30 million times in 2019. Let's take a closer look at some of the Mac families that dominated or disrupted the threat landscape this year.
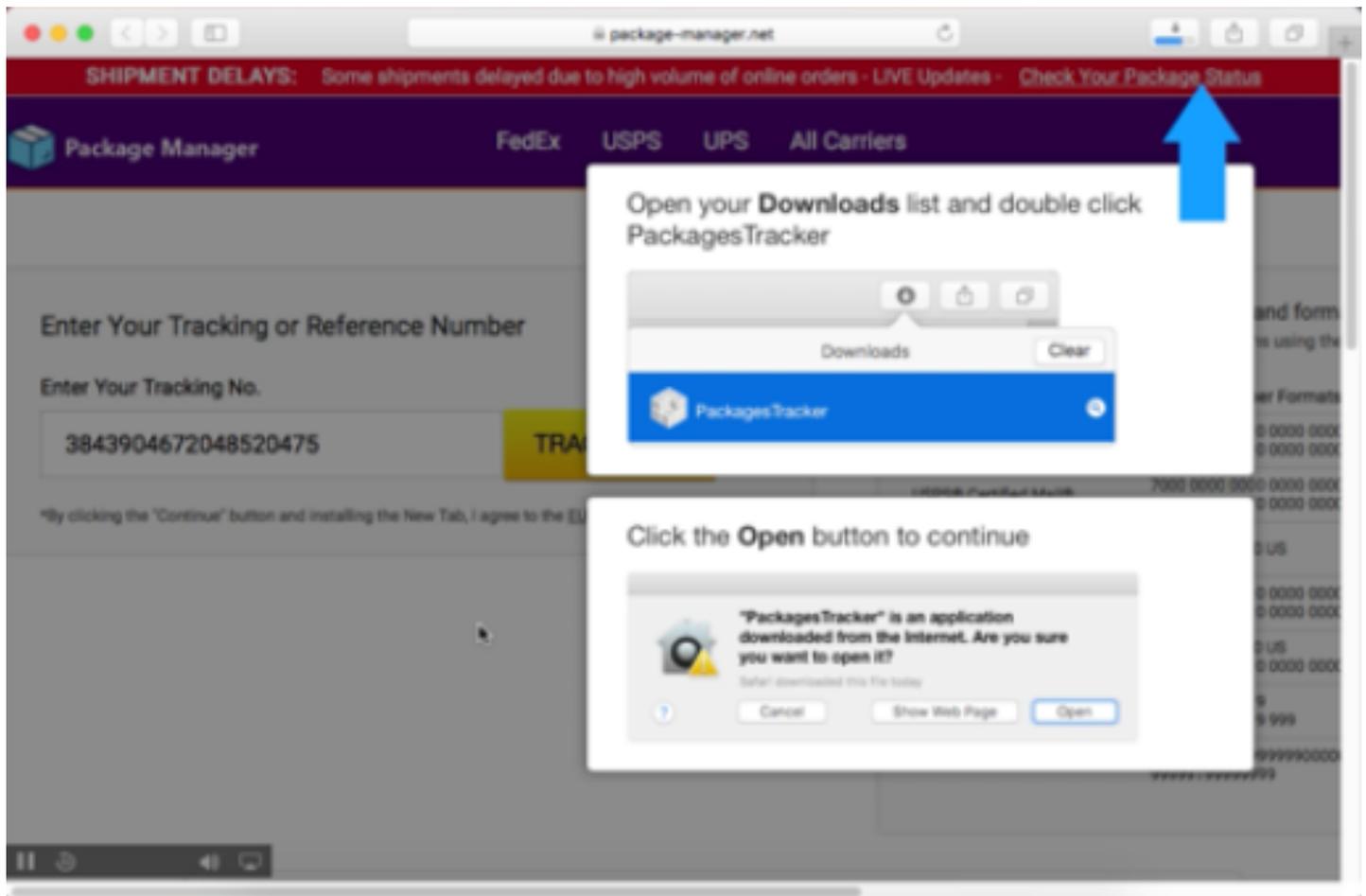
Figure 20. NewTab as a fake package tracker

NewTab

NewTab, at the top of the list, only appeared on the scene in December 2018, but rapidly rose to the top of our detections in 2019. NewTab is an adware family that attempts to redirect searches in the web browser for the purpose of earning illicit affiliate revenue, and it is mostly delivered in the form of apps with embedded Safari extensions.

NewTab apps are often spread through fake flight or package tracking pages, fake maps, or fake directions pages. In one early example, a fake package tracking page would accept any number entered, and regardless of the number, clicking the Track button would download a "PackagesTracker" app, with some instructions on how to open it. The app did not actually provide any tracking functionality.

![Malwarebytes logo]

Genieo

Genieo is another interesting piece of adware, crossing the line into malware due to some installation methods that abuse system vulnerabilities. It's one of the oldest pieces of adware in the Mac world—the only threat of its magnitude to operate successfully on the Mac since 2013. In 2019, our detections of Genieo reached nearly 7 million, placing it as our sixth most-detected Mac threat of the year.

Genieo has undergone fairly frequent changes since its introduction in 2013. The adware aims to earn affiliate revenue from redirected searches and home pages, and operates under hundreds of different names, often running from pages linked to that name that have a distinctive and consistent look (with only graphics and minor wording changes). Users affected with Genieo will find their search engines replaced and browser hijacked, with sponsored results served up to help the adware authors cash in. Uninstalling Genieo can also be difficult, pushing this adware further into aggressive, malware-like modality.
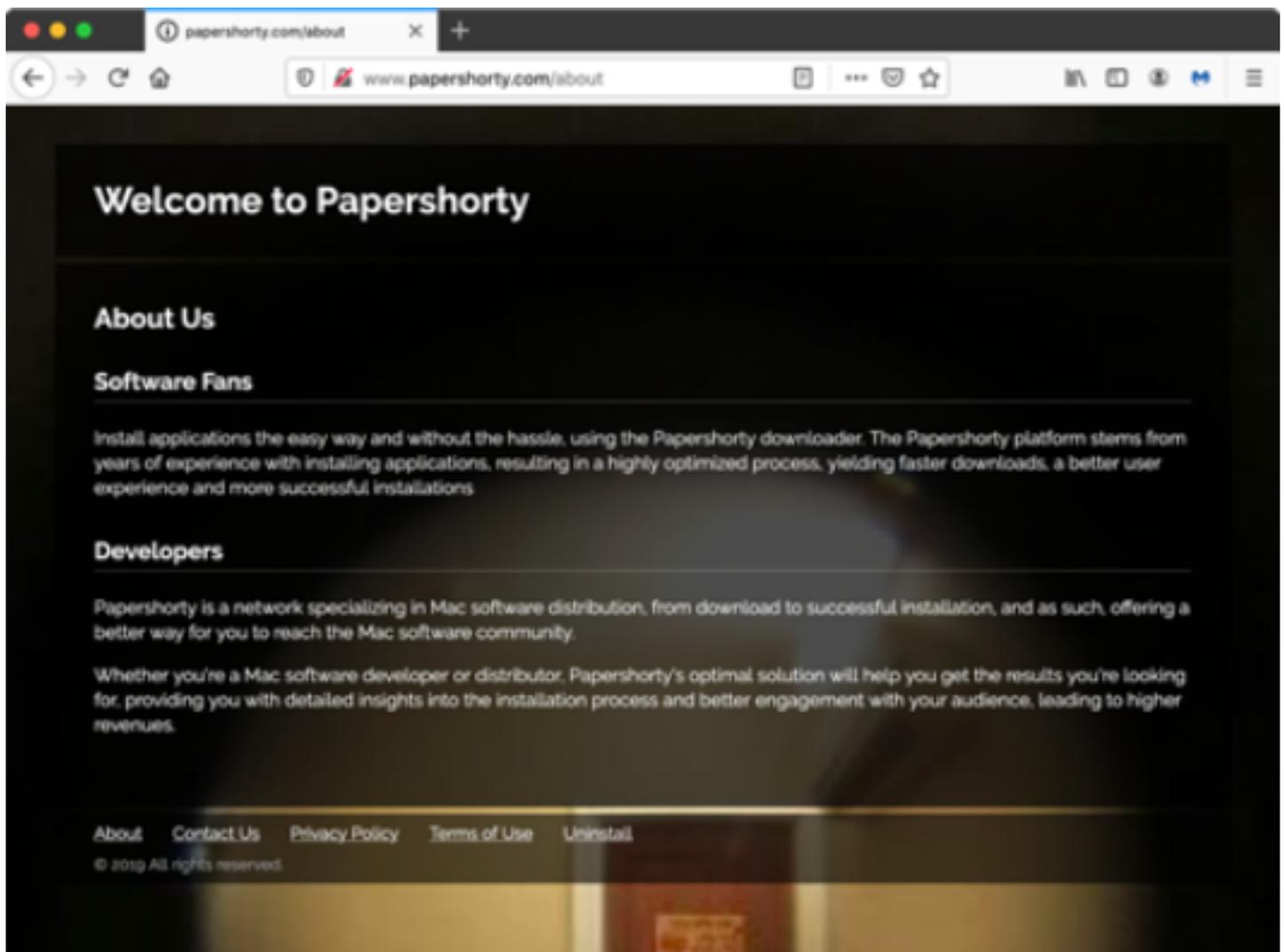
Figure 21. A web page serving up Genieo

OSX.Generic.Suspicious

When it comes to traditional Mac malware, such as backdoors, cryptominers, and spyware, the list is topped in 2019 by a group of files exhibiting similar malicious behavior, detected with a generic moniker: OSX.Generic.Suspicious.

Top Mac Malware Detections 2019

OSX.Generic.Suspicious	
OSX.FakeFileOpener	
OSX.FakeAV	
OSX.BirdMiner	

0K   100K   200K   300K   400K
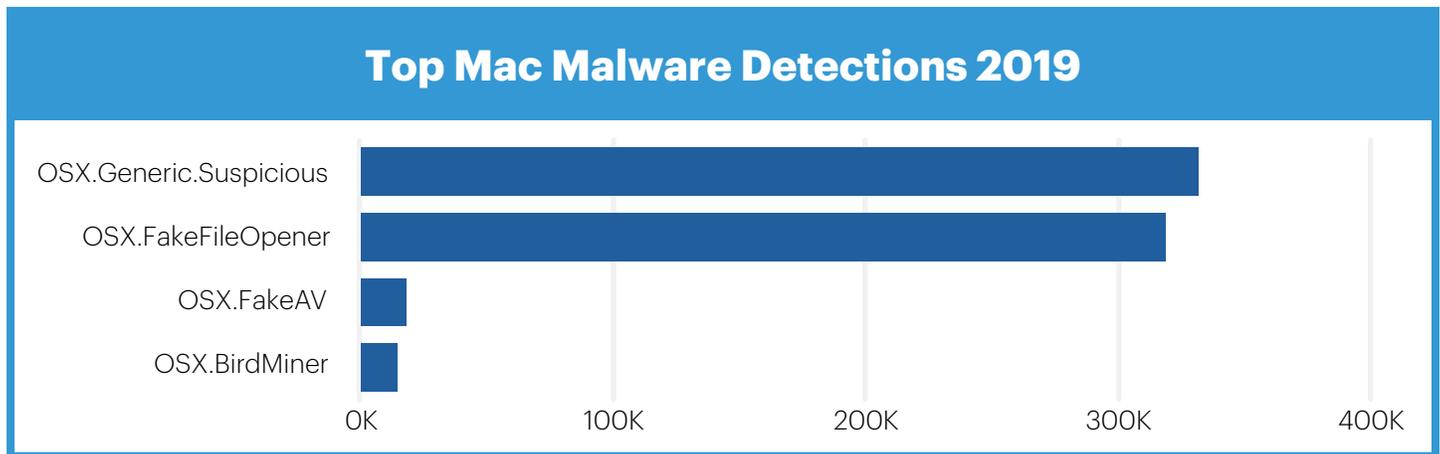
Figure 22. Top Mac malware detections of 2019

The OSX.Generic.Suspicious group of detections all exhibit known bad behaviors that no legitimate software program would engage in. For example, consider the following launch agent .plist:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
   <dict>
        <key>Label</key>
        <string>com.xpnsec.escape</string>
        <key>ProgramArguments</key>
        <array>
            <string>python</string>
            <string>-c</string>
            <string>import sys,base64,warnings;warnings.filterwarnings('ignore');exec(base64.b64decode('aW1…pKQ=='));</string>
        </array>
        <key>RunAtLoad</key>
        <true/>
   </dict>
</plist>
```

There's no reason for legitimate software to decode base64-encoded data and then execute it, especially within a launch agent .plist file. This is classic malware behavior, and it would trigger our OSX.Generic.Suspicious detection criteria.

We have seen a rise in this behavior over the past couple years, and expect to see that trend continue in 2020 as Apple tightens the requirements and conditions for checking, code signing, and notarization. Since shell scripts are exempt from these restrictions, we expect to see them used more and more by malware.

FakeFileOpener

FakeFileOpener is another interesting piece of malware, designed to abuse and imitate legitimate macOS

functionality to direct users to scam websites. This revolves around what happens when the user opens a file that no app on the system knows how to open. Normally, macOS will offer to search the App Store for you. When the FakeFileOpener malware is installed, the user is instead redirected to a page that indicates they may be infected with malware, offering malicious downloads to remedy the situation (ironic).

These apps have been circulating since 2016 and show no signs of stopping.
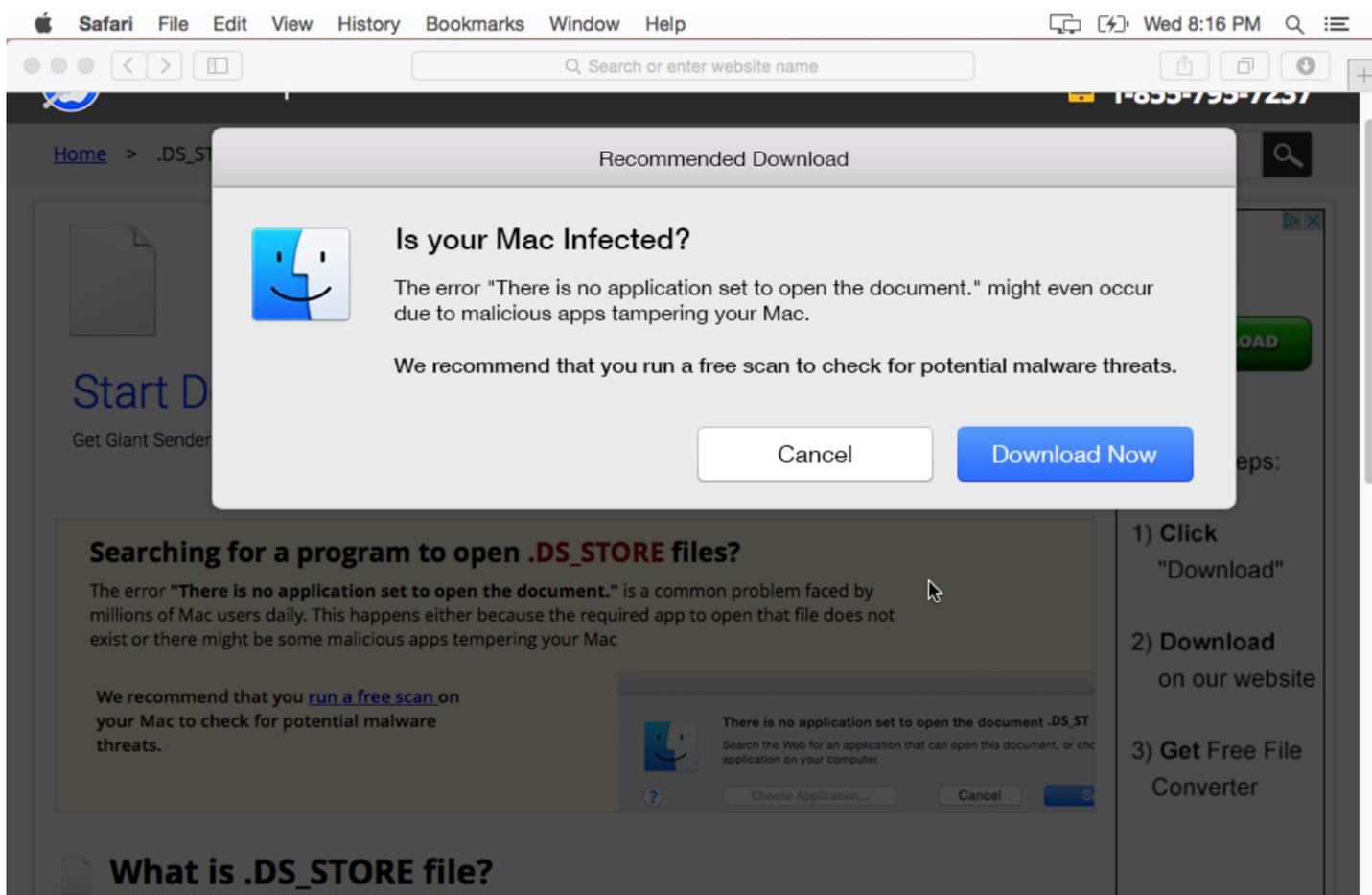
Figure 23. A message from FakeFileOpener urging users to (unbeknownst to them) download more malicious apps

iOS

On the iOS side, malware exists, but there's no way to scan for it. Most iOS malware is nation-state malware, spread via targeted attacks through iOS vulnerabilities, such as NSO's Pegasus spyware. It was learned this year

that China had gotten in on the action as well, using iOS zero-days to infect phones in a targeted attack against the Uyghur people.

Also found this year was an unprecedented zero-day

vulnerability in the bootrom of iPhones ranging from the iPhone 4S up to the iPhone X, as well as a number of other iOS, watchOS, and tvOS devices. The presence of this bug in the bootrom meant that it could not be patched; the only way to fix the bug was to buy a new phone. Dubbed [checkm8](), this vulnerability was soon leveraged to create the checkra1n jailbreak, capable of jailbreaking many devices regardless of what version of iOS they were running.

Although initially feared, checkm8 turned out to be not much of a problem for iPhone users, and more of a boon for iOS security researchers, who suddenly had a powerful tool they could use to analyze any recent iOS system and most iPhone hardware.

Mac threat summary

Of all the threats seen this year, only one incident involved anything other than tricking the user into downloading and opening something they shouldn't. That is the incident in which Coinbase, and several other cryptocurrency companies, were targeted with malware that infected systems through a Firefox zero-day vulnerability. Affected systems were infected with the older Wirenet and Mokes malware. This was the first time such a vulnerability had been used to infect Macs in any significant way since 2012, when Java vulnerabilities were used repeatedly to infect Macs (until Apple ripped Java out of the system, ending the threats).

Beyond that what we saw was a virtual landslide of adware and PUP detections, far outpacing growth on the Windows side. While these threats are not considered as dangerous as traditional malware, they are becoming a much larger and more noticeable nuisance for Mac users, who can no longer say that their beloved systems are immune from malware. And despite the relative low-grade hassle from adware compared to that of, say, ransomware, these families are becoming more and more aggressive, displaying malicious and persistent behaviors to trick users into a false sense of security.

Meanwhile, straight-forward malicious behavior from Mac files is increasing year-over-year, with more deceptive techniques to evade Apple's rather stringent eye. And breakthroughs on the iOS side may have the tech behemoth reconsidering whether they should allow antivirus products on their beloved mobile devices. If 2019's threat landscape tells us anything, it's that it's time to take a good hard look at Mac security and finally get serious.

Android threat landscape 2019

Mere stats cannot fully explain the threat landscape for Android users in 2019. Although numbers help guide our conclusions, it takes an extra level of expertise to get the true lay of the land. By digging through the highest-detected categories and families of Android malware, we can determine how many Malwarebytes users were affected by which threats. However, some threats made a massive impact without having to infect such a wide swath of devices. In the following sections, we take a look at some of the most influential malware categories and families of the 2019 Android threat landscape.

Pre-installed malware

Pre-installed malware. Sounds like a fallacy, doesn't it? How could manufacturers ship devices pre-installed with malicious apps? Unfortunately, it's a reality, and one that's becoming a growing problem. Although still concentrated on budget manufacturers' devices, such as the US-funded UMX mobile phone that shipped with pre-installed, unremovable Trojan malware, these malicious apps are starting to trick big name brands as well.

At the height of the conflict is a well-known PUP we detect as Android/PUP.Riskware.Autoins.Fota, a variant of Adups. Adups is malicious app is found on China-made mobile devices running the Android OS. This baked-in auto installer is used to update the device's firmware, but it also steals personal information. This year, it's our top-rated mobile threat, with 255,514 detections. Not too far down the list is another variant, Android/PUP.Riskware.Autoins.Fota.INS, with 65,589. Combined, this makes a staggering 321,103 detections for this one family of pre-installed malware alone.

Figure 24. A look inside UMX U683CL, the US-funded mobile phone that came pre-installed with malware

HiddenAds

Unsurprisingly, the second-most detected Android malware is a large family of Android Trojans we detect as Android/Trojan.HiddenAds. Why is that unsurprising? Because it is a favorite silent install of the aforementioned Adups variant. Just looking at the top 10 list of Android threats, excluding the PUP, monitor, and adware categories, variants of HiddenAds are seen four times. Combined, this accounts for 283,233 detections in 2019.

Although the Adups auto installer accounts for a number of these infections, it is also a favorite among infected apps found on third-party app stores. HiddenAds' only symptoms are to aggressively display advertisements—by any means necessary. This includes but is not limited to: ads in notifications, on the lock screen, and full screen pop-ups. Users who install HiddenAds apps are not informed of the advertising behavior beforehand.

Monitor category: stalkerware

Our monitor category saw a huge bump in detections this year, but this cannot be attributed to an overall increase of these types of threats on Androids, though their prevalence and public awareness does indeed seem to be growing. Thanks to concerted efforts between our research, writing, and product teams—as well as a new coalition formed in 2019 among security vendors, digital rights advocates, shelters, and domestic violence victim groups—Malwarebytes has cracked down on apps deemed to be stalkerware.

The term stalkerware can be applied to any application

with capabilities that allow it to be used to stalk or spy on someone else. That includes collecting the following data from someone else's device without their informed consent: GPS location data, photos, emails, text messages, call logs, contacts lists, non-public social media activity, and more. In addition, some stalkerware apps can be installed without displaying an icon or remotely operate a user's device, microphone, or camera. With over 100 new variants added in 2019, we are taking an even harder stance on these creepy apps, some of which still appear in Google Play and Apple's iTunes stores.
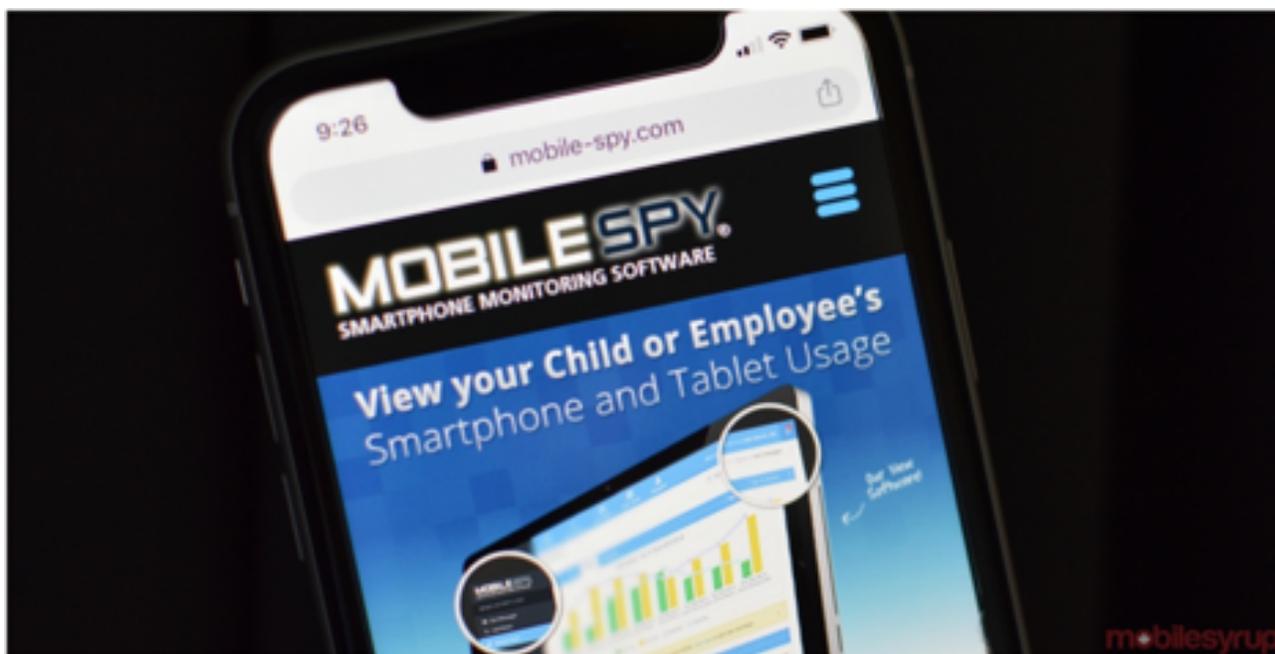
Figure 25. In October 2019, the FTC slapped Retina-X Studios, makers of the MobileSpy app, with a suit banning the company from selling its apps until changes were made—the first enforcement against stalkerware in US history.

Android threat summary

There are two pieces of stealthy mobile malware that deserve mentioning in 2019. First up is Android/Trojan. Dropper.xHelper. First seen in spring 2019, this malware topped the charts for many weeks before fizzling out at the end of the year. There is high probably that this accounted for a drop in Android/Trojan.HiddenAds as well. The second stealth malware, Android/Trojan. FakeAdsBlock, was first seen in October and is still going strong into 2020. Just like HiddenAds, this Trojan aggressively displays ads while hiding its presence on the mobile device.

These two new variants highlight the increase of a stealthier and more aggressive breed of Android malware in 2019. Whether its functionality is to drop other adware or to display aggressive ads itself, the proliferation of this type of threat shows cybercriminals' intent to skirt the law by the skin of their teeth while attempting to evade detection by mobile scanners. Make money and fly under the radar seems to be the name of the game in 2019. We predict this trend will continue into 2020.

Web threat landscape 2019

There is a strong correlation between the web threat landscape and browser market share. In 2019, Google Chrome still has the dominant position over rivals, such as Mozilla Firefox or Microsoft Edge. However, it is interesting to note that Microsoft's browser is one of many to switch or adopt Chromium (the open-source web browser

project developed by Google) as its main engine.

The majority of web attacks we observe happen in the background, leveraging server-side compromises or relying on social-engineering. However, throughout 2019 Internet Explorer was still getting exploited, keeping drive-by downloads alive.

Compromised infrastructure

As we've seen in the past, any website, big or small, can be valuable to threat actors. The eventual payload will depend on several factors in order to best maximize this resource.

One of the top Windows threats of 2019, Emotet, largely used compromised sites as part of its payload delivery. Disassociating the malware binary from the spam email is not a new technique, but it continues to be

an effective one, especially when it is done at scale by relying on a large supply of hacked web properties.

A researcher described how Emotet is using WSO webshells on compromised WordPress sites to keep the malware payloads updated. This is another way of attempting to bypass detection by repacking code and then pushing it back onto the distribution nodes.

Spam email   Decoy Document   PowerShell   Compromised Site   Final Payload

Figure 26. Emotet distribution flow via attached document

Malwarebytes

Web skimmers

E-commerce website   **Exfiltration server**   **Underground forums**
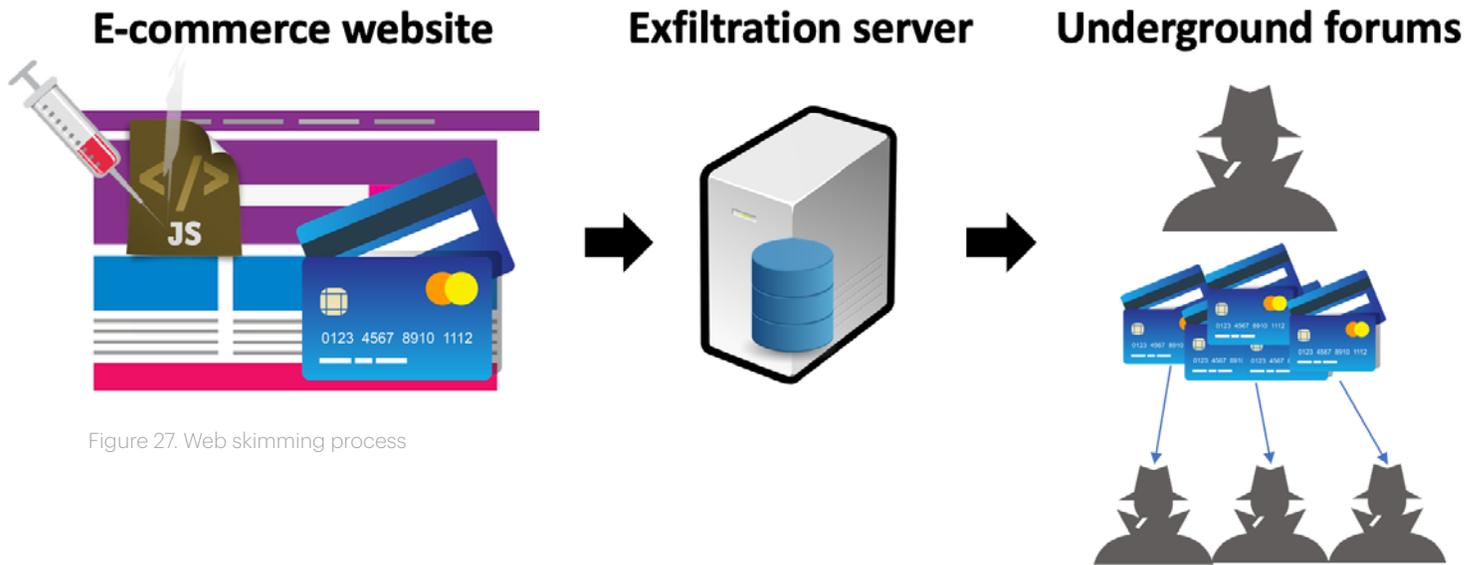
Figure 27. Web skimming process

Online shoppers in 2019 were the target of credit card skimmers, also known as web skimmers, or more generally referenced as Magecart.

E-commerce sites are most valuable to attackers as a source to steal payment information from unaware customers. By injecting malicious code (the skimmer) into one of those sites, criminals can monitor when someone is on a checkout page and leak the data they type (name, address, credit card number, etc.) in real time.

Web skimming became one of the most prevalent web threats we tracked through 2019. During the past year, the techniques improved, and the number of threat actors involved multiplied as well.

Unlike other attacks that often require to either infect users (banking Trojans) or social engineer them (phishing), web skimming works quietly on all devices and browsers. This makes it particularly effective and scalable to harvest and monetize stolen credit cards.

The challenge for defenders is to be able to detect these compromises in order to map out and subsequently block the criminal infrastructure. While many skimmers are virtually invisible because they rely on server-side code, even client-side ones can be very

hard to identify. While threat actors could concentrate on server-side skimmers only, in practice there are some benefits to doing both. For example, many of the e-commerce hacks can be traced to database injections which are easier to do and harder for site owners to detect and clean up.

Some of the latest trends include using steganography (a technique that consists of hiding data inside image files) as well as relying on the WebSocket protocol instead of HTTP.

Steganography has long been used by malware authors to smuggle their code inside innocuous images. In the case of web threats, images are the perfect vehicle because they tend to be excluded from web scanners due to their size. Parsing data other than typical HTML and JavaScript requires different tooling and takes up time as well.

The same goes for WebSocket, which is a different protocol than the most commonly used HTTP. Rather than looking at a series of requests and responses, one has to observe the bidirectional messages inside the WebSocket. By adding custom obfuscation to those communications, the exfiltration of stolen credit card data will most likely never be caught.
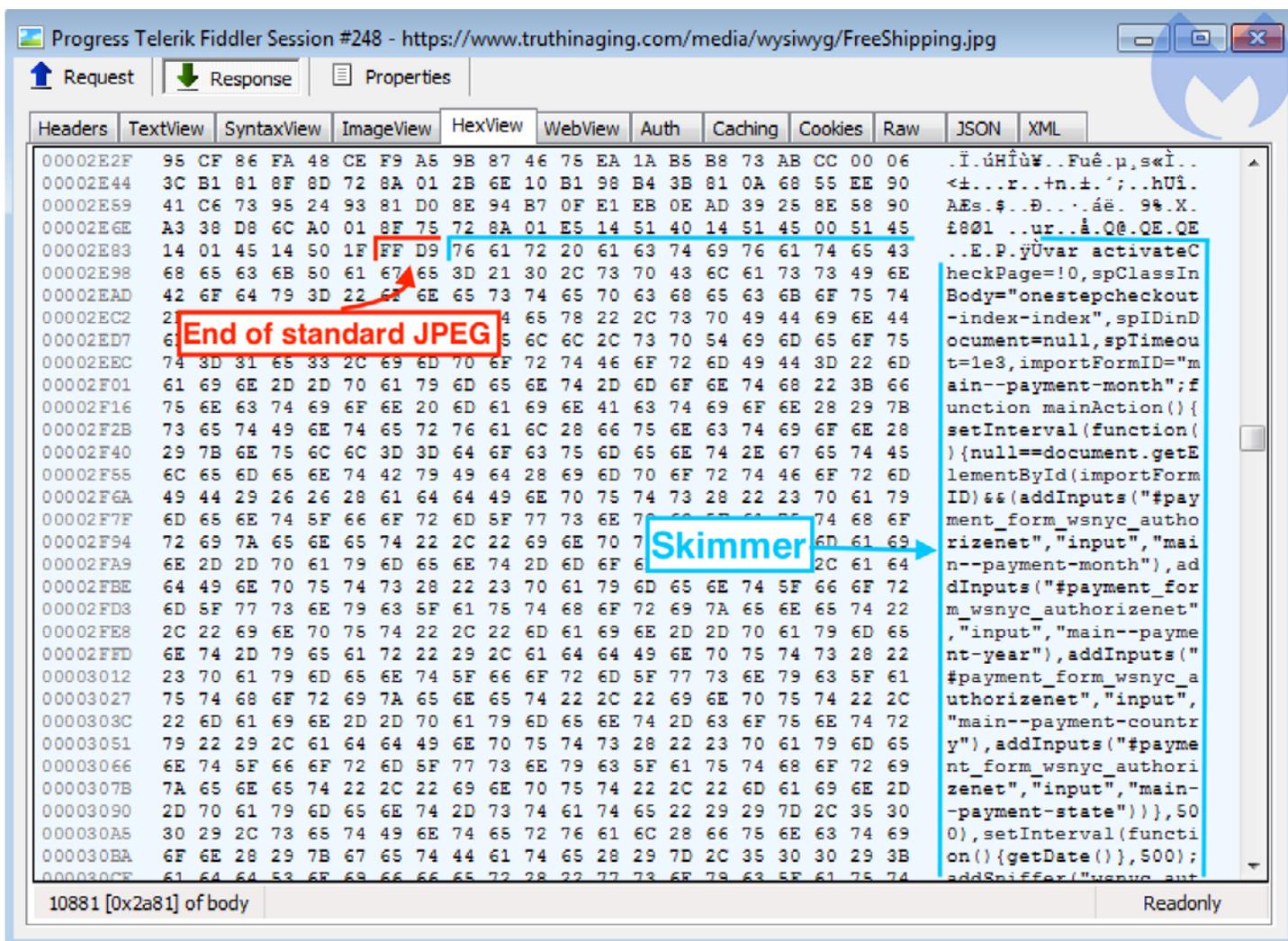
Figure 28. Skimmer hidden inside an image

Exploit kits

The drive-by download threat landscape is alive and well, despite the fact that it still relies on an aging and ever less popular Internet Explorer browser. 2019 brought in many surprises on this front, with the identification of several new exploit kits and the increased adoption of fileless payloads.

In fall 2019, we had registered nine active exploit kits ranging from fairly unsophisticated ones, to more advanced frameworks. Despite relying on less potent vulnerabilities (and no zero days), their developers managed to pack in some clever techniques to evade sandboxes and distribute their payloads in covert ways.

Fallout EK, Spelevo EK, and RIG EK came out as the top three most active exploit kits serving stealers, ransomware, and a variety of other malware. Stealers were actually one of the most common payloads we saw, either as a first drop or secondary via loaders such as Smoke Loader.

One particular exploit kit called Underminer EK has given us a lot of research material due to its unique payload (Hidden Bee) and tricks, including steganography, to deceive researchers. We believe that it may be the work of an advanced group, rather than a standalone malware author.

Malwarebytes

Figure 29. Traffic capture from Underminer EK

Malvertising and redirection campaigns

As always, malvertising is adapting to the threat landscape itself by pushing more scams onto desktop and mobile users. It remains the primary vector to distribute fake software updates.

However, we have seen a return of compromises on larger sites as well with the purpose of redirecting traffic. This includes the FakeUpdates campaign discovered in 2018 and the newly-discovered Domen toolkit, which combines several elements from various predecessors and was built on a rental model.

Browser lockers, also known as browlocks, continue

to fuel most of the calls leading to tech support scams. Users are redirected to these fake pages via a combination of malvertising or redirection from compromised sites. While many browlocks can be closed using the user interface, occasionally the crooks come up with new templates that effectively block users out of their computer, short of forcefully killing the browser process. Google Chrome was historically the most targeted browser in this area, but Mozilla Firefox seems to be the newer focus, and was caught in a true browlock in November 2019.

```
var banner = '3'; // 1 - Browser Update | 2 - Font | 3 - Flash
```
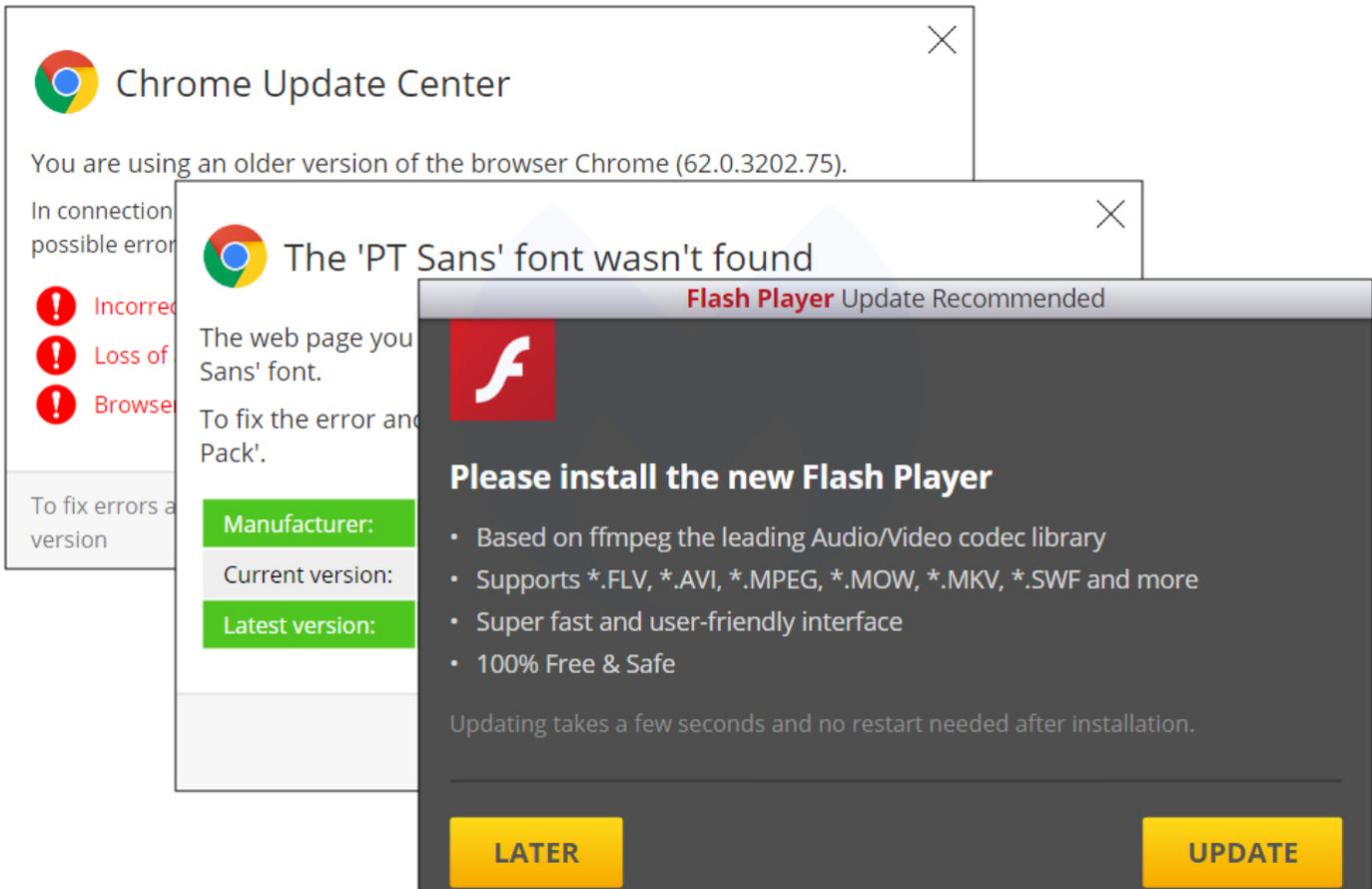
Figure 30. Fake error messages from the Domen toolkit

Web threats summary

The web threat landscape in 2019 was dominated by online credit card skimmers as they provide direct and quick monetization to criminals with limited effort. Web skimmers can also be more difficult to protect against, especially because they do not compromise machines via exploit and can reside only inside the infrastructure of online stores.

Compromised infrastructure on its own is a problem that has large repercussions on the overall web ecosystem. It's clear that threat actors will continue to automate the hacking of sites in bulk and use them as a commodity for distributing malware, such as Emotet.

Exploit kits generated a level of activity that surprised us and, despite relying on using older vulnerabilities,

showed some creative ways of infecting systems. As Windows 7 comes out of support in 2020, it remains to be seen how much longer threat actors will be able to abuse IE. What we may see instead is a shift to other browsers, as the few zero-days seen in 2019 indicate that as a possibility for targeted or mainstream attacks.

Malvertising and malicious redirections in general have been a continuous problem, despite the wide adoption of ad blockers. Attackers keep coming up with clever ways to abuse technologies that were meant to make the web better and faster. Although the browser market is dominated by Google Chrome, a new browser way (where privacy and ads are at the center of discussions) may very well be looming.

Regional threats 2019

Regional detections 2019
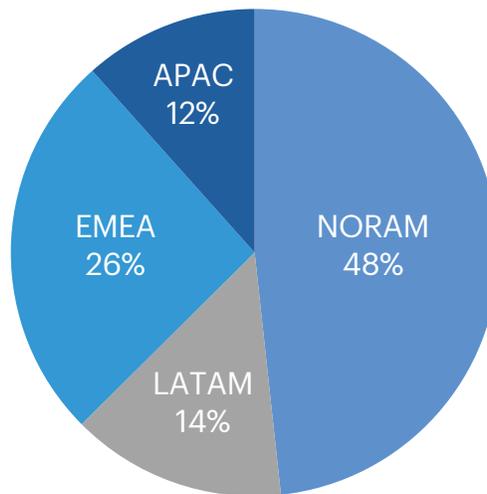
Figure 31. Percentage of threats per region

Swinging back around to "traditional malware," we'll now slice and dice our 2019 detections according to four distinct regions: North America (NORAM), Europe, the Middle East, and Africa (EMEA), Asia Pacific (APAC), and Latin America (LATAM). Unsurprising, NORAM came away with the lion's share of threats, with 48 percent of the world's malware aimed at the North American continent. EMEA also grabbed a large slice of the pie at 26 percent. LATAM and APAC brought up the rear at 14 and 12 percent, respectively.

NORAM threat landscape 2019

North America was at the receiving end of more than 24 million threats, up 10 percent from 2018 and comprising almost half of all detections in 2019. The top five countries impacted in NORAM were, in descending order: the United States, Canada, Puerto Rico, US Virgin Islands, and Guam.

Adware features heavily in NORAM regions, taking most of the top five positions across the US, Canada, and Puerto Rico for consumer detections. Emotet and TrickBot both made strong showings for both US and Canadian business detections (first and second place for Canada; second and third place for the US), while Puerto Rico's top business detection is a worm known as Conficker.

While overall detections decreased by 1 and 5 percent for Canada and Puerto Rico, detections in the US shot up by 10 percent from 21,371,182 in 2018 to 23,625,567 in 2019. For all the potency of Emotet and TrickBot, the number one detection for US businesses is the Yontoo adware. The US is traditionally the home of a huge array of adware and PUP development, yet it may still surprise some to discover that browser extensions are so

North America threat detections 2018-2019

Year	Detections
2018	22,172,244
2019	24,417,465
% Change	**10%**

Top 5 threat families 2019

Consumer		Business	
1.	Adware.MindSpark	1.	Adware.Yontoop
2.	Adware.SearchEncrypt	2.	Trojan.Emotet
3.	Adware.InstallCore	3.	Trojan.Trickbot
4.	Trojan.Emotet	4.	Adware.MindSpark
5.	Adware.IronCore	5.	Hijack.SecurityRun

Figure 32. Top NORAM threats 2019

pervasive in corporations, where locked-down browsers and other software should, in theory, make for smooth day-to-day operations.

Even so, the power of Emotet and TrickBot should never be discounted. Major North American attacks took place throughout the year, with large spam runs and more focused phishing tactics for Emotet, and new techniques and targets, including healthcare organizations, for TrickBot as well. NORAM users should expect to see plenty of this dangerous duo in 2020.

EMEA threat landscape 2019

Looking at the developments in EMEA from 2018 to 2019, we can see a major trend that reflects what happened around the globe: the number of cryptominer detections for both consumers and businesses dropped to make room for more adware. Overall detections decreased minimally by roughly 2 percent, except for France, which dropped by almost 16 percent.

While EMEA detections don't differ much from those in NORAM from a broad, regional perspective, we start to see more "cultural differences" in the top detections when we compare the top three countries and their most prevalent malware.

Malwarebytes

United Kingdom	France	Germany
Consumer	**Consumer**	**Consumer**
Adware.Installcore	Adware.Installcore	Adware.KeenValue
Adware.Mindspark	Adware.Mindspark	Adware.Installcore
Riskware.BitCoinMiner	Hacktool.Filepatch	Riskware.BitCoinMiner
Adware.FusionCore	Riskware.BitCoinMiner	Hacktool.Filepatch
Hacktool.Filepatch	Adware.FusionCore	Adware.FusionCore
Business	**Business**	**Business**
Hijack.SecurityRun	Ransom.WannaCrypt	Trojan.Emotet
Trojan.Emotet	Adware.FusionCore	Trojan.Trickbot
Trojan.Trickbot	Riskware.BitCoinMiner	Backdoor.Bot
Trojan.Injector	Riskware.RemoteAdmin	Adware.KeenValue
Adware.Installcore	Rootkit.Cidox	Adware.Yontoo

Figure 33. Top consumer and business threats in the UK, France, and Germany

EMEA's top five countries in 2019 by threat volume were, in descending order: the United Kingdom, France, Germany, Spain, and Russia. Compared to 2018, the only notable change is Russia dropping from second place to fifth.

Once again, we see Emotet, TrickBot, SecurityRun, HackTools, and various adware families. But some notable differences include an adware family called KeenValue as the top German consumer threat, and a backdoor making its way to the third most-detected threat on German business endpoints. In France, WannaCry (detected as WannaCrypt) still factors heavy in detections as the top business threat, while a rootkit named Cidox came in at fifth place in business detections. Meanwhile, the UK looked the picture of the North American threat landscape, with the exception of a Trojan injector wiggling its way into fourth place in business detections.

Not to be outdone by the action across the pond, Emotet managed to make quite a splash in EMEA in

2019. In the public sector, the botnet crippled the city of Frankfurt, one of the largest financial hubs in the world and the home of the European Central Bank.

Missing from top detections, but not to be discounted: The dominance of ransomware as the main threat continued to make headlines in EMEA. Noteworthy European victims of ransomware were the universities of Freiburg and Maastricht. But the commercial sector was hit almost as bad. The most newsworthy stories were those of Norwegian Norsk Hydro ASA, which is a major global player in the aluminum and renewable energy sectors, as well as Belgian metal producer Nyrstar. On the other end of the EMEA region, the city of Johannesburg, the largest city in South Africa, fell victim to a ransomware called Bitpaymer.

Malwarebytes

APAC detections w/o Singapore/Aus/NZ 2018-2019

Year	Detections
2018	5,458,081
2019	4,809,605
% Change	**-11%**

Top 5 threat families 2019

Consumer		Business	
1.	Riskware.BitCoinMiner	1.	Adware.Sogou
2.	Adware.InstallCore	2.	Asware.ChinAd
3.	HackTool.File.Patch	3.	Ransom.WannaCrypt
4.	Ransom.WannaCrypt	4.	HackTool.Mimikatz
5.	Adware.Linkury	5.	Riskware.BitCoinMiner

Figure 34. Top APAC detections in 2019

APAC threat landscape 2019

Our APAC detections (not including Singapore, Australia, or New Zealand) showed an 11 percent decrease from 2018 to 2019, slipping from 5,458,081 to 4,809,605.

The number one threat for consumers in APAC is Riskware.BitcoinMiner, the generic detection name for cryptominers found on infected systems. Bundlers are a big source of these infections, and after a period when it seemed ransomware may trump miners as operators lost interest in small returns for lots of investment, they've powered their way to the top regardless. Meanwhile, businesses in APAC attempted to tackle problems brought on by adware, with Sogou and ChinAd taking the top two positions.

The ever-present threat of ransomware hasn't gone away, however. WannaCry continues to wreak havoc on APAC business and consumers, appearing at positions three and four, respectively. More broadly, attacks delivered over remote access applications were popular in the region, and our teams report having seen multiple business email compromise attacks in the Philippines, Myanmar, Singapore, and more. The ASEAN region specifically could lose up to US$19 billion in a hypothetical global ransomware attack due to costs from incident response, backup, loss of productivity, and ransom payments. This thinking is strengthened when looking at some of the biggest breaches to have occurred during 2019.

Malwarebytes

In 2019, the top five countries for infection (again, outside of Australia, New Zealand, and Singapore) were Indonesia, Philippines, India, Thailand, and Malaysia. The only change from 2018 is that Malaysia nudged Vietnam out of fifth place, essentially maintaining the status quo.

Indonesia

Indonesia's infections (and indeed, most other countries) showed a similar pattern to overall APAC trends, with WannaCry and cryptominers putting in strong performances in both consumer and business detections.

Asia Pacific - Indonesia

Consumer

	Top 5 threats 2018		Top 5 threats 2019
1.	Ransom.WannaCrypt	1.	Riskware.BitCoinMiner
2.	Riskware.BitCoinMiner	2.	Ransom.WannaCrypt
3.	Adware.Wajam	3.	Adware.Linkury
4.	Adware.Tuto4PC	4.	Adware.IClouder
5.	Virus.Renamer	5.	Adware.Installcore

Business

	Top 5 threats 2018		Top 5 threats 2019
1.	Ransom.WannaCrypt	1.	Ransom.WannaCrypt
2.	Riskware.BitCoinMiner	2.	Worm.EternalRocks
3.	Trojan.ShadowBrokers	3.	Trojan.Shadowbrokers
4.	Riskware.PowershellSP	4.	Riskware.BitCoinMiner
5.	Adware.ChinAd	5.	Hacktool.Equation

Figure 35. Top consumer and business detections in Indonesia in 2019

Worryingly, there's a lot of EternalBlue activity taking place in the form of Worm.EternalRocks and Trojan. Shadowbrokers detections, which suggests businesses aren't patching SMB vulnerabilities dating back to 2017. There's also Hacktool.Equation in fifth place, also made public by the Shadowbrokers group, so 2019 in Indonesia had a retrospective feel about it.

Australia and New Zealand

A 14 percent drop in overall detections ushered in the end of 2019 for Australia and New Zealand, with a focus on adware for both consumers and businesses. Our

cryptomining detection only mustered third place for consumer detections in this sub-region, as the revenue from advertising, bundlers, and PUPs is the clear priority here. Most examples of security events, breaches, and other incidents unsurprisingly resembled what was happening around the globe. There were organizations affected by ransomware refusing to pay ransoms, and multiple hospitals across Australia brought down by similar attacks. Just in case we somehow forgot Emotet exists, it decided to remind us via ACSC issuing an alert on a campaign targeting critical infrastructure and government agencies.

Australia/New Zealand detections 2018-2019

Year	Detections
2018	1,101,209
2019	950,727
% Change	**-14%**

Top 5 threat families 2019

	Consumer		Business
1.	Adware.InstallCore	1.	Adware.Sogou
2.	Adware.MindSpark	2.	Adware.MindSpark
3.	Riskware.BitCoinMiner	3.	Adware.ChinAd
4.	Adware.FusionCore	4.	Hijack.Shell
5.	HackTool.FilePatch	5.	Adware.FusionCore

Figure 35. Top consumer and business detections in Indonesia in 2019

Singapore

Singapore experienced a -4 percent change in overall detections, and though we saw many familiar faces in the form of cryptominers and Emotet, we also observed yet another strong showing for consumer adware detections. On the business side, detections were topped by a Trojan named FakeAlert. This is an interesting one, as it's a little bit retro—harking back to the days of fake infection alerts and bogus antivirus software.

Singapore experienced numerous high-profile attacks during 2019, including data exfiltration potentially exposing the details of Singapore Armed Forces (SAF) and Ministry of Defence (MINDEF) personnel. Elsewhere, ransomware put in its usual appearance, causing problems throughout the region in multiple business sectors (in particular, transportation, travel, and financial services). And a data-stealing malware called Rancor deployed spear fishing attacks in both Singapore and Cambodia. Always on the front lines of proactive security measures, Singapore continues to fight back against attacks with plans to harden critical systems.

Singapore detections 2018-2019

Year	Detections
2018	109,617
2019	105,379
% Change	**-4%**

Top 5 threat families 2019

	Consumer		Business
1.	Adware.ChinAd	1.	Trojan.FakeAlert
2.	Adware.InstallCore	2.	Adware.Sogou
3.	Riskware.BitCoinMiner	3.	Adware.Elex
4.	Hacktool.FilePatch	4.	Trojan.Emotet
5.	Adware.Elex	5.	Adware.InstallCore

Figure 37. Top detections in Singapore in 2019

LATAM threat landscape 2019

In stark contrast to declining volumes in the NORAM, EMEA, and APAC regions, year-over-year detection numbers in LATAM showed a 26 percent increase, up from about 5.7 million threats to 7.2 million. Top countries contributing to the incline are Brazil (+31 percent) and Mexico (+25 percent). On the lower end of the scale, Argentina scored just a 1 percent increase, matching the overall global threat detection pattern in 2019.

The top five countries in LATAM for 2019 threat volume were, in descending order: Brazil, Mexico, Argentina, Colombia, and Peru. This represents minimal change from 2018, in which Venezuela was in fifth place and Peru in sixth. This year, Venezuela slid down one spot to sixth, switching places with its Peruvian neighbor.

Latin America detections 2018-2019

Year	Detections
2018	5,720,163
2019	7,220,748
% Change	**26%**

Top 5 threat families 2019

	Consumer		Business
1.	Adware.InstallCore	1.	Trojan.Emotet
2.	HackToo.WinActivator	2.	Adware.InstallCore
3.	HackTool.FilePatch	3.	HackTool.WinActivator
4.	HackTool.AutoKMS	4.	Riskware.BitCoinMiner
5.	RiskWare.BitCoinMiner	5.	Virus.Renamer

Figure 38. Top LATAM detections in 2019

Looking across the LATAM region, we saw an increase in different adware families against the slowly disappearing cryptominers and noticed Emotet as the most prevalent non-adware threat for businesses. However, hack tools mostly aimed at using Microsoft products illegally made their way into both consumer and business detections. Somewhat crazily, a virus known as Renamer climbed into the top five business threats in LATAM, something we haven't seen in years.

Latin America has traditionally been the home of banking Trojans, but even here we saw an overwhelming dominance by ransomware. Petroleos Mexicano (Pemex), a Mexican state oil and gas conglomerate, was the most prominent victim of what looked to be another Bitpaymer attack.

Top industry threats

When the Stuxnet worm hit Iran's nuclear centrifuges in 2010, the world got its first glimpse at the potential for cyberattacks to compromise a country's critical infrastructure. Although less than a handful of these attacks targeted supervisory control and data acquisition (SCADA) systems within the decade, we've seen a tremendous amount of cybercriminal activity focused on the critical infrastructure of the world's top industries—

one to multiple organizations at a time. In 2019, threat actors turned up the heat on industry attacks, bringing US cities to a screeching halt with ransomware infections, halting daily instruction in schools compromised with Emotet, and putting patient lives at risk in TrickBot attacks on healthcare organizations.

Malwarebytes has been tracking the threat landscape

Top 10 sectors impacted by threats

	2018	2019
1.	Education	Services
2.	Retail	Education
3.	Manufacturing	Retail
4.	Services	Manufacturing
5.	Government	Medical
6.	Retail	Education
7.	Manufacturing	Retail
8.	Services	Manufacturing
9.	Government	Medical
10.	Government	Medical

Figure 39. The top 10 industry sectors impacted by threats in 2018 and 2019

Malwarebytes

and how its ebb and flow affect our vital infrastructures. In an age when headlines of seemingly consistent compromises against businesses have become painfully commonplace, users could be easily swayed into believing hackers are only hammering on a couple sectors. In viewing our telemetry, however, we see that cybercriminals nowadays are less fixated on singular industries, but more on their victims' relatively vulnerability and ability to pay up.

The services sector, which ranked fourth in 2018, is 2019's top industry affected by cyberthreats, with a noteworthy 155 percent leap. Meanwhile, education, retail, and manufacturing—ranked first, second, and third, respectively in 2018—slid down a notch and swapped positions. All three remain prized targets of threats actors in 2019, yet only education experienced a surprising decrease of 63 percent. Meanwhile, retail and manufacturing experienced a nominal increase of 7 percent and 28 percent.

The medical sector also climbed three places up the ranks to fifth place as the number of detections increased by 98 percent. The marketing sector also showed a chilling growth of 174 percent, climbing two

places to the eighth spot in 2019. The government sector descended two places to seventh, showing a meager 3 percent growth in detection volume.

As the transportation and utilities and travel sectors exit the top 10—at 11th and 19th places in 2019, respectively—we saw new industries enter our top tally: the finance and construction industries. The former experienced a 109 percent increase in detections, while the latter a 46 percent increase.

There are other industries that were no close to the top 10 but reached such significant volumes of detection that we'd be remiss to not mention them. The electronics and not-for-profit (NFP) sectors, for example, experienced a 101 percent and 106 percent growth, respectively, in 2019. Meanwhile, organizations in aerospace and defense saw a jaw dropping 791 percent increase this year, while real estate shot up by 910 percent.

We'll now take a deeper dive into the top three verticals impacted in 2019 and look at why threat actors might be targeting them.
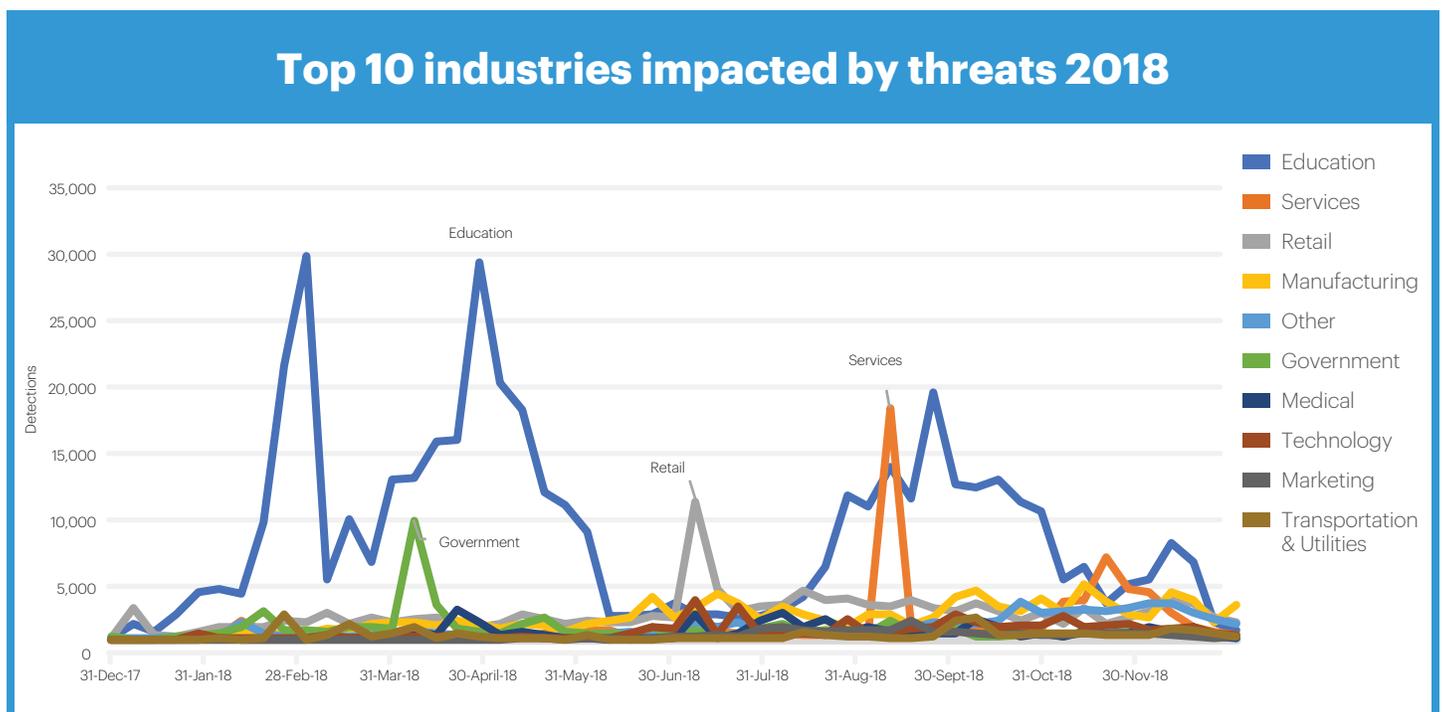
Figure 40: The top 10 impacted sectors in 2018 show the overwhelming number of detections from the education industry.

Malwarebytes

Top 10 industries impacted by threats 2019
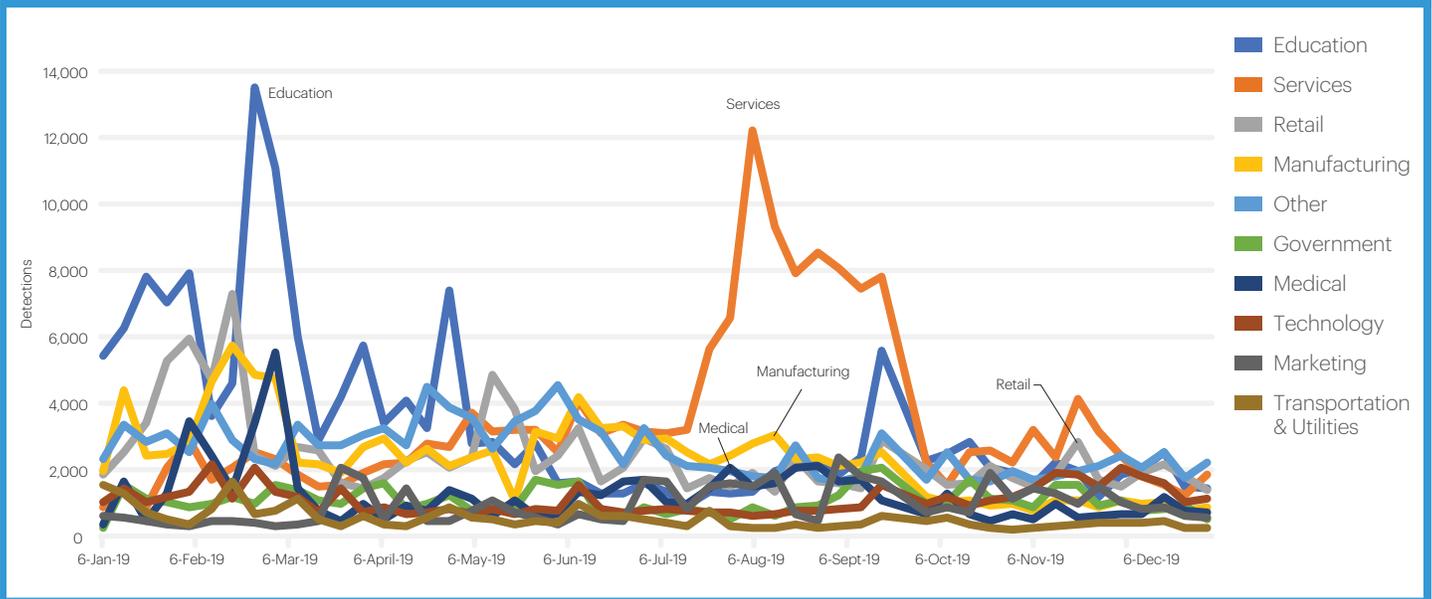
Figure 41: 2019 detections demonstrate education threats dropping mid-year, with services spiking in the summertime.

Services

The sector that our telemetry identifies as "services" is a composite of a wide variety of professional practices, including managed service providers (MSPs), accounting, consultancy, web hosting, and photography, as well as consumer services, such as gardening, repairs and maintenance, and waste management.

Our telemetry recorded a significant jump to 162,214 detections in 2019 for this sector, up from 63,622 in 2018.

As services is an amalgamation of several industries, it is difficult to pinpoint which among them threat actors are targeting. However, judging by public reports and intel gathered from affected business prospects, MSPs are becoming increasingly juicier targets for compromise in their own right, as well as for gaining a foothold into larger enterprise networks. Often a victim of their own negligence, MSPs have been attacked

Top threats affecting the services sector

	2018	2019
1.	Trojan.Emotet	Adware.Sogou
2.	Trojan.Trickbot	Adware.ChinAd
3.	Adware.IStartSurf	Virus.Neshta
4.	Worm.Qakbot	Trojan.Emotet
5.	Trojan.PasswordStealer	Trojan.Trickbot

Figure 42. Top five threat detections for the services industry in 2018 and 2019

through weaknesses introduced via mishandling of administration credentials, failure to update software vulnerabilities, poor asset management, and lack of appropriate log analysis tools.

Malware, of course, will always be a go-to tool to infiltrate organizational systems in any industry. The top families affecting the services sector in 2018 and 2019 feature a few of the usual suspects, plus a couple surprises, such as a Trojan PasswordStealer and QBot in 2018, but adware and—another virus?!—in 2019. Of course, then there are our friends Emotet and TrickBot, sliding down the scale from first and second place to fourth and fifth.

Education

Institutions within the education sector have been hit heavily by cyberattacks in the last two years. Staff shortage and tight budgets are normally to blame for this industry's susceptibility. Although it appears that many of them have begun taking steps to improve their security posture, a considerable number of educational organizations remained vulnerable in 2019.

This year, the education industry was hit with 63 percent fewer threats, a total of 159,846 reported detections—

and a far cry from its 434,556 count in 2018. Figure 44 shows the top threats that affected this sector from 2018–2019.

In 2019, schools wisened up on ransomware, patching those old SMB vulnerabilities and removing dusty WannaCry infections. Cryptominers also fell off the list this year, replaced by yet more adware and an old Trojan called Bunitu, which exposes infected computers to be used as proxy servers for remote clients.

Top threats affecting the education sector

	2018	2019
1.	Trojan.Emotet	Trojan.Emotet
2.	Backdoor.Qbot	Trojan.Trickbot
3.	Trojan.Trickbot	Backdoor.Qbot
4.	Riskware.BitCoinMiner	Adware.MindSpark
5.	Ransom.WannaCrypt	Trojan.Bunitu

Figure 43. Top five threats impacting education in 2018 and 2019

Retail

The retail sector experienced a nominal uptick of activity in 2019 compared to 2018. At a 7 percent increase with 114,654 total detections, it remains one of the most sought-after targets by cybercriminals. This is because cybersecurity—not to mention privacy—have taken a backseat in retail. Having little resources allotted for

security and a severe lack of training among employees only compound the problem. Also, retail has a wide range of potential attack vectors, from Magecart skimmers, malvertising, and other online compromises to antiquated or vulnerable point-of-sale (POS) systems, to openness to fraud. Organizations in the retail

Top threats affecting the retail sector

	2018	2019
1.	Ransom.WannaCrypt	Trojan.Emotet
2.	Trojan.Emotet	Ransom.WannaCrypt
3.	Adware.Sogou	Adware.Sogou
4.	Rogue.UnVirex	Trojan.Trickbot
5.	Trojan.Trickbot	Trojan.DNSChanger

Figure 44. The top 5 malware families impacting retail in 2018 and 2019

sector are highly prone to attack, ripe with personally identifiable information (PII), payment information, credentials, and other valuable data for stealing.

It's not surprising to see adware make this list two years in a row. In fact, what's more surprising is that it isn't higher up on the list or that there aren't multiple families dominating the top five, considering retail are

some of the strongest advertisers themselves. In 2019, Emotet and TrickBot made more of an impact on retail organizations, and WannaCry infections fell one spot to second place. The Trojan DNSChanger jumped into fifth place, displacing UnVirex, a rogue anti-malware application.

Data privacy in 2019

For years, the story of data privacy remained the same: The public lamented how some of the biggest technology companies were allowed to misuse, lose, and sell their data, all without meaningful consequence. At the same time, the public was disappointingly content to offer private data for minor incentives, such as a single pizza to share with friends, according to a Massachusetts Institute of Technology study in 2017.

In 2019, that story changed. Last year, consumers more readily questioned the data collection practices of popular platforms like Facebook and Google, along with smaller mobile apps like FaceApp. Further, federal and state lawmakers introduced dozens of bills to better protect Americans from invasive data-sharing practices,

proposing new rights for citizens and stricter controls for the tech companies that vacuum up their data. The flurry of interest in data privacy—both by consumers and by lawmakers—became national and local news.

The Wirecutter, an outlet that reviews everything from electric kettles to yoga mats, reviewed consumer VPNs. A reporter for The Verge wrote about their decision to switch from Google's Chrome browser to the more privacy-focused Brave browser. The New York Times launched its ongoing "Privacy Project," a collection of stories, articles, and opinion pieces that look at the public's ongoing relationship with technology and privacy. This new year should mark the beginning of a long trend: Data privacy has finally become relevant.

Data privacy in commerce

As consumers pushed back against online platforms, a handful of small and large companies took the opportunity to turn data privacy into a competitive advantage.

The browser plugin-maker Ghostery released a full desktop application last year that bundles ad blocking, online tracker protection, and a VPN service. Malwarebytes released its own browser plugin last year, Browser Guard, which protects users from scams, hijackers, pop-up ads, and trackers. The open source developers at Purism shipped their first mobile phone, called the Librem 5, which the company promises will give users better control over their privacy and security. Encrypted email provider and Gmail competitor ProtonMail released an encrypted calendar tool. And Mozilla, developers of the Firefox browser, urged Apple to place extra barriers between iPhone users and online advertisers.

Away from iPhones, iPads, Macbooks and iMac Pros, Apple had a new, premiere good to offer in 2019, according to tech site Gizmodo: "Apple's newest luxury product is privacy." About one month after Mozilla's request, Apple unveiled a separate, impressive feature—a Single Sign-On service that prevents users' real email addresses from being shared with third parties. Bundled into the mobile operating system iOS 13, Apple also included more options for how users manage their location sharing preferences. These companies' efforts aimed to shape public concern about data privacy into

profit. But others moved in the opposite direction.

At the start of 2019, the Amazon-owned, smart doorbell maker Ring received its first major credibility hit: The company had reportedly allowed several employees to access user video with little oversight. In the following months, multiple lawmakers demanded answers about the company's data privacy policies, including how it protects video and images of children. Several outlets revealed Ring's close partnerships with hundreds of local law enforcement agencies in which, in return for being able to easily request user video data from a neighborhood, police were nudged into acting as Ring sales representatives for the communities they patrol.

Not far from Amazon's home privacy failure was Google, which somehow forgot to tell consumers that its home security product came installed with an internal microphone. The two tech juggernauts did little to correct the problem—Google apologized, Ring's CEO had a good "cry." But the same cannot be said of Facebook, which, in 2019, seemed to finally acknowledge years of data privacy pitfalls it had encountered, and sometimes dug itself.

In March, Facebook CEO Mark Zuckerberg told users that his company was turning over a new leaf: It would care—really—about privacy. Zuckerberg promised several new features that would respect users and their decisions to protect their information online. The new Facebook would include end-to-end encryption across its three largest platforms (Facebook Messenger,

Malwarebytes

Instagram, and WhatsApp), disappearing messages, posts, and photos, and a commitment to store less user data, while also refusing to put that data in countries with poor human rights records.

Facebook's end-to-end encryption project is [nowhere near done](#), but that is largely due to the expected technological complexity of rehauling and merging three different chat systems into one, secure system. Facebook's announcement received mixed responses from a public burnt out on the company's mishaps. Two weeks after Zuckerberg made his promises, Facebook admitted that it previously stored [hundreds of millions of user passwords](#) in plain text for years. Less than one month later, researchers found [146 GB of user data stored on third-party databases](#), and documents revealing earlier plans by Facebook to monetize user data leaked to the public. The documents also revealed that Facebook's plan to restrict certain third-party access to user data—though described to the public as a pro-

privacy move— [was focused on revenue](#).

Facebook finally paid a literal price for its poor user privacy protections in the summer, when the [US Federal Trade Commission fined the company $5 billion](#). Hit with the historic fine, Facebook's share prices...shot up. So, while data privacy is popular, it's not that popular.

Data privacy in US law

For a few of the above privacy fiascos, Congress stepped in. One Senator asked Amazon about Ring's partnerships with police and its data collection protections. Another Senator asked Google about how it failed to tell consumers about an internal microphone installed in a device that is meant for the home.

But 2019 was not just a year of Congressional questions. [It was a year of Congressional and legislative demands](#). Across the US, federal and state lawmakers introduced dozens of bills and bill amendments to protect Americans' data privacy. There were efforts to [make tech platforms "interoperable" with one another](#), to introduce new rights similar to those in the European Union's GDPR, to [pay people for their data](#), and to ensure that tech companies ascribe to a "duty to care" for their users' data.

One federal bill, introduced just before Thanksgiving, found warm reception from digital rights groups and

privacy advocates alike—[the Consumer Online Privacy Rights Act, or COPRA](#). COPRA aims to improve the relationship that Americans have with technology companies by empowering them with new rights to control their data, while also placing new restrictions on how companies collect and share that data.

If passed, Americans would enjoy new data privacy rights, including the rights to access, delete, and correct certain types of data, along with the right to take their data and move it to another company. Further, some data, which COPRA calls "sensitive covered data," would be prohibited from collection unless a user gives explicit, opt-in approval. That type of data includes passport numbers, Social Security numbers, information about physical and mental health, financial account usernames and passwords, biometrics, precise geolocation, communications content and metadata

(the time a message was sent and what user or phone number it was sent to), emails, phone numbers, and any information that reveals race, religion, sexual orientation and behavior, and union membership.

Perhaps most importantly, under COPRA, individuals would have the right to sue a company that violated their data privacy rights. And while COPRA gives the public new rights, it also gives companies new responsibilities. If the bill passes, companies would need to post a clear, easy-to-find data privacy policy on their websites, select and name a data privacy officer and data security officer, install data security practices, and commit to "data minimization," which would prohibit companies from processing or transferring certain user data "beyond what is reasonably necessary, proportionate, and limited."

Though many of COPRA's legislative contenders were introduced in the Senate, a separate data privacy bill introduced in the House of Representatives caught

attention last year—the Online Privacy Act of 2019. As the bill states, its purpose is "to provide for individual rights relating to privacy of personal information, to establish privacy and security requirements for covered entities relating to personal information, and to establish an agency to be known as the United States Digital Privacy Agency to enforce such rights and requirements, and for other purposes."

The proposed "United States Digital Privacy Agency" would serve as a government enforcement arm devoted to the increasing problem of data privacy violations. But that idea has sparked opposition by lawmakers who believe data privacy enforcement should remain with the Federal Trade Commission.

Unfortunately, that agency's track record for effective enforcement has been less than stellar—remember that when Facebook received its record-breaking $5 billion fine, its public stock price shot up.

Data privacy summary

On January 1, California's Consumer Privacy Act came into effect, almost a year and a half after it was signed by the former governor. Its eventual, regulatory impact will take time to assess, but its immediate, influential impact can already be measured.

As one of the first states to pass data privacy legislation, California's efforts have been matched by Maine and Nevada, which both passed data privacy laws last year.

Meanwhile, data privacy legislation has been introduced in a bevvy of other US states, including Connecticut, Hawaii, Illinois, Louisiana, Maryland, Massachusetts, Minnesota, New Jersey, New Mexico, New York, North Dakota, Pennsylvania, Rhode Island, Texas, and Washington. It appears that, whether Congress is ready or not, data privacy will become the law of the land.

2020 cybersecurity predictions

We've had a predictably unpredictable year for cybercrime in 2019, though many of the issues we were concerned about heading into the year turned out to be justified by increased activity or efforts to exploit, infect, collect, and blackmail users and their systems.

So, what about 2020? Is it going to be different? We've collected six highly likely predictions for the next 12 months, based on what we've seen in the past and what we're most afraid of in the future.

Ransomware attacks on organizations will continue at a more rapid pace, thanks to a diversification in attack vectors.

Over the last two years, malware developers have turned their focus to business targets over consumers, and ransomware is the threat of choice. While in the past, ransomware was typically delivered via exploit, 2019 saw a huge diversity in attack vectors dropping their favorite malware on organizations' endpoints, from exploit kits to botnets to hacking tools and manual infection.

We saw more vulnerabilities in 2017 and 2018 than in any year before, and 2019 was a close match in volume. More vulnerabilities means more exploits, and we're likely to see some of the 43,000 vulnerabilities discovered over the last two years show up in future EK offerings. We saw an example of this with BlueKeep, a software vulnerability that affects older versions of Microsoft Windows. It attacks an operating system's Remote Desktop Protocol (RDP), which connects to another computer over a network connection to quickly spread.

We've seen so much Emotet and TrickBot in the last two years—often the precursors to ransomware payloads—

we've starting saying their names in our sleep. The "triple threat" attack model has proven so effective, we expect even more Trojans and droppers and downloaders and botnets to join the party in 2020, offering affiliates a multitude of options for multi-stage attacks.

Finally, the development and prevalence of malicious hacking tools designed to more effectively attack networks will surely attract ransomware authors and affiliates to first penetrate, then decimate business infrastructures in 2020.

Bottom line, this ransomware problem isn't going away. We are likely to see more non-affiliated cybercriminals using tricks developed by state-sponsored malware groups (APT), as we did with EternalBlue. And if we do, we're in for a turbulent year of cybercrime.

Web skimmers will broaden their impact by going after more e-commerce platforms and plug-ins.

Looking at web skimming activity in 2019, we saw that there was no target too big to take on and no platform spared. As long as there is data to be stolen, criminals will put the effort into compromising online merchants directly or indirectly. The indirect attacks are, in fact, more dangerous, more pervasive, and easier to pull off. Essentially any third-party code such as web libraries

Malwarebytes

can be tampered with and loaded by a number of websites downstream. The current state of web security is still way behind, and most shops are not validating external content before loading it. That's why we expect to see a lot more of these attacks in 2020.

Another shift we will see is in the placement of skimmers. The majority of them are loaded at the checkout form, where customers enter their payment data. However, we now see skimmers impersonating payment processors, social engineering users with phishing-like tricks. Overall, this is a dynamic field where we can expect to see many novel attack techniques introduced over the next year.

Exploit kit activity will be at its highest since the post-Angler era.

While this may seem counterintuitive, since Internet Explorer market share is decreasing, we expect to see a surge of exploits and zero days pivot to Chrome and Chromium-based browsers in 2020. This year, we heard of at least a few zero-day vulnerabilities for Google Chrome. While rare and difficult to achieve, they are becoming more common. And since the browser market will be even more dominated by Chrome/Chromium because of Microsoft's Edge browser switch to a Chromium engine in January 2020, attackers will see these two as prime targets for exploitation.

In addition, we expect to see more drive-by attacks involving fileless malware. Magnitude EK, Underminer EK, and Purple Fox are all current examples of exploit kits that do not drop a typical payload on disk. Their success will fuel copycats and code-toppers in 2020 looking to edge out the old guard.

Biometrics and genetic tracking will draw an international outcry for data privacy laws.

Over the last year, we've seen some worrying developments in the collection, dissemination, selling, sharing, and stealing of health data. Consumer DNA testing kits drew warnings from the Pentagon about national security, accuracy, and career implications. Meanwhile, Canada, the United States, and China quietly amassed DNA databases for tracking immigrants and citizens. London's police force rolled out facial recognition cameras throughout the city in January 2020, much to the chagrin of its citizens. Google's purchase of Fitbit worried users about the dissemination of health data to advertisers, though the company publicly stated that health and wellness data would not be used for Google ads. Menstrual tracking apps have drawn much the same ire.

What will happen to this private healthcare information? Consumers are generally unaware that their health tracking devices could be used for unauthorized purposes, by legitimate companies and cybercriminals alike. And health tracking apps, facial recognition cameras, and DNA databases all paint concerning pictures when considered in the context of abuse by law enforcement, immigration, or repressive governments. The increased use of biometric data for authentication calls for stronger regulations for data privacy, and consumers and pro-privacy organizations will push hard on lawmakers to make that a reality in 2020.

Election security mishaps will undermine the confidence of US voters.

From compromised voting machines to fake news spread across the Internet and social media, US voters will call into question the reliability of the voting process, especially if the results of the 2020 presidential election once again fail to align with projections. Foreign

disinformation is at an all-time high, the result of nation-state actors tasked with destabilizing the country. Scammers and malware authors will, of course, use the election to spread their threats via phishing emails. However, we will also see plenty of deepfakes and cheapfakes technology used political purposes. And while some journalists will be able to verify the veracity of a particular soundbyte or video, users following propogandist or radial publications on both sides of the political spectrum will likely believe what they want to believe.

From a lower tech perspective, we expect to see floods of bot accounts on social media, created with more background and "humanity" than we've seen before. With a greater deployment of refined AI technologies, it will be harder to spot these accounts in 2020 because of how convincing they are made. Regardless of scam tactics or potential voting machine compromises, the real threat will be the attacks on our hearts and minds through social media and media manipulation.

Hybrid attacks with multi-stage payloads will escalate.

A multi-stage attack allows for an attacker to infiltrate a network in the most efficient and effective way possible. The first stage gathers information so the attacker can consider the best way to launch the next stage of the attack, which could include further infection across the network or the sale of the infection to someone who wants to mine for cryptocurrency or spread more malware.

While we already mentioned the triple threat in reference to ransomware, we predict there will be more types of malware developed in 2020 where the dwell time will be days or even weeks before attackers decide on what to do next. This is an interesting type of monetization by alternating payloads and conducting proper victim triage.

So those are our predictions for 2020, today. From bots to exploits to criminals stealing your DNA, the future is all about privacy, authentication, and non-repudiation. Let's hope that the attacks launched against our identities and how, or who we trust online, push forward new development of tech and policy that combats this growing trend.

Conclusion

Despite relative plateaus in threat numbers across the globe, it's been a fascinating and tumultuous year in cybercrime. Mac and Android threats increased in volume and severity. Businesses, governments, and schools were hit with sophisticated and diverse threats aimed at disrupting critical infrastructure. Adware inundated consumer and business users on all platforms and in all regions. Exploit kits, malvertising campaigns, and web skimmers threatened browsers. Consumers and lawmakers worried about the safety of their PII and other data. There was no oasis where users could escape from cybercrime in the 2019 threat landscape.

Ten years ago, average Internet users embraced social media, browsed without abandon, and just started experimenting with smart devices, holding mini computers in their hands instead of simple phones. Remote work was uncommon. Data breaches were unheard of. Cybercrime, security, and data privacy were hardly matters of public concern, relegated to lone basement-dwellers and super-technical early adopters. As we march into the next decade, considering how quaint those early days of the 2010s sound now, we realize how far we've come—and how seriously we should all be taking our cybersecurity practices now.

Contributors

Adam Kujawa
Director of Malwarebytes Labs

Wendy Zamora
Editor-in-chief, Malwarebytes Labs

Jerome Segura
Director of Threat Intelligence

Thomas Reed
Director of Mac and Mobile

Nathan Collier
Senior Malware
Intelligence Analyst, Mobile

Jovi Umawing
Senior Threat Content Writer

Chris Boyd
Senior Threat
Intelligence Analyst

Pieter Arntz
Senior Threat
Intelligence Analyst

David Ruiz
Threat Content Writer,
Online Privacy

LABS

🌐 blog.malwarebytes.com

@ corporate-sales@malwarebytes.com

📞 1.800.520.2796