

CYBER SECURITY RISK RADAR

OCTOBER 2018 | Q4

CONTENT

- 2** Executive summary
- 4** Fileless attacks aren't flying under hackers' radars
- 5** GandCrab creator continues agile development practices
- 6** Reddit suffers a breach that shows risk of SMS-based authentication
- 7** Google prevents phishing by adding U2F to its MFA
- 8** Microsoft integrates password-less authentication with Edge
- 9** Magecart malware digitises payment card skimming
- 10** PowerGhost goes corporate with enterprise cryptojacking
- 11** IcedID and Trickbot collaborate on Trojan distribution
- 12** AZORult update fuels dual-pronged malspam campaign
- 13** Old Necurs botnet learns new tricks and targets banks
- 14** DanaBot uses FTP to trick users into phishing attack
- 15** GoDaddy AWS misconfiguration shows even Amazon can get it wrong
- 16** WhatsApp turning into breeding ground for mobile phishing
- 17** Samsung S7 and other phones exposed to Meltdown vulnerability
- 18** Ticketmaster, Harvey Norman breached due to compromised third-party vendors
- 19** Quarterly report spotlight: Ponemon

Executive summary

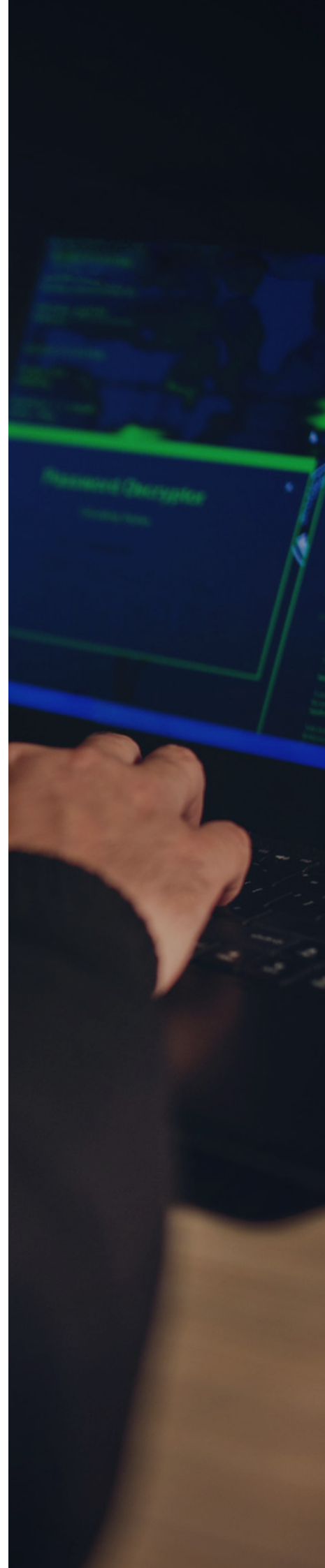
The third fiscal quarter of 2018 is in the rear-view mirror and there's a sizable shift in hacking trends on the road ahead. Here's a quick look at a few of the risks that businesses dealt with over the last three months:

- ✔ Researchers found that the frequency of **fileless attack methods rose sharply** over the first half of 2018.
- ✔ The creator of **GandCrab continues to reinvent the ransomware at a frenzied pace** to evade detection.
- ✔ Social news platform **Reddit suffered a data breach**, and the company attributed the attack to an intercepted SMS-based authentication code.
- ✔ Google released the results of its year-long campaign using token-based authentication, revealing that 85,000 employees had **zero successful phishing attempts** against them.
- ✔ Microsoft has **plans to support password-less authentication** using the biometric verification in its Windows Hello feature.
- ✔ Over **800 e-commerce retailers have fallen victim to the Magecart threat group's three-year campaign**, which targets customer payment information.



Executive summary

- ✔ Cryptojacking moves into the enterprise spotlight as **PowerGhost brings cryptomining to corporate networks.**
- ✔ The banking trojan playing field got rougher as **IcedID and Trickbot seem to have teamed up** to distribute one another's payload.
- ✔ One phishing campaign took an aggressive approach by **deploying both AZORult for data exfiltration and Hermes ransomware.**
- ✔ Necurs botnet re-emerged to **launch a spear phishing campaign against over 3,500 banks,** and used a unique file attachment to deliver its payload.
- ✔ The DanaBot phishing campaign is **using the File Transfer Protocol (FTP)** to get around users' suspicions of clicking on HTTP links.
- ✔ One of the **S3 buckets of domain host GoDaddy was found to be publicly accessible,** yet it wasn't the company itself who was at fault.
- ✔ Phishing campaigns are beginning to **curate content to target mobile users** through WhatsApp and similar platforms.
- ✔ Samsung's Galaxy S7 is understood to be **vulnerable to the Meltdown exploit,** and experts believe more smartphones could be at risk.
- ✔ **Ticketmaster UK and Harvey Norman suffered data breaches,** and serve as an example of the legalities surrounding GDPR and third-party vendors.



Fileless attacks aren't flying under hackers' radars

SentinelOne have reported a 94 percent surge in fileless attack frequency among enterprise endpoints over the first half of the 2018 fiscal year. The methodology is linked to a rise in techniques that rely on Microsoft's PowerShell, too.

Fileless attacks allow malicious code to run in the background, unbeknownst to the individuals using the infected computer. The payloads are often executed through attachments found in emails or websites, which download malware or ransomware from command and control servers.

The frequency of fileless attacks rose 94 percent in the first half of 2018.

360 Insight

Stopping fileless attacks demands a coordinated cyber security strategy that stretches across the enterprise. First and foremost, employee training to spot phishing attempts that are normally associated with the method is essential.

Security Information and Event Management (SIEM) tools can give IT teams a way to spot abnormal user behaviour. Next-generation, behavioural-based anti-virus and endpoint solutions are also recommended to address the rise in fileless malware attacks, and function as a datapoint for the SIEM.

GandCrab creator continues agile development practices

GandCrab has continued its run as the most prolific ransomware in 2018. Its author released version 4.0 and version 5.0 over the course of the third fiscal quarter, with one of the major additions including a switch from less robust encryption standards to Salsa20.

In response to AhnLab researchers announcing a vaccine for GandCrab version 4.1.2, the creator retaliated by releasing a new version which rendered the tool useless soon after its release. The ransomware continues to evolve at a rapid pace to evade detection and remediation.

360 Insight

WannaCry was the hot topic in 2017, and GandCrab has now taken over the spotlight. Given the pace with which the author is updating the ransomware's code, businesses must stay prudent and continue to patch systems and vulnerabilities as soon as possible.

Multiple anti-ransomware solutions are in the process of patching GandCrab, and use of the tools should be a given considering the frequency with which not just this attack but also other campaigns use the malware. Ensure there are backups of sensitive files and that network traffic and inbound files are being monitored.

GandCrab is being updated at a rapid pace to evade remediation.

Reddit suffers a breach that shows risk of SMS-based authentication

Reddit, a social news platform, announced that it suffered a data breach in mid-June, 2018. The scope of the attack was limited to read-only access on a backup database containing user credentials and other information from 2007, as well as current email accounts subscribed to the company's newsletter.

Reddit attributed the breach to a compromised employee account that was taken over after hackers intercepted the SMS-based authentication code in the business' two-factor authentication (2FA) strategy.

360 Insight

The company attributed the success of the attack to the liabilities of SMS-based authentication, and the result could have been far worse than what it was. It's important to note that even though SMS-based authentication has its security flaws, adoption of 2FA is strongly recommended as a baseline control for every business.

The business reported that it would bolster its access control strategy by applying token-based authentication to its most vulnerable and valuable parts of its systems. Furthermore, the fact that scope was limited pointed to the effectiveness of having an established security framework that mitigates attackers' lateral movement upon entry.

Reddit's data breach highlights the flaws of SMS-based authentication.

Google prevents phishing by adding U2F to its MFA

Google revealed that it equipped roughly 85,000 members of the company with physical security keys for their devices as a part of its Multi-Factor Authentication (MFA) strategy. In the one year since doing so, the company has yet to see a reported account hijacking that's attributed to phishing within the group.

The Universal 2nd Factor (U2F) standard uses either USB drives, Near-Field Communication (NFC) or Bluetooth connectivity to introduce a physical authentication component. The strategy is already endorsed by the Fast Identity Online (FIDO) Alliance, which includes industry players like Microsoft, RSA and Intel.

Google was able to stop account takeovers via phishing with U2F.

360 Insight

MFA is an essential component of a high-functioning cyber security strategy. Although current iterations like 2FA have yet to be perfected, they provide a far greater sense of security than relying on passwords alone.

U2F is one of the strategies that allows companies to move away from one-time codes like SMS-based authentication, which proved susceptible in the Reddit data breach. Expect new standards like U2F to become baselines for compliance with major security frameworks in the near future.

Microsoft integrates password-less authentication with Edge

Microsoft recently reported that its Windows Edge browser will soon be able to support Web Authentication. The new update will allow users to log into websites and approve sensitive transactions using the Windows Hello feature or software and hardware MFA.

Windows Hello enables people to leverage biometric security by replacing a password with their fingerprint or a picture of their face. This type of access control is also known as the Universal Authentication Framework (UAF), which is supported by the FIDO Alliance.

Microsoft will soon support UAF authentication through biometric security.

360 Insight

UAF is the FIDO Alliance's answer to replacing a long-time account vulnerability: the password. Its effect on cyber security strategies has yet to be fully realised considering how new the technology is, but it's possible that it sets the standard for access control.

Pairing Identity and Access Management (IAM) tools with innovative MFA features has the potential to greatly reduce the success rate of phishing. Considering that a compromised account is an easy access point for hackers, businesses should follow these developments closely moving forward.

Magecart malware digitises payment card skimming

The Magecart threat actor group has now jeopardised over 800 e-commerce websites since first originating in 2015, according to research from RiskIQ. This includes 100 top-tier retail domains, as well as the Ticketmaster, British Airways and Newegg data breaches that were announced in June and September.

Magecart is deploying a strategy that closely mimics physical card skimming on ATMs. The group is targeting third-party vendors in the supply chain or leveraging known vulnerabilities to send a copy of customer payment information to domains they've registered as it's collected.

360 Insight

Businesses that have yet to expand their cyber security frameworks to accommodate risks outside of their control are exposing themselves to increased vulnerability. Magecart has now exploited multiple third-party vendors.

Continuously monitor outbound traffic and refine the website's Content Security Policy (CSP) to defend against cross-site scripting. GDPR compliance extends to securing data collected by software vendors, and should be accounted for to reduce the chance that a costly data breach takes place.

The Magecart group has compromised over 800 e-commerce websites' payment platforms

PowerGhost goes corporate with enterprise cryptojacking

Kaspersky Lab researchers have identified a new large-scale cryptojacking campaign that targets enterprises as opposed to personal users. PowerGhost leverages a fileless attack method to infiltrate the target's device, and uses PowerShell to download and execute the code.

The cryptominer uses the mimikatz tool kit to access user credentials and gain high-level privileges. It also exploits the EternalBlue vulnerability to move laterally through the corporate network and embed itself in neighbouring computers.

360 Insight

It was only a matter of time before cryptojacking campaigns started targeting companies. Their vast architectures give cryptominers the added benefits of delayed detection and a massive hunting ground for large-scale operations.

Attacks like PowerGhost are emerging as a popular alternative to ransomware, the latter of which may not always provide hackers with a financial reward for their efforts. User behaviour monitoring analytics and tools are critical in spotting the abnormal network traffic associated with cryptomining.



PowerGhost is built specifically to target corporate networks.

IcedID and Trickbot collaborate on Trojan distribution

Fortinet researchers have found instances where banking trojans IcedID and Trickbot have partnered up to distribute each other's payload to infected enterprise computers via their respective command and control servers.

The team also noticed that updated variants of IcedID share similar behaviour patterns with Trickbot in terms of its distribution techniques and encryption standards. This suggests that the creators are collaborating with one another to shore up potential weaknesses.

360 Insight

Banking trojans are notoriously selfish when it comes to potential targets, even going as far as to check for and delete any trace of malware upon infection. While this isn't the first time two threat actors have teamed up, it does signal that a turning point - namely, better collaboration - lies ahead.

It's likely that this won't be the last time hackers collaborate with each other. Businesses should look to improve threat and vulnerability management to reduce exposure, segment the network to limit lateral movement and incorporate or enhance existing IAM policies.

IcedID and Trickbot trojan authors are collaborating on distribution.



AZORult update fuels dual-pronged malspam campaign

Shortly after the AZORult trojan's capabilities were improved, researchers found it being paired with Hermes ransomware in a campaign that targets corporate employees. The phishing email prompts users to download a Microsoft Word file disguised as a CV or related document.

The payload passes security tools undetected, but downloads and executes malicious code after a password is entered and macros are enabled. The AZORult trojan steals sensitive information, then installs the Hermes ransomware to encrypt the computer's files.

360 Insight

This new malspam campaign represents a challenge for businesses that have yet to fully invest in phishing awareness training or penetration testing. With the file able to slip through defences undetected, it can wreak havoc in poorly managed digital environments.

Coupling anti-malware solutions with better employee education about phishing tactics can generally reduce the chances a company falls victim. The Hermes ransomware will make a lot of noise, and even basic cyber security tools have a likelihood of catching it.

The malspam campaign exfiltrates data and plants ransomware.

Spam

ategoi

eted/It

Old Necurs botnet learns new tricks and targets banks

The Necurs botnet has been on the scene since 2012 and boasts one of the largest networks in the world. Recently, researchers discovered that it was at the heart of a spear phishing campaign which targeted over 3,500 banks before being shut down by its creators.

Attackers loaded emails that were disguised as payment requests or receipts with a combination of infected Microsoft Publisher and PDF attachments. Once the executable is triggered, the campaign plants a FlawedAmmy Remote Access Trojan (RAT), which gives hackers remote desktop access.

The Necurs botnet used a Microsoft Publisher file attachment to deliver a RAT.

360 Insight

Office 365 is a widely used platform and most cyber security awareness training seminars cover its vulnerabilities - namely, Word and Excel. Employees may not be as cautious when opening a Publisher file, and it's a unique attack vector for the Necurs botnet to try and exploit.

Keeping your threat intelligence practices in line with staff training exercises is key to staying ahead of evolving phishing attacks. With new file attachment types being employed by hackers, spam detection and email sandbox tools are becoming invaluable components of a cyber security strategy.

DanaBot uses FTP to trick users into phishing attack

DanaBot is a phishing campaign that was discovered targeting small and medium-sized enterprise employees. Attackers send emails with FTP links to PDFs - usually invoices or receipts - which then executes a PowerShell command that downloads the DanaBot trojan.

Once in control of the user's device, the trojan can communicate with a command and control centre to send screenshots and steal personal information. The resulting data can be used for spear-phishing campaigns or to gain access to financial services.

360 Insight

Phishing is a well-established method of acquiring account credentials, but hackers are constantly evolving their efforts to outwit employees. Using FTP linked to compromised servers instead of directing a user to a website is an increasingly popular technique being used to evade detection.

Keep cyber security awareness training up to date with the latest advancements in hacking methodology so that enterprise users are better able to spot these new tactics. Furthermore, leverage advanced spam detection tools that don't solely rely on identifying signatures.

The DanaBot trojan was delivered through a phishing campaign that used FTP.

GoDaddy AWS misconfiguration shows even Amazon can get it wrong

In August, cloud security researchers found a publicly accessible Amazon Web Services (AWS) Simple Storage Service (S3) bucket stored on GoDaddy's cloud. The information contained inside largely pertained to pricing and resource consumption estimations.

Amazon later revealed that the misconfigured "abbottgodaddy" S3 bucket was the result of an AWS salesperson failing to follow best practices. While the data stored in the database could have compromised GoDaddy's competitiveness, it did not contain any customer information.

360 Insight

There hasn't been a shortage of high-profile AWS misconfigurations leading to publicly exposed databases, but the GoDaddy incident is unique. It shows that even AWS employees trained in best practices can be susceptible to critical errors - never mind inexperienced IT teams.

Continuously audit the cloud's architecture to find flaws in its configuration before they're exploited. Furthermore, using a Data Activity Monitoring (DAM) tool can help a company gain better visibility into interactions on the cloud. Be sure to take advantage of the bucket permissions check feature in the Amazon S3 console.

Researchers found a publicly exposed GoDaddy S3 bucket.

WhatsApp turning into breeding ground for mobile phishing

Mobile device usage is proliferating and attackers are taking note. There have been a number of phishing campaigns targeting WhatsApp users across the globe, and they're experiencing higher success rates than traditional methods would garner.

These phishing campaigns are creating near-legitimate looking websites that share commonalities with established vendors by leveraging SSL certificates and optimising the experience for mobile users instead of desktop.

360 Insight

Many companies operate in a Bring Your Own Device (BYOD) workplace and future phishing attempts will try to take advantage of that. Employee training should include education about spotting common mobile phishing scams - essentially telling staff to ignore free giveaways.

Mobile Device Management (MDM) tools should be mandatory in all cyber security strategies at this point in time to prevent attackers from soliciting unauthorised access. Furthermore, MFA strategies should be in place as a failsafe for compromised accounts.

Phishers are increasingly targeting mobile users and applications.

Samsung S7 and other phones exposed to Meltdown vulnerability


Meltdown rocked the security world last year, but its after-effects are still being felt. Researchers revealed that the Samsung Galaxy S7 – previously thought to be invulnerable – could be exploited using the CVE.

Hackers would be able to gain access to the memory on the Galaxy S7, though Samsung has worked diligently to patch the vulnerabilities. It's currently unknown if there are any other phones that may be impacted by Meltdown, but haven't been identified yet.

360 Insight

Companies' security teams have focused on patching enterprise devices affected by Meltdown to reduce risk, but failing to keep up with developments on the vulnerability could lead to an exploitable cyber security posture.

With the vast majority of businesses giving employees corporate phones – the Galaxy S7 and other Samsung products included – those endpoints shouldn't be overlooked. The IT team should be able to update them through a MDM tool to ensure that even if one person fails to patch, the whole organisation isn't at risk.



The Samsung Galaxy S7 could be vulnerable to the Meltdown exploit.

Ticketmaster, Harvey Norman breached due to compromised third-party vendors


Ticketmaster UK announced in late June that itself and a number of its subsidiaries had suffered a data breach. The business found malware on its customer service platform, which was provided by Inbenta. Attackers were able to manipulate a line of JavaScript to gather payment information.

Harvey Norman revealed in late June that the retail company had been the victim of a data breach. The enterprise learned about the event through Typeform, its web form provider. While customer information was exposed in the breach, sensitive financial details were not.

360 Insight

Ticketmaster UK and Harvey Norman experienced the first two major data breaches after GDPR went into effect in late May. Both businesses were able to report the incident within the 72-hour window mandated by the legislation.

Despite the fact that third-party providers were breached, both of the companies were legally responsible in these situations. It's an important distinction that organisations should keep in mind when soliciting vendors' services.



Ticketmaster and Harvey Norman suffered a data breach through third-party vendors being hacked.

Quarterly report spotlight: Ponemon

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.

The Ponemon Institute's 2018 Cost of a Data Breach study has become a household name in an industry brimming with reports and information. The insights provide a baseline for the research surrounding data breaches and their effect on businesses and the threat intelligence community at large.

In the 13th annual edition, Ponemon explores in-depth a variety of factors surrounding data breaches, including:

1. Global and industry cost differences.
2. Root causes.
3. Factors that influence the cost of a data breach.
4. Trends in the frequency of compromised records and customer turnover.
5. Trends in the cost components of a data breach.
6. Direct and indirect costs.
7. The likelihood an organisation will have another data breach.
8. The time to identify and contain data breaches impacts costs.
9. Days to identify and contain the data breach by industry sector.
10. Security automation impacts costs.
11. The cost of a mega breach.

You can read the entire [Ponemon 2018 Cost of a Data Breach study 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