CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Recent Cyber Events and Possible Implications for Armed Forces

#1 – April 2020

About this paper

This paper is the collaborative view of NATO CCDCOE researchers highlighting the potential effects on the military of current events and of developments in cyberspace during the previous month, based on publically available information, but 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.

1. COVID-19 changes the cyber landscape

NATO CyOC: 'A global challenge exists with COVID-19 impacting a number of areas. Cyberspace is no different. Where most seek solutions to mitigate or resolve the crisis, others see opportunity. Cyberspace actors are quick to spread malware and launch attacks, attempting to capitalise on the public's need for information during the coronavirus outbreak.'

European External Action Service (EEAS): 'The coronavirus is a relentless and daily topic in pro-Kremlin media, including state-owned outlets. As of 19 March, the East StratCom Task Force has collected over 110 corona-related disinformation cases in the public EUvsDisinfo database since 22 January 2020. These messages are characteristic of the Kremlin's well-established strategy of using disinformation to amplify divisions, sow distrust and chaos, and exacerbate crisis situations and issues of public concern'.

Foreign Policy Research Institute: 'It is not surprising […] that the Kremlin, even if it has not explicitly commissioned a disinformation campaign, sees value in having its news and information outlets push narratives that seek to accelerate discord and disunity among NATO members. Depending on the course of the pandemic, we could very easily see a new Russian information campaign. Such a campaign would target publics in southern and western Europe and would question the value of an alliance which was ineffective in its response to the virus but which demands that they be prepared to risk conflict with Russia—while also sowing more doubts in both NATO and non-NATO neighbors about how much faith they are willing to place in alliance guarantees.'

The Hacker News: 'The direct impact of the Coronavirus is a comprehensive quarantine policy that compels multiple organizations to allow their workforce to work from home to maintain business continuity. This inevitably entails shifting a significant portion of the workload to be carried out remotely, introducing an exploitable opportunity for attackers.'

Impact

Increased remote working

One of the most noticeable effects of the spread of COVID-19 is the dramatic increase in remote working. An unprecedented number of people are working from home and holding meetings via teleconferencing solutions such as Zoom, Skype or Teams.

The quick switch to this mode of working has created new vulnerabilities and risks and malicious actors have not been slow in identifying this and attempting to capitalise on

it.[1] In the rush to get services accessible remotely, it may be tempting to cut corners on implementing adequate security measures. Best practice dictates that such services should be available only through a secure VPN-connection, but implementing such a solution, if it was not already in place, may be a challenge for many organisations. Poorly protected home networks will also pose a risk for the military networks, especially if a VPN is not used.

Teleconferencing is another challenge. Commercial cloud-based solutions are often used, which means that trust is put in a service provider that may or may not have been adequately vetted. If the software to be used is not already present on work devices, it will also be tempting for the staff to use their personal devices. Such devices will, typically, be less secure than devices owned and managed by the employer.

For the military, the need for many employees to access classified information will be a challenge. Most VPN and other solutions in place lack the level of encryption and other safeguards required for handling classified information. The number of devices available for working with classified information is limited. Even if devices are available, deploying them will also require the right level of physical security and the necessary procedures for managing encryption keys, etc. Lacking this, work will have to continue physically at ordinary sites, or without access to classified information, which could negatively affect operations.

To mitigate this, a balance between security and making tools for remote working available must be struck. At least two principles can be recommended:

1. Protecting internal networks by exposing only necessary services and making sure they are encrypted and authenticated, if possible using VPN and two-factor authentication; and
2. Not handling sensitive information in un-trusted online services or on employees' personal devices.

CERTs and cyber security authorities have issued guidelines for remote working, including the UK National Cyber Security Centre (NCSC) and the EU Agency for Cyber Security (ENISA).

COVID-19 themed attacks and scams

Threat actors are using the current COVID-19 pandemic as bait for their campaigns. It is to be expected that whenever a situation or phenomenon becomes a hot topic in the news and among the public, some will try to trick the public into doing or believing the wrong things.

In terms of preferred methods, email is probably the most popular entry point, either using malicious attachments to try to get malware onto the intended victim's computer or phishing for log-in credentials with links to fake websites. A popular tactic this time is to use apps or websites with data on the spread of the pandemic. Using these untrusted sources will pose a great risk of the target computer becoming infected or encrypted for ransom, or having its data stolen. In one example, a website was claiming to give away free vaccine kits, asking for payment of a small shipping charge and then stealing the buyer's credit card information.[2]

Mobile devices are also a target in the COVID-19 themed attacks using malicious apps that can work as spyware or ransomware.[3] The malicious apps may also be used for surveillance including the use of the microphone and the geographical location of the device. This will have an impact on the security of remote working using devices without central management and adequate security measures, and potentially affect the ability of the military to work with sensitive information remotely.

There are some signs that organisations that are critical during the pandemic are being targeted in these attacks. Even though some of the criminals behind common ransomware have claimed not to target hospitals during the crisis,[4] the healthcare sector seem to continue to be a target of such attacks.[5] There are also reports of advanced attacks targeting the World Health Organization (WHO).[6] WHO is

[1] Bank Info Security: 9 Cybersecurity Takeaways as COVID-19 Outbreak Grows
[2] ThreatPost: Fake Coronavirus 'Vaccine' Website Busted in DoJ Takedown
[3] Bank Info Security: COVID-19-Themed Malware Goes Mobile
[4] BleepingComputer: Ransomware Gangs to Stop Attacking Health Orgs During Pandemic
[5] Help Net Security: Healthcare cybersecurity in the time of coronavirus
[6] Forbes: 'Elite Hackers' Thought Behind Cyber Attack On World Health Organization

regarded as a vital hub for factual reports, advice and response coordination during the COVID-19 pandemic. Information provided by WHO has a direct effect on military readiness. Their advice influences exercises, troop movements and the daily routines of military personnel. Nations make strategic decisions such as travel restrictions based on their research and guidance.

In general, the choice of COVID-19 as a theme is probably more common in opportunistic criminal attacks without a single specific target. Users in any setting, even military, need to be vigilant and be wary of suspicious emails or websites. Well protected mail servers are an essential part of protection against phishing and other malicious email and using security technologies such as SPF, DKIM and DMARC[7] will make it more difficult to convincingly use fake senders in emails and thus will make it easier for users to spot the malicious ones.

Disinformation about COVID-19

Disinformation about the pandemic is feeding panic and mistrust in the handling of the situation. This undermines the credibility of information from the authorities, makes it more difficult to disseminate with accurate information and may cause people to make the wrong decisions on how to act during the pandemic.

The narratives in the disinformation campaigns include claims that the virus is a biological weapon created in NATO laboratories, [8] something that clearly could affect the public's trust in the military of NATO nations.

Cyber means are used to spread this disinformation fast and to amplify whatever available information will serve the purpose of the malicious actor. Disinformation regarding the response to COVID-19 can hurt a government's legitimacy in the eyes of its people and damage the trust need between Allies. These political realities, in turn, weigh on cooperation between the nations' militaries.

Social media platforms such as Twitter and Instagram are trying to limit the flow of false information, [9] but this is not enough. Employees need to be given regular and dependable information through whatever trusted channels are available and reminded to exercise good judgment, not to spread unconfirmed information and to consult official sources. Appropriate cyber security measures also have to be in place to protect official websites and email servers.

In the current situation when there is an increase in disinformation and at the same time an increased need to protect networks and information systems, the resources of the military may need to be strengthened by the use of reserves, voluntary defence organisations or other temporary resources.

2. Leaks of sensitive information potentially facilitating cyberattacks

ZDNet: 'A hacker has published this week a massive list of Telnet credentials for more than 515,000 servers, home routers, and IoT (Internet of Things) 'smart' devices. The list, which was published on a popular hacking forum, includes each device's IP address, along with a username and password for the Telnet service, a remote access protocol that can be used to control devices over the internet. According to experts to whom ZDNet spoke this week, and a statement from the leaker himself, the list was compiled by scanning the entire internet for devices that were exposing their Telnet port. The hacker then tried using (1) factory-set default usernames and passwords, or (2) custom, but easy-to-guess password combinations.'

Impact

Although the threat is not new, a publicly leaked list of vulnerable servers and devices is a goldmine for any malevolent actor looking to disrupt the operations of a target. For a military organisation with such devices exposed to the internet, it could mean that it will now be easier for less sophisticated

[7] Sender Policy Framework (SPF), Domain Keys Identified Message (DKIM) and Domain-based Message Authentication, Reporting & Conformance (DMARC), are email authentication techniques and protocols that can improve protection against fraudulent email.

[8] EU vs Disinfo: The Virus to Liberate us from Freedom

[9] Reuters: Instagram to remove coronavirus related content from recommendations

malicious actors to find and attack these devices. Depending on the type of device, the disruption could be the defacing of websites, denial of service for email and other services and, in the case of IoT-devices, even physical effects such as changes in temperature or ventilation in buildings.

The potential vulnerabilities deserve extra attention. Default passwords should not be used, and devices are should not be reachable directly from the internet unless it is absolutely necessary. Other cyber security measures such as keeping devices updated with the latest security patches are of critical importance.

3. Critical Windows vulnerability disclosed by the NSA

Wired: 'In a shift toward transparency, the [US] National Security Agency announced a bug that could have left over 900 million PCs vulnerable to attack. Microsoft released a patch for Windows 10 and Server 2016 today after the National Security Agency found and disclosed a serious vulnerability. It's a rare but not unprecedented tip-off, one that underscores the flaw's severity—and maybe hints at new priorities for the NSA.'

Schneier on Security: '[NSA's Cybersecurity Directorate head Anne Neuberger] said that this is not the first time the NSA sent Microsoft a vulnerability to fix, but it was the first time it has publicly taken credit for the discovery. The reason is that the NSA is trying to rebuild trust with the security community, and this disclosure is a result of its new initiative to share findings more quickly and more often.'

Significance

If organisations like the NSA share vulnerability information with a wide audience, it is good for information security in general, including for the military. Similar organisations in other nations also have programmes for doing this regularly. The fact that the NSA is doing it so publicly this time may help to build trust with the wider security community and thus improve the all-important civil-military cooperation in the field.

4. Contractors can put sensitive information at risk

Security Affairs: 'UK printing company Doxzoo exposed hundreds of gigabytes of information, including documents related to the US and British military. Security experts at vpnMentor discovered 343GB worth of files belonging to the printing company Doxzoo that were exposed on an AWS server. […] Exposed records included names, addresses, email addresses, payment method, last four digits of the payment method, passport scans, order details, copyrighted publications (e.g. books, screenplays, TV show scripts), teacher's guides with answers for tests, certifications, diplomas and degrees, medical documents, floor plans, musical compositions, religious texts, internal military documents (including classified information).'

Impact

Information is only as secure as the least secure place where it is stored. If the leaked documents contained classified information, it suggests that a service that could not securely handle such information was trusted to print it. This is not the same situation as using a cloud service for your data processing needs. The large cloud service providers have the capacity to put appropriate security controls in place, often to a higher standard than a small organisation may be capable of in-house, but usually not to the standards needed for classified material. A company that provides a completely different service, such as printing or travel services, may have considerably lower capabilities when it comes to information security. The company will also be one more place where the information is held (in addition to having it in-house) and thus one more place where it can be attacked. In some cases, subcontractors are also used, meaning even greater exposure. An advanced malicious actor will always look for the softest target possible to get at the information.

Before information is entrusted to another party, the proper controls have to be in place so that the information can be protected. The whole information chain and all actors that will have access to sensitive information should be considered. Frameworks like the Cybersecurity Maturity Model Certification (CMMC) can provide tools to ensure that contractors have the capabilities needed to

protect sensitive data. Consider handling the most sensitive data only in-house.

5. Ransomware attacks increasingly targeted

ET CIO.com: 'Global cybersecurity firm Trend Micro on Wednesday [26 February 2020] said it recorded a 10 per cent increase in ransomware detections in 2019 compared to 2018. The healthcare sector remained the most targeted industry, with more than 700 providers affected in 2019, the company said in its 2019 security roundup report. 'A likely contributor to this trend was the willingness of many organisations to pay ransom so as to speed up the recovery of their data and systems. This inclination might have even been bolstered by their insurance coverage for ransomware attacks,' said the report.'

BleepingComputer: 'BSI, Germany's federal cybersecurity agency, recommends local governments and municipal institutions not to pay the ransoms asked by attackers after they get affected by ransomware attacks.'

Bank Info Security: 'Ransomware-wielding attackers - aided by a service economy that gives them access to more advanced attack tools - are increasingly targeting organisations rather than individuals to shake them down for bigger ransom payoffs, says McAfee's John Fokker. The allure of businesses is clear: Attackers can demand more money, earning a bigger potential haul from any given attack, aided by a service economy designed to help them more easily turn a criminal profit via increasingly advanced attack tools, he says.'

Significance

Ransomware is a threat that can cripple any sort of business or organisation by making computers unusable and information unavailable, including the military. Mission-critical systems connected to the internet continue to be common in all sorts of organisations. If not protected, they can become the target of highly sophisticated ransomware attacks. A successful attack will affect operations for hours or days, even if proper backups are available and can be restored. Avoiding becoming the target of such attacks should, therefore, be a priority.

Ransomware is clearly still good business for criminals and we can expect that sectors where there is a willingness to pay ransoms will continue to be hit by these attacks. Even though the threat may also affect sectors where ransoms are seldom paid, making a point of not giving in to ransom demands may keep the more targeted attacks away. The advice from BSI, the German Federal Office for Information Security, joining several other government sources, is that ransoms should not be paid. This is also good advice for the military.

The UK National Cyber Security Centre (NCSC) has published new guidelines which, while mostly a reorganisation of old advice, provides a useful reminder on how to mitigate the ransomware threat. One area that has been updated is the advice on keeping offline backups that are not at risk of being encrypted by an attack. If the threat from targeted attacks can be reduced by a policy of not paying ransoms, the guidelines will probably be effective in mitigating at least the less sophisticated non-targeted threats that will likely remain.

6. The Cyberspace Solarium Commission presents its report

Cyberspace Solarium Commission: 'The Cyberspace Solarium Commission (CSC) was established in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 to 'develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences.' The finished report was presented to the public on March 11, 2020. The Cyberspace Solarium Commission proposes a strategy of layered cyber deterrence. Our report consists of over 80 recommendations to implement the strategy.'

Significance

The recommendations in the Cyberspace Solarium report may be of interest for anyone devising a cyber defence strategy. The recommendations seek to build deterrence through a layered approach. The strategies – for example of denying an adversary benefit from cyberattacks by building resilience – can be used in strategies on national as well as organisational level.

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