Integrity360

your security in mind

CYBER SECURITY RISK RADAR

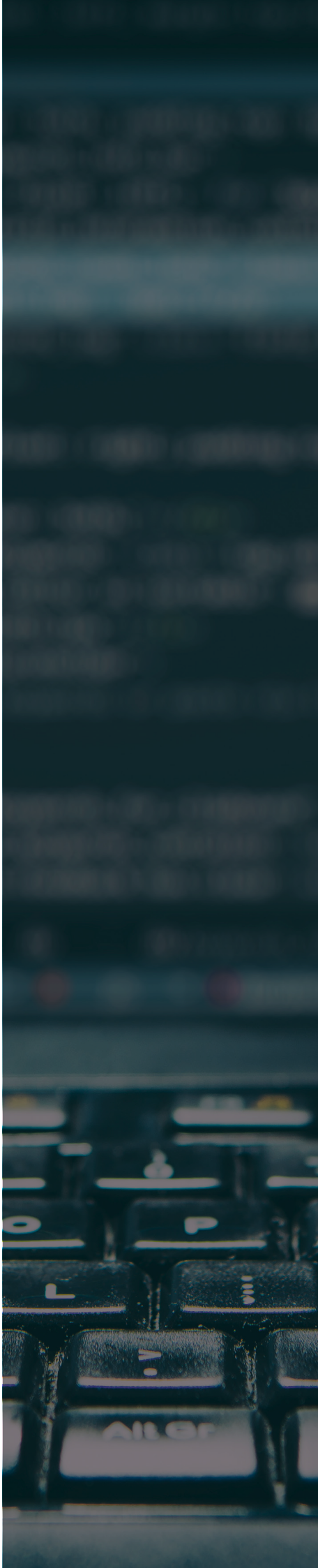
JULY 2018

CONTENT

Executive summary

The second fiscal quarter of 2018 is in the books, and the cyber security industry has a lot to learn from. Here's a brief glance at the various risks that gained prominence over the last three months:

- **Phishing saw an uptick in frequency**, and its volume of attacks outnumbered malware 21:1 over the past three months.
- You'd better believe that **pretexting is on the rise** – analysts saw a 183 percent jump in reported incidents over the past year.
- **Meltdown and Spectre vulnerabilities** have re-entered the spotlight as Variant 4, the latest iteration of the exploit, was discovered and patched by Intel researchers.
- Employees are continuing to use their **personal online passwords** for business accounts, ignoring the risks that are associated with it.
- **The Orangeworm hacking group** is taking advantage of healthcare organisations by targeting their outdated operating systems and cyber security defences.
- A major **DDoS-for-hire** website has been shut down, but many more still exist.
- **SamSam ransomware** takes the road less travelled to distribution by deploying hundreds or thousands of iterations of its code after infiltrating a network.



Executive summary

- Well known cyber-crime groups have been using **advanced persistent threats** to target enterprise smartphones.
- **Roaming Mantis malware** is an emerging threat for mobile devices across EMEA and Asia, but it's gaining most of its notoriety for its creators' fast-paced expansions of the code.
- **Gandcrab creators have shown a knack** for overcoming patches by quickly rewriting its malicious code.
- **Continuous threat management** became a rewarding venture for one company, as Twitter unveiled and patched an exploit before hackers got a chance.
- **Google is changing its policy** to only alert users of unsecure websites, marking the final transformation of HTTPS from a luxury to a standard.
- **A zero-day exploit named Double Kill** is making its way into crimeware kits, just as companies are losing interest in patching.
- **The Hide and Seek IoT botnet** has been identified as the first IoT botnet that isn't removed from a host after a system reboot.
- The Wi-Fi Alliance announced that **new WPA3 features will be released** by the end of 2018.

Integrity360
your **security** in mind

Hackers go phishing across international waters

The first quarter of 2018 saw a massive influx in phishing attacks, including the discovery of a campaign that targeted over 550 million individuals across the world.

The prevalence of the attacks, which were discovered by analysts at Vade Secure, outnumbered malware 21:1 over the last three months and were spread across the U.S. and most of Europe.

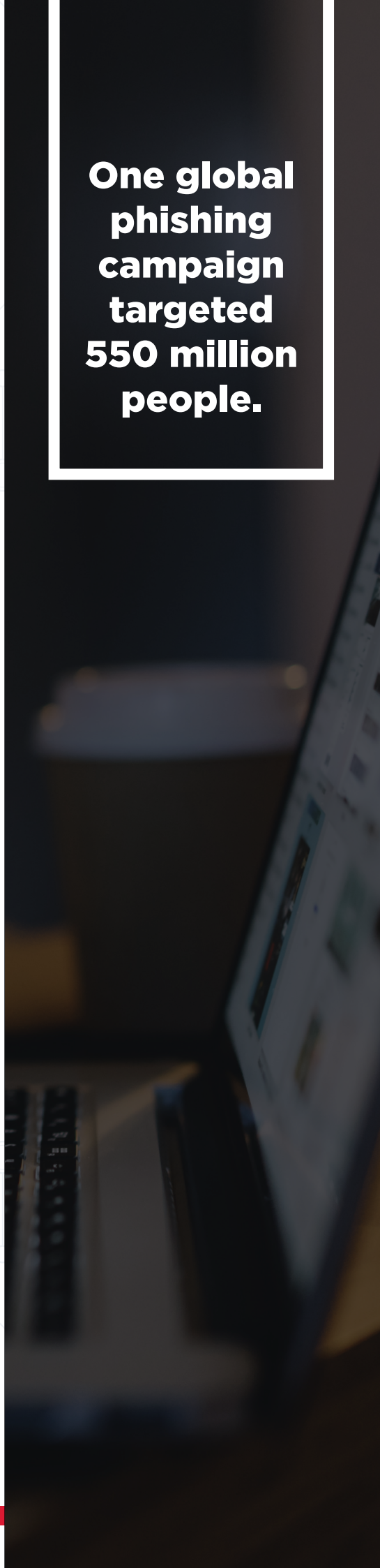
The scale of the ongoing attack has the trademark of being financed by a large criminal organisation. The campaign is taking the form of coupons and quizzes in emails, where threat actors then include shortened URLs that are designed to steal banking information.

360 Insight

Phishing is a low-risk, high-reward opportunity for threat actors that's comparable to a thief in a carpark – he or she is just trying to find out which vehicles are unlocked.

Ensure the proper email and web filters are in place, as well as an advanced firewall. Continue to change staff training over time to represent the most pertinent and immediate threats they'll need to keep an eye out for.

One global phishing campaign targeted 550 million people.

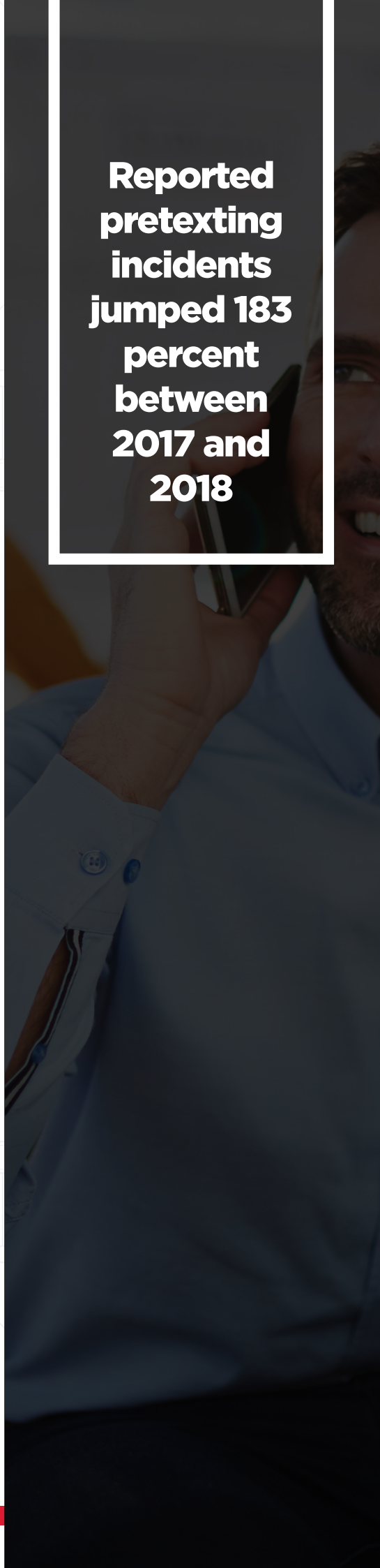


Trust us, pretexting is on the rise

Pretexting is a form of phishing that has been in the spotlight in recent years. It relies less on mass-distributed malware, and instead focuses on gaining a social foothold within specific areas of the organisation – namely the finance or human resources department. This allows threat actors to orchestrate corporate wire transfers while posing as a high-ranking executive.

There was an increase of 61 to 170 reported incidents of pretexting between 2017 and 2018, according to Verizon's 2018 Data Breach Investigations Report. It's possible there were more that went unreported, considering some organisations may not view pretexting as a traditional form of hacking.

Reported pretexting incidents jumped 183 percent between 2017 and 2018



360 Insight

Pretexting uses social engineering to gain the level of access they need to manipulate funds. There is no digital solution to this; only good old, common sense.

Red Team exercises can help your business understand its vulnerability points beyond the traditional security infrastructure. It could be a willingness to reply to an email, to pay a wire transfer, or to open a door into the building for someone waiting outside. These are seemingly innocuous instances that can have a devastating financial and reputational toll.

Meltdown and Spectre re-enter vulnerability spotlight

Meltdown and Spectre quickly became household names as the scope of the Common Vulnerabilities and Exposures (CVE) extended to a broad portion of the world. Now, Intel and Microsoft researchers have revealed there's another vulnerability.

The new iteration is being dubbed Variant 4, and it represents the same security risks that Spectre and Meltdown had – namely, giving hackers the ability to extract sensitive information. The only difference with Variant 4 is that criminals use another methodology, known as Speculative Store Bypass, to accomplish that task.

Variant 4 carries the same risks as Meltdown and Spectre.

360 Insight

Variant 4 hasn't been used so far, according to Intel cyber security experts. The company released a patch for the vulnerability in June, and it's only expected to affect computer performance slightly.

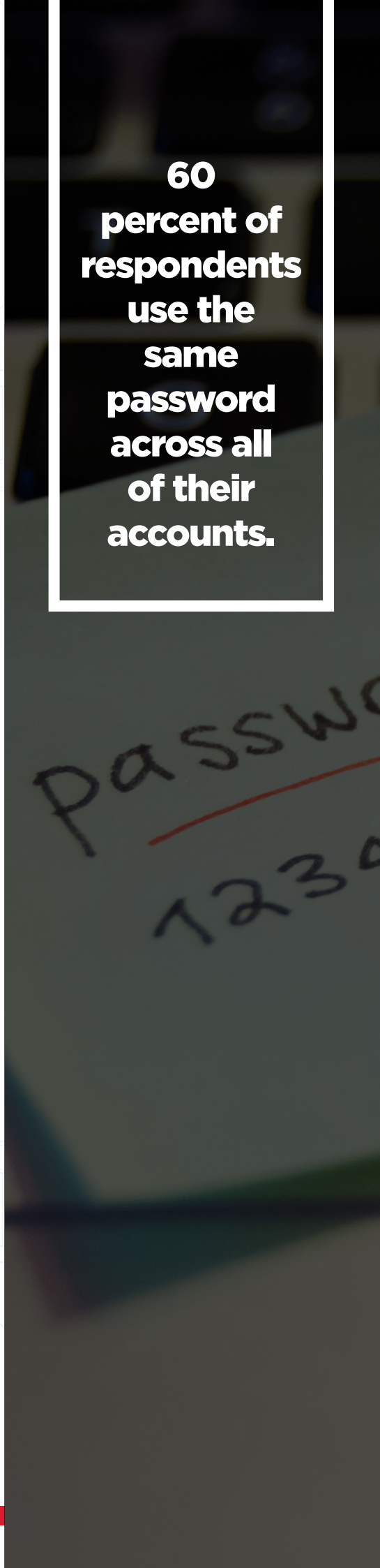
Spectre, Meltdown and now Variant 4 all carry various levels of cyber risk. But patching the systems as soon as updates are available can negate the vulnerabilities. It's a simple solution that many companies continue to overlook.

Weak passwords still a top concern

Weak passwords have been a concern as long as the internet has been around, and a new survey by LogMeIn shows that not much has changed. Although nine in every 10 global respondents acknowledge the danger in using the same password across all their accounts, roughly six in 10 admit to doing so regardless.

Just 20 percent of those polled have created secure passwords for work that are separate from their personal accounts. This is an issue given that almost 80 percent of respondents have between one and 20 personal and work accounts combined. Furthermore, a little over half of the respondents didn't change their password once over the last year.

60 percent of respondents use the same password across all of their accounts.



360 Insight

Bad password management stems from poor – or a complete lack of – cyber security policies. These weak configurations give social engineering specialists an easy access point to high value assets, which can result in a data breach.

Work with cyber risk and assurance (CRA) advisors to identify gaps in your current policies and procedures. Furthermore, user behaviour analytics that are paired with machine learning algorithms can detect compromised accounts in real-time before malicious threat actors have a chance to gain a foothold in the network.

Orangeworm group targeting legacy system users

An aggressive hacking group, Orangeworm, has been found to primarily target healthcare, manufacturing, IT and logistics organisations. The group uses Trojan. Kwampirs to enter a backdoor on victims' security infrastructures, taking over mission-critical systems and pulling healthcare records.

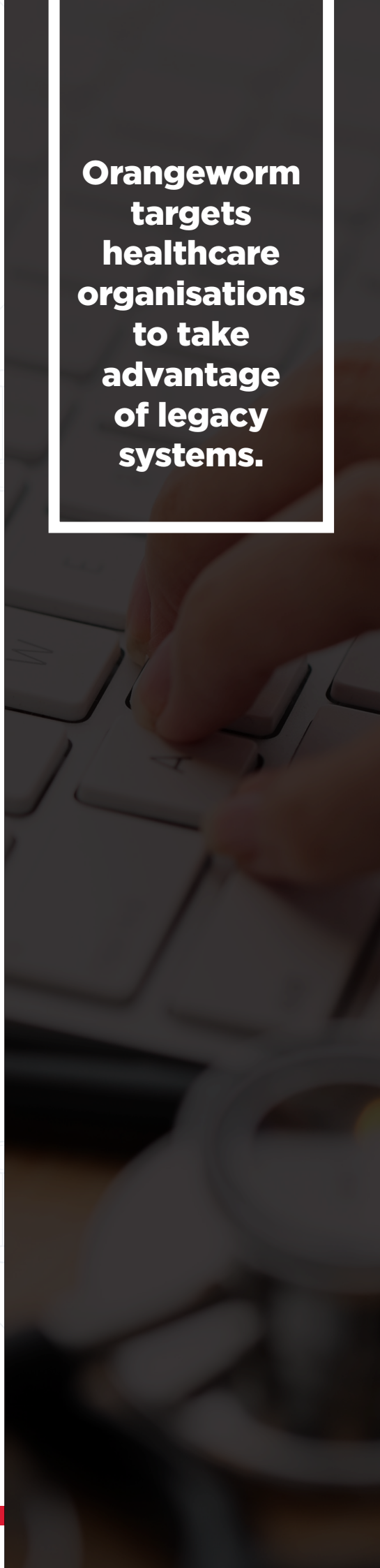
It's an attack that's simple to detect, which is why the hackers are going after targets who have outdated systems in place, according to Symantec. This has put healthcare most at risk, given that many locations still employ the help of older Windows operating systems in some capacity.

360 Insight

Orangeworm represents the crux of the argument for investing in modern cyber security tools. It's easily identifiable with an IPS or sandbox, and simply having them in place is enough to protect the organisation.

Expect these types of straightforward attempts to continue to be popular moving forward. Where devastating attacks may cripple unprepared businesses, companies that have taken the proper precautions will see the majority of vulnerabilities 'bounce off' their security infrastructure.

Orangeworm targets healthcare organisations to take advantage of legacy systems.



DDoS-for-hire website hits unemployment – for now

The gig economy is in full swing, but it's not just limited to Uber or freelance graphic designers. WebStresser, which sold Distributed Denial of Service (DDoS) attacks to over 136,000 users, was shut down by Europol after facilitating 6 million attacks over the last three years.

The platform was regarded as one of the most popular providers of DDoS services, and it also allowed customers access to the DDoS tool itself. Its takedown is expected to significantly reduce the amount of attacks across the world, but its existence poses a question – how many more of these types of providers are out there?

WebStresser launched 6 million attacks in three years.

360 Insight

Hackers-for-hire aren't a new concept, but giving any random internet user the capability to unleash a devastating cyber-attack on a target certainly is. It's indicative of the dangerous digital environment that people and organisations currently find themselves in.

Given how popular these tools are becoming, it's wise to have an explicit service level agreement for your DDoS protection as to how quickly your website can respond to these attacks. Furthermore, ensure all basic cyber security defence mechanisms are in place to defend against simple attempts.

SamSam gets creative with payload distribution

Ransomware continues to be a tool of choice for hackers, as it rounded out the top five most utilised data breach techniques in 2017, Verizon reported. SamSam is a form of ransomware that has recently entered the spotlight for its success in getting victims – mainly in the healthcare sector – to pay up.

Cybercriminals use one of two methods to deploy SamSam: exploiting network vulnerabilities, or brute-force password cracking. But instead of sending the same file to numerous targets, hackers create hundreds or thousands of iterations to deploy within one organisation. This allows them to overwhelm businesses with weak security strategies, coercing them into paying for its removal.

SamSam is deployed through thousands of iterations within one business.

360 Insight

SamSam has been a highly effective version of ransomware, netting over $625,000 in Bitcoin as of April 30, SC Media reported. Hackers have been able to cleanly cover their tracks, and keep lateral movement within the network hidden to some extent.

The ransomware variant is a perfect example of why fully integrated security systems have become such a popular solution for cyber security strategies. Without full visibility into network activity and the help of machine learning to sift through the large volume of machine data, detecting advanced threats like SamSam becomes nearly impossible – and surrendering to that fact is proving to be costly.

APTs mobilise on one primary enterprise target

Advanced Persistent Threats (APTs) have been around for a little over a decade, and they're now being used to infiltrate another technology with a similar lifespan: Mobile devices at enterprises.

Smartphones have become a primary target given how much information is stored and accessed on them. Two malicious threat acting groups have been leading the front, with NSO Group securing roughly €430 million in annual software sales as a cyber-arms dealer and Dark Caracal holding targets across 38 different countries, according to Mike Murray, Vice President of Security Intelligence at Lookout.

360 Insight

It was only a matter of time until hackers decided to lock in on the one aspect of cyber security that's sometimes overlooked: mobile. APTs lie in wait, collecting information and staying hidden from detection. Failing to find them can lead to severe operational and reputational impacts.

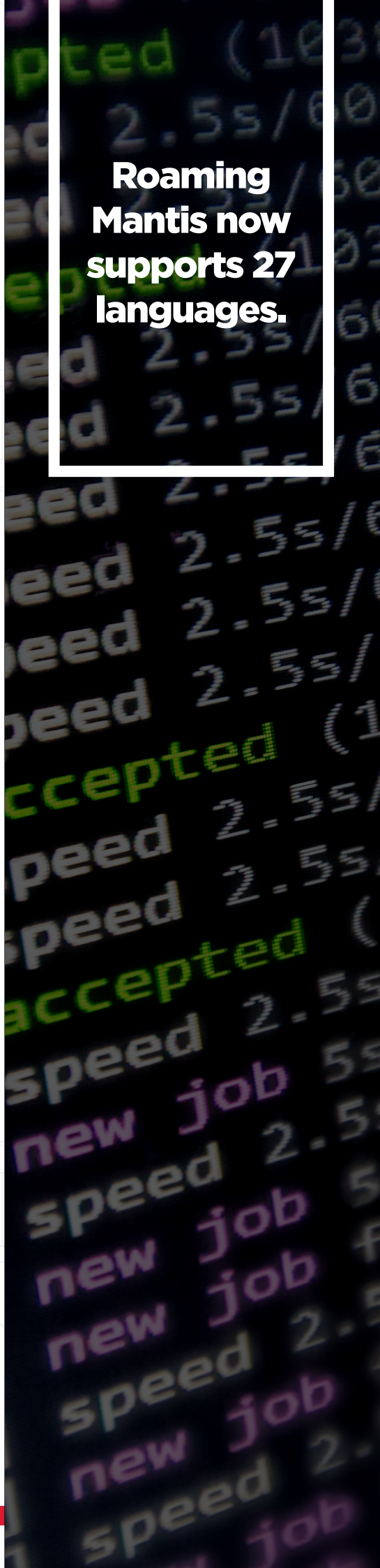
Ensure your business is utilising a mobile device management (MDM) tool, as well as mobile security software. Furthermore, event data from smartphones should be fed into and analysed by cyber security experts.

Roaming Mantis malware ramps up expansion, targets mobile users

Roaming Mantis malware first appeared on analysts' radars in April 2018, mainly targeting South East Asia through Android operating systems. Since then it has expanded to iOS users, incorporated cryptojacking and has been rewritten to support 27 different languages.

One dangerous aspect of Roaming Mantis is its ability to spread through DNS hijacking, as well as create a spoofed DNS service that directs users to a web page that steals their login credentials.

Roaming Mantis now supports 27 languages.



360 Insight

The uptick in Bring Your Own Device (BYOD) policies that allow users to access privileged data from a mobile device hasn't gone unnoticed by attackers. Smartphones are becoming an increasingly popular vector given their reliance in the average workplace.

Mobile security platforms and tools that monitor and apply controls to user access levels are a staple of any modern cyber security strategy. They cannot be forgotten in the grand scheme of things, as attackers are making the devices a primary focus.

GandCrab takes tips from agile software development

GandCrab first emerged in April 2018 and immediately found space in the industry's spotlight. This is in no small part due to its creators' ability to quickly rewrite the ransomware code to overcome the patches and kits released by security researchers.

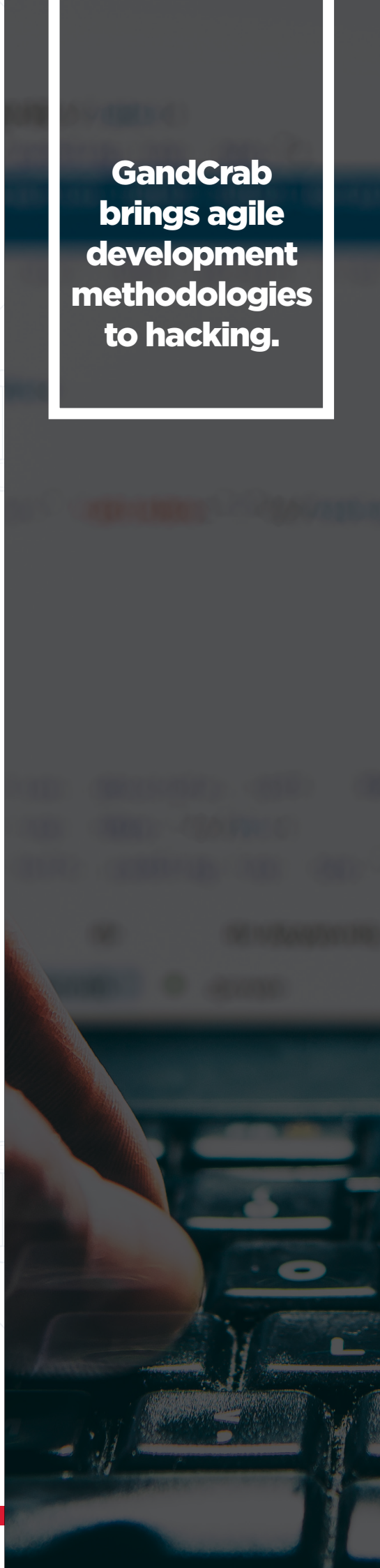
Since then it has officially entered its third iteration, though within that version it will likely be rewritten multiple times to overcome remediation. Attackers are operating as if the ransomware itself is a product, wherein analysts' patches are seen as bugs. This results in the ineffective code being rewritten and redistributed.

360 Insight

GandCrab is an example of where the methodology and techniques of cyber-attacks are heading: Agile development that enables its creators to overcome remediation. This makes it incredibly difficult to detect with legacy systems, as its signature is continuously changing.

GandCrab's third version is being distributed through the Magnitude exploit kit, and in a malspam campaign that encourages users to download a spoofed shipping order. Endpoint protection, web and email security software play key roles in preventing GandCrab attacks.

GandCrab brings agile development methodologies to hacking.



Twitter exposes its own flaw and prevents a data breach

Twitter alerted its user base in early May that an analysis of its internal logs revealed some passwords were stored in plain text. The company advised that its customers change their passwords, and noted that no known data breach had taken place.

The system flaw came from a hashing process error, which stored the passwords in their original format instead of encrypting them through a randomly assigned series of numbers and letters. Given that the company advised all users to change their passwords, the scope of the issue could be deemed as widespread.

360 Insight

Cyber security isn't a passive effort. Twitter took a proactive approach through continuous threat and vulnerability management, helping it secure its network from malicious threat actors so that they couldn't take advantage of the configuration flaw.

In doing so, Twitter avoided a data breach and the various repercussions that would have gone with it. Ensure your processes and procedures are working properly through ongoing evaluations that test their integrity, before hackers get a chance to conduct penetration tests of their own.

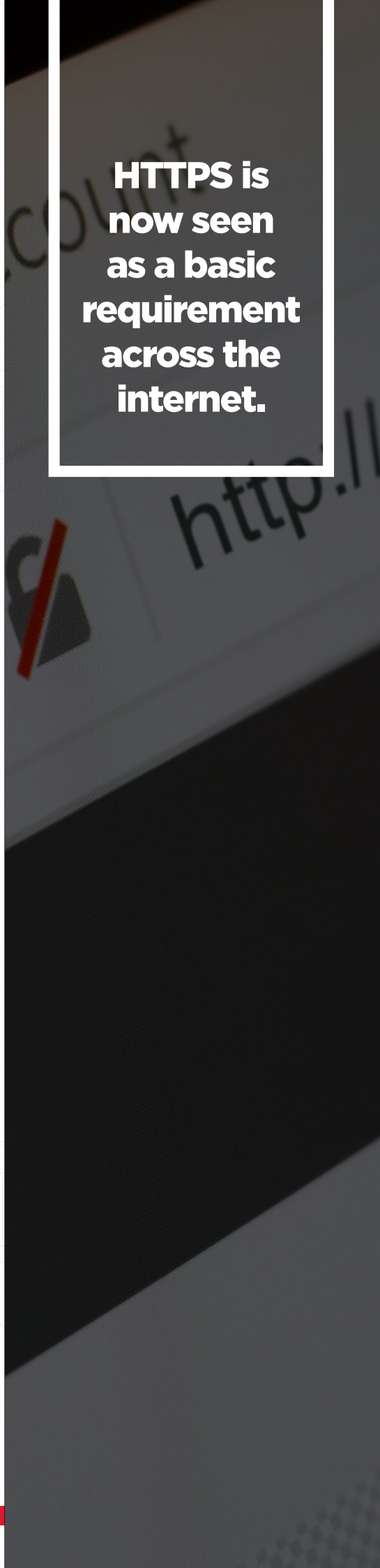
Continuous threat and vulnerability management helped Twitter avoid a data breach.

Google switches stance on secure domains

Google is changing its policy regarding the Secure Sockets Layer (SSL) protocol for HTTPS websites. Instead of marking a website as secure, the company will only alert users of unsecure domains.

The move is going live in Chrome version 69 and establishes HTTPS websites as the standard on the internet. Unencrypted websites will be flagged to users immediately upon entering the domain, shifting the view of HTTPS from a privilege to a basic requirement across the world wide web.

HTTPS is now seen as a basic requirement across the internet.



360 Insight

SSL certificates are easy to obtain and keep up to date – but that's not the story here. The conversation surrounding cyber security efforts is changing and more responsibility is placed on businesses who operate websites, especially those that capture consumers' personal information.

Unsecure domains are vulnerable to cross-site scripting and other exploits. Google's stance to move away from identifying secure websites shows that they see HTTPS as an absolute bare minimum in today's cyber security environment – and your business should too.

Windows Double Kill hits crimeware

Double Kill is a zero-day CVE that can be used to infiltrate all Windows operating systems. It was patched by Microsoft in late May, and was still frequently used at that point in time.

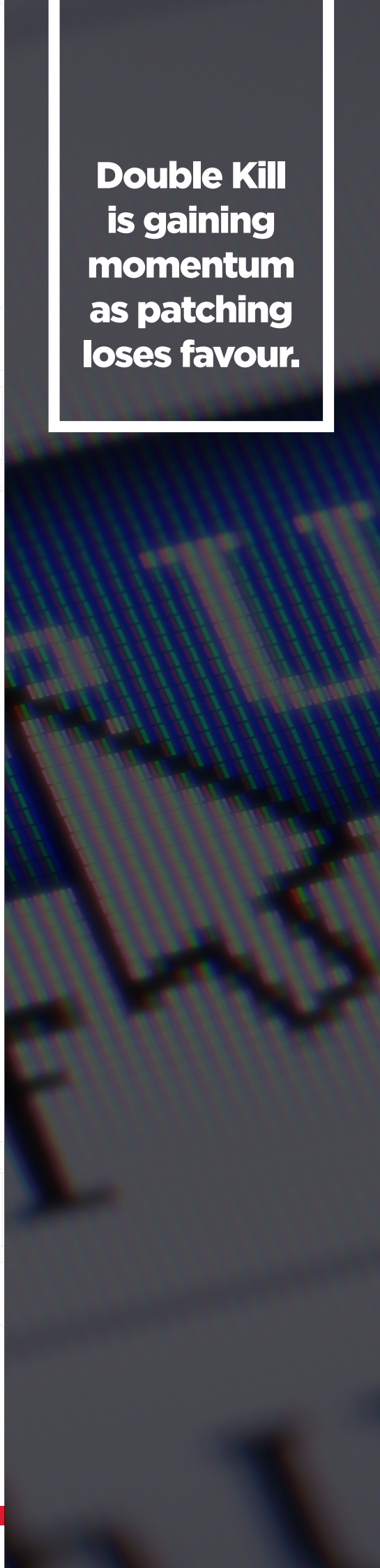
Researchers have since found the exploit in multiple crimeware kits. It allows hackers to remotely execute code, rewrite memory and gain administrative access. Unfortunately, given the arduous patching process associated with Meltdown and Spectre, the security community has seen a downtick in companies patching to the latest software version.

360 Insight

Double Kill allows threat actors near unfettered access to sensitive information, and is actively being distributed throughout the hacking community. With a Microsoft patch already released, there's no excuse to remain vulnerable to the malicious code.

Ensure your systems are up to date with the latest patching recommendations. Furthermore, evaluate how quickly your IT staff is applying these patches and develop a set schedule to upgrade the software as soon as possible.

Double Kill is gaining momentum as patching loses favour.



HNS botnet evades system restarts

Hide and Seek (HNS) is an Internet of Things (IoT) botnet that was recently discovered as the first of its kind. Bitdefender researchers found that unlike its predecessors – the Mirai DDoS botnet that struck Dyn in 2016, for instance – HNS can't be removed from a system by rebooting the IoT product.

The exact number of IoT systems HNS has exploited is unknown, but it's estimated to be in the tens of thousands. Criminals are using brute-force password cracking tactics that attack default credentials, and identifying targets through vulnerable Telnet ports.

HNS is the first botnet that can't be removed by a system restart.

360 Insight

IoT can be overlooked in the greater scheme of cyber security, but the systems are still able to give hackers access to high value assets, as well as help them add to their botnet army for use in a DDoS attack. As it gains more operational prominence, the frequency with which IoT products are targeted will increase.

HNS is quite easy to defend against – don't rely on default configurations. Changing credentials from manufacturers' settings is a low-effort, high-reward cyber security strategy that can protect an organisation from a large number of attacks.

WPA3 to make debut by 2019

The Wi-Fi Alliance announced its intention to roll out Wi-Fi Protected Access III (WPA3) security features and standards before the end of 2018. Its predecessor, WPA2, was introduced in 2005 and has been a well-known target of attackers in recent years.

WPA3 aims to enhance data encryption at an individual level to provide better security in open networks, like when someone connects to free Wi-Fi at a coffee shop. The new standard will be built into new routers, and will feature a 192-bit key packet transfer protocol – an improvement over WPA2's 128-bit key.

WPA3 will be introduced by the end of 2018.

360 Insight

WPA2 was released nearly 15 years ago, and we can expect a similar estimated lifespan for WPA3. The new security features will seek to prevent campaigns like VPNFilter or supply chain attacks that allow hackers to listen in on network traffic.

Adopting WPA3-certified routers and other hardware as soon as they are released is the physical equivalent to patching software. Deploying the new features as the first available moment will instantly improve the security posture of an organisation.

Quarterly report spotlight: Verizon

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.

Verizon's 2018 Data Breach Investigations Report is a must-read for anyone concerned with protecting their organisation's high-value assets from the latest techniques being used by malicious threat actors.

The 11th edition collects data from a variety of sources to better understand the cyber risks facing specific industries, and what tactics are most popular among attackers. The 15 most common actions that contributed to a data breach in 2017 were:

1. Denial-of-Service (hacking)
2. Loss (error)
3. Phishing (social)
4. Misdelivery (error)
5. Ransomware (malware)
6. C2 (malware)
7. Use of stolen credentials (hacking)
8. RAM scraper (malware)
9. Privilege abuse (misuse)
10. Use of backdoor or C2 (hacking)
11. Backdoor (malware)
12. Theft (physical)
13. Pretexting (social)
14. Skimmer (physical)
15. Data mishandling (misuse)

You can find the rest of the **Verizon 2018 Data Breach Investigations Report here**

DoS, phishing and ransomware were among the top five common actions that led to a breach in 2017.

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