Short Notes

a) Formjacking

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

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

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

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

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

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

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

b) Cryptojacking

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

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

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

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

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

c) Ransomware

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

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

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

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

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

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

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

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

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

d) Living off the Land, and Supply Chain attacks

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

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

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

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

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

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

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

e) The rise of Targeted Attacks

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

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

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

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

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

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

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

One of the most dramatic developments during 2018 was the significant increase in indictments in the United States against people alleged to be involved in state-sponsored espionage. Forty-nine individuals or organizations were indicted during 2018, up from four in 2017 and five in 2016. While most of the headlines were devoted to the indictment of 18 alleged Russian agents, most of whom

were charged with involvement in attacks relating to the 2016 presidential election, the indictments were far more wide ranging. Alongside Russian nationals, 19 Chinese individuals or organizations were charged, along with 11 Iranians, and one North Korean.

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

f) Security Challenges of Cloud

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

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

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

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

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

g) IoT Attacks

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

The overall volume of IoT attacks remained high in 2018 and consistent (-0.2 percent) compared to 2017. Routers and connected cameras were the most infected devices and accounted for 75 and 15

percent of the attacks respectively. It's unsurprising that routers were the most targeted devices given their accessibility from the internet. They're also attractive as they provide an effective jumping-off point for attackers.

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

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

h) Election Interference 2018

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

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

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

Adversaries continued to focus on using social media platforms to influence voters in 2018. While this is nothing new, the tactics used have become more sophisticated. Some Russia-linked accounts,

for example, used third parties to purchase social media ads for them and avoided using Russian IP addresses or Russian currency. Fake accounts also began to focus more on promoting events and rallies, which are not monitored as closely as politically targeted ads.

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

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

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