ATTACK LANDSCAPE H1 2020

F-Secure

CONTENTS

INTRODUCTION

Virus. Quarantine. Outbreak. They are words we're used to in the context of digital security, but in 2020 we became all too familiar with them in the real world. The COVID-19 pandemic hit, leaving its effects on cyber security and across the globe. Businesses have had to adapt to their employees working from home and cyber security teams have had to grapple with the security implications of this shift.[1] Technologies facilitating remote work have seen exponential increases in usage, but have also had their security flaws highlighted.[2] Russian nation-state attackers began to focus attention on obtaining intellectual property from organizations engaged in vaccine research and development.[3]

With the shift to remote work, the borders of an organization's network – and therefore its attack surface – are now exponentially larger. Even more data is now physically held or accessible outside an organization's own borders. Teleworkers are more likely to be working from less secure devices and networks, and have less access to IT security teams.[4]

It's against this backdrop that we present our half-year report on the trends and patterns of our slice of the security landscape, including malware and phishing targeting people and organizations, and traffic logged by our worldwide network of honeypots.

Attackers were quick to adjust to the "stay-at-home" pandemic world. The industry has seen more phishing for online credentials, a constant deluge of COVID-themed emails, and elevated levels of attacker traffic to remote desktop ports.

1 https://blog.f-secure.com/control-on-the-edge-how-can-it-security-managers-cope-with-the-sudden-explosion-of-home-working/
2 https://blog.f-secure.com/podcast-mikko-hypponen-covid-19/
3 https://blog.f-secure.com/covid-19-vaccines/
4 https://blog-assets.f-secure.com/wp-content/uploads/2020/04/03111817/2020-04-01-Cyber_security_guidance_for_COVID-19.pdf

MALWARE TRENDS

The COVID-19 crisis has given attackers new hooks and angles to leverage in their attacks. What hasn't changed in 2020 is that malware authors are constantly looking out for new techniques in their efforts to bypass security checks and evade detection.

Distribution methods

The most common method attackers use to spread malware continues to be spam email, which has only increased as an infection vector: email accounts for 51% of attempted infections so far in 2020, compared to 43% last year. The coronavirus has played a role in this increase, as attackers have capitalized on new opportunities for email story lines opened up by worldwide interest in the virus. Attackers have also been happy to take advantage of email's potential to socially engineer newly home-based workers who may be using less-secure remote devices or who are distracted by the sudden introduction of new workflows.

Also a likely factor in the increase in email distribution has been the shift of some malware, especially ransomware, toward targeting organizations instead of consumers. Given common organizational restrictions, such as managed software installation and blocked access to certain websites, the success rate of software cracks and bundled applications has likely diminished. Software cracks, or files that bypass license checks or other usual requirements, and bundled software, our term for potentially unwanted applications that are packaged with legitimate software, have dropped in usage overall, from 10% of attempted infections last year to just 5% so far in 2020.

Exploit kits dipped only slightly in usage, from 10% in 2019 to 9% this year. Exploits often take more effort to implement and may result in a lower infection rate than email. However, as not all organizations are well-equipped to implement a quick turnaround period for applying vulnerability patches, exploits will remain part of the attacker toolset.

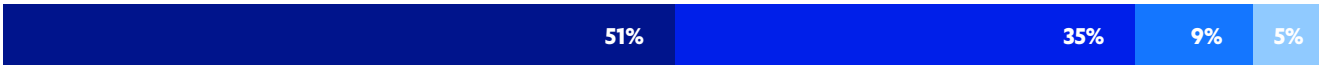
35% of malware, up from 24% last year, arrived via a manually installed or second stage payload, indicating that the malware was installed either by the user or by the attacker. This rise could be due in part to cyber criminals registering thousands of fake "Zoom" domains to trick users into downloading malware disguised as the video conferencing software.[5] Another attacker tactic is to manually install ransomware as a second stage payload after having gained an initial foothold into the company through an unsecured RDP port. According to reports, vulnerable RDP ports have only grown more plentiful during the transition to remote work.[6]

5 https://thehackernews.com/2020/03/zoom-video-coronavirus.html
6 https://www.zdnet.com/article/jump-in-vulnerable-rdp-ports-is-leaving-networks-open-to-hacking-and-cyberattacks/

Malware distribution methods

Email
Manually installed/ Second-stage payload
Exploit kit / Software exploit / Malvertising / Drive-by download
Software cracks / Bundled software

H1 2020



Email threats

We have seen a deluge of COVID-19-themed emails containing a mixture of spam, phishing attempts, and malicious attachments as cyber criminals capitalized on the fear and uncertainty generated by the crisis.

As the coronavirus spread around the world, we noticed localized COVID-19 email campaigns following not far behind, using news and advisories as hooks in regions that were already battling the real-world virus.[7] One of the first of these was an Emotet campaign targeting Japan in January after the country had confirmed its first coronavirus infection: an email purporting to be from a Japanese public health authority included an attachment that supposedly contained information on preventing the spread of the virus. We saw similar localized campaigns subsequently spreading along with the virus: Lokibot in Vietnam, Remcos in Hong Kong, and more campaigns further west to countries like Italy.


JAPANTODAY

NATIONAL CRIME ENTERTAINMENT POLITICS BUSINESS TECH SPORTS

National

Japan confirms 1st domestic case of coronavirus infection

Jan. 29 | 08:35 am JST | 0 Comment

京都府山城南保健所福祉室 2020 Jan 30 - Message (Plain Text)

Sent: Thu 1/30/2020 3:18 AM

Subject: 京都府山城南保健所福祉室 2020 Jan 30

inf Jan 30 2020.doc (74 KB)

管内　通所・施設系障害福祉サービス事業者　様

お世話になっております。

新型コロナウィルス関連肺炎については、中国武感市を中心に患者が報告され、
国内でも茨城県で患者が報告されているところであり、

つきましては、別添通知をご確認いただき、
感染予防対策についてよろしくお願いいたします。

＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊
京都府山城南保健所福祉室（担当：海野）
〒619-0214京都府木津川市木津上戸18-1
電　話：
ＦＡＸ：
＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊

After news of Japan's first COVID infection, this Emotet spam email capitalized on the crisis.

For a look at the types of COVID-19 spam we've seen, it's interesting to divide the email subject lines into two buckets: those with and without attachments. Emails without attachments are mostly pure spam without a malicious code element. Attempts to sell novel or dubious products fall into this category, as do outright scams such as emails peddling face masks that will never actually be delivered to the buyer.

7 https://blog.f-secure.com/coronavirus-email-attacks-evolving-as-outbreak-spreads/

Emails with attachments typically present the files as documents containing important information about COVID-19, relief funds, or other supposedly urgent related topics, when they are in reality documents with malicious code to download and run malware. In a reflection of the crisis Italy faced in H1, the most common malicious coronavirus-themed email we saw was authored in Italian.

Top COVID-themed email subjects without attachments

1. Urgent Security Update
2. Infrared Thermometer Non-Contact Temperature
3. Body temperature measurement: aiming towards the forehead
4. Medical Masks starting from â‚¬ 0.4 - â‚¬ 0.5
5. No-Contact Multi-Fnctional Digital Thermometer
6. Tracks your body temperature
7. CoronaVirus is scary! Breathe Easier With SafeMask
8. Revolutionary Thermometer Used By Medical Staff Worldwide Now Available to Public
9. CORONAVIRUS ALERT: FREE Breathing Masks For USA
10. Test Your Knowledge to Get 2 Free Health Courses

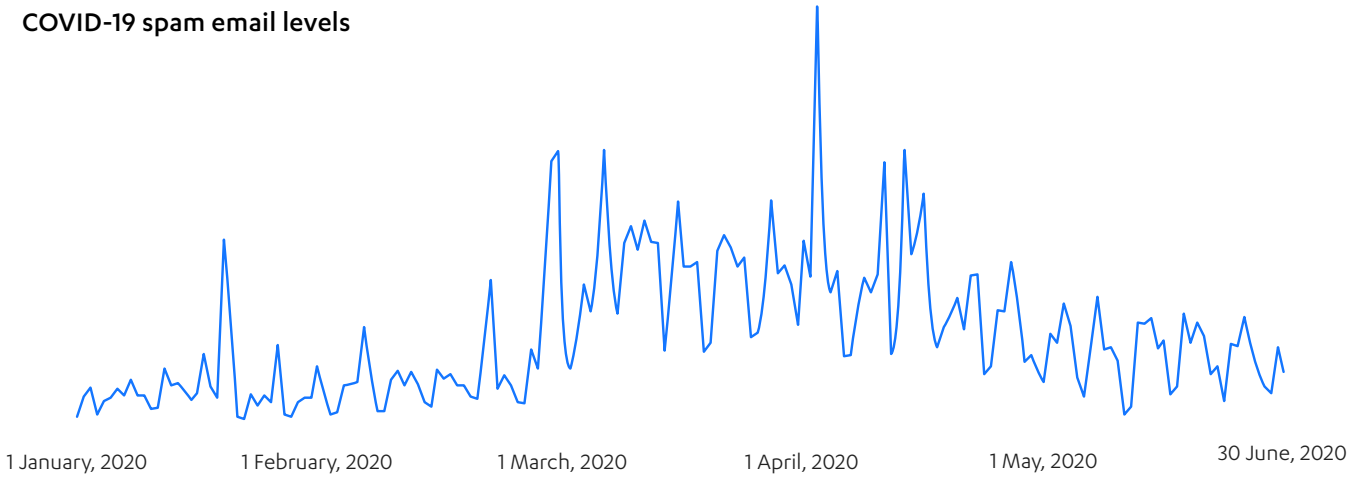
Top COVID-themed email subjects with attachments

1. Coronavirus: Informazioni importanti su precauzioni
2. Standard Bank: COVID-19 Payment Relief Funds Approved
3. Absa Online Cashflow Relief Funds Urgency
4. COVID-19 UPDATE - NSL Analytical Services
5. Coronavirus: an important information about precautionary measures for the enterprises
6. Absa Online Relief Urgency
7. Government Response to Coronavirus COVID-19
8. Coronavirus (COVID-19)
9. Receive Score eStatements Absa.pdf
10. COVID-19 USA

75% of the coronavirus-themed email attachments we saw distributed either Lokibot or Formbook, infostealers that were found delivered in 38% and 37% of COVID attachments respectively. Spam campaigns with attachments in general contained mostly .doc, .zip, and .pdf. However, in a trend continuing from 2019, we noticed a small but consistent percentage of malware unconventionally disguised as ISO or IMG files that in turn run an executable file. One example is Agent Tesla, a RAT that spread via an ISO file attached to a quotation request email.

We also saw atypical archive and compression file types, such as .gz and .ace, being used to get around mail gateways configured to detect malware executables enclosed in more conventional formats like .zip.

COVID-19 spam email levels



March, April and early May saw the highest levels of COVID-19 spam, after which the trend continues, but at a reduced rate. As the world becomes more aware of pandemic-related fraud tactics, attackers have begun re-incorporating their usual subjects of shipping documents or invoices. We also saw a short stint of emails in June that leveraged the Black Lives Matter movement to deliver Trickbot.

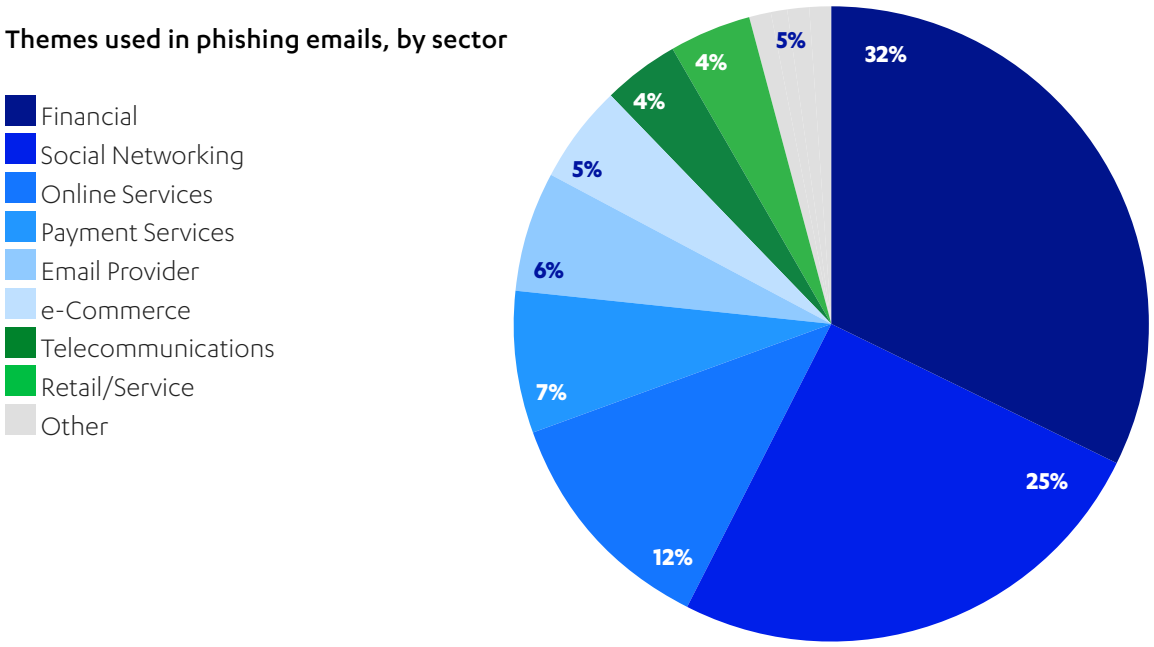
Phishing

Phishing emails attempt to convince the user to give up personal information or click a malicious link or attachment by appearing to be sent by a well-known brand. Of phishing emails coming across our telemetry over the period, the largest share, 19%, imitated Facebook. Financial companies proved to be popular for spoofing, with several banks together making up 32% of attempts.

Themes used in phishing emails, by brand

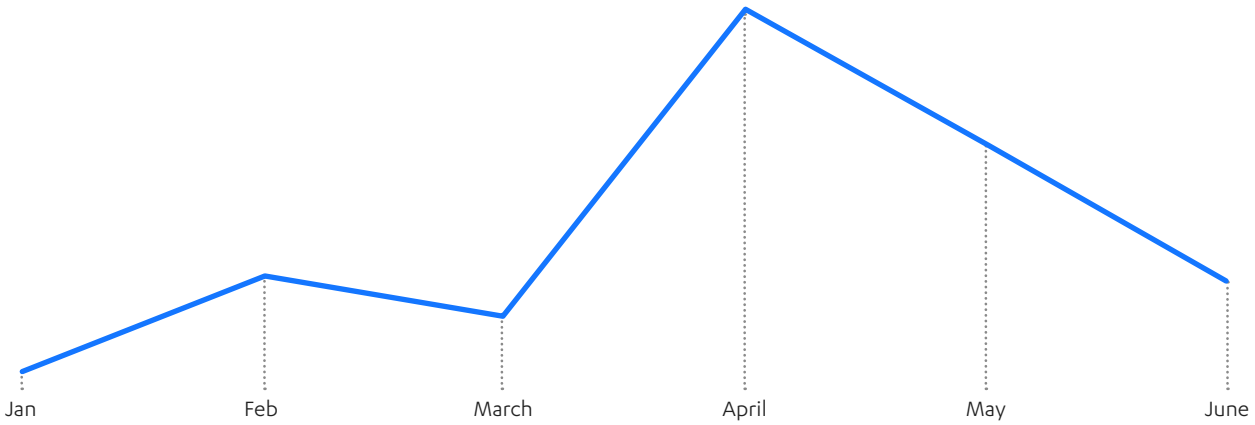
Facebook, Inc.	19%
Chase Personal Banking	11%
Microsoft Office365	6%
PayPal Inc.	6%
Bank of America	5%
WhatsApp	4%
Webmail Providers	3%
Wells Fargo & Company	3%
Amazon.com Inc.	2%
Apple Inc.	2%
eBay Inc.	2%
Itau Unibanco S.A	2%
Netflix Inc.	2%
Adobe Inc.	1%
Alibaba	1%
Americanas.com S/A Comercio Electronico	1%
Bancolombia	1%
Canadian Imperial Bank of Commerce	1%
DHL Airways, Inc.	1%
Google Inc.	1%
LinkedIn Corporation	1%
Orange	1%
Outlook	1%
Steam	1%
Other	23%

Themes used in phishing emails, by sector



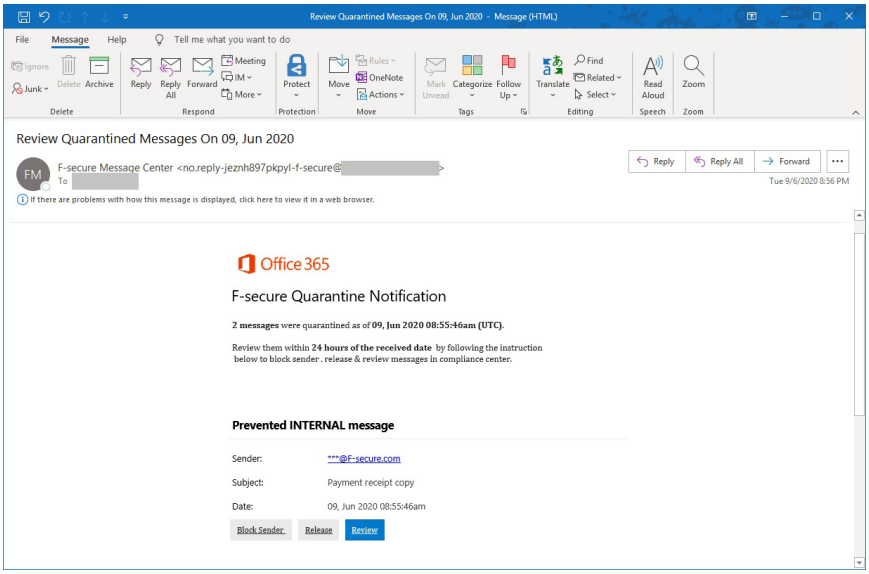
Overall, the industry has seen an increase over the past year in attacks leveraging cloud-based email providers such as Microsoft Office 365[8] as cyber criminals adjust their methods toward phishing and credential theft to capitalize on companies' continued migration to cloud services. This trend will only continue as cloud migration intensifies to better accommodate legions of remote workers.

Phishing emails leveraging Office 365

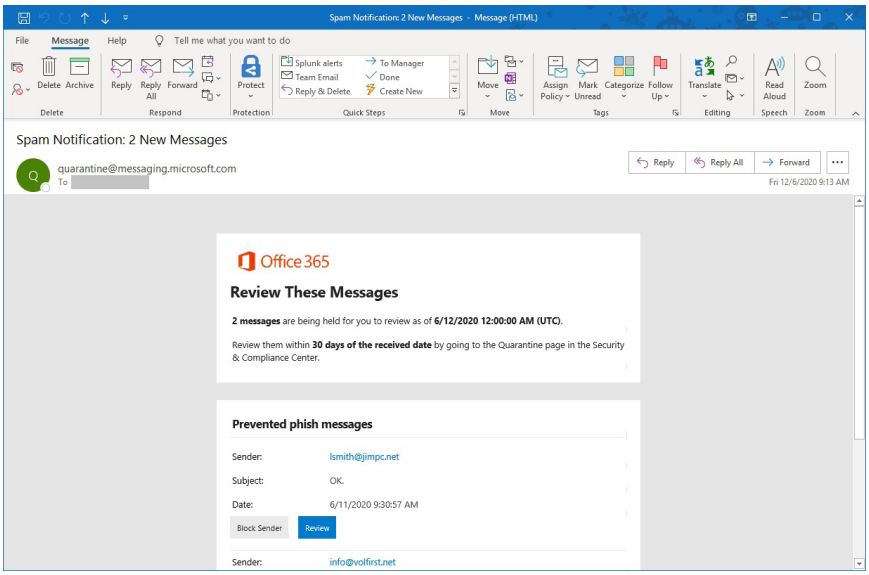


Phishing campaigns against cloud services like Office 365 are effective because end users are already accustomed to receiving notifications from the service itself, especially if the service is part of the organization's software infrastructure. Typical notifications attackers send include failure of delivery emails, alerts for hitting storage limits, quarantine notifications, requests for reactivation, or "update your password" emails.

8 2020 Verizon Data Breach Investigations Report https://enterprise.verizon.com/en-gb/resources/reports/dbir/



Fake quarantine review email



Real Office 365 quarantine review email

Traditionally, phishing attacks have been crafted to trick end users. If successful, the attacker's access in these cases is limited to the victim's email and to the services the victim is permitted to access. As attackers seek to gain wider access however, we are also seeing an increase in cyber criminals launching targeted spear phishing attacks against Microsoft Office 365 administrators.[9] These attacks, if successful, would allow the attacker to gain full administrative control over an organization's Office 365 domain and accounts.

Similar phishing attacks have been observed against other cloud-based email services such as Google's Gmail and G-Suite. Given the prevalence of Google accounts and how they are leveraged across the internet to log into various websites, it's no surprise that attackers have created phishing schemes in this arena as well.

9 Understanding the Email Threat Landscape https://www.f-secure.com/en/business/campaigns/your-complete-guide-to-email-security

Threat families

Our top threats of the period are based on data sourced from both our detection upstream as well as external threat feeds. Infostealers and remote access trojans (RATs) were the most prevalent in our top 20, having gained traction by spreading mostly through coronavirus-themed emails. Lokibot and Formbook were the two most prevalent infostealers, while Remcos and Ave Maria made up the majority of RATs.

Emotet continues to play a prominent role in the malware scene.[10] Having started off as a banking Trojan, it has since evolved into a much more modular threat that includes botnet capabilities. Nowadays we are seeing Emotet deployed as first-stage malware distributed mostly through email attachments in widespread spam campaigns. It's been known to usher in banking Trojans such as Trickbot and Qakbot, and ransomware such as Ryuk.

Top 20 malware threats

NAME		TYPE
1.	Lokibot	Infostealer
2.	Emotet	Botnet
3.	Generic behavior*	Trojan
4.	Formbook	Infostealer
5.	Remcos	RAT
6.	Ave Maria	RAT
7.	Ransomware	Ransomware
8.	Agent Tesla	RAT
9.	Trickbot	Trojan-Banker
10.	Qakbot	Trojan-Banker
11.	NanoCore	RAT
12.	Netwire	RAT
13.	Raccoon	Infostealer
14.	Ursnif	Trojan-Banker
15.	AZORult	Infostealer
16.	GULoader	Trojan-Downloader
17.	IcedID	Trojan
18.	Malicious Packer	Trojan
19.	njRAT	RAT
20.	DarkComet	RAT

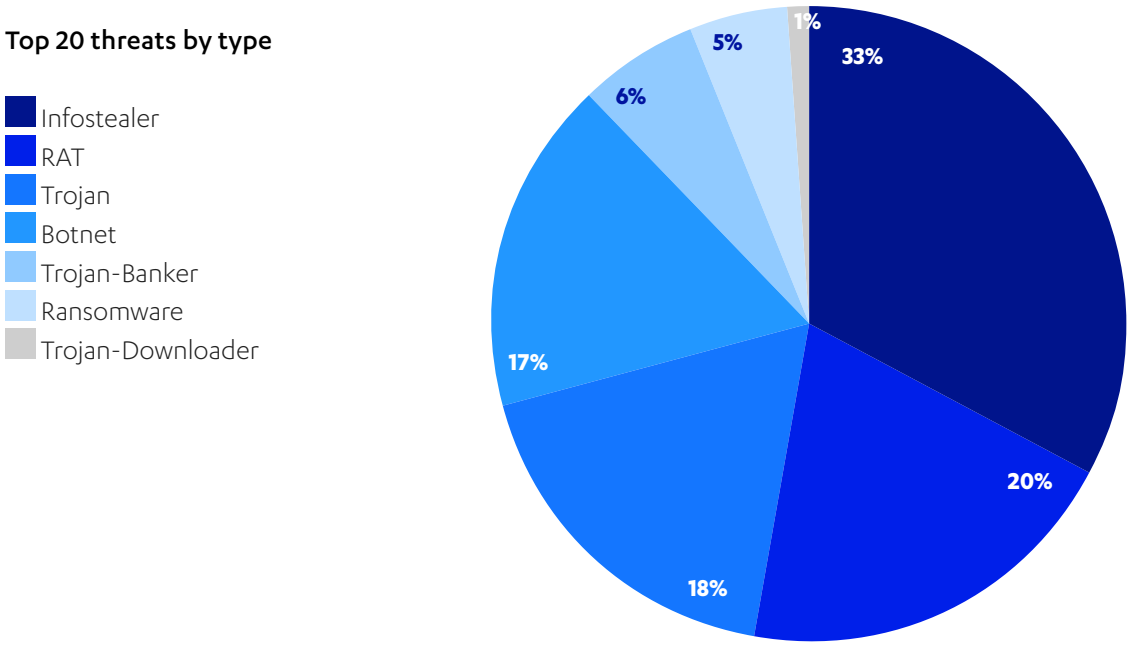
*"Generic behavior" denotes malware that does not map directly over an existing known threat family, but displays typical malicious behavior such as dropping additional files, modifying registry keys, or connecting to the internet to download more files.

MALWARE TERMS

Botnet: A collection of devices that are infected with a bot program, which allows an attacker to control each individual device, or collectively direct all the infected devices.
Exploit: A program that takes advantage of a vulnerability in an application or operating system to enable an unauthorized action such as delivering a malware payload.
Infostealer: A program that is designed to steal sensitive and confidential information, such as passwords and credentials, from an infected system.
Ransomware: Malware that takes control of the user's data or device, then demands a ransom payment to restore it.
RAT: Remote Access Trojan. A program used that allows an attacker to control a victim's system remotely and execute commands.
Trojan: A file or program that appears to be desirable or harmless, but secretly performs actions that are harmful to your device, data or privacy.
Trojan-Banker: a Trojan that uses a variety of techniques, such as stealing credentials, to monitor or intercept online banking sessions.
Trojan-Downloader: A Trojan that contacts a remote server and downloads other harmful programs from it.

10 https://blog.f-secure.com/emotet-returned-from-vacation-and-is-active-again-how-to-reduce-risk-in-your-environment/

Top 20 threats by type



Ransomware only made up 5% of our top 20 threat families, a deceptively small number that is due to the way it is now typically being spread. Rather than being deployed as a first-stage payload, attackers are usually spreading ransomware as a second-stage payload after a first-stage malware such as Emotet has cleared the way. Because our endpoint protection technologies detect and block the first stage payload, the ransomware that would have followed is never dropped or executed, precluding these would-be ransomware incidents from being reflected in our telemetry.

Certain families have also been observed using software vulnerabilities to gain an initial network foothold. For example, Black Kingdom uses an exploit to target organizations who have neglected to patch the recent Pulse Secure VPN vulnerability.[11] Nefilim[12] and Sodinokibi/REvil[13] ransomware have been seen exploiting Citrix server vulnerabilities to gain access. In addition, some ransomware families are using unsecured RDP to gain access to organizations.

The new modus operandi of major ransomware players in 2020 has been to first infiltrate a network, obtain and exfiltrate as much data as possible and finally, deploy ransomware to encrypt the data. The threat of data exfiltration and subsequent public exposure serves as an additional incentive in case the organization balks at paying the ransom demand. This is perhaps a side effect of GDPR: companies who refuse to capitulate to ransom demands will still find themselves taking a financial hit, but in the form of customer lawsuits or GDPR fines resulting from data leaks.

Aside from our top 20 threats, the rest of our telemetry was populated with either generic Trojans or threats that are insignificant in number.

11 https://www.bleepingcomputer.com/news/security/black-kingdom-ransomware-hacks-networks-with-pulse-vpn-flaws/
12 https://www.bleepingcomputer.com/news/security/toll-group-hit-by-ransomware-a-second-time-deliveries-affected/
13 https://twitter.com/UnderTheBreach/status/1220687658701246464

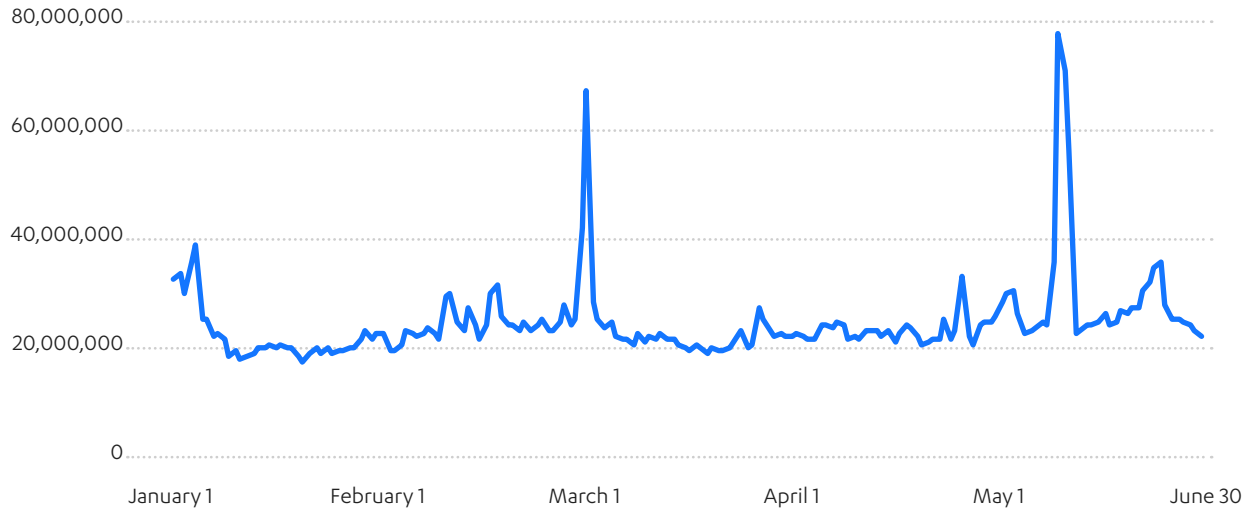
HONEYPOTS: WHO'S AFTER WHO?

In contrast to the malware and phishing we see attempting to attack client machines, our global honeynet observes network-based traffic encompassing a wide range of activity including attackers scanning the open internet for vulnerable workstations, as well as attempts to penetrate and compromise such systems.

Our honeypots saw nearly the same levels of traffic compared to last year – in total, there were over 2.8 billion hits to the network in the first half of this year, compared with 2.9 billion in H1 of last year and 2.8 billion in H2 2019. It's evidence that pandemic or no pandemic, attackers will continue their activities.

Throughout the period, activity remained mostly constant. The exceptions were significant peaks in mid-March and early June, DDoS reflection campaigns targeted at UDP port 1900, the default port for network device discovery protocols UPnP and SSDP. A major portion of these attacks hit China, and the majority were sourced in Chinese, Brazilian, US, and Singaporean IP spaces.

Honeypot traffic throughout H1



Looking at the countries whose IP spaces emanated the highest levels of traffic to our honeypots, China, US and Russia figure prominently, followed by the Netherlands, Hong Kong, Brazil, Germany, Ukraine, and Singapore, all of which are usual traffic sources. Ireland registers unusually high this time at number three. Traffic from Ireland's IP space was mostly aimed at SSH, was consistent throughout the period, and was spread out hitting a variety of countries.

WHAT'S A HONEYPOT?

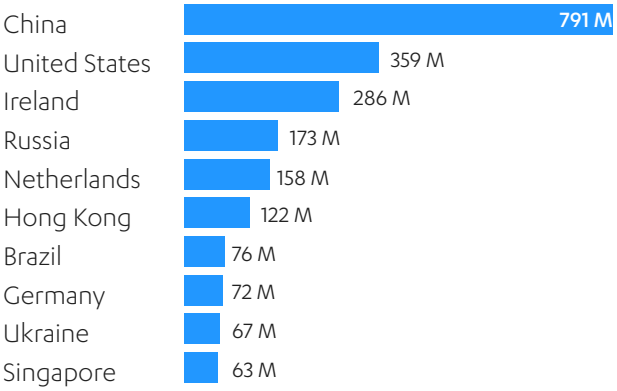
Our honeypots are decoy servers set up in countries around the world to gauge trends and patterns in the global cyber attack landscape. Because their specific purpose is to gauge potentially malicious activity, any incoming connection registered by a honeypot is deemed suspicious and likely a result of an attacker's scans of the internet. Even so, the rare mistyped IP address can also register a connection.

Over 99% of traffic to our honeypots is automated traffic coming from bots, primarily because they can perform menial tasks repeatedly. Interactions may come from any sort of infected connected device such as a traditional computer, smartwatch or even an IoT toothbrush.

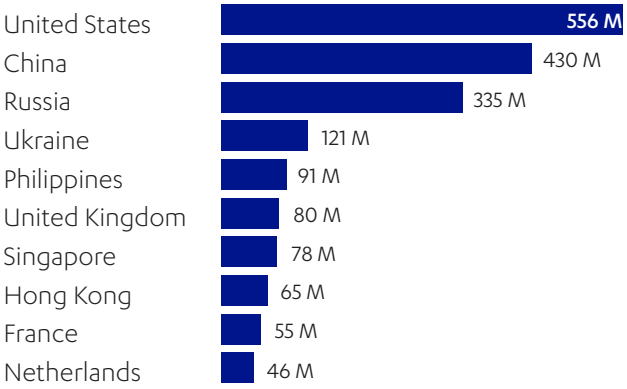
A hit on our honeypots constitutes any sort of interaction, from a simple exploratory ping to full-on service access.

Countries may appear on the top source list for a variety of reasons. They often tend to be those with an extensive internet presence. Attackers also gravitate toward using hosts in countries other than where the attacker is located, with less stringent or less effective cyber crime laws – reducing the attacker's chance of being found and prosecuted. Also attractive are servers in regions attackers generally perceive to have a higher prevalence of vulnerable software and hardware they can infect and leverage to propagate their attacks.

Top source countries H1 2020



Top source countries H2 2019



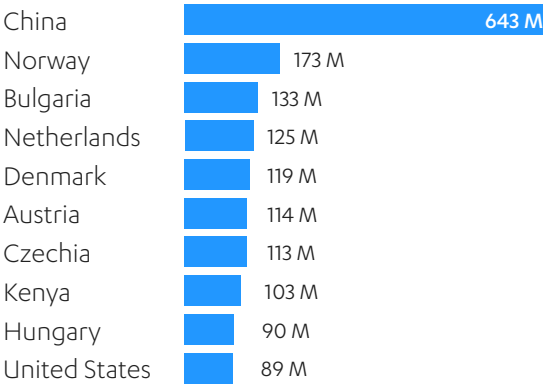
A significant share of traffic coming from the top source countries, including from within China itself, was aimed at Chinese IP space, making China also the top attack destination. Norway appeared as the number two destination.

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.

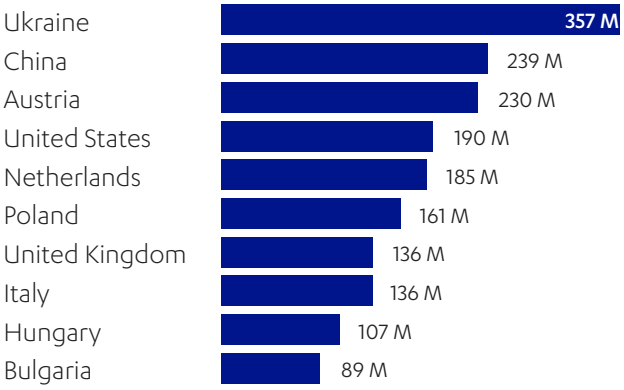
In addition, we do not mean to imply that this activity is predominantly nation-state behavior. The majority of these attacks are instigated by cyber criminals who are carrying out DDoS attacks and sending malware for financial gain.

Although it's difficult to know exactly why Norway's IP space was so popular, it may be worth noting that the country has experienced several high profile hacks lately – Norsk Hydro in 2019 and shipbuilder VARD, automotive parts dealer MECA/Mekonomen and investment fund Norfund in 2020. Increased traffic could be coincidental or as a result of increased media exposure.

Top destination countries H1 2020



Top destination countries H2 2019

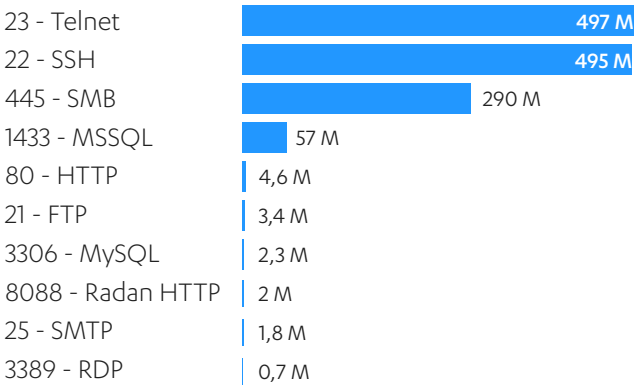


Ports and protocols

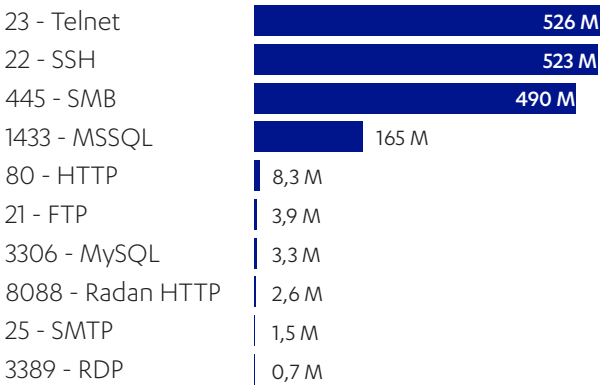
The top targeted ports of the period, with a few exceptions, stayed relatively constant compared to the previous period. Ports 23 and 22, the leading two, represent attacker attempts to obtain remote access to the victim server via unencrypted Telnet and the more secure SSH, respectively. The most common version of Telnet and SSH attacks were based on attempts to authenticate as local users, mostly by using commonly known username and password combinations.

Telnet is still employed far too widely, mainly on servers and IoT device connections. Its numbers this period are slightly down from 2019 counts. A great deal of Telnet traffic was instigated by the Mirai malware, variants of which made up the vast majority of malware found in our honeypots.

Top TCP ports targeted H1 2020



Top TCP ports targeted H2 2019



Third on the list is port 445, representing SMB connections, which are also at lower levels than seen in 2019. SMB traffic likely represents attempts to upload malicious data to be used in exploitation or to exfiltrate data from the server. Some of this traffic is still exploiting the EternalBlue vulnerability. In addition, a few more SMB-related vulnerabilities have been disclosed this year, SMBGhost[14] and SMBleed,[15] so we can expect that SMB vulnerabilities are still actively being researched as a target.

Traffic to port 1433, MSSQL, was the fourth largest attack target, representing database attacks such as SQL injection as well as attempts to spread cryptocurrency miners, remote access backdoors and ransomware. MSSQL traffic was also diminished from 2019 levels.

Attacks against HTTP include activities such as the scraping of potentially sensitive files or site pages that should have been restricted or removed; uploading malicious files to gain a server foothold; enumeration of hidden network shares; flooding server resources; command injection, and reflection attacks.

File transfer-based attacks (FTP) mainly download various malicious files, some of which turn out to be cryptocurrency miners. These also are commonly combined with remote access commands as part of automated scripts.

In the case of mail-related attacks (SMTP), we most often see attempts to distribute malicious payloads and user enumeration as well as the relaying of various spam or phishing attempts.

14 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0796
15 https://blog.zecops.com/vulnerabilities/smbleedingghost-writeup-chaining-smbleed-cve-2020-1206-with-smbghost/

As remote work spread around the world and as companies raced to adapt, outside reports detailed increases in RDP brute force attacks.[16] Attacks against vulnerable Remote Desktop Protocol (RDP) connections are frequently characterized by brute-force login attempts, utilizing credentials often obtained from dark web RDP shops. The BlueKeep vulnerability, revealed in late spring of 2019, is likely linked to some of the RDP traffic we're seeing as well.[17]

UDP port 1900 saw a good deal of traffic, with nearly 85 million hits, many of which took place during the aforementioned March and June campaigns. Port 1900 is used by both SSDP and UPnP, which allow devices and services to discover and communicate with one another without prior configuration, enabling data sharing, communications and network streaming. Largely intended for small home/office environments, SSDP and UPnP are extremely widespread and implemented in millions of devices worldwide: routers, printers, and IoT in general. Unfortunately, due to poor inbuilt security as well as their use of multicast routing, where a single network packet can be transmitted to multiple destinations simultaneously, both protocols are often abused on a large scale during attacks such as those experienced by Amazon Web Services[18] and global CDN provider Akamai[19] in the first half of 2020.

16 https://www.csoonline.com/article/3542895/attacks-against-internet-exposed-rdp-servers-surging-during-covid-19-pandemic.html
17 https://www.rapid7.com/research/report/nicer-2020/
18 https://siliconangle.com/2020/06/17/aws-mitigated-record-breaking-2-3-tbps-ddos-attack-february/
19 https://blogs.akamai.com/2020/06/akamai-mitigates-sophisticated-144-tbps-and-385-mpps-ddos-attack.html

CONCLUSION

If the threats we've seen in 2020 are any evidence, attackers have opportunistically jumped on the pandemic crisis by leveraging the fear it has raised as an effective lure to gain more revenue. As they expand their affiliate programs and run recruitment drives to attract elites to join their teams,[20] it remains to be seen which other attack vectors they may use in H2.

The situation is another example of a scenario we continually see play out: threat actors have the capability to adapt to new situations by shifting their operations to target trending topics without losing momentum. Sadly, the healthcare industry was not spared, and has continued to face cyber attacks even as they fight on the front lines.[21] On a positive note, volunteers from the cyber security community have stepped forward to lend a helping hand in securing this essential industry in a time of grave need.[22]

To protect themselves from threats, organizations should ensure they adhere to general best practices and recommendations provided by cyber security professionals: stay on top of updates and patches; lock down services that are outright vulnerable or could lead to further compromise; try to segregate employees' work computing environments from their personal; always remain vigilant for spam or phishing campaigns; and educate employees about these campaigns. Organizations can find more detailed advice for securing a remote workforce in COVID-specific guides.

As a whole, the industry will also have to work toward reducing the success rate of email as an attack vector, not only through technology enhancement, but also by companies evolving their cyber security strategies and providing constant security awareness education and training. We have much to do in terms of educating the world about ever-present cyber threats. The outlook, however, is not a bleak one, for if the COVID-19 pandemic has taught us anything, it's that everyone can play a role in securing the cyber world.

20 https://www.bleepingcomputer.com/news/security/ransomware-recruits-affiliates-with-huge-payouts-automated-leaks/
21 https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-healthcare-sector-during-covid-19-pandemic
22 https://www.csoonline.com/article/3539319/legions-of-cybersecurity-volunteers-rally-to-protect-hospitals-during-covid-19-crisis.html

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

F-Secure