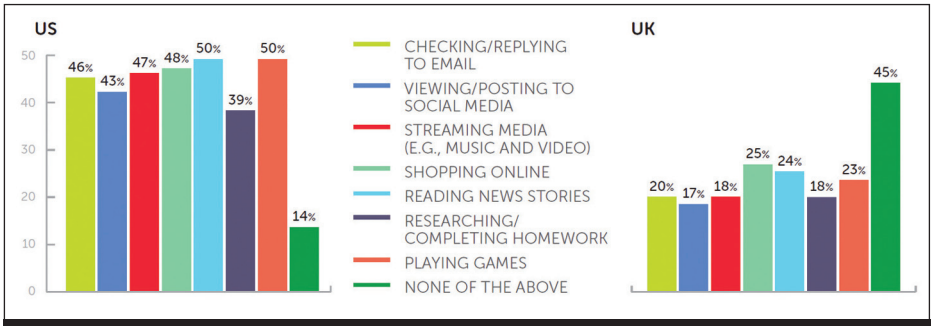

Figure 2: Answers to the question, 'What personal activities do you allow family members or trusted friends to perform on your corporate device?'. Source: Wombat Security.

ents wouldn't even hazard a guess on this multiple-choice query.

- 33% of UK respondents and 19% of US respondents don't know what a VPN is; 23% of those in the UK and 16% in the US said they know what a VPN is but don't use one.
- 14% of UK employees said they don't use any sort of locking mechanism – PIN, password, biometric or otherwise – on their mobile devices.
- 19% of UK respondents and 12% of US respondents admitted to password reuse.

If we extrapolate just some of these percentages to people – imagining a 2,000-person organisation – the dire nature of low awareness is clear:

- 600 employees would not understand what phishing is.
- Around 1,200 employees wouldn't be able to define ransomware.
- More than 300 employees would be reusing the same one or two passwords on all their accounts.

Darker edge

With the fundamentals of cyber-security so lacking in the average worker, there is an even darker edge to the reality that corporate devices are being fairly widely used for risky non-business activities. Organisations should stop thinking about what their employees *should* know about cyber-security and recognise that, unfortunately, they don't know much. That must – and can – change.

Employees need to be brought up to scratch about not only fundamental best practices, but also their responsibilities in handling corporate devices, data and systems. Security awareness and training programmes should not only be aimed at stopping the latest phishing and ransomware attacks (though that must be part of the goal), they should also have the goal of cleaning up cyber hygiene across the board. Thoughtful, engaging and ongoing education can do this. Employees who have the knowledge they need to make the right decisions about the threats they face – inside and outside of email – can help build a better cyber-security posture overall.

About the author

André Mouradian was appointed senior manager EMEA at Wombat Security in February 2017. His experience spans more than 30 years and he has held marketing roles at companies such as LogRhythm, ActivIdentity and Websense, including marketing director at GrIDsure. In his current position, Mouradian assumes overall responsibility for the strategic planning and execution of all marketing activities across Europe as well as strategic business planning and lead generation development across all target sectors. He is also responsible for driving the company's EMEA channel marketing programmes.

Reference

1. '2017 User Risk Report'. Wombat Security. Accessed Jul 2017. https://info.wombatsecurity.com/user-risk-report.

Defending against spear-phishing

Jason Steer, Menlo Security

Jason Steer

There is no doubt about it, spear-phishing is big business – it is even becoming a serious political and diplomatic weapon. Last year saw a 1,300% increase in business email compromise attacks and a 400% rise in ransomware. And 90% of successful data breaches could be traced back to a spear-phishing email (according to PhishMe research). This is how attackers can evade your defences and assume the privileges of an insider.

The silver lining in recent major attacks such as WannaCry and Petya is that big news coverage does at least help to spread user awareness and increase caution. Last year, 65% of employees surveyed by cyber-security company Avectom were already wary about clicking on emails sent by strangers – and yet 68% still had no qualms about clicking on links sent by friends and colleagues. And this is the point where general phishing attacks escalate into more targeted and dangerous spear-phishing.

Baiting the hook

For years we have known not to respond to dodgy emails from strangers promising to share a huge inheritance with anyone who can help them by providing a few bank details. Those crude emails gave themselves away with their clumsy grammar and absurd claims. In more recent years we have learnt that even a properly presented email bearing a realistic bank or courier logo should not be clicked on without checking the actual sender's address – better still to go to the site directly rather than from the email.

That is where those 65% stood last year, and we can be sure the number has improved already this year. But with every increase in vigilance, the attackers are responding with ever more subtle enhancements. Scroll over the email address that appears to be from FedEx and you see that the actual address is totally different. Check the link URL to make sure it really is from your bank, and at first glance it looks real – but closer inspection might show that the word Barclays had been substituted by Barlays or Barelays – directing you to a fraudulent website. Even worse, a recently disclosed 'punycode hack' exploits some browsers' ability to work with different, non-Roman alphabets. The letter 'a' in that address might actually be a letter from a different alphabet that just looks like our letter 'a', and it would take the eye of a trained typographer to notice the difference.

The attackers seem to be unbeatable, with everything stacked in their favour: the defender has to recognise and defend against every single attack, whereas the attackers only have to get through the defences once and they are into the system. With their ability to automate malware variations and deploy massive botnets to drench the Internet with malware – what chance does the defender have?

Behind the smokescreen

Behind that smokescreen of general phishing attacks there is an even more dangerous threat from innocent-seeming messages closely targeted for specific individual employees. This is the difference between generalised phishing and spear-phishing, which takes advantage of those 68% who would trust an email from a friend or colleague by including names of friends, hobby interests, places visited etc. This is data that can be uncovered by searching social media and it means that the attacker could forge a truly convincing email from a colleague on the lines: "Hi George, thanks for inviting me to last week's 40th birthday party at your house: click here for some of the photos I took" – a first foot in the door that could lead to sharing more personal details and eventually opening the whole corporate system to attack.

Where the monetary or political stakes are high enough, attackers could spend weeks and months crafting such messages for maximum chance of success. You can debate the merits of artificial intelligence and sophisticated malware detection algorithms all day long, but the best targeted attacks will still not be detected, because they need not contain any malware. They could simply and politely invite you to give away credentials needed to login, move laterally within the organisation and dig deeper into the system. That is the meaning of 'persistent' in the term Advanced Persistent Threat (APT).

Dodging the spears

If there are so many potential enemies out there, there is no chance of halting the deluge of spears being hurled your way. So a better solution must be found.

Malware detection can only go so far, because it's impossible to create enough rules to address every iteration of every possible phishing email without slowing down the service so much that employees can no longer work efficiently. There is also a delicate balance between being able to detect enough of the bad stuff without blocking too much good stuff – because really smart phishing emails can look exactly the same as good ones.

Then there is the question of security training for employees and raising awareness with posters and messages. This should never be overlooked as a defence against less targeted phishing, but the above examples show that they could end up spending every working minute scrutinising emails and web content – with no time left for real work.

Compare the situation with a discovery that the water supply to the office is dangerously infected. Would you expect staff to take every possible hygienic precaution every time they drank, washed their hands, or touched a tap? Or would you take the first opportunity to make sure that the water supply was properly sterilised before it reached the office?

Isolation technology does just that to your data supply: it means that all web and email content is sterilised and made safe before being delivered to the office along a secure highly encrypted link. Early versions of the technology relied on pixel mirroring to reproduce the web page or email as an array of pixels, without any of the hidden active content provided by the likes of Flash or Java. This approach makes no allowance for the actual content – whether text, image or

Continued on page 20...

...Continued from page 19
video – so pixel mirroring tends to slow down page loading, reduce responsiveness and makes common operations, such as printing and copy-paste, more tiresome.

Safe pages

The newer approach uses the Document Object Model (DOM) to allow for the actual content type. It actively monitors the currently loaded page for changes, translates those changes into DOM commands (without the hidden active content) and sends those commands to an end user's 'safe' page that automatically updates in sync with the original. The result is a page that looks, feels and behaves just like the original. For example, it lets the document reflow to suit the local printer – unlike the pixel mirroring approach that freezes the page as a rigid array of pixels.

These safe, sterile pages are created in the cloud, protected with high-grade encryption and served by a secure web proxy. Active content blocking and transcoding makes sure that all DOM elements are checked against a whitelist in both the isolated browser and the safe page, while the strictest Content Security Policy reinforces the ban on active content in the safe page. Protocol checking and enforcement places strict limits on the format of all DOM updates so that no channel is left open for probing for vulnerabilities or leaking data.

From the user viewpoint nothing is changed. There is no difference to the appearance of the pages or emails and they are as responsive as before – but now employees can work with confidence. Isolation makes their Internet experience as malware-free as a printed page.

Trust nobody

The trouble with most security approaches is that they rely on the ability to recognise a threat and avoid it. As the above spear-phishing examples suggest, this can become an immensely complex and time-consuming task. If it is entrusted to human users, it wastes a lot of time and reduces efficiency. If sophisticated malware detection systems are installed, then they need to be continuously updated.

The isolation approach simply assumes that all Internet content could be infected, nothing can be trusted, so everything is sterilised. So how does it work in practice? Does it increase latency? Does it require installing a lot of extra hardware or software at the endpoint? Is it proving successful in a real business environment?

As a cloud service it was first developed for the financial services sector in collaboration with JPMorgan Chase. According to its chief information security officer, Rohan Amin, the platform was deployed "with zero impact to users, providing a seamless user experience for our employees". In just two years the same technology has been successfully adopted by many other critical sectors – including government, technology, healthcare, oil and gas. As a cloud service it does not require hardware or software installation and its transparency means that there is no training or acclimatisation needed, making it quick and easy to roll out right across any organisation. So this solution is also catching on with smaller or less critical organisations.

The service can be readily tailored to match any organisation's – or specific user group's – security policies. 'Health warning' banners can be added to dubious websites to discourage casual browsing, emails can be specified as 'read only', links can be removed and further restrictions are readily added.

Cloud-based web and email isolation really does offer a powerful defence against the wave of increasingly clever spear-phishing attacks.

About the author

Jason Steer is EMEA CTO for Menlo Security. He has worked at a number of technology companies over the past 15 years, including IronPort, Veracode and FireEye. Steer has worked as a cyber-expert with CNN, Al Jazeera and the BBC as well as the EU and UK Government on cyber-security strategy.

EVENTS

4–5 September 2017
International Conference on Cyber Intelligence and Cyber Terrorism
Prague, Czech Republic
http://bit.ly/2sqdt70

5–7 September 2017
Cyber Intelligence Europe
Bucharest, Romania
http://bit.ly/2rn1GH2

6–7 September 2017
Cybersphere 2017
Manila, Philippines
www.cybersphere.ph

11–12 September 2017
Information Security Network
Reading, UK
https://thenetwork-group.com/information-security-network/

13–15 September 2017
44Con
London, UK
https://44con.com

18–19 September 2017
Gartner Security & Risk Management Summit
London, UK
http://gtnr.it/2rHwCoE

19–22 September 2017
OWASP AppSec USA
Orlando, Florida, US
https://2017.appsecusa.org/

19–20 September 2017
Insider Threat
London, UK
http://bit.ly/2qDphGA

25–27 September 2017
(ISC)^2 Security Congress
Austin, Texas, US
http://bit.ly/2rHhlyD