Smarttech
YOUR 24/7 SECURITY PARTNER

Cybersecurity Insights For 2022 - Report

www.smarttech247.com

Smarttech
YOUR 24/7 SECURITY PARTNER

Table of Contents

Foreword

Cybersecurity – Reaching New Levels Of Uncertainty

Ransomware, Nation State Attacks and Supply Chain Threats have defined 2021, a year in which cybercrime has put tremendous pressure on healthcare systems, educational institutions, critical infrastructure and businesses.

Earlier in May, we experienced one of the **most devastating attacks ever conducted in Ireland** – with many hospitals still facing the aftermath of the Conti ransomware attack to date. Other countries have also suffered similar attacks on their health systems and critical infrastructure.

We have witnessed an **increase in sophistication and creativity** when it comes to threat actors' TTP (tactics, techniques and procedures) with attacks getting larger, more personal, and more devastating. Multidimensional extortion has become a popular tactic for ransomware threat actors – putting organisations' data and operations at higher risks than ever. The connected nature of our world as well as the dependency on digital have expanded the supply chain attack surface with vulnerabilities.

Complex ecosystem structures (cloud providers, SaaS organisations, Internet of Things (IoT) device manufacturers, etc.) are making it easier for adversaries to infiltrate systems and, conversely, more difficult for defenders to predict and prevent these threats.

What will be the cybersecurity challenges to overcome in 2022?

Understanding the threat landscape is a crucial step in building robust defences. The Smarttech247 experts have compiled this report to share insights into what security challenges CISOs should prepare for and how organisations can build greater resiliency and integrate this into all aspects of business operations.

Most Prominent Threats of 2021

2021 has seen many remarkably high-profile cyberattacks, noted by the extent of the damage caused, including the cost to businesses and the broad impact on their customers.

The year saw a significant spike in ransomware attacks and continued elevated levels of phishing and endpoint attacks. The incidents themselves have also seen significant increases in sophistication, persistence and prevalence.

Log4j Meltdown

CVE-2021-44228 - The severity 10 vulnerability that broke the hearts and minds of IT Security Teams globally in **December** as buzzers went in off through the night over 'Log4j2'. The vulnerability was a in a Java-based logging utility (API), commonly used together with the well known open-source web application framework 'Apache Struts'. This new vulnerability allowed attackers to craft malicious input data using a JNDI Lookup pattern resulting in remote code execution (RCE), denial of service (DOS) attacks and more. **But what was the fuss really about?** Well unlike a regular software based vulnerability, Log4j is essentially embedded into most Java based web services due to its association with Apache - widely used by enterprises globally to develop Java Web applications, Web Servers, Application Servers and more.

With estimates suggesting over 65% of the Fortune 100 companies relying on web applications built with the Apache Struts framework, this disclosure not only sent a shiver down the spines of CISOs and IT directors, but it once again highlighted the fragility of web-facing global infrastructure.

Emotet – we're back!

In late **November 2021**, just as IT directors were setting their sights on consolidating Q4, the primary access 'back-door' group (previously thought to have been dismantled by Europol in January 2021) is reborn – and operating en-force. First observed in mid-2014, the Eastern Europe & Russian Federation group's objectives included credential stealing, sending spam campaigns, and installing banking malware or other payloads such as Trickbot & Dridex. This actor primarily uses compromised infrastructure for payload hosts and proxies for its Command and Control. With Emotet re-entering the battlespace acting as a primary access broker, we are likely to see a rise in further headline grabbing Ransomware attacks. Current deployment tactics seen include wide-scale spam campaigns using Excel macro documents and PDF attachments containing URLs linking to Jscript downloaders to download Emotet on the unsuspecting victim.

Most Prominent Threats of 2021

Vive la 'Tiny Nuke'

The **Banking Malware** that nearly exclusively targets French organizations, was first seen in 2018 and reared its head in time for Christmas 2021 with campaigns targeting hundreds of organizations in various industries including manufacturing, technology, construction, and business services. The campaigns leverage invoice-themed lures written in French language.

Tiny Nuke is used to steal credentials and other private information and can be used to enable follow-on malware attacks. The author initially released the code on GitHub in 2017, and although the original repo is no longer available, other open-source versions of the malware exist. The attack is launched via email, with messages sent to victims containing URLs that lead to the download of a compressed [ZIP] executable responsible for installing the second stage malware - Tiny Nuke. The actor generally uses legitimate but compromised French language websites to host the payload URL and C2 communications occur via Tor.

SocGholish

SocGholish targets USA, GBR, FRA, ESP, JPN, and AUS via Drive-by-Downloading supported by Russia-based cybercriminal groups. **The operators behind these campaigns use compromised sites to spread fake updates masquerading as expired anti-virus programmes, Adobe Flash notifications, Chrome, and Firefox updates.** Compromised websites harbouring 'SocGholish HTML injects' are tailored on the user environment (such as geo location, operating system, and browser). These pages use **social engineering** in order to convince potential victims to take an action such as clicking a button, which in turn causes a JavaScript or HTA file to be downloaded [mostly from a Dropbox link]. If executed, the script will fingerprint the system and (if the user's geography is targeted) download and execute a second stage malware.

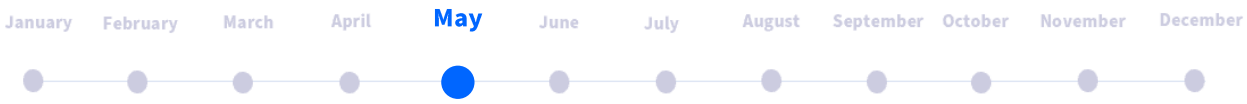
The overwhelming majority of SocGholish threat volume for December shows a rise of compromised websites within the United States, and second-stage payloads including Dridex (banking malware) and more recently deploying PayloadBin Ransomware.

Notable Cybersecurity Events 2021

The University of California suffered a significant data breach that resulted in the exfiltration of personal information of staff and students, including social security and financial details. The attackers exploited a vulnerability in Accellion's legacy File Transfer Appliance to gain access to the systems. The attacker then used the contact information in the stolen records to contact each affected person by email, threatening to disclose their personal details in an attempt to blackmail the victims.

The Chinese state-sponsored hacking group **HAFNIUM** used a zero-day exploit to attack Microsoft Exchange Servers worldwide to steal sensitive information. This attack leveraged 4 vulnerabilities to provide a sophisticated attack profile. The attacks were targeted at specific sectors, primarily related to the defence and medical research sectors. It is believed that over 30,000 organisations were affected.

US-based CNA Insurance suffered a ransomware attack that resulted in the temporary halt to all trading and the disclosure of staff's personal data, including social security numbers. The attack was conducted by the Russia-based hacking group **REvil** Corp using a novel ransomware code, and it's reported that a ransom of $40 million was paid to restore the systems.



The Irish Government's Health Service Executive (HSE) suffered a ransomware attack resulting in a systems shutdown. This disruption resulted in an inability to access digital medical records, cancelled outpatient appointments, and affected some non-critical services. The attack was traced to the Conti criminal group who demanded a $20 million ransom. However, services were restored without payment being made. Recently released reports show that the attackers gained access to systems as early as March 2021, when a user opened a malicious attachment received through a phishing email. The ransomware that was introduced into the system was set off on May 14th, which led to an immediate crisis across the health service.

The Colonial Pipeline suffered a ransomware attack resulting in the pre-emptive shutdown of computer-based systems to limit potential damage. This refined oil pipeline network is the largest in the USA, over five and a half thousand miles in length, transporting two and a half million barrels of gasoline, diesel, and jet fuel from refineries in Texas up the East Coast to New York City. The affected pipeline connects twenty-nine refineries with 267 distribution terminals, accounting for up to 15% of the daily oil capacity in the US. The attack resulted in the controlled shutdown of the pipeline for six days, with two more days required before returning to regular service. With the pipeline providing around 45% of the fuel used in the East Coast states, this led to significant shortages and caused knock-on effects, including changes to flight schedules and price rises at affected automotive filling stations. The attack was traced to the **DarkSide** criminal group based in Russia. One giveaway to their identity was a line in the ransomware software preventing installation on any device where the operating system language was set to Russian.

Meat processor JBS Foods suffered a ransomware attack that resulted in a temporary halt to all operations across the US, Canada and Australia. The attack was conducted by the Russia-based hacking group **REvil** and resulted in JBS Foods paying a ransom of $11 million.

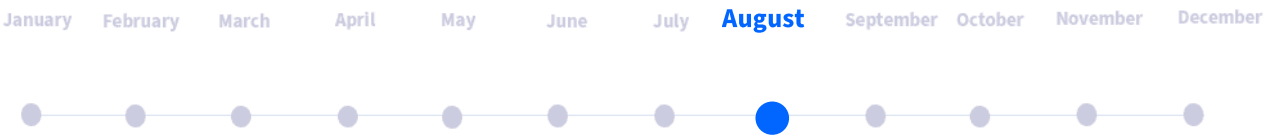
Computer manufacturer Acer suffered a ransomware attack that resulted in the disclosure of sensitive commercial and financial information samples. The attack was conducted by the Russia-based hacking group **REvil** using a vulnerability in Microsoft Exchange.

European insurance company AXA suffered a ransomware attack traced to the **Avaddon** group. The attack affected the companies' Asian operations, with over 3 TB of data stolen. The attack occurred after the company announced that its cyber insurance products would no longer cover ransomware payments.

The widely used Kaseya Virtual System Administrator (VSA) remote network management tool was leveraged by the Russia-based hacking group **REvil** to launch ransomware attacks on thousands of users of this tool. VSA is used by Managed Service Providers (MSP) to provide software updates to their clients.

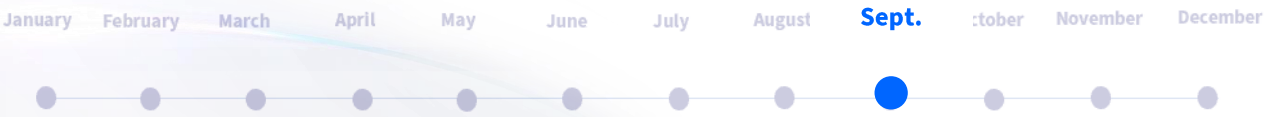
As a result of the compromise of the VSA tool, it automatically deployed the **Sodinokibi** malware to around 60 of Kaseya's direct customers and between 800 to 1,500 end clients. The attack exploited a newly discovered SQL injection vulnerability to compromise the VSA application. Unlike most recent malware attacks, the ransomware payload was executed almost immediately with no time for data exfiltration.

Post-incident analysis suggests this tactic was employed as the attackers believed a patch under development for the vulnerability would be quickly issued.



Consulting firm Accenture suffered a ransomware attack resulting in the theft of over 6 TB of proprietary data.

The attack was traced to the **LockBit** group who demanded a $50 million ransom. While systems were restored from backups, over 2,000 stolen files were subsequently published online.



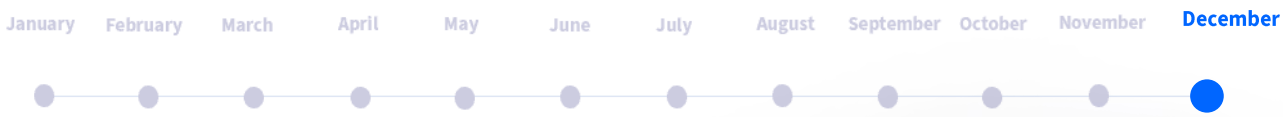
In September, the former digital camera specialist, Olympus was forces to shut down its networks in Europe, Africa and the Middle East due to a ransomware attack.

The company was hit again, almost one month later, this time leading to the shut down of their IT systems in the U.S., Canada, and Latin America with no impacts on other parts of the world. Olympus did not disclose whether or not customer data was accessed during the cyber attack. The attack is believed to have been carried out by the ransomware-as-a-service (RaaS) group **BlackMatter**.

On 9th November, Robinhood Markets Inc. announced a security breach that exposed the personal information of 7 millions of its users. Most of the 7 million affected accounts had only one piece of personal information exposed: either the user's name or their email address. But in over 300 of these cases, more sensitive data such as date of birth and zip code was uncovered, as well as the user's full name. The main threat from this breach is that the exposed information could be used to facilitate further attacks.

MediaMarkt, Europe's largest consumer electronics retailer has suffered a Hive ransomware with an initial ransom demand of $240 million, causing IT systems to shut down and store operations to be disrupted in Netherlands and Germany.

MediaMarkt employs approximately 53,000 employees and has a total sales of €20.8 billion. Hive Ransomware is believed to be behind the attack and initially demanded a huge ransom of $240 million to receive a decryptor for encrypted files. This size of a ransom is typical to allow room for negotiation

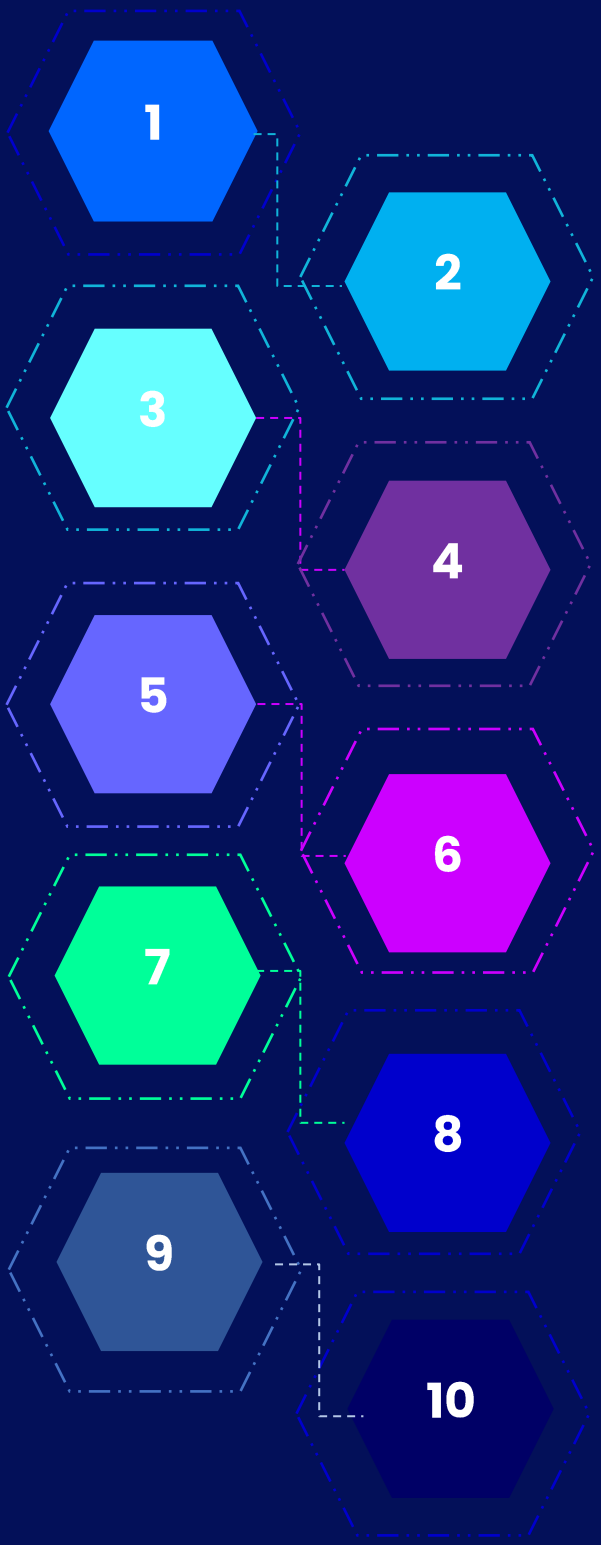


As mentioned in the beginning of our report, in December the world faced the implications of the Log4j vulnerability and we saw the first public case of Log4Shell used to download and install ransomware.

Mid month, the Irish health system suffered another attack where the Coombe Women & Infants University Hospital in Dublin was hit with Ransomware. The incident triggered many other hospitals to temporarily cut access to the wider network and take precautionary measures in order to avoid another national crisis.

Smarttech
YOUR 24/7 SECURITY PARTNER

Cybersecurity Insights for 2022



1. Supply Chain breaches will continue to make headlines
2. A new era for recalculating cybersecurity risk
3. Cloud security is growing – and so will the attack surface
4. Phishing is here to stay – and it's only getting worse
5. Operational Technology threats will continue to put pressure on critical infrastructure
6. Nation-state attacks must be top of mind for CISOs in 2022
7. The cryptocurrency industry expected to steal the limelight
8. Privacy concerns around augmented reality will grow
9. Resource Hijacking
10. Ransomware will continue to shape the threat landscape

1 Supply Chain Breaches Will Continue To Make Headlines

Supply chain security continues to be a significant factor for businesses. It's predicted that most security incidents in the commercial sector will include a third party in the attack vector. The **SolarWinds** incident brought supply chain attacks to prominence, and the expectation is that such attacks will increase in prevalence. Small vendors and suppliers typically implement less robust security controls than large organisations and governmental departments, providing an easier ingress point for an advanced persistent threat.

Modern appliances increasingly leverage APIs to provide connectivity for information flows. As a result, managing authentication and monitoring processes to prevent attackers from exploiting API weaknesses to launch attacks across the interconnections will be critical.

The majority of supply chain attacks leverage network connectivity as part of the attack profile. For example, access credentials for an authorised supplier can gain access to an organisation's supply chain network. This compromise provides the base for the attacker to move laterally across to other systems within the organisation to either continue up the supply chain or search for information of value. This was best seen in 2013 when an attack on a refrigeration service company allowed access to the network of the US retail giant Target and the subsequent theft of the payment details for over 110 million customers.

Using what was believed to be SQL-injection attacks for initial ingress, the attacker laterally moved across systems and was able to install malware on the point of sale devices that captured and exfiltrated sensitive payment information.

Supply chain attacks can also exploit trust-based relationships with product vendors and their customers. Embedding malware within equipment at the production stage can provide a mechanism to gain access to the customers' systems of the equipment. The majority of organisations operate on the assumption that new equipment is secure by default, rarely conducting security checks before its connection to their networks. Advanced malware can evade the traditional security controls that detect abnormal behaviour of a new endpoint inside the perimeter defences.

Adopting the Industry 4.0 philosophy and digital transformation processes rapidly expands the prevalence of network-connected devices across businesses. As a result, significant growth in electronic network-connected entities is expected, from simple Internet of Things (IoT) to complex operation technology and manufacturing equipment. Consequently, managing the security of these endpoint identities will become an increasingly vital part of business operations. As a result, enterprise-wide machine identity management is expected to be an emerging feature of integrated security solutions.

2

A New Era For Recalculating Cybersecurity Risk

One of the ramifications of the advanced threat landscape is recognising that no single security solution can offer perfect protection over its lifetime. State nations devote significant resources to analysing popular security products and technologies to discover exploitable vulnerabilities. The answer is **strength in depth**, **overlapping security solutions that provide functional redundancy**.

A vulnerability or flaw in one security control will be covered by the protective capabilities of at least one other security control. The key to redundancy is independence. Products produced by the same vendor will likely rely on shared modular components or be developed using the same tools, processes, and practices. Therefore, there is a high probability that a vulnerability inadvertently designed into one product will appear in all those vendors' products. While closed ecosystem product suites offer financial benefits in volume discounts and simpler maintenance processes, they offer less robust security controls than diverse security solutions from independent providers.

This diversification can be challenging for customers when security providers are currently going through a consolidation process. Mergers and acquisitions mean that several separately branded security solutions have single common ownership and have potentially lost or will lose functional independence in the future.

Identity-first security will become more crucial than ever.

The predicted increase in the use of hybrid environments continuing trend for migration to cloud applications is placing greater emphasis on identity-based perimeter defences. As a result, the importance of Identity-first security is becoming more critical as attackers are expected to target identity and access management functions to obtain a silent, persistent presence on systems.

Currently, identity and access management rely on **usernames and passwords**. Typically the username is a name or email address which generally are publicly available information. Security robustness then comes down to the password. Unfortunately, most security incidents where access credentials are compromised can be traced back to users having weak passwords that are easy to guess or the result of the user providing the password to the attacker via a phishing technique or other social engineering method. **Multi-factor authentication** protects against these risks but comes with increased user inconvenience.

2

A New Era For Recalculating Cybersecurity Risk

The world of password security is changing

Passwordless authentication techniques are being seen as the answer to this dilemma and are expected to receive broader adoption in the future. Users identify themselves using biometric information such as a fingerprint or present physical proof of identities such as a proximity badge, USB device or hardware token. Combined with a single sign-on solution, this offers users maximum convenience, eliminating the inherent flaws of a memorable password. The downside is the increased costs associated with the technology, but the potential long-term savings in reduced risk of cyberattack will balance this initial capital outlay.

Passwordless authentication should be coupled with access rules based on contextual information such as location, time, endpoint device identification to prevent misuse of a lost, stolen or cloned physical token or the replay of compromised biometric data. These additional restrictions will provide a more robustly secure solution.

3

Cloud Security Is Growing – And So Will The Attack Surface

Remote working has seen a growth in the adoption of software-as-a-solution services, cloud-based applications providing the ideal solution for enabling working from home for collaborative work practices that act on central corporate data. Access credentials for such SaaS services are an attractive target for attackers looking to access such data. Social engineering and phishing are relatively simple, low tech attack vectors. Working from home has made inter-employee interactions using email and other messaging services more commonplace, increasing the success rate of phishing techniques. Two-factor authentication is a popular solution to protect against credential threats, but many organisations do not implement authentication processes correctly. Unless the two factors are genuinely independent, they offer little additional protection. For example, a second factor that sends a code by email can be relatively simple to intercept by a capable attacker who has stolen an employee's username and password.

A method of securing SaaS applications expected to gain traction is a cloud access security broker (CASB). This service acts as an intermediary between users and cloud services, including SaaS and Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) environments. A key element of CASB is identity verification and access control. The CASB allows an organisation to extend its security policies to cover the cloud-based services, irrespective of how the user accesses the services. This service offers significant benefits for working from home practices that allow users to access corporate systems using personal devices. It also eliminates the security issues of users accessing services or applications that are not under corporate control, the Shadow IT problem.

With worldwide revenues currently at around $2 billion, the CASB provider market is expected to double within the next three years.

As well as managing access controls and Shadow IT discovery, CASB providers may also include data loss prevention, compliance and governance services. Typical CASB services are implemented using cloud-hosted software, though some providers offer on-premises software or hardware solutions.

An emerging solution for the protection of sensitive data against security breaches is privacy-enhancing computation techniques. This approach goes beyond protecting data at rest and in transit and applying protection techniques while data is in use. This technique is expected to deliver more secure data processing and sharing, protecting data even in an untrusted environment.

4 Phishing Is Here To Stay – And It's Only Getting Worse

Another issue seen with the broader adoption of SaaS services is the threat of phishing techniques. Phishing will remain a substantial cyber security problem as attackers look to steal access credentials. **More than 75% of targeted cyberattacks are believed to begin with a successful phishing email.** The majority of businesses still place significant reliance on perimeter defences in the form of firewalls and intrusion protection systems to protect their infrastructure. However, an attacker can leverage stolen credentials to bypass these controls. Unless the organisation has deployed a network detection and response (NDR) solution or invested in deception-based security, the attacker can maintain a hidden presence within systems to execute persistent surveillance and intelligence gathering, evading basic network security controls. While there are many anti-phishing techniques available to organisations, the most effective solution is employee awareness training. However, there are limits to the effectiveness of automated content scanning. Machine learning techniques to identify potentially suspicious links have limitations with the vast resources that organised criminal enterprises can devote to crafting enticing phishing material. Unfortunately, employees are inherently fallible, forgetting their training over time or acting in haste when under perceived time pressure to react to a compelling request.

The best defence is the multi-layered approach that offers a customised phishing solution. First, technical controls can weed out the obvious and highlight the possibly suspicious. Then, training in phishing recognition and critical thinking techniques followed by refresher training and test campaigns can reinforce awareness.

Breach and attack simulation (BAS) services are predicted to emerge as part of security-as-a-service offerings, providing organisations with continuous testing and validation of security control against simulated external threats. Vulnerability detection and remediation combined with targeted training are intended to help organisations validate and enhance their security posture.

"43% of breaches involved phishing in 2021"

(*Verizon 2021 Data Breach Investigations Report*)

5

Operational Technology Threats Will Continue To Put Pressure On Critical Infrastructure

Operational technology (OT) is predicted to become a crucial battleground as advanced persistent threats seek to exploit vulnerabilities to gain access to better-protected information systems.

OT are the programmable devices that interact with the physical environment, including industrial control systems, building management systems, physical intruder alarm and fire control systems, and physical access control mechanisms.

Traditionally separate from information systems, network connectivity and automation mean that OT is now an integral part of an organisations infrastructure. The primary issue is that the IT department does not manage such systems and is not covered by IT security solutions for many organisations. However, their connectivity allows them to be exploited as a point of ingress for an attacker.

Incidents have been seen where OT equipment has been observed to include undocumented connectivity with mobile telephone networks for vendor diagnostic and maintenance purposes while also providing documented network connectivity for local control and monitoring. This connectivity creates a bridge between the internal network and an external, unprotected network. An attacker with knowledge of this bridge could effortlessly use it to gain unconstrained network access.

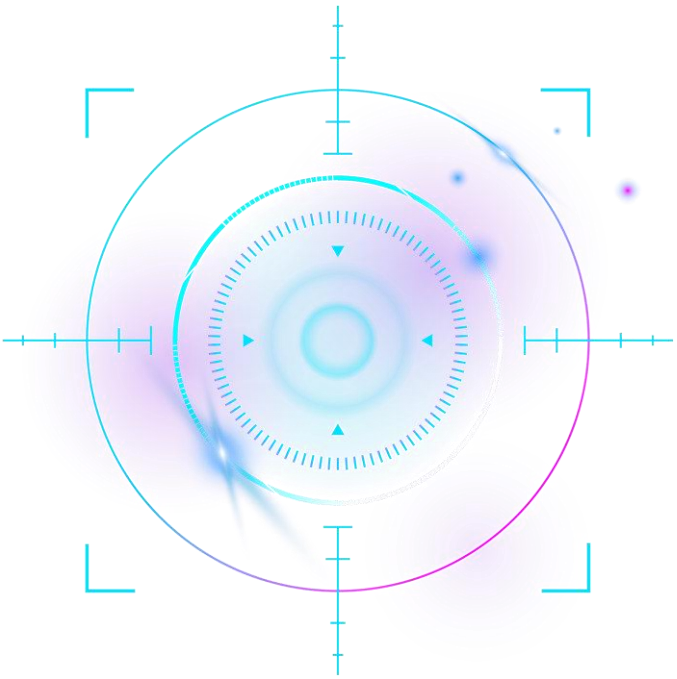
The most significant risk is that OT equipment is used extensively to control and manage critical infrastructure from power distribution networks, telecommunications, the supply of local utilities, including gas and water.

These are all routinely targeted by nation-states looking to cause disruption or criminal groups looking to extort payments. For example, the Colonial Oil Pipeline ransomware attack is a case where criminal extortion ended up causing significant and widespread disruption to a large area of the united states.

5

Operational Technology Threats Will Continue To Put Pressure On Critical Infrastructure

OT security solutions are expected to become more prevalent and visible as organisations recognise the significance of the threat and look to manage the risks.



While the principles of protecting OT and IT are remarkably similar, OT has differences that require a bespoke approach. For example, for critical infrastructure, downtime due to security patch installation processes is typically unacceptable. In the past, this led to unpatched systems and the acceptance of risk. Now, sophisticated and more frequent attacks mean the risk landscape has changed, along with risk appetite. As a result, OP security solutions that offer live patching with zero disruption are expected to become more widely adopted. In parallel, OT will be seen as part of IT within organisations and included in the overall security solutions.

6

Nation-state Attacks Must Be Top of Mind for CISOs in 2022 – Not Only For Governments

Nation-states have long used cyberattacks to disrupt services and infrastructure in other countries and exfiltrate sensitive information for intelligence gathering.

In 2020, a cyberattack on water companies across Israel attempted a coordinated attempt to increase the amount of chlorine added to drinking water to harmful levels. The attack, attributed to Iran, was unsuccessful and led to retaliatory cyberattacks.

In July 2021, a cyberattack affected the information boards at railway stations across Iran and train tracking systems, leading to large-scale delays and cancellations of train services. This attack was followed in October 2021, when a cyberattack shut down every gas station in Iran by disabling the government-issued electronic payment cards that allow citizens to purchase fuel at subsidised prices. Both attacks had common traits that suggested they were linked. In both cases, the intent was to inconvenience ordinary citizens across the country.

The use of cyberattacks are part of disputes between nation-states is expected to increase.

The risk to organisations is the collateral damage that they can experience when attacks spread beyond intended targets. This effect was most widely seen in 2010 when the Stuxnet computer virus caused widespread disruption worldwide by attacking the supervisory control and data acquisition (SCADA) systems used in industrial control systems. Nation-states originally developed the virus to attack specific equipment being used by Iran for nuclear weapons development. While this attack successfully disrupted uranium enrichment processes, it also spread across the internet to other equipment located around the world. Victims included Chevron, the US energy provider.

Cyberattacks are also employed for intelligence gathering. China, Russia and Iran routinely target governments and commercial organisations in the US and UK. Defence, aerospace and telecommunications companies are frequently attacked. However, the last two years have seen significant efforts spent by these countries looking to attack medical research organisations to gather covid-19 vaccine information. It is not uncommon for such attacks aimed at stealing information to disrupt the activities of the target organisations, which can have serious consequences. The recent SolarWinds attack is an example of a state nation deploying an advanced persistent threat to infiltrate government and defence organisations to gather intelligence on a wide scale.

6

Nation-state Attacks Must Be Top of Mind for CISOs in 2022 – Not Only For Governments

Currently, over 58% of attacks on the US originate from Russia, and success rates have grown from 21% in 2020 to 32% in 2021. The vast majority of these attacks were for intelligence gathering rather than extortion or disruption.

While China remains highly active in intelligence gathering, its focus has moved away from the US to targets related to its Belt and Road initiative.

The significance of leveraging attacks for geopolitical purposes is that cyberspace levels the combatants. Any nation can launch cyberattacks with an actual or perceived grievance against any other country or international organisation. The size and wealth of the parties involved have little bearing on the capability of the attack. Arguably countries in North America and Europe having more reliance on information systems and critical infrastructure connectivity are more vulnerable to attack than countries in other less developed regions.

European Russian, American Chinese and Israeli Iranian tensions are the current focus of geopolitical tensions, with North Korea being an ever-present threat. Financial sanctions remain the primary tool used by the West to leverage change on what it sees as rogue states and their leadership. However, cyberwarfare is now seen as a critical tool used to resist such sanctions. The expectation is that climate change will provoke more significant tensions, particularly between those countries most affected and those that emit the most greenhouse gases. This development may well see a substantial increase in nation-state-backed cyberattacks between a broader set of countries.

For balance, there have been instances of political cooperation. For example, following the ransomware attack in July 2021 by the REvil group, the US President engaged in direct talks with the Russian president. It appears the Kaseya attack was the last straw for what had been a very productive year for this Russia-based organisation. Shortly after the talks, all servers operated by the REvil group went offline, and their activities appeared to have ceased.

7

The Cryptocurrency Industry Expected To Steal The Limelight

Criminal organisations are expected to continue to leverage the anonymity that cryptocurrency offers for extortion and money laundering activities. In almost all cases, ransom payments must use cryptocurrency to obfuscate the financial trail back to the perpetrator. The unregulated nature of cryptocurrency transactions and the low adoption rate of this technology made it easy for such payments to be converted to cash or other assets reasonably anonymously. However, they will need to evolve their tactics.

The investigative capabilities of law enforcement agencies have significantly become enhanced in recent years, providing the ability to track the movement of large cryptocurrency transactions. As a result, while the collection of payments remains straightforward, the criminals are finding it increasingly difficult to realise the financial value of the cryptocurrency without attracting unwanted attention. This challenge for attackers was seen with the recent Colonial Pipeline attack. The attack was traced to the DarkSide criminal group who are believed to be based in Russia. The attack generated significant publicity worldwide due to the extensive, if unintended, impact across the east coast of the USA. Shortly after the attack, the authorities in an unnamed country seized servers used by this group. Consequently, the US Department of Justice could trace and recover around 85% of the cryptocurrency used to pay the ransom.

One of the tools expected to be exploited more by cybercriminals is cryptocurrency mixing services. These services efficiently conceal the origin of funds by hiding transactions amid regular legitimate activity. A mixer takes cryptocurrency and deposits it into a central reserve. It then pays out cryptocurrency from this reserve, less a management fee, to a newly created account. By randomising the frequency and value of transactions, tracing the funds entering the reserve to funds leaving the reserve can be sufficiently complex to provide definitive proof. The laundered cryptocurrency can then be transferred to an exchange where it can be anonymously traded into a legal tender.

The other key trend in the use of cryptocurrencies is nation-states looking to bypass sanctions. **Using cryptocurrencies can disguise transactions that would otherwise be identified as breaking imposed sanctions.** This technique is noticeable in North Korea and Iran, where long-standing US-led sanctions are intended to disrupt military capability. Cryptocurrencies allow these countries to anonymously purchase equipment through third parties and disguise the actual end customer. As sanctions persist and agencies attempt to identify rogue cryptocurrency transactions, nation-states are expected to evolve to negate the effect of sanctions.

8 Privacy Concerns Around Augmented Reality Will Grow

Augmented reality is another technology that is expected to see exponential growth following the rebranding of Facebook and its focus on a metauniverse. Initial attention is on the social nature of virtual interactions, but broader regulatory and legal issues will need to be addressed early into the adoption lifecycle. The metauniverse is presented as a virtual world where digital goods and services can be traded using real-world funds. This use raises issues of contractual compliance and jurisdictions in the case of dispute, theft or other criminal activities that can be undertaken.

A potential privacy issue for the metauniverse is where the cross over between real-world identity and the virtual world blurs. The virtual world will contain vast quantities of users' personal data in a form that can be potentially stolen en masse by a capable attacker. The attack vectors are almost limitless, theft of virtual funds, using records of activities for blackmail or extortion, using virtual data for real-world identity theft.

Another potential issue is the ambition to merge real and virtual worlds through wearable augmented reality equipment that observes the actual world and overlays it with a virtual world. As a result, images captured in the real world can be transferred into a digital form that potentially breaches a host of laws, from personal privacy to copyright theft.

The expectation is that such legal concerns will follow rather than lead the technology, opening early technology adopters to significant risk before regulatory and legislative controls catch up. The different approaches to personal privacy around the world will no doubt complicate this evolution.

9 Resource Hijacking is Still Dangerous

Cryptocurrencies such as Bitcoin rely on computer resource intensive processing to create a currency that has a real-world value.

Overall, the cryptocurrency mining industry is worth around $1.6 billion, which is expected to double within the next five years.

Unfortunately, the process of creating currency uses significant quantities of electricity. For example, Bitcoin alone uses around 160 terawatt-hours per year, the equivalent of 2% of the USA's electricity consumption. The energy costs associated with the processing requirements are reaching the point where it is uneconomic in most countries to perform the required processing. This situation has spawned a new crime of resource hijacking where attackers seek to install malware onto as many computer systems as possible that silently performs the necessary processing without the system's owner being aware. This stealthy attack allows the attacker to collect the value of any coins created without incurring the electricity costs. As the value of coins increases, the prevalence of such attacks is expected to follow suit. For the infected system, the installed malware will consume any free processing time, increasing energy usage. Computers vulnerable to resource hijacking are also more likely to have other malware installed for more nefarious purposes using the same mechanism.

10 Ransomware Will Continue To Shape The Threat Landscape

Ransomware is now commonly used by criminal enterprises seeking to extort businesses for financial gain. Ransomware attacks at the start of 2021 were more than double those in 2020, which is **expected to increase**. Estimations are that attackers launch attacks worldwide every 11 seconds. The cost to global businesses of these attacks is estimated to reach $20 billion in 2021. This cost has grown more than fifty times the estimated cost impact seen in 2015. This staggering metric shows that ransomware is the fastest growing form of cybercrime, and the trend over the last three years shows the growth accelerating.

A key feature of ransomware is that it can be targeted at any business size, from the largest multinationals to individuals. As a result, every system is vulnerable and can be seen as a viable target for attack. Traditionally ransomware attacks were focused on large organisations where a high financial ransom could be extorted. However, the trend is for attackers to target large numbers of small, less well-protected businesses more likely to pay a modest ransom. These more minor victims are more willing to pay, and the attacks are less likely to attract the attention of law enforcement organisations.

Two key factors are at play. First, ransomware developers have created Ransomware-as-a-Service (RaaS). Less capable attackers can rent ransomware code along with instructions on how to perform attacks. RaaS offers the developers a substantial revenue stream with negligible risk to themselves. Instead, other attackers carry the risks and share any ransoms paid. The developers can then afford to invest their earnings into developing even better ransomware. Unfortunately, this means that more attacks are launched, and their sophistication is increasing.

The second factor is that ransomware attacks have evolved; they no longer just compromise data integrity and impact availability. The latest attack strategies include the exfiltration of data before encryption, followed by threats to compromise confidentiality by publishing or selling the stolen data. The ability to recover systems from backups is no longer sufficient to protect businesses from the impact of ransomware attacks. The focus must be shifted away from recovery to fast detection and effective response.

The **key takeaway** is that ransomware is becoming more common and more pervasive. The emergence of RaaS schemes enables any individual or group with criminal intent to launch an attack without a technical understanding of the attack mechanism. Anyone with basic computer skills and access to the internet access can launch an attack and take a share of any ransom paid. The groups providing the service make a lucrative income invested in improving the ransomware, increasing its capabilities and success rate. Businesses need to take action if they are to stay one step ahead.

Smarttech
YOUR 24/7 SECURITY PARTNER

Top 10 Practical Tips To Mitigate Cyber Risks

1 Manage the risk of Supply Chain Attacks by identifying and assessing your critical suppliers

You need to be able to triage the risk each supplier poses to your organisation to effectively mitigate that risk. We recommend to start by building a supply chain risk management framework, creating a risk register where you identify and document risks, then instituting governance and regular review and building strong defences to lower your risks.

2 Adopt A Zero Trust Methodology and Mindset

This means that you should implement defences based on the principle that your systems WILL be breached. When one starts from the premise that a breach is inevitable, it changes the decision matrix on next steps.

3 Cyber Security Awareness Training

All employees should be able to identify the signs of a cyber attack or a threat. Regular cyber security awareness training will ensure that your employees are always up-to-date with the latest phishing scams and malicious attempts to access your data or systems.

4 Limit access levels and permissions

The first step when it comes to protecting your data is to know exactly who has access to what. Review your access control policy, limit access based on a need-to-know basis and have a privileged access management strategy in place.

5 Visibility is key

Visibility of what hardware and software assets you have in your network and physical infrastructure will help you gain a greater understanding of your organisation's security posture. Whether you have IT and OT systems or just IT, gaining visibility is a crucial step in strengthening your defences.

Smarttech
YOUR 24/7 SECURITY PARTNER

Top 10 Practical Tips To Mitigate Cyber Risks

6

Updating and Patching

Make sure your devices have the latest security updates installed and an antivirus or anti-malware service. System patches also help avoid lost productivity.

7

Enable Multi-factor authentication

Most online services now provide a way to use your mobile device or other methods to protect your accounts in this way.

8

Make sure you have an up-to-date Incident Response Plan in place

Being prepared for an incident allows all stakeholders in the organisation to know what they need to do. Moreover, it is important to regularly test your incident response plan in order to simulate a real-life attack and document how your organisation is in a position to respond, should one occur.

9

Back- up your systems and data

Data loss is often as damaging, monetary and brand, to an organisation as a data breach. A copy of critical data in a secure offsite location is one small step that should not be overlooked.

10

Securing Containers from Potential Cyberthreats

Vulnerabilities in cloud-deployed containers are growing and gaining visibility into your container security using existing controls will be essential.

Smarttech
YOUR 24/7 SECURITY PARTNER

Conclusion

The growing digitisation of businesses encourages automation, integration, and interconnectivity. The result is that more companies, both large and small, rely on computerised systems to manage their day-to-day business activities along the supply chain. Unfortunately, this comes at a time when cyberattacks are growing in capability, persistence and frequency.

Data breaches remain a critical issue worldwide, and the risks have dramatically increased. Attacks are more sophisticated, able to evade traditional perimeter defences more easily. In addition, ransomware attacks now include data exfiltration for theft or blackmail purposes. Having an effective backup solution is no longer sufficient to allow a reactive ransomware recovery strategy. Now businesses need to look at proactive detection and response approach.

Smarttech
YOUR 24/7 SECURITY PARTNER

We keep you secure.

Smarttech247 is a multi-award-winning MDR (Managed Detection & Response) company and a market leader in Security Operations. Trusted by global organizations, our platform provides threat intelligence with managed detection and response to provide actionable insights, 24/7 threat detection, investigation, and response. Our service is geared towards proactive prevention and we do this by utilizing the latest in cloud, big data analytics and machine learning, along with our industry leading incident response team.

Our mission is simple: to keep our customers secure. That's why we have designed our platform to enhance the efficacy of your security infrastructure in order to optimize your protection, detection and remediation strategies. We are certified to ISO9001, ISO27001 and Cyber Essentials to provide assurance that our customers receive consistently high-quality services and that every aspect of their data and information security is protected. Our offices are located in Ireland, United Kingdom, Romania, Poland & in the US.

CONTACT US

www.smarttech247.com

info@smarttech247.com