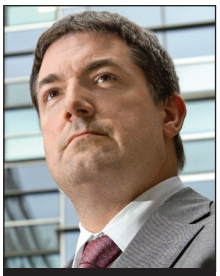
The ABC of ransomware protection


Steven Furnell


David Emm

Steven Furnell, Centre for Security, University of Plymouth, UK and David Emm, Kaspersky Lab UK

'Your files have been encrypted!' These five words have the potential to instil alarm as the realisation dawns that your system has fallen victim to ransomware. How it happened and what happens next, rather depends upon the precautions that may or may not have been taken beforehand. And as we will explore in this article, taking some basic steps in advance could help save a lot of problems later.

There is no escaping the fact that ransomware has become a significant problem and is now one of the most keenly recognised threats in the security landscape. Figures from SonicWall suggest that there were 638 million related attacks in 2016, which is a 167-fold increase on the 3.8 million seen in the previous year (which was mildly up from 3.2 million in 2014).[1]

"It is not only the threat that is old – so too are the basic safeguards that can help defend against ransomware attacks"

While it is getting a lot of attention, ransomware itself is far from a new threat. Indeed, the first large-scale incident goes back to 1989, with a physical worldwide mailing of 20,000 diskettes claiming to contain a database about the AIDS virus (which, upon installation, hid the user's files and demanded that $378 be sent to a post office box in Panama City in order to get instructions for restoring their data). It was not *called* ransomware at the time (the incident is commonly referred to as the AIDS information trojan), but the principle was very much in play.

Perhaps ironically, it is not only the threat that is old – so too are the basic safeguards that can help defend against ransomware attacks. The title of this article refers to the ABC of protection and indeed there are three particular measures that can significantly reduce the ransomware risk if given correct attention:

- Anti-malware.
- Back-up.
- Critical patching.

This highlights a set of valid core principles. Just like learning the ABC is fundamental to learning the alphabet, these measures ought to be fundamental to cyber-security (and not just because of ransomware). They are baseline and well-established points that are clearly stated in sources such as the international code of practice for information security controls (ISO/IEC 27002) and the NCSC's '10 Steps to Cyber Security'.[2,3]

Their importance is further explored later in the discussion. However, before this, it is relevant to look at the nature of the ransomware problem that they can help to combat.

Ransomware then and now

Looking at the evolution of the threat, the aforementioned AIDS trojan took place in a pre-web age, where financial transactions operated in the real world. Trying to monetise such attacks in that era was almost impossible. By contrast, with anonymous online payments today's environment offers plenty of scope for attackers to launch ransomware attacks, collect the money and get away with it. It is also easier, of course, to distribute the code, with no floppy disks

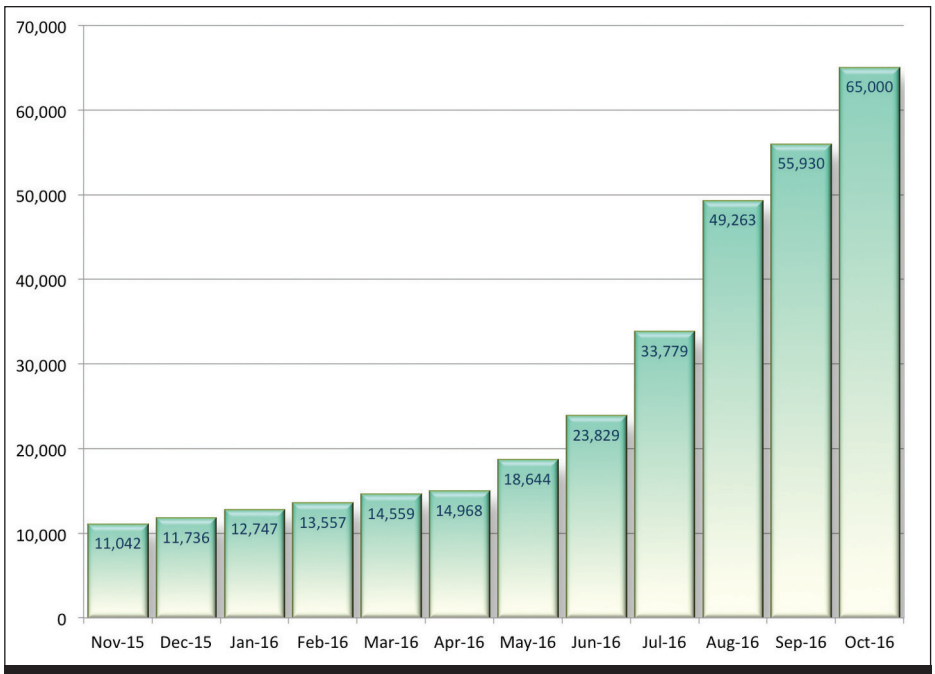


Figure 1: Crypto-ransomware modifications in 2015-16. Source: Kaspersky Lab.

required! Therefore, it is unsurprising that the scale of ransomware of today far surpasses earlier attempts to extort money using computers.

The re-emergence of ransomware began in the mid-2000s with Gpcode, which encrypted files on infected computers using its own algorithm. This was followed by Krotten, Cryzip and other ransomware families. In these early ransomware programs, encryption was often poorly implemented, making it possible for anti-malware programs to decrypt data as well as remove the malware. By 2010, we were also seeing blockers. These programs, rather than encrypting data, prevented people from accessing their desktop, browser or operating system. As this is easier to implement than data encryption, blockers made up the majority of ransomware for some time. This changed in 2015 and now the number of crypto-ransomware programs exceeds that of blockers. The growth in crypto-ransomware is illustrated in Figure 1.

"Even though the data was recovered, productivity was notably impacted. You do not need many occurrences of such incidents to severely jeopardise the viability of an organisation to operate at all"

The 'Cyber Security Breaches Survey 2017' indicated that 17% of respondent organisations had experienced ransomware in the prior 12 months, making it the fourth most frequently encountered category of identified breach.[4] However, incidence and impact are not necessarily equal partners and to illustrate the potential seriousness of the latter, the report also describes a case scenario in which ransomware was downloaded to a laptop that also mapped to its organisation's network drive. The mapping allowed the ransomware to infect the organisation's whole server and it took a working week to restore access from back-ups. As such, even though the data was recovered, productivity was notably impacted in this period. You do not need many occurrences of such incidents to severely jeopardise the viability of an organisation to operate at all.

Proven effective

Of course, the reason that ransomware has grown is because it has proven effective; victims are often willing to pay in the hope of getting their data back. Unfortunately, whether they actually *get* it is sometimes another matter. For example, findings from Kaspersky Lab suggest that 20% of small and medium businesses paying the ransom still did not recover their access afterwards.[5] Perhaps unsurprisingly, the standard advice is not to pay anyway, because it serves to reward the attackers and encourages the growth of the problem (as evidenced, for example, by the case of Kansas Heart Hospital, which paid up only to find the cyber-criminals returning with a further demand).[6] However, attackers can be virtually assured that some portion of victims will pay and even a small percentage will be enough for the economics to work in their favour. Moreover, those that pay up are not just end users. Findings from Bromium have suggested that an average of 10% of *security professionals* paid ransoms or hid breaches without notifying their teams.[7]

What tends to grab the headlines in any ransomware attack is the cost associated with paying the ransom. However, it is important to recognise that even if an organisation refuses to pay the ransom and has back-ups, there are significant costs associated with dealing with a ransomware attack. These include the IT costs associated with cleaning up computers, re-imaging machines and restoring data.

Clearly, the dilemma of whether or not to pay is one that most people would prefer to avoid altogether, which requires taking steps to avoid becoming a victim in the first place, as well as steps to mitigate the risks if the worst should still happen. With this in mind, it is worth looking at the biggest global ransomware outbreak to date and consider the extent to which its impact could have been lessened.

Makes you WannaCry

May 2017 saw a massive worldwide incident as a result of the WannaCry ransomware (also known as WannaCrypt or WanaCrypt0r). In concept this was no different from other ransomware that had become commonplace by this stage, and the user experience was the appearance of the ransom demand as illustrated in Figure 2.

"Even though Windows XP had been out of support since April 2014, a significant proportion of systems persisted in using it – indeed, its user base still exceeds that of Windows 8.1 and the Mac community"

What was different about WannaCry was the scale of the resulting incident and the realisation of why it was able to happen in the first place. The scale was far in excess of previous incidents, with reports suggesting infection of 200,000 computers across 150 countries (by contrast, Locky – a previous high-profile incident – affected 114 countries, but with numbers running into hundreds per country rather than thousands).[8,9] This in turn was linked to the means by which the incident had occurred. The malware exploited a Windows vulnerability that had first been publicised in Microsoft Security Bulletin MS17-010, which was released in mid-March 2017 and made the clear statement that the update was "rated Critical for all supported releases of Microsoft Windows".[10] As such, users running desktop versions of Windows from Vista onwards and Server versions from 2008, would have had two full months to have applied the patch.

FigurFigure 2: Payment demand from the WannaCry ransomware.

However, the key wording in the earlier quote is 'supported releases', meaning anyone still running versions of Windows predating these would remain unprotected. Notably, this does not mean that pre-Vista versions of Windows did not share the vulnerability; it simply meant that, having already passed their official end-of-life, Microsoft was no longer providing support for security updates and there was nothing for users to have downloaded to safeguard their systems. Nonetheless, even though Windows XP had been out of support since April 2014, Figure 3 illustrates that a significant proportion of systems persisted in using it – indeed, its user base still exceeds that of Windows 8.1 and the Mac community.

The scale of the WannaCry outbreak drew direct attention to the volume of systems still running vulnerable OS versions, with the media coverage of the resulting outage of UK National Health Service (NHS) systems drawing particular attention to their ongoing use of XP.[11] The severity of the incident quickly prompted Microsoft to take "the highly unusual step of providing a security update for all customers to protect Windows platforms that are in custom support only, including Windows XP, Windows 8 and Windows Server 2003".[12] As a result, those still running old systems quickly had a means to patch them as well.

However, despite the initial focus around the use of unsupported legacy systems, the subsequent analysis of the incident actually revealed that the majority of affected systems were running Windows 7 (with security industry findings suggesting between 67% and 97% of infections being on this platform).[13] On one level, this is not surprising, because in raw usage terms Windows 7 significantly outweighed that of XP, so there was a greater number of systems out there as potential targets. However, the notable and revealing point is that these were all patchable in advance and therefore any systems that got hit were avoidable incidents.

Lax admin

So why did so many remain unpatched? In the corporate context, it is possible to conjecture around lax administration. It's notable that WannaCry didn't affect *all* NHS trusts. Given that they all operate in similar conditions, it's tempting to suggest that the difference lies in effective housekeeping and that good network management practices can help to prevent an attack or, if one occurs, limit

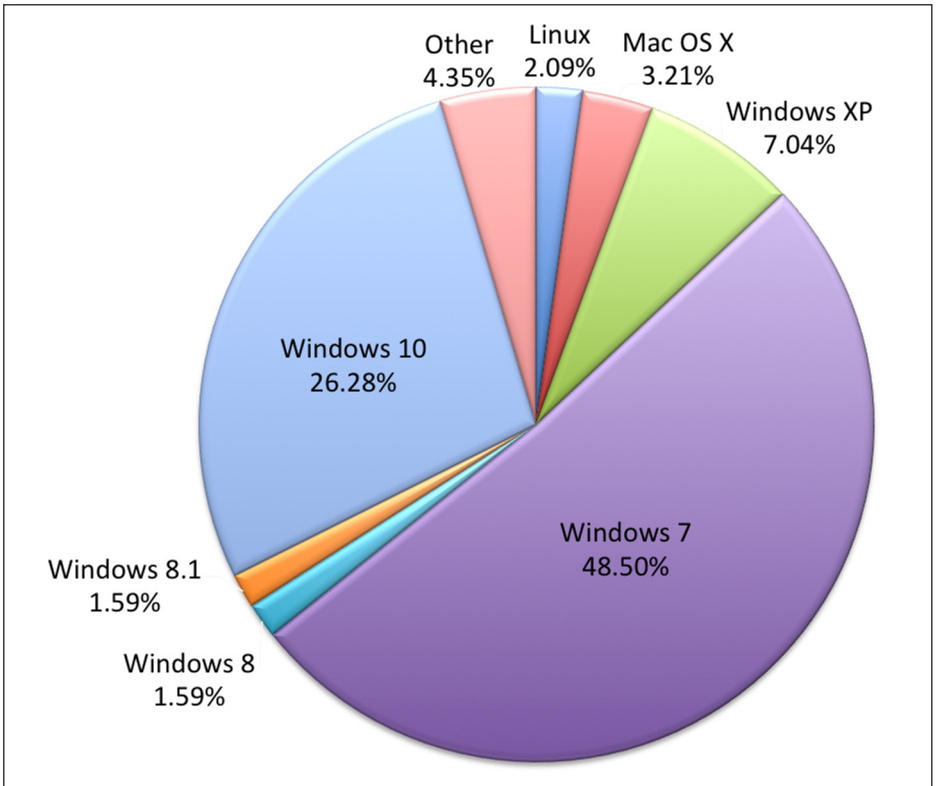


Figure 3: Desktop operating system market share at the time of the WannaCry outbreak. Source: NetMarketShare.

the spread of malware. This includes not assigning administrator rights indiscriminately, segmenting different parts of a network and limiting write access to data.

"The fact that unpatched systems are vulnerable to exploitation is very well-known and so perhaps the only thing that would not have been predicted was the scale of the vulnerability and the impacts that would result"

At the end-user level, laxity may also play a part, as well as the greater potential for lack of awareness. Even with supported versions of Windows, the potential for updating is variable. Depending upon how old a variant is being used, the user has different options and potential to defer updates until later. Looking, for example, at Figure 4, there is a notable contrast between the Windows 7 and Windows 10 approaches, with the current version basically mandating automated updates, whereas in the earlier version the user has the option to grant varying levels of autonomy to the process. This is notable not least because the use of earlier versions still vastly outnumbers Windows 10 and so there is a good chance that even though they *can* update automatically, many are likely to be configured not to do so. Moreover, some people find the update 'nag' messages annoying and the temptation is to keep putting them off because they get in the way.

The prominence of the incident prompted the UK's National Cyber Security Centre to update its ransomware guidance.[14] However, the key point was essentially to deploy a two-month-old patch if you were running the latest systems, or a one-day-old patch if your systems were already two or three years out of date!

The sad fact is that there is nothing new here and the core advice has all been offered many times before. The fact that unpatched systems are vulnerable to exploitation is very well known and so perhaps the only thing that would not have been predicted was the scale of the vulnerability and the impacts that would result. Of course, the scale and impact of WannaCry could have been much worse had a UK researcher not discovered a 'kill-switch' in the code that limited its spread (and if the authors hadn't included the kill-switch in the code in the first place).[15]

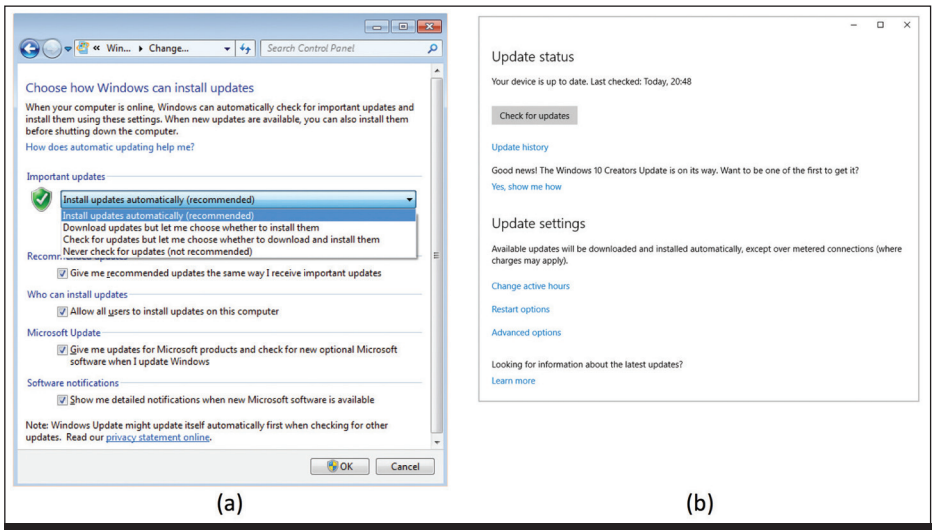


Figure 4: Windows Update configuration options in (a) Windows 7 and (b) Windows 10.

From extortion to NotPetya

Towards the end of June 2017, we saw reports of a new wave of ransomware attacks. The malware (known variously as ExPetr, Petya, Petrwrap and NotPetya) primarily targeted businesses in Ukraine, Russia and Europe – around 2,000 in total.[16] Like WannaCry, NotPetya used a modified version of the EternalBlue exploit, as well as using another exploit made public by the Shadow Brokers, called EternalRomance. The malware spread as an update to MeDoc (a Ukrainian accounting application) and through watering-hole attacks. Once inside the target organisation, the ransomware used custom tools to extract credentials from the system, which were then used to spread laterally within the infected network.

On the face of it, NotPetya seemed like yet another ransomware attack, with the attackers demanding £300 in bitcoins for the key to decrypt data.

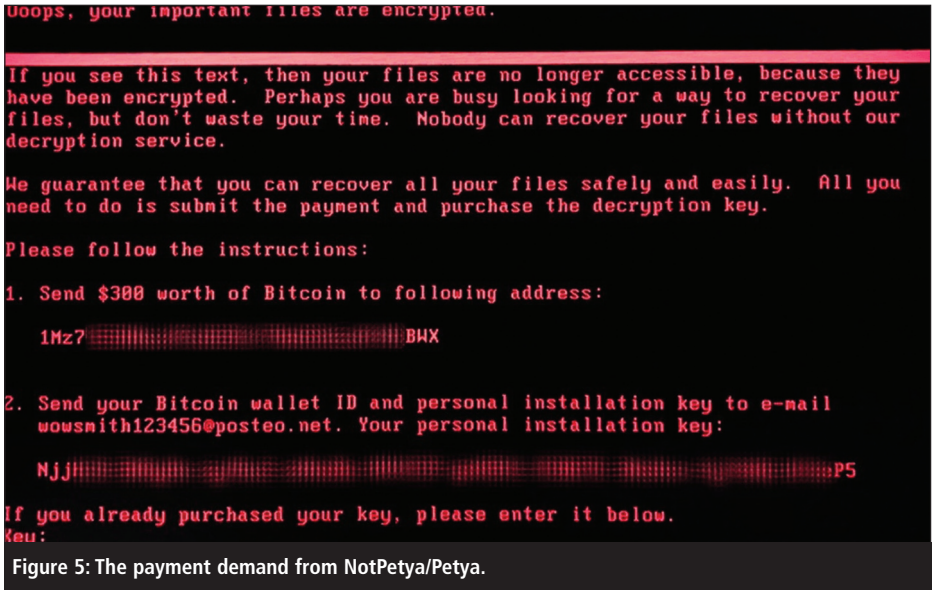


Figure 5: The payment demand from NotPetya/Petya.

However, unlike WannaCry, NotPetya also encrypted the Master File Table as well as the victim's files, and further analysis of the encryption routine revealed that it was not possible for the attackers to decrypt the victim's disks, even if the ransom demand was met, indicating that this was a 'wiper' masquerading as ransomware.

"Not only might ransomware attackers refuse to restore the victim's data, but they may not be able to"

The NotPetya attack throws into sharp relief the issue of paying the ransom. Not only might ransomware attackers refuse to restore the victim's data, but they may not be *able* to. What seems like ransomware might have an entirely different motive than making money.

Learning our ABC?

With incidents such as NotPetya offering no prospect of even paying to recover data, it is of even greater importance that the basics of preventative protection are rigorously followed. Therefore it is worth going back to the ABC list from which this article takes its title, to understand the relevance of each point:

- **Anti-malware:** Clearly, this is the direct defence against ransomware if it arrives on a target system. Normal caveats apply here, insofar as the protection may not be perfect and its effectiveness will depend upon signatures and other detection techniques having been kept up to date.
- **Back-up:** As already indicated, back-ups have a key role to play if the master copy of the data is encrypted by ransomware (or indeed lost or damaged through any other type of incident). Again, simply ticking the box that back-ups are taken is not a panacea; consideration also needs to be given to how and where they are stored (for example, back-ups to networked drives may be as easily reached by the ransomware as the original copies).
- **Critical patching:** Much of the opportunity for ransomware has come from systems that have not been updated to run the latest versions of operating systems and other key software and thus retain known vulnerabilities that attackers can exploit. Timely application of security-related patches and migrating away from platforms that are no longer supported, is therefore another import step in reducing the opportunity to fall victim.

In addition to the above, previously mentioned actions such as good network management (control of admin rights, network segmentation etc) will also help in reducing the scope of an attack.

It is also worth highlighting that the ABC protection is often available in a single product these days, especially for small and medium businesses. It also goes without saying that the advice is not new and is mentioned almost anywhere that has something to say about ransomware protection (for example, it is part of the standard advice from sites such as Get Safe Online (www.getsafeonline.org/protecting-yourself/ransomware/).[17] To illustrate the longevity of such advice, the snippets below are taken from the first security book that the first author ever read about security, with tips on back-up, dating back to 1985:[18]

- "The protection of data media against destruction demands the maintenance of back-up copies at other locations. It is a management responsibility as to which data are sufficiently critical and sensitive to require back-up but once the policy is established, the creation and storage of back-up copies away from the computer centre must be handled as a regular routine task".
- "Hold a number of generations of data files, possibly three generations, with each generation held in a different location".

Some of the language may be of another era, but the point is clear that back-up is something that ought to be recognised and done as standard. As an aside, the same book has nothing to say about anti-virus and software updates because it predates the emergence of malware or the notion of vendors pushing out security updates to software. Nonetheless, it shows just how long many have been ignoring the advice about back-up.

Cry no more?

Ransomware bucks the trend of malware by being obvious, whereas most malware is now deliberately unobtrusive. With a different type of attack, there might be no form of 'heads-up' at all, so if systems are unpatched they will be wide open and you will not know it.

"A significant part of the challenge is that systems should not be designed, developed and released with the vulnerabilities that ransomware and other attacks are able to exploit in the first place"

The WannaCry outbreak was an object lesson not only for ransomware but for our stance on security in general. For all the hype and even investment that surrounds cyber-security, what hit people was a lack of updating and not having back-ups. None of this is rocket science in terms of security and the entire ABC list is simply fundamental protection that ought to be practised regardless of ransomware coming along to remind us.

This problem is going to get worse and attacks are not going to stop. Moreover, some incidents may not be directly preventable. WannaCry was at least based on a known vulnerability, giving potential victims the advantage of at least the *opportunity* to have patched their systems. Future incidents may leverage a zero-day vulnerability, in which case anti-malware might not have helped and patching would not be an option. This leaves back-up as the remaining lifeline.

We are also likely to see ransomware evolving into wider contexts. It is already a threat across both desktop and mobile operating systems and it is easy to imagine the potential to hold other technologies to ransom. Attacks targeting Internet of Things (IoT) devices, smart homes and autonomous vehicles are all unfortunately well within the bounds of imagination. And it is equally hard to imagine that we will find ourselves naturally protected in these contexts when we have apparently failed to learn the lessons on the more established technologies to date.

Of course, there are lessons to be learned here beyond the user community and a significant part of the challenge is that systems should not be designed, developed and released with the vulnerabilities that ransomware and other attacks are able to exploit in the first place. This requires developers to take more direct account of security in their activities. It's worth noting, in this context, that many IoT devices are digital versions of devices that have delivered established functionality since long before the digital age – electricity meters, for example. And they are often brought to market by vendors whose primary focus isn't IT security. As a result, security is unlikely to be factored-in at the design stage. But as with the ABC list for users, there is again an underlying fact that these are not new insights. Even though the need for security-aware software development is well-established, the problem remains that it is not well-practised.

The '2017 Cyber Security Breaches Survey' report concluded that "the prevalence of ransomware in particular has heightened awareness and made cyber-security a more urgent issue for a wider range of businesses". In that sense, ransomware is potentially the trigger form action that organisations have otherwise been neglecting or under-prioritising. However, it is unfortunate that we continue to need such wake-up calls in order to attend to protection matters that ought now to be standard and routine.

About the authors

Prof Steven Furnell is a professor of information security and leads the Centre for Security, Communications & Network Research at Plymouth University. He is also an Adjunct Professor with Edith Cowan University in Western Australia and an Honorary Professor with Nelson Mandela University in South Africa. His research interests include usability of security and privacy, security management and culture, and technologies for user authentication and intrusion detection. He has authored over 280 papers in refereed international journals and conference proceedings, as well as books including Cybercrime: Vandalizing the Information Society *and* Computer Insecurity: Risking the System. *Furnell is the current chair of Technical Committee 11 (security and privacy) within the International Federation for Information Processing, and a member of related working groups on security management, security education, and human aspects of security. He is also a board member of the Institute of Information Security Professionals and chairs the academic partnership committee and southwest branch.*

David Emm is principal security researcher at Kaspersky Lab, a provider of security and threat management solutions, which he joined in 2004. He is a member of the company's global research and analysis team and has worked in the anti-malware industry since 1990 in a variety of roles, including that of senior technology consultant at Dr Solomon's Software, and systems engineer and product manager at McAfee. In his current role, Emm regularly delivers presentations on malware and other IT security threats at exhibitions and events, highlighting what organisations and consumers can do to stay safe online. Emm has a strong interest in malware, ID theft and the human aspects of security, and is a knowledgeable advisor on all aspects of online security.

References

1. '2017 Annual Threat Report'. SonicWall, February 2017. Accessed Sep 2017. www.sonicwall.com/whitepaper/2017-sonicwall-annual-threat-report8121810/.
2. 'Information technology – Security techniques – Code of practice for information security controls, ISO/IEC 27002:2013'. International Organisation for Standardisation, 1 Oct 2013. Accessed Sep 2017. www.iso.org/standard/54533.html.
3. '10 Steps to Cyber Security'. National Cyber Security Centre, 4 Aug 2016. Accessed Sep 2017. www.ncsc.gov.uk/guidance/10-steps-cyber-security.
4. 'Cyber security breaches survey 2017'. Department for Culture, Media & Sport, April 2017. Accessed Sep 2017. www.gov.uk/government/statistics/cyber-security-breaches-survey-2017.
5. Ivanov, A; Emm, D; Sinitsyn, F; Pontiroli, S. 'Kaspersky Security Bulletin 2016. The ransomware revolution'. Securelist, 8 Dec 2016. Accessed Sep 2017. https://securelist.com/analysis/kaspersky-security-bulletin/76757/kaspersky-security-bulletin-2016-story-of-the-year/.
6. 'Pay Ransomware and Attackers Come Back for More'. Cyber Sec Buzz, 26 May 2016. Accessed Sep 2017. https://cybersec.buzz/pay-ransomware-attackers-come-back/.
7. 'Cyber-criminals are winning: even security professionals admit to paying ransom and bypassing corporate security'. Bromium, 9 May 2017. Accessed Sep 2017. www.bromium.com/company/press-releases/cyber-criminals-are-winning-even-security-professionals-admit-paying-ransom.html.
8. 'Ransomware cyber-attack threat escalating – Europol'. BBC News, 14 May 2017. Accessed Sep 2017. www.bbc.co.uk/news/technology-39913630.

9. Sinitsyn, F. 'Locky: the encryptor taking the world by storm'. SecureList, 6 Apr 2016. Accessed Sep 2017. https://securelist.com/locky-the-encryptor-taking-the-world-by-storm/74398/.
10. 'Microsoft Security Bulletin MS17-010 – Critical Security Update for Microsoft Windows SMB Server (4013389)'. Microsoft, 14 Mar 2017. Accessed Sep 217. https://technet.microsoft.com/en-us/library/security/ms17-010.aspx.
11. Cellan-Jones, R. 'Ransomware and the NHS – the inquest begins'. BBC News, 15 May 2017. Accessed Sep 2017. www.bbc.co.uk/news/technology-39917278.
12. 'Customer Guidance for WannaCrypt attacks'. Microsoft, 12 May 2017. Accessed Sep 2017. https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/.
13. Goodin, D. 'WannaCry ransomware spread widely because of Windows 7, not XP'. ArsTechnica UK, 22 May 2017. Accessed Sep 2017. https://arstechnica.co.uk/security/2017/05/windows-7-not-xp-was-the-reason-last-weeks-wcry-worm-spread-so-widely/.
14. 'Ransomware: Latest NCSC Guidance'. National Cyber Security Centre, 13 May 2017. Accessed Sep 2017. https://www.ncsc.gov.uk/guidance/ransomware-latest-ncsc-guidance.
15. Newman, LH. 'How an accidental 'Kill Switch' slowed Friday's massive ransomware attack'. Wired.com, 13 May 2017. Accessed Sep 2017. www.wired.com/2017/05/accidental-kill-switch-slowed-fridays-massive-ransomware-attack/.
16. 'Schroedinger's Pet(ya)'. Securelist, 27 Jun 2017. Accessed Sep 2017. https://securelist.com/schroedingers-petya/78870/.
17. 'Ransomware'. Get Safe Online. Accessed Sep 2017. www.getsafeonline.org/protecting-yourself/ransomware/.
18. Lane, VP. 'Security of computer based information systems'. Macmillan Education, 1985.

Exposing fraudulent digital images

David Spreadborough, Amped Software


David Spreadborough

As a predominantly visual species, we tend to believe what we see. Throughout human evolution, our primary sense of sight has allowed us to analyse primeval threats. We are genetically hardwired to process and trust what our eyes tell us. Edgar Dale's cone of learning states that the brain retains information visually, over any other sensory stimulus.[1]

This innate hardwiring means that the arrival of digital images has posed a problem for the fraud investigation community. There are many different reasons why someone would want to maliciously alter a photo to 'tell a different story'. Although photos can be manipulated with ease, many people still harbour a natural tendency to trust photos as a true and accurate representation of the scene in front of us.

This innate trust in photos is engrained across all industries. Imagine the difficulty you would face by sketching your version of a contract with a pencil in a legal dispute, or submitting a painting as proof of a previously lost item when making a claim with an insurance company.

Digital manipulation

While this may sound a little extreme, photo manipulation techniques date back to the 19th century, almost as long as the history of photography itself. Modern digital manipulation tools have reached new levels of sophistication, with Photoshop now celebrating its 27th birthday. Such software can craft fantasies pixel by pixel, leaving the human eye none the wiser. Participants in a recent study could only spot irregularities in a doctored image 45% of the time.[2]

Even smartphone apps can alter images at the click of a button. Nowadays, children of primary school age can capture high-quality images, edit them and share with just a few finger swipes on their phones. It is easy to see how even minor changes can tell an entirely different story. For example, a quick rearrangement of words and letters on a document can change dates, statements and price quantities. Or the addition of just one face into a crowd scene creates an alibi out of thin air.

"Until now, many people have trusted the photographic image as being a true and accurate representation. This is evident in the news and media, where scandals of tampered images being 'fake news' run rife"

We cannot be so naive as to believe that fake images do not end up in fraud investigations. This is evident in the news and media, where scandals of