TECHNICAL ANALYSIS OF ADVANCED THREAT TACTICS TARGETING CRITICAL INFORMATION INFRASTRUCTURE

By MSc. Bernhards Blumbergs, GXPN, NATO CCD CoE
bernhards.blumbergs@ccdcoe.org

Critical information infrastructure (CII) provides vital functions for a nation's existence and the wellbeing of its citizens. This makes CII susceptible to an increasing number of targeted, strategically executed cyber attacks. Such sophisticated attacks lead to information system compromise, control takeover, component destruction, and sensitive information extraction. The grave consequences implied by actors behind the corresponding attacks have to be acknowledged and potential risks appraised, in order to raise the awareness and readiness level to defend against an advanced adversary.

To distinguish what technical means and tactics are employed by advanced threat actors when targeting the CII, this paper reviews targeted attack trends, assesses actor motivation and situational background, assembles data on known major incidents, and defines their analysis criteria to perform selected case studies.

From threat landscape assessment and incident case studies it can be identified that cyber means can be considered as a feasible approach for gaining advantage for competitive motivations, conflict situations, and maintaining presence in cyber space. This leads to the existence of increasingly resourceful and motivated threat actors, weaponisation of cyber means, virtualisation of forces, and the dawn of cyber espionage.

Keywords: *Critical information infrastructure; advanced persistent threat; cyber attacks.*

I. INTRODUCTION

The meaning of Critical Information Infrastructure (CII) is ambiguous as it has no single internationally agreed legal definition, and is defined differently by counties and states, depending on their internal requirements, security considerations, and situational environment. For example, compare the definition of Critical Infrastructure (CI) by the European Union (EU) and the United States of America (US). The EU directive of 2008 defines: "Critical infrastructure means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social wellbeing of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions"[1]. US Critical Infrastructure Protection Act of 2001 defines: "Critical infrastructure are the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof"[2]. These two definitions have distinct differences in the way they interpret CI and assess the disruption or destruction impact. For the scope of this paper, CII is considered as the entities and infrastructures which process, store, exchange information required to provide the services that are crucial to a nation's existence and the wellbeing of the society. These infrastructures have to be protected in order to ensure the CI continuity and dependability objectives, as defined by national and international policies.

The field related to CII is broad and dependant on various country relevant specifics, such as its development, resources and industrial capabilities. For instance, the diverse CI spectrum for a single EU state covers at least the following areas: energy (e.g., electrical power, oil, gas), sanitation (e.g. water supply, waste water collection and processing); transportation (e.g., roads, railway, traffic organisation, civil/military aviation); communications (e.g., information technology infrastructure, telecommunications, Internet access); security and safety (e.g., military, police, emergency services); medicine (e.g. health-care, hospitals); research (e.g., industrial and scientific developments); finances (e.g., state treasury, banks, money wire transfers); and politics (e.g., national secrets, foreign policy and affairs).

When assessing the CII, not only do legal differences have to be taken into account, the variety of technical approaches and means in granting their functionality, safety and security have to be considered. On one hand, traditional information technology (IT) security oriented approaches should be implemented and enforced for the majority of CII, but on the other hand accepted IT solutions are not fully applicable for specific domains such as industrial control systems (ICS)[3]. However, ICS/SCADA (Supervisory Control and Data Acquisition) systems are not to be solely attributed to CII; nevertheless, they play a very important role for vital service provision. ICS could be assumed as the backbone of industry, therefore drawing huge attention by security researchers and malicious actors due to the very nature of how these systems are operating, are being deployed, and are being merged with other technologies[4]. Ongoing ICS fusion with IT solutions provides a more scalable deployment and management; however, also implies a major risk on exposing them to the Internet[1], therefore putting an end to the myths of their "security through obscurity"[5].

Likewise, the state's governmental entities are implicitly vulnerable due to the way they conduct their operations as required by the law. For example, consider a foreign embassy secretariat which is required to open and process all incoming electronic mail messages and their attachments in order to provide its services to the public. This inherit operational characteristic can be acknowledged as a serious vulnerability which provides a pathway for client-side attacks, system compromise, and potentially sensitive information exfiltration[2]. These legal and technical ambiguities regarding CII[6] provide a path for malicious actors to launch targeted attacks[7] against the underlying national infrastructure, bringing the most grave consequences to its security, safety, functionality, and wellbeing of the people.

... SANS INSTITUTE SURVEY DERIVES THAT CYBER ATTACKS TARGETING ICS/SCADA WILL INCREASE IN THE COMING YEARS ...

The EU Agency for Network and Information Security (ENISA) Threat Landscape reports[8],[9] classify the targeted attack as an emerging and increasing threat directed towards cloud services, critical infrastructures and social technologies. SANS Institute survey[10] derives that cyber attacks targeting ICS/SCADA will increase in the coming years. A research conducted by Trend Micro[11] concludes that the threats targeting CII are real and cyber attacks are being executed constantly involving large numbers of countries, diverse motivations, and goals. As reported by

[1] Internet connected device search engine - SHODAN. http://www.shodanhq.com/. Accessed 05/05/2014

[2] "Data exfiltration is the unauthorized transfer of sensitive information from a target's network to a location which a threat actor controls." TrendLabs Security Intelligence blog. http://blog.trendmicro.com/trendlabs-security-intelligence/data-exfiltration-in-targeted-attacks/. Accessed 14/05/2014.

US ICS-CERT (ICS Cyber Emergency Response Team)[12] the majority (59%) of CII related cyber attacks for the fourth quarter of 2013 have been targeting the energy sector. Similarly, Symantec technical report of 2014[13] states that "the energy sector has become a major focus for targeted attacks and is now among the top five most targeted sectors worldwide". Concerns about increasing potential attacks targeting healthcare are also being recognised and addressed by government institutions[3]. The Verizon report for 2013[14] identifies a vast increase in targeted state-affiliated cyber espionage operations for sensitive information exfiltration. Mandiant "M-trends report"[15] concludes that in 2013 an increasing number of hacktivists[4] and major advanced threat actors affiliated to nation-states dominate the international cyber space. TrendMicro in their 2013 targeted attack report[16] identify the majority of attacks being directed at government (80%), IT (6%), and financial services (5%). The Report also determines the use of already well known vulnerabilities and spear-phishing e-mails as the primary method of initial attack.

The raised attention by security industry, governmental services, and infrastructure operators towards identifying vulnerabilities and countering attack actors, proves that serious action needs to be taken in order to safeguard CII dependability. Nevertheless, the adequate tendency towards increased security awareness still has major stumbling points. These involve the upkeep of legacy systems, ensuring backwards compatibility, maintaining interoperability, and being slow on introducing new security solutions or upgrades.

Chapter II of this paper estimates the characteristics and nature of actors behind advanced targeted attacks. Chapter III amasses revealed influential attacks directed at CII and specifies the incident selection criteria for further case study. Chapter IV selects and analyses case studies of major cyber incidents targeted at CII, involved actors, cyber attack technical tactics[5], vulnerabilities exploited, attack tools used, and evaluates the sophistication of the attack. Chapter V concludes this paper and suggests directions for further research.

II. ADVANCED THREAT OVERVIEW

Attacks, such as listed in table 1, on page 5, have derived the first cases of cyber weapon development, and shaped what is considered as motivated strategically targeted persistent cyber attack. The ultimate goal of such an attack could be considered as gaining a definite level of control over the target infrastructure or retrieving valuable information, therefore enabling an adversary to gain advantage over their target. Sophisticated targeted attacks as characterised in[17] have a common criteria of objectives, timeliness, resources, risk tolerance, skills and methods, actions, attack origination points, numbers involved in the attack, and sources of knowledge.

Advanced persistent threat (APT) is any sophisticated adversary engaged in information warfare in support of long-term strategic goals[18] that consistently uses tactical compromise via methods such as waterhole and spear-phishing attacks[19] to gain initial foothold in targeted information system. A typical APT has seven main stages of the execution: initial compromise, establishing a foothold, privilege escalation, internal reconnaissance, lateral movement, maintaining persistence, and mission accomplishment [20] [21], which makes it different from a regular automated attacks or cyber threats (e.g., bot-net activity, Denial-of-Service, server hacking, web defacements, hacktivism). The attack sophistication can be identified by uniqueness and advanced technical methods utilised, such as "advanced evasion techniques (AET)"[22] to circumvent network security devices.

[3] Exclusive: FBI warns healthcare sector vulnerable to cyber attacks. Reuters. http://www.reuters.com/article/2014/04/23/us-cybersecurity-healthcare-fbi-exclusiv-idUSBREA3M1Q920140423. Accessed 02/05/2014

[4] "A person [or a group of persons] who gains unauthorized access to computer files or networks in order to further social or political ends." Oxford dictionary of English

[5] An action or strategy carefully planned to achieve a specific end." Oxford dictionary of English

Client-side targeting in typical APT scenarios is feasible due to how information systems are developed (security, usability and functionality trade-off principle) in order to provide a working environment for users. This makes privileged users to be one of the weakest points of the network security, susceptible to targeted social engineering attacks. Network host-based egress defences typically are weaker with less strict perimeter policies being implemented for outgoing connections[6], allowing a more successful reverse command and control connection initialisation from within the network.

Security reports describe increased activity of cyber mercenary teams such as IceFog APT "hit-and-run" team[23] and Hidden Lynx[24], named as "hackers for hire" for executing fast paced precision strikes using unconventional approaches for targeting their victims opposing to well-executed, long-term attacks such as "Comment Crew" (i.e. APT1, China's PLA Unit 61398)[25] or a hacktivist group "Syrian Electronic Army" claiming its ties to Syrian regime[15]. Security researchers predict an increasing trend in fast precision operation execution by cyber mercenaries.

III. CASE SELECTION CRITERIA

The targeted persistent attacks in nature differ in the execution tactics and technical characteristics from a conventional attacks which security devices and analysts are able to identify and handle. Advanced attacks, however, might rely on conventional means of attack for initial system compromise. For further activities involving lateral movement, persistence, and manipulation, actors need to employ sophisticated methods, to ensure a certain level of stealth. This is especially important in the context of CII where long-term presence and control is desired. Nonetheless, even the most sophisticated cyber attacks can have a high execution tempo for precision strikes with only a single set of goals in mind (i.e. "hit-and-run").

From a global situational viewpoint, it can be seen that the majority of advanced attacks are conflict driven. This might lead to the conclusion and attribution of these cyber attacks to be nation state executed, sponsored, or affiliated[26]. The process of attack attribution is not simple and straightforward[27], as many different aspects of pre- and attack execution time line have to be assessed and evaluated (e.g., historical, geopolitical, motivation, technical capability, and resource availability information). Nevertheless, security analysts and experts tend to give estimations on possible actors or nation states behind the attacks. The differences between technical (e.g., execution technical details and sophistication) and political (e.g., motivation, resources and geo-political situation) attribution have to be accounted for. Amassing the evidence proving ones involvement in cyber attack is extremely difficult, and can therefore be treated more as a very rough estimation. Most notably this is due to such attacks being more commonly executed as covert deception operations (i.e., "no-flag", "false-flag"), making attribution difficult or practically impossible.

Availability of the cyber attack technical information and reports from open sources has to be estimated. Because of the likely sensitive nature of incidents, especially in the case of covert CII attacks, information might be limited as defined by organisation's information disclosure policy. Regarding nation's CII, this might even be regulated by national security or state emergency authorities, therefore making the attack information public availability very limited and discrete. The delicate nature of advanced attacks have to be taken into consideration which makes potential cases to remain still undiscovered. Security company Mandiant estimates a median 229 days since initial compromise until detection[15] which indicates that a typical network security implementation is not enough. The increase in reported target cyber attack cases and operations (as seen in table 1) does not mean, that there is an actual tremendous growth within targeted cyber attacks. However, the rise can be partially explained by security industry's escalated attention towards unconventional attacks and availability of threat detection technological means (e.g., full packet

[6] Defense against Drive-By Downloads. US NSA Vulnerability Analysis and Operations Group. p.7. http://www.nsa.gov/ia/_files/factsheets/I733-011R-2009.pdf. Accessed 19/05/2014

capture, large data analysis). For this paper, advanced attack case analysis reports and bulletins, freely accessible from open sources performed by recognised security industry representatives are considered.

Table 1 lists major publicly disclosed targeted attack cases which have made a significant impact on the security of CII, dating back to around the year 2000. Some of these attacks cannot entirely be classified as technically sophisticated, but can undoubtedly be distinguished as first cases of a specific attack execution approach, therefore making them unique.

Based on the aforementioned reasoning the following criteria is derived for further technical case study selection:

1. The cyber attack target can be classified as CII;
2. Attack technical information is sufficiently available from credible open sources;
3. Report originator attributes this to advanced threat actor activity, possibly affiliated with a nation-state;
4. A set of attack methods, goals and presence longevity can be identified.

Name	Year disclosed	Scope	Target	Possible attribution
Moonlight Maze	1999	Defence and intelligence networks	US	Russia
Titan Rain	2003	Sensitive information networks	US	China
GhostNet	2009	Cyber espionage	Worldwide	China
Operation Aurora*	2010	High tech. and security industry source code repositories	Worldwide	China
Stuxnet	2010	Nuclear enrichment facilities	Iran	US
DuQu	2011	Attack framework related to Stuxnet	Worldwide	Unidentified
Night Dragon*	2011	Energy industry	Worldwide	China
Nitro	2011	Chemical industry information	Worldwide	China
RSA attack	2011	Two-factor authentication product information	RSA	Unidentified
Flame	2012	Cyber espionage	Middle East	US/Israel
Gauss	2012	Online banking	Middle East	Unidentified
Shamoon*	2012	Oil industry	Saudi Arabia	Iran
Telvent	2012	Smart grid control software	Worldwide	China
Red October	2013	Cyber espionage	Worldwide	Unidentified
MiniDuke	2013	Cyber espionage	EU and NATO counties	Unidentified
NSA PRISM	2013	Various cyber operations	Worldwide	US/UK
Ke3chang*	2013	Diplomatic cyber espionage	Europe	Unidentified
The Mask	2014	Advanced cyber espionage	Worldwide	Spain
Uroburos	2014	Unknown / Restricted environments	Unknown	Russia

* - case selected for analysis in this paper.

Table 1: Historical timeline of reported major advanced targeted attacks.

A note on critical thinking. Part of security incidents date well back and no detailed technical information is available either due to not being disclosed or preserved, or being publicly restricted for incidents targeting nation state-owned critical industries. It has to be taken into account that the case analysis reports have been prepared by major security companies, which are also important governmental contractors for a considerable number of nations worldwide. These companies might be forced, or otherwise restricted, to withhold possibly important parts on attack and execution details. A complex and obscure picture of actual incident details is present, especially regarding those conflict-driven attacks involving information warfare aspects. Therefore, to abstract as much as possible from the probably disputable nature of information provided, critical thinking is encouraged, i.e., more focused on purely technical aspects presented in case reports.

IV. CASE ANALYSIS

Based on the selection criteria presented in Chapter III, applicable incidents affecting different CII sectors are selected for further case study. One prominent case per year is chosen starting from 2010, when a distinctive increase in targeted attacks can be identified.

The initial target system compromise presents an important phase of the attack execution, allowing to acknowledge if it is technically sophisticated and advanced. The use of undisclosed vulnerabilities not known to the security industry and vendors (i.e. zero-days or 0-days), or use of a very recently identified critical vulnerabilities presents a potentially resourceful, sophisticated and well-motivated adversary. The means and approaches used to exploit identified vulnerabilities and achieve the intended aims either long- or short- term, define the level of such an attack. The tools and methods used either ready- or custom made, directly imply the adversary's advanced capabilities on persistence, stealth and comprehensive covert operation success. Overall attack sophistication level can be assessed by taking into account the technical execution characteristics, estimated damage inflicted, time until being detected, and execution characteristics (e.g., tactics, stealth, persistence, precision, and intelligence).

Taking into account the reasoning above and in order to provide a unified and comparable attack evaluation the following technical aspects are assessed:

1. Attack vectors used and vulnerabilities exploited;
2. techniques and tools utilised;
3. Sophistication of the attack.

The upcoming subsections review selected complying case reports outlining the general incident information (e.g., sector affected, estimated longevity, impact induced, attribution), similar incidents (e.g., related sector affected, akin goals targeted, or same actor), technical characteristics, and sophistication estimation based upon given evaluation criteria.

A. Operation Aurora

In 2010 Google revealed[7] that it had been attacked by an adversary targeting at least twenty "Fortune 100" companies[8]. These attacks, possibly started in mid-2009, were aimed at high profile technology companies (such as Google, Adobe, Juniper Networks, and Rackspace) being attributed to the "Elderwood project"[28] which is allegedly affiliated with China's People Liberation Army (PLA) unit 61398 (also known as APT1 or "Comment crew"). The targeted companies cannot be accounted as CII per se; however, their services and products (e.g., software and hardware) are used throughout a vast majority of industries, including CII, worldwide thereby indirectly seriously endangering their operations if adversary gets hold of software source codes, hardware blueprints, or any other proprietary intellectual property.

[7] A new approach to China. Google official blog. http://googleblog.blogspot.ie/2010/01/new-approach-to-china.html#!/2010/01/new-approach-to-china.html. Accessed 05/05/2014

[8] Fortune 500 Magazine. http://money.cnn.com/magazines/fortune/fortune500/. Accessed 20/05/2014

"Operation Aurora" used Microsoft Internet Explorer vulnerability MS10-002[9] which at that time was known by Microsoft, but not publicly disclosed as it was not observed to be exploited "in-the-wild". Therefore no mitigation was available making the attack to be undetected for several months and allowing adversaries to inflict severe damage to technology companies. A targeted spear-phishing campaign was executed against several employees by delivering a message appearing to be originating from someone they trusted[29]. The message contained a link to a rigged web site hosting the attack code (e.g., drive-by exploitation)[30]. Internet Explorer "Aurora" vulnerability was just the entry point to drop (i.e. deploy) Hydraq trojan on the target systems. An in-depth analysis[31] reveals that Hydraq trojan was a sophisticated malware[10] which, upon successful compromise, allowed attackers to have full machine control, monitor activity, spread further in the network, gather and exfiltrate sensitive proprietary information via covert command and control (CnC) channels.

> ... NO MITIGATION WAS AVAILABLE MAKING THE ATTACK TO BE UNDETECTED FOR SEVERAL MONTHS AND ALLOWING ADVERSARIES TO INFLICT SEVERE DAMAGE TO TECHNOLOGY COMPANIES ...

The NSS "Aurora" vulnerability test report[29] states that "[d]isclosure of Operation Aurora attack elevated the public's awareness of cyber-warfare to an unprecedented level"; however, the attack approaches and methods were not new to the security community. Nevertheless, it is still estimated to be orchestrated and highly sophisticated[11] due to undisclosed vulnerabilities used and multiple technical methods implied (e.g., obfuscation, encryption, covert communication channels) in a single attack execution scenario.

An equally critical attack was directed at Schneider Electric subsidiary company Telvent – a major provider of ICS control devices and management software worldwide. Telvent in 2012 issued a warning[12] to customers on potential hacker activity, breaching their security and gaining access to the network and core OASyS SCADA project files, a product that helps energy firms mesh older IT assets with more advanced smart grid technologies. The attack also had the potential to compromise remote customer support access endangering a very wide ICS sector. Security company executed analysis of involved tools and malware names attributed this attack to APT1.

B. Night Dragon

In 2011 McAfee released a detailed technical white paper regarding discovered coordinated cyber attacks conducted against the global energy industry[32]. McAfee named this attack "Night Dragon" as they consider these attacks to be originating primarily from China. The goal of the attack is believed to be sensitive propriety information extraction regarding the energy sector such as competitive operations, project-financing information, oil and gas field bids, development plans, and SCADA data.

Initial breach of the network was achieved via external web server SQL injection, client side targeting

[9] MS10-002 Microsoft Internet Explorer "Aurora" Memory Corruption. Rapid7. http://www.rapid7.com/db/modules/exploit/windows/browser/ms10_002_aurora. Accessed 20/05/2014

[10] "Software which is specifically designed to disrupt or damage a computer system." Oxford dictionary of English

[11] Google Hack Attack Was Ultra Sophisticated, New Details Show. Wired. http://www.wired.com/2010/01/operation-aurora/. Accessed 19/05/2014

[12] Chinese Hackers Blamed for Intrusion at Energy Industry Giant Telvent. Krebs on Security. http://krebsonsecurity.com/2012/09/chinese-hackers-blamed-for-intrusion-at-energy-industry-giant-telvent/. Accessed 05/05/2014

(e.g., e-mails, drive-by-exploits, trojan dropper), and mobile user (e.g., laptops, VPN access) attacks. The primary attack method comprised variety of ready available remote access tool-kits (RATs), customisable trojan development kits, and typical system administration tools. Security researchers identified that used tools could be easily downloadable from hacker websites (e.g., rootkin.net.cn) originating from China. After gaining a foothold in the target infrastructure attackers employed passive network monitoring to harvest authentication credentials for lateral movement. Custom-generated RATs were employed to spread further in the network by using gathered administrative credentials and to establish a persistent infiltration channel into compromised companies.

The usage of ready made hacker tools and RAT development tool-kits makes this attack relatively unsophisticated. However, the characteristics of presence and actions done in the infiltrated network seemed as typical remote system administration and so it didn't raise any suspicion. The deployed malware was customised and did not have any further spreading or exploitation features, besides providing only remote access, therefore evading detection as malicious by anti-virus products. Although the attack cannot be classified as advanced or highly sophisticated, the tactics employed allowed an attack campaign to be successfully ongoing for at least two years, making it very successful and damaging to the targeted industry.

Similar in execution was the "Nitro" attack in mid-2011 targeting advanced chemical industry "Fortune 100" companies[13] aimed at intellectual property collection (e.g., advanced military-grade materials, research and development, designs, formulas, manufacturing processes). Multiple companies were struck by a targeted social engineering attack with seemingly generic security related e-mails which contained a common PoisonIvy back-door trojan as an attachment. Once taking initial control over computers it harvested administrative credentials to spread further into network. Adversary with a given pseudonym "Covert Grove" originating from China, was able to maintain at least a few months' presence during which it gained access to sensitive proprietary information.

C. Shamoon

Initial analysis reports by Symantec[14] and Kaspersky[15], followed by US ICS-CERT advisory[16] in mid-2012, disclosed information regarding a malware targeting directly Saudi Arabian oil company – "Saudi Aramco". This incident can be considered as one of the major targeted cyber sabotage attack cases rendering thousands of company computers inoperable and destroying intellectual property. A group from Iran called "Cutting Sword of Justice" claimed responsibility for this attack.

It is assumed to be spread by involved insiders[17] using removable media; however, there is no tangible evidence proving these allegations. US ICS-CERT security bulletin[33] identified that "Shamoon" had three main components intended for information gathering, reporting and destruction. After initial infection, "Shamoon" spread via network shares infecting other computers running Microsoft Windows operating system across the whole company's business network. However, its presence has not been identified in ICS/

[13] The Nitro Attacks Stealing Secrets from the Chemical Industry. Symantec. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf. Accessed 05/05/2014

[14] The Shamoon Attacks. Symantec blog. http://www.symantec.com/connect/blogs/shamoon-attacks. Accessed 05/05/2014

[15] Shamoon The Wiper. Secure List. http://www.securelist.com/en/blog/208193834/Shamoon_The_Wiper_further_details_Part_II. Accessed 05/05/2014

[16] Joint Security Awareness Report (JSAR-12-241-01B): Shamoon/DistTrack Malware. US DHS ICS-CERT. http://ics-cert.us-cert.gov/jsar/JSAR-12-241-01B. Accessed 05/05/2014

[17] Shamoon was an external attack on Saudi oil production. Info Security. http://www.infosecurity-magazine.com/view/29750/shamoon-was-an-external-attack-on-saudi-oil-production/. Accessed 20/05/2014

SCADA networks where it would have a very highly destructive potential, as many devices, such as Human-Machine-Interface (HMI) and control appliances, also run the same operating systems. "Shamoon" had a hard-coded kill-timer set for a specific date and time which triggered the "Wiper" module to raze information and disable computers. The highly destructive "Wiper" module, being a plausible copycat of Flame malware[18], utilised a secure wiping method to destroy electronic documents found in specific folders, Master Boot Record (MBR) and partition tables on the hard-drive.

No high sophistication can be attributed to this attack as the security industry called it "quick and dirty"[19] due to the low quality of self-developed tools. Nevertheless, the devastative impact imposed by this attack proves the crucial need for system monitoring, security awareness, and incident response especially considering the possibility of insider threat involvement.

The "Stuxnet" malware[20], discovered in 2010, can be acknowledged as the most outstanding case for cyber sabotage being particularly aimed at subverting Iran's nuclear programme. This certainly can be classified as the first known case of highly sophisticated cyber weapon development, employing multiple zero-day vulnerabilities and stealth techniques. As well as influencing such cyber weapon development open framework as "Duqu"[34].

D. Ke3chang

In 2013 FireEye released a cyber espionage operation "Ke3chang" analysis report[35] stating that this threat actor is considered to be very selective about its targets, having since late 2011 directed attacks against European ministries of foreign affairs and embassies. Security experts at FireEye believe that this actor has been active since at least 2010 and has targeted different sectors (e.g., aero-space, energy, government, high-tech, manufacturing). Twenty-two CnC servers have been identified to be involved in operation "Ke3chang" with majority of them being located in US, China and Hong Kong. FireEye monitored activity on one of the CnC servers for a brief time window and collected evidence regarding targeted attacks against European ministries and lateral movement within compromised networks. Security experts, by analysing malware artefacts, CnC servers and tools, found linguistic clues leading to the probability that attackers were operating from China. However, the exact identities of the adversaries remain unknown.

The initial strike started with a rigorously crafted targeted social engineering attack by using breaking news themed topics (e.g., London Olympics, Syria crisis, Carla Bruni naked pictures, European security and defence, McAfee security report). Adversaries sent out spear-phishing e-mails with malware attachments or a link to a malicious download. To hide the extensions of attached malevolent files attackers used a simple and common Unicode Right-to-Left-Override (RTLO) technique to obfuscate file names. Very recently published exploits and vulnerabilities for widely used software (e.g., Java, MS office, Adobe PDF reader) were used to compromise the computer once malicious attachment had been executed. It has been identified by FireEye that attackers tested malware on virtual machines prior to launching it against intended targets. Once inside, attackers followed a predetermined plan of scanning the systems and gathering authentication credentials for lateral movement.

Sophistication of this attack can be designated as intermediate due to initial infection vector being very simple as it relies on user interaction to launch the malicious file which employs recently disclosed vulnerabilities. However, for attack approach being nothing astonishingly new and uncommon it was

[18] Shamoon Malware Might Be Flame Copycat. Dark Reading. http://www.darkreading.com/attacks-and-breaches/shamoon-malware-might-be-flame-copycat/d/d-id/1105917?. Accessed 20/05/2014

[19] Shamoon cyberweapon the work of amateurs, Kaspersky says. Tech World. http://news.techworld.com/security/3381077/shamoon-cyberweapon-the-work-of-amateurs-kaspersky-says/. Accessed 05/05/2014

[20] The Real Story of Stuxnet. IEEE Spectrum. http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet. Accessed 05/05/2014

successful due to well-planned targeted spear-phishing campaigns and by exploiting known vulnerabilities despite security patch existence. Testing exploits before being launched at intended target leads to plausible conclusions that adversaries possessed some prior intelligence information regarding the target system inner architecture acquired either by reconnaissance or other rigorous sources. This incident clearly shows that common attack approaches still work very well, privileged system users can be deemed as the weakest link, and most administrators are negligent at deploying software security patches in a timely manner.

Cyber espionage can be identified as one of the most common reported targeted attacks, and includes such major cases as "GhostNet"[21] revealed in 2009, "Red October"[22] disclosed in 2013, US NSA (National Security Agency) massive clandestine data-mining program PRISM[23] made public in 2013 by E.Snowden, "The Mask"[36] published in 2014, and "Uroburos"[37] reported in 2014.

CONCLUSIONS AND FURTHER WORK

The threat implied by advanced adversaries is real and targeted attacks have a tendency to increase. It can be observed that a noticeable upsurge began around 2010 which could suggest that cyber means were identified as a relatively feasible approach when dealing with impacts inflicted by global economic recess, allowing to gather competitive and proprietary information. This could be described as the dawn of the "golden age of cyber espionage". Technological advancement and methods available enable to extend presence in cyber space and define attack vectors in context of conflicts between states, by utilising technical capabilities leading to weaponisation of cyber means and virtualisation of forces. Nation state affiliated actors are becoming more determined, sophisticated and resourceful by investing resources in cyber capability development, such as amassing cyber armed forces or establishing powerful server farms solely dedicated to software zero-day detection.

As CII is becoming more aware of targeted threats, it is still slow on implementing security measures due to legacy systems, operational procedures, and budget constraint considerations. From reviewed case studies in this paper it can be determined that major vulnerabilities are faced due to loose operational requirements, lack of user security awareness, and inadequate information system security life-cycle implementation (e.g., maintenance, patching, security-in-depth, auditing, situational awareness). Such high profile sectors should promptly prepare against imminent targeted attacks, and advance security beyond focusing purely on safety, availability and integrity considerations, by ensuring continuous situational awareness and consistent incident response. Critical industries can benefit from utilising

> ...CRITICAL INDUSTRIES CAN BENEFIT FROM UTILISING PASSIVE DETECTION SOLUTIONS WHICH MIGHT REDUCE THE TIME NEEDED TO DETECT ADVERSARY PRESENCE, OR PROVIDE VALUABLE FORENSIC INFORMATION IN THE AFTERMATH OF A SECURITY BREACH ...

[21] China's global cyber-espionage network GhostNet penetrates 103 countries. The Telegraph. http://www.telegraph.co.uk/news/worldnews/asia/china/5071124/Chinas-global-cyber-espionage-network-GhostNet-penetrates-103-countries.html. Accessed 24/05/2014

[22] Operation "Red Ocotber". Securelist. http://www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies. Accessed 05/05/2014

[23] "PRISM, Tempora, XKeyscore: What Is It? " Software Informer. http://articles.software.informer.com/prism-tempora-xkeyscore-what-is-it.html. Accessed 05/05/2014

passive detection solutions (e.g., full packet capture, deep packet inspection, big data analysis) which might reduce the time needed to detect adversary presence, or provide valuable forensic information in the aftermath of a security breach.

It is obvious that the security industry and vendors have created a new business model around APT niche, using it as a buzzword for developing and promoting expensive products and services. Currently, every self-respecting security vendor is doing at least something APT related to promote their visibility, increase income, and to be considered as a serious player in a huge security competitive market. However, this field saturation enhances targeted persistent threat identification, rises security awareness, promotes attack information disclosure and sharing, and incident handling collaboration.

Further research topics can be directed at evaluating attack vectors and tactics of covert network infiltration operations for comprehensive red-teaming and active cyber defence purposes. Also paying attention to vulnerability implications in IPv6 addressing implementations, extensions, and IPv4 to IPv6 transition workarounds, which may allow network security circumvention and covert infiltration. ■

REFERENCES

[1] The Council of the European Union, “Council directive 2008/114/ec on the identification and designation of european critical infrastructures and the assessment of the need to improve their protection,” 2008.

[2] US 107th Congress, “Public Law 107“56,” 2001.

[3] J. Stamp, J. Dillinger, W. Young, and J. DePoy, “Common vulnerabilities in critical infrastructure control systems,” tech. rep., Sandia National Laboratories, 2003.

[4] N. I. o. S. Computer Security Division, Information Technology Laboratory and Technology, *NIST Special Publication 800-82. Guide to Industrial Control Systems (ICS) Security.* Gaithersburg: NIST, U.S. Department of Commerce, 2011.

[5] E. Knapp and J. Langill, *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems.* Elsevier Science, 2011.

[6] R. E. Johnson III, “Survey of SCADA security challenges and potential attack vectors,” in *International Conference for Internet Technology and Secured Transactions,* pp. 1–5, 2010.

[7] N. Villeneuve, “Trends in Targeted Attacks,” tech. rep., Trend Micro Inc., October 2011.

[8] L. Marinos and A. Sfakianakis, “ENISA Threat Landscape: Responding to the Evolving Threat Environment,” tech. rep., ENISA, September 2012.

[9] L. Marinos, “ENISA Threat Landscape, Mid-year 2013,” tech. rep., ENISA, September 2013.

[10] M. E. Luallen, “SANS SCADA and Process Control Security Survey,” tech. rep., SANS Analyst Program, February 2013.

[11] K. Wilhoit, “Who’s really attacking your ics equipment?,” tech. rep., Trend Micro Inc., 2013.

[12] National Cybersecurity and Communications Integration Center, “ICS-CERT Monitor,” tech. rep., US Dep. of Homeland Security, December 2013.

[13] C. Wueest, “Targeted Attacks Against the Energy Sector,” tech. rep., Symantec Corp., January 2014.

[14] Verizon, “2014 Data Breach Investigations Report,” tech. rep., Verizon, 2014.

[15] M-Trends, “2014 Threat Report: Beyond the Breach,” tech. rep., Mandiant, 2014.

[16] TrendLabs, “Targeted Attack Trends 2H 2013 Report,” tech. rep., TrendMicro inc., 2014.

[17] S. Bodmer, M. Kilger, G. Carpenter, and J. Jones, *Reverse Deception: Organized Cyber Threat Counter-Exploitation,* ch. 1. McGraw-Hill Companies, Inc, 2012.

[18] Fortinet, “Threats on the Horizon: The Rise of the Advanced Persistent Threat,” solution report, Fortinet Inc., 2013.

[19] A. Cox, “The Cyber Espionage Blueprint: Understanding Commonalities In Targeted Malware Campaigns,” RSA FirstWatch Intelligence Report, EMC Corp., 2013.

[20] TrendLabs, “Lateral Movement: How Do Threat Actors Move Deeper Into Your Network? ,” tech. rep., TrendMicro inc., 2013.

[21] TrendLabs, “Data Exfiltration: How do Threat Actors Steal Your Data? ,” tech. rep., TrendMicro inc., 2013.

[22] O. P. Niemi and A. Levomäki, “Evading Deep Inspection for Fun and Shell,” *Black Hat USA*, July 2013.

[23] Kaspersky Lab Global Research and Analysis Team, “The ICEFOG APT: A Tale of Cloak and Three Daggers,” attack analysis report, Kaspersky Lab ZAO, 2013.

[24] S. Doherty, J. Gegeny, B. Spasojevic, and J. Baltazar, “Hidden Lynx - Professional Hackers for Hire,” security response, Symantec Corp., 2013.

[25] Mandiant Intelligence Center, “APT1: Exposing One of China’s Cyber Espionage Units,” report, Mandiant Corp., 2013.

[26] M. N. Schmitt, “Cyber activities and the law of countermeasures,” in *Peacetime Regime for State Activities in Cyberspace* (K. Ziolkowski, ed.), ch. 3, pp. 659–688, Tallinn: NATO CCD COE, 2013.

[27] International Group of Experts at the invitation of NATO CCD COE, *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge University Press, 2013.

[28] G. McDonald and G. O’Gorman, “The elderwood project,” tech. rep., Symantec corp., 2012.

[29] NSS Labs, “Vulnerability-based protection and the Google “Operation Aurora” attack,” tech. rep., NSS Labs Inc., March 2010.

[30] B. E. Binde, R. McRee, and T. J. O’Connor, “Assessing outbound traffic to uncover advanced persistent threat,” tech. rep., SANS Technology Institute, May 2011.

[31] Z. Ferrer and M. C. Ferrer, “In-depth Analysis of Hydraq,” tech. rep., CA Internet Security Business Unit, 2010.

[32] McAfee Labs, “Global Energy Cyberattacks: Night Dragon,” tech. rep., McAfee Inc., February 2011.

[33] National Cybersecurity and Communications Integration Center, “ICS-CERT Monitor,” tech. rep., US Dep. of Homeland Security, September 2012.

[34] B. Bencsath, G. Pek, L. Buttyan, and M. Felegyhazi, “Duqu: A Stuxnet-like malware found in the wild,” tech. rep., Laboratory of Cryptography and System Security, October 2011.

[35] N. Villeneuve, J. T. Bennett, N. Moran, T. Haq, M. Scott, and K. Geers, “Operation ke3chang: Targeted attacks against ministries of foreign affairs,” tech. rep., FireEye inc., 2013.

[36] Kaspersky Lab, “Unveiling Careto - The Masked APT,” tech. rep., Kaspersky Lab ZAO, February 2014.

[37] G Data SecurityLabs, “Uroburos: Highly complex espionage software with Russian roots,” tech. rep., G Data Software AG, February 2014.

ABOUT THE AUTHOR

Bernhards Blumbergs is a Researcher at NATO Cooperative Cyber Defence Centre of Excellence, Technology branch. He is a certified exploit researcher and advanced penetration tester (GXPN), and a team member of the Information Technology Security Incident Response Institution of the Republic of Latvia (CERT.LV). He has a strong military background, targeted at developing, administering and securing wide area information systems. Mr.Blumbergs is also a Cyber Security PhD student at Tallinn Technical University, with his research focusing on methods for network security mechanism evasions.