CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

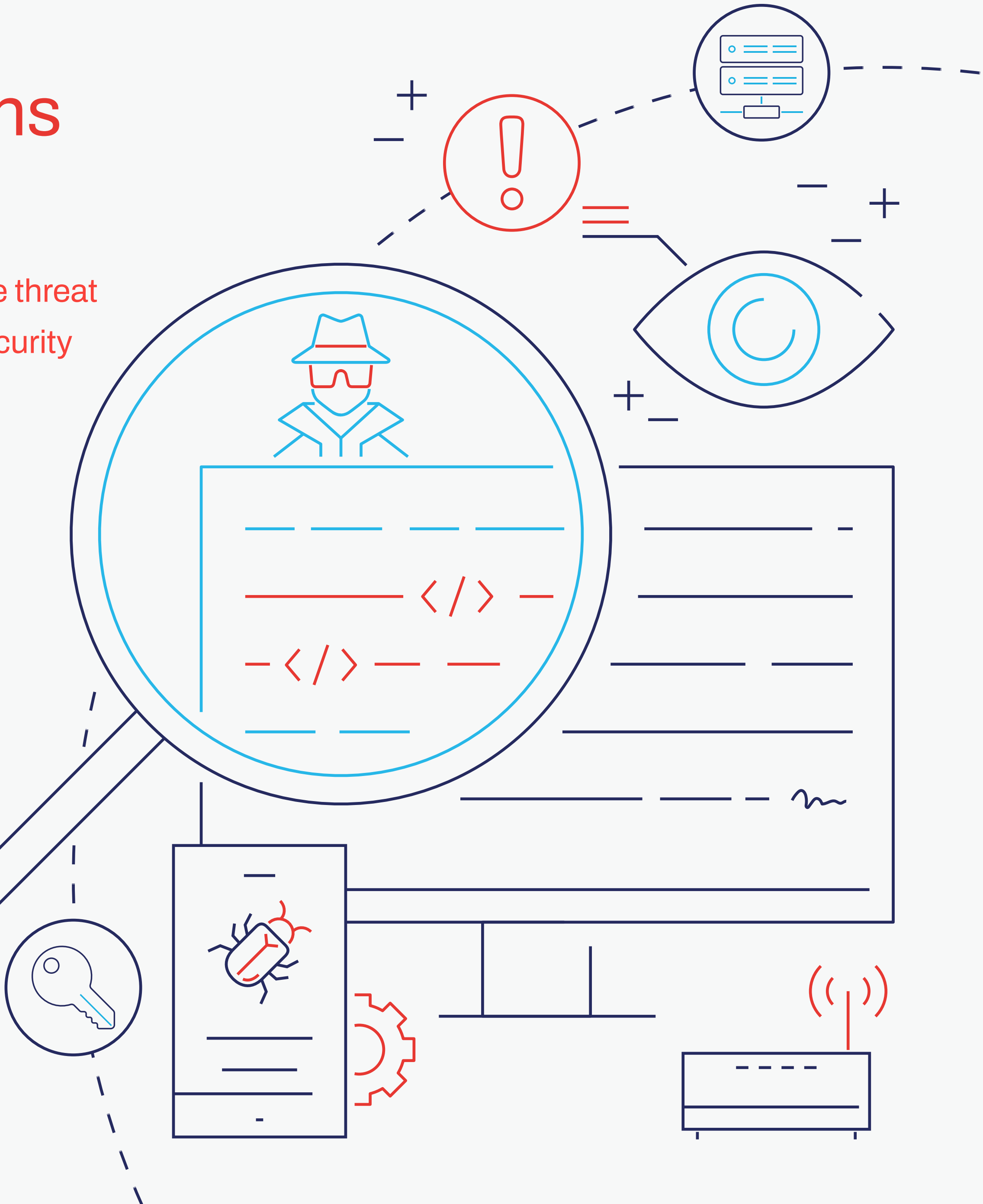
No 14 / January 2022

Recent Cyber Events:

Considerations for Military and National Security Decision Makers

Reflections on 2021:

→ The ransomware threat
→ Supply chain security
→ Spyware export controls



Published by CCDCOE

Reflections on 2021

2021 was an exciting year from a cybersecurity and cyber defence perspective. After dealing with the Solarwinds breach at the beginning of the year, the world experienced a series of serious ransomware incidents, in some cases causing disturbances to essential services. We also saw governments expressing their commitment to protecting critical services and to responding forcefully to nations carrying out malicious cyber operations or allowing criminals to do so. While impossible to cover all these developments in a brief report, we will take this opportunity to reflect on three important topics: ransomware, software supply chain security and spyware. Perhaps looking at these from a little distance will help us see the larger picture and allow us to prepare better for the future.

The ransomware threat

Malicious cyber activity has grown substantially over the past two years while the world has been learning how to keep turning with the omnipresent pandemic. One particular malware category, ransomware, made headlines frequently in 2021, partly because the operations were increasingly targeting high-value targets.

One of the first major ransomware incidents in 2021 may have been against the automakers Kia and Hyundai, although this has been denied by the alleged victims. The actors behind the compromise appear to have used the now common double extortion tactics, not only causing an outage but also threatening to expose data exfiltrated from the victims' systems.

In March, CNA Financial, the seventh-largest commercial insurer in the US, fell victim to ransomware. Shortly thereafter in April, the North American division of Brenntag, a German chemical distributor, faced a ransomware infection of their systems as well.

One of the most public ransomware incidents of this year was against Colonial Pipeline in May, an incident that was discussed in a previous issue of this series. The largest fuel pipeline was shut down as a result of a ransomware attack. This led to fuel shortages across the US East Coast and an increase in fuel prices. In the same month JBS, one of the largest meat suppliers in the US, suffered a compromise which caused it to temporarily shut down five of its plants and this also affected operations in the UK and Australia.

In July, Kaseya, an international IT service provider, announced it had fallen victim to ransomware which affected and shut down numerous companies in several countries. For example, Sweden's third largest grocery chain had to close down 800 stores for several days, some of them in remote areas with very few to no alternatives.

Over the past two years, hospitals have also seen an increase in malicious cyber operations, though not limited to ransomware. One of the most prominent victims was Ireland's health service which resulted in stolen patient data, the cancellation of appointments and delayed treatment. Other known incidents targeted health companies in the US and New Zealand.

These attacks not only show how closely linked our society and systems have become, but also how vulnerable and highly dependent on the functioning of national critical infrastructure (CI) our societies now are. According to the Department of Homeland Security (DHS), 16 CI sectors are considered to be of vital importance for the population of the US. Similar examples of sectorial divisions of CI can be found in almost any country; for example, 12 have been identified in France and 13 in the UK. The incidents mentioned above have all affected one or more of those sectors. Due to the close interconnection of systems and services, all sectors are potential targets and a compromise of one can have a domino effect on others with severe consequences. It is therefore of the utmost importance that nations define and strengthen their CI sectors and put in place contingencies to deal with any compromise.

Resilience need not only be built by having more robust or redundant digital systems. In many instances, we need to be prepared to operate without industrial control systems, or even to compensate for services affected by a cyberattack by other means, such as using local electrical generators to compensate for a power outage or to ship oil by sea or rail if pipelines are not operational.

Most of the companies targeted in the examples ended up paying ransom up to as high as $40 Million, even though the FBI and others advise against paying a ransom as it is no guarantee of getting data back and it incentivises criminals.

Discussions of public response to cyber threats have entered the military and political level as never before, with many states beginning to take steps both towards increasing the cyber security of CI on a national level through regulations or imposing costs on those responsible for malicious cyber operations. This is intended to constitute deterrence both by denial of benefits and by the threat of retaliation. The US government, for example, has taken a more active stance and combined resources from Cyber Command, NSA and other agencies and from international partners to lift responsibility to an all-of-government effort, including law enforcement. Public declarations will need to be followed by clear action such as the reported capture of 12 suspects for involvement in ransomware operations by Europol in November 2021. This type of layered approach to deterrence is critical to any kind of success and we can only hope that this will continue in the new year and that the results of such an approach will soon grow.

Supply chain security

The concerns and confusion over the security of the software supply chain triggered by the Solarwinds incident in December 2020 expanded in 2021. A number of investigations, analyses and follow-up measures related to the incident have been made but the effects were still being felt in May, six months after it first became public, when the US CISA released detailed guidance on how to evict Solarwinds-related malicious code, recommending blocking internet access for three to five days.

'Organizations can no longer protect themselves by simply securing their own infrastructures since their electronic perimeter is no longer meaningful; threat actors intentionally target the suppliers of more cyber-mature organizations to take advantage of the weakest link.' (NIST)

July 2021 was the peak period of concern over supply chain security as the ransomware group REvil distributed ransomware through the update file of Kaseya's endpoint management product, VSA. As a result of this supply chain ransomware attack, hundreds of companies suffered severe damage as their systems were encrypted and became unusable.

The Kaseya incident was not the only malicious cyber operation during the year which leveraged the supply chain. In January, the update server of BigNox, a Hong Kong-based software company used for distributing the Android emulator NoxPlayer for Windows and Mac, was compromised and malicious code was distributed through it. In April, the update server of German smartphone manufacture Gigaset was compromised, and malicious updates containing a trojan were distributed to its Android smartphones.

Reusing packages and libraries uploaded on the open source repositories is a common practice in the software industry to achieve rapid and efficient development of software. According to a survey on open source security, 98% of the over 1,500 commercial applications and services audited contained open source code, and 84% had publicly known vulnerabilities. The open source packages may contain malicious code intentionally injected by malicious actors and vulnerabilities simply due to developer mistakes. Six packages with hidden crypto-mining malware were uploaded to the Python Repository PyPI in April, and a malicious package with a hidden password stealer was found in the JavaScript repository npm[1] in July. Similar cases in which vulnerable or malicious packages were found in open source repositories have also been found.

By exploiting the vulnerabilities of the repository server itself, attackers may tamper with existing uploaded packages or upload new malicious packages circumventing authentication and authorisation requirements. In November, a vulnerability in registering the npm package without user authentication was found on the source code hosting site GitHub.

A new attack technique exploiting open source packages was also unveiled in 2021. In February, a security expert disclosed proof of concept, saying that a new attack technique named 'Dependency Confusion' could infringe on the systems of 35 companies, including Apple and Microsoft. The expert manipulated the software to execute malicious packages uploaded to the public repository instead of internal private packages by publishing malicious packages with the same name as the genuine ones. A few days after the announcement, hundreds of malicious npm packages copying the proof of concept were found to attack various companies, including Amazon and Slack.

Another severe attack that occurred this year was the abuse of Microsoft's code signing. Rootkits named NetFilter and FiveSys found in June and October, respectively, were signed by Microsoft. Attackers tricked Microsoft into signing the malicious drivers by submitting them for certification for the Windows Hardware Compatibility Program (WHCP) to make them look authentic. These rootkits were distributed only in the Chinese game sector, but it shows that signature by a major supplier alone is not always sufficient to ensure security.

Other types of supply chain compromises include exploiting software development tools. In January, a malicious code that steals credentials and sensitive information was injected into the uploader script of a DevOps platform company, Codecov. The uploader was used for its customers to upload their test reports. Several customers including security company Rapid7 and a Japanese e-commerce company Mercari had part of their source code exposed.

Meanwhile, a set of vulnerabilities in the Apache logging service Log4j was discovered in December. While the vulnerabilities themselves were not part of a supply chain attack, as many companies had difficulty in identifying which of their applications and products were using Log4j services[2], serious concerns have been raised from the perspective of supply chain security. The importance of clearly documenting specifications and dependencies when using third-party software and services has once again been shown by Log4j vulnerabilities as has how widespread the effects of a vulnerability in a single popular open source software package can be.

To secure the supply chain, developers must first take responsibility and carry out security activities related to the

[1] npm (Node package manager) is a service managing packages for the JavaScript programming language, making it easier for developers to share source code. https://www.npmjs.com/

[2] Robert Huber, Apache Log4j Flaw Puts Third-Party Software in the Spotlight, Tenable Blog, 12 December 2021

software development and delivery environment on their own. These activities include thorough security tests for the software being developed, segregation of the development network from the internet, secure configuration management, secure handling of code signing certificates and hardening software distribution platforms.

If a portion of the software development is inevitably outsourced, measures to prevent source code leakage should be established and extensive checks should be made against potential vulnerabilities and malicious codes.

Procuring organisations should be able to check detailed specifications at the individual component level and perform record keeping for software to be newly procured or updated. They should also actively consider requiring vendors to undergo third-party security certification for their software, such as Common Criteria. They may also require vendors to obtain security certification such as ISO 27001 for the security of development and delivery environments and contractually impose additional security requirements if necessary.

In the US, enhancing software supply chain security became mandatory for critical software to be used by federal agencies under Executive Order 14028 issued on 12 May. Its key aspects include an explicit definition of critical software; establishment of guidelines on secure software development framework that vendors should follow; identification of security measures that critical software and its platform need to have; revision of guidelines on supply chain risk management practices for vendors and customers; establishment of minimum standards for vendor verification of software; and an obligation to construct a Software Bill of Materials (SBOM) for every product, a formal record containing the details and supply chain relationships of various components used in building the software.

Spyware export controls

Over the last year, off-the-shelf spyware has made its way onto the communication devices of journalists, political leaders activists and it has also been a topic in the news. Even though the pace at which it has evolved on the desks of regulators has been slower, both the EU and US are tightening export controls to kerb the misuse and propagation of spyware. The revelations and developments of 2021 once again show that spyware is a concern for cybersecurity as much as it is for privacy.

NSO Group, an Israeli private company specialising in cybersecurity technologies, has allegedly been selling licences of a cyber-surveillance technology dubbed Pegasus since as early as 2013. The first wave of Pegasus revelations came already in 2018 when Citizen Lab and partners identified that between 2016 and 2018, there were at least 36 likely Pegasus clients operating in 45 countries.

In June 2021 a related investigative journalism initiative – Project Pegasus – obtained access to over 50,000 phone records of 'persons of interest' that had been subject to surveillance through Pegasus. The subsequent range of reported targets has grown to include the French President Emmanuel Macron, members of Catholic clergy, Princess Haya of Jordan, and civil rights activists from Palestine, India and Hungary. Despite the manufacturer's initial claims about inbuilt restrictions relating to US and Israeli phone numbers, the software has also been shown to have been used to spy on US government officials and diplomats.

The Israeli Ministry of Defence responded by blocking spyware exports to 65 countries with questionable human rights records. It also specified the conditions for dual-use exports so that the seller has to confirm that their cyber-surveillance tools are to be used solely for curbing terrorism or serious crime and not for the persecution of minorities or suffocating public criticism. Although the new requirements offer some guidance as to what can be viewed as serious crime or terrorism, the seller's decisions still ultimately rely on the accuracy and objectivity of the information provided by the buying state.

Israel is far from being the only spyware exporter – Russia's Positive Technologies, Germany's FinFisher and Italy's HackingTeam have been operating in the same niche as NSO. As new EU export controls came into force on 9 September 2021, advocacy organisations and members of the European Parliament alike have raised the need to apply them to the exports of Pegasus. According to reports, Pegasus exports were also mediated through Cyprus and Bulgaria which are both bound by EU rules. While the recent recast Dual-Use Regulation establishes a framework for cyber-surveillance exports that is somewhat more in line with confidentiality and integrity, in its current state it does not allow for a quick consolidated response in the form of an export ban.

An EU export ban can only be agreed on after lengthy consolidation procedures. This is further complicated by Member States' often diverging interpretations of which technologies are in whole or in part intended to be used for 'internal repression' or 'serious violations' of international human rights or humanitarian law. Given recent evidence, Pegasus is not leaving much room for interpretation. The US responded with a measure of immediate but only marginally deterrent effect. NSO and three other companies were added to a list of entities whose access to certain goods produced in the US, including software, will be restricted.

'The United States is committed to aggressively using export controls to hold companies accountable that develop, traffic, or use technologies to conduct malicious activities that threaten the cybersecurity of members of civil society, dissidents, government officials, and organizations here and abroad.' (Gina Raimondo, US Secretary of Commerce)

International export control instruments differ in their specifications, emphasis and underlying values. For instance, the Wassenaar Arrangement, which has the US, UK, India, Japan and all EU Member States except Cyprus among its signatories, focuses on military uses of various capabilities. Spyware, however, is more often than not used in a non-military context and therefore calls for a more holistic review.

The recent recast EU Regulation introduces 'cyber-surveillance items' as a separate category and takes into consideration peacetime human rights concerns. However, the domestic frameworks and practices have in time aligned with a Wassenaar-like approach and the procedural obstacles mentioned above make it unlikely that the recast Regulation will take practical dimensions any time soon. Therefore, the keys to any substantial developments are in the hands of national decision-makers. Alternatively, spyware's detrimental impact on product security and privacy has led private actors such as Apple and WhatsApp to sue NSO Group for unauthorised access and intentional damage to their systems.

Pegasus illustrates the two-fold effect of cross-border government hacking. States want to protect their citizens from becoming the targets of foreign cyber-surveillance, but they seek to promote their own military or dual-use technology industry and their security interests abroad. Therefore, it is both a challenge and an opportunity for national authorities to reflect on which technologies they want to spread and what they can do about it. Although it has lurked in the background for almost a decade, commercial spyware became one of the key issues of 2021 in terms of transparency, awareness and voicing the need for change. Hopefully, the near future will see it transform into concrete positive action.

CONTRIBUTORS

Sungbaek Cho
Amy Ertran
Lisa Schauss
Ann Väljataga
Jan Wünsche

PREVIOUS ISSUES

This paper is part of a series of monthly reports. This issue and all previous issues are available in the CCDCOE online library.

FEEDBACK

To continuously improve this regular report, input from readers is essential. CCDCOE encourages feedback on both how the reports are of use to you and how you think they can be made better.

Please send your comments and suggestions to feedback@ccdcoe.org

ABOUT THIS PAPER

This recurring report is the collaborative view of NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) researchers highlighting the potential effects of current events and developments in cyberspace on armed forces, national security and critical infrastructure, based on publicly available information. It does not set out to be exhaustive. While the authors have made every effort to describe events from a perspective relevant to NATO and partner nations, there may be national and regional differences which this paper does not address.

The authors of this paper are independent researchers at the NATO CCDCOE; they do not represent NATO, nor does this paper reflect NATO's position. The aim of the paper is not to replace information about vulnerabilities and incidents provided by CSIRTs and providers of CIS products and services