On the Top Threats to Cyber Systems

Houssain Kettani[1], Polly Wainwright[1,2]
[1]The Beacom College of Computer and Cyber Sciences, Dakota State University, Madison, South Dakota, USA
[2]Department of Computing and Information Sciences, Valparaiso University, Valparaiso, Indiana, USA
e-mail: Houssain.Kettani@dsu.edu, Polly.Wainwright@dsu.edu

***Abstract*—The technological innovation of cyber systems and increase dependence of individuals, societies and nations on them has brought new, real and everchanging threat landscapes. In fact, the threats evolving faster than they can be assessed. The technological innovation that brought ease and efficiency to our lives, has been met by similar innovation to take advantage of cyber systems for other gains. More threat actors are noted to be sponsored by nation-states and the skills and capabilities of organizations to defend against these attacks are lagging. This warrants an increase in automation of threat analysis and response as well as increased adoption of security measures by at-risk organizations. Thus, to properly prepare defenses and mitigations to the threats introduced by cyber, it is necessary to understand these threats. Accordingly, this paper provides an overview of top cyber security threats in together with current and emerging trends. The analyses include general trends in the complexity of attacks, actors, and the maturity of skills and capabilities of organizations to defend against attacks. Top threats are discussed with regard to instances of attacks and strategies for mitigation within the kill chain. A brief discussion of threat agents and attack vectors adds context to the threats.**

Keywords-cyber security; cyber threats; analysis; kill chain; mitigation

I. INTRODUCTION

The European Union Agency for Network and Information Security (ENISA) is a center of expertise in Europe that was formed in 2004 and is located in Greece with its seat in Heraklion, Crete and an operational office in Athens. Within that charge, ENISA seeks to create a culture of cyber security by assisting the European Union (EU) member states and organizations to meet security regulations, through involvement in current and future legislation, and by analyzing and disseminating cyber threat intelligence (CTI). To this end, ENISA holds events such as CTI-EU, a workshop for all European stakeholders in cyber threat intelligence, and the Cyber Europe Conference. In 2018, ENISA published the CTI Maturity Model for the purpose of identifying gaps in Threat Information Sharing (TIS) tools. The ETL 2018 is the seventh edition of the annual Threat Landscape report [2]. In addition, ENISA improved readability and usability of its report and has launched a web application containing information on the top fifteen cyber threats encountered in the previous calendar years. The application is available at [1] and offers intuitive navigation through relevant information objects.

The ETL 2018 was published for the purpose of analyzing the top fifteen cyber security threats which occurred between December 2017 and December 2018. The document was written in collaboration with the European Defense Agency (EDA), Computer Emergency Response Team for EU (CERT-EU), and the European Cyber Crime Center (EC^3), and in the context of existing EU policy such as the Cyber Security Strategy of EU and the Network and Information Security (NIS) Directive. General trends in the analysis include an increase in the complexity of attacks. There was advancement in the hiding of attacks. Attacks became multipurpose and. Monetization of cyber-crime through cryptocurrency increased. More actors are noted to be sponsored by nation-states. The skills and capabilities of organizations to defend against these attacks are lagging. The ETL describes the state-of-play in CTI as constantly evolving with threats evolving faster than they can be assessed. Further, ENISA notes a maturing in the strategy and infrastructure of CTI and a need for the sharing of CTI. Goals include automation of CTI analytics, cyber resilience, and an increase to CTI skills and capabilities leading to a multi-layered defense that makes attacks costly and inefficient [1].

The taxonomy of threats has evolved since the ETL inception. Earlier editions of the ETL listed targeted attack, for example, as separate category of threat. Now, a specific targeted attack might be classified as either phishing or a Denial of Service (DoS) attack. Cyber espionage did not appear as a unique threat until the ETL 2015 edition, coinciding with the increase in state sponsored attacks. Categories of threat continue to overlap. Ransomware, for example, is currently evaluated as a separate threat, even though it is also malware. Mitigation of all cyber threats is through disruption of the computer security kill chain. The ETL uses the Lockheed Martin Corporation's intrusion kill chain model [7]:

1. Reconnaissance: choose and research target and its vulnerabilities
2. Weaponization: create a malware weapon tailored to the vulnerability
3. Delivery: transmit the weapon to the target
4. Exploitation: execute malware code to exploit vulnerability
5. Installation: access point, "back door" is installed for use by intruder
6. Command and control: malware allows intruder access and control of target.

978-1-7281-3322-5/19/$31.00 ©2019 IEEE

7. Actions on objectives: action is taken to achieve attack objective

In the next section, we discuss the evolution of the landscape of cyber threats in this decade and sources of the threats. In Section III we analyze and explain each of the top cyber threats per ETL reports and present concluding remarks in Section IV.

II. Evolutions in the Threat Landscape

The top fifteen threats in 2018 were in this order: Malware, Web-Based Attacks, Web Application Attacks, Phishing, Denial of Service (DoS), Spam, Botnets, Data Breaches, Insider Threat, Physical Manipulation/ Damage/Theft/Loss, Information Leakage, Identity Theft, Cryptojacking, Ransomware and Crypto Espionage. The annual change in ranking of each cyber threat since 2012 is summarized in Table I as compiled from the annual ETL reports [2-6]. In 2018, Cryptojacking was introduced to the list and exploit kits was dropped [2]. The latter was dropping constantly in rank each year since it was at the fourth place in 2012 and 2013. Some of the top cyber threats belong to same distinct threat category. For example, Ransomware and Cryptojacking are a specialization of the threat type Malware. Likewise, Identity Theft is a special category of Data Breach. Nonetheless, the overlapping threats are handled separately because the threat is launched by special malicious artefacts.

The top fifteen threats in 2017 have been the same top fifteen threats since 2014, although some order and trending have changed [1-6]. The top three threats have remained consistent since 2012, namely Malware, Web-based and Web Application Attacks. Insider threat was not recognized as a distinct type of threat until 2013 while Cyber Espionage was not recognized until 2014. Position ranking was based on the number of incidents, impact, and relationship to other threats. A trend up indicates an increase in incidents but perhaps not an increase in rank. Table 1 shows the increased ranks of Phishing and Spam attacks as well as the decreased rank of Exploit Kit attacks which eventually exited the top fifteen threat list in 2018. The analyzed threat data are in the public domain, specifically from the Open Source Threat Intelligence Platform & Open Standards for Threat Information Sharing [8].

In addition to analyzing the type of threat, it is important to understand the source of the threat. The threats begin with humans and human motivation. The individual or organization must then gain access to the targeted computer or network. As pointed out in [1,2], threat sources consist of two entities:

A. Threat Agents

Threat agents are the actors, individuals or organizations, who can create a threat. Often threat agents try to mask their identity and alliances by claiming identification with another group. This masquerading can be accomplished through fake news and social media campaigns. In descending order, the most common categories of threat agents are cyber-criminals, insiders, nation-states, hacktivists, cyber-fighters, and terrorist groups.

B. Attack Vectors

Attack vectors are the path or means by which a threat agent gains access to a computer or network for the purpose of malicious activity. There is a large taxonomy of attack vectors. A short list includes the human element, web and browser attacks, internet exposed threat, mobile app stores, and malicious USB drives.

TABLE I. Annual Change in Ranking of the Top Fifteen Threats According to ETL

Top Threats	Year						
	2018	2017	2016	2015	2014	2013	2012
Malware	1	1	1	1	1	2	2
Web-Based Attacks	2	2	2	2	2	1	1
Web Application Attacks	3	3	3	3	3	3	3
Phishing	4	4	6	8	7	9	7
Denial of Service	5	6	4	5	5	8	6
Spam	6	5	7	9	6	10	10
Botnets	7	8	5	4	4	5	5
Data Breaches	8	11	12	11	9	12	8
Insider Threat	9	9	9	7	11	14	-
Physical Manipulation/ Damage/Theft/Loss	10	10	10	6	10	6	12
Information Leakage	11	13	14	13	12	13	14
Identity Theft	12	12	13	12	13	7	13
Cryptojacking	13	-	-	-	-	-	-
Ransomware	14	7	8	14	15	11	9
Cyber Espionage	15	15	15	15	14	-	-
Exploit Kits	-	14	11	10	8	4	4

III. Top Cyber Threats

An analysis of the top threats shows an increase in the incidences of attack and attack tactics as well as advancements in defense. Ransomware attacks were a dominant threat. There was a massive increase in phishing attacks. In the sequel we describe each of these cyber threats in order of their ranking in 2018 and as described in [1,2].

A. Threat 1: Malware

Malware is software with a malicious intent to destroy a computer, server, or network. It causes harm or acts against the interests of the user. Common malware are viruses, worms, Trojan horses, spyware, and ransomware. Malware remained the top cyber threat since 2014. In 2017, over four million samples of malware are detected each day by malware protection firms [3]. An increase in malware attacks is escaladed by ad wars and hijacked browser sessions. Click-less infections, which do not depend on user interaction for deployment, are on the rise. The ETL

describes 2017 as being highly mediatized with regard to leaked exploits. EternalBlue was one of several exploits attributed to the US National Security Agency (NSA) to be leaked by hackers. EternalBlue exploits a vulnerability in older versions of Microsoft Windows operating system and lead to a number of ransomware outbreaks. EternalBlue also serves as an example of the upward trending state intelligence development of malware. Noteworthy malware attacks of 2017 were WannaCry and NotPetya, both of which had a ransomware payload and exploited the EternalBlue vulnerability. The WannaCry ransomware attack lasted only a few days but is estimated to have resulted in hundreds of millions of dollars in damage in the US, Japan, and Australia. WannaCry was attributed to North Korea. Malware's roles in the kill chain are installation of the threat, command and control of the device, and execution of harmMitigation of malware includes malware detection on all in-bound and out-bound channels and sufficient security policies for response. In 2018, the attack vectors for detected malware were 92% by email compromise and 6% by web and browser.

B. Threat 2: Web-Based Attacks

Web-Based Attacks make use of web-enabled systems such as browsers, webpages, and content managers. They are the most common threat for financial attacks and remained the second top cyber threat since 2014. As a widely used content manager, WordPress is particularly vulnerable. Drive-by download attacks involve malicious JavaScript and do not require action from the user. Malicious URLs use Blackhat Search Engine Optimization (SEO) to attract targets. A web-based attack's roles in the kill chain are the creation, delivery, and execution of a payload targeted to a particular vulnerability. Mitigation includes patching vulnerabilities and web traffic filtering.

C. Threat 3: Web Applicaton Attacks

Web application attacks take advantage of Application Programming Interfaces (APIs) which are exposed and open. Government and financial institution apps are particularly popular targets. SQL injection can be used to retrieve passwords stored in databases. Web Application Attacks remained the third top cyber threat since 2012. Kill chain phases for web application attacks are reconnaissance for choosing targets and identifying vulnerabilities, exploitation of the vulnerabilities, and installation of access points which lead to command and control of the device. Mitigation includes policies for secure app development and for the authentication and validation of mechanisms.

D. Threat 4: Phishing

Phishing uses social engineering to lure targets into revealing sensitive information. Spearfishing targets people within a specific organization. Often disguised as legitimate organizations, one million new phishing websites are created each month. Phishing's roles in the kill chain are reconnaissance, weaponization, and delivery. The human element is the weak link in the Phishing Attack. In fact, in 2018 over 90% of malware infections and 72% of data breaches in organizations originate from Phishing Attacks [2]. Mitigation includes the education of potential targets about fake email, random clicking, and oversharing of personal information.

E. Threat 5: Denial of Service Attacks

Denial of Service (DoS) attacks occur when machine or network resources are made unavailable to their intended users by disrupting service, usually by flooding the network with requests, often from botnets. The DoS is particularly damaging to organizations that rely on a web presence. Distributed Denial of Service (DDoS) attacks strike a target from many sources and are harder to stop. Pulse wave DDoS attacks come in short bursts on multiple targets and can last for days. The DoS attacks can be used to mask other attacks. In 2017, the Mirai Internet of Things (IoT) botnet was responsible for the largest DoS attack in history. The attack lent credence to warnings about IoT vulnerabilities and led to massive increases in security of IoT devices. These new measures led to some decrease in botnet activity and in DoS attacks, but the overall trend of DoS attacks is still increasing. Kill chain phases for a DoS attack are reconnaissance, weaponization, command and control of device, and execution of harm. Mitigation includes a reaction plan, Internet Service Providers (ISPs) with DoS protection, and organization specific protections such as firewalls and access control lists.

F. Threat 6: Spam

Spam is flooding users with unsolicited messages by email and messaging technologies. It comprised close to half of total email volume or nearly 300 billion to 450 billion emails per day in 2018 [2]. Most spam comes from botnets, 80% of which are thought to have been created by a group of about 100 spam gangs. In spite of the uncovering of several large botnets, spam attacks are still upwardly trending. Spam is the main means of malware delivery through attachments and URLs, although most spam is simply advertisement without malware. The roles of spam in the kill chain are weaponization and delivery. Mitigation is through spam filters and user education.

G. Threat 7: Botnets

Botnets consist of several Internet connected devices, each device running a bot, or script, that performs a simple task at high repetition. The IoT botnets were the second most important threat of 2017, responsible for an enormous DoS attack. Approximately 8.4 million new devices were added to the Internet in 2017. A large percentage connected devices are considered to be vulnerable. When such a device is compromised, it can become part of a botnet. There is concern that virtual machines can become part of botnets. Fewer than expected DoS botnet attacks occurred in 2017, but the fear is that the focus of botnets has turned to ransomware. The kill chain phase of botnets is command and control of the device. Mitigation is through application and network firewalling and traffic filtering.

H. Threat 8: Data Breach

Data Breach is the loss of data that can only be discovered after the fact. It is not a threat but the result of a successful attack. Data breaches are likely more prevalent than known. A high number of breaches result from stolen or weak passwords and user credentials continue to be sold on the dark web. Breaches through espionage can be part of a nation-state cyber-attack; however, 61% of data breach victims are small companies and 35.4% are in the healthcare sector. The EU's General Data Protection Regulation (GDPR) is intended to have an impact on careless breaches through repercussions. In the US, Equifax's breach of nearly 150 million customers' personal and financial records in 2017 resulted in lawsuits and government investigation. In addition to penalties, data breaches are avoided by preventing cyber threats. Mitigation includes encryption and reduction of access rights.

I. Threat 9: Insider Threat

Insider threat is the harm caused by an organization's insider with authorized access. The harm can be unintentional. This threat is thought to be on the rise but losses are hard to quantify so the threat is deprioritized. Breaches are most commonly caused by high level managers and outside contractors rather than non-managerial employees. In fact in 2018, 77% of the companies' data breaches are caused by insiders. Healthcare is a particular target with 59% of breached records resulting from insider threat. Insider threat involves all positions on the kill chain. User awareness is the most useful mitigation, in addition to segregation of duties and limiting access to data.

J. Threat 10: Physical Damage and Loss

Physical damage and loss of computers and equipment can result in data breaches. Encryption would solve the data breach problem, but only 43% of reporting organizations use encryption in 2018. Threat is more prevalent with IoT and mobile devices as device losses count for around half of all breaches in 2018. Additional examples of physical threat include Automatic Teller Machine (ATM) drilling in which a drilled hole near the PIN pad allows for wired access and control of the machine. Theft of devices for their valuable components used to be limited to copper wire but now includes back up batteries in cell towers. In addition to encryption, mitigation includes asset inventory.

K. Threat 11: Information Leakage

Information Leakage is a breach caused not by a direct attack but from unsecured data. Mobile devices make such breaches easier. Information leakage is the usually the result of human error, often an insider action or failure. However, information can also be leaked through coding errors, particularly on mobile devices. In fact, unintended disclosure is the profound reason for Information Leakage in 2018 and human error is the most crucial factor for data disclosure [2]. In 2017, a navigation app installed on many Android devices contained a coding error that allowed hackers to obtain hardcoded credentials for text messaging. In 2018, information collected by the mobile fitness tracking and sharing app Strava has highlighted the locations of secret US military bases worldwide.

L. Threat 12: Identity Theft

Identity Theft is a cyber threat in which the attacker obtains information about a person or computer system for the purpose of impersonating the target. Like a Data Breach, Identity Theft is the result of a successful attack. In the UK, identities were stolen at the rate of 500 per day in 2017. Personal and credit card data sell for as little as $10 on the black market. Yet most individuals report that they have few worries about identity theft. Top threats include skimmers on credit card devices, dumpster diving for hard copy personal information, phishing, hacking, and telephone impersonators. Mitigation includes protection of documents, strong privacy settings on social media, password protection on devices, and care when using public WiFi.

M. Threat 13: Cryptojacking

Cryptojacking (also known as Cryptomining) is a new term that refers to the programs that use the victim's device processing power to mine cryptocurrencies such as Bitcoin, without the victim's consent. It is a type of Malware and unlike Ransomware, the attacker is more focused on assuming the control of the machine's computational power and producing currency units indefinitely, than being paid a ransom amount once. Cryptojacking made it to the top fifteen cyber threat list in 2018. The number of victims was around half million per month in 2018.

N. Threat 14: Ransomeware

Ransomware is Malware that encrypts files or locks down a system until the target pays the actor to remove the restrictions. In the case of wipeware, the encryption is never removed. Twenty percent of organizations reported that even after paying the ransom, they did not get back their data. Ransomware as a Service (RaaS) allows cybercriminals easy entry to ransomware attacks by providing a complete set of launch tools for less than $400 on the dark web. Ransomware ranking in the ETL Top fifteen cyberthreat list decreased significantly from seventh place in 2017 to fourteenth place in 2018 due to the shifting of focus by attackers to cryptojacking. In the latter, a computer is invaded in a way similar to ransomware, but instead of demanding a ransom, a malicious software is installed to start cryptocurrency mining without the computer owner's noticing. However, over 85% of the Malware targeting medical devices in 2018 was Ransomware [2]. Noteworthy ransomware attacks of 2017 were Cerber and Jaff. Cerber is a family of ransomware payloads which are distributed through email, exploit kits, JavaScript, and Microsoft Word macros. Variants of Cerber include a Bit-coin wallet stealing function. Jaff is described as new but vicious. It is spread via the Necurs botnet and is downloaded in a .pdf file attachment. Jaff is said to check for the target computer's language setting. If the language is set to Russian, the payload destructs rather than deploying. The kill chain roles of ransomware are installation, command and control of the device, and execution of harm. Mitigation is through limited

access rights to data which potentially makes fewer data vulnerable to encryption, and an off-line backup to recover data as well as an up-to-date and patched software and operating system.

O. Threat 15: Cyber Espionage

Cyber Espionage involves the use of a computer network to obtain confidential information. Government, political, and commercial organizations are the typical targets. Actors include nation-states and organized crime. Cyber Espionage made it to the top fifteen list in 2014 but remains at the bottom of the list. Advanced Persistent Threats (APTs) are a collection of processes, tools, and resources used to infiltrate networks over a long period without detection. Even though cyber-espionage is last on the top fifteen list, it is perceived as a serious threat, likely due to press coverage. Widely covered attacks in 2017 include the US Democratic National Committee breach, and the Ukraine power grid take-down attributed to Russian cyber-spies. Since espionage is a composite threat, mitigation is through mitigation of all other cyber-threats.

P. Threat 16: Exploit Kits

Exploit Kits are a bundle of ready-made exploits used to infect websites or as part of a malicious advertising campaign. The kits identify vulnerabilities on web browsers and web apps then exploit automatically, an example of click-less attacks. The payload may be ransomware. Common targets are Java and Adobe Flash add-ons. Exploit Kits were in fourth place in the top fifteen threat in 2012, and increased in rank constantly until it exited the list in 2018. The scaling up of an Exploit Kit attack can lead to its detection which perhaps explains the trend. Mitigation is the detection and patching of vulnerabilities.

IV. Concluding Remakds

Cyber threats are constantly evolving and one cyber operation may see multiple avenues of threats taken to fulfill objectives of the cyber actors. There is a desire for the implementation of security during development rather than after, particularly for IoT devices. That is “built-in” versus “bolt-on” security. The complexity and maturity of malicious practices will continue to be analyzed. There is a prediction that data analytics will be used not just to mitigate threats but to develop attacks. There is concern that state-sponsored and military cyber weapons will be tested on easy targets already in crisis through poverty or war. There is also a call for an increase in cyber threat intelligence capabilities and training which is currently limited and lagging behind threats. In conclusion, a good reflection on the cyber threats from an individual’s standpoint may help educate ordinary users on prevention techniques to protect themselves, their organization and their societies.

References

[1] European Union Agency For Network and Information Security (ENISA). (2019). *ENISA threat landscape web portal*. Retrieved from etl.enisa.europa.eu.

[2] European Union Agency For Network and Information Security (ENISA). (2019). *ENISA threat landscape report 2018: 15 Top Cyber-Threats and Trends*. Heraklion: ENISA. https://doi.org/10.2824/622757

[3] European Union Agency for Network and Information Security (ENISA). (2017). *ENISA threat landscape report 2016: 15 top cyber-threats and trends*. Heraklion: ENISA. https://doi.org/10.2824/92184

[4] European Union Agency For Network and Information Security (ENISA). (2015). *ENISA threat landscape report 2014: Overview of current and emerging cyber-thretas*. Heraklion: ENISA. https://doi.org/10.2824/061861

[5] European Union Agency For Network and Information Security (ENISA). (2013). *ENISA threat landscape report 2013: Overview of current and emerging cyber-threats*. Heraklion: ENISA. https://doi.org/10.2824/022950

[6] European Union Agency For Network and Information Security (ENISA). (2013). *ENISA threat landscape report 2012: Responding to the evolving threat environment*. Heralion: ENISA. Retrieved from: http://www.enisa.europa.eu/

[7] Hutchins, E.M., Cloppert, M.J., & Amin, R.M. (2012). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. In J. Ryan (Ed.). *Leading Issues in Information Warfare and Security Research*, Volume 1 (pp. 80-106). Reading: Academic Publishing International Limited.

[8] Malware Information Sharing Platform (MISP) Project. (2018). *The Open Source Threat Intelligence Platform & Open Standards for Thret Information Sharing*. Rerieved from http://www.misp-project.org/