CYBER SECURITY RISK RADAR

CONTENT

Integrity360
your security in mind

APRIL 2019
Q2

Executive summary

The first fiscal quarter of 2019 saw an influx of research on just how effective global cyber security was in 2018. Billions of compromised records, data leaks from cloud misconfigurations and record-setting cyber-threats kept the industry busy. Here's what you need to know:

- The Data Protection Commission's (DPC) first annual report revealed that **3,542 data breaches were filed since GDPR went into effect.**
- Malware, social engineering and other forms of cybercrime **cost the average organisation $13 million** per year.
- In a down year, **6,515 data breaches were reported across the world** and 5 billion records were compromised.
- The majority of IT managers are able to **link data breaches to privileged credential abuse** and lack of account security.
- A small pool of global businesses faced **681 million cyber-attacks on their cloud services and applications** in 2018.
- Data leaks stemming from **misconfigured clouds are becoming all too common** and putting companies at risk.
- Researchers found **billions of stolen account details and personal records up for sale** and floating around freely on the Dark Web.

- Over **22,000 vulnerabilities came to light in 2018** but businesses continue to struggle when it comes to patching them.
- Organisations are finding it more **difficult to secure cyber security talent**, with some open positions taking six months or longer to fill.
- **Google and Facebook data privacy failures** prove that the spotlight is on companies that aren't taking information governance seriously enough.
- Researchers stopped the **largest Distributed Denial of Service (DDoS) attack on record**, which was four times larger than the attack on GitHub.
- Hackers' botnets carried out **28 billion credential stuffing attempts** over the course of the second half of 2018
- **Formjacking came to the forefront as a serious cyber-threat** with over 3.7 million attacks being stopped in 2018.
- **GandCrab evolved tactics and released a new version** as researchers continue to produce decryption tools for the ransomware.
- Hackers carried out an offensive cyber-attack, **destroying the entire infrastructure of VFEmail** in the process.

DPC releases first annual report on GDPR compliance

Ireland's DPC released its first annual GDPR report, covering events from its introduction in May 2018 to the end of 2018. Since the introduction of GDPR, 2,864 complaints were filed and companies notified the DPC of 3,542 data breaches.

Across Europe, 60,000 data breaches were reported over the first seven months that the law was in effect. Google received the largest GDPR fine at the time, totalling €50 million, for not giving users enough information about ad personalisation and not gaining legitimate consent.

60,000 data breaches were reported in EU after GDPR went into effect.

360 Insight

Digital privacy and data security are chief concerns among companies and consumers in the GDPR era. Multiple fines have already been issued and tens of thousands of instances were reported, showing that the law is already functioning effectively in some capacity.

Companies should actively be working with Cyber Risk and Assurance (CRA) teams, and specifically data protection consultants, to ensure they're following best practices. Ensure that mechanisms are in place to quickly detect, investigate and report any security incidents that fall under GDPR notification laws.

Organisational cost of cybercrime rises to $13 million annually

Cybercrime cost the average organisation $13 million in 2018, according to Accenture's 2019 Cost of Cybercrime Study. The figure, which is a result of the costs of malware, insider threats and social engineering, rose by $1.3 million over the previous year.

The expenses stem from the resources put into detecting, investigating and remediating security incidents. The average enterprise recorded 145 cyber-attacks throughout the year, which is an increase of 67 percent over the last half-decade.

Cybercrime cost the average company $13 million in 2018.

360 Insight

Cyber security can get expensive, but cyber-attacks are always costly. Unsurprisingly, the most pricey types of attacks were malware and web-based threats, totalling $2.6 million and $2.3 million per instance, respectively.

Boards of directors and decision makers must weigh the cost of poor cyber security and the high risk it comes with versus the cost of great cyber security and the low risk it's associated with. Experienced consultants can help businesses find the right mix of tools and policies to maximise an investment.

6,515 data breaches expose 5 billion records in 2018

Roughly 5 billion records were compromised worldwide as the result of 6,515 data breaches which were made public in 2018, according to Risk Based Security researchers. The figure fell slightly below the amount of breaches in 2017, which came in at 6,728 data breaches.

Despite GDPR coming into effect, the average time to report rose by one day to 49.6 days, according to the study. The number of records that were compromised dropped by roughly one-third of the 2017 total, which was likely attributed to the absence of a major worldwide cyber-attack.

360 Insight

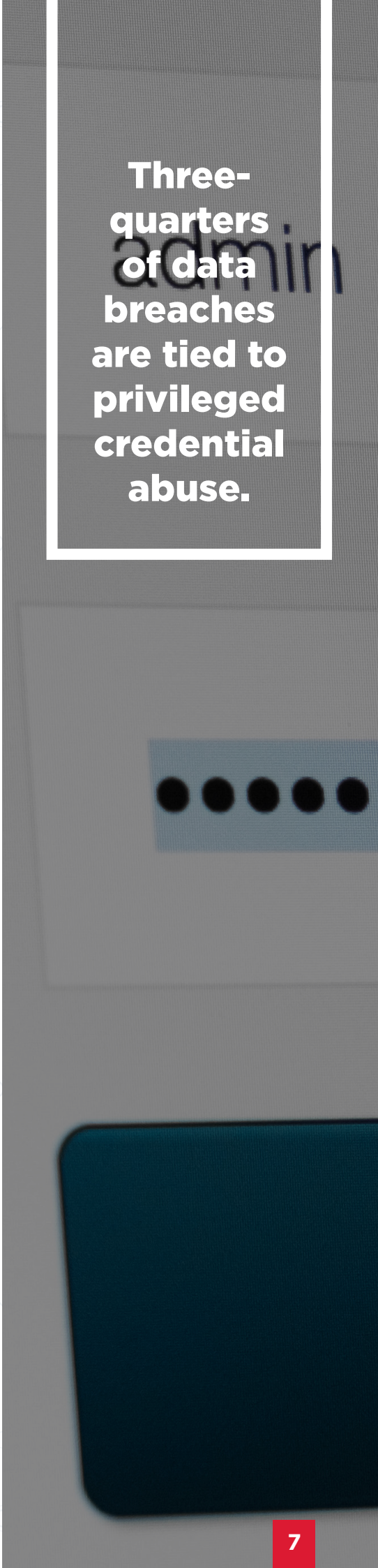
The world saw a host of breaches both large and small, complex and simple in 2018. GDPR had little effect on the frequency or size of them, as well as the average company's capability to detect a security incident. As a result, consumer information flowed freely on the Dark Web.

Organisations need to use the past failings of companies that suffered a data breach to shore up their own defences. Understanding how cybercriminals broke in and exfiltrated information at other businesses can provide a wealth of information on how to protect your own.

Three-quarters of data breaches tied to privileged credential abuse

Researchers found that the majority of data breaches can be tied to the abuse of privileged credentials at some point in the campaign. Nearly three in every four IT managers could link a data breach at their companies to privileged credential abuse, a Centrify study found.

Of the businesses that were breached, only 21 percent had multi-factor authentication in place. Another 65 percent were allowing near-regular access to system root privileges, rather than creating a new account for the user.



360 Insight

While many people's thoughts initially turn to a hooded hacker in front of a screen with green numbers and letters when they think of a data breach, Centrify's study shows it's often much more simple. Namely, people having access to systems they shouldn't for one reason or another.

Privileged Access Management (PAM) is a valuable part of any overarching cyber security strategy as it compartmentalises system access and ensures only those who need it have it. Investing in PAM tools is a sure-fire way to mitigate credential abuse.

Cybercriminals attempt 681 million cyber-attacks on cloud users in 2018

681 million cyber-attacks were attempted on cloud customers in 2018.

Hackers attempted 681 million cyber-attacks on cloud customers in 2018, according to cloud security provider Armor. The data was gathered from Armor's private and public cloud clients and represents a global pool of 1,200 companies.

While much of the activity was tied to cybercriminals scanning organisations' digital infrastructures, four types of attacks stood out as the most popular: leveraging software vulnerabilities, credential-based campaigns, web-based attacks and exploiting the Internet of Things (IoT).

360 Insight

Given the widespread use of the cloud and the limited access to data, it's near impossible to get a definitive understanding of how many cloud-based attacks took place in total in 2018. But Armor's snapshot raises the idea that it's a target which is growing in popularity for cybercriminals.

Enterprises that are rushing to integrate new cloud solutions should also be taking a step back before deployment to evaluate their security. Security assessments pre- and post-deployment are valuable tools in securing a digital environment.

Misconfigured clouds put customer data in jeopardy

A surge in data leaks borne from misconfigured or unsecure cloud storage servers are putting consumer information at risk. The largest in the last quarter saw at least 800 million email records exposed through a publicly accessible MongoDB database.

The Dow Jones recently suffered a data leak due to a misconfigured Amazon Web Services (AWS) instance, which revealed information on 2.2 million high-risk trading individuals. Researchers also accessed millions of customers' data from Gearbest, an e-commerce website, through an open Elasticsearch server.

A MongoDB database leak exposed 800 million email records.

360 Insight

Organisations are quickly moving to the cloud, but their frenzied speed is leaving them susceptible to common cyber-attacks. By deploying apps and hosting sensitive information on unsecure servers, companies are giving cybercriminals a free pass if they're able to find it.

Take the time to thoroughly audit a deployment before pushing it live into the wild. Cloud security assessments help organisations root out poor identity management policies and implement strong controls that will ensure sensitive data is not accessed by people or systems without adequate permissions.

Hackers spread billions of account details on Dark Web

Billions of records were shared and sold on the Dark Web forums in the first quarter of the 2019 fiscal year. The largest group of records were dubbed Collections #1, #2, #3, #4 and #5, which contained 25 billion records in total and were being freely shared by thousands of individuals.

Roughly 840 million records stemming from 32 different data breaches – many of which were previously unannounced – were made available for sale on the Dark Web. The seller asked for $43,900 in Bitcoin for the entire batch and reportedly made multiple sales.

Over 25 billion records were made freely available on the Dark Web.

360 Insight

With tens of thousands of data breaches in the rear-view mirror, we're now seeing the result of hackers' efforts. These compromised records can be used to commit fraud, set up phishing campaigns and conduct credential stuffing schemes to gain access to user accounts on an endless number of platforms.

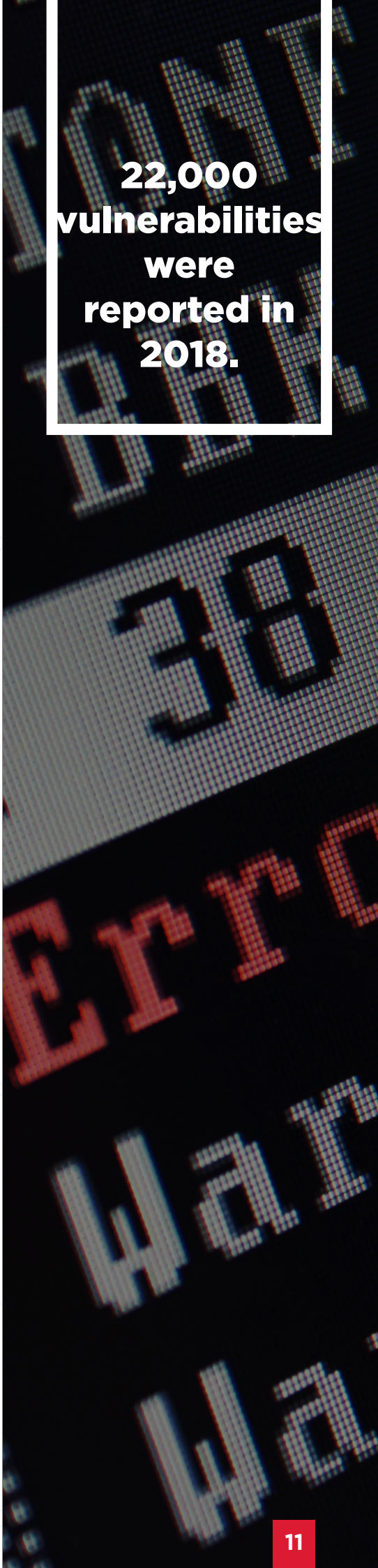
Organisations should use a variety of methods to protect against data breaches, including limiting access to sensitive information and segmenting the network. Individuals should practice good cyber security hygiene by creating unique passwords and regularly changing them in their accounts.

Companies struggle to patch thousands of vulnerabilities

Over 22,000 vulnerabilities were reported in 2018 and over one-quarter of them have yet to be patched by the software developer, Risk Based Security researchers found. Roughly 70 percent of all vulnerabilities identified in the last decade were attributed to memory safety flaws, a Microsoft engineer found.

At the end-user side, the average organisation is only able to remediate 10 percent of all vulnerabilities found in its network, research from Kenna Security and the Cyentia Institute found. The best performing organisation will close three-quarters of its vulnerabilities in around four months.

22,000 vulnerabilities were reported in 2018.



360 Insight

It shouldn't come as a surprise to anyone that skilled information security resources are scarce these days; that's why it's vital for organisations to be able to effectively prioritise patching and remediation efforts.

Patching and remediating 100 percent of vulnerabilities may not be practically feasible - and the data says that much. But companies still need to ensure they're not leaving their 'front doors' wide open. By being able to confidently identify externally exposed and exploitable assets, businesses can ensure they're not dangling low-hanging fruit for hackers.

Businesses compete to fill open cyber security positions

An organisation is forced to wait three to six months on average to find a suitable candidate for an open cyber security position, ISACA's State of Cybersecurity 2019 report found. Roughly one-third of companies have had to wait more than half a year to fill a position.

Over half of the businesses surveyed had an open cyber security position and another 69 percent felt they were understaffed. The top three reasons behind low retention rates were financial motivation, professional development opportunities and the workplace culture.

360 Insight

Move over data, oil and gold; cyber security talent is the most prized commodity nowadays. It's not easy to come by talented analysts and it's becoming even more difficult to get them to stay. The situation is leading to an uncertain talent market and less secure companies.

Rather than taking the burden of scouting the market for skilled individuals into their own hands, many organisations are turning to purpose-built resource placement services. These recruiters have a finger on the pulse of the market and more importantly, what skills are needed to fit requirements and job specifications.

Fortune 500s face backlash over data privacy failures

Google was issued the largest GDPR fine to date for its failure to abide by the EU's data privacy regulations. French data protection regulator, CNIL, issued a €50 million fine to the multinational corporation for not collecting genuine consent from users to collect their data.

Facebook was found to have stored users' passwords without encryption and in plain text on internal servers that were accessible by thousands of employees. Between 200 million and 600 million users across the social media giant's applications are initially thought to have been impacted, according to investigative journalist Brian Krebs.

360 Insight

Facebook and Google have dominated the news for all the wrong reasons over the past few years. With GDPR now in place and a brighter spotlight on their activities than ever before, the public is scrutinising every decision the Fortune 500 companies make in regard to data security and privacy.

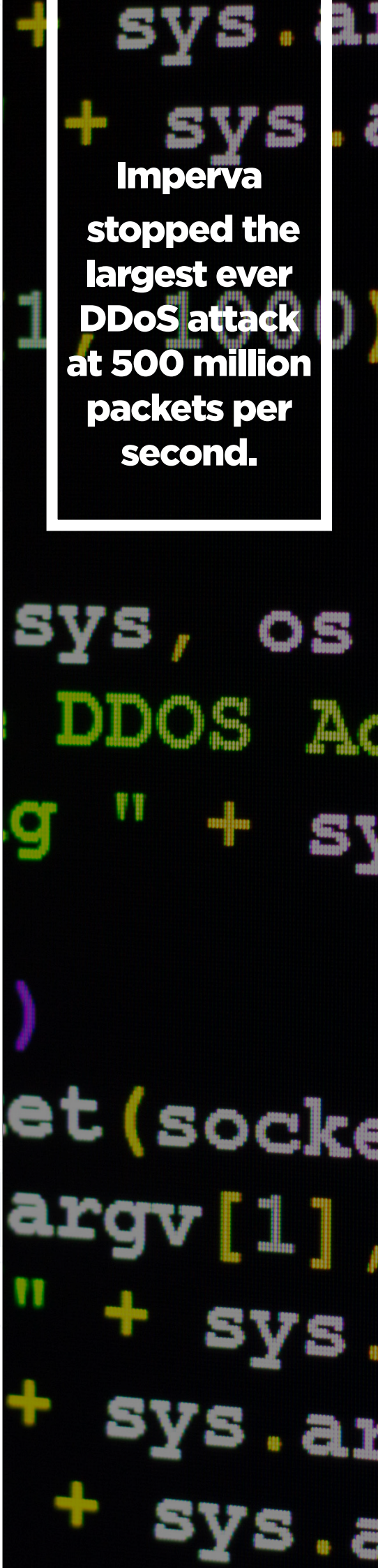
It's not only the largest companies in the world that are under review; every organisation that collects and holds personal information is increasingly being held accountable for what happens with it. Organisations must ensure that industry-approved frameworks are in place to mitigate the legal and reputational risks of poor information governance.

Imperva blocks largest DDoS attack ever recorded

Security analysts at Imperva stopped a DDoS attack that reached 500 million packets per second, the largest DDoS attack on record. The previous record holder was a campaign launched on GitHub in 2018, which reached 1.35 terabits per second.

The DDoS attempt stopped by Imperva was four times larger than the attack on GitHub. The cybercriminals attempted to exploit the TCP three-way handshake protocol; using a TCP SYN flood DDoS attack in an aim to overload the organisation's network servers and cause the servers to drop otherwise legitimate traffic.

Imperva stopped the largest ever DDoS attack at 500 million packets per second.



360 Insight

Hackers are getting smarter with their attempts which is helping them launch larger DDoS attacks than ever before. With the help of new technologies, methods and a growing inventory of IoT products, these massive campaigns will become more commonplace.

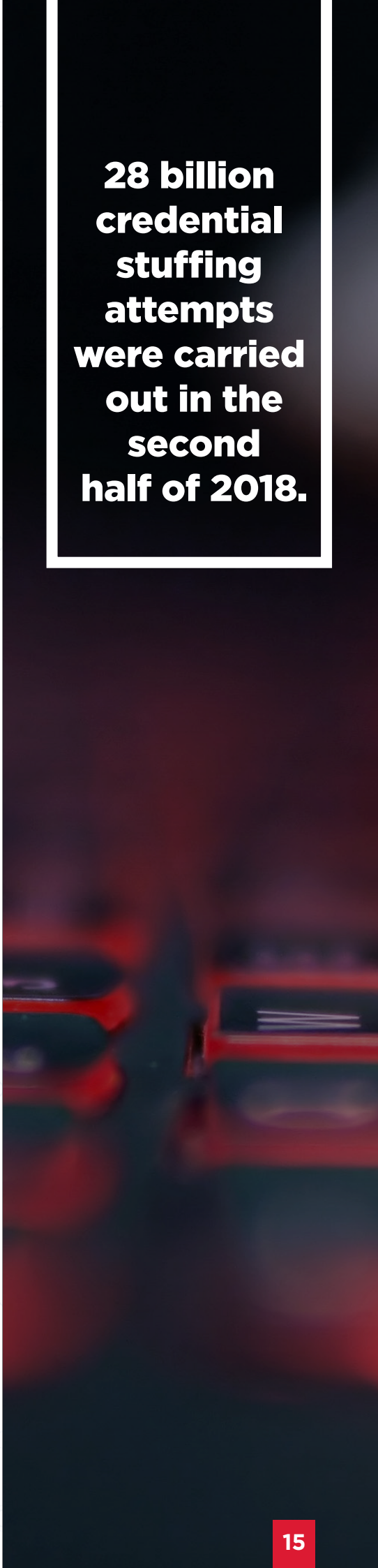
Organisations should ensure that they're working closely with their DDoS mitigation provider to set out a SLA that clearly states the size of attacks that can be stopped. Regularly evaluate this SLA to adjust with industry trends.

Hackers perform 28 billion credential stuffing attempts

Akamai security analysts detected over 28 billion credential stuffing attempts over the second half of 2018. Retail companies were the targets of over one-third of attacks, with dedicated botnets able to launch around 115 million login attempts per day.

Credential stuffing attempts are bolstered by large troves of data such as Collections #1 - #5, the personal records that were released to the public. The bundles of emails, usernames and password provide fodder for automated systems to work off of.

28 billion credential stuffing attempts were carried out in the second half of 2018.



360 Insight

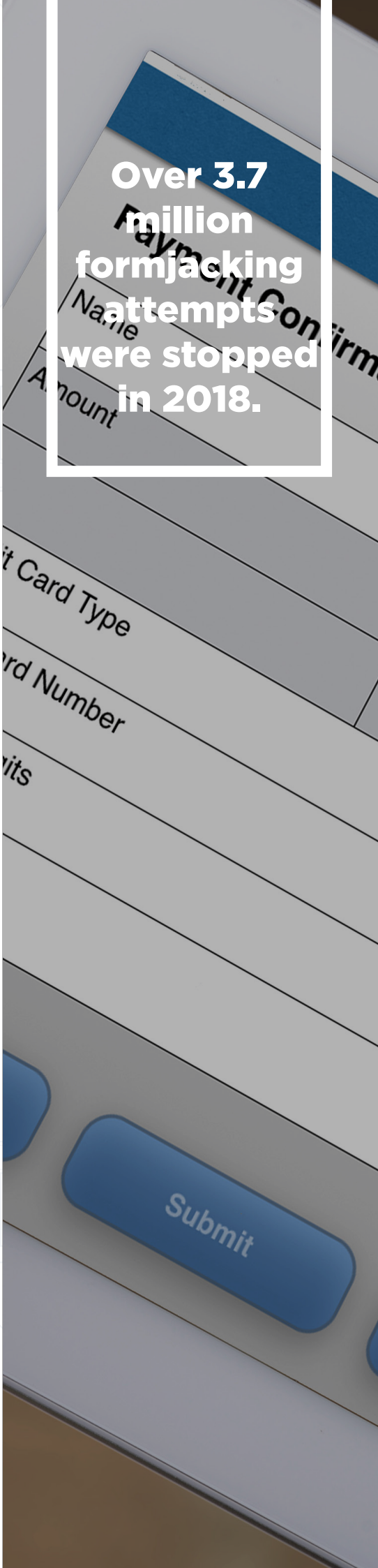
The 28 billion figure might seem large at first glance but given how many data breaches have taken place over the past few years alone, it's likely this could go much higher in the near future. Stolen information represents a great opportunity for hackers because consumers often reuse the same password in more places than one.

Companies should encourage employees and consumers to practice good cyber security hygiene by using a variety of passwords and ditching ones that were involved in a breach. Digital tools that report abnormal actions can help enterprises quickly identify large-scale credential stuffing attempts.

Formjacking cyber-attacks on the rise in 2018

Symantec analysts stopped over 3.7 million formjacking attempts and recorded over 4,800 unique websites being compromised every month in 2018. By stealing just 10 credit cards each month, Symantec estimates that hackers could generate over $2 million per month in revenue

Formjacking is a popular tactic among the Magecart threat group, which has multiple threat actors operating simultaneously. Group 12 was responsible for the Adverline hacking campaign that compromised around 280 websites in one week, according to Trend Micro.



360 Insight

The Magecart threat group was named one of Wired magazine's most dangerous people on the internet for a reason. Its attacks are very elusive and highly damaging – and so far, incredibly successful.

Formjacking will continue to rise and hackers will likely start targeting third-party vendor supply chains to slip their malicious code into the payment process. Enterprises should work closely to ensure third-party vendors have proper defences in place to detect these attacks.

GandCrab evolves as researchers release decryptor

Bitdefender released the third iteration of its decryption tool for GandCrab, which covers v5.0.4 to v5.1. Days later, the GandCrab creators released v5.2 as a workaround to the fix. There is currently a decryption tool available for every version besides v2, v3 and versions later than v5.2.

Elsewhere, GandCrab creators were found partnering with data recovery firms by providing them with a discounted ransom, letting the dishonest middlemen pocket the difference. CrowdStrike researchers report that GandCrab campaigns are becoming increasingly focused on compromising enterprise networks in search of larger payouts.

GandCrab decryption tools exist for all versions besides v2, v3 and versions later than v5.2.

360 Insight

Since first emerging at the beginning of 2018, GandCrab hasn't taken its foot off the gas pedal as the most pervasive form of ransomware in the wild. It has brought its creators and users millions in return as it continues to add new features and functionalities like it's a Lego kit.

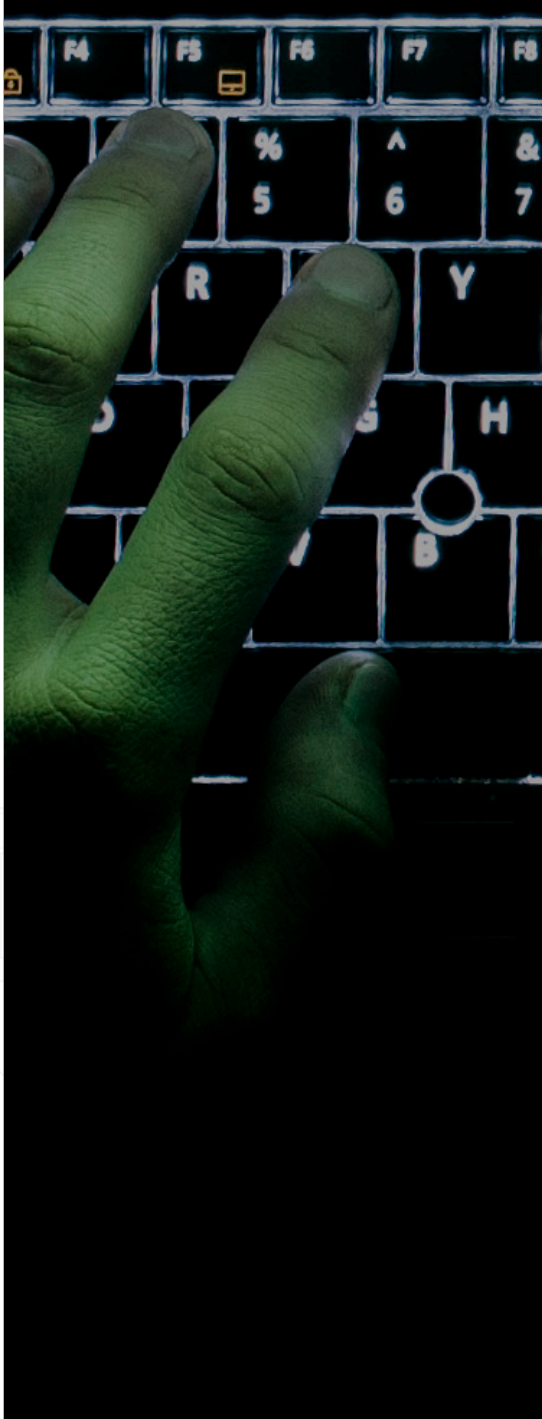
Companies should ensure they're actively patching vulnerabilities, as that's GandCrab's primary method of gaining a foothold in the system. Businesses should also improve phishing training, as GandCrab operators will commonly turn to social engineering for enterprise targets.

VFEmail infrastructure crippled by destructive hacking campaign

VFEmail, a US-based enterprise email provider, revealed that a cyber-attack caused "catastrophic destruction" to its infrastructure. Hackers carried out an offensive hacking campaign that wiped the primary and backup servers that operated its service and did not demand a ransom.

Virtual machines, SQL servers and mail hosts were targeted in the attack, deleting all the data that had been collecting since starting in 2001. VFEmail was able to partially recover information up to August 2016 and has since got the service up and running.

VFEmail saw hackers destroy its entire digital infrastructure.



360 Insight

The world hears about ransomware and phishing attacks, but rarely does news surface about a company's entire database being erased. That's because it seldom occurs and when it does, it's usually a part of a larger objective like making a statement.

Organisations can protect their data by implementing extensive recovery policies and protocols if an attacker manages to get by initial defences. Keeping data air-gapped from the network ensures that the company always has a valid backup to work with.

Quarterly report spotlight: Check Point

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.

Check Point is a leader in the industry and its coverage of the cyber-attack trends throughout the past year, as well as what to expect in 2019, is essential reading material for any team that wants to keep informed.

In its 2019 Cyber Attack Trends report, Check Point explores in-depth a variety of cyber security topics, including:

The report includes:

1. Major cyber-attacks that took place in 2018

2. Top cyber-threat trends witnessed in 2018

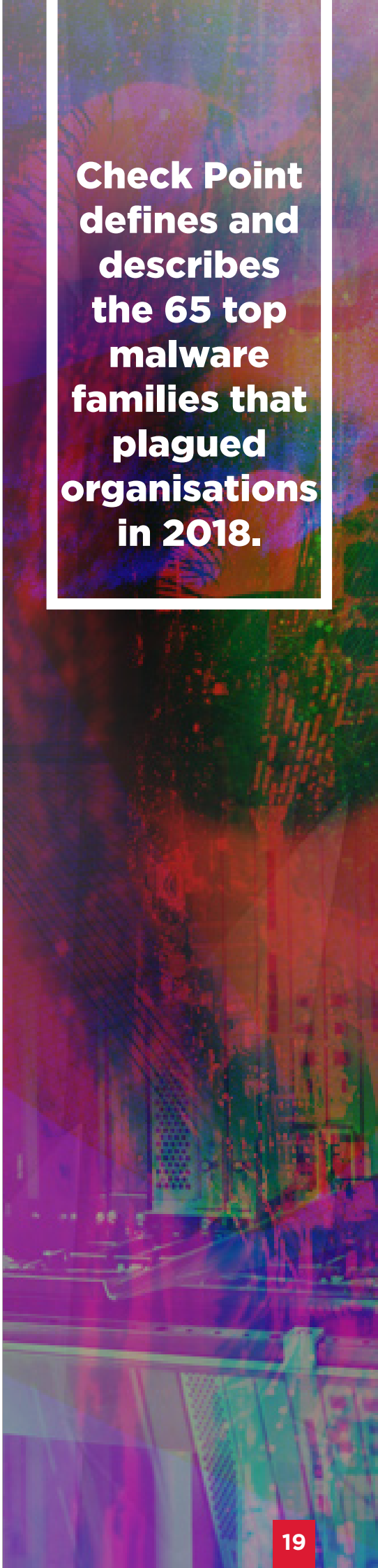
3. Review of Check Point's 2017 cyber security predictions

4. Top malware families in 2018

5. Top exploited vulnerabilities in 2018

6. Malware family descriptions

You can read the entire **Check Point 2019 Cyber Attack Trends report here.**



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

UK OFFICE
Church House, 32A Kneesworth Street
Royston, SG8 5AB
+44 1763 262 162

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

Integrity360

your **security** in mind