ELSEVIER

network SECURITY

ISSN 1353-4858 October 2020

www.networksecuritynewsletter.com

Featured in this issue:
Exploitable hosts used in cloud native cyber attacks

Can an in-depth analysis of elements from cyber attack campaigns teach us something new? The answer is yes.

Based on data from a honeypot, Assaf Morag of Aqua Security examines the mechanisms used to automatically infect a host with crypto-miners and then seek out new vulnerable hosts and infect them as well. He also analyses the IPs of the victims. The conclusions reveal an increasing number of vulnerable IPs and ever-greater sophistication by attackers.

Full story on page 6…

How threat actors abuse ICS-specific file types

Project files are integral to industrial control system (ICS) solutions, providing the data and instructions each machine on the operational technology (OT) network needs to operate.

While engineers will use them to ensure the smooth running of operations, security teams can use these files to gather an accurate picture of what machines are running, along with other critical data, such as where they are and what they are supposed to be doing. However, extracting information from ICS engineering project files is not always straightforward, and a lack of full visibility into what is running on the network and how it normally functions presents a significant security risk, explains Nadav Erez at Claroty.

Full story on page 10…

How organisations can ethically negotiate ransomware payments

Ransomware figures have been skyrocketing since 2017 when the globe was hit by WannaCry and NotPetya.

The onus lies on business leaders to make the ultimate decision – to pay or not to pay. Many leaders will take the high ground because they don't want to be seen negotiating with criminals. Yet other organisations have no option but to pay if they are to survive. Tom Hofmann of Flashpoint negotiates a way through this ethical minefield.

Full story on page 13…

Zerologon flaw exploited in the wild

The Zerologon vulnerability in Microsoft Server (CVE-2020-1472) is being increasingly targeted by both nation-state actors and cyber criminals due to a lack of patching.

The flaw revolves around the Netlogon Remote Protocol (MS-NRPC) process, which uses RPC communications with a domain controller to authenticate a user during login. Tom Tervoort at Secura found it was possible to force RPC to drop encryption, due to a flaw in the Netlogon AES-CFB8 cryptographic negotiation algorithm, by using multiple spoof login attempts. After an average of 256 attempts,

Continued on page 2...

Contents

NEWS

Zerologon flaw exploited in the wild 1

DDoS attacks hit hard and fast 2

Enterprise IoT at risk 3

FEATURES

Exploitable hosts used in cloud native cyber attacks 6

Using data from a honeypot, Assaf Morag of Aqua Security examines the mechanisms used to automatically infect a host with crypto-miners and then seek out new vulnerable hosts and infect them as well. He also analyses the IPs of the victims and finds an increasing number of vulnerable IPs and ever-greater sophistication by attackers.

How threat actors abuse ICS-specific file types 10

Project files are integral to industrial control system (ICS) solutions, providing the data and instructions each machine on the operational technology (OT) network needs to operate. Security teams can use these files to gather an accurate picture of what machines are running, along with other critical data, such as where they are and what they are supposed to be doing. However, extracting information from ICS engineering project files is not always straightforward, and a lack of full visibility into what is running on the network and how it normally functions presents a significant security risk, explains Nadav Erez at Claroty.

How organisations can ethically negotiate ransomware payments 13

When an organisation is hit by ransomware, the onus is on business leaders to make the ultimate decision – to pay or not to pay. And this raises a serious dilemma. Many leaders will take the high ground because they don't want to be seen negotiating with criminals. Yet other organisations have no option but to pay if they are to survive. Tom Hofmann of Flashpoint negotiates a way through this ethical minefield.

Data highway and the digital transformation: arguments for secure, centralised log management 17

Digital transformation has been forced, abruptly, on many organisations as a result of the Covid-19 pandemic. Almost overnight, companies found themselves having to adapt to a completely new mode of working. But one thing has remained constant – logs. If digital transformations are to be successful and secure, effective log management is crucial, says Robert Meyers of One Identity.

ThreatWatch 3

Report Analysis 4

News in brief 5

The Firewall 20

Events 20

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: smd@contrarisk.com

Columnists: Andrew Cooke, Airbus Security; Karen Renaud; Dave Spence, Context Information Security; Colin Tankard, Digital Pathways

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

an attacker could login as a domain administrator with any fake credentials. That would allow them to change user passwords and run any code. No genuine credentials are needed at any time.

After it was rated as a 10/10 critical vulnerability, Microsoft issued a patch in August 2020 and Secure followed up with a detailed report in September, available here: https://bit.ly/34EmxK7. A number of proof-of-concept exploits soon emerged, posted to GitHub, but so did genuine attacks from a variety of threat actors.

This prompted the US Cyber security and Infrastructure Security Agency (CISA), part of the Department of Homeland Defence, to issue a rare Emergency Directive (available here: https://bit.ly/2SFfqeS) requiring all federal organisations to implement mitigation procedures within a week.

The agency added: "This attack has huge impact. It basically allows any attacker on the local network (such as a malicious insider or someone who simply plugged a device into an on-premise network port) to completely compromise the Windows domain."

Towards the end of September, Microsoft issued a series of tweets, including: "Microsoft is actively tracking threat actor activity using exploits for the CVE-2020-1472 Netlogon EoP vulnerability, dubbed Zerologon. We have observed attacks where public exploits have been incorporated into attacker playbooks."

Attackers were using .NET executables, the most common having the name 'SharpZeroLogon.exe'. Microsoft again urged administrators to patch their systems.

"Given the large availability of working proof of concepts (PoCs), and overall impact from exploitation, it's unsurprising that known groups are looking to take advantage of this Netlogon vulnerability," said Rody Quinlan, security response manager at Tenable. Exploitation, if successful, allows the complete takeover of the Windows domain – that's the virtual equivalent of the keys to the kingdom. A quick search on GitHub reveals that there are currently at least 40 repositories containing PoC code relating to this flaw. There are also working exploit scripts that defenders and attackers alike can utilise to exploit this vulnerability.

Among the attackers exploiting the vulnerability is the cybercrime group TA505 (aka Chimborazo), which is known for a whole range of criminal activities, most recently the spread of ransomware. According to Microsoft, the group has implemented a version of the Mimikatz post-exploitation tool that includes exploit code for Zerologon.

Microsoft also warned that the advanced persistent threat (APT) group that it tracks as Mercury (aka MuddyWater, Static Kitten and Seedworm) has been engaged in active campaigns exploiting Zerologon over the course of weeks. The APT group is associated with the Iranian Government and is known primarily for attacks against targets in the Middle East and Asia, especially those operating in the telecommunications, government (IT services) and petrochemical sectors.

Microsoft's patches came in two phases. The first addressed the security flaw in Active Directory domains and trusts, as well as Windows-based devices. However, administrators also need to take manual steps themselves – simply implementing the patch is not enough.

However, it's not only Windows systems that are affected. The Samba file-sharing solution makes use of the Netlogon protocol when it is used as a domain controller, and so was also affected. Samba and 0patch issued patches to address the problem.

Microsoft has also issued new guidance (http://bit.ly/nw-zerologon) on how to mitigate the problem, clearing up a lot of confusion around the process.

DDoS attacks hit hard and fast

According to the latest threat intelligence report from Netscout, criminals mounting distributed denial of service (DDoS) attacks have changed tactics.

They are now employing complex, high-throughput attacks designed to over-

Threatwatch

Interplanetary Storm

A new variant of the InterPlanetary Storm malware has infected roughly 13,500 machines across 84 different countries, according to Barracuda Networks in its September Threat Spotlight research. The original InterPlanetary Storm malware was first seen in May 2019 and attacked Windows machines. The new variant, first detected in late August, is now also targeting Internet of Things (IoT) devices, such as Android-based smart TVs and Linux-based devices such as routers. The malware gains access to machines by running a dictionary attack against the SSH server, similar to FritzFrog, another peer-to-peer (p2p) malware. It can also gain entry by accessing open ADB (Android Debug Bridge) servers. The malware detects the CPU architecture and running OS of its victims, and it can run on ARM-based machines, an architecture that is quite common with routers and other IoT devices. The purpose of the malware is not known yet, but it's likely that campaign operators will be able to gain access to infected devices so they can later be used for crypto-mining, distributed denial of service (DDoS) or other large-scale attacks.

Router bypass

The Synopsys Cybersecurity Research Centre has released details of authentication bypass vulnerabilities in wireless router chipsets used in products by Mediatek, Qualcomm and Realtek. The vulnerabilities (CVE-2019-18989, CVE-2019-18990 and CVE-2019-18991) refer to a partial authentication bypass flaw that allows an attacker to inject packets into a WPA2-protected network without knowledge of the preshared key. Upon injection, these packets are routed through the network as would be valid packets, and responses to the injected packets return encrypted. However, since attackers can control what is sent through the network, they can eventually ascertain if the injected packets successfully reached an active system. As a proof-of-concept, Synopsys researchers were able to open a UDP port in the router's NAT by injecting UDP packets into a vulnerable WPA2-protected network. The packets route through the public Internet and are eventually received by an attacker-controlled host listening on a defined UDP port. After receiving this response, the attacker-controlled host can use this opened UDP port to communicate back to the vulnerable network. There's more information here: https://bit.ly/2GOavWg.

Black-T

According to Palo Alto Networks, the TeamTNT group, best known for infecting Amazon Web Services (AWS) instances in order to mine Monero crypto-currency, has added some new capabilities with its latest malware, dubbed Black-T. The new features include network scanning, targeting and shutting down rival crypto-mining tools that might be running on the network (particularly Kinsing, Kswapd0, ntpd miner, redis-back-up miner, auditd miner, Migration miner, the Crux worm and Crux worm miner), and password scraping. There's more information here: https://bit.ly/30QG88J.

Tenda router botnet

Tenda routers, which are popular with home and small office users, have two vulnerabilities that are being exploited to create a Mirai-like botnet. One vulnerability (CVE-2018-14558) has been targeted since November 2019, although it wasn't disclosed until July 2020. There's a firmware update to patch it, but how widely this has been applied isn't certain. Another vulnerability (CVE-2020-10987) was also disclosed in July. Both flaws rate 9.8 out of 10 on the CvSS vulnerability-severity scale. The Ttint botnet that is exploiting them is not only being employed to mount distributed denial of service (DDoS) attacks, but also has remote access trojan (RAT) and spyware capabilities. Researchers at 360Netlab said that one of the key RAT functions is the command to bind a specific port issued by a command and control server to enable Socket5 proxy service, which allows attackers to remotely access the router's intranet and reach out across the network. There's more information here: https://bit.ly/3dbGPhO.

whelm and quickly take down targets. And they are focusing on organisations playing critical roles in the Covid-19 pandemic, such as healthcare, e-commerce and educational services.

"The first half of 2020 witnessed a radical change in DDoS attack methodology to shorter, faster, harder-hitting, complex multi-vector attacks that we expect to continue," said Richard Hummel, threat intelligence lead at Netscout. Among the findings of the Netscout '1H 2020 Threat Intelligence Report' are that cyber criminals set new records for attacks on online platforms and services during the pandemic. More than 929,000 DDoS attacks occurred in May, representing the single largest number of attacks ever seen in a month. Some 4.83 million DDoS attacks occurred in the first half of 2020, a 15% increase. However, DDoS attack frequency jumped 25% during peak pandemic lockdown months (March through June).

In addition, bad actors focused on shorter, more complex attacks. Super-sized, 15-plus vector attacks increased 2,851% since 2017, while the average attack duration dropped 51% from the same period last year. Moreover, single-vector attacks fell 43% while attack throughput increased 31%, topping out at 407Mpps. The increase in attack complexity and speed, coupled with the decrease in duration, gives security teams less time to defend their organisations from increasingly sophisticated attacks.

The report is available here: https://bit.ly/3iHIHQv.

Enterprise IoT at risk

New research by Palo Alto Networks paints a stark picture of the vulnerability of Internet of Things (IoT) devices and their potential impact on enterprise networks.

Devices including such diverse products as smart teddy bears, implanted heart monitors, connected cars and other connected devices are regularly connecting to corporate networks, which could open up significant vulnerabilities.

A survey by Palo Alto found that many organisations are seeing a rise in the number of IoT devices connecting to their networks, including connected trash cans, light bulbs and hand sanitiser stations. Some 41% of respondents said they need to make a lot of improvements to the way they approach IoT security and 17% said that a complete overhaul is needed.

Nearly a quarter of organisations with at least 1,000 employees reported that they have not segmented IoT devices onto separate networks – a fundamental practice for building safe, smart networks. Only 21% reported following best practices of using micro-segmentation to contain IoT devices in their own tightly controlled security zones.

Business Insider Intelligence forecasts there will be more than 41 billion IoT devices by 2027.

The report is here: https://bit.ly/33KJsUO.

Report Analysis

Microsoft Digital Defense Report

It can't have escaped your notice that technology develops rapidly, and the same applies to the ways people use it. In most cases this is a good thing: but, unfortunately, the same principles apply to those who use technology for malicious ends.

The key message of Microsoft's annual report is that cyber criminals – especially those that operate in organised gangs or on behalf of national governments – are becoming increasingly sophisticated. Malware is ever more intricate and smarter at evading automated defences. Cyber criminals are making extensive use of cloud services as a way of obfuscating their origins. And while information security technologies and practices are evolving too, it's a moot point as to whether they are keeping up with the ability of threat actors to change tactics and search for new weak points in our constantly morphing technology landscape.

In any case, it's not just a matter of technology. In 2019, Microsoft said it blocked more than 13 billion malicious and suspicious emails. More than a billion of these contained URLs created purely for phishing-based credential theft. What's significant here is that phishing is not a sophisticated form of attack. Fundamentally, it requires the ability to send emails and build a legitimate-looking web page (which, if it's mimicking a real site, such as bank login, can use assets like graphics stolen from the real thing). Sending out mass phishing emails does require the services of a botnet, which takes technical skills to establish. But a criminal can just rent a botnet on the dark web now.

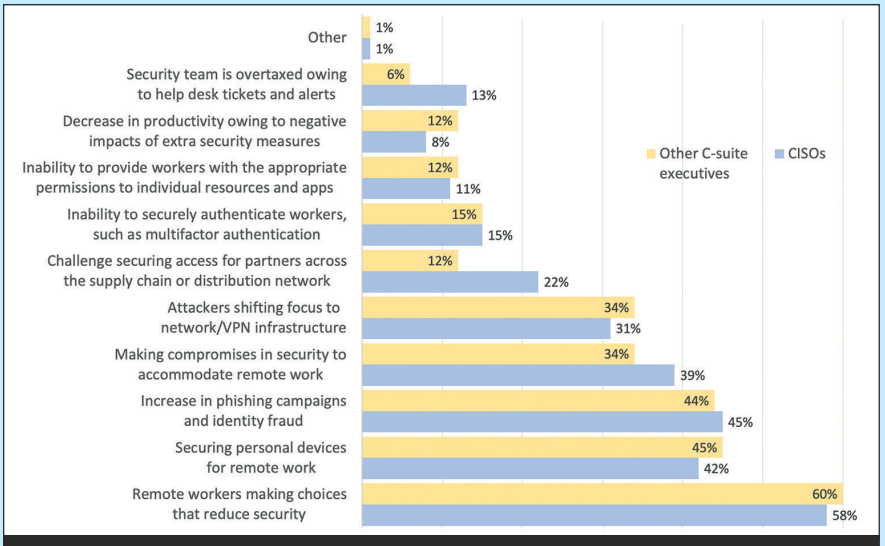
Microsoft also notes that, since October 2019, the majority of its incident response engagements have been concerned with ransomware. Again, writing ransomware code can take skill – indeed, some ransomware displays high levels of coding talent – but if that's the business you choose, then both the malware and the botnets to distribute it are available for rent.

This hints at where the key developments lie in the cybercrime world. It's in better organisation and what one might term the 'professionalisation' of the industry. These days, when you rent malware, buy databases of credentials or buy time on a botnet, you can often count on customer service support, instructional videos and even money-back guarantees. The fact that those with the technical skills most often use them to create service-based businesses, rather than deploying the products themselves, has opened up the cybercrime world to many more players.

Microsoft has also noted a change in how cyber criminals may combine attack techniques for the most lucrative result. For example, a credential-stealing phishing attack may be the prelude to a business email compromise (BEC) scam. If an attacker can log into the company systems as a real user, it's easier to make subsequent BEC emails appear legitimate.

Cyber criminals also demonstrate some savvy marketing talent. For example, brand imitation is increasingly exploited to lure victims into clicking on phishing emails and 'logging in' to fake websites. The top five spoofed brands are Microsoft, UPS, Amazon, Apple and Zoom.

This is seen most clearly in email-based attacks (malware or phishing), where attackers take advantage of current events to increase the likelihood of their emails being read and links or attachments clicked. This is not new – spammers have long exploited major sporting events, major disasters, elections and the like.



Concerns related to the use of remote workforces. Source: Microsoft.

But this approach is definitely becoming more subtle and successful – and, of course, the most pernicious and cold-blooded example of this is the way cyber criminals have exploited the Covid-19 pandemic for their own benefit.

It's not only common criminals out to make a quick buck that have jumped on the pandemic bandwagon, either. It has been enthusiastically adopted by nation-state actors. Attack campaigns by such groups – which account for most of the so-called advanced persistent threat (APT) groups – commonly begin with phishing or spear-phishing attacks designed to steal credentials, although this is usually just the first stage in a sustained, intricate and multi-layer assault.

The fact that they, too, would exploit the pandemic is predictable, but one of the bigger surprises in the Microsoft report is the organisations they are targeting. The term 'nation-state actor' is frequently used in the same breath as 'critical national infrastructure' (CNI). And, yes, CNI remains a target and a concern. However, of the attacks by nation-state actors logged by Microsoft over the course of a year, 90% of them were against organisations with no connection with CNI, many of them being, "non-governmental organisations (NGOs), advocacy groups, human rights organisations and thinktanks focused on public policy, international affairs or security".

This suggests that much of the effort of government-backed hackers is going into bolstering the geopolitical, propaganda and international policy aims and ambitions of certain nations. According to a blog post by Tom Burt, corporate VP for customer security & trust at Microsoft: "Most of the nation-state activity we observed the past year originated from groups in Russia, Iran, China and North Korea."

Another area of concern, inevitably, is the Internet of Things (IoT). While awareness of issues such as default passwords that are never changed has grown, there are still too many devices being sold with baked-in weaknesses. This applies to both consumer products and industrial IoT systems, with the latter posing significant concerns for the security of CNI.

And finally, there is the issue of the remote workforce, which has grown enormously and rapidly – and often in a barely controlled manner – since the arrival of the pandemic. Microsoft's report shows this to be a major headache for security bosses, and for good reason.

The report is available here: https://bit.ly/3jHQq2k.

In brief

Windows source code leaked

The source code for Windows XP, Windows Server 2003, MS-DOS, Windows CE and Windows NT – including a number of variants – has been leaked online. The 43GB-worth of code was leaked via a torrent link on the 4chan forum. The code was accompanied by a collection of weird conspiracy theory videos centred around Bill Gates. One researcher has already proved that the code is genuine by successfully compiling Windows XP, although the leaked sources lacked one element that would enable installation. However, Windows Server 2003 compiled without issue. Although all the Windows versions that were leaked are obsolete, some – Windows XP in particular – are still in use. This is particularly true in the healthcare centre where certain equipment, such as imaging devices, were built around XP and cannot be upgraded to later operating systems. The leak therefore represents an opportunity for malicious hackers to find vulnerabilities in the code that could be used for zero-day attacks.

Bluetooth bugs

A bug in Bluetooth Low Energy (BLE) systems creates a vulnerability that potentially affects billions of devices. Dubbed BLESA, the vulnerability was discovered by researchers at Purdue University and stems from inadequate re-authentication when a previously authenticated device reconnects. This can happen, for example, when a connected device goes out of range or disconnects and then reconnects. The lack of full authentication during the reconnection allows attackers within range to spoof authenticated devices and potentially pass malicious data. BLE is used by a wide variety of devices, such as smartphones and Internet of Things (IoT) products. The bug affects Linux, Android and iOS platforms, although Apple, which assigned CVE-2020-9770 to the flaw, has already issued a patch. The Purdue paper is here: https://bit.ly/3dnB0xV.

BLESA came one week after another Bluetooth issue, affecting versions 4 and 5, was announced. The vulnerability (CVE-2020-15802), discovered independently by researchers at the École Polytechnique Fédérale de Lausanne (EPFL) and Purdue University, has been dubbed BLURtooth and resides in the Cross-Transport Key Derivation (CTKD) process used during pairing. "Devices… using [CTKD] for pairing are vulnerable to key overwrite, which enables an attacker to gain additional access to profiles or services that are not restricted, by reducing the encryption key strength or overwriting an authenticated key with an unauthenticated key," said a security advisory released by the Carnegie Mellon CERT Co-ordination Centre. There's more information here: https://bit.ly/34LJLxT.

New cyber espionage group

A sophisticated and well-resourced cyber espionage group, dubbed Bahamut, has been discovered by researchers at BlackBerry. According to the firm's report, the group has been engaged in a "staggering" number of attacks against government officials and private-sector VIPs in the Middle East and South Asia. These are "targeted and elaborate phishing and credential-harvesting campaigns, hundreds of new Windows malware samples, use of zero-day exploits, anti-forensic/AV evasion tactics, and more," says the report. "They rely on malware as a last resort, are highly adept at phishing, tend to aim for mobile phones of specific individuals as a way into an organisation, show an exceptional attention to detail and above all are patient – they have been known to watch their targets and wait for a year or more in some cases." The report is here: https://blck.by/353m0ll.

US federal agency breached

The US Cyber security and Infrastructure Security Agency (CISA) has issued an alert that gives unusually detailed information about the breach of an unnamed federal agency. CISA's intrusion detection system, Einstein, picked up the breach, but not before the attacker had spent some time ransacking accounts. The initial access to the system was through valid access credentials for Microsoft Office 365 and domain administrator accounts. While CISA doesn't know how the attacker came to be in possession of these, it suspects they were obtained via an unpatched Pulse Secure VPN server that was vulnerable to the CVE-2019-11510 flaw. The attackers went on to trawl documents, create an SSH shell and reverse SOCKS proxy, install malware and create a locally mounted remote share for exfiltrating documents. It's not known what or how much data was taken because the attacker's activity was so well masked. The CISA alert is here: https://bit.ly/2SIEzW6.

UK criticises Huawei security

The UK's signals intelligence agency, GCHQ, has issued a highly critical report about the quality of Huawei's software, saying that the flaws represent a significant national security risk. Due to the use of Huawei equipment in critical national infrastructure, such as telecomms systems, for some years now GCHQ has collaborated with Huawei on code review at a special facility known as the Huawei Cyber Security Evaluation Centre (HCSEC), or more commonly 'The Cell'. Staffed by GCHQ personnel, the HCSEC provides controlled access to Huawei's source code for its products. There have been many complaints in the past about the low quality of the code, and the new report says that little progress has been made in addressing them. It also says that the number of bugs has risen "significantly" in the past year and that a vulnerability was discovered in 2019 that was of "national significance". "The Oversight Board advises that it will be difficult to appropriately risk manage future products in the context of UK deployments, until the underlying defects in Huawei's software engineering and cyber security processes are remediated," the report notes. "At present, the Oversight Board has not yet seen anything to give it confidence in Huawei's capacity to successfully complete the elements of its transformation programme that it has proposed as a means of addressing these underlying defects." The report is here: https://bit.ly/2Fm9STB.

TrickBot attacked

TrickBot, one of the most pernicious pieces of malware currently in use, is itself under attack. According to reports by security journalist Brian Krebs, a group with access to TrickBot's botnet has twice sent commands to infected machines under the botnet's control to disconnect themselves from TrickBot's command and control servers. In addition, the attacker inserted millions of fake records into TrickBot's database, making the activities of the malware's operators less effective. Following Kreb's revelation, the Washington Post followed up with a story, quoting unnamed intelligence sources, that the attacker was, in fact, US Cyber Command, a branch of the Department of Defense. The aim, it was claimed, was to disrupt the botnet and make it ineffective in the run-up to the forthcoming presidential election in the US. There's more information here: https://bit.ly/3nDl934.

Governments demand lawful access

The ongoing saga of governments demanding 'lawful access' to encrypted communications, and the providers of such communications services explaining that this can't be done without compromising users' security, has been ramped up a notch. The 'Five Eyes' countries of Australia, Canada, New Zealand, the US and the UK as well as Japan and India have issued a statement calling on communications service providers, such as WhatsApp, Signal and Apple, which use end-to-end encryption in their products, to open up backdoors so that law enforcement and intelligence agencies can perform interception. The request is presented as a public safety issue, but it brushes aside the issue that any form of backdoor could be discovered and misused by criminals, nation-state hackers and other governments. The statement actually says that the countries, "challenge the assertion that public safety cannot be protected without compromising privacy or cyber security. We strongly believe that approaches protecting each of these important values are possible and strive to work with industry to collaborate on mutually agreeable solutions." To date, no such solutions have been found. The statement is here: https://bit.ly/2ImmzPm.

Exploitable hosts used in cloud native cyber attacks

Assaf Morag, Aqua Security

Can an in-depth analysis of elements from cyber attack campaigns teach us something new? The answer is yes. As we've seen all too often, crypto-mining campaigns often initiate a vicious circle that starts by infecting and exploiting the host to seek new targets and infect new victims with the same malware.

Of course, there is nothing unique about this, but a recent malware campaign using this tactic did expose something new. An attacker deployed a container image on one of Aqua's honeypots. It contained a text file with a list of around 6,000 host IPs in one of its image layers. An analysis was performed by the cyber research team, Nautilus, comparing it with similar lists from past attacks. The comparison revealed some interesting information that could shed light on the future direction of cyber attacks against cloud native environments.

A vicious circle

First, let's review how these automated attacks are carried out. Although there are some variants in the images used to attack vulnerable hosts, the core behaviour is very similar. Below we portray how one infected host infects another:

1. After the host is compromised, a malicious image is pulled from Docker Hub and then container entry point commands are run. TOR and SSH services are initiated in order to disguise out-going traffic and open a backdoor to the attacker.
2. A shell script is designed to download further scripts and configuration files from the attacker's command and control (C2) server. The configuration files contain lists of Shodan queries and vulnerable IP addresses.[1]
3. A Shodan search is executed. There are several scripts that support this process. All of these files are designed to allow maximum connection metadata randomness (eg, user agents, cookies, using several different Shodan credentials, etc) to avoid being blocked by Shodan.
4. Each new vulnerable host, which was detected by Shodan, was attacked.

One script is responsible for seizing all competing malicious software, while another is designed to deploy and execute a malicious container image.

Vulnerable hosts

On 12 April 2020, a single attack was launched against a honeypot. The image 'stringscene/thttpd:0.04' was designed

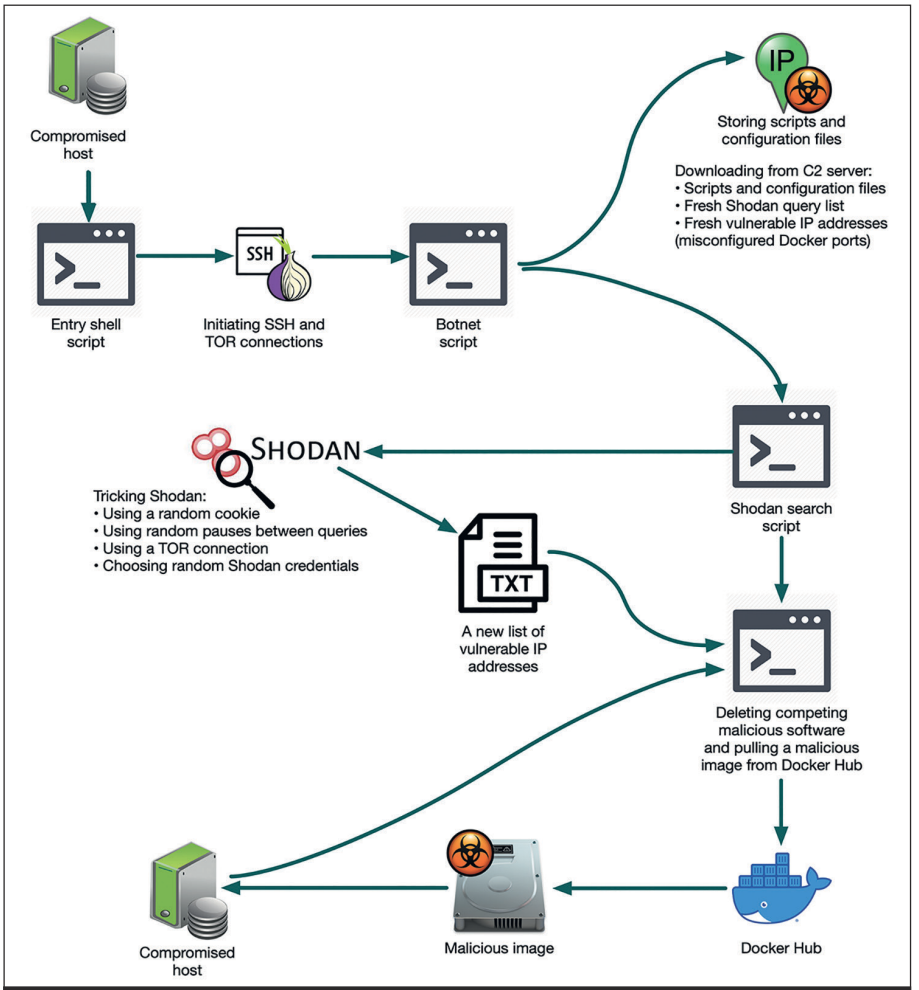


Figure 1: The process by which one host infects another.

to mine crypto-currency. The adversary hid a list of IP addresses within a layer of the container image. Each IP address on the list was set to use port 2375. Traditionally, this port is used as the Docker REST API for unencrypted communication. An examination revealed a list of vulnerable IP addresses, each with a misconfigured Docker API on port 2375.

"Adversaries want to find vulnerable hosts. In order to do so, they need to conduct a mass scan of millions of IP addresses, then determine which ports are open and what services are running on them and find vulnerabilities that can be exploited"

Wanting to learn more from this analysis, we sampled the image from two other past attacks and extracted lists of vulnerable IP addresses. Details are in Table 1.

In total, we analysed the data of 8,558 distinct vulnerable IP addresses. The discrepancy between the sum of IPs that were extracted from these three attacks (8,671) and the number of distinct IP addresses (8,558) suggests that very few IPs appeared in more than one attack – which was indeed the case. Out of 8,558 distinct IP addresses, 97 IPs appeared in two attacks and eight IPs appeared in three attacks. It is unreasonable to assume any organisation would expose such a crucial port for so long (several months), so, it's more reasonable to assume that these IPs are honeypots. Hence, we excluded them from our analysis.

Analysing the Shodan queries

Adversaries want to find vulnerable hosts. In order to do so, they need to conduct a mass scan of millions of IP addresses, then determine which ports are open and what services are running on them and find vulnerabilities that can be exploited.

The adversaries made a smart choice to use Shodan, an online search engine, which stores the metadata of servers. When running a query, the adversary is looking for compromised hosts against a static curated intelligence database. For the end user, Shodan is a passive tool, which means a victim doesn't know that it is being queried. Unlike Shodan, active port scanning tools (eg, Nmap) may leave their imprint on the target's host and tip off the security team when an organisation is being scanned more than usual.

From past attacks, we have collected several configuration files. We retrieved a little over 500 distinct Shodan queries and noticed that the adversaries are:

1. Only looking for vulnerable port 2375. Port 2375 is officially an Internet Assigned Numbers Authority (IANA) used as the Docker REST API for unencrypted traffic. There are several other ports, however, which are also traditionally and officially related to Docker services (for instance 2376, 2377, 4243, 5000, 7946, 9324). Based on the files that we obtained, we haven't seen any references by the adversaries to these ports.

Attack dates	Image	Number of IPs
April 2020	stringscene/thttpd:0.04	5,289
September – October 2019	pocosow/centos:7.6.1810	2,099
June 2019	jzulu/xauto:latest	1,283
Total		8,671

Table 1: List of vulnerable IPs extracted from three attacks on the honeypot.

```
https://www.shodan.io/search?query=port:2375+country:"SG"
https://www.shodan.io/search?query=port:2375+country:"SG"+sh
https://www.shodan.io/search?query=port:2375+country:"JP"+sh
https://www.shodan.io/search?query=port:2375+country:"JP"
https://www.shodan.io/search?query=port:2375+country:"CN"+sh
https://www.shodan.io/search?query=port:2375+country:"CN"
https://www.shodan.io/search?query=port:2375+apache
https://www.shodan.io/search?query=port:2375+xmr
https://www.shodan.io/search?query=port:2375+xmrig+country:"US"
https://www.shodan.io/search?query=port:2375+xmrig+country:"CN"
https://www.shodan.io/search?query=port:2375+xmrig+org:"Aliyun+Computing+Co."
https://www.shodan.io/search?query=port:2375+xmrig
https://www.shodan.io/search?query=port:2375+python
https://www.shodan.io/search?query=port:2375+php
https://www.shodan.io/search?query=port:2375+debian
https://www.shodan.io/search?query=port:2375+nginx
https://www.shodan.io/search?query=port:2375+org:"Hangzhou+Alibaba+Advertising+Co.%2CLtd."
https://www.shodan.io/search?query=port:2375+org:"AWS+Asia+Pacific+%28Seoul%29+Region"
https://www.shodan.io/search?query=port:2375+org:"Amazon+Data+Services+Ireland+Limited"
https://www.shodan.io/search?query=port:2375+org:"Hangzhou+Alibaba+Advertising+Co.%2CLtd."
https://www.shodan.io/search?query=port:2375+version:"1.13.1"
https://www.shodan.io/search?query=port:2375+java
https://www.shodan.io/search?query=port:2375+sh
https://www.shodan.io/search?query=port:2375+mysql
https://www.shodan.io/search?query=port:2375+sql
https://www.shodan.io/search?query=port:2375+country:"KR"
```

Figure 2: Analysing Shodan queries.

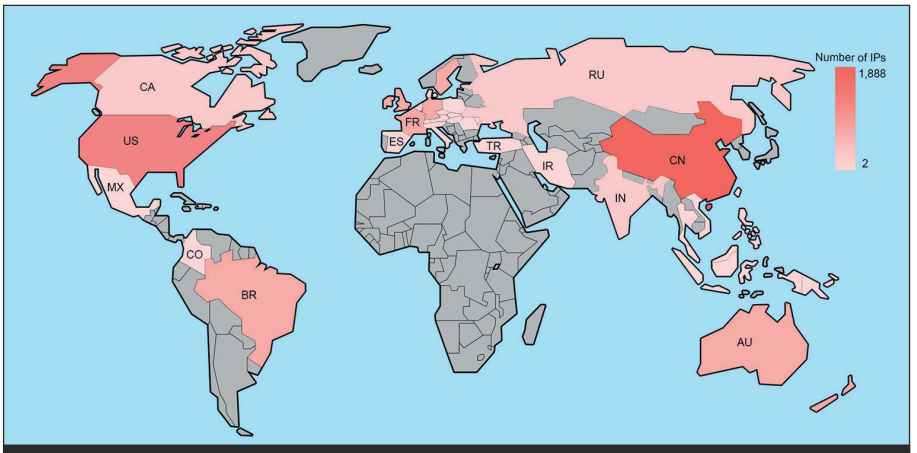


Figure 3: Distribution of vulnerable IPs.

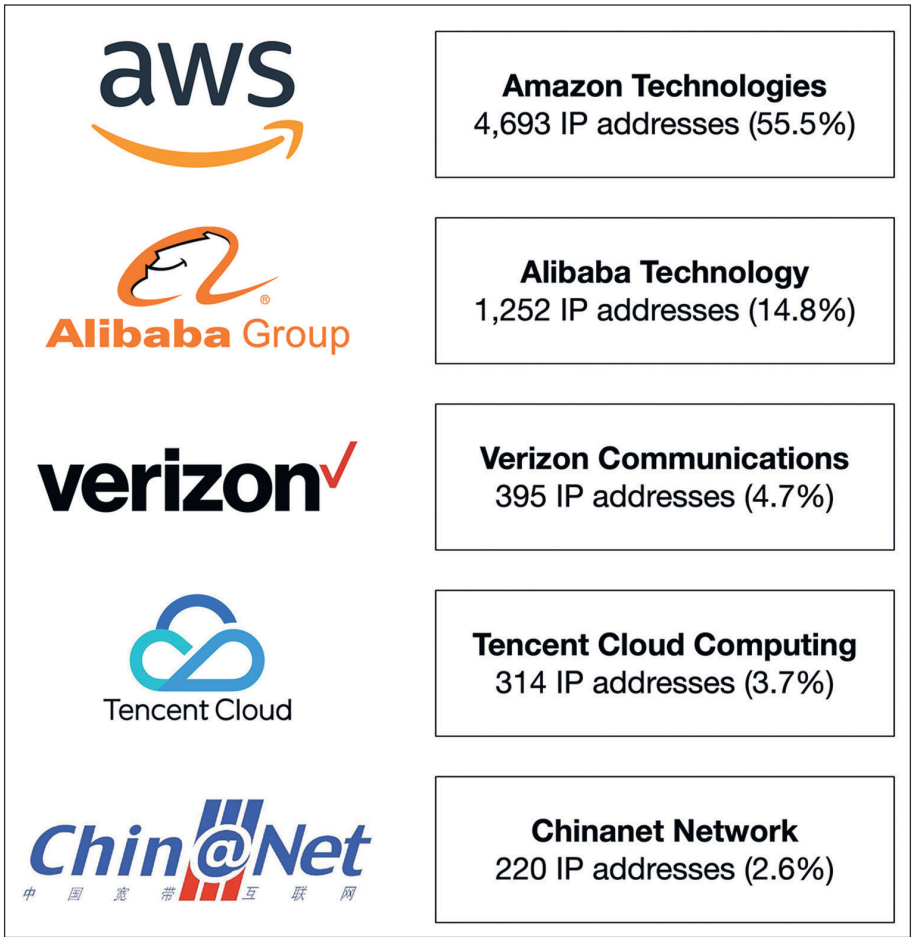


Figure 4: The top five organisations with vulnerable IP addresses.

2. Primarily targeting China, the US, Korea, Singapore, Japan, Brazil, Australia, Russia and India.
3. Using queries to find various services that may run on the Docker port 2375, such as databases, server software, etc.
4. Looking for competing malicious software, such as Kinsing Malware and malicious images (eg, Kannix, avfinder, etc) to block their activity.

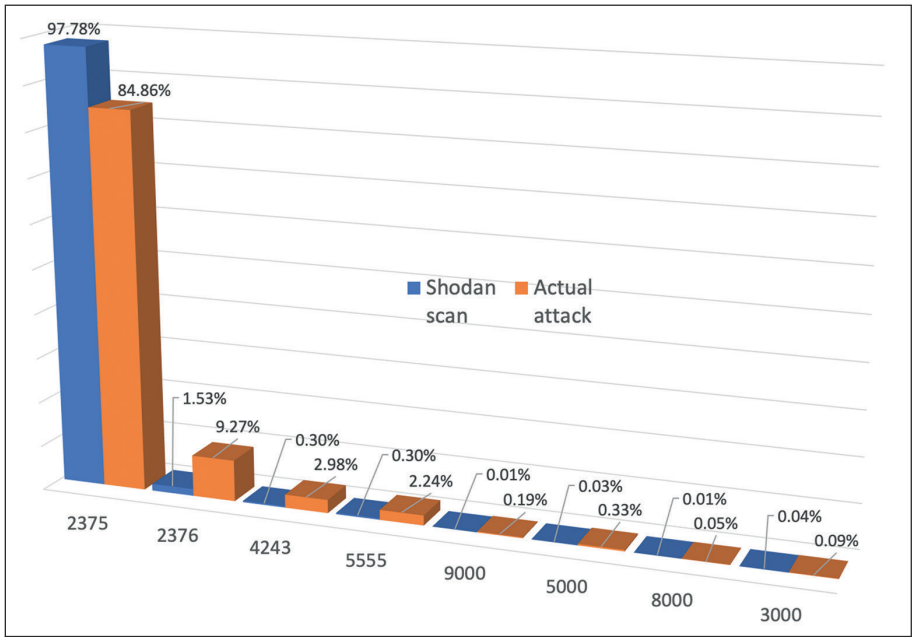


Figure 5: Vulnerable ports found with a Shodan scan and attacks mounted against them.

Analysing vulnerable addresses

Geo-location distribution: Based on the available evidence, China, the US, Japan, Korea and Singapore are the top five most targeted IP addresses, totalling around 60% of the vulnerable IP addresses. This is consistent with our Shodan queries where adversaries are targeting these countries.

Organisation distribution: In Figure 4, you can see the top five organisations with vulnerable IP addresses (based on lists of vulnerable IPs extracted from past attacks). Amazon has the most vulnerable IP addresses. But this is not particularly surprising, since Amazon is ranked as the number one cloud services provider, with an estimated market share of 33%.[2]

Nevertheless, the identity of the rest of the companies in the top five is somewhat surprising. Alibaba, which is ranked fifth, has only 5% market share, but the second most vulnerable IP addresses. Verizon and ChinaNet, which are not even ranked in the top eight cloud services providers, are three and five on the vulnerability ranking, respectively. On the other hand, Microsoft (market share of around 18%) and Google (market share of 8%) have market share estimates putting them in second and third places, but with very few vulnerable IP addresses.

Although some of these findings were a surprise, we should avoid jumping to conclusions. A wrong conclusion might suggest that Amazon and Alibaba may have low security standards, while Microsoft and Google security standards are high. This is not what the data suggests. The reality is much more nuanced, as it could simply be that our data sample is too small or unknowingly biased.

Another problematic aspect is the low dimensionality of details. Many details are missing, such as the identity of the attackers, devices and software targeted, etc. These details could shed more light on these findings and suggest different conclusions.

Vulnerable ports

Unlike what was found in the configuration files, in one of the attacks, a list

Port Number	Role
2375	Docker REST API (plain text) (IANA official)
2376	Docker REST API (ssl) (IANA official).
2377	IANA registered for RPC interface for Docker Swarm.
3000	IANA registered for Cloud9 Integrated Development Environment server. Malware often uses this port as a backdoor
4243	The port is also commonly used by Docker implementations, redistributions and setups (TCP).
5000	Docker Registry server.
5555	Microsoft Dynamics CRM 4.0 (IANA official) There are many reports of malware using this port as a backdoor.
7946	Docker Swarm communication among nodes.
8000	Traditionally used for AWS Local DynamoDB, there are some reports of malware using this port as a backdoor.
9000	ManageEngine AssetExplorer (IT asset management software) uses port 9000 TCP by default. Some online games use this port.
9324	Google Assistant docker containers commonly run a web server listening for HTTP requests on TCP ports 9324 and 5000.

Table 2: A list of ports used in attacks and their official or traditional purposes.

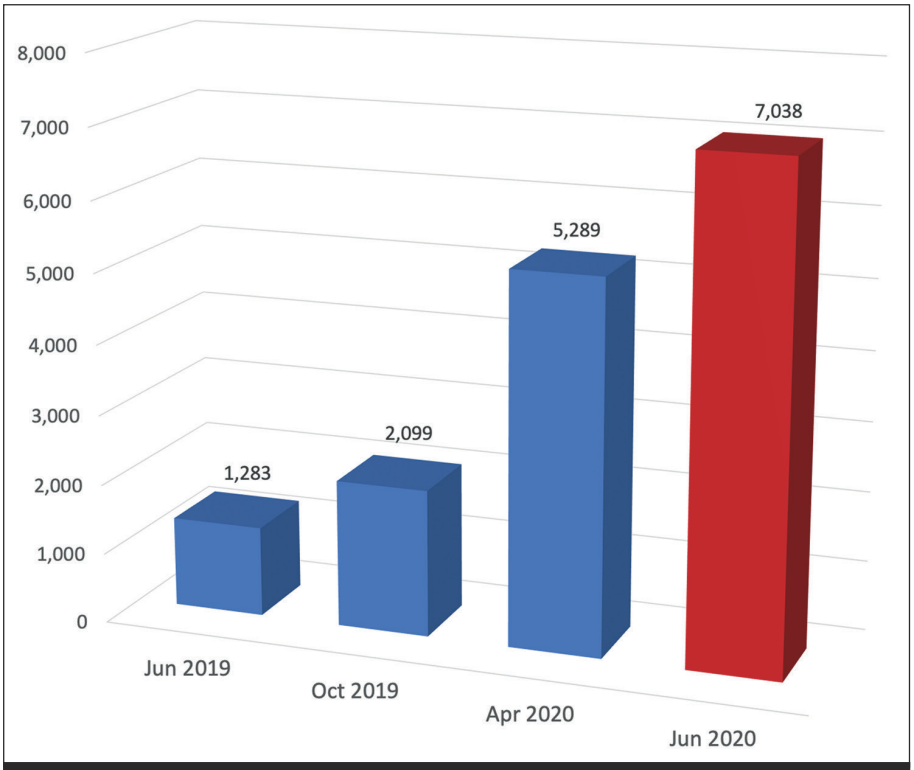


Figure 6: Number of vulnerable IP addresses running Docker services.

of vulnerable IP addresses was detected with various port numbers. This information led to running Shodan queries to detect vulnerable IP addresses with those port numbers. Figure 5 shows a comparison between open ports found with the Shodan scan and actual attacks mounted.

Based on the configuration files retrieved, it appears as though adversaries are mostly targeting port 2375. Nevertheless, there are other vulnerable ports in the wild and adversaries could easily target them – if they haven't done so already. Table 2 shows a list of ports and their official and traditional purposes.[3] Adversaries can also expand their operations to look for more ports that run Docker (or Kubernetes) services.

DevSecOps best practice

Below are some recommendations for DevSecOps. You could implement these as part of your ongoing efforts to mitigate the risks from hidden threats lurking in the cloud:

- Ensure that you are using security and compliance best practices for your public cloud IaaS to mitigate configuration issues across AWS, Azure, Google Cloud, etc. Consider using solutions such as a cloud security posture management tool.
- Scan every image that you use – even from trusted sources. Make sure you are familiar with their use and capabilities. Use a vulnerability scanner such as Trivy (open source).[4]
- Adhere to least privileges access guidelines and avoid root user and privileged modes.
- Dynamically scan images using a dynamic threat analysis tool to uncover hidden suspicious/malicious processes and network communication under simulated runtime conditions using a secure sandbox.

Change over time

As mentioned above, Shodan queries were executed to detect further vulnerable IP addresses running Docker services. Figure 6 shows the results, including the figures that were extracted from the configuration files.

As we suggested above, you shouldn't read too much into any single data point. Nonetheless, in this case, we feel more confident about what the data suggests. It seems like the number of vulnerable hosts running Docker services is increasing over time. This increase appears to be consistent with the following points:

- Using Docker is becoming more robust and easier over time, therefore more people are using these services.
- The variety of people who are using Docker is increasing. This means the

skill level of users is highly variable, which may cause more mistakes and more misconfigured Docker APIs.
- Adversaries are becoming more sophisticated. They are using automated tools to scan and acquire new targets and using more advanced queries to detect vulnerable hosts.

Out of 8,558 IP addresses that were examined, only 105 appeared in more than one list (around 1.2%). This strongly supports our hypothesis that the use of vulnerable IP addresses is increasing.

Summary

This review consisted of three lists of vulnerable IP addresses that were taken from past cyber attacks against Aqua's honeypot. The review included a re-evaluation of the mechanism used to automatically infect the host with crypto-miners and then seek out new vulnerable hosts and infect them as well. Also, there was a review of the analysis regarding the IPs themselves. From this we can draw a number of conclusions:

- The number of vulnerable IP addresses with misconfigured Docker API ports is increasing. This increase is most likely attributable to the increase in Docker usage and adversaries expanding their attack vectors.
- Amazon is the most targeted cloud services provider, and, not surprisingly, has the most vulnerable IPs. Because of its large market share, Amazon may have more end users who are less proficient with cloud native security best practices. This condition often results in environments that are less protected.
- Adversaries are constantly ramping up their game. For instance, they use online search engines to find vulnerable hosts and have automated the infection process.

About the author

Assaf Morag is a lead data analyst at Aqua Security. As part of Aqua's research group – Team Nautilus – his work focuses on supporting the diverse data needs of the team.

References

1. Shodan, home page. Accessed Oct 2020. www.shodan.io.
2. Richter, Felix. 'Amazon leads $100 billion cloud market'. Statista, 18 Aug 2020. Accessed Oct 2020. www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/
3. 'Ports database' SpeedGuide. Accessed Oct 2020. www.speedguide.net/ports.php.
4. Trivy, GitHub page. Accessed Oct 2020. https://github.com/aquasecurity/trivy.

How threat actors abuse ICS-specific file types


Nadav Erez

Nadav Erez, Claroty

Project files are integral to industrial control system (ICS) solutions, providing all the necessary data and instructions each machine on the operational technology (OT) network needs to operate. While engineers will use them to ensure the smooth running of operations, security teams can use them to gather an accurate picture of what machines are running on the system along with other critical data, such as where they are and what they are supposed to be doing.

However, extracting information from ICS engineering project files is not always straightforward. While some ICS software vendors offer simple import-export functionality supporting standardised file types such as CSV, others use binary, proprietary formats that can only be interpreted using vendor-specific software.

A lack of full visibility into what is running on the network and how it normally functions presents a significant security risk, because threat actors could infiltrate the network and the security team would be none the wiser. Further, due to their inherent vulnerabilities, ICS project files present an opportunity for threat actors to change how machines operate to cause significant damage, which can be achieved by luring engineers into phishing scams.

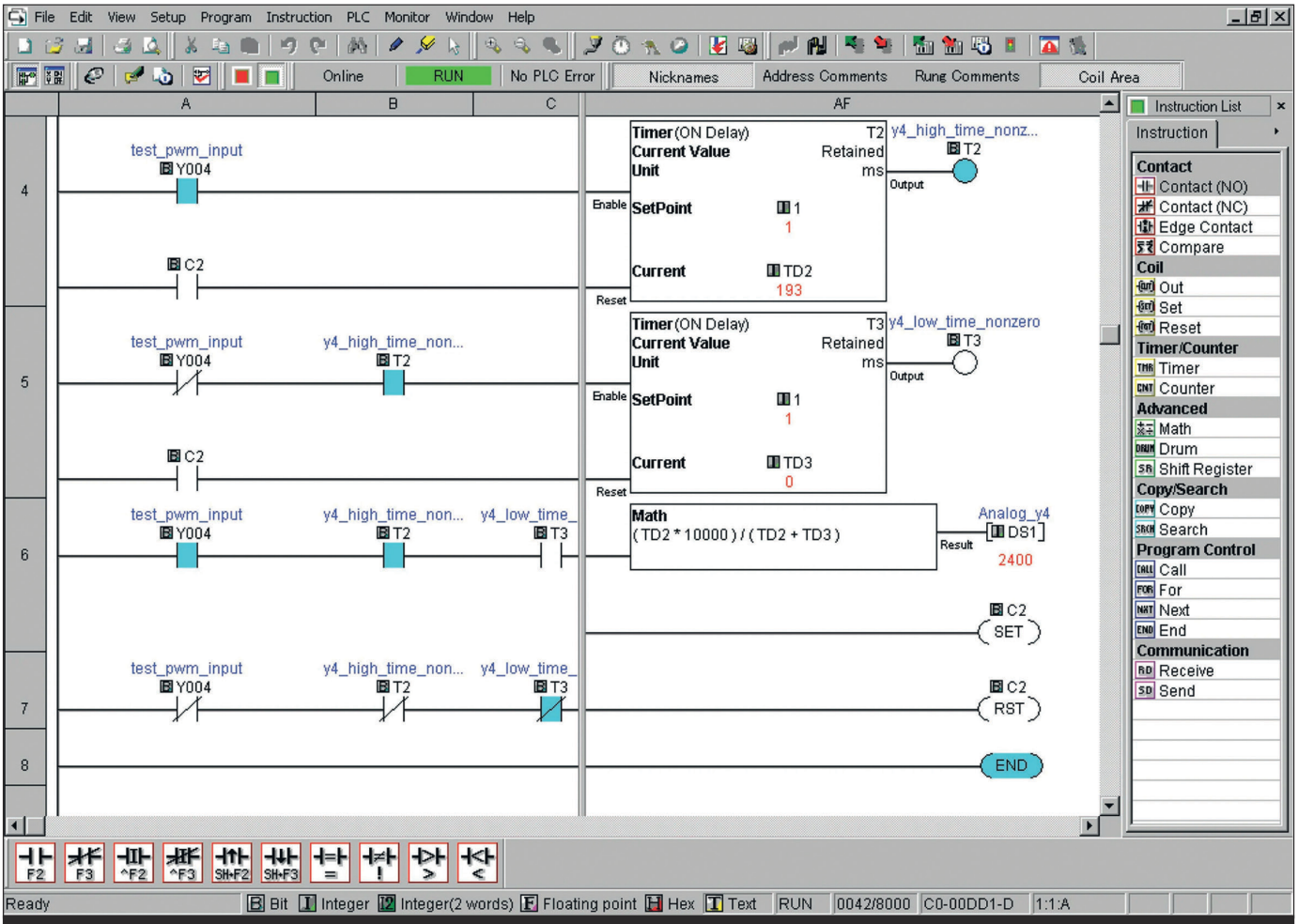
ICS project files

An ICS project file is made up of several different files containing a whole range of data that is necessary to carry out the saved project.

What information should we expect to see in these project files? At the top level it would be the network layout, which holds information about what assets are on the network. This might be a PROFIBUS, a standardised, open, digital communications system used in manufacturing automation, along with any stations connected to it.

Additionally, the project file needs to contain details about each individual asset on the network. This will include the devices' IP addresses and serial numbers, as well as data about the slots that each device has and what they are being used for, including module details and order numbers.

The logic necessary for these devices is also saved on the project file, which includes function block or ladder dia-



An example of a ladder diagram.

grams. Function block logic and ladder logic are programming languages used for developing logic expressions in order to automate tasks. Such tasks include counting, timing, arithmetic, sequencers, PID control and data manipulation functions, to name a few.

ICS project files come in all shapes and sizes. The most basic are text files such as Excel documents containing information about the asset, including IP address, model number and the application version it is running. However, many ICS software vendors use project files in proprietary binary formats. Retrieving the information out of these files requires specialist software or even reverse engineering.

Project files can also be directories, which in turn contain subdirectories holding various types of files. In this case it is not just about being able to read the file, but also understanding where it is in the first place – a task easier said than done when such directories can contain thousands of files. This is further complicated by the reality that while most of these directories will be stored as .zip files, some are still stored in .cab format, which has long been superseded by .zip, meaning that the right script needs to be found to open up the file.

Why are project files useful?

Security teams wishing to understand the layout of their OT network can do so by capturing the traffic running across it and building a topography based on that information. However, this does take considerable time and effort. Alternatively, if security teams are able to extract and read the information from those project files accessible on engineers' servers, these together will more quickly provide a complete picture of what the network looks like, what's running on it, and so on.

Using the project file-created map as a baseline, a security team can then compare this to what is actually happening on the network to identify any suspicious activity, such as new devices being connected.

Project files also give a clear picture of the role of each asset, so that in the event of something unexpected happening, the security team can track down the root cause and reset the affected machines. Further, having a detailed inventory of each device and what it is running on enables the security team to assess their security posture, information about which can be used to identify vulnerabilities and where updates and patching are required.

But to achieve all of this, security teams need to have a solution in place that is able to extract and parse all the pertinent data in a format that is easy to access and understand.

Useful to threat actors

If threat actors manage to infiltrate an OT network, they can use any project

files they find to build a picture of which machines are connected to the network and what their function is. Using this information, they can target exactly those assets that will cause the most disruption if they are compromised.

There are also significant vulnerabilities within project files themselves that threat actors can exploit as part of their attack. For example, we have already seen that project files often come zipped, particularly when they need to be transferred from one system to another. The 'zip slip' vulnerability enables attackers to modify paths within a .zip file so that when it is unzipped, the files contained within it are uploaded to a different location from the target file. This means that the attacker can write files to anywhere on the network where the file is extracted. Such a capability means that the attacker could take over a computer, for instance, if he overwrites a program in the start-up directory.

The binary formats used in many types of project file are vulnerable, as they are created using code that is usually many years old. This would often have been written at a time before coders were aware of how to protect their code, and this is unlikely to have been maintained since then. Vulnerabilities of binary formats continue to be published on a regular basis and create a real issue for owners.

Possible attack

One way a threat actor could attack an OT network is through uploading a Dynamic Link Library (DLL) file, which contains instructions that other programs use to carry out specific tasks. To carry out such an attack, threat actors would first need to create or clone a project file that has a vulnerability, for example an instruction to import a file from a specified location when the project starts. They can then change the code to ensure the file imported contains a malicious DLL to carry out an assigned task, which could be used to shut down the system.

To get an engineer to open the file, threat actors could send a phishing email with it attached. To make this look convincing, the file is likely to be in an engineer-friendly format, one that the victim would be familiar with and that opens through some form of ICS software. This makes it more likely to pass casual scrutiny than, say, a .doc file, and makes the engineer more curious about the contents. This has the added benefit that the engineer will open the file up on a computer that has engineering software on it, which will most likely be connected to the OT network. If it were a simple .doc file, the engineer might just use a home PC, meaning the threat actors would not be able to continue their attack.

Threat actors have recently been seen targeting organisations that run OT networks in this way. For example, earlier this year organisations in the oil and gas industry were subject to spear-phishing attacks, in which the attackers were looking to steal information.[1]

Another method that threat actors use to get engineers to open malicious project files is with specialist support forums. They may send a simple message saying that they need help opening a project file, that they don't have the right software to extract it. Those wishing to assist their perceived peer might download the file to convert it for them. Of course, this is a malicious file, so as soon as the engineer opens it, his or her machine will start carrying out the functions specified in its code.

Motives for an attack

While one motivation for these attacks might be to shut everything down and demand a ransom for its release, the most likely reason is to cause sabotage. Attacks against OT networks tend to focus on critical national infrastructure (CNI) and industries necessary to the economies of nation states and look to cause as much disruption as possible.

The most notorious examples of such attacks were those against the Ukraine energy industry in 2015 and 2016 that left thousands of residents without power for several hours.[2]

Protecting against attacks

To prevent malicious project files from being downloaded onto the network, organisations need to look at deploying strong endpoint protection and email security to prevent phishing emails getting through to the engineers, as well as restricting what they are able to download onto the OT network. This will prevent the vast majority of these files getting onto the system in the first place. Also worth considering is cyber security training for engineers so that they are able to spot a suspicious file and know how to handle it.

Yet despite these measures, there is always a possibility that a malicious file will make it onto the network. As such, security teams require visibility of all project files on the OT network, regardless of what format they are in, and know how these should normally look. Further, they need to be able to monitor the network traffic to be able to identify anomalous behaviour that could indicate that a project file has been compromised. This monitoring should also include looking at any intersections between the IT and OT networks, so that any files being moved from one to the other, which could be a potential security risk, are flagged.

As the average OT network will run on many thousands of project files, this is not a task that can be achieved manually. Therefore, automated solutions that can carry out this monitoring and alert the security team to anything that requires attention are essential.

Project files are a vital component of any OT network, but they are also one of the most vulnerable. By knowing how they work and what the inherent risks are, security teams can take appropriate steps to ensure that those project files that are so useful to engineers are not as beneficial to threat actors.

About the author

Nadav Erez leads the research team at Claroty (www.claroty.com), performing extensive ICS protocol research and reverse engineering, as well as leading Claroty's vulnerability research efforts, which led to reporting dozens of vulnerabilities on targets ranging from PLCs to Scada servers and engineering software. Erez has over 10 years of security research experience and prior to joining Claroty, he served in an elite cyber unit of the IDF's Intelligence unit, where he led a team of cyber security

researchers in a number of disciplines and in a fast-changing landscape.

References

1. Paganini, Pierluigi. 'Spear-phishing attacks hit the oil and gas industry sector'. Security Affairs, 21 Apr 2020. Accessed Oct 2020. https://securityaffairs.co/wordpress/101967/cybercrime/spear-phishing-energy-oil-gas-industry.html.
2. Park, Donghui; Summers, Julia; Walstrom, Michael. 'Cyber attack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks'. University of Washington, 11 Oct 2017. Accessed Oct 2020. https://jsis.washington.edu/news/cyber attack-critical-infrastructure-russia-ukrainian-power-grid-attacks/.

How organisations can ethically negotiate ransomware payments

Tom Hofmann

Tom Hofmann, Flashpoint

By 2021, a new organisation will be falling victim to ransomware every 11 seconds.[1] However, ransomware figures have been skyrocketing since 2017 when the globe was hit by WannaCry and NotPetya. At that time, the term 'ransomware' entered common parlance and 54% of businesses were hit by these attacks.

These numbers are even more striking when considering the average cost of a single ransomware attack. Before even paying the ransom, the accumulated cost of downtime, people time, device cost, network cost and lost opportunity is estimated to be around $713,000 on average.[2]

So, how do the majority of businesses that are targeted by these insidious attacks deal with them? While it is an IT or IT security responsibility to protect and remediate against ransomware, the onus lies on business leaders to make the ultimate decision – to pay or not to pay. And for many this raises an ethical dilemma.

Many leaders will initially take the higher ground because they don't want to be seen as a business that negotiates with criminals or sends money to people who may invest it into other illicit activities such as drug or weapons dealing. On the flip side, depending on what is being held to ransom, whether that is personal data that it is an organisation's role to protect, critical infrastructure or even life-saving medical devices, sometimes organisations have no option but to pay. And with 95% of organisations that pay the ransom having their data or systems restored to them, for many this is simply the safer strategy.

This article will discuss the latest ransomware trends before giving some insight into unspoken codes of conduct among cyber criminal groups that will help readers understand the inner workings of why these attacks happen. It will then conclude with some advice on how to negotiate with cyber criminals to lessen the impact on the organisation, if this is a safer and more ethical option for businesses than not paying.

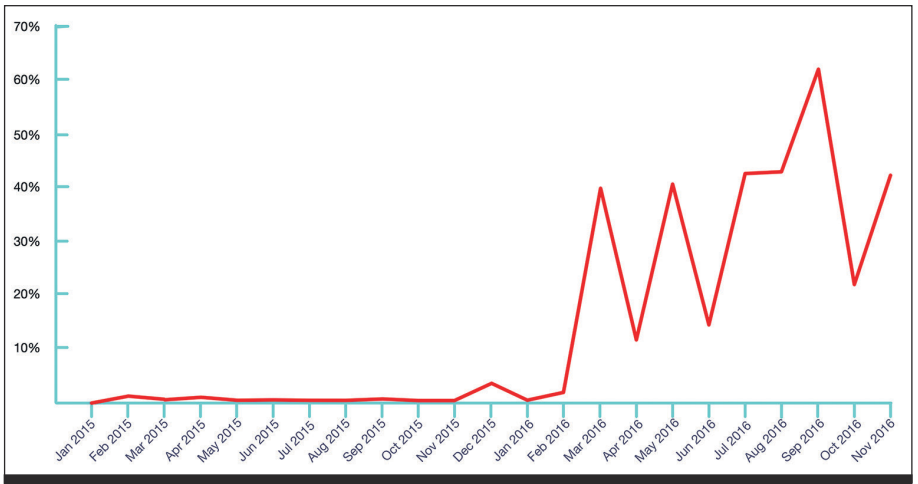
Ultimately, paying the ransom should always be the last option, but if a business has no other choice, ensuring that the payment and remediation process is completed strategically and in a safe manner is paramount to the business recovering as quickly as possible.

Latest trends

The 2016 ransomware attack against the Hollywood Presbyterian Medical Centre was a turning point in the history of ransomware.[3] It was the first attack that put human lives at risk (threatening to turn off life-saving equipment) and – even though the hospital claimed the infrastructure was never truly at risk – Hollywood Presbyterian paid the 40 bitcoin ransom ($17,000 in 2016 but worth over $400,000 today) in just over a week. In the following months, ransomware globally increased by 6,000% and 70% of businesses affected chose to pay the ransom.[4]

Over the following year, the world was rocked by the likes of WannaCry, NotPetya and CryptoLocker, which are still widely considered the largest ransomware attacks to have ever taken place. However, since then this indiscriminate attack style has been replaced by a more targeted approach, run by more nimble threat actors.[5]

While still largely relying on commodity exploits for known vulnerabilities or configuration weaknesses to gain access to a network, rather than dropping malware on certain machines, attackers have been hitting organisations hard by flooding ransomware onto endpoints and network shares and demanding drastically high ransoms in return for decrypted data. Already, state and local government operations have suffered major incursions, with one of the biggest being the attack against the city of Atlanta in 2018. Atlanta was infected, according to investigators, with the SamSam ransomware, which is spread via exploits rather than through shotgun-style spam or phishing emails.[6] Victims in other industries, notably financial

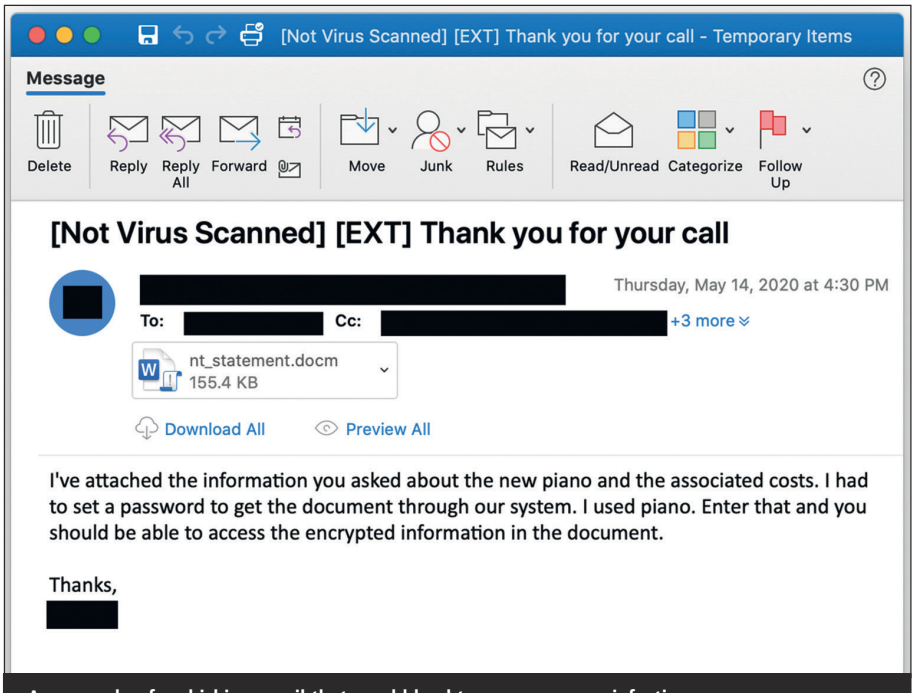


Percentage of spam with ransomware attachments, showing how the ransomware menace fully emerged in 2016. Source: IBM.

services, telecommunications and healthcare, have also felt the brunt of targeted ransomware attacks.

This section will conclude with three of the most recent ransomware trends. First, ransomware-as-a-service – these programmes have been developed with great care to ensure that encrypted files can be successfully restored after the ransom is paid in order to keep these attacks as a viable way of making money. Second, ransomware attacks are increasingly focused on threatening to leak data if the ransom isn't paid, with leak sites including AKO, CLOP and DoppelPaymer.[7] This trend reflects the development of global data protection regulations such as the General Data Protection Regulation (GDPR) which have significant financial repercussions for organisations experiencing breaches, leading to a higher probability of firms paying the ransom to prevent breaches altogether.

Finally, the coronavirus pandemic has seen an explosion of themed attacks of all varieties. Ransomware has been less common than phishing and fraud-related attacks but we have seen some groups targeting healthcare organisations. For example, the Maze ransomware group conducted an attack on Hammersmith Medicines Research, which performs clinical tests for drugs and vaccines.[8]



An example of a phishing email that would lead to a ransomware infection.

Codes of conduct

While the latest ransomware trends are frequently discussed in cyber security forums and recently in more mainstream media as well, cyber criminal communications about ransomware and the nuances of their activities are shadier. Readers may be surprised to learn that despite the popular image of the hooded, faceless cyber criminal, generating a notion that these individuals are less than human, there is in fact an unspoken code of conduct within cyber criminal communities and these attacks can cause 'ethical dilemmas' for hackers perpetrating ransomware attacks.

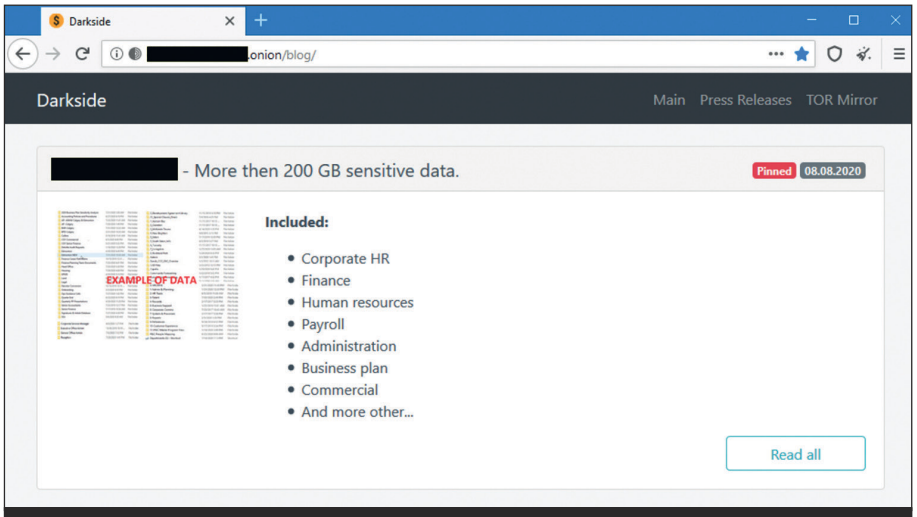
For example, while monitoring online illicit communities in Eastern Europe from early 2014 to early 2016, Flashpoint identified the forewarnings of a shift in attitude towards ransomware.[9] Prior to 2016, administrators of the Russian cybercrime underground stated that ransomware should not be practised for two reasons: either it was a waste of botnet installs and exploit kits or it was seen as 'intellectual death' and therefore a low-end manoeuvre.

These administrators firmly believed that ransomware attracts too much attention, may impede other types of cybercrime or could be too easily turned toward Russian targets. The increase may cause the Russian Government to take a harsher stance towards deep and dark web communities.

Cold reception

Returning back to Hollywood Presbyterian, despite this attack targeting Westerners – which is highly encouraged by many cyber criminal groups – it was coldly received by Eastern European cyber criminals, many of whom regarded the incident as reckless and unacceptable. While some in the community supported the attack, the majority condemned the unknown assailants, which created an ethical divide in the underground.

One highly reputable member of a Russian top-tier cybercrime forum expressed his frustration with ransomware, writing: "From the bottom of my heart, I sincerely wish that the mothers of all ransomware distributors end up in the hos-



An example of a data leak page from a ransomware group – in this case, Darkside.

pital, and that the computer responsible for the resuscitation machine gets infected with [the ransomware].” In response, a prominent ransomware operator countered that view: “[the attackers] scored. It means everything was done properly.” Rather than adhering to the ethical code imposed by administrators, he proposed that targeting places that were guaranteed to pay was not wrong because, at the end of the day, cybercrime is always about making money.

Unfortunately, this latter way of thinking appeared to win the debate, as from 2016 (WannaCry debilitating the NHS as a case and point) criminal perceptions of ransomware appeared to move beyond ethical concerns into being largely financially motivated. The majority of those perpetrating these kinds of attacks do, however, encourage each other to live up to the promises they gave to their victims, otherwise ransomware could lose its money-making power (this is echoed in the statistic at the top of this article, that 95% of people who have paid a ransom had their data restored to them).

The purpose of this section has been to showcase that when defending the organisation against any cyber security threat, seeing cyber criminals as people rather than shadowy figures without nuanced motivations or ethics is key in protecting organisations from attack. The combination of monitoring activity in the deep and dark web and closely monitoring observed attacker behaviours inside the organisational environment yields a much deeper perspective on the actors threatening the business. This dramatically improves situational awareness and provides necessary perspective when developing effective mitigation strategies for defence.

When to negotiate

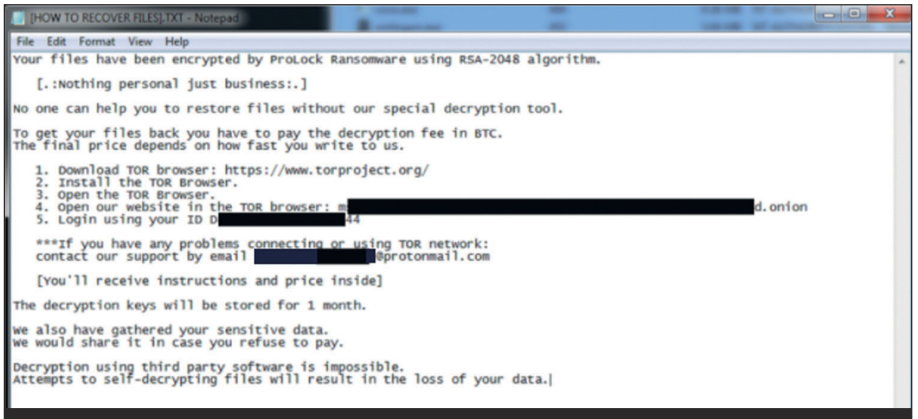
On 7 May 2019, the City of Baltimore in Maryland was hit by a ransomware attack.[10] The attack shut down the majority of the city’s servers, meaning online services and more were completely shut down while the attackers demanded a 13 bitcoin ($100,000) ransom. But Baltimore never conceded. Instead it focused all of its efforts on forensic analysis and detection, deploying new systems, hardware and software, replacing hard drives and additional recovery at a cost of $18.2m.

Baltimore was able to recover without paying the ransom but organisations must understand that paying a ransom can drift toward becoming a viable option when weighed against unacceptable losses that system and service unavailability may bring to an enterprise or government or civilian agency. This flies in the face of stern recommendations from law enforcement and the security community, both of which are adamant against paying for fear of propping up a criminal ecosystem, and without a steadfast guarantee that encrypted files and locked-down systems will be returned intact.

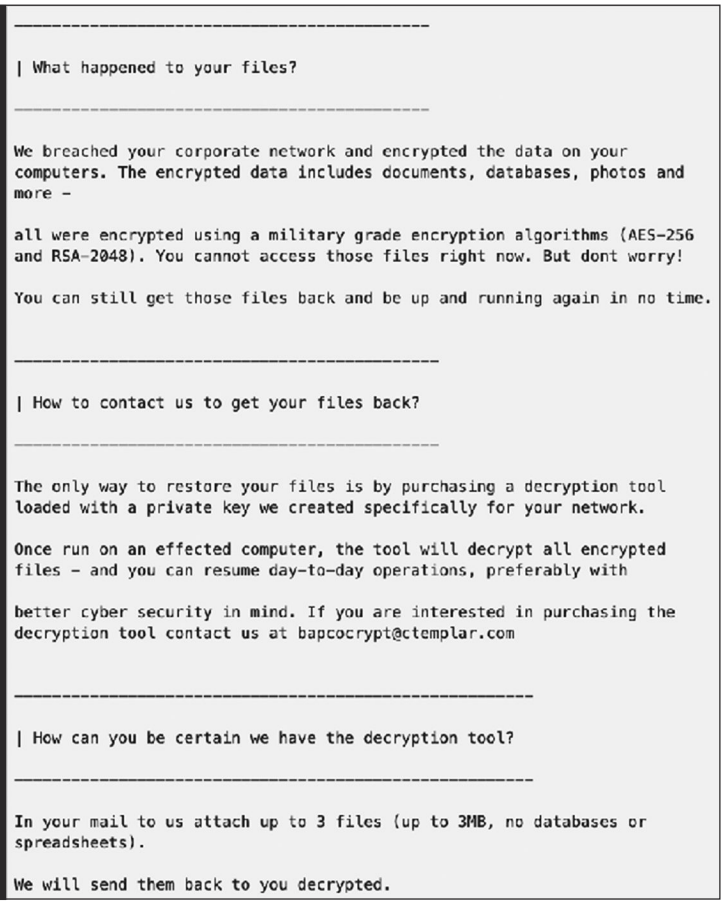
The immediate and future financial viability of a company and fiduciary responsibility to stakeholders could heavily sway such a conversation toward meeting an attacker’s demands. Even so, organisations must tread carefully should they choose to pay; there are no guarantees that a decryption key will be delivered, nor would there be an assurance that files haven’t been corrupted, or that internal staff have the wherewithal to handle the keys properly and decrypt every file and unlock every system.

Nonetheless, research and advisory firm Forrester Research also says it has been tracking a notable increase in ransomware payouts.[11] Its analysts now recommend that paying ransomware should at least be considered a viable option in order to offset potentially catastrophic business interruption. The firm does remind potential victims that paying a ransom isn’t an automatic path to recovery, which is complicated in any extortion scam.

The long and short of this is that organisations should always be prepared to be targeted by a ransomware attack: and with this in mind, back-up is a victim’s best friend. A recent, reliable and secure back-up can have an organisation



A Prolock ransomware note requesting an amount in Bitcoin that “depends on how fast you write to us”.



```
------------------------------------------

| What happened to your files?

------------------------------------------

We breached your corporate network and encrypted the data on your
computers. The encrypted data includes documents, databases, photos and
more -

all were encrypted using a military grade encryption algorithms (AES-256
and RSA-2048). You cannot access those files right now. But dont worry!

You can still get those files back and be up and running again in no time.


------------------------------------------

| How to contact us to get your files back?

------------------------------------------

The only way to restore your files is by purchasing a decryption tool
loaded with a private key we created specifically for your network.

Once run on an effected computer, the tool will decrypt all encrypted
files - and you can resume day-to-day operations, preferably with

better cyber security in mind. If you are interested in purchasing the
decryption tool contact us at bapcocrypt@ctemplar.com


------------------------------------------------------

| How can you be certain we have the decryption tool?

------------------------------------------------------

In your mail to us attach up to 3 files (up to 3MB, no databases or
spreadsheets).

We will send them back to you decrypted.
```

A Snake ransomware note.

up and running relatively quickly and with minimal downtime. It will also be spared the potentially risky task of engaging directly with a threat actor, as well as procuring and transferring crypto-currency to meet the attacker's ransom demand. These tasks aren't covered in traditional incident response plans where system clean-up and reimaging is self-contained and can be accomplished in relatively short order.

However, if restoring a back-up isn't an option because it will take too long or there are other ethical barriers in place – for example, if critical technology has been shut down – firms may have to turn to incident response and, potentially, ransomware negotiation.

Effective bargaining

As this article has argued, the driving factors behind whether to pay a ransom or not are twofold: ethical (if what is at stake is very sensitive personal data, critical infrastructure or people's lives) and financial (if the cost of downtime will exceed the cost of the ransom). So, if an organisation decides to pay the ransom, what actions must it take to ensure that the process is handled as professionally and safely as possible?

First, conventional incident response must take place, where the team runs forensics and validates the possibility of recovering data and systems from back-up. In parallel with this, firms must begin communication with the attacker, which could include negotiation for a discount and validation by asking for a decrypted key. It is highly recommended that you use a negotiation specialist for this because he or she will bring expertise in particular ransomware strains as well as re the threat actors. That type of intelligence can help an organisation make its final decision and understand whether successful recovery is possible. There's also a skill to the negotiation and professionalism provided by someone marginally detached from the incident.

Key elements of the negotiation process include demanding a 'proof of life' from the hackers, whereby the business requests they decrypt a portion of the hostage files. Organisations must also try their utmost to pay out strategically – they must work quickly to identify which critical operations need to be restored urgently and which could be rebuilt at less cost than paying the ransom. They can then negotiate an immediate payment with the criminal to restore these systems before quickly backing them up so they are fortified against being attacked again.

Ever-changing threats

To conclude, this article has tracked the evolution of ransomware from when it became one of the most used forms of cyber attack in 2016, examining the different forms it has taken today to showcase how it is always evolving. For this reason, all organisations should maintain an ongoing interest in protecting themselves from the ever-changing threats and attack methods used. It then examined the changing ethics of threat actors to highlight the importance of seeing cyber criminals as human beings with a host of different motivations. As a result, having a team or partner that understands threat actors can make a huge difference in defending against and responding quickly to not just ransomware but all kinds of cyber attacks.

We concluded with an analysis of the 'to pay or not to pay' alongside actionable advice on incident response and ransomware negotiation. As argued throughout, decision-makers must make the call as to whether to pay in a ransomware incident, and only after all options have been considered and all recovery options exhausted. Ultimately, paying a ransom demand is a business decision and one that organisations must prepare for in advance by contracting with a negotiations specialist and consider procuring crypto-currency in the event of an infection.

Often, specific expertise isn't in the wheelhouse of an enterprise's incident response team; ransomware requires a new paradigm of contingencies related to response. Few organisations today know how to best interact with an adversary, acquire crypto-currency and successfully and safely move that money to an attacker's wallet without putting the firm at further risk. When it comes to ransomware, the popular phrase "it's not a matter of if it will happen to you, but when" applies.

Being as prepared as possible to respond to an attack is business critical.

About the author

Tom Hofmann leads the intelligence directorate at Flashpoint that is responsible for the collection, analysis, production and dissemination of deep and dark web data. He works closely with clients to prioritise their intelligence requirements and ensures that internal Flashpoint operations are aligned to those needs. Hofmann has been at the forefront of cyber intelligence operations in the commercial, government and military sectors, and is known for his ability to drive effective intelligence operations to support offensive and defensive network operations.

References

1. Morgan, Steve. '2017 Cybercrime Report'. Cyber security Ventures, Feb 2017. Accessed Aug 2020. https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf.
2. Graham, Luke. 'Ransomware can cost firms over $700,000; cloud computing may provide the protection they need.' CNBC, Aug 2020. Accessed Aug 2020. www.cnbc.com/2017/08/04/cloud-computing-cyber security-defend-against-ransomware-hacks.html.
3. Yadron, Danny. 'Los Angeles hospital paid $17,000 in bitcoin to ransomware hackers'. The Guardian, Feb 2016. Accessed Jul 2020. www.theguardian.com/technology/2016/feb/17/los-angeles-hospital-hacked-ransom-bitcoin-hollywood-presbyterian-medical-centre.
4. 'Ransomware: How consumers and businesses value their data.' IBM, Dec 2016. Accessed Jul 2020. www.ibm.com/account/reg/us-en/signup?formid=mrs-form-10908.
5. 'The crippling effects of targeted ransomware attacks.' Flashpoint, Apr 2016. Accessed Jul 2020. www.flashpoint-intel.com/blog/cybercrime/the-crippling-effects-of-targeted-ransomware-attacks/.
6. Ventura, Vitor. 'SamSam – The Evolution continues netting over $325,000 in 4 weeks'. Talos Blog, 22 Jan 2018. Accessed Jul 2020. https://blog.talosintelligence.com/2018/01/samsam-evolution-continues-netting-over.html.
7. Cimpanu, Catalin. 'Here's a list of all the ransomware gangs who will steal and leak your data if you don't pay.' ZD NET, Apr 2020. Accessed Aug 2020. www.zdnet.com/article/heres-a-list-of-all-the-ransomware-gangs-who-will-steal-and-leak-your-data-if-you-dont-pay/.
8. 'HMR targeted by cyber criminals'. Hammersmith Medicines Research, 29 Apr 2020. Accessed Jul 2020. www.hmrlondon.com/hmr-targeted-by-cyber criminals.
9. 'How ransomware has become an 'ethical' dilemma in the Eastern European underground'. Flashpoint, 20 Sep 2017. Accessed Jul 2020. www.flashpoint-intel.com/blog/ransomware-ethical-dilemma-eastern-european-underground/.
10. 'Here's what went wrong in the Baltimore ransomware attack that cost the city $18.2 million' Cyware Social, 1 Oct 2019. Accessed Jul 2020. https://cyware.com/news/heres-what-went-wrong-in-baltimore-ransomware-attack-that-cost-the-city-over-182-million-3b6ac1a2.
11. Zelonis, Josh; Lyness, Trevor; Balaouras, Stephanie; Cyr, Madeline; Dostie, Peggy. 'Forrester's guide to paying ransomware: paying ransom can be a valid recovery option based on business need and circumstances'. Forrester, Jun 2019. Accessed Jul 2020. www.forrester.com/report/Forresters+Guide+To+Paying+Ransomware/-/E-RES154595.

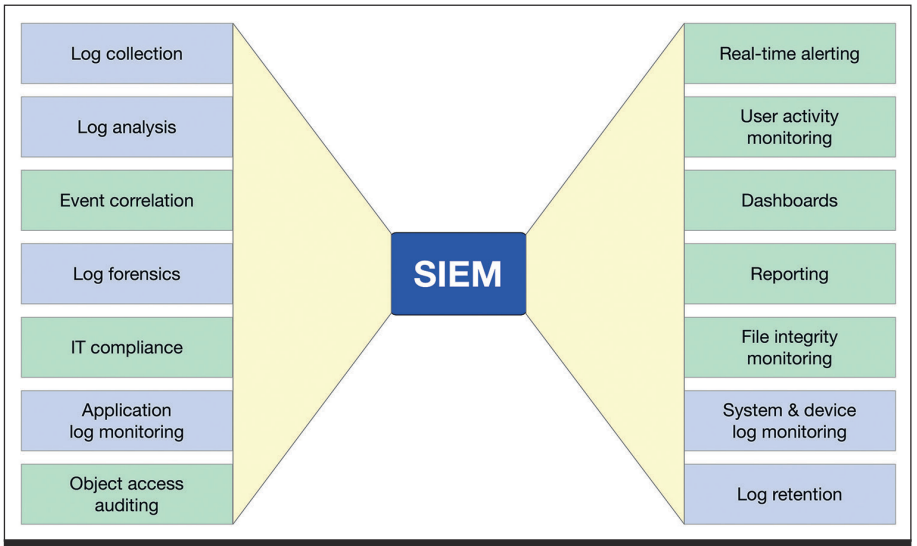
Data highway and the digital transformation: arguments for secure, centralised log management

Robert Meyers

Robert Meyers, One Identity

Digital transformation happened all of a sudden, not with a gradual shift towards more sophisticated tools, but with a televised announcement from prime ministers and presidents across the globe asking organisations to do their part in containing the coronavirus outbreak. Almost overnight, companies found themselves having to adapt to a completely new mode of working. Some saw their remote workforce increasing exponentially, others had to swiftly make arrangements as they had previously always worked on-premise.

Faced with this challenge, companies had to put policies and technologies in place to allow employees to continue doing their job as they would have in the office. That meant that all the tools workers



For many organisations, everything is just fed through the security information and event management (SIEM) and that is considered 'job done'.

previously accessed from the corporate network now had to become accessible from outside the company perimeter. Some organisations opted for a VPN, others went for SSL connections through web applications or used Citrix farms.

"The logs that are sent into the SIEM include the logs from external access points such as remote machines, server logs, and things like terminal services and Citrix, as well as application logging"

But as all of this was happening, one thing remained the same: logs. These continued to be collected, regardless of whether users were within the network perimeter or in their own living rooms.

The importance of logs

Logs are collections of data about the activity and the performance of applications, systems and users. These are very useful from a security perspective, but also to monitor the overall performance of certain applications and tools. Normally, logs are fed into the organisation's security information and event management (SIEM), which ultimately helps identify activity that shows signs of compromise or is potentially suspicious.

Interestingly, most companies don't archive all the logs from their workstations, but favour storing just the 'important' logs. These traditionally include server logs, remote access logs, multi-user system logs, security logs and web application logs. Collected in a SIEM, these are used to provide real-time analysis.

Archiving only the more important logs helps SIEM vendors such as Splunk to control their costs. The model has generally worked well, especially given that the price of maintaining a SIEM is usually based on either the number of gigabytes of logs per day, or on the total amount of storage a customer requires.

Digital transformation

But when a company goes from 50 remote workers to 5,000 in a matter of weeks, things change. The logs that are sent into the SIEM include the logs from external access points such as remote machines, server logs, and things like terminal services and Citrix, as well as application logging. This is what happened during the lockdown: organisations that previously only had a fraction of their workforce generating remote access logs and such now found themselves with an exponentially larger stream of logs feeding into their SIEMs.

Nor did this digital transformation happen in a gradual way, allowing for security procedures to be gradually implemented. Instead, it rapidly crushed our external user capabilities. Even companies like Microsoft and network providers are running into issues with so many changes taking place at the same time.

Organisations' mode of working isn't the only thing that was transformed rapidly. Privacy laws have continued to be refined to include certain logs in the definition of personal data. By virtue of being personal data, these logs must be kept encrypted and secured.

Centralised management

The concept of log management is often overlooked or unknown. Recently, many organisations simply stashed their logs into their SIEM and considered the job done, which has now been made impossible by the dramatic increase in the volume of logs to be collected.

To address the problem, organisations should consider implementing a centralised log management solution (CLM), which consolidates all the log data and pushes it to one, central data highway. This data highway will collect all the logs and direct them wherever they need to go. Essentially, a CLM is a product designed to make companies' lives easier and reduce their SIEM costs, as SIEMs are not effective log management tools.

"Using a CLM would lift the burden of having to hire the staff, provide the training and the support for the deployment and the operation of a SIEM. Furthermore, it would reduce the costs that organisations would incur with their SIEM providers"

Dropping all logs into a SIEM means that these are sometimes fragmented or incomplete, thus impacting security monitoring and incident response. Using a CLM would lift the burden of having to hire the staff, provide the training and the support for the deployment and the operation of a SIEM. Furthermore, it would reduce the costs that organisations would incur with their SIEM providers, as well as the risk of endangering the

SIEM infrastructure by storing unmanaged logs.

Fragmented data collection becomes unified data collection. If your SIEM infrastructure was at risk due to the huge volume of data, now you can reduce the costs by filtering that data and delivering only what you need. This can also help with overcoming the age-old strategy of letting IT teams have their own source of data, which could instead be directed to the appropriate team via the data highway that is a CLM.

Cleaning up the data

Once logged, the data then needs to be parsed. Parsing is the process of analysing a string of data or pulling specific items out. In computing, we use parsing to build a structure for the data that we want. In this way, there are a few neat things that can be done to help security teams during this digital transformation.

Before you get to parsing out the specific items you want, let's filter out the excess. The first way in which filtering can really help a company is by using this concept to remove unnecessary and unwanted information from the logs that are sent to the SIEM. That sounds a little weird, right? With parsing, it is possible to take a log and remove superfluous information, rewriting it on the fly to diminish the storage space it will take up and increase the usability of the data.

What kind of information is superfluous? One example is the timed mark that many applications add into the log of their system to show they are online. If this type of information isn't something that a security auditor will need to see, then there is no reason why an organisation should be paying to store it in its SIEM. In fact, what about filtering out all the extraneous text that ends up in the log, or going the extra mile and adding parsing for specific events from your logs? As you can see, this could quickly and easily reduce the costs that are likely spiralling out of control during this time.

"Parsing, filtering, masking and other transformation techniques in a CLM will also allow security teams to overcome the privacy issues of log management and filter out personal information that shouldn't be distributed"

Parsing, filtering, masking and other transformation techniques in a CLM will also allow security teams to overcome the privacy issues of log management and filter out personal information that shouldn't be distributed. Specific personal data can be matched to a pattern and removed before the log is sent to the SIEM. This data can also be masked or de-identified. Resolving this problem could become crucial as more and more personal data is being collected than ever before, and as privacy laws are becoming stricter.

Efficient team

While not as important to the digital transformation in many ways, always remember that not everyone that is going to be reviewing logs will be utilising the SIEM or be highly skilled as a Linux or Unix administrator (or even be one at all). Or they just might like to have a graphical user interface.

Know that the team that will have to be able to easily operate your new data highway before selecting one, because you don't want it to become an ornament on a shelf: your team must be able to use it.

Build the data highway

So, in this crush of new technologies spiralling into the new digital transformation age, don't forget the importance of effective log management. You can optimise the SIEM and increase the likelihood of meeting compliance requirements. It's possible to log from more places, and easily search them. With that encrypted data store, the compliance officer may even be able to sleep at night. And beyond the SIEM, it's possible to then send data anywhere, including things like: Kafka, MongoDB, any database, big data systems, or anywhere else you can think of. Don't just optimise your SIEM, build that data highway, collect those logs once, distribute them where they need to go, and cut costs with centralised log management.

Security teams don't have to be put in the position where they have to go to the company's management to say that they have uncontrolled SIEM costs. They can be managed and reduced without losing their effectiveness by simply feeding to the SIEM only the data that needs to be there.

About the author

Robert Meyers is a compliance and privacy professional, as well as the channel programme solutions architect for One Identity. He is a 30-year veteran of the identity and access systems and information security industry, including mergers and acquisitions, and with more than 10 years of that time focused on planning, supporting and managing privacy programmes such as FERPA, HIPAA, the GDPR and CCPA. His experience also includes leadership responsibilities for nearly 100 mergers and acquisitions. Meyers regularly speaks at events about privacy topics. His extensive certifications include IAPP Fellow of Information Privacy, CIPP/E, CIPT and the ISACA CISM and CDPSE.

The Firewall

Remote working reset now required

Colin Tankard, Digital Pathways

It has been impressive to see how businesses and their IT teams have been able to swiftly switch staff to remote working during the pandemic lockdown. It has demonstrated that organisations are resilient and, by and large, have effective business continuity plans. It also brings into question whether businesses need to maintain a disaster recovery (DR) or secondary office, should the primary office be rendered unusable.

A consequence, however, of the unplanned move to home working has been the loss of control as to exactly where data is, making a data breach much harder to deal with.

Often, boards of directors forget the myriad of work that IT has to deal with in the case of a breach. Customers calling to ask if their data is affected, the resourcing of an investigative team and dealing with external parties such as the Information Commissioner's Office (ICO). And of course, dealing with the fallout of legal actions, which are becoming far more prevalent. If data is scattered, multiply this effort by ten, and you will start to see the ever-growing issue of uncontrolled data.

What needs to happen is to bring the end-user into the equation, installing tools that search out data, wherever it has been 'hidden'. Giving data owners the ability to remediate on sensitive data is the fastest, and possibly only, way to deal with the problem.

For solutions to be attractive, they need to work with the people who own the data, wherever it may be – Office 365, endpoints, network drives, or even in spaces such as Dropbox.

The latest systems alert end users when sensitive data is found on their machines or within their cloud repositories. They will take them, at the click of a button, to where that sensitive data is, allowing them to obfuscate, delete or make decisions around that data, based on policy and education, which is within the system. This self-help process follows the user so that they can understand the actions to take and report back, once the process is completed.

Thereafter, all a system security analyst needs to do is to confirm that data has been found, remediation has taken place and the risk has been mitigated. This can then be a bona fide line of report back to the board.

Sensitive data discovery, particularly on endpoints, needs to be elegant, simple to deploy and use, and accessible to everyone. Large IT departments or IT-literate personnel are not a prerequisite to be able to use these solutions.

Organisations may also consider virtual desktop infrastructures (VDI), which enable control of data handling. Such systems eliminate the need to have costly laptops and reduce support issues surrounding remote workers. VDI systems are highly flexible and can scale very quickly, so there is no need to pay for full capacity until it is needed. This controls costs, offering a quick return on investment (ROI) and enables organisations to maintain data security standards to the same level as when staff were office-based and on corporate networks. It also gives the business agility, by making onboarding new systems or processes simple, enhancing the support they are giving to their remote staff.

It only takes one subject access request to hit the headlines for the flood gates of data breach investigations to open. Now is the time to get back in control of data, educate users in new ways of working, and use the latest technology to keep the organisation compliant and the board safe from prosecution.

EVENTS CALENDAR

Due to the Covid-19 pandemic, many conferences are being cancelled, postponed or converted into virtual events. The events listed here were still planned to proceed at the time of publication.

10–11 November 2020
DACHsec
Virtual conference
https://dach.cyberseries.io

18 November 2020
European Interdisciplinary Cybersecurity Conference
Rennes, France
www.fvv.um.si/eicc2020/

19 November 2020
Cyber Security & Data Protection Summit
Virtual conference
https://cybersecuritysummit.co.uk

25–27 November 2020
InfoSek
Nova Gorica, Slovenia
www.infosek.net

2–3 December 2020
Legal Cyber Security Expo
London, UK
https://bit.ly/3jA5Rd8

7–10 December 2020
Black Hat Europe
Virtual conference
https://bit.ly/32g0Pw7

14–16 December 2020
19th International Conference on Cryptology and Network Security
Virtual conference
https://bit.ly/3lf5Ds9

11–14 January 2021
FloCon
Virtual conference
https://bit.ly/2F0WyUm