CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

No 9 / March 2021

Recent Cyber Events:

Considerations for Military and National Security Decision Makers

Internet Blackout in Crises

Other topics in this issue:

- → Operation LadyBird: Takedown of a Major Botnet
- → Water Treatment Plant in Florida Hacked
- → Campaign Against Security Researchers
- → New “Tools” Against State-Sponsored Hackers
- → New EU Cybersecurity Strategy

Published by CCDCOE

ABOUT THIS PAPER

This recurring report is the collaborative view of NATO 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.

---

1. Blackout: Limiting internet access in crises

'A near-total internet shutdown is in effect in Myanmar as of 1 a.m. local time Monday 15 February 2021. Real-time network data show national connectivity at just 14% of ordinary levels, in the third registered state-ordered information blackout brought implemented since the military coup.' (NetBlocks)

According to multiple sources, Myanmar's internet access was severely limited during the recently reported coup. Business Insider reports that some areas of the country were completely cut off, while others had limited access. In addition to the loss of network connectivity, there were reports of telephone and television signal inaccessibility. The NGO NetBlocks followed events in Myanmar and reported that during the night, access to the network gradually went down from 70% to 50%, affecting both state and commercially operated networks. According to the report, remote parts of the country and critical infrastructures were less affected. Users also reported that Facebook services including Instagram and WhatsApp were disrupted on the state-owned operator's network on 3 February.

Over the past year, an increasing number of internet or social media blackouts during national crises, riots and protests have been reported. Recent Cyber Events last year reported on the internet blackout during the Belarus protests and the US company Sandvine reportedly selling network equipment to Belarusian authorities. Yet the practice of preventing or restricting access to the internet during national unrest is nothing new. Almost exactly 10 years before the incident in Myanmar, the internet was blocked in Egypt following protests in which social media were said to have played a major role. However, media and watchdog organisations do not always seem to be clear about who is responsible for the blackouts or what is causing them, as was the case in Belarus or Egypt. Apart from the blackout in Myanmar, there have been at least two further blackouts associated with riots, elections and protests in 2021. During the presidential elections in Uganda, social media, messaging services and the Google Play Store were reportedly unavailable, and in Russia, partial network disruptions were detected in the two largest Russian cities (Moscow and St. Petersburg) during protests over the arrest of Alexei Navalny.

The Arab Spring events suggest that cyberspace and especially social media can be catalysts during unrest and protests. Accordingly, reports such as those in the New York Times which reveal that the storming of the US Capitol was planned on social media come as no surprise. Platforms such as Gap and Parler are said to have been used by insurgents after more prominent platforms such as Facebook and Twitter acted against groups of QAnon and Proudboys supporters. The decision to cause a blackout to deprive users of the means to organise may therefore seem like an efficient and simple cyber method for an authoritarian regime. Looking at the example of the protests in Hong Kong, according to The Guardian, China's so-called Great Firewall is also coming to Hong Kong; a security law will allow the police to censor online speech and network operators will be forced to shut down platforms.

Taking down internet infrastructure, state TV, radio and phone lines is a common military tactic and is expected to hamper the other side's command and control capability. However, it will affect both sides in a conflict as communication networks are required to facilitate decision-making and command and control. Interference with internet infrastructure may also have effects beyond the military targets which must be considered for the action to be lawful and proportionate. The internet is a fundamental enabler for the essential functions of the state and society, the continuity of critical infrastructure, and fundamental rights.

Blackouts of the internet in the interconnected world of today could make the command and control of military operations more difficult; as it is not uncommon to use mobile internet connections as one part of the communications solution. At the same time, it allows military forces to become less visible. For example, military units and their movement can be tracked through social media through accidental exposure because of weak security culture or because of pre-planned open-source intelligence collection activities by the adversaries, or even through things like surveillance cameras connected to the internet.

Information, as a joint function, supports military commanders in decision-making and leading forces. From a military operations planning perspective, it is reasonable for military planners to consider how communications and internet blackouts will affect operations and how to be prepared to operate in such conditions.

2. Operation LadyBird: Takedown of a major botnet

'Law enforcement and judicial authorities worldwide have this week disrupted one of most significant botnets of the past decade: EMOTET. Investigators have now taken control of its infrastructure in an international coordinated action. This operation is the result of a collaborative effort between authorities in the Netherlands, Germany, the United States, the United Kingdom, France, Lithuania, Canada and Ukraine, with international activity coordinated by Europol and Eurojust.' (Europol press release)

After a coordinated effort on the part of law enforcement, the operation of the notorious and often dubbed most dangerous botnet in the world – EMOTET – has been disrupted. According to Naked Security, the group behind EMOTET used infected documents or links in emails with current news topics to trick users into opening the file. Once opened, a warning would pop up prompting the user to enable a Microsoft Word macro which in turn would launch a PowerShell command to install EMOTET on the machine. After installation, EMOTET enabled the theft of information and the insertion of trojans and ransomware. EMOTET is one of the most long-lasting cyber threats, emerging as a banking Trojan in 2014 and showing strong resilience due to its polymorphic nature. According to EUROPOL, a database with usernames, passwords and e-mail addresses was discovered by the Dutch National police and it is possible for individuals to check if an e-mail address was compromised. CSIRTs were also provided with this information.

After this successful intervention, the question now is to what extent and whether the botnet can recover. In February last year, Recent Cyber Events reported on the Trickbot botnet, which had been successfully disrupted several times by US Cyber Command. However, the botnet seems to be back after a coordinated takedown by Microsoft in October last year. ZDnet reports that there is now another campaign that prompts users through phishing emails to

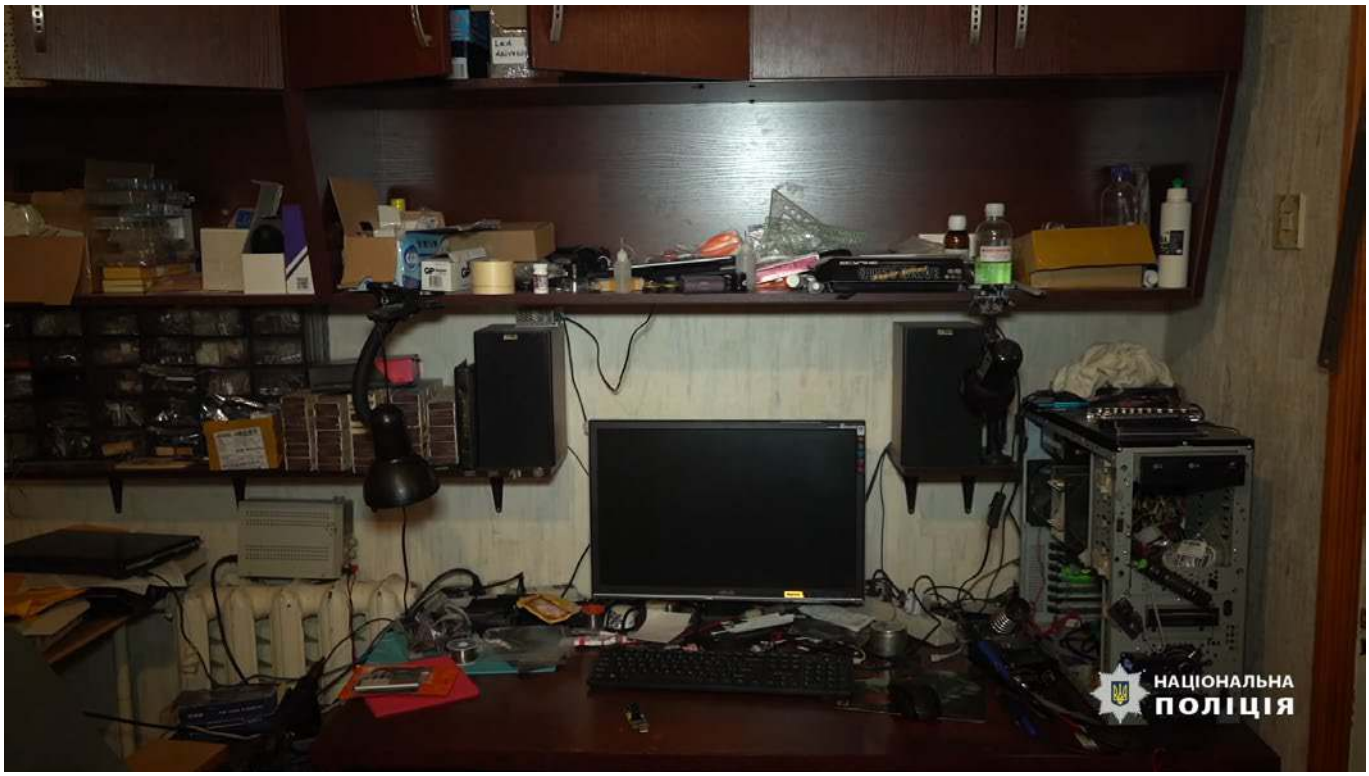

Image of the facilities raided by the police. Source: National Police of Ukraine (Національна поліція України) Youtube Channel (published 27 January 2021)

click on a link that starts the download of a zip archive containing a malicious JavaScript file. The email claims that the recipient was involved in a traffic violation and the link is supposed to be evidence.

While the criminal organisation behind EMOTET does not currently have access to the botnet, there is still a possibility that others do. It is believed that access to EMOTET-infected computers has been sold to third parties in the past. However, ZDnet reports that 25 April is supposed to mark the absolute end for EMOTET, as the Dutch police plan to shut down the botnet once and for all. There are supposed to be two primary command and control servers on Dutch territory and the police plan to install an update on them which will uninstall EMOTET from the terminals.

A takeaway from Trickbot is that malware is re-designable. In line with a basic military cyber tenet, an enemy can re-use already developed code. While there is a possibility that the botnet activities will be diminished, it is unclear if this will be permanent due to the relative ease of restarting activity. C4ISR.NET published an opinion about the Solorigate breach where it is argued that the concept of deterrence in cyberspace has failed.

An interesting aspect of the disruption of the EMOTET botnet is that the operation affected hijacked computers all over the world. It shows what cyber operations in peacetime can look like with coordinated efficient forceful law enforcement operations as opposed to relying on military or intelligence agencies.

3. Water treatment plant in Florida hacked

The control system of a water treatment plant in Oldsmar, Florida was breached and the attackers attempted to increase the concentration of sodium hydroxide in the water to potentially dangerous levels.

'The guy was sitting there monitoring the computer as he's supposed to and all of a sudden he sees a window pop up that the computer has been accessed. The next thing you know someone is dragging the mouse and clicking around and opening programs and manipulating the system.' (Sheriff Bob Gualtieri)

Monitoring and safeguards in the plant ensured that the attempt was thwarted before the concentration could reach a dangerous level, and the population was never in danger.

The incident is reminiscent of similar attempts against water treatment plants in Israel in April 2020, believed by many to be linked to Iran. Was this a state-sponsored operation, or could a less well-funded actor be behind the attack? It is difficult to assess the security of this particular plant without more detailed information, but according to cybersecurity media and the alert from the US-CERT, desktop sharing software could have been used to gain access. This and the suggestion of weak or even shared passwords and the use of an outdated operating system indicate a less-than-ideal security posture, something we know is all too common with industrial control systems. Security at that level could allow almost anyone to make a similar attack including disgruntled former employees or hobby hackers wanting to test their skills in the real world. Remote access tools such as desktop sharing software are often misused in scams and hostile account takeovers, which have risen by 20% from 2019 to 2020.

Larger critical infrastructure operations where the effects of a breach will be on a larger scale will usually have better security in place, but the vulnerabilities in smaller plants like the one in Oldsmar may still have devastating effects, even on a national scale. If a large number of smaller plants, usually the ones closest to the consumer of the utilities, are targeted, the combined effect may mean that a large portion of the population will be without water or any other utility as the remaining plants struggle to keep up with demand. Many organisations, including the armed forces, which have their own operational technology (OT) well-protected from cyber threats are still often dependent on smaller public or private utility companies that may still be using older poorly-protected systems vulnerable to simple attacks.

A whole-of-society approach needs to be taken to protect what collectively is critical infrastructure. The smaller players need to work together and be given support from government and society to reach a higher level of cyber maturity. Armed forces and other customers that may suffer serious consequences from an outage need to consider and select the right cybersecurity requirements for their suppliers, even when contracting non-cyber services. They also need to work with the suppliers to help them live up to these requirements. Finally, it is important to build resilience for situations where an outage would still occur because no matter how well you design your security requirements, it will never be possible to make an operation 100% secure.

4. Social engineering campaign against security researchers

'Hackers masquerade as security researchers to befriend analysts and eventually infect fully patched systems at multiple firms with a malicious backdoor.' (ThreatPost)

Social engineering is one of the oldest methods of influencing and manipulating people. In a general sense, it is the 'management of human beings in accordance

with their place and function in society[1]. In the information environment, social engineering is defined as 'the use of fraud to manipulate individuals in the disclosure of confidential or personal information that may be used for fraudulent purposes[2].

Social engineering uses various techniques and tactics to influence, mislead and deceive targets. Hence, fraud can be purely digital or Social engineering uses various techniques and tactics to influence, mislead and deceive targets. Hence, fraud can be purely digital or analogue, or a combination of offline and online actions taken to deceive or compromise individuals, groups or organisations.[3] Some of the most common forms of digital social engineering are phishing, spear-phishing, mass phishing, vising (phone calls), fake news, market manipulation, political sabotage, scareware and baiting.

Social engineering methods are becoming extremely elaborate and sophisticated. In recent months, Google's Threat Analysis Group (TAG) and the Microsoft Threat Intelligence Center (MSTIC) have detected a sophisticated cyber incident and attributed it to ZINC, a purportedly DPRK-affiliated and state-sponsored group. The APT group affiliated with North Korea-linked Lazarus Group has been targeting security researchers with an elaborate social engineering method that attempts to establish trusted relationships with them. Microsoft spotted ZINC's activities on Twitter in mid-2020 when ZINC began building its reputation, carefully constructing fake online personas to build trust in the research community. Adam Weidemann (TAG) found that ZINC's activities were not only on Twitter, but also on LinkedIn, Telegram, Discord, Keybase and email. Once the research community was built, the second phase began. According to Microsoft, ZINC retweeted high-quality security content and published exploitation research on a blog they controlled. For malicious activities, reports state that ZINC was possibly exploiting zero-day vulnerabilities of the Chrome browser and malicious Visual Studio code via email.

Thus, it was once again proven that social networks may also have negative consequences for their users, even when the users are experienced security professionals. Walter Weiss points out that social engineering works mainly because of a lack of user knowledge and because it is difficult for users to verify every communication they receive. The fact is, many users have access to a lot of privileged information, which creates a large area of attack for the organisation. Therefore, the success of socio-technical attacks depends on the level of sophistication of individuals, organisations or the general population, and their technical solutions.

Foreign intelligence services and criminals are very active in the information environment. They can steal confidential documents, create a database of experts and military personnel and target vital sectors including critical infrastructure and defence. Everyone needs to be aware that negligence or inattention on their part may threaten not only themselves but also the organisation they work in, or even national security. Therefore, we all need to be vigilant and aware of our vulnerabilities and responsibilities in the information environment and ask ourselves a few simple questions: Do I need this social media account? Do I know this person? Did I check this person or organisation before confirming it? Did I set a spam filter? Is my computer up to date?

Awareness of information and cybersecurity is not only individual, but should also exist on an organisational and national level to protect employees and the population. Both the organisation and the state must take organisational and technical measures to prevent malicious activities. Organisational measures include specific security policies and measures such as audit of privileged accounts, effective awareness programmes, education and training programmes and the implementation of exercises. At the same time, more budget-intensive measures may need to be taken, such as the use of tools facilitating automatic intrusion detection and technical prevention and mitigation solutions.

5. New 'tools' from NIST for protecting against state-sponsored hackers

The National Institute of Standards and Technology (NIST) has released a new publication giving guidance on how to defend against state-sponsored hackers. The new guidance, SP 800-172, is not a stand-alone document but complements earlier NIST publications, in particular SP 800-171, and contains frequent references to other guidance.

The new document provides tools intended to counter threats posed by state-sponsored actors, an aspect that was not within the scope of other publications. Although the document is said to have been inspired by an incident in 2018 that compromised sensitive information, several recent incidents, not least the SolarWinds supply chain compromise, have made it clear that state actors are very active in the cyber domain, and that one may be targeted without realising it.

1 Merriam Webster: definition of social engineering.

2 The Oxford/Lexico: definition: of social engineering.

3 Vircom: What are the most common social engineering techniques? Social engineering is not hacking, downloading the code on non-secure websites (Ibid.). Social engineering uses psychological manipulation to gain the victim's trust and to trick them into making security mistakes or giving away sensitive information (Imperva: Social Engineering).

'Because you may not 'feel' the direct effects of the next hack yet, you may think it is coming someday down the road; but in reality, it's happening right now.' (Ron Ross, Computer scientist and a NIST fellow)

The guidance is intended to provide a set of enhanced security requirements for US non-federal systems processing sensitive but unclassified information that may be the target of state-sponsored cyberattacks and can be used when contracting such services. We believe, however, that it can be of use to a larger audience looking for cyber safeguards for other systems facing similar threats.

The guidance in SP 800-172 includes security requirements covering people, process and technology, showing that security cannot be achieved by technological defences alone. The recommendations include elements such as awareness training, configuration management and network segmentation. Another interesting recommendation is to employ techniques to confuse and mislead adversaries.

The new publication is just one of the many useful resources published by NIST and by other standards bodies and cybersecurity organisations. They may not be immediately applicable to every situation or tailored to your specific needs, but in most cases, they are a useful starting point and can be adapted to many different contexts. Broad documents on processes and generic technical solutions work well in most situations since the basic security issues facing us are seldom domain-specific. This means that developing policies and guidelines for an organisation does not have to start with a blank piece of paper. It also suggests that there is great value in international cooperation in developing standards and guidance.

6. New EU Cybersecurity Strategy and legislation

Late last year, the EU published its new Cybersecurity Strategy for the Digital Decade. Visibly the most ambitious and compre¬hen-sive of the four EU cyber strategies since 2009, it sets out 26 strategic initiatives across four areas: European resilience and technological sovereignty; cyber operational capacity across the EU; advancing a global and open cyberspace; and cybersecurity baselines of EU institutions.

Given Europeans' extensive reliance in all core functions of society on interconnected digital infrastructure, it is unsurprising that a major step in the updated approach is the revision of the NIS Directive; the new draft directive was published with the strategy and is currently in the Council negotiations phase. The same goes for the proposed network of Security Operations Centres across the EU, which may be viewed as an organic evolution of the member states' strategic and operational cooperation networks set up under the NIS Directive. However, the strategy also outlines several new initiatives, including €4.5 billion worth of investments in the EU's supply chain autonomy.

Efforts to strengthen cyber operational capacities across the EU will involve a new pan-EU operational incident response platform (Joint Cyber Unit) to ensure preparedness, provide shared situational awareness and reinforce coordinated response. Across law enforcement, diplomacy and defence, a list of initiatives is suggested to address a broad spectrum of threat actors.

Concerning cyber defence and military cyber capabilities, in particular, the strategy sheds light on the plans to update the EU's 2018 Cyber Defence Policy Framework (CDPF) and adopt an EU Military Vision and Strategy on Cyberspace as a Domain of Operations in support of Common Security and Defence Policy (CSDP) missions and operations. Stimuli are offered for member states' cyber defence capability development, notably through PESCO and the European Defence Fund, and the EDA plans to set up a military CERT network among EU member states to promote interaction and information exchange.

Above its predecessors, the new strategy expresses the EU's commitment to efforts that advance a global, open, stable and secure cyberspace – it commits to promoting broad support to international law and cyber norms, and plans increases in engagement in international standardisation processes.

CONTRIBUTORS

Kadri Kaska
Damjan Štrucl
Urmet Tomp
Jan Wünsche
Philippe Zotz

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