F-Secure

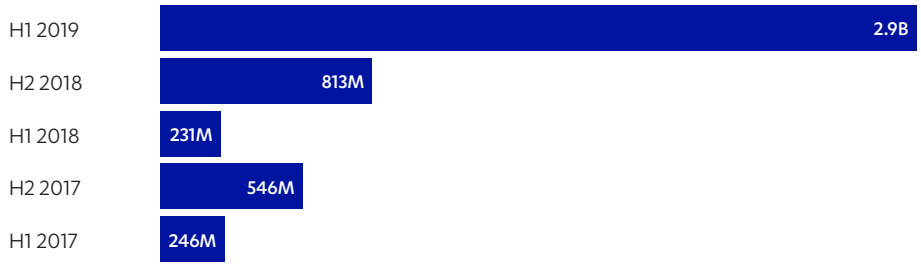
ATTACK LANDSCAPE H1 2019

INTRODUCTION

From millions to billions. In the first half of 2019, our global network of honeypots measured more than triple the attack traffic of the previous period, to a total of over 2.9 billion events. It's the first time since we've begun publishing data from our honeypot network that traffic has ever hit the billion mark.

Our honeypots are decoy servers that we've set up in countries around the world to gauge trends and patterns in what's going on in the global cyber attack landscape. We've configured them to look like actual servers, inviting the type of traffic that hits actual servers. Honeypots are highly effective tools for collecting information on the methods and target selection processes used by modern attackers. They can also be a good source of malware samples and shell scripts.

Total Global Honeypot Attacks Per Period



Because honeypots are decoys not otherwise meant for real world use, an incoming connection registered by a honeypot is either the result of a mistake (someone typing in a wrong IP address, which is rather uncommon) or of the service being found during an attacker's scans of the network or the internet.

We are always improving and upgrading our honeypot network, and doing so can contribute to increased traffic measurements. Since our last report from H2 2018[1] we've added a few new honeypots. We've also made some improvements to our Telnet and SMB plugins, which results in better recognition of those events. There's no doubt that these improvements have contributed to higher numbers of events, but there's also no doubt, given the continuing spread in infected IoT devices,[2] the prevalence of Eternal Blue, and increasing numbers of DDoS attacks,[3] that attack traffic is also simply on the increase.

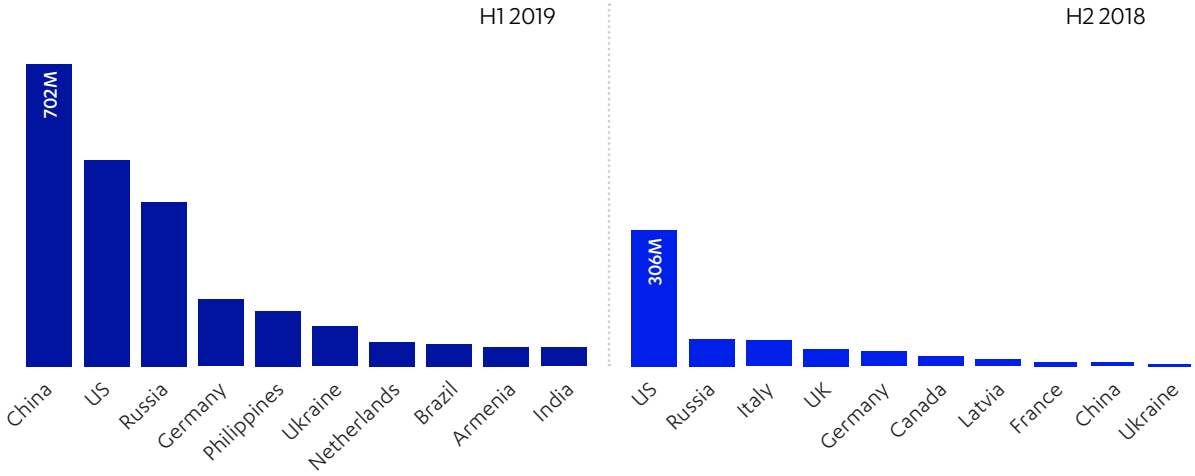
99.9% of traffic to our honeypots is automated traffic coming from bots, malware and other tools. Attacks may come from any sort of connected computing device – a traditional computer, malware-infected smartwatch or IoT toothbrush can be a source.

1. https://blog.f-secure.com/attack-landscape-h2-2018/
2. https://www.openaccessgovernment.org/iot-malware-attacks/69870/
3. https://www.comparitech.com/blog/information-security/ddos-statistics-facts/

WHO'S AFTER WHO

Where in the world are these attacks taking place? Populating the top ten list of attack source countries for H1 2019 are, as usual, the US, Russia, Germany and China. However, this is the first time that traffic volumes from the Chinese IP space has overshadowed other countries to take top spot. Traffic from China ballooned to 702 million attacks. (A breakdown of the types of traffic from the top three countries can be found later in this document.)

Top Source Countries



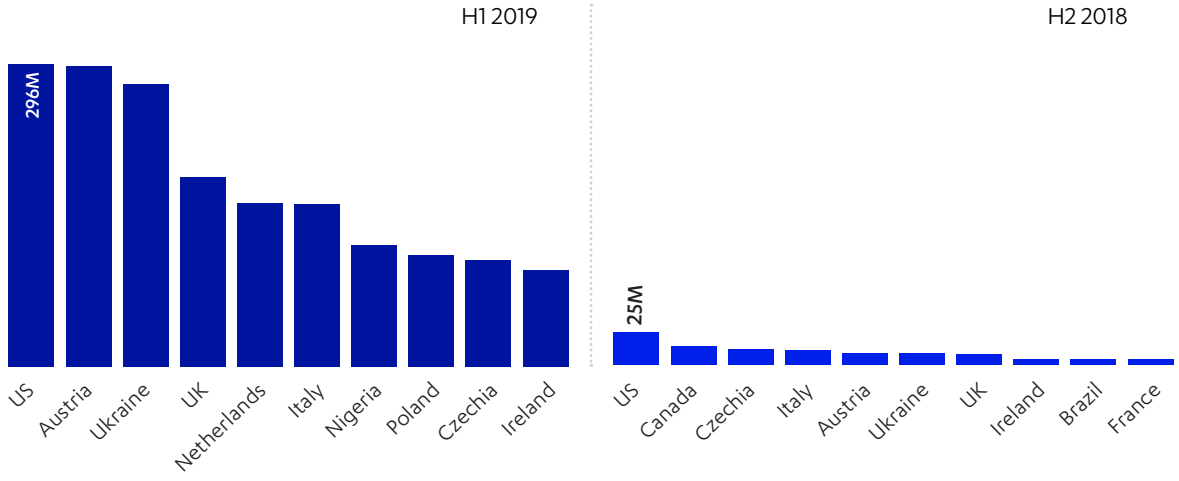
Also, for the first time, the United Kingdom just missed this list, coming in at number 11. India is a new entrant to the top ten, lighting up with 44 million attacks, which makes sense given it's also taken the distinction of being a top botnet-infected country,[4] according to Spamhaus. Philippines, Brazil and Armenia are also newcomers.

As we always point out, the list of source countries must be taken with a grain of salt. Attackers can route their attacks through proxies in countries other than where they themselves are located to avoid identification by law enforcement. 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.

As usual the US heads the list of top attack destinations. And while the rest of the countries on this list commonly appear here, just in varying order, Nigeria is new as a top attack destination. Ukraine is prominent on both source and destination lists, not a surprise given its status as a cyber battlefield[5] and a target of Russian hackers.

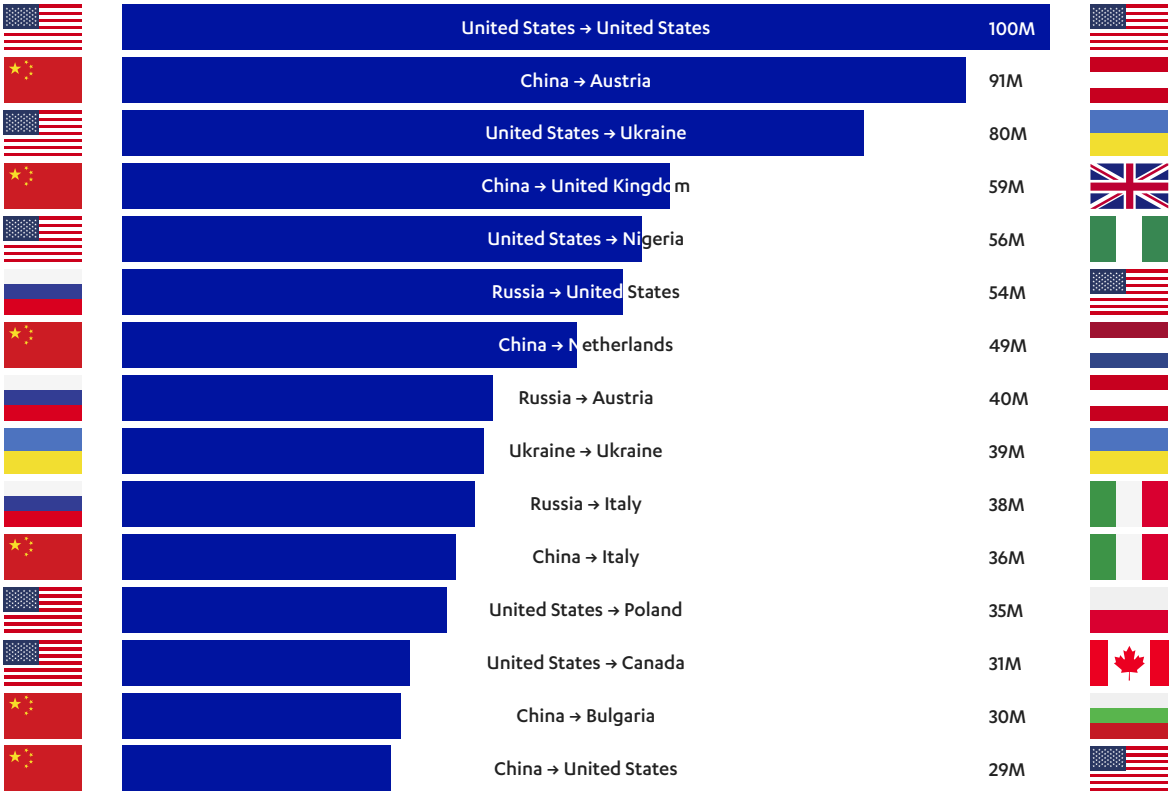
4. https://www.spamhaus.org/statistics/botnet-cc/
5. https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/

Top Destination Countries



Our who's-after-who list shows which countries' IP spaces have the most common aggressor-to-target relationships.

Top Sources to Destinations



PORTS AND PROTOCOLS

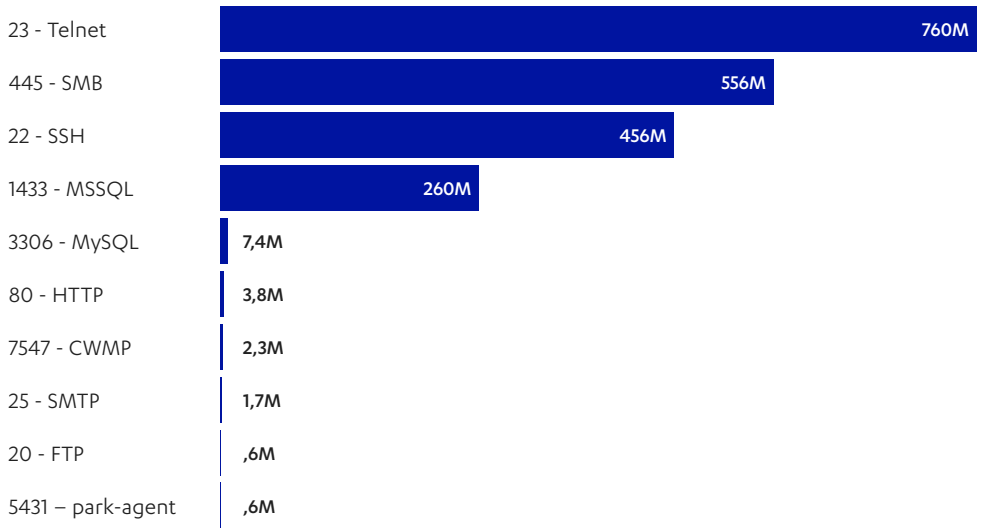
Of the 2.9 billion hits, 2.1 billion were on TCP ports. Telnet, which is rarely used anymore outside the realm of IoT devices, saw the greatest volumes during the period. Due to the continuing spread of infected IoT devices perpetrated by malware such as Mirai, Telnet continues the run it began in the last half of 2018. The greatest share of Telnet traffic came from the US IP space, followed by Germany, UK and the Netherlands.

Traffic to port 445 was the next most prevalent, representing SMB worms and exploits such as Eternal Blue. Since its debut during WannaCry over two years ago, Eternal Blue continues to be used by criminals, and it's currently at the height of its popularity.[6] Data from our malware labs backs this up, as WannaCry is currently one of the most prevalent forms of malware in our telemetry. China was the biggest source of SMB traffic, followed by the Philippines and Russia.

Attacks on SSH port 22 came in third, representing brute force password attempts to gain remote access to a machine, but also IoT malware, which uses SSH as well. Russia was by far the biggest aggressor when it comes to SSH traffic.

Traffic to SQL-related ports represent database attacks such as are common in data breaches. But more recently in a new trend, attacks are also targeting the server with cryptomining bots[7] or even ransomware.[8] China was by far the most active country targeting these ports.

Top TCP Ports Targeted

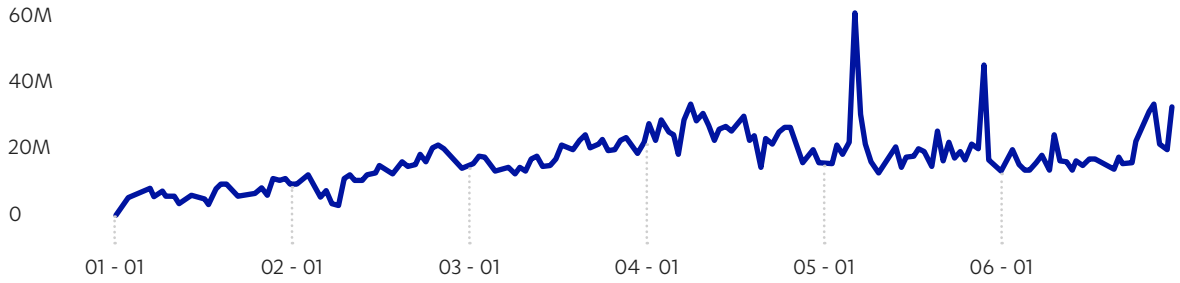


6. https://www.welivesecurity.com/2019/05/17/eternalblue-new-heights-wannacryptor/
7. https://news.sophos.com/en-us/2019/04/30/a-taste-of-the-onslaught-at-the-networks-edge/
8. https://www.zdnet.com/article/hackers-are-scanning-for-mysql-servers-to-deploy-gandcrab-ransomware/

Apart from TCP traffic, the majority of the remaining traffic was to UPD port 1900, with 611 million hits. 1900 is commonly used for scanning to determine if the target is running UPnP, or plug-and-play devices, which are used for exploitation or in DDoS attacks. (TCP port 5431 is one of the UPnP service ports.) The heaviest traffic on 1900 came from the IP spaces of China, the US, Australia and Brazil.

Top 5 UDP Ports Targeted

Attack volumes throughout the period

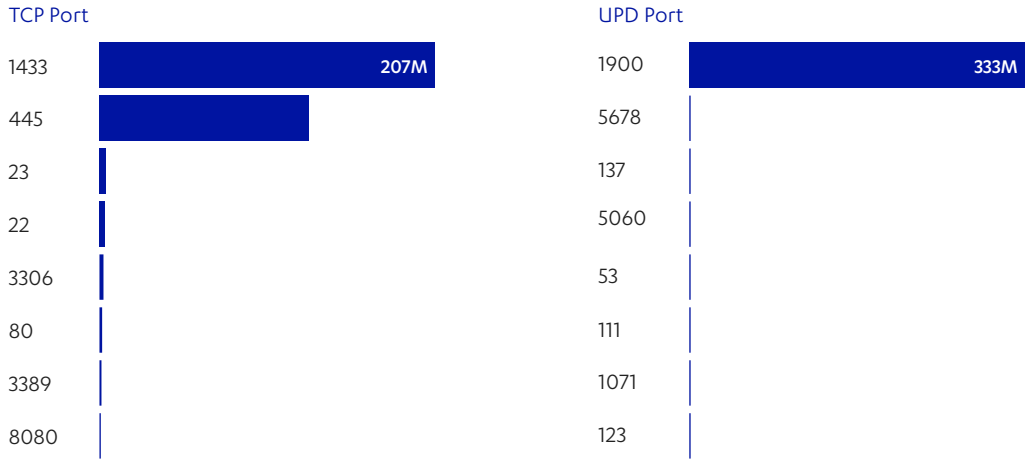


The graph above shows all activity on all ports throughout the period. The peaks on May 7 and May 29 are due to strong campaigns targeting UDP 1900. The May 7 campaign, which came from the Australian IP space, hit several countries hard, most prominently Austria, Italy and Ukraine, but also the United Kingdom, Germany, France and India. The May 29 campaign came from the Chinese IP space and hit Austria, the UK, US and Ukraine most prominently.

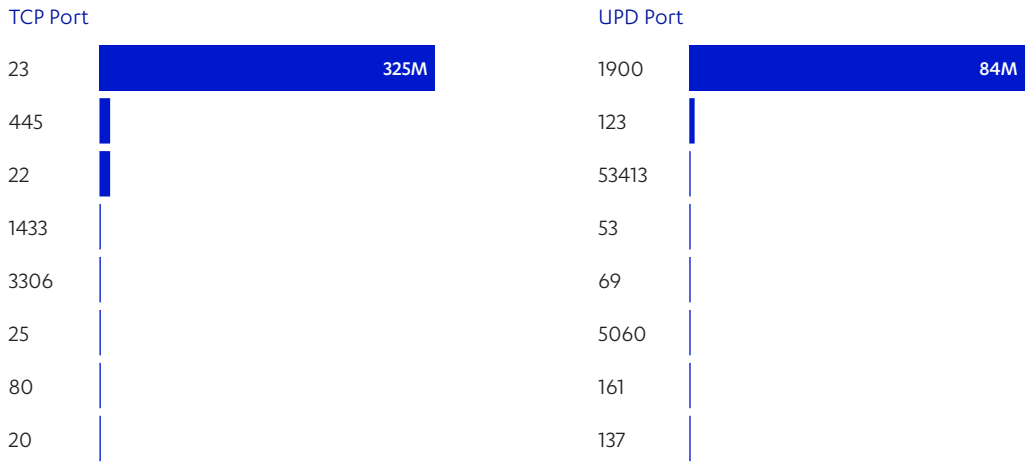
Breaking down the most common ports targeted by the top three attack source countries, it's apparent that attackers in all three countries' IP spaces actively targeted the IoT. On the TCP side, attackers using the US and Russian IP spaces heavily targeted ports 22 (SSH) and 23 (Telnet). On UDP, attacks from the Chinese IP space directed at port 1900 were likely attempts to attack a vulnerability common on D-Link routers.

Ports most commonly targeted by top 3 attack source countries

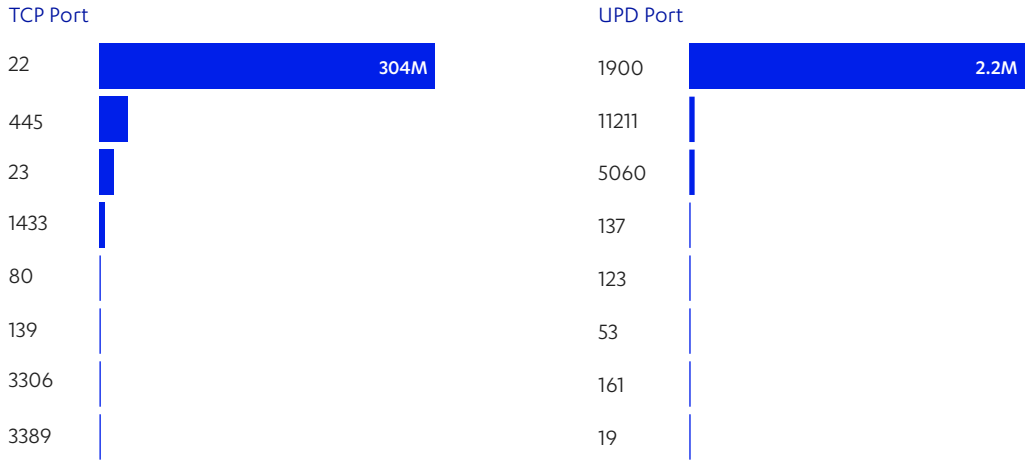
CHINA



US



RUSSIA



MALWARE

Malware found in the honeypots is dominated by various versions of Mirai, which is still going strong three years after it first burst onto the scene in 2016. Mirai targets IoT devices such as IP cameras and routers, infects those using default credentials, and co-opts them into botnet armies.

In a new trend that should concern every business, Mirai has recently spawned variants that are specifically engineered to infect enterprise IoT[9] devices such as wireless presentation systems and digital signage TVs. The expansion to enterprise allows attackers access to greater bandwidth connections than are available with consumer devices, affording them greater power for DDoS attacks.

Visualization of the top malware variants found in honeypots

Turning away from honeypots to the actual customer endpoints we protect, the main types of malware we see are still ransomware, banking trojans, and cryptominers.

We've seen some evolving trends in the malware sphere in the first half of the year. First, while ZIP, PDF, DOC and XLS files are the most commonly used attachment type for spreading malware, we've noted[10] an increasingly popular trend of attackers employing disc image files (ISO and IMG). Campaigns using this technique delivered the AgentTesla infostealer and the NanoCore RAT.

9. https://www.scmagazine.com/home/security-news/cybercrime/the-infamous-mirai-malware-has-grown-into-more-than-60-known-variants-and-has-since-set-its-sights-on-enterprise-devices/
10. https://labsblog.f-secure.com/2019/05/08/spam-trends-top-attachments-and-campaigns/

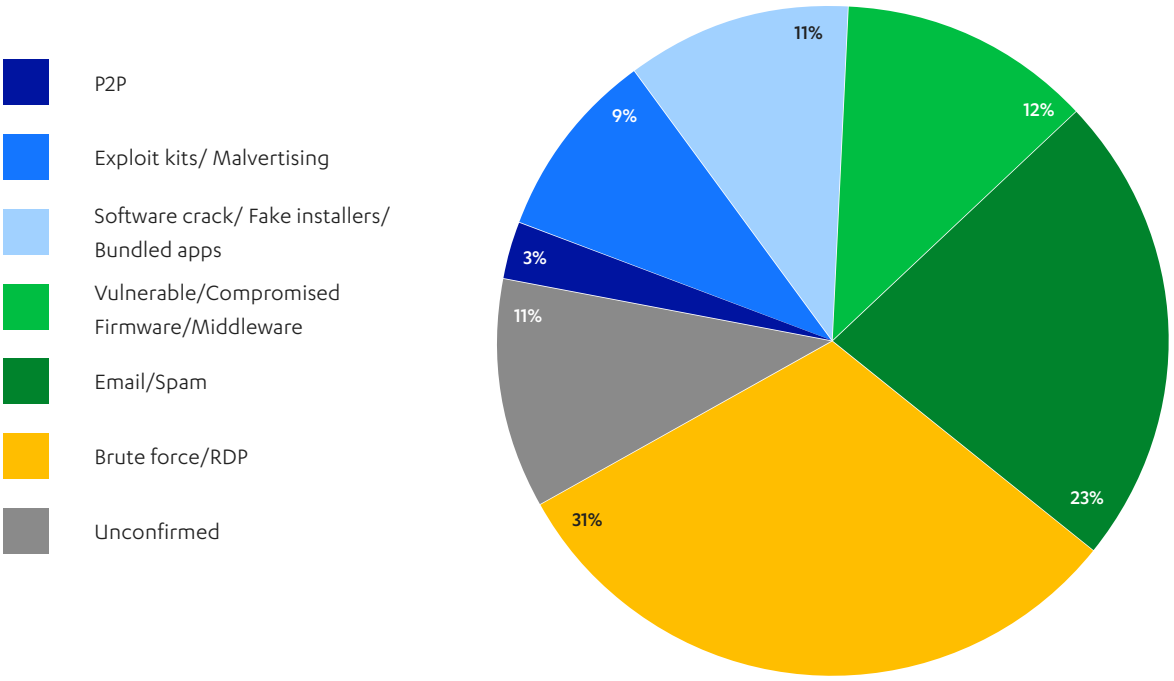
We've also observed a trend of financially motivated attackers abusing the trust users put in the digital certificate system by purchasing certificates to sign their executable files.[11] Traditionally this sort of tactic has been limited to the toolbelt of nation states and other highly advanced attackers. It's just another example of the trickle down in TTPs from the elites down to the common criminals.

With lower prices of Bitcoin and the shutdown of CoinHive in March, cryptomining appeared to be on the way out. But recent increases in Bitcoin and other currencies following suit seem to have prompted a revival in cryptomining. Security researchers are seeing cases of Eternal Blue being used to escort in XMRig, a Monero miner, as well as mining infections in Android devices in Asia, among other clues.

After an apparent lull in 2018, ransomware is back and has been busy disrupting companies, public entities and other organizations over the past several months. Some of the most notable attacks involved aluminum producer Norsk Hydro,[12] who lost over $35 million in the first week after being hit by LockerGaga in March, and global forensic testing provider Eurofins Scientific, whose compromise in June affected police work.[13]

The chart below shows the variety of methods by which threat actors distributed ransomware during the period. The infection vector used by the greatest share of ransomware families was RDP at 31%, underscoring the trend of cyber criminals putting more energy into infecting companies. Email spam was second with 31%; an example is the February and March spam campaigns we noticed[14] which used ZIP files passed off as photos to deliver GranCrab ransomware.

Ransomware distribution methods (January-May 2019)



11. https://www.bleepingcomputer.com/news/security/volume-of-signed-malware-increases-cas-need-better-vetting/
12. https://www.securityweek.com/ransomware-attack-costs-norsk-hydro-tens-millions-dollars
13. https://www.helpnetsecurity.com/2019/06/24/eurofins-ransomware-attack/
14. https://labsblog.f-secure.com/2019/05/08/spam-trends-top-attachments-and-campaigns/

CONCLUSION

Every half year it's a different story. This time, it's the jump to billions of honeypot attacks, the rampant exploitation of IoT devices via Telnet and UPnP, China's domination of traffic, a comeback in ransomware and a rally of cryptominers. The attacks may change, the methods may change and the vulnerabilities may change, but what doesn't change is that following solid security practices and procedures will keep your business on much safer ground.

- Map your attack surface. Know what devices and servers you have and why they're needed. Retire old assets that aren't necessary.
- Know what you need to protect most, and guard it. Keep your most critical assets protected with a higher level of security.
- Keep your systems and applications updated with current software and security patches.
- Be skeptical of unsolicited, unexpected emails and especially of links or attachments in them.
- Enforce a password policy of changing default passwords to unique, long and strong passwords, and of never reusing passwords. Encourage employees to use password managers.
- Monitor your network with detection and response technology to catch malicious actors already in the network.

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