a web link or a link to a web document (Word, Excel, PowerPoint, etc) – and isolates the web session. It launches the web page or web document in isolation, dealing with it separately. It sequesters any malware in a virtual, disposable container and returns a clean, rendered web page to the user's endpoint device.

There is no sandboxing – which, by the way, many of the latest ransomware infections look for and if one is found, the malware does not start. There is no 'good vs bad' assessment, which can lead to false positives – or worse, false negatives. There is just no more malware, no more phishing, no more ransomware. It's 100% safety via isolation, making it safe to click.

About the author

Jay Kelley is senior product marketing manager for Menlo Security. Prior to joining the company in February 2017, he was senior product marketing manager at F5 Networks for its application access and mobile products and services. Before that, Kelley was senior product marketing manager for Juniper Networks' Junos Pulse product line for over eight years. He has over 30 years' experience in a variety of senior management roles in marketing, product marketing and product management. Kelley has worked for seven start-ups in his career. He has presented at many technology events, including VMworld, RSA Conference and SecureWorld. He also co-authored the book 'Network Access Control for Dummies', published by John Wiley & Sons in 2009.

References

1. Ashok, India. 'Are hackers the new pirates on high seas? Billionaire superyacht owners can be held to ransom'. International Business Times, 8 May 2017. Accessed Nov 2017. www.ibtimes.co.uk/are-hackers-new-pirates-high-seas-billionaire-superyacht-owners-can-be-held-ransom-1620520.
2. Prasad Philbrick, Ian. 'It Took a Specialist Less Than Half an Hour to Hack Into a Superyacht'. Slate, 16 May 2017. Accessed Nov 2017. www.slate.com/blogs/future_tense/2017/05/16/it_specialist_hacks_into_superyacht_in_less_than_30_minutes.html.
3. Cimpanu, Catalin. 'Ransomware infects electronic door locking system at Austrian hotel'. Bleeping Computer, 29 Jan 2017. Accessed Nov 2017. www.bleepingcomputer.com/news/security/ransomware-infects-electronic-door-locking-system-at-austrian-hotel/.
4. 'Gartner says 8.4 billion connected "things" will be in use in 2017, up 31% from 2016'. Gartner, 7 Feb 2017. Accessed Nov 2017. www.gartner.com/newsroom/id/3598917.

Resisting the persistent threat of cyber-attacks


Gavin Russell

Gavin Russell, Wavex

If there's one issue that businesses across all sectors should be concerned about in 2017, it's the threat of cyber-attacks. Cyber-security-related stories have rarely made it out of the news this year, and this has resulted in increased public awareness surrounding the topic.

The severity of cyber-attacks on businesses was made clear in a report published this year by the UK Government in conjunction with Ipsos MORI and the University of Portsmouth.[1] Research within the report found that just under half (46%) of all businesses in the UK had detected at least one cyber-attack of some sort within the past 12 months. When zooming in on these findings and looking at medium-sized firms only, the figure rises to 66%, while focusing exclusively on large-sized firms sees a further increase of up to 68%.

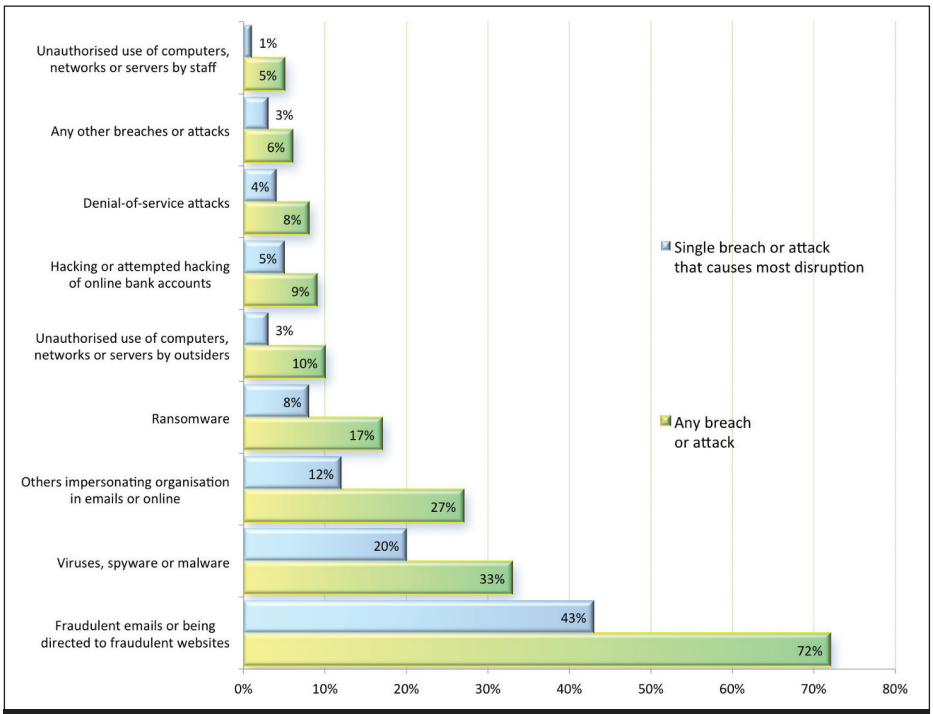
The findings become even more interesting when considering the frequency of these cyber-attacks. Of those businesses that had admitted detecting an attack, 37% said they typically experience an attack at least once a month, while well over one in 10 (13%) said they are coming under attack *every day.*

Of course, cyber-attacks are not universally identical. They come in many different shapes and sizes, and certain varieties can pose a much more serious risk to businesses than others.

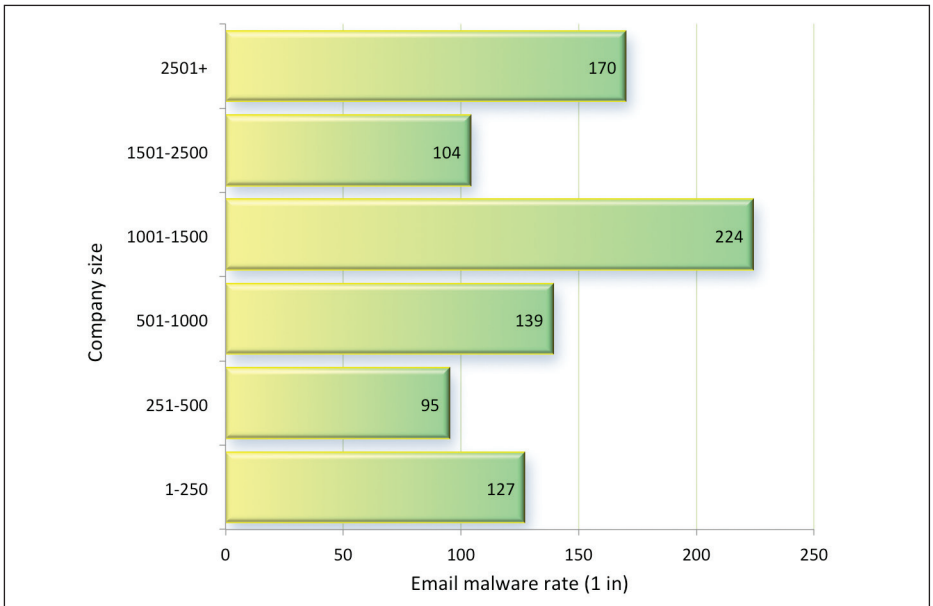
Malware

One of the most common and serious cyber-attack threats from a business point of view is malware. In its purest form, malware is a link or item that might appear to the victim as a curious-looking pop-up screen within an Internet browser, or as an inconspicuous attachment within an email. These are designed to mislead the user into thinking the item is genuine, and once the user has been fooled and clicks on the link, the hacker can quickly gain access to his or her network to either seize data or damage the network itself in some way. It is not a particularly new form of cyber-attack, but it remains dangerously effective.

It is also one of the most prolific. In its 'Internet Security Threat Report' from last year, security software company Symantec revealed it had discovered



Attacks on organisations over a one-year period. Source: UK Government, Ipsos MORI and the University of Portsmouth.



Ransomware detections by country. Source: Symantec.

357 million new variants of malware in 2016 alone.[2] More specifically, it found that one in every 131 emails sent in 2016 contained malware of some kind.

Ransomware

Another popular form of attack – and one that has some crossover with malware – is ransomware. This is a form of malicious software that is often unknowingly downloaded onto a computer by a user, perhaps once again through an email attachment or a counterfeit web page. Once the software has been downloaded, it blocks the user's access to the computer, encrypts the files within and renders the system unusable until a ransom is paid.

Ransomware has been the cause of many successful and well-documented cyber-attacks recently – most notably the global WannaCry attack back in May – and its impact is reflected in recent statistics.[3] The same report from Symantec revealed a total of 463,841 ransomware detections in 2016 – a huge increase compared with the 340,665 detected in 2015. There was also a sharp spike in the average amount of money being requested through each ransomware case, rising from $294 in 2015 to $1,077 in 2016.

DDoS attacks

Distributed denial of service (DDoS) attacks are primarily targeted towards businesses and involve using botnets or other tools to flood servers with so much website traffic that they can no longer cope and they crash under the strain. Following a successful DDoS attack, users will find they can no longer access the affected websites until the issue has been resolved – something that results in considerable downtime depending on the severity of the attack.

This method cannot result in a data breach or a hacker being able to access any networks, but it still holds serious consequences for the victim in terms of lost revenue and website traffic. It is also commonly used as a tactic to distract businesses while a more serious attack takes place.

"According to business Internet service provider Beaming, cyber-attacks in 2016 alone cost UK businesses as much as £30bn, while Lloyds of London recently warned that a serious global cyber-attack could cost the global economy up to £90bn"

One prominent example of how DDoS attacks can impact businesses is the Mirai botnet, a piece of malware created in 2016. Mirai worked by automatically infecting Internet of Things (IoT) devices and then conscripting them to a botnet. From here, all of these infected IoT devices could be used to launch huge DDoS attacks on companies across the globe. Mirai managed to wreak havoc on a global scale throughout 2016, taking 900,000 Deutsche