ATTACK LANDSCAPE H2 2019

F-Secure

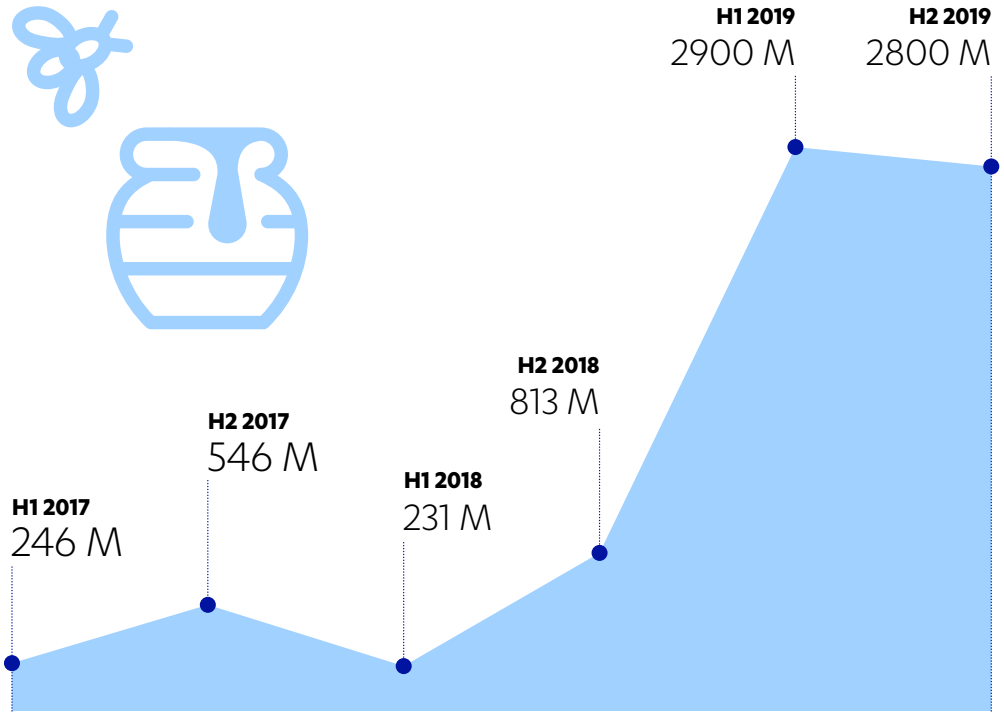
2019 wrapped up with high-impact ransomware attacks on enterprises, as well as continued high rates of attack traffic throughout our global network of honeypots. Honeypot traffic was driven by action aimed at the SMB and Telnet protocols, indicating continued attacker interest in the Eternal Blue vulnerability as well as plenty of infected IoT devices. The end of the year also served as the end of the decade, prompting a look back at where we've come since 2010.

In this report, we cover the attack traffic seen by our global network of honeypots over the last six months of 2019, as well as malware seen by our customer endpoints throughout the year. We also take a trip down memory lane, revisiting cyber security highlights of the decade.

HONEYPOT ATTACK TRAFFIC: WHO'S AFTER WHO?

In the first half of 2019, we documented[1] a jump in cyber attack traffic to our global network of honeypots from millions of hits to 2.9 billion. In the second half of the year, this frenetic pace of attack traffic continued but at a slightly reduced rate, with 2.8 billion hits to our servers. DDoS attacks drove this deluge, accounting for two thirds of the traffic.

Total Global Honeypot Attacks Per Period



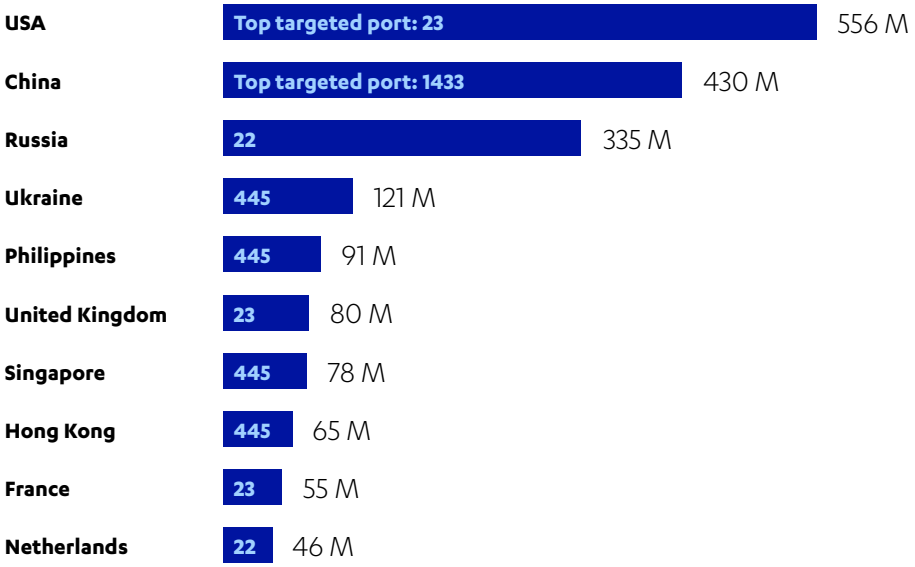
Our honeypots are decoy servers set up in countries around the world to gauge trends and patterns in the global cyber attack landscape. Because honeypots are decoys not otherwise meant for real world use, an incoming connection registered by a honeypot is either the result of a mistyped IP address, which is rather uncommon, or of the service being found during an attacker's scans of the network or the internet.

99.9% of traffic to our honeypots is automated traffic coming from bots, malware and other tools. Attacks may come from any sort of infected connected device – a traditional computer, smartwatch or even IoT toothbrush can be a source.

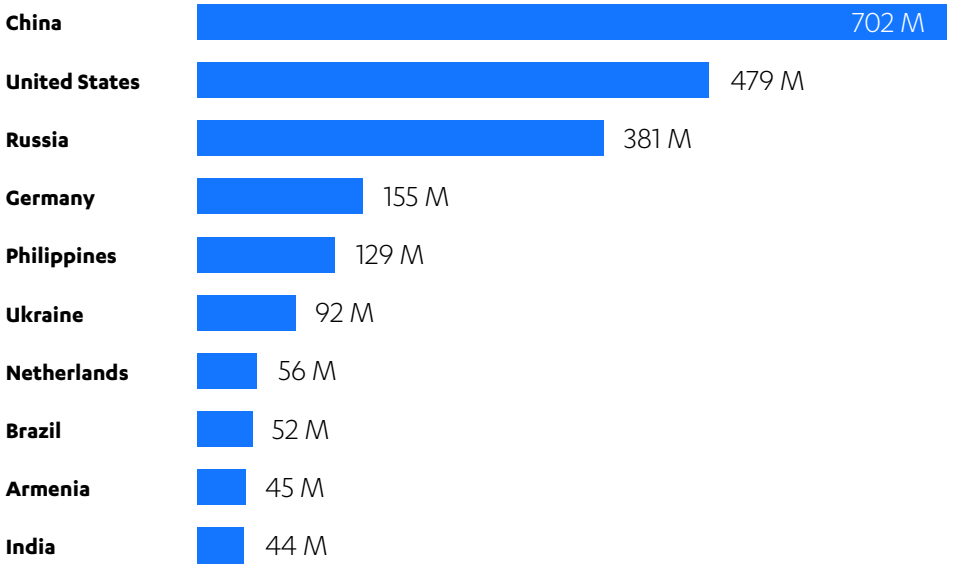
1 https://blog.f-secure.com/attack-landscape-h1-2019-iot-smb-traffic-abound/

The country whose IP space played host to the greatest number of attacks was the US, followed by China and Russia. Germany, a regular to the top 10 list, dropped off the list to number 12 with 43 million attacks, while attacks from Ukraine's IP space were enough to replace Germany in the number four spot.

Top Source Countries H2 2019



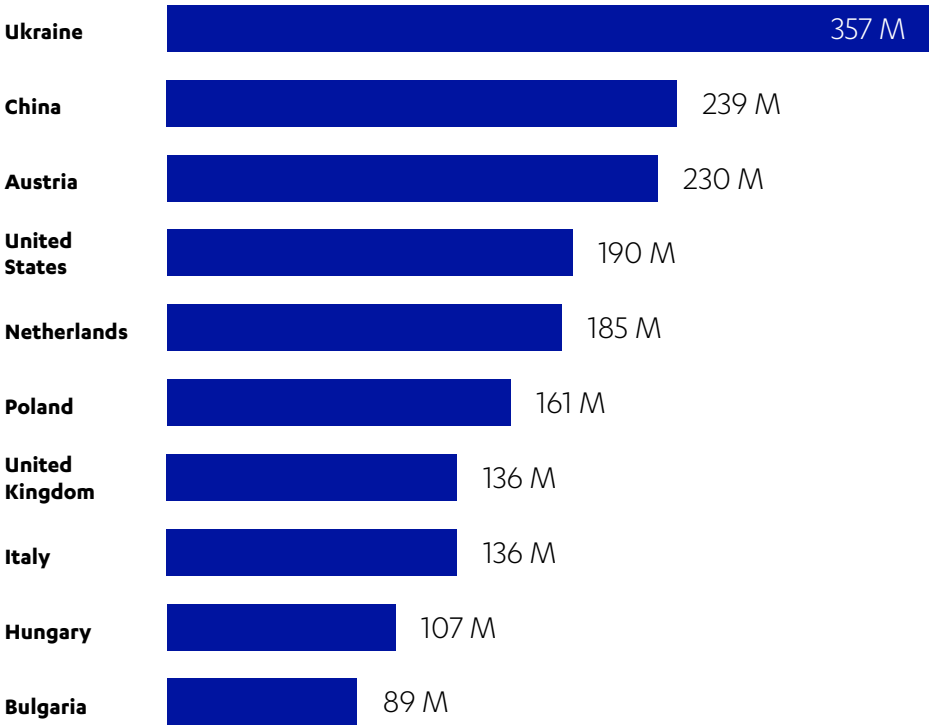
Top Source Countries H1 2019



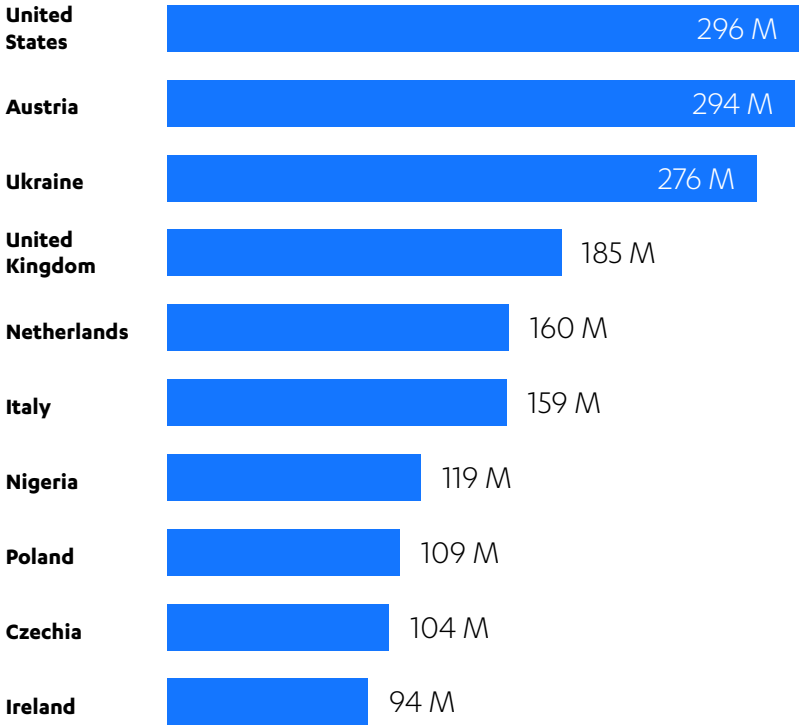
The list of source countries must be taken with a grain of salt, as attackers can route their attacks through proxies in other countries to avoid identification by authorities.

In addition, we do not mean to imply that this activity is predominantly nation-state behavior. The majority of these attacks are instigated by cyber criminals who are carrying out DDoS attacks and sending malware for financial gain.

Top Destination Countries H2 2019



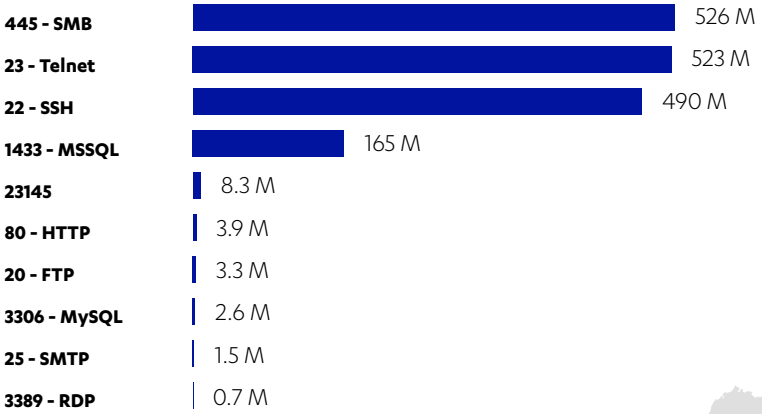
Top Destination Countries H1 2019



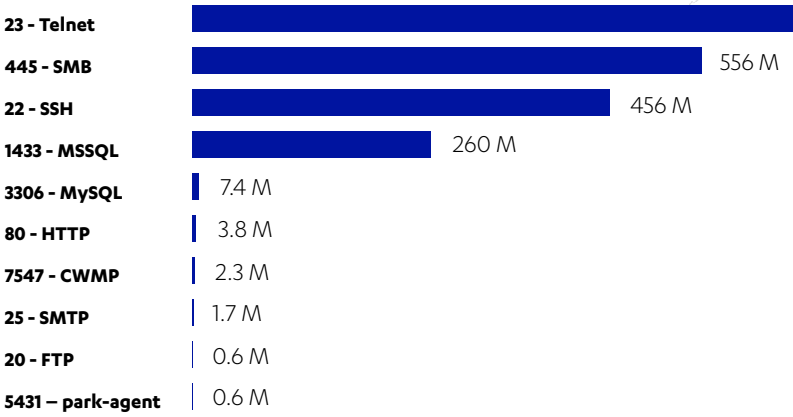
Ukraine was the top attack destination, followed by China, Austria and the US. The top aggressors hitting the Ukraine were the United States, the Ukraine itself, and Russia. In the number two spot, the top countries hitting China were China itself, the United States and France, while Austria was hit by China, Russia and the United States. Attacks hitting the United States came from primarily the US, followed by Russia and China.

PORTS AND PROTOCOLS

Top TCP Ports Targeted H2 2019

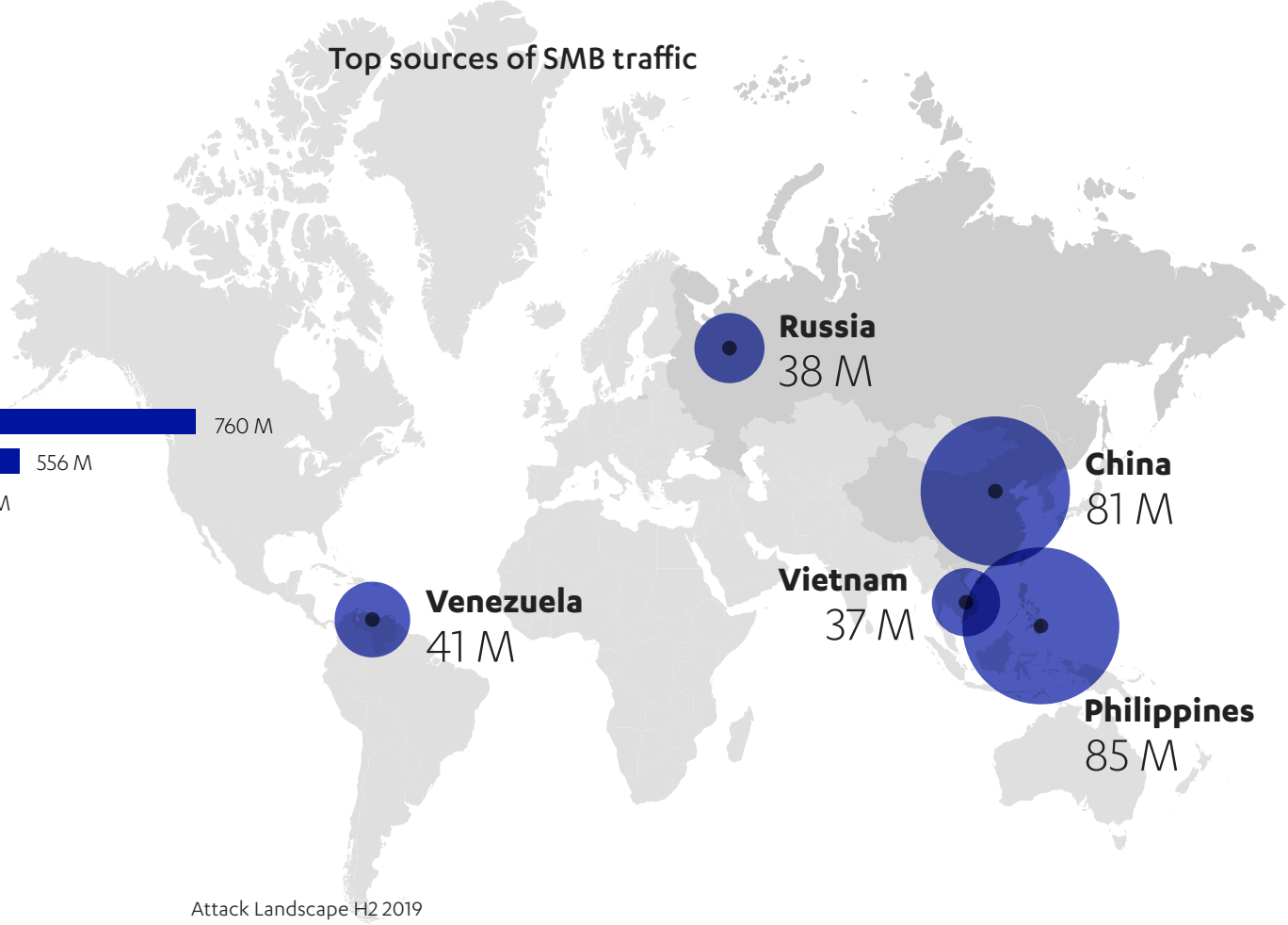


Top TCP Ports Targeted H1 2019



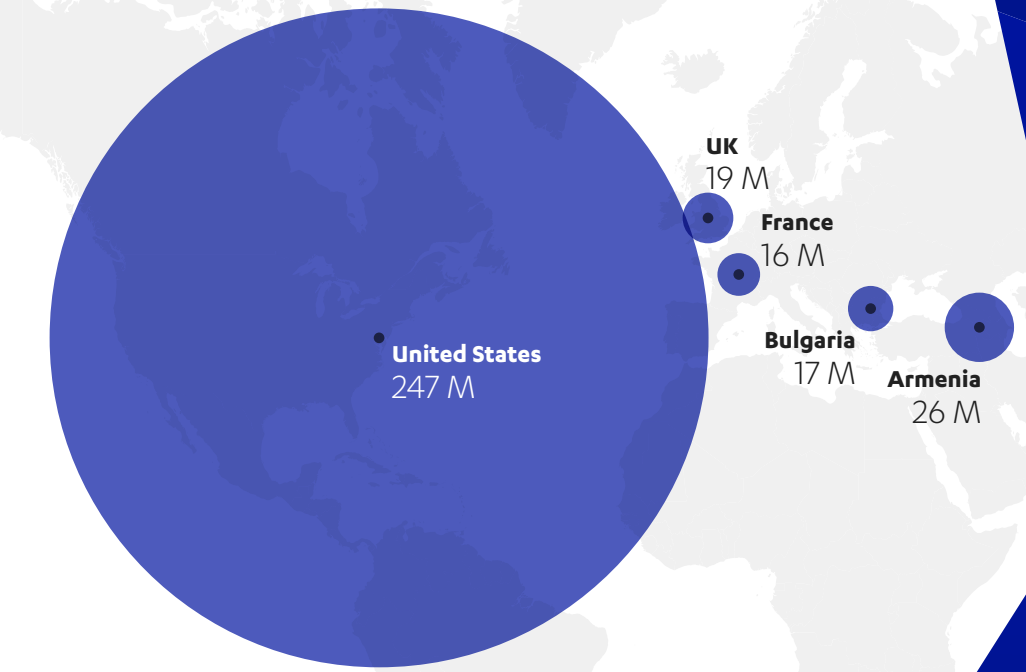
SMB port 445 took the position as most-targeted port over the period, indicating that, as in the first half of the year, attackers are still keen to use SMB worms and exploits such as Eternal Blue. For example, Trickbot, one of the top spam payloads we observed hitting endpoint devices, leverages Eternal Blue as a means of spreading. There were 526 million hits on SMB this period, slightly less than the previous period's 556 million.

Top sources of SMB traffic



Telnet was a close second with 523 million hits. While that's a reduction from a high of 760 million in H1 of 2019, it's a continued indicator that attacks on an ever-growing pool of IoT devices are still going strong. The ease with which attackers can acquire tools such as Mirai, which enable high-volume, low-sophistication attacks, continues to result in the compromise of large numbers of these poorly secured devices.

Top sources of Telnet hits



Malware found in honeypots

Other:Malware-gen [Trj]

Trojan.Linux.Mirai.K!c

Linux.Mirai

Backdoor.Linux.asqp

HEUR:Backdoor.Linux.Mirai.b

Linux/GenericAA-GR

DFI - Suspicious ELF

ELF/Trojan.GDNL-5

ELF/Mirai.AT!tr

Mal/Generic-S

Backdoor.Linux.Mirai.wan

HEUR:Backdoor.Linux.Mirai.ba

a variant of Linux/Mirai AT

Win32/Backdoor.805

Linux.Mirai.793

Trojan.Linux.Mirai.4!c

Trojan.Linux.Mirai

Linux.Trojan.Agent.JBO5LM

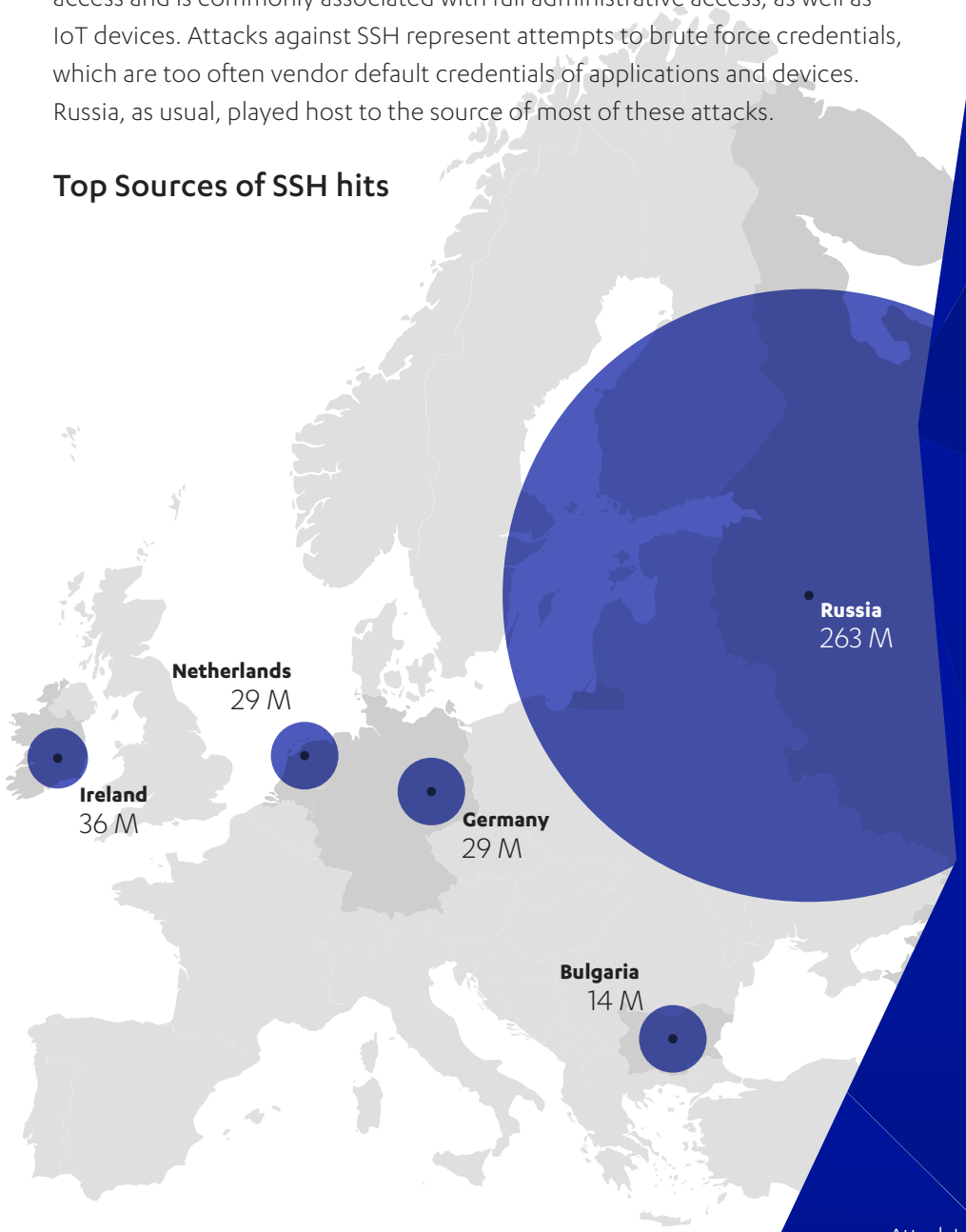
Linux.backdoor.Mirai.Aljc

LINUX/Mirai.vzbxp

Most of the malicious traffic we see today is generated by Linux-based malware like Mirai.

SSH on port 22 followed with 490 million hits. SSH enables secure remote access and is commonly associated with full administrative access, as well as IoT devices. Attacks against SSH represent attempts to brute force credentials, which are too often vendor default credentials of applications and devices. Russia, as usual, played host to the source of most of these attacks.

Top Sources of SSH hits



SQL-related attacks, which represent database attacks common in data breaches as well as attempts to spread cryptocurrency miners, remote access backdoors and ransomware, followed, with China the overwhelming source of attacks on MSSQL.

Top 10 Passwords used in honeypots

admin
vizxv
default
1001chin
sh
taZz@23495859
12345
password
ttnet
root

A great way to see what attackers are interested in is to check out the list of passwords they use. The everpresent "admin" is predictably in first place. The number two password of the period, "vizxv," is a default for Dahua DVRs, and two other passwords on the list, "1001chin" and "taZz@23495859" represent the factory defaults for other embedded devices such as routers.

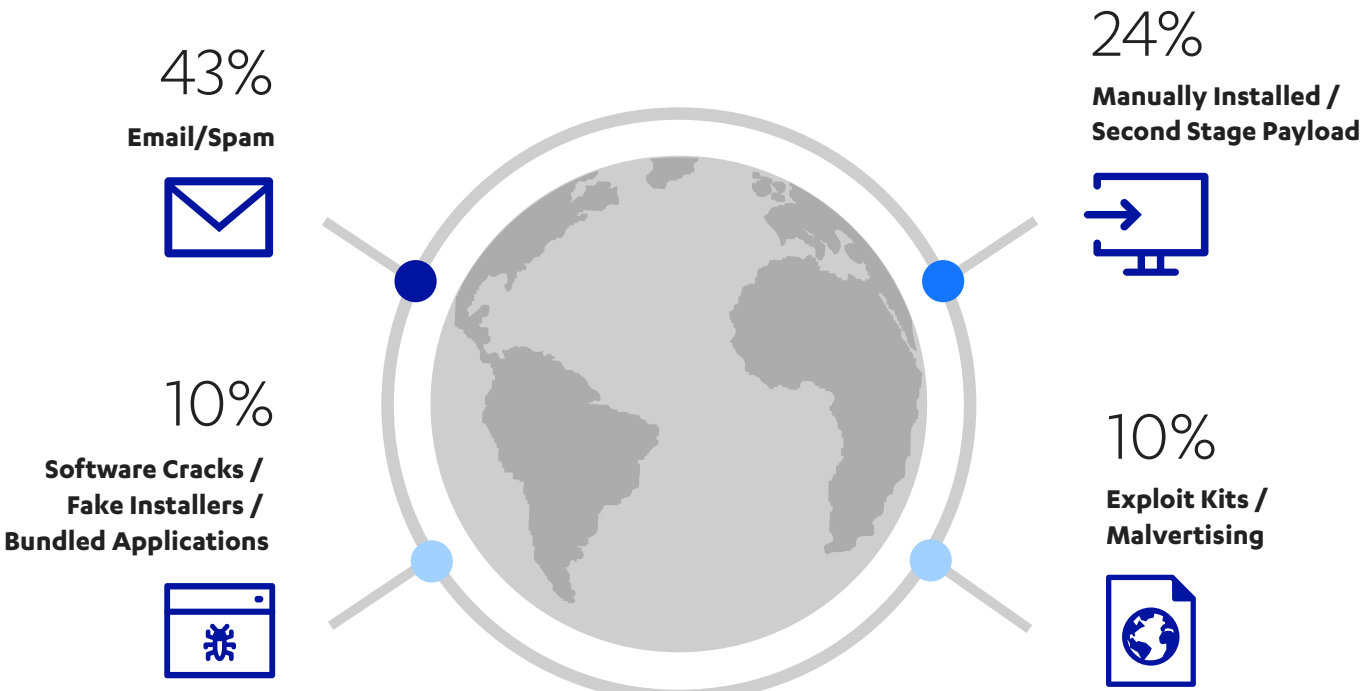
Brute forcing factory default usernames and passwords of IoT devices continues to be an effective method for recruiting these devices into botnets that can be used in DDoS attacks.

THE YEAR IN MALWARE

When it comes to malware, we turn to our customer endpoints to see what's happening in the wild.

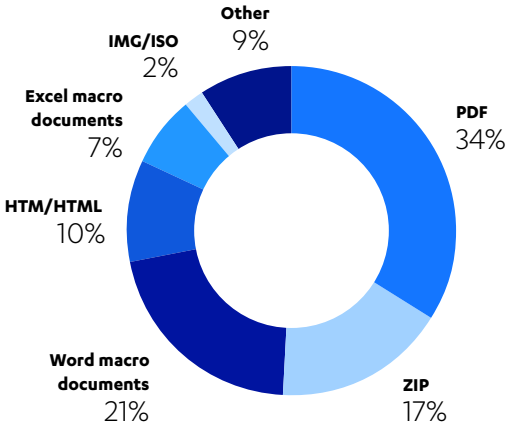
In 2019, we identified four main infection vectors for the malware samples we have observed, most of which are ransomware variants. The most popular delivery method by far was via email and spam, which accounted for 43%. Nearly a quarter were second stage/followup payloads or were delivered manually through brute force or RDP attacks. We also saw delivery through exploit kits and malvertising as well as software cracks, fake installers, and bundled applications.

Malware distribution methods



With spam being the delivery method preferred by attackers, we saw three main types of malicious attachments, the most common being PDF attachments. ZIP files were also quite common. Malicious Word and Excel macro documents were also steady throughout the year, mainly serving as downloaders for malicious binaries such as Emotet, one of the most prevalent threats of the year.

Spam attachment file types

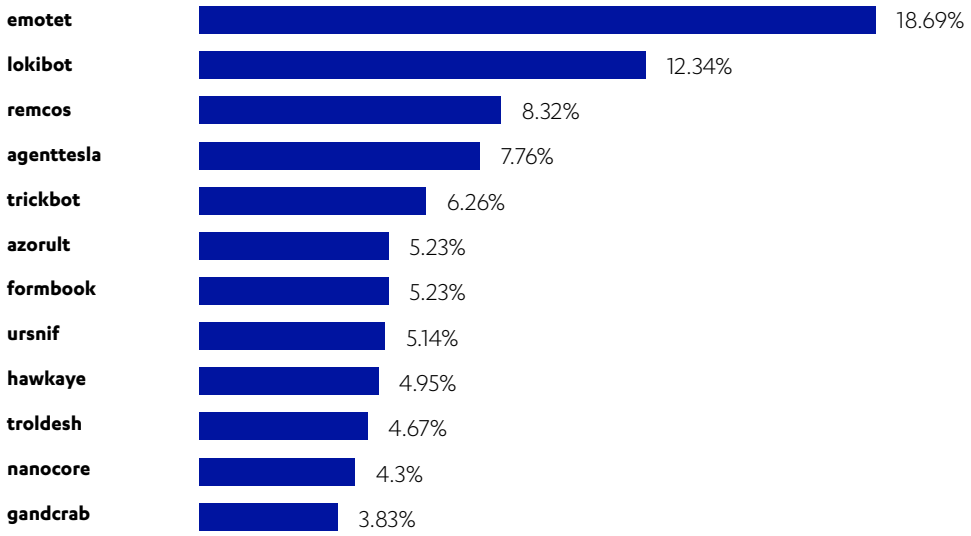


We also noticed a new trend in ISO and IMG files containing malicious executables. While low in volume, the trend was consistent throughout the year, probably because of its effectiveness as a social engineering tactic. These files are easily opened in Windows 10 – the user simply needs to click on the image file, which opens up a new window and displays the content.

The payloads seen in spam consisted of mostly infostealers and downloaders. Modular malware, which launches attacks in stages and adapts its payloads depending on analysis of the target environment, was prominent. Emotet and Trickbot represent two of the most well-known modular threats.

Emotet, an advanced modular banking trojan, was the most commonly seen first stage payload. Notable for its persistent and aggressive nature, Emotet is known to deliver any of six different malware payloads, among them Dridex, Panda and Trickbot. Besides its banking trojan functionality, it also serves as a mail account stealer, credential stealer, spammer, and DDoS attack tool.

Spam payloads



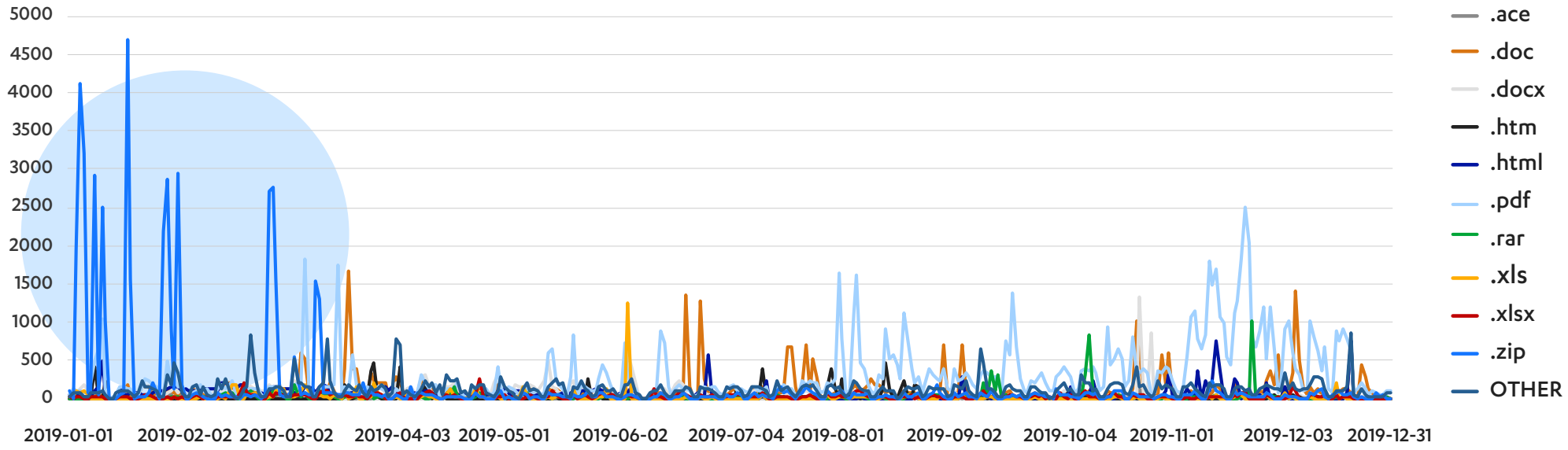
Emotet was observed in about 19% of first stage payloads.

Like Emotet, Trickbot is delivered through malicious macro documents and has infostealing capabilities. Often employed by Emotet as one of its second payloads, Trickbot was also dropped as a first stage payload in some spam campaigns and used to deliver followup payloads such as the Ryuk ransomware.

The successful ransomware strain known as GandCrab was seen about 4% of the time. Its prevalence would have been higher had it not been for the actors behind it retiring in May[2], after claiming to have earned over $150 million. Sure enough, GandCrab's retirement announcement coincided with a drop in ransomware in spam.

2 https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-shutting-down-after-claiming-to-earn-2-billion/

Ransomware levels in spam throughout the year



GandCrab's May retirement coincided with a drop in ransomware spam.

Despite a drop in ransomware spam, the year was a big one for ransomware, with attackers also relying on infection via second stage payloads and exploit kits combined with malvertising, among other methods. A list of new high-profile infections hit the headlines: Ryuk targeted organizations globally, hitting, among others, Louisiana schools in July[3] and the US Coast Guard at the year's end[4]. LockerGoga also focused on large organizations around the world, hitting Norsk Hydro[5] and Altran[6]. Sodinokibi, also known as REvil, famously hit local governments in 22 Texas towns[7], as well as Travelex[8] and the New York Airport[9].

3 https://gov.louisiana.gov/index.cfm/page/76

4 https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/MSIB/2019/MSIB_10_19.pdf?ver=2019-12-23-134957-667

5 https://blog.f-secure.com/norsk-hydro-lockergoga-encrypts-everything-f-secure-researchers-say/

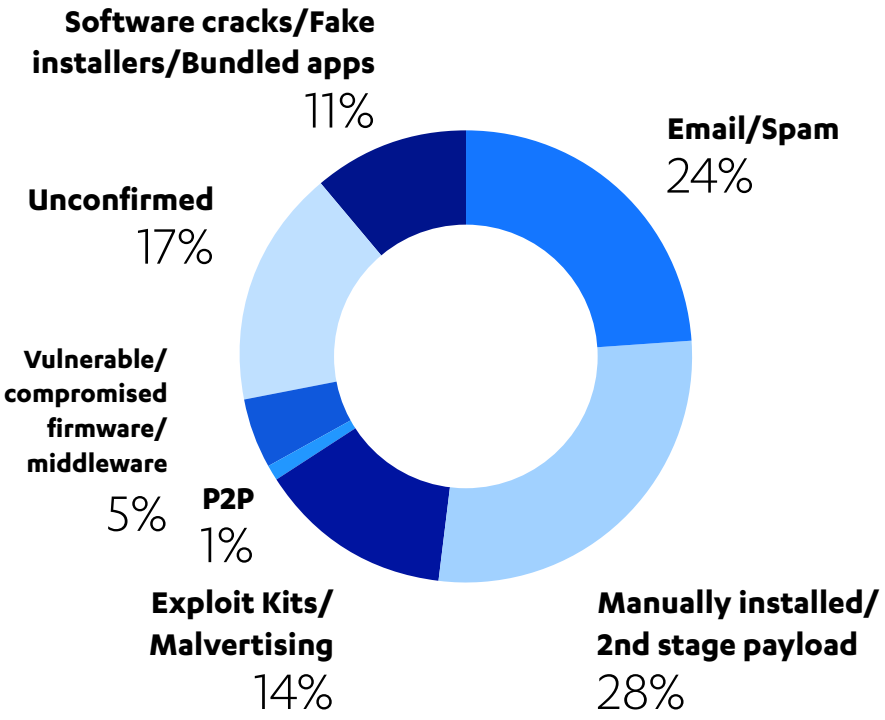
6 https://www.bleepingcomputer.com/news/security/new-lockergoga-ransomware-allegedly-used-in-altran-attack/

7 https://www.zdnet.com/article/at-least-20-texas-local-governments-hit-in-coordinated-ransomware-attack/

8 https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-hits-travelex-demands-3-million/

9 https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-hits-new-york-airport-systems/

Ransomware distribution methods



While ransomware families have declined in numbers, the damage and impact inflicted by these fewer families can be devastating. Victims have been forced to pay out tens or even hundreds of thousands of dollars, with publicly disclosed sums as high as $400,000. Attacks have become more sophisticated and targeted towards enterprises who can afford to shell out large sums of money. Just one high profile victim can net enormous sums for a group of threat actors.

In a new trend from late 2019, ransomware such as Sodinokibi and Maze have begun threatening to publicly leak stolen data if payment is not remunerated. With the trend continuing into 2020, organizations should now be prepared to assume that a successful ransomware attack would also mean a data breach scenario, substantially raising the stakes for everyone.

THE CYBER DECADE IN REVIEW

Looking back at highlights that shaped the past ten years in cyber security.

2010

Stuxnet uncovered
This game-changing attack on industrial control systems was the first nation state cyber weapon. It showed us malware was not just for cyber criminals attacking PCs and servers anymore.

Blackhole exploit kit spotted
Available to rent for up to $700 a month, this crimeware package would dominate the world of cyber fraud for the next few years, becoming one of the most successful exploit kits ever seen.

Wikileaks begins dump of US intelligence
A trove of US diplomatic messages and military documents leaked by Chelsea Manning were dumped by Wikileaks, bringing hacking to the forefront.

Google hacked by actors linked to Chinese government
Operation Aurora compromised Google and various other US companies. In response, Google effectively exited the Chinese market and began making major investments in security technologies, the effects of which are still visible today.

2011

A year of hacktivism
Anonymous hacked into HBGary Federal, exposing not only sensitive details of the security services firm's client relationships, but also its technical insecurities.
LulzSec's attacks on high profile companies and government agencies like Sony, the CIA, Fox, PBS and AT&T showed that even large, powerful entities can be vulnerable to a few hackers with keyboards.

The rise of Android
As the popularity of the OS grew, it attracted the attention of cyber criminals. Android malware spiked, outpacing other platforms as malware hosts.

2012

Mac malware threat emerges
Flashback, a malicious update masquerading as Flash player update, infected 600,000+ Mac OS devices, showing that Mac was not immune to threats.

Dropbox hacked
68 million accounts were compromised, but the hack wasn't publicly disclosed until 2016.

Another nation state malware discovered
Flame, larger and more complex than Stuxnet, was an APT nation state malware targeting middle eastern countries.

Rise of police-themed ransomware
Informed victims the authorities had found illegal material on their computers and demanded a fee in prepaid cash vouchers.

2013

Snowden revelations rock the world
Exposed the mass digital surveillance activities being carried out by the US government and members of the Five Eyes, spurring public interest in data privacy.

Cryptolocker ransomware
This re-emergence of encrypting ransomware accepted Bitcoin payment, ending the need for prepaid cash vouchers.

More huge breaches of widely used services show us anyone's data can be compromised
The Yahoo breach affected 3 billion user accounts, the Adobe breach compromised 38 million, and 40 million credit card accounts were stolen in Target's supply chain hack.

2014

Shellshock and Heartbleed vulnerabilities hit
These flaws affected popular software Bash and OpenSSL, and forced us to question the security of HTTPS communications in transit.

More nation state malware discovered
Regin was used by the NSA and GCHQ as a data collection tool. OnionDuke, attributed to the Russian government, used a Tor exit node to wrap legit executable files with malware.

LizardSquad came and went
Conducted massive DDoS attacks on gaming companies, favorite targets Sony PlayStation and Xbox.

2015

Ashley Madison breached
The hack that devastated relationships and lives and brought home the fact that nothing online is ever truly private.

The irony of the Hacking Team hack
Exposed the company's sale of surveillance tools to authoritarian governments and democracies around the world, along with a series of zero day exploits that were quickly added to exploit kits.

C&C servers go sci-fi
To avoid takedown, Russian APT group Turla began using satellites for its command and control servers.

Malicious apps in Apple App Store
In China, trojanized versions of Apple Xcode injected malicious code into applications they compiled, showing iPhone could be vulnerable.

2016

International banking heists
Exploited the way international banking works via the SWIFT system by hitting the Bangladesh central bank and Vietnamese commercial banks.

Cloud Hopper: Corporate espionage supply chain attack by Chinese APT
Multiple corporations were breached via their cloud service providers. The hack showed that even big-spending cloud companies are not immune to nation state attacks.

Magecart attacks: The digitization of credit card skimming
Online shopping via compromised implementations of Magento resulted in customers' credit card information being harvested.

IoT-powered botnet takes down part of the internet
Mirai, the most effective IoT botnet malware to date, changed the scale of the size of DDoS attacks when it took down Domain Name System provider Dyn with ensuing casualties including Netflix, Spotify, and Twitter.

DNC emails hacked
The Democratic National Committee was hacked and its emails exposed by Wikileaks, arguably affecting the outcome of the US election.

2017

WannaCry and NotPetya spread around the world
Release of EternalBlue exploit resulted in fast-spreading worm outbreak the likes of which had not been seen since the previous decade.

More supply chain mayhem
Avast's build server was compromised and malicious code in free CCleaner software tool was downloaded by more than 2 million users.

Equifax breach
One of the most dangerous, detrimental breaches of the decade, this hack exposed not only usernames and passwords but full names, addresses, birthdates and social security numbers, affecting more than 150 million people.

Cryptocurrency mining emerges
As cryptocurrency values rose, Coinhive offered an alternative to ads: Allowed websites to monetize visitors' computing power to mine cryptocurrency.

2018

From cryptomining to cryptojacking
Cyber criminals began illegally compromising websites with coinmining code that used site vistors' computers to mine for cryptocurrency.

Spectre and Meltdown
Dangerous, widespread processor vulnerabilities that allowed access to sensitive information from memory and affected the vast majority of devices on the market.

Cambridge Analytical scandal blew wide open
Made people question Facebook and practices of information harvesting.

GDPR
Came into force for EU citizens, to bring control of data back to users.

2019

Crypto-ransomware everywhere
LockerGoga infected industrial firms including Norsk Hydro; 22 Texas towns fell victim to Sodinokibi/REvil; Ryuk targeted organizations & agencies globally including the US Coast Guard; and the year saw five and six-figure ransom payments.

Coinhive died
and with it a bunch of cryptominer families.

Supply chain attacks continued
ShadowHammer, sophisticated attack involving a backdoored version of ASUS Live Update Utility, downloaded to tens of thousands of machines.

CONCLUSION

This report marks the close of a decade. As we begin 2020, we reflect back on the past ten years – a decade marked by the emergence of a cyber arms race between nation states; devastating supply chain attacks; cyber events influencing political events; mass surveillance programs; rampant data breaches; and broken trust in established security measures.

But looking ahead, there's reason for optimism. After a decade filled with varying breaches of consumer privacy, 2018's GDPR is a step forward in that arena. As other governments follow suit with similar legislation such as the California Consumer Privacy Act, we just might be starting to get a handle on a complex and critical issue.

The IoT, which was still a futuristic idea for most in 2010, is now a reality in many aspects of life and business. Still unacceptably insecure, there is hope that this could change as governments like the UK begin to consider or enact legislation (like California's new IoT Security Law) that will mandate security for manufacturers of these devices.

Optimism, however, should never lead to overconfidence. Actors on the dark side will continue to evolve and adapt to measures the defenders put in place; and malware is a prime example of this. Exploit kits once reigned as a top vector for dropping payloads. Due to the phaseout of Flash and improvements in Java, exploit kits, while still remaining a potent threat in and of themselves, have declined in prevalence. This has merely forced attackers to gravitate to profiting by the distribution of ransomware via email spam. And while 2019 concluded with fewer ransomware families than at the start of the year, attacks have become more sophisticated and impactful, targeted against high profile victims that will net huge payouts for attackers.

The future promises to introduce cyber security issues colored by artificial intelligence, as AI technology spreads and as attackers find ways to exploit it. As the security community confronts these obstacles and as they spill over into other areas of our ever more technology-intertwined world, areas such as human rights and politics, the infosec community will be tasked with not only ensuring our technologies are sound, but will have a role in ensuring that society is free and secure as well.

ABOUT F-SECURE

Nobody has better visibility into real-life cyber attacks than F-Secure. We're closing the gap between detection and response, utilizing the unmatched threat intelligence of hundreds of our industry's best technical consultants, millions of devices running our award-winning software, and ceaseless innovations in artificial intelligence. Top banks, airlines, and enterprises trust our commitment to beating the world's most potent threats.

Together with our network of the top channel partners and over 200 service providers, we're on a mission to make sure everyone has the enterprise-grade cyber security we all need. Founded in 1988, F-Secure is listed on the NASDAQ OMX Helsinki Ltd.

f-secure.com | twitter.com/fsecure | linkedin.com/f-secure