CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

No 12 / September 2021

Recent Cyber Events:

Considerations for Military and National Security Decision Makers

The Global Threat:

- → Kaseya: A global ransomware attack
- → The Pegasus spyware controversy
- → Cyberattack against South African ports
- → North Korean hacks against South Korea
- → Reactions to the compromise of Microsoft Exchange

Published by CCDCOE

Kaseya: A global ransomware attack

On 2 July Coop, one of the major supermarket chains in Sweden was forced to close hundreds of stores due to malfunctioning cash registers. It quickly became clear that it was not an operational issue, but the result of a cyberattack and that hundreds, maybe thousands, of businesses all over the world were affected. The common factor turned out to be that they all used managed IT service providers that employed the VSA IT management software from Kaseya.

Subsequent investigations point at a zero-day vulnerability in VSA being used to stage the attack against the service providers. This amounts to a supply chain attack since the ultimate victims were attacked through their suppliers of services. In this way, the attack is reminiscent of operation Cloud Hopper. Both the devastating effects of hitting a large number of victims through one service provider and the power of finding vulnerabilities in software that is widely used are noteworthy.

The ransomware wave and its effect on essential services, as reported in the previous issue of this series, does not seem to be waning. This attack has been called the biggest yet by some observers, and its impact was global. Like many of the recent attacks of this kind, its origin seems to be a Russian criminal gang. Many are also continuing to call for the Russian government to take action against these organisations. Like the privateers enrolled in maritime warfare of old, these criminals are seen as being allowed to attack foreign targets and keep the spoils.

'I made it very clear to [President Putin] that the United States expects when a ransomware operation is coming from his soil, even though it's not sponsored by the state, we expect them to act if we give them enough information to act on who that is.' (President Biden)

The ransom demands were addressed at all levels; against Kaseya, the service providers and the businesses finally hit. A master key to unlock all the affected computers was supposedly offered for $70 million. Kaseya has denied paying the ransom, but some affected businesses may have chosen to pay. A master key seems to have surfaced, but it is unclear if the ransom was paid by someone else, or if perhaps this has been obtained through state-level negotiations or even an intervention by the Russian authorities.

A pattern also seems to be emerging where the groups responsible closedown or go into hiding after a major attack. It is not unlikely that they are just reorganising under another name; there are examples of other groups doing this and also releasing decryption tools as the old 'business' is closed.

The ransomware threat and its effect on critical infrastructure and services will continue to be one of the major global cyber threats. Since the protection of the targeted IT systems is mostly out of their control, it is difficult for affected organisations to take effective measures against the threat. The level of protection in many cases is still far too low with, for example, old unpatched software deployed, and the attacks are still highly profitable. To address the issues a whole of society approach, as well as international cooperation, is needed, both raising the level of cyber security overall and working to deny the attackers any benefits.

The Pegasus spyware controversy

A joint investigative journalism initiative[1] called the 'Pegasus Project' has revealed the extent to which controversial spyware technologies are being used to digitally surveil targets across the globe, including human rights campaigners and journalists. The Project used information originally leaked to human rights campaign organisation Amnesty International and media non-profit Forbidden Stories which included over 50,000 phone records of 'persons of interest' that had been selected for surveillance through *Pegasus*, a spyware solution sold by NSO Group, an Israeli private company specialising in cybersecurity technologies.

The project revealed potential targets that included politicians and world leaders (with French President Emmanuel Macron's phone number part of the leaked records), journalists, and human rights defenders, with the evidence contributing to fears that the spyware is being used by repressive regimes as a means to track and enable further negative actions against any potential opposition.

'NSO Group's targeted digital surveillance tool is inherently prone to human rights violations, given its design and the lack of checks in place to ensure its proper deployment. States have wilfully used Pegasus to unlawfully target individuals, completely violating their right to privacy.' (Amnesty International, Pegasus Project Press Release)

NSO's spyware, Pegasus, enables the remote surveillance of smartphone devices. The spyware is installed on a device either by tricking the target individual into clicking on a link that then prompts the download by email or via a messaging application, or by exploiting vulnerabilities in common applications. Once installed, the spyware

1 The Project involved Amnesty International, Forbidden Stories, and 17 media partners

is theoretically capable of harvesting data from SMS messages, emails, social media messaging logs photos and video files, as well as the calendar, contacts book and GPS locator tool. The spyware is capable of recording calls and activating the device's camera and microphone, and passing all this information back to those behind the installation (NSO Group on behalf of its clients). The first wave of Pegasus revelations came in 2018 when Citizen Lab and partners identified 36 likely Pegasus customers in 45 countries between 2016 and 2018.

Forensic analysis by Amnesty International's Security Lab of 67 smartphones revealed successful infections in over half the devices through a vulnerability in iPhone devices observed as recently as July 2021 and affecting devices up to a fully patched iPhone 12 running iOS 14.6. Apple has subsequently been the subject of criticism for not publicly collaborating with the security community to prevent similar exploitation of its software.

The publicity around the scale and nature of targeted individuals has raised significant understandable concern in terms of privacy and human rights violations as the investigative project revealed potential Pegasus clients including Azerbaijan, Bahrain, Hungary, India, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia, Togo and the United Arab Emirates (UAE). Surveillance technology like Pegasus falls under defence export control, with exports restricted and subject to licensing by the Israeli Ministry of Defense.

NSO Group has pushed back strongly against the allegations, denying the investigations' findings and comparing the international disapproval as similar to 'criticising a car manufacturer when a drunk driver crashes', arguing that it is clients who are responsible for how the spyware capabilities are used – and against whom. NSO's 2021 Transparency Report argues Pegasus spyware is used by states to 'collect data from the mobile devices of specific suspected major criminals', contradicting the Project's forensic evidence. It also stated that in-built restraints rendered Pegasus incapable of targeting phone numbers starting with Israeli or US prefixes. Unfortunately, there are no publicly available comprehensive statistics as to the technology´s actual efficacy in curbing crime or terrorism.

At the end of July, the Israeli government commenced an investigation into the Project's allegations and the adequacy of the current export controls framework.

'It is highly dangerous and irresponsible to allow the surveillance technology and trade sector to operate as a human rights-free zone,'… 'Such practices violate the rights to freedom of expression, privacy and liberty, possibly endanger the lives of hundreds of individuals, imperil media freedom, and undermine democracy, peace, security and international cooperation.'(Statement: UN human rights experts)

In international human rights law, states have obligations to take appropriate measures to protect against human rights abuses from third parties[2]. A group of UN experts have requested a memorandum on spyware technology, citing the requirement for corporate bodies to perform human rights due diligence as part of the UN Guiding Principles on Business and Human Rights.

Cyberattack against South African ports

On 22 July reports emerged that the South African state-owned enterprise Transnet was experiencing problems with its IT networks. Transnet manages South Africa's rail, port and pipeline infrastructure transporting minerals and other commodities for export.

The disruption primarily affected container terminals forcing Transnet to halt operations at container terminals in Durban, Ngqura, Port Elizabeth and Cape Town.

A few days after the incident, Transnet acknowledged that it had suffered a cyberattack forcing it to declare force majeure at container terminals and switch to manual processing of cargo. On 28 July, South Africa's Department of Public Enterprises announced that Transnet had restored full operations at all its ports following the cyberattack.

The 2017 NotPetya malware attack targeting Ukraine's critical infrastructure ended up infecting the IT systems of Maersk thereby affecting the functioning of 76 Maersk port terminals worldwide.

The Transnet incident was the first time the operational integrity of South Africa's critical maritime infrastructure suffered a severe disruption of its cargo movement due to a cyberattack, but it may be a sign of what lies ahead for ports worldwide.

As maritime ports seek to increase efficiency and effectiveness through digitalisation, the number of similar incidents is likely to increase. The crippling effects of an attack may make paying a ransom an attractive option for operators, harbour facilities and other transport infrastructure, thereby making them lucrative targets for cyber criminals. Cyber security is gradually being recognised as an important dimension of maritime security but the integration into maritime security frameworks and instruments cannot be overestimated and should be accelerated to protect critical information infrastructure. The CCDCOE has covered the importance of ports and other infrastructure for military mobility, and their vulnerability to cyberattacks, in a food-for thought-paper.

2 UN Human Rights Committee (HRC), General Comment 31 [80]: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, UN Doc. CCPR/C/21/Rev.1/Add. 13, para. 8

The port in Durban is the busiest shipping terminal in sub-Saharan Africa, handling approximately 60% of South Africa's container traffic. The attack against Transnet will therefore certainly have caused long-lasting damage to South Africa's economy at a time where it is struggling to recover from the effects of the COVID-19 pandemic. The actual severity of the incident is hard to estimate, leaving experts to speculate about its nature, scope and consequences.

Bloomberg has reported that the hackers left a ransom note on computers belonging to Transnet SOC Ltd. The location and identity of the Transnet hackers are currently unclear but, according to Adam Meyers, vice president of intelligence at the cybersecurity firm CrowdStrike, they are likely from Eastern Europe or Russia where many ransomware groups are based. The ransom note was similar to others seen in recent months, linked to ransomware strains known variously as 'Death Kitty,' 'Hello Kitty' and 'Five Hands' exploiting security vulnerabilities in SonicWall products.

North Korea hacked South Korea's Nuclear Institute and Aerospace Company

In May and June, suspected North Korean hackers infiltrated South Korea's nuclear research institute, the Korea Atomic Energy Research Institute (KAERI) and defence company Korea Aerospace Industries (KAI) respectively and stole data stored in internal networks. KAERI is a government-run institute with original technologies for nuclear power plants and nuclear fuel, and KAI is South Korea's largest defence company manufacturing fighter jets, utility helicopters, unmanned aerial vehicles, space launch vehicles and satellites.

Although no official investigation results about the extent of damage or the attribution of attackers have yet been announced, the National Intelligence Service (NIS) of Korea, an agency responsible for national security including cybersecurity, reported to the National Assembly's Intelligence Committee on 8 July that North Korean state hackers were believed to have hacked these organisations and that most-sensitive information was not affected. Regarding the KAERI incident, the US Department of State's spokesperson commented that North Korea poses a significant cyber threat and the international community should work together to mitigate the threat.

'It's vital for the international community, for network defenders, and the public to stay vigilant and to work together to mitigate the cyber threat posed by North Korea' (US State Department Press Briefing on 8 July)

The initial attack vector of these incidents was a vulnerability in a Virtual Private Network (VPN) product made by a Korean IT security company. In April, the NIS identified the vulnerability and distributed security advisories to all organisations using it. However, mitigation actions were not followed by these organisations, resulting in hacking incidents.

VPNs build a virtual network on the internet, like a leased line, and were considered an essential security solution as working-from-home exploded due to COVID-19 and, for this reason, cyberattacks targeting VPNs have continued to occur. In 'Top Routinely Exploited Vulnerabilities' announced by the US Cybersecurity and Infrastructure Security Agency (CISA) on 28 July, VPNs such Pulse Secure's and Fortinet's products were included in the list of the top 5 most exploited products in the first half of this year along with Microsoft's Exchange, Excellion's File Transfer Appliance, and VMware's vSphere.

VPNs are widely used not only for telecommuting but also for the maintenance of various critical IT systems including industrial control systems. IT administrators of each organisation should always monitor security news for their VPN products and apply vulnerability patches promptly. In addition, multi-factor authentication should be implemented in preparation for possible leaks of VPN user credentials, and application-specific access control should be applied rather than allowing authorised users access to all IT resources inside the perimeter of the organisation. Implementation of zero-trust security solutions that are capable of contextual awareness based on access ID, access time and security status of access device should also be considered.

Reactions to (China's) compromise of Microsoft Exchange

On 2 March Microsoft announced that it had detected multiple zero-day exploits being used to attack on-premises versions of Microsoft Exchange Server in limited and targeted attacks. In the attacks observed, the threat actor used these vulnerabilities to access on-premises Exchange servers which enabled access to email accounts and allowed the installation of additional malware to facilitate long-term access to victim environments.

Media reported that tens of thousands of servers were hit, even mentioning 250,000. While a lot of the victims were small companies and businesses, the servers of bigger originations were also attacked including the European Banking Authority and the Norwegian Parliament.

The Microsoft Threat Intelligence Center (MSTIC) attributed this campaign with high confidence to HAFNIUM, a group assessed to be state-sponsored and operating out of China, based on observed victimology, tactics and procedures.

On 19 July, NATO released a statement in which it condemned such malicious cyber activities which are designed to destabilise and harm Euro-Atlantic security and disrupt the daily lives of our citizens. Acknowledging statements made by Allies such as Canada, the United Kingdom, and the United States attributing the attack to the People's Republic of China, NATO calls all states, including China, to uphold their international commitments and obligations and to act responsibly in the international system, including in cyberspace.

In a press release on 19 July the High Representative, on behalf of the European Union, urged Chinese authorities to take action against malicious cyber activities undertaken from its territory. In this statement, it referred to other hacker groups like Advanced Persistent Threat 40 and Advanced Persistent Threat 31 operating from China.

In its Summit Communiqué issued by the heads of state and government participating in the meeting of the North Atlantic Council in Brussels on 14 June, the Allies 'recognise that the impact of significant malicious cumulative cyber activities might, in certain circumstances, be considered as amounting to an armed attack'. They are committed to acting on such cyber activities 'in accordance with international law, including the UN Charter, international humanitarian law, and international human rights law as applicable'.

The Microsoft Exchange hack once again highlighted the risk of zero-day exploits and the need for constant vigilance and awareness. As with all malicious cyber activities, attribution is important and often necessary to be able to respond. Attribution is difficult and even in the best of times it may, as Microsoft stated for the Exchange compromise, be attributed only with 'a high confidence' rather than with certainty. President Biden has warned, that a significant cyberattack may result in the United States ending up in a 'real shooting war' with a 'major power', highlighting the potentially serious consequences of getting attribution wrong.

CONTRIBUTORS

Henrik Beckvard
Sungbaek Cho
Amy Ertan
Ben Valk
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.