REDUCING CYBER INCIDENT RESPONSE TO PROTECT CNI FROM CYBER ATTACKS USING AN N-SIEM INTEGRATION WITH AN ICTI-CNI

Igli Tafa and Kevin Shahollari

Department of Computer Engineering, Polytechnic University of Tirana, Tirana

ABSTRACT

The rapid evolution of technology has increased the role of cybersecurity and put it at the center of national critical infrastructure. This role supports and guarantees the vital services of (CNI) while provides the proper functionalities for running operations between the public and private sectors. This evolution has had the same impact on cyberattack tools, methods, techniques used to gain unauthorized access to these computer systems that contain confidential and high-value information in the digital data sales market or asit called "darkweb".

As a result, it has become necessary to monitor all events of the National Critical Infrastructure (CNI) computer systems. This proposed system uses a centralized National SIEM (N-SIEM) specializing in the correlation of security events caused by cyber attacks, collected by CNIs systems while integrating with anInternational Cyber Threat Intelligence system (ICTI-CNI).

In addition, this conceptual model collects security breach events of CNIs systems, analyzes only cyber attacks, and correlates these security events in real-time with an intelligent automated platform while reducing the response time of security analysts.

KEYWORDS

CNI, N-SIEM, ICTI-CNI, IOC, cyber attacks security events.

1. INTRODUCTION

Today, cyber security incidents are constantly increasing in frequency and size, becoming more complex and unrestricted by state borders.[1] Consequently, when incidents occurred in these critical infrastructures, they can cause catastrophic damages for the country and its sectors by directly affecting human society.

1.1. Critical National Infrastructure (CNI)

Protecting critical national infrastructure is the primary goal of cyber security.[2] The Critical National Infrastructure (CNI) includes all the sectors of a country that work at all capacity 24 hours, seven days to ensure the existence, continuity, and vitality of the essential services used by society today. The protection and provision of this infrastructure is a responsibility shared between the two constituent sectors of the country: public and private, to ensure the availability of these services. By definition [3], Critical National Infrastructure (CNI) includes these categories: Food, Water, Chemicals, Health, Energy, Communications, Transport, Emergency Services, Civil

David C. Wyld et al. (Eds): MLDS, NECO, SEMIT, IBCOM, SPPR, SCAI, CSIA, ICCSEA - 2021
pp. 211-226, 2021. CS & IT - CSCP 2021 DOI: 10.5121/csit.2021.111818

Nuclear, Finance, Government, Defence, and Space. But each country can specify its most critical infrastructure, relying on those individuals sectors that provide the most necessary and crucial services to their society. Almost all of this infrastructure (CNI) has fallen under the control of advanced computer systems.[4] Damage to the security and availability of this infrastructure (CNI) would bring chaos throughout the country. This chaos comes because these sectors do not function separately but together consequently, a cyberattack on one of the infrastructure sectors would negatively affect all other sectors. In this way, is requisite complete security between the critical national infrastructure at the local, country, regional and international levels. Attackers often target this infrastructure (CNI)for various purposes ranging from gathering financial and confidential information to terrorist purposes.

2. BIG PICTURE

The most advanced cyber attacks can paralyze the most crucial communication hubs of the country by blocking public or private services but can also have devastating effects if these attacks affect the physical damage of critical national infrastructure which can cause human loss. Cybersecurity and Infrastructure Security Agency (CISA) identified critical national infrastructure (CNI) as the primary target of SolarWinds mass hacking that happened this year and the true impact of this attack is still unknown. [5] In the future, as a result of the exposure of this information and computer systems, countries may have interruption of services provided by this infrastructure (CNI). From this study [6], CISA, National Security Agency (NSA), and Federal Bureau of Investigation (FBI) have instructed all countries and organizations to do all the recommended patches of computer systems, especially vulnerabilities that are targeted by state-sponsored hackers.

For this reason, all sectors of CNI and the services they provide that are considered critical must be monitored and protected in real time 24 hours in 7 days from cyber attacks, ensuring 99.999% availability of the necessary services in the daily life of human society. To ensure these vital services to society is required not only that monitoring of this infrastructure but more decisive is the reaction time to these cyber attacks when they occur toward CNI. According to [7], the process of sharing information between countries and organizations that have previously encountered these cyber threats to their critical national infrastructure is relevant for detecting and preventing possible future cyber attacks.

This paper will be divided as follow: in section 3 we are presenting the essential role of this infrastructure, which is vital for the maintenance of societal functions and analyze the cyber threats that can be occurred to these CNIs.In section 4 will be analyzing the advantages and disadvantages of the actual technologies where our proposed will be mostly based. The proposed approach will be then presented in section 5, a new model and architecture for monitoring this critical infrastructure from security events generating by real attacks based on National SIEM integrated with a ICNI-CTI platform. Finally, section 6 is dedicated to the cyber attackers that had attacked that infrastructure in the past and a list of their APTs, group by countries suspected of these attacks.

3. RELATED WORKS

3.1. Definition

A cyberattack is a malicious attempt by an individual or group to attack and compromise the confidentiality, integrity, and availability of the systems that store valuable information which can be stolen and used for various purposes.

3.2. Requirements of cyberattack

Cyber attacks targeting this infrastructure (CNI) require more time and experience than attacks on widely used computer systems. The impact of these factors is reduced when considering that most cyber attacks are organized by the countries and their intelligence agencies that have the proper resources to attack this type of infrastructure (CNI).

3.3. Goals of cyberattack

The principal goal of a cyber attack is to affect the actual world but the real actions happen in the virtual and artificial world where they have involved: computers, servers, databases, or other devices that may have exploitable vulnerabilities. [8].

3.4. Categories of cyber attacks to CNI

Cyber crime (CC) - The activity of using technology or exploitable vulnerabilities discovered in these computer systems [9] to gain unauthorized access to confidential data that are used for financial gain.

a. Cyberthieves are individuals or groups involve in illegal cyber attacks for monetary gain and those stealing are considered low-risk for cyberattackers and costly for victims, with some estimates placing the annual global cost as high as hundreds of billions of dollar [10]. Cyber espionage (CE) - The activity of using technology or exploitable vulnerabilities discovered in these computer systems [9] to gain unauthorized access to classified data, stealing: industry or military trade secrets for economic gain, competitive advantage, or political reasons

b. Cyberspies are individuals or groups involve in illegal cyber attacks who steal classified or proprietary information used by governments or private corporations to gain a competitive strategic advantage. These individuals often work at the behest of and take direction from, foreign government entities [10]. Cyber warfareand Cyber sabotage (CW/CS) - The activity of using technology or exploitable vulnerabilities discovered in these computer systems [9] to damage the critical national infrastructure (CNI) of the target country, an action that could bring military precedent.

c. Cyberwarriors are state-sponsored and non-state actors who develop capabilities and undertake cyber attacks in support of a country's strategic objectives [10]

4. CNI MONITORING SYSTEMS

To monitor the critical services provided by this infrastructure (CNI), a security event management system (SIEM) is required to monitor all types of security events related to cyber attacks that can occur on a CNI.

4.1. Definition of SIEM

Gartner describes this security incident management system (SIEM) as a system needed for real-time data analysis for faster detection of information leakage and cyber attacks against internal or external threats. This system also collects, stores, and reports these cyber attacks in log format to respond more rapidly against cyber incidents. Additionally can be used in the digital forensics process or for legal procedures and compliance policies. [11].

4.2. Components of SIEM

A SIEM is composed of two main components which are:

1) Security Event Management (SEM) - provides real-time analysis, correlation, normalization of data collected from computer systems, infrastructures, network devices, and applications in log data format to provide a manual or automatic response, thus simplifying the management processby cyber security analysts.

2) Security Information Management (SIM) – SIM provides real-time analysis, storage, and reporting of collected (historical) security events to provide a data collection database by providingadditional functionalities that simplify the process of investigating cyber events.

When these two microsystems are combined, a Security Information and Event Management (SIEM) is created with the focus on collecting, analyzing, storing, and presenting the data collected by technological devices and entirely monitoring theinfrastructure.

4.3. Disadvantage of SIEM

Most of today's SIEMs function by collecting, correlating, analyzing, and presenting security events in the most understandable forms by the cyber security analyst whose function is to investigate cyber incidents. In the case of critical national infrastructure, theresponse should be as fast as possible. This event affects the response time because it needs time to accurately the data received, manually reduce the false positives, and verifythe real malicious indicators.

4.4. Reaction time dependence of SIEM

This time depends on the accuracy of data collected and correlated by all their internal and external IT and ICS infrastructures. Response time increases if the cyberattack has recently been identified and there is no available information on the methods used by theattackers to compare with other organizations or the infrastructure of the countries that may have been affected by this type of cyber attack

4.5. Monitoring and Intelligence integration

These systems are integrating with a new technology called Cyber Threat Intelligence (CTI) which includes more than raw data. This technology requires more detailedinformation collected only when human analysis is involved in this process.

This detailed information includes the tactics, tools, and procedures used by an attacker to predict those techniques that may use during other cyber attacks in the future. It shouldalso include the link between compromise indicators (IP addresses, risk-related domains,or hashes associated with malicious files and intruders (motivations, goals, and information about what they are targeting). [12]

5. PROPOSED SYSTEM DESIGN

Given the increasing complexity and vulnerability of CNI, the security of this infrastructure will continue to be crucial in the future. Consequently, the response to thesecyber incidents should be as fast as possible, considering this importance.

5.1. Why a new system?

At present, there is a high number of open-source or commercial platforms of this technology used to share cyber attacks. These platforms sometimes have many Indicators of Compromise (IOCs), obtained either from cyber attacks that have occurred and verifiedor from voluntary that can manually add the (IOCs) and those are not verified.

Add to the fact that these platforms don't orientate according to the critical national infrastructure sectors where the same threat feed serves for all (CNIs) sectors. Soincreases the likelihood that some of these indicators (I0Cs) will be false positives by notifying security analysts about preventing cyber attacks that are not actually happening, thus wasting time responding to and preventing cyber attacks that are likely to occur.

5.2. The concept of new system

“Share early and share often” it is essential in times of crisis. A cyber attack on critical infrastructure can have a cascading impact on multiple sectors across multiple jurisdictions, providing little time to contain and mitigate damage and prevent any follow-on attacks. [13]

The new system should rely on threat feeds focused on exact national critical infrastructure sectors, analyzing and correlating security events occurring in the internal (CNI) with events that appeared in the (CNI) of other countries that had the same attack behavior. This system (ICTI-CNI) should work as a correlation platform with their actualcurrent N- SIEM.

5.3. Requirements of new system

1. Reciprocal cooperation is required between countries and sectors of the same category, where shared information from a country that has been attacked is usedto prevent an attack on another country within the same group.
2. The ICTI platform should create a clear channel for the classification and declassification of attack information. The exchange process must take place between specific sectors of the CNI and countries, also the same between the public and private sectors providing vital services to society.

This proposed system is supposed to provide a more effective service while offering automated information sharing and alerting each other to incidents or cyber attacks that just happened in similar infrastructure.

5.4. Architecture of the system

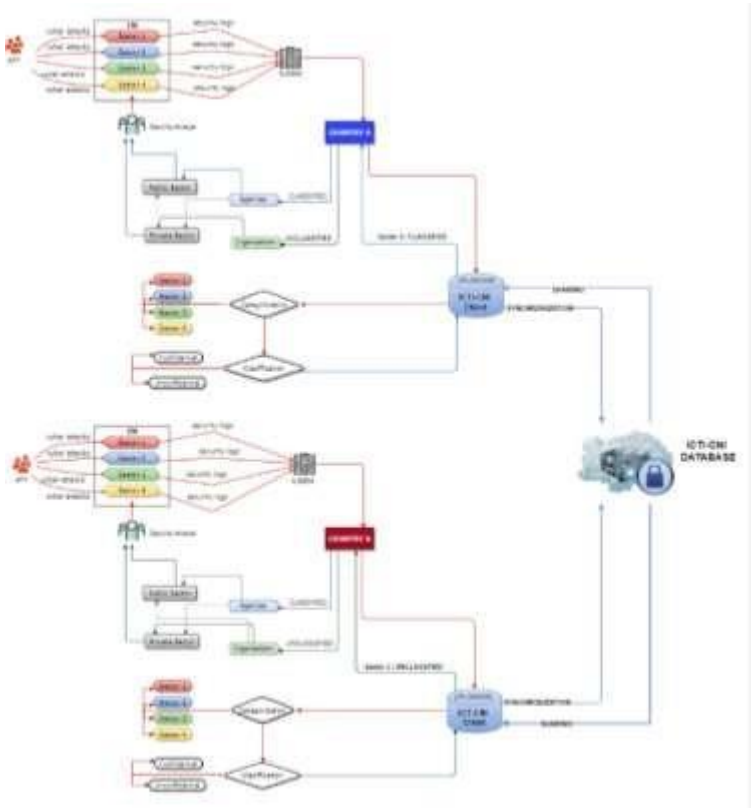

Figure 1. Architecture of the proposed system ICTI-CNI

This proposed system is composed of two components which are:

1) ICTI - CNI Client

It will be called any country that agrees to exchange information on cyber attacks occurring on their infrastructure (CNIs). Once the ICTI-Client is synchronizing with the central database, cyber attacks events that occurred in this client infrastructure (CNIs) will be an automatic correlation with other cyber incidents stored in the database.

2) ICTI - CNI Database

It will be called the central database, where all the information collected from the clients infrastructure that will be part of this exchange process will be stored and analyzed.

After the correlation of security events related to cyber attacks and according to the analysis of this information, the proper classification and categorization will be achieved. The information is then authorized to be shared with other clients within thesame group.

5.5. Integration with existing systems

All agencies that have the responsibility to protect those infrastructures can have their own commercial or open-source Threat Intelligence Feeds and continues to use even afterimplementing this proposed system. But on the ICHI, they should only share indicators of compromise

(IOCs) of attacks that have occurred in these infrastructures (CNIs) by grouping them in specific sectors.

5.6. Non-Disclosure secret agreement

All agencies that share information that corresponds to cyber attacks detected in other countries, in critical national infrastructure, must maintain the confidentiality of data and not share it with other organizations outside the sector where it operates

6. ADVANCED PERSISTENT THREATS

In most cases, cyber attacks conducted on CNI are state-sponsored, and detection of those attack campaigns has become extremely difficult while considering the evolution of strategies, techniques, and tactics used by cyber attackers on these infrastructures.

Advanced persistent threat (APT) refers to a group state-funded or the foreign government using intelligence gathering techniques to access sensitive information targeting a specific entity. [14] Objectives of APT attacks include continuous exfiltration of information, cyber warfare, damage to critical infrastructure, and degradation of military assets. [15]

Why is calling APT?

Advanced

Attackers use a variety of intelligence gathering techniques, including computer and conventional technologies such as telephone-interception technologies and satellite imaging. They often combine multiple targeting methods, tools, and techniques to reach and compromise their target and maintain access to it. [14]

Persistent

Attackers give priority to a specific task guided by external entities. The targeting is conducted using a “low-and-slow” approach through continuous monitoring and interaction to achieve the defined objectives. If the attackers lose access to their target, they usually will reattempt access because the purpose of this attack is to maintain alwayslong-term access to the target. [14]

Threat

Attackers are a threat because they are skilled, motivated, organized, and well-funded also have both capability and intent to attack and damage these critical infrastructures. Those attacks are executed by coordinated human actions rather than by automated piecesof code. [14]

Below are listed the most known dangerous APTs, which are often state-sponsored, where each of them has attack campaigned against many sectors of CNIs, including international and military organizations.

All pieces of information on APT are taken from [16] [17] [18] [19], analyzed, grouping, and presented graphically in the following tables on the most popular APTs groups that exist today.

6.1. Suspected attribution

6.1.1. China

NAME	A.K.A	TARGET SECTORS	TARGET COUNTRIES	ASSOCIATED MALWARE
Suspected attribution: CHINA				
APT1	Comment Crew (Symantec) Comment Panda (CrowdStrike) Shanghai Group ,TG-8223 (SecureWorks) APT 1 (Mandiant) BrownFox (Symantec) Group 3 (Talos) Byzantine Hades (US State) Byzantine Candor (US State) Shanghai Group (SecureWorks) GIF89a (Kaspersky)	Aerospace, Chemical, Construction, Defense, Education, Energy, Engineering, Entertainment, Financial, Food and Agriculture, Government, Healthcare, High-Tech, IT, Manufacturing, Media, Mining, Satellites, Telecommunications, Transportation and Navigation	Belgium, Canada, France, India, Israel, Japan, Luxembourg, Norway, Singapore, South Africa, South Korea, Switzerland, Taiwan, UAE, UK, USA, Vietnam.	Auriga, bangat, BISCUIT, Bouncer, Cachedump, CALENDAR, Combos, CookieBag, Dairy, GDOCUPLOAD, GetMail, GLASSES, GLOOXMAIL, GOGGLES, GREENCAT, gsecdump, Hackfase, Helauto, Kurton, LIGHTBOLT, LIGHTDART, LONGRUN, Lslsass, ManItsMe, MAPIget, Mimikatz, MiniASP, NewsReels, Oceansalt, Pass-The-Hash Toolkit, Poison Ivy, ProcDump, pwdump, Seasalt, ShadyRAT, StarsyPound, Sword, TabMsgSQL, Tarsip, WARP, WebC2, Living off the Land.
APT2	Putter Panda (CrowdStrike) TG-6952 (SecureWorks) APT 2 (Mandiant) Group 36 (Talos) Sulphur (Microsoft)	Military and Aerospace. Defense, Government,	USA	3PARA RAT, 4H RAT, httpclient, MSUpdater, pngdowner.
APT3	APT 3 (Mandiant) Gothic Panda (CrowdStrike) Buckeye (Symantec) TG-0110 (SecureWorks) Bronze Mayfair (SecureWorks) UPS Team (Symantec) Group 6 (Talos)	Aerospace and Defense, Construction and Engineering, High Tech, Telecommunications, Transportation	Belgium, Hong Kong, Italy, Luxembourg, Philippines, Sweden, UK, USA, Vietnam.	APT3 Keylogger, Bemstour, DoublePulsar, EternalBlue, HTran, Hupigon, LaZagne, OSInfo, Pirpi, PlugX, RemoteCMD, shareip, TTCalc, w32times and several 0-days for IE, Firefox and Flash.
APT4	APT 4 (Mandiant) Maverick Panda (CrowdStrike) Wisp Team (Symantec) Sykipot (AlienVault) TG-0623 (SecureWorks) Bronze Edison (SecureWorks)	Aerospace and Defense, Industrial Engineering, Electronics, Automotive, Government, Telecommunications, and Transportation	USA	Sykipot, XMRig.
APT5	APT 5 (FireEye) Keyhole Panda (CrowdStrike) TEMP.Bottle (iSight) Bronze Fleetwood (SecureWorks) TG-2754 (SecureWorks) Poisoned Flight (Kaspersky)	Defense, High-Tech, Industrial, Technology, Telecommunications.	Southeast Asia.	LEOUNCIA.
APT9	Nightshade Panda (CrowdStrike) APT 9 (Mandiant) Group 27 (ASERT) FlowerLady (Context) FlowerShow (Context)	Energy, Government, Media, Utilities.	Myanmar, Thailand, USA and Europe.	3102 RAT, 9002 RAT, EvilGrab RAT, MoonWind RAT, PlugX, Poison Ivy, Trochilus RAT.

APT10	Stone Panda (CrowdStrike) APT 10 (Mandiant) menuPass Team (Symantec) menuPass (Palo Alto) Red Apollo (PWC) CVNX (BAE Systems) Potassium (Microsoft) Hogfish (iDefense) Happyyongzi (FireEye) Cicada (Symantec) Bronze Riverside (SecureWorks) CTG-5938 (SecureWorks) ATK 41 (Thales) TA429 (Proofpoint) ITG01 (IBM)	Aerospace, Defense, Energy, Financial, Government, Healthcare, High-Tech, IT, Media, Pharmaceutical, Telecommunications and MSPs.	Australia, Belgium, Brazil, Canada, China, Finland, France, Germany, Hong Kong, India, Japan, Netherlands, Norway, Philippines, Singapore, South Africa, South Korea, Sweden, Switzerland, Taiwan, Thailand, Turkey, UAE, UK, USA, Vietnam.	Anel, BloodHound, certutil, ChChes, China Chopper, Cobalt Strike, Derusbi, DILLJUICE, DILLWEED, Ecipekac, Emdivi, EvilGrab RAT, Gh0st RAT, HTran, Impacket, Invoke the Hash, Mimikatz, MiS-Type, nbtscan, P8RAT, PlugX, Poison Ivy, Poldat, PowerSploit, PowerView, PsExec, PsList, pwdump, Quarks PwDump, QuasarRAT, RedLeaves, Rubeus, SharpSploit, SodaMaster, SNUGRIDE, Trochilus RAT, Living off the Land.
APT14	Anchor Panda (CrowdStrike) APT 14 (Mandiant) Aluminum (Microsoft)	Aerospace, Defense, Engineering, Government, Industrial	Australia, Germany, Sweden, UK, USA and others.	Gh0st RAT, Poison Ivy, Torn RAT.
APT15	Ke3chang (FireEye) Vixen Panda (CrowdStrike) APT 15 (Mandiant) GREF (SecureWorks) Bronze Palace (SecureWorks) Bronze Davenport (SecureWorks) Bronze Idlewood (SecureWorks) CTG-9246 (SecureWorks) Playful Dragon (FireEye) Royal APT (NCC Group)	Aerospace, Aviation, Chemical, Defense, Embassies, Energy, Government, High-Tech, Industrial, Manufacturing, Mining, Oil and gas,	Afghanistan, Belgium, Brazil, Chile, China, Egypt, France, Guatemala, India, Indonesia, Iran, Kazakhstan, Kuwait, Malaysia, Pakistan, Saudi Arabia, Slovakia, Syria, Turkey, UK, Uzbekistan.	BS2005, CarbonSteal, Cobalt Strike, DarthPusher, DoubleAgent, GoldenEagle, HenBox, HighNoon, Ketrican, Ketrum, Mimikatz, MirageFox, MS Exchange Tool, Okrum, PluginPhantom, ProcDump, PsList, RoyalCli, RoyalDNS, SilkBean, spwebmember, SpyWaller, TidePool, Winnti, XSLCmd, Living off the Land.
APT17	APT 17 (Mandiant) Tailgater Team (Symantec) Elderwood (Symantec) Elderwood Gang (Symantec) Sneaky Panda (CrowdStrike) SIG22 (NSA) Beijing Group (SecureWorks) Bronze Keystone (SecureWorks) TG-8153 (SecureWorks) TEMP.Avengers (FireEye) Dogfish (iDefense) Deputy Dog (iDefense) ATK 2 (Thales)	Defense, Education, Energy, Financial, Government, High-Tech, IT, Media, Mining, NGOs.	Belgium, China, Germany, Indonesia, Italy, Japan, Netherlands, Switzerland, Russia, UK, USA.	9002 RAT, BlackCoffee, Briba, Comfoo, DeputyDog, Gh0st RAT, HiKit, Jumpall, Linfo, Naid, Nerex, Pasam, Poison Ivy, PlugX, Vasport, Wiarp, ZoxPNG, ZoxRPC and several 0-days for IE.
APT18	APT 18 (Mandiant) Dynamite Panda (CrowdStrike) TG-0416 (SecureWorks) Wekby (Palo Alto) Scandium (Microsoft)	Aerospace, Construction, Defense, Education, Engineering, Healthcare, High-Tech, Telecommunications, Transportation and Biotechnology.	USA	AtNow, Gh0st RAT, hcdLoader, HTTPBrowser, Pisloader, StickyFingers and 0-day exploits for Flash.
APT26	Turbine Panda (CrowdStrike) APT 26 (Mandiant) PinkPanthe, Shell Crew (RSA) WebMasters (Kaspersky) KungFu Kittens (FireEye) Group 13 (Talos) Black Vine (Symantec) Bronze Express (SecureWorks)	Aerospace, Aviation, Defense, Energy, Financial, Food and Agriculture, Government, Healthcare, Non-profit organizations, Telecommunications, Think Tanks.	Australia, Canada, China, Denmark, France, Germany, India, Italy, UK, USA and Southeast Asia.	Cobalt Strike, Derusbi, FormerFirstRAT, Hurix, Mivast, PlugX, Sakula RAT, StreamEx, Winnti, Living off the Land.
APT27	Emissary Panda (CrowdStrike) APT 27 (Mandiant) LuckyMouse (Kaspersky) Bronze Union (Secureworks) TG-3390 (SecureWorks) Budworm ,TEMP.Hippo (Symantec) Group 35 (Talos) ATK 15 (Thales) Earth Smilodon (Trend Micro) Budworm (Trend Micro)	Aerospace, Aviation, Defense, Education, Embassies, Government, Manufacturing, Technology, Telecommunications, Think Tanks.	Australia, Canada, China, Hong Kong, India, Iran, Israel, Japan, Mongolia, Philippines, Russia, Spain, South Korea, Taiwan, Thailand, Tibet, Turkey, UK, USA and Middle East.	Antak, ASPXSpy, China Chopper, Gh0st RAT, gsecdump, HTTPBrowser, HTran, Hunter, HyperBro, Mimikatz, Nishang, OwaAuth, PlugX, ProcDump, PsExec, SysUpdate, TwoFace, Windows Credentials Editor, ZXShell, Living off the Land.

APT40	Leviathan (CrowdStrike) APT 40 (Mandiant) TEMP.Periscope (FireEye) TEMP.Jumper (FireEye) Bronze Mohawk (SecureWorks) Mudcarp (iDefense) Gadolinium (Microsoft) ATK 29 (Thales) ITG09 (IBM)	Defense, Engineering, Government, Manufacturing, Research, Shipping and Logistics, Transportation and other Maritime-related targets across multiple verticals.	Belgium, Cambodia, Germany, Hong Kong, Malaysia, Norway, Philippines, Saudi Arabia, Switzerland, USA, UK and Asia Pacific Economic Cooperation (APEC).	AIRBREAK, BADFLICK, BlackCoffee, China Chopper, Cobalt Strike, DADJOKE, Dadstache, Derusbi, Gh0st RAT, GRILLMARK, HOMEFRY, LUNCHMONEY, MURKYTOP, NanHaiShu, PlugX, scanbox, SeDLL, Windows Credentials Editor, ZXShell, Living off the Land.
APT41	APT 41 (FireEye) TG-2633 (SecureWorks) Bronze Atlas (SecureWorks) Red Kelpie (PWC) Blackfly (Symantec)	Construction, Defense, Education, Energy, Financial, Government, Healthcare, High-Tech, Hospitality, Manufacturing, Media, Oil and gas, Petrochemical, Pharmaceutical, Retail, Telecommunications, Transportation	Australia, Brazil, Canada, Chile, Denmark, Finland, France, Hong Kong, India, Indonesia, Italy, Japan, Malaysia, Mexico, Myanmar, Netherlands, Pakistan, Philippines, Poland, Qatar, Saudi Arabia, Singapore, South Korea, South Africa, Sweden, Switzerland, Taiwan, Thailand, Turkey, UAE, UK, USA, Vietnam.	9002 RAT, AceHash, ADORE.XSEC, ASPXSpy, Barlaiy, BIOPASS RAT, BlackCoffee, certutil, China Chopper, Cobalt Strike, COLDJAVA, Crackshot, CrossWalk, DEADEYE, Derusbi, DIRTCLEANER, EasyNight, GearShift, Gh0st RAT, HDRoot, HighNoon, HighNote, HKDOOR, Jumpall, LATELUNCH, LIFEBOAT, Lowkey, MessageTap, Meterpreter, Mimikatz, njRAT, NTDSDump, PACMAN, PipeMon, PlugX, POTROAST, pwdump, RedXOR, ROCKBOOT, SAGEHIRE, ShadowHammer, ShadowPad Winnti, Skip-2.0, Speculoos, SWEETCANDLE, TERA, TIDYELF, WIDETONE, Winnti, WINTERLOVE, xDll, XDOOR, XMRig, ZXShell, Living off the Land.

6.1.2. Russia

NAME	A.K.A	TARGET SECTORS	TARGET COUNTRIES	ASSOCIATED TOOLS
Suspected attribution: RUSSIA				
APT28	Sofacy (Kaspersky) APT 28 (Mandiant) Fancy Bear (CrowdStrike) Sednit (ESET) Group 74 (Talos) TG-4127 (SecureWorks) Pawn Storm (Trend Micro) Tsar Team (iSight) Strontium (Microsoft) Swallowtail (Symantec) SIG40 (NSA) Snakemackerel (iDefense) Iron Twilight (SecureWorks) ATK 5 (Thales) T-APT-12 (Tencent) ITG05 (IBM) TAG-0700 (Google) Grizzly Steppe (US Government) together with APT 29, Cozy Bear, The Dukes	Automotive, Aviation, Chemical, Construction, Defense, Education, Embassies, Engineering, Financial, Government, Healthcare, Industrial, IT, Media, NGOs, Oil and gas, Think Tanks and Intelligence organizations.	Afghanistan, Armenia, Australia, Azerbaijan, Belarus, Belgium, Brazil, Bulgaria, Canada, Chile, China, Croatia, Cyprus, France, Georgia, Germany, Hungary, India, Iran, Iraq, Japan, Jordan, Kazakhstan, Latvia, Malaysia, Mexico, Mongolia, Montenegro, Netherlands, Norway, Pakistan, Poland, Romania, Slovakia, South Africa, South Korea, Spain, Sweden, Switzerland, Tajikistan, Thailand, Turkey, Uganda, UAE, UK, Ukraine, USA, Uzbekistan, NATO and APEC and OSCE.	Cannon, certutil, Computrace, CORESHELL, DealersChoice, Downdelph, Drovorub, Foozer, HIDEDRV, JHUHUGIT, Koadic, Komplex, LoJax, Mimikatz, Nimcy, OLDBAIT, PocoDown, ProcDump, PythocyDbg, Responder, Sedkit, Sedreco, SkinnyBoy, USBStealer, VPNFilter, Winexe, WinIDS, X-Agent, X-Tunnel, Zebrocy, Living off the Land.
APT29	APT 29 (Mandiant) Cozy Bear (CrowdStrike) The Dukes (F-Secure) Group 100 (Talos) Yttrium (Microsoft) Iron Hemlock (SecureWorks) Minidionis (Palo Alto) CloudLook (Kaspersky) ATK 7 (Thales) ITG11 (IBM) Grizzly Steppe (US Government) together with Sofacy, APT 28, Fancy Bear, Sednit UNC2452 (FireEye) Dark Halo (Volexity) SolarStorm (Palo Alto) StellarParticle (CrowdStrike) Nobelium (Microsoft) Iron Ritual (SecureWorks)	Defense, Energy, Government, Law enforcement, Media, NGOs, Pharmaceutical, Telecommunications, Transportation, Think Tanks and Imagery	Australia, Azerbaijan, Belarus, Belgium, Brazil, Bulgaria, Canada, Chechnya, China, Cyprus, Czech, France, Georgia, Germany, Hungary, India, Ireland, Israel, Japan, Kazakhstan, Kyrgyzstan, Latvia, Lebanon, Lithuania, Luxembourg, Mexico, Montenegro, Netherlands, New Zealand, Poland, Portugal, Romania, Russia, Slovenia, Spain, South Korea, Turkey, Uganda, UK, Ukraine, USA, Uzbekistan, NATO.	7-Zip, AdFind, ATI-Agent, AtNow, CloudDuke, Cobalt Strike, CosmicDuke, CozyDuke, FatDuke, GeminiDuke, GoldFinder, GoldMax, HammerDuke, LiteDuke, meek, Mimikatz, MiniDuke, OnionDuke, PinchDuke, PolyglotDuke, POSHSPY, PowerDuke, RAINDROP, RegDuke, SeaDuke, Sibot, SoreFang, SUNBURST, SUNSPOT, SUPERNOVA, TEARDROP, WellMail, WellMess, Living off the Land.
RUS1	Berserk Bear (CrowdStrike) Dragonfly 2.0 (Symantec) Dymalloy (Dragos)	Energy	Azerbaijan, Belgium, Canada, France, Germany, Italy, Norway, Russia, Singapore, Spain, Switzerland, Turkey, UK, Ukraine, USA.	Goodor, Impacket, Karagany, Phishery, Living off the Land.
RUS2	Cobalt Group	Financial, High-Tech, Media, Retail.	Argentina, Armenia, Austria, Azerbaijan, Belarus, Bulgaria, Canada, China, Czech, Estonia, Georgia, Italy, Jordan, Kazakhstan, Kuwait, Kyrgyzstan, Malaysia, Moldova, Netherlands, Poland, Romania, Russia, Spain, Taiwan, Tajikistan, Thailand, Turkey, UK, Ukraine, USA, Vietnam.	ATMSpitter, ATMRipper, AtNow, Cobalt Strike, CobInt, Cyst Downloader, FlawedAmmyy, Formbook, Little Pig, Mimikatz, Metasploit Stager, More_eggs, NSIS, Pony, SDelete, SoftPerfect Network Scanner, Taurus Loader, ThreatKit, VenomKit.
RUS3	Cyber Berkut	Defense, Financial, Government.	Estonia, Germany, Ukraine, USA, NATO.	No information

RUS4	Energetic Bear (CrowdStrike) Dragonfly (Symantec) Crouching Yeti (Kaspersky) Group 24 (Talos) Koala Team (iSight) Iron Liberty (SecureWorks) TG-4192 (SecureWorks) Electrum (Dragos) ATK 6 (Thales) ITG15 (IBM)	Aviation, Construction, Defense, Education, Energy, Industrial, IT, Manufacturing, Oil and gas, Pharmaceutical.	Canada, France, Germany, Greece, Italy, Norway, Poland, Romania, Russia, Serbia, Spain, Turkey, UK, Ukraine, USA.	Commix, CrackMapExec, Dirsearch, Dorshel, Goodor, Havex RAT, Hello EK, Heriplor, Impacket, Industroyer, Inveigh, Karagany, LightsOut EK, Listrix, nmap, PHPMailer, PsExec, SMBTrap, sqlmap, Subbrute, Sublist3r, Sysmain, Wpscan, WSO.
RUS5	Gamaredon Group (Palo Alto) Winterflounder (iDefense) Primitive Bear (CrowdStrike) BlueAlpha (Recorded Future) Blue Otso (PWC) Iron Tilden (SecureWorks)	Defense, Government, Law enforcement,	Albania, Austria, Australia, Bangladesh, Brazil, Canada, Chile, China, Colombia, Croatia, Denmark, Georgia, Germany, Guatemala, Honduras, India, Indonesia, Iran, Israel, Italy, Japan, Kazakhstan, Malaysia, Netherlands, Nigeria, Norway, Pakistan, Papua New Guinea, Poland, Portugal, Romania, Russia, South Africa, South Korea, Spain, Sweden, Turkey, UK, Ukraine, USA, Vietnam	Aversome infector, EvilGnome, FRAUDROP, Gamaredon, Pteranodon, RMS, Resetter, UltraVNC.
RUS6	Indrik Spider (CrowdStrike) Gold Drake (SecureWorks) Gold Winter (SecureWorks) Evil Corp (self given)	Financial, Government, Healthcare	Worldwide	Advanced Port Scanner, Babuk Locker, BitPaymer, Cobalt Strike, Cridex, Dridex, EmpireProject, Hades, MEGAsync, Metasploit, Mimikatz, PayloadBIN, Phoenix, PowerSploit, PsExec, SocGholish, WastedLoader, WastedLocker.
RUS7	OldGremlin	Financial, Healthcare, Media.	Russia	Cobalt Strike, TinyCryptor, TinyNode, TinyPosh.
RUS8	Sandworm Team (Trend Micro) Iron Viking (SecureWorks) CTG-7263 (SecureWorks) Voodoo Bear (CrowdStrike) Quedagh (F-Secure) TEMP.Noble (FireEye) ATK 14 (Thales) BE2 (Kaspersky)	Education, Energy, Government, Telecommunications.	Azerbaijan, Belarus, France, Georgia, Iran, Israel, Kazakhstan, Kyrgyzstan, Lithuania, Poland, Russia, Ukraine.	BlackEnergy, Gcat, P.A.S., PassKillDisk, PsList.
RUS9	TEMP.Veles (FireEye) Xenotime (Dragos) ATK 91 (Thales)	Critical infrastructure, Energy, Manufacturing, Oil and gas.	Saudi Arabia, USA and others.	Cryptcat, Mimikatz, NetExec, PsExec, SecHack, Triton, Wii.

6.1.3. Iran

RUS10	Turla (Kaspersky) Waterbug (Symantec) Venomous Bear (CrowdStrike) Group 88 (Talos) SIG2 (NSA) SIG15 (NSA) SIG23 (NSA) Iron Hunter (SecureWorks) CTG-8875 (SecureWorks) Pacifier APT (Bitdefender) ATK 13 (Thales) ITG12 (IBM) Makersmark (ESET) Krypton (Microsoft) Belugasturgeon (Accenture) Popeye (?) Wraith (?) TAG-0530 (Google)	Aerospace, Defense, Education, Embassies, Energy, Government, High-Tech, IT, Media, NGOs, Pharmaceutical, Research, Retail.	Afghanistan, Algeria, Armenia, Australia, Austria, Azerbaijan, Belarus, Belgium, Bolivia, Botswana, Brazil, China, Chile, Denmark, Ecuador, Estonia, Finland, France, Georgia, Germany, Hong Kong, Hungary, India, Indonesia, Iran, Iraq, Italy, Jamaica, Jordan, Kazakhstan, Kyrgyzstan, Kuwait, Latvia, Mexico, Netherlands, Pakistan, Paraguay, Poland, Qatar, Romania, Russia, Serbia, Spain, Saudi Arabia, South Africa, Sweden, Switzerland, Syria, Tajikistan, Thailand, Tunisia, Turkmenistan, UK, Ukraine, Uruguay, USA, Uzbekistan, Venezuela, Vietnam, Yemen.	AdobeARM, Agent.BTZ, Agent.DNE, ASPXSpy, ATI-Agent, certutil, CloudDuke, Cobra Carbon System, COMpfun, ComRAT, Crutch, DoublePulsar, EmpireProject, Epic, EternalBlue, EternalRomance, Gazer, gpresult, HTML5 Encoding, HyperStack, IcedCoffee, IronNetInjector, Kazuar, KopiLuwak, KSL0T, LightNeuron, Maintools.js, Metasploit, Meterpreter, MiamiBeach, Mimikatz, Mosquito, Nautilus, nbtscan, nbtstat, Neptun, NetFlash, Neuron, NewPass, Outlook Backdoor, Penquin Turla, PowerShellRunner-based RPC backdoor, PowerStallion, PsExec, pwdump, PyFlash, RocketMan, Satellite Turla, SScan, Skipper, SMBTouch, Topinambour, Tunnus, Uroburos, Windows Credentials Editor, WhiteAtlas, WITCHCOVEN, Living off the Land
RUS11	Wizard Spider (CrowdStrike) Grim Spider (CrowdStrike) TEMP.MoMaster (FireEye) Gold Blackburn (SecureWorks) Gold Ulrick (SecureWorks)	Defense, Financial, Government, Healthcare, Telecommunications.	Worldwide.	AdFind, Anchor, BazarBackdoor, BloodHound, Cobalt Strike, Conti, Diavol, Dyre, Gophe, Invoke-SMBAutoBrute, LaZagne, LightBot, PowerSploit, PowerTrick, PsExec, Ryuk, SessionGopher, TrickBot, TrickMo, Upatre.

6.1.4. North Korea

NAME	A.K.A	TARGET SECTORS	TARGET COUNTRIES	ASSOCIATED MALWARE
Suspected attribution: North Korea				
APT37	Reaper (FireEye) TEMP.Reaper (FireEye) APT 37 (Mandiant) Ricochet Chollima (CrowdStrike) ScarCruft (Kaspersky) Thallium (Microsoft) Group 123 (Talos) Red Eyes (AhnLab) Geumseong121 (ESRC) Venus 121 (ESRC) Hermit (Tencent) ATK 4 (Thales) ITG10 (IBM)	Aerospace, Automotive, Chemical, Financial, Government, Healthcare, High-Tech, Manufacturing, Technology, Transportation.	China, Hong Kong, India, Japan, Kuwait, Nepal, Romania, Russia, South Korea, UK, USA, Vietnam.	CARROTBALL, CARROTBAT, CORALDECK, DOGCALL, Erebus, Final1stSpy, Freenki Loader, GELCAPSULE, GreezeBackdoor, HAPPYWORK, KARAE, KevDroid, Konni, MILKDROP, N1stAgent, NavRAT, Nokki, Oceansalt, PoohMilk Loader, POORAIM, RokRAT, RICECURRY, RUHAPPY, ScarCruft, SHUTTERSPEED, SLOWDRIFT, SOUNDWAVE, Syscon, WINERACK, ZUMKONG and several 0-day Flash and MS Office exploits.
Lazarus Group	Andariel (FSI) Silent Chollima (CrowdStrike) BeagleBoyz Bluenoroff (Kaspersky) APT 38 (Mandiant) Stardust Chollima (CrowdStrike) CTG-6459 (SecureWorks) Nickel Gladstone (SecureWorks) T-APT-15 (Tencent) ATK 117 (Thales)	Aerospace, Engineering, Financial, Government, Media, Shipping and Logistics, Technology and BitCoin exchanges	Australia, Bangladesh, Brazil, Canada, Chile, China, Ecuador, France, Germany, Guatemala, Hong Kong, India, Israel, Japan, Mexico, Philippines, Poland, Russia, South Africa, South Korea, Taiwan, Thailand, UK, USA, Vietnam and Worldwide (WannaCry).	3proxy, 3Rat Client, Andaratm, AppleJeus, ARTFULPIE, Aryan, ATMDtrack, AuditCred, BADCALL, Bankshot, BanSwift, BISTROMATH, Bitsran, BLINDINGCAN, BlindToad, Bookcode, BootWreck, Brambul, BTC Changer, BUFFETLINE, Castov, CheeseTray, CleanToad, ClientTraficForwarder, Concealment Troy, Contopee, CookieTime, COPPERHEDGE, Dacls RAT, DarkComet, DeltaCharlie, Destover, Dozer, DoublePulsar, Dtrack, Duuzer, DyePack, ELECTRICFISH, EternalBlue, FALLCHILL, Fimlis, Gh0st RAT, HARDRAIN, Hawup, Hermes, HOPLIGHT, HotelAlfa, HOTCROISSANT, Hotwax, HtDnDownLoader, Http Dr0pper, HTTP Troy, Joanap, Jokra, KEYMARBLE, KillDisk, Koredos, Lazarus, MATA, Mimikatz, Mydoom, NachoCheese, NestEgg, NukeSped, OpBlockBuster, PEBBLEDASH, PhanDoor, Plink, PowerBrace, PowerRatankba, PowerShell RAT, PowerSpritz, PowerTask, ProcDump, Proxysvc, PSLogger, Quickcafe, Ratankba, RatankbaPOS, RawDisk, Recon, RedShawl, Rifdoor, Rising Sun, Romeos, RomeoAlfa, RomeoBravo, RomeoCharlie, RomeoDelta, RomeoEcho, RomeoFoxtrot, RomeoGolf, RomeoHotel, RomeoMike, RomeoNovember, RomeoWhiskey, SHARPKNOT, SheepRAT, SierraAlfa, SierraCharlie, SLICKSHOES, Stunnel, TAINTEDSCRIBE, Tdrop, Tdrop2, TFlower, ThreatNeedle, Troy, TYPEFRAME, ValeforBeta, VHD, Volgmer, VSingle, Vyveva, WannaCry, WbBot, WolfRAT, Wormhole, Yort.

6.1.5. USA and UK

NAME	A.K.A	TARGET SECTORS	TARGET COUNTRIES	ASSOCIATED MALWARE
Suspected attribution: USA and UK				
CIA	Longhorn (Symantec) The Lamberts (Kaspersky) Platinum Terminal (SecureWorks) Platinum Colony (SecureWorks) APT-C-39 (Qihoo 360)	Aerospace, Aviation, Education, Energy, Financial, Government, IT, Oil and gas, Research, Telecommunications.	China and 16 countries in the Middle East, Europe, Asia and Africa, North Korea, Russia.	Black Lambert, Blue Lambert, Corentry, Cyan Lambert, Gray Lambert, Green Lambert, Lambert, Magenta Lambert, Pink Lambert, Purple Lambert, Silver Lambert, Violet Lambert, White Lambert.
Equation Group	Equation Group (real name) Tilded Team (CrySys) Platinum Colony (SecureWorks)	Aerospace, Defense, Energy, Government, Media, Oil and gas, Telecommunications, Transportation and Nanotechnology, Nuclear research, Islamic activists	Afghanistan, Bangladesh, Belgium, Brazil, Ecuador, France, Germany, Hong Kong, India, Iran, Iraq, Israel, Kazakhstan, Lebanon, Libya, Malaysia, Mali, Mexico, Nigeria, Pakistan, Palestine, Philippines, Qatar, Russia, Singapore, Somalia, South Africa, Sudan, Switzerland, Syria, UAE, UK, USA, Yemen.	DarkPulsar, DOUBLEFANTASY, DoublePulsar, Duqu, EQUATIONDRUG, EQUATIONLASER, FANNY, Flame, GRAYFISH, GROK, Lambert, OddJob, Regin, TRIPLEFANTASY, UNITEDRAKE
GCHQ	GCHQ	Government, Telecommunications.	Belgium, UK.	INCENSER, Regin Prax, WarriorPride

7. CONCLUSIONS

Most of these CNI are connected to the Internet because it is easier to remotely manage these complex sectors while using technology devices than to physically send a technician engineer to manually checking the functionality of every individual of them.
As the use of the Internet increases, so does the probability of these infrastructures being cyber-attacked by APTs groups to steal unauthorized confidential information for various purposes such as intelligence gathering, financial gain, or sabotaging vital services of a country.
In this paper, we proposed a new system to monitor and protect these critical infrastructures (CNI) based on National SIEM integrated with a CNI-CTI platform from cyber-attacks that occurred in different sectors of CNI.
The way to achieve this advanced cyber intelligence is by improving the exchange information process on cyber attacks across all countries' infrastructure (CNI) sectors.
The efficiency and velocity of this system improve security analyst's response time to take accelerated countermeasures by applying specific policies to their CNIs.

REFERENCES

[1] ENISA (European Union Agency for Network and Information Security), “Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches”, 2015, pp. 06. online:https://www.enisa.europa.eu/publications/cybersecurity-information- sharing.
[2] Presidency of the Council of Ministers, “NATIONAL STRATEGIC FRAMEWORK FOR CYBERSPACE SECURITY”, 2013, pp. 12-15, online:https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian- national-strategic-framework-for-cyberspace-security.pdf
[3] Cabinet Office UK, “Public Summary of Sector Security and Resilience Plans UK” 2018, pp. 5, online

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786206/20190215_PublicSummaryOfSectorSecurityAndResiliencePlans2018.pdf
[4] Misha Glenny, "DarkMarket. How Hackers Became the New Mafia" 2012, pp. 11
[5] CISA (Cybersecurity and Infrastructure Security Agency), "Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations Alert (AA20-352A)" April 15 2021, online https://us-cert.cisa.gov/ncas/alerts/aa20-352a
[6] NSA (National Security Agency), "APT29 Targets U.S. and Allied Networks", U/OO/132340-21, April 2021 Ver. 1.0, pp. 21, 0292, online:https://media.defense.gov/2021/Apr/15/2002621240/- 1/-1/0/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF
[7] Executive Order No 13636 President of USA, "Improving Critical Infrastructure Cybersecurity", The White House, February 12, 2013. Sec. 4-c, online: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving- critical-infrastructure-cybersecurity
[8] Kenneth Geers, "The Cyber Threat to National Critical Infrastructures: Beyond Theory", July 7, 2009, pp. 2, online https://ccdcoe.org/uploads/2018/10/Geers2009_The-Cyber-Threat-to-National-Critical-Infrastructures.pdf
[9] The Federal Council, "National strategy for the protection of Switzerland against cyber risks (NCS) 2018-2022" 2018, pp, 4 online: https://www.ncsc.admin.ch/ncsc/en/home/strategie/strategie-ncss-2018-2022.html
[10] Eric A. Fischer, Edward C. Liu, John W. Rollins, Catherine A. Theohary, Congressional Research Service, "The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress" pp. 3, online: https://sgp.fas.org/crs/misc/R42984.pdf
[11] Gartner, "Security Information And Event Management", online:https://www.gartner.com/en/information-technology/glossary/security-information-event-management
[12] FireEye, "Cyber Threat Intelligence 101" online: https://www.fireeye.com/mandiant/threat-intelligence/what-is-cyber-threat-intelligence.html
[13] INSA (Intelligence and National Security Alliance), "Managing A Cyber Attack On Critical Infrastructure: Challenges Of Federal, State, Local, And Private Sector Collaboration" August 2018, Pp. 13, online:https://www.insaonline.org/wp-content/uploads/2018/08/INSA-Managing-Cyber-Attack-Critical-Infrastructure.pdf
[14] ENISA (European Union Agency for Network and Information Security), "Advanced persistent threat incident handling" September 2014, pp.2 online https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/advanced_persistent_threat_incident_handling_toolset
[15] N. Pissanidis, H. Rõigas, M. Veenendaal, "Countering Advanced Persistent Threats through Security Intelligence and Big Data Analytics" pg.1, NATO CCD COE Publications, Tallinn, online: https://www.ccdcoe.org/uploads/2018/10/Art-15-Countering-Advanced-Persistent-Threats-through-Security-Intelligence-and-Big-Data-Analytics.pdf
[16] FireEye, "Advanced Persistent Threat Groups", online: https://www.fireeye.com/current- threats/apt-groups.html
[17] MITRE ATT&CK, "Advanced Persistent Threat Groups", online: https://attack.mitre.org/groups/G0082/
[18] ThaiCERT (Thailand Computer Emergency Response Team) "Advanced Persistent Threat Groups", online: https://apt.thaicert.or.th/cgi-bin/listgroups.cgi
[19] Malpedia, "Advanced Persistent Threat Groups", online: https://malpedia.caad.fkie.fraunhofer.de/

© 2021 By AIRCC Publishing Corporation. This article is published under the Creative Commons Attribution (CC BY) license.