

network SECURITY

ISSN 1353-4858 October 2021

www.markallengroup.com/brands/network-security

Iran-based hackers target defence, aerospace and telco firms, but Russia still biggest threat

Two new reports have highlighted the threats posed by state-backed hacking groups based in Iran. However, Russia still represents the greatest threat to organisations' security.

US security firm Cybereason has released details of what it calls 'Operation Ghostshell', a cyber espionage campaign targeting aerospace and telecommunications industries, primarily in the Middle East. The attacks use a previously undocumented and very stealthy reverse access trojan (RAT) called ShellClient that wasn't detected until July 2021.

"The ShellClient RAT has been under ongoing development since at least 2018, with several iterations that introduced new functionalities, while it evaded anti-virus tools and managed to remain undetected and publicly unknown," Cybereason says in its report.

According to Cybereason, the attacks are being carried out by a newly identified group based in Iran, which the firm has called MalKamak. "Our research points out possible connections to other Iranian state-sponsored APT threat actors such as Chafer APT [aka APT39 and Remix Kitten] and Agrius APT," says the firm. "However, we assess that MalKamak has distinct features that separate it from the other Iranian groups."

The ShellClient RAT has evolved over time, from a simple reverse shell to what Cybereason describes as, "a stealthy modular espionage tool".

The most recent versions of ShellClient have been exploiting Dropbox for their command and control channels, making it hard to detect. The malware drops 'cold' files into remote Dropbox folders using the

cloud service's API and an embedded API key. The data is encrypted with a hard-coded AES key. ShellClient is able to run with system privileges and can perform lateral movement across networks. Stolen files are compressed with WinRAR before being exfiltrated. While most of the threat actor's activities have been against organisations in the Middle East, Cybereason also logged attacks against targets in the US, Russia and Europe.

The Cybereason report is here: <https://bit.ly/2YDq0tz>.

Researchers at Microsoft have warned of Iran-based hackers using password spraying in an attempt to break into defence organisations in the US, Israel and the Middle East. It's believed that the attackers are attempting to steal intellectual property and there has been a focus on organisations producing military-grade radar systems, drone technology, satellite systems and emergency response communication solutions.

The group – identified as DEV-0343 by Microsoft – has tried to brute force its way into at least 250 Office 365 accounts, "with a focus on US and Israeli defence technology companies, Persian Gulf ports of entry, or global maritime transportation companies with business presence in the Middle East".

Microsoft goes on to say: "This activity likely supports the national interests of the Islamic Republic of Iran based on pattern-of-life analysis, extensive crossover in geographic and sectoral targeting with Iranian actors, and alignment of techniques and targets with another actor originating in Iran. Microsoft assesses this targeting supports Iranian government tracking of adver-

Continued on page 2...

Contents

NEWS

Iran-based hackers target defence, aerospace and telco firms, but Russia still biggest threat	1
Major telecoms firm hacked for five years	3

FEATURES

A network with nowhere to hide	7
Industry-standard tools and processes do a reasonable job of finding garden-variety attacks, but they break down in the face of targeted attackers who are aware of modern defensive techniques. For those who are targets for this type of breach, a new strategy is necessary, explains Alex Kirk of Corelight.	

CISOs should work closely with their ITAM colleagues	9
---	---

While traditionally referred to as the department that 'counts computers', ITAM has an important role to play in cyber security. In fact, security will become one of the most important areas for ITAM development by the end of the decade. Martin Thompson of the ITAM Forum explains why.

How financial services firms can mitigate the next wave of attacks	12
---	----

As criminals seek to take advantage of the recent chaos, cyber security strategy and practices have never been more important or front of mind for those operating in the financial sector. But, says Max Locatelli of Infoblox, in order to make investments count, organisations need to look for the tools and training that will set them up for success tomorrow.

The future of security in a remote-work environment	15
--	----

The new model of hybrid and remote work that companies worldwide are set to adopt will bring with it an array of challenges. To address both the problems we face today and the ones that lie ahead, believes Jason Sabin of DigiCert, companies need to prioritise a robust digital infrastructure.

Shining a light on organisational risk	18
---	----

When we consider how to rein in and limit nefarious activity on organisational networks, it helps to think like the individuals behind the attacks. Graph technology helps you accurately assess your risk and informs you where you need to improve defences, says Amy Hodler of Neo4j.

REGULARS

ThreatWatch	3
Report Analysis	4
News in brief	5
Threat Intelligence	6
The Firewall	20
Events	20

Photocopying

Editor: Steve Mansfield-Devine
Email: smd@contrarisk.com

Managing Director: Jon Benson
Group Content Director: Graham Johnson
Executive Director Digital Resources: Matthew Cianfarani
Subscription Director: Sally Boettcher
Circulation Manager: Chris Jones
Production Manager: Nicki McKenna
Chief Executive Officer: Ben Allen
Chairman: Mark Allen

MA Business

Part of

Mark Allen

Network Security is published by MA Business Limited
 Hawley Mill, Hawley Road,
 Dartford, Kent DA2 7TJ, UK
 Tel: +44 (0)1322 221144
 Website: www.markallengroup.com/brands/network-security

Subscription enquiries

UK: 0800 137201

Overseas: +44 (0)1722 716997

Email: institutions@markallengroup.com

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.

Permissions may be sought through the following channels: in the USA, through the Copyright Clearance Center, Inc, Marketplace website at <https://marketplace.copyright.com> and in the UK, via Publishers' Licensing Service Ltd at <https://plsclear.com/>. Other countries may have a local reprographic rights agency for payments.

Derivative Works

Subscribers may reproduce tables of contents or prepare lists of articles including abstracts for internal circulation within their institutions. Permission of the Publisher is required for resale or distribution outside the institution. Permission of the Publisher is required for all other derivative works, including compilations and translations.

Electronic Storage or Usage

Permission of the Publisher is required to store or use electronically any material contained in this publication, including any article or part of an article. Except as outlined above, no part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without prior written permission of the Publisher. Address permissions requests to the copyright agencies listed above.

Notice

No responsibility is assumed by the Publisher for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in the material herein. Because of rapid advances in the medical sciences, in particular, independent verification of diagnoses and drug dosages should be made. Although all advertising material is expected to conform to ethical (medical) standards, inclusion in this publication does not constitute a guarantee or endorsement of the quality or value of such product or of the claims made of it by its manufacturer.

Following the acquisition of *Network Security* by MA Business Ltd from Elsevier Limited, on 14th June 2021, MA Business Ltd is now the data controller of personal data in respect of *Network Security* and will process personal data in accordance with its Privacy Policy - please visit <https://privacypolicy.markallengroup.com> to understand how we process, use & safeguard your data and to update your contact preferences. Please note that there may be a delay with updating the website to reflect this change.

For a press release on the purchase, please visit <https://markallengroup.com/our-news/>

Digitally Produced by Mayfield Press
 (Oxford) Limited

12987

... *Continued from front page*

sary security services and maritime shipping in the Middle East to enhance their contingency plans. Gaining access to commercial satellite imagery and proprietary shipping plans and logs could help Iran compensate for its developing satellite program. Given Iran's past cyber and military attacks against shipping and maritime targets, Microsoft believes this activity increases the risk to companies in these sectors."

The password spraying activities emulate a Firefox browser and originate from IPs on a Tor proxy network. The attacks usually target from dozens to hundreds of accounts within each organisation, enumerating each account as many as thousands of times. Generally, from 150 to more than 1,000 unique Tor proxy IP addresses are used against each organisation. This allows the attackers to mask failed attempts by constantly switching the apparent origin of the login attempts. Fewer than 20 targets have actually been compromised, says Microsoft.

Microsoft recommends enabling multi-factor authentication for Office 365 accounts and to switch to passwordless authentication methods, as well as blocking all incoming traffic from anonymisation services such as Tor, if possible.

Microsoft's report is here: <https://bit.ly/3aqUXDz>.

In a separate report, Microsoft singled out Russia as the greatest online threat. Its 'Digital Defense Report' says that 58% of nation-state attacks in the past year have emanated from that country. And those threat actors are becoming better, achieving a 32% successful compromise rate, compared to 21% the year before.

"Russian nation-state actors are increasingly targeting government agencies for intelligence gathering, which jumped from 3% of their targets a year ago to 53% – largely agencies involved in foreign policy, national security or defence," said Microsoft in a blog post to accompany the report. "The top three countries targeted by Russian nation-state actors were the United States, Ukraine and the UK."

The most active threat actor in Russia is the one tracked by Microsoft as Nobelium (and by others as APT29, Cozy Bear etc). It's responsible for 92% of the notifications Microsoft has sent to customers about Russian-based attacks in the past year.

"Over the past year, Russia-based activity groups have solidified their position as acute threats to the global digital ecosystem by demonstrating adaptability, persistence, a willingness to exploit trusted technical relationships and a facility with anonymisation and open-source tools that makes them increasingly difficult to detect and attribute," says the report. "They have also shown a high tolerance for collateral damage, which leaves anyone with connections to targets of interest vulnerable to opportunistic targeting."

In a recent talk at the Chatham House think tank, Lindy Cameron, chief executive of the UK's National Cyber Security Centre (NCSC), underlined the threat from Russia. "Cyber criminals based in Russia and neighbouring countries are responsible for most of the devastating ransomware attacks against UK targets," she pointed out.

Aside from Russia, Microsoft identifies North Korea, Iran and China as the major threats – so no surprise there. China accounted for less than 10% of state-backed hacking attempts, although it achieved a success rate of 44%.

Microsoft also notes rising activity by groups based in Turkey and Vietnam, although they are currently at a low volume. According to Thailand's CERT, APT32, which operates from Vietnam, has targeted human rights and civil organisations as well as, "foreign corporations with a vested interest in Vietnam's manufacturing, consumer products, and hospitality sectors". Turkish groups have been seen attacking telcos in the Middle East and Balkans.

The report is here: <https://bit.ly/3iTGNZD>.

Meanwhile, the European Union has officially blamed a Russian hacking organisation dubbed Ghostwriter for attacks against EU officials, journalists and the general public.

"These malicious cyber activities are targeting numerous members of parliaments, government officials, politicians, and members of the press and civil society in the EU by accessing computer systems and personal accounts and stealing data," European Council officials said.

German authorities have linked the Ghostwriter group to Russia's military

Threatwatch

Vidar gets social

The Vidar information stealer malware has been adapted so that it now uses the decentralised Mastodon social media network as its command and control (C2) channel. Vidar has been around since late 2018 and sells for as little as \$150 on underground forums. It is capable of stealing browser data (including passwords, cookies, history and payment card details), crypto-currency wallets, files, Telegram credentials and more. By using the trusted Mastodon platform as a C2 mechanism, the malware can evade many traffic monitoring systems. Cyberint, the security firm that discovered this technique, said that each C2 account it found had 500-1,500 campaign IDs. There's more information here: <https://bit.ly/3lv9lkq>.

Malware targets Linux

Security firm ESET has identified a new rootkit that targets Linux servers and has been heavily deployed in Southeast Asia. Dubbed FontOnLake, the sophisticated malware has been continuously updated, suggesting that it's under active development. Early samples were seen as far back as May 2020. The rootkit has a wide range of capabilities: in addition to providing remote access to its operators it can also steal credentials and operate as a proxy server. "The sneaky nature of FontOnLake's tools in combination with advanced design and low

prevalence suggest that they are used in targeted attacks," ESET said. "To collect data or conduct other malicious activity, this malware family uses modified legitimate binaries that are adjusted to load further components." There's more information here: <https://bit.ly/3awMfUk>.

Windows 10 rootkit

A new Windows 10 rootkit is being deployed by Chinese-speaking threat actors and has been used to attack Southeast Asian government organisations and telecoms firms for the past year, according to research by Kaspersky. The threat group, named GhostEmperor by Kaspersky, has used the Demodex rootkit to gain and maintain access to servers. "To bypass the Windows Driver Signature Enforcement mechanism, GhostEmperor uses a loading scheme involving a component of an open-source project named 'Cheat Engine'," said Kaspersky. "This advanced toolset is unique and Kaspersky researchers see no similarity to already known threat actors." There are full technical details available here (PDF): <https://bit.ly/3IARGrm>.

FoggyWeb attacks AD

The Nobelium threat group, which is linked to Russia's SVR intelligence agency, is using a new malware tool that can create a backdoor in Active Directory and steal credentials, warns

Microsoft. The FoggyWeb malware targets Microsoft Active Directory Federation Services (AD FS) servers. As well as stealing logins, it's capable of exfiltrating configuration databases, decrypted token-signing and token-decryption certificates. It can also download additional components to set up a permanent backdoor to enable attacks against the wider network. Because FoggyWeb is loaded into the same application domain as the AD FS managed code, it gains programmatic access to the legitimate AD FS classes, methods, properties, fields, objects and components that are subsequently leveraged by FoggyWeb to facilitate its malicious operations," said Microsoft. There's more information here: <https://bit.ly/3v2Mj7I>.

Backdoored since 2012

A UEFI bootkit has been exploited by threat actors to create backdoors in Windows systems since 2012, according to researchers at ESET. By loading at boot time, before the operating system, such bootkits can maintain persistence on systems and are hard to detect and remove. The ESPecter bootkit identified by ESET loads its own unsigned driver to bypass Windows Driver Signature Enforcement. "Interestingly, we traced the roots of this threat back to at least 2012, previously operating as a bootkit for systems with legacy BIOSes," the firm said. There's more here: <https://bit.ly/3awpv6Q>.

intelligence agency, generally known in the West as the GRU. This followed an attempt to steal the login credentials of German politicians just before the September federal elections.

The attacks and other activities by Ghostwriter are believed to be part of a wider disinformation and information manipulation campaign.

Finally, Positive Technologies says it has identified a new threat actor that is probably government-backed, although it's unable to say from which country it's operating. Dubbed ChamelGang, it has targeted fuel, energy and aviation production industries in Russia, the US, India, Nepal, Taiwan and Japan.

"To achieve their goal, the attackers used a trending penetration method – supply chain," the researchers said about one particular attack they investigated. "The group compromised a subsidiary and penetrated the target company's network through it." There's more information here: <https://bit.ly/3FEHZQP>.

Major telecoms firm hacked for five years

Syniverse, a firm that provides connectivity services to many of the biggest telecommunications companies worldwide, has discovered that hackers have been in its operational technology (OT) and IT networks for at least the past five years.

The admission came in the company's latest filing with the US Securities and Exchange Commission (SEC).

"The results of the investigation revealed that the unauthorised access began in May 2016," the company wrote in the SEC filing. "Syniverse's investigation revealed that the individual or organisation gained unauthorised access to databases within its network on several occasions and that login information allowing access to or from its Electronic Data Transfer ('EDT') environment was compromised for approximately 235 of its customers."

The firm went on to say: "Syniverse did not observe any evidence of intent to disrupt its operations or those of its customers and there was no attempt to monetise the unauthorised activity."

However, this may not be much comfort to its customers – or their customers. Syniverse provides connectivity for around 1,250 telecoms firms in 200 countries. These capabilities include text messaging routing for the likes of Vodafone, AT&T, T-Mobile, Verizon, China Mobile and many others. It processes more than 740 billion messages each year. The firm describes itself as "the world's most connected company" with a "secure global network [that] reaches almost every person and device on Earth."

The apparent lack of exploitation of the access by the attackers suggests that this is the work of a nation-state group that is probably more interested in stealing data (such as messages) than 'monetising' the breach.

An investigation is underway.

Report Analysis

Secureworks: State of the Threat



Threat actors of all kinds are more innovative than ever, and are also adept at taking working strategies and techniques and refining them further. These are among the takeaways of Secureworks' new report, which serves to confirm with data what most security practitioners already instinctively know.

The report is based on an analysis that Secureworks' Counter Threat Unit (CTU) carries out on trillions of security events each year. The incidents covered by this report took place over the year ending June 2021. It's certainly been an interesting time. As Barry Hensley, chief threat intelligence officer of Secureworks, writes in the report: "After the global uncertainties of 2020, I think we all hoped that 2021 would shape into a degree of normality. But when it comes to cyber security, that has not been the case. We started the year looking at the aftermath of SolarWinds, and we haven't looked back. From Hafnium to Colonial Pipeline to Kaseya, the headlines have kept coming all year long."

Ransomware continues to hog the headlines, not least because such attacks typically result in very public downtime. And with ransomware as a service operations using leak sites to further blackmail their victims, the whole process takes place in the public sphere. It's also a highly effective form of attack – from the perspective of the cyber criminals. The truth is that many victims pay the ransom, especially if their insurance will cover the cost. And while ransomware attackers have been known to target organisations that can least afford to

have downtime – such as those responsible for critical infrastructure – any business is a valid target.

"There are very few other threats that can cause total loss of business operations for an extended period of time," says the report. "Ransomware attacks are opportunistic – any organisation that is perceived to have money can be a target – and most attacks occur due to gaps in security controls."

In the period covered by the report, Secureworks saw an 8% rise in incident response engagements that involved ransomware. This is a modest increase compared with some other reports, and inevitably one has to wonder if some organisations are not invoking incident response plans but are dealing with the issue themselves – ie, by paying up.

There were notable developments in other areas too, says the report – some of them with less visibility. For one thing, 2021 saw a significant increase in the use of zero-day exploits. This is both puzzling and worrying, given the value of zero-days.

"Zero-day vulnerabilities in the wild used to be very rare, but Google Project Zero data showed that the number of zero-days exploited in 2021 had passed 2020's annual total of 25 by mid-2021," says the report. "By early August 2021 it stood at 37. Zero-day vulnerabilities typically take lots of time, resources and expertise to identify, and they're generally used sparingly to avoid detection. It's unclear what has fuelled the growth in identified zero-day exploits; it could be that we are all just getting better at detecting their usage, or it could be that threat groups – particularly state-sponsored and ransomware groups – have more resources at their disposal to buy or find them."

Of the groups mentioned, nation-state entities are the most likely purchasers of zero-days, given that they can sell for seven figures. But when they do buy them, intelligence agencies and police forces typically keep quiet about it, because keeping the vulnerabilities a secret is a large part of an exploit's value.

That said, the size of the problem

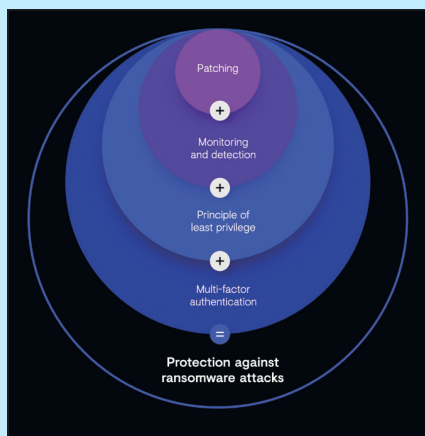
involving zero-days is entirely dwarfed by the ever-present issue of organisations being owned as the result of known but unpatched vulnerabilities. And Secureworks' data shows that this problem isn't abating at all – a depressing example of business as usual.

The same goes for other forms of cybercrime. Business email compromise (BEC) tends to get overshadowed by the ransomware plot, but it is nonetheless a growing part of the cybercrime world. Perhaps one reason this form of fraud doesn't get the attention it deserves is that it is relatively unsophisticated, often requiring little more in the way of technical capabilities than the ability to set up fake email accounts. Yet, according to the FBI, BEC resulted in losses of \$1.85bn in the US alone in 2020.

The Secureworks report also looks at nation-state attacks and, in particular, at the usual suspects – China, Iran, North Korea and Russia. Attacks by nation-state actors also largely come under the heading of 'business as usual'. However, we have seen some evolutionary developments. China's threat groups, for example, are getting better at managing their own operational security, says Secureworks, and are thus becoming harder to detect. Iran is focusing more heavily on Middle East targets, particularly journalists, academics, human rights defenders and governments, intergovernmental organisations (IGOs) and non-governmental organisations (NGOs). Russia still uses a mix of subtle espionage and blunt force, with the SolarWinds breach bringing it more attention than it probably wanted. And North Korea is becoming increasingly sophisticated, its main focus being revenue generation.

Secureworks also takes the time to examine the role of Cobalt Strike, a legitimate penetration-testing tool used by red teams everywhere. It is also, alas, becoming the go-to tool of malicious actors. It's fully featured, under active development, easy to use and good at hiding who is deploying it. Security tools continue to be a double-edged sword.

The report is available here: www.secureworks.com/resources/rp-state-of-the-threat-2021.



The key steps that organisations can take to defend themselves against ransomware. Source: Secureworks.

In brief

First ransomware fatality?

A woman in the US is suing a hospital over the death of her baby in what may prove to be the first case of a death caused by ransomware. Teiranni Kidd of Mobile, Alabama gave birth to her daughter Nicko at a time when the Springhill Memorial Hospital had many of its systems shut down by a ransomware attack. Nicko was born with the umbilical cord around her neck – something that might normally have been picked up by foetal heart rate monitors. But those monitors were out of action. Many of the hospital's computing systems were down for a total of eight days and staff were forced to use outdated paper-based systems. Kidd's lawsuit against the hospital claims that its management failed to take adequate remedial action and also failed to advise of the extent of the problems, robbing her of the opportunity to choose to have the birth at another facility.

US intelligence stolen

Reuters has reported that hackers from Russia's foreign intelligence agency, the SVR, succeeded in stealing sensitive counterintelligence information from US organisations as part of the SolarWinds attack. According to anonymous sources within the US Government's investigation into the attacks, the hackers were able to steal "information about counterintelligence investigations, policy on sanctioning Russian individuals and the country's response to COVID-19," said Reuters. The SVR was also able to obtain a signing certificate that enabled its malicious code to run on SolarWinds Orion platforms. Russia has denied responsibility for the attacks.

Too many tools

Staff in security operations centres (SOCs) have given up using many of the tools they have installed because of a lack of integration, too few trained staff to operate them, a lack of understanding of how they can be used in practical applications and the fact that many of them are out of date. According to research by Trend Micro, SOCs have an average of 29 monitoring solutions in place, but struggle to prioritise the alerts created by them. Just over half (51%) have abandoned at least some of the tools. And a fifth of those simply don't trust the tools to give them accurate and useful information. As a result, many organisations are looking to managed security offerings – some 92% have considered this option. "Not only do organisations have to pay for licensing and maintenance, but SOC teams are increasingly stressed to the point of burnout trying to manage multiple solutions," said Bharat Mistry, technical director (UK) at Trend Micro. "Being unable to prioritise alerts may also expose the organisation to breaches. It's no surprise that

many are turning to SOC-as-a-Service." The report is here: <https://bit.ly/3AxqjMA>.

Fake financial network taken down

Law enforcement and judicial authorities from Bulgaria, Cyprus, Germany, the Netherlands and Ukraine, supported by Europol and Eurojust, have broken up a gang operating a fake online trading platform for financial services. There were eight house searches in Kiev, Limassol and Sofia, with 17 individuals being questioned in Bulgaria and one "high value target" being arrested in Cyprus. The gang had lured German investors into making transactions worth a total of at least €15m, advertising financial services online and via social media. The group used more than 250 domain names and had connections with a company in Ukraine and a call centre in Bulgaria. The 100 or so employees of the two call centres contacted 'clients', acting as financial advisers, and pushed fake financial services in the field of binary options. Most of the employees were not aware that the company they were working for was involved in a fraud scheme. The investigation has so far led to 246 criminal proceedings across 15 German federal states.

Encrypted malware

Most malware is now being delivered via HTTPS-encrypted connections, according to an analysis by WatchGuard Threat Lab. Its latest quarterly report shows a massive increase in the use of encrypted connections, which reached 91.5% of all malware delivered. This means that any organisation that isn't inspecting encrypted traffic is missing most malware. Malicious code is also increasingly making use of PowerShell tools to bypass defences, says WatchGuard. And it found alarming surges in fileless malware threats, a dramatic growth in ransomware and a big increase in network attacks – the latter in spite of the move to remote working. Network attacks rose by 22% over the previous quarter and reached the highest volume since early 2018. The report is here: <https://bit.ly/3ADv2mC>.

Massive Android malware campaign

A malware campaign has infected as many as 10 million Android devices in more than 70 countries, according to research by Zimperium zLabs. The GriftHorse trojan is hidden in more than 200 apps that were uploaded to Google's Play store and third-party app stores. The malware uses alerts offering gifts and prizes to trick victims into subscribing to premium SMS services, and has potentially earned the criminals behind the malware hundreds of millions of dollars. In many cases, these are recurring fees. By trojanising so many apps across multiple categories, the GriftHorse operators were

able to evade detection for months. Zimperium said that the campaign has been running since at least November 2020. There's more information here: <https://bit.ly/3iTz1Wj>.

NSA warns about wildcards

The US National Security Agency (NSA) has issued guidance about the use of wildcard TLS certificates, saying that they can create security weaknesses. "Wildcard certificates are typically used to authenticate multiple servers to simplify management of an organisation's credentials, often saving time and money. Common uses include a proxy representing multiple servers. However, using wildcard certificates to validate unrelated servers across the organisation introduces risk," said the agency. The compromise of one server covered by a certificate effectively puts all others at risk. The NSA also gave details of the 'application layer protocols allowing cross-protocol attack' (Alpaca) technique that is capable of performing cookie theft and cross-site scripting attacks by exploiting weaknesses in one protocol to attack another. The advisory is here: <https://bit.ly/3Azj9OC>.

REvil scammed customers

The REvil ransomware as a service operation may have cheated its customers – the criminals who pay for and deploy the malware against victims. A number of security researchers have confirmed the suspicions of many cyber criminals who had been posting on underground forums about shady practices by REvil. It appears that the malware included a backdoor that allowed the REvil group to monitor ransomware infections and provide victims with decryption keys, effectively cutting the affiliates, who launched the attacks, out of the loop and denying them their 70% cut of the ransom.

Supply chain risk

Nearly all (93%) of global organisations suffered some kind of breach in the past year as a result of weaknesses in their supply chain. According to research by BlueVoyant, the average number of breaches in the past 12 months was 3.7, compared to 2.7 the previous year. The good news is that more companies are analysing the risk they face from third parties, such as suppliers – the portion of those not doing this dropped from 31% to just 13%. However, there has been an increase – from 31% to 38% – in the number of firms that admit to having no way of knowing if an incident has occurred in their supply chains. And while 91% of firms claimed that they are increasing security budgets to deal with these issues, there is little sign that this investment is paying off yet. There's more information here: <https://bit.ly/2YMQg5b>.



Warning: it's attack season

Tom McVey, Menlo Security

The UK calendar offers several yearly festivities and ample opportunity for celebration. Yet, unfortunately, a minority continue to view those events that are supposed to bring us together as an opportunity to exploit others.

Cybercrime tends to spike during seasonal events, for a few reasons. First, while some hackers operating in gangs work full time, many cyber criminals are often working relatively normal jobs and only running their attacks outside of these hours. As a result, when seasonal events come around, hackers – like the rest of us – may have additional time off work or enjoy bank holidays, providing them with more time to execute attacks.

Second, security may be diminished during these times for the same reason. Just as cyber criminals have time off, so too do cyber security professionals, reducing the ability of organisations to analyse, respond to and remediate attacks at such times.

And third, people expect to receive communications at Christmas, Easter and during other festivities. Because of these expectations, many people are more prone to letting their guard down and opening themselves up to phishing attacks.

A recent example of such a zeitgeist is the return of children to schools. Parents have received multiple emails on the topic of 'back to school', be it official communications from schools themselves or retailers sending out promotional offers to market their products at a period of higher market demand. Where people have become used to such communications, vigilance may have dropped, and cyber criminals are able to deploy attacks that are far more likely to go under the radar.

In terms of techniques, there is a variety of options that threat actors

may choose to use. They might opt for impersonating a school with fake emails, sending messages to individuals living in the local area, or impersonating official school websites, for example.

Equally, it was recently announced that children in the UK aged between 12 and 15 will be offered Covid-19 vaccinations. Here, attackers may pose as an official body asking parents to register their children for the jab via a malicious link.

It is worth noting that most of these attacks will target users' personal accounts over their professional accounts. Threat actors often target personal accounts as a means of more easily gaining access to professional endpoints or credentials, these often being the ultimate targets. And there is good reason for this. Personal devices are significantly less likely to deploy security software, for example, while at the same time housing critical information such as email addresses that can lead hackers to accessing an individual's work accounts.

Further, research by 1Kosmos revealed that almost half (48%) of employees use the same passwords in both their personal and work accounts, providing easy opportunity for lateral movement.

With this in mind, while seasonal attacks may at first appear to affect individuals mostly on a personal basis, organisations need to be aware that they are usually the end target. Taking steps to ensure better protection is, therefore, of paramount importance.

To achieve this, training is the first step. Poor password hygiene, such as the duplication of passwords between personal and professional accounts, is often the key that can unlock a treasure trove of applications and accounts for hackers. Therefore, organisations need to ensure that all individuals know that

this must not happen.

At the same time, however, companies should invest in key solutions capable of bolstering their overall security posture on all fronts. It is not enough to simply defend against email-based attacks. Rather, organisations must be aware of the variety of different threats and adopt solutions that can effectively deal with the entire roster.

Here, a cloud access security broker (CASB) is a highly useful tool. As a service capable of acting as an intermediary between users and cloud service providers, it can drastically improve overall IT visibility and control of a variety of SaaS applications, uncovering potential weak points such as employees using work devices to view personal emails.

Zero-trust policies can also provide some much-needed protection, achievable through isolation technologies. Isolation works by shifting the point of execution for active content away from a user's browser and into a disposable, cloud-based container, essentially acting as a screen that prevents all active content from reaching the endpoint. In other words, isolation can comprehensively prevent any web-based, email-based, or other form of attack on a user's machine.

This separates the enterprise network from public access, while also providing users with secure, low-latency connections to vital resources and SaaS applications. All content is rendered safely in a remote browser and therefore potentially malicious code does not have any opportunity to execute on the endpoint.

Through such solutions, organisations can move from a place of being 'almost safe' to preventing malware stemming from seasonal attacks from executing and stopping lateral movement holistically.

A network with nowhere to hide

Alex Kirk, Corelight



Alex Kirk

Supply chain compromises are at the top of every security professional's mind in the wake of the SolarWinds Sunburst breach.¹ The attackers behind that campaign were able to out-manoeuvre everything from point-in-time indicators of compromise (IOCs) to advanced heuristic algorithms, by thinking like a defender and crafting their malware to look like legitimate infrastructure.

While industry-standard tools and processes do a reasonable job of finding garden-variety attacks conducted at large scale across the Internet, they break down rapidly in the face of targeted attackers who are aware of modern defensive techniques. For those who are legitimate targets for this type of breach, a new strategy is necessary – one that allows defenders to outmanoeuvre adversaries. We'll discuss aspects of this new strategy as we review how the SolarWinds attackers so effectively compromised systems protected by current approaches to defence.

Defence in depth

Modern security architecture in large enterprises is often implemented as a 'defence in depth' strategy. Security operations centres (SOCs) layer multiple technologies, each of which specialises in a particular style of detection – IPS, email gateway, URL filter, etc – hoping to cover each of the different vectors by which malware can spread. In many cases, these systems come from disparate vendors, with no coherent linkage between the data each of them produces, or between the alerts they generate and the underlying system/network telemetry that lets analysts understand the impact of those alerts.

While technologies like security information and event management (SIEM), user entity and behaviour analytics (UEBA), AI/machine learning and extended detection and response (XDR) all attempt to take the data generated by this myriad of security devices and produce an understandable narrative of what is happening and whether it's bad, the giant

resulting compatibility matrix means that critical details that could feed advanced detections often slip through the cracks of vendor feature support. Alerts are missed, or are so difficult to track down that they are ignored altogether. Analysts are so busy with cumbersome workflows that they are hard-pressed to keep up, let alone have a chance to think strategically about outwitting attackers on the network.

Organisations should instead be pursuing a strategy that begins with a solid foundation of data – from the network and the endpoint – upon which intelligent detection and clean workflows can be built. Analytics of all types produce better results with better data inputs, and human analysts can be more productive and happier with their jobs with consistent access to the information they need in order to answer the questions necessary to keep up with advanced attackers.

Let's examine the status quo and how its problems can be solved through the lens of the details of the Sunburst attacks, focusing on what open network detection and response (NDR) providers do best – Layer 7-aware network-level detection. Note that we're choosing this angle in part because SolarWinds' best practices prior to the breach involved excluding its operations from endpoint security inspection and enforcement, a sadly common practice for mission-critical server software today.

Detection breakdown

First, we need to acknowledge that IOC-driven systems will inevitably fail against targeted attackers. It's simply too easy for them to stand up fresh infrastructure that

has never been seen by any security vendor and thus will never be on any sort of blacklist from even the industry's best vendors. While they have value against less-advanced attackers, they're largely moot for campaigns like Sunburst.

Broadly applicable anomaly detections also came up short with Sunburst, because the attackers were intelligent about how they designed their infrastructure. In-country servers hosted on Amazon Web Services (AWS) were used to make geolocation algorithms useless and hosting reputation scores look normal. Traffic was designed to use normal protocols in standards-compliant ways, so that detections like new ports or services or strange encryption algorithms for SSL did not fire, either.

So how did defenders stand a chance of detecting these attackers? Two possible techniques stood out in our work with impacted customers following the breach, both of which are made possible through a foundation of deep network telemetry that allows analysts to ask the right questions and get answers to them in real time.

Before we dive in, we should preface this by saying that both of these techniques involve understanding where your critical assets are, so that you can monitor them more closely than other devices. A startlingly high number of major enterprises had to spend days hunting down whether they had potentially impacted devices on their network. Given that SolarWinds devices announce themselves constantly over SNMP and through queries to subdomains of solarwinds.com – and that other critical servers are often just as obvious when you examine their traffic patterns closely – it's no wonder that leading vulnerability management vendors urge their customers to use both active and passive network data to create a complete picture of a network.

Paying attention to what your devices are already shouting across the wire is not only a great way to minimise the need for active scanning – which wastes bandwidth and generates alerts that your SOC has to work to suppress – but to ensure that you're not missing critical details because of 30-day windows between scans, the scan target being in a state that kept it from responding normally during a regularly scheduled scan, and so on.

Non-sanctioned servers

Going back to Sunburst, many of the DNS queries involved in the first stage of the command and control (C2) communications were made to non-enterprise sanctioned servers. These rogue DNS servers were located in AWS to help evade reputation-check-based detection, and used queries structured similarly to legitimate cloud-based infrastructure update tools to try to avoid analysis techniques focused on the queried names themselves.

For the large number of organisations that monitor DNS as it passes through their enterprise resolvers, queries like these are invisible, as they never pass through the monitored path. Tools like NetFlow or a next-generation firewall (NGFW) are often used to provide rogue query visibility – but only work when configured with a list of official enterprise resolvers to start with. Because many rogue DNS queries in the real world come from poorly programmed but ultimately benign devices, alerts generated by the network for out-of-policy DNS are typically set at ultra-low priority levels, often without any detail about what name was queried or the response that came back – which means that both human analysts and advanced algorithms often disregard them altogether, and are back at the mercy of their data normalisation process when they do try to look further.

In the context of a network where detections are built on top of a clear foundation of data, however, it becomes straightforward to operationalise alerts for rogue DNS – at least for critical assets that are the most likely to be involved in an advanced breach. With all of the query names directly available whenever a rogue DNS lookup occurs, an off-the-

shelf whitelist of known good domains can screen out enough traffic to allow for detailed analysis of the remaining queries. Using the answers to the remaining queries as a way to find the traffic those lookups generate, enough context can be automatically associated to those queries to let humans determine very rapidly if a query was benign and can be added to the whitelist going forward, or if it is suspicious enough to warrant the sort of manual investigation that was necessary to find Sunburst.

When discussing purpose-built, vendor-specific systems, SOCs can and should put the onus on those vendors to explain why such requests are legitimate and necessary – both to save their own time investigating and to help push vendors to make their devices behave better in the future.

Second angle

The second detection angle was equally simple in concept, but difficult to execute with a tool-layering strategy: tracking SSL connections made by SolarWinds devices to domains not on solarwinds.com. As with DNS, the attackers hosted their infrastructure in common places like AWS to keep away reputation-based detections, and used sufficiently clean domains to keep IOCs from triggering.

Nothing about the SSL server names they used was sufficient on its own to raise heuristic alerts – and because there is no pre-definable set of in-policy locations where SSL connections should ever be made, alerts for generic out-of-policy SSL connections were impossible to generate as well.

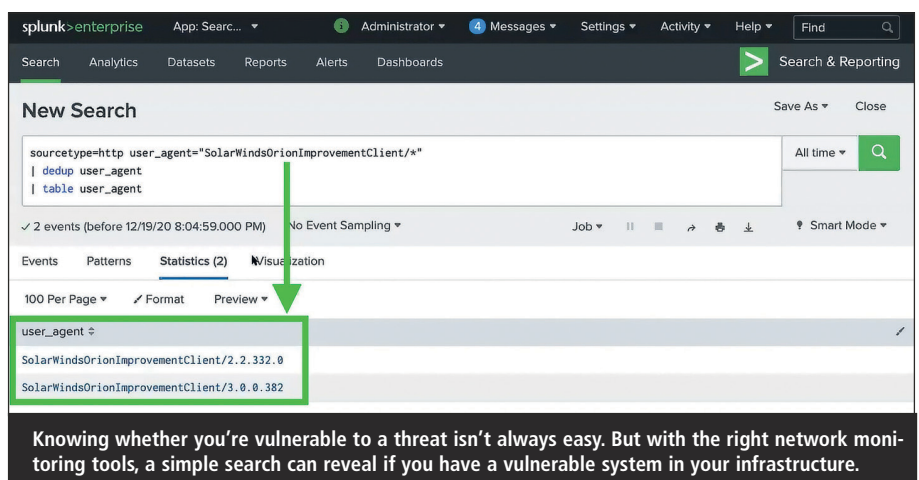
A detailed analysis, released just days after Sunburst was announced, showed how detailed data made detecting proxied SSL connections by SolarWinds devices to servers not hosted on solarwinds.com a single, easily automatable query.² While not all attacker SSL connections will go through proxies, as discussed there, an open NDR monitoring setup would still capture all of the SSL server names being connected to, and details about the resulting connections – making the problem nearly identical in scope to the DNS monitoring discussed above, with the added bonus that all computers make fewer SSL connections than DNS lookups.

Long-term strategy

While this and many other discussions around detecting advanced attackers focuses on actions that can yield results in the short term – often 30 days or less – the fact that the Sunburst attackers were on victim networks for over nine months speaks to the need to contemplate a strategy that spans much longer timeframes. One approach is the strategic data reserve (SDR), which builds on top of open source solutions for maximum utility.

The details of the SDR are quite simple: in addition to logging to an often capacity-limited (by performance and/or price) SIEM or analytics stack, a secondary copy of every movement observed on your network is sent to cold, inexpensive storage.

While jaded veterans of full PCAP projects might scoff at the idea of storing everything long-term, Zeek – an open-source monitoring tool – originally arose as a response to packet capture being too



The screenshot shows the Splunk Enterprise web interface. At the top, there's a navigation bar with 'splunk>enterprise' and various menu items like 'App. Search...', 'Administrator', 'Messages', 'Settings', 'Activity', and 'Help'. Below that, a 'New Search' window is open, displaying a search query: `sourcetype=http user_agent="SolarWindsOrionImprovementClient/*"`. The search results are shown in a table with two rows:

user_agent
SolarWindsOrionImprovementClient/2.2.332.0
SolarWindsOrionImprovementClient/3.0.0.382

A green box highlights the search query and the search results table. A green arrow points from the search query to the search results table. Below the table, there's a black banner with white text: "Knowing whether you're vulnerable to a threat isn't always easy. But with the right network monitoring tools, a simple search can reveal if you have a vulnerable system in your infrastructure."

voluminous to be practical for incident response.³ Between its focus on capturing everything relevant to security in as small a footprint as possible, and the compression bonus that comes from the inherent repetitiveness of network traffic, a year's worth of 5Gbps traffic sustained for 12 hours per day, 365 days per year comes out to a very manageable 15TB or so of data storage – which, given modern hard drive prices, is on the order of \$1,000 – a trivial amount for major enterprises.

This 'flight recorder black box' strategy provides two key outcomes against advanced attacks. The first is a solution to the all-too-common problem of baselining anomaly detection algorithms, where the realities of evaluating products and implementing them in production means that they often get to observe 30-60 days' worth of data – time during which an attacker might already be on your network. By contrast, UC Berkeley – birthplace of Zeek – has more than two decades of logs, which have produced award-winning research on topics like detecting credential spear-phishing attacks in enterprise settings.⁴

The second, yet much more likely outcome for most organisations, is ultra-efficient response when the next major breach of Sunburst's scope is announced. Since modern best practice for teams announc-

ing the discovery of a global malware campaign is to provide indicators of compromise – often in open source formats that the best kind of open NDR technology natively ingests – having a single, comprehensive data source means that analysts can run a single set of simple queries and immediately understand whether they were victimised, and if so, to what extent.⁵

Conclusion

Building a complete picture of your network that allows your defenders and their detection logic to manoeuvre across protocols, devices and time might seem like an insurmountable task – but is actually simpler to manage than modern defence-in-depth strategies, while giving organisations more flexibility in how they apply detections and greater efficiency as they investigate their alerts. More important, it's the only way defenders will be able to keep up with their extremely capable adversaries and stand a chance of catching the next Sunburst before it's too late.

About the author

Alex Kirk is an open source security veteran, with a combined 17 years at Sourcefire, Cisco, Tenable and now Corelight, where he serves as global principal for Suricata. Formerly a malware zookeeper and IDS

signature writer, today he spends his time helping SOC analysts and advising on security policy for government agencies, universities and large corporations around the world.

References

1. 'Highly evasive attacker leverages SolarWinds supply chain to compromise multiple global victims with Sunburst backdoor'. Mandiant/FireEye, 13 Dec 2020. Accessed Oct 2021. www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.
2. Reardon, Ben. 'Detecting Sunburst/Solarigate activity in retrospect with Zeek'. Corelight, 21 Dec 2020. Accessed Oct 2021. <https://corelight.com/blog/2020/12/22/detecting-sunburst-solarigate-activity-in-retrospect-with-zeek-a-practical-example>.
3. Zeek, home page. Accessed Oct 2021. <https://zeek.org/>.
4. 'Paper on detecting spearfishing awarded Facebook's Internet Defense Prize'. International Computer Science Institute. Accessed Oct 2021. www.icsi.berkeley.edu/icsi/news/2017/08/Internet-defense-prize.
5. 'Hunting for SolarWinds backdoors in Splunk with Zeek'. YouTube, 16 Mar 2021. Accessed Oct 2021. www.youtube.com/watch?v=uY10UynFqt0.

CISOs should work closely with their ITAM colleagues

Martin Thompson, The ITAM Forum

How many CISOs do you know that are proactively working with their IT asset management (ITAM) colleagues? In fact, how many CISOs have even heard of ITAM? While traditionally referred to as the department that 'counts computers', ITAM has an important and often overlooked role to play in cyber security. In fact, security will become one of the most important areas for ITAM development by the end of the decade. Let's see why.

If you're reading this, there is a chance you're not sure what ITAM is, or have never even heard of it. ITAM is the profession that helps organisations maximise the value of their IT assets, be that

software, hardware or IT services. At a practical level, ITAM incorporates multiple disciplines, from cost optimisation, to software licence compliance, to hardware re-use and recycling. ITAM profession-

als are among the few who routinely interact with almost everyone in the business – not just those in IT, but also procurement, finance, security, operations and even end users themselves. So, that's pretty much everyone in the organisation.

Senior levels

Originating as a back-office, operationally-focused team that maintained a data-



Martin Thompson

base of the organisation's IT assets (that is, counting computers), ITAM has grown significantly in importance and strategic value as the discipline itself has matured. ITAM has effectively pulled itself out of the basement and up to the more senior levels of the business. According to research conducted by the *ITAM Review* in 2018, more than one third (37%) of ITAM practitioners reported directly to the C-suite. This is compared with 45% reporting to more operationally-focused IT service management (ITSM) back in 2011.

This elevation of ITAM in a relatively short period of time has happened for a number of reasons:

- Digital transformation has elevated IT itself (and ITAM along with it) into a more strategic function within the business (if not *the* strategic function of many businesses today).
- With SaaS/cloud software, everyone has become an IT buyer, resulting in the need for ITAM to expand its reach significantly to remain effective and accountable.
- The continued expansion of vendor-led software audits combined with the pressures of shadow IT (see the last point) has made software compliance more difficult than ever, raising the real monetary costs of non-compliance and, inversely, raising the cost-saving potential of ITAM to the organisation.
- Then there's the growing realisation that ITAM is needed to support information security.

Foundational to security

The financial and reputational cost of a security failure is well known. In the UK for example, the Information Commissioner's Office (ICO) is coming down increasingly hard on security failures. British Airways was recently fined £20m for failing to protect the per-

sonal and financial details of more than 400,000 of its customers due to processing a significant amount of personal data without having adequate security measures in place.¹ Marriott Hotels received a similar fine of £18.4m for failing to keep its customers' data secure.²

IT asset management and information security are closely related, but historically, their roles have had limited co-operation and integration. As cyber security risks have grown, there is now a necessity for the ITAM and infosecurity functions to work together. This is because ITAM can help to bring visibility and control to such exposures in order to prevent them from happening in the first place – or at the very least, to mitigate their impact significantly.

While the key driver for many ITAM functions is managing costs and addressing contractual or regulatory risk, there is significant value in ITAM and infosecurity building a stronger partnership. This is demonstrated by the fact that two major sources of cyber security guidance put IT asset inventories or IT asset management as their top priority. These are the Center for Internet Security's CIS Controls and the US Government's Cybersecurity Framework.^{3,4}

Benefits of collaboration

The first benefit of collaboration is a foundational aspect of IT management – knowing what we have, who is using it, how it is configured and what it is being used for. NIST believes that: "ITAM enhances visibility for security analysts, which leads to better asset utilisation and security." It also sees ITAM as, "foundational to an effective cyber security strategy."⁵

The NIST guide outlines the following benefits of an ITAM system:

- Discovery of device location, configuration and ownership.

- Identification of most valuable assets.
- Meeting IT audit requirements (ie, SoX, PCI-DSS – not licence compliance audits).
- Inventory vs entitlement.
- Patching.
- Helpdesk response improvement.

In addition, ITAM can help certify the authenticity of both hardware and software to verify that it is what it claims to be and provide business intelligence on IT assets to support business continuity planning. Core competencies within ITAM teams include managing intellectual property rights and contracts and ensuring the legal use of software, asset acquisition through trusted sources, and the safe return or disposition of assets, all of which are typically on the radar of a CISO.

Similarly, the NIST cyber security framework puts 'identify' as a first foundational step: "To develop an organisational understanding to manage cyber security risk to systems, people, assets, data and capabilities."

Potential value

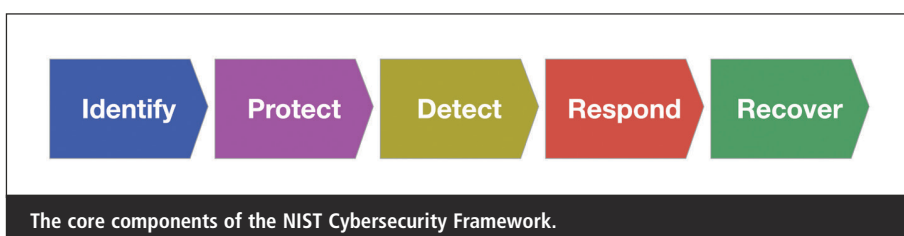
The practice of IT asset management is to treat an organisation's investment in IT as an asset, throughout its lifecycle, so that its potential value can be delivered as promised.

ITAM's role in security enhancement is typically achieved by focusing on the following areas:

- Shared inventory and discovery.
- Application lifecycle management shared with the information security function.
- Identity and access management.
- Hardware asset management (including hardware and software configuration management).
- Managing ephemeral assets (eg, containers, serverless computing and FaaS).
- Addressing code hygiene (especially with open source).

Additional reasons

The ITAM Forum has members across the world who are working to enhance the strategic value of ITAM within their



organisations. Many of them have their own, additional reasons for working with their cyber security colleagues.

According to Yvette Matthews of ITS Partners: “HAM (hardware asset management) and SAM (software asset management) policies reduce unplanned out-of-band hardware and software and help discover out-of-band items that sneak by. These items significantly increase the workload for security and the risk to the organisation. For example, an organisation that has removed Java for security reasons may no longer follow up on Java vulnerabilities, but a good SAM practice will help identify teams or individuals that have re-introduced Java into the organisation.”

“As cyber security risks have grown, there is now a necessity for the ITAM and infosecurity functions to work together. This is because ITAM can help to bring visibility and control to such exposures”

She adds: “A mature disposal practice will also ensure that hardware and software are removed from the environment once they are past their manageable life, greatly reducing unmanageable risk. For example, a model of laptop could be retired and fully removed before the vendor ends upgrade support. Without this programme, some devices may remain in use or be stored, and when returned to the network, they pose a threat that cannot be mitigated.

“Maintaining ownership records for hardware and software drastically reduces the time to contain an incident by providing the security operations centre (SOC) critical information during a breach.”

At-risk assets

George Arezina, global ITAM leader for an international business information services organisation, reiterates the security benefit of ITAM in retiring out-of-date, at-risk assets.

“From a security standpoint, the SAM team helps the information security risk management (ISRM) organisation

identify and counter potential threats by ensuring that end-of-life products get decommissioned, and that product updates and security patches are applied in a timely way,” he says. “In a recent potential security threat, the SAM team was able to quickly identify the deployments of the software in question along with the version. This helped to mitigate the risk. In collaboration, both ITAM and ISRM are working together in developing and maintaining software white and blacklists.”

Julia Veall, ITAM manager for an international telecommunications firm, engages with her security colleagues in a similar fashion. “We support security by managing a blocklist for risky software,” she says. “This could be simple unauthorised stuff but also software that has potentially other malicious uses. This can be used to track activity, be used in dismissal cases, or can be passed to relevant authorities.”

Rick Shepherd from Ray Allen shares a unique perspective on how ITAM is being deployed to manage software defined networks (SANs). “Enterprise businesses are rapidly evolving their internal IT networks to cloud-based software-defined network services,” he explains. “The convergence and/or migration of on-premise legacy hardware to cloud-based SDN solutions has created new complexities for managing the full estate of assets. Managing the various hardware and software configurations that span legacy and new technologies is why ITAM has become a fundamental requirement for cyber security.”

Helping yourself

Over the course of the past decade, IT asset management has been slowly rising out of the shadows. It deserves to become a de facto business practice within every organisation, in the same vein as other common disciplines such as marketing, HR, accounting and so on. ITAM is an essential prerequisite for a modern, digitally-enabled business, yet approximately one third of businesses still don't have a formal ITAM function. CISOs have a role to play in helping to grow the ITAM function within their own organisations – and to their benefit. CISOs should be

ITAM security checklist

IT asset management enhances security in a number of ways:

Identifying vulnerable applications:

By maintaining a database of every device and application in use across the organisation – and crucially the specific software version – ITAM can proactively identify vulnerable applications during its regular scans of the network.

Keeping software up to date: ITAM ensures that end-of-life products are decommissioned and that product updates and security patches are applied in a timely manner.

Identifying shadow IT: User-installed devices and cloud-based applications could pose an unknown security risk. If you don't know it's there, you can't protect yourself from it.

Supporting the swift resolution of a security breach: During a security breach, ITAM can quickly identify the deployments of the software in question, along with the specific version, to help mitigate the risk.

lobbying their CEOs to install ITAM functions within their businesses as a security priority.

About the author

Martin Thompson is the founder of The ITAM Forum (<https://itamf.org>), a non-profit, global trade body for the advancement of the IT asset management industry. He is also the owner and founder of The ITAM Review (www.itasset-management.net), an online resource for worldwide ITAM professionals, best known for its newsletter, LISA training platform, Excellence Awards and conferences in the UK, US and Australia.

References

1. ‘ICO fines British Airways £20m for data breach affecting more than 400,000 customers’. Information Commissioner's Office (ICO), 16 Oct 2020. Accessed Oct 2021. <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/>.
2. ‘ICO fines Marriott International Inc £18.4 million for failing to keep

customers' personal data secure'. Information Commissioner's Office (ICO), 30 Oct 2020. Accessed Oct 2021. <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-fail->

[ing-to-keep-customers-personal-data-secure/](https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-fail-).

3. 'CIS Controls'. Centre for Internet Security. Accessed Oct 2021. www.cisecurity.org/controls/.
4. 'Cybersecurity Framework'. National Institute of Standards and Technology

(NIST). Accessed Oct 2021. www.nist.gov/cyberframework.

5. 'IT Asset Management'. National Institute of Standards and Technology (NIST). Accessed Oct 2021. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-5>.

How financial services firms can mitigate the next wave of attacks



Max Locatelli

Max Locatelli, Infoblox

Every organisation operating in the world today is a potential victim of cyber-crime. However, financial services (FS) firms are a particularly tempting target for those looking to make a profit. This is neither a surprising nor a new concept. Throughout history, the FS sector has been relentlessly targeted by criminals, whether it's the traditional bank robbers of old or the hackers of today, stealing millions through phishing and ransomware attacks.

In fact, according to Boston Consulting Group's 'Global Wealth 2019: Reigniting Radical Growth' report, FS firms are up to 300 times more likely than other companies to be targeted by a cyber attack.¹ Meanwhile, Clearswift revealed in November that 62% of FS firms in the UK had suffered a cyber attack over the course of just 12 months.²

"Regional compliance regulations and laws as well as cyber security concerns relating specifically to the sector all make network security extremely complex. However, since the pandemic broke out last year, these challenges have increased ten-fold"

Thanks to the many layers of sensitive data and the huge financial sums they regularly handle, FS organisations have become one of the most high-value targets for hackers. This is something that is not likely to change anytime soon, with digital transformation and cloud adoption initia-

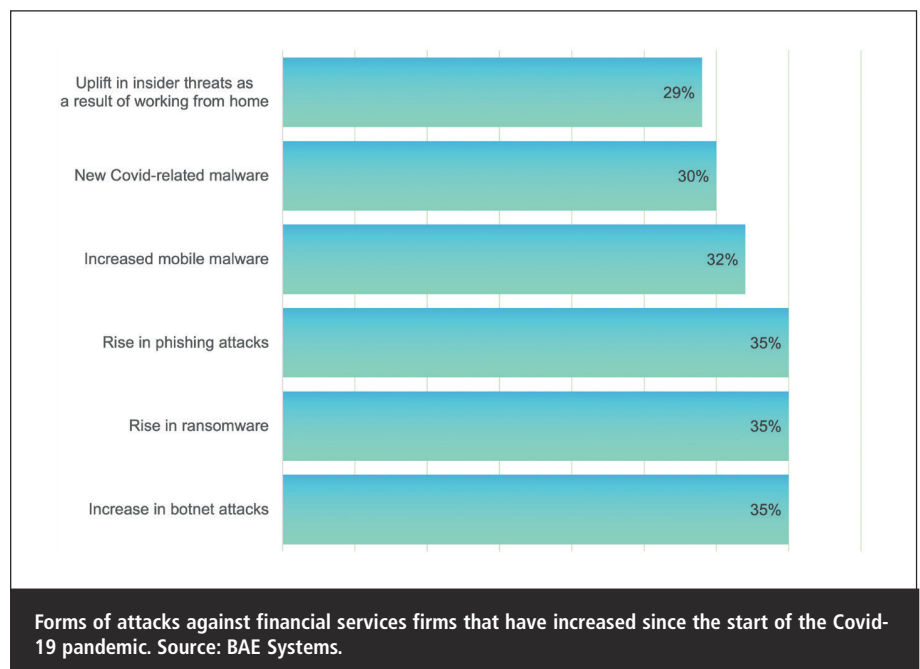
tives – both of which are necessary for survival in the current landscape – expanding the attack surface even further.

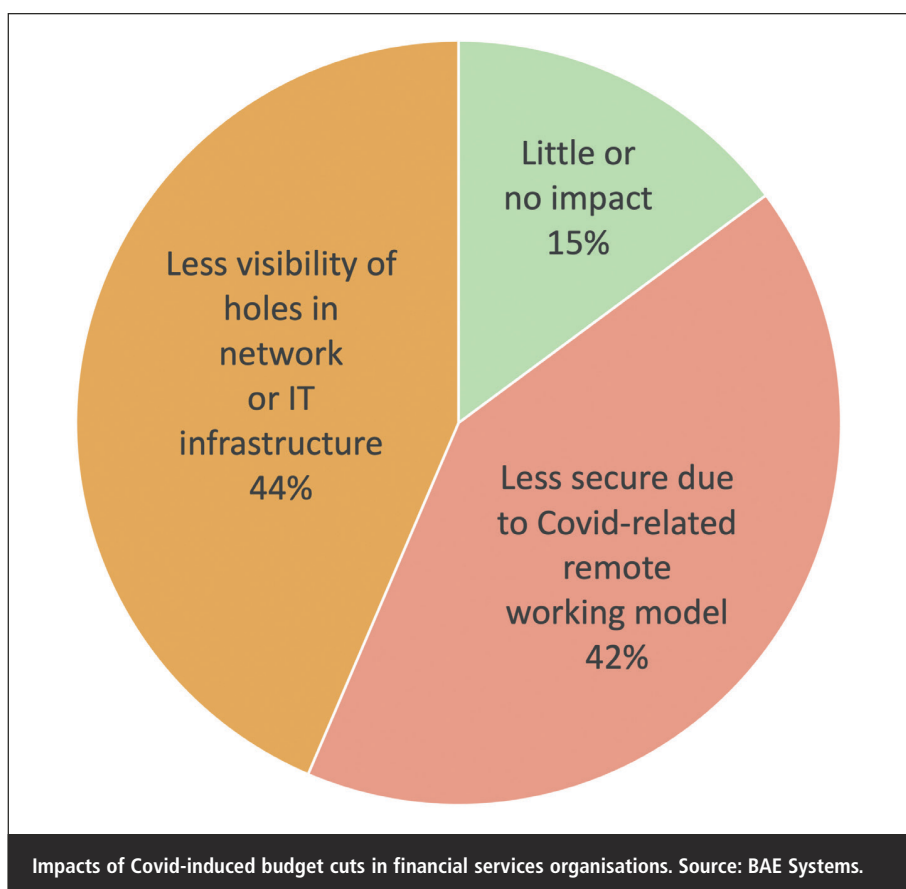
In order to avoid the potentially devastating cyber attacks and data breaches of tomorrow, FS organisations need to act

today. Failure to adapt to the landscape and adopt a proactive approach to cyber security could spell disaster long-term.

Challenging year

FS firms face a whole host of challenges when it comes to protecting their users' data from cyber criminals. Regional compliance regulations and laws as well as cyber security concerns relating specifically to the sector all make network security extremely complex. However, since the pandemic broke out last year, these challenges have increased ten-fold.





While many FS firms were already moving steadily towards the digitisation of services – in an effort to keep up with competitors and meet ever-growing customer expectations – the Covid-19 crisis undoubtedly accelerated these efforts. As office closures took hold and the majority of operations became virtual, many FS organisations were forced to embrace digital transformation at a rapid pace in order to continue to deliver their services and try to achieve some level of ‘business-as-usual’.

During this time, the digital attack surface expanded significantly. Individuals moving from centralised locations – ie, corporate campuses – to the edge of the network in homes brought greater risk. Not only were IT teams responsible for making sure staff were set up with the right equipment and systems, and that those systems were optimised for the cloud, but teams found themselves scrambling to make sure employees had basic security protections wherever they were located and whatever device they were using.

As many FS organisations found themselves at their most vulnerable, innovative cyber criminals were able to adapt rapidly and take advantage of the chaos to launch

multiple attacks. In fact, according to recent research, three-quarters (74%) of FS organisations have seen an increase in malicious activity since the beginning of the crisis.³ This increase has been primarily driven by threats to corporate systems and data such as mobile malware, phishing, botnet attacks, ransomware and insider threats.

“More than half of all firms (54%) reported being hit by data breaches during a 12-month period, while nearly half (49%) encountered cloud-based malware attacks”

A recent Cybersecurity Insight Report – released in May 2021 – broke down the increase in cybercrime to find out which types of attack have become most prevalent since the pandemic took hold and how FS organisations are responding.⁴ More than half of all firms (54%) reported being hit by data breaches during a 12-month period, while nearly half (49%) encountered cloud-based malware attacks. Cloud malware isn’t a new threat but has certainly become more prevalent

in recent months. Since it exists outside the enterprise network and beyond the firewall, many of the firms questioned said they were primarily concerned about the security and integrity of their data as they migrate to public and third-party clouds in the medium to long term.

Cost of a breach

For FS organisations, a single data breach can have far-reaching consequences. Depending on the severity of the attack, and how much and what type of data is impacted, some might never fully bounce back – whether that’s in monetary terms or related to reputation.

For example, one of the biggest data breaches in recent history involved US-based credit rating agency Equifax. In 2017, due to flaws in the company’s systems, 145 million people’s personal records were compromised by hackers. The breach was sizable but what really made it so alarming was the nature of the information stolen, ranging from full names and addresses to credit card information. Equifax subsequently revealed that costs relating to the incident, as well as expenditure on IT and data security, have reached at least \$1.35bn, excluding legal fees for lawsuits.⁵ The company’s former chief information officer has also been sentenced to four months in prison and handed a substantial fine for insider trading.

While this case is extreme, Equifax is far from being the only company to face severe financial repercussions following a breach. In fact, the Cybersecurity Insight Report discovered that, on average, FS firms that experienced a data breach reported an estimated loss of \$4.2m. Of course, this goes up if we take into account the unplanned network outages that often follow a breach or ransomware attack.

For FS organisations, any unplanned outages can seriously impact the bottom line. Even if an outage is due to a non-malicious interaction or perhaps a result of collateral damage from an attack on another company, the consequences can be the same as a targeted attack. For example, when a multi-tenant cloud server is taken down because someone from another company unintentionally introduced malware that impacted the server’s operat-

ing system, the resulting outage can be just as detrimental as a planned attack by malicious outsiders.

According to the same report, financial repercussions are the top impact of network outage attacks, with 60% of FS organisations agreeing. However, it's not just the initial cost that victims need to worry about. Almost half (45%) of respondents also highlighted the reputational damage caused by a breach. This can have a long-term impact, both on retaining current customers and the ability to win new ones. In today's ultra-connected, competitive landscape, it ultimately could be the difference between an FS organisation surviving and failing.

Proactive approach

FS firms must take this time to embrace a more strategic approach to security, rather than hanging on to a model that isn't compatible with the cloud-first networks that the new digital wave in remote work requires. Network architecture is no longer centralised on a physical campus, with a core datacentre into which users connect, and security practices need to reflect this.

“Almost half (45%) of respondents also highlighted the reputational damage caused by a breach. This can have a long-term impact, both on retaining current customers and the ability to win new ones”

In order to defend against the latest and most-sophisticated threats, FS organisations must use a full range of offensive and defensive tools and techniques. One such tool, which uses a centralised, cloud-managed provisioning management and control solution, is DDI – an integration of Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP) and IP address management (IPAM) into a unified service or solution. It is designed with the modern borderless enterprise in mind, to eliminate the management complexity and bottlenecks of the traditional branch office.

DDI augments visibility into network activities and increases control. It grants

visibility into networking activities, no matter where devices might be connected from – including remote locations. Some 90% of malware touches DNS – the first D in DDI – when entering or leaving the network, making DNS a critical detection tool that, when connected to the security stack, can enable stronger threat remediation. Additionally, DDI includes a software-defined perimeter that supports network identity and context for policy rules and their enforcement in security orchestration, automation and response (SOAR); security information and event management (SIEM); cloud access security brokers (CASBs); zero trust; next-generation firewalls and more. Ultimately, DDI enables the network team to quickly detect and fix any vulnerabilities, no matter where they originate.

Front of mind

The past year or so has presented many challenges for FS organisations to overcome – from the almost overnight switch to a remote working model to the accelerated digitisation of many services in an effort to meet customer needs and continue ‘business-as-usual’. As cyber criminals seek to take advantage of the chaos, cyber security strategy and practices have never been more important or front of mind for those operating in the sector. It's hardly surprising that the Cybersecurity Insight Report discovered that more than three quarters (77%) of respondents had increased spending on prevention in 2020. This isn't going to change any time soon, with 82% expecting their spending to rise again this year.

“It's no longer enough to solely promote centralised practices. Instead, cyber security needs to stretch across the entire infrastructure and protect users no matter where they are located”

But, in order to make these investments count, FS organisations need to look for the tools and training that will protect them today and also set them up for success tomorrow. It's no longer

enough to solely promote centralised practices. Instead, cyber security needs to stretch across the entire infrastructure and protect users no matter where they are located. Defending from the network edge will be critical moving forward and using modern technologies such as cloud-first DDI will enable FS organisations to stop and remediate attacks before they have the opportunity to cause significant damage and disruption.

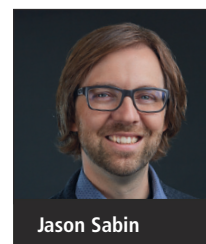
About the author

Currently the regional director for Western Europe (UK & Ireland) at Infoblox (www.infoblox.com), Max Locatelli is an internationally experienced sales and business leader in networking, video and telecommunications technologies. Prior to joining Infoblox in December 2019, he held a number of roles at Cisco, including client director for the Sky Group and director service provider, Italy. Before Cisco Locatelli held sales management roles at CompuServe (UK), MaxCom (US) and Olivetti (Italy).

References

1. ‘Reigniting Radical Growth’. Boston Consulting Group, 2019. Accessed Oct 2021. https://image-src.bcg.com/Images/BCG-Reigniting-Radical-Growth-June-2019_tcm9-222638.pdf.
2. ‘Cybersecurity Challenges in Financial Services - Market Survey Report’. Clearswift. Accessed Oct 2021. www.clearswift.com/cta/financial-services-cyber-security-report.
3. Viney, Simon. ‘The Covid Crime Index: A look at pandemic-related security and fraud trends’. BAE Systems, 29 Apr 2021. Accessed Oct 2021. www.baesystems.com/en-financialservices/insights/blog/the-covid-crime-index-2021.
4. ‘The CyberRisk Alliance Insight Report on the Global Financial Services Sector’. Infoblox, May 2021. Accessed Oct 2021. <https://info.infoblox.com/resources-whitepapers-cyber-risk-alliance-insight-report-on-the-global-financial-services-sector>.
5. ‘Equifax data breach: Ex-CIO to serve four months in prison for insider trading’. ITPro, 2 Jul 2019. Accessed Oct 2021. www.itpro.co.uk/data-breaches/29418/equifax-data-breach-cost-14-billion-so-far.

The future of security in a remote-work environment



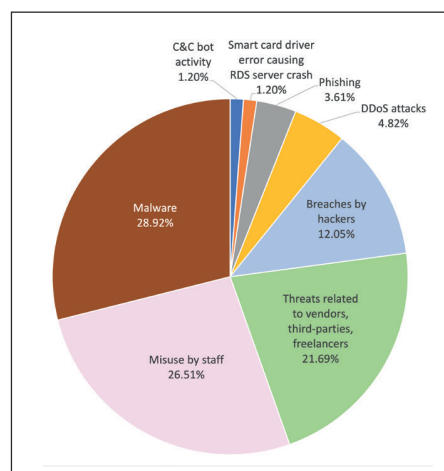
Jason Sabin

Jason Sabin, DigiCert

Cyber security threats were a concern before the Covid-19 pandemic. But a year after businesses and employees vacated office complexes, the risks of falling victim to a cyber attack have only grown. In an article published by the Journal of Medical Internet Research, researchers found that the number of cyber attacks increased by 500% throughout the pandemic, and by 2021 are on track to cost world businesses \$6tr annually.¹

Concerned about the toll that a hack could take on their own companies, global IT leaders have taken notice. Fudo Security conducted a survey showing that 42% of respondents said that Covid-19 had changed their cyber security priorities, and one in four said that their companies had already been victims of cyber attacks.² The surge in cybercrime has emphasised that businesses large and small need to take a proactive approach to protect their operations from the malware and ransomware attackers prowling the Internet.

“To address both the challenges we face today and the ones that lie ahead, companies need to prioritise a robust digital infrastructure that is built for the future of work”



What organisations see as the greatest remote access cyber security challenges. Source: Fudo Security

The new model of hybrid and remote work that companies worldwide are set to adopt will bring with it an array of challenges comparable to those of the earliest days of the pandemic. To address both the challenges we face today and the ones that lie ahead, companies need to prioritise a robust digital infrastructure that is built for the future of work.

The threats

To cope with cyber security threats, companies must first recognise them. And perhaps the most notable threats that have arisen during the Covid-19 pandemic have been related to remote work.

During the ongoing pandemic, Pew Research recorded a 51% increase in the number of people working from home, a total of 71% of all participants surveyed. In the same study, 54% of people said they would prefer to work from home going forward.³ Although this was not indicative of whether or not their companies would let them go remote or to what degree, it was indicative of the remote-work trend. Several security risks immediately are brought to the forefront as issues that companies should consider.

Creating a security-focused culture:

Human error is the biggest threat to information security that companies face, and it can come in many forms. An employee who connects to public wifi without using a VPN; someone's child who uses their parent's computer and visits unauthenticated sites; an employee who gets a phishing email after a long day and clicks on the link without thinking

twice – all are gateways to a data breach.

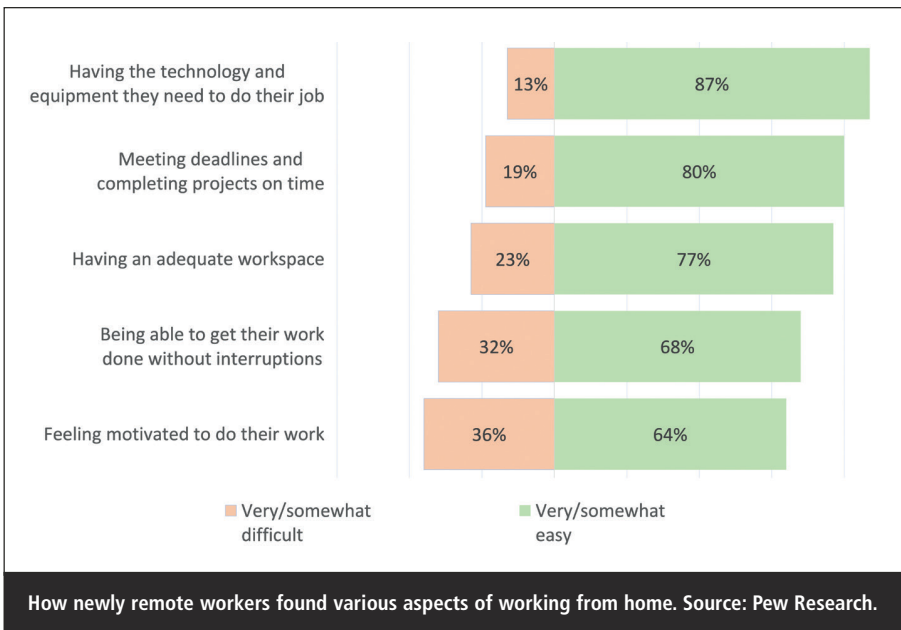
While no companies are 100% perfect, 100% of the time, one of the most proactive steps to take is to purposefully engage the entire workforce on where risks are the highest, what their common traits are, and the resources that they have available to them to protect themselves. Making sure that people understand the ramifications of a data breach is also important and why due diligence is the best weapon against attacks. Seminars and classes can also be helpful and can also be framed as helping employees protect their personal data.

Device and account security: It is commonplace for companies to issue laptops or tablets for work use, but often that technology does not cut it for employees when they work remotely. Many people access email on their phones, review documents on tablets, or use a more powerful desktop to get things done, even if it is company policy not to. This enhances the risk of password theft, ransomware or malware placement.

To combat the risks of remote device insecurity, companies should implement accessible security measures such as VPN and two- or multi-factor authentication to protect employee data, and institute an enterprise-wide mobile device management policy. They should also emphasise secure password protection and management, such as what makes a good password and encourage the use of secure enterprise password management tools.

Safely using the cloud: The cloud is remote-friendly by nature, and many companies finally made the shift after being forced to collaborate away from the workplace. While it may have been a heavy lift for companies used to keeping data onsite, what it lacks in ease it makes up for in security.

Particularly for small and mid-sized businesses that were less inclined to



invest in enterprise-level cloud computing before the pandemic, doing so offers a similar level of security to onsite data storage and is significantly more practical. Cloud operations offer end-to-end encryption, privacy controls and maintenance controls that keep systems up to date. Vulnerability testing is another common tool that cloud vendors use to evaluate risk and secure operations.

Future-proofing

It is likely that many of the pandemic-era workplace policies will stay in place. The most apparent result of that will be employees continuing to work from home, in some cases permanently, but in most circumstances on a hybrid basis. The new working arrangements bring to the forefront the issues of combating cyberthreats for employees who are no longer in the same building – a challenging task, but not an impossible one.

The most significant challenge remains the same – working in an online environment that has not been adapted to enterprise-level security. The networks that people work on at home are the same ones that their kids watch Netflix on and to which their smart doorbells are connected. Wifi is rarely secured, and firewalls are mostly unheard of for home networks. To adapt to those challenges on an enterprise level and for the long term, it is critical for companies to scale VPN

access to all secured devices and create a zero-trust zone that requests credentials for every login. Two-factor authentication is even more secure. Such measures are crucial steps to making sure that even if bad actors gain network access, they face barriers to breaching actual information systems.

Companies will also face the tragedies of human error during the transition to new work models. Like the vulnerable positions they were in during the initial transition in spring 2020, as employees adapt to new circumstances, cyber security can fall by the wayside. The result could be clicking attachments to messages disguised as return-to-work guidance, vaccination protocols, or other appropriately timed subjects, all of which could serve as an entryway to the broader network.

Malware and ransomware are also not always used immediately by bad actors. A common practice, and one that is particularly threatening to companies with employees who are about to re-plug into the corporate network for the first time, is malware that has been installed but is dormant. While most endpoint security systems offer protection against most threats, they do not offer the certainty of a firewall, so companies would be wise to mitigate risk by implementing zero-trust quarantine policies, in which IT departments would scan each and every returning device before it returned to the network. The vetting process would

cleanse the entire system of threats, literally before they arrive.

Next-generation threats

The remote transition that took place in early 2020 was chaotic, to say the least. As businesses eye the short- and long-term futures of their workplaces this time around, they have the luxury of being afforded more time and resources to make a more efficient and well-thought-out transition. The workforce plans that they will implement are also likely to be the ones that they will live with for decades to come, so making security a priority when building them will ensure a strong foundation for new threats that arise.

Enhanced phishing techniques:

Phishing attacks have spiked by 350% during the pandemic, and they are only going to become more frequent and sophisticated as time goes on.⁴ Cyber criminals took notable advantage of the Covid-19 crisis from the beginning, using it as an opportunity to ensnare people in links to phony CDC guidelines or health advisories. Attackers will certainly continue to use the guises of vaccination instructions or requests to share personal information in return for health data. In more extreme scenarios, criminals could even request addresses and use them to arrive at employees' houses and hack into home networks.

“A common practice, and one that is particularly threatening to companies with employees who are about to re-plug into the corporate network for the first time, is malware that has been installed but is dormant”

Home network attacks: If workers are bound to their home networks, hackers will certainly try to follow. Rather than using energy and resources to breach a corporate network onsite, a cheaper and likely easier option for cyber criminals is to breach under-protected home networks and through that window enter corporate networks.

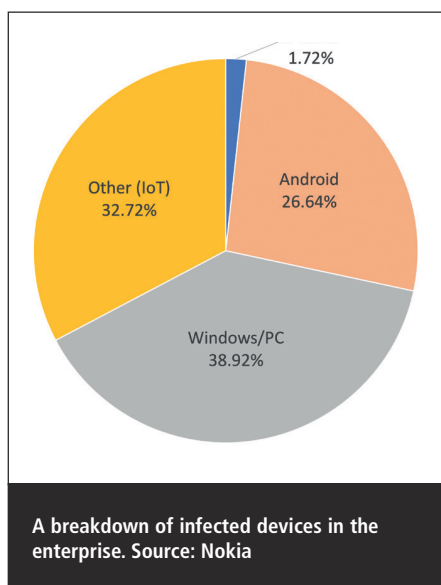
Security measures that companies can take to combat this future threat are

uncertain but include better employee education and offering resources to protect homes. However, the strongest approach is to continue to provide cloud-based patch and endpoint management.

Supply chain attacks: One of the more sophisticated attacks that companies are seeing on the horizon exploits the vulnerabilities that come from known, third-party software – tools routinely trusted by employees and tech experts alike – that are planted into coding or servers and migrate into devices when they undergo routine updates. By changing source code, such attacks often go undetected because third parties are unaware that the coding has been infected. Endpoint machines themselves are also none the wiser because the malware runs under the same permissions as the unadulterated app would.

“Companies can mitigate many of the risks related to them by employing strong code integrity protocols and only allowing verified applications to run on enterprise systems”

Supply chain attacks are particularly harmful because of their ability to infect many devices quickly. But companies can mitigate many of the risks related to them by employing strong code integrity protocols and only allowing verified applications to run on enterprise systems. Strong endpoint management systems are



another strong tool to mitigate risks.

Distributed denial of service (DDoS): This is a tactic used to overwhelm whole networks rather than individual employees. As hackers become more fluent in gaining access to devices, they are more frequently using those devices as tools to disrupt operations at unsuspecting companies. Directing the attention of an entire botnet to a single corporate website is an effective way to quickly disable a website for either ransom or activism.

To combat this new wave of cyber attacks, best practice dictates that companies retain third-party firms with advanced expertise in DDoS defence, and their capabilities for blackhole routing, rate limiting, network diffusions and strong firewalls will be far beyond any enterprise-level hardware on the market today.

Attacks on the Internet of Things (IoT): To the dismay of companies and employees alike, hackers are becoming proficient in invading devices beyond computers. As speakers, watches, home security systems and even refrigerators become Internet-enabled, they also become targets for malware.

A report from Nokia found that IoT devices made up nearly 33% of infections in 2020, a number that is sure to rise as the Internet becomes fluent in more devices.⁵ The threat is serious for devices on home networks, but also will extend to AI used in the workplace and on the manufacturing floor, threatening the stoppage of essential operations if hacked. User education is critical to mitigating the threat of IoT attacks, and alongside two-step authentication, segmentation from the network, and software updates, can go a long way towards digital safety.

The new normal

Whether the new normal is completely remote, hybrid, or mostly in-person, addressing the security threats that have been emphasised by Covid-19 will be paramount to any return-to-work strategy.

By strategising early and adopting plans that take into consideration current and future threats, not only will companies be able to avoid the collective chaos that ensued at the beginning of the pandemic,

they will also be able to build a strong foundation for threats on the horizon – because if there is one thing we know for sure, it is that they are out there.

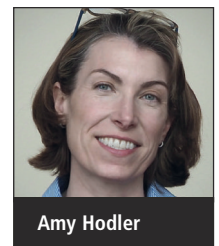
About the author

Jason Sabin joined DigiCert in 2012 and before being promoted to chief technology officer in 2020, he held roles including VP of research and development, chief security officer and chief information officer. As CIO, he spearheaded the move to SaaS and cloud services over on-prem instances. Sabin has more than 20 years of engineering and R&D experience working in the identity and security industry, with roles prior to DigiCert at NetIQ, Novell and Volera. He is a regular speaker at security, IoT and technology conferences. He has twice been named a Utah Genius for top inventor, with more than 50 patents issued.

References

1. Williams, Christina; Chatuverdi, Rahul; Chakravarthy, Krishnan. 'Cyber security Risks in a Pandemic'. Journal of Medical Internet Research, 17 Sep 2020, vol.22, no.9. Accessed Oct 2021. www.jmir.org/2020/9/e23692/.
2. '42% of security leaders said the pandemic has changed their cyber security priorities'. Help Net Security, 15 Dec 2020. Accessed Oct 2021. www.helpnetsecurity.com/2020/12/15/pandemic-cyber-security-priorities/.
3. Parker, Kim; Menasce Horowitz, Juliana; Minkin, Rachel. 'How the Coronavirus Outbreak Has – and Hasn't – Changed the Way Americans Work'. Pew Research Center, 9 Dec 2020. Accessed Oct 2021. www.pewresearch.org/social-trends/2020/12/09/how-the-coronavirus-outbreak-has-and-hasnt-changed-the-way-americans-work.
4. 'UN reports sharp increase in cyber-crime during pandemic'. Associated Press, 7 Aug 2020. Accessed Oct 2021. <https://apnews.com/article/virus-outbreak-counterterrorism-health-crime-phishing-824b3e8cd5002fe238fb9cb-d99115bca>.
5. 'Threat Intelligence Report 2020'. Nokia, 2020. Accessed Oct 2021. <https://onestore.nokia.com/asset/210088>.

Shining a light on organisational risk



Amy Hodler

Amy Hodler, Neo4j

When we consider how to rein in and limit nefarious activity on organisational networks, it helps to think like the individuals behind the attacks. In short, it pays to ‘think like a criminal’ to respond better to any attack.

Vulnerabilities are what criminals look for, much like the seasoned art thief. It would be a far stretch to walk into London’s National Gallery and announce that you’ve come to steal a Rubens. Instead, thieves look to exploit any minor vulnerability to their benefit. Cyber criminals are no different.

Criminals think in ‘graphs’, while the organisations they target are more inclined to think in lists, working to combat crime by a process of elimination. Graphs are a way of representing reality in terms of nodes and the connections or relationships between them. Those of criminal persuasion are on the lookout for undetected relationships.

“Algorithms allow you to locate the kinds of connections that pinpoint your system’s vulnerabilities. They also permit you to take the necessary corrective actions to render your system more robust”

We see this in the Netflix series *Lupin*, where the master of disguise dresses as a cleaner to avoid suspicion. He can access the door for the cleaning store that another cleaner has left open, and he can hide because they don’t do a sweep of every room. What *Lupin* does is to identify multiple weaknesses to create his own mental ‘graph’ in order to commit the perfect crime.

All about connections

These weaknesses are inherent vulnerabilities. They are the multiple small connections that criminals look out for

when trying to circumvent the security measures an organisation has in place. The criminals look for the initial small vulnerability to take them to the next hop. This graph-like approach enables them to spot the weakness in the security system that gets them to their ill-gotten end.

Technology systems are built to withstand attacks, but there are often many entry points that exploit systemic vulnerabilities. Criminals will keep on trying to discover these. Perhaps they will access the HR system to get to the financial accounts.

The way around this is to change our way of thinking, so we see the world as the bad actors do.

Graph databases help you map out the flows between assets you want to protect and the vulnerabilities between them. Graph technology is unique in this relationship-centred approach. And it has reached a point of maturity where we can run off-the-shelf algorithms over a network. These algorithms allow you to locate the kinds of connections that pinpoint your system’s vulnerabilities. They also permit you to take the necessary corrective actions to render your system more robust.

The shortest path

What a pathfinding algorithm does, essentially, is to find the shortest path in a network. A security team is able to use that algorithm to discover how it links to the largest potential vulnerability. The security team can see the way in and close the door to it. Pathfinding can also locate the central system that has access to the majority of the systems in

the same network. This could be either a system or a piece of equipment that allows access to important information. The system won’t have proper protection. Perhaps this could be an HR system that connects to a financial system or your IP storehouse.

“Graph thinking had the effect of minimising exposure to cyber hacks and any possible negative impact on other components in the system”

Graph technology is being deployed to help organisations stave off system breaches in the energy sector, for instance. The recent ransomware take-downs of US East Coast power grids are a great example of how this technology can work.¹ Thanks to a customer who identified system vulnerabilities, they were able to make the system less connected. This graph-informed approach was chosen over simply strengthening anti-virus capabilities. Graph thinking had the effect of minimising exposure to cyber hacks and any possible negative impact on other components in the system.

Where are you vulnerable?

How do we ensure that systems are least vulnerable to attack? Where graph technology helps is by searching for system irregularities in real time, based on patterns in the network. It could be an IT network where you know the regular patterns flow in a hub-and-spoke fashion. An unusual pattern could be when edge devices, such as IoT devices in a telecoms configuration, try to connect to each other or an outside area. This kind of irregularity suggests possible interfer-

ence by an outside agent. Cyber security teams can set a threshold based on anomalous system behaviour. A breach of this threshold will trigger an alarm for intervention or isolation of the suspect part of the system.

Malware on an email network could be another clue. For example, Person A emails Person B every day and only occasionally emails Person C. Now Person A is emailing all employees back-to-back in a five-minute window, which is suspect. What you can now do is isolate the problem email address because you have isolated a suspicious pattern.

Predictive patterns

One of the most useful ways to employ graph technology is to use it to make predictions to prevent future problems. It is possible to identify previous patterns where cyber security was potentially under threat. These seemingly innocuous patterns could easily have been cyber attacks.

Rather than just reacting to issues, taking these patterns and running them in a graph database allows for prediction and comparison with other patterns. With this, you can create models of prior attacks, using machine learning to which new data is added. Comparisons can then be drawn to determine where weaknesses lie to guard against assaults on your IT system.

Comparisons like these are particularly helpful for anti-money laundering (AML) and anti-fraud work. In AML, an analysis of a customer activity dataset using graph-based machine learning will reveal behaviour that shows both fraudulent and non-fraudulent behaviour.

Locating 'influence'

Another area to explore is personalised page rank, which examines the general influence in a network. 'Influence' refers to people or a type of business, and personalising PageRank focuses on a particular element.

A good example of this is a financial network where you want to gauge the influence on business-to-business (B2B)

transactions. Here, you would apply the page ranking and customise it for B2B transactions. Specific behaviours are deemed normal in cyber security, whether for a person, a business, or a technology communication. A personalised page rank algorithm allows the individual to be alerted when regular patterns, appropriate for a specific device, deviate from the norm.

Acceptable risk

An acceptable level of risk is paramount in all situations, so do remember to incorporate a degree of flexibility and don't err too heavily on the side of caution. What you need to avoid is closing off all access and harming the business. If you lock the business down entirely to be free from attack, you will be unable to operate as usual. An acceptable level of risk is essential to maintain business continuity.

"Graph technology helps you accurately assess that risk and what cyber security threats you face. It informs you of where you need to add in defences and how much you need to invest to be properly protected"

Financial services companies offer a great case in point when dealing with fraud. Credit applications, which could appear fraudulent, risk being rejected across the board. The last thing you want to do is lock out customers, partners or suppliers completely and alienate them. Find instead a reasonable level of risk tolerance.

A graph database helps you to learn from the criminal world and see where you are vulnerable. There's no need to turn yourself into a gentleman thief, like Lupin, but you can learn from him and his ilk.

When you examine your level of risk and decide what's acceptable, you retain business flexibility. Graph technology helps you accurately assess that risk and what cyber security threats you face. It informs you of where you need to add in defences and how much you need

to invest to be properly protected. In the battle for strong cyber security, you need to know your enemies and how they operate. When you understand this, you'll be able to outsmart them time after time.

About the author

*Amy Hodler is director of the analytics and AI programme at Neo4j (<https://neo4j.com>), a graph database company, and co-author of *Graph Algorithms: Practical Examples in Apache Spark & Neo4j*, published by O'Reilly Media.*

Reference

1. 'US recovers millions in crypto-currency paid to Colonial Pipeline ransomware hackers'. CNN. Accessed Oct 2021.

The big picture

As a provider of cyber security for seven US R&D laboratories, including the Centre for National Security, The Mitre Corporation has its work cut out. Anti-virus warnings, intrusion alerts as well as seemingly low-level events like logins and file share access can all be potentially linked to attack activity.

Its challenge was to understand the data relationships between these disparate and often isolated pieces of information. Without this understanding, the cyber security team was finding it hard to fully comprehend a given security environment and map all known vulnerabilities. Since network environments never remain static, the team needed a flexible architecture that allowed for advanced analytics, ad hoc queries and facilitated visualisation.

Mitre used graph technology to bring together its disparate data to create CyGraph, a dynamic tool that presents all its cyber security information in a big picture. Rather than being fixed, Cygraph evolves over time, taking in new knowledge. This allows for appropriate attack responses and protection of mission-critical network assets.

As attacks occur, the team can now map intrusion alerts to known points of vulnerability and take the appropriate action.

The Firewall

Wifi 6 – has it delivered?

Colin Tankard, Digital Pathways



Wifi 6 was released in late 2019 and was promoted as being the saviour for our wireless needs. It claimed to provide faster data transfer, better performance in congested areas and more security. But is its security really better?

Most threats to wifi have been due to human error. If a hacker attacked a network, it was usually because the administrators had not set up the router to secure it properly, with a typical error being not setting a password for the network.

In 2017 we saw an increase in attacks, with new vulnerabilities being discovered. One was concerned with WPA2, which suffered from a vulnerability called the key re-installation attack, or Krack, which was able to affect every single access point that uses WPA/WPA2 across the world. This allowed a hacker to act as a middleman between a user and the wifi access point serving the connection.

Public wifi networks have always been insecure, since they offered no built-in encryption to devices connected to them. The encryption in WPA and WPA2 has vulnerabilities which meant that, by gaining access to the network, a hacker could sniff out, intercept and decrypt wifi traffic passing between computers and access points.

Therefore, WPA3 was developed and is the core security feature in wifi 6.

WPA3 secures wifi connections significantly and in several ways.

First, there is protection against brute force dictionary attacks. These systematically submit every single word in a dictionary file as a password, allowing constant attempts of different words and phrases with no recourse on the part of the network device.

With WPA3, the standard accepts that passwords are insecure. As more users add more devices to their networks, each new device acts as a brick added to the barrier between users and updating insecure passwords. Assuming this all-too-common scenario, WPA3

uses a protocol called Simultaneous Authentication of Equals (SAE), which was originally used for authentication of nodes used in mesh networks to authenticate device connections.

This method of authentication is important, as the password for the actual network is never shared between two devices. Instead, the devices enter into what's called an SAE exchange where two devices verify whether each knows the same password, without actually transmitting it. Once it has been established that they both know it, a cryptographically strong key is then shared between them for actual authentication. From this key, a session key is derived. Would-be attackers listening to the network traffic may be able to 'sniff out' that session key, but would be unable to compromise the actual key which depends on the authentication key created between those two devices, not the original password.

WPA3 also offers stronger encryption. WPA2 requires a 64-bit or 128-bit encryption key. But WPA3 uses a 192-bit encryption security suite for protecting wifi users' networks. The higher the encryption and security framework, the harder to crack.

Finally, WPA3 offers simplification for security with the Internet of Things (IoT). The WPA3 protocol eases the process of configuring devices that have limited or no display interface, often the case with IoT devices. Given the growth in IoT, such devices need locking down, which is often not possible. WPA3 allows this to take place via the network.

In summary, wifi 6 provides significant advances on previous standards. It will make wifi faster, more secure and stable. It will take some time for manufacturers to implement it, and even longer for hardware to be refreshed. However, it's important to start planning ahead so that the correct infrastructure is in place. Perhaps, at last, we will have a secure, trusted wifi system for both users and their guests.

EVENTS

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.

8–12 November 2021
OWASP Global Appsec USA
 Virtual event
<https://owasp.org/events/>

14–15 November 2021
THOTCON
 Chicago, IL, US
<https://thotcon.org/>

15–19 November 2021
Hack in Paris
 Virtual event
<https://hackinparis.com>

16–18 November 2021
European Cyber Week
 Rennes, France
<https://en.european-cyber-week.eu>

5–8 December 2021
Security Weekly Unlocked
 Florida, US
<https://events.securityweekly.com/unlocked2021>

9–10 December 2021
ICCS
 Cardiff, UK
<https://iccs2021.iaasse.org/index.html>

10–13 January 2022
FloCon
 Virtual event
<https://bit.ly/2F0WyUm>

2–4 February 2022
IT-Defense 2022
 Berlin, Germany
<https://bit.ly/3mh1Ahj>

2–3 March 2022
Cloud & Cyber Security Expo
 London, UK
www.cloudsecurityexpo.com