computing research

RESEARCH PAPER

Real-time threats require real-time defences

A discussion of present threat trends and the practical challenges of the application of security best practice in the real world

July 2017

Sponsored by

Malwarebytes

CONTENTS

Executive summary

It is unlikely that any reader of this paper harbours any comforting illusions about the level of security threats facing businesses and public or third sector organisations. The last year in particular has seen turmoil in western politics, allegedly aided and abetted at times by nation states. These states have often been unwelcome at the establishment table and have used cyber-attacks to simply kick it over. The tactics used by these states have been adopted enthusiastically by criminal gangs and opportunistic individuals keen to use either meticulously researched, beautifully crafted and targeted attacks or less sophisticated, brute force and widely distributed attacks for the same purposes – easy money.

Computing surveyed 110 business decision makers representing businesses ranging in size from 250 employees to those with many thousands and from multiple industry sectors. Our objectives were to first to establish the perceptions of respondents about the threat landscape, and where and if they perceived vulnerability in their organisations. A discussion follows about the reality of attacks that our respondents have faced, with a focus on three areas – ransomware, IoT botnets/DDoS and the growth in advertising fraud malware. This discussion is followed by a discussion of findings on the difficulty of finding a balance between the imperatives of security, productivity and enablement.

The paper concludes with a discussion of the role that real-time threat detection and remediation can play in assisting organisations to keep their data and reputations safe as well and realise the agility necessary to deliver goods, applications and services at the speed market conditions require.

Chinks in the armour

The first part of our survey established the areas which our respondents believed were most vulnerable to security breaches and the types of threat that they considered to be increasing in severity. The area of greatest vulnerability was considered to be public Wi-Fi. This is, in some ways, unsurprising – unsecured, public Wi-Fi has been notorious for years among those with even a fairly basic understanding of data security.

However, what is surprising is that the warnings do not appear to be filtering down to individual users, for whom the convenience of quick, free connectivity still seems to outweigh all other concerns. Related to this was the second largest area of concern which was mobile devices. The third was email communications – email still being the vector of choice for the transmission of ransomware and other types of malware and also that for mounting socially engineered attacks such as credential phishing and targeted attacks on individuals.

Fig. 1 : Please pick up to three main types of threat that you think are currently increasing in either severity and/or frequency

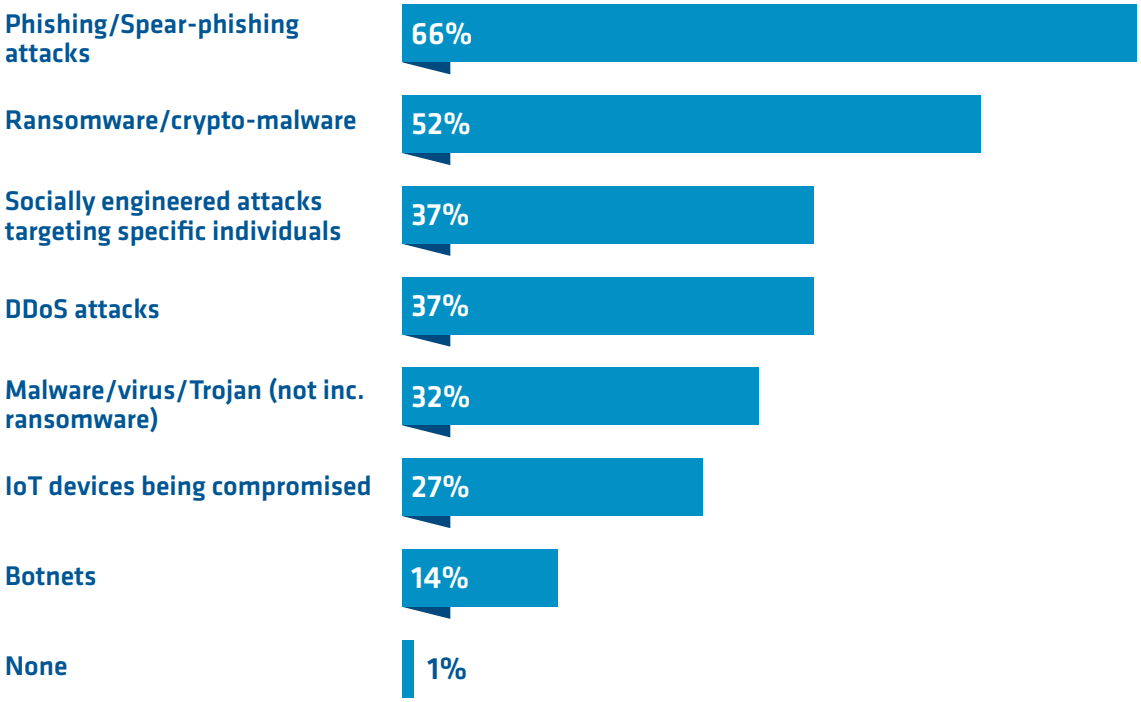


Figure 1 illustrates the answers of respondents to which threats they believed were increasing in severity. Top of the answers, by a significant margin was the fear of phishing and/or spear phishing attacks. Awareness of these attacks among our respondents is high but the degree to which that awareness extends to employees is variable.

Lower ranking employees are generally more likely to be duped by emails phishing for their network credentials or enticing them to click on a link to upgrade their mail box size. High ranking executives (particularly those holding purse strings) are more likely to be aware that they are a target but despite that awareness, some are still falling victim to targeted attacks which spoof email addresses of colleagues and mimic their style of writing in requests for funds. Indeed, socially engineered attacks targeting specific individuals were ranked third highest in our list.

Ransomware

Second in our ranking is, of course, ransomware. At the time of writing the smoke is clearing following the Petya attack which seems to have been aimed squarely at Ukraine, although it has spread to some degree beyond its initial target. It is beginning to become apparent that this ransomware attack wasn't actually ransomware at all. Earlier versions of Petya dating back to 2016 were ransomware, but the code now seems to have been changed in order to destroy rather than merely encrypt – which does rather throw into doubt early suggestions that this attack was perpetrated by criminals with nothing more than a desire for easy money. Petya comes hot on the heels of WannaCry in May which was unprecedented in scale. WannaCry was a text book zero-day attack and spread faster than fire until a blogger unexpectedly located a kill switch. There a

number of facts about WannaCry which make uncomfortable reading (not least the role of the NSA in hiding the EternalBlue exploit in the first place) but the most relevant for the purposes of this discussion, was that by any measure used by security experts, the attack was unsophisticated. It did however demonstrate to chilling effect the inadequacy of signature-based endpoint protection.

Few businesses admit to paying up to unlock encrypted data but many do. In research conducted by *Computing* in late 2016, approximately one quarter of respondents placed their willingness to pay a ransom at somewhere between four and seven (with seven being highly likely top pay and one being highly unlikely). That's enough for any attacker to turn a profit. Ransomware-as-a-Service has effectively democratised cyber-crime. Would-be cyber-criminals no longer require technical ability. A desire for easy money and a dubious moral code is all that's required to mount a ransomware campaign.

It is not controversial to state that ransomware attacks are increasing in volume, but it is also important to note that those behind them are amending their tactics to retain profits in the face of corporations refusing to pay, secure in the knowledge that data is backed up and that their inconvenience will simply run to re-imaging some endpoints.

New variants of malware include threats to release private data onto the very public internet, or send copies of the "kidnapped" data to contacts in the event that a ransom goes unpaid. This tactic significantly increases the likelihood of certain businesses (healthcare for example) paying up – as well as increasing the potential value of the ransom. Other variants locate any back-ups attached to the network and encrypt those as well. Another tactic is a digital twist on the chain letter whereby attackers agree to waive ransoms provided the victim in turn infects multiple victims.

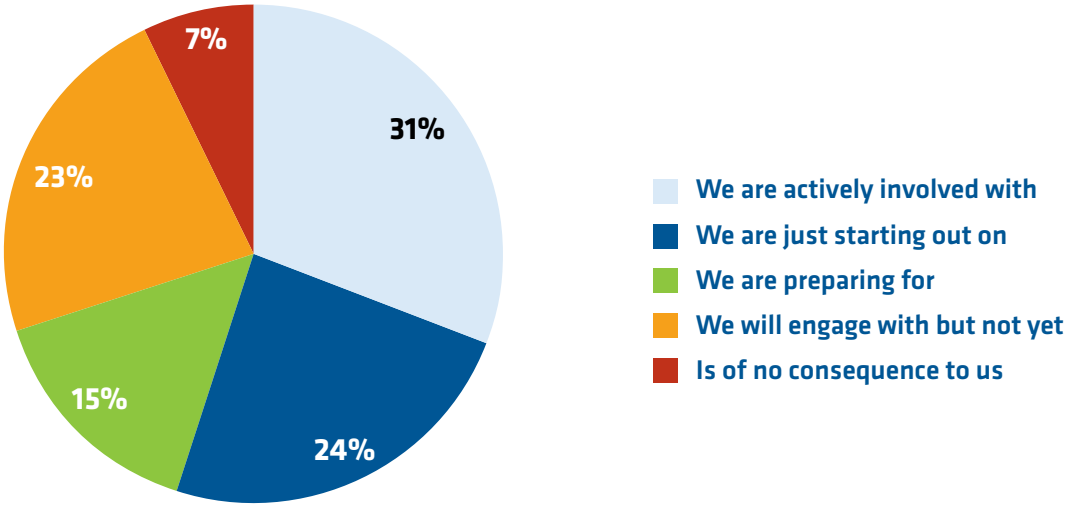
DDoS and IoT security

Only slightly further down the rankings came DDoS attacks (ranked joint third with socially engineered attacks) – with the related areas of compromised Internet of Things (IoT) devices and botnets only slightly behind. The IoT has offered up irresistible opportunity for those wishing to cause disruption to businesses as well as government and other organisations because of the rapid proliferation of poorly secured devices connected to the internet. These devices can be tethered to a botnet and used to bombard servers with traffic.

The motivations for DDoS attacks are more varied than other types of attack. There may be a profit motive – either via extortion by means of DDoS or as a way to misdirect attention and distract organisations from a far more serious data theft. Rather than pure profit, the motive can be espionage – especially when national or local government or public organisations are targeted.

Nation states or hacktivists may often lie behind these disruptive attacks. However, DDoS also remains the tool of choice for script kiddies, and amateurs who simply revel in an opportunity to stick it to the man. The identity of the author of the Mirai worm which caused such havoc last autumn has yet to be conclusively proved but investigations have illuminated an otherwise dark web of botnets and DDoS wars between individuals and groups of hackers.

Fig. 2 : The Internet of Things is something that...



Computing wanted to establish the degree to which our respondents were involved with IoT. As Figure 2 illustrates, over half of our respondents were involved to some degree with IoT – either actively or just starting out. A further 15 per cent were preparing their strategy. Only seven per cent of those that we surveyed considered IoT to be of no consequence to their organisation.

Our findings here suggest that whilst organisations may be some way off the real-time analysis and data driven decision making that is the majority destination for IoT, initiatives are getting off the ground in many organisations. That security considerations have, at least for manufacturers often played second fiddle to those concerning speed to market, means that we are at a dangerous stage in development.

The rise in botnets and DDoS attacks in the last eighteen months does rather underline the point. Mirai may be the most famous example of an IoT botnet but it is not the only one. Until the manufacturers of IoT devices stop cutting corners on security (and owners wise up to the fact that their home security system genuinely could be hijacked as part of an attack) the problem will persist – and is likely to worsen.

Ad-fraud malware

When asked which threats they believed were increasing in severity, respondents placed malware/virus/Trojans not including ransomware, joint third in the list. The writers of non-ransomware related malware have been able to enjoy a declining public profile courtesy of ransomware attacks featuring strongly in both technical and mainstream media. This has given those with ill intentions the space to develop new forms of malware – such as file-less. These attacks work by directly placing code into working memory so conventional antivirus scanning tools are rendered useless because there is no .exe file for them to block. This is the sort of malware required for long term siphoning of information. It can sit undetected for as long as the attacker wishes, harvesting network information, access credentials, and any other data required.

Malware is also quietly enslaving unwitting organisations (or more specifically their devices) into bots for the purposes of advertising fraud. According to industry estimates, around seven billion dollars of advertising investment is wasted because not a single human being actually sees the advertisements.[1]

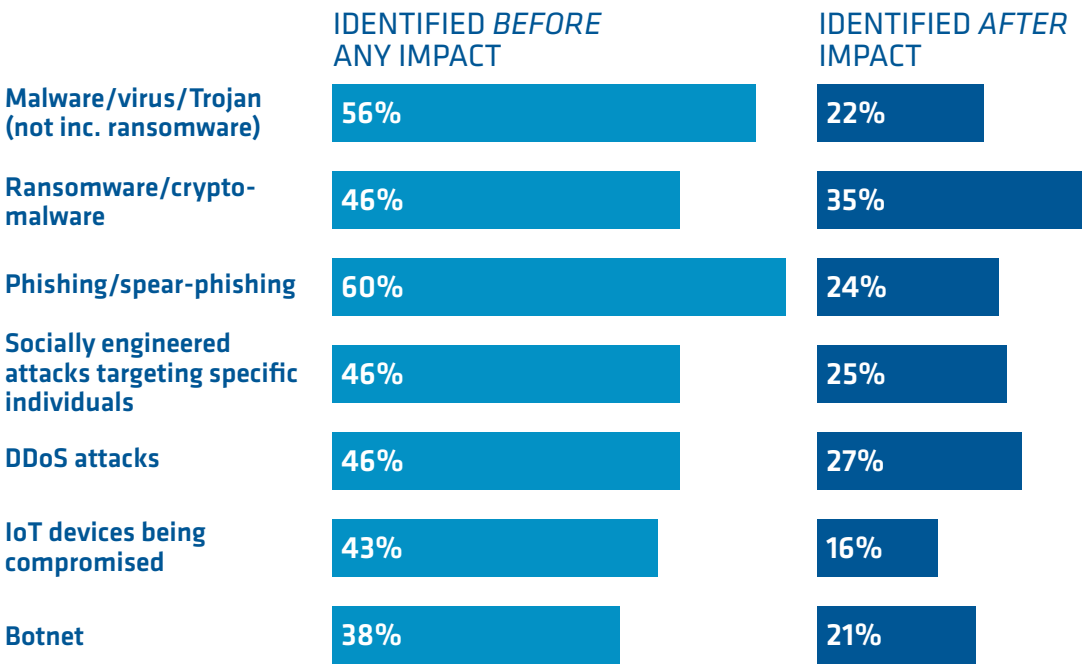
Endpoints (or servers) are infected with a Trojan or worm via the usual mechanisms such as spam, phishing email or drive-by download. These machines then become part of a wider botnet and generate clicks and traffic to bogus sites to defraud digital advertisers and publishers.

It is tempting to conclude that the biggest problem here is for the marketers paying for clicks that are made by bots rather than people. However, in addition to the theft of network resource and bandwidth, machines infected with clickbots often subsequently become infected with other malware or ransomware as traffic is requested from compromised sites. There is also the question of the privacy of the employee being affected which has potential implications for the employer.

The reality of attack

We asked our survey respondents to confidentially share with us whether they had suffered any sort of data breach or attack in the last 12 months. The responses were sobering. Fifty-seven per cent of respondents had been affected. A further 13 per cent were unsure. Only 30 per cent had, to their knowledge, escaped any sort of attack.

Fig. 3 : What types of attacks have you experienced in the last 12 months and were they identified before or after they had made an impact?



* Completed by those who said they have suffered a cyber attack in the last 12 months

[1] http://www.adweek.com/brand-marketing/whats-being-done-rein-7-billion-ad-fraud-169743/

Figure 3 illustrates the kinds of attack experienced by respondents, and whether the attack was identified before or after it made an impact. In keeping with previous findings was the fact that the most frequently occurring attack was phishing/spear-phishing, with 84 per cent of the respondents who had been attacked, suffering this sort of event. The majority of those so affected (approximately three quarters) identified the attack before it had made an impact. The remaining respondents were not as fortunate.

Only slightly fewer respondents (81 per cent) had been hit by ransomware. Ransomware attacks were more likely to be identified after they had caused damage. The third most frequently occurring attack was malware/virus/Trojan not including ransomware category.

Any strong risk management program will focus not just on the prevention of compromise but how to remediate and recover from any breach. *Computing* asked those who had been compromised in some way, how long it took them to remediate the issue after identifying it. The greatest proportion of respondents (48 per cent) managed to remediate in minutes. 30 per cent did so in hours and a less fortunate 14 per cent took days. Three per cent took weeks to neutralise the problem.

Recovery begins after the threat is neutralised, and should be considered part of the threat management process. Seventy-eight per cent of our respondents were able to recover fully from the attack. However, 18 per cent never fully recovered compromised data and for five per cent the battle for full recovery was still ongoing.

Finding a balance

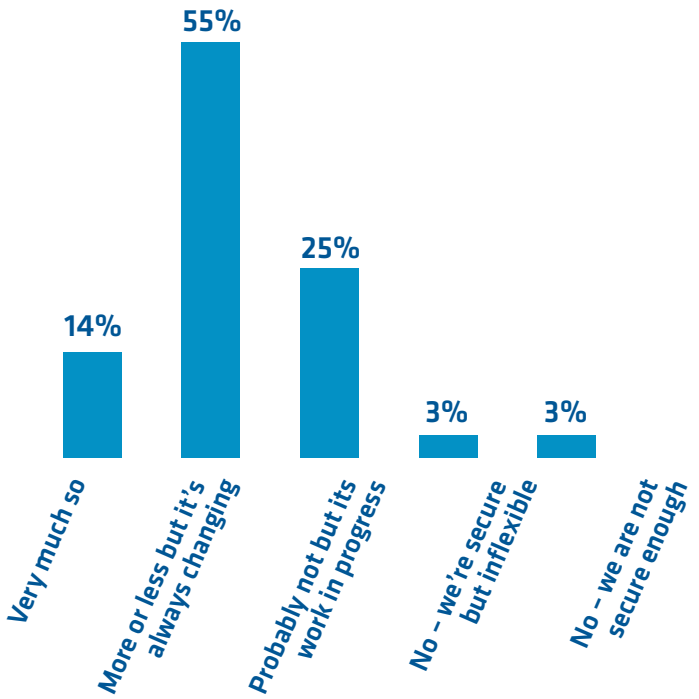
The perennial challenge facing organisations is the balancing of the security imperative with enablement and productivity. The challenge never abates because the two factors are subject to continual change, so equilibrium can never be maintained. *Computing* asked, "Do you believe that the right balance between security and usability/performance has been achieved at your organisation?" Figure 4 illustrates the shifting nature of the goal (*see next page*).

Whilst 14 per cent of respondents were confident that they were in the right place, a more cautious 55 per cent said, "more or less, but it's always changing". A refreshingly honest 25 per cent admitted that they probably had the wrong mix but that it was work in progress. Three per cent came down on the "secure but inflexible" side of the equation and a further three per cent on the opposite side.

Where are delays being experienced? The biggest issue was people, or more specifically the burden of implementing compliance and security procedures impeding employees. Forty-seven per cent of respondents stated that they had issues here. Twenty-eight per cent had experienced problems of security tools causing latency in applications and/or networks. Twenty-five per cent were struggling with the day-to-day mundanity of patching, upgrading and testing systems.

Organisations affected by WannaCry were criticised in the media for not having applied the Windows security updates that would have prevented the attack. However, the nitty gritty of managing and administering enormously complex, distributed infrastructure means that updates have the potential to cause disruption and the evaluation process can be long. The decision making process is not as straight forward as perhaps people outside of IT sometimes perceive it should be.

Fig. 4 : Do you believe that the right balance between security and usability/performance has been achieved at your organisation?



When asked to rate the overall manageability of present security infrastructure in terms of how well solutions are customised integrated and maintained, the average rating was 61 per cent which again is indicative of dissatisfaction with the status quo.

Conclusions

The last 18 months have seen significant changes in the types of threats that organisations must deal with. The increase in volumes is taken for granted by most businesses but in addition to dealing with low rent "throw enough mud at a wall and some will stick" attackers, they are also having to educate users about threats that could also be targeted and nigh on impossible to spot. Awareness of phishing and spear-phishing is high but individuals are still sometimes being duped through no fault of their own but because attacks are designed to exploit the very things which make us human.

Three trends in particular stand out. Awareness of ransomware has never been higher – and for good reason. Criminals are changing their tactics to avoid back-ups taking the sting out their attacks and to avoid the crowded ransomware market driving the average ransom paid down. Hence newer variants threatening to leak the relevant data, seeking out back-ups of offering incentives for victims to save their own skins by infecting others.

DDoS attacks have also increased in volume in the last year – and when they do occur the attacks seem to be more sustained. This rise in DDoS has been fueled in large part by IoT massively increasing the pool of poorly secured devices connecting to the internet. IoT botnets can be hired

for relatively small sums of money – all those with ill intent have to do is track down a bot for hire. The most famous botnet is undoubtedly Mirai, but given that in excess of half of our survey was involved with IoT to at least some extent, and that a further 15 per cent were preparing their strategy, Mirai will not be the last to cause widespread damage.

Bots (or more specifically the criminals behind them) are also depriving businesses of billions of dollars of marketing spend via the widespread distribution of advertising fraud malware. None of these trends has developed in isolation from the others. Ad-fraud malware for example, in turn directs browsers to sites where further malware, including ransomware can be distributed. If IoT adoption continues along its present growth trajectory and security continues to be little more than an afterthought, it won't be long before we start seeing IoT devices being held to ransom. Once IoT becomes a critical part of day-to-day operations in a business, it becomes worth attacking.

Regardless of future developments, our survey results suggest that corporate defences are struggling to cope with the new normal. Fifty-seven per cent of our respondents had been affected in some way by an attack with only 30 per cent completely confident that they avoided compromise. Attacks are likely to be blended with phishing mails being used to deliver ransomware or other Trojans/worms etc. Phishing/spear-phishing was the most commonly reported attack but around three quarters of those who had seen this sort of attack managed to remediate it prior to it making an impact. Eighty-one per cent of those who had been attacked had been so by ransomware – and ransomware was more likely to be identified after impact. Other types of malware were the third most likely attack.

The amount of time it takes organisations to isolate and neutralise threats of this type is what defines where an attack sits on the scale between minor inconvenience and unmitigated disaster. Our survey suggests that remediation tools are not presently up to the tasks required of them in many organisations. Whilst 48 per cent of those affected managed to remediate in minutes, 30 per cent took hours to do so. Fourteen per cent took days and a further three per cent took weeks.

These numbers do not tell us the resource that was expended in the remediation effort. It can take several man hours to re-image even one machine. Manually having to clean up multiple end-points takes inordinate amounts of resource that would almost certainly be better spent on more strategic activity. Recovery is also a key part of threat management, yet our survey suggests again that the solutions in place in some organisations are not sufficient because approximately one quarter of those who were compromised had not been able to fully recover data – or were still engaged in doing so.

Our survey shows that in many organisations, the battle between security technology and those who seek to disrupt and extort is being won by the bad guys. However, applying knowledge of this threat landscape to real world infrastructure is not as straightforward as many in business and technology would like it to be.

Businesses need to be agile enough to meet the expectations of instant availability of applications, goods and services for customers, employees and other third parties. It has been observed time and time again that employees in particular will find ways to circumvent security measures which they deem unproductive. If security policy is to achieve its objectives, employees must be on board.

Unfortunately, 47 per cent of respondents stated that they were experiencing delays because compliance and security procedures were impeding employees. 28 per cent found that security tools were causing latency in applications and/or networks. The manageability, integration and customisation of security solutions have a huge impact on those responsible managing and maintaining them. Twenty-five per cent of our survey respondents were struggling with keeping systems upgraded, patched and tested.

It is becoming clear that the management heavy AV solutions still in place in many organisations are neither keeping their data and systems safe nor providing the agility needed. It is common to refer to infrastructure which has been in place for several years as "legacy." However, such is the pace of change in the threat landscape, that the age of a security tool is less relevant than its type. Recent events have illustrated with stark clarity the ineffectiveness of many traditional security solutions in such a fluid threat environment.

We asked respondents how confident they were that security infrastructure was robust enough to protect data against present threats such as targeted attacks and ransomware. The average response was six out of ten, which suggests considerable room for improvement.

In order to meet these expectations, organisations must look to a layered approach, compromising anti-exploit, anti-malware and anti-ransomware. This adds extra layers of protection to the traditional security infrastructure components which have often been in place for some time. These real-time security tools should proactively aggregate internal and external data, using machine learning to deduce what constitutes a deviation from normal behavior – and block it. The nature of real-time threat detection means that it doesn't have to parse thousands of rules or signatures to make a decision. Real-time should therefore be less intrusive to users than more traditional security measures. Extra layers should not constitute extra management.

They should also have far less of an impact on operations, requiring less resource to manage and update. The process of threat prioritisation and remediation should also be real-time, with centrally managed tools proactively searching for unwelcome code and removing it. If these tools are in place, organisations stand a chance of balancing security and productivity – and keeping their data and reputations safe.

About the sponsor, Malwarebytes

Malwarebytes is the next-gen cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against dangerous threats such as malware, ransomware, and exploits that escape detection by traditional antivirus solutions. The company's flagship product combines advanced heuristic threat detection with signature-less technologies to detect and stop a cyberattack before damage occurs. More than 10,000 businesses worldwide use, trust, and recommend Malwarebytes. Founded in 2008, the company is headquartered in California, with offices in Europe and Asia, and a global team of threat researchers and security experts.

For more information:

Visit: www.malwarebytes.com/business

Malwarebytes founder and CEO Marcin Kleczynski started the company to create the best disinfection and protection solutions to combat the world's most harmful Internet threats. Marcin was recently named "CEO of the Year" in the Global Excellence awards and has been named to the Forbes 30 Under 30 Rising Stars of Enterprise Technology list and the Silicon Valley Business Journal's 40 Under 40 award, adding those to an Ernst & Young Entrepreneur of the Year Award.

Follow us on **Facebook**: GO TO

Follow us on **Twitter**: @malwarebytes GO TO

Follow us on **LinkedIn**: GO TO

See us on **YouTube**: GO TO

Read our latest Malwarebytes Labs **blog**: GO TO

Malwarebytes