ELSEVIER

network SECURITY

ISSN 1353-4858 February 2021

www.networksecuritynewsletter.com

Featured in this issue:

Who's that knocking at the door? The problem of credential abuse

At the heart of IT security is a simple concept – proving that you are who you say you are. But the ways we have of doing that, through credentials of some form, are flawed.

Credential abuse comes in many forms. The question we need to ask is, where does it sit in terms of an organisation's attack surface and security priorities? In the first of a two-part feature, Steve Mansfield-Devine surveys a number of industry experts to get their views on what forms of credential abuse are being encountered and the threat these pose to enterprises.

Full story on page 6…

The state of zero trust in the age of fluid working

While many organisations had some form of fluid working before the pandemic, it is now non-negotiable.

As a result, we've seen a boom in the adoption of enterprise technologies to support this new way of working. However, one aspect of business that shouldn't be forgotten is cyber security, because cyber criminals are taking advantage of the shift to working from home to launch increased numbers of cyber attacks, explains Ollie Sheridan of Gigamon.

Full story on page 15…

Avoiding costly downtime – how MSPs can manage their networks

For managed service providers (MSPs), managing a network is a big responsibility. When it goes down – perhaps as the result of a cyber attack – the results can be costly.

The need for network resilience has become even greater during the pandemic. The requirement to work from home has placed increased strain on networks and greater importance on seamless connectivity. The need for MSPs to ensure greater resilience and uptime may be here to stay, says Brendan Walsh of Opengear.

Full story on page 17…

Florida facility hacked in attempt to poison water

An unknown attacker attempted to poison the water supply of a Florida city by taking over a control system at the water treatment plant. The attempt failed but has heightened concerns over the security of critical infrastructure.

The attacker used the Microsoft TeamViewer app to access the water treatment system for the city of Oldsmar, which serves around 15,000 people. TeamViewer is commonly used for remote access to systems for management purposes, but is usually secured and requires authentication. It's not yet known how the attacker managed to breach or sidestep any security placed on the system – assuming there was some.

Continued on page 2…

Contents

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

Publishing Director: Sarah Jenkins
Editor: Steve Mansfield-Devine
E-mail: smd@contrarisk.com

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

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

Subscription Information
An annual subscription to Network Security includes 12 issues and online access for up to 5 users.
Subscriptions run for 12 months, from the date payment is received.

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

12987
Digitally Produced by
Mayfield Press (Oxford) Limited

"From a cyber security standpoint, we should be particularly concerned about how the attacker was able to authenticate into the remote access software," commented Tim Erlin, VP at Tripwire. "That entry point should be very well protected, given that it provides access to such obviously sensitive capabilities. Protecting remote access into industrial systems where these types of changes can be made should be a high priority for any industrial environment."

With full control over the system, the attacker modified the concentration of sodium hydroxide (NaOH) added to the water. Also known as lye or caustic soda, this is used to control the water's acidity and remove heavy metals. However, the attacker increased the concentration from the normal 100 parts per million (ppm) to 11,100ppm – a level at which it would be toxic to anyone drinking the water. It took just a few minutes for the attacker to make the changes, suggesting some familiarity with the system.

"Even if the plant operator had not quickly reversed the increased amount of sodium hydroxide, it would have taken between 24 and 36 hours for that water to hit the water supply system and there are redundancies in place where the water is checked before it would have been released," said Pinellas County Sheriff Bob Gualtieri.

The plant operator had seen an attempt to remotely control the system earlier in the day, but assumed it was his supervisor. On the second attempt, it was only when he saw the sodium hydroxide levels being increased to dangerous levels that he realised something was amiss.

Fortunately, the plant operator on duty noticed the activity and reset the sodium hydroxide to the correct level. There is no indication yet as to whether the attack originated within the US or from abroad, but the Sheriff's office said they had some leads on suspects. This is not the first attack on water facilities. Most of those we've seen have, like this one, tended to be of low sophistication and easily mitigated. However, Verizon's 2016 'Data Breach Investigations Report' described a similar attack on an unnamed US water facility. And in 2020, there were numerous attacks against Israeli water facilities.

The Pinellas County Sheriff's Office, the FBI, and the Secret Service are investigating the incident.

More fallout from SolarWinds hack

The hack affecting SolarWinds' Orion product continues to have an impact as more information emerges about affected organisations and further vulnerabilities.

The attackers were able to insert backdoor malware, dubbed Sunburst, into Orion's source code, which was then subsequently signed and distributed by the company. The backdoor could then be used for further infiltration of targeted systems.

Researchers at Trustwave's SpiderLabs found two more vulnerabilities in the Orion product and another in Serv-U FTP for Windows. All three (CVE-2021-25274, CVE-2021-25275 and CVE-2021-25276) are classed by the firm as severe. The most critical bug would allow remote code execution with high privileges. And another vulnerability could allow any local users, despite privileges, to take complete control over the SOLARWINDS_ORION database. An adversary could steal information or add a new admin-level user to be used inside SolarWinds Orion products. SpiderLabs has produced proof-of-concept code for all three flaws. SolarWinds has now issued patches.

There are full details here: http://bit.ly/2MMzKLS.

According to Symantec, the Sunburst backdoor has been used to install malware known as Raindrop on some victims' systems. This is based on Cobalt Strike, a legitimate penetration-testing tool which malicious actors use to make lateral movement through networks, exfiltrate data, deliver malware and more. The file archiver 7-Zip and DSInternals – again, both legitimate pieces of software – have also been installed by attackers. DSInternals allows an attacker to query Active Directory servers and retrieve data such as passwords, keys or password hashes. There's more information here: http://bit.ly/3cZ4UdC.

A number of cyber security vendors seem to have been particularly targeted. FireEye was the first to disclose a breach,

Threatwatch

RDP amplification

Criminals running distributed denial of service (DDoS) services have turned to Microsoft's Remote Desktop Protocol (RDP) to amplify attack volumes. According to researchers at Netscout, relatively small messages sent to Internet-accessible RDP ports can result in much larger responses – up to 89 times the amount of data. By using the intended victim's IP address as the spoofed 'from' address in the initial message, this can lead to sites being bombarded with traffic. Although not the most effective amplification technique, it has still resulted in DDoS attacks by so-called booter or stresser services achieving attack traffic volumes of 20Gbps to 750Gbps. There's more information here: http://bit.ly/3rITj6y.

RAT evades anti-virus

A new variant of the Agent Tesla remote access trojan (RAT) has added capabilities that enable it to evade detection by anti-malware products. Sophos found that the latest version directly targets Microsoft's anti-malware software interface (AMSI), which is used by many anti-virus products to integrate with the operating system. Agent Tesla attempts to overwrite AMSI code in memory, changing just eight bytes in a function that, if successful, makes all memory scans appear invalid. The new variant of the malware is also able to deploy a Tor client, helping it to communicate invisibly with command and control servers. There's more information here: http://bit.ly/3rJgpKj.

Cisco router flaw

Vulnerabilities in the web interface of Cisco's RV160, RV160W, RV260, RV260P, and RV260W VPN routers, which are aimed at small businesses, could allow a remote attacker to view or manipulate data and perform unauthorised actions on the device. The problems stem from a lack of proper validation of HTTP requests, which means that an attack could be mounted simply by sending a specially crafted HTTP request. Overall, the vulnerabilities have been given a CVSS score of 9.8, categorising them as highly critical. No fewer than seven CVEs have been assigned – CVE-2021-1289, CVE-2021-1290, CVE-2021-1291, CVE-2021-1292, CVE-2021-1293, CVE-2021-1294, CVE-2021-1295. Cisco has released patches, but it will be up to users to apply them. There's more information here: http://bit.ly/3a6MeXF.

Kubernetes hijacking

A new piece of malware, dubbed Hildegard, is being developed by the TeamTNT threat group to target Kubernetes clusters with the aim of using them for crypto-currency mining, according to researchers at Palo Alto Networks. The malware appears to be still in development – what Palo Alto calls a "reconnaissance and weaponisation stage" – but the firm warned that it may soon see wide-scale deployment for crypto-jacking purposes. Infection is achieved via a misconfigured kubelet – software that manages a number of pods on a Kubernetes cluster. Once this is achieved, Hildegard then looks for more vulnerable kubelets in order to spread to as many pods as possible. This obtains the processing power for crypto-currency mining. There's more information here: http://bit.ly/3cVqGPH.

Supercomputer attacks

Attackers are targeting supercomputer clusters with a piece of malware that steals SSH credentials and opens a backdoor. Dubbed Kobalos by researchers at ESET, the malware not only provides access to the machines but could be used for data exfiltration and crypto-currency mining – the last being highly likely, given the computing power of the targeted machines. The malware itself is said to be tiny and platform-agnostic, working on Linux, BSD, Solaris and possibly AIX and Windows machines. The main targets so far have been high-performance computing (HPC) clusters, although an ISP in Asia, an endpoint security vendor in North America and a few personal servers have also been attacked. There's more information here: http://bit.ly/3peqFcc.

before the link to SolarWinds was established. Palo Alto said it was able to block the threat internally and Qualys said the malware was downloaded into an isolated lab environment.

Crowdstrike said it was contacted by the Microsoft Threat Intelligence Centre in mid-December. "Specifically, a reseller's Microsoft Azure account used for managing CrowdStrike's Microsoft Office licences was observed making abnormal calls to Microsoft cloud APIs during a 17-hour period several months ago," it said. "There was an attempt to read email, which failed, as confirmed by Microsoft." It has now released a reporting tool for Azure to help organisations review excessive permissions in their Azure AD environments. It's available here: https://github.com/CrowdStrike/CRT.

Email security firm Mimecast has now said that a security breach it disclosed early in January was caused by the SolarWinds Orion compromise. It previously announced that a certificate used to authenticate some of the company's products to Microsoft 365 Exchange Web Services had been compromised.

"Our investigation also showed that the threat actor accessed, and potentially exfiltrated, certain encrypted service account credentials created by customers hosted in the United States and the United Kingdom," the company said in a statement. "These credentials establish connections from Mimecast tenants to on-premise and cloud services, which include LDAP, Azure Active Directory, Exchange Web Services, POP3 journaling and SMTP-authenticated delivery routes."

There is no evidence that encrypted credentials have been decrypted or misused, the firm insisted. But it has suggested that US and UK customers reset their credentials.

According to Kaspersky, around a fifth of all Sunburst victims are in the manufacturing sector, spread across a large number of countries. Its ICS CERT researchers extracted nearly 2,000 domains generated by the Sunburst DomainName Generation Algorithm. Around a third (32.4%) of all victims were industrial companies, with manufacturing (18.11%) being the most common. This was followed by utilities (3.24%), construction (3.03%), transportation and logistics (2.97%) and oil and gas (1.35%).

Kaspersky's report is here: http://bit.ly/3tINmbN.

It has also been suggested that China-based attackers have exploited organisations compromised by Sunburst to break into US Government computers. Reuters reported unnamed sources as saying that: "FBI investigators recently found that the National Finance Centre, a federal payroll agency inside the US Department of Agriculture, was among the affected organisations, raising fears that data on thousands of government employees may have been compromised."

However, it's still believed that the original source of the SolarWinds breach came from Russia. The Reuters report is here: http://reut.rs/3aUkvJ1.

Report Analysis

Veracode: State of Software Security v11

We all know that software contains flaws and that this is the major cause of security vulnerabilities. Veracode makes it its business to examine code for errors that could lead to disaster and its annual report often makes for uncomfortable reading. This year is no different.

The data is the result of scanning more than 130,000 active applications. Most of them had weaknesses of some kind and while only a minority had serious vulnerabilities, that's still a big enough proportion to explain why breaches remain in the headlines.

One business area that has shown itself to have both problems and solutions is the retail and hospitality sector. Veracode found that more than three-quarters (76%) of the applications it examined had at least one flaw. That's not an especially bad figure – according to the report it's about average when compared to economic sectors such as financial services, technology, healthcare and others. The problem is that more than a quarter (26%) of the vulnerabilities were ranked as high severity – the second-highest level of the six sectors examined in the report (the average is 24%).

This is an industry that handles very high volumes of customer data – not just payment card information but also data from loyalty schemes, membership accounts and marketing data from third-party sources. Most breaches in this sector are via web attacks and Veracode cites Verizon's '2020 Data Breach Investigations Report' in claiming that half of these breaches result in the theft of personal or payment data.

According to Veracode, the sector faces some particular challenges in its use of large, complex code that is typically older than in many other industries. The behaviour of developers in terms of employing static and dynamic vulnerability scanning, and the frequency at which they carry out these tests, is pretty middle of the road.

To give them their due, developers in this sector are quite good at avoiding common flaws, such as information leakage and input validation. But they struggle in areas like preventing flaws that can lead to SQL injection. Overall, this is an industry, the report says, that could definitely benefit from adopting DevSecOps practices.

On the positive side, the retail and hospitality sector ranks second-best in its overall fix rate for software vulnerabilities, with half of flaws remediated in 125 days. This might not seem all that quick, but it's a month better than the next-fastest, and across all industries it's common for flaws to remain unfixed for considerably longer – if they get fixed at all.

"Retail and hospitality companies face the dual pressure of being high value targets for attackers while also requiring software that allows them to be highly responsive to customers and compliant with industry regulations such as PCI," said Chris Eng, chief research officer at Veracode. "Developers in the retail and hospitality sector appear to do a better job than others when dealing with issues related to information leakage and input validation. Using API-driven scanning and software composition analysis to scan for flaws in open source components offers the most opportunity for improvement for development teams in the retail sector."

Looking more generally at the results Veracode obtained, the use of open source libraries is highlighted once again. This is not to say that open source code is bad per se. Many libraries are actively maintained by large numbers of contributors who work hard to ensure a high standard of coding, including security. But not all. Some libraries are the part-time work of a single person. And comparatively few libraries are ever subject to proper security audits or penetration testing.

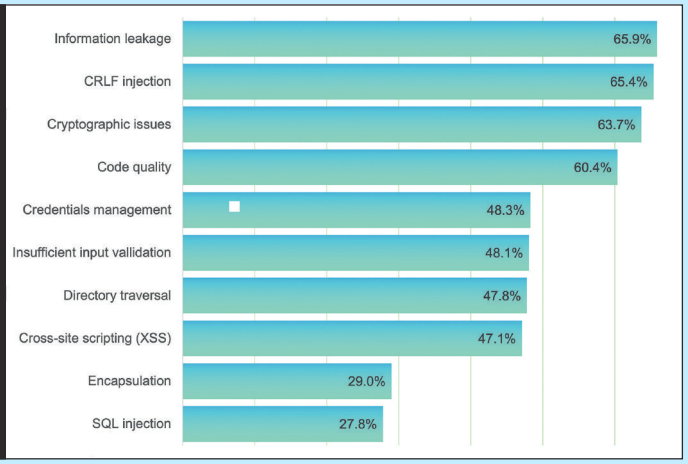
Yet open source libraries are eagerly adopted by overworked developers who just need a particular functionality for their code and have neither the time nor the inclination to reinvent the wheel. This leads to the situation, reported by Veracode, where 97% of a typical Java application consists of open source libraries stitched together by the developer, but just a light dusting of original code to pull it all together and customise the code for the job at hand.

On a more optimistic note, Veracode is now tracking software flaws over the whole lifetime of an application, rather than just the problems it had in the past year, and the report found that two-thirds (67%) of application are either maintaining or reducing the total number of observed flaws. In other words, they're not getting worse.

The ability to eliminate flaws – and the speed at which that's done – depends on a number of factors. Organisations that do frequent scanning and implement either static application security testing (SAST) or dynamic application security testing (DAST), do best. In fact, those that combine SAST with DAST generally fix flaws 24.5 days faster than the average. On the other side of the equation, having old or large applications, being a large organisation and having a high flaw density – ie, significant 'security debt' – makes it tougher to rid applications of flaws. Applications with higher flaw densities generally take 63 days longer than average to fix.

As for the flaws themselves, there are few surprises. The OWASP top 10 feature large, with issues such as SQL injection, cross-site scripting and CRLF injection being among Veracode's top 10. But it also highlights information leakage as the most serious flaw, with cryptographic issues, code quality and credentials management also being among the most serious.

The report is available here: https://info.veracode.com/report-state-of-software-security-volume-11.html.



The top 10 flaw types. Source: Veracode.

In brief

China-based hackers steal airline data

A hacking group, believed to be operating out of China, has been mounting attacks against the airline industry, most likely in an attempt to track the movement of persons of interest. The group, which the cyber security industry has been tracking under the name of Chimera, was first reported by CyCraft, which gave a presentation at Black Hat 2020. But now, a new report from NCC Group and its subsidiary Fox-IT claims that Chimera's activities are much broader than originally believed. In some cases, the attackers have compromised systems and remained hidden for up to three years. Chimera uses a range of methods, including scraping the memory of infected systems for passenger name records (PNR). The initial compromise often comes from credential stuffing, using login records leaked from other data breaches. The Fox-IT report is here: http://bit.ly/3rzd8NC.

Parler host loses IP addresses

DDoS-Guard, a Russia-based company that provides websites with distributed denial of service (DDoS) protection and infrastructure services, has been stripped of a range of IP addresses, including one currently used to host the controversial social networking site Parler. While DDoS-Guard operates out of Russia, it is incorporated in other countries, including Scotland and Belize. Ron Guilmette, a researcher who studies and tries to de-platform conspiracy theorist and far-right groups, complained to LACNIC, which controls the assignment of IP addresses in Latin America and the Caribbean, that the Belize registration was made purely in order to obtain a range of addresses (given that IPv4 addresses are in short supply) and that DDoS-Guard actually has no real business presence in the region. LACNIC agreed and has stripped the company of 8,192 IPv4 addresses. Parler will probably be moved to another IP address owned by DDoS-Guard.

CISA cloud warning

The US Cybersecurity and Infrastructure Security Agency (CISA) has warned about several recent successful attacks against US organisations using cloud services. The attacks make use of poor security practices and misconfigurations. According to the agency: "These types of attacks frequently occurred when victim organisations' employees worked remotely and used a mixture of corporate laptops and personal devices to access their respective cloud services. Despite the use of security tools, affected organisations typically had weak cyber-hygiene practices that allowed threat actors to conduct successful attacks." Phishing attacks are being used to harvest account credentials and the attackers are bypassing multifactor authentication by stealing browser cookies. There's more information here: http://bit.ly/3rEmuaZ.

Retiring ransomware

The operators behind the Ziggy ransomware campaign have decided to call it a day and have shut down the operation. They have also publicly released all the decryption keys for 922 current victims in a SQL file. An announcement on Telegram said: "We are very sad about what we did," and in a conversation with the Bleeping Computer website, the ransomware admin claimed that the group needed money because it is in a "third-world country". However, a more likely explanation for the sudden change of heart is that the group are worried about law enforcement breathing down their necks, having witnessed recent operations against Emotet and Netwalker.

Phishing attack uses Morse code

A targeted phishing attack is using Morse code to obfuscate malicious URLs in an attempt to get past anti-malware systems. The malicious emails come with an Excel file attached, whose name is customised to the target. The file may even contain the target company's logo. Inside is a piece of JavaScript in which most of the letters of a URL are rendered in Morse code, with a full stop for a dot and a hyphen for a dash. A function in the JavaScript then converts this to a hexadecimal string, which uses another function to convert to the URL of the attackers' server. This presents an Office 365 login screen in an attempt to steal the user's credentials.

Clear and present danger

The World Economic Forum has released its latest 'Global Risks Report'. In the section of 'clear and present dangers', describing what respondents believe will become the most critical threats to the world in the near future, cyber security failure ranks fourth – behind infectious diseases, livelihood crises and extreme weather events. Digital inequality comes fifth. Both are ahead of terrorist attacks and human environmental damage. The report is here: https://bit.ly/36ZA4hm.

GDPR fines

Regulators across Europe have imposed fines totalling €272.5m under the General Data Protection Regulation (GDPR), according to research by law firm DLA Piper. Some €158.5m in fines has been imposed since 28 January 2020, a 39% increase on the previous 20-month period since the implementation of the GDPR. There has also been a 19% growth in breach notifications for the second year running, with 121,165 breaches notified since January 2020, compared to 101,403 in the previous year. Per capita, Denmark saw the most notifications. The numbers come from DLA Piper's analysis of reports in the 27 EU member states plus the UK, Norway, Iceland and Liechtenstein. Italy's regulator tops the rankings for aggregate fines, having imposed more than €69.3m since the application of the GDPR on 25 May 2018. Germany and France came second and third with aggregate fines of €69.1m and €54.4m respectively. However, attempts to fine companies haven't always worked out the way regulators expected. After high-profile breaches by BA and Marriott, the UK's Information Commissioner's Office (ICO) tried to levy fines totalling £282m but the two fines were later reduced to £20m and £18.4m. The Austrian supervisory authority suffered a setback when a €18m fine was successfully appealed in December 2020.

Swedish NCSC

Following a number of high-profile attacks against Swedish organisations, including the compromise of security firm Gunnebo, which led to a leak of customer data, the Swedish Government has decided to create a National Cyber Security Centre (NCSC). It will be established and operated by a coalition of state security organisations led by the Swedish Armed Forces and the National Defence Radio Establishment (Försvarets Radioanstalt), the armed forces signals intelligence agency. Also involved is Säpo (Säkerhetspolisen), the Swedish national security agency tasked with counter-espionage and counter-terrorism roles, and the Swedish Civil Contingencies Agency, which is responsible for protecting the nation's critical infrastructure and managing emergency responses.

Financial attacks

Research by the Ponemon Institute, sponsored by Keeper Security, found that 70% of financial organisations in the UK suffered at least one cyber attack in 2020. More than half (59%) of these were enabled as a result of people working at home during the pandemic. Some 70% of firms said that the use of personal devices has created problems with security and 41% of finance firm executives believe that working from home is putting the business at risk. The report is here: http://bit.ly/2LFjXhy.

Work from home phishing

Perhaps not surprisingly, there has been a significant rise in phishing attacks aimed specifically at people working from home, according to KnowBe4. Attackers are using subject lines and email content designed to look important and relevant, such as changes to company policies, annual inventories, changes to health benefits, scheduled Zoom meetings and security alerts. Social media alerts are another popular topic, with nearly half (47%) of the phishing emails in this category relating to LinkedIn.

Who's that knocking at the door? The problem of credential abuse

Steve Mansfield-Devine

Steve Mansfield-Devine, Editor, *Network Security*

At the heart of IT security is a simple concept – proving you are who you say you are. In this context, 'you' might be a human logging into a network or service, a device interacting with an application programming interface (API), one network talking to another or any number of other scenarios. And the proof could be a certificate, an SSH key, a token of some form or our old favourite – and inevitably the artefact we'll be talking most about here – the old, fragile and yet seemingly unkillable password.

The humble password is the most familiar and yet also the most heavily abused form of credential used in computer authentication processes. Its use on computers dates back to 1960 when Fernando Corbató, working on MIT's Compatible Time-Sharing System (CTSS), suggested passwords as a way of securing access to files on shared computer systems. Technology has progressed rapidly and enormously in the past 60 years, but the password hasn't. We've attempted to shore up its effectiveness with technology (such as password managers) and all-too-rarely-followed best practices – such as using long passphrases, mixing cases, adding numbers and symbols and so on. Yet the password remains one of the most vulnerable instruments in the security domain.

Credential abuse comes in many forms. The simplest is an employee 'borrowing' the user ID and password of a co-worker. The purpose may be benign – to get a job done on time – or malicious, but this kind of behaviour is rampant and makes a nonsense of assigning privilege levels to individuals. However, while this happens a lot, it only rarely leads to significant consequences for the organisation.

Of more concern is the use of stolen credentials by people with malicious intent. This could be the exploitation of a single set of credentials for a privileged person – perhaps the email login for the chief financial officer – being used to commit a business email compromise (BEC) attack. Or it might be the large-scale deployment of millions of stolen credentials, often aggregated from multiple data breaches, being thrown at a system in rapid succession to see if anything works – so-called credential stuffing, of which more later. There are also the traditional brute force methods, such as dictionary attacks using files containing common words that will be tried in various combinations and capitalisations, and others that use files of the most popular passwords – and yes, 'password', '123456' and 'qwerty' are still in widespread use, along with thousands of others that users believe are clever (such as 'password1') but which hackers know only too well.

"There are also the traditional brute force methods, such as dictionary attacks using files containing common words that will be tried in various combinations and capitalisations"

A survey by BeyondTrust found that nearly two-thirds (64%) of firms believed they had suffered a breach because of misused or abused employee credentials.[1] Almost as many (62%) blamed compromised credentials belonging to third parties, such as suppliers. It's little wonder that of the firms surveyed, only 37% said they trust their employees and 25% trust their vendors.

Top priority

There's no denying that credential abuse happens – but how much? Where does it sit in terms of an organisation's attack surface and security priorities?

"Depending on their goals, hackers can develop the attack to gain control over the domain and access to critical resources"

"Credential abuse should always be in the top 10 list of priorities for CISOs," says Alexandre Cagnoni, director of authentication at WatchGuard Technologies. "Every year, when we look at the Verizon Data Breach report, malicious use of credentials is implicated in more than 80% of the cases for breaches worldwide. The most common way to start an attack is by impersonating real users."

Ekaterina Kilyusheva, Positive Technologies: "Credential abuse is relevant for any company."

Credential abuse: an overview

Rob Otto, EMEA Field CTO, Ping Identity

Credential abuse represents a significant attack surface for most organisations today. An attack based on the use of stolen credentials typically has a low barrier to entry and can often yield the best 'bang for buck' for an attacker, particularly if high-value resources are accessible using passwords alone.

There are several paths to obtaining stolen credentials; password hygiene is poor as a rule and attackers will place a decent bet on a compromised password found on a list being re-used elsewhere by the same individual. Alternatively, email-based phishing campaigns offer a relatively straightforward way to dupe an unsuspecting user into revealing a password and these can often be well constructed and very targeted towards highly privileged individuals. Social engineering is the third obvious path of attack, with many password-based systems that rely on knowledge-based authentication for account recovery particularly susceptible. CISOs should be taking this threat seriously: they should assume that credential abuse will happen against their systems and should be taking steps to ensure that they have additional countermeasures in place to thwart this type of attack.

API channels are, unfortunately, no less susceptible to credential abuse and may in many ways actually be even more vulnerable, due to a proliferation of poor API security practices, such as relying on shared API keys and credentials, as well as API authorisation policies that do not conform with least privilege. There are far too many API implementations that do little to ensure minimisation of access to data, based on a strongly authenticated caller.

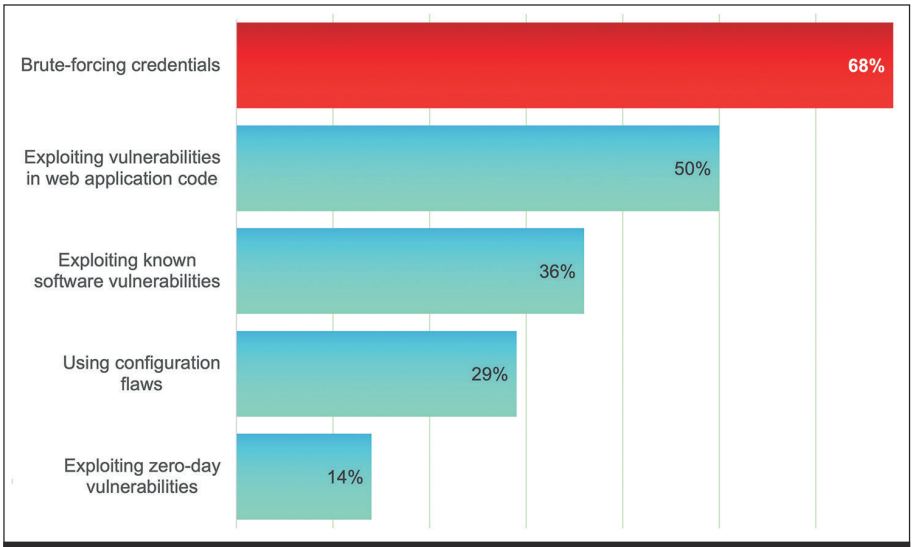
Multi-factor authentication is certainly one of the strongest defences that an organisation can and should deploy in response to these threats, but it is important to note that MFA is not a silver bullet and needs to be thoughtfully deployed in a way that minimises impact on the user experience. Modern MFA solutions that use a combination of smartphone push as well as standard FIDO2 authenticators offer a significantly better experience than legacy OTP-based offerings, particularly those that rely on insecure delivery mechanisms such as SMS.

Regardless of the delivery mechanism, 2FA deployed as a blunt instrument inevitably causes user resentment and these roll-outs tend to be less successful than those that are coupled with a risk-based approach that only calls for a strong authentication challenge when certain conditions are met. A machine-learning capability is vital here and offers the ability to analyse patterns of application and API usage and use this model to detect anomalous behaviour in real time. Combined with other approaches, such as the ability to do contextual analysis of each transaction (such as looking for known risk factors, including changed user behaviour or signs of browser compromise), unusual or high-risk IP addresses can help organisations move towards a model of zero trust, making an adaptive decision to allow, step-up or block user access based on the calculated risk associated.

Every organisation, irrespective of size or sector, is vulnerable, a fact underlined by penetration tests.[2] "It's not just a user account that may be at risk," says Ekaterina Kilyusheva, head of the Information Security Analytics Research Group at Positive Technologies. "This is only the first step of an attack. Depending on their goals, hackers can develop the attack to gain control over the domain and access to critical resources. An employee's account can be used to carry out attacks on clients and partners of the company, or used in phishing mailings with malware. Recently, there have been frequent business email compromise attacks aimed at financial fraud."

Attacks exploiting credential abuse are becoming more frequent and more sophisticated, thanks in no small part to the availability of automation tools. They also have a high success rate, with two key factors at play here – enterprise defences that just aren't suitable to stop these attacks and the fact that stolen or misused credentials are, in themselves, genuine.

"Stolen credentials are seen as legitimate by most standard security measures and therefore attackers have free access into an organisation's data and systems



Types of web application attack that, during penetration testing engagements, led to penetration of the local network. Source: Positive Technologies.

to do as they please," says Ben Freeney, advanced threat services manager, UK & Ireland at Fujitsu.

What's the damage?

Having unauthorised people roaming your networks is obviously a problem – but how much of a problem?

"Compromised credentials can be used for more than just data theft and tampering with systems," says Freeney. "If an attacker can login and use an individual's email account they can potentially instruct others within an organisation to perform actions on their behalf. Also, stolen credentials (especially privileged credentials) unlock a treasure trove of sensitive data and allow hackers to move through an organisation's network at their leisure until they find the most valuable information that they can sell on the black market or use to extort the organisation. Stolen credentials also allow attackers to engage in BEC. This technique can also be used with customers."

"Stolen credentials (especially privileged credentials) unlock a treasure trove of sensitive data and allow hackers to move through an organisation's network at their leisure until they find the most valuable information"

Although our focus here is on the challenges for enterprises when it comes to credential abuse, Mike Nathan, senior director of solution consulting at LexisNexis Risk Solutions, points out that, "Credential abuse fraudsters focus on two key targets: employees and consumers. For employees, credential targeting is trending, specifically on ransomware. There have been many media-linked cases in this space. For consumers, fraudsters target accounts to obtain goods purchased via card-not-present transactions or to perform payment fraud through online banking."

In fact, credential abuse pops up everywhere. Pascal Geenens, director of threat intelligence at Radware, who

Pascal Geenans, Radware: "Easy-to-guess passwords are a risk."

spends a lot of his time running honeypots to trap hackers and understand the vulnerabilities they are exploiting, gave some examples that happened over the course of just a few weeks recently.

"At the end of July, Zoom fixed a security oversight that allowed unlimited and unrestricted password guessing for private password-protected meetings," he says. "It takes only about one million brute force attempts to break a six-digit password, and these can be performed as fast as the API allows."

Shortly after, then-President Trump's Twitter account was compromised by a white-hat hacker.[3] "Leveraging the information of several leaked accounts of the president across multiple leaks, in just five guesses the security expert was able to guess the password to gain full access to Trump's Twitter account, which did not have dual-factor authentication enabled," he says. The password, allegedly, was 'maga2020'.

And then Brian Krebs recently published an article describing how the security blueprints of many companies were leaked in a hack of Swedish firm Gunnebo.[4] "Krebs notified the company that the password to the Gunnebo RDP account was being traded on the underground," says Geenans. "The password was 'password01'. There is no direct evidence that this is how the malicious actors breached the organisation – it might be pre-dating the notification and password being traded – but it makes the point that easy-to-guess passwords are a risk and highlights how they are traded on the underground."

Covid complications

The Covid-19 pandemic hasn't helped the situation. Organisations have had to scramble to put in place the necessary infrastructure to enable working from home. And just as the distinction between work life and home life has become blurred, so has the use of personal and company-issued devices. The employee's personal laptop or smartphone is beyond the management and protections put in place by the organisation – and this includes such precautions as anti-malware, anti-phishing, data loss prevention and even basics like password rotation and minimum password standards.

It's not just a matter of non-approved hardware and software being employed for company business – the tools the organisation itself has adopted might not be up to its usual security standards, and Zoom certainly comes to mind here. Hastily configured VPNs or other collaboration tools may not have been implemented with the usual care and testing – and the various new tools just add to the number of passwords employees have to remember. All of this adds up to an increased attack surface.

"Enterprise security is even more complex and bordering on being unmanageable – a trend that started before the pandemic and global lockdowns"

Also, as Jeremy Hendy, CEO at Skurio, points out: "With many organisations adopting remote working, unauthorised access is harder to detect. Criminals may spend weeks or months monitoring email communications waiting for the right opportunity, for example, to execute a payment diversion attack by impersonating a member of staff or a supplier."

You have to think beyond the users, too. Brian Trzupek, SVP product emerging markets at DigiCert, points out that, "Credentialing is more than just users – it also includes devices. In a remote work environment, companies may adopt a bring-your-own-device (BYOD) policy, allowing personal devices to access the corporate network. Those devices need to be authenticated as attackers may target home devices for individuals working from home."

That authentication is unlikely to have happened with personal devices. And the working-from-home phenomenon, which is likely to linger long after the pandemic has faded away, has resulted in the increased use of cloud services and infrastructure. That's not necessarily a good thing, because things were difficult even before the pandemic hit.

"Across SaaS and cloud apps, credential abuse is a top attack vector," says Peter Margaris, head of product marketing at Skybox Security. "Enterprise security is even more complex, and bordering on being unmanageable – a trend that started before the pandemic and global lockdowns. Most organisations have transitioned and continue to transition from on-premise networks to a distributed workforce that relies heavily on cloud applications, spawning credential-based attacks that infiltrate the new ingress and egress points to corporate entities from home networks."

Who's doing it?

As for who is behind credential abuse, it's a case of the usual suspects.

"Often the most common abusers are nation states or those suspected of being affiliated with nation states," says Chris Hickman, chief security officer at Keyfactor. "Attackers running a nation-state campaign will look at larger credential repositories and seek to compromise multiple points of data to build a profile related to a targeted identity. These kinds of campaigns often have financial or political motivations driven by information-gathering intent. We have seen these attacks materialise with the massive Marriott breach and smaller breaches through the US Government. These breaches follow the same method, which is to create patterns around activities and behaviours for target access."

However, cyber criminals haven't been slow to take advantage of the same data sources and tools.

"There is an entire underground ecosystem behind this type of attack and monetisation process," explains Anna Chung, principal researcher, Unit 42 at Palo Alto Networks. She lists some of the key players as:

Anna Chung, Palo Alto Networks: "There is an entire underground ecosystem behind this type of attack and monetisation process."

- Account takeover (ATO) tool developers: programmers/developers with technical skills building phishing sites, phishing kits, brute-forcing tools and account validation tools, allowing other criminals to automate the ATO processes.
- Attackers: hackers conduct the actual attacks and sometimes sell and trade the compromised credentials collected from victims.
- Dump shops: virtual shops allow cyber criminals to sell compromised credentials to others.
- Fraudsters who purchase compromised account credentials to commit fraud or other illegal activities.

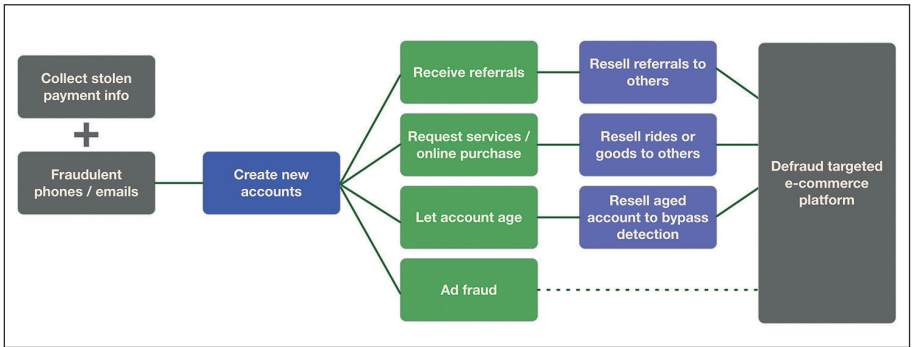
"More fraudsters are trying their hand and quickly realising they need to automate their jobs just like any analytics professional"

"Phishing is also a common approach to collecting large amounts of user credentials," she adds. "There is a different business model/workflow abusing stolen credentials to create new accounts for the victims on the new platforms. It is more like an account integrity issue and advertisement fraud."

Chung expanded on this with a presentation at Black Hat Asia 2018 (see diagram).[5]

This is creating thriving markets, as Nathan of LexisNexis explains. "The price of credentials for accounts purchased on the dark web has actually increased as much as 80% over the last five years," he says. "More fraudsters are trying their hand and quickly realising they need to automate their jobs just like any analytics professional. Other methods typically focus around brute force attacks used on RDP service to deploy ransomware, social engineering and web inject malware used to retrieve credentials."

And, of course, we can't rule out the insider threat. A maliciously minded employee with genuine credentials is a serious threat, which is why so many security practitioners have been preaching the gospel of least privilege for so long. But even without evil intent, insiders can be a problem. As mentioned earlier, sharing credentials to get the job done is an all-too-common practice. Poor protection of credentials (including the infamous sticky notes) is a factor too. But arguably the most prevalent threat is when workers innocently hand over credentials. As Hickman of Keyfactor explains: "100% of the time, insiders are unknowingly involved in credential abuse, though having insiders knowingly involved is more of an exception than the rule. Last year's Shopify breach is a good example of a breach that was fully driven by a willing insider participant. We see less of those types of incidents and more events driven by phishing attacks where insiders unknowingly surrender credentials."[6]



The fraud and monetisation flow model. Source: Anna Chung, Palo Alto Networks.

Old credentials

Strangely, bad actors continue to trade compromised credentials from data breaches that happened years ago.

"We need to ask ourselves why? I mean surely credentials exposed years ago have either expired or have been identified and changed right?" asks Bryan Jardine, director of product management at Appgate. "Surprisingly, this is not always the case. If we look at these lists the way we would look at data in our environments, say for model validation or a set of testing data, then it is easy to see that as a potential bad guy I have a good sample set of data I can use to validate my software. Additionally, by using aged data sets I can determine potential security weaknesses or policy weaknesses to exploit if some of those credentials are still valid. Lastly, with the reduced cost of sophistication and the adoption of proxy networks by many legitimate users, it becomes harder to isolate the abuse-like access attempts to filter traffic."

"Once attackers are inside the account, they will look for certain opportunities to commit some very targeted fraud. One way they do this is by finding email exchanges dealing with invoices, purchase orders, etc"

Most leaked datasets that come from breaches include a lot more than just usernames and (hopefully hashed and salted) passwords.

"We have seen the breached data is more of a multi-purpose dataset," says Jardine. "The automation of creating dossiers of data with both known and unknown variables has allowed for a lot of automated 'guess work' in which with just a known-good email address, a bad actor can start to generate password fields based on information they may have gathered from associated credentials or previous breaches, even if password sharing is not involved.

"Additionally, with the broad adoption of account-based access for trivial Internet platforms like social media, news, music, gaming or video, as an attacker I have a number of testbeds to perform my credential validation attacks before using them on my intended target. This keeps me under the radar longer, with a more focused and deliberate list of credentials to use. Doing so helps my attacks from appearing to be detected as brute force, or masking a velocity attack by allowing me to only hit the site a number of times that is more in line with expected traffic and removes my dependency on using botnets that may be known and blocked."

"With the broad adoption of account-based access for trivial Internet platforms like social media, news, music, gaming or video, as an attacker I have a number of testbeds to perform my credential validation attacks"

He adds: "The open concern here is anonymised traffic. The institutions we do business with have a valid sub-set of account accesses occurring through anonymisers or proxies. Due to this legitimate traffic, security controls have a harder time isolating targeted attacks, while brute force is still relatively easy to see in the NOC [Network Operations Centre]."

Standard techniques

At the beginning of the article, we touched on the various forms that credential abuse takes. Here, we're specifically concerned with automated or large-scale attacks.

"Both brute force and credential stuffing are effective when dealing with accounts that use weak passwords or whose owners are not cyber-savvy, but less so with some of the more secure accounts," says Kamal Bechkoum, head of the School of Computing and Engineering at the University of Gloucestershire.

But we shouldn't dismiss the threat to organisations from such crude techniques as brute forcing. "In Q2 of 2020, 5% of all attacks on organisations were performed by brute forcing credentials," says Positive Technology's Kilyusheva. "In the first half of 2020, brute-force attacks gained more relevance, because many companies transferred employees to remote work and made some of the services available from the Internet. Other popular methods include phishing emails with links to a fake authentication form."

And it's working, she says. "The share of credentials stolen has grown from 15% in Q1 in 2020 to 30% in Q2 of all data stolen in attacks on organisations.[7,8] Corporate credentials are in particular demand. They are sold by cyber criminals on the dark web or used for further attacks – for example, to send emails with malicious attachments on behalf of compromised organisations. Credentials of compromised companies' clients are also in demand."

Targeted attacks are potentially more devastating. It means the attacker is specifically going after your organisation. There are many things an attacker can do with valid credentials, but one increasingly popular option is a BEC scam.

"These attacks come in a wide range of formats," says Troy Gill, manager of security research at Zix. "Many of these involve using stolen credentials to access a user's email account through a web portal. Once attackers are inside the account, they will look for certain opportunities to commit some very targeted fraud. One way they do this is by finding email exchanges dealing with invoices, purchase orders, etc. The attackers will then create new messages using these existing threads to solicit payments to an account controlled by them. The threat actors will generally limit their amount in accordance to what they think they can get from the target. The majority of these are in the neighbourhood of $30,000-$50,000 but when the opportunity presents itself they will net millions, like what happened to a Toyota subsidiary.[9] Additionally, we have also seen very similar attacks where instead of committing financial/wire transfer fraud once inside the account, attackers will use them to launch

malware attacks from existing email conversations. We dubbed this the 'conversation hijacking attack' and it can be used to distribute malware like banking trojans, ransomware and spyware."[10]

Credential stuffing

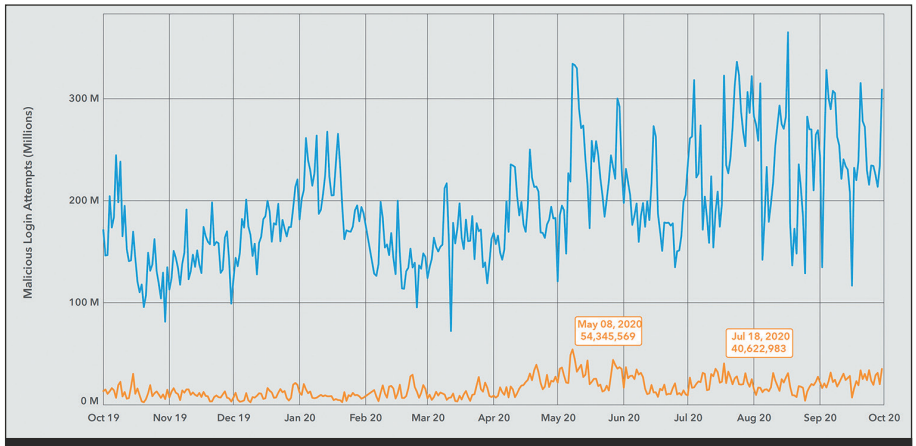
Increasingly, though, the attacks we see revolving around credential abuse exploit credential stuffing – using lists of previously breached usernames and passwords. This problem stems from people reusing their passwords and being unaware that their credentials were involved in a data breach.

"One of the reasons credential stuffing attacks are so popular, especially with new hackers, is that they are so simple, and require barely any technical expertise or flair"

The 2020 edition of Akamai's 'State of the Internet' report, and its offshoot that specifically looked at credential stuffing in the media sector, saw an overall ramping up of activity.[11] There was one notable dip at the end of August 2020 when the Empire darknet marketplace went offline and criminals had to scatter in search of other locations to buy and sell stolen credentials. Overall, though, Akamai noted that there is an increasing flood of credential lists, leading to tens of millions of attacks per day.

The media sector isn't the only major target of credential stuffing. Back in 2019, Akamai reported that streaming services were the most commonly attacked targets. Services such as Netflix, Hulu et al are considered high-value targets and stolen credentials are heavily traded on the dark web.[12] And gaming is another sector that Akamai highlights as a popular target. Over a 17-month period the firm recorded around 55 billion credential stuffing attacks against online services, of which 12 billion were aimed at the gaming industry.[13]

And as you might expect, the financial sector is another favourite among cyber criminals. On 7 Aug 2019, Akamai registered more than 55 million credential stuffing attempts against a single financial services firm.



Daily credential abuse attempts in the period October 2019 to September 2020 – overall and for the media sector. Source: Akamai.

"One of the reasons credential stuffing attacks are so popular, especially with new hackers, is that they are so simple, and require barely any technical expertise or flair," explains Stuart Jubb, head of consulting at Crossword Cybersecurity.

"The first ingredient of an attack is sets of credentials and these are extremely easy to find and buy online. Research earlier this year from Digital Shadows found that the number of username and password credentials openly for sale on the dark web has tripled in two years to more than 15 billion."

"It's not so much who is doing the abusing, but what. Humans are now the minority of Internet users, with automated bot traffic accounting for more than half of all Internet traffic"

Another factor, he says, is the easy availability of proxy services, "which help hackers evade detection by making logon attempts appear to come from multiple locations, in the same way normal login attempts would. Lists of proxy servers are readily available online, and tools can be configured to rotate through a provided list."

Credential stuffing is, therefore, a highly effective technique with relatively low risk, although many threat actors may use a combination of techniques.

"Take, for instance, the database with about 500,000 Zoom users, on sale on the dark web a few months ago," says Cagnoni. "Zoom wasn't hacked, they just used credential stuffing to check which accounts were using a password leaked within another breach. Brute force is not that effective unless you have enough time. Most applications have account lockdown after consecutive errors. With that, an attack would need to use just a couple of tries per day, for example. If the attackers get access to users and a hashed passwords database, they can use cracking tools to get passwords. If they have access to a machine, they can use tools like Mimikatz to dump local passwords and this has been one of the top three malwares used on attacks in the past couple of years. Finally, phishing attacks can be quite effective. Remember that for a remote access/VPN attack, all it takes is one stolen credential."

It's also worth bearing in mind that a credential stuffing attack can affect your organisation in more ways than just hoodwinking your authentication processes.

Stuart Jubb, Crossword Cybersecurity: "One of the reasons credential stuffing attacks are so popular, especially with new hackers, is that they are so simple."

Andy Still, Netacea: "We're now onto the third generation of bots, which look like browsers and are often executed from consumer browsers or even browsers modified to bypass client-side protections."

"Thousands of credentials might be thrown at a website and tested from multiple servers," says Jubb at Crossword. "This leads to poor performance on the website and can even take it offline, in a type of denial-of-service attack. Where this is the goal, no black market credentials are needed at all."

Curse of the botnets

As far back as 2018, Akamai noted that botnets were increasingly being repurposed, moving away from distributed denial of service (DDoS) and turning to credential abuse.[14] In two months, the firm monitored 17 billion login requests through its platform and found that 43% were attempts at credential abuse.

The increase in credential abuse was also highlighted by Centrify in its 'Mid-Year Data Breach Report' in 2019, where the firm ranked it as the top threat facing organisations.[15,16] It noted that three-quarters (74%) of data breaches involved privileged access abuse; half of firms (52%) don't use a password vault; 65% share credentials between multiple people for root or privileged access to systems; and 55% don't use privileged access management (PAM) solutions for cloud workloads.

"It's not so much who is doing the abusing, but what," says Andy Still, CTO at Netacea. "Humans are now the minority of Internet users, with automated bot traffic accounting for more than half of all Internet traffic. Manually sifting through stolen passwords and usernames, known as combo lists, to hijack accounts won't yield results. Yet, bots can check thousands of credentials every minute, making finding the needle in the haystack not just possible but extremely profitable."

He adds: "We're now onto the third generation of bots, which look like browsers and are often executed from consumer browsers or even browsers modified to bypass client-side protections. The third generation of bots can carry out much more sophisticated types of account takeover, application distributed denial of service (DDoS), API abuse, carding and ad fraud attacks as well as specific targeted business logic attacks. They can simulate basic human-like interactions, such as simple mouse movements and keystrokes, which allows them to fly beneath the radar of legacy cyber security solutions."

"Once bad actors have bought these lists, they use automated bots to trial these passwords and usernames on login pages at a far greater rate than a human possibly could"

The botnet is now seen as the key enabler of credential stuffing. "There are darknet marketplaces of botnets available for attackers to use to automate their attacks," says Jamie Hughes, lead solutions engineer at Auth0. "Some of these botnets are already pre-configured to attack certain organisations. With very sophisticated tools, which allow a list of proxies to be loaded as a parameter, the botnet will switch out the IP address for each request. A large percentage of these IPs will be recycled from residential networks (not on blacklists) – one bot sending five requests every 10 minutes doesn't look that suspicious. Multiply that by 10,000 and you're getting somewhere, and the victim site doesn't really notice. Upon a successful breach, some botnets even scrape the account and mark its value so it's ready to be packaged up and sold on a darknet marketplace."

Those marketplaces are also where cyber criminals go to pick up the so-called 'combo' lists – aggregated user data compiled from multiple breaches – which will then be fed to the bots. "Troy Hunt, a cyber security expert, found 770 million matching usernames and passwords for sale back in 2019," says Still. "Once bad actors have bought these lists, they use automated bots to trial these passwords and usernames on login pages at a far greater rate than a human possibly could, and find those accounts that are still 'open for business'."

"Once bad actors have bought these lists, they use automated bots to trial these passwords and usernames on login pages at a far greater rate than a human possibly could"

And as with every other aspect of computing, artificial intelligence (AI) is now being exploited to make attacks more effective. "The use of AI augmented algorithms adds sophistication to the attacker's arsenal," says Bechkoum. "AI bots are used to gather pertinent data – for example, chatbots realistically befriending employees on social media, using convincing impersonation to bypass controls. This 'AI-powered reconnaissance phase' limits the search space. AI algorithms (eg, machine-learning password crawlers) are then applied to guess the credential(s) in a matter of seconds.

Target for tonight

Everyone is a target for a credential abuse attack, but not necessarily in the same way. In the world of cyber attacks, we see some that are bulk, spray-and-pray campaigns that rely on large numbers of attacks to reap a relatively small number of hits. Many spam and phishing campaigns fall into this category. Others are carefully targeted – spear-phishing and BEC are good examples here. So what do we see with credential abuse-based attacks – bulk or targeted?

"Both," says WatchGuard's Cagnoni. "It really depends on what the attacker is looking for, but I would say most target bulk users. Bulk attacks are commonly used when targeting consumers in general, for example to get access to accounts

Brian Trzupek, Digicert: "APIs do expose another public endpoint that needs to be analysed for risk."

to make purchases. It's also very common to use those attacks to install ransomware within a company network."

He adds: "Targeted attacks usually take more time and require strategy to achieve specific objectives. In 2019, we saw attacks targeted at managed service providers (MSPs). The main goal of the hackers was to steal credentials from anyone from the MSP's technical team. With those credentials, they would potentially get access to computers in multiple companies, managed by the MSP. This is a very smart way to reach dozens of companies, while targeting just the one."

"Connected devices can leave an organisation vulnerable if not secured properly. Managing the pool of devices connected to your corporate network is a pressing and growing challenge, with serious risks if not handled correctly"

Again, it's worth pointing out that this is a problem that affects not only people – although we readily associate credentials with user passwords – but also hardware, some of which gets too little attention when it comes to authentication.

"We're going to see Internet of Things (IoT) devices becoming a larger threat within all organisations as IoT devices themselves become a larger breach target," says Hickman. "Webcam-based attacks are an example of the kinds of events that will grow in frequency and popularity. The reality is that a large majority of IoT devices are still being brought to the same level and standards as enterprise security. There is more work to do to better secure IoT; in the meantime, these devices will continue to be a popular attack target."

The same extends to many other devices, such as routers, VPN servers – and indeed anything that is connected to the Internet.

"Connected devices can leave an organisation vulnerable if not secured properly," says Trzupek. "Managing the pool of devices connected to your corporate network is a pressing and growing challenge, with serious risks if not handled correctly. You will probably want multi-factor authentication or even public key infrastructure (PKI) for secure login. And if a device joins your VPN, you want to be able to have control over the device remotely. Remote device control provides you with the ability to manage what is on that device, how it accesses your network and resources, and who can use it."

Vulnerable APIs

Analysis by Akamai over two years noted more than 85.4 billion credential abuse attacks, nearly 20% of them against API endpoints.[17] APIs have become a crucial part of many organisations' IT infrastructure. "They allow for automating a larger volume of data and are designed for when a manual process just would not be able to keep up with demand," says Trzupek of Digicert. However, he adds: "APIs do expose another public endpoint that needs to be analysed for risk. As with other endpoints that increase the attack surface, they need to be secured in a manner that protects the consumer as well as the organisation providing the API."

"In digital banking, five years ago we saw a 50:50 split between account takeover and social engineering. Now it's approaching 80:20 in favour of social engineering"

The problem is that they are almost the perfect target for attacks such as credential stuffing. "APIs by their nature enable automation of attacks by hackers and their bots," says Luis Martinez, director of engineering, cloud operations at JumpCloud. "To deal with this, organisations need to add more security, including more alerting, monitoring and auditing at their API layer."

Mike Nathan, LexisNexis: "As organisations have increased spending on cyber and fraud systems, they have realised the weakest point in the chain is not the organisation but the end user."

Hughes at Auth0 explains that it's more than just having a single interface against which you can try lots of passwords: "Attacks specifically target the authentication endpoints of an API which would issue the necessary authentication tokens if successfully breached with a valid set of credentials. Once the attacker has this token it could then potentially be used to call other endpoints to query that user's data or perform actions on behalf of the user. This is where API security and authorisation are key, to ensure a user doesn't have privileged access by only using a first factor (like a username and password). Organisations should be adopting the principle of least privilege, ensuring that customers authenticating with only a first factor are only authorised for a minimum set of permissions. Sensitive data and actions are protected with step-up authentication (such as MFA)."

Attack trends

Nothing remains the same, even with something as apparently simple as misusing credentials. As technology and defences evolve, threat actors will always look for any vulnerable spots that have been created. For example, while the one-time passcode (OTP), such as a PIN sent via SMS to your phone, is one of the oldest forms of

multifactor authentication (MFA), criminals still find new ways of subverting it.

"Hackers are now using complex social engineering and SIM-swapping attacks to undermine the protections that OTP provides," says Chad Thunberg, CISO at Yubico. "Companies will need to adopt more modern authentication technologies like smartcard, universal two-factor authentication (U2F), or WebAuthn if they are interested in a more resilient multi-factor authentication solution."

Nathan at LexisNexis says his organisation has also seen a significant increase in the use of social engineering. "As organisations have increased spending on cyber and fraud systems, they have realised the weakest point in the chain is not the organisation but the end user," he says. "In digital banking, five years ago we saw a 50:50 split between account takeover and social engineering. Now it's approaching 80:20 in favour of social engineering. And social engineering losses are typically much higher than account takeover."

And credential attacks are not always about passwords. "From the underground credential shops' perspective, criminals have started to sell stolen browser cookies instead of victims' emails and passwords," explains Chung at Palo Alto. "Cookies allow cyber criminals to access unique sessions without a password and login."

Targeted attacks often leverage a large amount of research carried out by the attackers in order to improve their chances of success and often leading to a form of blended attack. According to Bechkoum at the University of Gloucestershire: "There is traditional credential-stealing, but also the manipulation of business practices. A combination of these were used in the Scattered Canary attack on US financial benefits early in the coronavirus epidemic.[18] This took advantage of non-verification of financial claims, but was also built on credential theft and presumably the storage of credentials in preparation for just such an opportunity."

It's clear that credential abuse is one of the greatest threats facing organisations.

The next issue of Network Security *will include the second part of this feature looking at mitigations and solutions designed to address the problem.*

About the author

Steve Mansfield-Devine is a freelance journalist specialising in information security. He is the editor of Network Security and its sister publication Computer Fraud & Security.

References

1. 'Privileged Access Threat Report 2019'. BeyondTrust, 2019. Accessed Feb 2021. www.beyondtrust.com/resources/whitepapers/privileged-access-threat-report.
2. 'Penetration testing of corporate information systems'. Positive Technologies, 2020. Accessed Feb 2021. www.ptsecurity.com/upload/corporate/ww-en/analytics/external-pen-tests-2020-eng.pdf.
3. Brodkin, Jon. 'Hacker says he correctly guessed Trump's Twitter password – it was "maga2020!"'. Ars Technica, 22 Oct 2020. Accessed Feb 2021. https://arstechnica.com/tech-policy/2020/10/hacker-says-he-correctly-guessed-trumps-twitter-password-it-was-maga2020/.
4. Krebs, Brian. 'Security blueprints of many companies leaked in hack of Swedish firm Gunnebo'. Krebs On Security, 28 Oct 2020. Accessed Feb 2021. https://krebsonsecurity.com/2020/10/security-blueprints-of-many-companies-leaked-in-hack-of-swedish-firm-gunnebo/.
5. Chung, Anna, 'Hourglass Model 2.0: Asia-based underground services abusing global 2FA'. Black Hat Asia 2018, Mar 2018. Accessed Feb 2021. https://i.blackhat.com/briefings/asia/2018/Asia-18-CHUNG-Hourglass-2.0.pdf.
6. Cimpanu, Catalin. 'Shopify discloses security incident caused by two rogue employees'. ZDNet, 23 Sep 2020. Accessed Feb 2021. www.zdnet.com/article/shopify-discloses-security-incident-caused-by-two-rogue-employees/.
7. 'Cybersecurity threatscape: Q1 2020'. Positive Technologies, 2020. Accessed Feb 2021. www.ptsecurity.com/upload/corporate/ww-en/analytics/cyber security-threatscape-2020-q1-eng.pdf.
8. 'Cybersecurity threatscape: Q2 2020'. Positive Technologies, 2020. Accessed Feb 2021. www.ptsecurity.com/upload/corporate/ww-en/analytics/cyber security-threatscape-2020-q2-eng.pdf.
9. Lindsey, Nicole. 'Toyota subsidiary loses $37 million due to BEC scam'. CPO Magazine, 20 Sep 2019. Accessed Feb 2021. www.cpomagazine.com/cyber security/toyota-subsidiary-loses-37-million-due-to-bec-scam/.
10. Gill, Troy. 'Attackers leverage stolen email credentials in malware attacks'. AppRiver. Accessed Feb 2021. https://appriver.com/blog/201802attackers-leverage-stolen-credentials-malware-attacks.
11. 'State of the Internet 2020'. Akamai. Accessed Feb 2021. www.akamai.com/uk/en/resources/our-thinking/state-of-the-Internet-report/archives/state-of-the-Internet-security-reports-2020.jsp.
12. 'Streaming services among the most targeted by credential stuffing attacks according to Akamai report'. Akamai, via Cision, 8 Apr 2019. Accessed Feb 2021. www.prnewswire.com/news-releases/streaming-services-among-the-most-targeted-by-credential-stuffing-attacks-according-to-akamai-report-300825838.html.
13. Barth, Bradley. 'Gaming industry has become popular target of credential stuffing attacks: study'. SC Media, 13 Jun 2019. Accessed Feb 2021. www.scmagazine.com/home/security-news/gaming-industry-has-become-popular-target-of-credential-stuffing-attacks-study/.
14. Sutton, Mark. 'Botnets being turned to credential abuse, says Akamai'. ITP.net, 27 Feb 2018, Accessed Feb 2021. www.itp.net/616656-botnets-being-turned-to-credential-abuse-says-akamai.
15. McNeely, David. 'Centrify Mid-Year Data Breach Report: Credential Abuse, a Top Threat of Cyber

Attacks'. Centrify, 5 Aug 2019. Accessed Feb 2021. www.centrify.com/blog/centrify-data-breach-credential-abuse/.
16. 'Survey: Privileged Access Management in the Modern Threatscape'. Centrify. Accessed Feb 2021. www.centrify.com/resources/centrify-privileged-access-management-in-the-modern-threatscape-2019/.
17. 'Most credential abuse attacks against the financial sector targeted APIs'. Help Net Security, 20 Feb 2020. Accessed Feb 2021. www.helpnetsecurity.com/2020/02/20/credential-abuse-attacks/.
18. Brunner, Jim; Roberts, Paul; Malone, Patrick. 'How missed 'red flags' helped Nigerian fraud ring 'Scattered Canary' bilk Washington's unemployment system amid coronavirus chaos'. Seattle Times, 24 May 2020. Accessed Feb 2021. www.seattletimes.com/seattle-news/times-watchdog/how-missed-red-flags-helped-nigerian-fraud-ring-scattered-canary-bilk-washingtons-unemployment-system-amid-coronavirus-chaos/.

The state of zero trust in the age of fluid working


Ollie Sheridan

Ollie Sheridan, Gigamon

Businesses have been thrown a curve ball that could never have been predicted at the beginning of last year, and one that has changed businesses practices forever. While many organisations had some form of fluid working before, it is now non-negotiable as business leaders have seen first-hand that the workforce can be just as productive at home as they can in the office.

As a result, we've seen a boom in the adoption of enterprise technologies to support this new way of working – everything from video conferencing software to virtual communication tools. However, one aspect of business that shouldn't be forgotten is cyber security.

Taking advantage

Cyber criminals are taking advantage of the shift to working from home to launch increased numbers of cyber attacks – the numbers of phishing schemes, data breaches and insider threats have all risen this year. In fact, the results of a recent survey found that 84% of EMEA decision-makers have experienced an increase in attacks since the beginning of 2020.[1] This can be largely attributed to the increased responsibility that employees have been granted – they have become the gatekeepers of the network, away from the watchful eye of IT and security teams. However, this is a preventable threat. With thorough and continual cyber security awareness and education, which will minimise the use of shadow IT and make employees more aware of how to identify a phishing attack, organisations can ensure that their perimeter stays secure.

It's important to remember that, while there has been an adjustment process for many businesses, malicious actors have always worked remotely and this period hasn't slowed them down. If anything, they've benefitted from the pandemic. Many organisations have implemented a patchwork of software to quickly enable remote working – overnight in some cases – meaning that cyber criminals could easily find their way through the cracks, especially as a dangerous number of employees are using insecure devices and wifi to access corporate networks. Therefore, as well as education, organisations have been seeking to invest in new cyber security measures to ensure that their users, assets, applications and infrastructure stay secure.

Never trust, always verify

Zero trust is one such security framework that has been gaining traction over recent months. At the base level, zero trust moves a business's core line of defence from the network edge to within its boundaries. This involves not granting implicit trust to any user, device or application inside or outside the network until it has been verified, removing the risk of malicious actors leveraging a privileged account to access the network. However, it doesn't stop there. As well as authentication and access control policies, zero trust requires the continuous monitoring of all information-in-motion on the network to enable the rapid identification of threats.

"Zero trust is an ongoing process that evolves with the organisation and its needs, but decision-makers will feel the benefits from the offset"

This framework isn't a new idea but it has traditionally had negative connotations due to its 'never trust, always verify' message – the idea being that employee productivity is hindered. However, perceptions are changing, as 89% of decision-makers have already adopted or are considering adopting zero trust architecture. What's more, 87% of those who

have adopted this strategy have found it has actually improved their productivity – a by-product that has been especially welcome this year as economic uncertainty hit and businesses were faced with the prospect of operating with a skeleton workforce. These productivity gains can be attributed to the system running faster, fewer security breaches and reduced downtime. What's more, in addition to restricting access, zero trust enables trust by ensuring that each user or device is granted access to the resources they need, when they need them – reducing the frustration and delay that comes with trying to obtain access.

"Enterprises have coped well so far, but the only way they can hope to survive in the fluid working landscape is with enhanced investment into cyber security, including zero trust"

So, away from improved productivity, what's the motive behind adopting zero trust in today's landscape? EMEA decision-makers concluded that it is to make their network more secure and mitigate risk (54%), to make their data more protected and easier to manage (51%) and to reduce the risk of employees compromising the system (49%). Visibility is a key theme here and is synonymous with zero trust as you can't manage what you can't see. With network complexity increasing due to the plethora of devices and users that are accessing the network from multiple locations, unclouded visibility is crucial to grant access, monitor the actions of users to identify suspicious activity and respond to threats quickly.

Stepping stones

It is important to note, however, that zero trust isn't a product – it can't be bought. Rather, it's a journey that must be undertaken, an architecture or mindset that must be adopted. Zero trust is an ongoing process that evolves with the organisation and its needs, but decision-makers will feel the benefits from the offset.

As with any journey, business leaders must first ensure that they're prepared. This starts with laying the correct groundwork in order to maximise ROI. Ensuring that IT and security teams have full visibility into all information-in-motion on the network is a necessity here. Without visibility, adopting a zero trust framework is impossible.

To lay the foundations of a zero trust approach, businesses need to understand where their most valuable data and applications are in order to protect and verify access to them. This is often an advisable starting point for companies just beginning their journey, as it can allow them to create a tailored perimeter around the most critical parts of the network, which is far more manageable than implementing the framework indiscriminately. This discovery also needs to extend to the users, applications and devices on the network. Monitoring and analysing traffic will uncover the typical behaviour exhibited by every asset, and anomalies will become clear, allowing IT and security teams to rapidly neutralise possible threats.

"Many organisations have implemented a patchwork of software to quickly enable remote working – overnight in some cases – meaning that cyber criminals could easily find their way through the cracks"

What's more, enterprise networks are expanding and evolving. Businesses need to ensure that IT and security teams' complete visibility extends to physical, virtual and cloud environments, as well as into encrypted traffic – especially TLS 1.3 traffic, which is more complex than previous versions of the industry standard. No stone can be left unturned or else network monitoring tools will be running blind.

In order to streamline the process, enterprises can look to invest in a tool that will decrypt all encrypted data on the network and send only the relevant traffic to each monitoring tool to analyse before re-encrypting it. This centralised approach will improve the effectiveness of the network tools – as they no longer have to trawl through irrelevant or duplicated traffic – and will mitigate network latency.

As zero trust directly impacts employees' day-to-day jobs, cultivating a culture of acceptance is also key. In fact, wrong company culture was the biggest challenge (65%) cited by those who looked into starting their zero trust journey but decided against it. At the opposite end of the spectrum, it's crucial to obtain board support – especially as purse strings remain tight – but this isn't as simple as it seems, given the benefits of this framework. Some 49% of businesses feel that while IT and security teams recognise the value of zero trust, this belief hasn't yet risen up to the board. While cyber security is starting to appear on the boardroom agenda, this is something that must be evaluated before beginning on the journey.

What's next?

IT and security teams have battled the Covid storm and the majority have emerged safely into the 'new tomorrow'. So, what are they set to face next? In terms of challenges, EMEA decision-makers still see digital transformation (50%) as a key issue they will face over the next few years – legacy IT obviously remains a major headache – as well as shadow IT (45%), employee security education (37%), an increase in applications to monitor and protect (36%) and managing a complex working landscape (35%). These results exemplify the pressure that IT teams are under, and the evolution that their roles – and the network itself – are set to undergo as time goes on. It is only by investing in new technologies and altering their processes to suit the new cyber-landscape that they'll keep up.

Fortunately, decision-makers expect to heavily prioritise security going forwards – keeping developments safe and secure in the cloud (44%) and ensuring no security breaches or compromise (41%) are their top priorities. However, the long-term effects of the pandemic are unavoidable and are likely to linger for a

while yet. Businesses expect to focus on maintaining a work-from-home (WFH) infrastructure (37%) and managing digital transformation but with lower budgets and uncertainty (36%) as well.

Enterprises have coped well so far, but the only way they can hope to survive in the fluid working landscape is with enhanced investment into cyber security, including zero trust. With this framework, businesses can not only mitigate the expanding cyber threatscape but can benefit from increased visibility and a clearer view of everything on the network, which will enhance IT efficiencies. Going forward, employees will continue to hold more power when it comes to keeping the network secure, so as well as investment into security architecture, security education and awareness training is paramount. Fortunately, industry perceptions of zero trust are changing and we hope to see adoption increasing. As long as decision-makers lay the correct groundwork, a zero trust framework will help them stay secure and emerge stronger into the new tomorrow.

About the author

Having been a Certified Information Systems Security Professional (CISSP) for over 13 years, Ollie Sheridan is Gigamon EMEA's principal security engineer and security strategist. His experience in assisting organisations to improve their security posture has ranged from developing security standards and writing security assessments for major financial institutions, to providing assistance in dealing with complex security incidents such as DDoS attacks.

Reference

1. 'Survey: The IT and security landscape for 2020 and beyond and role of zero trust'. Gigamon, 2020. Accessed Feb 2021. www.gigamon.com/resources/resource-library/analyst-industry-reports/ar-zerotrust-surveyreport.html.

Avoiding costly downtime – how MSPs can manage their networks

Brendan Walsh

Brendan Walsh, Opengear

For managed service providers (MSPs), managing a network is a big responsibility. Availability is the top priority in order to provide customers with constant access to critical applications that help to ensure that their businesses are able to function.[1] When a network goes down this can be due to a variety of causes such as cyber attack, hardware failure or human error and this downtime can be extremely costly. ITIC's latest 'Global Server Hardware, Server OS Reliability Survey' found that a single hour of downtime now costs 98% of firms at least $100,000.[2]

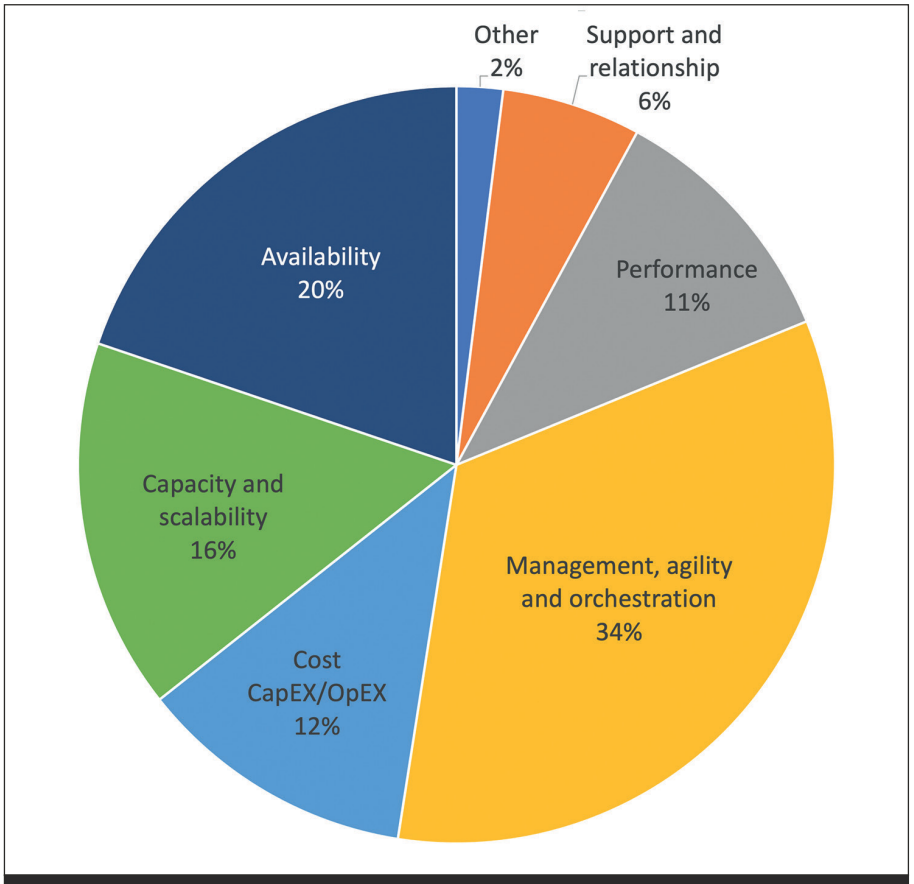
The need for network resilience has become even greater during the Covid-19 pandemic. Many employees who have adapted to working from home are continuing to do so. The requirement to work from home has placed increased strain on networks and a heightened sense of importance on seamless connectivity. With some businesses choosing to switch permanently to a hybrid model where workers can choose to work from home or the office, it seems that the need for MSPs to ensure greater resilience and uptime may be here to stay.

Causes and consequences

Surges in demand and increased network traffic from the remote working revolution and the switch to the hybrid model could potentially cause an increase in outages. A scaled-back workforce could make dealing with the increased network traffic and demand more challenging for MSPs and could also provide hackers with exploitation opportunities.

There is a range of other factors at play here that, even if not increasing network downtime, at least make organisations more vulnerable to it. Historically, branch offices used to run their own servers, which synched up as a local area network. Staff working in those branches could work autonomously away from the main wide area network. Today, when staff lose access to the corporate network, they can't work effectively, making it more vital than ever that the network stays up.

Yet, there are many threats to their network uptime still in place. While there is constant investment and improvement of network reliability and robustness, there is always a chance that a hardware failure from software updates or misconfiguration, through to database faults can lead to downtime. Depending on the severity of the fault, that downtime can last for days. Even in the best-case scenario where downtime might last



Organisations' main criteria when evaluating network solutions. Source: Gartner.

only a couple of minutes, the impact on the enterprises relying on the affected network can be serious.

"The momentary loss of business-critical applications that rely on an affected network can bring enterprises to a grinding halt"

Take supermarkets, for example: many of them simply can't operate without a network in place. On numerous occasions, supermarkets have had to close their doors because the network for their point of sale (POS) equipment failed, preventing them from processing payments. Sometimes, such problems have stemmed from the datacentre, sometimes it was the broadband provider and sometimes it was the local branch network. The result is typically the same though – without a working network, the supermarket has to shut down. We have seen petrol stations shut down also. They may be able to dispense fuel but if the payments network is down, they are not able to charge anyone and will have to close their doors to the public.

For banks, network downtime inevitably means loss of customers and reputation. Customers will be unable to access funds and may defect to competitors; deals will fail to go through, which will impact brand image. Depending on the nature of the outage, there may also be regulatory fines to contend with. In the airline sector, another industry that has suffered badly from network downtime, outages typically result in cancelled or delayed flights, loss of income and loss of customer trust.

Negative impacts

The truth is, however, that across all industries, downtime has negative impacts on enterprises, from huge revenue losses, to damaged customer relationships leading to reputational damage, to loss of productivity. Worse still, the momentary loss of business-critical applications that rely on an affected network can bring enterprises to a grinding halt. In this scenario, the loss of data from that application can result in legal and financial headaches.

In such scenarios, relationships between enterprises and MSPs they once relied on can quickly turn sour as network outages are often a breach of service level agreements (SLAs). Some enterprises might seek financial recuperation from the MSP while others might look to change providers completely. For MSPs, this can result in more than losing valuable customers – it can also have a negative impact on their reputations and can result in fines.

Protecting SLAs

Every MSP knows full well it needs to ensure uptime for customers. MSPs also know that maintaining uptime is key to improving margins and meeting SLAs. Today, also, in the current difficult economic times, with Covid-19 continuing to impact business confidence the world over and businesses more reliant on the network than ever, MSPs need to accept that their clients are going to be pushing them really hard to 'keep the network alive'. The days of addressing an outage within an allowable response time allocation are quickly coming to an end. That's reflected in the much tougher SLAs that many MSPs are having to work to these days.

Where MSPs might previously have been able to negotiate remote-site SLAs based on a two- or even four-hour response time, clients across multiple sectors are now updating their requirements. It is not uncommon to now see requests for pricing in similar scenarios to be provided on a 30-minute resolution time at remote sites.

Again, MSPs need to accept this and they need to accept that even where a network failure or outage is not directly their fault, where facilities management have made changes to the systems at a site, for example, causing an outage and not directly informed the IT function, they will have to take the blame.

Finding a solution

Guaranteeing uptime, even during an outage, and exceeding customer expectations are the aims of almost every MSP. To do so effectively though, they need to invest in their infrastructure. Yet some have focused on driving down prices to the point where they are not able to put investment back into long-term infrastructure or design.

"Raising levels of uptime comes down to implementing the right solution that can provide the visibility and the ability to remotely manage infrastructure from multiple vendors. It has to be about investment in infrastructure"

Ultimately though, raising levels of uptime comes down to implementing the right solution that can provide the visibility and the ability to remotely manage infrastructure from multiple vendors. It has to be about investment in infrastructure. As we look to the future, Internet availability will be increasingly seen as a utility that effectively has to be there. So providing guaranteed uptime moving forwards should, in fact, be seen by MSPs as more of an opportunity than a threat. So how do they deliver that?

In broad terms, it has to be by harnessing network automation and around proactively addressing issues before they turn into problems or get out of control. MSPs must also highlight to clients that the network should always be seen as a critical infrastructure that has to be resilient. That vision is not always fully realised today. Often, we see clients driving it themselves but typically only after they have already experienced a couple of major issues. The second aspect is that MSPs have to redesign their business to ensure that they are delivering a rapid response when network disruptions occur, thereby helping to eliminate the negative impacts of outages.

In technology terms, the right platform should allow MSPs to manage their critical infrastructure remotely without having to rely on expensive 'feet on the street' or issues around travel restrictions and reduced site access. This means implementing a solution that includes smart out-of-band (OOB) management, which provides an independent management network that allows secure access to the MSP's critical devices. This will provide engineers with 'virtual' direct access to infrastructure around the clock and will facilitate faster fix times. The platform should operate separately from the network data plane, providing engineers with an advanced OOB console server connected to all the critical equipment at each location and a centralised management portal. This will give engineers access to manage, monitor the MSP's IT infrastructure, anticipate network issues and resolve them remotely, removing the requirement to travel out to sites where issues are occurring.

"The right platform should allow MSPs to manage their critical infrastructure remotely without having to rely on expensive 'feet on the street' or issues around travel restrictions and reduced site access"

Now, more than ever, MSPs need to ensure uptime using a proven solution that will guarantee reliability and the network resilience that their customers expect. Investing in a platform that provides always-on access to customer devices at all times and allows engineers to manage everything from one central location will help to accelerate fix times, meet SLAs, reduce costs and exceed customer expectations.

About the author

Brendan Walsh is director of sales, Asia Pacific for Opengear. He has over 20 years of sales and marketing experience and is responsible for sales leadership in the Australian region. Prior to joining Opengear, he held senior roles with Qbt and Avocent, forging new partnerships with key partners and developing direct relationships with corporate customers. Walsh holds an Advanced Diploma of Computer Science from RMIT in Melbourne.

References

1. Lerner, Andrew. 'Network downtime'. Gartner, 11 Jul 2014. Accessed Feb 2021. https://blogs.gartner.com/andrew-lerner/2014/07/11/network-downtime/.
2. 'Hourly downtime costs rise: 86% of firms say one hour of downtime costs $300,000+; 34% of companies say one hour of downtime tops $1m'. ITIC, 16 May 2019. Accessed Feb 2021. https://itic-corp.com/blog/2019/05/hourly-downtime-costs-rise-86-of-firms-say-one-hour-of-downtime-costs-300000-34-of-companies-say-one-hour-of-downtime-tops-1million/#:~:text=Additionally%2C%20ITIC's%20latest%202019%20study,million%20to%20over%20%245%20million.&text=This%20is%20the%20equivalent%20of,per%20month%20of%20unplanned%20downtime.

The Firewall

Credential stuffing – the new hack

Colin Tankard, Digital Pathways

We hear all of the time about large amounts of data being compromised, but exactly what happens to it and how are hackers profiting from it?

One scheme used by hackers is called credential stuffing. This is where stolen account details, usually user IDs with corresponding passwords, are used to get into various systems or websites through large-scale automated login requests. Substantial numbers of spilled credentials are automatically entered into websites until they are finally matched to an existing account: the attacker can then hijack it, empty the account, place high-value orders for products or simply take personally identifiable information and use it to scam the actual user. The stolen information can continue to be used across multiple other websites.

Over the years, hackers have focused on gaining large amounts of user credentials to feed credential-stuffing attacks rather than the previous method of trying random IDs and then using brute force programs to guess the password. This trend of gathering large data sets can be tracked as far back as 2005, when we saw the first data breach of over a million records. This was shocking at the time until another breach of 94 million records occurred in the same year! Then in 2013, the Yahoo breach alone exposed 3 billion records. And, in 2019, over 15.1 billion reported records were stolen.

The reason that credential stuffing is so prevalent and often successful is that it is easy to do, requiring very little costly technology, and it thrives on the fact that most people do not change their passwords and use the same password across multiple accounts.

Credential stuffing is a significant problem for organisations. They are witnessing more and more fraudulent transactions costing them money, damaged reputation or – due to the nature of these attacks – website failure. That last is due to high volumes of authentication requests, stopping valid users from logging on.

So how can we protect ourselves against such hacks? The easiest thing is to have users change their passwords on a regular basis, or force users to have multifactor authentication. This is not always easy to deploy and can even lose clients, as many refuse to embrace better password management.

Therefore, strong defence and authentication systems need to be used to stop data breaches. If the hacker can't get to users' credentials, it starves them of the fuel to launch credential-stuffing attacks.

There are numerous actions you can take: use Captcha – it is not a guaranteed defence, but it is an obstacle that can deter attackers; use device and browser fingerprinting – by collecting software, hardware and browser information, you can tell when the same device is attempting multiple account logins; use IP rate limiting – this blocks IP addresses that attempt high-volume logins; deny known bad IP addresses; log and monitor website traffic – it is a fact that by looking at logs you can see odd behaviour such as high volumes of login out of normal hours, excessive denied-access requests and spikes of traffic, and you can compare IDs against known stolen credentials.

All of these measures will lead you to an awareness that your site is under attack and you can then take proactive measures to mitigate the impact.

As ever, hackers – like burglars – look for the easiest way in and while users keep reusing passwords for multiple accounts, credential-stuffing attacks will continue. Networks will need to step up to protect themselves by advertising their protective measures, just like we do in our houses with evidence of locks, alarm systems and security lights.

EVENTS CALENDAR

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

22–26 March 2021
Fifth International Workshop on Security, Privacy and Trust in the Internet of Things (SPT-IoT)
Kassel, Germany
https://bit.ly/2Tv5Lbe

19–20 April 2021
Rethink! IT Security
Berlin, Germany
www.rethink-it-security-2021.de

4–7 May 2021
Black Hat Asia
Virtual event
www.blackhat.com/asia-21/

10–11 May 2021
Paranoia
Oslo, Norway
https://paranoia.watchcom.no

11–12 May 2021
CyberUK
Newport, UK
https://bit.ly/3juOBoN

17–20 May 2021
RSA US
San Francisco, UK & virtual conference
www.rsaconference.com/usa

24–26 May 2021
Privacy + Security Forum
Virtual conference
https://bit.ly/2HFsIGb

28 June – 2 July 2021
Hack in Paris
Paris, France
https://hackinparis.com