Hybrid CoE Paper 11

FEBRUARY 2022

Cyber threat actors: how to build resilience to counter them

MERLE MAIGRE

Hybrid CoE

Hybrid CoE Paper 11

Cyber threat actors: how to build resilience to counter them

MERLE MAIGRE

Hybrid CoE Papers are finalized pieces of analysis on a topic related to hybrid threats, based on one or several research questions. They may be either conceptual analyses or based on a concrete case study with empirical data.

The European Centre of Excellence for Countering Hybrid Threats tel. +358 400 253800 www.hybridcoe.fi

ISBN (web) 978-952-7472-16-3
ISBN (print) 978-952-7472-17-0
ISSN 2670-2053

February 2022

Hybrid CoE is an international hub for practitioners and experts, building Participating States' and institutions' capabilities and enhancing EU-NATO cooperation in countering hybrid threats, located in Helsinki, Finland.

The responsibility for the views expressed ultimately rests with the authors.

Contents

Introduction

Malicious cyber activity has increased substantially over the past two years, while the world has been learning how to keep turning amid the omnipresent pandemic. States, non-state actors and criminal groups compete and are increasingly weaponizing information to gain advantage, infiltrating other countries' networks to steal data, seed misinformation or disrupt critical infrastructure. The proliferation of cyber tools increasingly blurs the line between various threat actors.

This Hybrid CoE Paper first describes the way in which coronavirus has amplified cyber threats. It proceeds with a closer examination of different incentives for cyberattacks, and concludes by suggesting response measures that could be taken by NATO and the EU, as well as by national governments in building cyber resilience. The framework of cyber threat actors looks at two general categories – state and non-state actors, both of whom are engaged in theft, subversion or sabotage. An important differentiator in these categories is their motivation – financial gain, espionage, political interference or harmful attacks against critical infrastructure.

The impact of coronavirus on the cyber threat landscape

The coronavirus pandemic has further complicated the cyber threat landscape. In March 2020, Covid-19 led to social distancing measures and travel restrictions. The global effort to slow down infection rates caused a rapid shift to remote working. In a short space of time, IT security professionals had to respond to the challenges introduced by working from home arrangements, such as enterprise data movements whenever employees use their home internet to access cloud-based apps, corporate software, videoconferencing, and file sharing.[1] Even though hardware and software solutions may have been in place to secure the organization's data, there were often no established policies to help employees through the jungle of threats and vulnerabilities they would face when moving their workplace out of the traditional office environment.[2]

With a lack of appropriate guidelines, training and cybersecurity awareness, adapting to such a 'digital by default' normal is difficult, and remote workers may inadvertently act in ways that expose the business to cyber threats. Frequently reported examples of these kinds of mistakes include connecting work devices to public Wi-Fi networks, sharing corporate devices with family members without authorization, connecting work devices to personal equipment without permission, using personal devices to access work applications, and downloading unauthorized applications contrary to organizational policies. All such habits increase the risk of data exposure.

1 ENISA, The Year in Review. ENISA Threat Landscape from January 2019 to April 2020, https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-the-year-in-review/view. [Unless otherwise indicated, all links were last accessed on 7 February 2022.]
2 NATO CCDCOE, Recent Cyber Events: Considerations for Military and National Security Decision Makers, No 10 / May 2021, https://ccdcoe.org/uploads/2021/05/Recent-Cyber-Events-10_May-2021.pdf.

Financially motivated cybercrime

Within the spectrum of incentives for the infliction of cyber harm, financially motivated cyberattacks account for a substantial proportion. This refers to cyberattacks designed to gain access to credit card data, health records, or other corporate and personal data that can be monetized. Financially motivated cyber criminals participate in the black market, which is a playground for organized groups.[3]

According to the FireEye Mandiant *Special Report: M-Trends 2021*, the top five most targeted industries in 2020 were business and professional services, retail and hospitality, financial, healthcare, and high technology. The main methods used included extortion, ransom demands, payment card theft, and illicit transfers. Direct financial gain was the likely motive for 36% of intrusions, and an additional 2% of intrusions were likely perpetrated to resell access. In 2021, data theft remained an important mission objective for threat actors – in 32% of intrusions, adversaries stole data. [4]

Likewise, the *ENISA Threat Landscape* study covering the period 2019–2020 outlined that the number of incidents resulting in the theft of information, data and user credentials was the highest ever observed.[5] All across Europe, more than 620 million account details were stolen from sixteen hacked websites and offered for sale in the popular dark-web marketplace, Dream Market.[6]

Currently, the most significant threat comes in the form of highly organized, technically proficient criminal syndicates. These pose a threat not only to states, but also to businesses of all sizes, and even to individual citizens. These groups try to steal data or extort money through **ransomware**, which is one of the most potent threats that we face.

The Estonian Information System Authority 2021 annual review explains the logic of ransomware as follows: "Classical ransomware attacks occur in three stages. First, an attacker installs ransomware on a victim's computer or server. Remote desktop protocol is increasingly used for this; however, a lot of malware is still sent via files and links added to e-mails. Second, the ransomware encrypts some of the files on the computer or server, or the entire hard drive. After that, the victim can no longer open their files. Third, the attacker demands a ransom for file recovery, i.e. for a decryption key, usually in some cryptocurrency, such as Bitcoin."[7]

Ransomware has become a popular weapon in the hands of malicious actors. Interplay often occurs between financially motivated cybercriminals and state-based hackers. Cybercriminal gangs are learning from the better-resourced state-based organizations. Likewise, the state-based groups are borrowing from the criminal gangs – launching their disruptive attacks under the guise of ransomware with no indication as to whether victims will in fact get their files back in exchange for a ransom.

Ransomware attacks are becoming sophisticated not just in technical terms, but also in the sense that the criminals themselves appear to be studying potential victims. This intelligence-gathering involves actively researching an organization's turnover and profitability to estimate how much they can afford to pay. Ransomware criminals go

[3] Zachary K. Goldman, Damon McCoy, 'Deterring Financially Motivated Cybercrime', *Journal of National Security Law & Policy*, Vol 8:595, 2017, https://jnslp.com/wp-content/uploads/2017/10/Deterring-Financially-Motivated-Cybercrime_2.pdf.
[4] Fireeye Mandiant Services, Special Report, *M-Trends 2021*, pp. 17-19.
[5] ENISA, Main incidents in the EU and worldwide. Threat Landscape from January 2019 to April 2020, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents.
[6] Ibid.
[7] Republic of Estonia Information System Authority, Cyber Security in Estonia 2021, https://www.ria.ee/sites/default/files/content-editors/kuberturve/kuberturvalisuse_aastaraamat_2021_eng_final.pdf.

around in circles trying doors and if the owner has been careless, the damage is quickly inflicted. In some cases, ransomware criminals boldly incentivize insiders by offering them 40% of the anticipated ransom if they help to install ransomware on a company computer or Windows server.[8]

Throughout the coronavirus pandemic, a growing number of hospitals in Europe and the US have found themselves locked out of life-critical systems by ransomware attacks. Since early 2021, the trend of criminal groups using ransomware for economic gain has been spreading like wildfire at the global level. In May 2021, the entire Irish health service was crippled for weeks. In October 2020, a cyberattack occurred against the Vastaamo Psychotherapy Centre in Finland, where sensitive information related to tens of thousands of patients was compromised.

Understanding the evolving tactics being employed by ransomware attackers is critical to mitigating this problem. One of the most significant developments in ransomware since 2020 has been threats against target organizations to leak their stolen data and publish it on a public internet site if the organization in question refuses to pay.[9] This additional fear factor could be effective if the data is sensitive. In the words of Mikko Hypponen, researcher at F-Secure, "The Vastaamo case is an example of an attacker who is motivated by money and attempting to monetize personal data by blackmailing not only healthcare institutions, but by directly contacting patients themselves."[10]

In fact, Finnish cyber security company F-Secure predicted that this would become a trend, and most ransomware cases throughout 2021 proved the point, marking the evolution into what has been called 'ransomware 2.0'.[11] Unlike corporate data that is usually stored for a relatively short period, health data always needs to remain accessible, secure and private. With limited budgets and legacy systems, this poses a massive challenge for the health sector.

[8] Ravie Lakshmanan, 'Cybercrime Group Asking Insiders for Help in Planting Ransomware', The Hacker News, 20 August, 2021, https://thehackernews.com/2021/08/cybercrime-group-asking-insiders-for.html?m=1.
[9] F-Secure, 'Attack Landscape Update', 2020, https://blog-assets.f-secure.com/wp-content/uploads/2021/03/30120359/attack-landscape-update-h1-2021.pdf.
[10] Ibid.
[11] Ibid.

Espionage

But cybersecurity is not just about money. Another set of threats comes in the form of belligerent states that seek to steal sensitive data for espionage purposes. One of the most classic recent cyber espionage cases was the SolarWinds incident in December 2020, whereby the Russian intelligence services infiltrated the digital systems run by American tech firm SolarWinds and inserted malware into the code. During the company’s next regular software update, it inadvertently spread the virus to about 18,000 of its clients, including large corporations, the Pentagon, the State Department, Homeland Security, the Treasury and other US government agencies. The hack went undetected for months, until the victims started discovering that enormous amounts of their data had been stolen. [12]

SolarWinds is characterized as a supply chain attack that targets the process by which a trusted organization updates software for their clients. According to the US National Institute of Standards and Technology (NIST) glossary, supply chain attacks are: “Attacks that allow the adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, information technology products or services at any point during the life cycle.”[13] A report by the Atlantic Council further explains: “A software supply chain attack occurs when an attacker accesses and modifies software in the complex software development supply chain to compromise a target farther down on the chain by inserting their own malicious code.”[14]

In this way, the effect of an attack on a single organization can be multiplied by the number of clients that the organization serves. Understanding how the supply chain may be compromised is important for organizations procuring or maintaining software so that they can assess the security measures taken across the supply chain. It is also of interest to anyone developing or customizing software in-house. Any intermediary handling the software package, such as a reseller or systems integrator or even one’s own IT department, may be targeted, and hence checks need to be performed to ensure the integrity of the software throughout the entire chain.

[12] Jack Stubbs, Raphael Satter & Joseph Menn, ‘U.S. Homeland Security, thousands of businesses scramble after suspected Russian hack’, 14 December, 2020, https://www.reuters.com/world/us/us-homeland-security-thousands-businesses-scramble-after-suspected-russian-hack-2020-12-15/.
[13] Computer Security Resource Center, ‘Supply chain attack’, https://csrc.nist.gov/glossary/term/supply_chain_attack.
[14] Trey Herr, William Loomis, Stewart Scott & June Lee, ‘Breaking Trust: Shades of Crisis Across an Insecure Software Supply Chain’, Atlantic Council, 26 July, 2020, https://www.atlanticcouncil.org/in-depth-research-reports/report/breaking-trust-shades-of-crisis-across-an-insecure-software-supply-chain/.

Political interference

There are also politically motivated cyberattacks mandated by states that interfere in democratic processes and political discourse. Democratic institutions are vulnerable targets of intelligence operations. The 2021 annual review by the Estonian Information System Authority warned that: "Cyberattacks are often aimed at candidates or parties, not necessarily the organisers of elections. Websites of candidates and parties, their social media pages, or e-mail servers could be attacked by a foreign adversary, a domestic attacker or trolls."[15]

One of the most recent examples of a politically motivated cyberattack occurred in January 2022 when the Ukrainian government was hit by a series of cyberattacks that defaced government websites and wiped out data on some government computers. More specifically, hackers changed the visual appearance of about 70 Ukrainian websites, including the ministries of foreign affairs, defence, energy, education and science, as well as the State Emergency Service and the Ministry of Digital Transformation, whose e-governance portal gives the public digital access to dozens of government services. The main webpage of about a dozen sites was replaced with a threatening message telling users to "be afraid and expect worse". After a couple of days, most of the sites were restored.[16]

In September 2020, the internal email system of Norway's parliament was hacked.[17] Ine Eriksen Soreide, the Minister of Foreign Affairs of Norway, underlined the significance of the attack by calling it an important cyber incident that had an effect on the "most important democratic institution" of the country.[18] After the incident, the Norwegian authorities identified Russia as the actor responsible for the attack. This was the first time that the Norwegian authorities had made a political attribution to such an attack.

Around the same time that Russian hackers breached the Norwegian parliament's email system, the Finnish parliament was also the target of a cyberattack. In this instance, hackers gained entry to the internal IT system and accessed the email accounts of some members of parliament. The Speaker of the Parliament described the breach as "a serious attack on our democracy and Finnish society".[19]

While the intent to interfere in Western political systems is present, the impact remains limited. These attacks are increasingly made public and we should not undermine confidence in our own democratic systems by overstating the impact of these Russian operations.

[15] Information System Authority of Estonia, *Cyber Security in Estonia 2021*, https://www.ria.ee/sites/default/files/content-editors/kuberturve/kuberturvalisuse_aastaraamat_2021_eng_final.pdf.
[16] Kim Zetter, 'What we know and don't know about the cyberattacks against Ukraine - (updated)', Zero Day, 17 January, 2022, https://zetter.substack.com/archive?sort=new.
[17] Catalin Cimpanu, 'Finland says hackers accessed MPs' email accounts', ZDNet, 28 December, 2020, https://www.zdnet.com/article/finland-says-hackers-accessed-mps-emails-accounts/.
[18] 'Norway blames Russia for cyber-attack on parliament', BBC, 13 October, 2020, https://www.bbc.com/news/world-europe-54518106.
[19] 'Cyber attack in Finland hits email accounts of MPs and parliament', Euronews, 28 December, 2020, https://www.euronews.com/2020/12/28/cyber-attack-in-finland-hits-email-accounts-of-mps-and-parliament.

Attacks against critical infrastructure

The most worrying attacks occur when states or state-backed actors design sophisticated malware to act as 'time bombs' in target countries' critical cyber networks, such as the energy sector, telecoms and transportation. For example, on at least two occasions – in December 2015 and 2016 – hackers attacked Ukraine's electricity distribution system, plunging thousands of citizens into darkness for extended periods of time. In a similar manner, in 2016, the Mimikatz malware – subsequently linked to a Russian military intelligence service – was spotted in the SCADA system of an Estonian holding group of oil shale, power generation and public utility companies.[20]

More recently, in Ukraine, in addition to the defacements that occurred on front-end internet-facing government systems, Microsoft announced that destructive wiper malware had been identified on Ukrainian systems that "provide critical executive branch or emergency response functions".[21] The so-called WhisperGate malware masqueraded as ransomware, but was actually designed to wipe or overwrite critical files on infected systems, leaving computer hard drives corrupted and unrecoverable. According to researchers from Cisco's Talos Intelligence Group, the hackers gained access to Ukraine systems months before deploying the wiper. The researchers found indicators of compromise revealing that the intruders were in the Ukrainian networks in late summer 2021.[22]

Ageing critical infrastructure around the globe has long been "open" to attack. In 2020, the UK's National Cyber Security Centre issued a joint warning alongside the US warning of Russian attacks on millions of routers, firewalls and devices used by infrastructure operators and government agencies.[23] However, the line between state and non-state attacks is becoming blurred. The increase in the skills of criminal cyber groups highlights a new risk to all infrastructure, illustrated by the case of the DarkSide attack against the US energy company Colonial Pipeline in May 2021, which affected the pipeline that provides almost half of the fuel used on the East Coast of the country. The pipeline was shut down for almost a week, leading to fuel shortages in several states.

Several reports[24] show that criminal groups offering Advance Persistent Threat-style attacks, whereby the intruder establishes a long-term presence in a network in order to mine highly sensitive data, are becoming more readily available and that the tactics, techniques and procedures used in these attacks are beginning to resemble the highly sophisticated state-sponsored campaigns.

[20] Republic of Estonia Information System Authority, 'Annual Cyber Security Assessment 2017', https://www.ria.ee/sites/default/files/content-editors/kuberturve/ria_csa_2017.pdf.

[21] 'Destructive malware targeting Ukrainian organizations', Microsoft Security, https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/.

[22] Kim Zetter, 'Hackers were in Ukraine systems months before deploying Wiper', Zero Day, 21 January, 2022, https://zetter.substack.com/p/hackers-were-in-ukraine-systems-months.

[23] Alix Pressley, 'The "cumulative effect" of ransomware and the lessons for UK national infrastructure', 20 July, 2021, https://www.intelligentcio.com/eu/2021/07/20/the-cumulative-effect-of-ransomware-and-the-lessons-for-uk-national-infrastructure/#.

[24] Fireeye Mandiant Services, Special Report, M-Trends 2021; BlackBerry, BAHAMUT: Hack-for-Hire Masters of Phishing, Fake News, and Fake Apps, https://www.blackberry.com/us/en/forms/enterprise/bahamut-report.

Response measures

Cybersecurity is essential for individuals and organizations alike. Regardless of whether the threat actor is a criminal group or a state, the adversary always looks for the easiest targets. Or, if the focus is on a specific target, the adversary searches for the easiest way into that target. Therefore, every effort to strengthen one's security is important in building resilience.

Due to an increased risk of fallout from recent cyberattacks targeting Ukraine, the UK's National Cyber Security Centre[25] and the US Cybersecurity and Infrastructure Security Agency (CISA)[26] have offered extensive advice on how to bolster cyber defences. Specific guidance recommends:

- Keeping all systems patched and updated with security fixes.
- Improving access controls and enabling multifactor authentication.
- Implementing and maintaining effective incident response plans.
- Ensuring all backup and restore mechanisms are working.
- Keeping a close eye on threat and mitigation information.

Cybersecurity has to be a fundamental consideration of any information system or solution. It should be practised together across sectors through training sessions, baseline standards and knowledge-sharing. Member state governments and the EU have to incentivize improvements in the quality of writing software and building hardware.

Looking at how decision-makers can become better prepared to anticipate and understand the effects of cyberattacks, conducting **exercises to respond to cyber-attacks** is one of the best ways to raise awareness at the political level, both in the EU and in NATO. As NATO CCDCOE, which annually organizes the Locked Shields exercise that involves a strategic decision-making element, pointed out about cyber exercises at the strategic level: "It is important to exercise the strategic level of cybersecurity for decision-makers. Decision-making at the strategic level forms an integral part of cyber resilience and must therefore be part of exercises. National security is dependent on our ability to defend networks that support our critical functions. This is not purely a technical issue. How our national cybersecurity strategies are translated into policies and procedures needs to be understood by all stakeholders." [27]

In September 2017, as part of the EU Council presidency, Estonia organized the first-ever cyber exercise for all EU defence ministers, with the NATO Secretary-General also in attendance. The then German Defence Minister, Ursula von der Leyen, called it an "extremely exciting" wargame that demonstrated the need for EU governments to be more aware of the impact of cyberattacks on critical infrastructure in the EU.

In July 2019, as part of Finland's presidency of the European Union Council, EU Ministers of Internal Affairs gathered for a meeting in Helsinki and participated in a scenario-based discussion exercise that Finland had prepared as host of the meeting. The exercise for ministers simulated a hybrid crisis which, inter alia, included cyberattacks and disinformation campaigns. As Finnish Minister of Internal Affairs Maria Ohisalo stated, the aim

[25] Mathew J. Schwartz, 'Cyberattack spillover from Ukraine: Be prepared, UK warns', Data Breach Today, 28 January 2022, https://www.databreachtoday.com/cyberattack-spillover-from-ukraine-be-prepared-uk-warns-a-18397.

[26] 'Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats', CISA, 18 January, 2022, https://www.cisa.gov/sites/default/files/publications/CISA_Insights-Implement_Cybersecurity_Measures_Now_to_Protect_Against_Critical_Threats_508C.pdf.

[27] 'Recent Cyber Events: Considerations for Military and National Security Decision Makers', NATO CCDCOE, November 2021, https://ccdcoe.org/uploads/2021/11/Report_Zero_Trust_A4.pdf.

was to "find a way to build resilience and raise awareness in the EU".[28]

During the Nordic-Baltic foreign ministers meeting in Tallinn in September 2020, a 90-minute tabletop exercise was organized.[29] It tested the foreign ministers' ability to respond and attribute an escalating cyberattack. They answered multiple-choice questions about the communication and about possible diplomatic countermeasures to the attack. The ministers learned through first-hand experience that a timely exchange of technical information can be key in responding to any cyberattack. "The shared view of the Nordic countries and Baltic states – especially when it comes to complicated issues – is crucial," said Urmas Reinsalu, the then Foreign Minister of Estonia.[30]

Ultimately, whether the adversary is a state's elite unit, or a criminal group rendering ransomware as a service, cybersecurity is about risk management, and about solid pragmatic defence measures to improve the security of the digital environment. There is a technical aspect to hardening defences and building redundancy in data and services, but the core of resilience is leadership that does not ignore the problem.

A consistent feature of cybersecurity over the years is that it has become a theatre for great-power conflict. The character of that conflict focuses on governments and militaries fighting in the hybrid 'grey zone', where the boundaries between peace and war are blurred. The actors navigate a complex web of ambigious and deeply interconnected challenges, where cyberattacks are not even a separate front, but rather an extension of the conflict itself.[31]

Both NATO and the EU will issue strategic documents in 2022 that will set the course for these two organizations' military planning for the next decade. This will require more transatlantic consultation on political-military matters with an emphasis on cybersecurity and cyber defence.

[28] Eszter Zalan, 'Finnish presidency to war-game hybrid threat response', *Eurobserver*, 27 June, 2019, https://euobserver.com/political/145283.

[29] Ministry of Foreign Affairs of Estonia, 'Joint Statement from Nordic-Baltic (NB8) Foreign Ministers' annual meeting', 9 September, 2020, https://vm.ee/et/uudised/joint-statement-nordic-baltic-nb8-foreign-ministers-annual-meeting.

[30] Press statement of the Ministry of Foreign Affairs of Estonia, 'Nordic and Baltic foreign ministers discuss regional and global politics in Tallinn', 9 September, 2020, https://vm.ee/en/news/nordic-and-baltic-foreign-ministers-discuss-regional-and-global-politics-tallinn.

[31] Dmitri Alperovitch, 'How Russia Has Turned Ukraine Into a Cyber-Battlefield', *Foreign Affairs*, January 28, 2022, https://www.foreignaffairs.com/articles/russia-fsu/2022-01-28/how-russia-has-turned-ukraine-cyber-battlefield.

Author
Merle Maigre is a Senior Cybersecurity Expert at the e-Governance Academy in Tallinn, Estonia.

Hybrid CoE