ELSEVIER

network SECURITY

ISSN 1353-4858 October 2016

www.networksecuritynewsletter.com

Featured in this issue:

The DNC server breach: who did it and what does it mean?

In June 2016, the computer networks of the US Democratic National Committee (DNC) were hacked. As a result, a number of documents were leaked online.

Security companies analysed the breach and quickly came to the conclusion that the hackers were based in Russia. But what does it tell us about the role of cyber-attacks in modern politics? And what lessons can organisations learn for their own security? Michael Buratowski of Fidelis Cyber-security examines the hack and draws some conclusions.

Full story on page 5…

Ransomware: taking businesses hostage

Europol recently declared ransomware to be the biggest cyber-threat facing European businesses and citizens. Both the nature of the chief targets and the ways in which they are being attacked are changing quickly as criminals spot new opportunities for extorting money.

A large proportion of organisations have been affected at some time, with cyber-criminals apparently turning their attentions to those that are most vulnerable, such as hospitals. The ransomware itself is evolving too, and while some of it is poorly executed, the most advanced strains show great sophistication. Steve Mansfield-Devine explores the nature of the threat and how businesses should respond.

Full story on page 8…

Ransomware: threat and response

How and why is the ransomware scourge growing? And what can organisations do about it?

In this interview, Tim Erridge of Context Information Security, explains the kind of damage to businesses that can result from an infection, discusses the dilemma of whether to pay the ransom, explores how you can protect yourself and speculates on how the threat will evolve in the future.

Full story on page 17…

US officially accuses Russia of DNC hack while election systems come under attack

US intelligence agency officials have now openly blamed Russian hackers for the theft of emails from the Democratic National Committee (DNC).

"The US intelligence community is confident that the Russian Government directed the recent compromises," said a joint statement by the Department of Homeland Security (DHS) and Office of the Director of National Intelligence.

The statement went on to say that the leaks were "consistent with the methods and motivations of Russian-directed efforts" and are intended to "interfere with the US election process. Such activity is not new to Moscow – the Russians have used similar tactics and techniques across Europe and Eurasia, for example,

Continued on page 2...

Contents

Editorial Office:
Elsevier Ltd
The Boulevard, Langford Lane, Kidlington,
Oxford, OX5 1GB, United Kingdom
Tel: +44 1865 843239
Web: www.networksecuritynewsletter.com

Publishing Director: Bethan Keall

Editor: Steve Mansfield-Devine
E-mail: smd@contrarisk.com

Senior Editor: Sarah Gordon

Columnists: Karen Renaud, Colin Tankard

International Editoral Advisory Board:
Dario Forte, Edward Amoroso, AT&T Bell Laboratories; Fred Cohen, Fred Cohen & Associates; Jon David, The Fortress; Bill Hancock, Exodus Communications; Ken Lindup, Consultant at Cylink; Dennis Longley, Queensland University of Technology; Tim Myers, Novell; Tom Mulhall; Padget Petterson, Martin Marietta; Eugene Schultz, Hightower; Eugene Spafford, Purdue University; Winn Schwartau, Inter.Pact

Production Support Manager: Lin Lucas
E-mail: l.lucas@elsevier.com

Subscription Information
An annual subscription to Network Security includes 12 issues and online access for up to 5 users.
Prices:
€1424 for all European countries & Iran
US$1594 for all countries except Europe and Japan
¥189 000 for Japan
Subscriptions run for 12 months, from the date payment is received.
More information:
http://store.elsevier.com/product.jsp?isbn=13534858

12987

Pre-press/Printed by
Mayfield Press (Oxford) Limited

...Continued from front page

to influence public opinion there." It added: "We believe, based on the scope and sensitivity of these efforts, that only Russia's senior-most officials could have authorised these activities."

The "similar tactics" include using sites such as DCLeaks.com and Wikileaks to publish the stolen data. A hacker (or team) using the name 'Guccifer 2.0' has also cropped up multiple times in investigations into a variety of breaches. The joint statement is available here: http://bit.ly/2erkJfP.

A number of organisations affiliated with the Democratic Party have come under attack in recent months – apparently the work of two separate Russian groups known in the security community as Cozy Bear (aka APT 29), believed to be linked to Russia's military intelligence service the GRU, and Fancy Bear (aka APT 28).

There have been attempts to breach voter registration systems in at least 20 US states. These were of sufficient severity to prompt the DHS to get involved, although it's been confirmed that data was taken from only two – Arizona and Illinois – with possibly another two having been breached in some way. According to FBI director James Comey, the hackers – widely assumed to be Russian – have been "poking around". In a statement, he said: "We are urging the states just to make sure that their deadbolts are thrown and their locks are on and to get the best information they can from DHS just to make sure their systems are secure. And again, these are the voter registration systems. This is very different than the vote system in the United States which is very, very hard for someone to hack into because it's so clunky and dispersed."

The DHS has created an Election Infrastructure Cybersecurity Working Group to bolster security and offer services to individual states.

"These services include cyber 'hygiene' scans of Internet-facing systems, risk and vulnerability assessments, information sharing about cyber incidents, and best practices for securing voter registration databases and addressing potential cyber-threats," the DHS said.

The veracity of the leaks coming from Russia and via sites such as Wikileaks has been called into question after suggestions that data stolen from the World Anti-Doping Agency (WADA) had been altered before being leaked. The Fancy Bear group apparently leaked the documents from WADA's Anti-Doping Administration and Management System (ADAMS) in retaliation for Russian athletes being banned from the Olympics. But WADA said that "not all data released by Fancy Bear (in its PDF documents) accurately reflects ADAMS data".

The attackers were able to gain access to the ADAMS database after they obtained login credentials via phishing.

Bellingcat, a 'citizen journalist' organisation that has been actively investigating the shooting down of Malaysian Airlines flight M17 by a Russian missile over Ukraine, has come under repeated cyber-attack.

"From February 2015 to July 2016 three researchers at Bellingcat – [Eliot] Higgins, Aric Toler and Veli-Peka Kivimaki – who had contributed MH17 articles received numerous spear-phishing emails, with Higgins alone receiving at least 16 phishing emails targeting his personal email account," said researchers at ThreatConnect. Domains and IP addresses used by the attackers match those associated with the Fancy Bear group.

Russian hackers are now also being blamed for a cyber-attack against French TV station TV5Monde in April 2015 – an attack that was originally claimed by a pro-Daesh group calling itself the 'Cyber Caliphate'.

The station's director, Yves Bigot, recently told the BBC that: "We were saved from total destruction by the fact we had launched the channel that day and the technicians were there. One of them was able to locate the very machine where the attack was taking place and he was able to cut out this machine from the Internet and it stopped the attack."

Coming just a couple of months after the *Charlie Hebdo* attacks, the claim by an Islamic extremist group had credibility. But investigation by law enforcement agencies now point to the Fancy Bear group. It took the station several months before it could reconnect to the Internet. Bigot put the cost of remediation at $5.6m.

In brief

New SSH exploit

Akamai Technologies' Threat Research team has identified a recent spate of attacks in which Internet of Things (IoT) devices are being used to remotely generate attack traffic. This exploits a 12-year old vulnerability in OpenSSH which Akamai is calling SSHowDowN Proxy. The attacks originate from such devices as CCTV and other video surveillance systems, satellite antenna equipment, networking devices (including routers, access points, cable and ADSL modems, etc), and Internet-connected Network Attached Storage (NAS) systems. Other devices could be susceptible as well. Compromised devices are being used for mounting attacks against a multitude of Internet targets and Internet-facing services, such as HTTP and SMTP as well as network scanning and mounting attacks against internal networks that host these connected devices. Once malicious users access the web administration console of a vulnerable device they are able to compromise the device's data and, in some cases, fully take over the machine. Akamai recommends changing passwords from the vendor defaults. If the device offers direct file system access, add 'AllowTcpForwarding No' into the global sshd_config file and 'no-port-forwarding' and 'no-X11-forwarding' to the ~/ssh/authorised_ keys file for all users. If neither option above is available, or if SSH access is not required for normal operation, disable SSH entirely via the device's administration console. If the device is behind a firewall, consider disabling inbound connections from outside the network to port 22 of any deployed IoT devices and/or disabling outbound connections from IoT devices except to the minimal set of ports and IP addresses required for their operation. The report is available here: http://akamai.me/2d7nIcW.

Security fears damaging the economy

A reluctance to use apps and engage with businesses digitally has cost the UK economy nearly $2.5bn in the past year alone, according to research by Rackspace. A third of the people surveyed said that privacy concerns were a major disincentive, slightly more (36%) are reluctant to use apps out of security concerns and a quarter said a failure in apps had prevented them from doing something important. Next year, these fears could cost the app industry as much as $3.6bn, suggesting that security worries are getting worse, not better.

Twitter cuts off feed to law enforcement

A company that was selling social media monitoring services to law enforcement agencies as a way of monitoring activists has had its data feed cut off by Twitter. Geofeedia was the subject of a report by the American Civil Liberties Union (ACLU) which showed how it used data bought from Twitter, Facebook and Instagram to track targeted people. Facebook and Instagram stopped selling data to the firm, but it continued to get tweet data via a Twitter subsidiary. Twitter attempted to impose limitations on how the data was used. When that didn't work it attempted a cease and desist letter in an attempt to get Geofeedia to change the way it was exploiting the information. Now it has cut off the data stream altogether. There's more information from the ACLU here: http://bit.ly/2e9kWBd.

UK police run vulnerable sites

A quarter of UK law enforcement websites are insecure, according to research by the Centre for Public Safety. Its review of 71 websites found that more than 25% were not using SSL/TSL connections (HTTPS). Of those, 12 police forces or other agencies allowed users to submit personal data – in some cases information relating to a crime – via these unsecured pages. Only 27% of the sites came up to international security standards. Strangely, these seemed to be the organisations with the most limited budgets and resources. The Metropolitan Police Authority, the biggest and most well-funded force in the country, earned only a middling cyber-security grade. And like many other forces, it appears that its website might still be vulnerable to the Poodle attack because of the use of outdated protocols. There's more information here: http://bit.ly/2dXu6Dw.

Firms fail to scan clouds

Most firms either don't scan the cloud services they use for malware or don't know if they do. This is the conclusion reached by research carried out by Netskope and the Ponemon Institute. The 'Cloud Malware and Data Breaches: 2016 Study' also found that while 36% of business applications are now stored in the cloud, fewer than half of them are known, officially sanctioned or approved by IT departments. While people understand the risk of data breaches, nearly a third could not determine if they had been breached or what types of data were lost in the breaches. Over half of respondents say the use of cloud services significantly increases the likelihood of a data breach, yet the majority have neither visibility nor have they taken the correct precautions to prevent breaches involving the cloud. For companies that did experience a data breach in the past year (19%), 38% say it was the cloud service itself that was breached. However, 30% don't have any idea how the breach occurred, and 33% could not determine what data was lost or stolen. Of those organisations that do inspect the cloud for malware, 55% say they found it. The report is available here: http://bit.ly/2dJrTLg.

Pupil database used to target immigrants

In spite of ministerial promises to the contrary, it appears that the UK Government's National Pupil Database has been used to target immigrant families. In response to a Freedom of Information request, the Department for Education (DfE) said that the database, which contains information on 20 million children dating back to 2000, has been used to counter the "abuse of immigration control". Data from the annual census carried out by schools was passed to border control officials even though, when answering Parliamentary questions in July, Nick Gibb, Minister for School Standards, said that no-one outside the DfE would be granted access to the data. He said: "The data will be collected solely for internal departmental use for the analytical, statistical and research purposes. There are currently no plans to share the data with other government departments unless we are legally required to do so." However, in its response, and in earlier FOI requests, the DfE has admitted that the data is made available to the police and the Home Office. The DfE response is available here: http://bit.ly/2dL0WFN.

Three-quarters of firms hit by DDoS

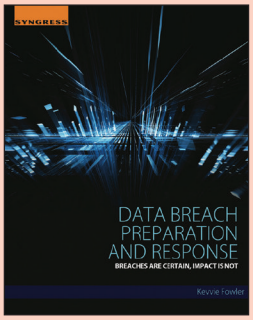
Research by security firm Neustar has concluded that nearly three-quarters of organisations have been hit by a distributed denial of service (DDoS) attack in the past year – and 85% of those had been hit multiple times. Around half of the victims said the attacks cost them up to $100,000 an hour during peak periods, and for a third of firms this went up to $250,000 an hour. Nearly three-quarters of the firm took up to an hour to recognise the DDoS attack for what it was and another hour to respond. More than half the companies were hit with multi-vector attacks in which malware and ransomware were also deployed. Sub-saturation attacks, where DDoS is used to mask other hacking activity, are also becoming more common. The report is available here: http://bit.ly/2d7GP6G.

Second group attacks Swift

Symantec says it has identified a second group, dubbed Odinaff, that is targeting the Swift inter-banking service. As many as 20 organisations may have been infected with malware designed to give the attackers access to the Swift messaging system, which in turn would allow them to initiate funds transfers. This follows breaches at the beginning of this year carried out by a gang known as Lazarus which, among other exploits, stole $81m from the Bank of Bangladesh. Symantec is sharing technical details of its findings with banks, governments and other security companies.

Reviews

BOOK REVIEW



Data Breach Preparation and Response
Kevvie Fowler. Published by Syngress.
ISBN: 9780128034514.
Price: €50.95, 254pgs, paperback and e-book editions available.

These days, everyone will tell you that it's not a matter of if your organisation will be breached but when. It's a truism repeated often enough to be annoying. And it's true enough to be scary.

Even more frightening is the fact that when the computer systems of organisations are breached these firms often don't know about it for a considerable time – 10 months is one figure that has been bandied around recently. And many of them never find out for themselves – they are informed of the compromise by researchers, security firms or law enforcement agencies after the organisation's data has been found being traded on underground forums.

No organisation is immune from attack. The notion that "hackers wouldn't be interested in little old me" has never been true. And now every firm has data or systems that are of value to criminals, industrial spies and other bad actors. If you haven't prepared for an attack then you'd better prepare for the aftermath.

The real issue here is suggested by this book's subtitle: 'Breaches are certain, impact is not'. Actually, the sad truth is that, for the overwhelming majority of organisations, some kind of impact *is* certain – because they have not anticipated a breach and have no idea how to respond when it happens. And if you imagine that applies only to smaller, under-resourced firms, then think back over the headlines of the past couple of years and reflect on the big names that have been forced to do the digital equivalent of the walk of shame.

It would be reasonable to argue that no organisation can be 100% prepared for a breach, just as no security is 100% foolproof. But the more effort you put into detecting, stopping and remediating a breach the less damaging it's going to be. And that damage can be significant. For example, TalkTalk's breach resulted in a loss in stock value of 11% and a reduction in revenues of £80m in the quarter following the attack, partly as a result of having lost an estimated 101,000 customers. It was also fined £400,000 by the Information Commissioner's Office – and on that score it can consider itself lucky. If the forthcoming EU General Data Protection Regulation (GDPR) had already been in force, the fine could have been up to £70m.

This book provides guidance on how to deal with every aspect of a breach. And that starts with understanding what your attackers want and how they operate. That's important because it provides the right perspective when you look at your data and decide what is valuable – to cyber-criminals, industrial spies and even nation states – and therefore what you most need to protect.

The author, Kevvie Fowler, details the classic breach lifecycle that highlights how speed – of detecting the breach and responding to it – is important, but so is reacting in the right way. Without the right information, some of it gleaned before you are attacked from threat intelligence sources, you may find yourself responding to the wrong kind of attack. A common example these days is the sub-saturation distributed denial of service (DDoS) attack. These are designed to look like a crude attempt to knock your organisation offline. In fact, they carefully leave you with just enough bandwidth for the attackers to sneak into your systems – unnoticed because you're busy dealing with the DDoS assault – and carry out other forms of hacking, such as stealing data.

If you haven't already thought about what you'd do in the event of a breach by the time the alarms start going off, then you're in trouble. So Fowler starts with how you need to create and test a Computer Security Incident Response (CSIR) plan that you can invoke the moment you suspect something is wrong.

Detection is the next stage, and one important aspect that has to be dealt with in a timely manner is to decide whether you're under attack at all. False alarms are common. For example, someone scanning your network ports is not the same thing as an attack, although it may be an indication that hackers are probing your defences. Most network managers will tell you that scans are a daily occurrence. So how do you decide whether this is a threat deserving of a heightened state of readiness?

You need to understand when to invoke that CSIR plan as well as who and what needs to be involved. For example, at what stage do you need to engage public relations and legal teams? And are you going to require the services of outside forensic specialists, or is the attack something you can deal with yourself?

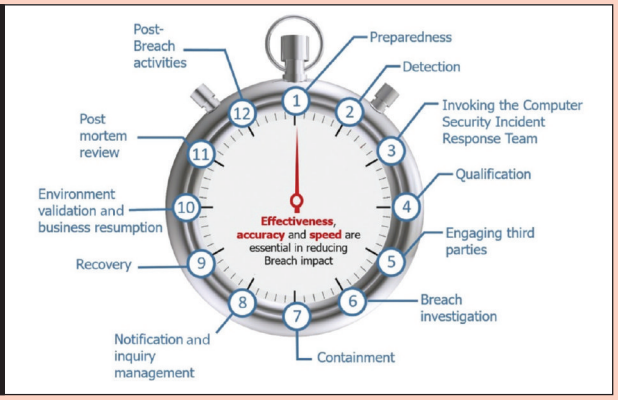
Clearly you need to be able to contain the breach – to shut it down or at least stop it from spreading. But then comes much of the hard work. Notification is a tricky topic – who do you tell about the breach and what do you tell them? This is something that can get you into deep trouble these days, from both legal and public relations perspectives. Good communication could make the difference between a survivable dent to your reputation and your organisation being forced out of business in a hail of lawsuits and regulatory fines.

There follows the inevitable remediation, cleaning up and repairing your systems and getting the business running again. And you can't simply go back to how you were before because that was a situation that led to you being breached. This step has to involve a full post-mortem on what went wrong and how to fix it. And how do you know you can trust the newly restored and improved system?

There is one other bit of preparation you need to do, covered in Fowler's final chapter, and that's getting ready for the inevitable litigation. In the recent breach of Yahoo's email servers, a class-action suit was filed in California within two days of the public notification. Lawyers represent a critical part of your data breach team.

This book provides a thorough grounding in all the aspects of preparing for, dealing with and mopping up after a data breach and is likely to present issues you hadn't considered.

– SM-D



The breach lifecycle. Responding quickly, accurately and effectively is essential.

The DNC server breach: who did it and what does it mean?

Michael Buratowski

Michael Buratowski, Fidelis Cybersecurity

With all that has been happening in UK politics over recent months, it is easy to forget that the US has also been at the centre of some serious political controversy. On 14 June 2016, the computer networks of the US Democratic National Committee (DNC) were hacked. As a result, a number of documents were leaked online, including plans to spend more than £600,000 on a 'counter-convention' to compete with the Republican National Convention (RNC), as well as internal memos, financial spreadsheets and planning documents.

Two groups of hackers were reported to have infiltrated the network, one of which had been on the inside for approximately a year. While the other group had been there for a much shorter amount of time, evidence suggests it was on the hunt for specific information. Both groups were removed from the system before the DNC publicly announced the breach. Most of the interest in this cyber-attack centred on the uncertainty around who was responsible.

The hack of the Democratic National Congress is widely believed to be an attempt to destabilise the US political process, including the presidential campaign of US Secretary of State Hillary Clinton.

Initial blame

A blog by cyber-security vendor Crowdstrike, the company that conducted the initial breach forensics, concluded that the incident was attributed to Advanced Persistent Threat (APT) actors associated with the Russian Government named 'Cozy Bear' and 'Fancy Bear'.[1] Shortly after this blog was published, an individual by the name of 'Guccifer 2.0' came forward to claim that he had been the one to penetrate the DNC's servers. In response to the uncertainty surrounding who was responsible for the breach, Fidelis Cybersecurity was approached by personnel handling the investigation for the DNC and carried out an independent investigation to pinpoint the perpetrator as well as provide its own perspective on the intrusion.

Before delving into the findings from the Fidelis analysis, it is useful to first understand the many different names that security researchers have used to refer to these threat actors. It is also important to note that actor mappings between attribution sets are not precise. Different research methodologies and necessarily separate encounters with these actors lead to unique attributes sets. However, the overlaps noted in Table 1 are commonly accepted within the security industry.

Investigation highlights

As part of Fidelis Cybersecurity's investigation, it reverse engineered the malware samples from Crowdstrike that matched the description, form and function in the DNC incident. In doing this, Fidelis found that the malware contained complex coding structures and utilised obfuscation techniques that the company has seen advanced adversaries utilise in other investigations it has conducted.

In addition, the malware used was similar and, at times, identical to the malware that other vendors have associated with these actor sets. For instance, in a blog by Palo Alto Networks, it provided detailed reverse engineering and analysis on other malware that it attributed to Cozy Bear named 'SeaDuke'.[2] Fidelis noted that

Crowdstrike	FireEye	Palo Alto Networks	Kaspersky	Microsoft	Sample malware names
Cozy Bear	APT 29	CozyDuke	CozyDuke		ADobeARM, ATI-Agent, SeaDaddy, Mimikatz, SeaDuke and MiniDonis
Fancy Bear	APT 28	Sofacy	Sofacy	Strontium	Sofacy, X-Agent, X-Tunnel, WinIDS, Foozer

Table 1: Threat actor naming protocols, by security vendor.

in the samples of 'SeaDaddy' that were provided to the company from the DNC incident, there were nearly identical code obfuscation techniques and methods. In fact, once decompiled, the two programs were very similar in form and function and they both used identical persistence methods (Powershell, a RUN registry key, and a .lnk file stored in the Startup directory). What's more, the SeaDaddy sample had a self-delete function named 'seppuku' which was identified in a previous SeaDuke sample described by Symantec and attributed to the Cozy Bear APT group. It's worth noting that seppuku is a Japanese word for hara-kiri, or self-disembowelment.

Another piece of malware discovered during the DMC breach was X-Tunnel – malware that is associated with Fancy Bear. Again, the Fidelis investigation confirmed some distinct features. First, a sample component in the code was named 'Xtunnel_Http_Method.exe'. This had previously been reported by Microsoft and attributed by the company's researchers to Fancy Bear (or 'Strontium' as it calls the group) in its Security Intelligence Report Volume 19. Second, there was a copy of OpenSSL embedded in the code – or, to be more specific, version 1.0.1e from February 2013, which was reported by Netzpolitik and attributed to the same attack group in 2015.[3] Third, the Command and Control (C2) IPs were hardcoded into the sample provided, which also matched the Netzpolitik's report. Finally, the arguments in the sample were also identical to those picked up by Netzpolitik.

The size of the malware samples was also flagged in the investigation. The malware samples were conspicuously large – 1.9MB for X-Tunnel and 3.1MB for SeaDaddy – and contained all or most of their embedded dependencies and function code. This is a very specific *modus operandi* that less sophisticated threat actors do not generally employ.

What does all this mean?

Based on the independent investigation carried out by Fidelis, the company found that Crowdstrike was correct in concluding that the Cozy Bear and Fancy Bear APT groups were involved in the intrusions at the DNC. The malware samples from the breach contained data and programming elements that were similar to malware that Fidelis had already encountered in past incident response investigations, which were attributed to these specific threat actors. In addition, Crowdstrike, as well as several other security firms, independently analysed and published its own findings on the malware samples. It too found the malware to be similar to, if not identical to, those used in the DNC incidents. Many of these firms also attributed the malware to Russian APT groups.

"A huge problem that companies face is that IT teams usually receive an abundance of alerts on a daily basis indicating a potential incident. They then have to review and triage those incidents, making validating whether an incident is real or not exceptionally time-consuming and error-prone"

This brings us to the issue of Guccifer 2.0 claiming responsibility for the attack and for the subsequent leak of documents to news sites. These included information on Donald Trump and Hilary Clinton as well as convicted Democratic Party donors. Investigations by security researchers do, however, cast doubt on the legitimacy of these claims. The virtual machine that leaked the documents to the media was indeed using a Russian language setting. This has sparked rumours that Guccifer 2.0 was actually a 'red herring' planted by the Russian Government as a tool to deny they had any involvement in the attack.

How to protect yourself

It's not unusual for malware to reside on a network for a long time before it is detected, as we saw with one group that hacked the DNC servers. The DNC hack serves as a wake-up call for all companies to continually monitor all of the network and endpoints for anomalous and potentially malicious activity. This monitoring is vital if businesses are to stay one step ahead of the hackers. In particular, alerts should be set up so that IT teams are notified whenever an unusual amount of data is being exfiltrated – in such instances, it's even possible to automatically quarantine the activity – shrinking the time it takes to detect, investigate, analyse and resolve a security incident.

It is worth noting that a huge problem companies face is that IT teams usually receive an abundance of alerts on a daily basis indicating a potential incident. They then have to review and triage those incidents, making validating whether an incident is real or not exceptionally time-consuming and error-prone for analysts. In order to improve response to these incidents, companies should look into automating processes – for example, reducing the number of manual steps required to piece together data from multiple sources and streamlining workflows to shrink the time it takes to detect, investigate, analyse and resolve an incident.

Consider an RDRM

By adopting a Rapid Detection and Response Model (RDRM), companies will be able to accelerate their ability to detect, investigate and stop attacks by ensuring that the organisation is prepared from a people, process and technology perspective.

Step one: Identify. The purpose of the 'identify' step is to create situational awareness of the organisation's threat environment by identifying technology and process gaps that lead to blind spots. It establishes a baseline understanding of a company's ability to manage cyber-security risks and an organisation's incident response maturity level. For example, this step involves documenting existing security infrastructure, analysing the capabilities of security technologies and examining operational processes, as well as reviewing detection and responsible metrics and evaluating the threat landscape.

Step two: Prepare. The 'prepare' step

makes use of the analysis and situational awareness obtained in the identify step to close gaps that hinder an organisation's ability to efficiently detect, respond to and resolve incidents. Many organisations have invested in a collection of security technologies, but may not be experiencing the full benefit of their investment due to poor integration, unnecessarily complex processes or unused functionality. Also, organisations often put security tools in place as a reaction to a breach instead of in preparation for one. The RDRM helps you accelerate rapid detection and response by focusing attention on technology that makes security personnel better and faster.

Step three: Detect. Advanced, targeted attacks are not instantaneous events. These persistent attacks involve a series of actions and phases staged to occur over a prolonged period of time. Professional cyber-criminals are so adept at cloaking their activities that they routinely go unnoticed for months and often years. In the case of the DMC, the malware lay hidden for around 12 months. Such covert operations require hackers to conduct detailed reconnaissance missions. If deemed necessary, they will even develop custom-tailored exploits to penetrate enterprise networks and steal sensitive corporate data, intellectual property, business plans and personal information. Detecting security incidents as early in the attack lifecycle as possible is paramount to an organisation's security. It also lowers the complexity and costs associated with breaches. Simply put, the less damage the malware has done, the easier and cheaper it is to remedy.

Step four: Respond. During the 'respond' step, security teams confirm, analyse and document attacks that they have detected in the previous phase. The goal is to assess the impact so an appropriate strategy to remediate and resolve the incident can be developed. This is where most organisations face severe challenges, including poor metrics for response and remediation.

Consolidate and integrate

Rapid detection and response is not a new concept: it has been undertaken by leading security operations centres and incident response teams for many years through tremendous in-house efforts, with dedicated programmers to integrate and automate a multitude of disparate point products. Thankfully, the security vendor ecosystem has been moving in the direction of consolidating and integrating complementary capabilities, making rapid detection and response technologies more accessible.

"Russian hackers – whom many say are among the best in the world – could have been attempting to destabilise the US political system, more particularly the Democratic Party, in order to add weight to the Republican campaign"

As organisations struggle to overcome talent shortages, keep up with modern threats and reduce risk, efficiency has become a necessity. The stakes are too high and there simply aren't enough skilled people to continue relying on overworked, scarce experts. By embracing an RDRM, organisations can disrupt attack lifecycles and achieve a faster and much more effective incident response that comes from greater visibility and context, consolidation and integration of security tools and automation of mundane steps.

The threat of cyberwar

While the DNC server breach is a strong reminder to all companies that they must up the ante when it comes to their own cyber-security, it also demonstrates the very real threat of cyberwar on a global scale. For hackers, it's no longer only about causing disruption and making a statement, it is also about espionage and surveillance.

In the case of the DNC, Russian hackers – whom many say are among the best in the world – could have been attempting to destabilise the US political system, more particularly the Democratic Party, in order to add weight to the Republican campaign. Although this is purely speculation, it would not be the first time Russian hackers have made a beeline for US government information. For example, the White House's computer systems were hacked back in April 2015, reportedly by Russian hackers who had obtained access to email correspondence involving White House employees, many of whom were in contact with President Barack Obama.

Ultimately, much as with traditional espionage, governments and other intelligence agencies across the globe use cyber-espionage to gather valuable information. It's safe to conclude that the DNC breach wasn't the first – and certainly won't be the last – time we see an attack of this nature.

About the author

Michael Buratowski is senior vice-president, cyber-security services at Fidelis Cybersecurity (www.fidelissecurity.com) and is responsible for managing the company's network defence and forensics business area, including the Digital Forensics Lab. Prior to joining Fidelis, he was the business area director for the Cyber Operations Solutions business and programme manager for the US-CERT contract in the Cyber Division of General Dynamics Advanced Information Systems. Buratowski also served in various operational roles at General Dynamics.

Reference

1. Alperovitch, Dmitri. 'Bears in the Midst: Intrusion into the Democratic National Committee'. Crowdstrike, 15 Jun 2016. Accessed Sep 2016. www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.
2. Grunzweig, Josh. 'Unit 42 Technical Analysis: Seaduke'. Palo Alto Networks, 14 Jul 2015. Accessed Sep 2016. http://researchcenter.paloaltonetworks.com/2015/07/unit-42-technical-analysis-seaduke/.
3. 'Digital Attack on German Parliament: Investigative Report on the Hack of the Left Party Infrastructure in Bundestag'. Netzpolitik.org, 19 Jun 2015. Accessed Aug 2016. https://netzpolitik.org/2015/digital-attack-on-german-parliament-investigative-report-on-the-hack-of-the-left-party-infrastructure-in-bundestag/.

Ransomware: taking businesses hostage

Steve Mansfield-Devine

Steve Mansfield-Devine, editor, *Network Security*

Cybercrime has its fashions. As technologies evolve and defences improve, so hackers and cyber-criminals modify their methods of attack. We're currently seeing a burgeoning in the use of ransomware, the digital form of blackmail in which your computer is effectively taken hostage. And both the nature of the chief targets and the ways in which they are being attacked are changing quickly as criminals spot new opportunities for extorting money.

The rise of ransomware

In its 'Internet Organised Crime Threat Assessment' (IOCTA 2016) report, Europol classed ransomware as the "dominant concern for EU law enforcement".[1] Other reports presented a similarly bleak outlook. In its 'McAfee Labs Threats Report' for Sept 2016, Intel Security said it had seen a 127% rise in ransomware malware samples over the past year.[2]

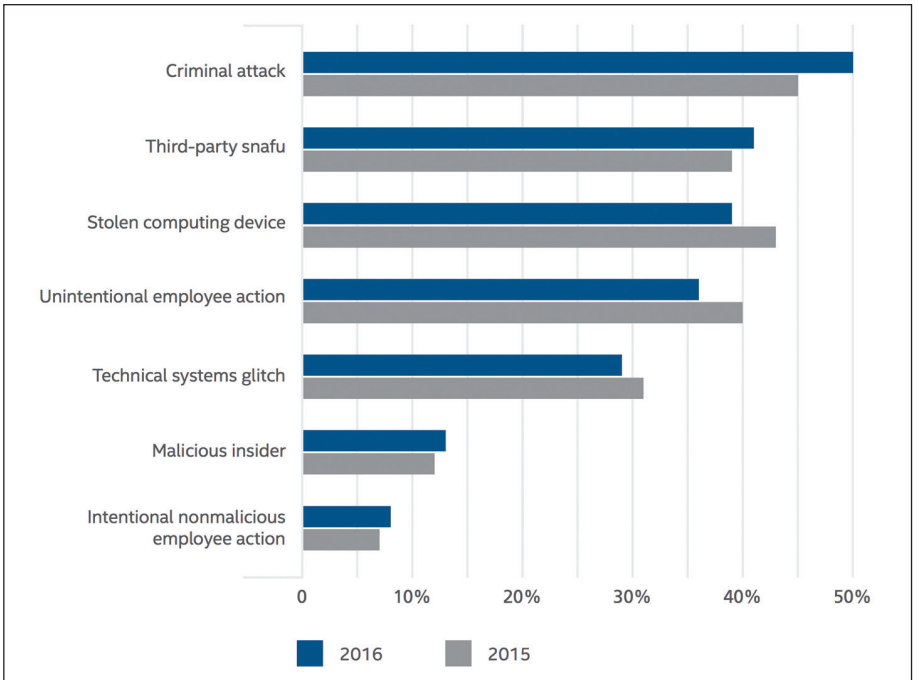
Meanwhile, Trend Micro found that 44% of businesses it surveyed had suffered at least one ransomware infection in the previous two years, with 27% having been hit more than once. Nearly two-thirds (65%) of the affected firms paid the ransom. In its report for the first half of 2016, Trend Micro said it had seen 79 new ransomware families, compared to 29 for the whole of 2015.[3]

More than half of all malware files targeting UK Internet users contained some form of ransomware in 2015, according to data collected by Bitdefender, which also said that recent forms of ransomware, such as CryptoWall 4.0, have become increasingly hard to detect and almost impossible to stop.

The rapid rise of ransomware suggests that it's a profitable form of attack for cyber-criminals. Proofpoint dubbed it a "billion dollar industry" and other figures seem to bear that out. In its examination of attacks on hospitals, Intel Security identified a number of Bitcoin wallets that seemed to be implicated and which had become enriched by around $100,000. The firm also found a ransomware developer and distributor on an underground forum who, as part of his sales pitch, showed evidence of payments in response to campaigns. These payments amounted to 189,813 bitcoins, around $121m. Even deducting the cost of renting botnets, Intel believes this one developer may have made $94m in six months.

In October 2015, research by McAfee Labs with the Cyber Threat Alliance revealed a ransomware campaign based around the CryptoWall malware that netted the cyber-criminals nearly $325m in two months.

Jordan Wright, Duo Security: "Phishing continues to be an efficient and popular method of infecting devices."



The root of breaches in healthcare organisations. Source: 'Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data', May 2016, Ponemon Institute.

Targeting businesses

As well as growing, ransomware is also evolving, both technically and in terms of targets. "During recent years we have seen a shift in ransomware targets from individuals to businesses, which offer attackers larger monetary gains," says the recent McAfee Threats report.

"Cyber-criminals go where the money is and 2016 has shown them that large organisations that aggregate valuable data including financial, HR, and health records are too rich to ignore"

"Cyber-criminals go where the money is and 2016 has shown them that large organisations that aggregate valuable data including financial, HR and health records are too rich to ignore," says Tom Patterson, VP for global security at Unisys. "The change in business enterprise strategy to move beyond four walls and embrace clouds, mobile and more, is leaving many organisations that haven't also updated their 'security thinking' vulnerable to today's cyber-attacks. Until enterprises deploy more modern defences that actually work in today's world, they will continue to be successfully targeted."

Initially, hitting individuals via mass phishing and spamming campaigns was the easy route. Once the infrastructure is set up – the malware, the botnets to spread it and the back-end systems to take victims' money via Bitcoin – then the criminals can sit back and wait for the cash to roll in.

However, there is some evidence to suggest that this is not as easy a money-making scheme as it once was. Modern operating systems and applications are not free from exploitable vulnerabilities, but they are getting harder to exploit at a mass scale. In other areas of cyber-crime activity we've seen a shift to more targeted attacks using social engineering, often via spear-phishing in which known, clearly identified individuals are picked out for attack.

What is ransomware?

Ransomware is, as the name suggests, a form of technological blackmail. The malware encrypts files on the hard drive of your computer and then presents a message telling you how to get the documents unlocked again. That process usually involves making a transfer of funds to the cyber-criminals, most commonly through the use of Bitcoins, in return for a decryption key.

To protect themselves, the attackers work via the dark web. In many cases, victims are instructed to download the Tor Browser package and connect to a darknet site via the .onion protocol. Whether you ever receive a decryption key seems to vary considerably. And whether it works is another matter. Usually there's a time limit, after which your files are deleted and gone forever.

For the malware to work, it needs to get on your computer. Infections can happen as a result of the cyber-criminals exploiting software vulnerabilities, sometimes via drive-by attacks on maliciously crafted web pages. Exploit kits such as Angler, Neutrino and Nuclear have the capability to deliver ransomware.

"Phishing continues to be an efficient and popular method of infecting devices, and also reveals a widespread lack of solid security fundamentals," says Jordan Wright, R&D engineer at Duo Security. "The persistence of phishing, coupled with loose BYOD policies, continues to weaken an organisation's endpoint security."

Recent months have seen massive spamming campaigns in which emails purport to contain reports, invoices, payment details or other files that victims might find enticing. Many of these are Word documents with malicious macros. When the programs or macros are run, they download the main ransomware payload.

Overwhelmingly, this malware is designed to run on Windows platforms, but Apple macOS versions have been reported: for example, a server hosting downloads of the popular bittorrent client Transmission was compromised and a version of the software infected with ransomware inserted in place of the legitimate code. This went unnoticed for around 24 hours, during which time it was downloaded an unknown number of times. The malware has been dubbed KeRanger and appears to be a modified version of the Linux Encoder trojan, said security firm Bitdefender. The infected version of the software was signed with a legitimate developer certificate issued to someone in Turkey and so was able to bypass OS X's Gatekeeper protection. The certificate has been revoked by Apple.

For the attackers, one advantage of ransomware is that they don't have to bother with the tricky issue of actually stealing data. The exfiltration of data takes resources – especially if done as part of large-scale campaigns. It also requires a skill level – for example, to evade data loss prevention systems or outbound firewalls – that ransomware operators rarely display.

And it's not just desktop systems that are affected. Quick Heal Technologies issued a report in which it showed a 200% increase in mobile ransomware in the second quarter of 2016, nearly all of it on the Android platform.

Hitting healthcare

The McAfee report picks up on a trend that had already been noted by many in the industry. First there was a shift by ransomware operators towards targeting small businesses with reasonably large attack surfaces but with poor security and little in the way of resources (such as daily back-ups) that would help them recover from an attack. Then the attackers seemed to form a preference for one sector in particular – healthcare.

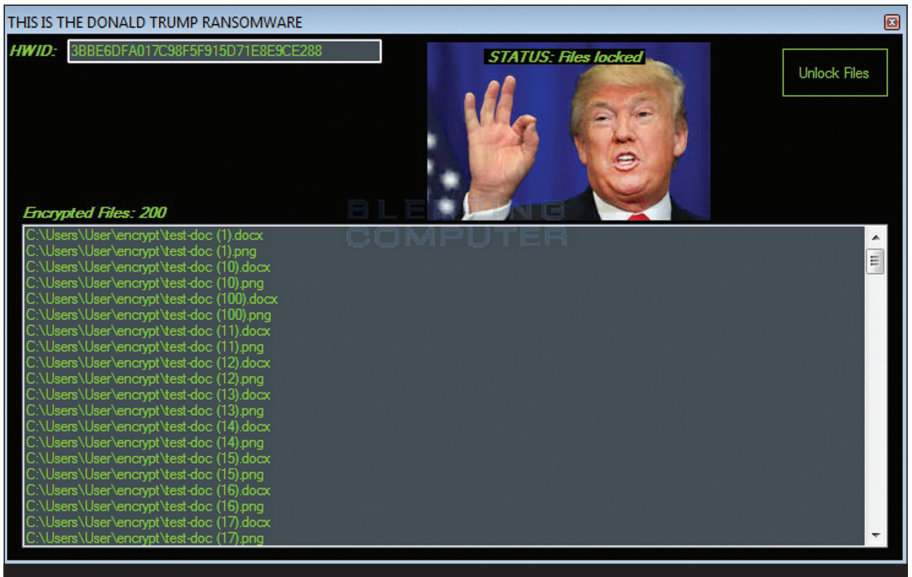
Without looking into the minds of ransomware operators we can only make educated guesses as to why this might be. Certainly, many medical

The warning screen presented by the MarsJoke malware that has recently been targeted against local government agencies and educational institutions in the US. Source: Proofpoint.

institutions are running on infrastructures that, either through lack of investment or because of the difficulty of updating specialised systems, are using vulnerable operating systems and applications. At the same time, it is critically important that the services delivered by these systems and the organisations that depend on them are not disrupted. If systems become unavailable then lives could be put at risk. At the very least, the institutions could suffer significant reputational damage.

For these reasons, the attacks often work, although not necessarily as well as the criminals expect. For example, when a Californian hospital fell victim in Feb 2016, the attackers demanded payment of $5.77m. However the hospital claims it paid $17,000. The affected systems were restored, but only after five days of downtime.

In Aug 2016, FireEye reported a massive wave of attacks using the Locky ransomware dropped via macro-enabled Word (.docm) documents in phishing emails and mostly targeted again at healthcare organisations in the US, Japan, Korea and Thailand.[4] Previously, Locky had mostly been spread through spam campaigns carrying JavaScript payloads.

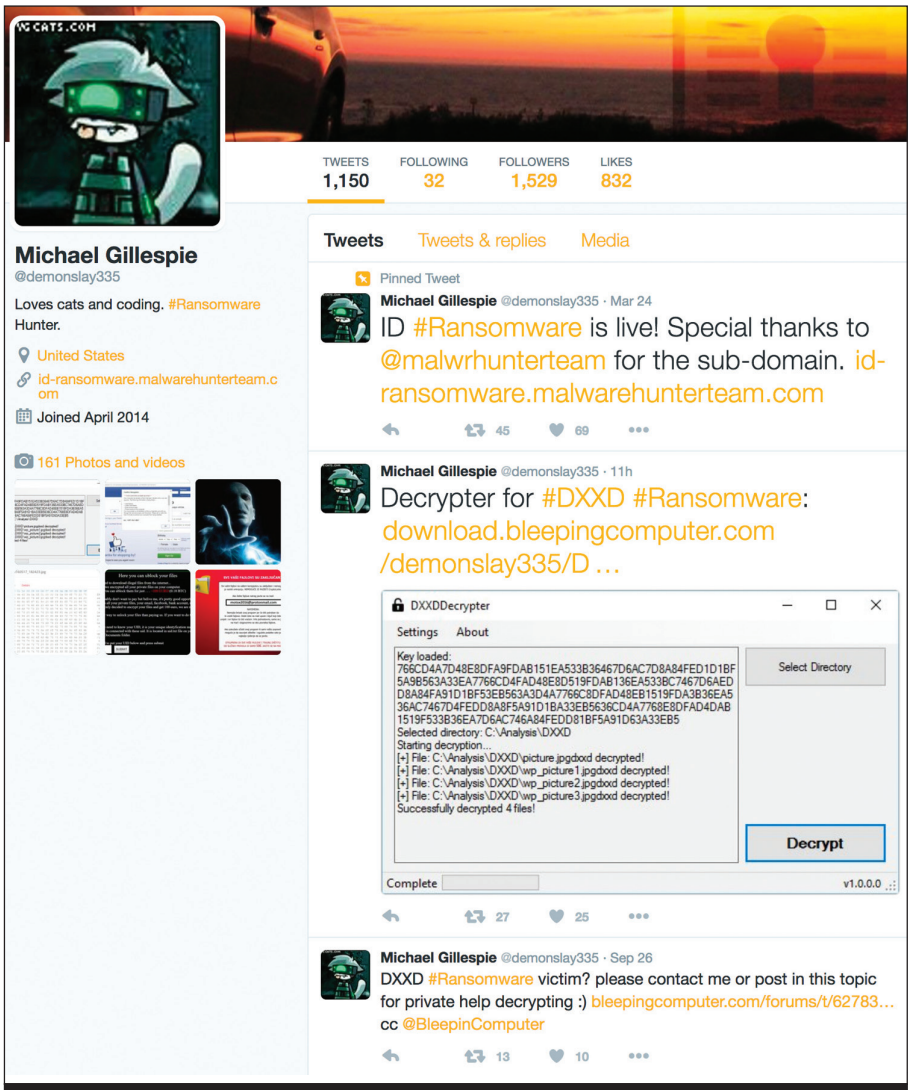


The Donald Trump ransomware. It doesn't work. Source: Bleeping Computer.

The Intel Security Threats Report notes 24 attacks against hospitals and other medical facilities in the first half of 2016. In some cases there were attacks against multiple targets, such as one in January that focused on several hospitals in the Rhine-Westphalia region of Germany. And freedom of information (FOI) requests filed by security firm NCC Group revealed that 47% of NHS Trusts in the UK had been hit by ransomware over the course of the previous year. The real picture may be higher, though, because only 60 Trusts responded and 31 of these withheld information, mostly on the basis of patient confidentiality. In fact, only one Trust said that it had *not* been a victim of ransomware in the past year although it had been hit previously.

"Not long after MarsJoke was spotted, researchers at Kaspersky Lab cracked its encryption thanks to weak randomisation in a string used in the encryption algorithm"

A separate FOI request by Channel 4 painted a somewhat less dramatic picture, with 39 out of 152 Trusts having been affected. Nonetheless, there is clearly a need to improve security in the health service and the ransomware scourge may be one of the incentives behind a new initiative by NHS Digital, which provides information, data and IT services for healthcare providers and patients. Its CareCERT service, originally launched in Nov 2015 to disseminate information about security threats, was expanded recently to offer three additional services, all of them currently in the testing phase.[5] These are: CareCERT Knowledge, an educational portal to provide the staff of healthcare organisations with basic cyber-security training; CareCERT Assure, to help organisations assess their own cyber-security capabilities against industry standards; and CareCERT React, offering advice on reducing the impact of a security incident.



Researcher Michael Gillespie announced the discovery of the Nagini ransomware, and its decryptor, via Twitter.

Special attention

Local governments have also come in for special attention. The motivations may have been quite similar in that such organisations typically run on systems that aren't exactly at the leading edge – indeed, much of the infrastructure is old enough to be classed as 'legacy'. Security skills are usually thin on the ground. And local governments run services that have significant impact on people's lives, making any interruption embarrassing and thus encouraging them to pay up.

In Sept 2016, researchers at Proofpoint spotted a new strain of ransomware, MarsJoke, that is being pushed towards state and local government agencies and educational institutions in the US.[6] As usual, it's being pushed via mass emailing, but rather than attaching a malicious document it simply contains a URL to an executable file called file_6.exe. It's similar in many ways to an earlier ransomware campaign, CryptFile2, that also used URLs and focused on the same range of targets. Not long after MarsJoke was spotted, researchers at Kaspersky Lab cracked its encryption thanks to weak randomisation in a string used in the encryption algorithm. Kaspersky's researchers were able to find keys within just a few minutes after the weakness was found. The firm has now added decryption keys to its Rannoh Decryptor tool.

Universities have also been singled out. Security firm SentinelOne also used FOI requests and found that 56% of the UK universities that responded had been hit. In fact, one institution suffered no fewer than 21 attacks. Some 13 of the 71 institutions contacted refused to answer because they felt it would damage their commercial interests – so read into that what you may. No university admitted to paying a ransom and in all but one case they dealt with the problem internally, without contacting the authorities: only Brunel got in touch with the police.

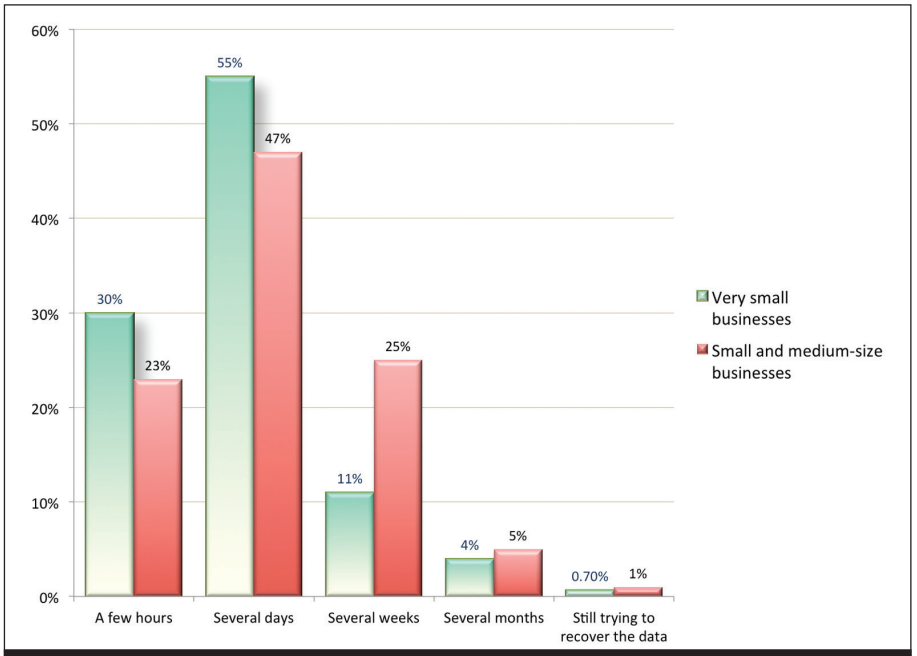
In the news

Cyber-criminals often exploit topical events to spread malware. Disasters, celebrities and major sporting events are effective ways of luring victims into visiting malicious websites or downloading dubious apps because curiosity so often trumps caution. It's not surprising then that researchers have found ransomware writers looking to cash in on current events.

"Freedom of information (FOI) requests revealed that 47% of NHS Trusts in the UK had been hit by ransomware over the course of the previous year. The real picture may be higher"

On the day of the first US presidential debate, malware and computer forensics specialist Lawrence Abrams trawled the Internet looking for malware linked to one or other of the candidates. He found one piece of malware in development dubbed 'The Donald Trump Ransomware'.[7] Perhaps appropriately, the software didn't actually perform properly – it simply base64-encoded files in one folder and change their extensions. Abrams concludes that this ransomware is unlikely ever to be used in anger.

Another recent discovery that exploits celebrity was made by researcher Michael Gillespie. He uncovered a strain of ransomware that presents victims with an image of the character Voldemort from the Harry Potter movie franchise. The malware is named after the character's snake, Nagini. Again, the



Time spent on restoring access to data encrypted by ransomware. Source: Kaspersky Lab.

ransomware is still in development, and Gillespie has already provided a decryptor for it, but these examples show how the ransomware community is highly active and always looking for new avenues of exploitation.

Technical evolution

In many ways, the technical developments in ransomware have been less marked than the switch in targets. The 'typical' piece of ransomware (if one can use that term) will encrypt the files in certain directories on the hard disk that normally hold a user's personal files, photographs (often more highly valued by victims than documents), videos, music and so on. Generally, the malware will leave the computer in an otherwise usable state – after all, it's important that you are able to log on to the Internet in order to make the necessary Bitcoin transfer.

"Too often, we see reports of organisations getting infected with ransomware, not having tested back-ups in place and being forced to pay the ransom in the hopes of getting their data back"

Some malware writers have upped the ante. The Petya strain, for example, encrypts the master file table (MFT) of the victim's hard drive.[8] The victim's files are unaffected, but the computer simply can't find them anymore. Fortunately, Petya was flawed and not particularly widespread.

"Some of the most prevalent ransomware strains, such as CTB Locker, Cryptowall and Locky deploy strong encryption and there is little sign that this is going to be broken anytime soon"

Another strain spotted by Sophos is more aggressive. Mamba makes use of a pirated copy of the open source package DiskCryptor full disk encryption tool.[9] The Mamba malware simply uses the tool to encrypt the whole disk with its own key, while also installing itself as a Windows service. That means the computer retains just enough functionality to reboot and present the ransom message, although you'll need a separate computer or mobile device to access the web and pay.

There have been some odd developments, too, with novel types of ransomware adopting new tactics – in some cases, it seems, because their creators lack the talent to develop proper malware. One of these presents a photograph of Adolf Hitler with the message 'This is the Hitler-Ransonware' [sic]. It claims to have encrypted the victim's files, but in fact simply deletes file extensions for anything found in certain directories. After an hour, it then crashes the PC and, on reboot, deletes the files. The payment demanded is a cash code for a €25 Vodafone Card. Text found in the code suggests it originated from Germany.

Another form of ransomware, which appears as a fake Windows 10 lock screen and tells users that their licences have expired, turned out to have the decryption key buried in the code. Researchers from Symantec discovered that, while the criminals had gone to considerable effort to set up fake tech support websites for the scam, the phone number they gave out for victims to call was never answered and was soon disconnected. On reverse engineering the code, the researchers found the decryption key (8716098676542789) plainly visible.

While security researchers frequently encounter poorly written and ineffective strains of ransomware, the overall trend is to more sophistication. For example, researchers at Netskope recently discovered an update to the Virlock family that is using techniques from computer viruses.[10] Most ransomware acts like a trojan, affecting only the victim's machine, although it may reach out across the network to find as many storage devices as possible to encrypt. But Virlock also infects files in such a way that, if they are shared, any other user who opens them also has their PC infected. In a corporate environment, this could lead to the malware spreading rapidly. Using polymorphic techniques, the signature of the virus changes each time it is copied, which will help it evade detection by anti-malware. Its ransom demand masquerades as an official fine levied for a bogus 'copyright infringement'.

Cost of an attack

"Ransomware is damaging to businesses because it can completely bring their operations to a halt," says Wright

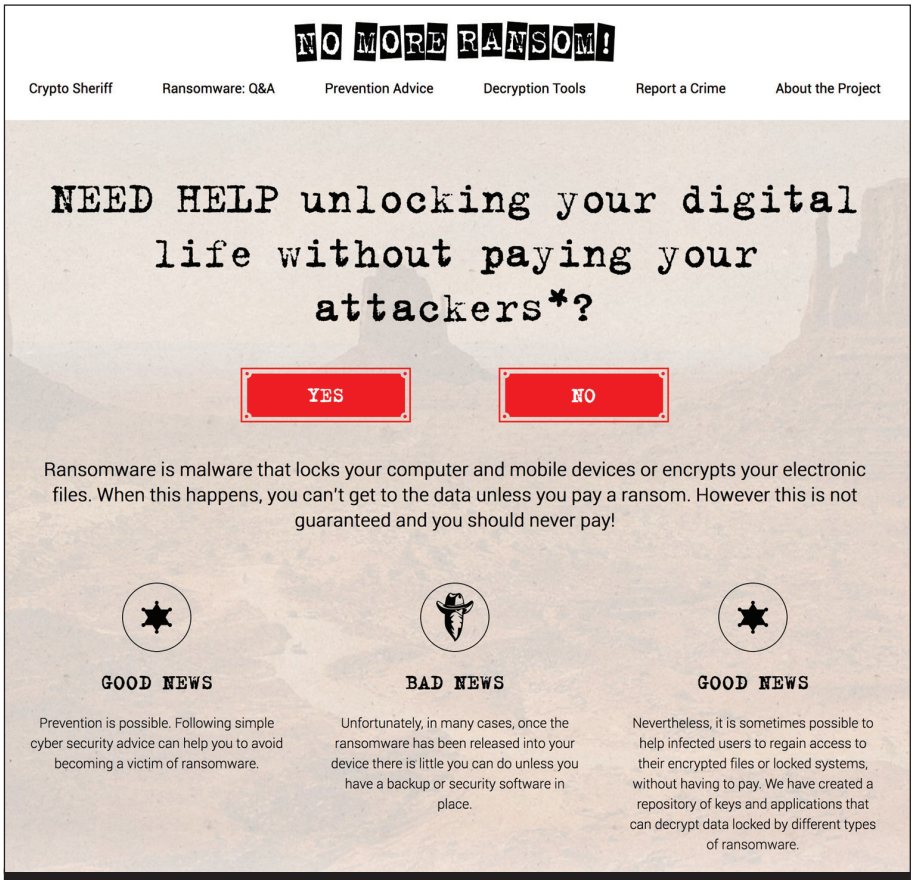
at Duo Security. "Too often, we see reports of organisations getting infected with ransomware, not having tested back-ups in place, and being forced to pay the ransom in the hopes of getting their data back. The other aspect that makes ransomware so damaging is how widespread the attacks can be. Everyone is a target. Traditionally, attackers needed to find a buyer who would value the assets they stole (credentials, access to a device, etc). With ransomware, attackers are just selling your data back to you."

"The malware is sophisticated in the way it spreads within an organisation and uses the same high levels of encryption that the good guys use, so it's difficult to recover from"

The actual costs of being hit by a ransomware attack are several. For individuals there's the cost of paying the ransom, if you decide to go that route. If you don't, or if it doesn't work, then there's the emotional pain of all those lost files and possibly the price of a new hard disk or computer. For organisations it's much worse, and calculating the cost is not going to be easy. Paying the ransom is the least of it.

Kaspersky Lab issued a report in which ransomware – or cryptomalware as the firm prefers to call it – was cited as the third-most serious threat by small to medium-size businesses (SMBs).[11] And for smaller companies, it becomes the second most worrying form of attack. It also claims that 34% of firms admitted to paying the ransom. Kaspersky's survey found that the average cost of an attack was $99,000 for SMBs when everything was taken into consideration.

"As we can see, almost one-third of SMBs still believe that paying the ransom is the most cost-effective way of getting their data back," says Vladimir Zapolyansky, head of SMB marketing at Kaspersky Lab. "The reality, however, is that the total damage for companies ends up being much greater and there is still no guarantee of recovering the corporate data in question."



The No More Ransom initiative offers advice on dealing with ransomware attacks.

Tom Patterson, Unisys: "Most organisations still focus primarily on securing their perimeter, rather than the 80% of their traffic that flows within their borders, which is where the ransomware does its damage."

Around half of SMBs (47%) take several days to restore their data and for a quarter of them it's a matter of weeks. A small percentage (1%) never get the data back, according to the Kaspersky survey. That disruption translates into lost business, damaged reputation and possibly loss of intellectual property assets if critical files are not recovered. There's also the cost of carrying out the remediation – at the very least a full restore from back-ups – and potentially the expense of calling in outside expertise.

Of course, the ransom itself may be significant. Often it's surprisingly low, probably because the cyber-criminals reckon that a modest amount is more likely to be paid without driving victims to seek assistance from law enforcement. But as the focus has shifted towards organisations so have the ransom demands grown. Recently, the cloud-based applications provider Vesk admitted to paying 29 bitcoins (around £18,600) after being hit by the Samas DR ransomware – a new strain that had managed to slip past the firm's anti-malware systems. Vesk had back-ups and immediately began to restore from those, but it also opted to pay the ransom to ensure that it could get systems up and running again as quickly as possible.

Stuart Facey, Bomgar: "The biggest threat to any organisation is understanding who actually has access to information."

Fighting back

No More Ransom (nomoreransom.org) is an initiative created by Kaspersky Lab and Intel Security in co-operation with Europol and the Dutch National Police to fight ransomware.[12] It offers guidance on how to avoid malware infections and what to do if they happen. And it is acting as a central distribution point for those decryption keys that have been discovered by security companies and researchers. At the time of writing, four decryption tools – decryptors – were available that made use of such keys. The site is also a place for victims to report attacks.

There have been a number of successes in the battle against ransomware. In July 2016, the organisations behind No More Ransom took down the operation behind the Shade malware which had been operating since 2014. They were able to identify and seize control of the command and control servers and these yielded the information needed to develop a decryption tool.

Intel and Kaspersky also released a decryptor for the 'Wildfire' strain that mainly affected people in Belgium and the Netherlands and was said to have made the attackers $79,481 in a month. As with many strains of malware, the software checks the language and location of the victim and doesn't run if it suspects they are in Russia or certain East European countries, giving a clue to the attackers' whereabouts.

A criminal group using the Angler exploit kit to operate a ransomware operation was closed down by Cisco, which said the gang had been making $60m a year. Researchers at the firm's Talos security unit found that a large number of the crime operation's proxy servers were being hosted by service provider Limestone Networks. As much as half of all activity using the Angler exploit kit, involving as many as 90,000 victims a day, was going via these servers. Working with Level 3 Threat Research Labs and OpenDNS, Cisco was able to interrupt traffic to the servers. It also released Snort rules and published communications mechanisms, including protocols, so other organisations can protect themselves and customers.

In a couple of cases the task was easier. Two pieces of ransomware, dubbed 'PowerWare' and 'Bart', turned out to have serious flaws. Specialists at Palo Alto Networks found that PowerWare not only used weak encryption but also had the encryption key hardcoded into the software, allowing them to create a decryption tool. Meanwhile, researchers at AVG developed a decryptor for Bart by comparing original files to the encrypted versions and reverse engineering the feeble encryption process.

The encryption keys for the Chimera malware, which largely targeted German SMBs in a somewhat minor ransomware campaign – were leaked by a rival gang. A cyber-criminal going under the name of 'Janus', who is reputed to be the author of the Petya malware – not only published the keys online but also bragged about using some of the Chimera source code in another piece of ransomware, Mischa. It seems that the leak was an attempt to reduce competition.

That said, some of the most prevalent ransomware strains, such as CTB Locker, Cryptowall and Locky, deploy strong encryption and there is little sign that this is going to be broken anytime soon.

Countermeasures

The standard protections – keeping all software fully patched and running an anti-malware package – will work against ransomware that relies on vulnerable software. However, a significant proportion of ransomware attacks use social engineering techniques, most commonly via phishing attacks. Guarding oneself against such methods requires a level of security awareness and vigilance that seems to be sorely lacking both in the general population and within businesses. And so we can be confident that ransomware will continue to be effective.

Researchers at the University of Florida and Villanova University have developed a potential defence against ransomware that relies on spotting what the malware is up to and stopping it in its tracks.[13] They describe the approach as a "save what you can" technique that is capable of recognising when ransomware has started to encrypt a victim's files. It then halts the process and alerts the user – the latter being important because it's possible that the encryption activity is actually genuine, such as when tools like PGP disk encryption or compression utilities are being used. In tests, the researchers say they managed to stop ransomware in its tracks when it had encrypted only 0.2% of the files on a drive.

"The malware is sophisticated in the way it spreads within an organisation and uses the same high levels of encryption that the good guys use, so it's difficult to recover from," says Tom Patterson, VP for global security at Unisys. "Most organisations still focus primarily on securing their perimeter, rather than the 80% of their traffic that flows within their borders, which is where the ransomware does its damage."

Having recent back-ups is critical. If you can restore from back-ups without losing too much data, then that's a cheaper and more assured way of recovering. But the back-ups need to be 'air-gapped' from your other systems. Some ransomware is capable of reaching out to other attached or networked storage. So if your 'back-up' is a USB hard drive plugged into the computer, it's likely to become a victim too.

Containing the problem

"The most effective defence to protect against any form of ransomware is to consider some form of containment

strategy, such as micro-segmentation, which allows enterprise managers to effectively divide their physical networks into hundreds or thousands of logical micro networks, or microsegments," says Patterson. "This limits the spread of ransomware within an organisation, as well as protects the known-good files from takeover. Micro-segmentation works at the Internet packet level, cryptographically sealing each packet in such a way that only packets that are within the approved microsegment will be processed. That way users within your communities of interest – employees, partners, suppliers, customers – can only send and receive packets for their group. This means that in the situation of a ransomware-based breach, only the targeted and effective segment of that network is compromised (while still protecting the back-ups), limiting the malware from spreading to alternative areas of the network or organisation, profoundly minimising its detrimental impact."

It's also important to think about where information is stored and whether it should be available to everyone.

"Companies should inform employees of the risks and vulnerabilities and teach situational awareness. Having the entire workforce involved in the process can go a long way towards improving company defences"

"The biggest threat to any organisation is understanding who actually has access to information and at what levels within the network," explains Stuart Facey, VP of EMEA at Bomgar. "This access can come in many forms and therefore they must ensure that the right person is accessing the network or device each time a request takes place with the correct level of attributed trust. However, even when an authorised access has been made to a network, there is no guarantee that a cyber-criminal hasn't 'piggy-backed' the connection or placed ransomware on the device through rogue emails or RATs [reverse access trojans]. These are the methods hackers can utilise to open the connection to the network to gain the same level of access as the member of staff. This proven method of entry has encouraged cybercriminals to target gateway devices that require a network connection. They can simply place ransomware on a system and once opened, it provides gateway access to sensitive information on the

Should you pay the ransom?

Deciding whether to pay the ransom in the hope of getting your files back is tricky. Phil Richards, chief security officer at LANDESK, offers the following advice.

While it is easy to say never pay the ransom, sometimes there are practical considerations that need to be evaluated. Here are some potential questions you will face and need to effectively analyse before making that decision.

Can you live without the files? Files encrypted by ransomware are locked and cannot be viewed or accessed by anyone in the organisation. It is important to catalogue the extent of the loss. Files can be grouped based on how critical they are to the organisation.

Do you have back-ups, and if so, how recent? The existence of back-ups for encrypted files gives you options. You might have the ability to recover encrypted files through your own back-ups. The existence of back-ups varies by company and by type of system that has been compromised.

Recovery. If you have back-ups of the encrypted files, how quickly can you recover from back-up? Companies have varying strategies for back-up/storage and retrieval. Recovery can take multiple days. When that happens, paying the ransom may be a viable alternative to restore files more quickly.

Do you have an obligation to outside parties? File availability requirements may impact your decision-making. If you need to have files available quickly, that may tilt the balance in favour of paying the ransom for the possibility of recovering them quickly. Obligations may be to customers, suppliers, regulatory organisations, legal entities and many others.

Is it possible to decrypt the files without paying the ransom? Some ransomware is not well written. If you are lucky enough to have become infected with a weaker variant of encryption, it is possible to use a recovery pack. A good resource for identifying and remediating some types of ransomware can be found in this list of decryptor tools.

Assess the likelihood of getting the encryption key after paying the ransom. Not all ransomware organisations are trustworthy (big surprise). Some will take your money and not provide you with the decryption keys. On 20 May 2016, Kansas Heart Hospital paid a ransomware organisation an undisclosed amount, only to have the organisation extort them for a second time for additional money. The hospital refused to pay the second ransom, stating: "The policy of the Kansas Heart Hospital in conjunction with our consultants, felt no longer was this a wise manoeuvre or strategy".

Other risk factors. You need to consider reputational, regulatory and financial risk when deciding whether to pay or not pay the extortionists. Make sure you're considering all angles. The recommendation from the FBI and several non-government organisations is to never pay a ransom. Some reasons to not pay the ransom include:

- There is a possibility that you will not recover the files after you pay.
- It encourages bad actors to continue developing ransomware.
- You fuel a perception that you are weak by giving in to the bandits.
- You fuel a perception that you are inept if you don't know how to prevent/resolve security breaches.

network. It is here that a strategy of implementing a privileged access solution that manages the access to, as well as the accounts of, users should be considered in order to allow organisations to gain control and tailor access rights dependent on the user."

Given that a large proportion of ransomware is introduced to an organisation via phishing emails, ultimately you need to look at having a properly educated staff as your first line of defence.

"Education and training is important," says Duo Security's Wright. "Companies should inform employees of the risks and vulnerabilities and teach situational awareness. Having the entire workforce involved in the process can go a long way toward improving company defences."

Paying up

When you're faced with that screen demanding money with menaces, should you give in and pay? If you can't restore your systems – say, from back-ups – you may feel you have no option. But this isn't necessarily going to help.

In a public service announcement released by the FBI in September 2016, the agency urged victims to contact law enforcement and stated: "The FBI does not support paying a ransom to the adversary. Paying a ransom does not guarantee the victim will regain access to their data; in fact, some individuals or organisations are never provided with decryption keys after paying a ransom. Paying a ransom emboldens the adversary to target other victims for profit, and could provide incentive for other criminals to engage in similar illicit activities for financial gain. While the FBI does not support paying a ransom, it recognises executives, when faced with inoperability issues, will evaluate all options to protect their shareholders, employees, and customers."[14]

Back in Oct 2015, one FBI agent caused a furore when he suggested that victims should pay. Speaking at a security conference in Boston, Joseph Bonavolonta, assistant special agent in charge of the cyber and counterintelligence programme at the local FBI office, said: "The ransomware is that good ... To be honest, we often advise people just to pay the ransom." He was also quoted as saying that the "overwhelming majority of institutions just pay the ransom" and that, "You do get your access back" (ie, to your files).

The general advice, though, is not to pay. A Trend Micro survey found 65% of UK firms hit by ransomware opted to pay the ransom, but that a third of them failed to recover their data. The average amount paid was £540, although in a fifth of cases it was more than £1,000. The most common reasons for paying was the fear of fines if they were discovered to have lost data, the confidential nature of the data itself and the fact that the amounts demanded were reasonably low. Surprisingly, the cyber-criminals are often willing to negotiate over the price. Security firm F-Secure says that three out of four ransomware gangs would haggle, giving discounts averaging 29% on the fee first demanded.[15]

Of those that decided not to pay, two-thirds said that it was because of a policy not to give in to criminals. It probably helped that 60% of them were able to recover using back-ups and around a quarter (26%) thought the affected data wasn't valuable or confidential.

"Victims should not pay," insists Andy Norton, risk officer EMEA for SentinelOne. "It will only make things worse for everyone. However, in the real world, bad things happen and people need their data back, which they value more than the cost of the ransom. This is why people end up paying. The real mistake is paying twice, by getting infected, paying, not learning from it, getting infected again and paying again and so on."

Conclusion

So how is the ransomware issue likely to develop?

"As enterprises evolve toward hyper-connectivity we will see ransomware evolve to be utilised and distributed much more effectively through mobile and the cloud, with popular cloud-based applications being subject to the next wave of attacks," reckons Patterson. "Hackers will transform their approach to affect a much more varied and unknowing user base that will find it increasingly difficult to react to breaches of this nature. This approach to cloud-based hacking will change our understanding of the concept of infection, if one individual within an organisation uploads a breached file from such a platform, it could spread to anyone else that has the need or opportunity to interact with that file."

In its '2016 Midyear Cyber-security Report' Cisco claimed that ransomware has become the most profitable kind of malware and that it's set to evolve into an even greater menace.[16]

"Cisco expects to see this trend continue with even more destructive ransomware that can spread by itself and hold entire networks, and therefore companies, hostage," says the report. "New modular strains of ransomware will be able to quickly switch tactics to maximise efficiency. For example, future ransomware attacks will evade detection by being able to limit CPU usage and refrain from command-and-control actions. These new ransomware strains will spread faster and self-replicate within organisations before co-ordinating ransom activities."

According to SentineOne's Norton: "This is an 'in your face' problem. It's not a stealthy threat that security experts disagree on the likelihood of it being found in any given environment. The fact that the impact is so visible is driving change in security infrastructures – it is one of the catalysts for the rapid growth in next-generation endpoint security. Not only can it be defeated, it is an opportunity to fundamentally reform how we do security."

About the author

Steve Mansfield-Devine is a freelance journalist specialising in information security. He is the editor of Network Security *and its sister publication* Computer Fraud & Security. *He also blogs and podcasts on infosecurity issues at Contrarisk.com.*

References

1. 'Internet Organised Crime Threat Assessment 2016'. Europol. Accessed Sep 2016. http://g8fip-1kplyr33r3krz5b97d1.wpengine.netdna-cdn.com/wp-content/uploads/2016/09/IOCTA-2016-FINAL.pdf.
2. 'McAfee Labs Threats Report: September 2016'. Intel Security, Sep 2016. www.mcafee.com/us/resources/reports/rp-quarterly-threats-sep-2016.pdf.
3. 'The reign of ransomware'. Trend Micro. Accessed Sep 2016. www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-the-reign-of-ransomware.pdf.
4. Chong, Ronghwa. 'Locky ransomware distributed via DOCM attachments in latest email campaigns'. FireEye, 17 Aug 2016. Accessed Sep 2016. www.fireeye.com/blog/threat-research/2016/08/locky_ransomwaredis.html.
5. 'New service to manage cyber-security threats in health and care'. NHS Digital, 3 Sep 2015. Accessed Sep 2016. http://content.digital.nhs.uk/article/6693/New-service-to-manage-cyber-security-threats-in-health-and-care.
6. MarsJoke ransomware mimics CTB-Locker'. Proofpoint, 23 Sep 2016. Accessed Sep 2016. www.proofpoint.com/us/threat-insight/post/MarsJoke-Ransomware-Mimics-CTB-Locker.
7. Abrams, Lawrence. 'The Donald Trump Ransomware Tries to Build Walls around your Files'. Bleeping Computer, 26 Sep 2016. Accessed Sep 2016. www.bleepingcomputer.com/news/security/the-donald-trump-ransomware-tries-to-build-walls-around-your-files/.
8. Ducklin, Paul. 'New ransomware with an old trick: Petya parties like it's 1989'. Naked Security, Sophos, 4 Apr 2016. Accessed Sep 2016. https://nakedsecurity.sophos.com/2016/04/04/new-ransomware-with-an-old-trick-petya-parties-like-its-1989/.
9. Ducklin, Paul. 'Mamba ransomware strikes at your whole disk, not just your files'. Naked Security, Sophos, 27 Sep 2016. Accessed Sep 2016. https://nakedsecurity.sophos.com/2016/09/27/mamba-ransomware-strikes-at-your-whole-disk-not-just-your-files/.
10. Vamshi, Ashwin. 'Cloud malware fan-out with Virlock ransomware'. Netskope, 27 Sep 2016. Accessed Sep 2016. https://resources.netskope.com/h/i/290799411-cloud-malware-fan-out-with-virlock-ransomware.
11. 'The cost of cryptomalware: SMBs at gunpoint'. Kaspersky Lab. Accessed Sep 2016. https://business.kaspersky.com/files/2016/09/IT_Security_Risks_Report_Cryptomalware_Cost_.pdf.
12. No More Ransom, home page. Accessed Sep 2016. www.nomoreransom.org
13. Scaife, N; Carter, H; Traynor, P; Butler, K. 'CryptoLock (and Drop It): stopping ransomware attacks on user data'. 2016 IEEE 36th International Conference on Distributed Computing Systems. Accessed Sep 2016. www.cise.ufl.edu/~traynor/papers/scaife-icdcs16.pdf.
14. 'Ransomware victims urged to report infections to federal law enforcement'. FBI Public Service Announcement, 15 Sep 2016. Accessed Sep 2016. www.ic3.gov/media/2016/160915.aspx.
15. 'Evaluating the customer journey of crypto-ransomware'. F-Secure. Accessed Sep 2016. https://fsecureconsumer.files.wordpress.com/2016/07/customer_journey_of_crypto-ransomware_f-secure.pdf.
16. '2016 Midyear Cyber-security Report'. Cisco. Accessed Sep 2016. http://bit.ly/2bnFSXY.

Ransomware: threat and response

How and why is the ransomware scourge growing? And what can we do about it? *Network Security* spoke to Tim Erridge, director of advisory at Context Information Security.

Network Security (NS): What are the most common infection vectors for ransomware?

Tim Erridge (TE): Phishing is still the most common infection vector, so it is imperative that all staff understand what a phishing email looks like and use caution when clicking on links embedded in emails, especially emails that are unsolicited. However, ransomware can infect you via several different methods, all of which are a significant threat. It could be a malicious program that's downloaded, a web drive-by or watering hole attack. More recent ransomware has spread through malvertising – malicious embedded advertisements that execute JavaScript and download ransomware silently in the background.

Tim Erridge, Context Information Security: "Ransomware that is targeted will seek to have the biggest adverse effect. But indiscriminate ransomware that self-propagates internally affecting large numbers of systems can be equally damaging."

NS: What are the most damaging aspects for businesses?

TE: Ransomware can have a huge impact on your business, especially if it strikes mission-critical systems or data. Ransomware that is targeted will seek to have the biggest adverse effect. But indiscriminate ransomware that self-propagates internally affecting large numbers of systems can be equally damaging, especially if internal networks are flat and implicitly trusted.

"Even if you have paid, you should still take action to report the attack. This should never be dismissed out of hand as a nuisance attack"

The original objective of ransomware is business disruption, to incentivise victims to pay the ransom. However, as it has grown in popularity as a cyber-attack tool, the motivations for its use can be more sinister, seeking to inflict reputational damage on a business or an individual – ie, it's less about the ransom and more about the impact of the attack.

Potential financial damages can be incurred not only in the form of the cost to mount a response investigation, but also due to any PR consequences through the loss of current and future customers, potentially even legal action from any directly affected if client data has been disclosed. Provision of credit protection and identity theft monitoring may also be necessary. There may also be fines to pay should you be found in breach of the Data Protection Act (DPA) or in the future, the General Data Protection Regulation (GDPR).

NS: Should victims pay? And is it understandable if they do?

TE: It's not recommended to pay, as this will only fuel the phenomenon. However, if an attack strikes at the heart of your business and the economics of the situation make sense to do so, then it's understandable. But, even if you have paid, you should still take action to report the attack. This should never be dismissed out of hand as a nuisance attack. Some are, absolutely, and some larger enterprises would not miss a few bitcoins versus the potential lost revenue of a non-responsive trading system, or the negative impact on their share price if the attack was known publicly. Yet we all have a duty not to underestimate this ransomware blight. It stems from criminal enterprise and as such we must report every incident to the appropriate authorities and get the support of experts to conduct a full digital forensic investigation to understand the true nature of the attack.

It is only by being collaborative that we can combine forces and stand any chance of beating ransomware. We must build an accurate picture of how prolific it is, and we must understand new variants as quickly as possible after they emerge. Only by building up as much knowledge as possible is it going to be realistic to build effective prevention techniques and empower individuals and organisations to defend themselves.

In general, you shouldn't be embarrassed or shamed into following ransom instructions where threats and accusations are the tactics, as the majority are unfounded. It's best to get the malware investigated and expertly removed. Also, whereas early ransomware tended to provide the victim with genuine decryption keys, recently we see increasingly poorly written malware code that simply doesn't work; dishonourable thieves who fail to provide decryption keys to the data; or worse still, malware that doesn't even have the ability to be reversed, so despite paying up, there is no chance of ever unlocking your information again.

On the defence

NS: How do you defend yourself? Is this a technology issue (eg, anti-malware, frequent back-ups) or is it mainly a staff awareness/training issue?

TE: It's actually threefold: technology, training and process.

It is imperative to have a rigorous back-up regime, to ensure all business-critical systems and data are regularly backed up offline and the restoration of back-ups is tried and tested. If you have complete confidence that you can recover any lost data or systems rapidly within your tolerance of business impact, then the impact of ransomware is almost completely diminished, but not entirely. Reputational damage can still hurt the business. So it's important to do all you can to try and establish roadblocks for as many of the infection vectors as possible to reduce the chances of being infected in the first place.

"What if these seemingly benign infections that go uninvestigated and unremoved, are actually a decoy? What if there is much more dangerous functionality hidden in the code?"

Staff awareness helps to build a suspicious mind-set to spot, report and not click. Try a program of simulated attacks to teach familiarity of common techniques employed by attackers, so users have the ability to recognise phishing emails.

However, there are several defensive technologies that will make it harder

to get infected and for the infection to spread around your networks. Use of email security products to block known malicious senders and strip out known malicious attachment file types. Ad-blockers and script-blockers in browsers can help to a degree, but can be subverted if a user's machine is already infected. New isolation technologies can be very effective in preventing the download and execution of ransomware from phishing links, malvertising, web drive-bys and waterhole attacks.

Vulnerabilities can also be a factor so it's important to improve cyber-security hygiene such as keeping patches up to date to minimise the likelihood of a successful exploit.

Use of appropriate network segregation, access controls, privilege management and data access management helps to restrict ransomware's internal propagation and data discovery methods.

The future

NS: How do you see ransomware developing, both technically and in terms of how it is deployed by criminals?

TE: We've already seen ransomware evolve from targeting individuals to organisations, from a tool used by script kiddies to embarrass, to a versatile and effective cyber-attack tool that has fuelled a multi-hundred-million dollar criminal enterprise. We've already seen it be embraced by the crime-for-hire underground circuit and a 'design your ransomware' attack sold 'as-a-service'. So it's easy to predict a continuation of growth at both the top end and the bottom end of the market. New variants, exploiting new weaknesses will be developed. Some will be more and more targeted towards high-value systems to justify higher ransom demands and payouts. Whereas a more dangerous side effect is the low-end proliferation, whereby every pretender can have a go at writing ransomware and this could result in bad code and attacks that you may not be able to recover from.

A perhaps more sinister reflection – unfortunately, given how prevalent ransomware is – is that organisations are downgrading it as a threat and becoming complacent. This could leave us susceptible to ransomware as the wolf in a fox's outfit. While we dismiss it as a commodity threat that isn't impactful, in the meantime, ransomware is spreading merrily throughout our networks, perhaps sometimes not even locking up critical files. So it's allowed to reside dormant, deemed as unsuccessful. But what if these seemingly benign infections, which go uninvestigated and unremoved, are actually a decoy? What if there is much more dangerous functionality hidden in the code, that could be remotely activated, resulting in a widespread tool capable of espionage or permanent damage to systems and networks? This could be the future of ransomware, a tool that is masquerading as one type of threat but covertly achieving its objectives anyway. What if, while your board is debating whether or not to pay 1,000 bitcoins, the ransomware has already stolen a copy of all of the data it has currently locked up? Unless you get an expert in to investigate, you'll never know.

NS: Is this a problem that can be defeated?

TE: It's probably a crime that's here to stay, as whatever the defenders do to improve our ability to prevent and detect ransomware, it will only apply a selective pressure on the criminals to evolve their techniques and find new alternative methods of infection, discovery, harvest, targeting critical data and systems and encrypting them. While organisations and individuals do pay the ransoms, the business model is too lucrative for cyber-criminals to walk away from. This is why it is imperative for everyone infected to report the crime and get expert help. It will take a collaborative ecosystem to sufficiently raise the stakes for the attackers to make the attack no longer economically viable.

You can assist in working towards defeating the ransomware threat and in doing so hopefully avoid or minimise the impact it could have on your business by following these steps:

- Don't pay.
- Report any infections to the authorities.
- Treat it seriously and respond appropriately – get expert assistance fast, to investigate and fully understand the scope of the attack.
- Implement technical controls to prevent against known ransomware infections and rapidly detect when new infections occur.
- Follow security best-practice guidelines to maintain a good state of internal 'hygiene' to make it harder for the infection to spread and discover your critical data or systems.
- Ensure you have backed up all mission-critical systems and data and that these can be reliably and quickly restored to allow the business to be fully operational.
- Train your staff to raise awareness of the threat, how the attacks come into the business and the impact they could have.

The Firewall

Smart buildings need joined-up security

Colin Tankard, managing director, Digital Pathways

Today, much discussion in the technology world revolves around the Internet of Things (IoT), where billions of things will be interconnected over IP networks. Gartner estimates that, as of 2015, smart homes and commercial buildings made up 45% of the IoT.

Smart buildings are often run using building automation systems that are used to centrally control areas such as heating, ventilation, air conditioning, lighting and lifts.

But cyber-security is often an afterthought, which is an issue owing to the inter-connectivity of the systems involved over IP networks. There is the risk that building automation systems and all systems that connect to them, could be compromised by attackers who don't even need physical access.

Some attacks against smart buildings could easily incorporate a combination of attacks against both logical and physical controls. For example, a criminal could cause malware to be downloaded via a cyber-security attack that could lead to controls over the ventilation system being overridden.

To counter these problems, a protection platform is required that will take feeds from all systems connected to the building automation system, as well as those from cyber-security controls, so that events and log records can be collected centrally, allowing them to be analysed for patterns that could identify criminal activity.

Such a platform not only acts as a monitoring and reporting tool but enables more effective incident response. It should provide the capability to classify incidents recorded according to type and severity. To guide security operations teams through the incident response process, the platform should provide 'run books' according to the type of incident seen. These should be customisable for the needs of the organisation running the facility and its particular needs, providing guidelines for the steps that responders should take for remediating a particular threat, along with the ability to assign processes to members of the team best able to respond to particular issues.

This will then form a trail that not only provides reports to management that incidents have been dealt with in an appropriate manner, which is required not only for good corporate governance, but that will also provide auditable evidence that the organisation is complying with regulations such as PCI, data protection and health and safety regulations. It will prove that standard operating procedures have been followed and that the organisation has done what is necessary to safeguard itself and any building occupants from harm.

With the IoT, physical and logical security controls are finally seeing the convergence that has long been predicted. Control can only be achieved for connected devices if logical and physical security is brought together and fed directly into one platform that provides centralised management over all systems in use. The platform becomes the 'manager of managers'.

Smart buildings are already a reality and look set to be the norm in the future. They bring many benefits, including opportunities to reduce costs and increase efficiencies, but they also bring new types of risks that are not associated with traditional buildings. To deal with those risks, physical and logical security needs to be dealt with in a joined-up manner.

EVENTS CALENDAR

1–5 November 2016
Hackfest Infinity
Quebec, Canada
www.hackfest.ca/en

14–16 November 2016
World Congress on Internet Security
London, UK
www.worldcis.org/

18 November 2016
GreHack
Grenoble, France
https://grehack.fr/

6–7 December 2016
Threat Intelligence Summit
New Orleans, US
http://threatintelligence.misti.com/

6–7 December 2016
Payment Security & Identification
London, UK
www.pay-sec.co.uk

12–14 December 2016
World Congress on Industrial Control Systems Security
London, UK
www.wcicss.org

4–6 January 2017
Real World Cryptography Conference
New York City, NY, US
www.realworldcrypto.com/rwc2017

13–15 January 2017
Shmoocon 2016
Washington, DC, US
www.shmoocon.org

24–25 January 2017
FIC 2017
Lille, France
www.forum-fic.com