J Inf Process Syst, Vol.15, No.4, pp.865~889, August 2019
https://doi.org/10.3745/JIPS.03.0126

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

Cyber Kill Chain-Based Taxonomy of Advanced Persistent Threat Actors: Analogy of Tactics, Techniques, and Procedures

Pooneh Nikkhah Bahrami*, Ali Dehghantanha**, Tooska Dargahi***, Reza M. Parizi****
Kim-Kwang Raymond Choo*****, and Hamid H. S. Javadi******

Abstract

The need for cyber resilience is increasingly important in our technology-dependent society where computing devices and data have been, and will continue to be, the target of cyber-attackers, particularly advanced persistent threat (APT) and nation-state/sponsored actors. APT and nation-state/sponsored actors tend to be more sophisticated, having access to significantly more resources and time to facilitate their attacks, which in most cases are not financially driven (unlike typical cyber-criminals). For example, such threat actors often utilize a broad range of attack vectors, cyber and/or physical, and constantly evolve their attack tactics. Thus, having up-to-date and detailed information of APT's tactics, techniques, and procedures (TTPs) facilitates the design of effective defense strategies as the focus of this paper. Specifically, we posit the importance of taxonomies in categorizing cyber-attacks. Note, however, that existing information about APT attack campaigns is fragmented across practitioner, government (including intelligence/classified), and academic publications, and existing taxonomies generally have a narrow scope (e.g., to a limited number of APT campaigns). Therefore, in this paper, we leverage the Cyber Kill Chain (CKC) model to "decompose" any complex attack and identify the relevant characteristics of such attacks. We then comprehensively analyze more than 40 APT campaigns disclosed before 2018 to build our taxonomy. Such taxonomy can facilitate incident response and cyber threat hunting by aiding in understanding of the potential attacks to organizations as well as which attacks may surface. In addition, the taxonomy can allow national security and intelligence agencies and businesses to share their analysis of ongoing, sensitive APT campaigns without the need to disclose detailed information about the campaigns. It can also notify future security policies and mitigation strategy formulation.

Keywords

Advanced Persistent Threats (APT), Cyber-Attacks, Cyber Kill Chain (CKC), Intelligence Sharing, Knowledge Sharing

1. Introduction

Cyber-attacks are increasingly sophisticated, particularly as advanced technological countries start to place heavier emphasis on acquiring and strengthening their cyber-offensive and defensive capabilities.

Manuscript received January 3, 2019; first revision April 5, 2019; accepted April 18, 2019.
Corresponding Author: Kim-Kwang Raymond Choo (raymond.choo@fulbrightmail.org)
* Dept. of Computer Science, University of Tehran, Tehran, Iran (nikkhahbahrami@ut.ac.ir)
** Cyber Science Lab, School of Computer Science, University of Guelph, Guelph, Canada (ali@cybersciencelab.org)
*** School of Computing, Science, and Engineering, University of Salford, Manchester, UK (T.Dargahi@salford.ac.uk)
**** School of Computing and Software Engineering, Kennesaw State University, Kennesaw, GA, USA (rparizi1@kennesaw.edu)
***** Dept. of Information and Cyber Security, University of Texas at San Antonio, San Antonio, TX, USA (raymond.choo@fulbrightmail.org)
****** Dept. of Computer Science, Shahed University, Tehran, Iran (h.s.javadi@shahed.ac.ir)

This is partly due to the ever-increasing dependency of governmental and commercial organizations on data centers and computer networks and the importance of gaining access to such information and systems to secure strategic and political advantages. For example, it has been observed that there has been an increase in the number of advanced persistent threats (APTs) targeting both governmental and commercial organizations [1-3].

Generally, APT attackers research on their targets prior to carrying out a carefully planned attack, in order to maximize the impact (e.g., identify data/assets of interest with the aim of obtaining the most valuable information) while minimizing the risk of exposure. One such high-profile APT campaign is APT1 [4]. The features of APT actors can be broadly categorized into the following: (1) pre-determined, well-researched targets with a clear mission [1]; (2) using and/or customizing sophisticated tools and techniques to exploit vulnerabilities, particularly zero-day vulnerabilities, in systems and computing devices [5]; (3) creating an approach to monitoring and exfiltrating data from a specific target using both cyber and physical means [5]; and (4) sophisticated, well-organized, well-resourced campaigns [5].

The objectives of APT attacks include compromising the target system to exfiltrate data and information of interest covertly, compromising critical infrastructure systems to facilitate other nefarious activities, and degrading military installations. APT targets are not restricted to government and military organizations only [5]. For example, APT30 [6] is reportedly one of the longest operating groups whose objective is to compromise and steal commercial intellectual property (IP) from cutting-edge technology companies.

A number of scholars have developed taxonomies to classify cyber-attacks using different models [7-11]. For example, Chapman et al. [7] introduced a taxonomy based on the different types of attacks used by cyber-attackers and described the access requirements for a successful attack. Note, however, that their model does not consider the different stages of an attack, and it cannot guide cyber-defenders in dealing with sophisticated campaigns. The taxonomy proposed by Hansman and Hunt [8] is multi-dimensional, having categorizations for attack vectors, targets, vulnerabilities, and payloads. Nonetheless, the taxonomy only describes specific campaigns run by different APT actors such as the Code Red Computer worm, not the overarching activities of different actors.

The Cyber Kill Chain (CKC) model [12] has been used to break down a complex attack into consecutive stages to help analysts study, focus on, and solve the attacks stage-by-stage. In addition, a mitigation strategy can be developed for each of the stages, if needed. Lemay et al. [13], for example, reviewed existing known APT groups and provided a general summary of their activities without examining the technical details of the attacks. Chen et al [5]. summarized the techniques used at each step of an APT attack for three APT groups: Operation Aurora and Operation Snowman attributed to APT17, and Operation Ke3chang attributed to APT15. Virvilis and Gritzalis [14] also analyzed four complex malware families used in the respective sophisticated APT campaigns (i.e., Stuxnet, Flame, Duqu, and Red October) by studying their initial infection vector and the capabilities and features of the malware. Note, however, that the authors did not study the APT group's lifecycle. Ussath et al. [15] analyzed the techniques used by 22 APT groups using only the three phases of the CKC model (i.e., Initial compromise, lateral movement, and Command and Control). We argue that it is important to analyze comprehensively the APT group's tactics, techniques, and procedures (TTPs) in every step of the CKC model, in order to design more effective and efficient security systems and countermeasures against APT campaigns. Yadav and Rao [16] categorized the methodologies, techniques, and tools involved in each stage of the CKC model, but the level of details is minimal. For example, additional factors like evaluation of attacks by

APT attackers were not considered. Table 1 summarizes the previously developed taxonomies for analyzing APT actors.

Table 1. Existing APT and related taxonomies: a comparative summary

Study	Year	Taxonomy categorization	Advantages	Defects
[8]	2005	Multi-dimensional	– Allows the detailed characterization of broad spectrum of attacks – Evaluates an attack from different aspects	– Narrow in scope, describes only specific attacks – Evaluation of real attacks by cyber-attackers are not considered
[7]	2011	Based on attack type	– Explains the intrusion approaches undertaken by an attacker	– Not designed to capture sophisticated attacks – Applicable defense mechanism cannot be proposed for sophisticated attacks – Not based on real-world attacks
[14]	2013	Initial infection vector	– Identifies the common patterns and techniques of APT actors – Proposes countermeasures to mitigate attacks	– Categorization based only on four APT actors, other attacks cannot be mapped to this taxonomy – Attack phases or APT groups' campaign lifecycle not considered
[5]	2014	CKC	– Analyzing the techniques commonly seen in APT attacks	– Evaluation of real-world attacks is limited, so the taxonomy is not generalizable – Results do not include detailed information
[16]	2015	CKC	– Categorized methodologies, techniques, and tools involved in each stage of the CKC model	– Level of details provided in the categorization of technologies used in each stage of an attack is limited – Categorization is too general and limited, the taxonomy is not based on real-world APT attacks
[15]	2016	CKC	– Analysis on techniques of 22 APT campaigns – Proposes a prevention and detection approach	– Focuses only on the three stages of CKC model – The defense mechanism is limited – The analysis of APT attacks is based on only one report for each campaign
[13]	2018	APT actors	– A quick reference on the status of knowledge of APT actors – Focuses on the APT activities	– The technical details of the attacks are not considered – Defensive measures are not included

Another challenge faced by cyber-security professionals is the fragmentation of information across sectors (e.g., industry, government, and academe); in some cases, the information may be classified and unavailable to industrial practitioners and researchers. This complicates efforts in compiling information about a specific APT actor's TTPs and in some cases makes for a nearly impossible task. This has motivated us to carry out a comprehensive study on the different APT groups and provide a detailed taxonomy of their TTPs. A key requirement underpinning a comprehensive taxonomy is completeness [17], which means that it should include detailed characterization of a broad spectrum of attacks. In addition, our taxonomy can serve as a means of sharing information/knowledge about the attacks without disclosing sensitive information about a specific ongoing APT campaign.

In this paper, we perform a comprehensive analysis of 40 APT attacks and, based on the analysis, present a CKC-based taxonomy. The CKC model provides information regarding the intrusive steps that

an attacker generally follows to perform a successful attack and consists of seven phases: (1) reconnaissance, (2) weaponization, (3) delivery, (4) exploitation, (5) installation, (6) command and control (C2), and (7) action on objectives (AoO). It is also important to note that APT attackers continuously evolve their strategies and enhance their capabilities (e.g., learning from past experiences); thus, any such taxonomy should be a "live document," and it should evolve based on the analysis of new APT campaigns and groups.

The rest of this paper is organized as follows: Section 2 briefly introduces the CKC model; Section 3 describes our APT feature taxonomy based on the analysis of the 40 APT groups; finally, Section 4 presents our conclusion and outlines possible future work.

2. Preliminaries

In this section, we will explain the CKC model developed by Lockheed Martin [12], which underpins our taxonomy. The model consists of seven phases to provide better understanding of an adversary's TTPs as shown in Fig. 1. The phases are as follows:

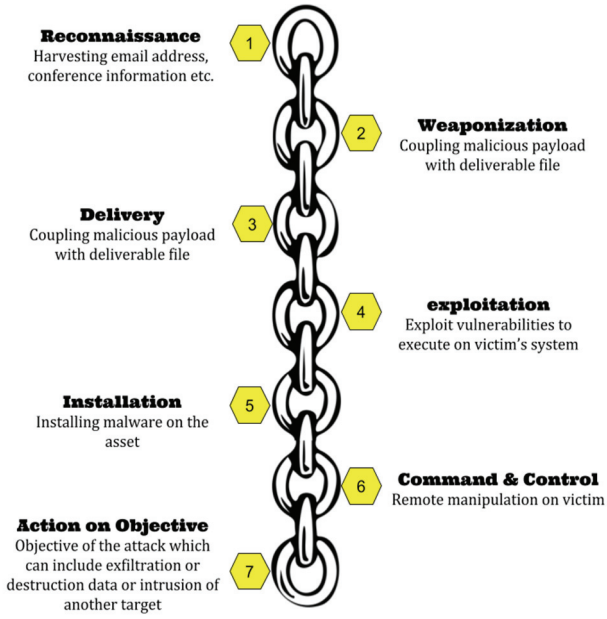

Fig. 1. Lockheed Martin's CKC steps (adapted from [9], [12]).

- Reconnaissance: This phase includes identification, choosing, and profiling of potential targets.
- Weaponization: This phase includes designing malware, including a Remote Access Trojan (RAT) integrated with an exploit code (exploit kit), into a deliverable payload, such as PDF or Microsoft office files. Weaponization efforts are made to reduce the risk of detection and evaluation by security analysts or solutions.
- Delivery: In this phase, the attacker attempts to transfer the payload (from the preceding phase) to the target's environment and, in some cases, through another third party in order to exploit a

trusted relationship between the third party and the target.

- Exploitation: In this phase, upon successful delivery of the weapon, exploitation will commence by leveraging various techniques to trigger the malicious code.
- Installation: In this phase, the attackers will attempt to install access points, such as backdoors or other payloads, to gain persistent access to the target's system or network.
- Command and Control (C2): In this phase, the adversary establishes communication with the compromised host(s) and some C2 server.
- Actions on objectives (AoO): In this phase, the attacker takes action to achieve his/her goals, which can be exfiltration or destruction.

3. Proposed Device Discovery Scheme

To protect a computing system, a network, or an organization against cyber-attacks, key challenges include the capability to perform real-time analysis and detection of an ongoing attack as well as performance of predictive analytics and identification of potential attacks to the target systems. To contribute to this research gap, first, we comprehensively analyze different known APT groups and campaigns in order to build the knowledge base on the cyber threat landscape and the potential attacks to different organizations, including which attacks may surface and so on. We build our taxonomy based on our analysis of APT campaigns obtained from sources such as published scientific research, industry reports, white papers, and blog posts [13]. The proposed CKC-based taxonomy is presented in Fig. 2. Tables 2 and 3 present the mapping between the collected APT features and our proposed taxonomy.

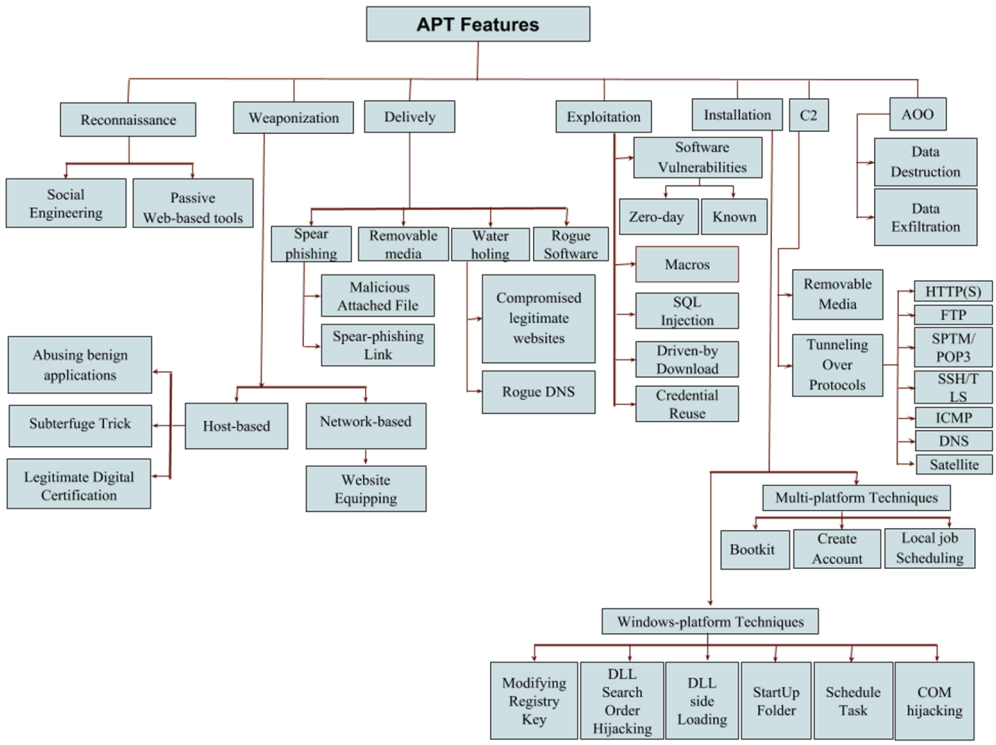

Fig. 2. CKC-based taxonomy of APT features.

Table 2. Mapping between the collected APT features and the proposed taxonomy: reconnaissance, weaponization, and delivery

APT groups	Cyber Kill Chain (CKS) stages											
	Reconnaissance		Weaponization				Delivery					
			Host-based			Network-based	Email/social network spear phishing		Watering hole		Replicate through removable media	Rogue software
	Social engineering	Passive web-based tools	Abusing benign applications' vulnerabilities	Subterfuge techniques	Legitimate digital certification	Web equipping	File attachment	Spear phishing link	Compromised legitimate websites	Rogue DNS		
APT16	√		√				√					
APT17	√		√	√	√	√	√	√	√			
APT1	√		√	√			√	√				
Shell Crew	√				√			√	√			√
Emissary Panda	√	√	√	√			√		√			
APT3	√		√			√	√	√	√			√
Hurricane Panda					√					√		
Ice fog			√	√		√	√	√	√			
APT15	√		√	√			√	√				
Net Traveler			√			√	√		√			
Night Dragon			√					√				
APT12	√		√	√			√					
APT2			√				√					
Hellsign				√			√					
APT30	√		√	√			√				√	
Energetic Bear	√		√			√	√		√			
Sand worm			√	√			√					
APT28	√		√	√		√	√	√	√		√	√
APT29	√		√	√	√	√	√	√				
Snake	√		√		√	√	√		√		√	
Project Sauron											√	√
Animal farm						√			√			
Regin					√							√
Equation Group			√			√			√		√	
Olympic Games	√	√	√		√		√		√			√
Iran	√	√	√	√		√	√	√	√			
Copy Kittens	√			√	√		√	√	√			
Desert Falcons	√			√			√	√				
Volatile Cedar	√					√					√	√
Molerats	√			√	√	√	√	√	√			
Trans parent Tribe			√			√	√		√			
Unnamed Group			√		√		√		√			√
Lotus Blossom	√						√		√			
Silent Chollima	√		√	√			√					
Operation Dust Storm			√			√	√		√			
Platinum			√				√					
Red October			√				√	√				
Careto			√		√	√		√				

Table 3. Mapping between the collected APT features and the proposed taxonomy: exploitation, installation, command and control, and actions on objectives

APT groups	Cyber Kill Chain (CKS) stages																											
	Exploitation						Installation										Command and Control (C2)									Actions on objectives		
	Software vulnerabilities		SQL injection	Macros	Driven-by download	Credential reuse	Windows-platform techniques						Multi-platform techniques				C2's using network protocols								C2's using removable media	Data exfiltration	Data destruction
	0-day EXP	Known EXP					Modifying Registry key	DLL Search Order Hijacking	DLL side loading	Startup folder	Scheduling task	COM hijacking	Bootkits	Create account with valid credential	Scheduling	HTTP(s)	FTP	SMTP/POP3	SSH/TLS	ICMP	DNS	Satellite			
APT16	√	√								√						√								√		
APT17	√	√	√				√			√				√		√								√		
APT1					√	√		√						√		√	√							√		
Shell Crew	√					√	√				√			√		√								√		
Emissary Panda		√			√		√		√		√			√		√					√			√		
APT3	√	√				√	√		√	√	√			√	√	√								√		
Hurricane Panda	√		√						√				√	√		√	√				√			√		
Ice fog		√		√	√		√	√								√		√						√		
APT15	√	√			√		√			√				√		√					√			√		
Net Traveler		√					√									√	√							√		
Night Dragon		√	√			√	√		√							√								√		
APT12	√	√					√			√						√								√		
APT2		√					√									√								√		
Hellsign					√			√								√								√		
APT30		√					√			√						√							√	√		
Energetic Bear		√			√		√			√	√			√		√								√		
Sand worm	√				√		√			√						√			√					√		
APT28	√	√			√	√	√					√	√	√		√		√					√	√	√	
APT29	√			√	√		√	√		√	√		√	√		√	√							√		
Snake	√	√					√			√						√					√			√		
Project Sauron	√						√				√			√		√	√	√		√	√		√	√		
Animal farm	√						√								√	√								√		
Regin						√	√									√				√				√		
Equation Group	√	√					√						√			√							√	√		
Olympic Games	√	√	√			√	√			√	√					√					√			√	√	
Iran					√	√	√							√		√	√					√		√		
Copy Kittens		√	√	√	√	√	√							√	√					√				√		
Desert Falcons					√		√									√								√		
Volatile Cedar					√	√	√							√		√								√		
Molerats					√		√			√				√		√								√		
Trans parent Tribe		√		√	√		√			√						√					√			√		
Unnamed Group		√								√						√								√		
Lotus Blossom							√			√						√								√		
Silent Chollima	√				√	√	√			√			√	√		√		√			√			√		
Operation Dust Storm	√	√					√			√						√		√						√		
Platinum	√				√		√							√		√	√	√						√		
Red October		√					√									√		√						√		
Careto		√					√	√				√				√								√		

3.1 Reconnaissance

Gathering information about a given target is generally the first and main step in any successful cyber-attack. Attackers attempt to gather as much information about the target organization (e.g., resources, system properties, employees and their intra-organizational relationships) using the resources available to them. Such information not only speeds up the cyber-attack process by eliminating potential dead ends but also reduces the chances of detection by reducing the number of intrusion attempts (e.g., due to the use of the right tools as well as targeting the right vulnerability, loophole and so on). One of the key objectives of reconnaissance is to identify valuable targets and find a suitable way to penetrate the target system(s), where the most valuable information is stored. Adversaries use various information-gathering techniques to avoid detection and circumvent security measures. Based on our analysis, social engineering and passive web-based recon tools are two commonly used approaches.

3.1.1 Social engineering

Generally, the most vulnerable asset in an organization is man (e.g., employees, vendors, and/or customers). People are a key target of social engineering attacks especially to gather information and to gain access to the system. Sophisticated social engineering techniques accelerate the hacking process and facilitate information gathering. Most of the APT attackers leverage this method to gather information, although the origin of reconnaissance activities is generally hard to detect.

3.1.2 Passive web-based recon tools

Online tools are commonly used for passive information collection and to perform reconnaissance for future attacks. These tools can be either specialized tools such as SpyFu and KeywordSpy, or generic tools such as search engines (e.g., Baidu search engine was heavily used by APT 27 to conduct recon activities [18]).

3.2 Weaponization

Weaponization includes all activities to subvert network- or system-level defense and detection mechanisms. These techniques can be divided into host-based and network-based evasion techniques.

3.2.1 Host-based evasion

It has been observed that APT campaigns use various techniques to trick users or evade conventional host-based security solutions such as anti-virus/anti-malware and application sandboxing installed on the user devices [19]. We will briefly explain this below.

Abusing benign applications vulnerabilities. APT attackers attempt to find vulnerabilities such as zero-day vulnerabilities or use known vulnerabilities in user applications such as Microsoft Office documents, WinCC, Adobe Portable Document Format (PDF), and Internet Explorer (IE) to inject their malicious code. Aurora Panda (a.k.a. APT17), which is well-known for its involvement in attacks against Google, is believed to have a tool for weaponizing MS Word documents [20]. It can allegedly take an arbitrary clean MS Word file with a selected exploit code and a Trojan and combine them together to generate a weaponized malicious document. Recon activities play a significant role in the attackers' choice

of targeted applications. For example, APT3 reportedly used vulnerabilities in the TTCalc application (a mathematical big number calculator) to Trojanize its targets [21].

Subterfuge techniques. Some attackers use subterfuge techniques, such as RTLO (right to left override) as well as a combination of icon spoofing and name padding to avoid detection of their malicious executable files. For example, APT1 actors in one of their attacks "zipped" the malicious file into a PDF payload. Consequently, the extension of the malicious file was PDF, but the filename actually includes 119 spaces after ".pdf" followed by ".exe." The latter is reportedly the actual file's extension [22]. Another method tries to compact the malicious files to make them more complicated for the antivirus / antimalware scanner to identify the malicious portion of the file. For example, APT29 (a.k.a. Dukes) reportedly compressed its Java Script malicious code to avoid host-based detection and compromise their victims [23].

Using legitimate digital certification. Some attackers generate a fake digital signature or compromise legitimate companies and abuse their digital signature to sign malicious files and deceive users and antimalware products. For example, in the summer of 2012, the VOHO Campaign (a.k.a. APT17) targeted a security firm (Bit9) using a Remote Access Trojan and stole their digital certifications. APT17 then used Bit9's digital certificates to sign custom variants of the Hikit rootkit in an effort to bypass host-based security monitoring systems [24].

3.2.2 Network-based evasion

The most frequently used network protection mechanisms are firewalls and intrusion detection system/intrusion prevention systems (IDS/IPS). No security solution is perfectly secure, including firewalls and IDS/IPS. For example, a known malicious executable file could be captured by most existing network security solutions, or a malicious document attached to an email may not be detected by network-based detection solutions [25,26]. Network-based defense mechanisms are rarely effective against APT actors, with the wide utilization of packet encryption significantly limiting their performance (Note, however, that there have been efforts by the security community to design tools to classify and detect encrypted malicious traffic. For example, in a recent work [27], the authors designed a traffic classification method to distinguish between compressed and encrypted traffic by evaluating the randomness of the data streams on individual packets without the need for access to the entire stream).

Website equipping. APT actors may also compromise a legitimate website and insert customized Java Script elements (e.g., crypto-miner) or put an Iframe on a webpage and redirect victims to their malicious website. For instance, NetTraveler (a.k.a. APT1) utilized an Iframe injection wherein a simple HTML code of a compromised website loads and runs a Java applet exploit [28].

3.3 Delivery

In this category, adversaries attempt to transfer the malicious weaponized payload to the target's system either directly or indirectly. In the direct mechanism, the adversary gains access to the target's system and sends the exploit via social engineering techniques, such as spear phishing and other viable approaches. In the indirect mechanism, adversaries compromise a third party trusted by the target and deliver the exploit using this mediator. A third party can be a system in the same network as the target or a compromised legitimate website frequently visited by the victims (watering hole attack).

3.3.1 Email/social network spear phishing

Trend Micro reported that more than 90% of targeted attacks were due to spear phishing emails [29]. In such spear-phishing attack, adversaries typically use information gathered during reconnaissance (e.g., information obtained from the organization's website or some social media websites such as LinkedIn) to increase the likelihood of an attack's success. Attackers have been known to use techniques, such as the following, to deliver a payload to the victim by email or social network:

Malicious attached file. Attackers attempt to convince victims to download a seemingly legitimate file attachment, for example, by choosing an eye-catching or a convincing subject line and a customized message that would appeal to the target [30]. Attachments can be in formats such as PDF, Flash files, or Microsoft Office files, with or without macros, as well as executable files. We also observed that executable files (.exe) are not commonly used as bait because they can be easily detected and filtered by security solutions. For example, the Naikon APT relied on emails as an attack vector with an attachment that first compromised victim systems using common spear-phishing techniques, such as exploiting CVE-2012-0158, while the malicious payload was altered with RTLO techniques as well as a combination of icon-spoofing and name padding for executable files [31].

Spear phishing Link. Attackers may include links to compromised websites in their targeted emails, which may impersonate a legitimate website, with the aim of redirecting victims and luring them to a website containing the actual exploit code. Attackers typically leverage zero-day or known vulnerability(ies) in widely used software [32]. Moreover, some attackers register a domain that looks very similar to the target's real domain and, in some cases, purchase a Secure Sockets Layer (SSL) certificate for the fake domain as part of preparation for the targeted attack. Links to these fake websites would be included in the spear-phishing emails and sent to targets. Fancy Bear (APT29), one of the most well-known groups associated with Russia actors, regularly used this technique [33].

In addition to using emails as a delivery method, some campaigns employed social networks like Facebook to redirect their targets to a malicious website. In 2013, CopyKittens reportedly abused several Facebook accounts to distribute links to a luring website impersonating Haaretz news, an Israeli newspaper [34]. This was likely used for exploiting browsers with known vulnerabilities. In some pages of the "luring" website, the malicious code gathered a list of installed browser plugins; in other cases, it collected the IP address of the victims.

3.3.2 Watering hole

The name of the attack is derived from predators in the natural world waiting near watering holes to attack a desired prey when the opportunity arises. Similar to this concept, cyber attackers compromise websites that would probably be visited by their given target. Although the scale of spear phishing attacks is significantly larger than watering hole attacks, the chances of a successful infection by visiting a compromised website are much larger. This is because re-visiting a trusted website is more likely than opening an attachment to an email [20].

Compromised legitimate website. In this technique, attackers first find vulnerabilities in the website of interest (known as pivot or redirector sites) and exploit the identified vulnerability(ies) to insert a hyperlink, or an Iframe, which points to another webpage that hosts the exploit code or the malware that delivers a Trojanized payload to the target environment. In some campaigns, attackers accessed the legitimate website's FTP and replaced legitimate files with one bound with some malware [35].

Nevertheless, compromising a website is not necessarily trivial and is usually carried out by sophisticated campaigns with significant supporting resources (e.g., in terms of technical expertise). The VOHO campaign reportedly carried out one of the largest and most successful watering hole attacks, at least at the time of the data collection in this research [36]. During the VOHO campaign, hundreds of organizations in the United States downloaded a malicious payload delivered from compromised legitimate websites [36]. Another sophisticated cyber espionage group known as Turla [37] (also known as Carbon, Uroburos, and Snake) was allegedly responsible for one of the worst breaches of US military systems, which relied on injected code on compromised websites to carry out the watering hole attacks [38]. In 2016, Turla was reported to have targeted and compromised successfully over 4,500 computers in more than 100 countries using a sophisticated watering hole distribution network known as Venom. To achieve this goal, they infected 84 legitimate websites using a drag network (Venom) that redirected all visitors to another malicious server; thus allowing information including configuration data, system and network information, operating system, browser version, and IP address to be harvested. Such information is then analyzed in real time to determine if a visitor is their target of interest; if it is determined to be one, then the visitor will receive a carefully crafted malicious payload.

Rogue DNS. This technique uses free DNS services to return a fake IP address for DNS lookup requests for popular domain names such as github.com and pinterest.com.

3.3.3 Replicate through removable media

Many critical organizations air-gap their networks (physically separating high-value information infrastructure from the rest of the network) in an attempt to protect them from cyber-attacks [39]. While air-gapped computers have long been considered one of the best practices in cyber security, particularly in a classified and sensitive environment, it is not foolproof. For example, some APT groups have compromised such isolated networks by delivering their payload and exfiltrated data through removable media [40]. At least two campaigns (APT28 and Stuxnet) reportedly used removable media for penetration into the target network and exfiltration of data [41,42]. It has also been demonstrated by researchers that data can be exfiltrated from air-gapped systems and devices, including mobile devices, using inaudible sound waves via the system's speakers and earphones [43,44].

3.3.4 Rogue software

Surprisingly, this is a less common method of delivering a malware to the target systems in our analysis. For example, according to Palo Alto's blog post [45], the Fancy Bear group (a.k.a. APT28, Pawn Storm, Fancy Bear, and Sednit) reportedly targeted individuals in the aerospace industry running the OS X operating system by delivering Komplex Trojan as a payload using a rogue Mackeeper antivirus application. In several campaigns by Strider [46,47] (project Sauron), rogue software update scripts replaced legit centralized software updates to compromise the target network.

3.4 Exploitation

Exploitation is a fundamental phase for initial penetration into the target system or network. By successfully carrying out this step, the APT actors establish a footprint in the target's network, for example

by exploiting the system's vulnerability(ies) [48]. Our analysis of the APT groups revealed that the following exploitation techniques were commonly used.

3.4.1 Software vulnerability exploitation

A software vulnerability is a security defect in software or in an operating system (OS) that may constitute a security threat upon execution. All software and operating systems are vulnerable, and no particular software vendor is an exception in this regard.

Zero-day exploitation. The goal of zero-day exploitation is to exploit a software flaw that is unknown and which has no patches or fix [49,50]. Zero-day exploits are not detectable with traditional security protection mechanism [51]. Note, however, that only advanced attackers are capable of finding zero-day vulnerabilities and writing zero-day exploits. The Axiom group launched a series of attacks in the Elderwood Project in 2009 against high-profile targets in North America and used a large number of zero-day vulnerabilities to deliver a malware (Hydraq) [36]. The number of zero-day exploits used by an APT attacker reveals its high level of technical proficiency. APT actors are very careful in using zero-day exploits, since any usage risk detection could lead to losing a valuable weapon against other targets. True zero-day exploits are scarce, but they would be very interesting if observed in natural conditions.

Known vulnerabilities' exploitation. Some cyber-attacks use exploit kits to penetrate using known vulnerabilities that are left unpatched on the target network. Exploit kits are software tools that include a collection of exploits for targeting known vulnerabilities. The intent of the attacker is to find a weakness in the victim system (unpatched or non-updated software) by trying different exploits. Apart from some sophisticated APT groups such as APT12 [52] that built their own exploit kits, others are usually buying exploit kits from darknet markets [53]. For example, CVE-2012-0158, a known buffer-overflow vulnerability in the ListView/Tree-View ActiveX controls in MSCOMCTL and patched almost a decade ago by Microsoft, is still the number 1 exploited vulnerability by exploit kits available in the black market [54].

3.4.2 SQL injection

An SQL injection attack allows attackers to execute their code or script of choice on the back-end database server. For instance, if an SQL server can be attacked by an injection, an attacker may go to a website search box and type the SQL script that would lead to dumping all the stored usernames and passwords. For example, in July 2012, Bit9 Inc. (presently Carbon Black Inc.) a cyber-security company that develops trust-based security software as an alternative to traditional signature-based antivirus solution, became exposed to successful SQL injection attack by a well-known APT group named Hidden Lynx (a.k.a. APT17). Since it was nearly impossible for attackers to install a malicious application like Remote Access Trojans (RATs) onto systems protected by Bit9 software, they dumped Bit9 digital certificates through an SQL inject attack, signed 32 malicious files with those certificates, and ran them against organizations using Bit9 solutions [36].

3.4.3 Malicious document with macros

Microsoft Office macros are a prime example of scripts that can be executed upon opening a Microsoft Office file. The auto-execution feature of macros and the fact that they can be embedded into benign

documents made them a great choice for malicious activities. In some of its spear phishing attacks, a Middle East threat actor, Coppy Kittens, sent a lure document that included instructions motivating the victim to enable macros, which led to the exploitation of the target [55].

The malicious macros usually perform some anti-forensics tests to make sure they are targeting real victims, and that they are not under analysis by a forensics examiner. For example, they may run the Application.RecentFiles.Count call, which checks which recent files have been opened. Once the macro verifies the computer, it drops another script, which could be a PowerShell script. Such behavior on its own is not malicious, as it has been seen that legitimate macros drop and execute benign scripts. Furthermore, the macro code does not need to contain the malicious script. It has been seen that malicious scripts have been stored in table cells or metadata [56]. The macro code then reads out this data and runs it on the target, for example from the author property field as can be seen in Table 4.

Table 4. Example of macro reading the author property field

	Example
Author command	powershell.exe -nop -w hidden; -c IEX ((new-object net.webclient)
Download string	http://192.168.0.42:80/a

3.4.4 Drive-by download attacks

Although sending an executable malware file to a given user by email is the easiest way of exploiting a system, there was usually very little reason anyone would send an executable file via email. Email services have become smarter in picking up executable files when an adversary sends them using old methods like changing the file extension, for instance to .jpg, by simply using a zip folder to send the executable file, or adding a non-existent file extension to the file.

Nevertheless, sophisticated APT attackers use novel techniques to bypass Email or antivirus protection by asking users to download and run the malicious files themselves. The Ke3chang group leveraged the Unicode RTLO technique to send Windows screensaver files (.scr) and executable files (.exe) encoded to disguise the original filename extension [57]. In Operation Deputy Dog Attack on Japanese Targets, APT17 attackers uploaded an executable file to a remote server and sent the link to their target. Although the malicious file extension was .jpg, it was not an image file but an executable file packed by XORing its codes with 0x95 [58].

3.4.5 Credential reuse

Legitimate credentials are a ticket through the front door of every account and organization. The process of exploiting the reused passwords begins when the credentials are stolen. There are some techniques leveraged by attackers to steal credentials, including social engineering, credential phishing, and spamming, reuse of stolen passwords or shared credentials, or even Brute force attacks [59].

In some cases, attackers used online chat with fake profiles to go after their targets, attempting an additional layer of legitimacy. In 2015, Dell SecureWorks reported a suspected state-sponsored activity that created fake LinkedIn profiles used by attackers known as Cobalt Gypsy, OilRig, TG-2889, and Twisted Kitten [60].

The most common way attackers steal credentials is via phishing, wherein an email message attempts

to lure its recipient by logging into an account. Successful credential phishing by Fancy Bear (APT28) is widely believed to be behind the well-publicized attacks against the United States Democratic National Committee (DNC) in the summer of 2016 [61,62].

Attackers do not just steal credentials to use for themselves only but for selling to other groups as well. Credentials are priced according to their potential profitability in underground forums and are often sold in darknet markets [63].

In some cases, the lack of strong passwords is the fault of the organization when it does not enforce the use of strong passwords and instead allows users to use weak passwords. Complex passwords protect primarily against scenarios wherein an attacker takes a stolen hash and subjects it to offline, brute-force attacks.

3.5 Installation

Upon successful exploitation, most common cybercriminals and some targeted attackers make effort to gain control of victims and laterally move across the compromised networks. During installation, most APT groups try to hide the malware and achieve a persistence load point on the compromised machines to continue operation even after system reboots [56,64]. The attackers usually drop a downloader or a dropper in the memory to download additional malware such as backdoors and rootkits. Upon downloading the main payload, like a backdoor, the dropper or downloader deletes itself and removes any traces of its existence. The backdoor leverages persistence techniques to create a continuous load point. In this section, we discuss the most common installation techniques used by APT actors.

3.5.1 Windows platform techniques

Windows has several AutoStart Extension Points (ASEP) that can be used to achieve persistence such as modifying Registry keys or DLL Search Order Hijacking [65,66]. All analyzed APT actors have used at least one of the following Windows-based techniques to achieve persistence:

Modifying registry keys. Achieving persistence on the Microsoft Windows platform is mostly done by modifying the Registry keys. Registering an application in some Registry locations would provide persistence against system reboot or even reinstallation of the operating system [67]. The most common Windows Registry addresses used to achieve persistence by APT actors are shown in Table 5.

Most APT campaigns achieve persistence by adding their malicious applications to the “run keys” in the registry or the startup folder. This registry modification leads to the launch of the malicious application in every logon or reboot, respectively. For example, APT 29 registered Backdoor.Miniduke in the Run key of its targets to make sure the backdoor is enabled every time the system is rebooted [68]. By escalating privilege, attackers may achieve Admin-level access, which allows modification of registry areas that affect all users or achieve longer-term persistence.

Although most of the APT actors achieve persistence by registering their malicious files in key Registry keys that allow execution at system startup/reboot, this provides a single point of failure for their campaigns as these keys are frequently investigated by forensics examiners! Therefore, more advanced groups such as APT28 achieved persistence in an attack against US government agencies by registering their Trojans as a DLL (btecache.dll) that is loaded every time a Microsoft Office document is opened [45]. Thus, APT28 could conceal the execution of its malicious payload during user interaction wherein detection is much more complicated.

Table 5. Common Registry keys used by malware to achieve persistence

Keys	Location\Values	Detail
Run/RunOnce Keys	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run	User level System level
BootExecute Key	HKLM\SYSTEM\CurrentControlSet\Control\hivelist HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Control\Session Manager	-
Keys used by WinLogon Process	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\Notify HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\Shell HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\IniFileMapping\system.ini\boot	Userinit Key Notify Explorer.exe
Startup Keys	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellFolders HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserShellFolders	-
Services	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices	Run at boot services Start at background services
Browser Helper Objects (BHO)	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects	-
AppInit_DLLs	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs	DLLs loaded by User32.dll
APPCert_DLLs	HKLM\System\CurrentControlSet\Control\Session Manager\AppCertDlls	DLLs loaded by calling the Win32 API function
IFEO	HKLM\Software\Microsoft\Windows NT\currentversion\image file execution options	
File Association keys	HKEY_LOCAL_MACHINE\Software\Classes HKEY_CLASSES_ROOT There are various keys that are used to specify the action when a certain type of files is open. For example, below is the Command value when a .txt file is opened in my system HKEY_CLASSES_ROOT\textfile\shell\open\command	-

Adversaries also achieve persistence through service-related Registry keys [69]. For example, adversaries may map their malicious services to a location registered for a benign service by changing the binPath/ImagePath key to launch their application each time the benign service is launched. Upon starting the affected service, the malicious program will be executed instead, consequently allowing the adversary to remain persistent. Night Dragon [70], a Chinese campaign and one of the first attackers focused specifically on the energy sector, installs a copy of itself in a randomly selected service and subsequently overwrites the ServiceDLL entry in the service's Registry entry. The service was configured to be a Win32 shared process like svchost that is autostarted by the system service control manager during system boot.

Appinit_DLL, AppCertDlls, and IFEO (image file execution options) are all registry keys that have been used for DLL injection, achieving persistence [71]. Attackers can insert the location of their malware's DLL under these registry keys to have another process loading their libraries. As an example, in the case of Appinit_DLL, its DLLs are loaded by calling the LoadLibrary() function during the DLL_PROCESS_ATTACH process of User32.dll [72]. If malware infects User32.dll by modifying its registry key, each process that requests loading User32.dll (which is very common for user applications)

will load the malicious library.

DLL Search Order Hijacking. When the application software sends a request to load a DLL file without declaring its location, Windows OS checks whether a DLL with the same module name is already loaded in the memory or if it exists in the application folder. If the DLL is not in the memory, the OS checks the list of known DLLs in the "\.KnownDlls" object [73]. This object is populated at boot-time using data from the registry at the following location:

HKEY LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SessionManagernKnow\DLLs

If the DLL is not in the KnownDLL address, OS tries to load the DLL from a fixed location (System32 folder). If Windows OS cannot find the DLL in KnownDLLs or System32, then the standard DLL search would be started [74].

In the DLL Search Order Hijacking (also known as DLL preloading or binary planting attacks), attackers insert their manipulated DLL with the same name as a legit DLL in a directory searched by Windows before the legit one. The location of tis directory is usually the current working directory of the program. Adversaries may use this behavior to make the program load a malicious DLL [69]. For instance, APT1 [75] dropped a malicious version of the svchost.exe file that uses DLL search order hijacking to achieve persistence. To this end, the malicious file saved itself as ntshrui.dll to the Windows directory; thus, it would be loaded before the legitimate ntshrui.dll in the System32 folder [76].

DLL side loading. DLL side loading takes advantage of the Windows side-by-side (SxS or WinSxS) assembly feature to load malicious DLL from a common directory like SxS [77]. The DLL side loading technique has been used by Emissary Panda (APT27) to leverage a legitimate Kaspersky antivirus, executing a shell code as a stub loader to load PlugX and HttpBrowser backdoor on the compromised machine [78].

Modifying the Startup folder. Some adversaries achieve persistence by creating a shortcut to their malicious file in the Windows Startup directory. Apt29 achieved persistence by dropping its main DLL component on the target system and subsequently created a .lnk shortcut to the dropped file address in the Startup folder [79].

Scheduled Task. It is likely that an adversary uses the Windows task scheduling system to run programs at system Startup or on a Scheduled basis to achieve persistence [66]. For example, APT3 actors achieved SYSTEM-level privilege by exploiting a local kernel vulnerability (CVE-2014-4113), and then achieved persistence by creating a scheduled task using the following shell code:

schtasks\create\t\"mysc" \tr C:\Users\Publicntest.exe\sc ONLOGON \ru "System"

Component Object Model (COM) Hijacking. Microsoft (COM) acts as an interface between software components and OS. Adversaries may run their malicious code instead of a legitimate software by hijacking the COM references. Since this technique does not require any DLL injection, which is usually monitored by antivirus software, it overcomes an important security measure. Hijacking a COM object is made by changing the Windows registry and replacing the reference to a legitimate system component, which probably causes that component not to work when executed [80]. An adversary may hijack frequently used objects to maintain regular persistence. APT28 used COM hijacking to gain persistence by substituting the legitimate MMDeviceEnumerator object, a legitimate Windows COM object, with a malicious payload (backdoor) [81].

3.5.2 Multi-platform installation techniques

APT actors have used different techniques to achieve persistence on non-Windows platforms as discussed in this section.

Bootkits. Launching malicious code from the master boot record (MBR) or the volume boot record (VBR) gives the malware the ability to start before loading the OS. It can carry out significant modifications to the OS code and drivers of system, such as installing software hooks, prior to the initialization of any security measure on the system [74]. Adversaries leverage Bootkits to achieve persistence on infected systems at a layer below the OS [59].

Create Account with valid credential. The most reliable method to achieve persistence is probably using a valid Key or the VPN credentials and gaining local or remote access to the target environment. This allows attackers to disguise themselves as a legitimate user to penetrate the corporate network and its internal resources [69]. APT1 has used stolen usernames and passwords to log into the victim's networks VPNs and achieved persistence [82].

Local Job scheduling. Multiple methods have been introduced on Linux and Apple systems for the creation of pre-scheduled and periodic background jobs, namely cron, at, and launchd. Contrary to Scheduled Task on Windows OS, job scheduling on Linux-based systems cannot be done remotely without a remotely authenticated session such as a secure shell (SSH).

3.6. Command and Control

Command and Control (C&C or C2) are usually used by APT actors to provide remote access to the target environment to execute malicious instructions or exfiltrate data [83]. In fact, most of the backdoor malware in the installation phase are used to connect the victim's system to the attackers' C2 infrastructure [79]. Backdoors may beacon to their servers via IP address or domain name. Attackers have used different strategies for remotely controlling compromised devices and bypassing network IDS, IPS, and Firewall. Our analysis of APT groups revealed two major C2 mechanisms as explained in this section.

3.6.1 C2s using network protocols

Most C2s utilize normal HTTP or other common network protocols such as FTP, SMTP/ POP3, SSH/TLS, ICMP, or DNS for remote connection and data transfer [46,84]. Some APT actors use a hard-coded IP to link up their backdoor to an external SMTP server to exfiltrate data. In cases wherein direct connections to an external mail server are not allowed, backdoors used SMTP and POP3 protocols on the victim mail server to send files via email to another address on the same mail server. Using email as the C2 channel is very common, and many APT actors such as Kimsuky or BlueTermite APT and ProjectSauron APT use this technique [46]. To bypass the usual network protection, attackers may transfer data over DNS packets, which tend to be less monitored. To avoid detection of DNS tunnels at the network level, and due to the limited size of DNS data transfer, APT actors tend to use DNS in low-bandwidth mode, which requires sending more but smaller DNS packets [85]. ProjectSauron has leveraged the most commonly used protocols such as ICMP, UDP, TCP, DNS, SMTP, and HTTP to exfiltrate target system data. ProjectSauron attackers used ICMP tunneling as a carrier for their payloads and to access or control compromised systems [46].

One of the significant problems of APT groups is avoiding detection of their activities and concealing

their physical location. In fact, APT's C&C servers or their related domains are quickly taken down or blocked by law enforcement as soon as they become disclosed. Thus, APT groups are using several techniques to hide and obscure their C2 traffic. For example, the Epic Turla [86] APT group utilized full-duplex satellite links to conceal their traffic. They sent their packets with IP addresses that do not belong to themselves and received responses by intercepting communications with spoofed IP address on a non-traceable interface, which was a satellite-based Internet receiver located anywhere in the covered area of the satellite. This technique provided a much higher degree of anonymity compared with other methods such as compromising legitimate servers while making taking the operation down very difficult.

3.6.2 C2s using removable media

Air-gapping a network is a security measure for protecting very critical data by keeping a network that is used for collecting, storing, and transferring critical data isolated from other less secure networks such as the Internet [87]. To circumvent air-gapped networks, attackers use removable media, such as USB or hard drive, as the means for transferring malicious files or exfiltrating data. To decrease the size of the partition on the removable media, they are specially formatted; thus, an amount of concealed data (several hundred megabytes) is reserved at the end of the disk for malicious purposes. Using this reserved space, a new custom-encrypted partition that cannot be detected by common OS tools is created. The partition has its own semi-file system (or virtual file system) with two core directories: In and Out. This method also bypasses many data loss prevention (DLP) products, since DLP software that disables the plugging unknown USB devices using the DeviceID would not detect the USB as a genuine drive. For example, ProjectSauron attackers exfiltrated data from air-gapped networks using specially prepared USB storage drives. In these USB drives, data were stored in an area that could not be detected by the OS [88].

3.7 Action on Objectives

After gaining a foothold on one computer, most of the APT groups attempt to move laterally in the network by infecting more devices and gain access to high-value targets. They may use publicly available tools such as WinExe (a remote command-line execution tool) and Mimikatz (a Windows credential-gathering tool) to move between computers via methods such as Pass the Hash (PtH) [89]. The ultimate goal of an APT attacker is mainly to exfiltrate sensitive information or intellectual assets. Note, however, that there are also campaigns wherein attackers followed out more ruinous objectives. For instance, the Stuxnet campaign subverted centrifuges of a nuclear facility to frustrate Iran's nuclear program [15].

4. Conclusion and Future Work

In this paper, we presented a comprehensive CKC-based taxonomy based on our large-scale analysis of attacks of 40 APT campaigns. The taxonomy captures the TTPs most widely utilized by attackers, with the aims of providing up-to-date cyber situational awareness for individuals or organizations to be prepared against cyber-attacks, including those carried out by APT groups. Social networking techniques appeared to be used widely as a first step to identify their targets during their research, and spear phishing is a popular means of delivering malware or some malicious payload. Vulnerability(ies) was/were often exploited to help the attackers in establishing a footprint in the target's network. Due to the popularity of

Windows systems, Windows OS appeared to be most targeted by APT attackers compared to other platforms. We also observed that registry keys were often modified to ensure persistence on a compromised Windows platform. HTTP(s) protocol has mainly been utilized for command and control, for example to exfiltrate data from a compromised or a targeted system. The use of zero-day exploits observed in more than half of the attackers studied in this paper also suggested the sophistication and availability of significant resources in terms of technical expertise, financial resources, time, and so on.

As discussed earlier, this taxonomy needs to be updated continuously in order to keep pace with the constantly evolving cyber threat and political landscape. Thus, future research includes extending this taxonomy to include in-depth analysis of different and emerging APT actors' TTPs and extending our taxonomy with network defense frameworks, such as 7D, to provide a more comprehensive network defense analysis against APT actors. We also intend to utilize machine learning and deep learning techniques to automate the extraction and identification of the relevant TTPs and other features to be incorporated into the taxonomy.

References

[1] B. De Decker, J. Dittmann, C. Kraetzer, and C. Vielhauer, *Communications and Multimedia Security (LNCS 8099)*. Heidelberg: Springer, 2014.

[2] E. Cole, *Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization*. Waltham, MA: Syngress, 2013.

[3] L. Wang, M. Zhang, and A. Singhal, "Network security metrics: from known vulnerabilities to zero day attacks," in *From Database to Cyber Security*. Cham: Springer, 2018, pp. 450-469.

[4] B. Donohue, "What is APT?," 2013 [Online]. Available: https://www.kaspersky.com/blog/apt/2050/.

[5] P. Chen, L. Desmet, and C. Huygens, "A study on advanced persistent threats," in *Communications and Multimedia Security*. Heidelberg: Springer, 2014, pp. 63-72.

[6] FireEye Labs, "APT 30 and the mechanics of a long-running cyber espionage operation," 2015 [Online]. Available: https://www.fireeye.com/blog/threat-research/2015/04/apt_30_and_the_mecha.html.

[7] I. M. Chapman, S. P. Leblanc, and A. Partington, "Taxonomy of cyber attacks and simulation of their effects," in *Proceedings of the 2011 Military Modeling & Simulation Symposium*, Boston, MA, 2011, pp. 73-80.

[8] S. Hansman and R. Hunt, "A taxonomy of network and computer attacks," *Computers & Security*, vol. 24, no. 1, pp. 31-43, 2005.

[9] C. A. Meyers, S. S. Powers, and D. M. Faissol, "Taxonomies of cyber adversaries and attacks: a survey of incidents and approaches," Lawrence Livermore National Lab., Livermore, CA, Report No. LLNL-TR-419041, 2009.

[10] C. Simmons, C. Ellis, S. Shiva, D. Dasgupta, and Q. Wu, "AVOIDIT: a cyber attack taxonomy," in *Proceedings of the 9th Annual Symposium on Information Assurance (ASIA'14)*, Albany, NY, 2014, pp. 2-12.

[11] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on SCADA systems," in *Proceedings of 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, Dalian, China, 2011, pp. 380-388.

[12] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," *Leading Issues in Information Warfare & Security Research*, vol. 1, no. 1, pp. 80-106, 2011.

[13] A. Lemay, J. Calvet, F. Menet, and J. M. Fernandez, "Survey of publicly available reports on advanced persistent threat actors," *Computers & Security*, vol. 72, pp. 26-59, 2018.

[14] N. Virvilis and D. Gritzalis, "The big four-what we did wrong in advanced persistent threat detection?," in *Proceedings of 2013 International Conference on Availability, Reliability and Security*, Regensburg, Germany, 2013, pp. 248-254.

[15] M. Ussath, D. Jaeger, F. Cheng, and C. Meinel, "Advanced persistent threats: behind the scenes," in *Proceedings of 2016 Annual Conference on Information Science and Systems (CISS)*, Princeton, NJ, 2016, pp. 181-186.

[16] T. Yadav and A. M. Rao, "Technical aspects of cyber kill chain," in *Security in Computing and Communication*. Cham: Springer, 2015, pp. 438-452.

[17] R. Derbyshire, B. Green, D. Prince, A. Mauthe, and D. Hutchison, "An analysis of cyber security attack taxonomies," in *Proceedings of 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, London, UK, 2018, pp. 153-161.

[18] Dell SecureWorks Counter Threat Unit Threat Intelligence "Threat Group 3390 Cyberespionage," 2015 [Online]. Available: https://www.secureworks.com/research/threat-group-3390-targets-organizations-for-cyberespionage?_ga=1.132970126.1294297346.1479934134.

[19] A. Chesla, "Cyber-security system and methods thereof," U.S. Patent 9565204, 2017.

[20] G. O'Gorman and G. McDonald, *The Elderwood Project*. Mountain View, CA: Symantec Corporation, 2012.

[21] M. Scott, "Clandestine Fox, Part Deux," 2014 [Online]. Available: https://www.fireeye.com/blog/threat-research/2014/06/clandestine-fox-part-deux.html.

[22] Mandiant, "APT1: exposing one of China's cyber espionage units," 2013 [Online]. Available: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

[23] C. Raiu, I. Soumenkov, K. Baumgartner, and V. Kamluk, "The MiniDuke mystery: PDF 0-day government spy assembler 0x29A micro backdoor," Kaspersky Lab, 2013 [Online]. Available: https://media.kaspersky contenthub.com/wp-content/uploads/sites/58/2013/03/21182654/themysteryofthepdf0-dayassemblermicro backdoor.pdf.

[24] Novetta, "Operation SMN: Axiom Threat Actor Group Report," 2014 [Online]. Available: http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf.

[25] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," National Institute of Standards and Technology, Gaithersburg, MD, 2012.

[26] A. Fuchsberger, "Intrusion detection systems and intrusion prevention systems," *Information Security Technical Report*, vol. 10, no. 3, pp. 134-139, 2005.

[27] F. Casino, K. K. R. Choo, and C. Patsakis, "HEDGE: efficient traffic classification of encrypted and compressed packets," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 11, pp. 2916-2926, 2019.

[28] C. Raiu, "NetTraveler is back: the 'Red Star' APT returns with new tricks," 2013 [Online]. Available: https://securelist.com/nettraveler-is-back-the-red-star-apt-returns-with-new-tricks/57455/.

[29] Trend Micro Incorporated, "Spear-phishing email: most favored APT attack bait," 2012 [Online]. Available: https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf.

[30] I. Ghafir, V. Prenosil, M. Hammoudeh, F. J. Aparicio-Navarro, K. Rabie, and A. Jabban, "Disguised executable files in spear-phishing emails: detecting the point of entry in advanced persistent threat," in *Proceedings of the 2nd International Conference on Future Networks and Distributed Systems*, Amman, Jordan, 2018.

[31] K. Baumgartner and M. Golovkin, **"**The Naikon APT and the MsnMM campaigns," 2015 [Online]. Available: https://securelist.com/the-naikon-apt-and-the-msnmm-campaigns/70029/.

[32] M. Shahzad, M. Z. Shafiq, and A. X. Liu, "Large scale characterization of software vulnerability life cycles," *IEEE Transactions on Dependable and Secure Computing*, 2019. http://doi.org/10.1109/TDSC.2019.2893950.

[33] L. Kharouni, F. Hacquebord, N. Huq, J. Gogolinski, F. Merces, A. Remorin, and D. Otis, "Operation pawn storm using decoys to evade detection," Trend Micro, 2014 [Online]. Available: https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-pawn-storm.pdf.

[34] ClearSky Cyber Security, Trend Micro, "Operation wilted tulip: exposing a cyber-espionage apparatus," 2017 [Online]. Available: https://www.clearskysec.com/wp-content/uploads/2017/07/Operation_Wilted_Tulip.pdf.

[35] Kaspersky Lab, "Energetic Bear - Crouching Yeti," 2014 [Online]. Available: https://media.kaspersky contenthub.com/wp-content/uploads/sites/43/2018/03/08080817/EB-YetiJuly2014-Public.pdf.

[36] S. Doherty, J. Gegeny, B. Spasojevic, and J. Baltazar, "Hidden Lynx - professional hackers for hire," 2013 [Online]. Available: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/hidden_lynx.pdf.

[37] Symantec Corporation, "The Waterbug attack group" 2016 [Online]. Available: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/waterbug-attack-group.pdf.

[38] S. Shevchenko, "Agent.btz: a threat that hit pentagon," 2008 [Online]. Available: http://blog.threatexpert.com/2008/11/agentbtz-threat-that-hit-pentagon.html.

[39] Trend Micro Incoporated, "A look at the threats to air-gapped systems," 2017 [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/a-look-at-the-threats-to-air-gapped-systems.

[40] M. Guri and D. Bykhovsky, "air-jumper: covert air-gap exfiltration/infiltration via security cameras & infrared (IR)," *Computers & Security*, vol. 82, pp. 15-29, 2019.

[41] R. Benchea, C. Vatamanu, A. Maximciuc, and V. Luncasu, "APT28 under the scope," 2015 [Online]. Available: https://download.bitdefender.com/resources/media/materials/white-papers/en/Bitdefender_In-depth_analysis_of_APT28%E2%80%93The_Political_Cyber-Espionage.pdf.

[42] J. Calvet, "Sednit espionage group attacking air-gapped networks," 2014 [Online]. Available: https://www.welivesecurity.com/2014/11/11/sednit-espionage-group-attacking-air-gapped-networks/.

[43] Q. Do, B. Martini, and K. K. R. Choo, "The role of the adversary model in applied security research," *Computers & Security*, vol. 81, no. 156-181, 2018.

[44] S. O'Malley and K. K. R. Choo, "Bridging the air gap: Inaudible data exfiltration by insiders," in *Proceedings of the 20th Americas Conference on Information Systems (AMCIS)*, Savannah, GA, 2014, pp. 7-10.

[45] D. Creus T. Halfpop, and R. Falcone, "Sofacy's 'Komplex' OS X Trojan," 2016 [Online]. Available: https://unit42.paloaltonetworks.com/unit42-sofacys-komplex-os-x-trojan/.

[46] Kaspersky Lab, "The ProjectSauron APT," 2016 [Online]. Available: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07190156/The-ProjectSauron-APT_Technical_Analysis_KL.pdf.

[47] GReAT, "ProjectSauron: top level cyber-espionage platform covertly extracts encrypted government comms," 2016 [Online]. Available: https://securelist.com/faq-the-projectsauron-apt/75533/.

[48] R. S. Ross, "Managing information security risk: organization, mission, and information system view," National Institute of Standards and Technology, Gaithersburg, MD, 2011.

[49] FireEye Labs, "Less than zero: a survey of zero-day attacks in 2013 and what they say about the traditional security model," 2013 [Online]. Available: https://www.fireeye.jp/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-zero-day-attacks-in-2013.pdf.

[50] L. Ablon and A. Bogart, *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits*. Santa Monica, CA: Rand Corporation, 2017.

[51] L. Bilge and T. Dumitras, "Before we knew it: an empirical study of zero-day attacks in the real world," in *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, Raleigh, NC, 2012, pp. 833-844.

[52] N. Moran and M. Oppenheim, "Darwin's Favorite APT Group," 2014 [Online]. Available: https://www.fireeye.com/blog/threat-research/2014/09/darwins-favorite-apt-group-2.html.

[53] V. Kotov and F. Massacci, "Anatomy of exploit kits," in *Engineering Secure Software and Systems*. Heidelberg: Springer, 2013, pp. 181-196.

[54] Kaspersky Lab, "Exploits: how great is the threat?," 2017 [Online]. Available: https://securelist.com/exploits-how-great-is-the-threat/78125/.

[55] Minerva Labs and ClearSky Cyber Security, "CopyKittens Attack Group," 2015 [Online]. Available: https://s3-eu-west-1.amazonaws.com/minervaresearchpublic/CopyKittens/CopyKittens.pdf.

[56] Symantec Corporation, "The increased use of powershell in attacks," 2016 [Online]. Available: https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/increased-use-of-powershell-in-attacks-16-en.pdf.

[57] N. Villeneuve, J. T. Bennett, N. Moran, T. Haq, M. Scott, and K. Geers, "Operation 'KE3CHANG': Targeted Attacks against Ministries of Foreign Affairs," 2014 [Online]. Available: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-ke3chang.pdf.

[58] FireEye Lab, "Operation DeputyDog: Zero-Day (CVE-2013-3893) attack against Japanese targets," 2013 [Online]. Available: https://www.fireeye.com/blog/threat-research/2013/09/operation-deputydog-zero-day-cve-2013-3893-attack-against-japanese-targets.html.

[59] J. Miller-Osborn, "Credential-based attacks: exposing the ecosystem and motives behind credential phishing, theft and abuse," 2017 [Online]. Available: https://www.paloaltonetworks.com/resources/research/unit-42-credential-based-attacks.

[60] Dell SecureWorks Counter Threat Unit Threat Intelligence, "Hacker group creates network of fake LinkedIn profiles," 2015 [Online]. Available: https://www.secureworks.com/research/suspected-iran-based-hacker-group-creates-network-of-fake-linkedin-profiles.

[61] FireEye iSIGHT Intelligence, "APT28: at the center of the storm," 2017 [Online]. Available: https://www.fireeye.com/blog/threat-research/2017/01/apt28_at_the_center.html.

[62] D. Alperovitch, "Bears in the Midst: intrusion into the Democratic National Committee," 2016 [Online]. Available: https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

[63] C. Missaoui, S. Bachouch, I. Abdelkader, and S. Trabelsi, "Who is reusing stolen passwords? An empirical study on stolen passwords and countermeasures," in *Cyberspace Safety and Security*. Cham: Springer, 2018, pp. 3-17.

[64] M. S. Webb, "Evaluating tool based automated malware analysis through persistence mechanism detection," Ph.D. dissertation, Kansas State University, Manhattan, KS, 2018.

[65] N. Moran, S. Omkar Vashisht, M. Scott, and T. Haq, "Operation ephemeral hydra: IE Zero-Day linked to DeputyDog uses diskless method," 2013 [Online]. Available: https://www.fireeye.com/blog/threat-research/2013/11/operation-ephemeral-hydra-ie-zero-day-linked-to-deputydog-uses-diskless-method.html.

[66] Y. M. Wang, R. Roussev, C. Verbowski, A. Johnson, M. W. Wu, Y. Huang, and S. Y. Kuo, "Gatekeeper: monitoring auto-start extensibility points (ASEPs) for spyware management," in *Proceedings of the 18th Large Installation System Administration Conference (LISA)*, Atlanta, GA, 2004, pp. 33-46.

[67] N. Miloslavskaya, "Remote attacks taxonomy and their verbal indicators," *Procedia Computer Science*, vol. 123, pp. 278-284, 2018.

[68] Symantec Corporation, ""Forkmeiamfamous": Seaduke, latest weapon in the Duke armory," 2015 [Online]. Available: https://www.symantec.com/connect/blogs/forkmeiamfamous-seaduke-latest-weapon-duke-armory.

[69] B. E. Strom, J. A. Battaglia, M. S. Kemmerer, W. Kupersanin, D. P. Miller, C. Wampler, S. M. Whitley, and R. D. Wolf, "Finding cyber threats with ATT&CK-based analytics," The MITRE Corporation, Bedford, MA, Technical Report No. MTR170202, 2017.

[70] McAfee Labs, "Global energy cyberattacks: 'Night Dragon'," 2011 [Online]. Available: https://securingtomorrow.mcafee.com/wp-content/uploads/2011/02/McAfee_NightDragon_wp_draft_to_customersv1-1.pdf.

[71] A. Hosseini, "Ten process injection techniques: a technical survey of common and trending process injection techniques," 2017 [Online]. Available: https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process.

[72] Microsoft, "Working with the AppInit DLLs registry value," 2018 [Online]. Available: https://support.microsoft.com/en-us/help/197571/working-with-the-appinit-dlls-registry-value.

[73] M-Lab, "DLL search order hijacking revisited," 2010 [Online]. Available: https://www.fireeye.com/blog/threat-research/2010/08/dll-search-order-hijacking-revisited.html.

[74] Microsoft, "Dynamic-link library search order," 2018 [Online]. Available: https://docs.microsoft.com/en-gb/windows/win32/dlls/dynamic-link-library-search-order.

[75] S. Narang, "Backdoor.Barkiofork targets aerospace and defense industry," 2013 [Online]. Available: https://www.symantec.com/connect/blogs/backdoorbarkiofork-targets-aerospace-and-defense-industry.

[76] Symantec Corporation, "Backdoor.Barkiofork," 2013 [Online]. Available: https://www.symantec.com/security-center/writeup/2012-042403-0432-99.

[77] A. Stewart, "DLL side-loading: a thorn in the side of the anti-virus industry," 2016 [Online]. Available: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-dll-sideloading.pdf.

[78] Dell SecureWorks Counter Threat Unit Threat Intelligence, "Threat Group 3390 cyberespionage," 2015 [Online]. Available: https://www.secureworks.com/research/threat-group-3390-targets-organizations-for-cyberespionage?_ga=1.132970126.1294297346.1479934134.

[79] J. Grunzweig, "Unit 42 Technical Analysis: Seaduke," 2015 [Online]. Available: https://unit42.paloaltonetworks.com/unit-42-technical-analysis-seaduke/.

[80] G Data SecurityLabs, "COM Object hijacking: the discreet way of persistence," 2014 [Online]. Available: https://www.gdatasoftware.com/blog/2014/10/23941-com-object-hijacking-the-discreet-way-of-persistence.

[81] ESET, "En route with Sednit," 2016 [Online]. Available: https://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part1.pdf.

[82] V. Rusakov and S. Golovanov "Attacks before system startup," 2014 [Online]. Available: https://securelist.com/attacks-before-system-startup/63725/.

[83] J. Gardiner, M. Cova, and S. Nagaraja, "Command & Control: Understanding, Denying and Detecting-A review of malware C2 techniques, detection and defences," 2014 [Online]. Available: https://arxiv.org/abs/1408.1136.

[84] D. Chiu, S. H. Weng, and J. Chiu, "Backdoor use in targeted attacks," Trend Micro Incorporated, Irving, TX, 2014.

[85] S. Shafieian, D. Smith, and M. Zulkernine, "Detecting DNS tunneling using ensemble learning," in *Network and System Security*. Cham: Springer, 2017, pp. 112-127.

[86] S. Tanase, "Satellite Turla: APT command and control in the sky," 2015 [Online]. Available: https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/.

[87] J. Power, "Mind the gap: are air-gapped systems safe from breaches?," 2014 [Online]. Available: https://www.symantec.com/connect/blogs/mind-gap-are-air-gapped-systems-safe-breaches.

[88] Symantec Corporation, "Flamer: highly sophisticated and discreet threat targets the Middle East," 2012 [Online]. Available: https://www.symantec.com/connect/blogs/flamer-highly-sophisticated-and-discreet-threat-targets-middle-east.

[89] Microsoft, "Featured intelligence (Microsoft Security Intelligence Report Volume 19)," 2015 [Online]. Available: https://download.microsoft.com/download/4/4/C/44CDEF0E-7924-4787-A56A-16261691ACE3/Microsoft_Security_Intelligence_Report_Volume_19_English.pdf

Pooneh Nikkhah Bahrami https://orcid.org/0000-0002-1514-2920

She received her M.Sc. in Software Engineering from Tehran University, Iran in 2016 and her B.Sc. in Information Technology from University of IASBS, Iran in 2011. She is currently a lecturer in the Department of Computer Science, Azad University, Kish Island, Iran. Prior to joining Azad University, she worked as a research assistant at ICT research institute in Tehran. Her research interest includes security in wireless networks and cyber security.

Ali Dehghantanha https://orcid.org/0000-0002-9294-7554

He received his Ph.D. in Computer Security in 2011. Ali is the director of Cyber Science Lab (http://cybersciencelab.org/) in University of Guelph (UofG), Ontario, Canada. His lab is focused on building AI-powered solutions to support cyber threat attribution, cyber threat hunting and digital forensics tasks. Ali has served for more than a decade in a variety of industrial and academic positions with leading players in Cyber-Security and Artificial Intelligence. Prior to joining UofG, he has served as a Sr. Lecturer in the University of Sheffield, UK and as an EU Marie-Curie International Incoming Fellow at the University of Salford, UK.

Tooska Dargahi https://orcid.org/0000-0002-0908-6483

She is a lecturer in cybersecurity at the University of Salford, Manchester, UK. From 2015 to 2017 she was a postdoctoral researcher at CNIT- University of Roma Tor Vergata research unit, Rome, Italy, working on EU H2020 Projects. She received her Ph.D. in Computer Engineering from Azad University, Science and Research Branch, Tehran, Iran in 2014. She was a visiting PhD at University of Padua, Italy in 2014. Her main research interests are security and privacy in various networking areas, as well as applied cryptography and cybersecurity.

Reza M. Parizi https://orcid.org/0000-0002-0049-4296

He received the Ph.D. in Software Engineering in 2012 and M.Sc. and B.Sc. degrees in Computer Science respectively in 2008 and 2005. He is currently a faculty in the College of Computing and Software Engineering at Kennesaw State University, GA, USA. He is the member of IEEE, IEEE Blockchain Community, IEEE Computer Society and ACM. Prior to joining KSU, he was an Associate Professor at New York Institute of Technology. His research interests are R&D in blockchain, smart contracts, IoT and emerging issues in the practice of secure software-run world applications.

Kim-Kwang Raymond Choo https://orcid.org/0000-0001-9208-5336

He received the Ph.D. in Information Security in 2006 from Queensland University of Technology, Australia. He currently holds the Cloud Technology Endowed Professorship at The University of Texas at San Antonio (UTSA). In 2016, he was named the Cybersecurity Educator of the Year - APAC (Cybersecurity Excellence Awards are produced in cooperation with the Information Security Community on LinkedIn), and in 2015 he and his team won the Digital Forensics Research Challenge organized by Germany's University of Erlangen-Nuremberg. He is the recipient of the 2019 IEEE

Technical Committee on Scalable Computing (TCSC) Award for Excellence in Scalable Computing (Middle Career Researcher), 2018 UTSA College of Business Col. Jean Piccione and Lt. Col. Philip Piccione Endowed Research Award for Tenured Faculty, Outstanding Associate Editor of 2018 for IEEE Access, British Computer Society's 2019 Wilkes Award Runner-up, 2019 *EURASIP Journal on Wireless Communications and Networking* (JWCN) Best Paper Award, Korea Information Processing Society's *Journal of Information Processing Systems* (JIPS) Survey Paper Award (Gold) 2019, IEEE Blockchain 2019 Outstanding Paper Award, IEEE TrustCom 2018 Best Paper Award, ESORICS 2015 Best Research Paper Award, 2014 Highly Commended Award by the Australia New Zealand Policing Advisory Agency, Fulbright Scholarship in 2009, 2008 Australia Day Achievement Medallion, and British Computer Society's Wilkes Award in 2008. He is also a Fellow of the Australian Computer Society, an IEEE Senior Member, and Co-Chair of IEEE Multimedia Communications Technical Committee's Digital Rights Management for Multimedia Interest Group.

Hamid H. S. Javadi https://orcid.org/0000-0003-0082-036X

He received his B.Sc. in Computer Science and Mathematics, in 1993, his M.Sc. in Computer Algebra, in 1995, and his Ph.D. in Computational Algebra in 2002, from Amirkabir University of Technology, Tehran, Iran. He was ranked as the top student during his education. He is currently an Associate Professor in the Department of Mathematics and Computer Science, Shahed University, Tehran, Iran. His research interests are Algorithms, Algebra, and Combinatorial Designs and their applications in security and cryptography.