Symantec

ISTR

Internet Security Threat Report

Volume 24 | February 2019

TABLE OF CONTENTS

1 BIG NUMBERS

2 YEAR-IN-REVIEW

Formjacking

Cryptojacking

Ransomware

Living off the land and supply chain attacks

Targeted attacks

Cloud

IoT

Election interference

3 FACTS AND FIGURES

Messaging

Malware

Mobile

Web attacks

Targeted attacks

IoT

Underground economy

METHODOLOGY

B1G NUMBERS

Symantec™

MALICIOUS URLS

://

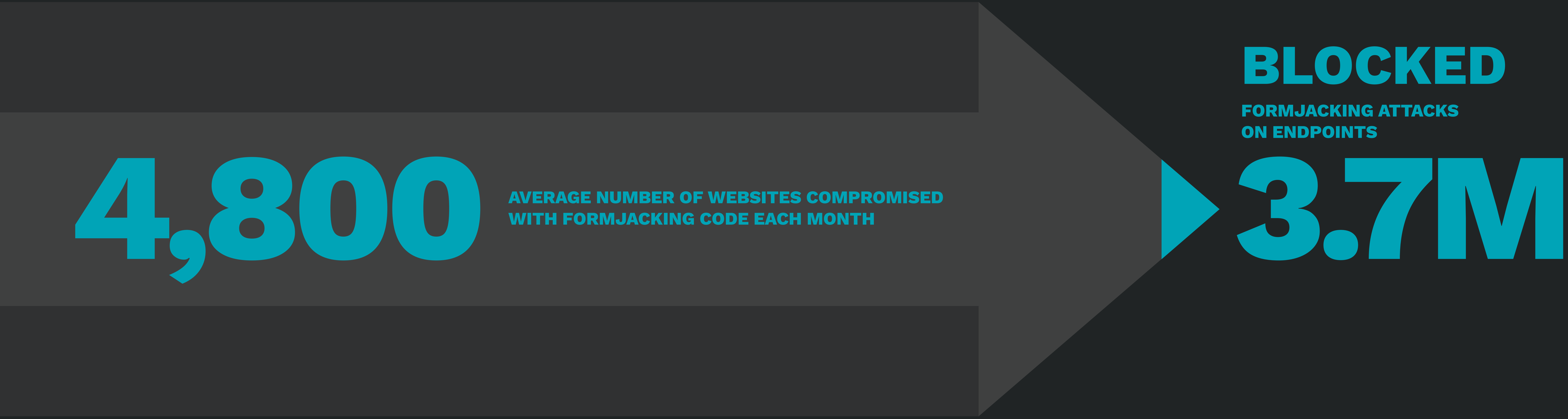
ONE IN TEN

URLS ARE MALICIOUS

WEB ATTACKS

56% ↑

FORMJACKING ATTACKS



4,800 AVERAGE NUMBER OF WEBSITES COMPROMISED WITH FORMJACKING CODE EACH MONTH

BLOCKED

FORMJACKING ATTACKS ON ENDPOINTS

3.7M

CRYPTOJACKING

8M
$362
4M
$48
JAN
DEC

4X

MORE CRYPTOJACKING EVENTS
BLOCKED IN 2018 VS 2017,
BUT TRENDING DOWN

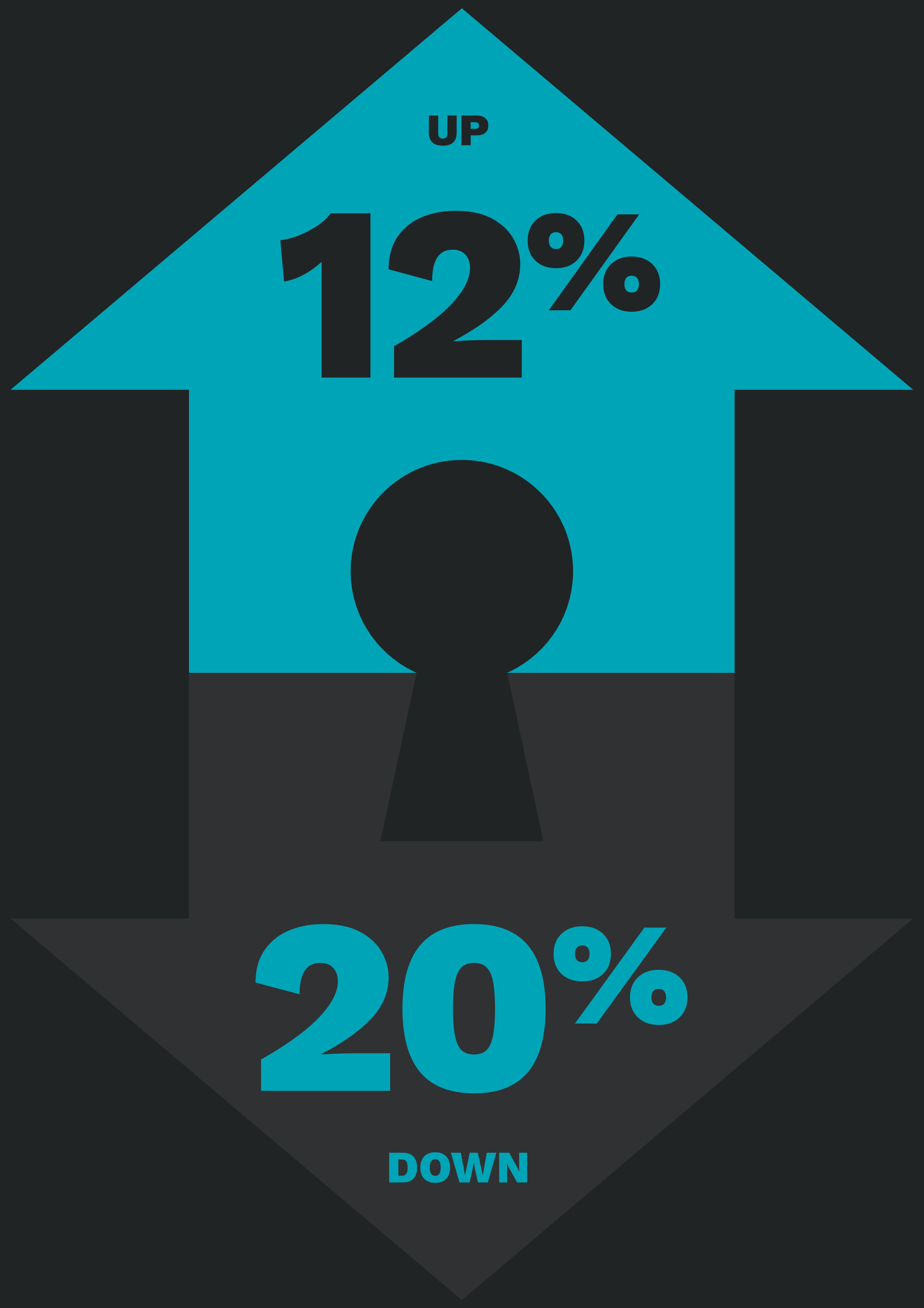
52% ↓

DROP IN CRYPTOJACKING EVENTS
BETWEEN JAN AND DEC 2018

90% ↓

DROP IN CRYPTOCURRENCY
VALUE (MONERO)

ENTERPRISE RANSOMWARE



UP

12%

20%

DOWN

OVERALL RANSOMWARE

MOBILE RANSOMWARE

33%

SUPPLY CHAIN ATTACKS

78%↑

MALICIOUS EMAIL

48%

OF MALICIOUS EMAIL ATTACHMENTS ARE OFFICE FILES, UP FROM 5% IN 2017

POWERSHELL

> 1000%

INCREASE IN MALICIOUS POWERSHELL SCRIPTS

NUMBER OF ATTACK GROUPS USING DESTRUCTIVE MALWARE

25% ↑

AVERAGE NUMBER OF ORGANIZATIONS TARGETED BY EACH ATTACK GROUP

55

YEAR IN REVIEW

2

Symantec™

{FORMJACKING}

CYBER CRIMINALS TARGET PAYMENT CARD DATA.

Incidents of formjacking—the use of malicious JavaScript code to steal credit card details and other information from payment forms on the checkout web pages of eCommerce sites—trended upwards in 2018.

Symantec data shows that 4,818 unique websites were compromised with formjacking code every month in 2018. With data from a single credit card being sold for up to $45 on underground markets, just 10 credit cards stolen from compromised websites could result in a yield of up to $2.2 million for cyber criminals each month. The appeal of formjacking for cyber criminals is clear.

Symantec blocked more than 3.7 million formjacking attempts in 2018, with more than 1 million of those blocks occurring in the last two months of the year alone. Formjacking activity occurred throughout 2018, with an anomalous spike in activity in May (556,000 attempts in that month alone), followed by a general upward trend in activity in the latter half of the year.

Much of this formjacking activity has been blamed on actors dubbed Magecart, which is believed to be several groups, with some, at least, operating in competition with one another. Magecart is believed to be behind several high-profile attacks, including those on British Airways and Ticketmaster, as well as attacks against British electronics retailer Kitronik and contact lens seller VisionDirect.

This increase in formjacking reflects the general growth in supply chain attacks that we discussed in ISTR 23, with Magecart in many cases targeting third-party services in order to get its code onto targeted websites. In the high-profile breach of Ticketmaster, for example, Magecart compromised a third-party chatbot, which loaded malicious code into the web browsers of visitors to Ticketmaster's website, with the aim of harvesting customers' payment data.

While attacks on household names make headlines, Symantec's telemetry shows that it is often small and medium sized retailers, selling goods ranging from clothing to gardening equipment to medical supplies, that have had formjacking code injected onto their websites. This is a global problem with the potential to affect any business that accepts payments from customers online.

The growth in formjacking in 2018 may be partially explained by the drop in the value of cryptocurrencies during the year: cyber criminals who may have used websites for cryptojacking may now be opting for formjacking. The value of stolen credit card details on the cyber underground is probably more assured than the value of cryptocurrencies in the current climate.

CRYPTOJACKING

TRENDING DOWN, BUT CERTAINLY NOT OUT.

Cryptojacking—where cyber criminals surreptitiously run coinminers on victims' devices without their knowledge and use their central processing unit (CPU) power to mine cryptocurrencies—was the story of the final quarter of 2017 and continued to be one of the dominant features in the cyber security landscape in 2018.

Cryptojacking activity peaked between December 2017 and February 2018, with Symantec blocking around 8 million cryptojacking events per month in that period. During 2018, we blocked more than four times as many cryptojacking events as in 2017—almost 69 million cryptojacking events in the 12-month period, compared to just over 16 million in 2017. However, cryptojacking activity did fall during the year, dropping by 52 percent between January and December 2018. Despite this downward trend, we still blocked more than 3.5 million cryptojacking events in December 2018.

This is still significant activity, despite the fact that cryptocurrency values—which were at record-breaking highs at the end of 2017 and played a major role in driving the initial growth of cryptojacking—dropped significantly in 2018. While this may have led some of the initial adopters of cryptojacking to turn to other ways to make money, such as formjacking, it's clear a significant cohort of cyber criminals still think cryptojacking is worth their time. We also saw some cryptojacking criminals targeting enterprises in 2018, with the WannaMine (MSH.Bluwimps) cryptojacking script, which uses the Eternal Blue exploit made famous by WannaCry to spread through enterprise networks, rendering some devices unusable due to high CPU usage.

The majority of cryptojacking activity continued to originate from browser-based coinminers in 2018. Browser-based coin mining takes place inside a web browser and is implemented using scripting languages. If a web page contains a coin-mining script, the web page visitors' computing power will be used to mine for cryptocurrency for as long as the web page is open. Browser-based miners allow cyber criminals to target even fully patched devices and can also allow them to operate stealthily without the activity being noticed by victims.

We predicted that cryptojacking activity by cyber criminals would be largely dependent on cryptocurrency values remaining high. As cryptocurrency values have fallen, we have also observed a decline in the volume of cryptojacking events. However, they haven't fallen at the same rate as cryptocurrency values—in 2018, the value of Monero dropped by almost 90 percent while cryptojacking dropped by around 52 percent. This means some cyber criminals must still find it profitable or are biding their time until another surge in cryptocurrency values. It also shows that there are other elements of cryptojacking that make it attractive to cyber criminals, such as the anonymity it offers and the low barriers to entry. It looks like cryptojacking is an area that will continue to have a role in the cyber crime landscape.

RANSOMWARE

For the first time since 2013, we observed a decrease in ransomware activity during 2018, with the overall number of ransomware infections on endpoints dropping by 20 percent. WannaCry, copycat versions, and Petya, continued to inflate infection figures. When these worms are stripped out from the statistics, the drop in infection numbers is steeper: a 52 percent fall.

However, within these overall figures there was one dramatic change. Up until 2017, consumers were the hardest hit by ransomware, accounting for the majority of infections. In 2017, the balance tipped towards enterprises, with the majority of infections occurring in businesses. In 2018, that shift accelerated and enterprises accounted for 81 percent of all ransomware infections. While overall ransomware infections were down, enterprise infections were up by 12 percent in 2018.

This shift in victim profile was likely due to a decline in exploit kit activity, which was previously an important channel for ransomware delivery. During 2018, the chief ransomware distribution method was email campaigns. Enterprises tend to be more affected by email-based attacks since email remains the primary communication tool for organizations.

Alongside this, a growing number of consumers are exclusively using mobile devices, and their essential data is often backed up in the cloud. Since most major ransomware families still target Windows-based computers, the chances of consumers being exposed to ransomware is declining.

ACTIVITY BEGINS TO DROP, BUT REMAINS A CHALLENGE FOR ORGANIZATIONS.

Another factor behind the drop in overall ransomware activity is Symantec's increased efficiency at blocking ransomware earlier in the infection process, either via email protection or using technologies such as behavioral analysis or machine learning. Also contributing to the decline is the fact that some cyber crime gangs are losing interest in ransomware. Symantec saw a number of groups previously involved in spreading ransomware move to delivering other malware such as banking Trojans and information stealers.

However, some groups are continuing to pose a severe threat. In further bad news for organizations, a notable number of highly damaging targeted ransomware attacks hit organizations in 2018, many of which were conducted by the SamSam group. During 2018, Symantec found evidence of 67 SamSam attacks, mostly against organizations in the U.S. In tandem with SamSam, other targeted ransomware groups have become more active.

Additional targeted threats have also emerged. Activity involving Ryuk (Ransom.Hermes) increased significantly in late 2018. This ransomware was responsible for an attack in December where the printing and distribution of several well-known U.S. newspapers was disrupted.

Dharma/Crysis (Ransom.Crysis) is also often used in a targeted fashion against organizations. The number of Dharma/Crysis infection attempts seen by Symantec more than tripled during 2018, from an average of 1,473 per month in 2017 to 4,900 per month in 2018.

In November, two Iranian nationals were indicted in the U.S. for their alleged involvement with SamSam. It remains to be seen whether the indictment will have any impact on the group's activity.

LIVING OFF THE LAND AND SUPPLY CHAIN ATTACKS

REMAIN A STAPLE OF THE NEW THREAT LANDSCAPE.

In previous reports, we highlighted the trend of attackers opting for off-the-shelf tools and operating system features to conduct attacks. This trend of “living off the land” shows no sign of abating—in fact, there was a significant increase in certain activity in 2018. PowerShell usage is now a staple of both cyber crime and targeted attacks—reflected by a massive 1,000 percent increase in malicious PowerShell scripts blocked in 2018 on the endpoint.

In 2018, Microsoft Office files accounted for almost half (48 percent) of all malicious email attachments, jumping up from just 5 percent in 2017. Cyber crime groups, such as Mealybug and Necurs, continued to use macros in Office files as their preferred method to propagate malicious payloads in 2018, but also experimented with malicious XML files and Office files with DDE payloads.

Zero-day exploit usage by targeted attack groups continued to decline in 2018. Only 23 percent of attack groups were known to use zero days, down from 27 percent in 2017. We also began seeing attacks which rely solely on living off the land techniques and don’t use any malicious code. The targeted attack group Gallmaker is an example of this shift, with the group exclusively using generally available tools to carry out its malicious activities.

Self-propagating threats continued to create headaches for organizations but, unlike worms of old, modern worms don’t use remotely exploitable vulnerabilities to spread. Instead, worms such as Emotet (Trojan.Emotet) and Qakbot (W32.Qakbot) use simple techniques including dumping passwords from memory or brute-forcing access to network shares to laterally move across a network.

Supply chain attacks continued to be a feature of the threat landscape, with attacks increasing by 78 percent in 2018. Supply chain attacks, which exploit third-party services and software to compromise a final target, take many forms, including hijacking software updates and injecting malicious code into legitimate software. Developers continued to be exploited as a source of supply chain attacks, either through attackers stealing credentials for version control tools, or by attackers compromising third-party libraries that are integrated into larger software projects.

The surge in formjacking attacks in 2018 reinforced how the supply chain can be a weak point for online retailers and eCommerce sites. Many of these formjacking attacks were the result of the attackers compromising third-party services commonly used by online retailers, such as chatbots or customer review widgets.

Both supply chain and living off the land attacks highlight the challenges facing organizations and individuals, with attacks increasingly arriving through trusted channels, using fileless attack methods or legitimate tools for malicious purposes. While we block on average 115,000 malicious PowerShell scripts each month, this only accounts for less than 1 percent of overall PowerShell usage. Effectively identifying and blocking these attacks requires the use of advanced detection methods such as analytics and machine learning.

MORE AMBITIOUS AND STEALTHIER

Targeted attack actors continued to pose a significant threat to organizations during 2018, with new groups emerging and existing groups continuing to refine their tools and tactics. The larger, more active attack groups appeared to step up their activity during 2018. The 20 most active groups tracked by Symantec targeted an average of 55 organizations over the past three years, up from 42 between 2015 and 2017.

TARGETED ATTACKS.

One notable trend was the diversification in targets, with a growing number of groups displaying an interest in compromising operational computers, which could potentially permit them to mount disruptive operations if they chose to do so.

This tactic was pioneered by the Dragonfly espionage group, which is known for its attacks on energy companies. During 2018, we observed the Thrip group compromise a satellite communications operator and infect computers running software that monitors and controls satellites. The attack could have given Thrip the ability to seriously disrupt the company's operations.

We also saw the Chafer group compromise a telecoms services provider in the Middle East. The company sells solutions to multiple telecoms operators in the region and the attack may have been intended to facilitate surveillance of end-user customers of those operators.

This interest in potentially disruptive attacks is also reflected in the number of groups known to use destructive malware, up by 25 percent in 2018.

During 2018, Symantec exposed four previously unknown targeted attack groups, bringing the number of targeted attack groups first exposed by Symantec since 2009 to 32. While Symantec exposed four new groups in both 2017 and 2018, there was a big shift in the way these groups were uncovered. Two out of the four new groups exposed during 2018 were uncovered through their use of living off the land tools. Indeed, one of those two groups (Gallmaker) doesn't use any malware in its attacks, relying exclusively on living off the land and publicly available hacking tools.

Living off the land has been increasingly used by targeted attack groups in recent years because it can help attackers maintain a low profile by hiding their activity in a mass of legitimate processes. This trend was one of the main motivations for Symantec to create its Targeted Attack Analytics (TAA) solution in 2018, which leverages advanced artificial intelligence to spot patterns of malicious activity associated with targeted attacks. Twice during 2018 we discovered previously unknown targeted attack groups in investigations that began with TAA triggered by living off the land tools. The rise in the use of living off the land tools has been mirrored by the decline of other, older attack techniques. The number of targeted attack groups known to use zero-day vulnerabilities was 23 percent, down from 27 percent at the end of 2017.

One of the most dramatic developments during 2018 was the significant increase in indictments in the United States against people alleged to be involved in state-sponsored espionage. Forty-nine individuals or organizations were indicted during 2018, up from four in 2017 and five in 2016. While most of the headlines were devoted to the indictment of 18 alleged Russian agents, most of whom were charged with involvement in attacks relating to the 2016 presidential election, the indictments were far more wide ranging. Alongside Russian nationals, 19 Chinese individuals or organizations were charged, along with 11 Iranians, and one North Korean.

This sudden glare of publicity may disrupt some of the organizations named in these indictments. It will severely limit the ability of indicted individuals to travel internationally, potentially hampering their ability to mount operations against targets in other countries.

CLOUD

SPECTRE

STORAGE

MELTDOWN

SECURITY CHALLENGES EMERGE ON MULTIPLE FRONTS.

From simple misconfiguration issues to vulnerabilities in hardware chips, in 2018 we saw the wide range of security challenges that the cloud presents.

Poorly secured cloud databases continued to be a weak point for organizations. In 2018, S3 buckets emerged as an Achilles heel for organizations, with more than 70 million records stolen or leaked as a result of poor configuration. This was on the heels of a spate of ransomware attacks against open databases such as MongoDB in 2017, which saw attackers wipe their contents and seek payment in order to restore them. Attackers didn't stop there—also targeting container deployment systems such Kubernetes, serverless applications and other publicly exposed API services. There's a common theme across these incidents—poor configuration.

There are numerous tools widely available which allow potential attackers to identify misconfigured cloud resources on the internet. Unless organizations take action to properly secure their cloud resources, such as following the advice provided by Amazon for securing S3 buckets, they are leaving themselves open to attack.

A more insidious threat to the cloud emerged in 2018 with the revelation of several vulnerabilities in hardware chips. Meltdown and Spectre exploit vulnerabilities in a process known as speculative execution. Successful exploitation provides access to memory locations that are normally forbidden. This is particularly problematic for cloud services because while cloud instances have their own virtual processors, they share pools of memory—meaning that a successful attack on a single physical system could result in data being leaked from several cloud instances.

Meltdown and Spectre weren't isolated cases—several variants of these attacks were subsequently released into the public domain throughout the year. They were also followed up by similar chip-level vulnerabilities such as Speculative Store Bypass and Foreshadow, or L1 Terminal Fault. This is likely just the start, as researchers and attackers home in on vulnerabilities at the chip level, and indicates that there are challenging times ahead for the cloud.

IoT

IN THE CROSSHAIRS OF CYBER CRIMINALS AND TARGETED ATTACK GROUPS.

While worms and bots continued to account for the vast majority of Internet of Things (IoT) attacks, in 2018 we saw a new breed of threat emerge as targeted attack actors displayed an interest in IoT as an infection vector.

The overall volume of IoT attacks remained high in 2018 and consistent (-0.2 percent) compared to 2017. Routers and connected cameras were the most infected devices and accounted for 75 and 15 percent of the attacks respectively. It's unsurprising that routers were the most targeted devices given their accessibility from the internet. They're also attractive as they provide an effective jumping-off point for attackers.

The notorious Mirai distributed denial of service (DDoS) worm remained an active threat and, with 16 percent of the attacks, was the third most common IoT threat in 2018. Mirai is constantly evolving and variants use up to 16 different exploits, persistently adding new exploits to increase the success rate for infection, as devices often remain unpatched. The worm also expanded its target scope by going after unpatched Linux servers. Another noticeable trend was the increase in attacks against industrial control systems (ICS). The Thrip group went after satellites, and Triton attacked industrial safety systems, leaving them vulnerable to sabotage or extortion attacks. Any computing device is a potential target.

The emergence of VPNFilter in 2018 represented an evolution of IoT threats. VPNFilter was the first widespread persistent IoT threat, with its ability to survive a reboot making it very difficult to remove. With an array of potent payloads at its disposal, such as man in the middle (MitM) attacks, data exfiltration, credential theft, and interception of SCADA communications, VPNFilter was a departure from traditional IoT threat activity such as DDoS and coin mining. It also includes a destructive capability which can "brick," or wipe a device at the attackers' command, should they wish to destroy evidence. VPNFilter is the work of a skilled and well-resourced threat actor and demonstrates how IoT devices are now facing attack from many fronts.

ELECTION INTERFERENCE 2018

With the 2016 U.S. presidential election impacted by several cyber attacks, such as the attack on the Democratic National Committee (DNC), all eyes were on the 2018 midterms. And, just one month after Election Day had passed, the National Republican Congressional Committee (NRCC) confirmed its email system was hacked by an unknown third party in the run-up to the midterms. The hackers reportedly gained access to the email accounts of four senior NRCC aides and may have collected thousands of emails over the course of several months.

Then, in January 2019, the DNC revealed it was targeted by an unsuccessful spear-phishing attack shortly after the midterms had ended. The cyber espionage group APT29, which has been attributed by the U.S. Department of Homeland Security (DHS) and the FBI to Russia, is thought to be responsible for the campaign.

In July and August 2018, multiple malicious domains mimicking websites belonging to political organizations were discovered and shut down by Microsoft. The cyber espionage group APT28 (which has also been attributed by Homeland Security and the FBI to Russia) is thought to have set-up some of these sites as part of a spear-phishing campaign targeting candidates in the 2018 midterms. To combat website spoofing attacks like this, Symantec launched Project Dolphin, a free security tool for website owners.

Adversaries continued to focus on using social media platforms to influence voters in 2018. While this is nothing new, the tactics used have become more sophisticated. Some Russia-linked accounts, for example, used third parties to purchase social media ads for them and avoided using Russian IP addresses or Russian currency. Fake accounts also began to focus more on promoting events and rallies, which are not monitored as closely as politically targeted ads.

Social media companies and government agencies took a more proactive role in combatting election interference in 2018. Facebook set up a "war room" to tackle election interference and blocked numerous accounts and pages suspected of being linked to foreign entities engaged in attempts to influence politics in the U.S., U.K., Middle East, and Latin America.

Twitter removed over 10,000 bots posting messages encouraging people not to vote and updated its rules for identifying fake accounts and protecting the integrity of elections. Twitter also released an archive of tweets associated with two state-sponsored propaganda operations that abused the platform to spread disinformation intended to sway public opinion.

Other efforts to combat election interference in 2018 included the United States Cyber Command contacting Russian hackers directly to tell them they had been identified by U.S. operatives and were being tracked; the DHS offering free security assessments of state election machines and processes; and the widespread adoption of so-called Albert sensors, hardware that helps the federal government monitor for evidence of interference with computers used to run elections.

ALWAR

EB **3** ATTAC

MESSAGING

FACTS AND

oT **FIGURES**

ARGETED

MOBILE

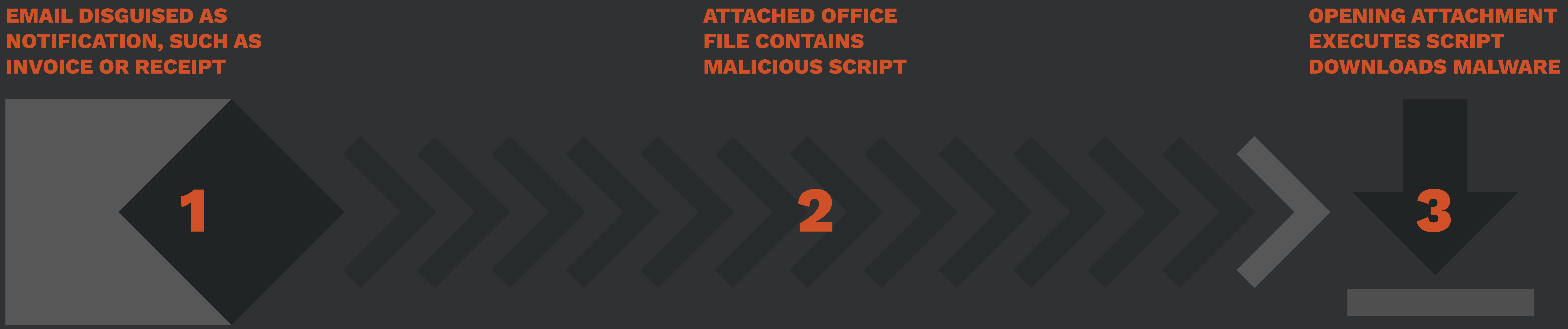
MESSAGING

In 2018, employees of small organizations were more likely to be hit by email threats—including spam, phishing, and email malware—than those in large organizations. We also found that spam levels continued to increase in 2018, as they have done every year since 2015, with 55 percent of emails received in 2018 being categorized as spam. Meanwhile, the email malware rate remained stable, while phishing levels declined, dropping from 1 in 2,995 emails in 2017, to 1 in 3,207 emails in 2018. The phishing rate has declined every year for the last four years.

We also saw fewer URLs used in malicious emails as attackers refocused on using malicious email attachments as a primary infection vector. The use of malicious URLs in emails had jumped to 12.3 percent in 2017, but it dropped back to 7.8 percent in 2018. Symantec telemetry shows that Microsoft Office users are the most at risk of falling victim to email-based malware, with Office files accounting for 48 percent of malicious email attachments, jumping from 5 percent in 2017.

48% ↑

OF MALICIOUS EMAIL ATTACHMENTS ARE OFFICE FILES UP FROM 5% IN 2017


EMAIL DISGUISED AS NOTIFICATION, SUCH AS INVOICE OR RECEIPT
1
ATTACHED OFFICE FILE CONTAINS MALICIOUS SCRIPT
2
OPENING ATTACHMENT EXECUTES SCRIPT DOWNLOADS MALWARE
3

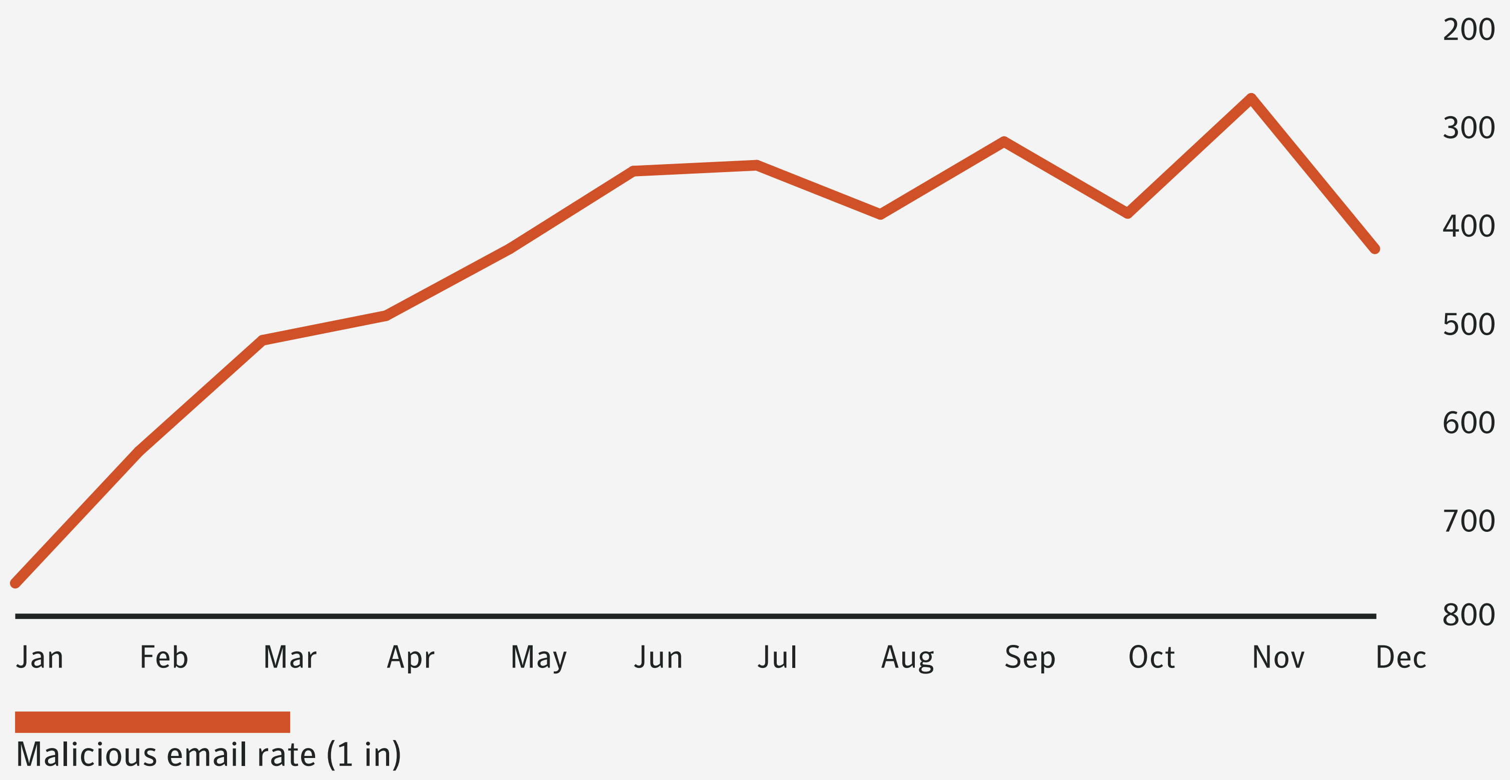
MALICIOUS EMAIL RATE (YEAR)

2018
1 in 412

MALICIOUS EMAIL URL RATE (YEAR)

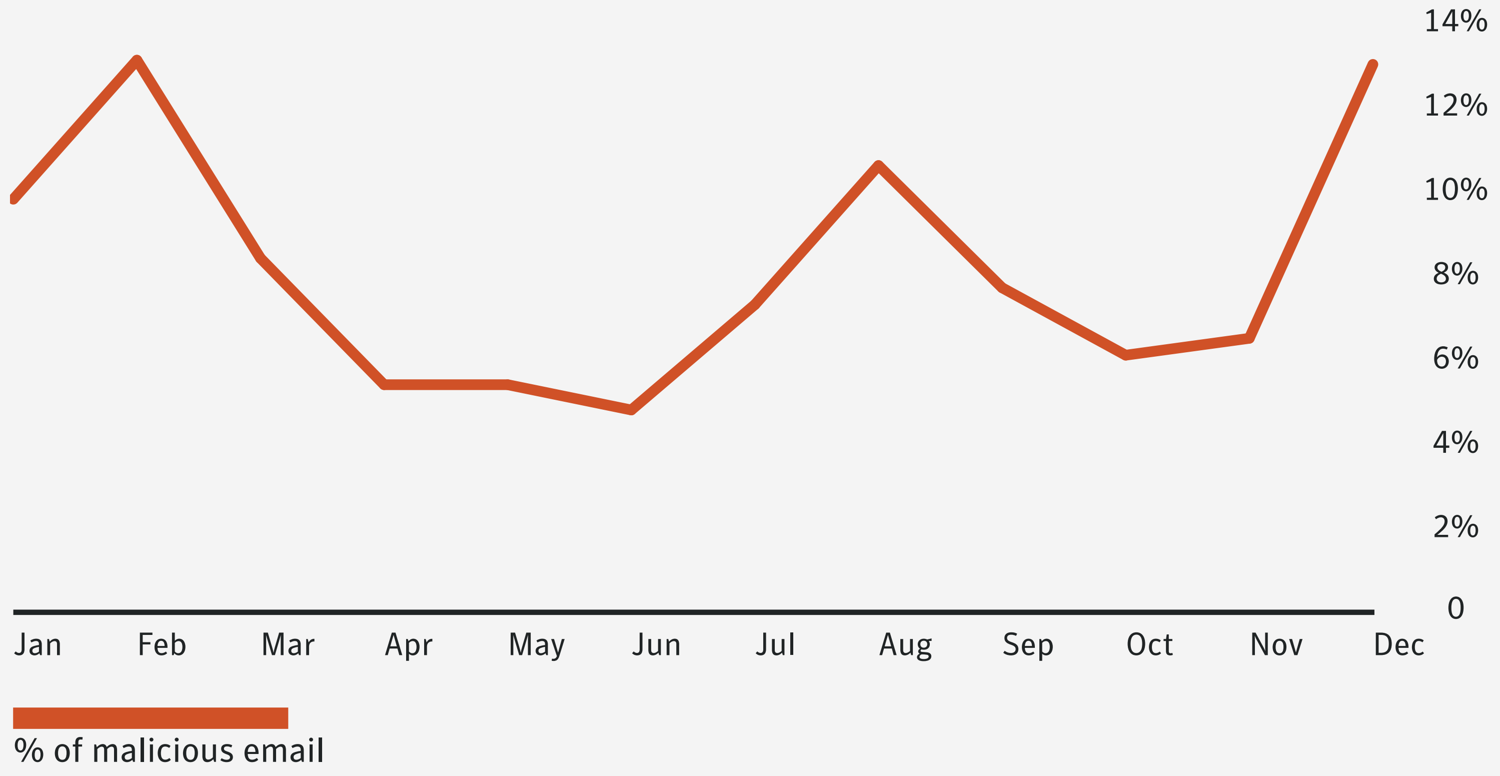
2018
7.8%

MALICIOUS EMAIL RATE (MONTH)

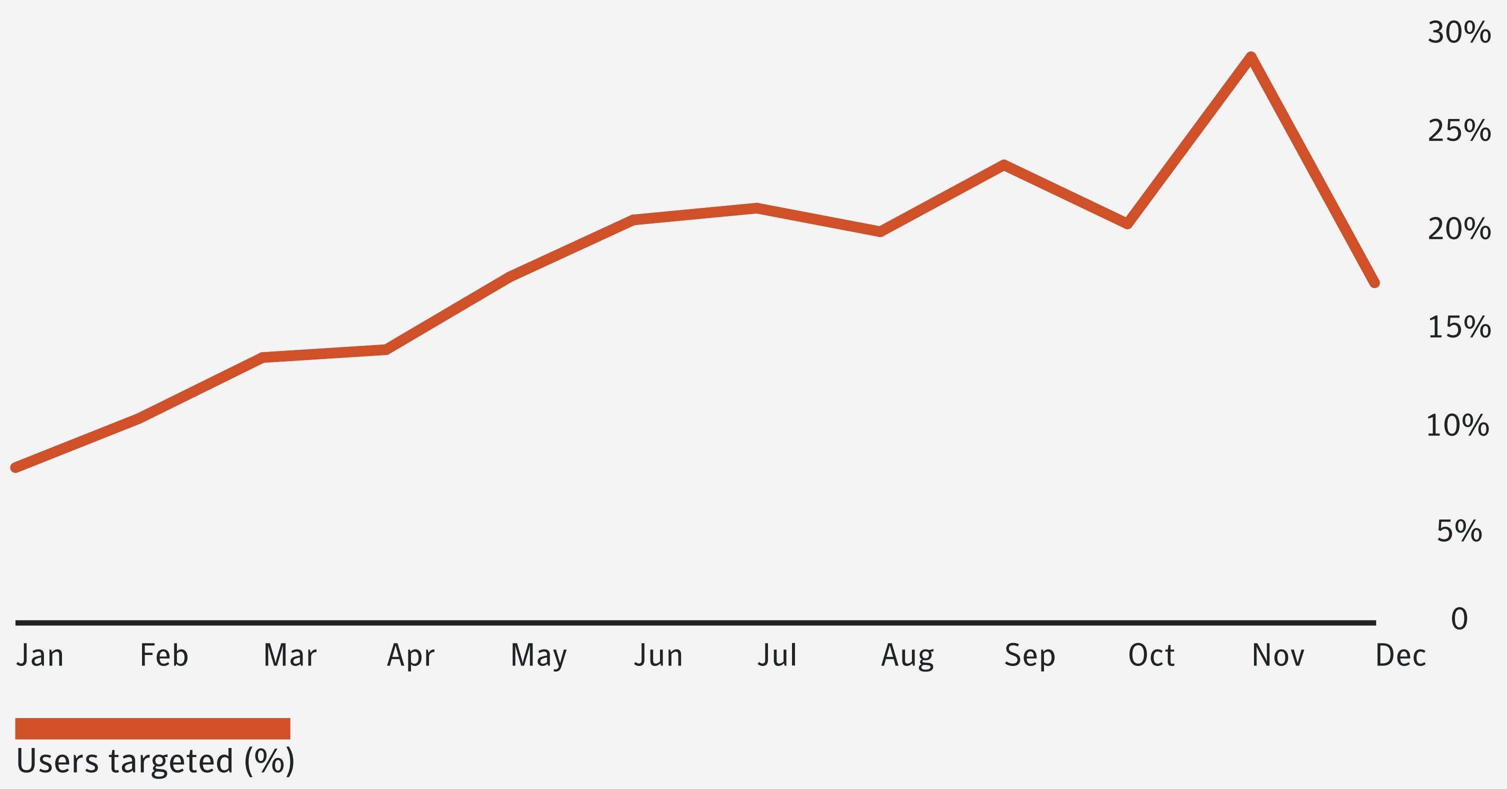


The pecentage of users hit with malicious email trended up during 2018

MALICIOUS EMAIL URL RATE (MONTH)



MALICIOUS EMAIL PER USER (MONTH)



MALICIOUS EMAIL RATE BY INDUSTRY (YEAR)

INDUSTRY	MALICIOUS EMAIL RATE (1 IN)
Mining	258
Agriculture, Forestry, & Fishing	302
Public Administration	302
Manufacturing	369
Wholesale Trade	372
Construction	382
Nonclassifiable Establishments	450
Transportation & Public Utilities	452
Finance, Insurance, & Real Estate	491
Services	493
Retail Trade	516

MALICIOUS EMAIL URL RATE BY INDUSTRY (YEAR)

INDUSTRY	EMAIL MALWARE (%)
Agriculture, Forestry, & Fishing	11.2
Retail Trade	10.9
Mining	8.9
Services	8.2
Construction	7.9
Public Administration	7.8
Finance, Insurance, & Real Estate	7.7
Manufacturing	7.2
Nonclassifiable Establishments	7.2
Wholesale Trade	6.5
Transportation & Public Utilities	6.3

Employees of smaller organizations were more likely to be hit by email threats—including spam, phishing, and email malware—than those in large organizations.

MALICIOUS EMAIL PER USER BY INDUSTRY (YEAR)

INDUSTRY	USERS TARGETED (%)
Mining	38.4
Wholesale Trade	36.6
Construction	26.6
Nonclassifiable Establishments	21.2
Retail Trade	21.2
Agriculture, Forestry, & Fishing	21.1
Manufacturing	20.6
Public Administration	20.2
Transportation & Public Utilities	20.0
Services	11.7
Finance, Insurance, & Real Estate	11.6

MALICIOUS EMAIL RATE BY ORGANIZATION SIZE (YEAR)

ORGANIZATION SIZE	MALICIOUS EMAIL RATE (1 IN)
1-250	323
251-500	356
501-1000	391
1001-1500	823
1501-2500	440
2501+	556

MALICIOUS EMAIL URL RATE BY ORGANIZATION SIZE (YEAR)

ORGANIZATION SIZE	MALICIOUS EMAIL (%)
1-250	6.6
251-500	8.3
501-1000	6.6
1001-1500	8.3
1501-2500	7.3
2501+	8.6

MALICIOUS EMAIL PER USER BY ORGANIZATION SIZE (YEAR)

ORGANIZATION SIZE	USERS TARGETED (1 IN)
1-250	6
251-500	6
501-1000	4
1001-1500	7
1501-2500	4
2501+	11

MALICIOUS EMAIL RATE BY COUNTRY (YEAR)

COUNTRY	MALICIOUS EMAIL RATE (1 IN)
Saudi Arabia	118
Israel	122
Austria	128
South Africa	131
Serbia	137
Greece	142
Oman	160
Taiwan	163
Sri Lanka	169
UAE	183
Thailand	183
Poland	185
Norway	190
Hungary	213
Qatar	226
Singapore	228
Italy	232
Netherlands	241
UK	255
Ireland	263
Luxembourg	272
Hong Kong	294
China	309
Denmark	311
Malaysia	311
Colombia	328
Switzerland	334
Papua New Guinea	350
Germany	352
Philippines	406
Belgium	406
Brazil	415
South Korea	418
Portugal	447
Spain	510
Finland	525
Canada	525
Sweden	570
New Zealand	660
USA	674
France	725
Australia	728
India	772
Mexico	850
Japan	905

MALICIOUS EMAIL URL RATE BY COUNTRY (YEAR)

COUNTRY	MALICIOUS EMAIL (%)
Brazil	35.7
Mexico	29.7
Norway	12.8
Sweden	12.4
Canada	11.5
New Zealand	11.3
Colombia	11.0
Australia	10.9
France	10.5
Finland	9.7
Switzerland	9.5
Spain	9.4
Qatar	8.9
USA	8.9
Portugal	8.4
India	8.3
Philippines	8.1
Singapore	7.7
Luxembourg	7.3
Italy	7.1
Austria	6.7
South Africa	6.7
Papua New Guinea	6.5
South Korea	6.5
Germany	6.3
Japan	6.3
Belgium	6.1
UK	6.1
Hungary	5.9
Saudi Arabia	5.2
Denmark	5.1
Hong Kong	5.1
Malaysia	5.1
China	4.9
Netherlands	4.9
Serbia	4.4
Taiwan	4.4
UAE	4.2
Sri Lanka	4.1
Ireland	3.9
Oman	3.6
Thailand	3.4
Greece	3.3
Poland	2.8
Israel	1.9

TOP EMAIL THEMES (YEAR)

SUBJECT TOPIC	PERCENT
Bill	15.7
Email delivery failure	13.3
Package delivery	2.4
Legal/law enforcement	1.1
Scanned document	0.3

TOP EMAIL KEYWORDS (YEAR)

WORDS	PERCENT
invoice	13.2
mail	10.2
sender	9.2
payment	8.9
important	8.5
message	7.7
new	7.2
returned	6.9
:	6.9
delivery	6.6

TOP MALICIOUS EMAIL ATTACHMENT TYPES (YEAR)

FILE TYPE	PERCENT
.doc, .dot	37.0
.exe	19.5
.rtf	14.0
.xls, .xlt, .xla	7.2
.jar	5.6
.html, htm	5.5
.docx	2.3
.vbs	1.8
.xlsx	1.5
.pdf	0.8

TOP MALICIOUS EMAIL ATTACHMENT CATEGORIES (YEAR)

FILE TYPE	PERCENT
Scripts	47.5
Executables	25.7
Other	25.1

MONTHLY AVERAGE NUMBER OF ORGANIZATIONS TARGETED BY BEC SCAMS (YEAR)

AVERAGE
5,803

AVERAGE BEC EMAILS PER ORGANIZATION (YEAR)

AVERAGE
4.5

TOP BEC EMAIL KEYWORDS (YEAR)

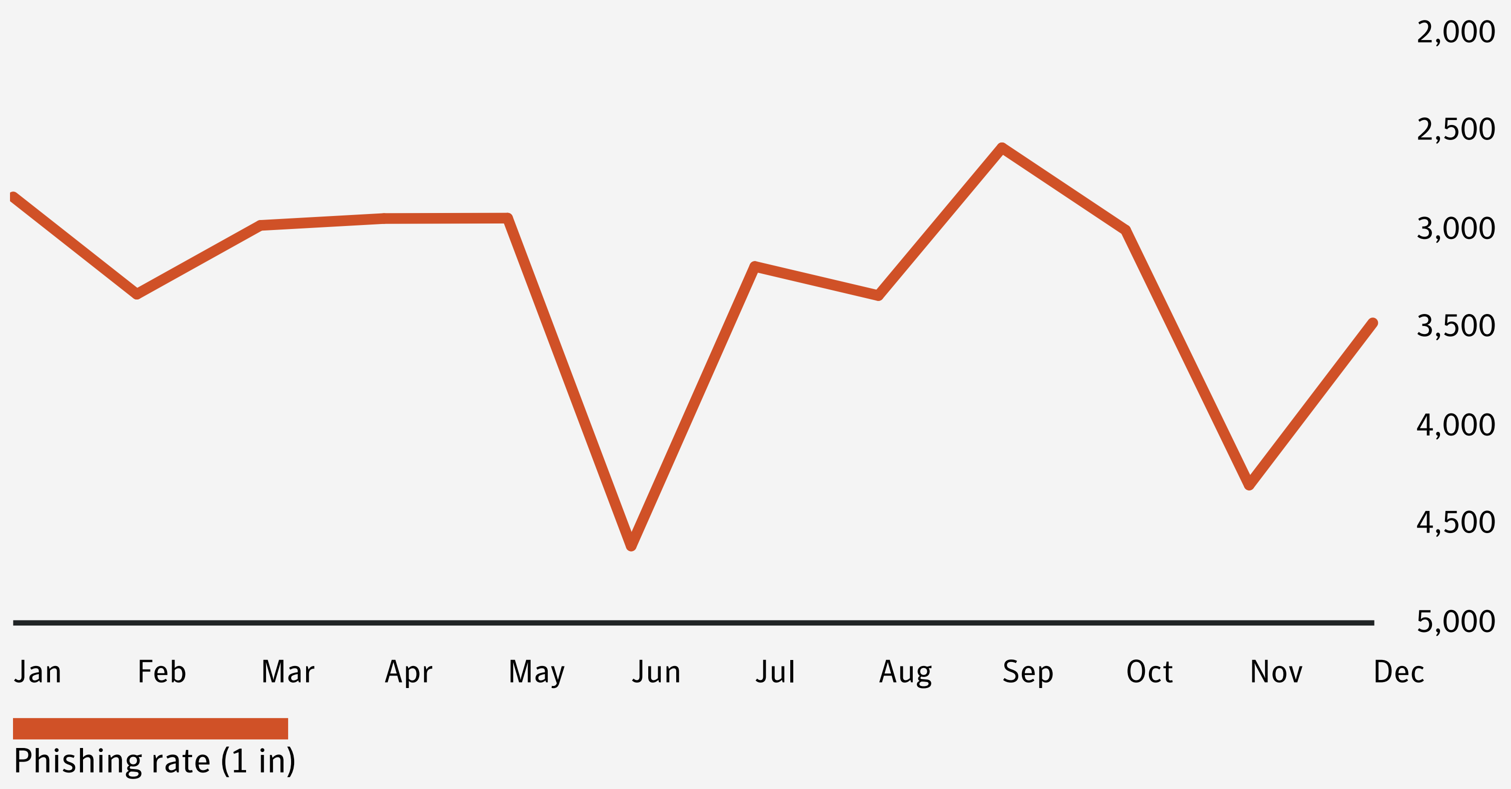
SUBJECT	PERCENT
urgent	8.0
request	5.8
important	5.4
payment	5.2
attention	4.4
outstanding payment	4.1
info	3.6
important update	3.1
attn	2.3
transaction	2.3

EMAIL PHISHING RATE (YEAR)

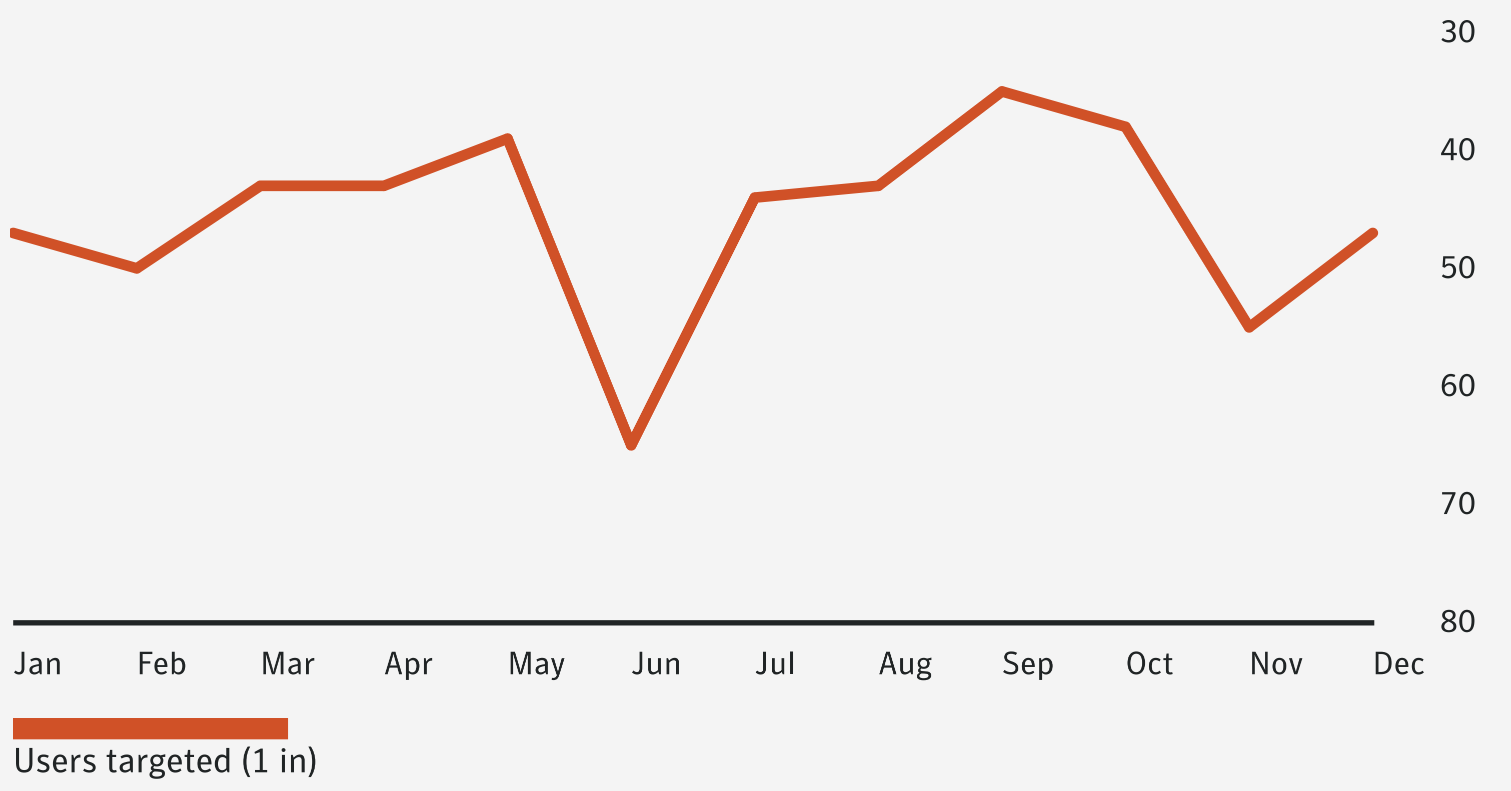
PHISHING RATE (1 IN)
3,207

Phishing levels declined, dropping from 1 in 2,995 emails in 2017, to 1 in 3,207 emails in 2018.

EMAIL PHISHING RATE (MONTH)



EMAIL PHISHING RATE PER USER (MONTH)



EMAIL PHISHING RATE BY INDUSTRY (YEAR)

INDUSTRY	PHISHING RATE (1 IN)
Agriculture, Forestry, & Fishing	1,769
Finance, Insurance, & Real Estate	2,628
Mining	2,973
Wholesale Trade	3,042
Public Administration	3,473
Services	3,679
Construction	3,960
Retail Trade	3,971
Manufacturing	3,986
Nonclassifiable Establishments	5,047
Transportation & Public Utilities	5,590

EMAIL PHISHING RATE PER USER BY INDUSTRY (YEAR)

INDUSTRY	USERS TARGETED (1 IN)
Wholesale Trade	22
Agriculture, Forestry, & Fishing	28
Mining	30
Retail Trade	36
Construction	39
Finance, Insurance, & Real Estate	46
Manufacturing	52
Nonclassifiable Establishments	53
Public Administration	57
Transportation & Public Utilities	62
Services	64

EMAIL PHISHING RATE BY ORGANIZATION SIZE (YEAR)

ORGANIZATION SIZE	PHISHING RATE (1 IN)
1-250	2,696
251-500	3,193
501-1000	3,203
1001-1500	6,543
1501-2500	3,835
2501+	4,286

EMAIL PHISHING RATE PER USER BY ORGANIZATION SIZE (YEAR)

ORGANIZATION SIZE	USERS TARGETED (1 IN)
1-250	52
251-500	57
501-1000	30
1001-1500	56
1501-2500	36
2501+	82

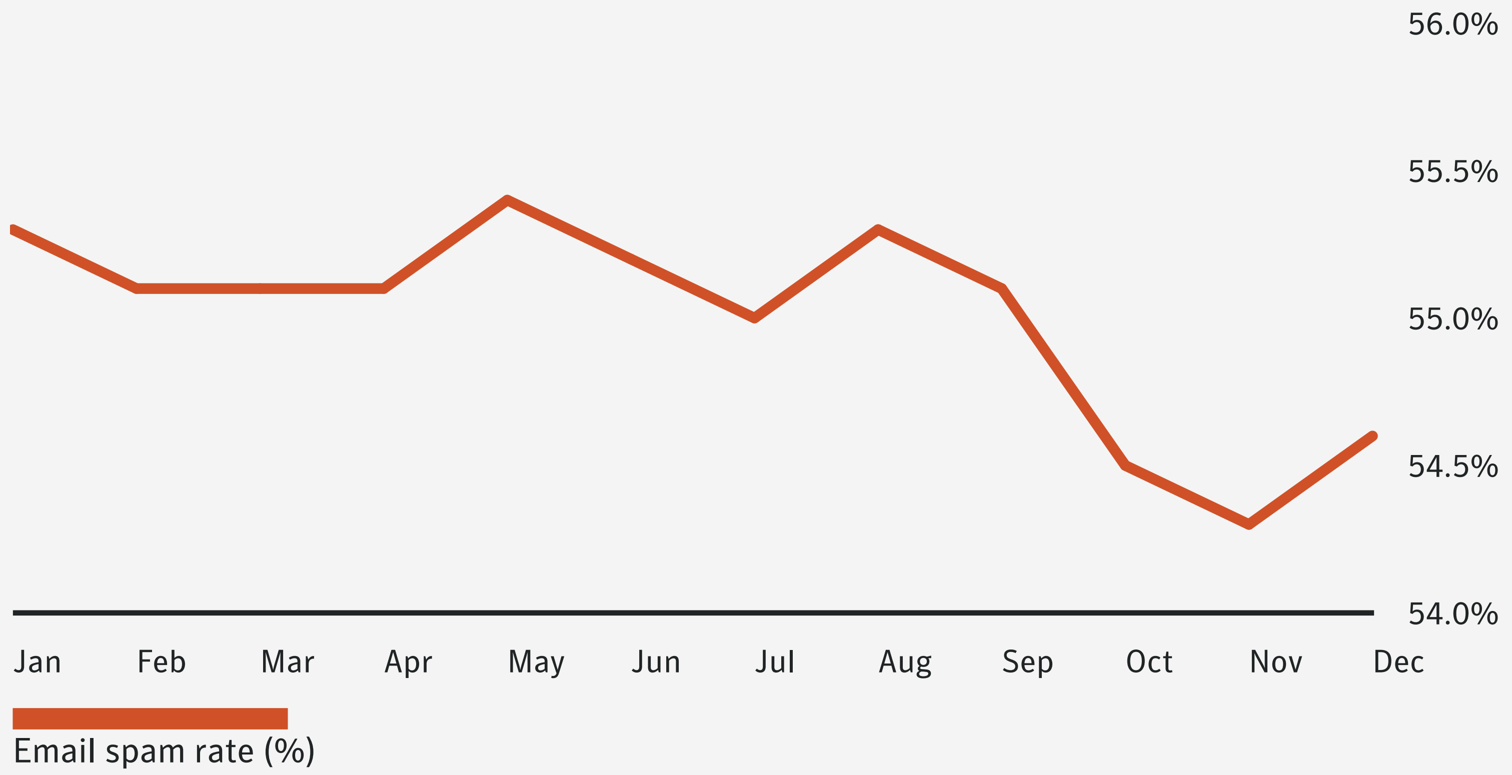
EMAIL PHISHING RATE BY COUNTRY (YEAR)

COUNTRY	PHISHING RATE (1 IN)
Saudi Arabia	675
Norway	860
Netherlands	877
Austria	1,306
South Africa	1,318
Hungary	1,339
Thailand	1,381
Taiwan	1,712
Brazil	1,873
UAE	2,312
New Zealand	2,446
Hong Kong	2,549
Singapore	2,857
Luxembourg	2,860
Italy	3,048
Qatar	3,170
China	3,208
USA	3,231
Ireland	3,321
Belgium	3,322
Sweden	3,417
Australia	3,471
Switzerland	3,627
Spain	3,680
UK	3,722
Oman	3,963
Papua New Guinea	4,011
Sri Lanka	4,062
Portugal	4,091
Philippines	4,241
Canada	4,308
Greece	4,311
Israel	4,472
Colombia	4,619
Malaysia	4,687
Germany	5,223
Denmark	5,312
Mexico	5,389
France	5,598
India	5,707
Serbia	6,376
Finland	6,617
Japan	7,652
South Korea	8,523
Poland	9,653

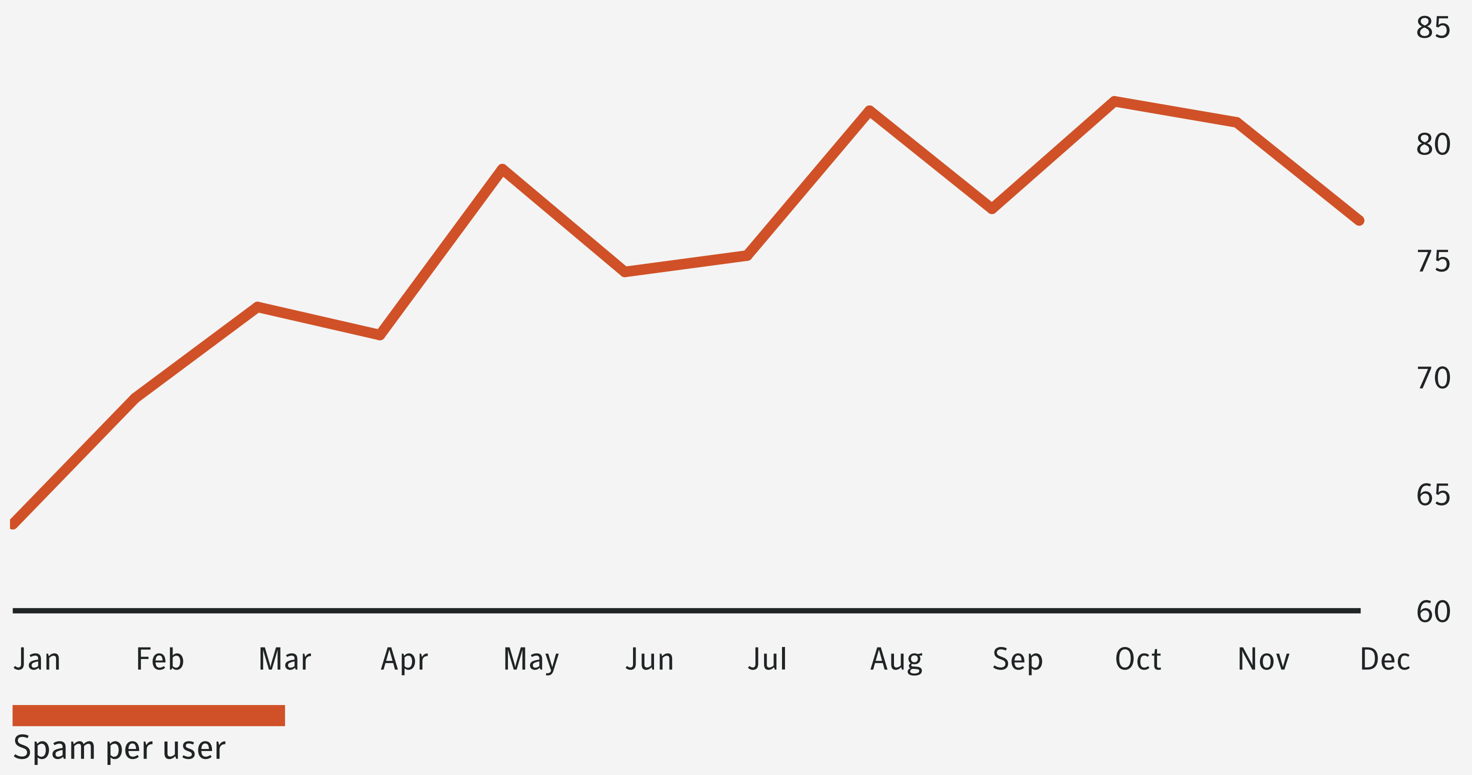
EMAIL SPAM RATE (YEAR)

EMAIL SPAM RATE (%)
55

EMAIL SPAM RATE (MONTH)



EMAIL SPAM PER USER (MONTH)



EMAIL SPAM RATE BY INDUSTRY (YEAR)

INDUSTRY	EMAIL SPAM RATE (%)
Mining	58.3
Finance, Insurance, & Real Estate	56.7
Manufacturing	55.1
Public Administration	54.9
Agriculture, Forestry, & Fishing	54.6
Transportation & Public Utilities	54.6
Nonclassifiable Establishments	54.2
Services	54.1
Retail Trade	53.7
Construction	53.6
Wholesale Trade	52.6

EMAIL SPAM PER USER BY INDUSTRY (YEAR)

INDUSTRY	SPAM PER USER
Wholesale Trade	135
Retail Trade	111
Mining	109
Construction	103
Nonclassifiable Establishments	97
Transportation & Public Utilities	93
Manufacturing	79
Agriculture, Forestry, & Fishing	66
Public Administration	63
Finance, Insurance, & Real Estate	61
Services	59

EMAIL SPAM RATE BY ORGANIZATION SIZE (YEAR)

ORGANIZATION SIZE	EMAIL SPAM RATE (%)
1-250	55.9
251-500	53.6
501-1000	54.5
1001-1500	56.9
1501-2500	53.7
2501+	54.9

EMAIL SPAM PER USER BY ORGANIZATION SIZE (YEAR)

ORGANIZATION SIZE	SPAM PER USER
1-250	55
251-500	57
501-1000	109
1001-1500	125
1501-2500	107
2501+	55

EMAIL SPAM RATE BY COUNTRY (YEAR)

COUNTRY	EMAIL SPAM RATE (%)
Saudi Arabia	66.8
China	62.2
Brazil	60.8
Sri Lanka	60.6
Norway	59.1
Oman	58.6
Sweden	58.3
Mexico	58.1
UAE	58.1
USA	57.5
Colombia	56.8
Belgium	56.2
Serbia	55.8
Singapore	55.4
UK	54.8
Germany	54.8
Taiwan	54.5
Austria	54.4
Finland	54.4
Hungary	54.4
Greece	54.2
Israel	54.1
Denmark	54.1
France	54
Netherlands	53.9
Australia	53.9
New Zealand	53.4
Canada	53.4
Italy	53.4
Poland	53.2
Spain	52.9
Qatar	52.6
South Korea	52.4
Portugal	52.1
Luxembourg	51.4
Malaysia	51.4
Thailand	51.1
Ireland	51
India	50.9
South Africa	50.8
Switzerland	50.8
Hong Kong	50.5
Papua New Guinea	50
Philippines	49.5
Japan	48.7

MALWARE

Emotet continued to aggressively expand its market share in 2018, accounting for 16 percent of financial Trojans, up from 4 percent in 2017. Emotet was also being used to spread Qakbot, which was in 7th place in the financial Trojans list, accounting for 1.8 percent of detections. Both of these threats present further serious challenges for organizations due to their self-propagating functionality.

Use of malicious PowerShell scripts increased by 1,000 percent in 2018, as attackers continued the movement towards living off the land techniques. A common attack scenario uses Office macros to call a PowerShell script, which in turn downloads the malicious payload. Office macro downloaders accounted for the majority of downloader detections, while VBS.Downloader and JS.Downloader threats declined.

In 2018, we also blocked 69 million cryptojacking events—four times as many events as we blocked in 2017. However, cryptojacking activity declined by 52 percent between January and December 2018. This mirrored the decline in cryptocurrency values, albeit at a slower rate. For the first time since 2013, the overall number of ransomware infections fell, dropping by more than 20 percent year-on-year. However, enterprise detections bucked the trend, increasing by 12 percent, demonstrating that ransomware continues to be a problem for enterprises. Fewer new ransomware families emerged in 2018, indicating that ransomware may hold less appeal for cyber criminals than it previously did.

EMOTET

SELF-PROPAGATING EMOTET JUMPS UP TO

16%

FROM 4% in 2017

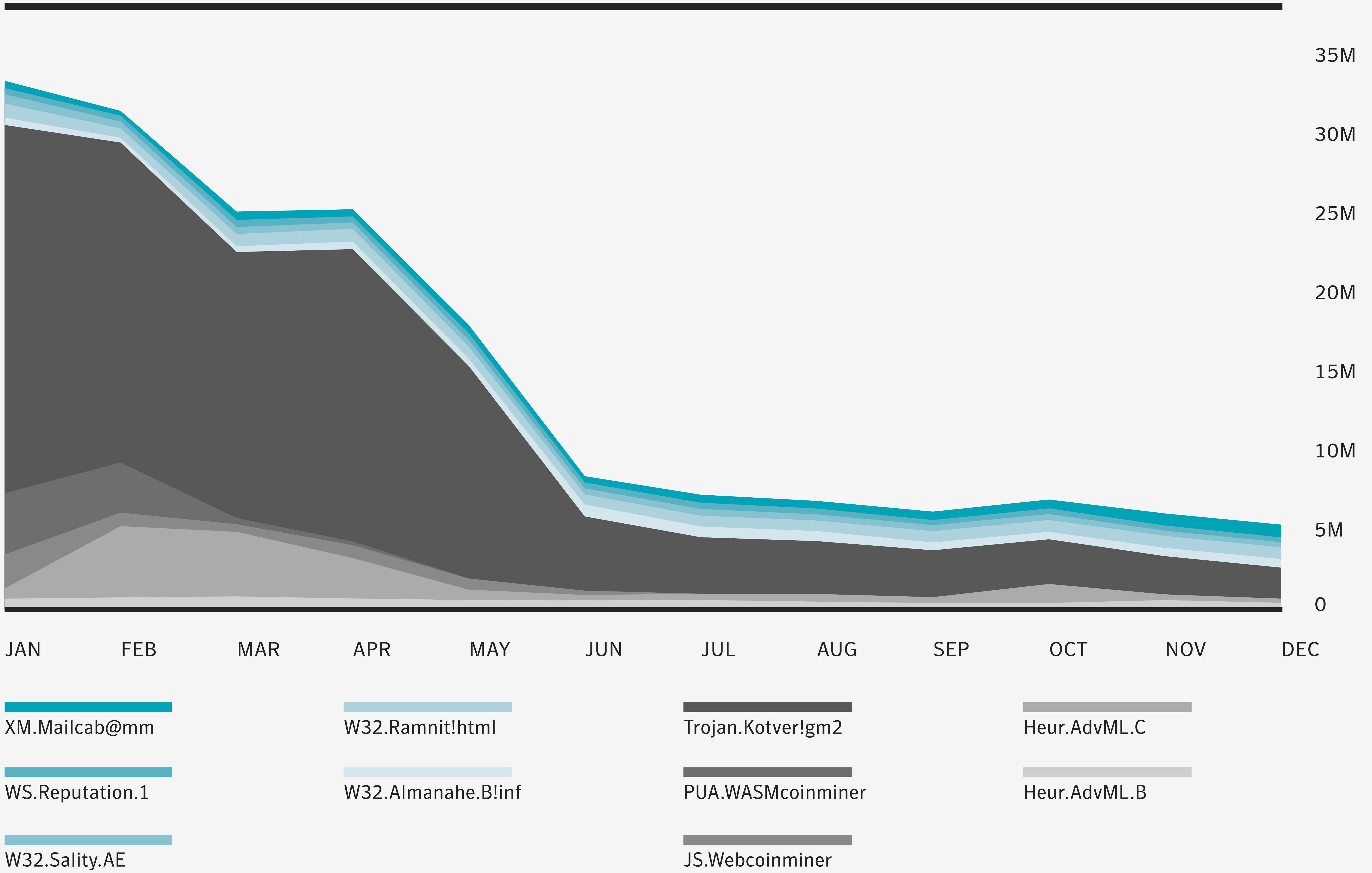
8,000,000
$450
$400
7,000,000
$350
$300
6,000,000
$250
$200
5,000,000
$150
$100
4,000,000
$50
0
3,000,000
TOTAL CRYPTOJACKING EVENTS BY MONTH
VALUE OF MONERO

NEW MALWARE VARIANTS (YEAR)

YEAR	NEW VARIANTS	PERCENT CHANGE
2016	357,019,453	0.5
2017	669,947,865	87.7
2018	246,002,762	-63.3

Emotet continued to aggressively expand its market share in 2018, accounting for 16 percent of financial Trojans, up from 4 percent in 2017.

TOP NEW MALWARE VARIANTS (MONTH)

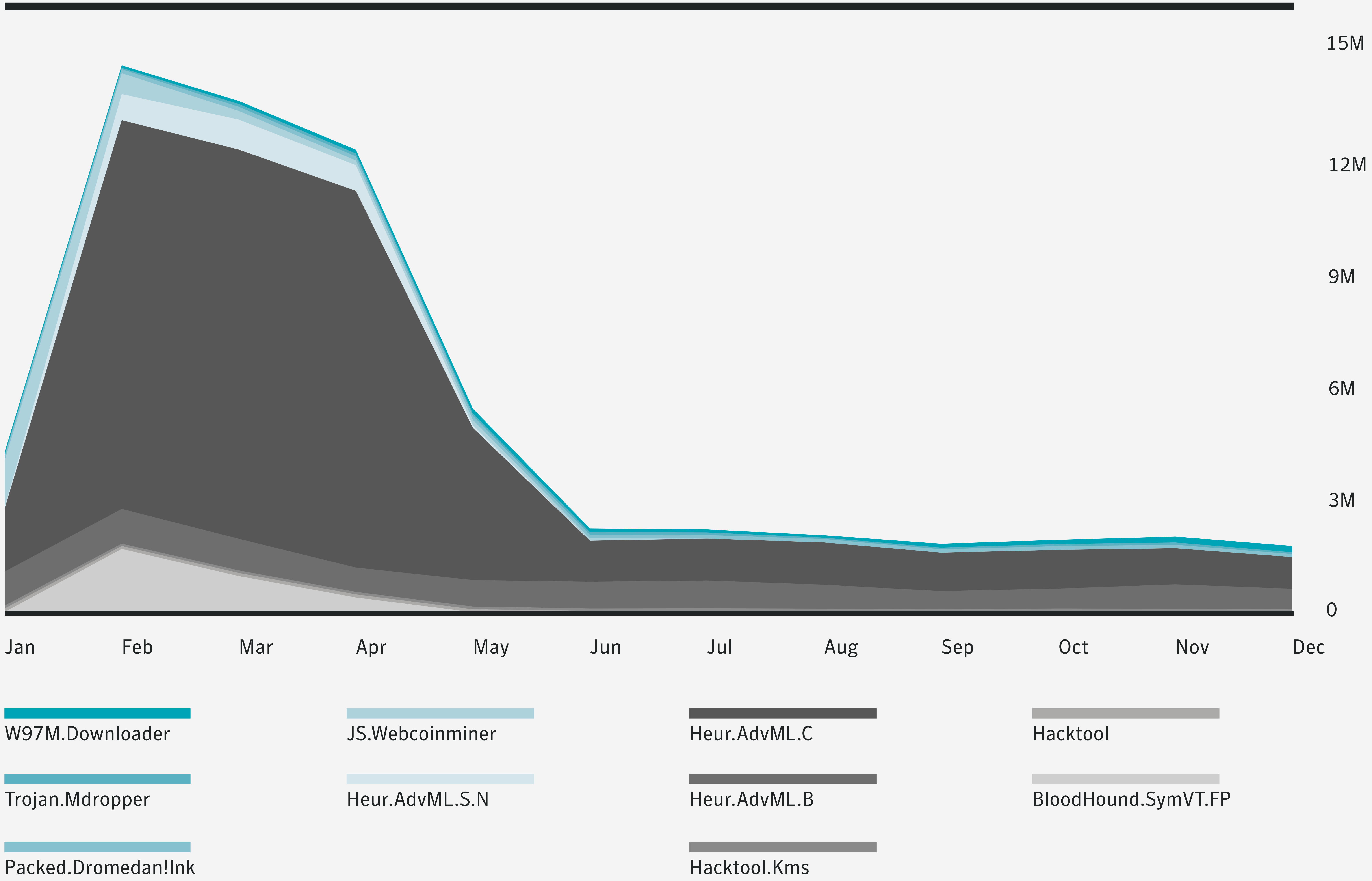


TOP MALWARE (YEAR)

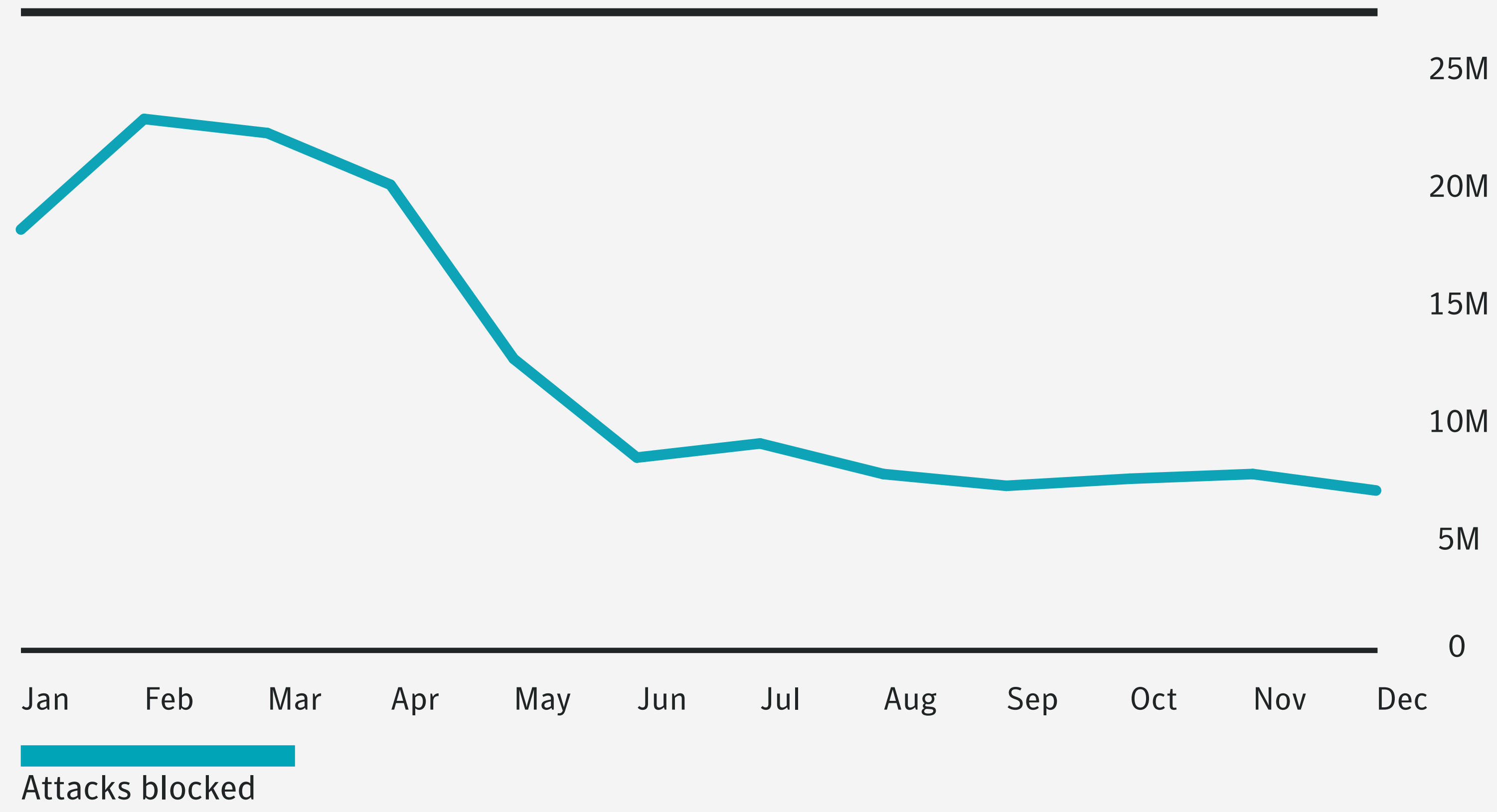
THREAT NAME	ATTACKS BLOCKED	PERCENT
Heur.AdvML.C	43,999,373	52.1
Heur.AdvML.B	8,373,445	9.9
BloodHound.SymVT.FP	3,193,779	3.8
JS.Webcoinminer	2,380,725	2.8
Heur.AdvML.S.N	2,300,919	2.7
W97M.Downloader	1,233,551	1.5
Packed.Dromedan!lnk	1,215,196	1.4
Hacktool	846,292	1.0
Hacktool.Kms	763,557	0.9
Trojan.Mdropper	679,248	0.8

Cyber crime groups, such as Mealybug and Necurs, continued to use macros in Office files as their preferred method to propagate malicious payloads in 2018.

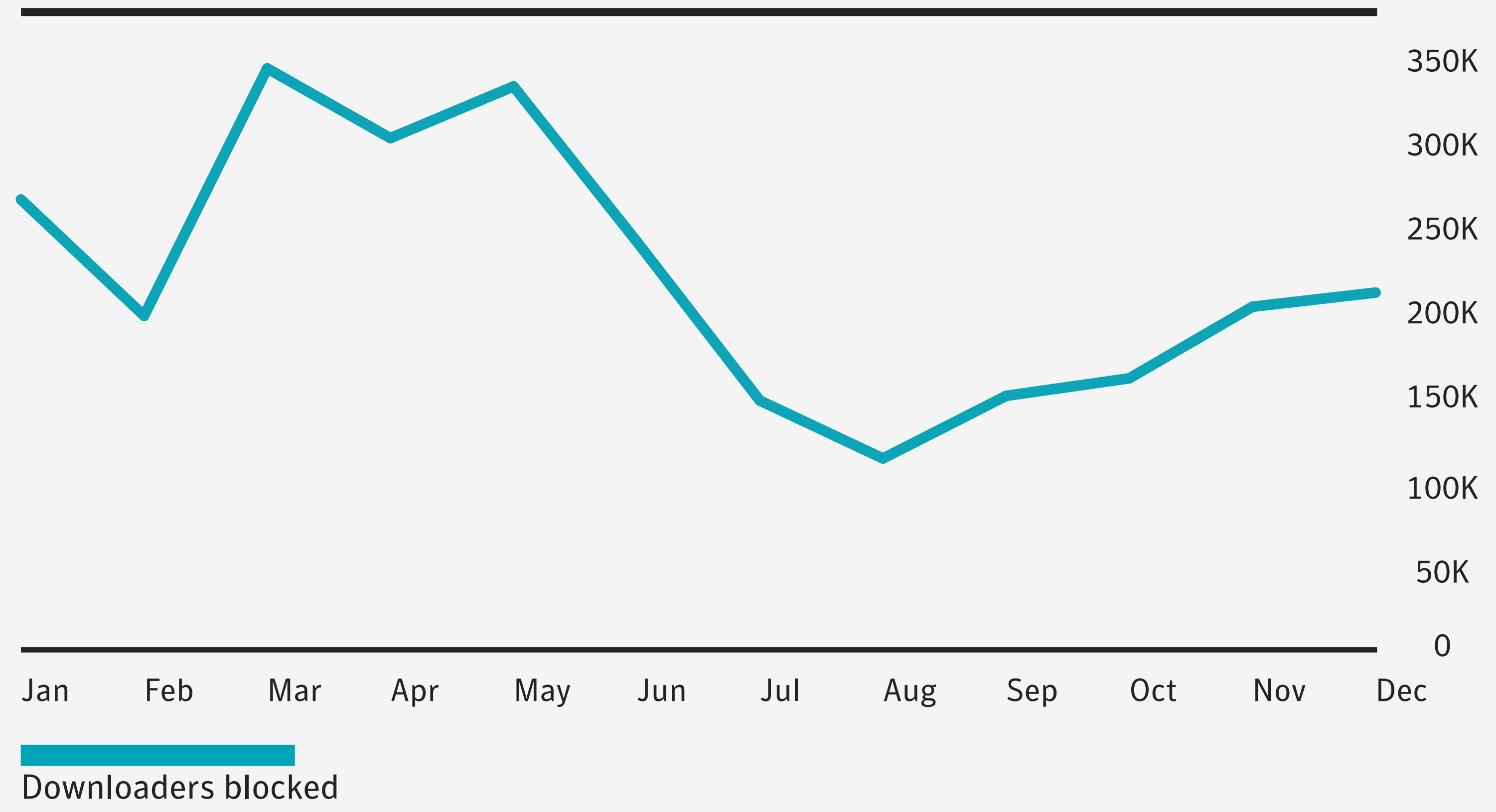
TOP MALWARE (MONTH)



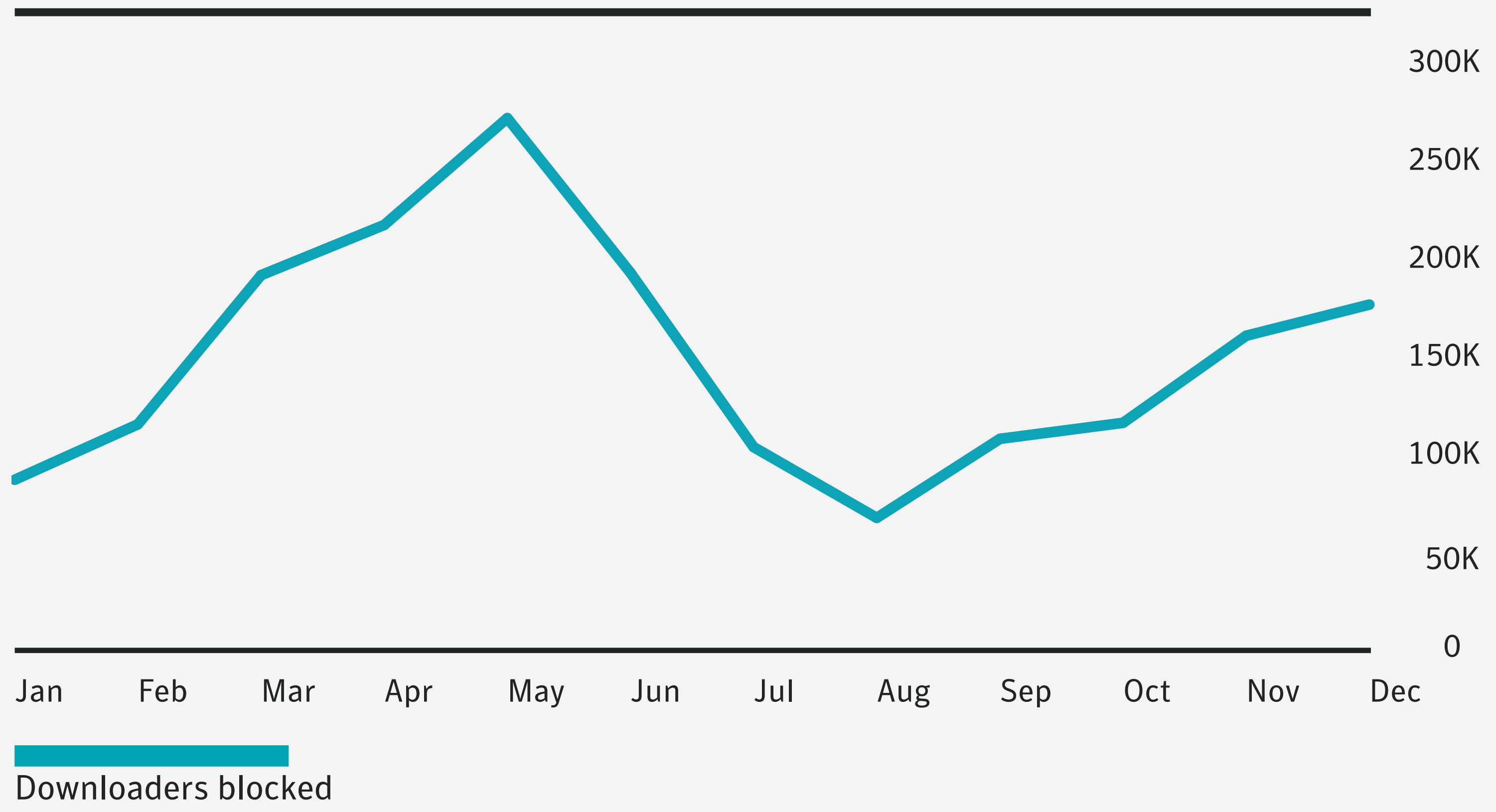
TOTAL MALWARE (MONTH)



TOTAL DOWNLOADERS (MONTH)

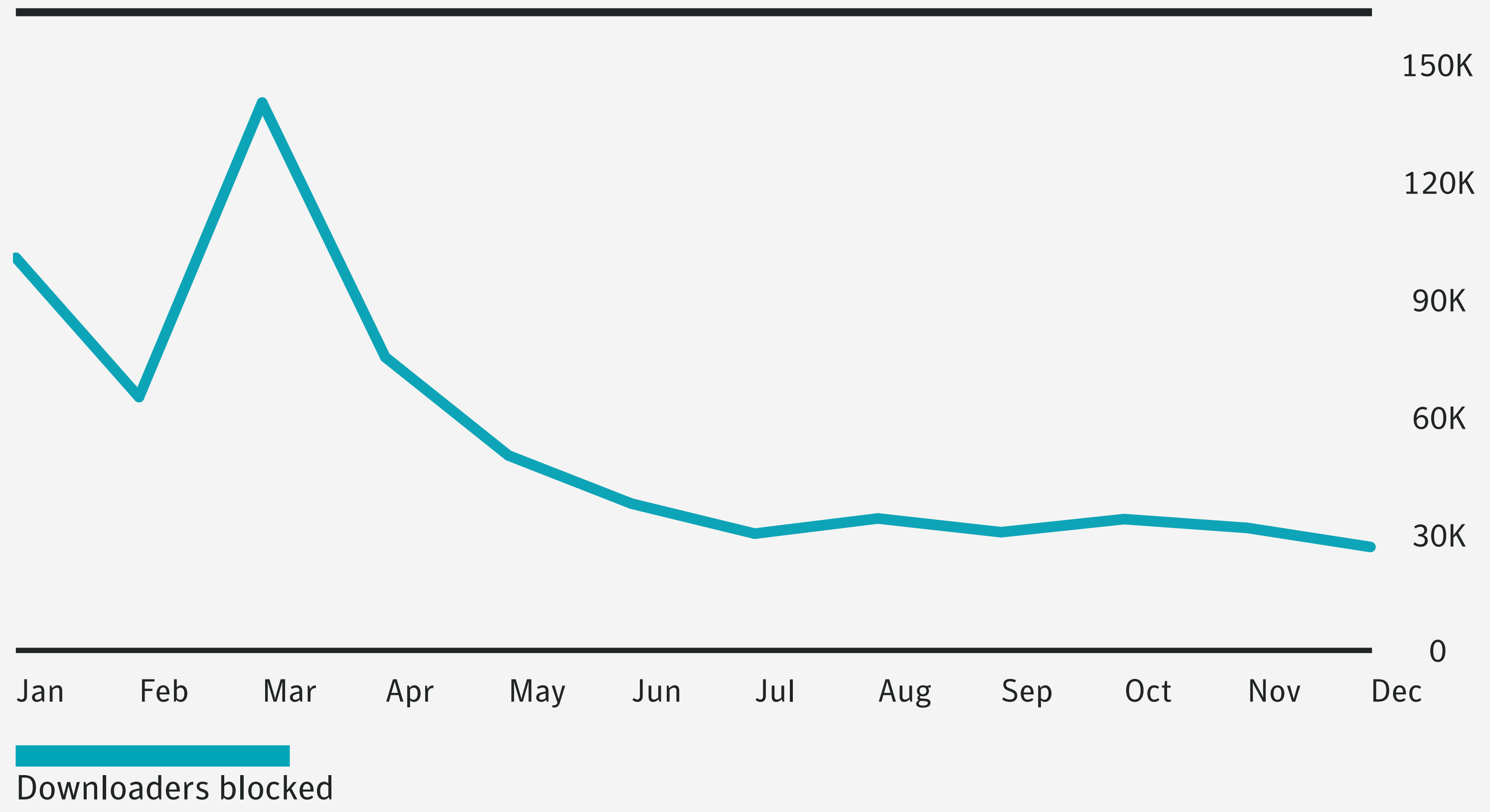


OFFICE MACRO DOWNLOADERS (MONTH)

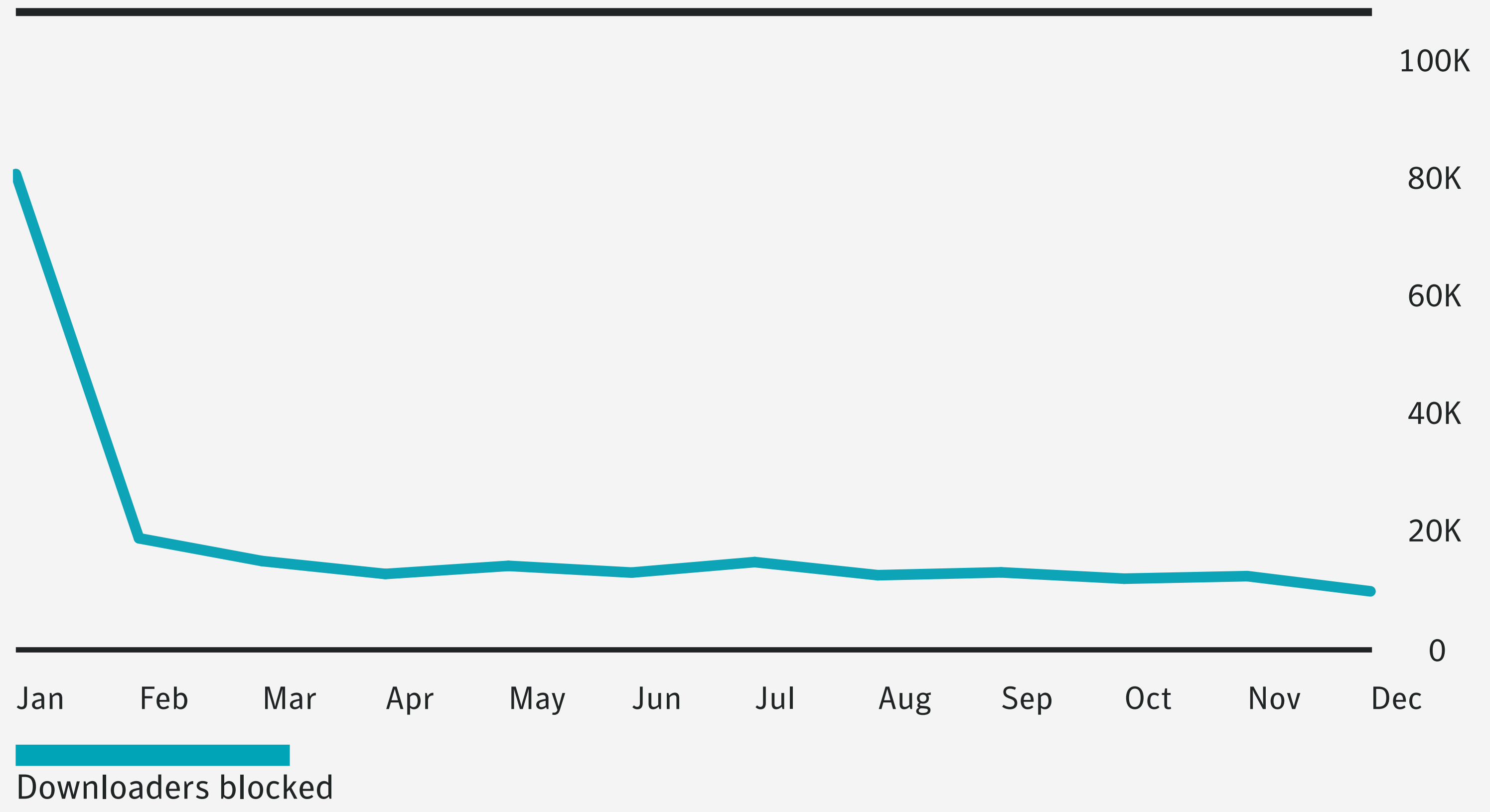


While VBS.Downloader and JS.Downloader threats trended downwards in 2018, Office macro downloaders trended upwards towards the end of the year.

JAVASCRIPT DOWNLOADERS (MONTH)



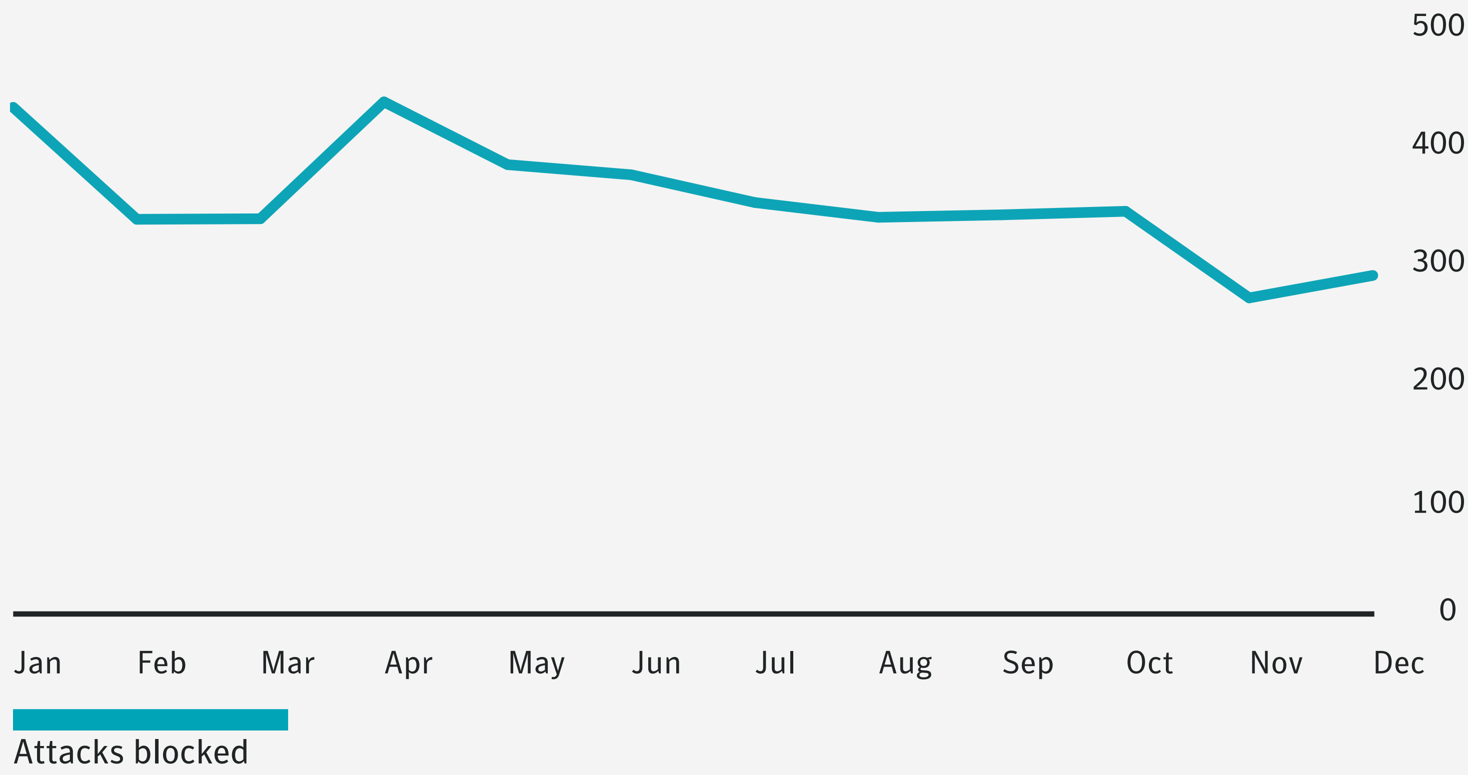
VBSCRIPT DOWNLOADERS (MONTH)



TOTAL MALWARE BY OPERATING SYSTEM (YEAR)

YEAR	OPERATING SYSTEM	ATTACKS BLOCKED	PERCENT
2016	Windows	161,708,289	98.5
	Mac	2,445,414	1.5
2017	Windows	165,639,264	97.6
	Mac	4,011,252	2.4
2018	Windows	144,338,341	97.2
	Mac	4,206,986	2.8

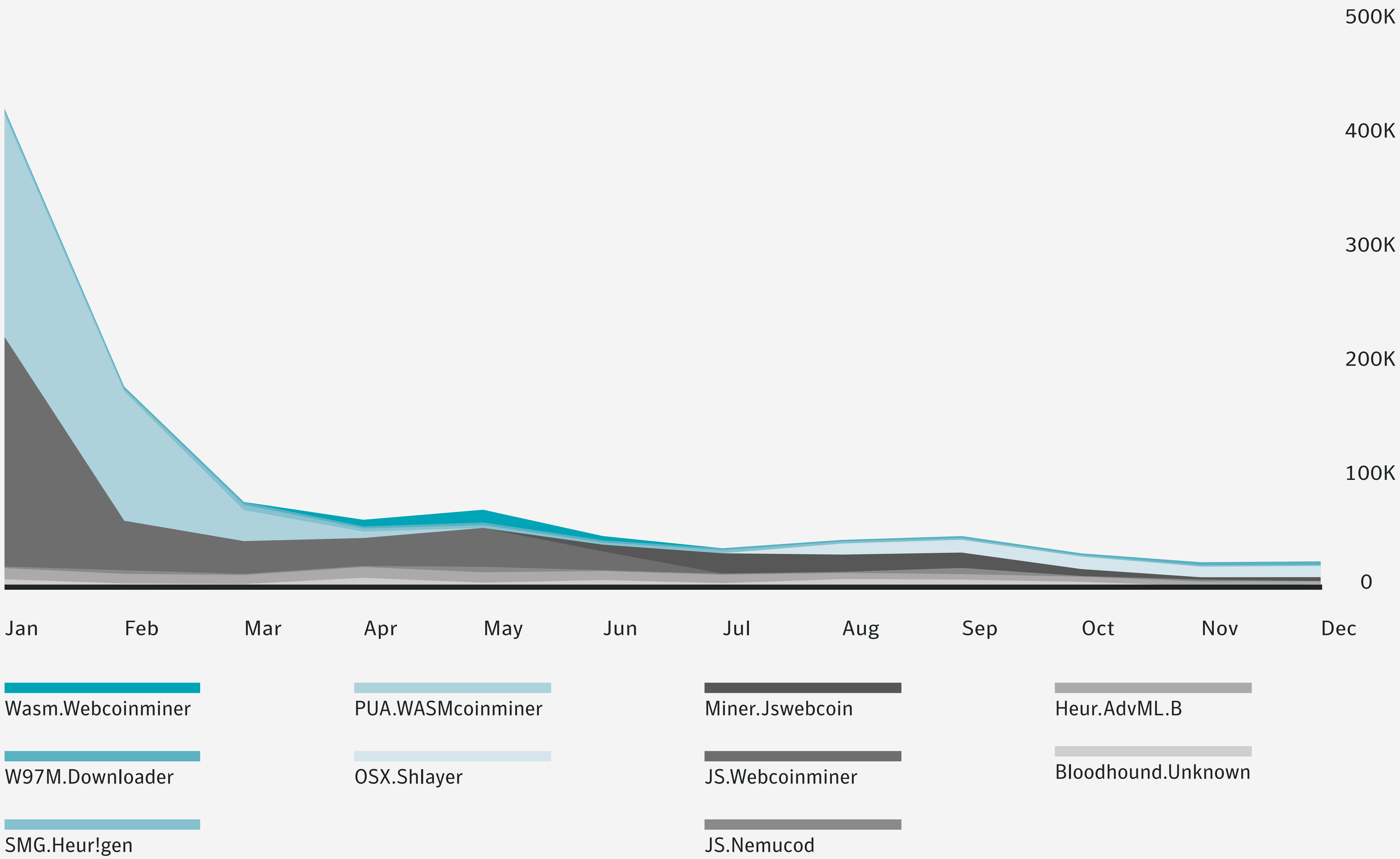
TOTAL MAC MALWARE (MONTH)



NEW MAC MALWARE VARIANTS (YEAR)

YEAR	VARIANTS	PERCENT CHANGE
2016	772,018	
2017	1,390,261	80.1
2018	1,398,419	0.6

TOP NEW MAC MALWARE VARIANTS (MONTH)

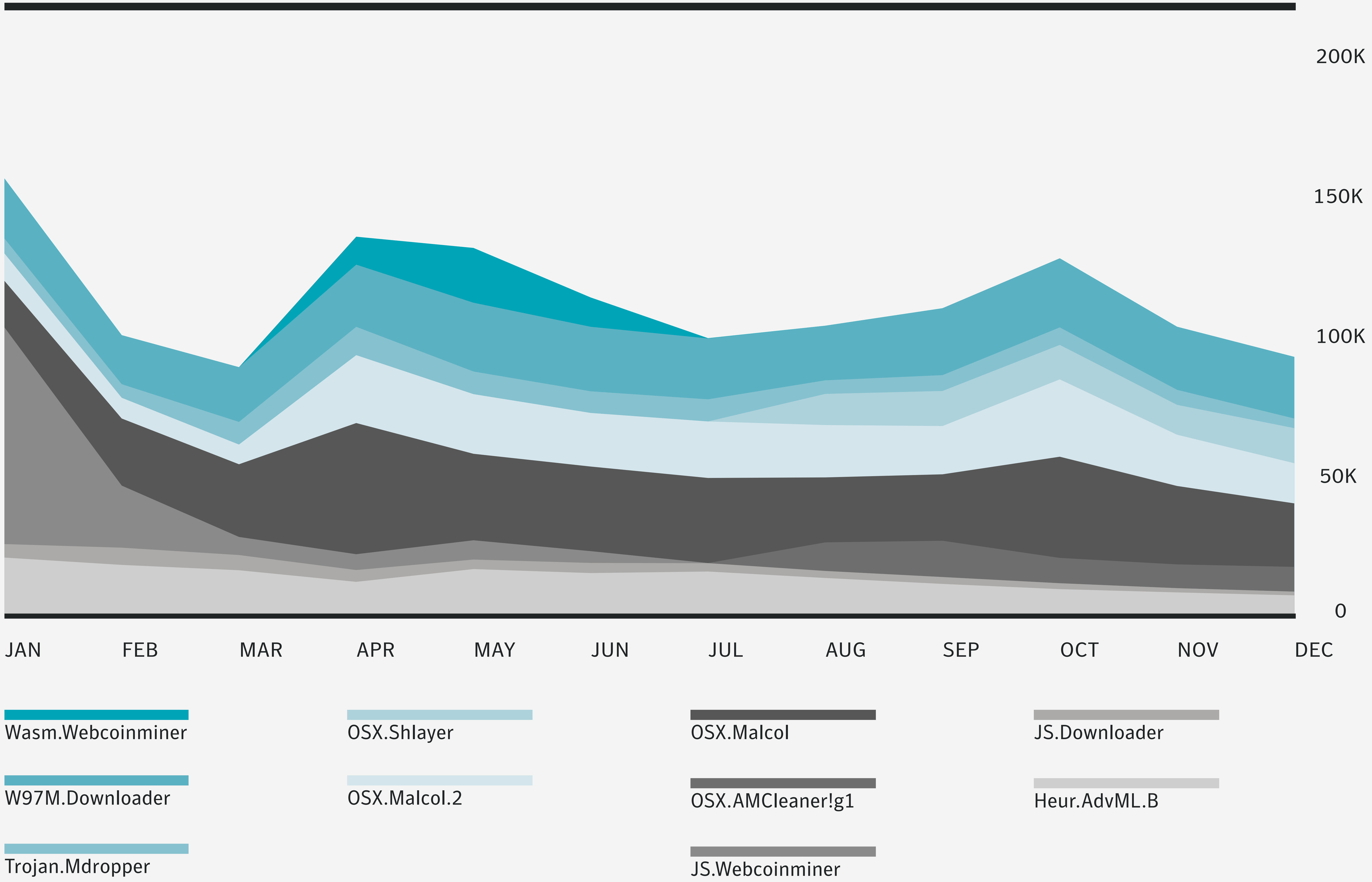


TOP MAC MALWARE (YEAR)

THREAT NAME	ATTACKS BLOCKED	PERCENT
OSX.Malcol	338,806	18.3
W97M.Downloader	262,704	14.2
OSX.Malcol.2	205,378	11.1
Heur.AdvML.B	166,572	9.0
JS.Webcoinminer	122,870	6.6
Trojan.Mdropper	77,800	4.2
OSX.Shlayer	59,197	3.2
OSX.AMCleaner!g1	49,517	2.7
JS.Downloader	40,543	2.2
Wasm.Webcoinminer	40,166	2.2

In 2018, Symantec blocked 69 million cryptojacking events—four times as many events as 2017.

TOP MAC MALWARE (MONTH)



PERCENTAGE SSL-ENABLED MALWARE (YEAR)

YEAR	PERCENTAGE OF MALWARE THAT USES SSL
2017	4.5
2018	3.9

TOTAL RANSOMWARE (YEAR)

YEAR	TOTAL
2018	545,231

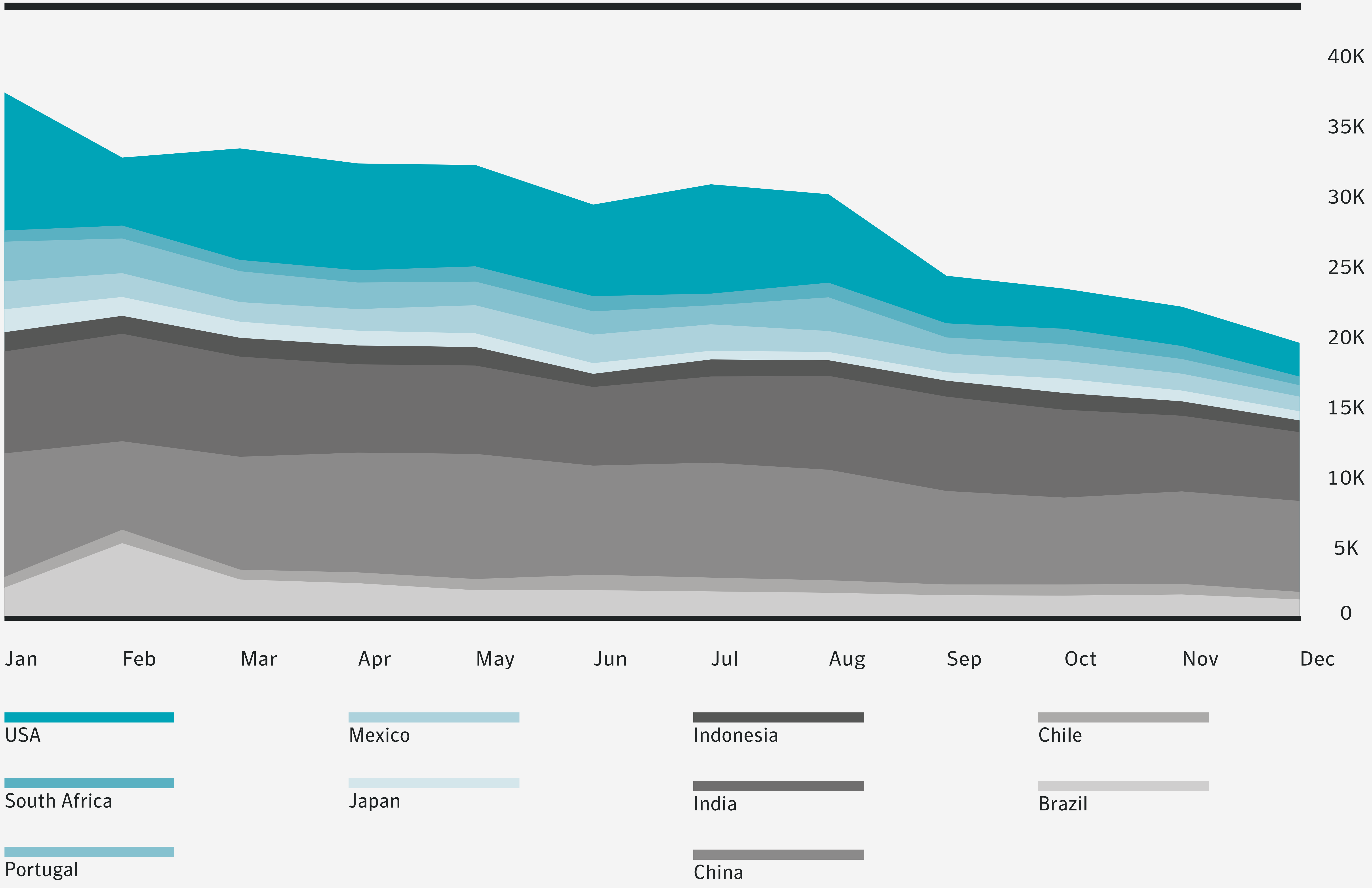
RANSOMWARE BY MARKET (YEAR)

MARKET	TOTAL
Consumer	100,907
Enterprise	444,259

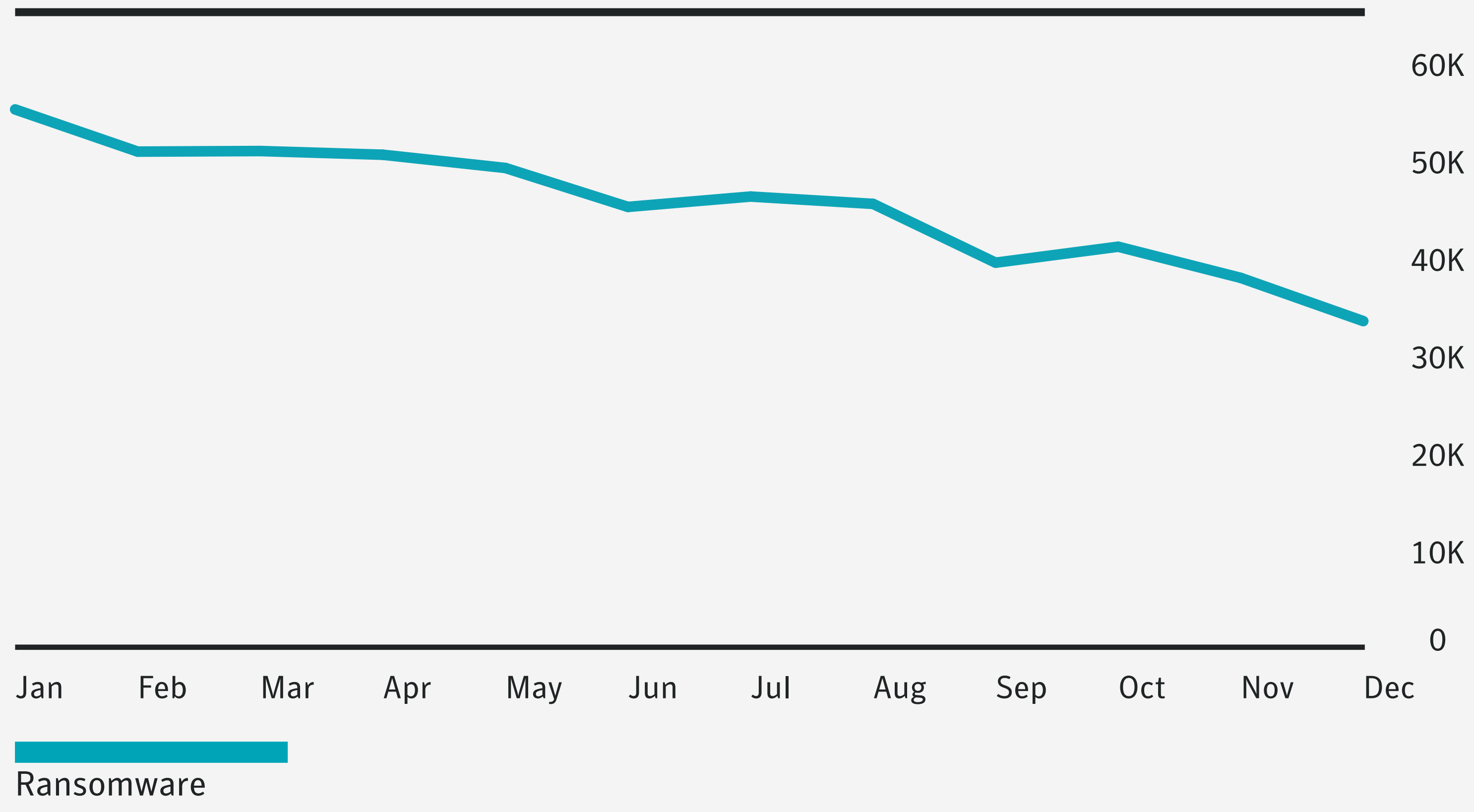
TOP RANSOMWARE BY COUNTRY (YEAR)

COUNTRY	PERCENT
China	16.9
India	14.3
USA	13.0
Brazil	5.0
Portugal	3.9
Mexico	3.5
Indonesia	2.6
Japan	2.1
South Africa	2.1
Chile	1.8

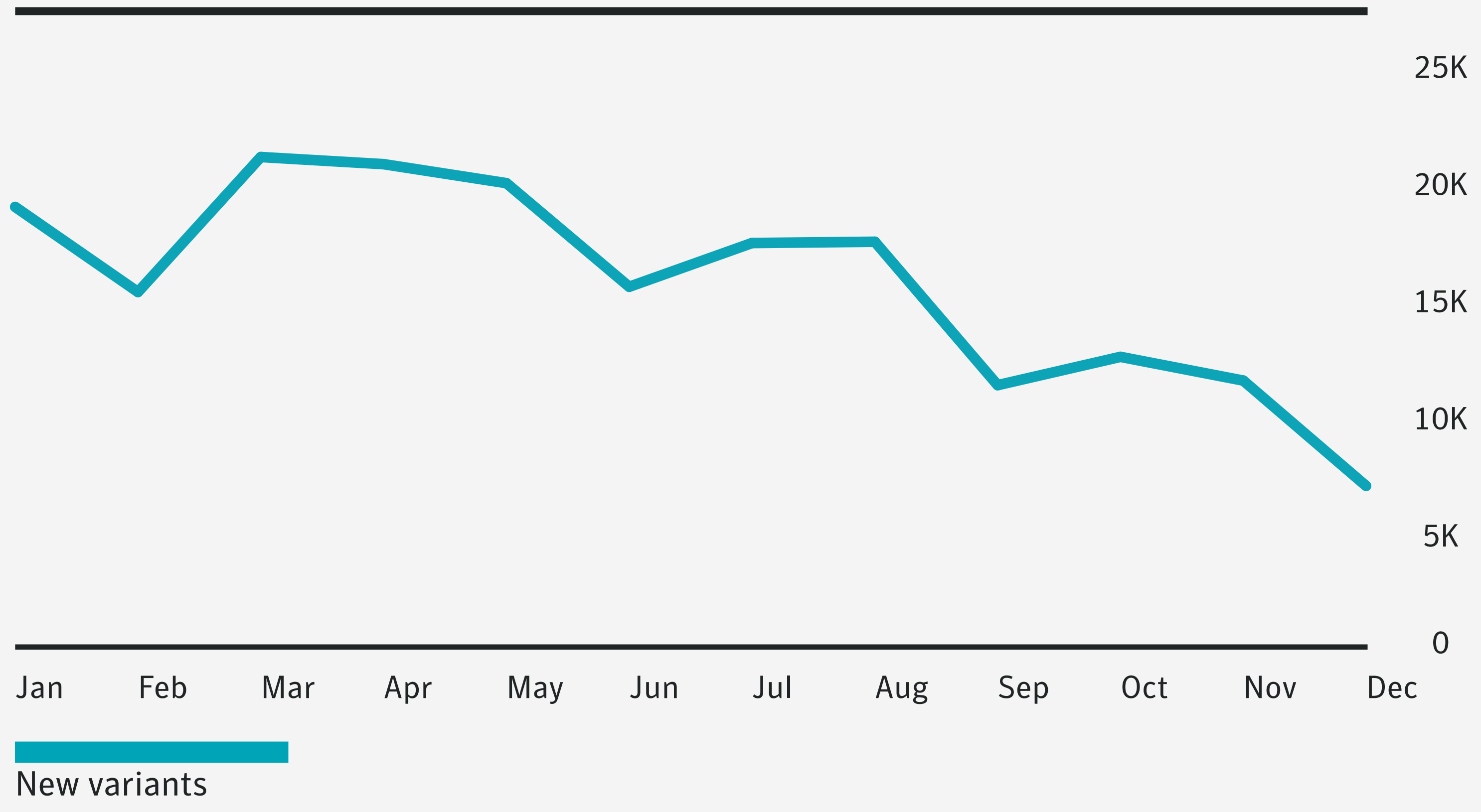
RANSOMWARE BY COUNTRY (MONTH)



TOTAL RANSOMWARE (MONTH)



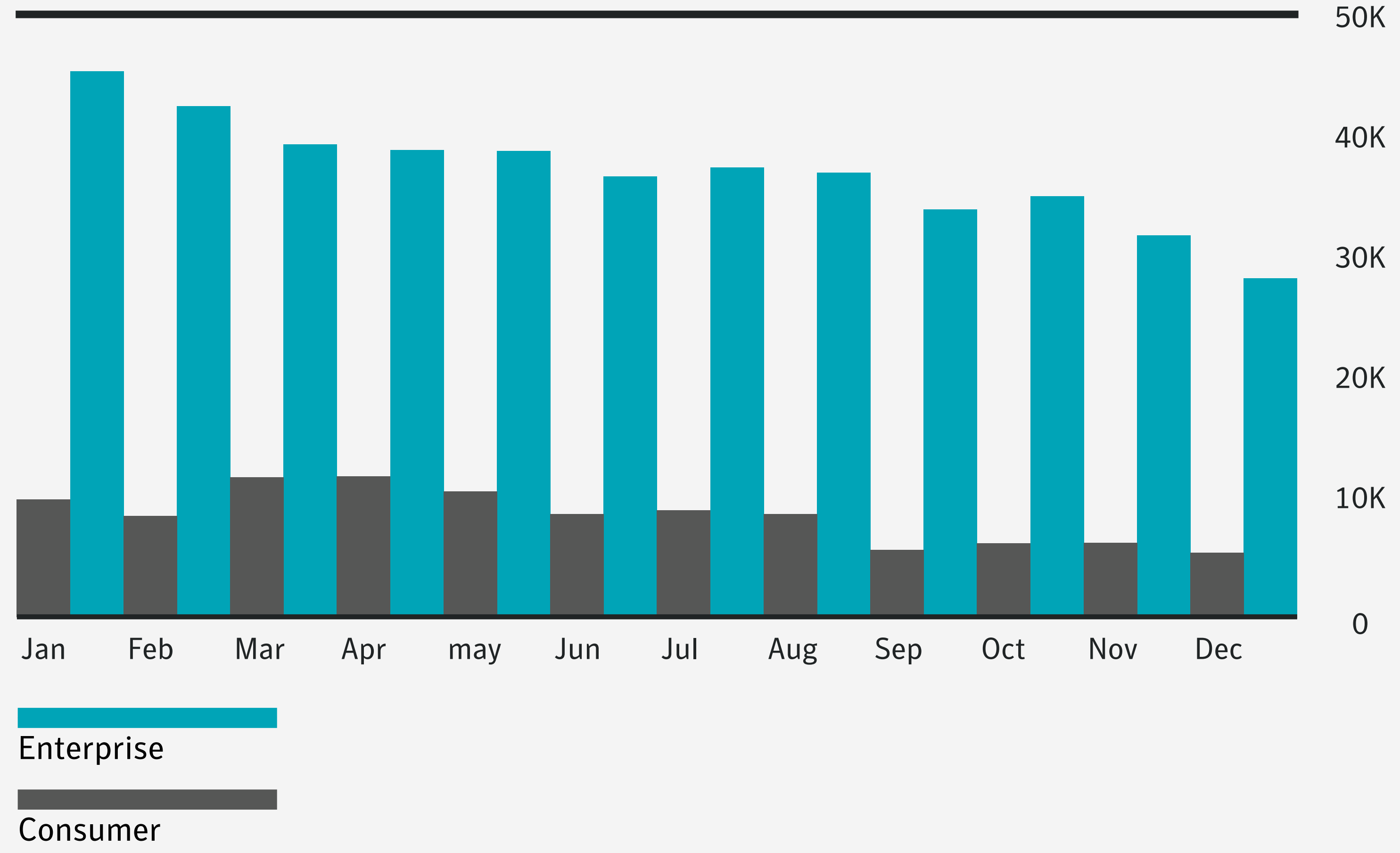
NEW RANSOMWARE VARIANTS (MONTH)



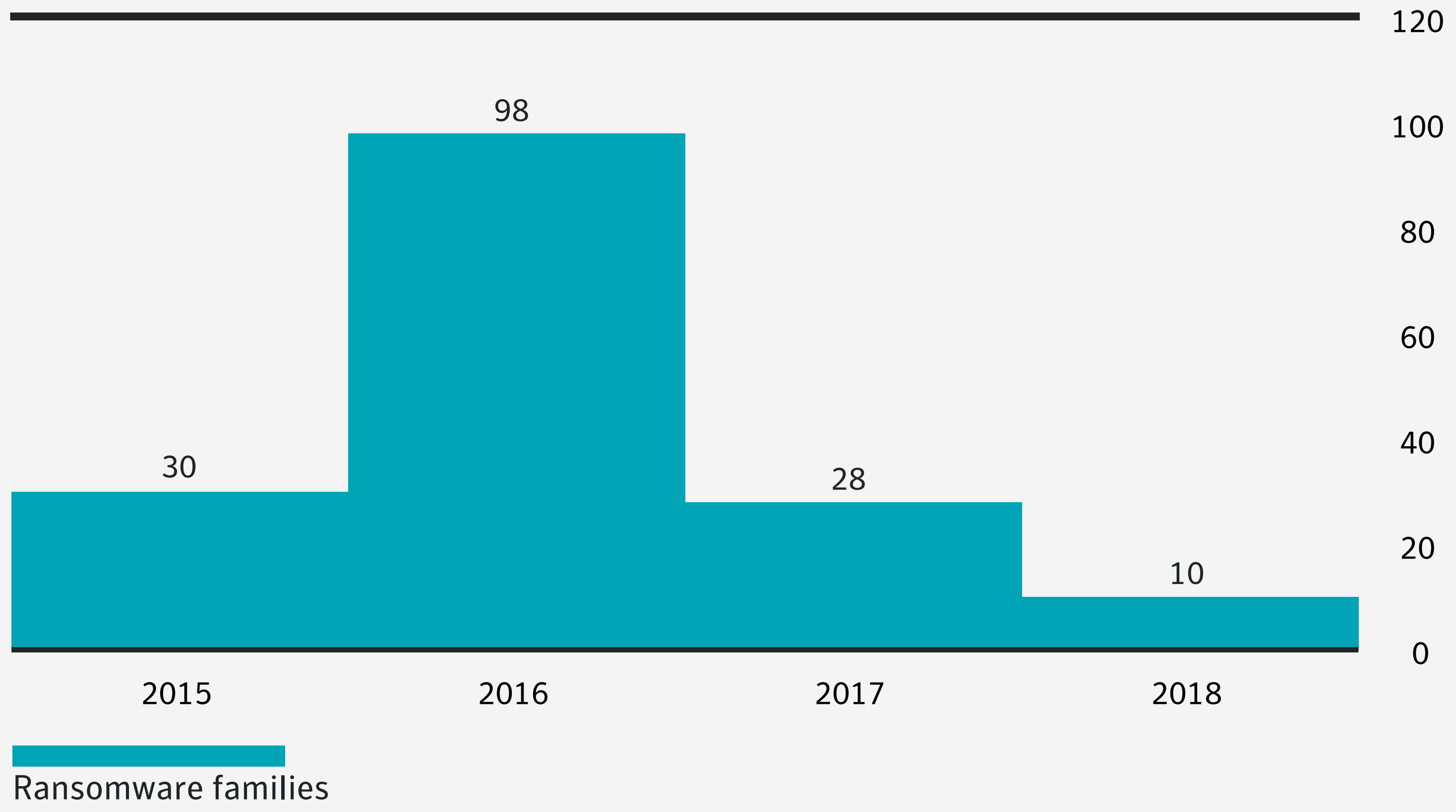
NEW RANSOMWARE VARIANTS (YEAR)

YEAR	TOTAL
2018	186,972

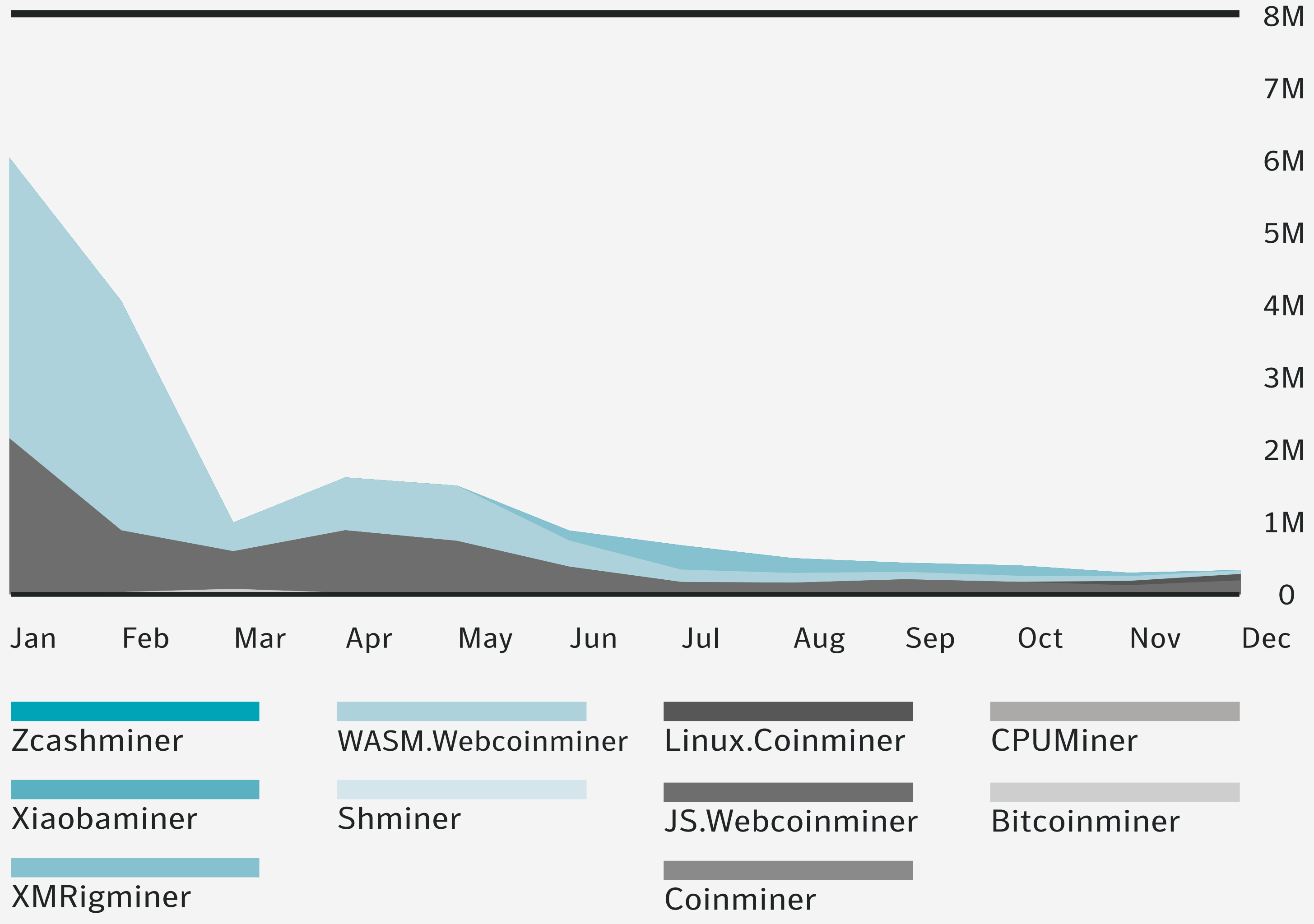
RANSOMWARE BY MARKET (MONTH)



NEW RANSOMWARE FAMILIES (YEAR)

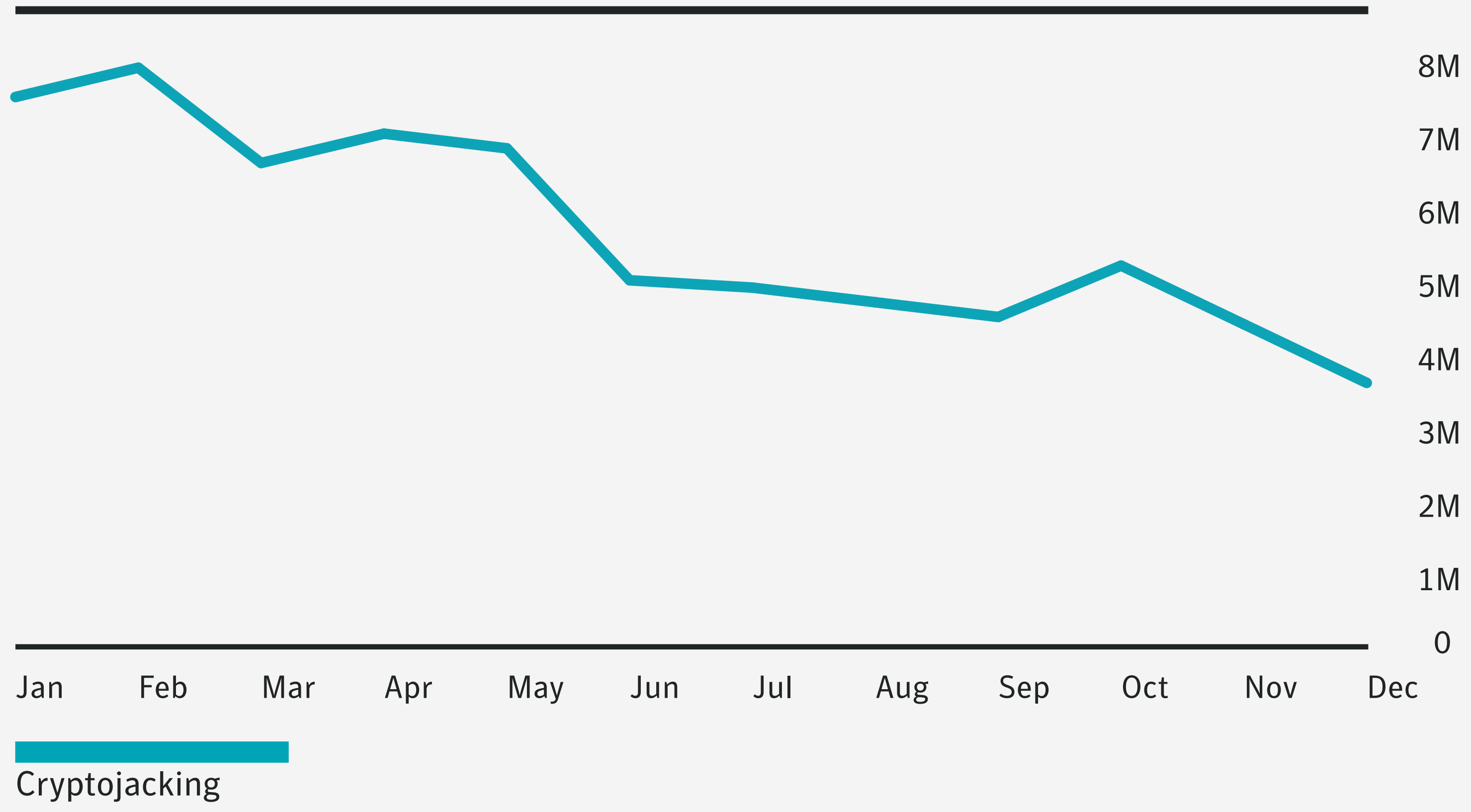


MALWARE: TOP COINMINER VARIANTS (MONTH)

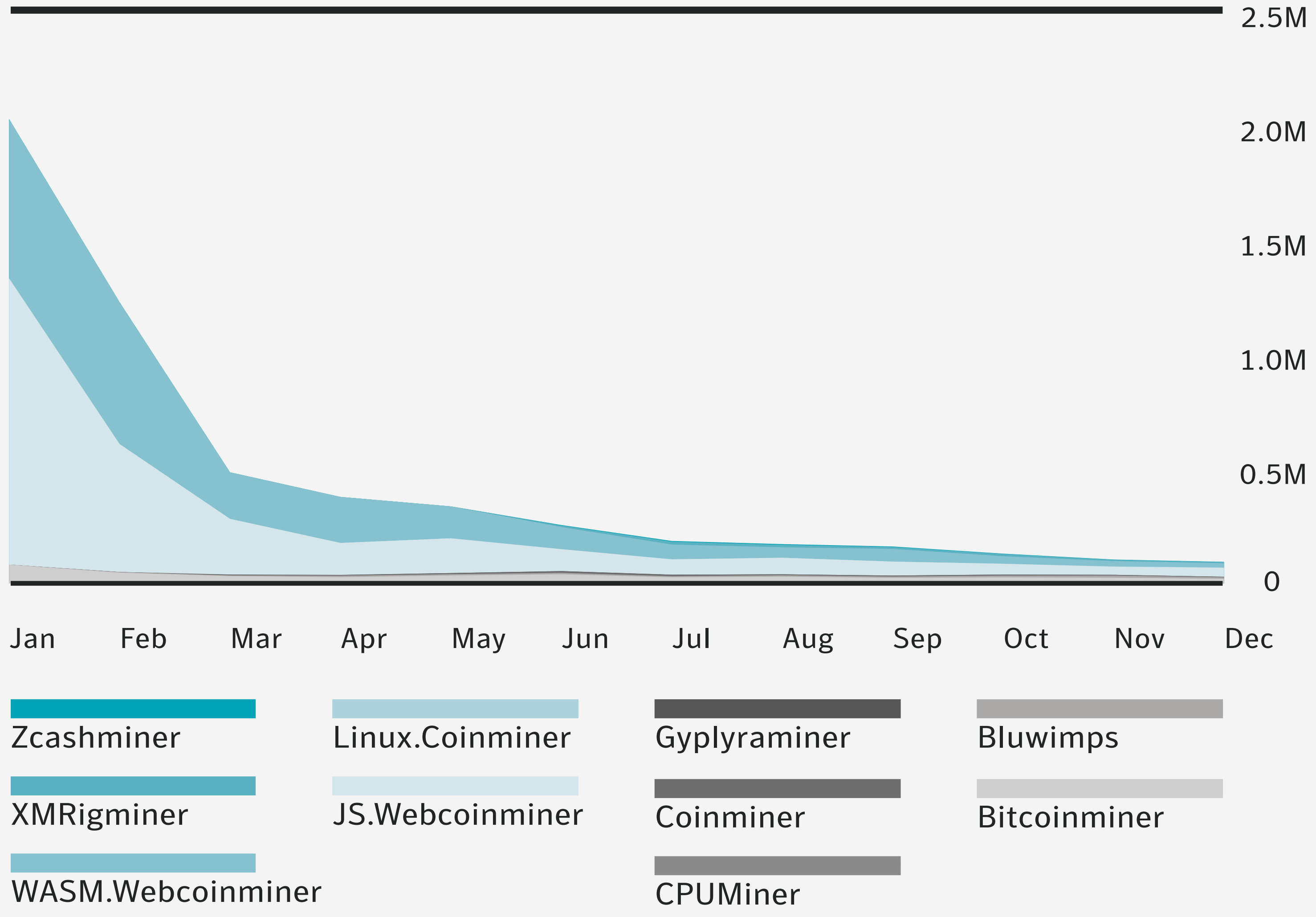


The overall number of ransomware infections fell, dropping by more than 20 percent year-on-year. However, enterprise detections bucked the trend, increasing by 12 percent, demonstrating that ransomware continues to be a problem for enterprises.

TOTAL CRYPTOJACKING (MONTH)



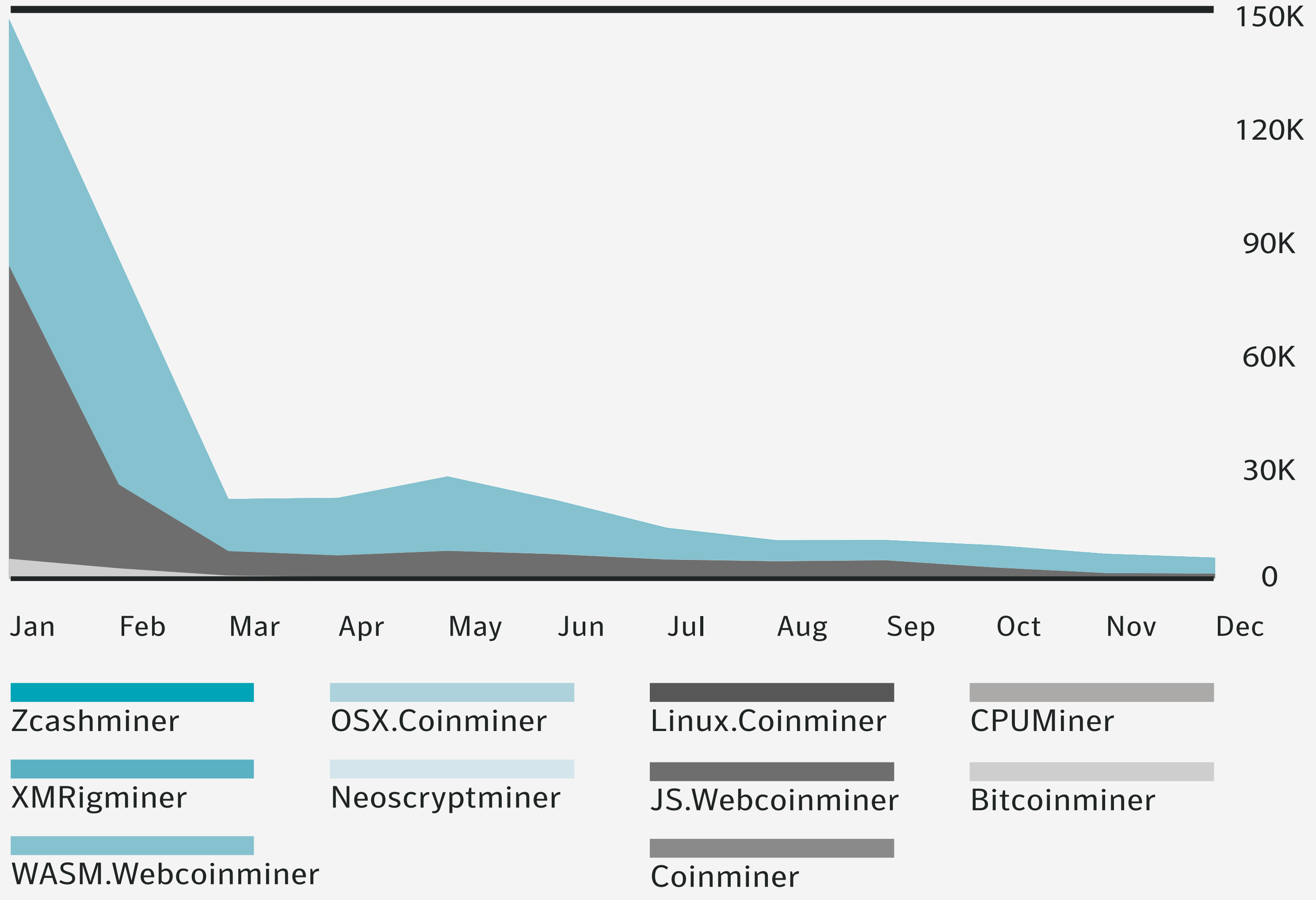
TOP COINMINERS (MONTH)



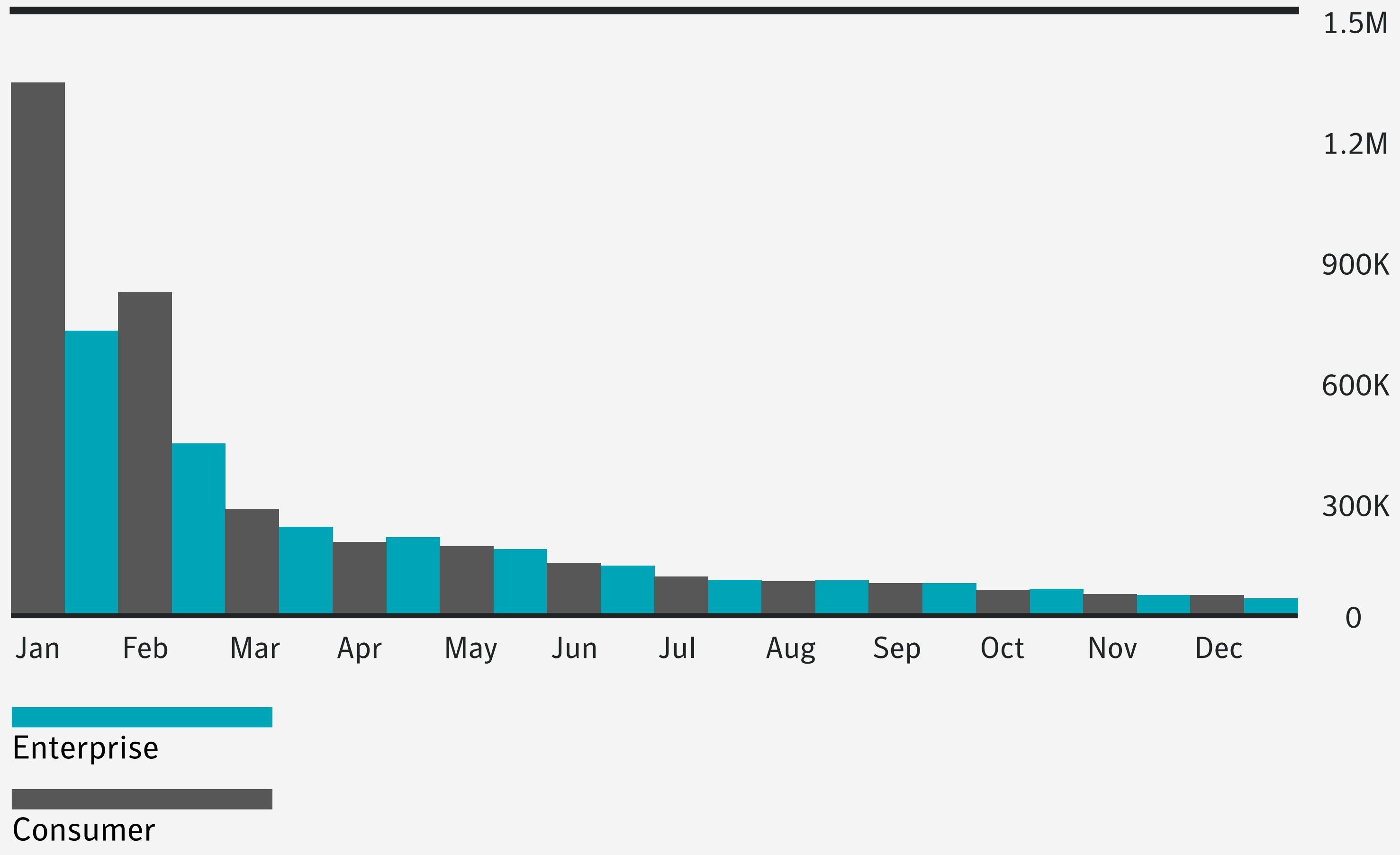
TOP COINMINERS (YEAR)

THREAT NAME	ATTACKS BLOCKED	PERCENT
JS.Webcoinminer	2,768,721	49.7
WASM.Webcoinminer	2,201,789	39.5
Bitcoinminer	414,297	7.4
Bluwimps	58,601	1.1
XMRigminer	58,301	1.0
Coinminer	38,655	0.7
Zcashminer	13,389	0.2
Gyplyraminer	5,221	0.1
CPUMiner	3,807	0.1
Linux.Coinminer	3,324	0.1

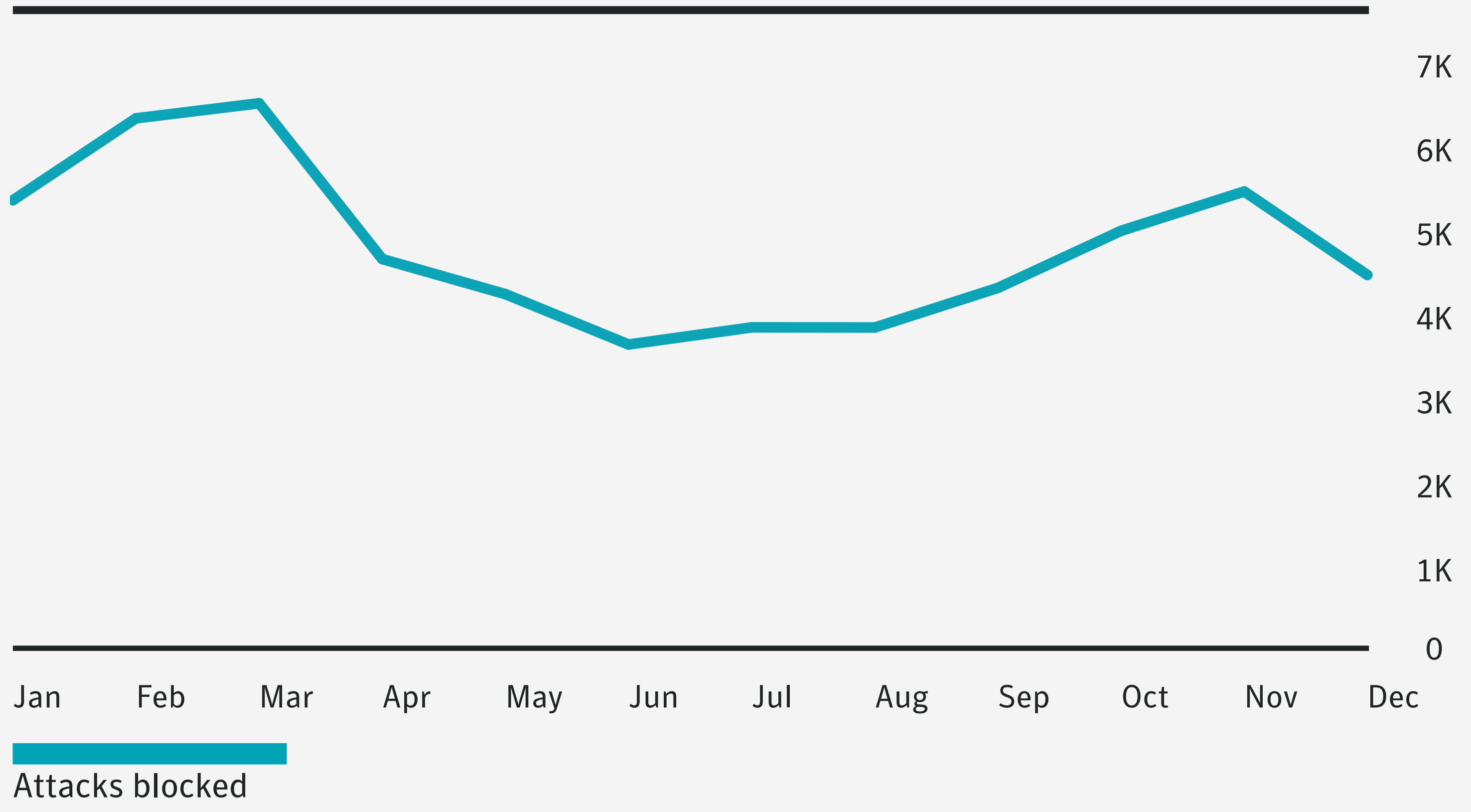
TOP MAC COINMINERS (MONTH)



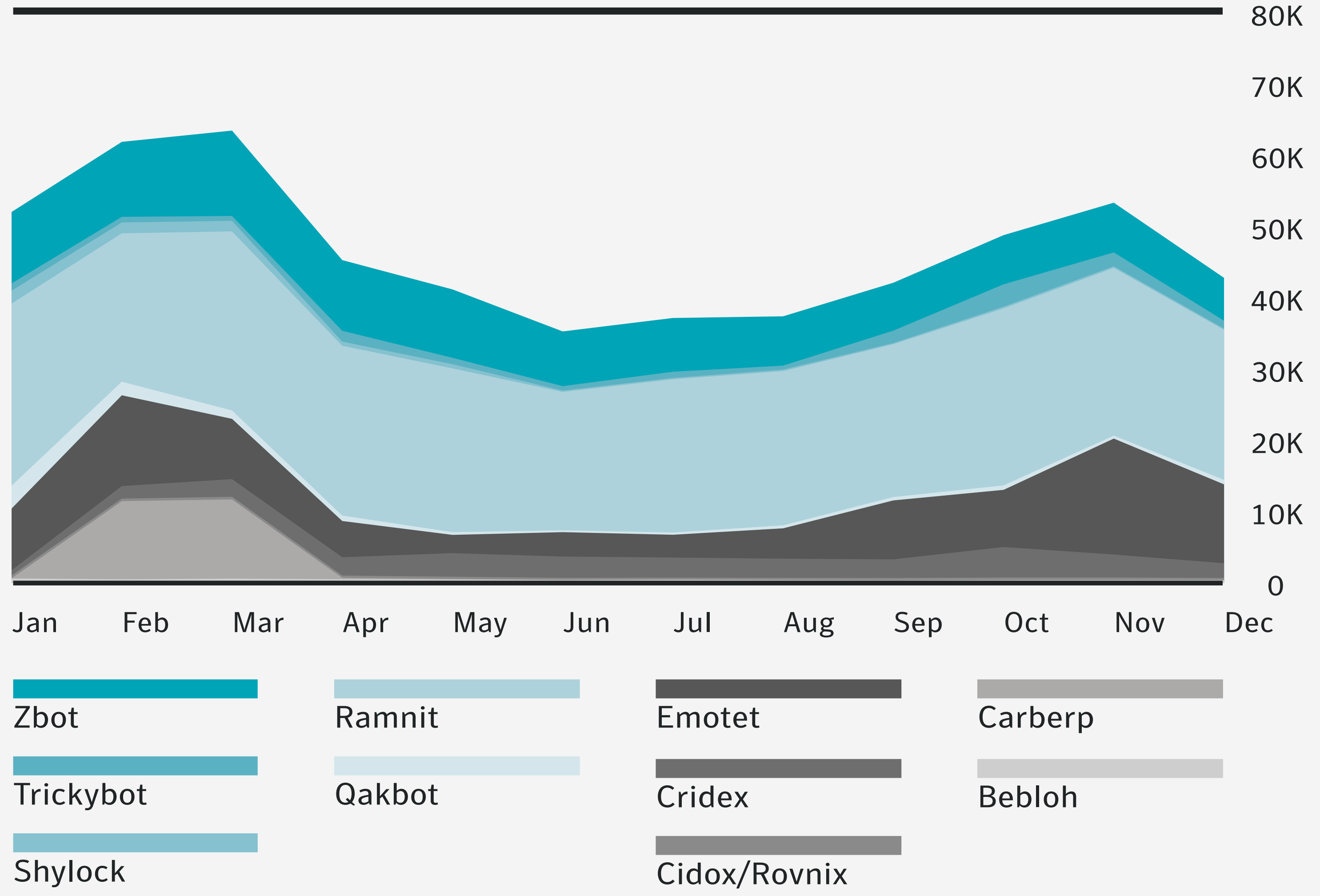
COINMINER BY MARKET (MONTH)



TOTAL FINANCIAL TROJANS (MONTH)



TOP FINANCIAL TROJANS (MONTH)

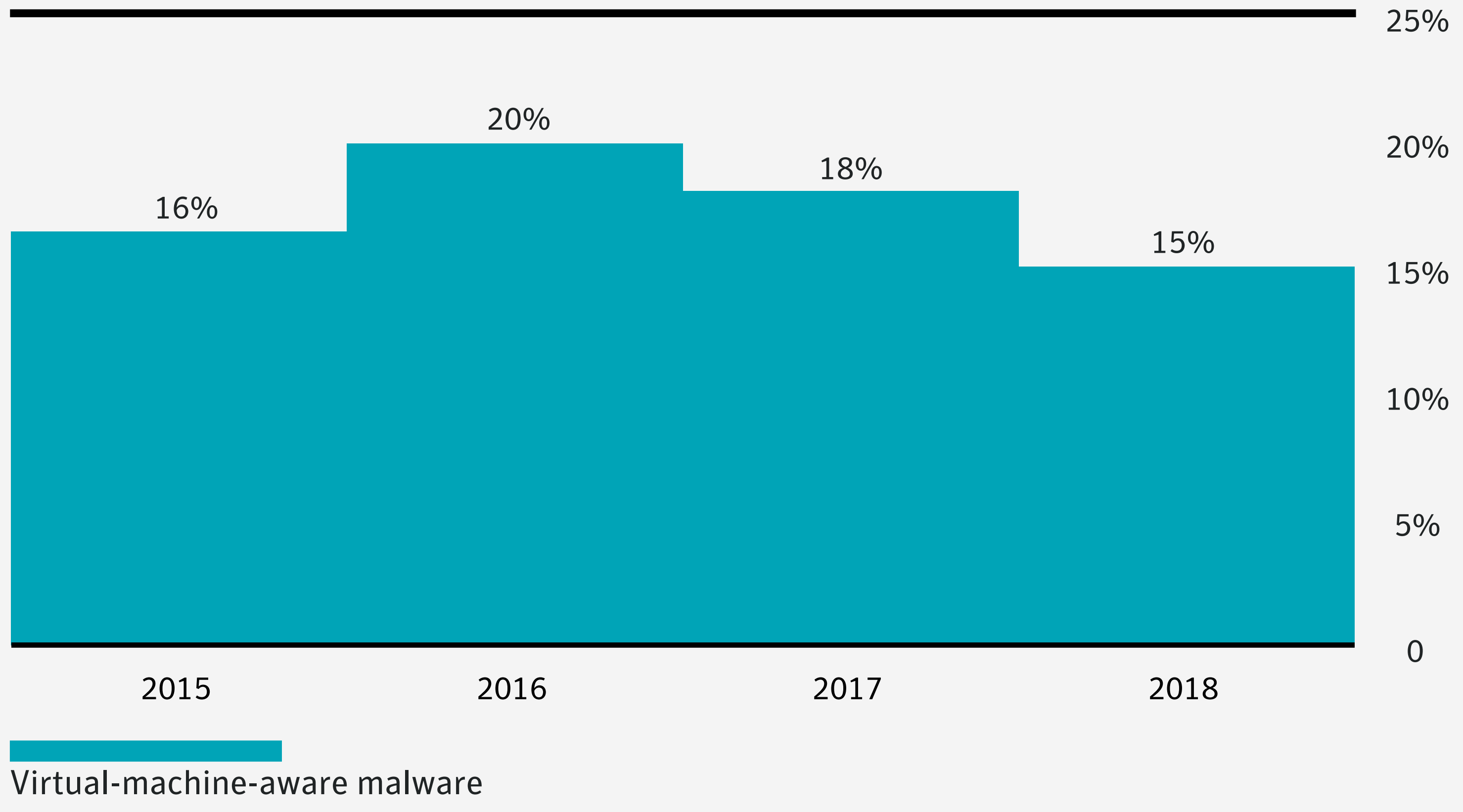


TOP FINANCIAL TROJANS (YEAR)

FINANCIAL TROJAN	ATTACKS BLOCKED	PERCENT
Ramnit	271,930	47.4
Zbot	100,821	17.6
Emotet	92,039	16.0
Cridex	31,539	5.5
Carberp	22,690	4.0
Trickybot	14,887	2.6
Qakbot	10,592	1.8
Shylock	7,354	1.3
Bebloh	5,592	1.0
Cidox/Rovnix	3,889	0.7

Use of malicious PowerShell scripts increased by 1,000 percent in 2018, as attackers continued the movement towards living off the land techniques.

VIRTUAL-MACHINE-AWARE MALWARE (YEAR)



POWERSHELL DETECTIONS (MONTH)

DATE	PERCENTAGE MALICIOUS POWERSHELL SCRIPTS	RATIO
Jan	0.1	1 in 1,000
Feb	0.5	1 in 200
Mar	2.5	1 in 40
Apr	0.4	1 in 250
May	1.3	1 in 77
Jun	0.9	1 in 111
Jul	1.4	1 in 71
Aug	0.8	1 in 125
Sep	1.0	1 in 100
Oct	1.0	1 in 100
Nov	0.7	1 in 143
Dec	0.7	1 in 143

POWERSHELL DETECTIONS (YEAR)

YEAR	PERCENT OF TOTAL WHICH IS MALICIOUS	RATIO	PERCENT INCREASE OF MALICIOUS SCRIPTS
2017	0.9	1 in 111	
2018	0.9	1 in 111	998.9

MOBILE

While the overall number of mobile malware infections fell during 2018, there was a rapid increase in the number of ransomware infections on mobile devices, up by a third when compared to 2017. The U.S. was the worst affected by mobile ransomware, accounting for 63 percent of infections. It was followed by China (13 percent) and Germany (10 percent).

Managing mobile device security continues to present a challenge for organizations. During 2018, one in 36 devices used in organizations were classed as high risk. This included devices that were rooted or jailbroken, along with devices that had a high degree of certainty that malware had been installed.

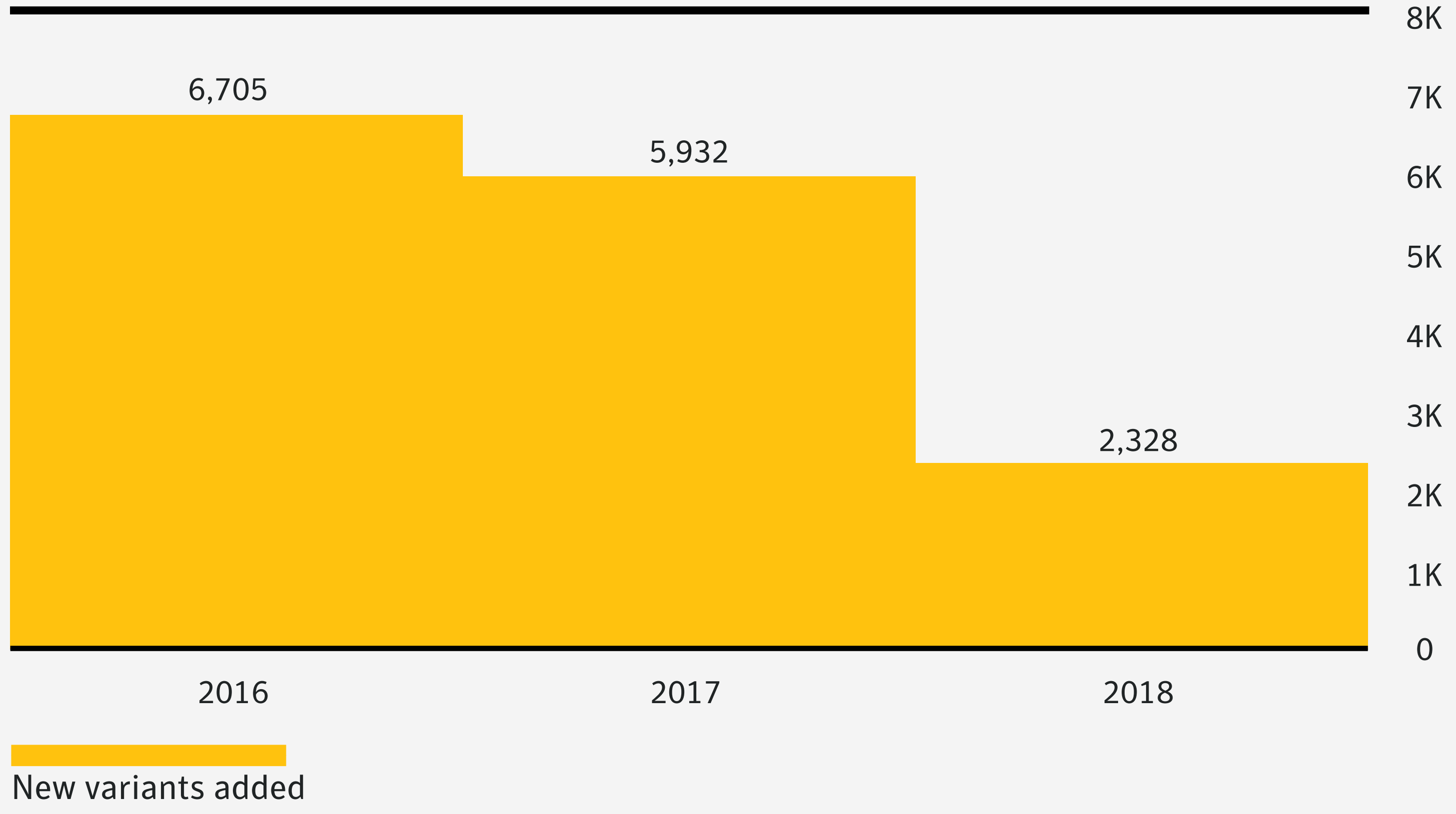
ONE IN 36

MOBILE
DEVICES
HAD HIGH
RISK APPS
INSTALLED

33% ↑

MOBILE
RANSOMWARE
INFECTIONS
INCREASED
FROM 2017

NEW MOBILE MALWARE VARIANTS (YEAR)



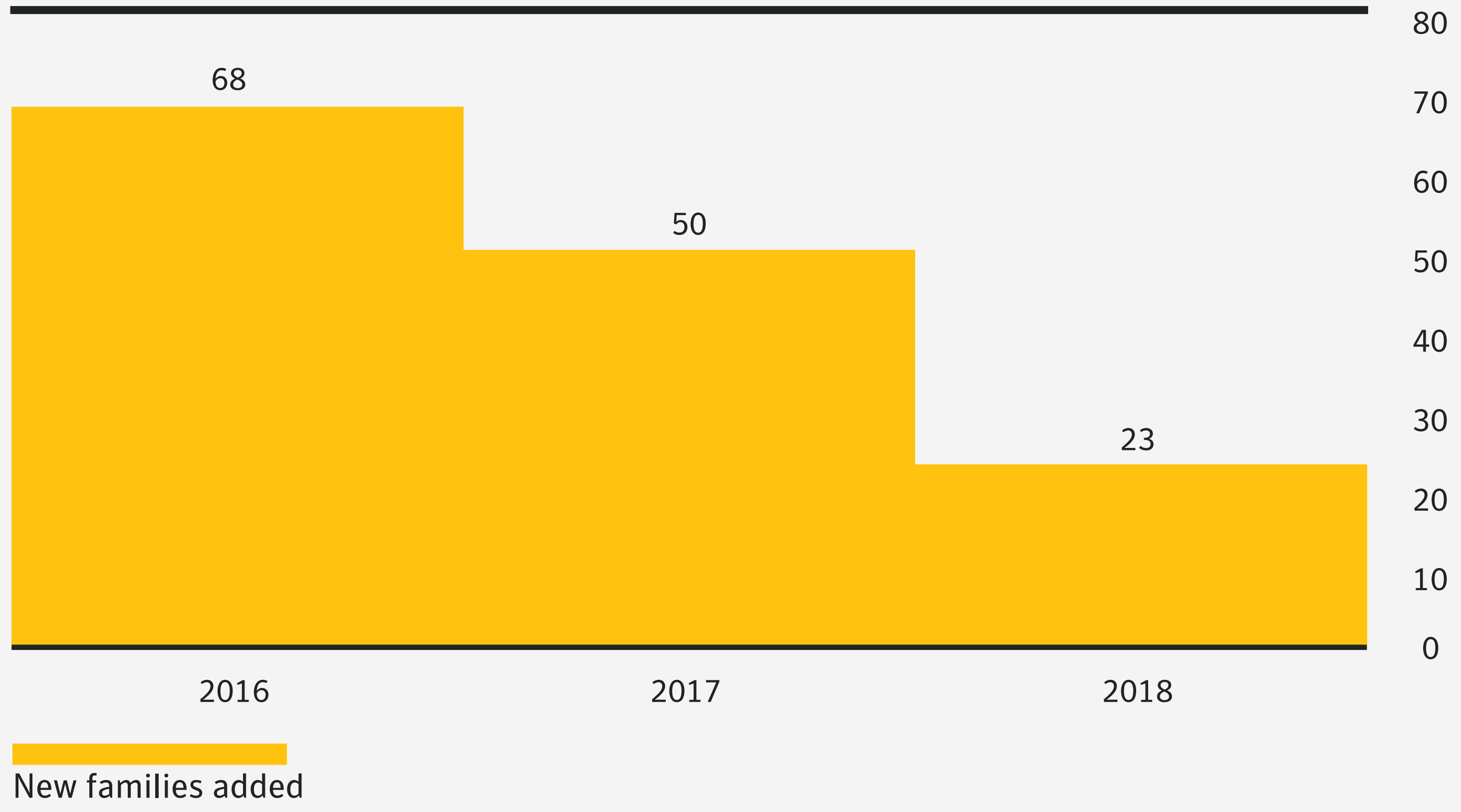
NUMBER OF BLOCKED MOBILE APPS (YEAR)

PER DAY
10,573

TOP MALICIOUS MOBILE APP CATEGORIES (YEAR)

CATEGORY	PERCENT
Tools	39.1
LifeStyle	14.9
Entertainment	7.3
Social & Communication	6.2
Music & Audio	4.3
Brain & Puzzle Games	4.2
Photo & Video	4.2
Arcade & Action Games	4.1
Books & Reference	3.2
Education	2.6

NEW MOBILE MALWARE FAMILIES (YEAR)



MONTHLY AVERAGE NUMBER OF MOBILE RANSOMWARE (YEAR)

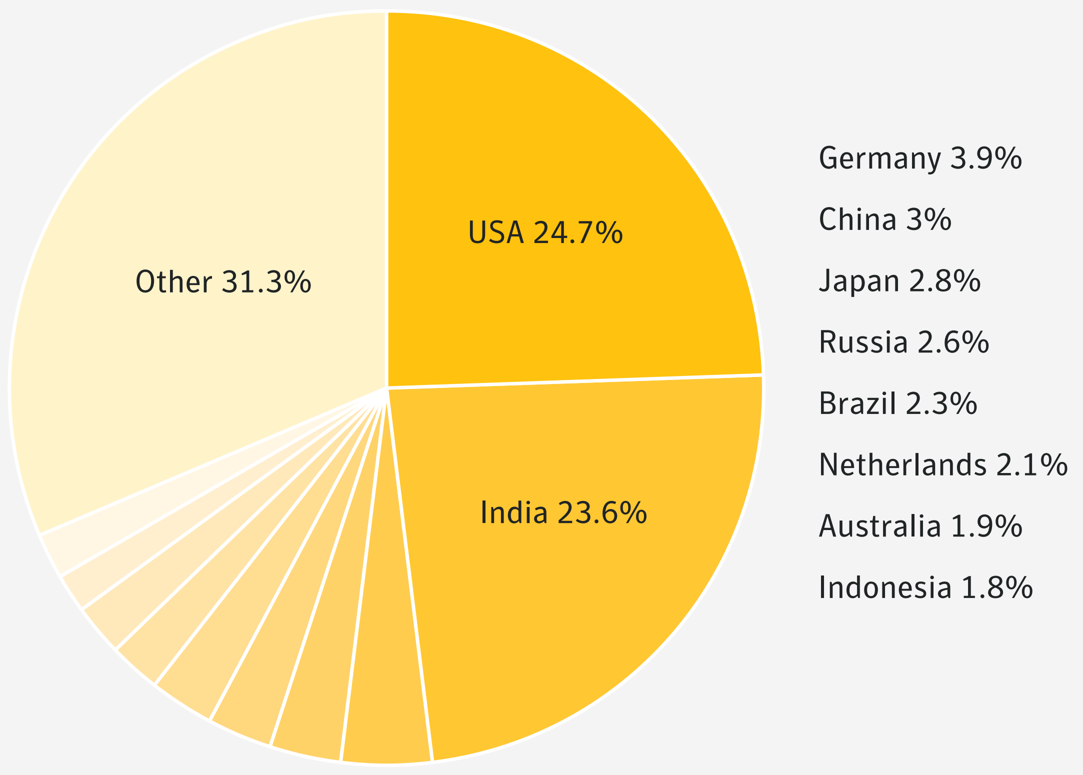
PER MONTH
4,675

TOP MOBILE MALWARE (YEAR)

THREAT NAME	PERCENT
Malapp	29.7
Fakeapp	9.1
MalDownloader	8.9
FakeInst	6.6
Mobilespy	6.3
HiddenAds	4.7
Premiumtext	4.4
MobileSpy	2.8
HiddenApp	2.5
Opfake	2.0

During 2018, Symantec blocked an average of 10,573 malicious mobile apps per day. Tools (39%), Lifestyle (15%), and Entertainment (7%) were the most frequently seen categories of malicious apps.

TOP COUNTRIES FOR MOBILE MALWARE (YEAR)



JAILBROKEN OR ROOTED MOBILE DEVICE RATE (YEAR)

SEGMENT	RATIO
Android Consumer	1 in 23
Android Enterprise	1 in 3,890
iOS Consumer	1 in 828
iOS Enterprise	1 in 4,951

PASSWORD PROTECTED MOBILE DEVICES BY MARKET (YEAR)

SEGMENT	PERCENT
Consumer	97.9
Enterprise	98.4

LENGTH OF EXPOSURE TO NETWORK THREATS FOR MOBILE DEVICES (YEAR)

DEVICES EXPOSED TO NETWORK ATTACKS	PERCENT
After 1 month (out of devices created 1-4 months ago)	15.1
After 2 months (out of devices created 2-5 months ago)	21.8
After 3 months (out of devices created 3-6 months ago)	27.4
After 4 months (out of devices created 4-7 months ago)	32.2

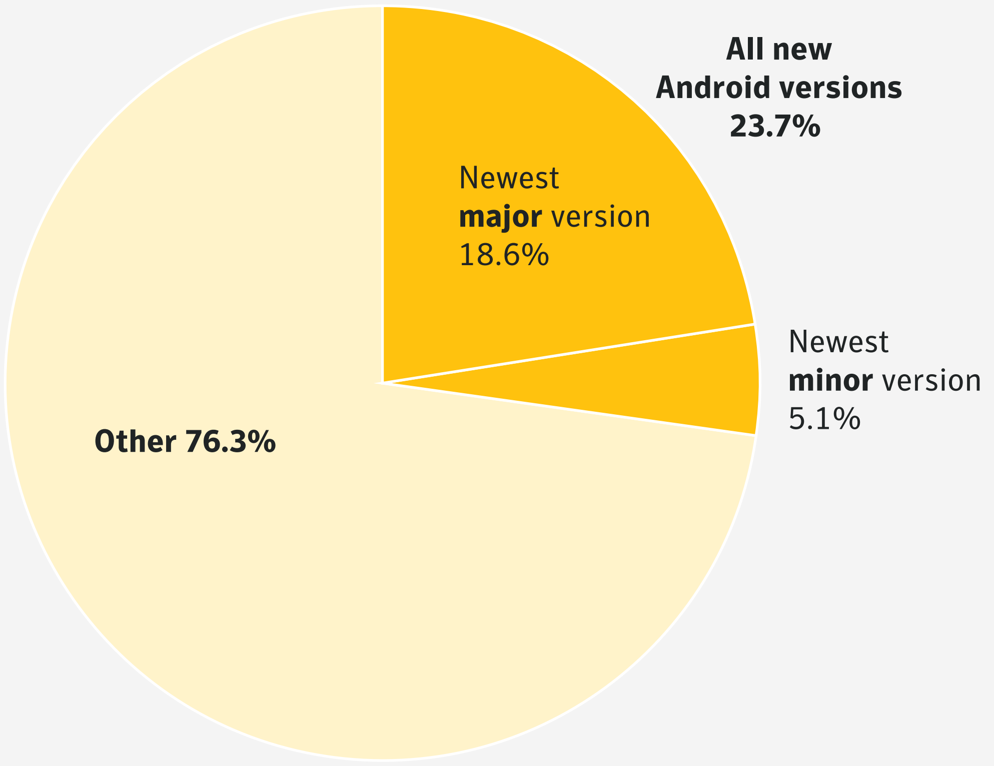
DEVICES THAT DO NOT HAVE ENCRYPTION ENABLED (YEAR)

SEGMENT	PERCENT
Consumer	13.4
Enterprise	10.5

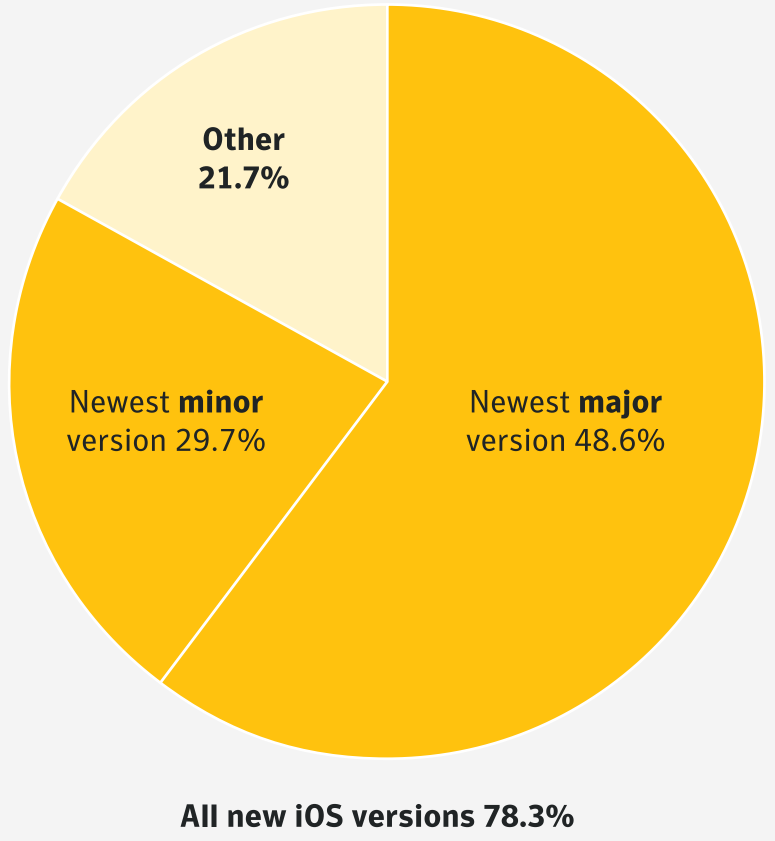
DEVICES RISK LEVELS (YEAR)

DEVICE RISK LEVEL	RATIO
Minimal	1 in 2
Low	1 in 4
Medium	1 in 4
High (including rooted/jailbroken/have high-certainty-malware apps installed)	1 in 36

DEVICES RUNNING NEWEST ANDROID VERSION (YEAR)



DEVICES RUNNING NEWEST IOS VERSION (YEAR)



The percentage of mobile apps that employ invasive advertising techniques dropped. Having stood at 30% in 2017, it fell to 26% in 2018.

RATIO OF APPS THAT ACCESS HIGH RISK DATA (YEAR)

YEAR	APPS ACCESSING HIGH-RISK DATA (%)	RATIO	CHANGE (PP)
2016	7.2	1 in 13.9	
2017	8.9	1 in 11.3	1.7
2018	6.9	1 in 14.5	-2

RATIO OF APPS THAT CONTAIN HARD CODED CREDENTIALS (YEAR)

YEAR	APPS CONTAINING HARD-CODED CREDENTIALS (%)	RATIO	CHANGE (PP)
2016	0.8	1 in 124.5	
2017	1.1	1 in 91.0	0.3
2018	1.0	1 in 99.1	-0.1

RATIO OF APPS THAT USE HOT PATCHING (YEAR)

YEAR	APPS USING HOT-PATCHING RISK (%)	RATIO	CHANGE (PP)
2016	0.7	1 in 142.1	
2017	0.35	1 in 285.1	-0.35
2018	0.01	1 in 7,146.0	-0.34

RATIO OF APPS THAT ACCESS HEALTH DATA (YEAR)

YEAR	APPS ACCESSING HEALTH DATA (%)	RATIO	CHANGE (PP)
2016	0.2	1 in 427.3	
2017	1.7	1 in 57.6	1.5
2018	2.2	1 in 46.3	0.5

RATIO OF APPS THAT USE INVASIVE ADVERTISING (YEAR)

YEAR	PERCENTAGE OF APPS USING INVASIVE ADVERTISING	RATIO	CHANGE (PP)
2016	19.4	1 in 5.2	
2017	30.5	1 in 3.3	11.1
2018	26.4	1 in 3.8	-4.1

PERCENTAGE OF ORGANIZATIONS AFFECTED BY APPS THAT ACCESS HEALTH DATA (YEAR)

YEAR	ORGANIZATIONS WITH 1+ APPS: HEALTH DATA (%)	RATIO	CHANGE (PP)
2016	27.6	1 in 3.6	
2017	44.9	1 in 2.2	17.3
2018	39.0	1 in 2.6	-5.9

PERCENTAGE OF ORGANIZATIONS AFFECTED BY APPS THAT ACCESS HIGH RISK DATA (YEAR)

YEAR	PERCENTAGE OF ORGANIZATIONS FOUND WITH APPS THAT ACCESS HIGH-RISK DATA	RATIO	CHANGE (PP)
2016	63	1 in 1.6	
2017	54.6	1 in 1.8	-8.4
2018	46	1 in 2.2	-8.6

PERCENTAGE OF ORGANIZATIONS AFFECTED BY APPS THAT CONTAIN HARD CODED CREDENTIALS (YEAR)

YEAR	PERCENTAGE OF ORGANIZATIONS FOUND WITH APPS THAT HAVE HARD-CODED CREDENTIALS	RATIO	CHANGE (PP)
2016	47.3	1 in 2.1	
2017	42.9	1 in 2.3	-4.4
2018	34.3	1 in 2.9	-8.6

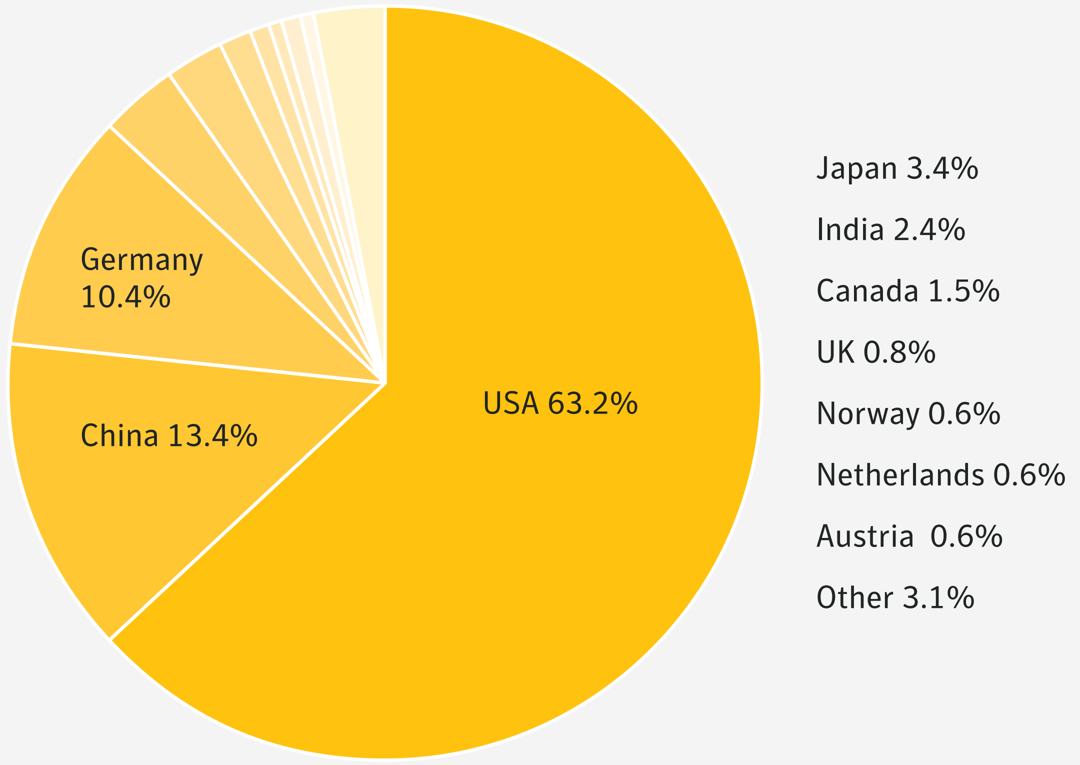
PERCENTAGE OF ORGANIZATIONS AFFECTED BY APPS THAT USE HOT PATCHING (YEAR)

YEAR	PERCENTAGE OF ORGANIZATIONS FOUND WITH APPS THAT USE HOT-PATCHING	RATIO	CHANGE (PP)
2016	31.3	1 in 3.2	
2017	11.7	1 in 8.5	-19.6
2018	6.8	1 in 14.7	-4.9

PERCENTAGE OF ORGANIZATIONS AFFECTED BY APPS THAT USE INVASIVE ADVERTISING (YEAR)

YEAR	PERCENTAGE OF ORGANIZATIONS FOUND WITH APPS THAT USE INVASIVE ADVERTISING	RATIO	CHANGE (PP)
2016	19.4	1 in 5.2	
2017	30.5	1 in 3.3	11.1
2018	26.4	1 in 3.8	-4.1

TOP COUNTRIES FOR MOBILE RANSOMWARE (YEAR)

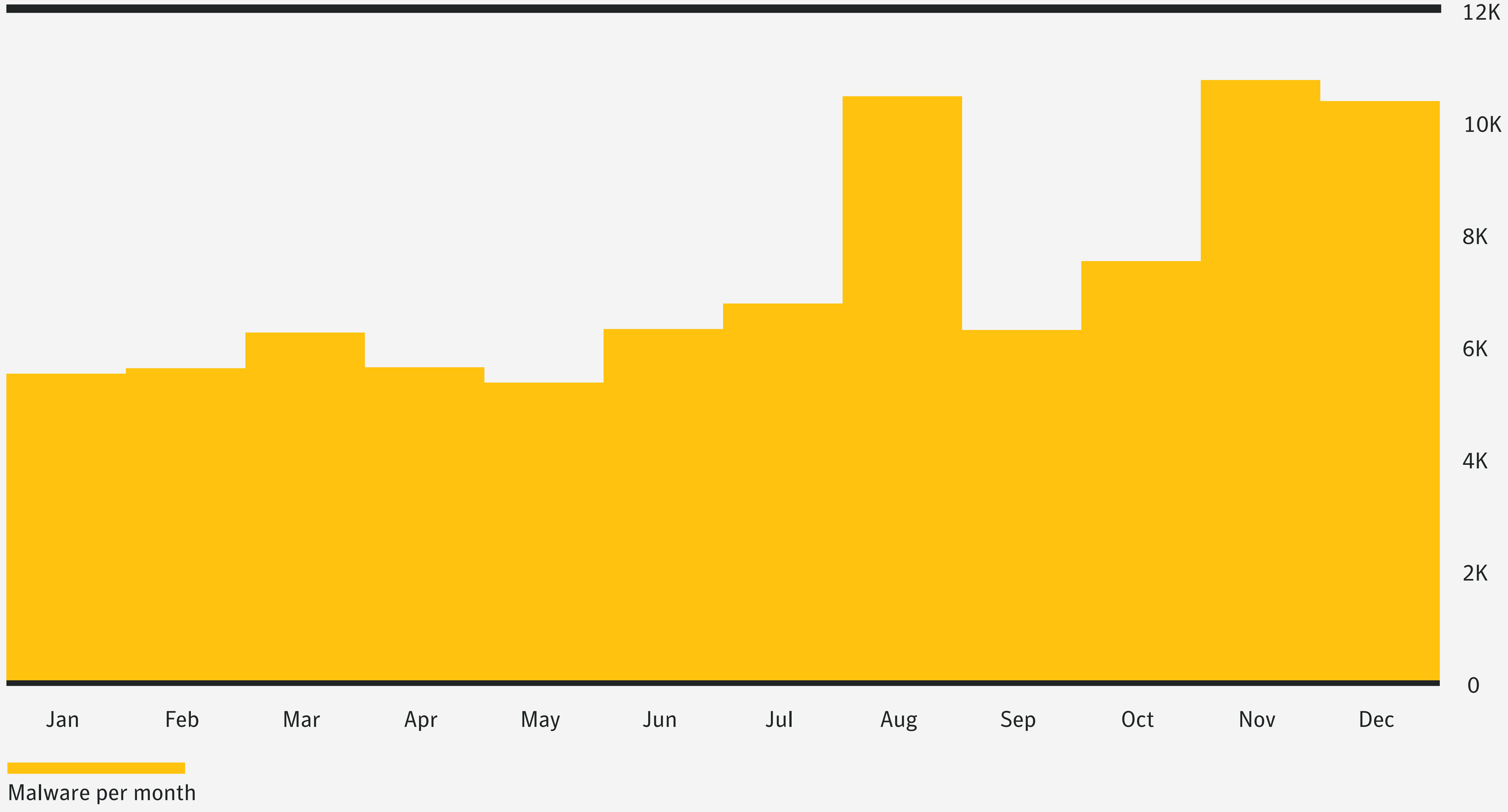


There was a marked increase in the number of ransomware infections on mobile devices during 2018, up by a third when compared to 2017.

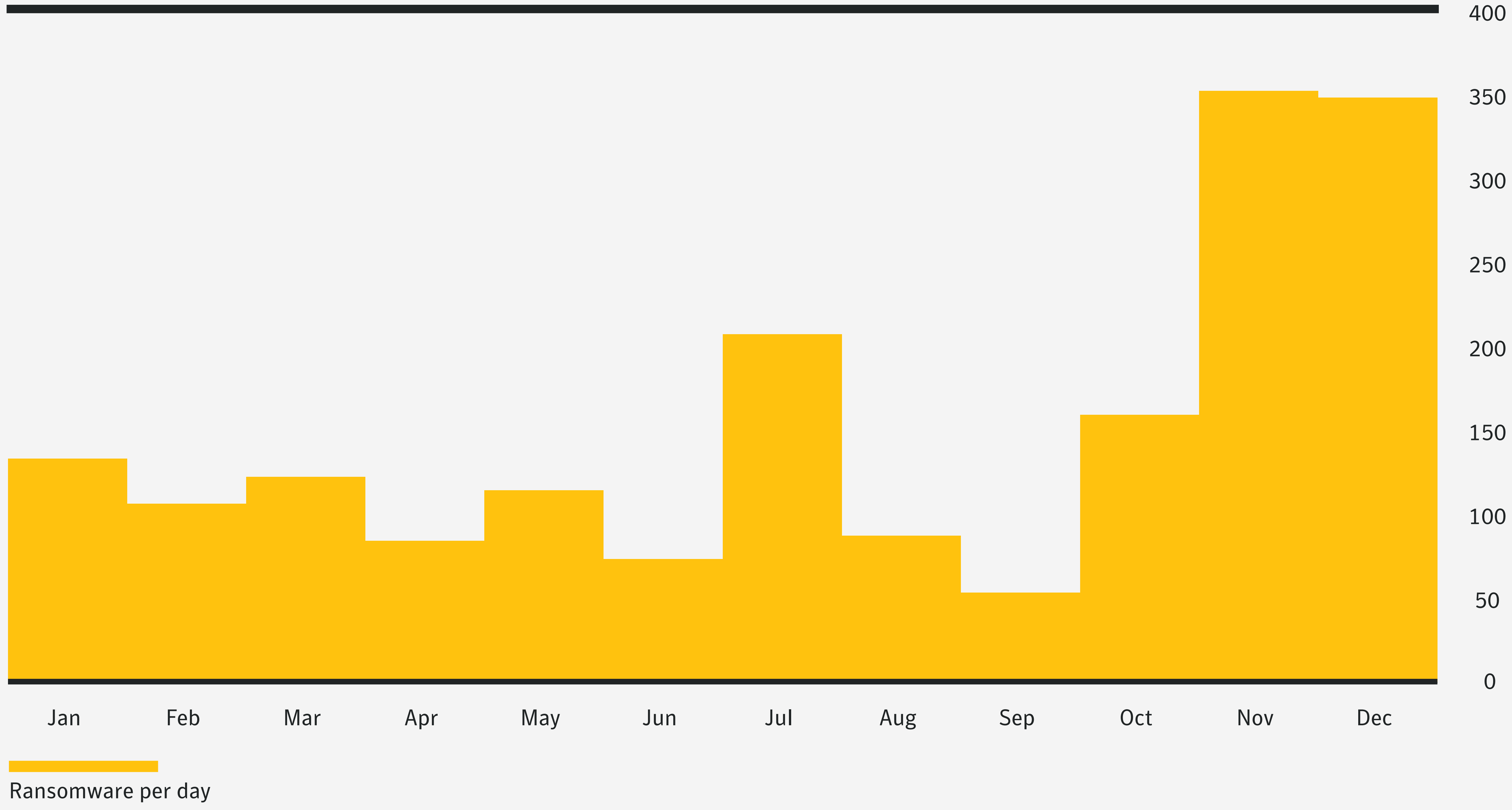
TOP MOBILE RANSOMWARE (YEAR)

THREAT NAME	PERCENT
Simplocker	59.3
Lockdroid.E	26.2
LockScreen	7.1
Simplocker.B	2.8
Ransomware	2.7
Ransomeware	1.0
Lockdroid.F	0.7
Android.WannaLocker	<0.1
WannaLocker	<0.1
Lockdroid.G	<0.1

NUMBER OF MOBILE MALWARE BLOCKED (MONTH)



NUMBER OF MOBILE RANSOMWARE BLOCKED (MONTH)



While the annual total of mobile malware infections fell in 2018, infection numbers began to climb upwards again during the fourth quarter of the year.

WEB ATTACKS

In 2018, 1 in 10 URLs analyzed were identified as being malicious, up from 1 in 16 in 2017. Additionally, despite a drop off in exploit kit activity, overall web attacks on endpoints increased by 56 percent in 2018. By December, Symantec was blocking more than 1.3 million unique web attacks on endpoint machines every day.

Formjacking was one of the biggest cyber security trends of the year, with an average of 4,800 websites compromised with formjacking code every month in 2018. Formjacking is the use of malicious JavaScript code to steal payment card details and other information from payment forms on the checkout web pages of eCommerce sites, and in total Symantec blocked 3.7 million formjacking attempts on endpoint devices in 2018. More than a third of formjacking activity took place in the last quarter of 2018, with 1.36 million formjacking attempts blocked in that period alone.

FORMJACKING ACTIVITY

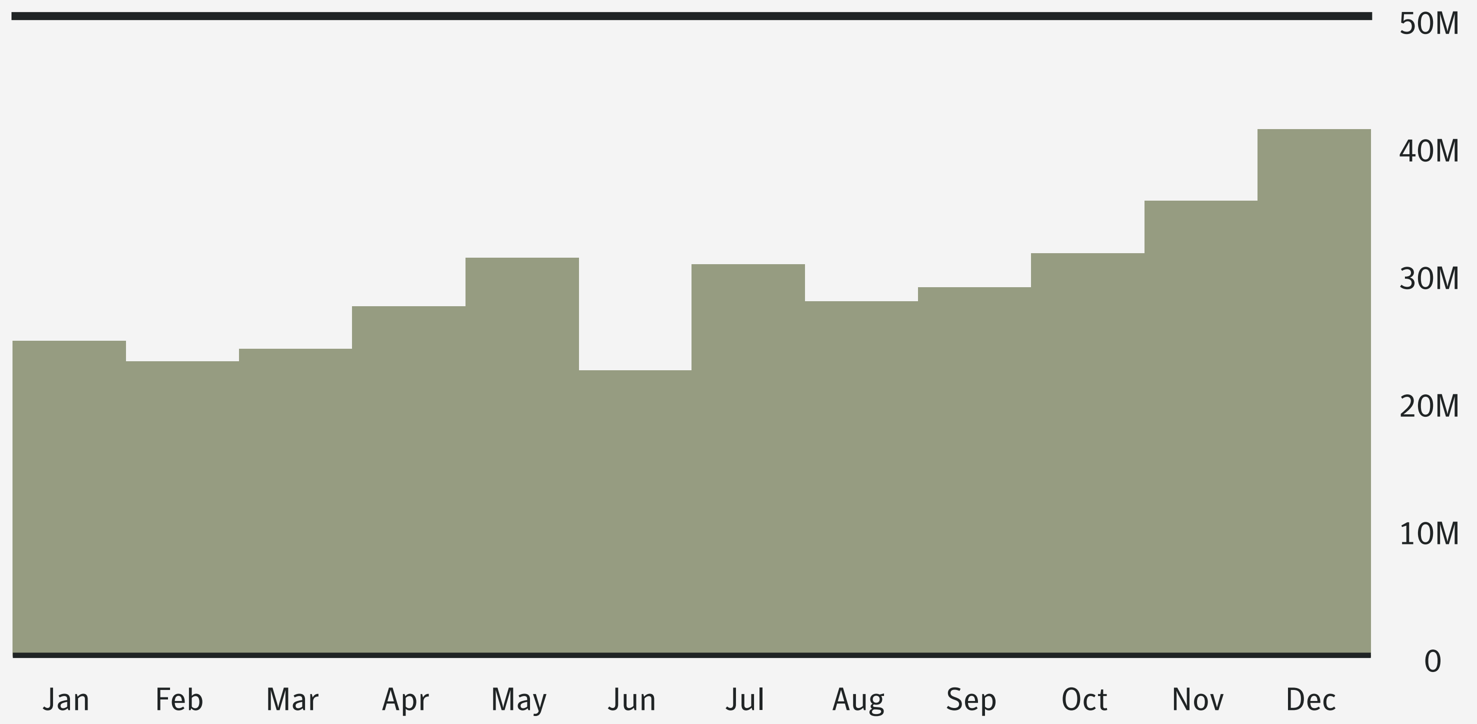
More than a third of the formjacking activity took place in the last quarter of 2018.

1,400,000
1,200,000
1,000,000
800,000
600,000
400,000
200,000
697,187
1st QTR
1,122,229
2nd QTR
551,117
3rd QTR
1,362,990
4th QTR
FORMJACKING BY QTR
FORMJACKING BY MONTH
JAN
FEB
MAR
APR
MAY
JUN
JUL
AUG
SEP
OCT
NOV
DEC

WEB ATTACKS (YEAR)

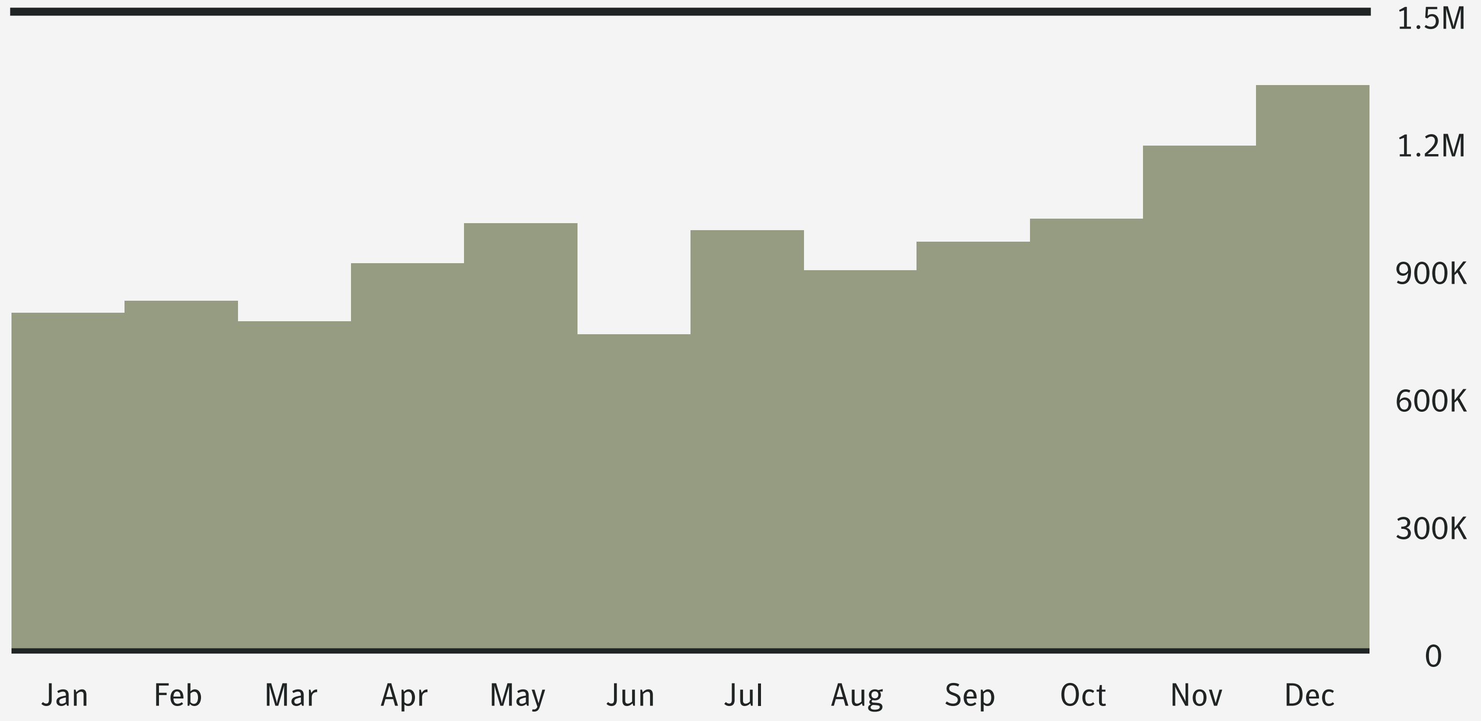
TOTAL WEB ATTACKS BLOCKED	AVERAGE WEB ATTACKS BLOCKED PER DAY
348,136,985	953,800

WEB ATTACKS (MONTH)



▨ Web attacks per month

WEB ATTACKS (DAY)



▨ Web attacks per day

TOP COMPROMISED WEBSITE CATEGORIES (YEAR)

DOMAIN CATEGORIES	2017 (%)	2018 (%)	PERCENTAGE POINT DIFFERENCE
Dynamic DNS	15.7	16.6	0.8
Gambling	7.9	16.3	8.4
Hosting	8.2	8.7	0.5
Technology	13.6	8.1	-5.5
Shopping	4.6	8.1	3.6
Business	9.0	7.2	-1.7
Pornography	3.2	5.2	2.1
Health	5.7	4.5	-1.2
Educational	3.7	3.9	0.2
Content Delivery Network	2.1	2.6	0.6

MALICIOUS URLS (YEAR)

YEAR	PERCENT OF TOTAL	RATIO	PERCENTAGE POINT CHANGE
2017	6.4	1 in 16	
2018	9.9	1 in 10	3.4

BOTNET URLS (YEAR)

YEAR	PERCENT OF ALL URLS	RATIO	PERCENT OF MALICIOUS URLS	RATIO	PERCENTAGE CHANGE	PERCENTAGE POINT CHANGE
2017	1.2	1 in 85	18.2	1 in 5		
2018	1.8	1 in 54	18.7	1 in 5	57.6	0.7

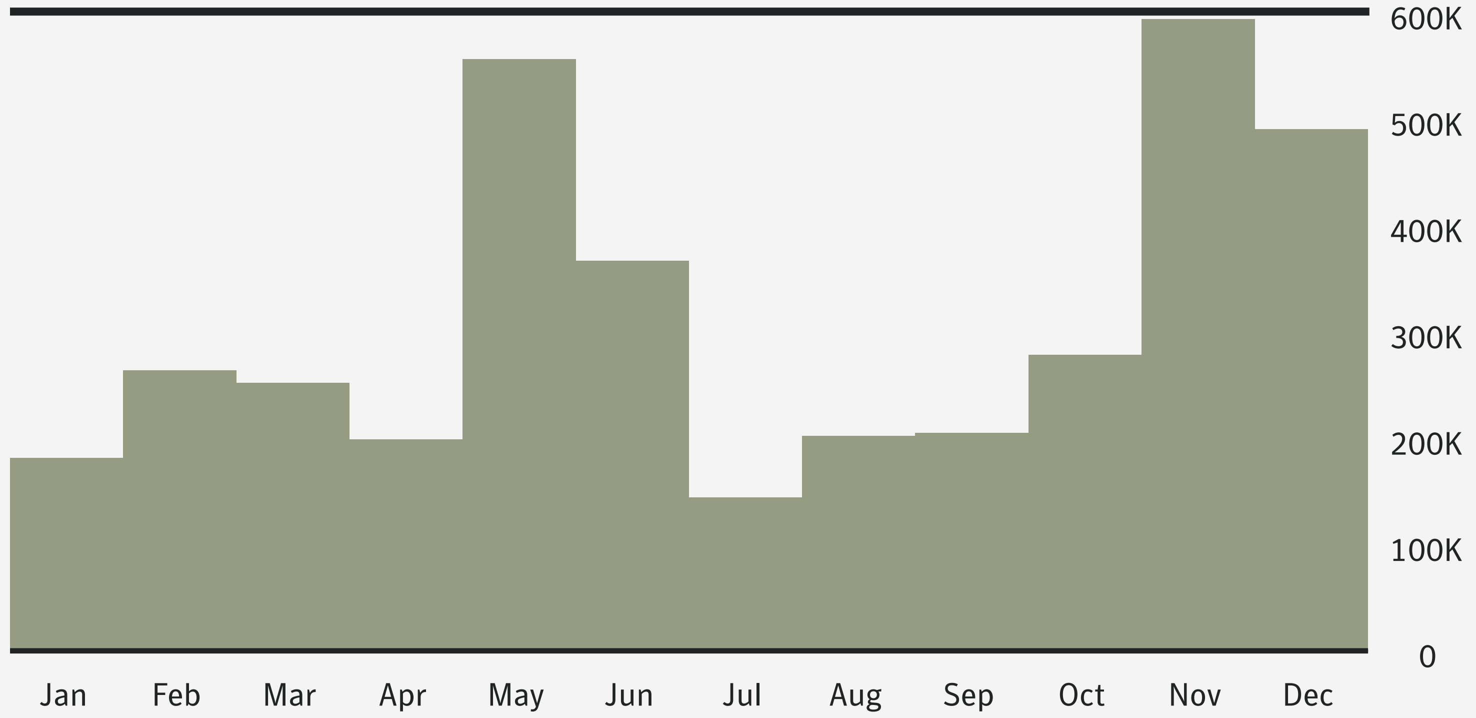
PHISHING URLS (YEAR)

YEAR	PERCENT OF ALL URLS	RATIO	PERCENT OF MALICIOUS URLS	RATIO	PERCENTAGE CHANGE	PERCENTAGE POINT CHANGE
2017	0.4	1 in 235	6.6	1 in 15		
2018	0.6	1 in 170	5.9	1 in 17	38.1	0.2

FORMJACKING ATTACKS (YEAR)

YEAR	FORMJACKING ATTACKS
2018	3,733,523

FORMJACKING ATTACKS (MONTH)



▨ Formjacking attacks

AVERAGE FORMJACKING WEBSITES (MONTH)

YEAR	AVERAGE WEBSITES EACH MONTH
2018	4,818

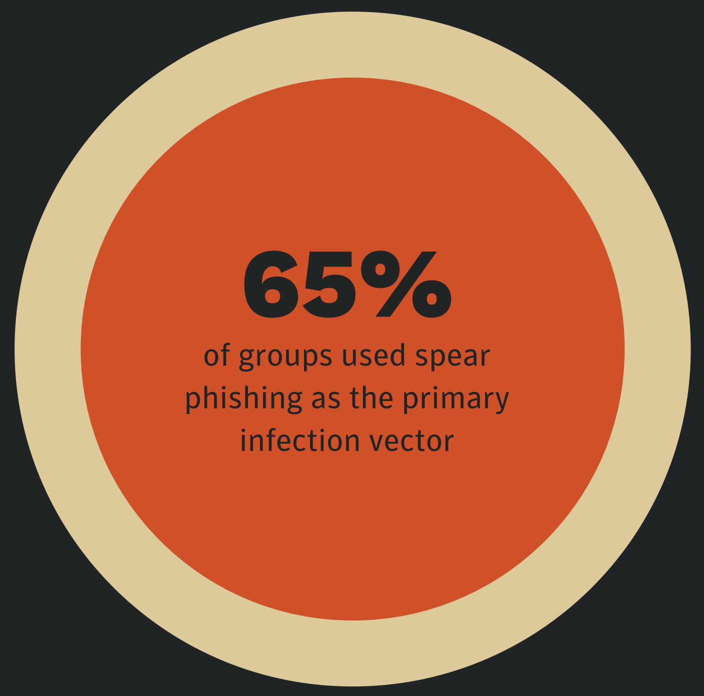
Back to ToC

TARGETED ATTACKS

While the overall number of targeted attacks was down somewhat last year, the most active groups stepped up their activity, attacking an average of 55 organizations over the past three years, up from 42 between 2015 and 2017. Spear-phishing emails remained the most popular avenue for attack and were used by 65 percent of all known groups. The most likely reason for an organization to experience a targeted attack was intelligence gathering, which is the motive for 96 percent of groups.

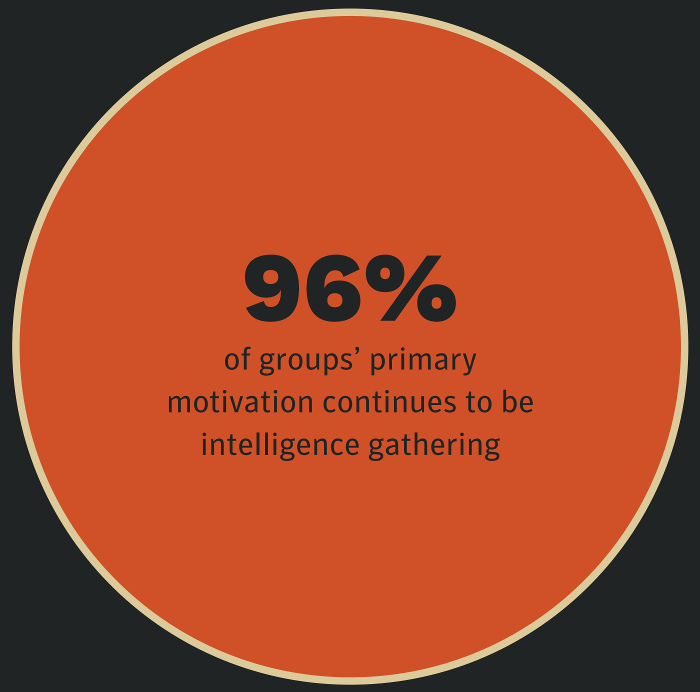
Alongside the rise in popularity of living off the land tactics, the use of zero-day vulnerabilities declined in 2018, with only 23 percent of groups known to have exploited zero days, down from 27 percent in 2017. While still a niche area, the use of destructive malware continued to grow. Eight percent of groups were known to use destructive tools, a 25 percent increase over 2017.

SPEAR PHISHING



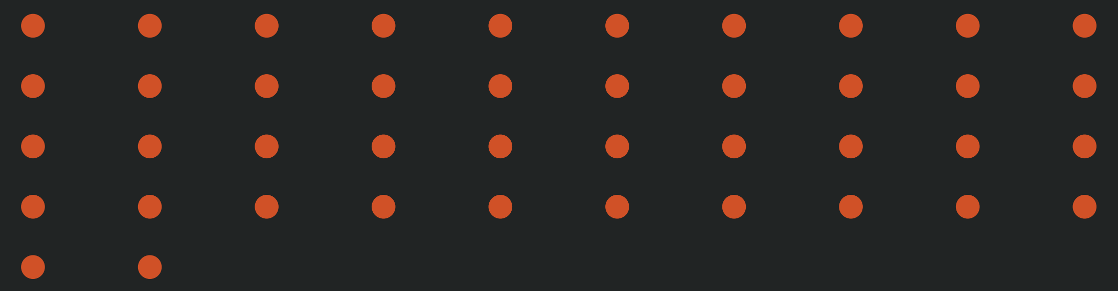
65% of groups used spear phishing as the primary infection vector

INTELLIGENCE GATHERING



96% of groups' primary motivation continues to be intelligence gathering

2015-2017: AVG 42 ORGS TARGETED PER GROUP (20 MOST ACTIVE GROUPS)



2016-2018: AVG 55 ORGS TARGETED PER GROUP (20 MOST ACTIVE GROUPS)

↓ **23%** Groups using zero-day vulnerabilities

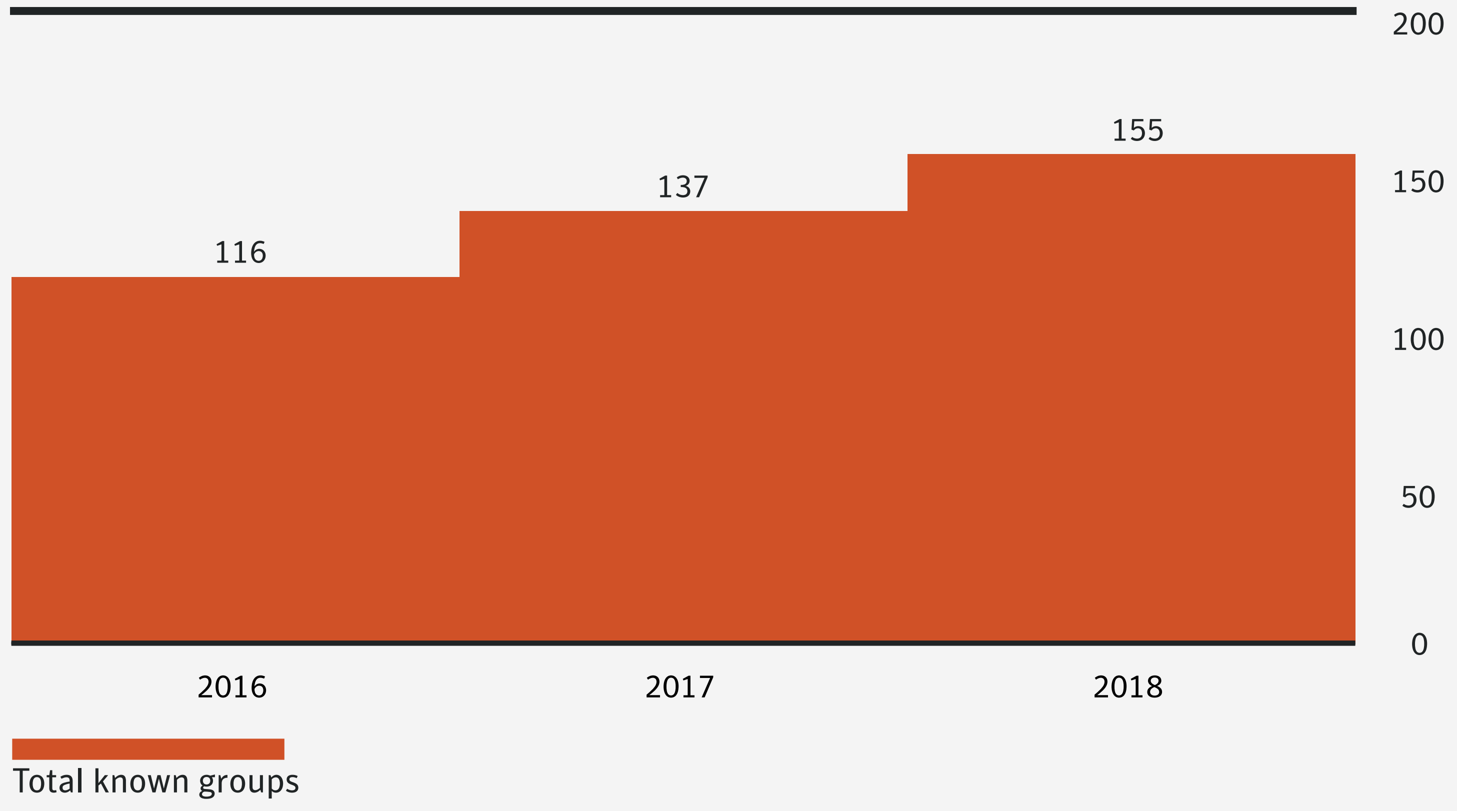
↑ **8%** Groups using destructive malware

ESPIONAGE INDICTMENTS BY U.S. AUTHORITIES

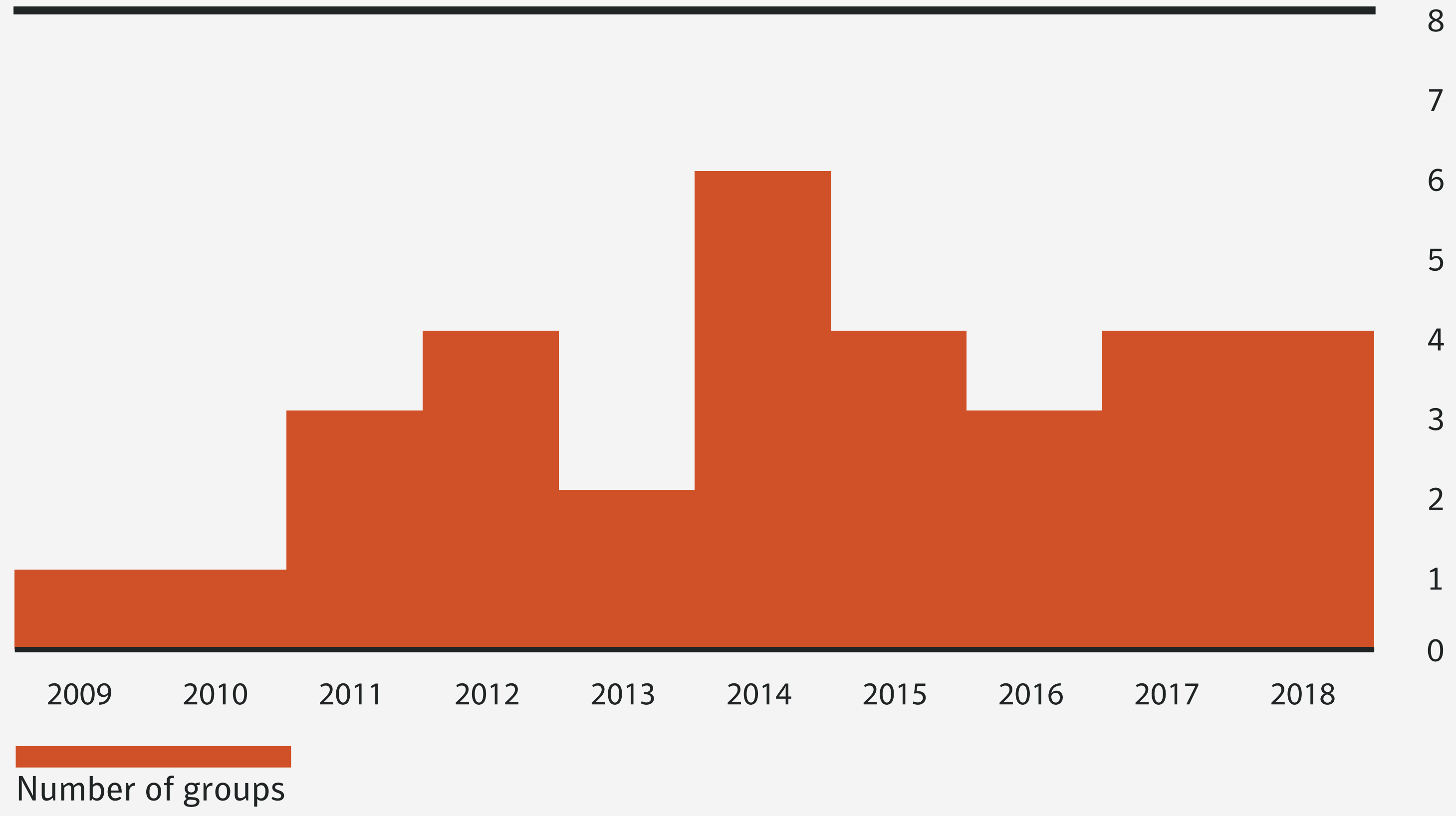
2016	2017	2018
5	4	49

2018: 19 CHINA; 18 RUSSIA; 11 IRAN; 1 NORTH KOREA

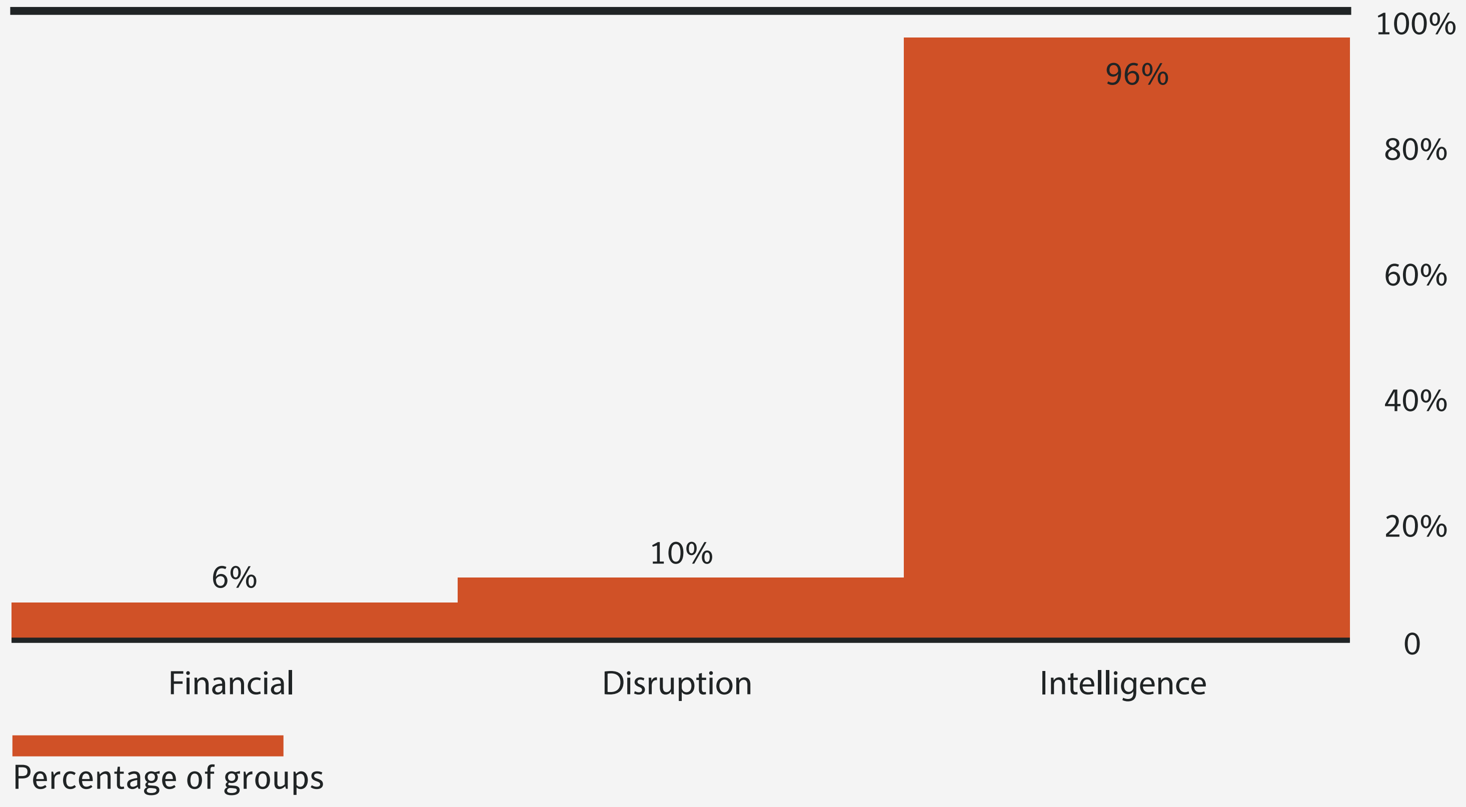
TARGETED ATTACK GROUPS KNOWN (YEAR)



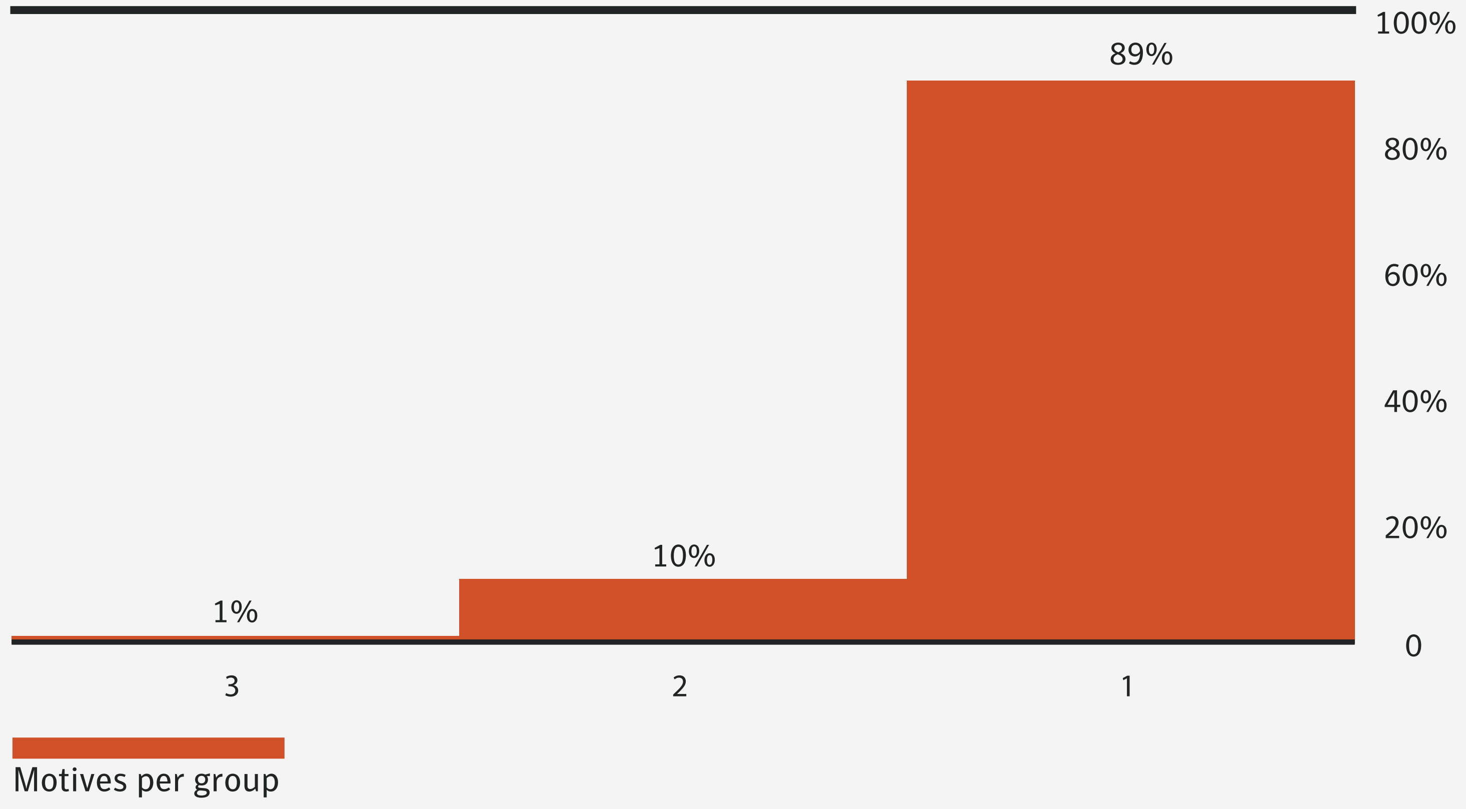
TARGETED ATTACK GROUPS EXPOSED BY SYMANTEC (YEAR)



TARGETED ATTACK GROUP MOTIVES (ALL TIME)



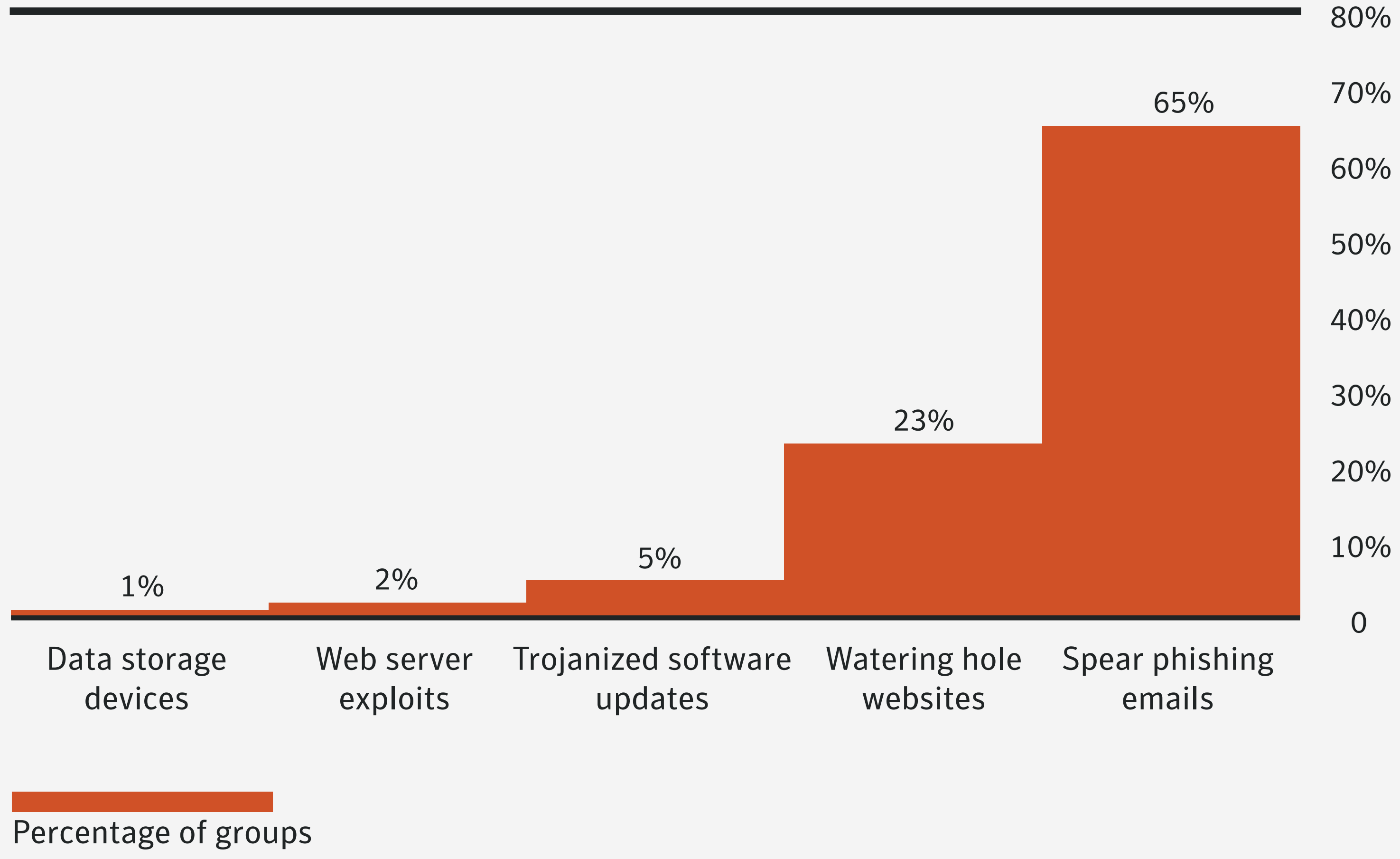
MOTIVES PER TARGETED ATTACK GROUP (ALL TIME)



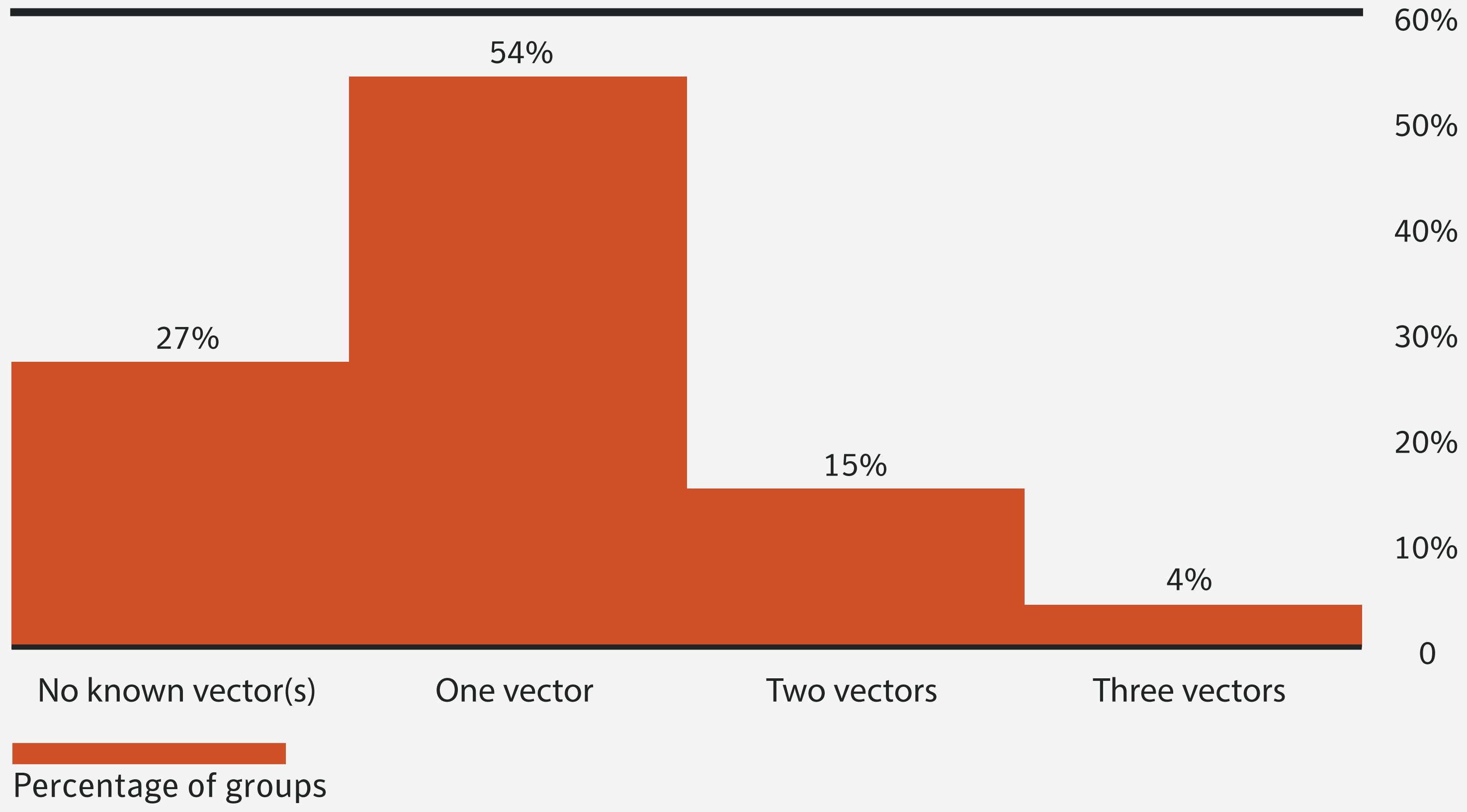
The most likely reason for an organization to experience a targeted attack was intelligence gathering, which is the motive for 96 percent of groups.

Spear-phishing emails remained the most popular avenue for attack and were used by 65 percent of all known groups.

TARGETED ATTACK GROUP INFECTION VECTORS (ALL TIME)



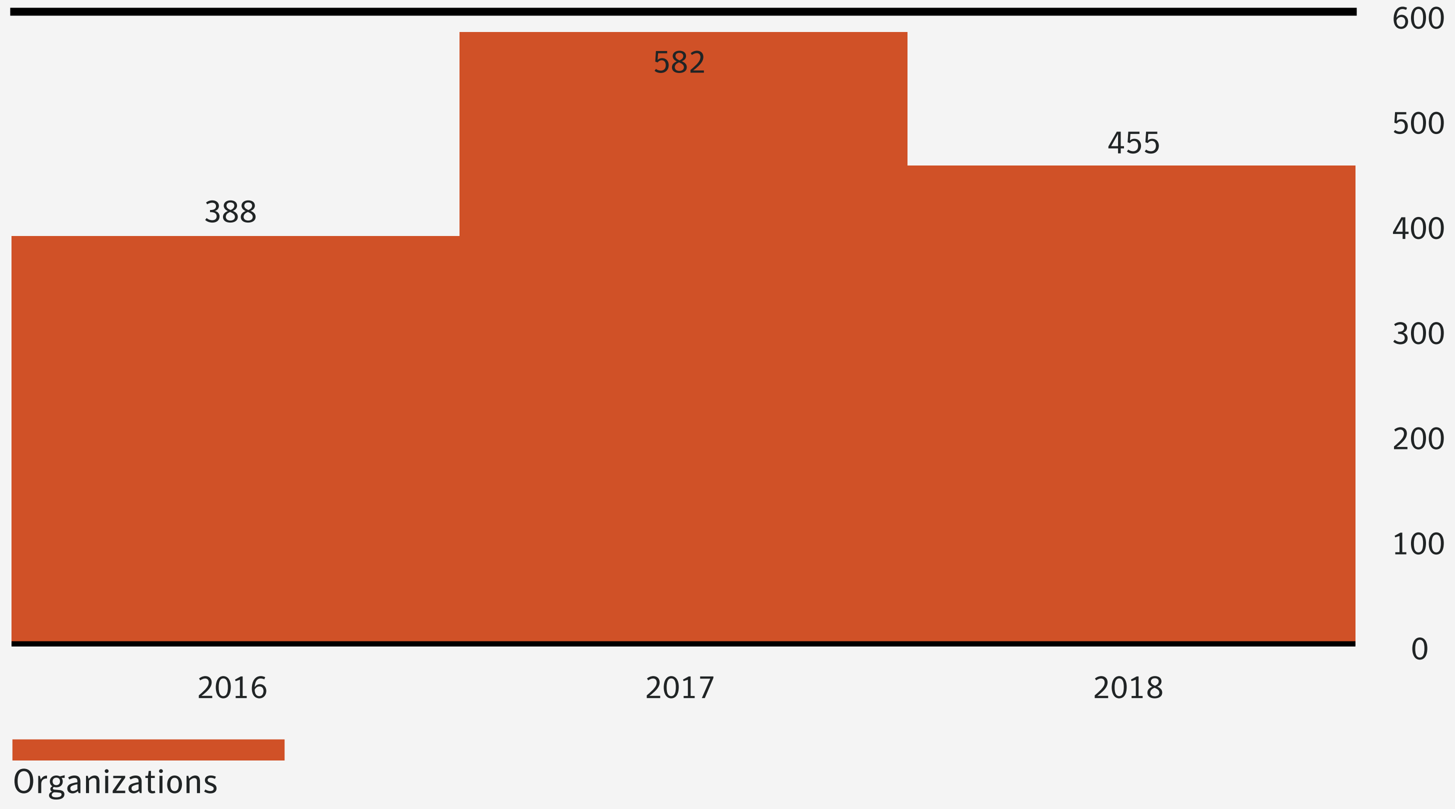
INFECTION VECTORS PER TARGETED ATTACK GROUP (ALL TIME)



TOP COUNTRIES AFFECTED BY TARGETED ATTACK GROUPS (2016-2018)

COUNTRY	ATTACKS
USA	255
India	128
Japan	69
China	44
Turkey	43
Saudi Arabia	42
South Korea	40
Taiwan	37
UAE	30
Pakistan	28

NUMBER OF ORGANIZATIONS AFFECTED BY TARGETED ATTACKS (YEAR)



NUMBER OF TOOLS USED BY THE 20 MOST ACTIVE GROUPS (2016-2018)

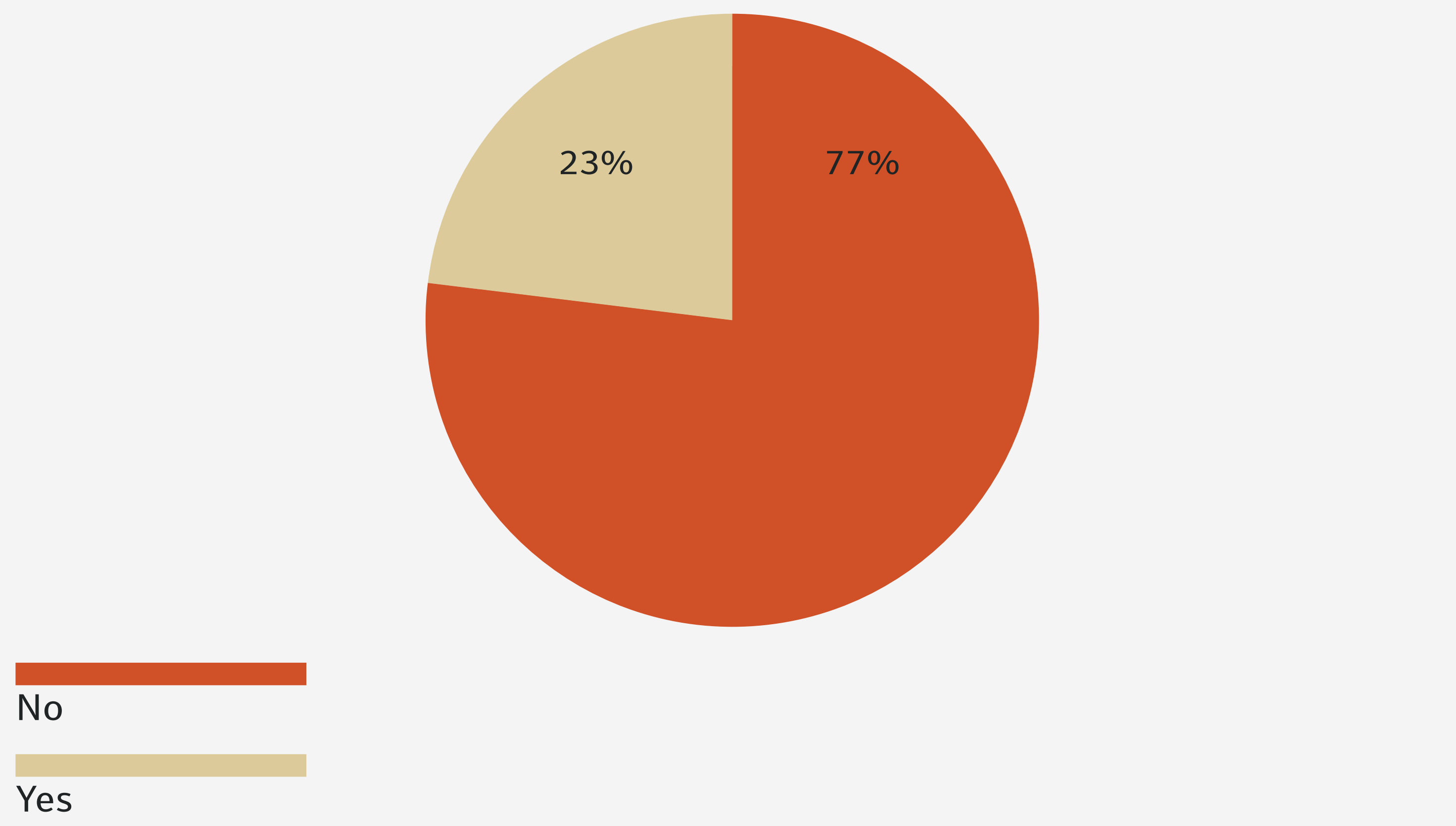
MINIMUM	MAXIMUM	AVERAGE
1	18	5

AVERAGE NUMBER OF ORGANIZATIONS TARGETED BY THE 20 MOST ACTIVE GROUPS (2016-2018)

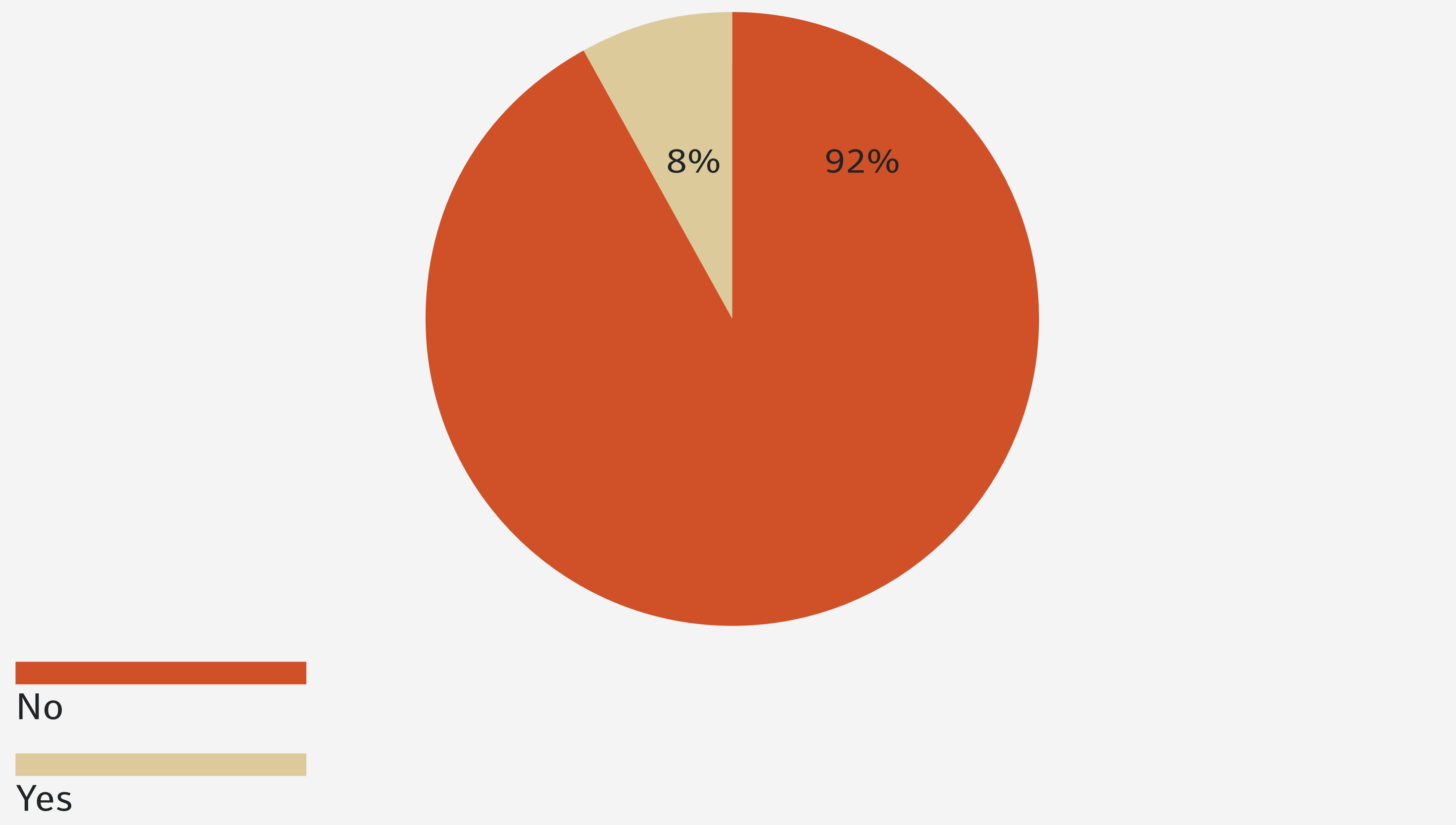
2016-2018
55

While still a niche area, the use of destructive malware continued to grow. Eight percent of groups were known to use destructive tools, up from 6 percent at the end of 2017.

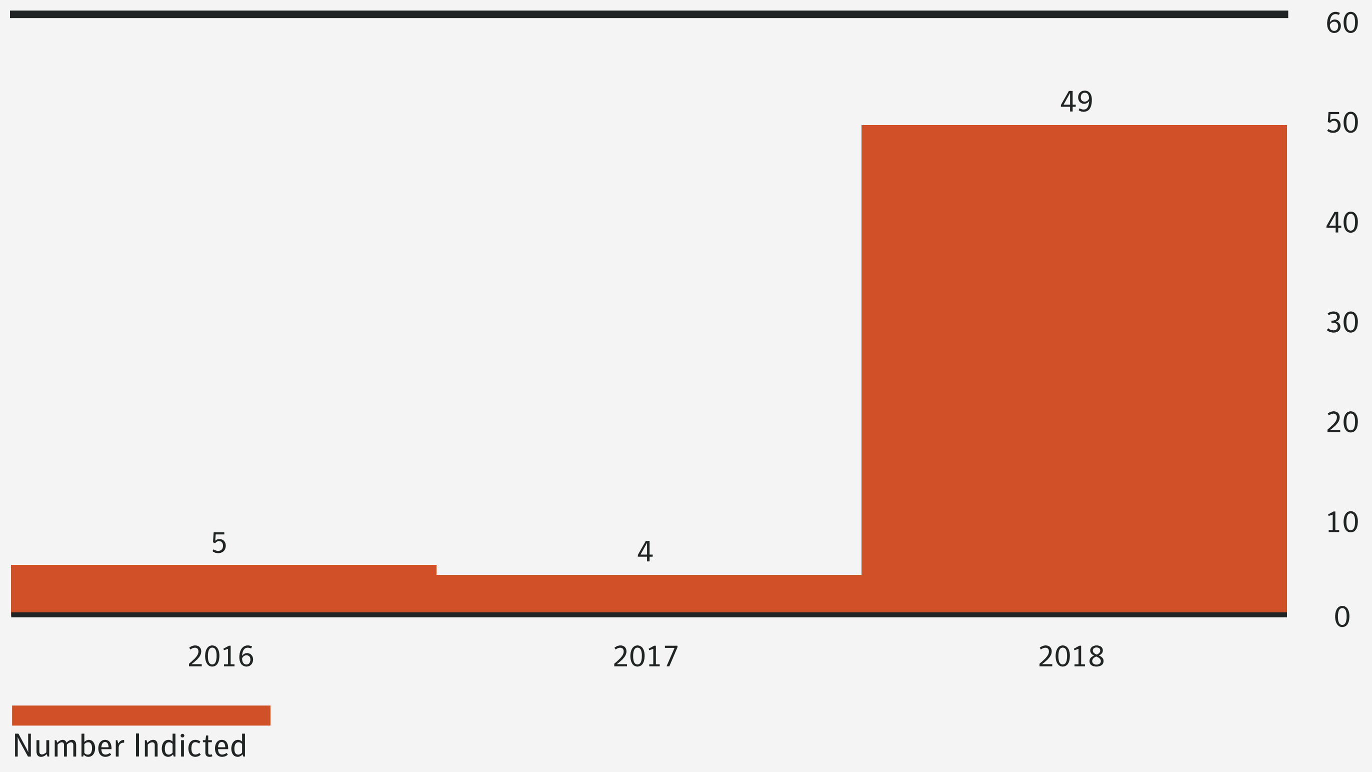
PERCENTAGE OF GROUPS KNOWN TO USE ZERO-DAY VULNERABILITIES (ALL TIME)



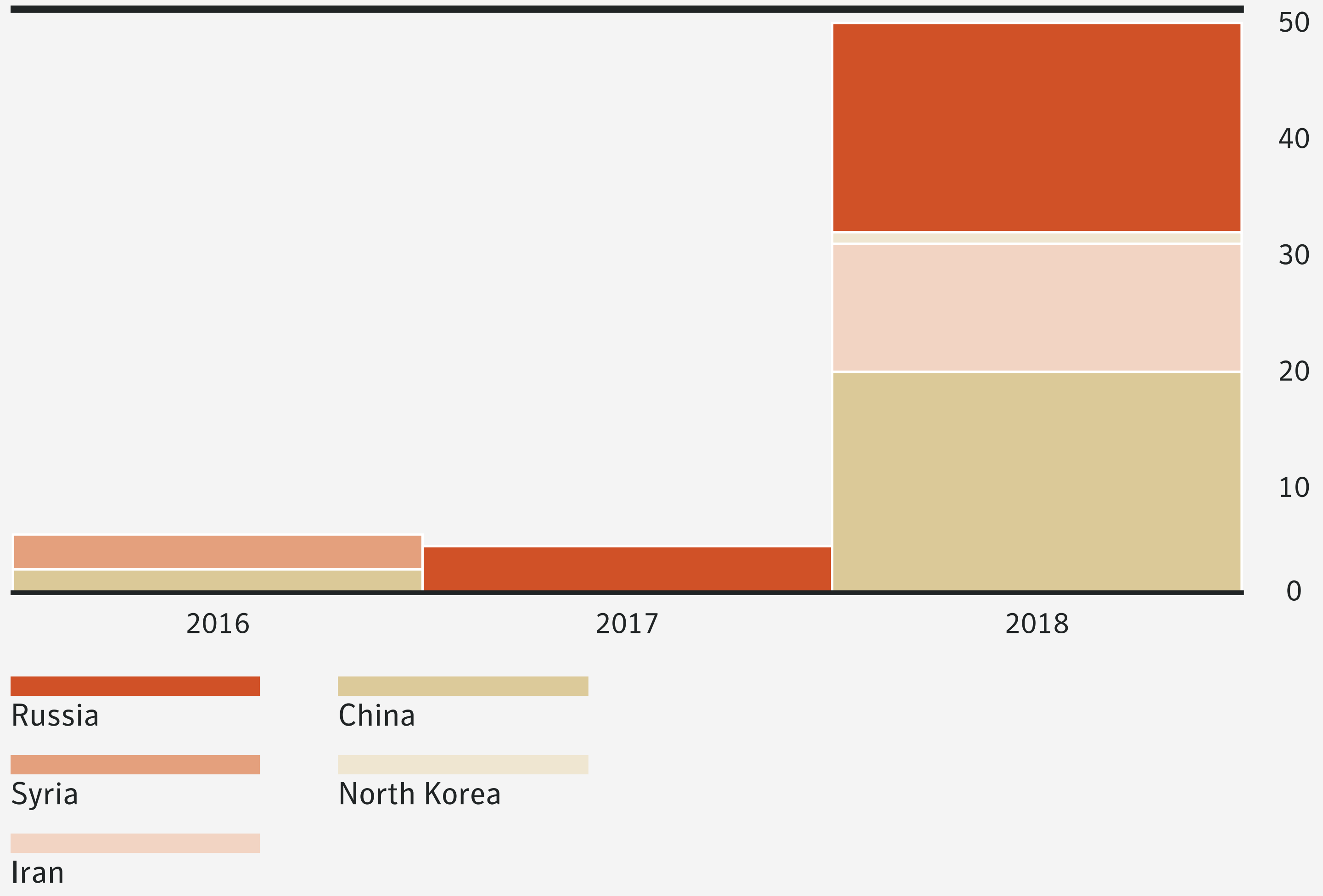
PERCENTAGE OF GROUPS KNOWN TO USE DESTRUCTIVE MALWARE (ALL TIME)



TOTAL INDICTMENTS BY U.S. AUTHORITIES (YEAR)



INDICTMENTS BY U.S. AUTHORITIES BY COUNTRY (YEAR)



IOT

After a massive increase in Internet of Things (IoT) attacks in 2017, attack numbers stabilized in 2018, when the number of attacks averaged 5,200 per month against Symantec's IoT honeypot. Routers and connected cameras were by far the main source of IoT attacks, accounting for over 90 percent of all attacks on the honeypot. The proportion of infected cameras used in attacks increased considerably during 2018. Connected cameras accounted for 15 percent of attacks, up from 3.5 percent in 2017. Attackers were also increasingly focused on Telnet as an avenue for attack. Telnet accounted for over 90 percent of attempted attacks in 2018, a jump from 50 percent in 2017.

ATTACKS INVOLVING CONNECTED CAMERAS UP FROM 3.5% IN 2017 TO 15% IN 2018

ROUTERS AND CONNECTED CAMERAS

WERE THE MAIN SOURCE OF IOT ATTACKS

ACCOUNTING FOR OVER

90 PERCENT

OF ACTIVITY.

IOT DEVICES EXPERIENCE AN AVERAGE OF 5,200 ATTACKS PER MONTH

TOP SOURCE COUNTRIES FOR IOT ATTACKS (YEAR)

COUNTRY	PERCENT
China	24.0
USA	10.1
Brazil	9.8
Russia	5.7
Mexico	4.0
Japan	3.7
Vietnam	3.5
South Korea	3.2
Turkey	2.6
Italy	1.9

TOP USER NAMES USED IN IOT ATTACKS (YEAR)

USER NAME	PERCENT
root	38.1
admin	22.8
enable	4.5
shell	4.2
sh	1.9
[BLANK]	1.7
system	1.1
enable	0.9
>/var/tmp/.ptmx && cd /var/tmp/	0.9
>/var/.ptmx && cd /var/	0.9

TOP PASSWORDS USED IN IOT ATTACKS (YEAR)

PASSWORDS	PERCENT
123456	24.6
[BLANK]	17.0
system	4.3
sh	4.0
shell	1.9
admin	1.3
1234	1.0
password	1.0
enable	1.0
12345	0.9

TOP IOT THREATS (YEAR)

THREAT NAME	PERCENT
Linux.Lightaidra	31.3
Linux.Kaiten	31.0
Linux.Mirai	15.9
Trojan.Gen.2	8.5
Downloader.Trojan	3.2
Trojan.Gen.NPE	2.8
Linux.Mirai!g1	1.9
Linux.Gafgyt	1.7
Linux.Amnesiark	1.1
Trojan.Gen.NPE.2	0.8

The notorious Mirai distributed denial of service (DDoS) worm remained an active threat and, with 16 percent of the attacks, was the third most common IoT threat in 2018.

Routers and connected cameras were the most infected devices and accounted for 75 and 15 percent of the attacks respectively.

TOP PROTOCOLS ATTACKED BY IOT THREATS (YEAR)

TARGETED SERVICE	PERCENT
telnet	90.9
http	6.6
https	1.0
smb	0.8
ssh	0.6
ftp	<0.1
snmp	<0.1
cwmp	<0.1
upnp	<0.1
modbus	<0.1

TOP PORTS ATTACKED BY IOT THREATS (YEAR)

TCP PORT NUMBER	DESCRIPTION	PERCENT
23	Telnet	85.0
80	World Wide Web HTTP	6.5
2323	Telnet (alternate)	5.8
443	HTTP over TLS/SSL	1.0
445	Microsoft Directory Services	0.8
22	Secure Shell (SSH) Protocol	0.6
8080	HTTP (alternate)	0.1
2223	Rockwell CSP2	<0.1
2222	Secure Shell (SSH) Protocol (alternate)	<0.1
21	File Transfer Protocol [Control]	<0.1

TOP DEVICE TYPES PERFORMING IOT ATTACKS (YEAR)

DEVICE TYPE	PERCENT
Router	75.2
Connected Camera	15.2
Multi Media Device	5.4
Firewall	2.1
PBX Phone System	0.6
NAS (Network Attached Storage)	0.6
VoIP phone	0.2
Printer	0.2
Alarm System	0.2
VoIP Adapter	0.1

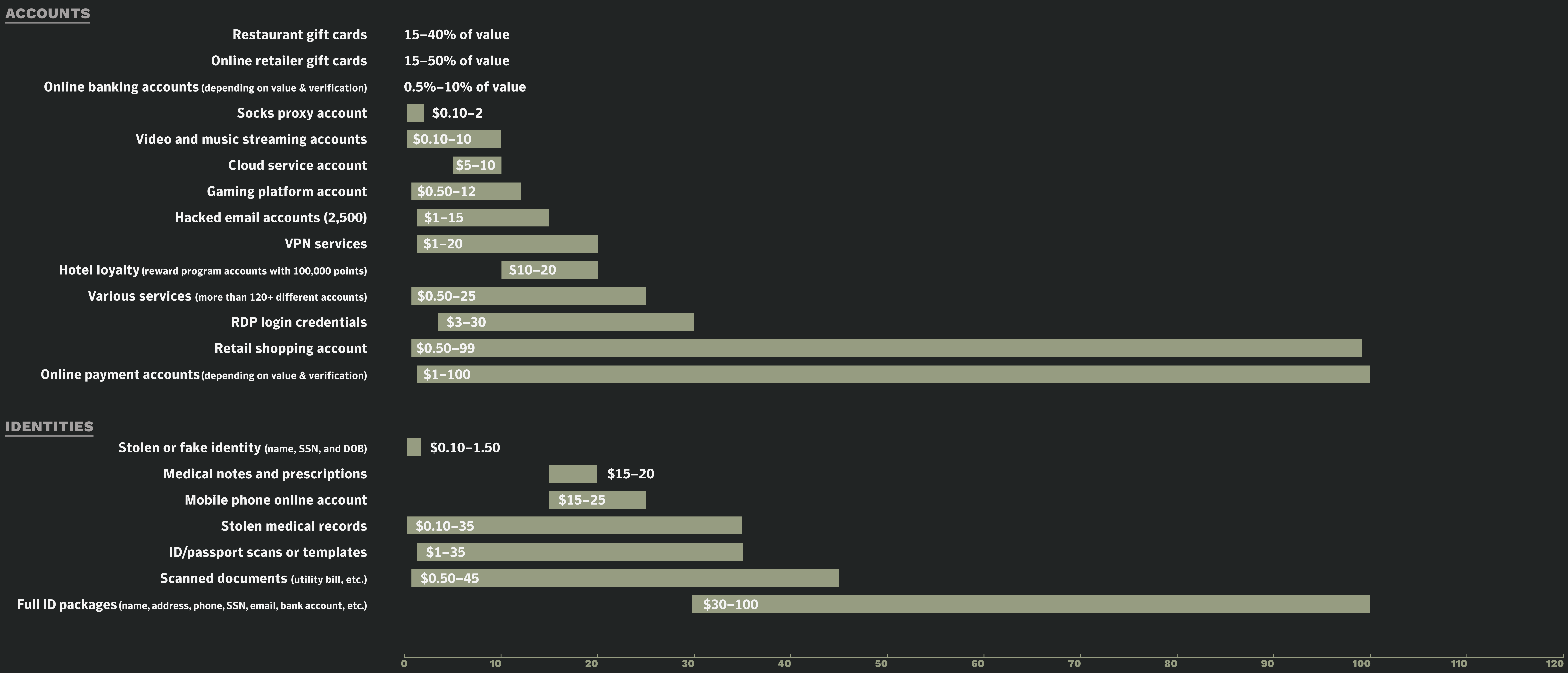
ATTACKS AGAINST IOT DEVICES (YEAR)

YEAR	TOTAL ATTACKS	PERCENT CHANGE
2017	57,691	
2018	57,553	-0.2

AVERAGE ATTACKS AGAINST IOT DEVICES (MONTH)

PER MONTH
5,233

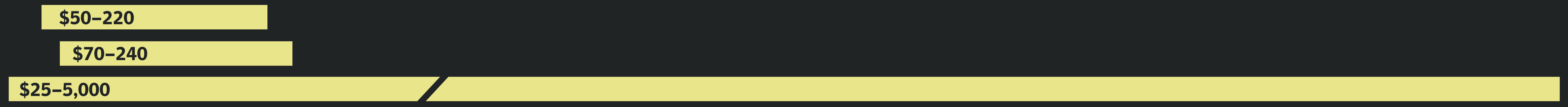
UNDERGROUND ECONOMY



UNDERGROUND ECONOMY

IDENTITIES (CONT.)

Fake health care ID cards	$50–220
Parcel drop off box for deliveries	$70–240
Fake ID, driver license, passport, etc.	$25–5,000

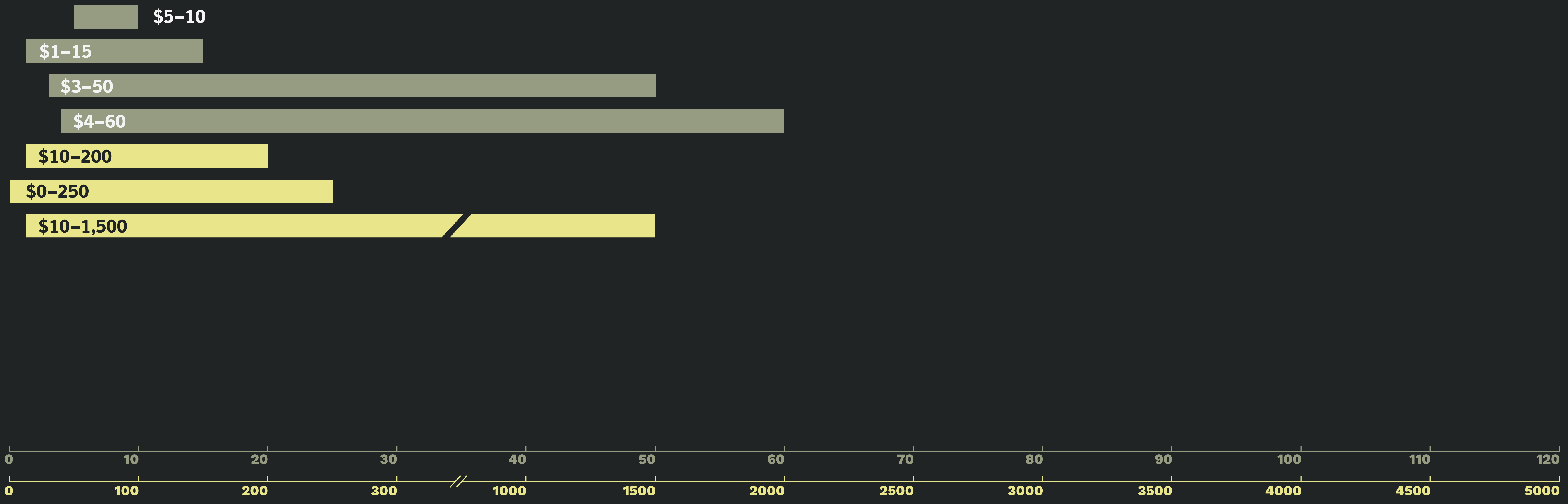


MONEY TRANSFER SERVICES

Cash redirector service for bank accounts	.1–15% of value
Cash redirector service for online payment system	1–5% of value
Pay $100 in Bitcoin and get a money transfer of $1000	$100
Cash redirector service	5–20% of value

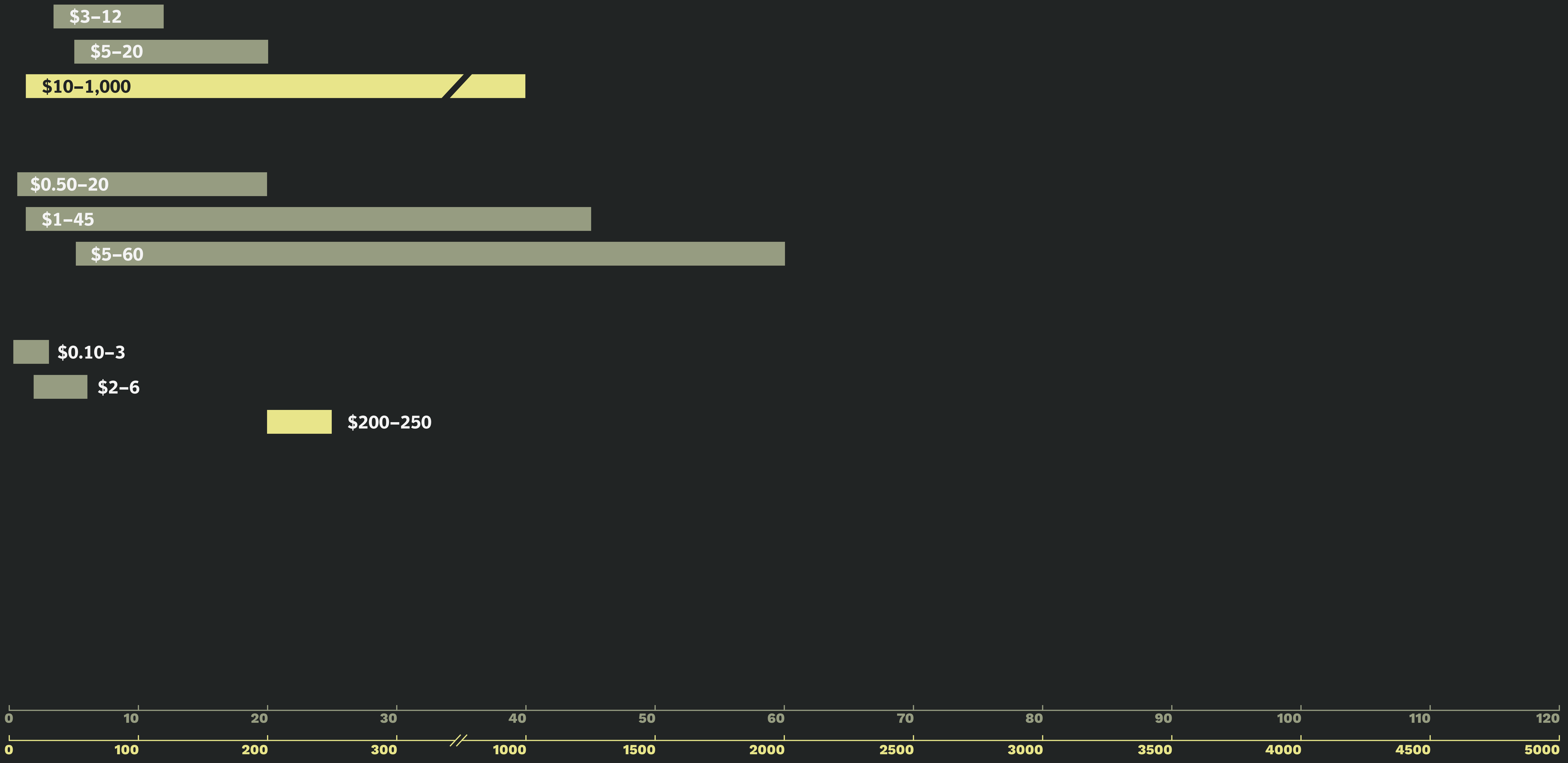
MALWARE

Office macro downloader generator	$5–10
DDoS bot software	$1–15
Spyware	$3–50
Cryptocurrency stealer malware	$4–60
Cryptocurrency miner (e.g. Monero)	$10–200
Ransomware toolkit	$0–250
Common banking Trojans toolkit with support	$10–1,500



UNDERGROUND ECONOMY

SERVICES	
Airline ticket and hotel bookings	10% of value
Money laundering service (into cash or cryptocurrencies)	4–40%
Cash out service (bank account, ATM card, and fake ID)	$350
Hacker for hire	$100+
Custom phishing page service	$3–12
DDoS service, short duration <1 hour (medium protected targets)	$5–20
DDoS service, duration >24h (medium and strong protected targets)	$10–1,000
PAYMENT CARDS	
Single credit card	$0.50–20
Single credit card with full details (fullz)	$1–45
Dump of magnetic strip track 1/2 data (e.g. from skimming)	$5–60
SOCIAL MEDIA	
100 likes on social media platforms	$0.10–3
500 social media followers	$2–6
100,000 social media video views	$200–250



These prices are taken from publicly accessible underground forums and dark web TOR sites. Closed, private forums tend to have even lower prices. We cannot verify if the goods are genuinely sold for the asked price, some of them might be fake offers.

METHODOLOGY

Symantec has established the largest civilian threat collection network in the world, and one of the most comprehensive collections of cyber security threat intelligence, through the Symantec Global Intelligence Network (GIN).

The Symantec GIN comprises more than 123 million attack sensors, recording thousands of threat events per second, and contains over 9 petabytes of security threat data. This network also monitors threat activities for over 300,000 businesses and organizations worldwide that depend on Symantec for protection. Telemetry from across Symantec's threat protection portfolio helps our 3,800 cyber security researchers and engineers identify the top trends shaping the threat landscape.

Analyses of spam, phishing, and email malware trends are gathered from a variety of Symantec email security technologies processing more than 2.4 billion emails each day, including: Symantec Messaging Gateway for Service Providers, Symantec Email Security.cloud, Symantec Advanced Threat Protection for Email, Symantec's CloudSOC™ Service, and the Symantec Probe Network. Symantec also gathers phishing information through an extensive anti-fraud community of enterprises, security vendors, and partners.

Filtering more than 322 million emails, and over 1.5 billion web requests each day, Symantec's proprietary Skeptic™ technology underlies the Symantec Email and Web Security. cloud™ services, utilizing advanced machine learning, network traffic analysis, and behavior analysis to detect even the most stealthy and persistent threats. Additionally, Symantec's Advanced Threat Protection for Email uncovers advanced email attacks by adding cloud-based sandboxing, additional spear-phishing protection, and unique targeted attack identification capabilities.

Billions of URLs are processed and analyzed each month by Symantec's Secure Web Gateway solutions, including ProxySG™, Advanced Secure Gateway (ASG), and Web Security Solution (WSS), all powered by our real-time WebPulse Collaborative Defense technology and Content Analysis System, identifying and protecting against malicious payloads and controlling sensitive web-based content.

Mobile threat intelligence, provided by Symantec Endpoint Protection Mobile (SEPM), is used to predict, detect, and protect against the broadest range of existing and unknown threats. SEPM's predictive technology uses a layered approach that leverages massive crowdsourced threat intelligence, in addition to both device-based and server-based analysis, to proactively protect mobile devices from malware, network threats, and app and OS vulnerability exploits. Additionally, mobile technology from Appthority, coupled with SEPM, offers the ability to analyze mobile apps for both malicious capabilities and unsafe and unwanted behaviors, such as vulnerabilities, risk of sensitive data loss, and privacy-invasive actions.

These resources give Symantec analysts unrivaled sources of data with which to identify, analyze, and provide informed commentary on emerging trends in cyber attacks, malicious code activity, phishing, and spam. The result is the annual Symantec Internet Security Threat Report™, which gives enterprises, small businesses, and consumers essential information to help secure their systems effectively now and into the future.

CREDITS

Team

Brigid O’Gorman
Candid Wueest
Dick O’Brien
Gillian Cleary
Hon Lau
John-Paul Power
Mayee Corpin
Orla Cox
Paul Wood
Scott Wallace

Contributors

Alan Neville
Alex Shehk
Brian Duckering
Chris Larsen
Christian Tripputi
Dennis Tan
Gavin O’Gorman
Parveen Vashishtha
Pierre-Antoine Vervier
Pravin Bange
Robert Keith
Sean Kiernan
Sebastian Zatorski
Seth Hardy
Shashank Srivastava
Shaun Aimoto
Siddhesh Chandrayan
Tor Skaar
Tyler Anderson
Yun Shen

INTERNET SECURITY THREAT REPORT

Symantec™

04/19

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043
United Stated of America

+1 650 527–8000
+1 800 721–3934

Symantec.com

For specific country offices and contact numbers, please visit our website. For product information in the U.S., call toll-free 1 (800) 745 6054.