Integrity360
your security in mind

CYBER SECURITY RISK RADAR

APRIL 2018

CONTENT

1 Executive summary

2 New year, new hardware vulnerabilities and threats

3 GitHub hit with biggest DDoS attack ever reported

4 Modern-day gold rush: Cryptojacking goes mainstream

5 Fileless attacks get a boost from PowerShell

6 Cross-site scripting continues to call for patching

7 MacOS loses its reputation as impenetrable fortress

8 Quarterly report spotlight: ENISA

Executive summary

The first fiscal quarter of 2018 has drawn to a close, but not without leaving a trail of cyber security risks in its wake. Here's a brief summary of them all:

- ✓ **Meltdown and Spectre vulnerabilities** continue to garner headlines as Microsoft and Intel work to patch remaining exploits.
- ✓ GitHub was hit with the **biggest DDoS attack** ever reported, yet managed to successfully recover in just 20 minutes.
- ✓ Hackers are increasingly latching onto **cryptojacking through all means**—software, fileless and browser plugins—as a way to monetise their efforts without having to pay for their mining operation.
- ✓ **Fileless attacks hit** the Winter Olympics in South Korea, underscoring the danger of the authentic programs that can conceal malicious activity.
- ✓ **Cross-site scripting** was one of the most common vulnerabilities among the 1,002 recorded vulnerabilities in the first annual Integrity360 2018 Penetration Testing Report.
- ✓ The perception that macOS users don't have to worry about cyber threats has turned into a misconception, as researchers have recently seen an **uptick in malware designed for the operating system**.

Let's take a closer look at the developments that cyber security analysts should monitor throughout 2018.

New year, new hardware vulnerabilities and threats

The common vulnerabilities and exposures (CVEs) dubbed Meltdown and Spectre were revealed in early January 2018, and dominated news headlines. The idea that a kernel could be manipulated to deliver real data from a device has led to a number of patches from Microsoft and Intel as they try to solve the problem.

Total Meltdown, a vulnerability stemming from a patch for Meltdown, was discovered in late March. It affected all devices running Windows 7 and Windows Server 2008 R2, and points to the challenge these two problems represent.

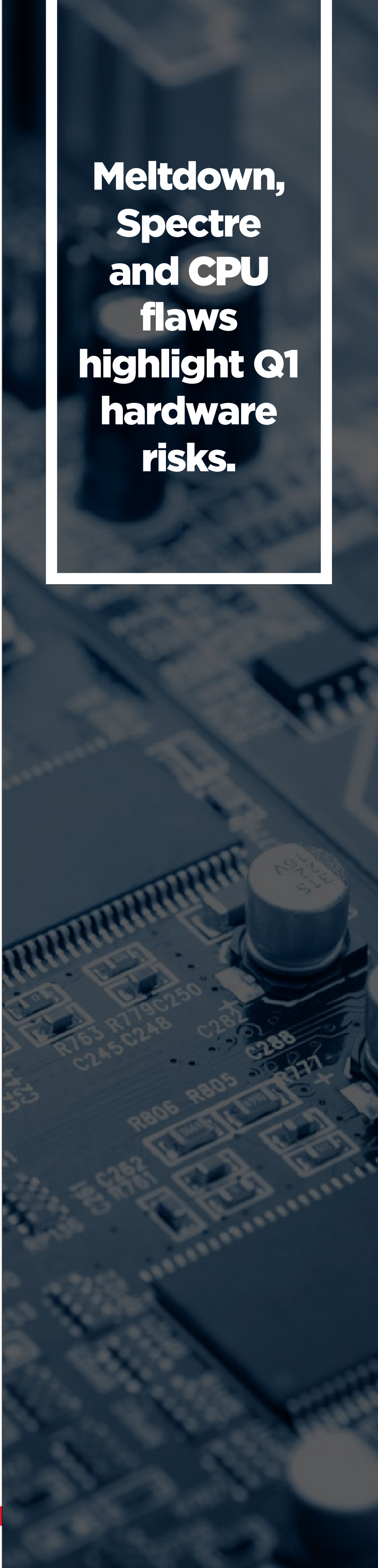
In March 2018, it was announced that flaws were found in processing chips that could potentially allow hackers to manipulate the devices they power.

360 Insight

The risks point to the fact that sophisticated hacking groups could leverage the exploits as they become more common.

One vector that attackers use to exploit these vulnerabilities is virtualised hardware, which can give them total access. Patching regularly, as well as applying emergency patches, can help mitigate exposure.

IT departments must be aware of any CVEs involving devices in use by the workforce, and adjust cyber security policies accordingly.



Meltdown, Spectre and CPU flaws highlight Q1 hardware risks.

GitHub hit with biggest DDoS attack ever reported

The popular software development platform, GitHub, suffered a massive distributed denial of service attack on February 28, 2018. Hackers sent an average of 1.35 terabits per second (Tbps) of traffic to the website.

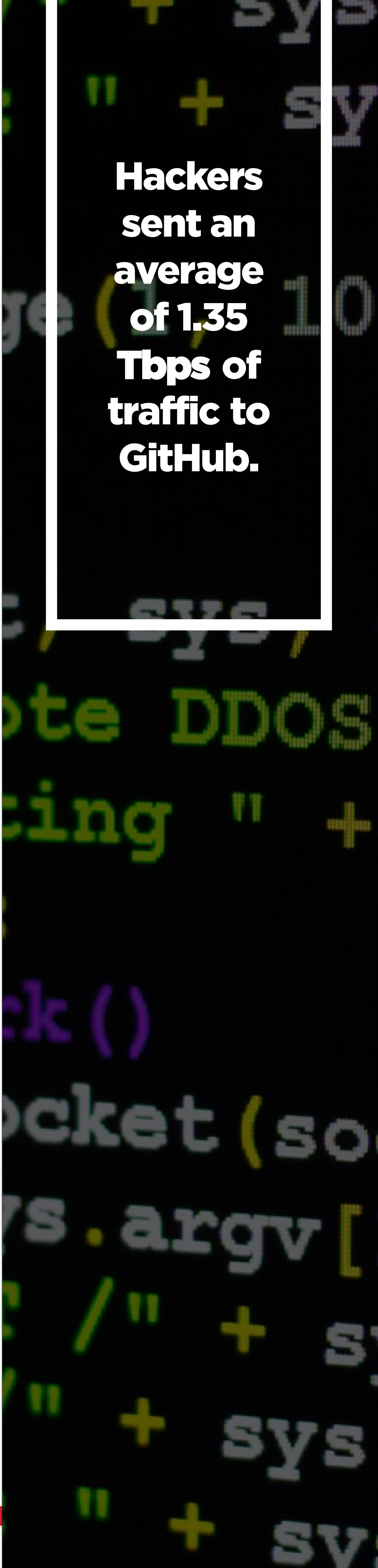
Days later, a 1.7 Tbps reflection/amplification attack targeted a customer of a US based Service Provider based on the same attack vector that made up the Github attack.

GitHub was able to resolve the situation in less than 20 minutes thanks to the DDoS mitigation platform it had in place, while the 1.7 Tbps attack on the Service Provider customer reported no outages. This successful remediation is a sign of the tremendous shift in opinion on cyber security strategies over the past two years.

360 Insight

These DDoS attacks were a result of exploited vulnerabilities found in Memcached servers. They allowed the hackers to manipulate packet commands sent to unprotected memory caching systems in a way that returned massive sets of data to the company's website.

The scale of the attacks could easily bring down vulnerable networks. Ensure that your DDoS protection service level agreement explicitly states how quick the platform can respond to attacks to mitigate negative impacts, such as service disruption for clients. Every minute your website is down may have a Financial and reputational cost attached to it.



Hackers sent an average of 1.35 Tbps of traffic to GitHub.

Modern-day gold rush: Cryptojacking goes mainstream

Rising exchange rates for cryptocurrencies like Bitcoin have pushed cryptojacking to the forefront of hackers' favourite methodologies. As the spotlight on ransomware brightens grows—and an unwillingness to pay cybercriminals develops—hackers are turning to cryptojacking as a way to slip into networks undetected and still generate a financial profit from their activities. They accomplish this through fileless attacks, ransomware and infected browser extensions.

An average of 644,000 devices unknowingly hosted the software programs each month between September 2017 and January 2018, according to Microsoft. A single attack on March 6, 2018, saw a program named Dofoil infect over 500,000 computers in less than 12 hours. It was only discovered in February that one hacker successfully mined over $3 million in a digital currency called Monero after being undetected on Jenkins servers for 18 months.

360 Insight

Cryptojacking presents both internal and external risks. If you find cryptominers on your network, you should be concerned that they were able to infiltrate it in the first place. Similarly, employees have been found mining the cryptocurrencies through their corporate PC, which can leave the company with elevated electricity bills and create further vulnerabilities on the network.

Cyber security analysts should continue to monitor their networks in real-time and build a whitelist for known software programs so that they can quickly identify and isolate cryptojacking software.

Dofoil infected over 500,000 computers in less than 12 hours.

Fileless attacks get a boost from PowerShell

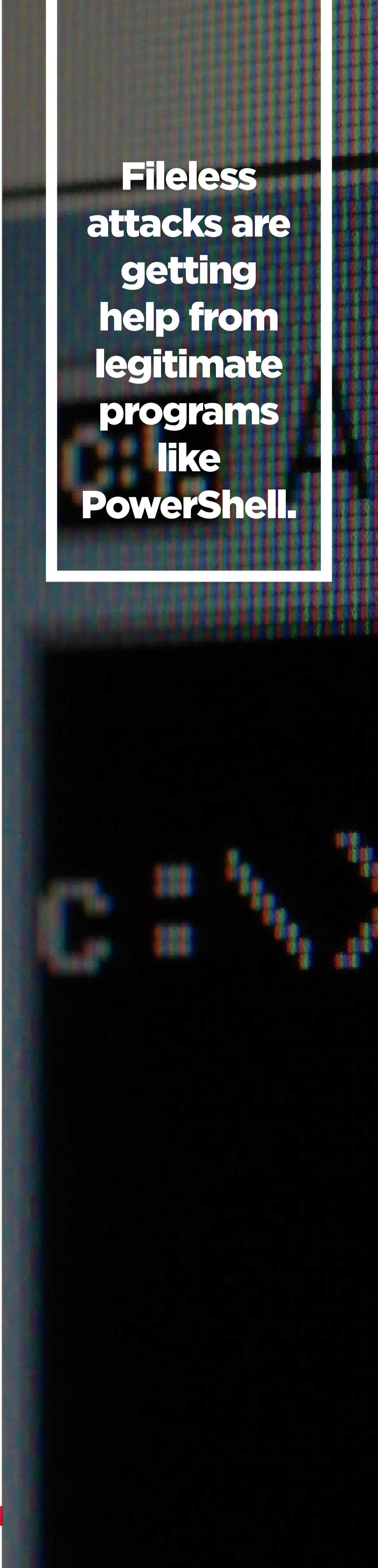
The popularity of fileless attacks has resulted in an uptick in frequency in 2018. A growing number of hackers are turning to PowerShell, the task automation scripting tool from Microsoft, to carry out their actions while hiding behind the guise of legitimate actions.

In February, 2018, Olympic officials reported that a cyber attack hit the Winter Olympics' opening ceremony in Pyeongchang, South Korea, Reuters reported. It was later revealed that hackers leveraged PowerShell to carry out the attack, which impacted the organisation's website and WiFi access that it had set up in the area.

360 Insight

Malicious activity concealed by authentic programs can be detrimental to companies that rely on signature-based detection mechanisms as hackers are able to easily modify their attack to bypass traditional security protocols.

Real-time analysis through a security information and event management platform will be a staple of high-performing security information and event management (SIEM) platform moving forward. It provides the visibility necessary to correlate potentially dangerous behaviour with common vulnerabilities and exposures.



Fileless attacks are getting help from legitimate programs like PowerShell.

Cross-site scripting continues to call for patching

Integrity360 penetration testers found cross-site scripting to be the second most common vulnerability among clients in 2017, just behind multiple SSL vulnerabilities.

Developers like Adobe, Drupal and Microsoft have all released new patches as recently as March, 2018, with the hopes to mitigate exposure. Although threat-level severity concerning cross-site scripting hovers around low- to moderate-risk, the fact that it's always on their radar shows its pervasiveness as a challenge for cyber security professionals.

360 Insight

Hackers use cross-site scripting to target organisations with simple or no defense mechanisms in place. These are commonly companies in the healthcare and financial industries, where some businesses only seek to meet compliance.

Regular penetration testing, as well as threat and vulnerability assessments, can help enterprises ensure their website won't contribute to a data breach through cross-site scripting.

Cross-site scripting was the second most common vulnerability found in our penetration tests

MacOS loses its reputation as impenetrable fortress

In the past, Mac computer users haven't had to watch out for too many potential threats. In 2018 that's turning into a misconception—attacks on the operating system increased by roughly 270 percent in 2017, according to Malwarebytes. At least four new exploits have been discovered so far in Q1.

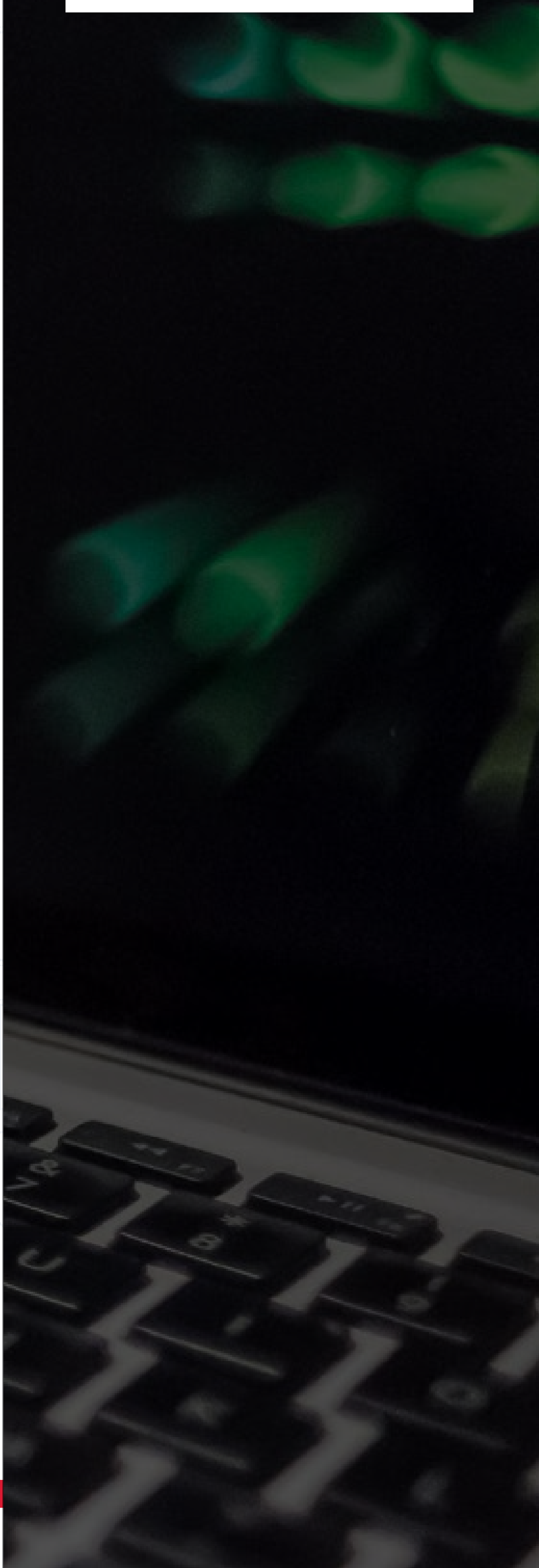
Coldroot, a remote-access Trojan, was recently identified as a threat to Mac users in February, 2018. It's inherently limited as it needs accessibility rights to perform malicious activities on a wide scale, but it was still able to function as a hidden keylogger on many devices for nearly two years.

360 Insight

Companies with a limited number of Mac users may have turned a blind eye on their activities to support other critical areas of the business, but this shouldn't be the case moving forward.

MacOS should be incorporated into formal cyber security policies if it isn't already; it's an overlooked endpoint that can allow a hacker free entry to cause havoc on the network. Schedule macOS build reviews to coincide with penetration testing services that will explicitly seek out vulnerabilities with the devices on your network.

Attacks on Mac computers increased 270 percent in 2017.



Quarterly report spotlight: ENISA

There's never a dull moment in the cyber security industry, and the reason behind that is the great work being done behind the scenes to bring important issues to the public spotlight.

You won't want to miss the latest report on the 2017 cyber security threat landscape released by the European Union Agency for Network and Information Security (ENISA).

The report covers the most important trends and news that hit the industry in 2017, including what it views as the top 15 threats to organisations in 2018. These are:

1. Malware
2. Web-based attacks
3. Web application attacks
4. Phishing
5. Spam
6. Denial of service
7. Ransomware
8. Botnets
9. Insider threats
10. Physical manipulation/damage/theft/loss
11. Data breaches
12. Identity theft
13. Information leakage
14. Exploit kits
15. Cyber-espionage

You can find the rest of the **ENISA 2017 Threat Landscape Report here ➔**

ENISA found malware, web-based attacks and web application attacks to be the three biggest threats to companies in 2018.

HEAD OFFICE
3rd Floor, Block D, The Concourse,
Beacon Court, Sandyford, Dublin 18.
+353 (0)1 293 4027

LONDON OFFICE
90 Long Acre,
Covent Garden, London, WC2E 9RZ
+44 203 397 3414

BIRMINGHAM OFFICE
TS2 Pinewood Business Park,
Coleshill Road, Birmingham, B37 7HG
+44 203 397 3414

NEW YORK OFFICE
260 Madison Avenue, 8th Floor
Manhattan, 10016
+1-212-461-3286

Integrity360

your **security** in mind