ATTACK LANDSCAPE UPDATE

Ransomware 2.0, automated recon,
supply chain attacks, and other trending threats

F-Secure

CONTENTS

FOREWORD:
2020 PROVED THAT OUR HEALTH DATA REALLY IS A TARGET

By Mikko Hypponen

For many years, our clients and customers have asked me about personal health data. "Isn't it true that health data is one of the prime targets of evil hackers? Isn't it true that they're after my medical history?" they have asked. For years my answer has been: "No, it's not."

Around 99% of the cases we investigate at F-Secure Labs are criminals who are trying to make money. My thinking has been that if you're trying to make money, your prime target is financial information like credit card data, not X-ray images.

But now I'm changing my mind.

The reason? The rise in attacks against hospitals, medical research units, and even patients that has occurred during the pandemic – in particular, the October attack against the Psychotherapy Center Vastaamo in Finland, in which sensitive information related to tens of thousands of patients was compromised.

Ryuk attacks have hit dozens of hospitals and healthcare organizations over the past year, particularly across the US, where COVID-19 has already stretched hospitals, health care organizations and staff to the limit.

The Vastaamo case is an example of an attacker who is motivated by money and attempting to monetize personal data by blackmailing not only healthcare institutions, but by directly contacting patients themselves. Going after individuals as opposed to institutions and companies is not a trend yet, but we are seeing indicators that it could become one in the near future. This should be very concerning to all of us.

The bulk of attacks targeting the healthcare sector are ransom Trojans. They usually involve a disruption like shutting down operations and demanding: "Pay us money if you want to continue saving lives." We have seen a number of ransom Trojan attacks during the pandemic, most importantly Ryuk. Ryuk attacks have hit dozens of hospitals and healthcare organizations over the past year, particularly across the US, where COVID-19 has already stretched hospitals, health care organizations and staff to the limit.

A massive challenge

Health data has always been an easy target for threat agents because it's typically not well protected. Most medical systems are publicly funded, which means the world's health data is often stored in old legacy systems running outdated operating systems. Attackers have always had easy access to these systems. Now that they are beginning to use it, the need to protect some of our most private and sensitive data is more urgent than ever.

An added complexity is that health data isn't like corporate data, which is stored for a relatively short period and can then either be destroyed or made public. Health data needs to remain accessible, secure and private forever. With limited budgets and legacy systems, this is a massive challenge that we are only now beginning to grasp.

The bottom line is that our health data is now a target for blackmail and other types of attacks. Solving this massive challenge will require a shift in attitude on many levels. And it is definitely not a problem that anyone can tackle alone. It will require both a deeper understanding of this emerging and growing threat and the willingness to address it on all possible levels.

The knowledge, insights and actions of cyber security professionals are a big part of the solution, but the only way to solve the problems we face is together.

INTRODUCTION

The past year has shaken up the world, forcing distance and isolation. In a year of lockdowns and quarantines, we have experienced digital technology not as a convenience, but as a lifeline to the outside world. Online infrastructure has enabled work, education, healthcare, and a host of other activities to continue remotely. Many of these adjustments will have a lasting impact.

Not everyone was forced to adjust, however. Cyber threat actors, who have always operated remotely, have continued their business as usual throughout theFileFix Professional, with new twists and turns. This report documents developments seen in the last half of 2020, and the trends we see continuing into 2021.

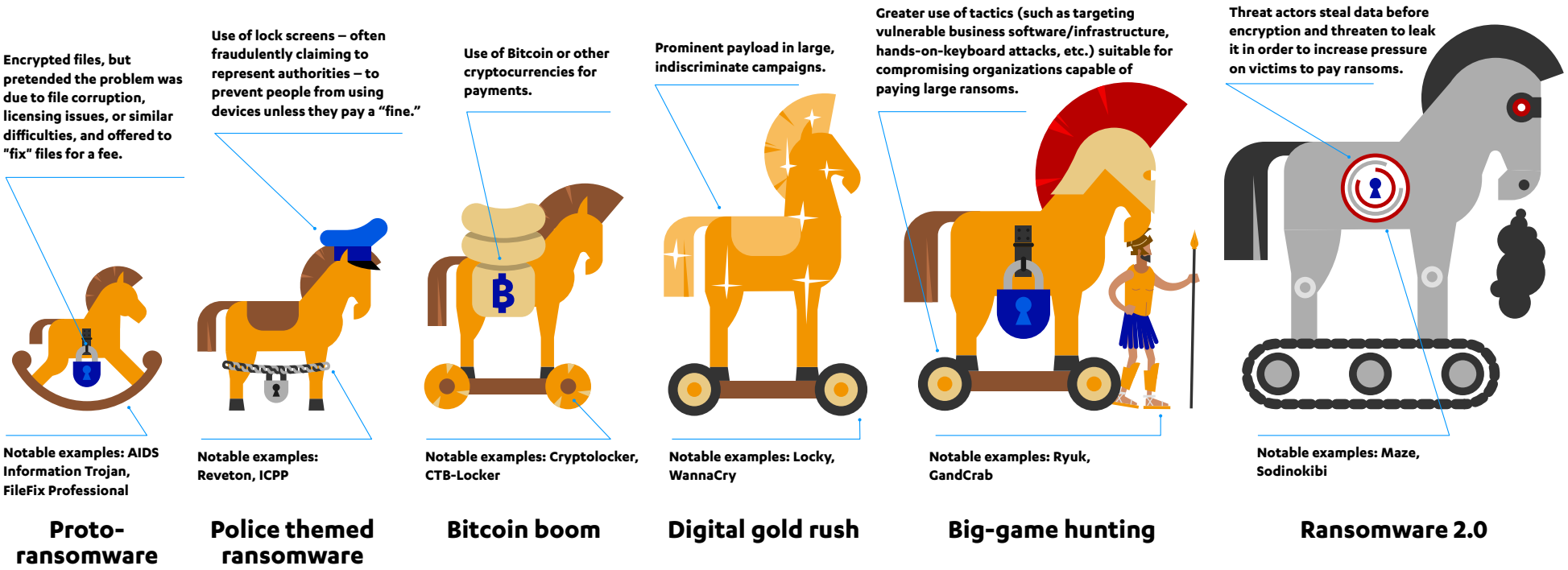
As ransomware perpetrators hammered their victims with even more damaging extortion tactics, advanced cyber actors performed a supply chain attack of historic proportions. We witnessed the continued use of information stealers to profile networks and exfiltrate data, and saw elevated levels of opportunistic traffic to our honeypots looking to exploit weakly secured devices and servers. Through it all, attackers used various techniques to attempt to bypass security measures, in a continuation of the back-and-forth battle between attackers and defenders.

TRENDING THREATS

Ransomware 2.0

2020's most notable ransomware development was the sudden increase in popularity of a new technique: extorting organizations by threatening to leak stolen data. In late 2019, attackers behind the Maze ransomware family demonstrated the efficacy of this approach when they threatened to leak stolen data unless the victim paid. By the end of 2020, the same activity was observed in 15 other ransomware groups. If an organization appeared to be avoiding payment, attackers threatened to publish exfiltrated data on their public website, and began following through on those threats. This development indicates the evolution of ransomware into "ransomware 2.0."[1]

Figure 1. The evolution of ransomware 2.0.



1 https://blog.f-secure.com/podcast-ransomware-mikko/

Data exfiltration became significantly more popular among ransomware groups in 2020. Out of the 55 new ransomware families/unique variants tracked by F-Secure last year, 21 were observed stealing data from victims – nearly 40%. Furthermore, several existing ransomware families incorporated data exfiltration to their operations. One out of every five ransomware families/unique variants identified since 2018 exhibited data exfiltration activity by the end of 2020.

Figure 2. List of ransomware families/unique variants with data exfiltration activity since 2018. Ransomware observed extorting companies by threatening to make information public are bold.

Ako	FTCode	Pay2Key/Cobalt
Avaddon	Hades	ProLock
BitPyLock	Hakbit/Quimera/Thanos	PwndLocker
ChaCha / Maze	**JungleSec**	**Ragnar Locker**
Clop	Lock2Bits/LuckyDay	Ranzy Locker
Conti	**LockBit**	**Sekhmet**
CryLock / Cryakl 1.9	Mailto/NetWalker	**SNAKE**
Darkside	Mespinoza/Pysa	**Snatch**
DroppelPaymer	Mount Locker	**Sodinokibi/Sodin/REvil**
Egregor	Nefilim/Nephilim	SunCrypt
EvilQuest/ThiefQuest	**Nemty**	Zeppelin

Ransomware groups also employed other methods to increase pressure on victims to pay. A SunCrypt ransomware affiliate bombarded a victim with distributed denial-of-service (DDoS) attacks when payment negotiations stalled.[2] The Egregor ransomware began "print bombing" victim organizations by repeatedly printing its ransom note from various printers in the organization.[3] Some groups, after receiving the initial ransomware payment, have begun demanding still more money to delete the data they have exfiltrated.[4]

In recent years the trend in ransomware attacks has been to move away from entirely automated attacks to more manual hands-on keyboard intrusions. Ransomware groups are also qualifying victims and looking to boost profits by ensuring maximum damage is done. These intrusions have significant commonalities in tooling and malware usage with other crimeware intrusions. For this reason, the activities that precede the actual ransomware payload are often detected in far greater numbers by defenders than the final payload, making ransomware seem rare in comparison to many other threats. However, out of all incident response investigations conducted by F-Secure's security consultants in 2020, approximately a third of them involved ransomware – often following hands-on-keyboard hacking by attackers. Its prominence in security incidents indicates that ransomware counts among the most common attacks impacting organizations.

2 https://www.bleepingcomputer.com/news/security/ransomware-gangs-add-ddos-attacks-to-their-extortion-arsenal/
3 https://www.bleepingcomputer.com/news/security/egregor-ransomware-print-bombs-printers-with-ransom-notes/
4 https://www.bleepingcomputer.com/news/security/ransomware-now-demands-extra-payment-to-delete-stolen-files/

Several other notable technique were used by ransomware groups in 2020. One such development was 'rapid' domain-wide ransomware deployment, which involves the deployment of ransomware across a full domain in a matter of hours after the initial access of the organization (as opposed to spending days or weeks learning where to "target" an organization). Other developments include the deployment of virtual machines to execute ransomware payloads as a way of hiding its malicious code from security software, and mounting virtual hard drives to expedite the process of encrypting large files.

While 2020 had more than its share of bad news, on the positive side, some of these newer ransomware techniques provide new opportunities for organizations to identify compromises early. Data exfiltration requires adversaries to spend more time performing additional malicious actions on the victim network, giving defenders more opportunities to detect an intrusion and additional time to respond and contain the threat. Rapid ransomware deployment will likely be 'noisier' – triggering detections and the thresholds of defenders who prepare themselves for such attacks.

> Out of all incident response investigations conducted by F-Secure's security consultants in 2020, approximately a third of them involved ransomware – often following hands-on-keyboard hacking by attackers.

Infostealers and automated recon

The widespread use of infostealers continued in the last half of 2020. Deploying infostealers near the beginning of an infection chain allows adversaries to gather information about the infected system. They profile the machine they are on, identifying the type of account privileges it has and the machine's functionality or purpose. Infostealers may gather and exfiltrate files. They can also be automated to move from one network device to another, mapping out the topology of the network. Raccoon, for example, has been known to steal credentials to be able to move laterally.[5] Harvested information is relayed back to the attackers, who can then decide the most profitable avenue for exploiting the system.

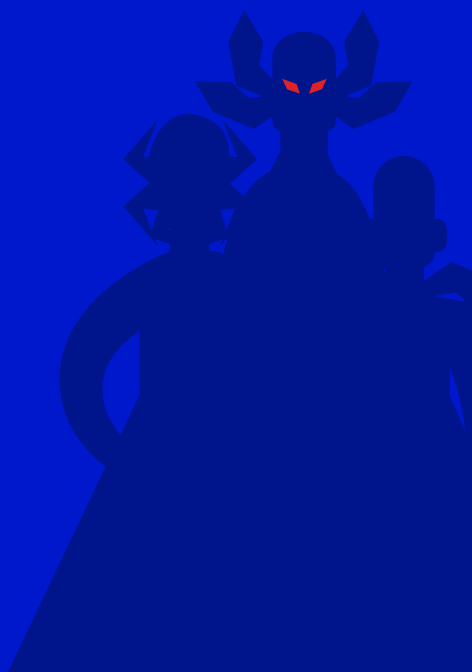
The top two malware threats seen in H2, Lokibot and Formbook, are both infostealers. Lokibot is known for stealing credentials from browsers, mail clients, file sharing programs, remote connection programs, and a wide range of other applications. It also contains a keylogger component.

Figure 3. Top 20 malware families H2 2020

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

"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.

"Ransomware" denotes malware that does not map directly over an existing known ransomware family, but displays behavior typical of ransomware.



5 https://www.bankinfosecurity.com/raccoon-infostealer-now-targeting-60-apps-report-a-13766

Formbook, so named for its formgrabbing capabilities, is offered as malware-as-a-service. It can log keystrokes, steal clipboard contents, extract data from SDP sessions, and grab passwords from browsers, among other features.

The data gathered by infostealers is valuable to threat actors, such as ransomware groups, who can use the information to deliver their payload.

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.

Infostealer: A program that is designed to steal sensitive and confidential information, such as passwords, credentials and system information, from an infected system.

Ransomware: Malware that takes control of the user's data or device, then demands a ransom payment to restore it.

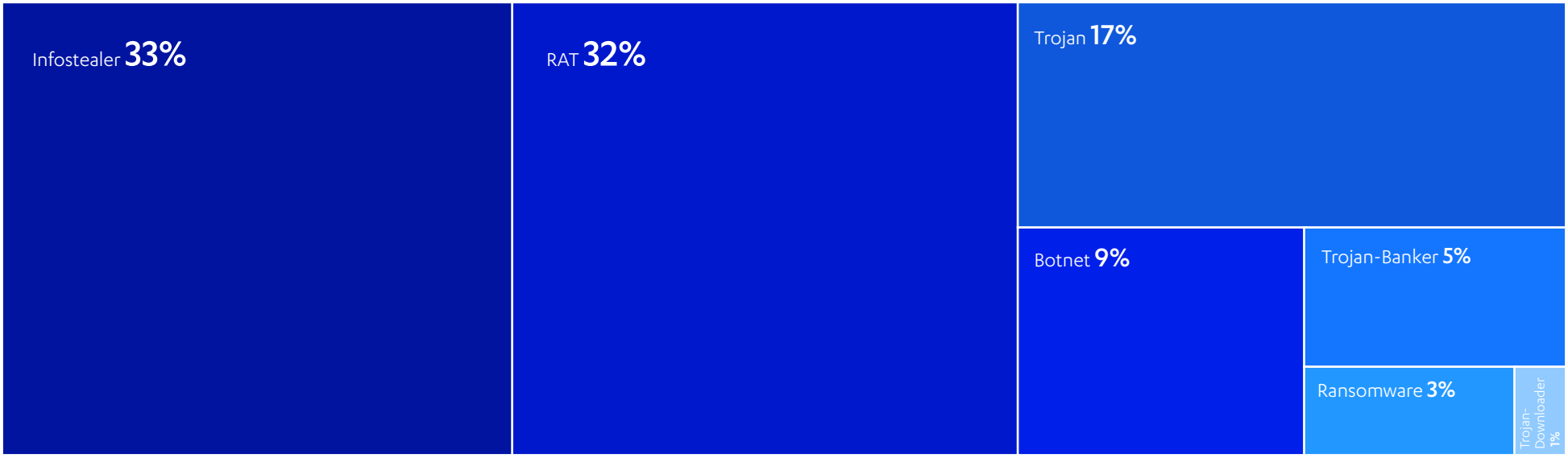
RAT: Remote Access Trojan. A program that allows an attacker to control a victim's system remotely and execute commands.

Trojan: A file or program that appears to be desirable or harmless, but secretly performs actions that are harmful devices, 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.

Figure 4. Top 20 malware threats by type, H2 2020



Poisoning the supply chain

The SolarWinds supply chain attack, disclosed in December of last year, has been called the most sophisticated supply chain attack ever. Around 18,000 organizations installed a tainted software update from the vendor, leading to widespread fallout affecting dozens of high-profile companies.[6] While generally interpreted as part of a cyber espionage campaign, the attack has significance for organizations around the globe. Similar approaches are being used for aggressive network access acquisition by highly capable actors across critical industries.

In an increasingly digital economy, supply chain attacks violate the trust we place in the technology we rely on. These upstream attacks have become more and more common in recent years. Attackers look for the easiest way in, and sometimes the way that makes the most sense is via a supplier.

Figure 5. Notable supply chain attacks of the past decade

6 https://www.reuters.com/article/us-cyber-solarwinds-microsoft-idUSKBN2AF03R

2021
Open-source repositories
(Threat: dependency confusion)

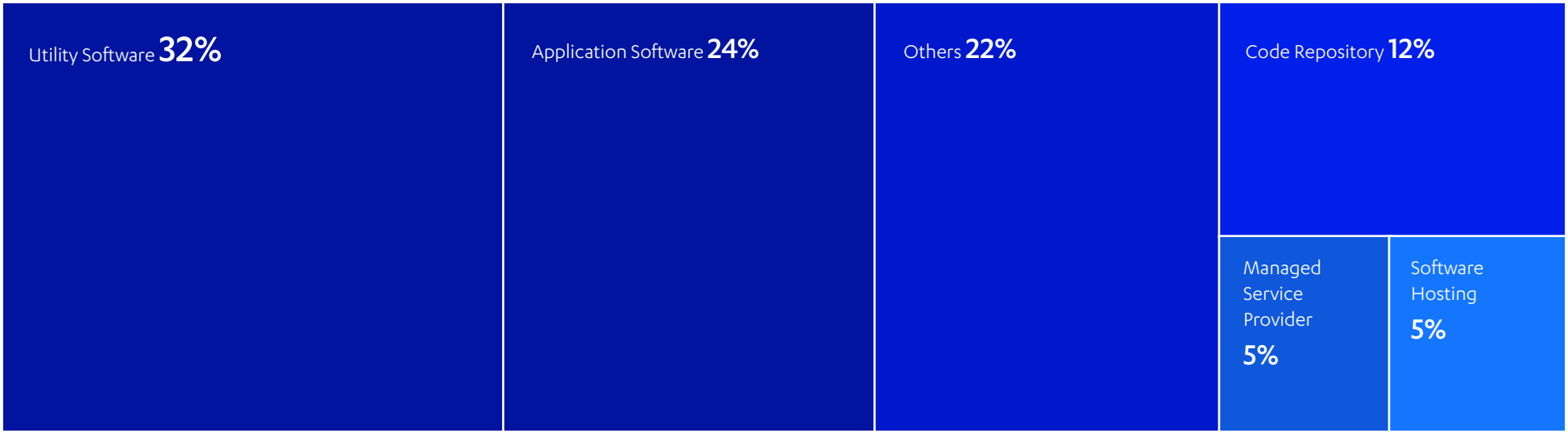
2020
Github (Threat: Octopus Scanner)
RubyGems (Threat: cryptocurrency stealers)
Able Desktop (Threat: backdoors)
VGCA (Threat: PhantomNet)
Websites that support WIZVERA VeraPort (Threat: Lazarus)
Noxplayer (Threat: backdoors)
Solarwinds (Threats: Sunspot, Sunburst, Teardrop)

2019
Asus live update (Threat: ShadowHammer)
DoorDash (Threat: unauthorized access to user data)

Using a chart (Figure 6) to represent the different types of software and services that have been targeted in the supply chain attacks featured in Figure 5, we can see that over half of attacks targeted different types of utility or application software. This can vary from text editors to video editors to video players to file managers, even to BitTorrent clients. Many organizations use open-source code, so attackers modifying code repositories can affect the organization as well.

Hope remains that fallout from the SolarWinds attack could have a positive effect. Among the international community, a collective realization exists that more must be done. There is also an increased determination to collaborate across international boundaries and between governments and private companies.

Figure 6. Supply chain attack targets



Dodging detection

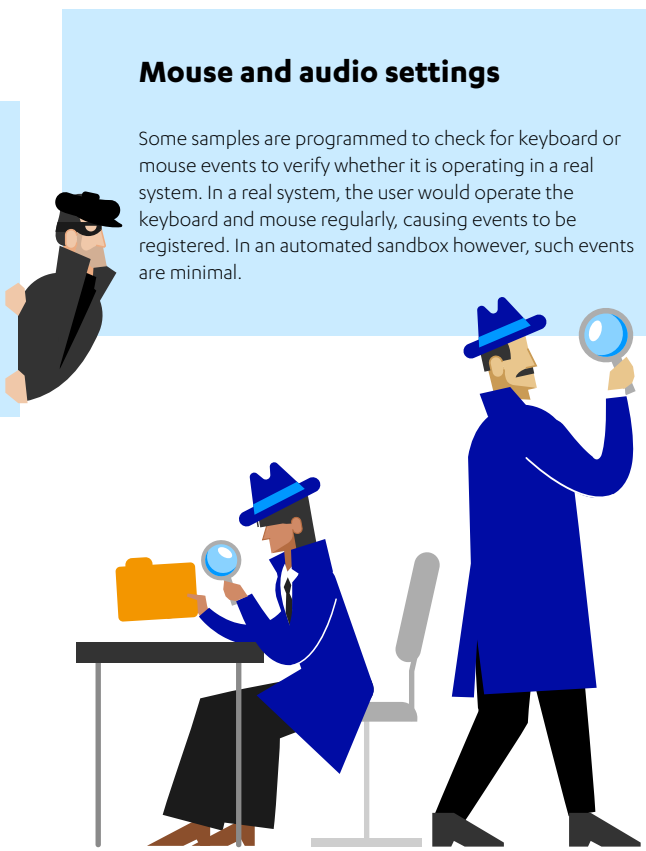
Ever seeking ways to get around detection systems and outsmart the sandboxes of malware researchers, attackers have been employing creative techniques. Some are novel, while others are tried and true methods.

Payload in registry instead of on disk

If a malicious sample is downloaded and stored as a file on a disk, it is open to detection by AV products. However, by storing malware as split registry keys rather than files on disk, some AV engines can be bypassed. This is an example of a fileless attack[8].

Mouse and audio settings

Some samples are programmed to check for keyboard or mouse events to verify whether it is operating in a real system. In a real system, the user would operate the keyboard and mouse regularly, causing events to be registered. In an automated sandbox however, such events are minimal.



Password-protected

Attackers sometimes lock their samples behind passwords to prevent automatic execution in a sandbox.

Piggybacking on Google

Organizations often have DNS filtering in place to block access to malicious websites, but they do not typically block traffic to Google. Attackers have taken advantage of this by sending DNS requests to https://dns.google.com and including a request to the malicious domain. A reply from Google DNS then contains the malicious payload, which escapes filtering, simply because it is coming from Google DNS[7].

Execution time

Some malware samples are programmed to check the time spent for execution and compare that time with a predetermined value. If the value is different than expected, they stop executing. Execution times that are longer than normal are suspected to be being debugged by an analyst, while quicker than expected execution could mean the sample is being executed inside a sandbox in fast power mode.

7 https://www.bleepingcomputer.com/news/security/attackers-abuse-google-dns-over-https-to-download-malware/
8 https://blog.malwarebytes.com/threat-analysis/2020/11/german-users-targeted-with-gootkit-banker-or-revil-ransomware/

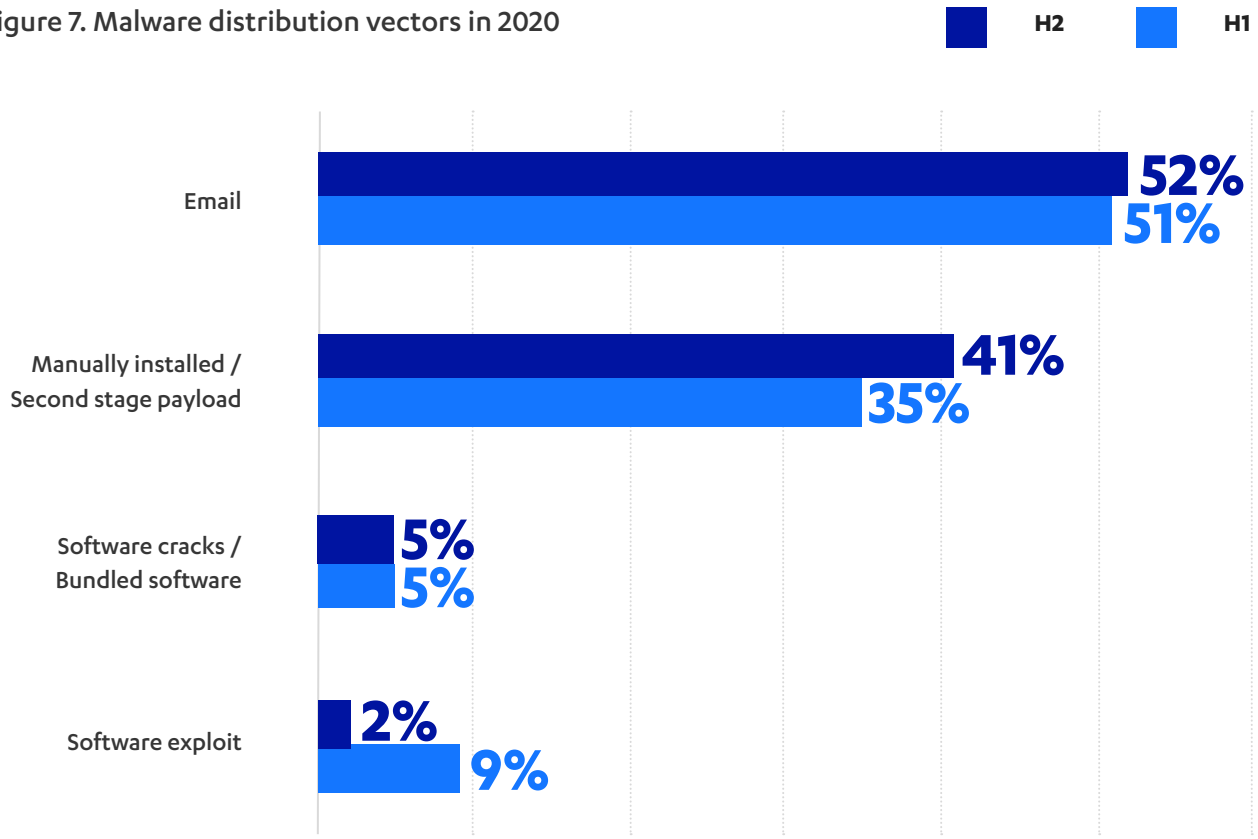
EMAIL THREATS: COMING TO AN INBOX NEAR YOU

You've got ~~mail~~ malware

Malware distribution was roughly consistent during the first and second halves of the year. Email spam continued to be the primary malware distribution method, delivering 52% of malicious payloads. 41% of malware was spread through manually installed or second stage payloads – up from 35% in the first half of the year. Manually installed payloads are those that the user is tricked into installing. Second stage payloads are those the attacker deploys after already having gained an initial foothold into the system through, for example, an unsecured RDP port or via a botnet that has infected the system.

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, accounted for 5% of attempted infections in H2. Software exploits accounted for distribution of just 2% of threats.

Figure 7. Malware distribution vectors in 2020



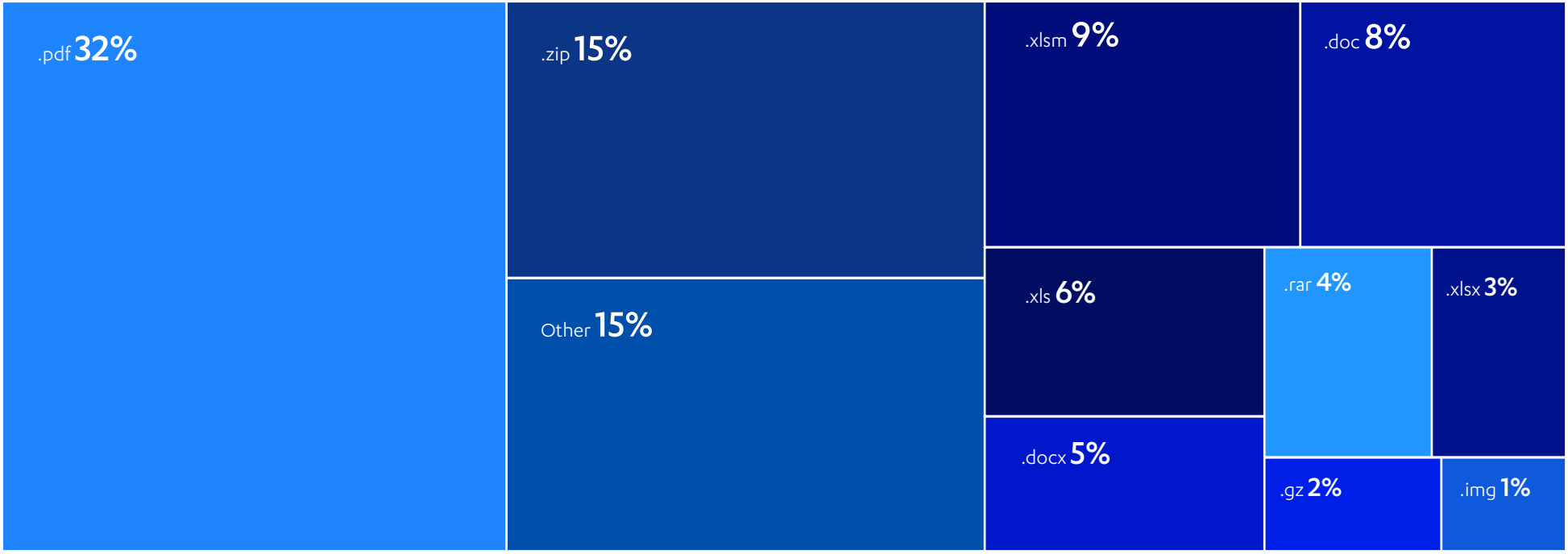
The prevalence of email as an initial attack vector warrants a deeper look into spam tactics. Roughly one out of three spam emails tracked by F-Secure include a malicious attachment, while the rest contain a URL.

Looking deeper into attachments, the most common filetype used by attackers was PDF, which made up 32% of attachments in the last six months of the year. While malicious PDFs have traditionally contained malicious code or an exploit to attack systems, PDFs with neither of these are becoming more common. Instead, these PDFs contain in-document URLs that lead to malicious webpages, which bypass automated scanners that flag malicious code.

PDFs' popularity with attackers rests in the portability of the filetype across devices and platforms. With the combination of a portable file featuring a URL, all that's needed is effective social engineering to lure users to click on the document and open the link inside.

Archive files such as ZIP, RAR, GZ and IMG accounted for about one out of every five attachments. Because some threat actors still use archive files to deliver malware, users should always take extra precautions if receiving one in their inbox.

Figure 8. Spam attachment filetype breakdown, H2 2020



In addition, adversaries are constantly on the lookout for new attack avenues. After years of using Office documents laden with malicious macros, attackers have improved this technique by using Excel formulas to obfuscate malicious code. As a core default feature of Excel, formulas cannot be blocked (although the macros they contain can be).

Usage of Excel formulas in attacks more than tripled in the second half of the year when compared with the first. The volume of files using this technique numbered in the hundreds per month during the first half of the year, and jumped to tens of thousands per month in the second half, with a particularly significant spike in September.

Figure 9. Malicious excel documents utilizing formulas per month (as a percentage of total seen in 2020)

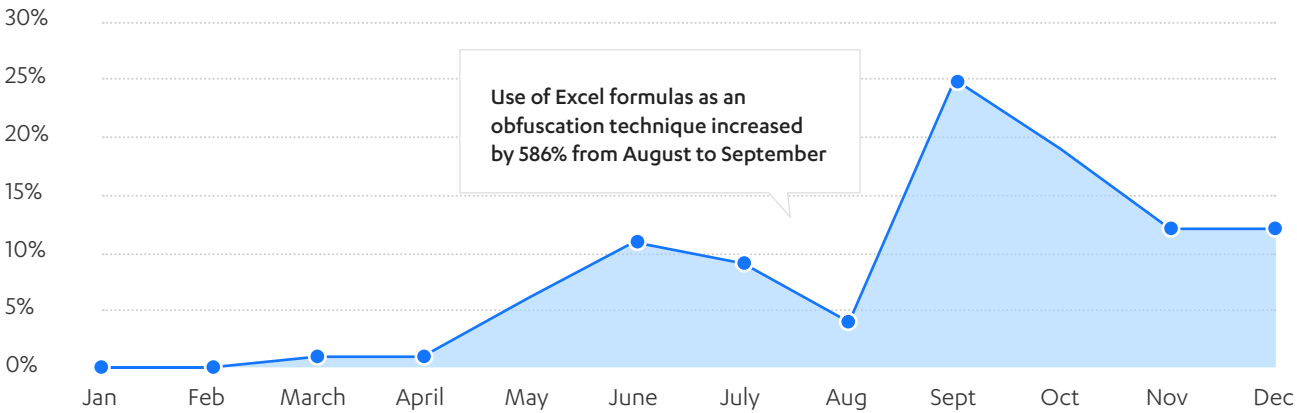
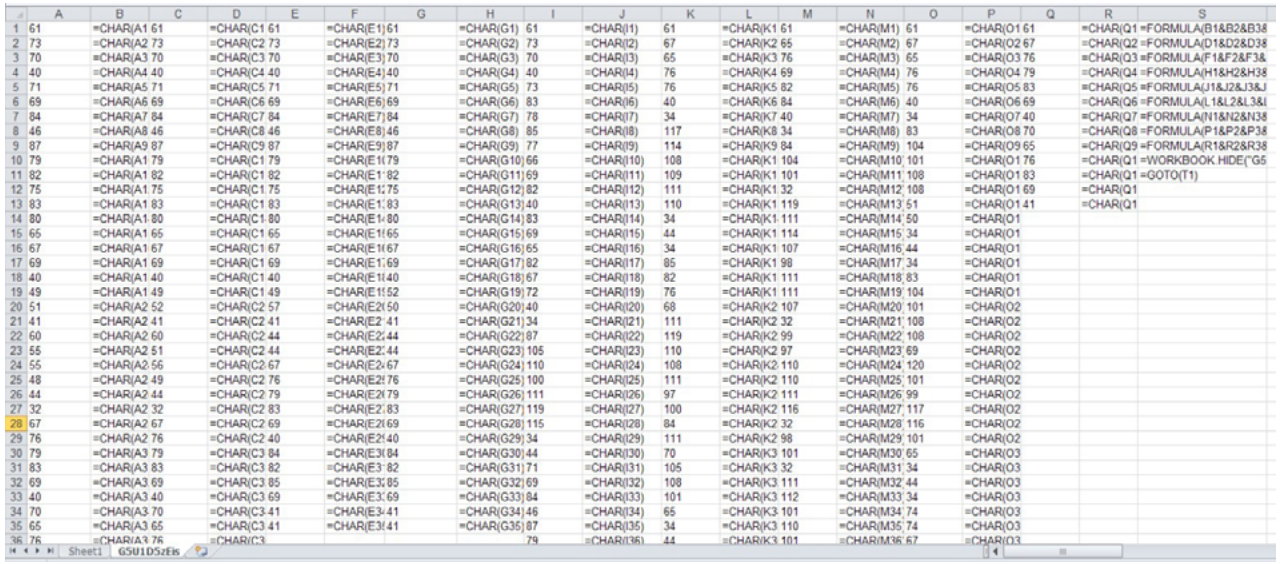


Figure 10. Example of an Excel document that uses formulas to store malicious code



Phishing for sensitive data

Of the spam emails containing URLs, 19% contained links to phishing pages, which collect sensitive data by tricking users into disclosing information to a web form. The remaining URLs were links to pages hawking questionable wares or pushing dodgy schemes, such as Bitcoin investment scams.

Domains used to host these phishing pages were a mix of web hosting/ cloud storage services; domains that have been compromised and hijacked for use in phishing; and dedicated phishing domains that are self-hosted by attackers, with their own URL and infrastructure.

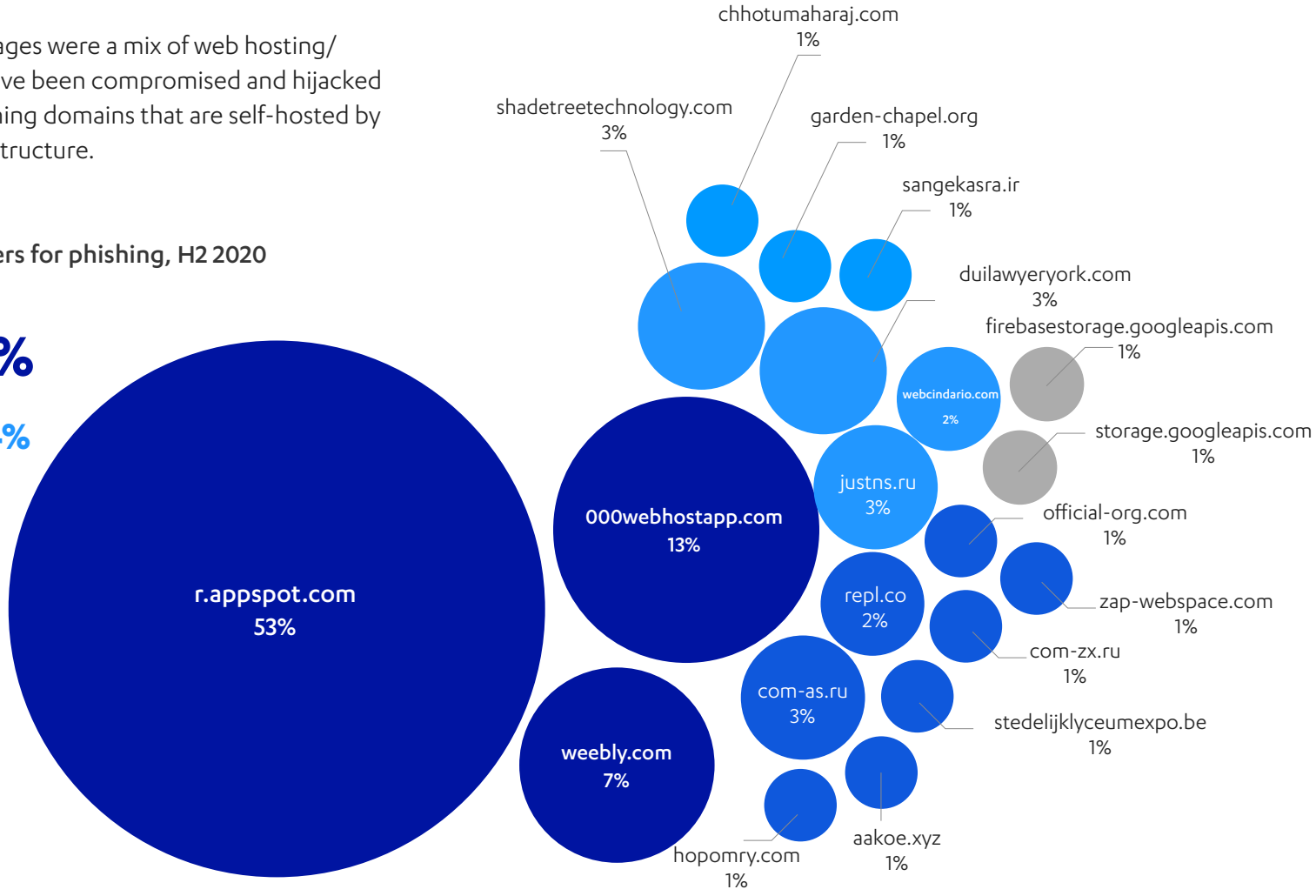
Figure 11. Top domains used by attackers for phishing, H2 2020

Web hosting 73%

Compromised domain 14%

Phishing domain 11%

Cloud storage 2%



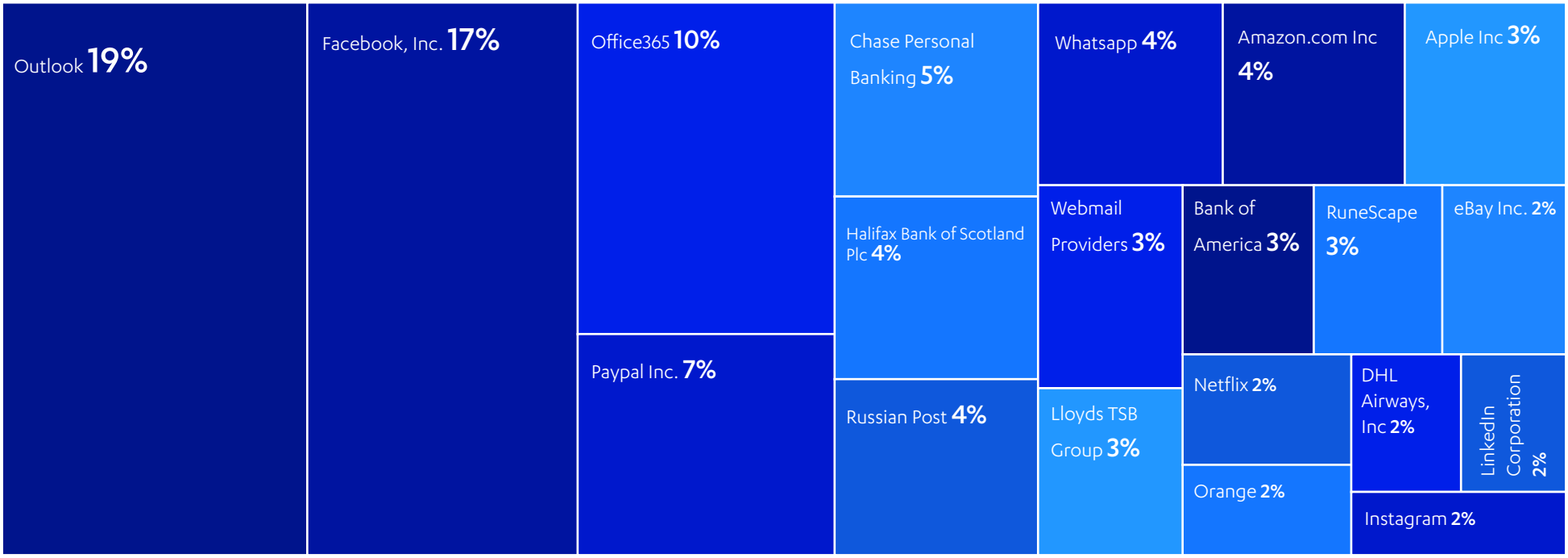
Web hosting services have recently become a popular choice for attackers because the costs involved in setting up a webpage through these services are relatively low. They can even be free for basic use. As phishing pages are often quickly removed after being reported, the use of hosting services enables threat actors to generate and switch their pages rapidly without substantial downtime.

Hosting services also present the user with a layer of legitimacy, as they provide SSL certificates (reflected in the "https" prefix of the URLs). A noteworthy new phishing method, for example, has been to host malicious documents on Google Docs or Microsoft OneDrive. Attackers use these services because of their reputation – no one blocks Google or Microsoft.

F-Secure expects the use of hosting services to remain a popular practice for threat actors because it saves phishers the effort of searching for and identifying domains or web servers they can compromise.

As in H1, attackers continued to leverage Facebook heavily as a theme in phishing emails to gain the trust of potential victims. However, in the second half of the year, emails impersonating Outlook were the most common.

Figure 12. Top impersonated brands in phishing, H2 2020



We also noted an increase in phishing for Office365 credentials in H2, making up 10% of top brand phishing activity compared to 6% the first half of the year. The rise is reflective of intensified organizational migration to cloud services to better support remote workers.

With the shift to remote work in many organizations, employees adopted collaborative tools such as video conferencing and online document sharing applications. Attackers moved quickly to exploit these changes by tricking users with fake emails impersonating collaboration services like Microsoft Teams and Zoom.

Figure 13. Phishing email spoofing Microsoft Teams

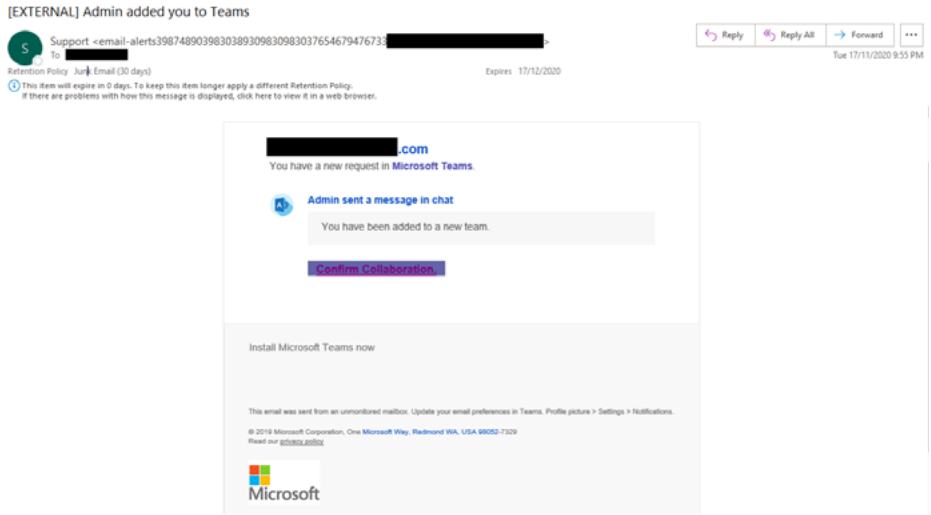
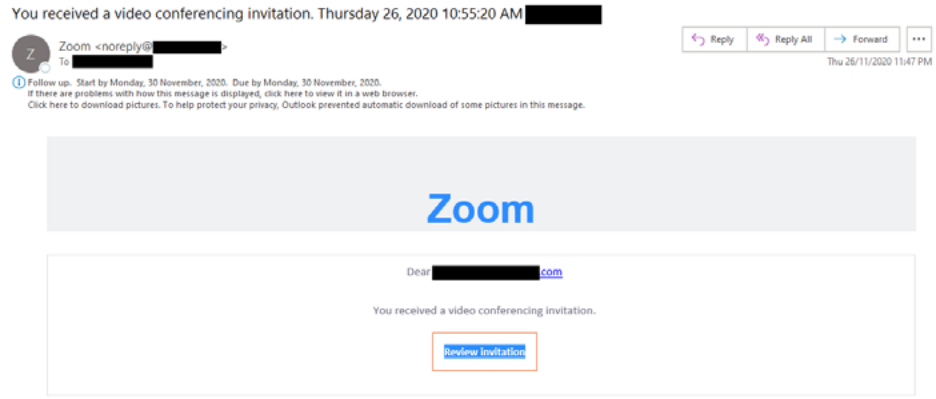


Figure 14. Phishing email spoofing Zoom



COVID-themed spam continues to spread

In our H1 report we noted a deluge of COVID-related spam that hit in the spring and died down as summer approached. The second half of 2020 saw a second wave of spam leveraging the coronavirus theme. After an initial spike in August, COVID-themed spam continued the rest of the year at a reduced but consistent rate.

The top threats delivered by COVID-related spam in H2 were all infostealers: AgentTesla was included in 27% of attachments, Formbook in 24%, and Lokibot in 18%. The remainder of COVID spam attachments delivered generic malware, malicious documents, PowerShell scripts and other malware families.

Figure 15. COVID-themed spam levels per month (as a percentage of total seen in 2020)

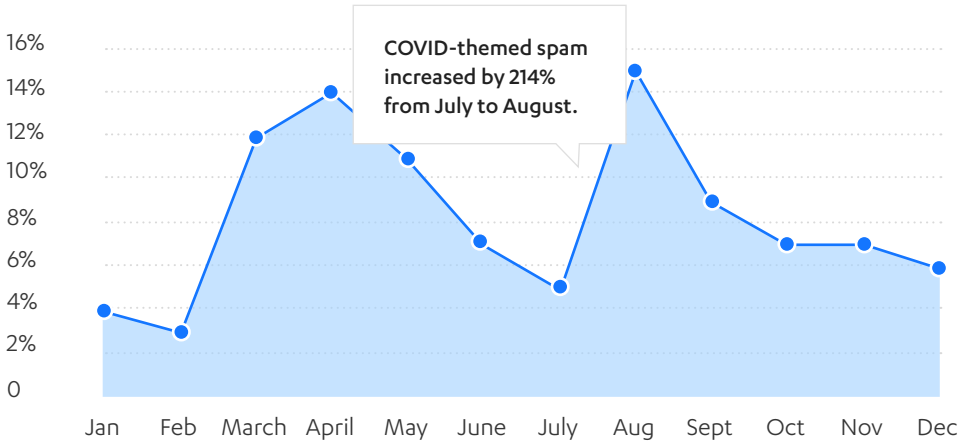
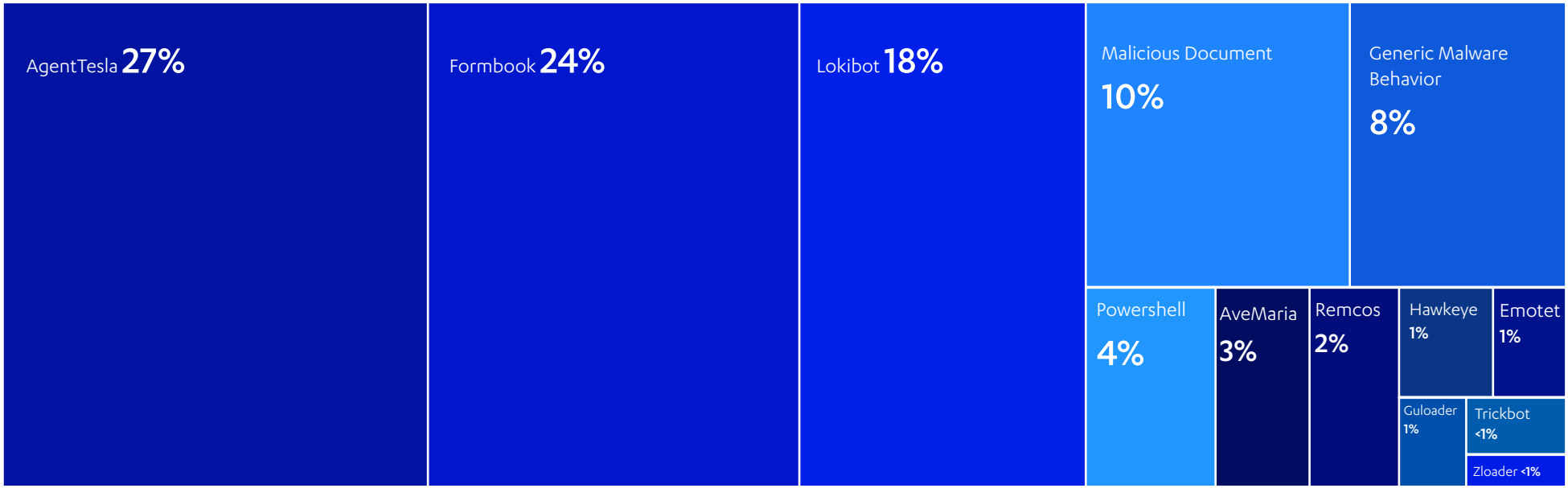


Figure 16. Top threats delivered by covid-related spam, H2 2020



VULNERABILITIES: THE LEGACY OF UNPATCHED SOFTWARE

With the increasing number of vulnerabilities discovered every year, companies need to carefully manage how patching is handled throughout the organization. The more prevalent a vulnerable software product is, and the more easily available exploit code for it is, as well as the more severe the exploit impact would be to a company, the more useful a vulnerability is to threat actors.

Researchers on F-Secure's vulnerability management team identified 11,950 different security issues in organizational networks in the second half of 2020, covering 43,669 different CVEs. Out of the nearly 12000, just 100 issues accounted for over 50% of detections.

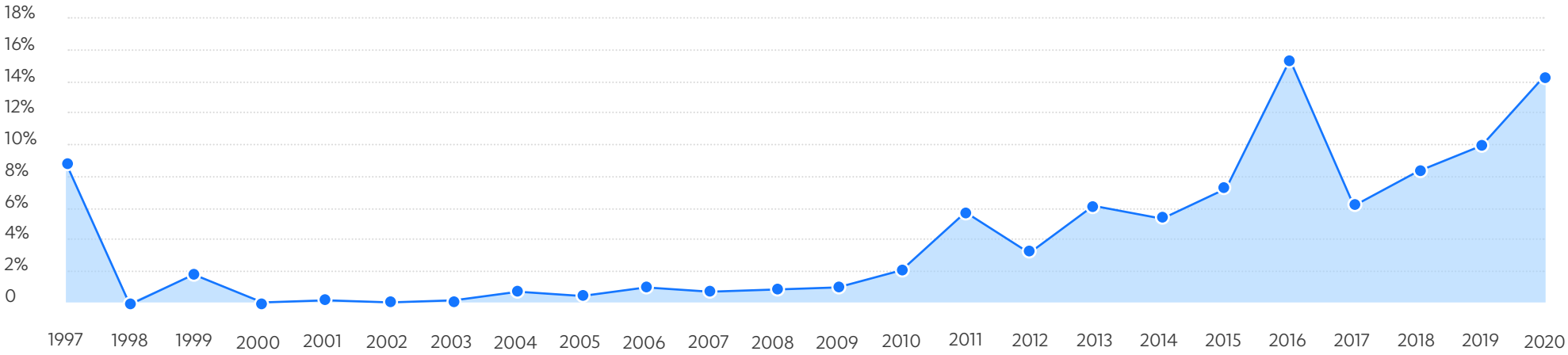
The majority (62%) of vulnerabilities were of medium severity, a finding that follows normal distribution, while 23% were high severity and 15% low.

What is perhaps a bit more surprising, however, is that when categorized according to the year they were first published, the greatest share, 15%, were published in 2016. 14% were made public in 2020 and 10% in 2019, findings that match expectations.

9% of issues found go back to 1997, predating the CVE system; these are mostly generic low-severity observations. Leaving those aside, high and medium severity issues from 1997 account for less than 2% of all high and medium severity findings.

Overall, 61% of all issues found were at least five years old, highlighting the prevalence of old, unpatched vulnerabilities.

Figure 17. Vulnerabilities found in company networks by year of publication (as a percentage of total number of vulnerabilities seen in H2 2020)



Legacy systems, legacy vulns

Going by sheer numbers of hosts vulnerable to a particular issue, the most prevalent vulnerabilities were encryption-related issues from 2016 and previous years. One of the most common findings, affecting tens of thousands of hosts, was CVE-2016-2183, SSL supporting weak ciphers, which enables the "SWEET32" attack.[9] With a severity rating of "high" on the CVSSv3 scale and a base score of 7.5, it affected multiple products supporting encrypted communication. The issue can typically be fixed by hardening the configuration or performing an upgrade. Newer products have the vulnerable ciphers disabled by default.

Other common findings are similar in nature and are caused either by the use of old versions of encryption libraries or insecure encryption configurations. Tens of thousands of hosts were found with RC4 cipher suites enabled in the SSL/TLS configuration, despite this practice being discouraged since 2013[10] and the ciphers being affected by CVE-2013-2566 and CVE-2015-2808. As the cipher can be broken, having it enabled could allow an attacker to decrypt parts of the communication and, for instance, access user credentials.

Another frequently found vulnerability, ten-year-old CVE-2011-3389, had a similar impact, enabling an attacker to perform an attack called "BEAST" and decrypt credentials and other sensitive details. The attack was possible due to a vulnerability in ciphers using CBC mode. Ironically, the recommendation at that time was to disable the CBC mode ciphers and use RC4 instead.

The 2015 vulnerability known as "SLOTH," CVE-2015-7575, was also a recurring finding. SLOTH is present in old versions of the Mozilla NSS library, an implementation of SSL/TLS. The vulnerability enabled a "downgrade" attack, allowing an attacker to trigger usage of an insecure key exchange signature algorithm. The issue can be easily solved by upgrading the NSS library; the patched version was released in December 2015.

The POODLE vulnerability, CVE-2014-3566, was another common issue. Discovered by Google engineers in 2014, it also allows for decryption of an SSL connection. At the time, the engineers recommended disabling SSL 3.0 and replacing it with its newer version (TLS), noting that SSL 3.0 was 18 years old. Now 24 years old and affected by a number of well-known vulnerabilities, the SSL protocol is still popular.

The prevalence of these issues across organizations highlights the problem of legacy infrastructure and the struggles of IT departments with keeping legacy systems secure. Furthermore, the situation serves as a reminder that security is a continuous process: Although an effort was initially made to secure the systems by enabling encryption, the encryption is no longer effective, leaving the systems insecure.

The prevalence of these issues across organizations highlights the problem of legacy infrastructure and the struggles of IT departments with keeping legacy systems secure.

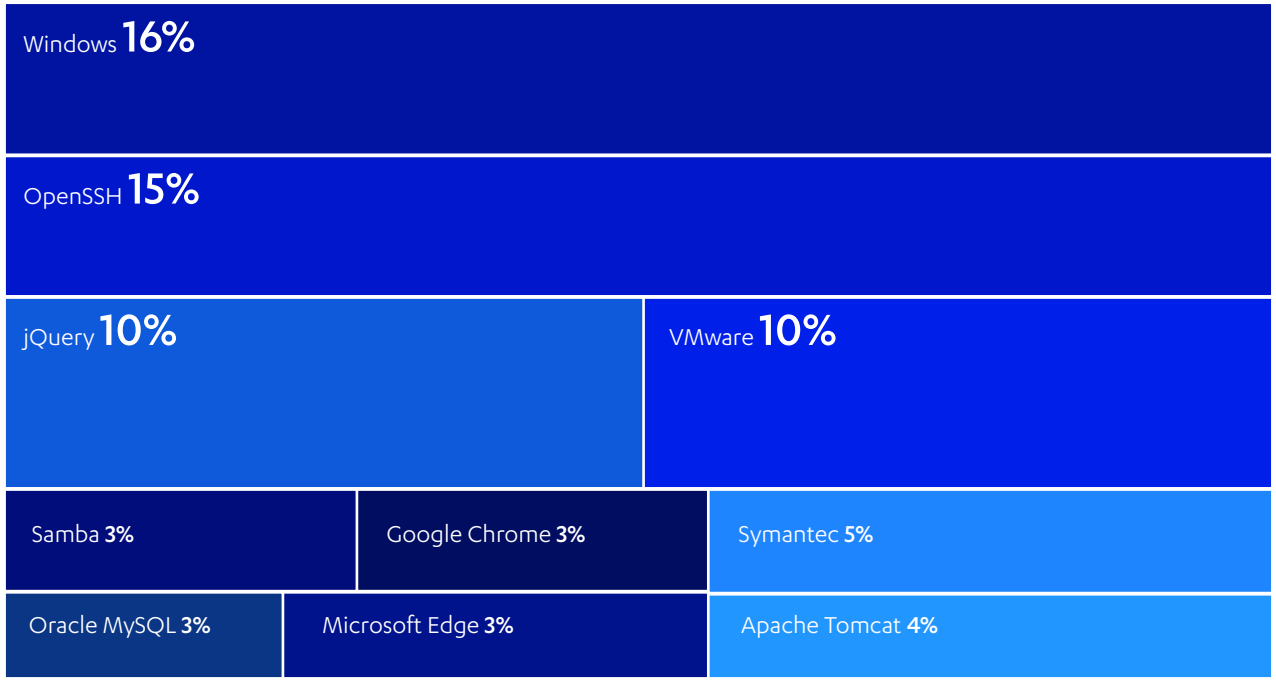
9 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2183
10 http://www.isg.rhul.ac.uk/tls/

The vulnerabilities of 2020

Of vulnerabilities discovered and published in 2020, the severity distribution is similar to that of the all-years dataset, with a slightly higher number of high-severity vulnerabilities (27%), a lower number having low severity, (9%) and the bulk being of medium severity (64%).

The greatest share of 2020 vulnerabilities affected Microsoft Windows (16%), OpenSSH (15%) and jQuery (10%), with VMware making up slightly below 10%. The results stem from the popularity of Windows in corporate environments, the presence of OpenSSH in nearly all Linux installations and the popularity of jQuery in web applications.

Figure 18. Products most affected by 2020 vulnerabilities found in organizations

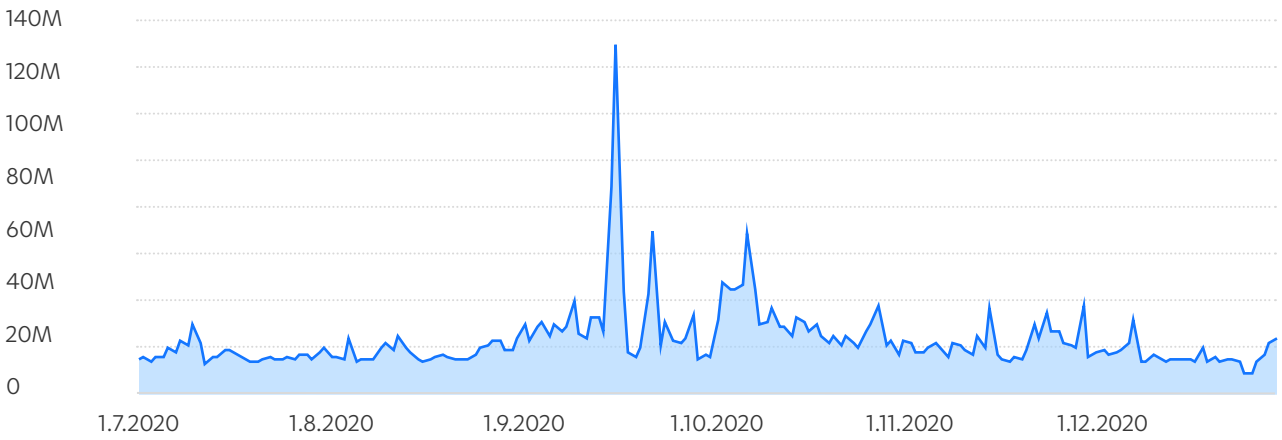


HONEYPOTS: TRACKING OPPORTUNISTIC ATTACKS

Our global network of honeypots saw a rise in events in the second half of the year, attracting 4.2 billion attacks, up from 2.8 billion in H1. The increase does not necessarily translate to a more active H2 overall, as the jump in events was fueled by a few major denial of service (DoS) campaigns on UDP port 1900. These attacks accounted for over half of events during the period.

The greatest share of attack events came from China's IP space, followed by the US and Ireland. Events sourced in China and the US were mostly DoS attacks, a significant portion of which were involved in the previously mentioned DoS attacks against UDP 1900. Both IP spaces were also the source of a high number of events targeting the SSH protocol.

Figure 19. Honeypot traffic throughout H2 2020



About our honeypots

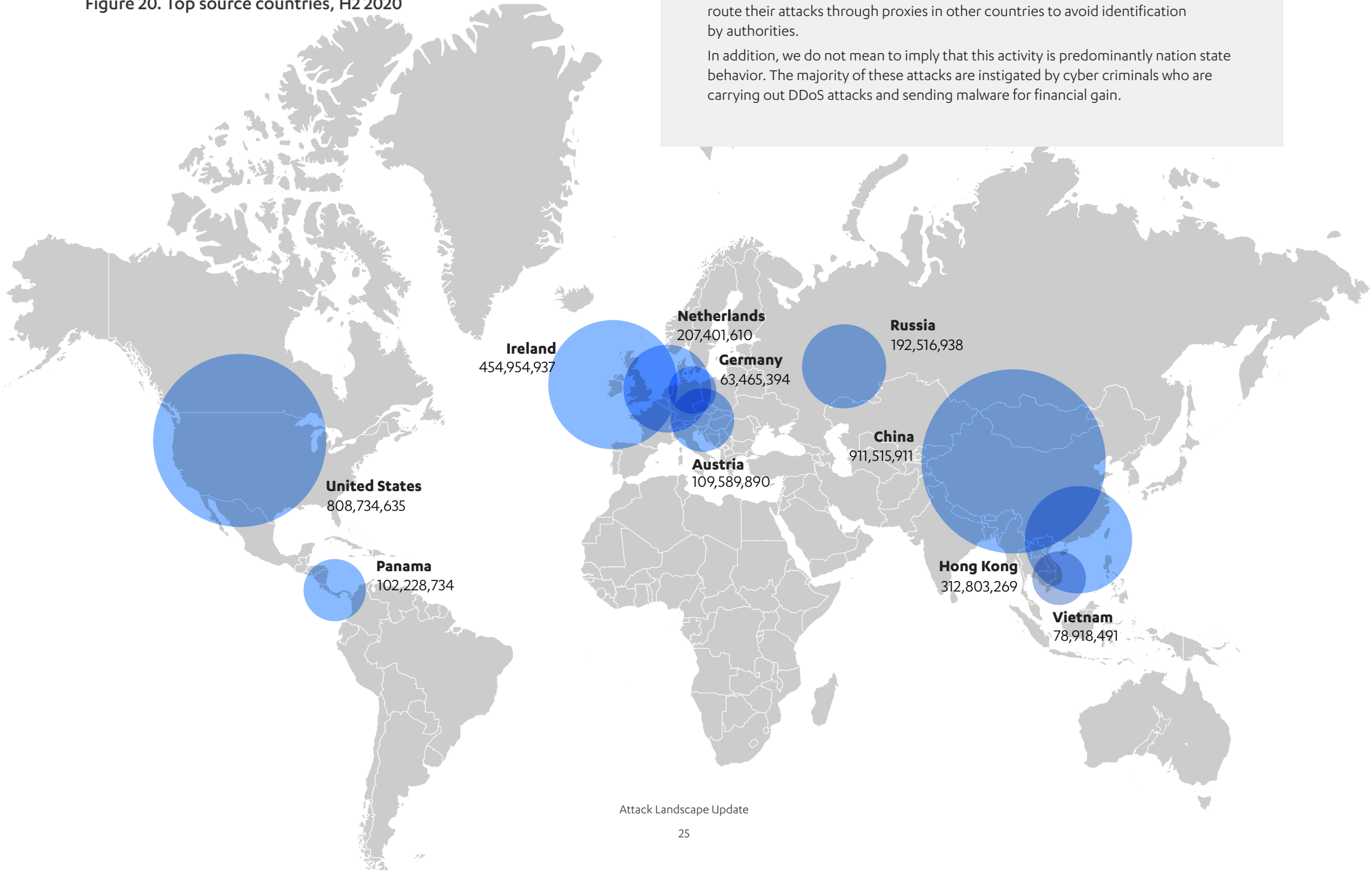
Our honeypots are decoy servers set up in countries around the world to gauge trends and patterns in the global cyber attack landscape. Because their specific purpose is to gauge potentially malicious activity, any incoming connection registered by a honeypot is deemed suspicious and likely a result 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.

Figure 20. Top source countries, H2 2020

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.



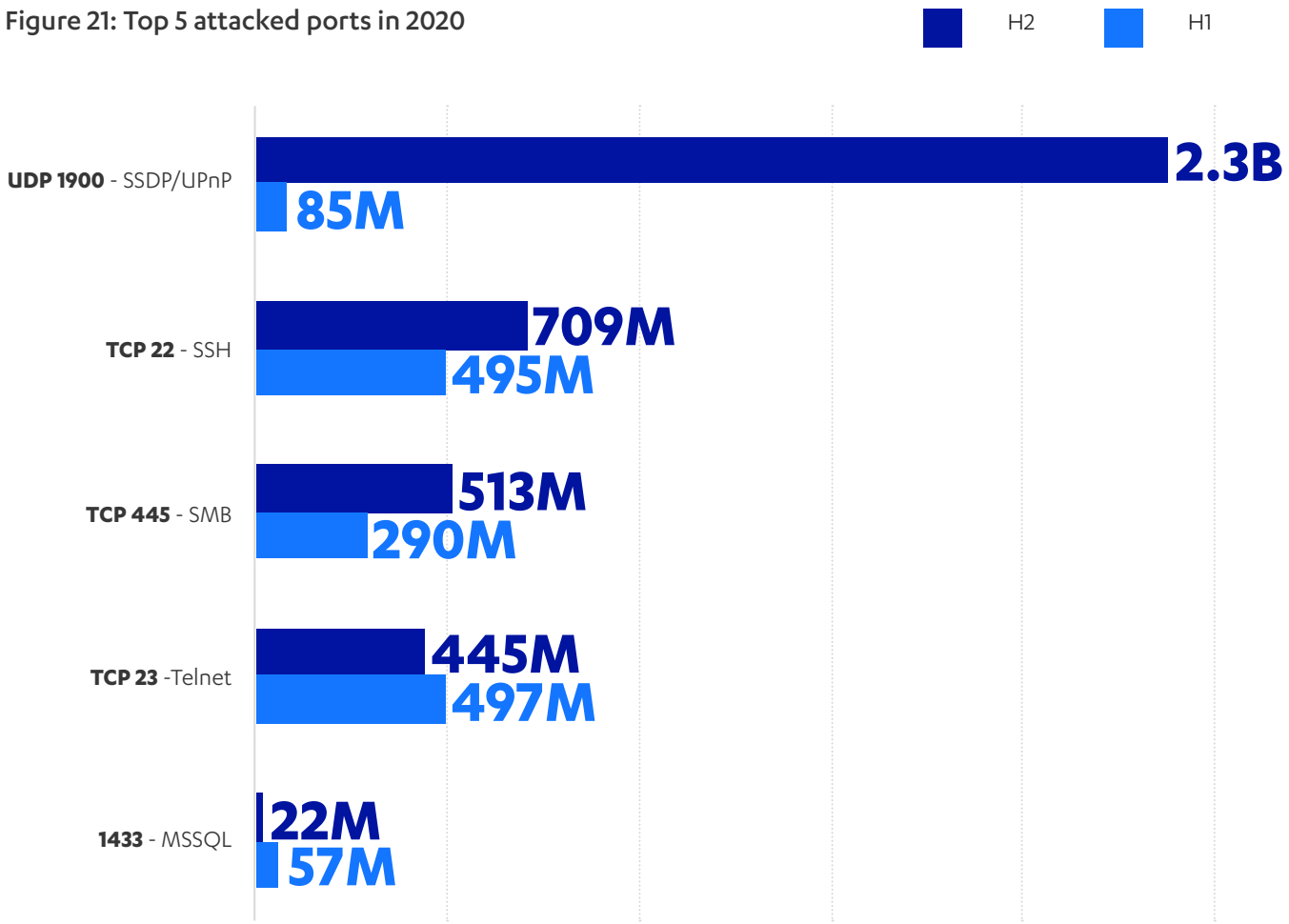
Attacks from the Irish IP space were mostly aimed at SSH port 22, representing attempts to gain access to a server by employing username and password combinations. Russian and Panamanian IP spaces were also significant sources of SSH attacks.

Looking at all the TCP port events over the 6-month period, the ports corresponding to SSH, SMB and Telnet services were the most popular by far. Traffic levels to all other ports were significantly lower.

SSH traffic on port 22 jumped about 43% in the second half of the year, likely due to many organizations' shift to remote work. Companies were faced with deploying new infrastructure in a very short amount of time, often without taking time to address potential security issues first.

Telnet traffic remained relatively stable compared to the first half of the year, while traffic on port 445 jumped 77% in H2, most likely driven by the disclosure of vulnerabilities like SMBGhost (in March) and SMBleed (in June). The volume of events related to MSSQL dropped in H2 to 38% of the volume seen in the first half of the year.

Figure 21: Top 5 attacked ports in 2020



On the UDP side, port 1900, which is associated with SSPD and UPnP, was an outlier. The port saw three major spikes in activity from mid-September through early October, DoS attacks that were significant enough to make 1900 the most-targeted port of the period.

SSDP's intended use is to allow UPnP devices to advertise their existence to and discover other devices on a network. Attackers take advantage of this characteristic for use in amplified reflection DDoS attacks.

In a reflection attack, a relatively small initial attack vector can be exponentially increased. An attacker begins by searching for publicly accessible devices that use SSDP and UPnP, which can serve as amplifiers. The adversary then crafts a packet ensuring that the target's response will contain as much information as possible. The attacker uses a botnet to distribute the packets to the discovered devices, changing the source address to an address associated with the target victim. Each device will reply by sending an amplified response (which can be more than 30 times the initial request size) to the target. The target victim is bombarded by the traffic from all devices. Overwhelmed, the victim is unable to respond to traffic from legitimate users of their site.

The choice of a UDP port rather than TCP means that while there is no guarantee of delivery as there is with TCP, there are also fewer processing requirements, making UDP faster and often preferred when communication is unidirectional and when neither integrity nor quality are high priorities.

DDoS attacks can be carried out for various reasons, including impairing competition, hacktivism, political motivation, general nation state activity, internal or external revenge attacks, distraction from another type of attack such as ransomware, or they may be used in combination with extortion requests.

CONCLUSION

From a malware perspective, we can say with certainty that attackers will continue to follow current events and use relevant themes to lure users in spam and phishing. As protections evolve, attackers will also continue to evolve and improve their techniques to get around security controls.

Ransomware continues to be a highly profitable venture, and attackers are finding more ways to take advantage of the data they obtain. With threat actors as opportunistic as they are, it is no longer enough to just have backups. Backups need to be smarter and more secure. As ransomware has been known to encrypt backups, newly made backups should be detached from the network immediately.

Files that are no longer being used should be uninstalled. Internet-facing services that are not being used should be disabled. Files that hold mission-critical data or the "crown jewels" must be encrypted, so they are not easily accessible if stolen, and access to them should be strictly limited. With infrastructure more complicated and complex than ever, companies need to employ varied security mechanisms. It's a race against time, especially when it comes to applying security patches for systems and software.

Threat actors are agile, and they don't play by predefined rules of engagement. As defenders, we will continue to keep up the fight, maintaining constant vigilance.

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**