ELSEVIER

network SECURITY

ISSN 1353-4858 January 2020

www.networksecuritynewsletter.com

Featured in this issue:
It's time to rethink DDoS protection

Retailers are having to rethink how they approach distributed denial of service (DDoS) protection following the rise of a stealthier incarnation of the threat.

There has been a significant increase in small-scale DDoS attacks and a corresponding reduction in conventional large-scale events. The hacker's aim is to remain below the conventional 'detect and alert' threshold that could trigger a DDoS mitigation strategy. Roy Reynolds of Vodat International explains the nature of the threat and the steps organisations can take to protect themselves.

Full story on page 6…

Operational technology security – a data perspective

With operational technology (OT) and the Industrial Internet of Things (IIoT), one of the most commonly overlooked security issues is the values in the data.

The primary concern is the data elements that actually have an impact on the physical realm via values being set or modified. The objective is to not allow a hostile piece of data (ie, a value change) to reach a destination endpoint, such as a programmable logic controller (PLC), causing a negative physical action. Andres Andreu of Bayshore Networks argues that we need to have a deeper understanding of this data if we are to properly secure such environments.

Full story on page 8…

Securing workers beyond the perimeter

Teleworking is expanding, but some organisations – especially in financial services and the public sector – remain concerned about security.

Part of the issue concerns organisations that have failed to evolve IT security to match the growth of teleworking. Security tools are also lacking. Securing the remote workforce requires IT or security teams to conduct regular audit refreshes and IT security policy training sessions. This must be within the context of maintaining best-practice IT security processes, says Scott Gordon of Pulse Secure.

Full story on page 14…

Ring under fire over weakness in video device security

Ring, the Amazon-owned vendor of home video surveillance devices, has been coming under intense scrutiny due to security flaws in its products and what many see as a cavalier attitude to privacy.

Ring sells home CCTV cameras and door-entry systems that are connected to its cloud servers, allowing users to log into their cameras and use their microphones and speakers from any location. Amazon bought Ring in 2018 for over $800m.

Hackers have been taking advantage of poorly secured Ring devices to view video feeds and even talk to homeowners

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: Sarah Jenkins

Editor: Steve Mansfield-Devine
E-mail: infosec@webvivant.com

Senior Editor: Sarah Gordon

Columnists: Ian Goslin, Karen Renaud, Dave Spence, 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. Subscriptions run for 12 months, from the date payment is received.

More information: www.elsevier.com/journals/institutional/network-security/1353-4858

12987
Digitally Produced by
Mayfield Press (Oxford) Limited

...Continued from front page

via the cameras. A podcast calling itself NulledCast, livestreamed via Discord, went as far as broadcasting pranks in which hackers talked to Ring owners, often abusing and harassing them. In one instance, they demanded a Bitcoin ransom. In another, the hackers streamed video of one of them talking to an eight year-old girl in a threatening way and telling her he was Santa Claus.

Following international media coverage of the stunts, NulledCast attempted to cover its tracks, deleting messages from its forum. There are more details here: http://bit.ly/384Oxa2.

Gavin Millard, VP of intelligence at Tenable, said: "These intrusions aren't due to vulnerabilities in the firmware but how the devices have been set up."

This echoes a statement released by Ring in which it pointed out that no breaches of the system had taken place. The attackers are using credentials leaked in other, unrelated breaches and trying them against Ring installations, which are probably discovered using search engines. Such credential stuffing attacks work where people have reused passwords.

"Upon learning of the incident, we took appropriate actions to promptly block bad actors from known affected Ring accounts, and affected users have been contacted," Ring announced on its website. "Out of an abundance of caution, we encourage Ring customers to change their passwords and enable two-factor authentication."

The company advised users to use two-factor authentication (2FA), which would have prevented these hacks, to use the 'shared users' feature rather than sharing login credentials, and to use strong, unique passwords. However, the most effective of these – 2FA – is not enabled by default.

"At the moment, many IoT device manufacturers consider usability versus security for an end-user's 'out of the box' experience," added Millard. "I'd advocate this must be reversed so we see security policies, such as two-factor authentication, enabled by default."

An analysis by Motherboard found that Ring had failed to implement some basic security precautions, such as raising alerts when logins occur from other countries or previously unknown IP addresses, or if concurrent logins happen from different geographies. Ring does not appear to check logins against credentials that have been compromised – a step that many services are taking now. The report is here: http://bit.ly/2FMkrf3.

Ring has also admitted, in a letter sent to the US Congress, that over the past four years it has sacked a number of employees after they accessed video data in an inappropriate way. "In each instance, once Ring was made aware of the alleged conduct, Ring promptly investigated the incident and after determining that the individual violated company policy, terminated the individual," the letter said. The firm has also reduced the number of employees who can access the data to three. But this follows earlier reports by the Intercept that workers in Ukraine were being given access for research purposes. The letter is here: http://bit.ly/30g2tuP.

Ring came in for criticism recently when it emerged it had entered into deals with more than 220 local governments under which police departments would promote and hand out or sell Ring doorbells at deeply discounted prices to people in their neighbourhoods. These initiatives, often paid for with taxpayer money, involved the recipients giving the police access to the device's data, which could include automatically captured video of bypassers on public streets. It's believed that Ring also has similar partnerships with more than 400 fire and police departments. Ring has claimed these programmes have reduced crime.

Dave Limp, chief of Amazon devices and services, said at a recent conference that he is proud of these deals and suggested that Ring cameras could be linked to Amazon's face recognition systems to automatically surveil people passing properties equipped with the devices and alert law enforcement if matches are made against known criminals.

Citrix flaw threatens large firms

At the end of December 2019, Citrix disclosed a critical security vulnerability (CVE-2019-19781) that affected its Application Delivery Controller

Threatwatch

Millions of cable modems at risk
Broadcom chips used in hundreds of millions of cable modems have a buffer overflow flaw that could make the devices vulnerable to exploits such as changing the default DNS server, disabling ISP firmware upgrades and installing malicious firmware, as well as a variety of man-in-the-middle attacks and use of the device in a botnet. The vulnerability, dubbed 'Cable Haunt' (CVE-2019-19494), would also allow hackers to snoop on all traffic flowing through the modems. There could be as many as 200 million affected devices in Europe alone. There's more information here: https://cablehaunt.com/.

Snake ransomware bites
Researchers at MalwareHunterTeam have identified a new family of ransomware that appears to be targeted at businesses. Dubbed Snake, the malware attempts to infect every machine it can find on a network. It deletes each machine's Shadow Volume Copies before stopping processes associated with SCADA systems, network management solutions, virtual machines and other tools. It then encrypts the machine's files, although leaving certain critical Windows folders and files untouched. It also appends the string 'EKANS' as a file marker. A file called 'Fix-Your-Files.txt' containing the ransom demand is placed inside the public desktop folder. There's a detailed analysis at Bleeping Computer: http://bit.ly/30g4c3v.

TrickBot learns new trick
The operators of the TrickBot banking trojan have added a new capability to the malware. According to researchers at SentinelLabs, the 'PowerTrick' version of the malware adds a stealthy backdoor capable of executing commands and sending the results back to the Russian-speaking criminals in Base64 format. The PowerShell script behind this new capability is downloaded once TrickBot has gained a foothold on a machine. SentinelLabs believes the new feature has been developed for use against high-value targets. The malware operators are also using PowerShell to carry out a number of other tasks, the report says, such as delivering payloads to other targets. There's more information here: http://bit.ly/2TjMF93.

Cisco Webex flaws
Cisco has issued patches for two high-severity flaws in its Webex and IOS XE products. One (CVE-2019-16005), with a CVSS score of 7.2, affected the web-based management interface for the highly popular Cisco Webex Video Mesh video conferencing system. The vulnerability would have allowed an attacker to run arbitrary commands with root privileges on the underlying Linux operating system. There are details here: http://bit.ly/2NhyUE7. The other issue is a cross-site request forgery (CSRF) vulnerability in IOS XE, through which an attacker could perform arbitrary actions with the privilege level of the targeted user. There are details here: http://bit.ly/2tX6ng4. Both flaws can be remotely exploited but would require authentication, Cisco said.

IoT certificate flaws
Many Internet of Things (IoT) devices are using weak security certificates that make them vulnerable to attack, according to research by Keyfactor. The company discovered that 1 in 172 certificates was created using a weak form of random number generator. The researchers collected more than 60 million RSA keys available on the Internet plus another 100 million from logs belonging to Google's Certificate Transparency project. Analysis revealed that at least 435,000 of them shared factors used during RSA key generation. The researchers were able to use this information to ascertain the second factor used in each certificate, effectively rendering it useless. There's more here: http://bit.ly/383jawl.

and Unified Gateway products. Some 80,000 organisations in 158 countries – mostly large enterprises – were thought to be at risk.

The flaw could allow an attacker to gain access to an organisation's network and execute arbitrary code, including malware. It could also be used for denial of service attacks.

The affected products provide facilities for application-aware traffic management and secure remote access. Citrix has released a number of mitigations, available here: https://support.citrix.com/article/CTX267679.

The problem affects all supported versions of the products, and all supported platforms, including Citrix ADC and Citrix Gateway 13.0, Citrix ADC and NetScaler Gateway 12.1, Citrix ADC and NetScaler Gateway 12.0, Citrix ADC and NetScaler Gateway 11.1, as well as Citrix NetScaler ADC and NetScaler Gateway 10.5.

Roughly two weeks after the announcement of the vulnerability and the release of patches, a search revealed that around 25,000 installations remained unpatched. This represents a major risk because researchers have now released proof-of-concept exploit code. This allows an attacker to run arbitrary code simply through a directory traversal technique that requires no account credentials. The GitHub page is here: http://bit.ly/385naMZ.

In addition, security firms running honeypots report that hackers are actively probing the Internet with automated scans looking for Internet-facing systems with this weakness.

"Citrix has not said a lot about the specifics of the vulnerability, leaving many admins wondering if they are actually affected and unsure of how to forensically identify attacks," wrote Craig Young, a computer security researcher with Tripwire's Vulnerability and Exposures Research Team on the company's blog. "It is alarming that so many organisations are currently at risk in such a sensitive part of their organisation. Each one of these devices is an opportunity for criminals or spies to gain access to restricted networks and impersonate authorised users."

The post is here: http://bit.ly/2tRMd7i.

TikTok dangers

The TikTok video-sharing platform is coming under intense scrutiny after the US Government declared it a security risk and researchers unveiled a number of vulnerabilities.

The platform, owned by Beijing-based ByteDance, has over one billion users who share video clips lasting 3-60 seconds.

The US Navy told personnel that they should refrain from installing the app on any government-issued phones and tablets, and to delete it if they have already installed the software.

"This decision was made based on cyber security threat assessments and is consistent with 10th Fleet efforts to proactively address existing and emerging threats in defence of our networks," said Dave

Continued on page 19...

Report Analysis

Upstream Security: 2020 Global Automotive Cyber security Report

Not very long ago, the concept of having to perform software updates for your car would have seemed bizarre. Today's vehicles, however, are just more nodes on the network. From streaming music, providing traffic data and keyless operation through to battery management and telematics, cars now bristle with computers and communications capabilities.

This development has many benefits, including greater efficiency and convenience. But there's always a second edge to a sword. This, of course, is the potential for vulnerabilities that comes with network connectivity.

Upstream Security's report looks at 10 years' worth of security incidents associated with vehicles, as reported by journalists, security researchers, the Common Vulnerabilities & Exposures (CVE) database, bug-bounty programs and other open, online sources. Only public sources were used – private data, including that held by the firm's own teams, does not form part of the analysis. Upstream Security found 367 incidents, of which 155 occurred in 2019, but the report acknowledges that there might be cases it has missed.

The fact that more than two-fifths of the incidents happened in the past year is hardly surprising. In fact, some of the report's headline statistics – that there has been a 99% growth in incidents since 2018 and a 94% year-on-year growth since 2016 – are only to be expected. The connected vehicle is still a relatively new phenomenon, and few people change their cars as often as they upgrade their laptops.

In addition, the degree of connectivity is ramping up all the time. From a security point of view, this means an expanding attack surface. As the report explains: "Each new service and capability introduces additional risks, points of entry for hackers and opportunities for potential privacy breaches. As the use of connected vehicles and smart mobility services increases, there is a growing number of cyber, fraud and data-breach incidents, threatening both companies and consumers."

What's perhaps more interesting is the variety of attacks. Many of us, particularly in the information security field, are familiar with hacks involving radio relays to unlock and start people's cars in their own driveway using key-fobs left indoors but within radio range. And there was the infamous Wired story about a proof-of-concept hacking of a Jeep while it was in motion. But cyber attacks in the automotive realm range much wider than that.

"The connected vehicle is still a relatively new phenomenon, and few people change their cars as often as they upgrade their laptops"

The attacks include hacking smart car alarms and anti-theft systems to track vehicles, and exploiting flaws in locking systems. But from a network perspective, what are arguably more interesting and significant are the breaches of back-end and cloud-based systems. The exploitation of the Car2Go car-sharing app, for example, resulted in more than 100 cars being stolen. Uber and Lyft both suffered account hacks that permitted cyber criminals to combine rideshare accounts with stolen payment card data to launder money. And Toyota, Honda and Mercedes-Benz all incurred database breaches that spilled the data of employees and customers.

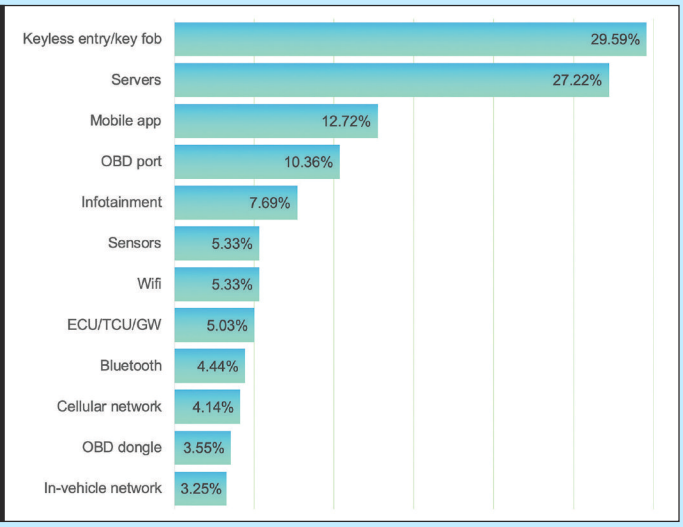
But to get back to the attack surface, where do the vulnerabilities lie? Predictably, keyless entry and starting systems feature most prominently, closely followed by 'servers' – ie, back-end or cloud systems. Cars' network connectivity – wifi, Bluetooth and cellular network connections are obvious points of attack, the onboard diagnostics (OBD) system perhaps less so. The OBD bus has been in cars for a long time, before remote connectivity and sophisticated onboard computers became common. But now that everything is connected inside the vehicle, any point of entry offers a route to compromise the entire system. And that's why the car's 'infotainment' system also features on the list.

Upstream Security is keen to emphasise that the 'majority' of incidents from 2019 were malicious, carried out by 'black hat' attackers. The figures don't paint quite such a black and white picture. Some 38% of the incidents or reports concerned proof-of-concept exploits or analyses by security researchers, with 57% – not much more than half – being carried out by cyber criminals. It's hard to say how these proportions compare to the wider information security realm, but with such a relatively small number of incidents to start with, this hardly represents a crime wave.

What those figures do tell us is that this is an area of security that's drawing a lot of interest and attention, from both sides of the cyber world. That's reflected in the growing number of bug bounties, including some from names not normally associated with such schemes, such as Ford, TomTom, BMW and Daimler.

The clearest message from this report is that automotive cyber security is not yet a major issue. Many of the vulnerabilities and incidents detailed here are – if one can put it this way – perfectly ordinary cyber security matters, such as breached databases. Once you remove those from the data, what's left – the stuff that's specific to vehicles and automotive businesses – is small in volume. But as we get closer to autonomous vehicles, and as transport becomes more connected, the problems can only increase.

The report is available here: www.upstream.auto/upstream-security-global-automotive-cyber security-report-2020/.



The most common attack vectors against vehicles. Source: Upstream Security.

In brief

Irish strategy

Ireland has published its National Cyber Security Strategy, which, it says, "sets out the Government's vision of a secure and reliable cyberspace to optimise and promote use of information systems for economic and social growth". The digital economy contributes 5% to the nation's GDP and employs more than 100,000 people. Ireland is a popular base for large tech companies, not least because of its friendly attitude to corporate taxes. The new document outlines how government departments will co-operate – with each other and with external organisations – to protect key systems and data. The strategy document is available here: http://bit.ly/2QSkufX.

ToTok returns after privacy worries

The ToTok social networking app has returned to Google's Play store after being removed due to fears that it was being used by the Government of the United Arab Emirates (UAE) to spy on citizens. A New York Times article cited intelligence officials when it reported that the recently launched app was being used by the UAE to grab conversations, locations, relationships, diaries and even audio and images from users in the country. The app is available globally but has become especially popular in the UAE. Google gave few details for the app's suspension, nor for its reinstatement, although it has been noted that small changes have been made to the code. Apple, which also suspended the app, has not so far reinstated it to its App Store. The New York Times report is here: https://nyti.ms/2FHpldt.

Interpol fights crypto-mining

Interpol is claiming a major victory against crypto-mining following the successful completion of an operation in Asia. Research showed that more than 20,000 routers in the ASEAN region were infected with crypto-mining malware, representing 18% of all infections worldwide. Over the course of five months, Operation Goldfish Alpha identified the routers, alerted their owners and installed patches to eradicate the malware. The operation was mounted by law enforcement agencies and CERT staff from Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam, as well as support from security firms, including Trend Micro. The end result was a 78% decrease in the number of infected routers, and work is continuing on locating and fixing the remainder.

Patients blackmailed

The patients of a facial surgery firm in Florida are being blackmailed by hackers who successfully breached the company's networks and stole private data. The Centre for Facial Restoration (TCFFR) was hacked in November 2019 and its owner, Dr Richard Davis, received a ransom demand. It's not clear if he paid it. Since then, Davis said that as many as 20 patients had individually received ransom demands, with threats that their personal information, including photographs, would be made public. There's more information here: http://bit.ly/2Rbc95U.

UK police losing devices

On average, UK police forces lost or had stolen four devices a day over the course of the most recent financial year, according to data from the Parliament Street thinktank. Based on a Freedom of Information (FoI) request, data from the 22 forces that responded showed 2,600 devices lost or stolen in the past three years, with 1,360 of them going missing in the past year. The most unfortunate force was West Midlands Police, which reported 1,012 missing devices over three-year period, including 16 laptops, 112 mobile phones and 884 police radios.

Facebook data exposed

A database containing the user IDs, phone numbers and names of more than 267 million Facebook users was left exposed on an ElasticSearch server, according to security researcher Bob Diachenko and a team from Comparitech. They believe the data was probably gathered by cyber criminals using web scraping techniques and might have been intended for "large-scale SMS spam and phishing campaigns, among other threats to end users". Although the data was removed by the ISP managing the IP address of the server, it subsequently turned up on a hacker forum. There's more information here: http://bit.ly/2uMYb2J.

SHA-1 hacked

The SHA-1 hashing algorithm, which has been known to contain weaknesses for some time, can now be compromised in what researchers are claiming is a 'practical' attack. Flaws in SHA-1 were first found in 2004, with a complex proof-of-concept collision attack being demonstrated in 2017. In 2019, Gaëtan Leurent, from Inria in France, and Thomas Peyrin, from Nanyang Technological University in Singapore, suggested a new attack method and, at the recent Real World Crypto Symposium in the US they announced an attack that can create colliding messages with two arbitrary prefixes, "which is much more threatening for real protocols". Their paper, 'SHA-1 is a shambles', is here: https://eprint.iacr.org/2020/014.pdf.

Windows 7 threat

As many as a quarter of Windows-based PCs are still running on Windows 7, according to figures from Veritas Technologies. This means that Microsoft's decision to 'end of life' the OS on 14 Jan 2020, with no further security patches or OS updates for the majority of users, will significantly increase the number of vulnerable machines. Mainstream support for Windows 7 ended in 2015, giving users a five-year period in which to move up to supported operating systems. But the Veritas research suggests that 26% of Windows users remain stubbornly attached to the obsolete software. A significant number of these will be in areas such as healthcare where the machines are used to run devices and services using software not compatible with later incarnations of Windows.

APT group pivots to power

An advanced persistent threat (APT) group, dubbed Magnallium, which is believed to have links to the Iran-based APT33 group, appears to have changed tactics and, instead of targeting the global oil and gas industry, is now focusing on electricity companies in the US. According to security firm Dragos, an off-shoot of Magnallium, which the firm has labelled Parasite, has been seen targeting known vulnerabilities in VPN systems used by electricity businesses in the US. There's more information here: http://bit.ly/2TfkWq6.

More mobile DDoS

The number of distributed denial of service (DDoS) attacks has risen by 86% in the past year, with mobile platforms playing an ever-larger role, according to the latest figures from NexusGuard. DNS amplification attacks are increasingly the attack method of choice for cyber criminals. But there's also been a 41% increase in application attacks coming from mobile gateways, and three-quarters of that traffic is coming from Apple iOS devices. There's more information here: http://bit.ly/2FKtYDp.

Data regulations

More than half (54%) of UK citizens believe that the Government should take greater steps to regulate the personal data it gathers, according to a report by Fujitsu. While most people want the easier and more efficient engagement with government services that are provided by consumer-like services, they are also worried about how the data is used. The biggest concerns are about the sharing of personal data (35%), lack of trust in how organisations use their personal data (34%) and doubts about the reliability of technology (31%). From the other side of the fence, more than two thirds (67%) of leaders in public sector organisations say they are concerned they will never fully satisfy citizens' expectations and a further 48% feel that that organisations are put under too much pressure to positively drive society. However, a third (66%) of them feel positive about the changes that their organisations are likely to experience in the next five years, with three in five (61%) saying that technological innovation (for example AI, mobile or automation) has had a positive impact. The report is here: http://bit.ly/35N7a0r.

It's time to rethink DDoS protection


Roy Reynolds

Roy Reynolds, Vodat International

When you think of distributed denial of service (DDoS) attacks, chances are you conjure up an image of an overwhelming flood of traffic that incapacitates a network. This kind of cyber attack is all about overt, brute force used to take a target down. Some hackers are a little smarter, using DDoS as a distraction while they simultaneously attempt a more targeted strike, as was the case with a Carphone Warehouse hack in 2015.[1] But in general, DDoS isn't subtle.

Now, however, retailers are having to re-think DDoS protection following the rise of a smaller, stealthier incarnation of the threat. A recent report by cyber security experts Neustar reveals a significant increase in small-scale DDoS attacks and a corresponding reduction in conventional large-scale events.[2] The hacker's aim here is to remain below the conventional 'detect and alert' threshold that could trigger a standard DDoS mitigation strategy so that an attack can continue unnoticed while specific areas of the target network are incapacitated.

Under the radar

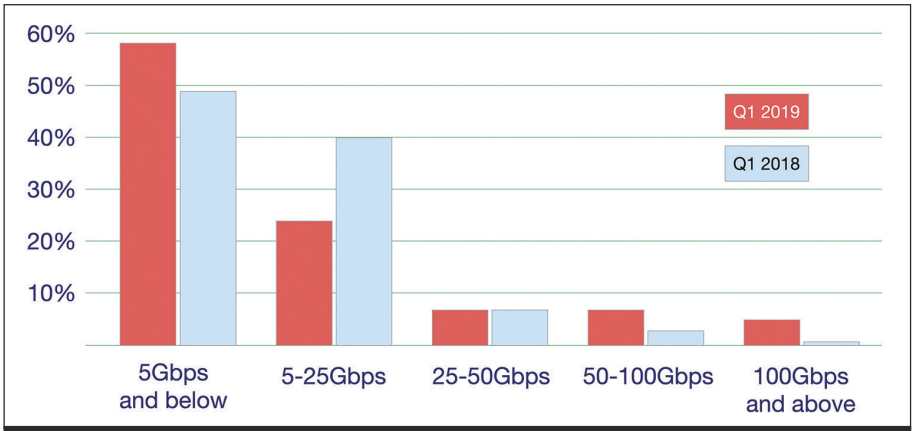
The Neustar report reveals that between April and June of 2019, over 75% of all attacks mitigated by Neustar were 5Gbps or less, while large attacks – those of 100Gbps and over – decreased by 64%. This showed an increase in these smaller attacks even compared to the previous quarter, when attacks in the 5Gbps or less range represented just under 60% of all DDoS incidents.

"Organisations need to create a business 'risk register' that enables them to focus primarily on their most critical business assets so security efforts can be prioritised correctly"

These smaller, stealthier DDoS attacks are designed to enable the perpetrator to get in and out of a network unnoticed or allow the attack to continue for quite a long time undetected. In fact, the longest duration for a single stealthy DDoS attack in Q2 of 2019 was nearly two days. Under-the-radar incursions like these are aimed at specific services, gateways and applications so they need less traffic to bring them down.

When quizzed by Neustar, 72% of CTOs, CISOs and security directors revealed that their systems would be unable to detect and protect against this new breed of stealth DDoS attacks.

The answer to the emerging threat is for organisations to deploy an 'always on' DDoS mitigation service that can constantly monitor traffic to ensure threats of all sizes are quickly detected, managed and neutralised. Organisations also need to create a business 'risk register' that enables them to focus primarily on their most critical business assets so security efforts can be prioritised correctly.



Various sizes of DDoS attacks seen by mitigation systems in the first quarters of 2018 and 2019. Source: Neustar.

Critical evolution

As well as the rise of stealth attacks, DDoS has evolved in five other critical ways:

1. **Access**: Black market services, known as 'rent-a-bot', make it easy for almost anyone to launch a powerful DDoS attack against a business for a nominal fee.
2. **Complexity**: New DDoS techniques have made DDoS exponentially more powerful and harder to defend against due to increased complexity and sophistication.
3. **Cost**: DDoS attacks now cost victims £40,000 per hour, with an average duration of six to 24 hours.
4. **Ransom**: Cyber extortion is now common with DDoS – 46% of companies that suffered DDoS attacks admit they received a ransom note.
5. **Diversion**: DDoS is frequently used as a smokescreen for other attacks, such as stealing customer data (33%) or implanting viruses and malware (50%).

Culture shift

Effectively combatting the DDoS threat requires a culture shift for many retailers

as, until now, they have been heavily focused on point-of-sale malware and online attacks targeting credit card data. In fact, some 33% of all cyber attacks on retailers employ DDoS, making it the most common digital threat the sector currently faces.

While in years past this type of attack was primarily used for pranks and petty mischief, it is now increasingly used by organised cyber criminals to threaten retailers' operational and financial security. When executing a DDoS attack, threat actors set their sights on any organisation that relies heavily on its website to generate revenue. This makes retailers ideal targets.

"The threat actors' success depends on their capabilities and credibility. While the accessibility of off-the-shelf tools to execute DDoS attacks has lowered barriers to entry, low-credibility, low-capability actors do still exist"

Attacks can start with a threat of DDoS action followed by a ransom demand, so the threat actors' success depends on their capabilities and credibility. While the accessibility of off-the-shelf tools to execute DDoS attacks has lowered barriers to entry, low-credibility, low-capability actors do still exist.

Protective steps

There are some key steps that retailers can take to protect themselves from the DDoS threat.

Identifying an attack: It's critical to identify a DDoS attack immediately, in order to prevent further damage, reputational loss and secondary attacks. To do this, establish a baseline of what normal network traffic looks like: that way you can quickly detect network traffic anomalies and attribute spikes in traffic to DDoS attacks.

DDoS attacks quickly cripple server performance and the first clue that you're under attack is a server crash. With IIS, the server often returns a 503 'Service Unavailable' error. It usually starts intermittently displaying this error, but heavy attacks lead to permanent 503 server responses for all of your users.

Another hint is that the server might not completely crash, but services become very slow. It could take several minutes to submit a form or even render a page. Whether you suspect that your server is under attack or you're just curious about its stats, you can start an investigation using the long-established Netstat utility included in any Windows operating system.

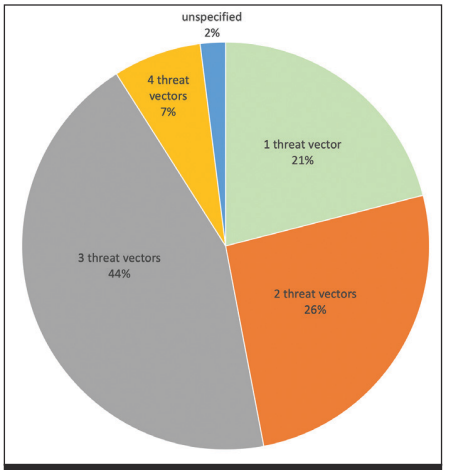
Establish a DDoS policy: At a bare minimum, every retailer should have a policy in place for educating staff about DDoS attacks and the various risks they pose, as well as how the company is expected to respond. For example: what will the company do to inform and reassure customers? How will the company deal with ransom requests?

It is best practice for IT departments to proactively monitor network traffic around the clock, and request logs and graphs for servers each day from the hosting provider. In case of an attack, the IT team should request graphs and logs for the attack IP so a company can go to its provider and identify the IP that is attacking it. SYN flood and UDP can be faked and therefore can't be used as evidence.

It is a good idea to have more bandwidth available for services to accommodate unexpected surges in network traffic that could be a result of a media press release, or a DDoS attack. Even though overprovision won't prevent a DDoS attack, it can give an organisation more time to act before resources are overwhelmed.

It also makes great sense to determine how many connections a network can hold in case of an attack. The IT team should also discover opportunities to cluster websites, DNS and parameters to push malicious traffic to other sites. There is also an option to deploy on-premise devices that inspect the incoming traffic and mitigate fake traffic after identification.

One possible option to prevent or mitigate DDoS attacks is to partner with the company's ISP, since the overload of traffic has to go over the ISP's network infrastructure. The ISP may have solutions available to shun specific IP addresses, which can reduce the impact



Numbers of threat vectors used in DDoS attacks mitigated by Neustar in Q1 2019. None of the most serious attacks used only a single vector. Source: Neustar.

of the attack. For example, an ISP may be able to apply black hole filtering, a technique that provides the ability to stop undesirable traffic before it makes its way into a protected network.

Approaches to DDoS mitigation

Before analysing DDoS risk, it is useful to understand the protection provided by various security methods and their limitations. Firewalls, for example, have long been deployed at network perimeters in an attempt to keep malicious attackers from penetrating retailers' networks.

The fact is that firewalls are not very effective in dealing with the modern-day, multi-vector DDoS attack. In-cloud scrubbing services go back to the early 2000s when DDoS attack methods were first being experienced. They began emerging as a way to inspect large volumes of traffic in ISP networks, in order to remove malicious traffic before traffic is allowed to enter corporate networks.

Given that the majority of DDoS attacks are based on volume, cloud scrubbing services deliver a high degree of protection. However, cloud-based scrubbing services do have a weakness. Due to the massive amount of traffic they are analysing, they struggle to recognise the 'low and slow' application-layer attack.

Preventing secondary attacks: To prevent a secondary attack during a DDoS event, avoid key mistakes: don't

overlook alerts issued by your monitoring system, be cautious of any other unusual activity on your network and be on the lookout for 'social engineering' attempts on IT personnel or other company staff, such as phishing emails or phone call scams.

"Some DDoS attacks are designed to deflect attention away from one target so that the attackers can conduct secondary attacks on other services within your network"

A secondary attack may be unseen because other hosts, assets, or services on the network may be the target. Some DDoS attacks are designed to deflect attention away from one target so that the attackers can conduct secondary attacks on other services within your network.

Cyber insurance: Retailers should also make sure DDoS incidents are covered by their cyber insurance plans, including costs associated with mitigation attempts, downtime and cyber ransoms. The three main areas of cover are: liability, to cover you for damages you are legally liable to pay to third parties in the event of a breach of privacy law where their personal data is lost, stolen or incorrectly made available; breach response, to cover investigation costs, legal and communications; and thirdly, cybercrime, to cover direct losses due to business interruption.

Conduct a simulated DDoS attack: DDoS 'black box' testing is the only way to test a retail network against a simulated real-world attack. This allows retailers to see exactly how their networks will react to a sophisticated DDoS attack and whether the defences put in place are sufficient. This means conducting network attack simulations with the largest number of attack types and levels of intensity. Gartner recommends quarterly testing as threat vectors alter so rapidly.

Call in the experts: Every retailer, no matter how big, should have a third-party always-on DDoS mitigation service that will reroute traffic and scrub out illegitimate traffic once an attack begins. The volume, scale and variety of DDoS attacks are increasing, so it is important to work with experts that have experience of attacks of all kinds in all types of industry.

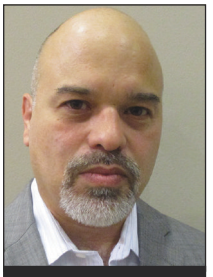
About the author

Roy Reynolds is technical director at Vodat International (www.vodat-int.com). He has over 20 years' experience in IT and communications. One of the founding members of Vodat in 2002, Roy was appointed to his current position in 2005, where he oversees the technical support function at Vodat International and is responsible for the creation and delivery of products, services and innovations to the marketplace by managing technical risks, opportunities and partner relations.

References

1. Buchanan, Rose; Merrill, Jamie. 'Carphone Warehouse hack: 2.4 million customers' details breached after cyber attack'. Independent, 9 Aug 2015. Accessed Jan 2020. www.independent.co.uk/news/uk/crime/carphone-warehouse-hack-24-million-customers-details-breached-after-cyber attack-10446745.html.
2. 'New cyberthreats report reveals that DDoS attacks still challenging'. Neustar. Accessed Jan 2020. www.home.neustar/resources/whitepapers/cyberthreats-report-q1-2019.

Operational technology security – a data perspective


Andres Andreu

Andres Andreu, Bayshore Networks

In the evolution of the operational technology (OT) and Industrial Internet of Things (IIoT) landscapes, one of the most commonly overlooked areas within cyber security is that of the actual values in the data. Contextually this means that when the term 'data' is used, the reference is to data seen beyond network metadata (ie, source address, source port, destination address, destination port, etc).

Specifically, the focal points of concern are the data elements that actually have an impact on the physical realm – via values being set and/or modified – by manifesting action (eg, a robotic arm performing some action, a centrifuge spinning at a specified rate, etc). This is so because when faced with a security incident, the objective is to not allow a hostile/dangerous element of data (ie, value change) to reach a destination endpoint, as in a programmable logic controller (PLC), where there is negative/unwanted physical action.

Chief information security officers (CISOs) and security practitioners on the defending side need to realise that the OT security space is at a stage eerily parallel to the web application security

space in the early 2000s. Back in those days, the information security (infosec) community was predominantly populated by those with a very heavy network-centric background and skillset who had rudimentary levels of understanding of web applications.

The OT security space is in a state where the skillsets and focus do not always match certain aspects of the problem and challenges at hand. In the early 2000s when web application experts – the ones who understood that a major aspect to securing web applications existed at the data level (think payload in an HTTP POST) – used to speak to the security experts, there was often friction due to the different perspectives. The answer to most web application problems existed in network-centric solutions and the use of SSL/TLS. There was this notion that simply because one implemented HTTPS, instead of HTTP, that their web applications were secure.

Obviously time has shown that true web application security goes way beyond simply encrypting communications streams via SSL/TLS. The pioneering web application security experts were pushing security awareness past the point of understanding because infosec experts of that era were not thinking in terms of the data and the values within the data.

The reasons for the disjointedness in security awareness levels were understandable. How does one explain code or data-level issues in a web application to people who live in a world of subnet masks? It's a different mindset. For example, Structured Query Language (SQL) injection (SQLi) attacks would be shown to people who had probably never written a SQL query in their entire careers.

In the OT security space, we currently see parallels to those early days of web application security. For instance, network segmentation and air-gapping networks are pushed a lot in respect to strengthening an OT network's security posture. While there is certainly some value to network segmentation and air-gapped networks, they are not silver bullets. And if either of those solutions are bypassed, there is very little left by way of real protection.

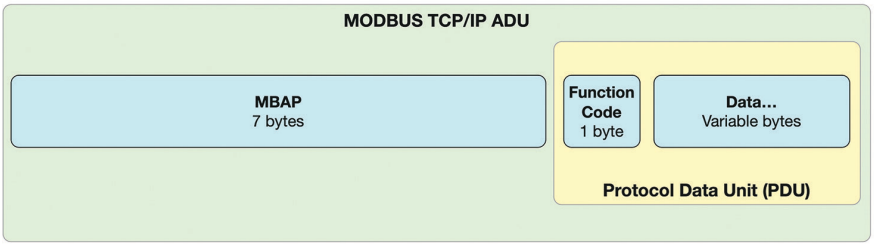


Figure 1: The typical structure of Modbus/TCP transactions.

Network visibility

One of the main focal areas is, and has been for the last five or six years, network level visibility (ie, asset discovery: what source is communicating with what destination, etc). This kind of visibility only gives you a partial view of the overall attack surfaces at hand. This data is certainly important but only provides a basic understanding that offers very little in the way of actual protection.

"But ultimately we are talking about an event where 'knowing what is on your network' offers little real security value other than some insight and understanding"

Sophisticated attacks, such as Stuxnet, have clearly shown that somewhere in the chain of an attack there will be a value-level trigger/event that forces a change downstream and that will have a physical impact on an environment. This will most likely take place with an action that forces an unwanted change at a data/value level. Think of set point data, such as coil/register values in the Modbus/TCP space as an example.

But ultimately we are talking about an event where 'knowing what is on your network' offers little real security value other than some insight and understanding.

"The OT security space is in a state where the skillsets and focus do not always match certain aspects of the problem and challenges at hand"

Let's use Modbus/TCP (typically used in manufacturing, process automation and similar operations) to point out some details relevant to these musings. We are talking about operations that take place at Layer 7 in the OSI Model. A 'master' is the client when it comes to network communications, and the server is a 'slave'. Let's focus on where the relevant data/value elements exist when Modbus/TCP transactions take place. These exist inside of the Protocol Data Unit (PDU), which in turn exists inside the Application Data Unit (ADU). The PDU is further broken down into a one-byte function code (an integer) and a variable byte length data section. See Figure 1 for a visual depiction of this structure as published in 'Real Time MODBUS Transmissions and Cryptography

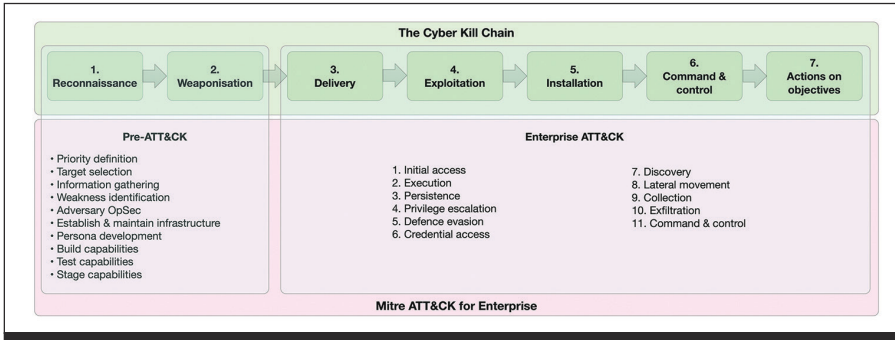


Figure 2: Mitre ATT&CK for Enterprise and the Cyber Kill Chain.

```
00 0c 29 60 d0 f0 40 8d  5c c6 8b f0 08 00 45 00   ..)`..@. \.....E.
00 3f f5 1c 40 00 40 06  fb ae c0 a8 64 63 c0 a8   .?..@.@. ....dc..
64 39 c5 72 01 f6 15 e1  94 75 98 e2 34 06 80 18   d9.r.... .u..4...
00 e5 b2 04 00 00 01 01  08 0a 01 92 61 6f 00 0d   ........ ....ao..
c8 eb 00 00 00 00 00 05  01 2b 0e 01 00            ........ .+...
```

Figure 3: An example of a Modbus/TCP traffic payload.

```
00 0c 29 60 d0 f0 40 8d  5c c6 8b f0 08 00 45 00   ..)`..@. \.....E.
00 3f f5 1c 40 00 40 06  fb ae c0 a8 64 63 c0 a8   .?..@.@. ....dc..
64 39 c5 72 01 f6 15 e1  94 75 98 e2 34 06 80 18   d9.r.... .u..4...
00 e5 b2 04 00 00 01 01  08 0a 01 92 61 6f 00 0d   ........ ....ao..
c8 eb 00 00 00 00 00 05  01 2b 0e 01 00            ........ .+...
```

Figure 4: The critical elements of data that identify the purpose of the request.

```
00 0c 29 60 d0 f0 40 8d  5c c6 8b f0 08 00 45 00   ..)`..@. \.....E.
00 3f f5 1c 40 00 40 06  fb ae c0 a8 64 63 c0 a8   .?..@.@. ....dc..
64 39 c5 72 01 f6 15 e1  94 75 98 e2 34 06 80 18   d9.r.... .u..4...
00 e5 b2 04 00 00 01 01  08 0a 01 92 61 6f 00 0d   ........ ....ao..
c8 eb 00 00 00 00 00 05  01 2b 0e 01 00            ........ .+...

>>> h = '0x2b'
>>> int(h, 16)
43
```

Figure 5: Calculating the decimal value of the hexdecimal byte.

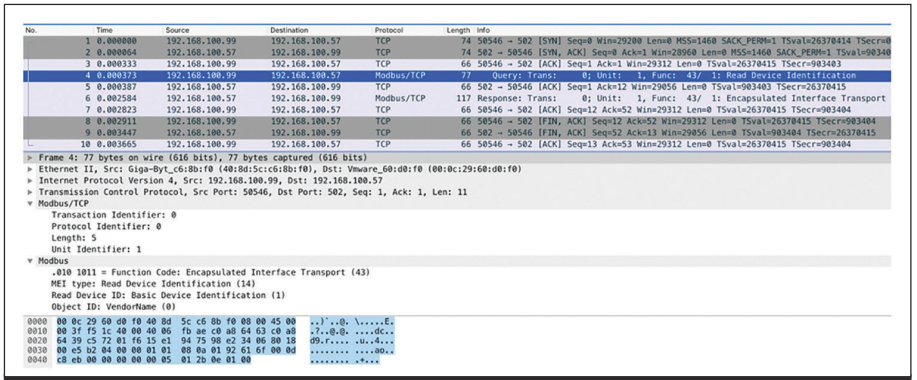


Figure 6: A tcpdump of a function code 43 request.

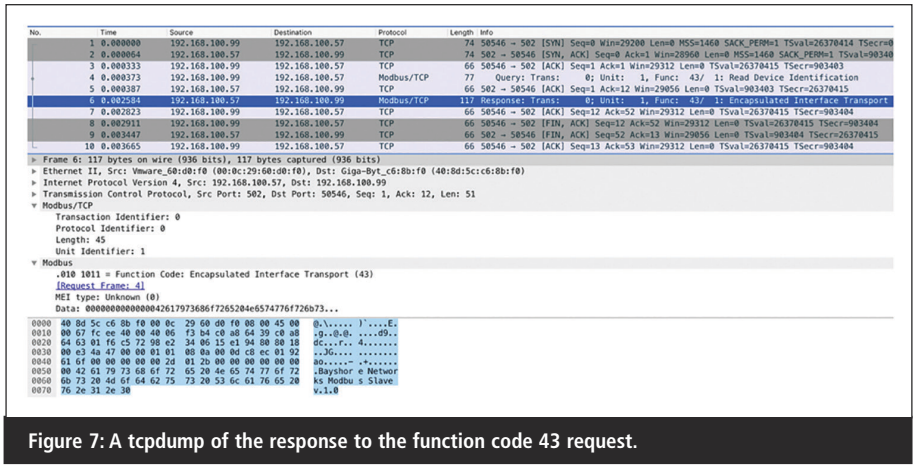


Figure 7: A tcpdump of the response to the function code 43 request.

Security Designs and Enhancements of Protocol Sensitive Information'.[1]

Keeping the security perspective focused on data-level elements and interactions, let's take a look at a few areas. These areas map to critical points in the Cyber Kill Chain model as set forth by Lockheed Martin and by Mitre's ATT&CK framework as seen in Figure 2.[2,3] While this model is generically enterprise focused, it serves as a solid reference. Author Daniel Ehrenreich also has a great analysis (a 12-step process) that extends past this Cyber Kill Chain model and provides a more detailed approach focused on advanced persistent threat (APT) approaches as they touch both enterprise and OT environments.[4] For the attack stages we cover in this body of work, the stage name from the Cyber Kill Chain is presented on the left side of a dash with the right side presenting the name from the 12-step process (where applicable).

Reconnaissance: initial access attempt

As far as reconnaissance activity is concerned, there are many aspects to this and they range from the technical to the social engineering realms. Since the focus here is the data level, and OT/ICS data specifically, we consider general areas with an extension past the IT network itself:

1. Port scanning (as in the traditional enterprise sense).
2. Device enumeration activity.
3. Device identification activity.

For the sake of this article we will focus on device identification reconnaissance activity as it is very relevant to the OT security landscape. Moreover, it is a highly subjective area given that OT, or ICS, communications protocols handle these types of requests in unique ways. Some OT communications protocols don't support this type of functionality at all but savvy attackers will study the target protocol at hand and use these types of discovery functions to their advantage. Staying with Modbus/TCP as the basis for our example area, it does generically support this type of capability via a specific function.

As a device identification example, Figure 3 shows an example of some Modbus/TCP traffic payload. It is important to note that most OT communications protocols – in particular some of the older ones that are still very much prevalent in the field – are binary, and not text-based, in nature. Looking at Figure 3, we see hexadecimal encoded values on the left and their respective ASCII equivalents on

the right. The right side purely displays the binary (ie, non-ASCII) nature of this type of network traffic.

Our objective is to identify the part of this granular data that establishes this traffic as requesting a Modbus endpoint (typically a slave) to identify itself. Figure 4 highlights the critical elements of data that clearly identify what this request is attempting to do. This is due to domain knowledge of the protocol in question where we know the first byte of the PDU represents the function code in a Modbus/TCP packet.

Figure 5 shows a bit of data conversion that makes the hexadecimal value, in this case 0x2b, more relevant to the analysis at hand. We now know that decimal 43 represents the function code in question. Referring to section 6.21 of version 1.13 of the protocol specification we see that function is a diagnostic function that asks the receiving entity to respond with its identifying information. So if that type of request packet makes it to a target Modbus slave, and the slave in turn responds with its identifying data, an attacker could gain a critical piece of information in order to craft very targeted attack patterns. Figures 6 and 7 show some tcpdump data (network packet captures) in Wireshark depicting a function code 43 request and response respectively.

Listing 1 shows a simple YARA (yet another recursive acronym) rule to detect this type of traffic on network flows.

```
rule Modbus_Reconnaissance_Slave {
    meta:
        description = "Disallow the ability to identify a
        ModbusTCP device"
    strings:
        $payload_byte = {2b}
    condition:
        $payload_byte at 7
}
```

Listing 1: A simple YARA rule to detect an attempt to identify a ModbusTCP device.

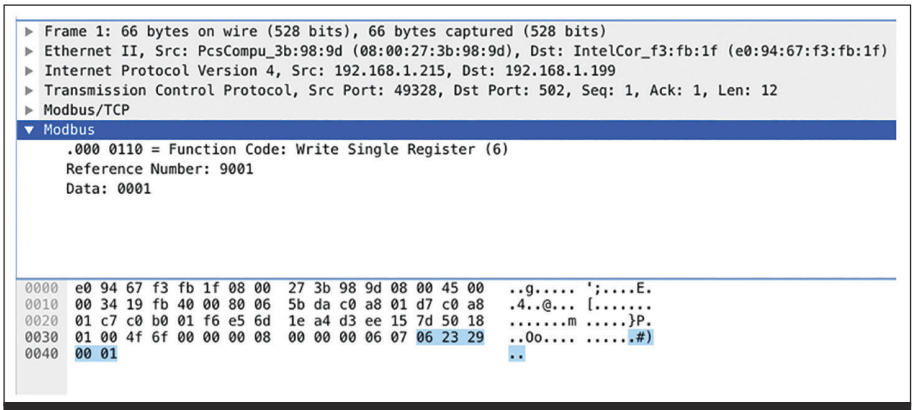


Figure 8: An example of a packet used to write to the Acceleration Ramp Time register.

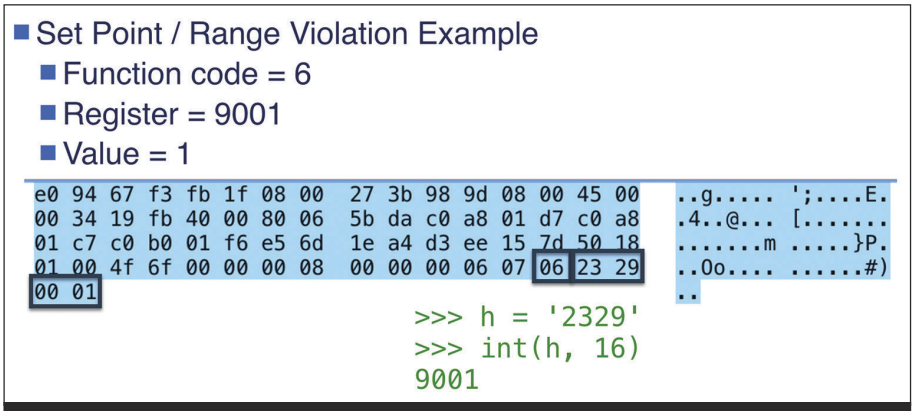


Figure 9: A more detailed view of the packet used to write to the Acceleration Ramp Time register.

Exploitation

Exploitation can come in many forms. Based on our focus here, the examples we look at map to native protocol-level attacks based on actual set point values (ie, data). The real world relevance of these concrete examples revolves around risk to human life. Here you will see some interesting examples based on data, or specifically register-level values. These examples are based on a real product and its data set points that communicates via Modbus/TCP, for a variable frequency drive (VFD) that interacts with a motor. The values that are set in certain registers are used to alter the physical behaviour of the motor and if set past normal operating constraints can create physical damage.

Let's look at some concrete, subjective (ie, they are for a specific make and model of VFD) examples of the effects of altering the configuration.

The Acceleration Ramp Time (register 9001) is used to control how quickly the VFD will accelerate a motor. The nominal value is 100. Writing a value of 1 to this register will cause the drive to accelerate as fast as possible, which is usually an unacceptable rate. On a large motor this can be physically destructive to it, as well as any devices connected to it. Figure 8 shows an example of this data when the packet is captured and displayed in Wireshark. Figure 9 gives a different level of detail of this same data.

The Deceleration Ramp Time (register 9002) is used to control how quickly the VFD will decelerate a motor. The nominal value is 100. Writing a value of 1 to this register will cause the drive to decelerate as fast as possible. This again is usually a rate that can be physically destructive.

The Low Speed Register (register 3105) is the lowest speed that the motor is allowed to run at. The High Speed Register (register 3106) is the highest speed that the motor is allowed to run. Writing a value of 100 to both of these

```
02 00 00 00 45 00 00 34 fb 55 40 00 40 06 00 00
7f 00 00 01 7f 00 00 01 c0 9d 5a 42 07 1e 77 ac
67 9b fb a2 80 10 31 d4 fe 28 00 00 01 01 08 0a
35 82 26 19 35 82 26 5b

        0x19 = 25

02 00 00 00 45 00 00 34 17 36 40 00 40 06 00 00
7f 00 00 01 7f 00 00 01 c0 9d 5a 42 07 1e 77 ac
67 9b fb a2 80 11 31 d4 fe 28 00 00 01 01 08 0a
35 82 26 6e 35 82 26 5b

        0x6e = 110
```

Figure 10: An example of a proprietary IIoT protocol.

registers forces the drive to run at 100%, which creates a condition where there is potential negative impact.

A hostile act can also include a change to the cooling fan mode (register 3130) to a value of 2, which turns the fan off. That will severely elevate the temperature of the VFD, and in turn shorten the life of the motor windings. Beyond this, there are other registers that can cause conditions of overheating and/or physical denial of service.

IIoT protocol

For the sake of variety, and in the spirit of the importance of data values, see Figure 10, which represents a proprietary IIoT protocol example.

This data is typically seen going across the wire in raw binary form. To an analyst who doesn't understand this type of binary data, represented in hexadecimal, the difference between '19' and '6e' may seem trivial. But when converted to decimal values (shown in Figure 10 in green and red) the numbers may not seem so trivial. There could be a huge difference when telling a downstream device to set a value to 25 as opposed to 110. Think about this in terms of the spinning speed of some physical device. The implications at that point start to seem non-trivial.

Ehrenreich wrote an article called 'ICS cyber security is a role for experts', and that sentiment is spot on.[5] The examples in this document showcase the importance of domain expertise – ie, knowing how this equipment works, and more importantly knowing the safe range of operational values for specific gear. Moreover, the examples showcase the relevance of data in the spectrum of security protection and safety in the OT security space. So, the question here becomes: is knowing that these value set conditions can create high risk situations, enough? If you are aware of this level of risk, and yet some malicious Modbus value set traffic makes it to your VFD – the negative impact is significant.

```
00 0c 29 24 3a 0a 00 50  56 c0 00 08 08 00 45 00   ..)$:..P V.....E.
00 37 03 1d 40 00 80 06  fd cf c0 a8 3c 01 c0 a8   .7..@... ....<...
3c 82 c1 0f 4e 20 8d 96  dc ad 35 be d5 1b 50 18   <...N .. ..5...P.
01 00 c6 d2 00 00 05 64  08 c4 0a 00 01 00 fc 42   .......d .......B
c0 c0 0d 9c 86                                     .....
```

Figure 11: An example of DNP3 data.

Figure 12: The DNP3 data as parsed by Wireshark.

```
▼ Distributed Network Protocol 3.0
  ▼ Data Link Layer, Len: 8, From: 1, To: 10, DIR, PRM, Unconfirmed User Data
      Start Bytes: 0x0564
      Length: 8
    ▶ Control: 0xc4 (DIR, PRM, Unconfirmed User Data)
      Destination: 10
      Source: 1
      Data Link Header checksum: 0x42fc [correct]
      [Data Link Header Checksum Status: Good]
  ▶ Transport Control: 0xc0, Final, First(FIR, FIN, Sequence 0)
  ▶ Data Chunks
  ▶ [1 DNP 3.0 AL Fragment (2 bytes): #4(2)]
  ▼ Application Layer: (FIR, FIN, Sequence 0, Cold Restart)
    ▼ Application Control: 0xc0, First, Final(FIR, FIN, Sequence 0)
        1... .... = First: Set
        .1.. .... = Final: Set
        ..0. .... = Confirm: Not set
        ...0 .... = Unsolicited: Not set
        .... 0000 = Sequence: 0
      Function Code: Cold Restart (0x0d)

0000  00 0c 29 24 3a 0a 00 50  56 c0 00 08 08 00 45 00   ..)$:..P V.....E.
0010  00 37 03 1d 40 00 80 06  fd cf c0 a8 3c 01 c0 a8   .7..@... ....<...
0020  3c 82 c1 0f 4e 20 8d 96  dc ad 35 be d5 1b 50 18   <...N .. ..5...P.
0030  01 00 c6 d2 00 00 05 64  08 c4 0a 00 01 00 fc 42   .......d .......B
0040  c0 c0 0d 9c 86                                     .....
```

Actions on objectives

As the example objective here, an attacker is intent on service disruption so as to negatively impact the availability of resources. A denial of service (DoS) attack is the right fit. Chances are that an enterprise-level DoS attack (eg, SYN flood, ICMP flood, Teardrop, etc) will be detected and handled without major incident, given that over the years the defending side has learned good lessons on how to deal with these. But DoS attacks that are native to specific OT communications protocols are possible and a deep understanding of native communications is necessary to mitigate these.

"DoS attacks that are native to specific OT communications protocols are possible and a deep understanding of native communications is necessary to mitigate these"

For the sake of clearly understanding a DoS scenario we will switch our OT communications protocol to Distributed Network Protocol 3 (DNP3), which is typically used in the utilities sector (eg, electricity, water, etc). DNP3 is a TCP-based protocol that has three main layers (link, transport and application). The application layer is the relevant one for this example.

The magic bytes (identifying data) for DNP3 are 0x0564 and they are at the start of the link layer. The link layer takes up 10 bytes followed by 1 byte for the transport layer. Next comes the application layer and the function code on DNP3 network data can be found in the second byte of the DNP3 application layer. Figure 11 shows an example of this type of data with the function code 0x0d pointed out.

Figure 12 provides this data as parsed and displayed by Wireshark. Function 0x0d turns out to be a 'cold restart' command that will obviously have a physical effect on the receiving outstation in the field. This type of command

```
rule cold_restart : DNP3 {
    meta:
        description = "Detect client sending cold restart
        command"
    strings:
        $dnp3_id = {05 64}
        $cold_restart = {0d}
    condition:
        $dnp3_id at 0 and $cold_restart at 12
}
```

Listing 2: A simple YARA rule to detect a cold restart message.

should only be allowed from a trusted network entity (eg, source IP address, IP address from a trusted range, etc) because if an attacker were to send this there would most likely be an outage of some sort.

Listing 2 shows a simple YARA rule to detect this type of traffic on network flows.

Unglamorous environment

We have to accept the fact that OT Security is not a sexy, or hip, thing. There is no cool mobile app that the younger generations will fall in love with. There are grey screens with primary colours on them that run on versions of operating systems that are no longer supported. There are hot and dusty environments where PCs and PLCs reside. There are those humble, honourable, non-glamorous PLCs that endlessly churn away at their simple instruction sets and keep many aspects of our modern lives in order. The data these devices transfer across networks need to be understood in order to be properly protected. More importantly, the network communications, that contain these key elements of data (ie, set points, etc) that touch those PLCs need to be understood in order for protection to actually exist.

The need to deeply understand these environments and their subjective data sets is critical to protecting them. It is virtually impossible to accurately protect someone that one does not understand. We need to do our jobs and be proactive in terms of gaining this deeper data level understanding so that we can build proper protective mechanisms that can operate into the future. Moreover, we need to be proactive in putting proper protective mechanisms in place such that disasters can be avoided.

"We need to be proactive in terms of gaining this deeper data level understanding so that we can build proper protective mechanisms that can operate into the future. Moreover, we need to be proactive in putting proper protective mechanisms in place such that disasters can be avoided"

Modern day CISOs need to push for this type of deep data understanding now that the emerging pattern is that of OT security being part of their responsibility. Accepting a lack of data intimacy will lead to not being able to deploy native OT security active protection mechanisms. Then the CISO must either accept the risk of non-active OT security solutions or diligently put accurate and actively protecting solutions, which are subjectively data aware, in place. Otherwise there will always be this risk gap within their domains. One key factor to that risk is in the data itself. Inside these data sets native and subjective payloads of some OT protocol exist and these need to be understood. We cannot simply exist in the realm of network-related metadata (ie, source address, destination address, etc). Our industry has grossly overlooked the values in the data and the risk gap it has created in the OT security space.

About the author

Andres Andreu CISSP-ISSAP is a founding member and chief technology officer of Bayshore Networks (www.bayshorenetworks.com). He was chosen as the CISO/leader of the week by the Cyber Startup Observatory in February 2019. He is an industry veteran, author of 'Professional Pen Testing Web Applications', and has deep experience in the software engineering and cyber security spaces with a focus on where those two fields converge. Some of his FOSS work can be seen on Github.

References

1. Shahzad, Aamir; Lee, Malrey; Lee, Young-Keun; Kim, Suntae; Xiong, Naixue; Choi, Jae-Young; Cho, Younghwa. 'Real Time MODBUS Transmissions and Cryptography Security Designs and Enhancements of Protocol Sensitive Information'. Symmetry, 2015. Accessed Nov 2019. www.mdpi.com/2073-8994/7/3/1176/htm.
2. Cyber Startup Observatory, Infographics section. Accessed Nov 2019. https://cyberstartupobservatory.com/wp-content/uploads/2019/03/ATT&CK_for_Enterprise&Cyber_Kill_Chain_2.pdf.
3. 'MODBUS application protocol specification v1.1b'. The Modbus Organisation. Accessed Nov 2019. www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf.
4. Ehrenreich, Daniel. 'A step by step analysis of how your ICS is compromised through an externally generated cyber attack'. Cyber Startup Observatory, Aug 2018. Accessed Nov 2019. https://cyberstartupobservatory.com/step-by-step-compromising-your-ics-through-externally-generated-cyber attack/.
5. Ehrenreich, Daniel. 'ICS cyber security is a role for experts'. Cyber Startup Observatory, Jul 2019. Accessed Nov 2019. https://cyberstartupobservatory.com/ics-cyber security-is-a-role-for-experts/.

Securing workers beyond the perimeter


Scott Gordon

Scott Gordon, Pulse Secure

Although the delayed WeWork IPO has had a troubled journey, the growth of the start-up highlights the wider shift in the commercial real estate market as more organisations embrace new working practices. Globally, teleworking is expanding, with a recent survey suggesting that at least 70% of knowledge workers work at least one day a week out of the office.[1] However, for some organisations in areas such as financial services and the public sector, one of the objections against teleworking is security. The fear that remote workers are more vulnerable to cyber attack means that these sectors are remaining locked into the old office model.

Remote working as a concept has grown in lock step with the evolution in compute and networking communication. Organisations that were traditionally tied to mainframes and green-screen terminals of the 1980s then moved to client-server computing in the 1990s, making IP network connectivity the critical requirement for workers to access IT systems. The introduction of broadband in the early 2000s and the growth of cellular data networks freed workers from their fixed desks – while culturally, the benefits of part-time and flexitime working have matched up with the needs of working parents and scalable workforces.

Remote concerns

The perception of teleworking being less secure than desk-bound staff in a managed office is real. It's highlighted by a 2018 Apricorn survey of 100 businesses with over 1,000 employees that suggested that 95% of UK businesses were still struggling with remote working and security.[2] The survey found that a third of organisations claim to have experienced a data loss or breach as a direct result of mobile working. However, this needs to be put in context compared to the much larger 'Cyber Security Breaches Survey 2019' run by the UK Government's Department for Digital, Culture, Media & Sport (DCMS) which found that 61% of all large businesses had had an attack or breach.[3]

Part of the issue is squarely in the lap of organisations that have failed to evolve IT security to match the growth of teleworking. For example, the DCMS survey found that only one in four businesses had implemented removable media controls with policies to cover what can be stored on removable devices. And only 20% of firms had created a secure home and mobile working policy.

"A quarter of survey respondents had not implemented basic security precautions for remote workers such as installing anti-virus software, and 30% don't have any measures in place to restrict file access"

Security tools are also lacking, as highlighted by a survey commissioned by CybSafe that found that a quarter of survey respondents had not implemented basic security precautions for remote workers such as installing anti-virus software, and 30% don't have any measures in place to restrict file access.[4]

A wider challenge

Although self-reporting surveys are useful, there are more rigorous analyses such as the highly regarded Data Breach Investigations Report 2019 which has examined over 41,000 security incidents and around 2,000 breaches.[5] It does not separate out incidents where the root cause was linked specifically to remote working. However, the types of attacks and causes of breaches vary significantly between industry sectors and some inferences can be drawn. Industries with low levels of remote working such as manufacturing and public sector organisations do not show a major increase in breaches in comparison with sectors that have higher levels of remote working such as professional services.

What is clear – as stated by the report – is that "many breaches are a result of poor security hygiene and a lack of attention to detail," with the recommendation that organisations must "clean up human error where possible, then establish an asset and security baseline around Internet-facing assets like web servers and cloud services." This sensible advice must be applied equally and consistently across on-premise, part time and fully remote workers for the benefit to be realised.

Where to start?

The popularity of remote working is tied to the social, economic and productivity benefits that have been well researched and peer reviewed across several studies. Across almost every metric, there is substantive research suggesting benefits, along with real world examples such as an insurance giant that switched to more remote working, reducing its office space by 2.7 million square feet with a sav-

ing of $78m.[6] Or there's the Stanford University report that found job attrition rates fell by over 50% when staff were given more flexibility.

But answering the question of whether remote staff are a security risk must start with quantitative data. This means auditing processes to find out how different types of workers carry out tasks within and outside of the office environment. This process is driven by both HR and IT with the aim of understanding how workers carry out tasks that may encompass IT – but not always. For example, are staff copying data from fileservers to work on reports while at home? If so, is that data copied via USB devices or is it shared via a service such as Dropbox – that the IT department may not even be aware of?

"Are staff copying data from fileservers to work on reports while at home? If so, is that data copied via USB devices or is it shared via a service such as Dropbox – that the IT department may not even be aware of?"

Audit processes should also focus on devices. Are staff accessing sensitive corporate systems from personal mobile devices? And if so, are these devices secure and free from malware that maybe be intercepting login credentials? Although IT departments can gain an understanding of what applications are being accessed by whom and through which device through examination of IP traffic and application logs – unless line of business managers are involved in the processes, there is a danger that entire 'shadow IT' platforms that are handling sensitive data or providing ingress into the corporate systems may be missed within any audit processes. Shadow IT security issues should not be underestimated, as highlighted by a recent survey from IBM that one out of three employees at Fortune 1000 companies regularly use cloud-based software-as-a-service (SaaS) apps that haven't been explicitly approved by internal IT departments.[7,8]

A successful audit, even in its most basic form, should be able to list all the applications in use by an organisation, who has access to these systems and how access is secured. It is also worth considering APIs that connect systems together. These may only be directly relevant to developers but could pose a systemic security risk that has been masked from the security team due to the lack of widespread usage.

Security everywhere

The audit may well show a clean bill of health all around, with office-based staff and teleworkers all using the same apps, same devices, same secure access methods and little in the way of divergence to warrant any remediation action. A more likely result is that remote workers that have been added organically over time will probably have slightly different app access paths and, in the worst case, will be doing things slightly differently to overcome security controls to get the job done. One of the most common examples is copying files and taking them offsite to write reports or prepare presentations.

"A better approach is to go with the tide and create a secured version of the tools that workers need to access remotely. In this case, IT-authorised collaboration and file-sharing tools that use encryption are a must"

IT and HR departments can respond in several ways. One method is policy-based through reiteration of IT security policy, along with technical methods to stop workers circumventing controls such as disabling USB ports and file copying from secure stores. Although valid, this may lead to rogue employees, some quite technical, finding more elaborate ways to get around the IT security policy without being noticed.

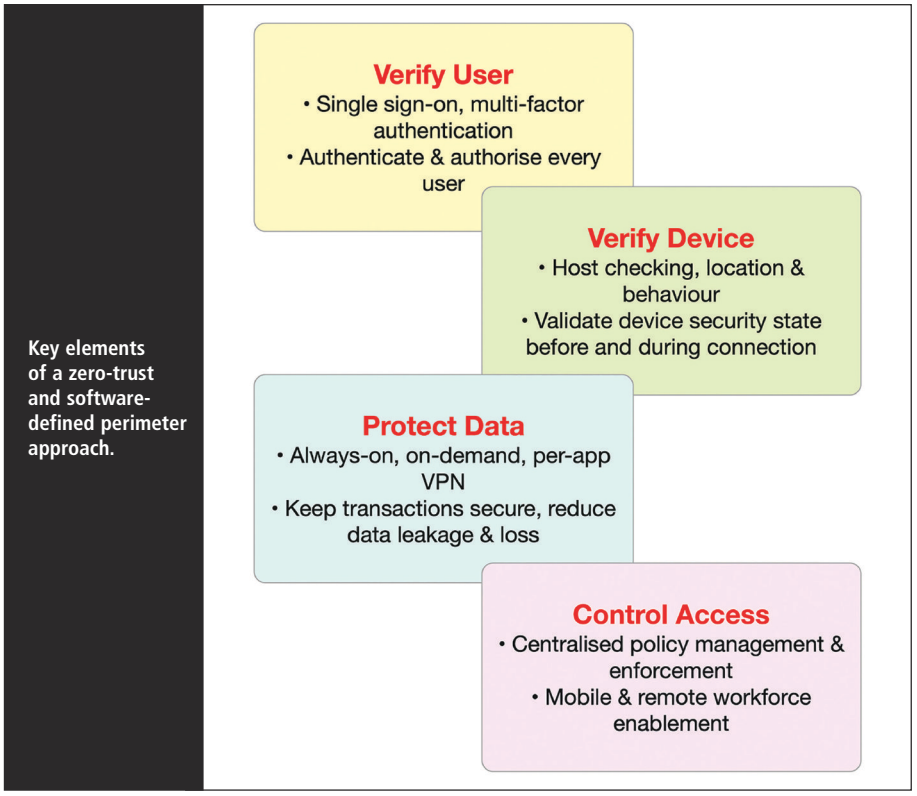
A better approach is to go with the tide and create a secured version of the tools that workers need to access remotely. In this case, IT-authorised collaboration and file-sharing tools that use encryption are a must. Enterprise mobility management that is centrally managed to secure devices with kill switches if devices are lost or stolen can overcome many holes in bring your own device (BYOD) security.

"Many of the elements needed to move to a zero-trust position, such as VPNs, directory services and application firewalls, are already used within an organisation – but often configured as a perimeter defence instead of an end-to-end secure architecture"

However, one of the biggest challenges is that organisations' IT security infrastructures are often designed based around a secure perimeter with applications within the core. Yet, the modern working world is increasingly moving to a hybrid model where key applications such as Microsoft Office are now delivered from the cloud. Although a highly popular platform, breaking into an Office 365 account of a senior executive is a treasure trove for a would-be attacker.

Think hybrid protection

By design, Office 365 and other SaaS applications are accessible from anywhere with an Internet connection, which makes them incredibly popular with teleworkers. However, organisations must start to think about moving security to a zero-trust IT security model that requires strict identity verification for every person and device trying to access resources on a private network or SaaS resource, regardless of whether they are sitting within or outside of the network perimeter. In this model, every user, irrespective of location, must be verified along with connectivity through a secure VPN or HTTPS tunnel maintained for each session.



Key elements of a zero-trust and software-defined perimeter approach.

This may sound draconian but the benefits are significant in terms of simplifying and unifying secure access across every user and application – and many of the elements needed to move to a zero-trust position, such as VPNs, directory services and application firewalls, are already used within an organisation – but often configured as a perimeter defence instead of an end-to-end secure architecture.

Moving to a zero-trust approach will not instantly stop poor security hygiene such as weak passwords, lack of multi-factor authentication and overly generous privileged access. But, once implemented, IT departments will have much clearer visibility of the exceptions and a way of allowing these less common access requirements through policy-based controls rather than ad hoc workarounds.

And finally

Securing the remote workforce is not a one-shot deal and instead should be considered a moving target. This requires IT or security teams within the organisation to conduct regular audit refreshes, instigate regular IT security policy training sessions and maintain dialogue with department heads and bellwether users to find out if the day-to-day requirements are changing. This must be within the context of maintaining best-practice IT security processes. This feedback loop is vital to ensure that, as teleworking grows, the IT infrastructure is designed with scale in mind and that as new systems and apps emerge, they are rolled out with the assumption that remote users are the norm and not the exception to the rule.

About the author

Scott Gordon CISSP, CMO of Pulse Secure (www.pulsesecure.net), possesses over 20 years' experience contributing to security management, network, endpoint and data security, and risk assessment technologies at innovative start-ups and large organisations across SaaS, hardware and enterprise software platforms. Previously, Gordon was CMO at RiskIQ and ForeScout. He has also held executive and management roles at AccelOps (acquired by Fortinet), Protego (acquired by Cisco), Axent (acquired by Symantec) and McAfee.

References

1. Browne, Ryan. '70% of people globally work remotely at least once a week, study says'. Make It, 30 May 2018. Accessed Jan 2020. www.cnbc.com/2018/05/30/70-percent-of-people-globally-work-remotely-at-least-once-a-week-iwg-study.html.
2. 'Ninety-five% of UK businesses still struggling with mobile working and security of data continues to cause concern'. Apricorn, 5 Jun 2018. Accessed Jan 2020. www.apricorn.com/press/ninety-five-percent-of-uk-businesses-still-struggling-with-mobile-working-and-security-of-data-continues-to-cause-concern.
3. 'Cyber Security Breaches Survey 2019'. UK Department for Digital, Culture, Media & Sport, UK Government, 3 Apr 2019. Accessed Jan 2020. www.gov.uk/government/statistics/cyber security-breaches-survey-2019.
4. Jones, Connor. 'A third of cyber attacks exploit unsecure remote working'. ITPro, 20 Dec 2018. Accessed Jan 2020. www.itpro.co.uk/security/32617/a-third-of-cyber attacks-exploit-unsecure-remote-working.
5. 'Data Breach Investigations Report 2019'. Verizon. Accessed Jan 2020. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf.
6. Ray, Sanjana. 'The three economic benefits of working from home'. YourStory, 28 Apr 2017. Accessed Jan 2020. https://yourstory.com/2017/04/economic-benefits-remote-working.
7. French, Jordan. 'Why shadow IT is the next looming cyber security threat'. Podium, 25 Apr 2019. Accessed Jan 2020. https://thenextweb.com/podium/2019/04/25/why-shadow-it-is-the-next-looming-cyber security-threat/.
8. Hernandez, Hector. 'Bring shadow IT into the light: Discover, assess, approve and educate'. IBM, 30 Aug 2017. Accessed Jan 2020. www.ibm.com/information-technology/bring-shadow-it-light-discover-assess-approve-and-educate-0.

Targeted cyber attacks: how to mitigate the increasing risk

Guy Bunker

Dr Guy Bunker, Clearswift

In the past year, it has felt as if cyber security breaches have rarely been out of the press, with more and more reports of organisations and individuals becoming victims of targeted attacks. Sainsbury's, Uber and Argos are just three examples of companies out of more than 100 who fell victim to this summer's Capital One breach.[1] This high-profile hack has led to a potential fine of $500m for the financial giant and the hacker in question has been charged with five years' imprisonment and over £200,000 in fines.

The combination of prominent names and huge numbers in this hack demonstrates the severity of cyber attacks in the current climate. It also acts as a well-publicised, stark reminder to businesses of all sizes that they need to invest in order to mitigate against the changing landscape of cyberthreats. Before this can be achieved, however, it's important for businesses to fully understand the origin of some of the newer threats.

Cloud services

Progressively, firms are beginning to understand the risks associated with cloud-based storage such as SharePoint and Google and file-sharing applications such as OneDrive and Dropbox. Just because a link comes from a big brand name, it doesn't necessarily mean it comes from a trustworthy source and it is becoming increasingly common for weaponised documents to be shared via links this way. Once the link is clicked and the malware is inside a system, it can transform itself and be used to download new payloads using steganography to receive its instructions from anywhere that hosts innocuous-looking images.

A lack of understanding of the potential threats creates unnecessary risk for businesses securing data in the cloud. Even if an organisation isn't targeted directly, to avoid being caught up as collateral damage in a wider cloud provider breach, organisations need a defence-in-depth strategy around all the information that is shared and accessed on the platform. Good security procedures should also be applied: this includes regularly patching servers and operating systems as well as watching for anomalous behaviour on the network. Trust should no longer be taken for granted.

Emerging technologies

Unfortunately, it is no longer the case of 'if' you will fall victim to a cyber breach, but 'when'. Recently, it was revealed that 70% of financial companies have experienced a cyber security incident in the past year, highlighting the extent of the threat.[2] Flipping this statistic on its head, it's a positive step that those financial companies are aware they've been victim of an attack.

"Even if an organisation isn't targeted directly, to avoid being caught up as collateral damage of a wider cloud provider breach, organisations need a defence-in-depth strategy"

Being aware of the different threat vectors in our fast-paced technology environment is a step in the right direction Being able to mitigate against them all is another challenge altogether. The technology we adopt in our everyday lives is constantly evolving and this puts responsibility on companies and their employees to keep up with the risks posed to cyber security.

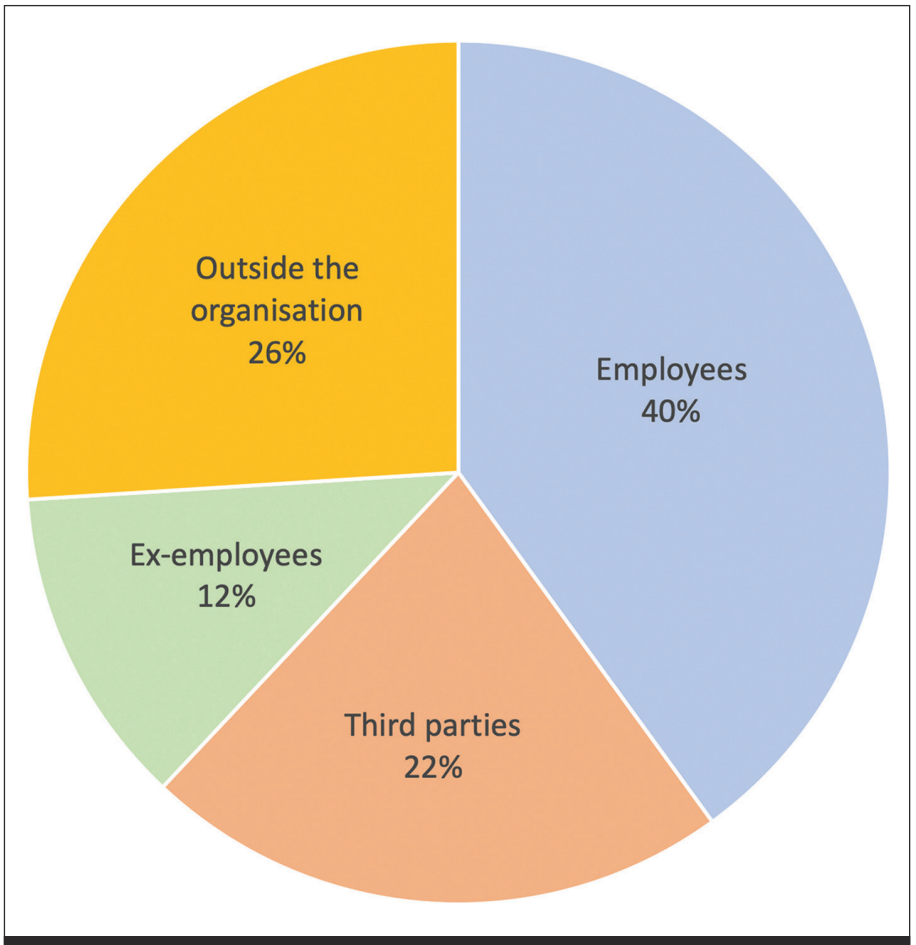
Hackers found a way around anti-virus and anti-spam filters, so it must be expected that they will find ways around any new tech that emerges and the way to exploit it to their own ends. The key is to try to stay ahead of this curve as much as possible and invest in technology that can protect against the ever-changing environment.

People and education

Central to a cyber security strategy in an organisation of any size is threat mitigation and education. Precautions such as monitoring activity are crucial in ensuring that no sensitive information or hidden metadata is exposed to the wrong people. People are often the root cause of the problem and this is evidenced by that fact that nearly half of cyber security incidents over the past 12 months were caused by internal errors such as employees failing to follow security protocols or data protection policies.[3]

The problem is, it's easy to do. A simple lapse in concentration and confidential data is sent to 'the wrong Dave.' With human error accounting for such a large proportion of data breaches, investment in technology to protect against this is vital.

However, technology on its own is not enough to mitigate today's cyber risks. Implemented technology should only be seen as a safety net in protecting businesses



The source of security threats in a 12-month period among organisations that experienced a security breach. Source: Clearswift.

from threats. In the long term, businesses must go above and beyond to prioritise the education of their employees.

Processes

Employees must understand how to carry out routine processes without putting sensitive information at risk. To this end, a proportion of the cyber security budget must go towards ensuring employees' knowledge of data-handling processes.

Discussing security with employees is an effective way to understand where the weaknesses are, as well as which processes are side-stepped and therefore need overhauling. Business email compromise (BEC) is so successful because people follow processes that need to be updated to mitigate the risk. Of course, data and the threats against it change every day. As a result, processes need to keep up with changing complexities and vulnerabilities too.

Businesses must adopt a versatile approach to cyber security training to enable them to spot vulnerabilities that are harder to anticipate and minimise them with the correct measures. An evolving company culture around cyber security needs to be holistic and collaborative. Education and awareness training must be ongoing to ensure that all employees, from the CEO to the cleaner, understand the risks and, more importantly, what to do if they suspect an issue.

Third-party threats

While technology is the last line of defence, ensuring that policies are enforced and therefore protecting the people, it is still crucial in any cyber protection strategy. To this end, a proportion of the cyber security budget must go towards ensuring that technology is up to date and new rings of security are put in place.

Ultimately, firms must take responsibility not only for the security of their own systems within the network, but also for the partnerships and third parties with which they collaborate. There are two strands of thinking when it comes to the source of cyber risk for large organisations, both equally valid: one is that, while most people perceive cyberthreats as predominantly coming into the organisation from external sources, the majority of incidents in fact occur within (as outlined in the 'Insider Threat' index).[4] On the other hand, an approach that's too internally focused can neglect the threat from third-party partners and applications.

"Very often the difference between business as usual and considerable jeopardy is down to a lack of foresight in deciding what data is shared with third parties and how"

The phrase that your security is 'only as strong as your weakest link' applies in either case. Cyber criminals have often been known to target smaller, connected organisations as an easier route into the firm that they are in fact aiming to infiltrate. Even apps, downloaded onto smartphones, can create risk that slips under IT and security teams' radars. For instance, an innocuous-seeming application may bring with it unnoticed permissions that function in the background, backing up data into the cloud or granting attackers access to an alternative route into a firm's systems and network.

Conclusion

Major data breaches usually bring attention to a lack of ownership and accountability of information within an organisation. Cyber security is a shared responsibility – there is no place for unconstructive finger-pointing in an environment where customer confidence in the security of their data is at an all-time low.

What is clear is that businesses of all shapes and sizes need to accept responsibility for the cyber security of their business and those in their

information supply chain. Yes, a great proportion of incidents occur due to employee error, but with a comprehensive security strategy in place, these incidents will reduce.

Investing in technology is a crucial step in any security strategy, but education and appropriate processes are equally important. The goal should be to create a company culture where every employee is on the same page when it comes to best practices around protecting information as well as appropriate policies and procedures.

Finally, companies making important decisions around project collaborations with third parties or the use of unvetted external applications should take a more cautious approach in evaluating the potential risks involved in their decisions. Very often the difference between business as usual and considerable jeopardy is down to a lack of foresight in deciding what data is shared with third parties and how.

All in all, taking a cautious, responsible and long-term approach to cyber security, combined with an appreciation for investment in technology and emphasis on firm-wide education is the most sustainable way to keep up with today's evolving cyber threatscape.

About the author

Dr Guy Bunker is CTO at cyber security company Clearswift. He is an internationally renowned IT expert with 25 years' experience in information security and IT management. Bunker is a frequently invited speaker at conferences, including RSA, EuroCloud and InfoSecurity and is a board advisor for several small technology businesses. He has published books on utility computing, back-up and data loss prevention and also holds a number of US patents. He is a Chartered Engineer with the IET.

References

1. 'Capital One Data Breach: A reminder to lock your back door'. Clearswift, 13 Aug 2019. Accessed Jan 2020. www.clearswift.com/blog/2019/08/13/capital-one-data-breach-reminder-lock-your-back-door.
2. '70% of Financial Companies Suffered a Cyber security Incident in the Past 12 Months'. Dark Reading, 15 Aug 2019. Accessed Jan 2020. www.darkreading.com/attacks-breaches/70 – of-financial-companies-suffered-a-cyber security-incident-in-the-past-12-months/d/d-id/1335541.
3. Gopalakrishnan, Chandu. '70% of UK financial companies report being hit by cyber-incidents; most blame internal error'. SC Media, 15 Aug 2019. Accessed Jan 2020. www.scmagazineuk.com/70-uk-financial-companies-report-hit-cyber-incidents-blame-internal-error/article/1594018.
4. 'Clearswift Insider Threat Index (CITI)'. Clearswift. Accessed Jan 2020. http://pages.clearswift.com/rs/591-QHZ-135/images/Clearswift_Insider_Threat_Index_2015_US.pdf.

...News continued from page 3

Benham, director of public affairs for US Fleet Cyber Command told USA Today. However, the Navy declined to go into details about what it sees as the risk.

The US Army has also banned the app, although it had previously used it for recruiting. Department of Defense guidance sent out to a large number of military personnel said: "Be wary of applications you download, monitor your phones for unusual and unsolicited texts etc., and delete them immediately and uninstall TikTok to circumvent any exposure of personal information."

Meanwhile, Check Point has released research that found a number of flaws in the app. These include: the ability to take partial control over other users' accounts, including the ability to delete and upload videos and make hidden videos public; spoofing SMS messages to users as though they are coming from TikTok; and obtaining users' personal information. Check Point alerted ByteDance to the problems and an update has been pushed out. There's more information here: http://bit.ly/2NmKU7b.

"While TikTok was able to patch the issues identified by Check Point Research, during investigation of the issue the attack path would have been investigated," commented Tim Mackey, principal security strategist at the Synopsys Cybersecurity Research Centre. "Developers performing this research would likely have identified not only the specific attack method, but could likely have discovered additional potential areas for user data to become compromised. This investigative process is common when faced with any security issue, but in addition to the patch the development team should have updated their threat models and performed a more thorough review of the security of their application."

The Committee on Foreign Investment in the US is now reviewing TikTok's purchase by ByteDance from its US creators, which occurred two years ago. This follows concerns expressed by two congressmen back in October that the platform could be abused for mounting foreign influence campaigns.

The Firewall

The power of voice

Colin Tankard, Digital Pathways

We are always being told that the passwords we create are far too simple and that they should be complex. However, complexity means that they become harder to remember. Consequently, people write them down or use an online password manager, which is not always easily accessible.

Another recommendation is to use two-factor authentication, 'the something you know plus the something you have'. Many of these are free and can operate from your smartphone. But have you ever tried to move your authentication to a new phone? Even with the old phone to hand it is hard, let alone trying to do it when your phone is dead or stolen! This is a 'put you off ever doing it again' procedure.

Biometrics were seen as the way ahead, but some devices just can't support the options, even if they have some form of biometric capability. They have never been very reliable, having a high degree of false/positive allowance.

Then there is the challenge of the different ways we connect – not everything is accessed by a PC. There are dial-in systems, mobile apps, gaming consoles and multiple OS platforms, which might not support your chosen authentication method.

The identifiers we do all carry are our brains and voices. With voice recognition widely adopted in most devices, our voice could be the key to secure access. Until recently voice recognition has been either in the 'command and control' space, where you give short, clear instructions and the service goes off to find the answers that match as closely as possible – Alexa, Siri and others fall into this category – or, the 'educate me' platforms, where you spend hours teaching the system how you speak, adding any complex words you use. These systems frequently are industry-specific, but you also find it in Word and other such applications.

Neither of these processes is ideal for complex speech, as they either take too long to train or are greatly affected by the clarity of speech, so struggle with heavy accents or background noise. The new form of speech recognition, Advanced Speech Recognition (ASR), is looking to address these issues and might be the breakthrough we have been looking for in user authentication.

In recent studies, quoted figures measure the proportion of words spoken that the ASR system correctly identified, measured against a ground-truth manual reference created by an external transcription agency. As a baseline comparison, a state-of-the-art research model from Edinburgh University, trained on 1,600 hours of TV broadcasts, scored 57.7% words correct on the five-hour test set. In security terms, at 58% the false/positive factor is still too high but if we could get that to 92% (given that humans only hear and understand 95% of what is said), then we can link our voice to a complex phrase, or personal information we select at random, to speak into our phone or through a microphone, which can accurately identify us.

There are systems now in the market from Auris Tech and Nuance, that are reaching these levels of accuracy, can handle complex speech and are not affected by accents or background noise.

With ASR, there is no forgetting passwords or needing a smartphone, it works on any platform, so no more vendor lock-in! It is also simple for anyone to use, which can't be said for some authentication methods, especially if you are elderly or visually impaired.

To talk easily to a system and be authenticated on a topic of your choice is a game-changer. I guess the only snag is if you have laryngitis!

EVENTS CALENDAR

4–5 February 2020
PrivSec
London, UK
https://london.privsec.info

14–15 February 2020
Offensive Security
Berlin, Germany
www.offensivecon.org

24–28 February 2020
RSA Conference USA
San Francisco, US
www.rsaconference.com

16–20 March 2020
Troopers
Heidelberg, Germany
https://troopers.de

16–18 March 2020
ACM Conference on Data and Application Security and Privacy
New Orleans, LA, US
www.codaspy.org

17–18 March 2020
Cybersecurity & Cloud Expo Global
London, UK
www.cybersecuritycloudexpo.com

30 March – 1 April 2020
InfoSec World
Florida, US
www.infosecworldusa.com

7–8 April 2020
Global Privacy Summit
Washington DC, US
http://bit.ly/2nLBsAy

5–8 May 2020
RuhrSec
Bochum, Germany
www.ruhrsec.de