






DEFENSE.COM™
ANNUAL
CYBER SECURITY
INDUSTRY REPORT
2022

 www.defense.com
 01438 500 500
 contact@defense.com



Defense.com™ is an all-in-one security platform that is transforming the way businesses manage cyber security.

We help simplify and solve the cyber security challenges facing organisations across all industry sectors to protect their brand and assets against today's evolving threat landscape. Businesses of all sizes rely on our security services to protect, detect and respond to cyber threats.

By combining world-class security technology with people-powered services, we're empowering organisations of all sizes to grow with confidence and significantly reduce the risk of cyberattacks.

CEO Foreword

Looking back over the data from the past year always brings mixed feelings. There's a sense of great achievement as we see unique technologies and businesses succeeding to significantly improve their security, but this is balanced with frustration when we still see common issues raising their heads. This frustration is not in the ability of businesses to deal with the challenge, more that attackers still succeed in exploiting businesses with attacks that are either already well known or simple to fix.

However, there is a great feeling of responsibility in our teams to do all that we can to share as many of our insights as possible and help businesses drive positive change.

A large proportion of our data comes from work that we are doing for businesses that are already investing in security. These businesses have budget to spend on improving cyber security, yet in many cases they still fail to fix common issues, even after they have been identified. I believe this comes down to some common business conundrums:

- Where is best for us to invest our valuable resources and time: growing our business or improving security?
- How do we hire the right people with the right skills, and how much time can they fully dedicate to critical compliance and security issues?
- How can we implement these controls and security best practices without slowing down business growth?
- How can we get our product/service to market as quickly as possible?

In our conversations with businesses, we often discuss the balance and appreciate the challenges involved. Every year we work hard to identify key data and new ways to understand the threat landscape. We bring together data from multiple teams and systems to document interesting trends and uncover unique threats that businesses should be aware of.

Our data not only shows us how attackers are operating and the most successful tactics, but it also allows us to evidence where businesses are failing to adopt basic security principles, else these attacks just simply would not work.

The reality is that many organisations feel underprepared or under-resourced to tackle even the basics. I hope you will agree that this report paints a picture of the real threats out there. It is written to ensure fear, uncertainty and doubt have been removed, and to provide encouragement to drive change in the business at a leadership and technical level.

I hope you enjoy the report. We welcome any feedback so we can continue making it a useful resource for you each year.

Oliver Pinson-Roxburgh
CEO & Co-Founder

Contents

CEO Foreword	3
Executive Summary	4
Findings at a Glance	6
Showcase - The LinkedIn Problem	8
Vulnerabilities & Risk Management	10
Threat Intelligence & Analysis	16
Showcase - The Risk in the Cloud	24
Compliance & Data Protection	26
Conclusion	31
Final Word	32

Authors

Oliver Pinson-Roxburgh
Kieran Roberts
Brian Wagner
Nicky Whiting

Edited by

Rajnish Ghaly
Stephanie Johnson
Mikey Anderson
Emma Dockerill

Designed by

Nadine Unwin

With contributions from

Andy Smith
AJ Wiggan
Neil Barnes
Jason Charalambous
Theodoros Danos



EXECUTIVE SUMMARY

Executive Summary

In this report, Defense.com™ looks back on a fascinating year in the world of cyber security and compliance, with a keen eye on emerging patterns for what to expect in 2022 and beyond. Assessing data from our SIEM platform, honeypots, penetration testing and compliance services gives us a great insight into new cyber security threats and the state of cyber defences across various industries.

Working closely with the key business units within Defense.com™ and using data from our platform has enabled us to gather insights into how businesses secure their systems. This provides a unique perspective that we hope you find useful when building out your future compliance and security strategy.

It's been another year of discovery and insight in the world of cyber security. The lasting impact of COVID-19 has meant drastic changes to working practices, processes, and how businesses stay protected. As such, we saw more businesses migrating to hybrid working in 2021.

An increase in cloud security due diligence has been necessary

Throughout the year we had some significant, critical vulnerabilities that not only hit the headlines because they were zero days, but also because the software and systems they affected were vast, making it difficult for businesses to patch the issues. Many businesses focused on the exposed services to buy time and secure internal assets; however, we could see the threat continued for some time as attackers adapted their targeting methods. In addition to this, our data showed that patching is still a major challenge for businesses, usually due to resource constraints. Many organisations only focus on the most critical vulnerabilities, which means they are not fully remediating other cyber threats facing their business.

Log4j is used by millions of computers worldwide

Another interesting change for the coming year is the announced changes to Cyber Essentials and the GDPR. Some of these changes will initially prove challenging for businesses, but we believe that it is important that regulations, compliance standards and best practices evolve over time as we learn more about new

threats. All businesses must support change to ensure the regulations remain effective against an ever-evolving threat landscape as data grows and the risk of exposure increases. In addition, businesses should also consider the security of their suppliers, with a high proportion of threats now occurring indirectly from supply chains.

Up to **40%** of cyber threats are now occurring indirectly through the supply chain¹

Lastly, our data shows that low-effort attacks are still being used successfully by threat actors against businesses of all sizes, from start-ups to enterprises. To combat this, businesses should focus their attention on reducing the threat of opportunistic attacks through thorough risk management, rather than focus on the cyber security arms race. It is with this awareness that we hope to see more companies realise the benefits of security best practices and how they can enable their businesses to grow securely in 2022 and beyond.

Key Findings at a Glance

“ The average cost of a data breach for a small business? **£8,460** ”

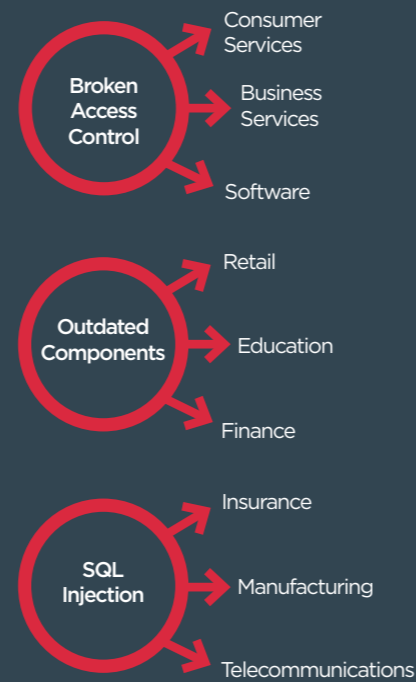
“ The average cost of a breach for a medium or large business? **£13,400** ”

“ The most common type of cyber attack is a phishing attack? **83%** ”

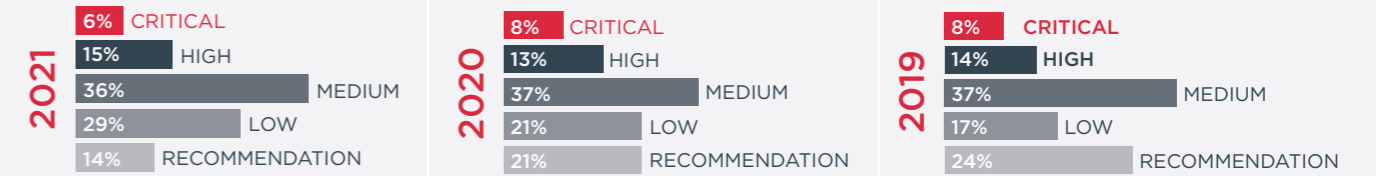
“ Linkedln-related social media phishing emails were clicked the most? **42%** ”

“ Today, bot traffic accounts for **UP TO 70%** of all website traffic on the internet⁴ ”

Most common critical issues by sector



How severe are the discovered vulnerabilities?

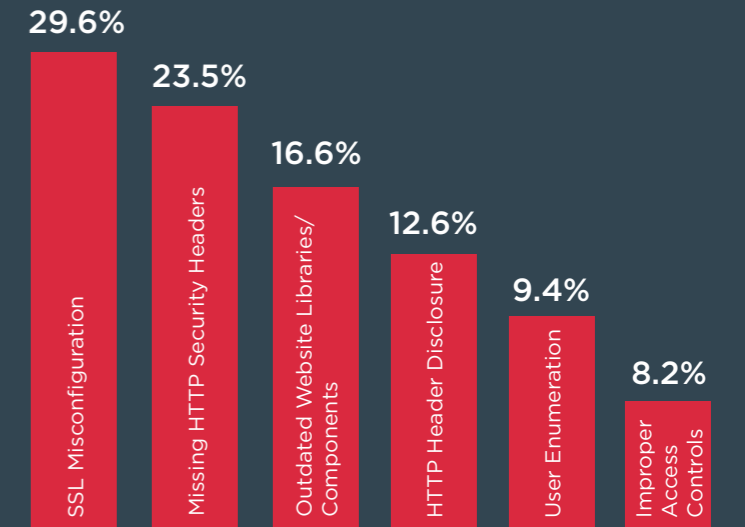


Vulnerability Scan Findings

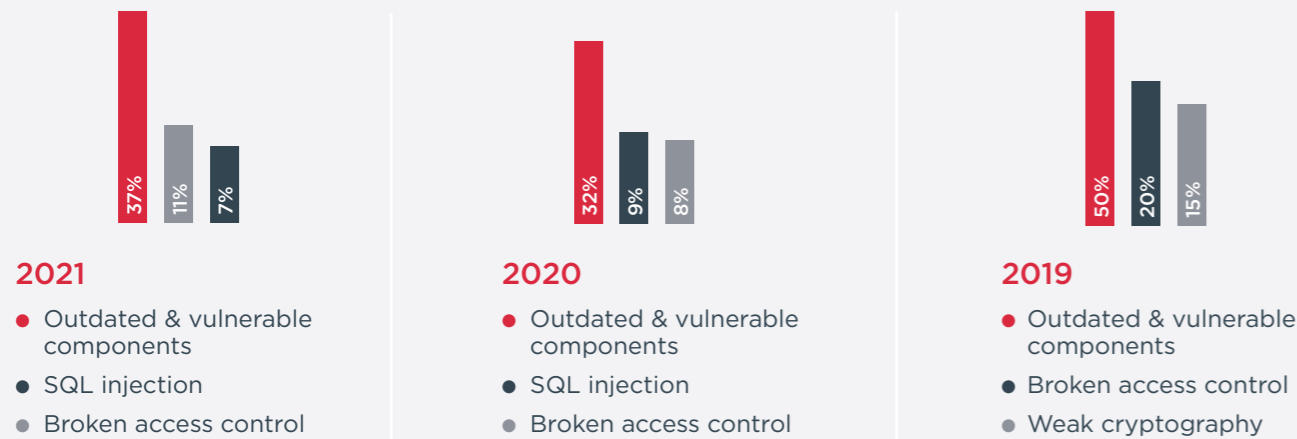
Likelihood of vulnerability being exploited



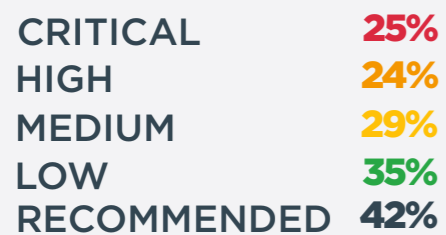
Top vulnerabilities seen in 2021



Most common critical weaknesses

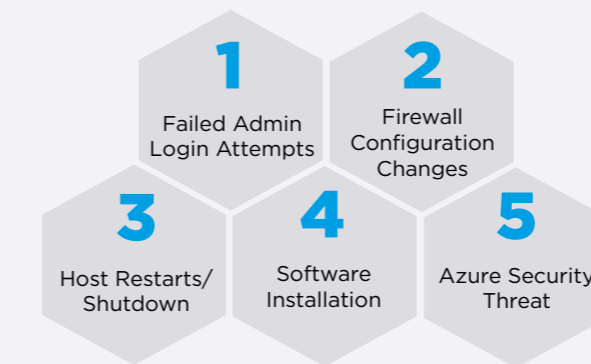


% of vulnerabilities identified during a retest that had not been fixed



“ This shows that even when retesting after an initial pen test, businesses are still not addressing all vulnerabilities identified ”

Top 5 SIEM Alerts



“ **24,806** businesses achieved Cyber Essentials certifications of which achieved Cyber Essentials Plus Status⁵ ”

⁵between 1 September 2020 & 31 August 2021

“ **54%** of over **5000** unique IP addresses that targeted our honeypot had intelligence that suggested they were bad actor IP addresses ”

Top GDPR failures that our DPO team has seen

- 1 Lack of awareness that the EU-US Privacy Shield was no longer valid
- 2 Not having visibly clear and obvious cookies banners on websites
- 3 Incomplete or missing Records of Processing Activities (RoPA) in accordance with the requirements of Article 30

LinkedIn is the largest professional networking website with over 750 million users worldwide, making it a great source of information for hackers. Its ubiquity also makes it a common theme in phishing attacks. As a reputable source for professionals and businesses, phishing emails seemingly from LinkedIn can appear legitimate to employees with low cyber awareness.



SHOWCASE

The LinkedIn Problem

Hackers understand that the path of least resistance is through people and so often use social engineering in their attacks. In 2021, the NCSC noted an increase in malicious email activity and password spraying campaigns targeting UK organisations.⁶ This was followed by the sophisticated email-based NOBELIUM attack, which targeted organisations in 36 countries.⁷

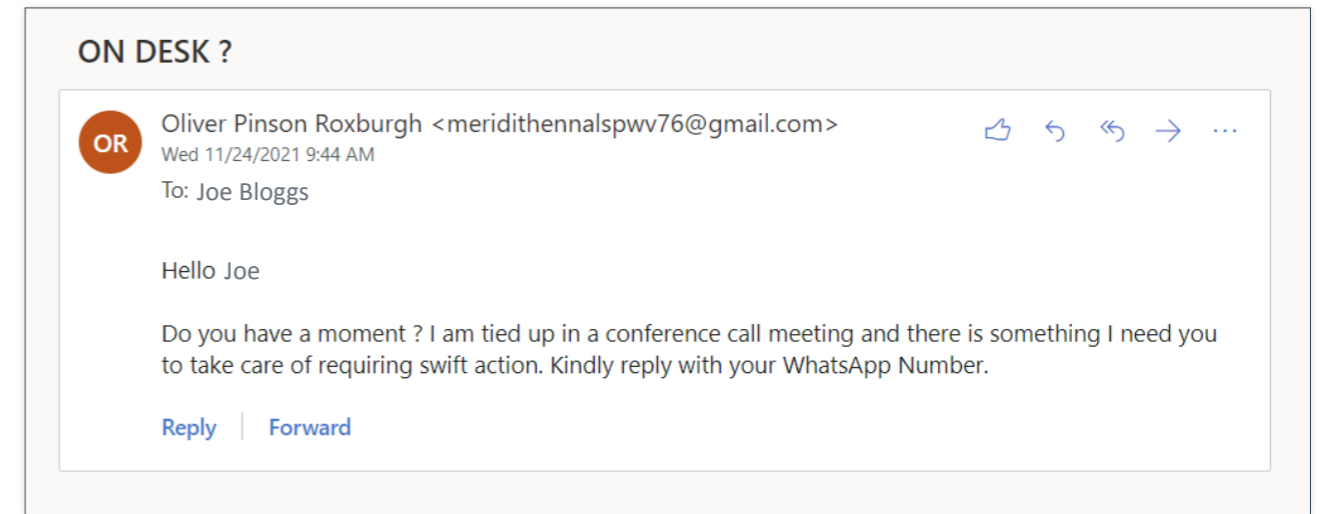
LinkedIn is the largest professional networking website with over 750 million users worldwide, making it a great source of information for hackers. Its ubiquity also makes it a common theme in phishing attacks. As a reputable source for professionals and businesses, phishing emails seemingly from LinkedIn can appear legitimate to employees with low cyber awareness. In Q1 of 2021, LinkedIn-related phishing emails remained the top clicked-on social media mail (42%), ahead of the likes of Facebook (20%) and Twitter (9%).⁸

Targeting new employees

Businesses continue to notify us after having been targeted by attackers with phishing campaigns directed at their new hires. The phishing campaigns typically appeared to have come from a CEO or senior-level employee, which gives hackers a greater opportunity to elicit sensitive data from an unwitting new starter by using an element of authority. During further research, we noticed employees were being hit with a phishing email within a month of changing their job status on LinkedIn. The premise of these phishing campaigns is simple; requesting employees to buy gift vouchers or call a given phone number to discuss an urgent requirement.

Hackers understand that the path of least resistance is through people and so often use social engineering in their attacks

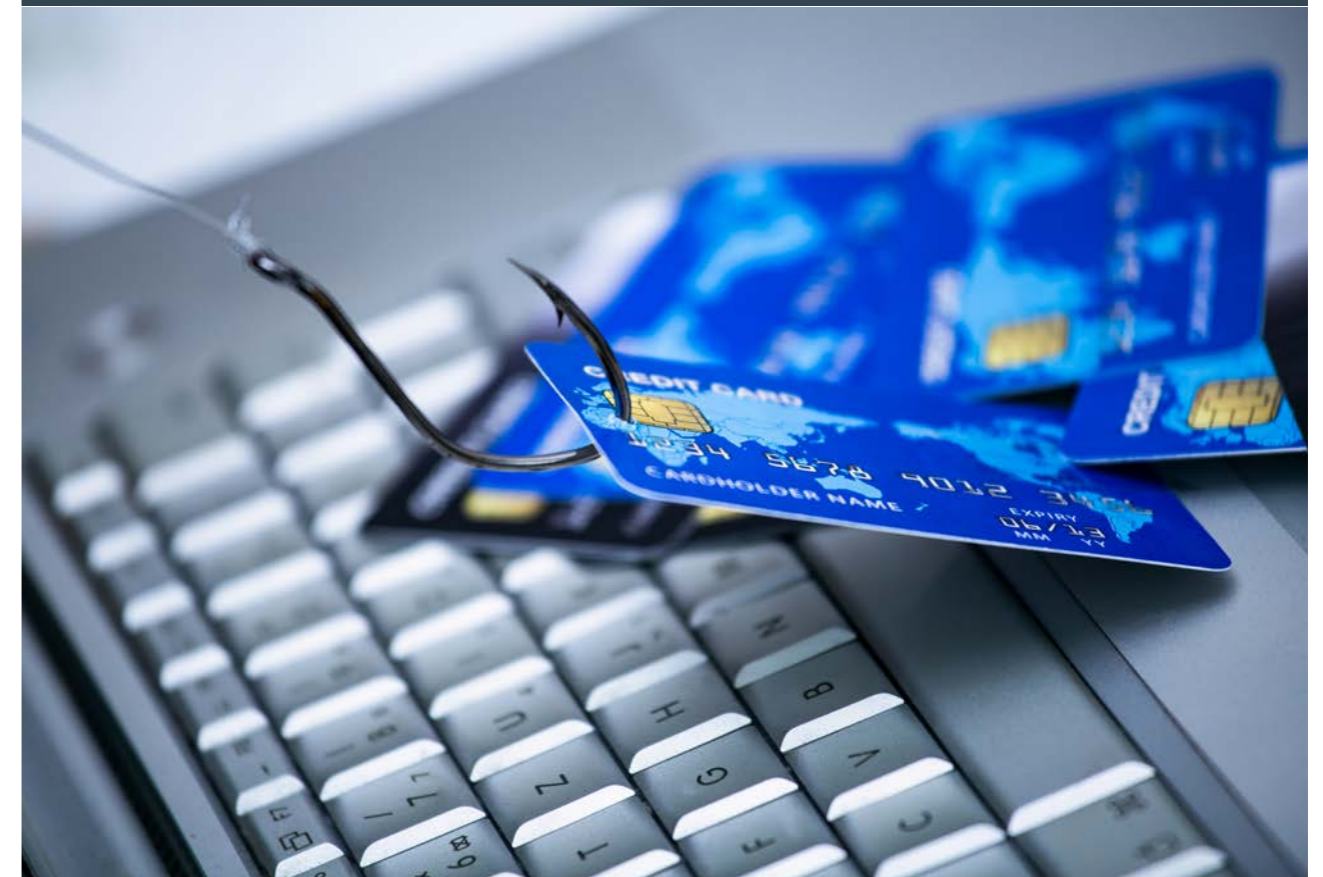
See below for a real-world example of a phishing campaign received by a new member of staff:



Overcome the Risk

The simplest attacks are often the most effective and with employees at the heart of every organisation, your business' cyber security is only as strong as your weakest employee. It's vital that you train staff to understand social engineering attacks and remain vigilant to suspicious requests.

As the psychology behind many phishing attempts is to create a sense of urgency, encourage your employees to be inquisitive. If someone says something is urgent, support a culture where it is acceptable for staff to ask questions and flag up any communication where they are unsure. After all, it's better for an employee to check before falling for a phishing attack.





VULNERABILITIES & RISK MANAGEMENT



Foreword

Over the last 12 months, our penetration testing team has gained a wealth of data, giving us vast insights into the vulnerabilities that leave businesses open to a cyber attack. One interesting find was the sheer number of outdated libraries and components discovered during web application and API assessments. This is a key find because it has intriguing implications for customer environments. Lags in patching provide a useful advantage to hackers, emphasising the need for a rapid response to new vulnerabilities from businesses IT departments.

Missing patches are high-risk security issues which are generally easy to fix. However, a core problem is when businesses do not have control over their libraries and rely on third parties to patch their systems, causing an issue in patch management continuity.

This is becoming an important talking point as it presents businesses with a dilemma, whether patch management is in their control or not, and whether it should be. We've seen IT departments becoming more efficient with their patch management, but there is always more that can be done to sustain secure environments and ensure businesses remain protected in addition to adopting new modern approaches to the architecture and design of their platforms.

K Roberts

Kieran Roberts
Head of Penetration Testing

Over the last 12 months, our penetration testing team has gained a wealth of data, giving us vast insights into the vulnerabilities that leave businesses open to a cyber attack. One interesting find was the sheer number of outdated libraries and components discovered during web application and API assessments.

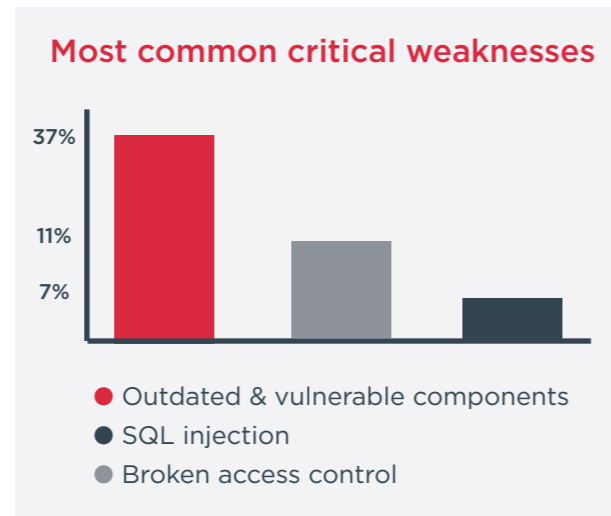
Vulnerabilities & Risk Management

Patching

Patching has always been one of the most important jobs in maintaining a secure cyber security environment, as vulnerabilities are constantly being discovered and PoC (Proof of Concept) exploits become public daily. With outdated website libraries and components ranking highly in our top vulnerabilities found during penetration testing in 2021, it's clear that organisations are still not following basic security measures, such as regularly updating software, to safeguard against cyber threats.

With outdated website libraries and components ranking highly in our top vulnerabilities found during penetration testing in 2021, it's clear that organisations are still not following basic security measures, such as regularly updating software, to safeguard against cyber threats.

There are several reasons why businesses are not patching in a timely manner. For large organisations, patch testing is crucial before implementation and if testing is delayed due to time constraints or lack of resources, this will cause delays in installing patches. Also, patches for legacy devices are not usually available, making them a high-risk target. Attackers will be looking to exploit known vulnerabilities, so legacy equipment is easily targeted, and the risk is compounded by the fact you can only mitigate vulnerabilities as no patching exists for this equipment. This raises a larger issue for businesses to ensure they have the resources available to replace legacy equipment to help maintain stronger cyber defences.



Web servers are commonly managed by separate teams or even third parties and as such may not fall into the same patch management policy. Third-party software has a similar problem, especially less common software. Centrally managed patching policies are extremely useful and are a vital part of modern system management, but it is important to remember that there may be gaps in the coverage. From our research, we found that many of the instances of outdated libraries, components and third-party patches had serious vulnerabilities, with the exploit code publicly available. Once exploit code is released, it can easily be weaponised by opportunistic hackers. Vendor due diligence is therefore crucial for understanding what suppliers and third parties are doing to improve the security of the assets they support, as well as identifying where a business' own patch management policy needs to cover any disparities.



Pen Testing Re-test Data

An interesting observation from our penetration test data is the amount of vulnerabilities that are not fixed before a re-test is carried out. We expect to see some lower risk vulnerabilities remaining, as many organisations have policies in place to only address more significant weaknesses (often due to time or resourcing restrictions), but we also observed that a quarter of high and critical vulnerabilities were left unaddressed, which is quite alarming. It's also worth noting that this data is only from businesses who are actively seeking out penetration tests and re-tests, assuming they have a fair interest in securing their networks and applications and leaving us to wonder exactly what these figures would be if extrapolated for all businesses.

Percentage of vulnerabilities identified during a retest that had not been fixed



A quarter of critical flaws are not fixed after a pen test

Log4J Vulnerability

The Apache Log4J vulnerability sent shockwaves through the cyber security industry as it's a simple yet effective flaw that unfortunately is difficult to detect. Log4Shell enables hackers to load arbitrary code onto a server and take control of a system, which can allow them to obtain credentials and potentially the sensitive data of millions of users.

Although we consider patching to be one of the most important roles in securing an organisation's IT systems, patching alone is not sufficient to safeguard businesses against every cyber threat. Due to some of the most recent patches for high profile vulnerabilities not fully fixing the issue, businesses should not rely solely on patching and should consider an in-depth defence strategy. This involves having multiple layers of security to protect systems and networks as effectively as possible. Regular patching is important but could provide a false sense of security if used in isolation. Businesses without other controls in place, such as strong segmentation and outbound traffic filtering, could still be at risk of an attack in certain scenarios.

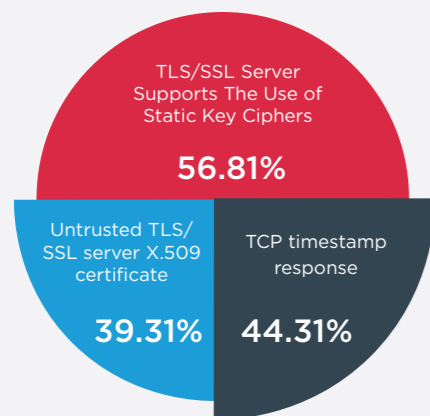
When looking at instances where the Log4J vulnerability has been successfully exploited, the impact on organisations has been significant. Businesses should therefore be regularly testing their incident response and business continuity plans for this very scenario. Equally, some organisations have been indirectly affected by attacks on their supply chain, which in turn has had a significant impact on critical business functions, highlighting the importance of supplier due diligence processes.

Vulnerability Scan Findings from Defense.com™

We run thousands of automated vulnerability scans every year on behalf of our customers through our platform, and our scan data often supports what we see in our manual assessments and rescans; many businesses are taking risks by not fixing all vulnerabilities.

Organisations often have policies in place to prioritise and fix issues that are medium or high risk, whilst ignoring low risk issues. However, low-risk issues can often be chained together by an attacker to create a more severe problem, which means it can be extremely damaging to a business to assume that low risk issues don't need to be addressed.

Top Vulnerabilities in 2021



i *SSL, or Secure Sockets Layer, is an encryption-based Internet security protocol first developed in 1995 for the purpose of ensuring privacy, authentication, and data integrity in Internet communications. SSL is the predecessor to the modern TLS encryption used today.*

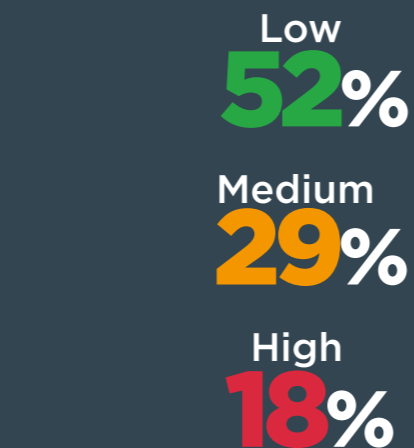
SSL and certificate management made up the largest share of vulnerabilities found over the course of 2021, but what is key to note is how attackers can use the above vulnerabilities in more targeted attacks. Information disclosure, such as that provided by a TCP timestamp response, can be leveraged to discover uptime on a specific machine, allowing attackers to be

more surgical in their approach. This information is used to target machines that are more likely to be vulnerable as they have not been rebooted and therefore are unpatched.

The spread of severity level across all findings shows an interesting pattern that we often see during penetration retests, which is that businesses are willing to accept and ignore lower-risk issues and often choose not to patch.

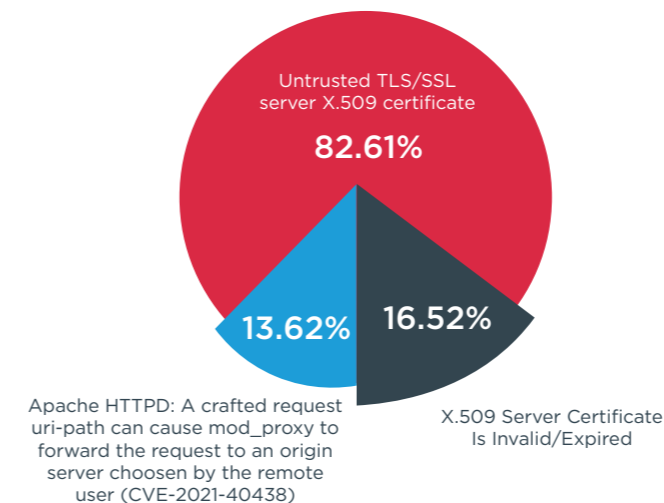


Likelihood of vulnerability being exploited



Filtered by a severity level of 'Severe' to 'Critical' changes the picture but we continue to see SSL issues make the list followed by Apache and SMBv2 issues, and unencrypted communications:

Top 3 % of scanned assets filtered by severe to critical vulnerabilities



Key Takeaways

- Effective patch management remains key to strengthening cyber resilience against malicious actors.
- Organisations still aren't applying best security practices, therefore becoming easy targets for hackers due to their weakened environments.
- Third-party software still poses problems for effective patch management with policies differing from the rest of the organisation, highlighting the need for supplier due diligence.
- Vulnerabilities that have public exploit code available are more likely to be leveraged by hackers and so should be priorities for remediation.
- Failing to mitigate low risk vulnerabilities can leave businesses open to vulnerability chaining.
- Defence-in-depth is the best strategy to reduce risks as it mitigates the reliance on just one control such as patching.



THREAT INTELLIGENCE & ANALYSIS



Foreword

Businesses are still providing clear openings for opportunistic hackers to exploit vulnerabilities across their critical systems. These vulnerabilities could stem from any number of issues including insecure APIs, unpatched systems, lack of multi-factor authentication (MFA), cloud environments that have not been hardened and SaaS solutions that are misconfigured.

A huge proportion of our data shows that businesses are being targeted every day with brute-force, spray and other credential-based attacks. The attackers rely on breached credential databases, default or common passwords, to target vast parts of the internet. This is such a significant issue that the US National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI) and the NCSC have published a joint advisory exposing malicious cyber activity by Russia's military intelligence service, the GRU, against organisations globally.

These insights, combined with our data, highlight the importance of proactive monitoring to ensure you are aware of the threats to your business on a daily basis, as well as a tried and tested incident response plan.

It's no longer good enough to just have the technology in place - you have to be in a position to understand and respond to what it's telling you.

B. Wagner

Brian Wagner
Chief Technical Officer (CTO)

Once again, some of the most interesting data comes from baiting attackers on the internet, as it gives us direct insights into their behaviours and tactics. Throughout the year Defense.com™'s SOC team ran servers in public cloud environments with deliberate security vulnerabilities. These honeypots allow us to gather valuable intelligence on the behaviour of hackers pre- and post-breaching the honeypot system.

In our previous industry report we highlighted how employees were the preferred target for hackers, and this didn't change throughout 2021. Phishing attacks were once again widespread and remain one of the most common threat vectors. Social engineering is still a useful tactic for hackers to get users to reveal sensitive information if they are not risk aware. With poor password hygiene continuing to threaten businesses and a significant target for attackers, the importance of cyber security awareness and training has never been greater.

Honeypot Findings



Our honeypot findings prove that within milliseconds of a server being put on the internet, it is already being scanned by all manner of entities. Botnets will be targeting it and a host of malicious traffic is then being driven to the server. Although some of our data shows legitimate research companies scanning the internet, the greatest proportion of traffic we encountered to our honeypot came from threat actors and compromised hosts.

Honeypot servers have a shelf life, meaning the effectiveness of the honeypot will decrease over time and therefore it's important to keep adapting the approach to avoid a drop-off in traffic.

It's worth noting that most of our traffic was SSH traffic to the hosts and the attackers were brute-forcing the SSH credentials. This makes sense, as at the time of writing this, there are over 20 million servers on the internet with port 22 (SSH) open to the world, generally used for remote administration and server maintenance, so it is no surprise that these are prime targets. However, we anticipate the number of servers

exposing port 22 being even greater, as it is only what we have seen at one point in time. Any organisation that sets up a server should expect to be hit with a high proportion of traffic and brute-force attacks, as servers produce ample opportunities for threat actors to deploy attacks. A simple proposition to eliminate the threat of a breach is to first limit access to specific IP addresses, as well as implement regular monitoring and auditing of activity on servers to help identify potential risks. This in turn allows for proactive threat remediation.

Our data shows that poor password management is one area hackers are using to their advantage to infiltrate servers. Specifically, default credentials and credentials that have been exposed during a breach are being used to facilitate brute-force attacks. Even the most advanced hackers use the path of least resistance, and there are well documented nation state attacks that have started with brute-force attempts.

Our honeypot findings prove that within milliseconds of a server being put on the internet, it is already being scanned by all manner of entities.

For example, here are the top 10 passwords used as part of brute-force attacks. These passwords are known to us and hackers as they are sourced from data dumps, therefore hackers are confident they will frequently result in a successful login:

Password	Credentials on the RockYou database
<No Pass>	FALSE
admin	TRUE
PASsw0RD	TRUE
1	TRUE
admin123	TRUE
PASsw0RD	FALSE
!QAZ2wsx	TRUE
0	TRUE
Huawei@123	FALSE

Over the course of the research, the bad actors initiated

over 240k sessions

From our analysis, these sessions consist largely of automated scripts and software continually trying to compromise our honeypot. It's an unsophisticated, yet often still successful, rinse and repeat method of installing software and logging out until the botnet hits a threshold of attacks.

Research also showed that the top IP address, connected from a German server, initiated

over 915 sessions

and spent a total of 5 hours on the honeypot. One attacker, likely to be a botnet, spent three times that duration logging in successfully 39 times with over 30 unique passwords.

It is important to note that many of the attacks and samples of files uploaded to our honeypots exhibited worm like behaviour:



A computer worm is a type of malware that spreads copies of itself from computer to computer. A worm can replicate itself without any human interaction, and it does not need to attach itself to a software program in order to cause damage.

We saw that many of the attacks are autonomous, continuous, and high in volume. Today, bot traffic accounts for

UP TO 70% of all website traffic on the internet⁹

Around a quarter (24.5%) of the passwords used by the attackers are on the RockYou database leak from December 2009. This clearly indicates they still work, or attackers wouldn't be doing it. In fact, even our own penetration testers use this password list during testing, due to its high success rate.



RockYou¹⁰ was a social application site that created widgets and implemented applications for social media networks like MySpace and Facebook. When hackers gained access to RockYou's unencrypted database using a 10-year-old SQL vulnerability, over 32 million user accounts were exposed. The data breach demonstrated RockYou's complacency in following the necessary steps to rectify the issue, such as emailing users unencrypted passwords during account recovery and not addressing their users about the breach.

The number of failed logins outweighed successful attempts as you would expect, and a large proportion continued with brute-force attempts to login without any concern for being noticed by the target.

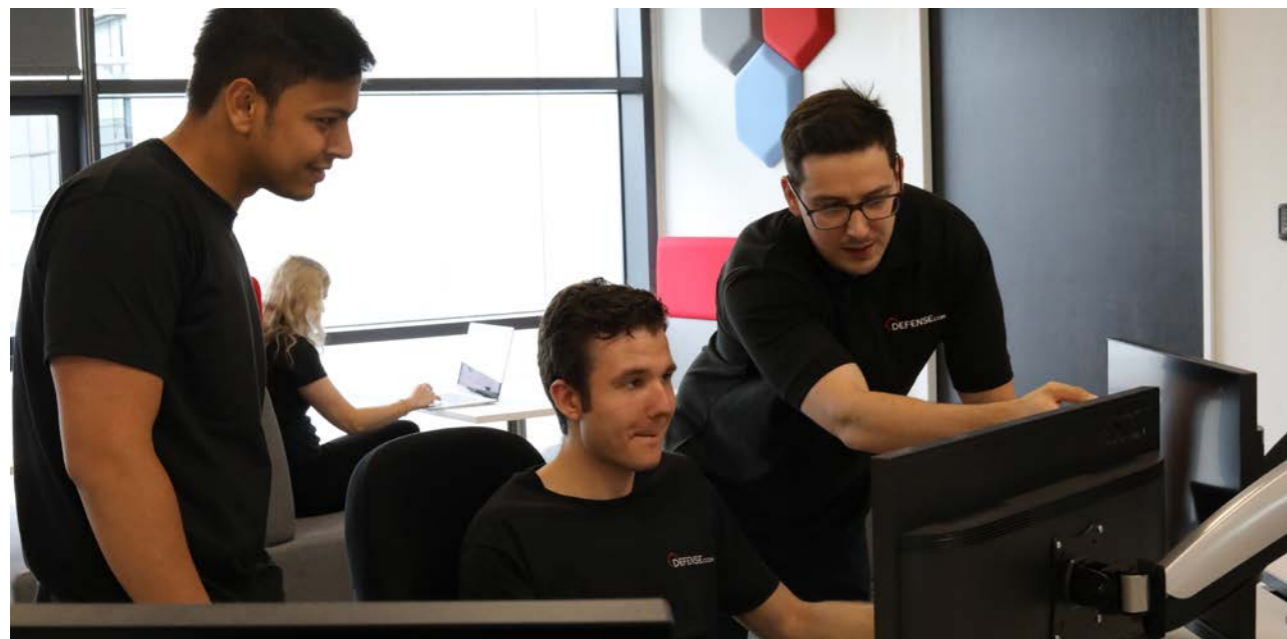


We also observed that the default Raspberry Pi credentials are in the list. This is not surprising as our research shows that there are well over 200,000 machines on the internet running the standard Raspberry Pi OS making it a decent number of systems to compromise. As the Raspberry Pi OS ships with default credentials (un:pi/pwd:raspberrypi) it's low-hanging fruit for hackers. What this tells us is that even default passwords are not being changed.

Raspberry Pi systems can be easily compromised by hackers. A target for a cyberattack could be as simple as an office display screen using the Raspberry Pi operating system. Hackers will generally focus their attention on easy targets first and Raspberry Pi devices are cheap, easy to setup, have out-of-the-box benefits and will likely be connected over a VPN or Wi-Fi. If setup incorrectly, they increase the attack surface, risking hackers taking full operational control, and expose sensitive areas of the business.

It's critical to change default credentials, as it's one of the easiest entry points for an attacker to disrupt your service by planting malware or steal business-critical data and sensitive information. Attackers benefit the most from using legitimate credentials, as it means that they do not have to rely on often unreliable vulnerabilities and this can allow attackers to avoid being detected in the first place, making investigating and monitoring the attack much harder.

IT departments are often reluctant to change default passwords, as it can be difficult to fix or get to the root cause of issues if people



need to remember which credentials to use when under pressure. It's often a time-pressure decision during the initial setup as it's easy to leave default credentials in their existing state and plan to come back to it later. However, sometimes the final step gets forgotten and passwords are left as their default values. This is especially problematic if users are sharing credentials and not storing them in a password vault with restricted access. Consequently, this leaves the door wide open for hackers.

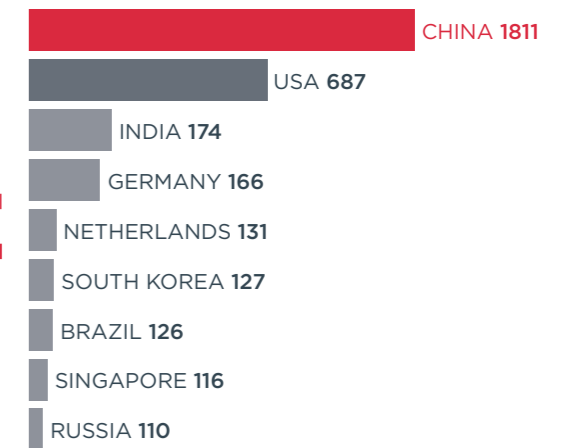
The following table shows the failed login attempts on our honeypot:

Username: knockknockwhosthere Password: knockknockwhosthere	61854
Username: nproc Password: nproc	4351
Username: user Password: 1	1143
Username: user Password: x	364
Username: user Password: 1234	242
Username: user Password: 123456	200
Username: root Password: root	138
Username: pi Password: raspberry	118
Username: mos Password: mos	103

We found that the machines that targeted our honeypot themselves have over 16,000 vulnerabilities. There is a good chance that these hosts have been hacked due to known vulnerabilities, as a large proportion of the systems hacking our honeypot used brute-force methods to gain access.

THE TOP NINE

countries by most IP addresses hitting our honeypot are:



From the IP addresses that targeted our honeypot, the following data shows by country how many total known vulnerabilities they have:

COUNTRY	VULNERABILITIES
China	4474
India	1618
South Korea	1611
Indonesia	1009
United States	614
Brazil	581
Argentina	390
Colombia	361
Russia	321

The activity on the servers showed that they were being used to download additional hacking tools and eventually malware, indicating that these attacks are more akin to organised crime with the purpose of making money. We also spotted many cases of crypto miners being downloaded, which again is a way for organised crime gangs to monetise a successful attack. Dota was the most prominent in the data.

Dota is a type of malware that has been active since 2019 and targets Linux machines still using default credentials with SSH brute-force attacks. Once the root account credentials have been compromised and a backdoor has been created, the botnet will attempt to deploy crypto mining campaigns. Dota can read system information and its payload also includes a worm module that helps the malware spread to different machines on a network.

Observing which tools hackers use is highly useful when detecting attacks, as you can proactively monitor for the use of those tools. One best practice approach is to work with your IT teams and partners to build a profile of what tools you regularly use, who uses them and when they are used so that you can detect anomalous activity.

The following list shows the top tools used to target our honeypots:

- Wget
- Curl
- Cat
- Echo
- Chpasswd
- Bash
- Uname
- whoami

Attribution is very difficult, as many of the systems that are used in attacks like those against our honeypots are from compromised machines used by attackers. The fact that China is at the top of the list of assets hitting our honeypot further highlights the vast number of systems exposed to the internet in that region with poor security controls. Based on our honeypot activity, it's fair to conclude that these attacks are not likely to be nation states, as those attacks are generally more targeted and are less likely to be hitting honeypot systems.

Although these are common Linux tools, with the right context it's easy to tell whether the activity is expected to be legitimate traffic or malicious in intent. In addition, many of these tools are not tools that would be used daily.

Anonymity

When discussing our research internally, we had a burning question to answer - when someone is targeting these systems, do they care about anonymity? And if we do see that hackers or bots are using anonymisers, does that suggest that they are less opportunistic and more targeted?

We checked all our data to see how much traffic came from Tor Exit nodes and encrypting communication through onion routing. There are two schools of thought around the ethical nature of the Tor Project. To many users it offers unlimited freedom of the internet, while others believe it allows users to access the dark web to perform illegal activities and mask malicious activities.

We found that a

**A TOTAL OF
31 IP ADDRESSES
initiated just over
40 SESSIONS**

They spent considerably less time in a session, which suggests that they would likely not attempt to access the system straight away and instead prefer to wait and come back to it at another time. This is usually to avoid firing at the honeypot, sounding the alarm and being detected, as that could lead to access potentially being removed. The pattern of the attempts to access the honeypot seems automated, but they were in fact more precise. - Once the other end confirmed they could access the system by simply logging in, they didn't do it again. Only 8 Tor IP addresses were seen accessing the system more than once. Due to the way that Tor works, this could signal that there was more than one malicious actor.

Windows honeypot data

Based on a full year's data, Windows' brute-force activity shows a similar story. Common usernames are being used to attempt to gain legitimate access, with the top 10 being a variation on 'administrator':

Username	Login Attempts
ADMINISTRATOR	68904085
administrator	41104489
Administrator	1671055
ADMIN	1105358
USER	299915
backup	187846
Admin	152260
Administrateur	148521
admin	103005
Administrador	100177

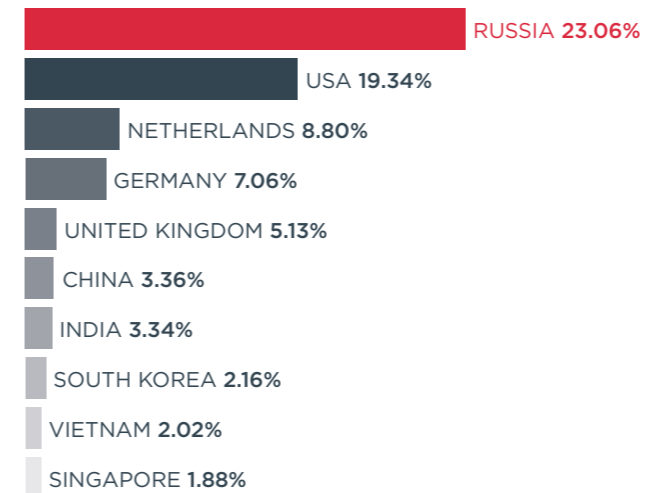
The attackers also use the hostname of the computer as the username which shows some level of intelligence to the automation.

If you remove the variations on 'administrator', the picture is a little different:

Username	Login Attempts
USER	299915
backup	187846
TEST	87825
AZUREUSER	64734
SERVER	62801
HRWORKSTATION	49071
TEMP	26377
MANAGER	24570
test	24365
SUPPORT	23348

It is worth noting that this machine is on Azure. Some attacks were using AZUREUSER as a username which suggest a slightly more intelligent bot or more strategic attempt to brute-force the system based on where the system is hosted.

Top 10 countries with failed login attempts:



Comparing SIEM Findings

In addition to our honeypot data, we also wanted to compare this with real customer log data we collect as part of our Security Information and Event Management (SIEM) platform. To do this, we analysed all the security issues that our customers encountered over the year and sorted them in order of the number of alerts generated per issue.

We see that the top security issue our customers experienced in 2021 from log data was failed admin login attempts, which remains unchanged from 2020. This correlates with our honeypot findings and confirms that it is critical to change default credentials to avoid opportunistic attacks.

Failed login attempts are somewhat expected to be top of the list, as attackers prefer to gain legitimate access. However, it's important to note that we usually see a small minority of these issues turn out to be genuine user activity. This is where a SIEM solution can be invaluable in understanding the actual risk for each security issue; a SOC analyst can raise an alert, investigate the potential threat and conclude if it is indeed a security risk or not, based on the log data for each event.

Key Findings

- Honeypots have proved to be an effective tool in understanding new cyber threats. They help us better understand the behaviour of hackers and where businesses are failing to implement effective cyber security management to keep up with these new threats.
- Best security practices are still not being followed. Poor password management is a recurring theme throughout 2021 and tells us that organisations are providing hackers with ample opportunity to breach their systems by not enforcing password changes or multi-factor authentication.
- Due to businesses not reducing their attack surface, the pool of targets available to hackers is vast.
- Cyber security awareness training for the workforce remains key to frontline protection of an organisation's network, infrastructure and employees.

Top 5 Security Issues by Year

2020	2021
1 Failed Admin Login Attempts	1 Failed Admin Login Attempts
2 Firewall Configuration Changes	2 Firewall Configuration Changes
3 Host Restarts/Shutdown	3 Host Restarts/Shutdown
4 Software Installation	4 Software Installation
5 Malicious Traffic	5 Azure Security Threat



SHOWCASE

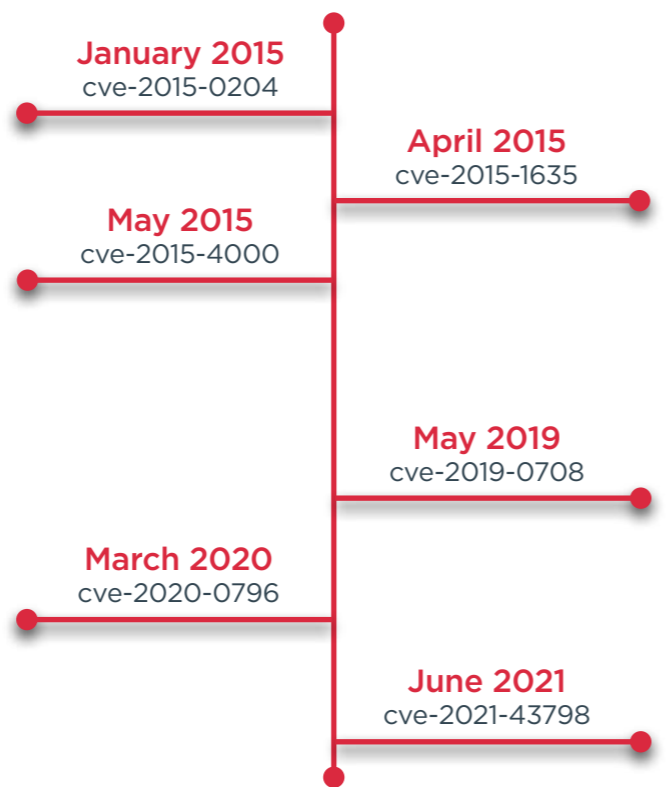
The Risk in the Cloud

As public cloud adoption continues to grow, it remains important to understand the risks it presents to businesses, particularly when the shared responsibility model leads some into a false sense of security. Supported by our honeypot data, which shows a large proportion of hacks coming from compromised public cloud environments, we explored just how vulnerable the top cloud providers were.

Since the pandemic started in 2020 and businesses shifted to working from home, Google's revenue from their cloud business has nearly doubled to around \$5 billion.¹¹ Additionally, 92% of enterprises now have a multi-cloud strategy and 82% have a hybrid cloud strategy which combines both private and public clouds.¹²

36% of enterprises spend more than \$12 million per year on public clouds,¹³ so it is not surprising that this is a big target for hackers. Using passive information gathering techniques, we assessed over 32 million cloud instances and found common vulnerabilities across multiple providers.

Release date of the most common vulnerabilities affecting the top 3 cloud providers in 2021



More About the Most Common Vulnerabilities

cve-2021-43798

The top vulnerability was found in Grafana, an open-source platform for monitoring and observability (cve-2021-43798). It was discovered in June 2021, however by the end of the year there were still almost 4,000 instances of running out-of-date versions of Grafana, suggesting over a 5-month lag in patching a high-risk issue.

cve-2015-0204

FREAK (Factoring Attack on RSA-EXPORT Keys) is a weakness in some implementations of SSL/TLS that may allow an attacker to decrypt secure communications between vulnerable clients and servers.

cve-2015-4000

Logjam is a security vulnerability for systems that use Diffie-Hellman key exchange with the same prime number. Publicly reported on 20th May 2015, Logjam allows an attacker to easily decrypt sensitive data without the user's knowledge. The researchers were able to demonstrate their attack on 512-bit (US export-grade) DH systems. They estimated that a state-level attacker could do so for 1024-bit systems (then widely used), thereby allowing decryption of a significant fraction of Internet traffic.

It's surprising to see this as the second most common vulnerability found since it was first discovered over 6 years ago.

cve-2020-0796

Exposed Microsoft Server Message Block (SMB) services have been a big concern for businesses over recent years, as some of the most severe vulnerabilities associated with it could allow remote code execution. It was also catapulted into the press a few years back as it facilitated

the WannaCry ransomware. It targeted a vulnerability called EternalBlue, which was an exploit of Microsoft's implementation of SMB, and was released by a hacker group called The Shadow Brokers. The Shadow Brokers published several leaks containing hacking tools, including numerous zero-day exploits from The Equation Group, who are widely suspected to be a branch of the National Security Agency (NSA) of the United States.

What shocks us is that SMB is still internet-facing for some businesses. Given the impact of several high-profile hacks at the time surrounding the leak of EternalBlue, it is concerning to still see this service exposed and vulnerable to the internet.

Additional Findings

- Google shows the most exposed instances, likely due to its default open network configuration compared to AWS and Azure's 'secure by default' rules.
- However, AWS has the most exposed instances that are vulnerable.
- The top three cloud providers all show the same top three vulnerabilities.
- Web application are the most exposed services running on the exposed cloud instances.
- Some of the vulnerabilities seen with sizable instances exposing it are over 7 years old demonstrating one of the biggest issues in cyber security is patching.



COMPLIANCE & DATA PROTECTION



Foreword

The changes to the UK GDPR are yet to be confirmed by the Information Commissioner's Office (ICO), but they will inevitably have a major impact on how businesses process data, particularly around giving greater flexibility on how that data is handled. It's likely the move will shift away from the current universal standard, allowing smaller businesses to demonstrate data compliance in ways more appropriate to them.

The Schrems II ruling continued to be challenging for businesses throughout 2021, with additional assessments and measures being put in place. This year we also saw a recurrence in fines being brandished across Europe centred on email marketing and PECR (Privacy and Electronic Communications Regulations) breaches.

Further afield, 2021 saw China and Brazil implementing data protection legislation and (late in 2020) Singapore amended its Personal Data Protection Act. Canada and Australia continue to review their privacy regulations and amendments to the California Privacy Rights Act, which are expected to result in new state laws and legislative action at the federal level. All these changes will likely affect UK businesses that operate globally.

We continue to notice the same barriers of implementation for businesses surrounding ISO 27001 and our consultancy sessions remain key in helping businesses understand what ISO 27001 is and how the process of certification works.

Every year, across all areas of compliance, we learn more about how data protection and conforming to industry standards present new challenges to keep businesses and cyber security professionals on our toes, and 2021 was no different.

Nicky Whiting

Nicky Whiting
Director of Consultancy Division

Compliance often proves to be difficult for businesses. With significant changes coming into play in 2022, compliance and data protection are set to be especially challenging as businesses learn how they will affect them both internally and with their supply chain.

In January, significant changes came into effect with Cyber Essentials, and we've also seen several proposed changes to the UK GDPR announced for discussion in 2022.

GDPR

We can't look back at the GDPR in 2021 without mentioning Brexit and the UK adequacy decision which resulted in a big sigh of relief for UK businesses.

Although the adequacy decision allows the free flowing of personal data between the UK and EU, what a lot of companies have yet to realise is that now that the UK is a third country (a country which has implemented the GDPR as national law), there is a need for UK companies to have an EU representative if offering goods or services into the EU. Equally, many EU companies now need to have a UK representative if offering goods or services into the UK.

Another hurdle many businesses have had to face is the additional measures required by the Schrems II ruling and data transfers to the US and other third countries with intrusive law enforcement regimes which are allowed access to personal data. These include conducting a data transfer assessment and putting in place supplementary data protection measures.

The ICO is currently reviewing the European Commission's new GDPR standard contractual clauses and is advising that "organisations should take stock of the international transfers they make" and "update their practices as guidance and advice become available."

Here are the top GDPR failures that our DPO team have seen:

- 1** Lack of awareness that the EU-US Privacy Shield was no longer valid
- 2** Not having visibly clear and obvious cookies banners on websites
- 3** Incomplete or missing Records of Processing Activities (RoPA) in accordance with the requirements of Article 30

GDPR Fines

Across Europe there have been some staggering GDPR fines but at present the UK seems to be very focused on breaches of direct marketing – so organisations should check that their email and telephone marketing practices are compliant with both PECR and the GDPR.

Another area we have seen increasing levels of activity since 2020 is in relation to cookies. There have been several instances of individuals approaching organisations with the threat of legal action, claiming "damages" because of unlawfully placed cookies. Our advice to companies is to review their cookie banners to ensure they meet the consent requirements and check their cookie policy is up to date. If they receive a request for damages, legal advice should be sought, however, a recent case in the Supreme Court appears to have made these claims less likely to succeed.



What's Next?

The UK government is currently consulting on changes to the UK GDPR with the aim to reduce "red tape". This is a tricky road to travel given that any significant divergence from the EU GDPR could result in the UK losing its adequacy decision. However, in his previous role as Privacy Commissioner in New Zealand, John Edwards, the UK's new Information Commissioner and successor to Elizabeth Denham, had successfully overseen the achievement of an EU adequacy decision despite the NZ privacy laws not being identical to the EU GDPR. He has stated that in his new role he is looking for privacy laws that are common sense and wants to avoid "box ticking".

Although there are no confirmed changes to the UK GDPR in 2022, there are several under consideration, including:

- Removing the obligation to appoint a DPO (Data Protection Officer)
- Removing the need for DPIAs (Data Protection Impact Assessments)
- Relaxing rules on cookies so that consent will not be needed for analytics cookies
- Removing the need to prepare records of processing
- Removing the need to consult the ICO in relation to high-risk processing.
- The need to implement a "privacy management programme"

We watch and wait with anticipation.

ISO 27001

Supply chain security is still very much the driver for most companies embarking on the journey to ISO 27001.

Up to **40%** of cyber threats are now occurring indirectly through the supply chain¹⁴

This is a growing trend with many of our customers seeking help with ISO 27001 implementation resulting from customer pressures.

Barriers to implementation

One of the biggest barriers we encountered in 2021 was a lack of understanding of what ISO 27001 is and what it entails. Many businesses only know about it because their customers have demanded it of them and currently, the vast majority hold a misconception that it is

simply a set of controls they need to apply. This results in the project being given to the IT department to implement which is not the right approach.

ISO 27001 is a business-wide management system that requires a fundamental cultural change and top-down approach from senior management, who will need to embed it across the entire business. Our experience has shown that companies still need to understand the importance of ISO 27001, what it involves, its demands, the resources needed, and the costs and processes involved in obtaining certification. With this knowledge, organisations will go into certification fully prepared and ready for the challenge ahead.

Our experience has shown that companies still need to understand the importance of ISO 27001.

What's Next?

With updates to ISO 27001 and 27002 planned in 2022, organisations that have already implemented ISO 27001 will need to review the new requirements and plan to implement the changes during the expected 2 year transition period that is usually provided when there is a major update.

Cyber Essentials & Cyber Essentials Plus

Cyber Essentials is growing in popularity as more businesses recognise the importance of being able to demonstrate that they are taking cyber security seriously and insist their supply chain does the same.

We find that these are the most common reasons why customers fail Cyber Essentials:

- 1 Not answering the question fully
- 2 Not having formally written down processes
- 3 Having out of date devices or operating systems

With Cyber Essentials Plus these are:

- 1 Letting the 90-day time limit expire
- 2 Malware and virus files not being blocked or hindered from internet downloads
- 3 Out of date software/ application versions, device types, and operating systems

What's Next?

The question sets for Cyber Essentials are reviewed on an annual basis, and with the changes to how businesses operate over the past two years, it's no surprise that we're seeing a significant amendment to the scheme in 2022. The changes have been implemented to address current cyber security risks, with organisations adopting remote working practices and the use of cloud applications which bring along new cyber security risks to networks and infrastructures. The updated set of Cyber Essentials requirements are the most significant change to the scheme since their introduction in 2014.

Key Takeaways

- In 2021, the EU formally recognised the UK as having high data protection standards, which meant the UK achieved an adequacy ruling allowing free flowing of personal data from the EU to the UK.
- Major Cyber Essentials updates which came into effect in early 2022. Organisations will need to understand the new questions and requirements to achieve certification, as well as understand when current assessments will need to be submitted by to meet existing requirements.
- GDPR fines remain prevalent in email marketing and breaches of PECR.
- GDPR fines issued around the unlawful use of cookies has also risen in 2021. We advise organisations to review their cookie banners and ensure they consent lawfully to legal requirements. Furthermore, organisations should be reviewing their cookie policies regularly and keeping them up to date.
- Smaller businesses have begun taking steps to implement ISO 27001 in 2021 as the previous year's growing trend of cyber threats occurring indirectly through the supply chain has shown no signs of change.

Conclusion

The data we gathered from our honeypot findings, penetration testing and other threat monitoring methods from the past year demonstrated common problems of cyber security that can affect companies no matter their industry or size. Our showcases highlight these everyday vulnerabilities amidst a threat landscape dominated by the changing working environments and an increase in cloud technology use. Cyber security complacency means businesses create open servers for cyber criminals to walk straight in and attack at their leisure.

Here's a summary of our 2021 report and the challenges businesses continue to face and will need to prepare for in the new year.

Vulnerabilities & Risk Management

The security vulnerabilities we encountered in 2021 showed us that a large proportion of organisations are not implementing the appropriate strategies to combat threats, primarily due to a lack of basic understanding, which can be extremely damaging. Simple measures such training staff can go a long way to improving a business's security posture.

Log4j and other major vulnerabilities this year will hopefully help businesses realise the need to prioritise and invest in their cyber security for 2022 and beyond.

We also found patching to be inconsistent between organisations who managed their web servers centrally to those who relied upon third parties.

Threat Protection & Intelligence

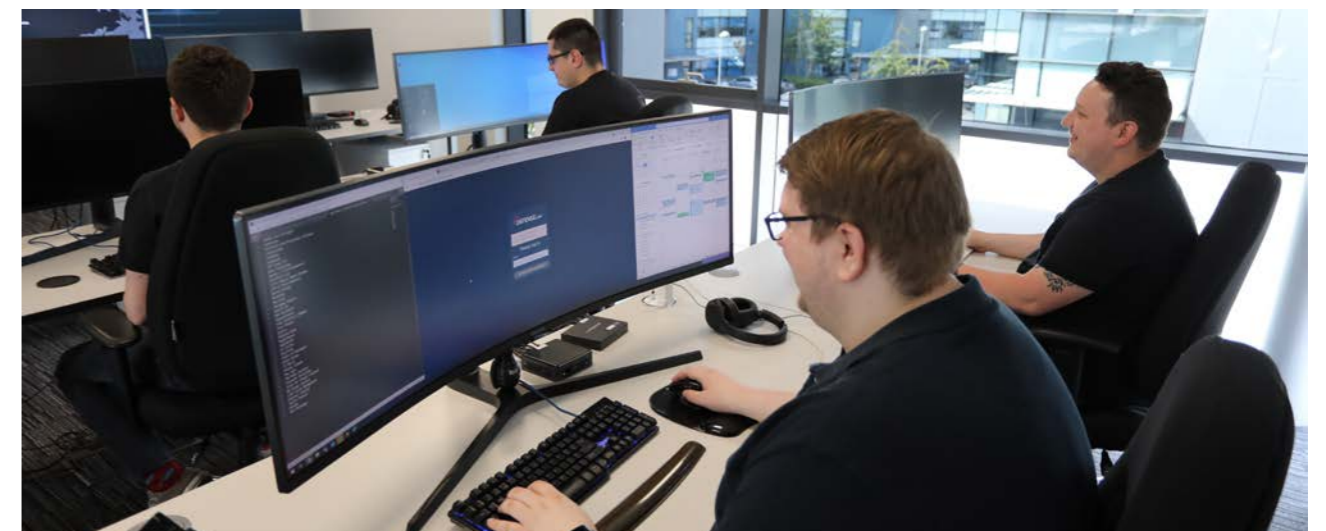
We've seen companies treat cyber security as a 'set and forget' method, leaving them vulnerable to multiple attack vectors. Cyber security is an ongoing process which needs continuous monitoring to understand, detect, and remediate any risks to the company's network and infrastructure.

One of the leading concerns is businesses being hit with brute-force attacks due to a lack of cyber security awareness training within the workforce. If the workforce is considered the first line of defence, then businesses need to ensure staff are following cyber security best practices to avoid human error. A key approach is to support a top-down privacy and security culture.

Compliance & Data Protection

2021 saw a considerable increase in companies wanting to achieve Cyber Essentials and ISO 27001. Defense.com™ noticed a year-on-year 146% and 228% increase in Cyber Essentials and Cyber Essentials Plus customers ordering and achieving both certifications, respectively. Also noticeable were the challenges businesses were facing in their general understanding of compliance, which if not addressed can lead to reputational and financial damage if a breach was to occur.

New changes were also announced this year for Cyber Essentials, which also highlights the importance of understanding compliance to stave off any barriers for implementation. Knowledge is the first step to achieving compliance, and with the world of data protection evolving each year, you should stay prepared for what 2022 may bring.





Final Word

Oliver Pinson-Roxburgh
CEO & Co-Founder

There's a discussion to be had over how much time, money and resources should be invested in your cyber security. Complacency has been a big factor when assessing how businesses are managing their security and how easily hackers are breaching their systems. I have heard too many customers talk about how they use a platform that already has security controls in place, which leads them to believe that they don't really need to do anything. This breeds complacency and can result in increased cyber risks.

What's more, there is a heavy reliance on the cyber security provided by third-party services. It's public knowledge that both nation states and APTs are targeting third parties, therefore vendor due diligence is a must for the future. The driver to use these third parties is often a decision made due to resource constrained businesses requiring a less resource intensive approach to running in-house solutions.

It's clear from our report that businesses need to be continuously monitoring for cyber attacks, no matter the size of the organisation. There are threat actors constantly targeting internet-facing systems because they are easy targets.

However, businesses need enough flexibility and customisation in these providers to make it more attractive than building their own, which is why cloud providers become ever more complex. This means it is important now more than ever that cloud providers

do enough to guide businesses to correctly harden their systems and not open themselves up to attack. Businesses must also understand that security and compliance is always your responsibility and should be secure by design.

Businesses are still missing daily best practices that reduce the risk of data breaches and strengthen their cyber resilience, often opting for an annual or 'as and when something happens' approach that puts pressure on and leads to mistakes. Hackers are opportunistic; sometimes they don't even know what data is on a target or what they will find before they try hacking. Having security measures in place is simply not enough - you need to be maintaining them because unless organisations are actively monitoring their systems, they will likely miss indicators of attack and subsequently they will have no chance to take corrective action. This can lead to attacks being missed completely or leaving the door wide open to cyber criminals. Not every business has the same risk appetite, so it is essential organisations are consistent when it comes to monitoring cyber threats and security is supported from the top of the organisation.

It's clear from our report that businesses need to be continuously monitoring for cyber attacks, no matter the size of the organisation. There are threat actors constantly targeting internet-facing systems because they are easy targets. Getting the fundamental best security practices right is critical, as hackers will focus on easier targets before embarking on more complex attacks, innovating and moving on to new vulnerabilities along the way.

Over the course of 2022 and beyond, we envisage hackers targeting users as a top priority via social engineering tactics. Cyber security gets complicated when you broaden your attack surface, for example when introducing widespread remote working, and the tools to manage this can become overwhelming. One strategy that is driving the attackers to focus more on social engineering techniques is the changing business landscape and flexible working arrangements. Attackers are now even reverting to techniques like sending USB sticks to remote workers to gain access to systems and install malware.¹⁵ The more disparate your workforce becomes, the more challenging it is to educate and monitor future cyber threats.

My five suggestions for the year ahead:

- 1 Consider your cloud instances and what is being deployed as we see lots of instances that don't seem to be following best practices.
- 2 User credentials are still the top target for opportunistic attacks. Use Two-Factor Authentication (2FA) and train your staff to spot suspicious activity.
- 3 Compliance is set to evolve even more this year, so make sure you are on top of the changes.
- 4 Monitor your systems properly; with the amount of ongoing malicious activity, it's important to be aware of what traffic is hitting your exposed systems.
- 5 Be aware of the latest vulnerabilities to prioritise remediation and being able to respond quickly to incidents. This is critical as your IT environments grow.

Thank you for reading our report and we hope that it helps to better inform your organisation's security strategy moving forward into 2022 and beyond.

References

1. https://www.accenture.com/_acnmedia/PDF-116/Accenture-Cybersecurity-Report-2020.pdf
2. <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021>
3. <https://www.bitdefender.com/blog/hotforsecurity/linkedin-email-subjects-remain-the-top-clicked-social-media-phishing-scams-in-2021/>
4. <https://www.akamai.com/content/dam/site/en/documents/ebook/top-10-considerations-for-bot-management-ebook.pdf>
5. <https://www.ncsc.gov.uk/files/NCSC%20Annual%20Review%202021.pdf>
6. <https://www.ncsc.gov.uk/news/microsoft-update-brute-force-password-spraying>
7. <https://msrc-blog.microsoft.com/2021/06/25/new-nobelium-activity/>
8. <https://www.bitdefender.com/blog/hotforsecurity/linkedin-email-subjects-remain-the-top-clicked-social-media-phishing-scams-in-2021/>
9. <https://www.akamai.com/content/dam/site/en/documents/ebook/top-10-considerations-for-bot-management-ebook.pdf>
10. <https://cybernews.com/security/rockyou2021-alltime-largest-password-compilation-leaked/>
11. <https://www.deccanherald.com/business/google-beefs-up-internet-security-with-simplify-buyout-1067973.html>
12. <https://www.flexera.com/blog/cloud/cloud-computing-trends-2021-state-of-the-cloud-report/>
13. <https://www.flexera.com/blog/cloud/cloud-computing-trends-2021-state-of-the-cloud-report/>
14. https://www.accenture.com/_acnmedia/PDF-116/Accenture-Cybersecurity-Report-2020.pdf
15. https://www.ncsc.gov.uk/report/weekly-threat-report-14th-january-2022#section_1