Security Vulnerability Assessment and Malware Analysis for Next-Generation ICT Technologies : Focused on the case of Cryptocurrency and IoT

Jiyeon Baek

Department of Future Convergence Technology Engineering

The Graduate School of Sungshin University

Security Vulnerability Assessment and Malware Analysis for Next-Generation ICT Technologies : Focused on the case of Cryptocurrency and IoT

A Master's Thesis
Submitted to the
Graduate School of Sungshin University

in partial fulfillment of the requirements
for the degree of
Master of Future Convergence Technology
Engineering

Jiyeon Baek

June, 2023

This is to certify that we have examined the
Master's Thesis of
Jiyeon Baek
Submitted to Department of Future Convergence
Technology Engineering

Approved as to style and content:

Thesis Advisor 김 성 민

Committee Chairman 이 일 구

Committee Member 임 연 섭

The Graduate School of Sungshin University

Abstract

Security Vulnerability Assessment and Malware Analysis for Next-Generation ICT Technologies : Focused on the case of Cryptocurrency and IoT

Jiyeon Baek
Department of Future Convergence Technology Engineering
The Graduate School of
Sungshin University

In the Fourth Industrial Revolution society, the next-generation ICT technologies are increasingly indispensable across diverse fields such as finance, transportation, and public institutions. For example, blockchain technology, renowned for its attributes of anonymity, reliability, and security, stands out as a representative example of its integration into various applications, including cryptocurrencies and decentralized exchanges. Similarly, the Internet of Things (IoT) occupies a significant position as one of the key elements in a hyper-connected society. It manifests itself through smart homes, connected cars, and drones, among others. Despite of the widespread adoption of these technologies, however, there remains a need for the evaluation and assessment of

their security aspects. In particular, the rise of malware that exploits cryptocurrencies, such as ransomware and crypto-miners, is impacting the next generation of ICT technologies, including IoT.

This study classifies malware that monetizes cryptocurrency into Advanced Persistent Threats (APTs) and non-APTs, and analyzes each malware in terms of cryptocurrency exploitation and damage scale to derive their characteristics. Furthermore, an IoT drone is specifically chosen to simulate an attack scenario targeting remote update technology. The study aims to investigate the possibility of deliberately delaying Over-The-Air (OTA) updates, hindering the installation of the latest firmware patches on IoT devices. Finally, by examining attack traces from a memory forensics perspective, the research highlights the potential for forensic analysis in future attacks.

Contents

Table Contents

Figure Contents

Ⅰ. Introduction

In the era of the Fourth Industrial Revolution, various fields are embracing next-generation ICT (Information and Communication Technology) technologies. An example of such technology is blockchain, which employs a distributed ledger technology (DLT) to document transactions within a network. Blockchain technology is renowned for its exceptional reliability and robust security measures and finds widespread application in various domains, including cryptocurrencies and decentralized finance (DeFi) exchanges.

Another example of next generation ICT is the Internet of Things (IoT), which stands out as a prominent technology that has gained broad adoption across numerous domains such as smart homes, connected cars, and smart cities. A report by Marketsandmarkets [1] indicates that the global IoT market is estimated to reach a size of $650.5 billion by the year 2026. This growth projection highlights the increasing significance and pervasive nature of IoT as a vital component of our interconnected world.

However, as these technologies continue to advance, the threat of malware targeting them is also on the rise. For example, in a specific incident involving a malware attack on a DeFi platform, a vulnerability in the decentralized exchange KyberSwap was exploited to compromise the platform and result in the theft of customers' virtual currency. The stolen funds were estimated to be valued at approximately $265,000 [2].

Furthermore, Shikitega malware specifically targets Internet of Things (IoT) devices and Linux systems. The malware infiltrates the compromised targets and installs a cryptominer, allowing attackers to generate illegal revenue [3].

Based on this background, this study conducts research on malware trends and security vulnerabilities in IoT devices.

(1) Analyzing the trends of malware that exploits cryptocurrencies for profit in terms of monetary damages, specifically classifying them into APT (Advanced Persistent Threat) types and non-APT types, and analyzing their respective characteristics and differences.

(2) Among the various types of IoT devices, IoT drones are chosen for vulnerability analysis and conducting security assessments to identify potential vulnerabilities for future malware infections.

This thesis is structured as follows. Chapter Ⅱ provides an analysis of malware trends and characteristics. Chapter Ⅲ presents a comprehensive security review of IoT drones, including an analysis of security vulnerabilities and forensic research. Chapter Ⅳ concludes the thesis by synthesizing the results of both studies.

Ⅱ. On the Analysis of Recent Malware Attacks and its Social Ramification

1. Introduction

In the age of hyper-connectivity, malware is constantly evolving and adopting new forms that pose a serious and ongoing threat. In particular, malware that exploits cryptocurrencies as a means of revenue is on the rise. According to Kaspersky, crypto-mining malware increased by 230% in 2022 compared to the previous year, and ransomware continues to hold a prominent position as a major trend in security threats [4][5]. In addition, the percentage of ransomware and cryptominators among malware installed through unpatched vulnerabilities has steadily increased throughout 2022 [6].

Historically, malware had a tendency to target random computers on the internet by spreading themselves through interconnected network without discrimination. However, in recent times, malware has shifted to a more focused approach with advanced persistent threats (APTs). APT malware specifically selects and targets certain companies or organizations, including government agencies, industrial systems, and private businesses. These sophisticated malware variants are designed to carefully gather sensitive information about their targets and gradually infiltrate their systems, enabling them to carry out long-term and persistent attacks. Compared to random attacks targeting unknown individuals, these targeted attacks yield greater financial gains for the attackers and have a more significant impact on society.

In this paper, the earlier indiscriminate malware attacks are classified as 'non-APT', and a comparative analysis is conducted to examine their economic damages and technical implications in relation to recent 'APT' malware attacks. Especially, the analysis focuses on the scale of financial losses associated with the exploitation of cryptocurrencies.

The remainder of the paper is organized as follows. Section 2 covers basic concepts related to the paper. Section 3 describes each non-APT malware and its impact on monetary damage, and Section 4 focuses on APT malware. Section 5 discusses the result of both analyses and analyzes relevant countermeasures around the world. The conclusion of this paper is presented in Section 6.

2. Background

1) Cryptocurrency

Cryptocurrency built on a peer-to-peer (P2P) blockchain network has become a predominant digital asset with the rise of non-fungible tokens (NFTs) and decentralized finance (DeFi). As the structure is decentralized, there is no third party with the exclusive ability to examine transaction data between users, therefore guaranteeing the anonymity of transactions. Such properties of cryptocurrencies, however, become a double-edged sword, as they are used for a wide range of crimes, including malware (e.g., ransomware), and regularly traded on associated Dark Web markets. Moreover, if a criminal utilizes a 'mixing' service that mixes the cryptocurrency transaction process, money laundering is conceivable, and transaction history monitoring becomes almost impossible [7].

Figure 1 depicts the percentage of cryptocurrency transactions disclosed by Coinmarketcap [8]. It states that Bitcoin is still the dominant option for trading products or other cryptocurrencies. As of September 11, 2022, Bitcoin held the greatest market share with 39.06%, followed by Ethereum with 20.45%. From the malware analysis perspective, a recent malware follows the trend; an attacker specifies a Bitcoin wallet address for a ransomware decryption payment, and it is the most typical currency to purchase illicit products on the Dark Web.

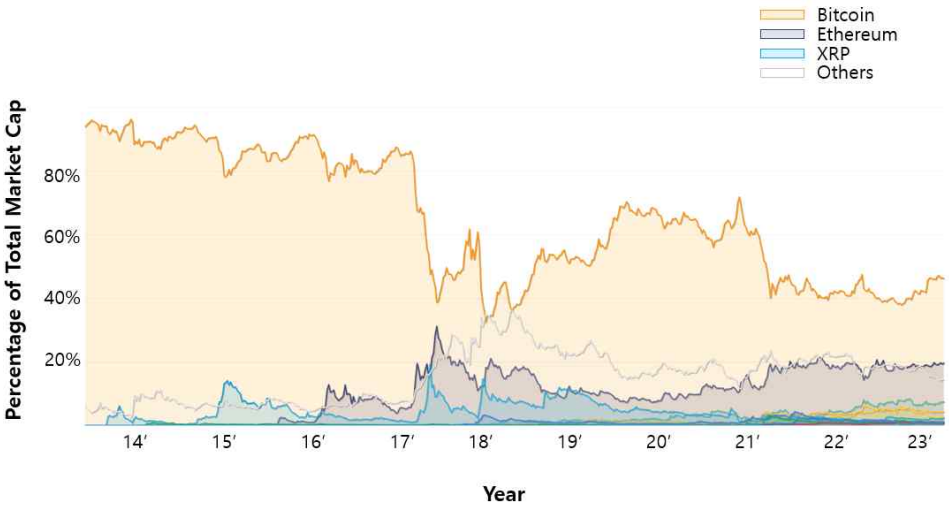


FIGURE 1. Major Crypto Assets By Percentage of Total Cryptocurrency Market Capitalization [8]

Bitcoin transactions are also considerable in terms of ransomware decryption payment methods. In 2021, however, the adoption of the cryptocurrency Monero as a ransomware decryption payment method grew marginally. Due to Bitcoin's anonymity concerns and the additional expenses associated with anonymizing transactions, ransomware attackers demand a 10% premium over other cryptocurrencies. For instance, after being infected with ransomware, Colonial Pipeline, an American oil pipeline corporation, could pick Bitcoin or Monero as payment for decryption. The victimized corporation paid 75 bitcoins despite the 10% surcharge, and the FBI was able to track down the payment and recover 63.7 bitcoins [9]. Monero and Dash, on the other hand, are likely to be misused for such crimes given that all transaction information is guaranteed to be

anonymous [10]. Nevertheless, despite the surge in Monero's trading volume, Bitcoin remains dominant due to its limited liquidity issue of Monero as it is also hard to cash it out [10].

Meanwhile, as institutional investments and individual transactions using virtual currency expands, the crime rate of money laundering using cryptocurrency is also increasing [11]. According to Chainalysis, around $8.6 billion worth of cryptocurrencies were misused in money laundering in 2021, a 30% increase over the previous year. As a quick response to such a phenomenon, the Financial Action Task Force (FATF)[1] on money laundering recommended the contents and application of the travel rule[2], a "money movement tracking system" that existed in the financial sector and to strengthen country-specific regulations by expanding their scope to include virtual currency [11].

2) Cryptojacking

One of the remarkable attacks on cryptocurrencies is covert crypto mining, called cryptojacking, a method of earning profit by mining by stealthily abusing the victim's computing resources. Among the cryptocurrency mining techniques, such as PoW (Proof of Work), PoS

---

1) It is an intergovernmental organization in which 37 nations and two international organizations participate, including Korea, the United States, the United Kingdom, and Japan. It formulates policies to prevent money laundering and reinforces international cooperation [13].

2) As an international rule to avoid money laundering, the sender's information must be recorded when remittances are made overseas in line with the mandated format of the Society for Worldwide Interbank Financial Telecommunications (SWIFT).

(Proof of Stake), and DPoS (Delegated Proof of Stake), PoW is the most dominant and typical case as it is used for Bitcoin and Ethereum [12]. For maintaining the PoW-based Blockchain network, devices that provide computing power (e.g., CPU and GPU) acquire the coins in exchange for a reward for performing complex calculations, such as hash computation processing. In addition, power consumption is substantial while mining Bitcoin using a CPU or GPU, making it challenging to generate significant profit [14]. To evade this, an attacker utilizes malicious crytominers to exploit the victims' devices and abuse their resources to mine Bitcoin. By doing so, an adversary successfully acquires Bitcoin without paying a mining fee. Once the host is infected with cryptojacking malware, symptoms include performance degradation owing to increased PC use; however, most victims are ignorant of the infection. Non-APT attacks that are further discussed in the upcoming sections, such as HackBoss, Crackonosh, and Mykings, contain malicious codes exhibiting these features.

3) Clipboard Hijacking

Clipboard hijacking is a method that penetrates loophole circumstances of cryptocurrency wallet users; when copying and pasting a cryptocurrency wallet address, the hijacker swaps the address with a particular address. Cryptocurrency wallet addresses include lengthy sequences of more than 30 characters and digits for

security concerns [15]. As it is hard to memorize, individuals often save it as a text file (e.g., using the notepad application) and copy-and-paste it while trading virtual currency. Malware that exploits such attack surface is known as a clipboard hijacker or clipper, and they have been discovered on PCs, smartphones, and tablets. Since users do not check and verify such long strings exactly, they will continuously generate transactions without realizing the hijacking. Note that Phorpiex (Twizt) and Mykings employed such vulnerabilities.

4) Ransomware as a Service (RaaS)

A recent trend in cybercrime marketplaces is the emergence of Ransomware-as-a-Service (RaaS). Ransomware is a denial-of-service (DoS) attack making an individual's data inaccessible by keeping them encrypted until the victim pay for the demands. Since malware, like ransomware, needs specialized knowledge to craft, hackers with special techniques can build and utilize them. However, with the emergence of ransomware as a Service (RaaS), anyone can purchase and use it without expertise. Hence, the entrance barrier for ransomware-based attacks has become extremely low, and similar attacks are still rising [16]. Indeed, based on the analysis, the vast majority of ransomware investigated in this study utilizes RaaS. Note that most ransomware is traded via Bitcoin on the Dark Web, and the purchasers share some of their gains with the ransomware developer in the case of a successful attack.

3. Malware classification: APT vs non-APT

As described above, malware analysis classification in this paper is based on the presence of APT attack capabilities. APT attacks are clandestine and prolonged attacks against the high-value targets, including large organizations, corporations across various industries, and even government departments. Once APT attackers gain an unauthorized access to a target system, they conceal themselves and deepen their access to acquire greater capabilities within the system. Generally, they establish connections to Command and Control (C&C) servers to remotely execute their objectives, while gaining knowledge of the system's functioning and ultimately sabotage the targeted entity.

The primary objectives of APT attackers are to generate financial gains and achieve notoriety by seizing a target's confidential data. Additionally, some APT attackers employ a tactic known as double extortion, which involves encrypting the victim's files and exfiltrating the data. This allows the attackers to threaten the victim with data leakage or the sale of stolen data if the victim refuses to pay for decryption.

Since the targets of APT malware are gigantic and their data is highly sensitive, the repercussions of APT malware are more severe compared to malware that randomly propagates to individuals. Given this characteristic, the malware analyzed in this study can be classified into two distinct categories: (i) APT malware, which is

associated with APT campaigns, and (ii) non-APT malware, which targets the uncertain.

The classification in this study is established on the basis of four criteria, which are detailed in Table 1. A malware case is classified as APT if it meets a minimum of three of these criteria, including the first criterion. The analysis specifically focuses on 19 instances of malware over a period of 10 years, during which financial information was compromised, with a particular emphasis on assessing the financial impact.

Table 1. Malware classification

Malware	Is its focus on specific targets?	Does it target more than just individuals?	Does it engage in active attack?	Does it specifically target confidential data?	Feature
Hackboss	X	X	X	X	Masquerades clipboard hijacker as a hacking tool and sells it on Telegram.
Crackonosh	X	X	X	X	Spread via cracked versions of popular games on torrent platforms.
Magniber	X	X	X	X	Distributed through malvertising, operating illegal websites, or by masquerading as update packages.
Phorpiex	X	X	X	X	Utilizes sextortion campaigns(scams) and operates in a P2P mode without the need for a C&C Server.
Mykings	X	O	O	O	Employs a brute-force attack to target vunlerable servers.
Dridex	X	X	X	X	Propagated through phishing emails and operated as a banking Trojan horse.
Klayswap	O	O	O	O	The first case of BGP hijacking in Korea.
Blackcat	O	O	O	O	Using Rust in ransomware programming which makes it easier to bypass security systems.
Blackmatter	O	O	O	O	Specifically targets entities with annual revenues exceeding $ 100 million, excluding certain entities.
Phoneix	O	O	O	O	Disguises itself as browser update software, targeting CNA financial.
Darkside	O	O	O	O	Known to be based in Eastern Europe and Russia, gained notoriety for their attack on the Colonial
Cuba	O	O	O	O	Targets across five sectors : financial, government, medical, manufacturing and IT.
Conti	O	O	O	O	Developed by Russian hacking group Wizard Spider, and capable of attacking all versions of Microsoft
Lockbit	O	O	X	O	The first ransomware to include their own bug bounty program.
Revil	O	O	O	O	Attacks a US software provider and infects 1,500 client companies associated with the target.
Netwalker	O	O	X	O	Primarily targets medical institutions with phishing emails relate to Coronavirus 19.
Clop	O	O	O	O	Targets entities that uses the Active Directory(AD), and infiltrates AD to obtain administrator privileges.
Lockergoga	O	O	O	O	Infects the Norwegian aluminum manufacturer, leading to a worldwide increase in the price of aluminum.
Ryuk	O	O	O	O	Used by Wizard Spider, specifically attacks high-value entities such as UHS hospital and EMCOR Group.

a. Is its focus on specific targets?

APT attacks are distinguished by their sustained preparation and execution over an extended duration, involving the selection of specific targets and in-depth prior analysis of their characteristics. In this study, the classification of malware as APT is determined by the fulfillment of three or more conditions, including the corresponding item.

b. Does it target more than just individuals?

Since APT attacks typically target corporations or organizations on a larger scale, individual-level attacks do not align with the typical characteristics of APT. The MyKings malware is classified as a non-APT malware due to its lack of specific targeting towards clearly designated targets and its primary use of crypto mining as a major attack technique. However, it does satisfy the condition as it demonstrates a pattern of multiple infections occurring within organizational units during the transmission process.

c. Does it engage in active attack?

This classification is based on the method of spreading malware and inducing infection, distinguishing between passive and active attacks. A 'passive attack' refers to situations where infection is facilitated without specifically targeting a predetermined number of individuals. Examples of passive attacks include uploading a program containing malware on an illegal download site or

distributing phishing emails to a large number of people. In contrast, an ‘active attack’ involves active interventions, such as sending customized spear phishing emails to certain targets. For instance, the distribution of Magniber malware involved inducing users to download apps disguised as normal files. This method is considered as a passive attack and is classified as X under the given conditions.

d. Does it specifically target confidential data?

The purpose of APT malware targeting companies or organizations extends beyond simply disrupting or destroying their services. Most often, APT attacks aim to steal and encrypt classified and confidential data for the purpose of demanding ransom or leaking it to illicit markets like the dark web. In other words, since the value of confidential data at the corporate level is generally higher compared to the information held by randomly infected individual victims, attacks that specifically target confidential data are classified as APT malware. Ransomware, which falls under the category of malware attack methods, fulfills this criterion as it extorts money by leveraging confidential data as hostage.

4. Non-APT Malware

This Section focuses on analyzing the non-APT malware and its financial damage, enumerating the details of the incident in technical aspects. Unfortunately, because the non-APT malware targets random victims on the internet, information about the monetary damage was not publicly available, which limited the ability to analyze a wider rage of malware.

1) HackBoss Malware

HackBoss is a cryptojacking malware that spreads using the popular messaging application Telegram. Since November 2018, a Telegram channel named "Hack Boss" has been promoting and distributing various hacking software under the slogan *"The best software for hackers (hack bank / dating / bitcoin)"*. In fact, these applications are only a camouflage for installing a clipboard hijacker on the user's computer, and do not deliver the Telegram-promoted functionalities. Once the user launches the fake application and clicks any button of it, the malicious payload triggered to install a clipboard hijacker. After the installation, the clipboard hijacker keeps detecting a wallet address form in the clipboard and exchanges it to hacker's wallet address. Figure 2 shows the UI of the application. More than 100 cryptocurrencies, such as Bitcoin, Ethereum, and Dogecoin, were mined by HackBoss over the course of 17 months from the time of release to April 2021, resulting in about

$560,000 in damages [17].

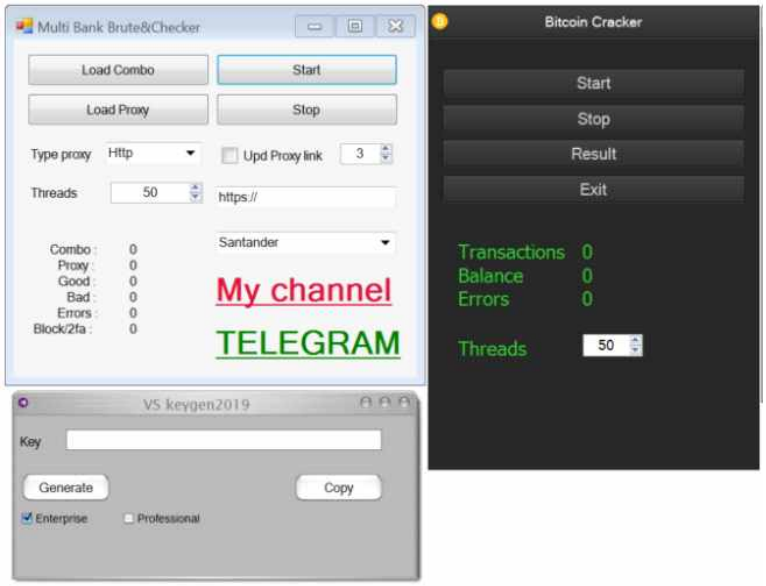


FIGURE 2. Application UI Examples [17]

2) Crackonosh Malware

Crackonosh is a cryptojacking malware that mines the cryptocurrency Monero (XMR), spread via cracked copies of popular games released for free on torrent platforms. When a user launches a crack game, Crackonosh alters the Windows Registry to boot the computer in safe mode and XMRig, a software that mines XMR in safe mode, finally begins to operate. Since its discovery in 2018, Crackonosh has been detected in over 12 countries, including the Philippines, Brazil, and India, and the estimated number of victims is over 220,000 [18]. As of June 2021, over 9,000 XMR has been mined, which is equivalent to over 2

million dollars [19].

3) Magniber Malware

Magniber is a ransomware appeared in 2017 and has been continuously identified to date. It is distributed through illegal free video download sites or malvertising techniques that abuse internet advertisements. Also, the distribution mechanism recently found in 2022 features a typo-squatting attack that redirects users to different websites in the case of user errors, such as misspelling the URL or wrong top-level domain entry. Once a user accidently visits the attacker-intended website, a ransomware masquerading as a Microsoft Windows update or Windows installation package (MSI) is automatically downloaded to the user's system. One of the noticeable features of Magniber is that it only operates when the language of the infected system is Korean; otherwise, it ceases to function and deletes itself. Magniber requires around $2,500 in Bitcoin for decryption and instructs to pay using the Tor browser [20]. Although the total amount of damage caused by Magniber is unknown, it accounted for about 61% of ransomware varieties identified in Korea between 2015 and 2021 according to the RanCERT(Ransomware Computer Emergency Response Team Coordination Center) in 2021 [21].

4) Phorpiex and Twizt Malware

Phorpiex is a botnet that first appeared in 2016 and has spread as sextortion spam, crypto-jacking, crypto-clipping, or performs as a

distributor of other ransomwares. Originally, the botnet utilized the Internet Relay Chat (IRC) protocol, but since 2018 it has been moved to a modular architecture and has remained active by loading more modules from the server over the HTTP protocol [22]. In the latter part of 2021, a new variation named Twizt botnet emerged, featuring a peer-to-peer (P2P) mode. This mode allows the infected PC to operate as a new server and provide orders to other connected bots, enabling the Twizt botnet to operate independently without relying on C&C servers. If a connection with C&C server is required due to extra payload downloads, it can dynamically alter the IP address of the server, allowing the C&C server to be connected as needed without revealing the actual IP of it [23].

Phorpiex and Twizt were discovered in 96 countries, mostly Ethiopia, Nigeria, and India, and launched crypto-clipping attacks against more than 30 cryptocurrency exchanges. Damage is assumed to exceed $500,000 from December 2020 to December 2021, including 3.64 Bitcoin (approximately $172,300), 55.87 Ethereum (approximately $216,000), and $55,000 worth of ERC20. Moreover, from April 2016, when the malware first emerged, to December 2021, 38 Bitcoins and 133 Ethereum have been lost, and the loss is expected to be substantially larger if other cryptocurrency losses are included [24].

5) Mykings Malware

The Mykings botnet, which is also known as Smominru, DarkCloud, and Hidden, specializes in cryptocurrency mining as well as other

malicious activities. It uses brute-force attacks to steal user information from vulnerable SQL servers or infects associated networks by exploiting vulnerabilities in unpatched servers [25]. After the infection, Mykings installs a cryptominer on the victim's computer or it utilizes the clipboard hijacker to swap the victim's cryptocurrency wallet address for the hacker's one. The Mykings botnet does not target a single company or industry, although certain universities and distributors have also been affected. Also, China, Taiwan, Russia, and the United States are among the most afflicted nations [26]. As of May 2021, the attackers gained more than 132 Bitcoin (approximately $6,630), about 2,158 Ethereum (approximately $7,430), and over 45 million Dogecoins (approximately $110 million), which is comparable to more than $24.7 million. It is anticipated to be more if revenues from the other 20 or so cryptocurrencies are included [27].

6) Dridex Malware

Dridex is a banking Trojan that steals online financial information and credentials with the purpose of access to victim's financial asset. It is mostly propagated through Word or Excel file attached to phishing email, which is sent to an unspecified number of people. When a user opens an attached file, the hidden macro is activated and the Dridex malware is downloaded. If a user's web browser (e.g. Chrome or Internet Explorer) is accessing online backing applications or websites, Dridex injects a keylogger to collects a user's login

credentials and financial information which are used to set up a fraudulent account. Recently, it has been distributed by exploiting the Log4Shell which is an up to date zero-day vulnerability in Apache Log4j [28]. From 2014 to the present, Dridex has evolved and spread throughout English-speaking countries, damaging over 300 banks in over 40 countries [29]. The entire amount of damage is expected to exceed one million dollars [30].

7) Summary

Table 2 shows a chronological summary of non-APT malware analysis. In the “Category” column, the “Etc” stands for alternative methods of attack. If a non-APT malware functions as Ransomware-as-a-Service (RaaS), it is indicated with a "Y," while a "-" signifies its absence. Under the "Related Cryptocurrency" column, "Other" refers to other cryptocurrencies employed by the malware, whereas "Unknown" indicates cases where information regarding the source of funds obtained by the malware is not provided. As evident in Table 2, non-APT malware have leveraged diverse attack techniques, including ransomware, crypto-jacking, and clipboard hijacking. Additionally, each of the malware analyzed in this paper has utilized numerous types of cryptocurrency as payment methods. Concerning monetary gains, aggregating revenue figures is challenging because the non-APT malware is spread in a scattershot way, resulting in limited cases within this paper. Nonetheless, the overall financial damage caused by non-APT malware typically exceeds $1 million, with some instances surpassing $25 million in losses.

TABLE 2. Summary of non-APT malware trend analysis

Non-APT Malware

Malware	Year	Category					RaaS	Monetary Gain (Million)	Related Cryptocurrency					
		Ransomware	Crypto-Jacking	Clipboard Hijacker	Financial Trojans	Etc			Bitcoin	Monero	Ethereoum	Dogecoin	Etc	Unknown
HackBoss	2018.11		✔				-	$560,000	✔	✔	✔	✔	✔	
Crackonosh	2018		✔				-	$ 2 million		✔				
Magniber	2017	✔					-	$ 3.4 million	✔					
Phorpiex(Twizt)	2016(2021)			✔			-	$ 1.1 million	✔	✔	✔	✔	✔	
Mykings	2016		✔	✔			-	$ 24.7 million	✔		✔	✔	✔	
Dridex	2015				✔		-	$ 1 million						✔

5. APT Malware

Next, this section provides an in-depth analysis of each APT malware, including both technical and economic aspects. As previously mentioned, APT malware specifically targets select victims, including large-scale targets. Consequently, the impact of these attacks is anticipated to be significantly more substantial compared to non-APT malware incidents.

1) The Case of Attack on KLAYSwap Service

The largest Decentralized Finance (DeFi)[3] service in Korea, KLAYSwap, was hacked by nameless malware in February 2022. The attack utilized the BGP Hijacking; a network attack where an attacker manipulates the routers to redirect the network traffic to an attacker's network. When implementing the service, KLAYSwap dynamically loads the Kakao SDK (Software Development Kit) from the server. But with the BGP Hijacking attack, attacker could make an arbitrary SSL certificate possible and redirect the normal SDK request connection to the attack server. Eventually, the redirected request would download the malware rather than Kakao SDK from the malicious server [31].

This is the first known incidence of a BGP hijacking attack in Korea, and it is suspected that the attacker planned the attack at least seven months in advance [32]. When a KLAYSwap customer made a

3) A blockchain-based decentralized financial service that uses bitcoin instead of cash.

deposit or withdrawal, the cryptocurrencies were transmitted to the attacker's wallet address. In consequence, 407 irregular transactions occurred in a total of 325 cryptocurrency wallets, and KLAYSwap had 2.2 billion won worth of cryptocurrency assets stolen [33].

2) Blackcat Malware

BlackCat is a RaaS ransomware that steals and encrypts the victim's data, but also threatens a Distributed Denial of Service (DDoS) attack if the victim does not cooperate. It has developed in the versatile Rust language, which is not frequently utilized as a ransomware programming language. Therefore, it makes reverse engineering more challenging, having a high chance of circumventing ransomware-related security systems [34]. In 2022, BlackCat targeted more than sixty organizations throughout the globe, including a German tank storage company (OilTanking GmbH) and a Swiss aviation company (Swissport). The maximum amount asked for decryption costs per company was 14 million dollars, while the average amount requested was 2.5 million dollars [35].

3) BlackMatter Malware

BlackMatter is a ransomware discovered in July 2021, which resembles DarkSide that detected in May of the same year. It usually gains unauthorized access by exploiting the vulnerabilities in the target infrastructures such as VPN or remote desktop and acquiring the target credentials through Dark web markets or other illegal

means. BlackMatter attacks only corporations with yearly revenues of more than $100 million and primarily targets the English-speaking countries such as United States, United Kingdom, Canada, and Australia. Especially, it states if any of the following corporations or organizations are infected, they will be decrypted for free [36].

- Hospitals
- National infrastructure (nuclear power plants, etc.)
- Oil and gas industry
- Defense industry
- Non-profit organizations
- Government agencies

Costs of ransom vary by corporations and range from 80 thousand to 15 million dollars [37]. Meanwhile, BlackMatter indicated that it will suspend operations in November 2021 owing to state pressure [38].

4) Phoenix Cryptolocker Malware

In March 2021, CNA Financial, a major American insurance corporation (hereinafter CNA) fell victim to an attack by Phoenix Cryptolocker, suspected to be a malware developed by the Russian hacking group Evil Corp. The attack was initiated by a CNA employee downloading the fake browser update software, which allowed Phoenix Cryptolocker to gain unauthorized access to the internal system of CNA. Subseqeuntly, the Phoenix Cryptolocker encrypted all 15,000 systems linked to the CNA network, appended the

.phoenix file extension and generated a ransom note with a Telegram contact named 'phoenix helpdesk'. Moreover, the compromised data contained the personal information of 75,349 CNA-related individuals and the company was ceased for three days [39]. CNA paid 40 million dollars for system recovery, which is believed to be the largest ransomware payment reported to date [40].

5) Darkside Malware

Darkside is a ransomware operated as RaaS by hacking group in Eastern Europe. It states that it only targets companies who can pay the desired amount and there are some exceptional companies as shown in Figure 3. Darkside generates individual keys to encrypt each file with Salsa 20, then encrypts the keys with RSA-1024 algorithm [41]. In April 2021, it halted the system of a bank in Italy and attacked the Colonial Pipeline in May. Especially, Colonial Pipeline attack caused gasoline shortages in some regions, including Virginia and South Carolina. Not only paralyzed the operation, Darkside extorted at least 5,810 of privacy data and took 75 Bitcoin worth around $4.4 million from the victim in a matter of hours. The FBI later recovered bitcoin worth $2.3 million from this case, but Darkside was responsible for countless economic losses of other victims [42].

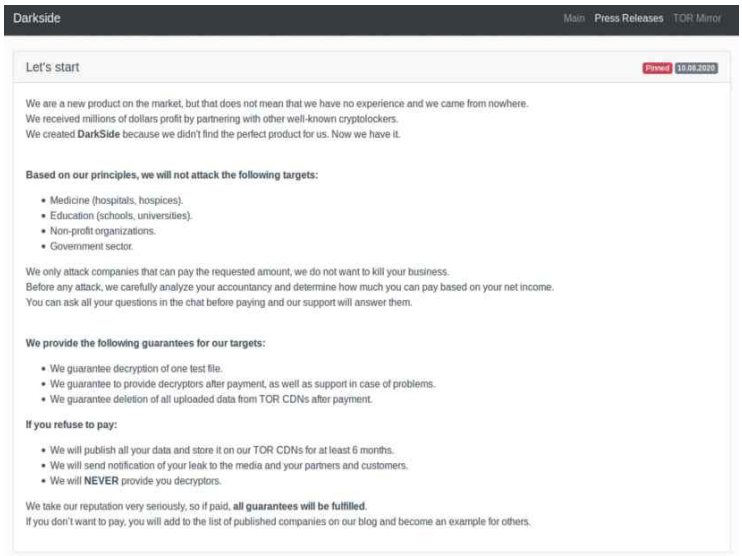


FIGURE 3. The website of Darkside Ransomware [41]

6) Cuba Malware

Cuba is a ransomware which primarily targets organizations and enterprises in five infrastructures (financial, government, medical, manufacturing, and information technology) and leaks or sells stolen data on it's dark web sites as shown in figure 4. In March 2022, the confidential data of a Korean vehicle manufacturer Hyundai Powertech was leaked by Cuba [43]. While accessing the victim's network, Cuba utilizes the Hancitor malware which is a loader that downloads RAT (Remote Access Trojans) or more ransomware. After infiltrating the network, it gains window administrator privileges via PowerShell, then remotely executes the ransomware process and encrypts all files with the file extension *.cuba*. Cuba struck at least 49 institutions and corporations by November 2021 and demanded victims pay up to $ 74

million, although profits are anticipated to be around half of their demand which is 43.9 million dollars [44].

FIGURE 4. Dark web page of Cuba Ransomware [45]

7) Conti Malware

Conti is a ransomware created by the Russian company Wizard Spider and uses RaaS model to operate. To gain initial access to the target, it distributes the trojan malware such as Trickbot or BazarLoader by spear phishing emails or exploits the Remote Desktop Protocol (RDP) credentials vulnerabilities. Conti is known as its fast speed of encryption and proliferation, and it also adopts the double extortion tactic [46]. As of January 2022, It has attacked more than 1,000 U.S. and international organizations including Ireland Health Service Executive (HSE) and has earned more than $ 150 million. Meanwhile, it declared its desire to back Russia's invasion of Ukraine,

but in retaliation, a Ukrainian researcher within the group disclosed the associated source code [47].

8) Lockbit Malware

Lockbit is the first ransomware that held its own bug bounty program to increase its completion and was the most widespread ransomware in 2022. Usually propagated via spear-phishing email at the initial breach, it can spread to other vulnerable networks by itself. Also, Lockbit has at least three variants so far. It's first name was ABCD ransomware with *.abcd* extension, which then changed to Lockbit ransomware with *.lockbit* extension and now Lockbit 3.0 is the ongoing version [48]. Lockbit targets various sectors in worldwide, such as government, education, electric, manufacturing and healthcare. One of the victims was an IT consulting firm Accenture, who was asked for $ 50 million as a ransom. On average, 85,000 dollars are demanded each case [49].

9) Revil(Sodinokibi) Malware

REvil, which began picking up steam in August of 2019, is a RaaS distributed via phishing emails, certificate forgery, and server vulnerabilities. Different from other ransomware, it uses Elliptic-curve Diffie-Hellman key exchange and Salsa 20 to encrypt victim data. It targets various enterprises and institutions throughout the world, with 60% of the known victims being US companies. One of the victim cases was a US software provider Kaseya, which distributes a remote

management service tool named VSA to its client organizations. REvil hacked the primary distribution infrastructure that disseminated the VSA and exploited zero-day vulnerabilities in the product, infecting more than 1,500 corporate networks globally. Kaseya was demanded around 70 million dollars in bitcoin for decryption, however, the FBI was able to unlock the encrypted files [50].

The profit collected in 2020 is projected to be $81 million; thus, if the subsequent profit is added, the size is anticipated to be quite significant [51]. In the meanwhile, in October 2021, with the cooperation of the United States and Russia, the REvil ransomware attack server on the dark web was shut down and several operating members were apprehended, but ransomware-related activity was identified again in May 2022 [52].

10) Netwalker Malware

Netwalker is a RaaS that usually targets medical and institutional organizations, detected for the first time in August 2019. As an example of its crime, medical institutions received phishing emails from Netwalker related to Coronavirus (COVID-19) in 2020, which was so serious that the FBI issued an emergency notification in July of the same year. Mostly spread by phishing emails, Netwalker encrypts files on local and network drives of an infected Windows system with the Salsa 20 algorithm and appends arbitrary extensions [53]. It primarily targets medical institutions in the United States and Europe, as well as manufacturing and educational organizations with

diverse infrastructures. The victims of Netwalker ransomware are listed below [54].

- 3 universities in the US (University of California, Michigan State University, Chicago College)
- US healthcare system (Crozer-Keystone Health System)
- Austrian city (Weiz) infrastructure
- Private electricity supplier in Pakistan (K-Electric)

In the case of the University of California San Francisco, medical school research data were encrypted, and the university spent 116.4 BTC which is around $1.14 million for decryption [55]. In addition, the declared amount of Netwalker's income is 2,795 BTC, which is comparable to $25 million. This money was made over the course of the five months from March to July 2020, therefore the entire amount is expected somewhat more [56]. In the meanwhile, Netwalker's dark web site for the victims to pays the decryption fee was seized by U.S. and Bulgarian law enforcement in January 2021 [57].

11) Clop Malware

Clop is a ransomware designed to attack corporations that use centralized management authentication with Active Directory (AD). Distributed by spear-phishing email, Clop is programmed to gain the administrator privileges of the Active Directory system. It encrypts victim's confidential data with AES encryption, and renames the file extension to *.Clop*. According to AhnLab, as of 2019, it had infiltrated

about 369 companies and 13,497 systems, such as public institutions, manufacturing, IT and education. The economic damage from Clop is estimated to be about $500 million by 2021 [58]. Additionally, in 2023, Clop carried out a zero-day attack on RCE vulnerability in GoAnyware MFT (Managed File Transfer) and has infiltrated 130 organizations, stealing 1 million patients' data from CHS Healthcare [59].

12) LockerGoga Malware

LockerGoga ransomware was first publicly known to the world through the attack on the French engineering company Altran in January 2019. In March of the same year, it infected a Norwegian aluminum manufacturer Norsk Hydro, which is one of the well-known OT cyber-attack as Colonial Pipeline of Darkside ransomware. In this case, some of Norsk Hydro's availability-critical production operations had to be shut down or manually converted, resulting in over $40 million in economic loss. As a result, the worldwide price of aluminum increased by 1.2%, and several American businesses and European IT systems were infected or disrupted [60]. The ransomware uses the phrase "Your Company" to refer to the victim in the ransom note, indicating that this was not a random attack but rather an APT aimed at a specific company. Unlike other ransomware, it cannot transmit itself via the network, so it is assumed that human interaction or extra tools were employed [61]. Meantime, LockerGoga decryption tool is currently available to the public.

13) Ryuk Malware

Ryuk is a ransomware created by the Wizard Spider group. It targets sectors and enterprises around the globe, including UHS (Universal Health Services) hospital and US construction group EMCOR. Delivered by spear-phishing email, it leverages the RaaS model to facilitate the distribution and has the capability to remotely execute encryption with RDP. In the event of encryption, a target's confidential data is encrypted with the AES-256 symmetric algorithm which is then encrypted with RSA-4096 asymmetric algorithm. Ryuk has one of the most expensive ransom demands, which is around $ 12.5 million per one case. Total ill-gotten gain of Ryuk was expected to be $ 150 million at the end of 2020 [62].

14) Summary

Table 3 presents a comprehensive collection of APT malware analyzed in this study, arranged in order of their most recent detection, as presented in the corresponding column of table 2. Notably, all APT malware cases except the KLAYSwap case, were categorized as ransomware. This finding suggests that when the objective of APT malware is to generate revenue rather than solely causing destruction to the target's system, ransomware tends to be the preferred choice. In contrast to non-APT malware, a significant majority of the investigated APT cases (over two-thirds) involve the utilization of RaaS for their operations. The size of the Monetary Gain

varies widely, ranging from $1.5 million to $500 million. Although certain APT cases address solely on a single malware attack, such as KLAYSwap and Lockergoga, the financial gains are significantly higher compared to non-APT malware cases. In terms of cryptocurrency diversity, the majority of APT malware exclusively employs Bitcoin, while some employ a combination of Bitcoin and Monero, or an "Unknown" cryptocurrency.

TABLE 3. Summary of APT malware trend analysis. 'Unknown' refers to cases where information is not provided.

APT Malware

Malware	Year	Category					RaaS	Monetary Gain (Million)	Related Cryptocurrency					
		Ransomware	Crypto-Jacking	Clipboard Hijacker	Financial Trojans	Etc			Bitcoin	Monero	Ethereum	Dogecoin	Etc	Unknown
KALYSwap case(no name)	02/2022					✔	-	$ 1.5 million						✔
BlackCat	11/2021	✔					Y	$ 2.5 million per ransom						✔
BlackMatter	07/2021	✔					Y	$ 15 million	✔	✔				
Phoneix Cryptolocker	03/2021	✔					-	$ 40 million						✔
Darkside	02/2020	✔					Y	$ 440 million	✔	✔				
Cuba	01/2020	✔					-	$ 43.9 million	✔					
Conti	2020	✔					Y	$ 150 million	✔					
Lockbit	09/2019	✔					Y	$ 85, 000 per ransom	✔					
Revil(Sodinokibi)	08/2019	✔					Y	$ 81 million	✔	✔				
Netwalker	08/2019	✔					Y	$ 25 million	✔					
Clop	02/2019	✔					Y	$ 500 million						✔
LockerGoga(GoGalocker)	01/2019	✔					-	$ 40 million	✔					
Ryuk	08/2018	✔					Y	$ 150 million	✔					

6. Discussion and Related Policy

1) Summary of Analysis

In this study, the set of four criteria is established to distinguish between APT malware and non-APT malware. Each case was analyzed with a particular emphasis on the monetary aspects involved. Through a comprehensive analysis of numerous instances of both non-APT and APT malware, several significant differences between the two categories have been identified.

Firstly, a notable distinction can be observed in the methods used to generate financial profits. Non-APT malware exhibits a diverse range of strategies, including ransomware, cryptojacking, and clipboard hijacking. In contrast, with the exception of KLAYSwap case, APT malware primarily manifests in the form of ransomware and is commonly associated with the RaaS model.

As anticipated, the financial ramifications caused by APT malware surpass those of non-APT malware. In certain cases, the accumulated profit generated by non-APT malware over several years are comparable to the ransom demanded by APT malware in a single targeted attack. Drawing on the examined case, when assessing the damage caused in 2018, the cumulative financial impact of non-APT malware, even when combining HackBoss and GandCrab cases did not exceed $3 million. In contrast, APT malware damages in the Ryuk case alone amounted to approximately $150 million. Furthermore, when

considering ransomware specifically, the variance in the amount demanded for each instance is substantial. For instance, while GandCrab, a non-APT malware, demanded around $3,000 for decryption, an APT malware BlackCat demanded $2.5 million.

Additionally, notable disparities were observed in the utilization of cryptocurrencies among APT and non-APT malicious codes. In the instances of APT malware, excluding Unknown type, bitcoin was exclusively employed or used in conjunction with Monero. Contrastively, non-APT malwar generated profits by employing a blend of different cryptocurrency types, except for Crackonosh which solely utilized Monero.

2) Related Policy

The majority of current trends in financial damage caused by malware are often associated with the misuse of cryptocurrencies such as Bitcoin. Unlike traditional centralized banking systems, cryptocurrencies operate on a decentralized peer-to-peer model, where transaction data and traders are spread and encrypted. This decentralized nature makes it challenging to collect transaction-related information, contributing to a level of anonymity. As a result, cryptocurrencies have been exploited as a tool for various crimes, including money laundering. Consequently, several international organizations are actively developing countermeasures to address the misuse and abuse of cryptocurrencies on a global scale. For instance, the European Union (EU) has implemented the Markets in

Crypto-Assets (MiCA) framework to regulate cryptocurrency transactions. This initiative aims to ensure transaction stability and market soundness in EU member states [63].

Furthermore, the United States has taken initiatives to address the prevention of cryptocurrency misuse linked to ransomware. One notable effort is the Counter Ransomware Initiative (CRI), which was hosted by the United States and involved 36 nations, including Korea. The aim of this initiative is to combat ransomware attacks and the misuse of cryptocurrencies. Additionally, there are plans to establish the International Counter Ransomware Task Force (ICRTF) [64]. An incident that highlights the need for such measures occurred in August 2022 when "Tornado Cash," a company providing mixing services for cryptocurrencies, was authorized in the United States. It was discovered that this service was utilized to launder stolen cryptocurrencies worth over $455 million by North Korean hackers [65].

Moreover, in 2019, the Financial Action Task Force (FATF) expanded the scope of its travel rule recommendation to include virtual assets, as part of the ransomware response. As a result, exchanges are required to collect sender and recipient information for cryptocurrency transactions of 1 million won or more. Korea implemented the "Act on the Reporting and Use of Certain Financial Transaction Information" on March 25, 2022, with relevant provisions. Other countries like Switzerland, the United States, and Singapore are also working towards implementing their own legal frameworks [11].

These collective endeavors underscore the implementation of various countermeasures globally to mitigate the misuse and abuse of cryptocurrencies. The establishment of institutional response mechanisms is crucial in preventing the exploitation of cryptocurrencies by malware, particularly in the context of ransomware attacks. With the increasing activation of global regulations and response mechanisms addressing cryptocurrency misuse and abuse, it is anticipated that these efforts will help prevent financial damages caused by cryptocurrency-related malware and facilitate international collaboration in investigations pertaining to such incidents.

7. Summary

Every year, malware attack is cited in numerous media outlets as one of the greatest challenges to global IT security, and it is continually being developed, evolved, and actively spread via methods such as RaaS. This study compared the amount of financial damage produced by these malware by classifying them as APT malware and non-APT malware and analyzed the relevant countermeasures.

The analysis conducted reveals that the majority of APT malware, accounting for a significant portion of the attacks, demonstrates characteristics of ransomware. This poses a threat not only to financial systems but also to national security. In response, various policies are being formulated and implemented worldwide to combat ransomware that exploits cryptocurrencies. Korea has also become a member of the Financial Action Task Force (FATF) and is currently working on enacting a bill to regulate virtual currencies starting in 2022. Although still in its early stages, it is expected that future policies will be established to effectively regulate and prevent the misuse of cryptocurrency by ransomware.

Ⅲ. A Study on Vulnerability Analysis and Memory Forensics of ESP32

1. Introduction

Despite the widespread adoption of IoT technology, preserving security guarantees for IoT devices has been less of a priority than functionality and performance due to the limited hardware resources and compact size, making developers focus on delivering concise features. This tendency, in turn, makes designing and implementing robust security in IoT devices challenging and leads to various security incidents. For example, Mozi botnet specifically targeted IoT devices for use in Distributed Denial of Service (DDoS) attacks. It successfully infected 12,000 IoT devices across 72 countries [66]. Additionally, wall-pad IoT devices were hacked in South Korea, resulting in privacy leakage for over 400,000 households through the device's built-in camera in 2021 [67].

Meanwhile, most IoT devices rely on over-the-air (OTA) technology to automatically update firmware or software remotely via the network connection to relieve users of the burden of manual updates. By utilizing OTA interfaces, devices can seamlessly receive and install updates over a network connection, ensuring that they stay up to date with the latest features, bug fixes, and security patches. This technology is best known for updating smart cars, but due to its convenience, OTA interfaces are also widely used in smartphones and smart home devices. Moreover, with the increasing adoption of modern system-on-a-chip (SoC) designs

in embedded systems and IoT devices, wireless connectivity features such as WiFi and Bluetooth Low Energy (BLE) are becoming commonplace. Many of these SoCs are equipped with OTA update capabilities, further increasing the convenience and prevalence of OTA.

However, despite of the ubiquity of OTA technology, potential security vulnerabilities still exist when utilizing OTA. Attacker can interpose the OTA channel by sniffing the update packets, taking unauthorized device control, and installing malware [68]. Once the OTA connection is compromised, an attacker gains the ability to update the firmware and take full control of the target device.

In this study, the security analysis on OTA updates is demonstrated using a commodity SoC called ESP32, developed by Espressif [69]. The ESP32 is a typical low-cost System on Chip (SoC) that offers low-power consumption and rich integrations with the OTA feature [70]. It is widely used across various domains, from Arduino drones to commercial low-end wearable devices and smart home IoT. Specifically, this research focuses on an IoT drone (referred to as ESP32 drone), which is based on the ESP32 DOIT DEVKIT board, to identify potential attack scenarios during OTA updates. The contributions of this paper are outlined as follows:

(1) Implementation of attack scenarios on the OTA process for security evaluation of ESP32 drones, ultimately disrupting the firmware updates of the drones. This highlights potential vulnerabilities in unpatched firmware.

(2) Conducting a forensic analysis of the chip after the attacks to obtain traces of the attacks, demonstrating the potential for extracting hacking evidence during the OTA process.

Section 2 of the paper presents several studies related to attack scenarios and forensics in IoT. Section 3 introduces and implements attack scenarios on OTA, and Section 4 conducts forensic analysis on the ESP32 memory after the attacks. Section 5 concludes the paper.

2. Related work

This section encompasses research studies focused on hacking pertaining to networks or OTA methods targeting IoT devices, as well as investigations conducted in the field of digital forensics concerning such devices.

Jeon and Lee [68] analyzed OTA update vulnerabilities in IoT healthcare devices constructed of Arduino MKR1000 WiFi board. They implemented reverse engineering of the sniffed OTA packet data and performed a mock attack on the OTA process to install a dummy program on the device.

Barybin et al. [71] employed various network hacking tools to simulate a hack on a digital temperature sensor built with the ESP DevKit V2. They disconnected the device's WiFi connection from the server and transmitted fake temperature data, pretending to be a victim. The study identified the UDP protocol as the most vulnerable point in this experiment and recommended using the TCP protocol for better security.

Li et al. [72] conducted practical memory forensic experiments on the ESP series to retrieve forensic evidence. They found that retrieving memory data through the USB port could be dangerous as the device automatically runs when connected, allowing potential tampering if a malicious program is installed. Instead, they classified the ESP series into three types by pins and suggested a forensic method using a combination of 3D printing, PoGo pins, and cold soldering.

This study stands out by presenting an attack scenario specifically focused on disrupting the OTA process of the ESP32 device. In contrast, reference [68] did not specifically target the ESP32 device, and [71] exploits the WiFi connection instead of OTA. Furthermore, this paper conducts an analysis of memory forensic artifacts resulting from the attacks through UART. It is important to note that the simulated attack scenario in this study does not involve the installation of malware. As a result, it does not address the issue of memory data extraction through USB, which was discussed in [72].

3. Simulation of OTA attack scenario

This section demonstrates a simulation of an OTA attack scenario, as shown in Figure 5. The scenario involves conducting a firmware update OTA to add wireless control functionality to an ESP32 drone, while simulating a network attack during the OTA update process. The simulation includes various steps: cracking the victim's WiFi network to obtain the IP address of the ESP32 drone, performing ARP spoofing to intercept OTA packet data, and executing a TCP SYN flooding attack to disrupt the update. The implementation of this scenario involves using Kali Linux on the attacker's PC and utilizing an IPTIME N604R plus router as the victim's access point, to which the ESP32 drone is connected.

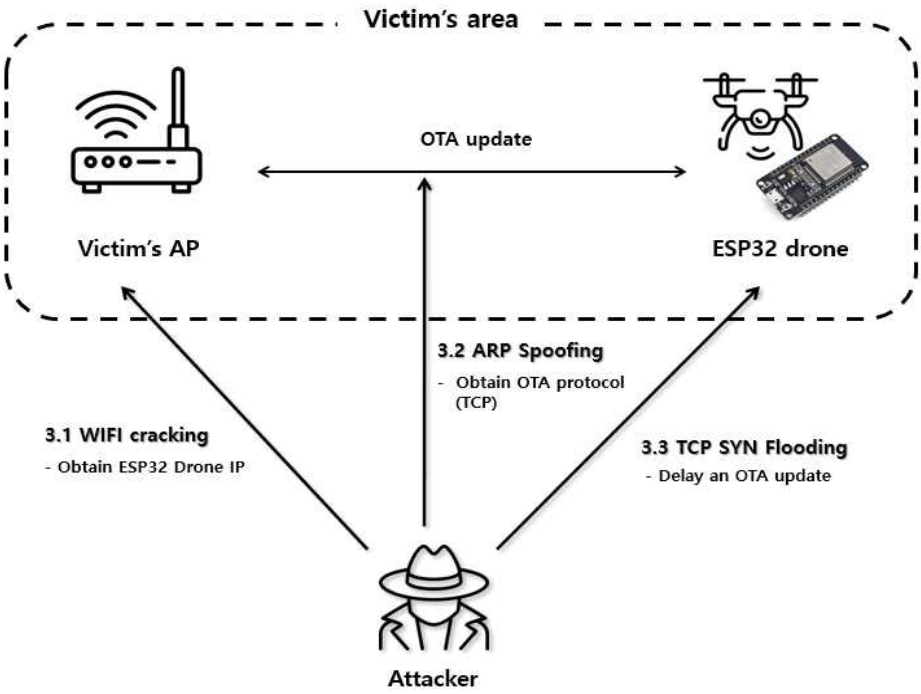


FIGURE 5. The attack scenario on OTA process of the ESP32 drone.

1) Cracking Wireless Access Point

In the initial stage of the attack scenario, several network hacking tools such as aircrack-ng, airmon-ng, airodump-ng, and aireplay-ng, known for their ability to crack WEP/WPA networks, were utilized to gain access to the victim's router [73]. The first step involved switching the wireless interface from managed mode to monitor mode using airmon-ng. This enabled the scanning of all WiFi connections, including the victim's network, using airodump-ng.

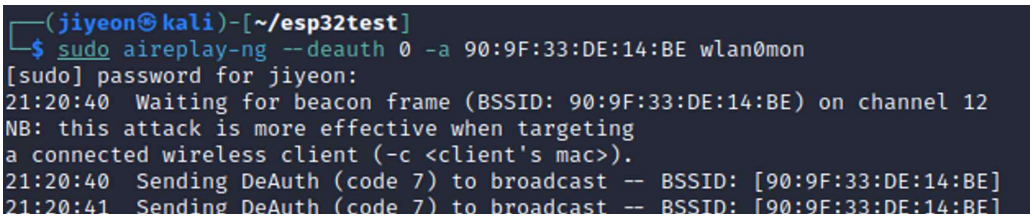


FIGURE 6. Using airplay-ng to infiltrate WiFi network

After scanning the victim's WiFi connection, aireplay-ng is employed to send de-authentication packets to the network, as depicted in Figure 6, in order to capture the WPA handshake of the victim's WiFi. Once the WPA handshake information is obtained, aircrack-ng is utilized in conjunction with the password dictionary rockyou.txt [74] to crack the password of the victim's WiFi, as shown in Figure 7. Subsequently, upon gaining access to the victim's WiFi connection, the IP address of the ESP32 drone is identified, which was utilized for ARP spoofing during the OTA update.

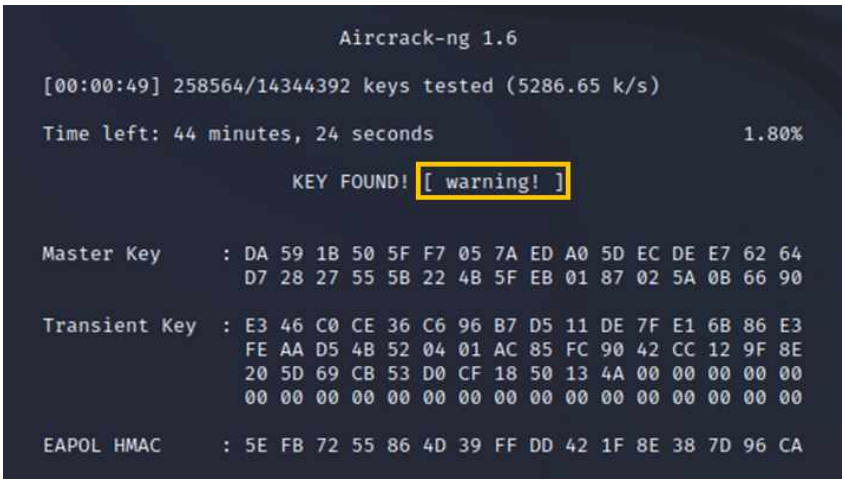


FIGURE 7. Crack the victim's WiFi password with aircrack-ng and rockyou.txt

2) OTA update packet sniffing

The simulation of OTA packet sniffing is conducted using Ettercap and Wireshark on the Kali Linux. Ettercap [75], an open-source tool, is utilized to facilitate man-in-the-middle (MITM) attacks on the local area network (LAN), while Wireshark [76], another open-source tool, is employed for comprehensive network packet and protocol analysis. In particular, the ARP poisoning technique, which is one of the MITM attack techniques supported by Ettercap, is employed to intercept and manipulate network traffic, allowing for the capture of OTA packets. Concurrently, Wireshark is utilized to capture and analyze the intercepted OTA packet.

During the ARP spoofing process, it was verified that the ESP32 drone, which had previously established a connection to the network

using the UDP protocol, initiated an OTA update and established a TCP connection for the transmission of the update data. Moreover, Figure 8 illustrates additional details obtained during this process, including information such as the board type of ESP32 and user-designated strings.

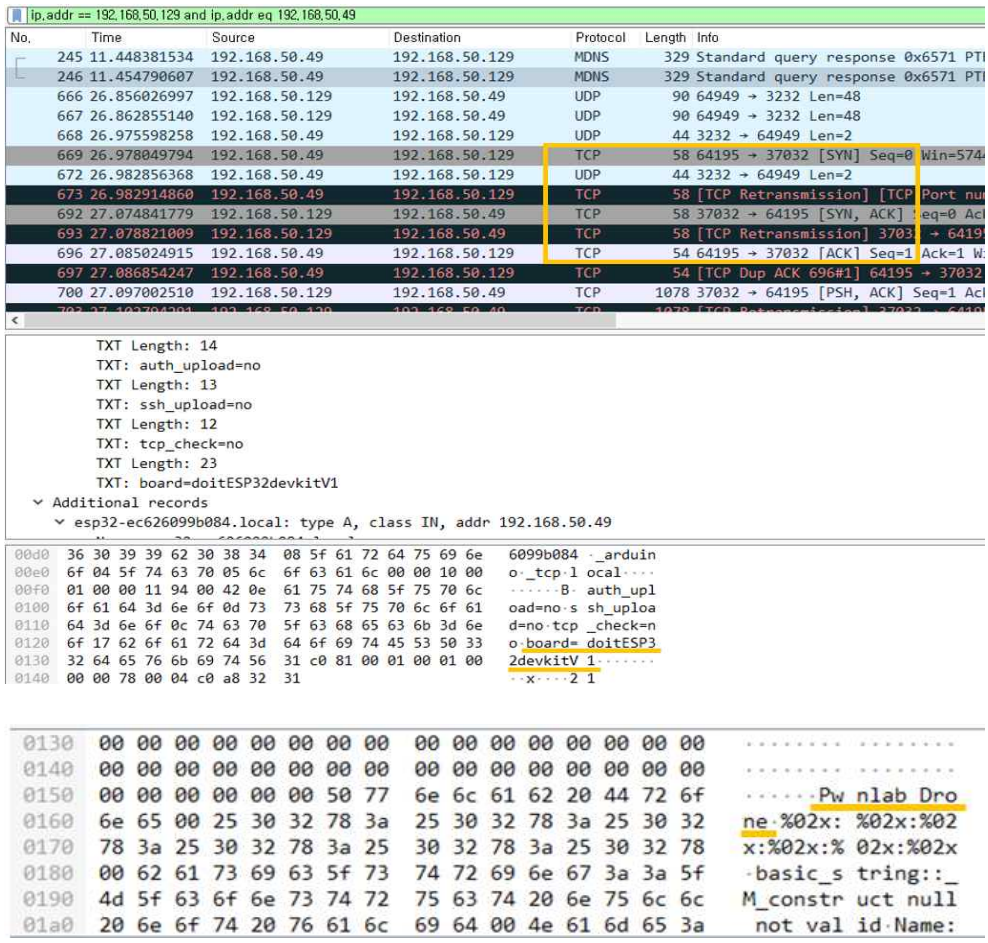


FIGURE 8. Discovered TCP 3-way handshake connection and ESP32 drone information during OTA update

3) TCP SYN Flooding attack during OTA update

Upon discovering that the OTA update utilizes TCP protocol, a TCP SYN flooding attack is executed to disrupt the OTA process on the drone. TCP SYN flooding is a form of Denial-of-Service(DoS) attack that exploits the TCP 3-way handshake of a target. To carry out this attack, the hping3 tool [77] is employed to repeatedly transmit SYN packets to the ESP32 drone. As a result, the update server ceases its attempts to establish a connection with the drone and generates an error message. Figure 9 illustrates the command used for the attack and the error message displayed from the server.

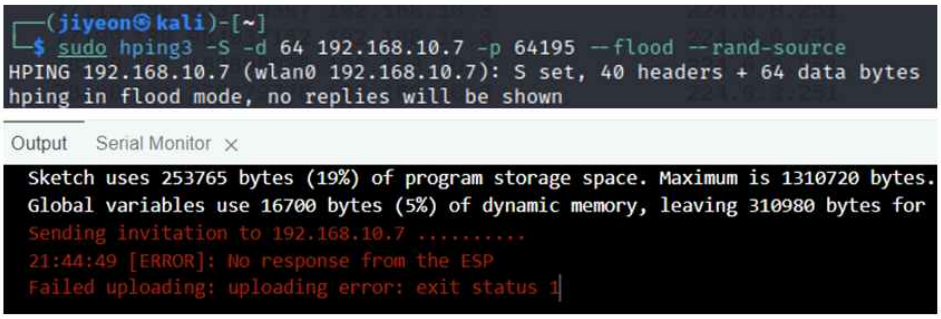


FIGURE 9. The OTA update process fails when a TCP SYN packet is sent to the ESP32 drone.

In summary, the attack scenario involved three attacks on the ESP32 drone during its OTA update process. Initially, the attacker gained unauthorized access to the access point to which the ESP32 drone was connected, by exploiting WiFi cracking techniques. Subsequently, an ARP spoofing attack was executed, revealing that the ESP32 OTA process

utilized the TCP protocol as the default. Finally, TCP SYN flooding attack was launched to disrupt the update process, resulting in a delay in patching the ESP32 drone with the latest firmware.

Maintaining the most up-to-date version of software and promptly patching vulnerabilities through software updates is crucial for ensuring device security. This OTA attack scenario highlighted that if an attacker continues to hinder OTA updates with malicious intent, the vulnerable software version may persist, leaving the possibility of future hacking.

4. ESP32 Memory Analysis

To excavate the forensic evidence of TCP SYN flooding attack aimed at delaying OTA updates, an analysis of the ESP32-WROOM-32 is conducted, which is the fundamental component of the ESP32 DOIT DEVKIT board. This particular module comprises 520KB of internal SRAM, 448KB of internal ROM, and 4MB of external SPI (Serial Peripheral Interface) flash storage which is non-volatile and stores user data [78]. The connection is established using the Universal Asynchronous Receiver /Transmitter (UART) interface, while the memory dump is performed using the esptool.py program, an open-source tool provided by the Espressif IoT Development Framework (ESP-IDF) [79].

1) ESP32 Memory Structure

The flash storage of the ESP32 is responsible for storing multiple applications through various partition configurations. Specifically, Espressif provides two built-in partition tables: (i) 'Single factory app, no OTA' that can only store factory apps, and (ii) 'Factory app, two OTA definitions', designed to support OTA updates [80]. The specific ESP32 being examined was configured with the latter partition table, enabling OTA functionality. The sturcture of this partition table is illustrated in Figure 10.

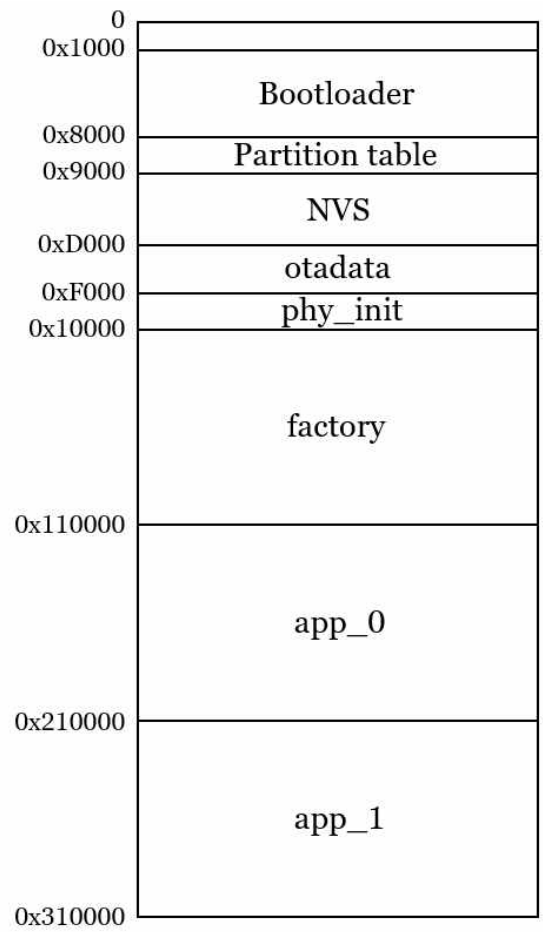


FIGURE 10. Partition table of ESP32

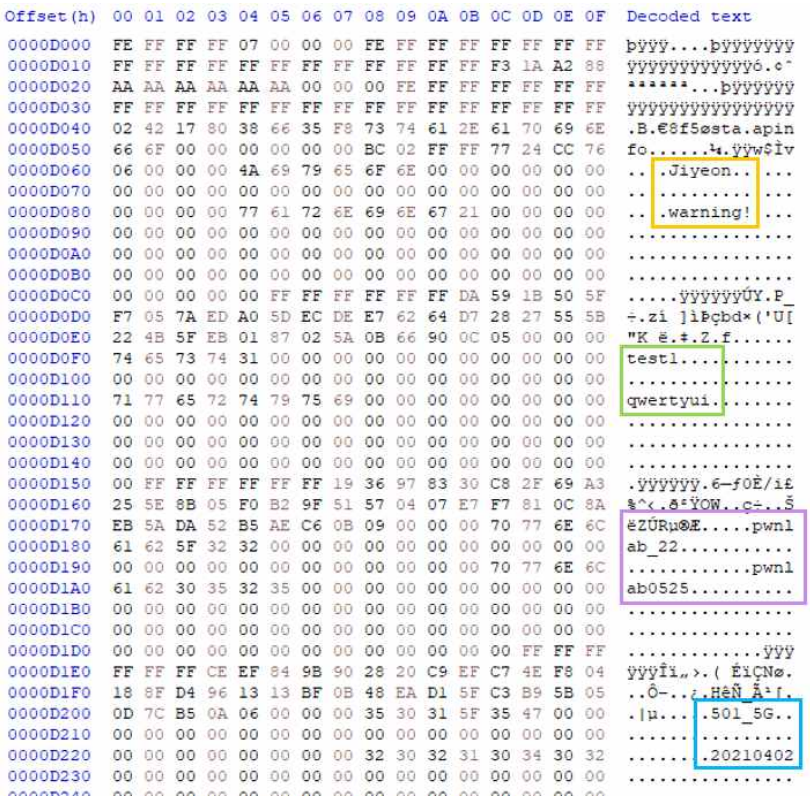
Following the execution of an OTA update, the updated data is written to one of the *app* partitions that is currently inactive. The partition ID associated with the updated data is stored in the *otadata* area. Upon successful completion of the update process, the ESP32 is undergoes an automatic reboot. During this reboot, the bootloader refers to the ID stored in *the otadata* to execute the corresponding partition [81]. In the event that the OTA data area is empty, the bootloader executes the factory partition, which contains the default application data.

2) Memory Dump Analysis

In order to extract the contents of dump the flash storage, a connection is established between the ESP32 chip and a PC using UART communication. The ESP32 is equipped with a UART port which enables serial communication for tasks such as firmware uploading or monitoring output [82]. To perform the flash dump, the esptool.py is utilized. This tool allows for the extraction of the flash storage as a binary file. To identify traces of the attack, a total of three memory dumps were performed. Two dumps were executed during normal update attempts, each of which was given the name "*esp32_dump.bin*" and "*esp32_dump2.bin*" respectively. Additionally, a memory dump was taken after the SYN flooding attack and labeled as "*synflooding.bin*".

a. Analyzing *esp32_dump.bin*

As part of the analysis to identify the memory relevant to the OTA update, the otadata partition within the esp32_dump.bin file was examined. It was discovered that this area contains a historical record of WiFi connections, which includes a collection of SSIDs (Service Set Identifiers) and their corresponding passwords. This information is depicted in Figure 11.



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
0000D000	FE	FF	FF	FF	07	00	00	00	FE	FF	FF	FF	FF	FF	FF	FF	þÿÿÿ....þÿÿÿÿÿÿÿ
0000D010	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	F3	1A	A2	88	ÿÿÿÿÿÿÿÿÿÿÿÿó.¢ˆ
0000D020	AA	AA	AA	AA	AA	AA	00	00	00	FE	FF	FF	FF	FF	FF	FF	ªªªªªª...þÿÿÿÿÿÿ
0000D030	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0000D040	02	42	17	80	38	66	35	F8	73	74	61	2E	61	70	69	6E	.B.€8f5østa.apin
0000D050	66	6F	00	00	00	00	00	00	BC	02	FF	FF	77	24	CC	76	fo......¼.ÿÿw$Ìv
0000D060	06	00	00	00	4A	69	79	65	6F	6E	00	00	00	00	00	00	....Jiyeon.....
0000D070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0000D080	00	00	00	00	77	61	72	6E	69	6E	67	21	00	00	00	00	....warning!....
0000D090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0000D0A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0000D0B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0000D0C0	00	00	00	00	00	FF	FF	FF	FF	FF	FF	DA	59	1B	50	5F	.....ÿÿÿÿÿÿÚY.P_
0000D0D0	F7	05	7A	ED	A0	5D	EC	DE	E7	62	64	D7	28	27	55	5B	÷.zí]ìÞçbd×('U[
0000D0E0	22	4B	5F	EB	01	87	02	5A	0B	66	90	0C	05	00	00	00	"K_ë.‡.Z.f.....
0000D0F0	74	65	73	74	31	00	00	00	00	00	00	00	00	00	00	00	test1.....
0000D100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0000D110	71	77	65	72	74	79	75	69	00	00	00	00	00	00	00	00	qwertyui.....
0000D120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0000D130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0000D140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0000D150	00	FF	FF	FF	FF	FF	FF	19	36	97	83	30	C8	2F	69	A3	.ÿÿÿÿÿÿ.6—ƒ0È/i£
0000D160	25	5E	8B	05	F0	B2	9F	51	57	04	07	E7	F7	81	0C	8A	%^‹.ð²ŸQW..ç÷..Š
0000D170	EB	5A	DA	52	B5	AE	C6	0B	09	00	00	00	70	77	6E	6C	ëZÚRµ®Æ.....pwnl
0000D180	61	62	5F	32	32	00	00	00	00	00	00	00	00	00	00	00	ab_22.....
0000D190	00	00	00	00	00	00	00	00	00	00	00	00	70	77	6E	6C	.....
0000D1A0	61	62	30	35	32	35	00	00	00	00	00	00	00	00	00	00	ab0525.....
0000D1B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0000D1C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0000D1D0	00	00	00	00	00	00	00	00	00	00	00	00	00	FF	FF	FF	.....ÿÿÿ
0000D1E0	FF	FF	FF	CE	EF	84	9B	90	28	20	C9	EF	C7	4E	F8	04	ÿÿÿÎï„›.(ÉïÇNø.
0000D1F0	18	8F	D4	96	13	13	BF	0B	48	EA	D1	5F	C3	B9	5B	05	..Ô–..¿.HêÑ_Ã¹[.
0000D200	0D	7C	B5	0A	06	00	00	00	35	30	31	5F	35	47	00	00	.|µ.....501_5G..
0000D210	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0000D220	00	00	00	00	00	00	00	00	32	30	32	31	30	34	30	32	20210402
0000D230	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

FIGURE 11. WiFi data is stored in *otadata* partition (offset 0xD000)

Furthermore, it was revealed that the updated firmware content was written starting from the offset 0x150000 instead of the initial offset of *app_0*, which is 0x110000. To investigate this further, the updated firmware content compared with the packets sniffed from the perspective of an attacker above. Consequently, it was observed that the same values as the sniffed packet data were stored in the memory locations ranging from 0x150010 to 0x243D89, as shown in Figure 12.

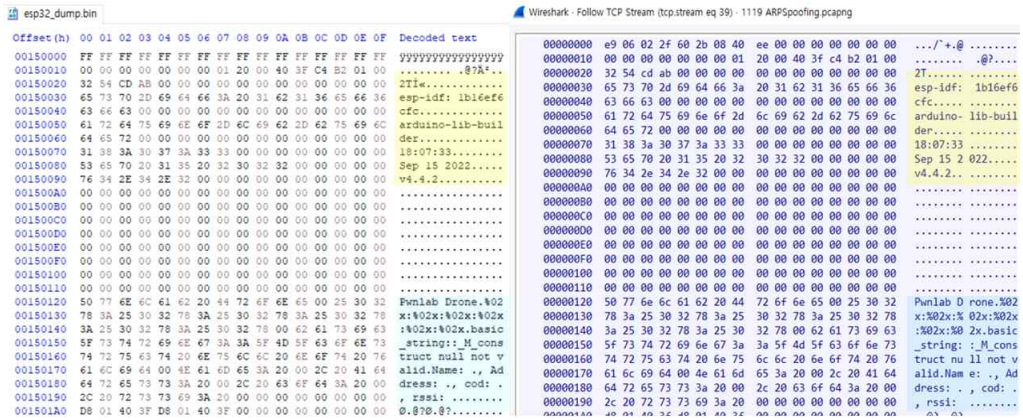
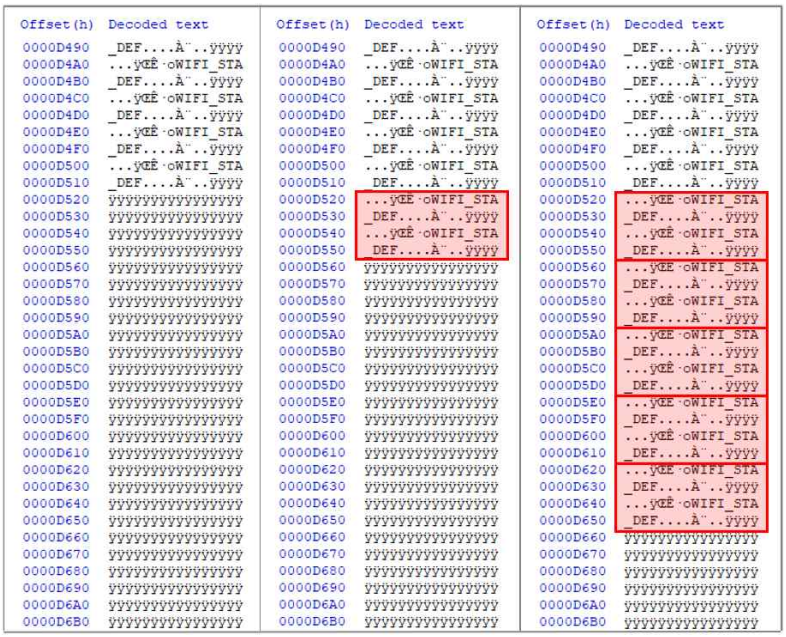


FIGURE 12. Comparing the *esp32_dump.bin* file (left) with the sniffed packet data (right)

This analysis implies that memory forensics enables the retrieval of a complete history of WiFi connections from the ESP32 drone. Not only does this apply to the attack case discussed in this paper, but this information can also serve as a valuable trace for identifying an attacker in various attack scenarios. Additionally, this information can provide crucial clues for detecting potential artifacts associated with the transmission of fake firmware.

b. Detecting evidence of TCP SYN Flooding

In order to identify memory artifacts of the SYN flooding attack, a comparison was made between the three dump files using WinMerge [83], a open-source file comparison tool. Figure 13 illustrates the comparision of the content within the files: *esp32_dump.bin*, *esp32_dump1.bin*, and *synflooding.bin*.



Offset(h)	Decoded text	Offset(h)	Decoded text	Offset(h)	Decoded text
0000D490	_DEF....À¨..ÿÿÿÿ	0000D490	_DEF....À¨..ÿÿÿÿ	0000D490	_DEF....À¨..ÿÿÿÿ
0000D4A0	...ÿŒÊ·oWIFI_STA	0000D4A0	...ÿŒÊ·oWIFI_STA	0000D4A0	...ÿŒÊ·oWIFI_STA
0000D4B0	_DEF....À¨..ÿÿÿÿ	0000D4B0	_DEF....À¨..ÿÿÿÿ	0000D4B0	_DEF....À¨..ÿÿÿÿ
0000D4C0	...ÿŒÊ·oWIFI_STA	0000D4C0	...ÿŒÊ·oWIFI_STA	0000D4C0	...ÿŒÊ·oWIFI_STA
0000D4D0	_DEF....À¨..ÿÿÿÿ	0000D4D0	_DEF....À¨..ÿÿÿÿ	0000D4D0	_DEF....À¨..ÿÿÿÿ
0000D4E0	...ÿŒÊ·oWIFI_STA	0000D4E0	...ÿŒÊ·oWIFI_STA	0000D4E0	...ÿŒÊ·oWIFI_STA
0000D4F0	_DEF....À¨..ÿÿÿÿ	0000D4F0	_DEF....À¨..ÿÿÿÿ	0000D4F0	_DEF....À¨..ÿÿÿÿ
0000D500	...ÿŒÊ·oWIFI_STA	0000D500	...ÿŒÊ·oWIFI_STA	0000D500	...ÿŒÊ·oWIFI_STA
0000D510	_DEF....À¨..ÿÿÿÿ	0000D510	_DEF....À¨..ÿÿÿÿ	0000D510	_DEF....À¨..ÿÿÿÿ
0000D520	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D520	...ÿŒÊ·oWIFI_STA	0000D520	...ÿŒÊ·oWIFI_STA
0000D530	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D530	_DEF....À¨..ÿÿÿÿ	0000D530	_DEF....À¨..ÿÿÿÿ
0000D540	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D540	...ÿŒÊ·oWIFI_STA	0000D540	...ÿŒÊ·oWIFI_STA
0000D550	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D550	_DEF....À¨..ÿÿÿÿ	0000D550	_DEF....À¨..ÿÿÿÿ
0000D560	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D560	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D560	...ÿŒÊ·oWIFI_STA
0000D570	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D570	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D570	_DEF....À¨..ÿÿÿÿ
0000D580	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D580	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D580	...ÿŒÊ·oWIFI_STA
0000D590	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D590	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D590	_DEF....À¨..ÿÿÿÿ
0000D5A0	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D5A0	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D5A0	...ÿŒÊ·oWIFI_STA
0000D5B0	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D5B0	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D5B0	_DEF....À¨..ÿÿÿÿ
0000D5C0	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D5C0	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D5C0	...ÿŒÊ·oWIFI_STA
0000D5D0	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D5D0	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D5D0	_DEF....À¨..ÿÿÿÿ
0000D5E0	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D5E0	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D5E0	...ÿŒÊ·oWIFI_STA
0000D5F0	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D5F0	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D5F0	_DEF....À¨..ÿÿÿÿ
0000D600	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D600	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D600	...ÿŒÊ·oWIFI_STA
0000D610	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D610	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D610	_DEF....À¨..ÿÿÿÿ
0000D620	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D620	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D620	...ÿŒÊ·oWIFI_STA
0000D630	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D630	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D630	_DEF....À¨..ÿÿÿÿ
0000D640	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D640	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D640	...ÿŒÊ·oWIFI_STA
0000D650	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D650	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D650	_DEF....À¨..ÿÿÿÿ
0000D660	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D660	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D660	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0000D670	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D670	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D670	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0000D680	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D680	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D680	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0000D690	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D690	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D690	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0000D6A0	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D6A0	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D6A0	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0000D6B0	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D6B0	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	0000D6B0	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ

FIGURE 13. The comparison was conducted between the following files: esp32_dump.bin, esp32_dump1.bin, and synflooding.bin (in the given order).

The analysis showed that the *otadata* partition recorded data block size of 0x40 during a regular OTA update. On the other hand, in the case of a TCP SYN flooding attack executed on the device, the memory registered five times the amount of data compared to a normal OTA update. This result suggests that an abnormally high number of the data blocks written in this partition can be considered an artifact of a SYN flooding attack.

Moreover, within the recorded data block, the field labeled "*WIFI_STA*" indicates the operational mode of the ESP32 device, functioning as a station and establishing an connection with an access point [84].

Considering that the block includes the device's access information to an access point (*WIFI_STA_DEF*), it becomes plausible to regard this as a potential indication of other types of Denial-of-Service (DoS) attacks that can disrupt network connectivity.

5. Summary

IoT is playing an integral role in the hyper-connected era, and at the same time, various attack vectors such as malware threats and network vulnerabilities are on the rise. This study focuses on the ESP32 SoC, widely utilized in various IoT devices, and implements an attack scenario that disrupts the latest firmware updates through a DoS attack on OTA. Additionally, the forensic analysis of the ESP32 drones was conducted from a memory forensics perspective after the attacks, revealing traces of the DoS attack and demonstrating potential forensic evidence.

The simulated OTA attack on the IoT drone highlights the criticality of OTA availability by revealing the potential consequences of leaving vulnerabilities unpatched. This scenario exposes the drone to a range of potential threats, emphasizing the significance of maintaining a secure and up-to-date OTA system to safeguard against future risks.

Ⅳ. Conclusion

With the rapid advancement of next-generation ICT technologies, the perpetual existence of malware threats necessitates the requirement for security assessments. In the initial phase of this study, malware was classified into advanced persistent threats (APTs) and non-APTs, with a specific emphasis on scrutinizing their distinctive features, particularly in terms of illicit revenue generation and the extent of damage caused by cryptocurrency. Additionally, an examination was conducted on diverse national policies aimed at countering ransomware, a prevalent component employed in APT attacks.

In the second part, the security vulnerabilities of OTA (Over-The-Air) update technology were evaluated, a prominent technology widely applied in the Internet of Things (IoT). The potential for update disruption attacks that hinder vulnerability patches was demonstrated. As mentioned earlier, there has been an increase in various forms of malware, such as ransomware or crypto miners, which exploit vulnerabilities and infiltrate systems. Therefore, regular updates and patches are crucial to eliminate vulnerabilities. Given that OTA technology is extensively utilized in IoT updates, the significant importance of security in ensuring the availability of secure OTA updates is confirmed.

ACKNOWLEDGEMENTS

본 논문들을 지도해주신 김성민 교수님과 PART 1 연구에 도움을 주신 장대희 교수님, 공저자로 함께 해준 안은영 학생, PART 2 연구의 공저자로 함께 해준 장지원 학생에게 감사를 드립니다.

본 논문의 PART 2: A Study on Vulnerability Analysis and Memory Forensics of ESP32 중 공격 시나리오는 2019 년 10 월 IEEE PIC S&T 에서 발표된 논문의 내용을 확장하여 작성되었습니다 [71].

References

[1] Markets and Markets, “Internet of Things (IoT) Market Analysis,” 2023. [Online]. Available : https://www.marketsandmarkets.com/Market-Reports/internet-of-things-market-573.html.

[2] KISA. Cyber Threat Trend Report for Second Half of 2022.

[3] AT&T Business, “Shikitega-New stealthy malware targeting Linux,” 2022. [Online]. Available: https://cybersecurity.att.com/blogs/labs-research/shikitega-new-stealthy-malware-targeting-linux.

[4] Kaspersky. “Crypto miners on the rise,” 2022. [Online]. Available: https://www.kaspersky.com/about/press-releases/2022_crypto-miners-on-the-rise-kaspersky-experts-report-more-than-230-growth-in-the-number-of-malicious-mining-programs.

[5] Kaspersky, “Top Ten Cybersecurity Trends,” [Online]. Available: https://www.kaspersky.com/resource-center/preemptive-safety/cyber-security-trends

[6] Securelist, “The state of cryptojacking in the first three quarters of 2022,” 2022. [Online]. Available: https://securelist.com/cryptojacking-report-2022/107898/.

[7] Uk Jo, GuemBo Kim, ShinWook Heo, and Howon Kim. A Study on the Response of Cryptocurrency Deception and Money Laundering Method Using Ransomware. Korea Institute of Information Security & Cryptology, 32(3), pp. 19-26, 2022.

[8] CoinMarketCap. “Global Cryptocurrency Market Charts,” 2023. [Online]. Available: https://coinmarketcap.com/charts/.

[9] Ars Technica. “US seizes $2.3 million Colonial Pipeline paid to ransomware attackers,” 2021. [Online]. Available: https://arstechnica.com/gadgets/2021/06/us-seizes-2-3-million-colonial-pipeline-paid-to-ransomware-attackers/.

[10] Edaily. “Monero Coin Instead of Bitcoin in Cybercrime,” 2021. [Online]. Available: https://www.edaily.co.kr/news/read?newsId=03952406629084344.

[11] KB Financial Group. “Significance of Travel Rule Application and Trends in the Domestic Virtual Asset Industry,” 2022.

[12] AAX Trends. “Consensus Mechanisms? How PoW, PoS, DPoS, and Other Blockchain Algorithms Work,” 2020. [Online]. Available: https://trends.aax.com/consensus-mechanisms-how-pow-pos-dpos-and-other-blockchain-algorithms-work.

[13] Korea Financial Intelligence Unit. “International standards and international organizations,” [Online]. Available: https://www.kofiu.go.kr/kor/policy/iois01_1.do.

[14] Won Seok Choi, Daehwa Rayer Lee and Hyoungshick Kim. Cryptojacking Research Trends. Korea Institute of Information Security & Cryptology, 28(3), pp. 33-37, 2018.

[15] Asiae. “Economy Bitcoin will be stolen while you ‘copy & paste’,” 2018. [Online]. Available: https://www.asiae.co.kr/article/2018070310083668541.

[16] Kiwoon Moon, Jong-Hyouk Lee. Latest ransomware trends and development directions. Korea Institute of Information Security &

Cryptology, 32(3), pp. 33-39, 2022.
[17] Decoded. “HackBoss: A cryptocurrency-stealing malware distributed through Telegram,” 2021. [Online]. Available: https://decoded.avast.io/romanalinkeova/hackboss-a-cryptocurrency-stealing-malware-distributed-through-telegram/.
[18] BBC News. “Crackonosh: How hackers are using gamers to become crypto-rich,” 2021. [Online]. Available: https://www.bbc.com/news/technology-57601631/.
[19] Decoded. “Crackonosh: A New Malware Distributed in Cracked Software,” 2021. [Online]. Available: https://decoded.avast.io/danielbenes/crackonosh-a-new-malware-distributed-in-cracked-software/.
[20] Acronis.“Magniber ransomware hiding in fake Windows updates,” 2022. [Online]. Available: https://www.acronis.com/en-us/cyber-protection-center/posts/magniber-ransomware-hiding-in-fake-windows-updates/.
[21] KBS News. “2 trillion won in ransomware damage in Korea last year,” 2021. [Online]. Available: https://news.kbs.co.kr/news/view.do?ncd=5233638.
[22] CheckPointResearch. “Phorpiex Breakdown,” 2019. [Online]. Available: https://research.checkpoint.com/2019/phorpiex-breakdown.
[23] Bleepingcomputer. “Phorpiex botnet returns with new tricks making it harder to disrupt,” 2021. [Online]. Available: https://www.bleepingcomputer.com/news/security/phorpiex-botnet-returns-with-new-tricks-making-it-harder-to-disrupt/
[24] CheckPointResearch. “Phorpiex botnet is back with a new Twizt: Hijacking Hundreds of crypto transactions,” 2021. [Online]. Available: https://research.checkpoint.com/2021/phorpiex-botnet-is-back-with-a-new-twizt-hijacking-hundreds-of-crypto-transactions/.
[25] Ahnlab. “What if the server keeps getting infected with coin mining malware?,” 2020. [Online]. Available: https://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=1&seq=29071.
[26] Sophos. “MyKings: The Slow But Steady Growth of a Relentless Botnet,” 2019.
[27] The Record. “A malware botnet has made more than $24.7 million since 2019,” 2021. [Online]. Available: https://therecord.media/a-malware-botnet-has-made-more-than-24-7-million-since-2019/.
[28] Bleepingcomputer. “Log4j vulnerability now used to install Dridex banking malware,” 2021. [Online]. Available: https://www.bleepingcomputer.com/news/security/log4j-vulnerability-now-used-to-install-dridex-banking-malware/.
[29] NJCCIC. “NJCCIC Threat Profile,” 2016. [Online]. Available: https://www.cyber.nj.gov/threat-center/threat-profiles/trojan-variants/dridex.
[30] SecureWorld. “Dridex Malware Kingpin: $5 Million if You Can Find Him,” 2019. [Online]. Available: https://www.secureworld.io/industry-news/dridex-malware-evil-corp-reward.
[31] Newsworker. “KLAYSwap was hacked 2.2 billion won by 'Kakao SDK'?,” 2022. [Online]. Available: http://www.newsworker.co.kr/news/articleView.html?idxno=146501.

[32] Boannews. “BGP hijacking attack technique revealed by KLAYS wap hacking,” 2022. [Online]. Available: https://www.boannews.com/media/view.asp?idx=104743.
[33] ZDNet Korea. “KLAYSwap, 2.2 billion won worth of cryptocurrency was stolen,” 2022. [Online]. Available: https://zdnet.co.kr/view/?no=20220204082206.
[34] Korea Fiscal Informaion Service. “Major security issues and incidents in the first half of 2022,” 2022. [Online]. Available: https://www.fis.kr/ko/major_biz/cyber_safety_oper/attack_info/notice_issue?articleSeq=2508.
[35] HelpNetSecurity. “BlackCat (aka ALPHV) ransomware is increasing stakes up to $2.5 million in demands,” 2022. [Online]. Available: https://www.helpnetsecurity.com/2022/07/11/blackcat-alphv-ransomware/.
[36] Varonis. “BlackMatter Ransomware,” 2022. [Online]. Available: https://www.varonis.com/blog/blackmatter-ransomware
[37] Joint Cybersecurity Advisory. “BlackMatter Ransomware,” 2021.
[38] The Record. “BlackMatter ransomware says its shutting down due to pressure from local authorities,” 2021. [Online]. Available: https://therecord.media/blackmatter-ransomware-says-its-shutting-down-due-to-pressure-from-local-authorities/.
[39] Bleepingcomputer. “Ransomware gang breached CNA’s network via fake browser update,” 2021. [Online]. Available: https://www.bleepingcomputer.com/news/security/ransomware-gang-breached-cna-s-network-via-fake-browser-update/.
[40] Medium. “CNA Financial Corp. Paid $40 Million after the Phoenix CryptoLocker Attack,” 2021. [Online]. Available: https://medium.com/spin-ai-ransomware-protection/cna-financial-corp-paid-40-million-after-the-phoenix-cryptolocker-attack-d54c3ca10a01.
[41] Korea Internet & Security Agency. “Ransomware Trends & Statistics Third Quarter for 2020,” 2020. [Online]. Available: https://www.kisa.or.kr/20206/form?postSeq=27&lang_type=KO&page=1.
[42] IstroSec. “DarkSide Ransomware,” 2021. [Online]. Available: https://www.istrosec.com/blog/darkside-ransomware/.
[43] Boannews. “Ransomware Organization of Cuba Hacks Hyundai Powertech and Claims to Leak Internal Files,” 2022. [Online]. Available: https://www.boannews.com/media/view.asp?idx=105654a
[44] ZDNet. “FBI: Cuba ransomware group hit 49 critical infrastructure organizations,” 2021. [Online]. Available: https://www.zdnet.com/article/fbi-cuba-ransomware-hit-49-critical-infrastructure-organizations/.
[45] McAfee. “Technical analysis of cuba ransomware,” 2021.
[46] ManageEngine. “Conti ransomware,” 2022. [Online]. Available: https://www.manageengine.com/log-management/cyber-security/conti-ransomware.html.
[47] TechTarget. “Google: Former Conti ransomware members attacking Ukraine,” 2022. [Online]. Available: https://www.techtarget.com/searchsecurity/news/252524685/Google-Former-Conti-ransomware-members-attacking-Ukraine.
[48] Dragos. “LockBit Ransomware Continued to Impact Operational

Technology(OT)," 2023. [Online]. Available: https://www.dragos.com/blog/lockbit-ransomware-continued-to-impact-operational-technology-in-2022/.
[49] ESTsecurity. "LockBit ransomware is being distributed via phishing mail," 2021. [Online]. Available: https://blog.alyac.co.kr/4456.
[50] ZDNet Korea. "Kaseya Ransomware Hacker Repatriates the United States...up to 115 years in prison," 2022. [Online]. Available: https://zdnet.co.kr/view/?no=20220314093000.
[51] ITWorld. "Key trends in 'Revill ransomware," 2021. [Online]. Available: https://www.itworld.co.kr/news/210884
[52] ESTsecurity. "A new sample of REVIL ransomware and its activity has been found," 2022. [Online]. Available: https://blog.alyac.co.kr/4689.
[53] Cybereason. "Cybereason vs. NetWalker Ransomware," 2021. [Online]. Available: https://www.cybereason.com/blog/research/cybereason-vs.-netwalker-ransomware.
[54] UpGuard. "What is Netwalker Ransomware? Attack Methods & Protection Tips," 2022. [Online]. Available: https://www.upguard.com/blog/what-is-netwalker-ransomware.
[55] Threatpost. "UCSF Pays $1.14M After NetWalker Ransomware Attack," 2020. [Online]. Available: https://threatpost.com/ucsf-pays-1-14m-after-netwalker-ransomware-attack/157015/.
[56] Bleepingcomputer. "Netwalker ransomware earned $25 million in just five months," 2022. [Online]. Available: https://www.bleepingcomputer.com/news/security/netwalker-ransomware-earned-25-million-in-just-five-months/.
[57] The United States Department of Justice. "Department of Justice Launches Global Action Against NetWalker Ransomware," 2021. [Online]. Available: https://www.justice.gov/opa/pr/department-justice-launches-global-action-against-netwalker-ransomware.
[58] AhnLab Security Emergency response Center. "CLOP Ransomware that Attacked Korean Distribution Giant," 2021. [Online]. Available: https://asec.ahnlab.com/en/19542/.
[59] CPO. "Clop Ransomware Breaches 130 Organizations, Steals 1 Million CHS Healthcare Patients' Records," 2023. [Online]. Available: https://www.cpomagazine.com/cyber-security/clop-ransomware-breaches-130-organizations-steals-1-million-chs-healthcare-patients-records/.
[60] Securityweek. "Aluminum Giant Norsk Hydro Hit by Ransomware," 2019. [Online]. Available: https://www.securityweek.com/aluminum-giant-norsk-hydro-hit-ransomware.
[61] SCADAfence. "Norsk Hydro's LockerGoga Ransomware Propagation Detection & Mitigation," 2019.
[62] Trendmicro. "What is Ryuk ransomware?," 2021. [Online]. Available: https://www.trendmicro.com/en_nl/what-is/ransomware/ryuk-ransomware.html
[63] Korea Capital Market Institute. "Key Content of the EU's Virtual Asset Market (MiCA) Bill," 2022.
[64] The White House. "FACT SHEET: The Second International Counter Ransomware Initiative Summit," 2022. [Online]. Available: h

ttps://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/fact-sheet-the-second-international-counter-ransomware-initiative-summit/.
[65] Korea JoongAng Daily. “Tornado Cash sanctioned by U.S. over North Korean hacking,” 2022. [Online]. Available: https://koreajoongangdaily.joins.com/2022/08/09/national/northKorno/North-Korea-US-Treasury-sanctions/20220809155332703.html.
[66] The Korea Herald. IoT devices hacking statistics, 2022. The Korea Herald. [Online]. Available : http://news.koreaherald.com/view.php?ud=20220119000736.
[67] Yonhap News. Home cameras hacking statistics, 2022. [Online]. Available : https://en.yna.co.kr/view/AEN20221220009100315.
[68] H. Jeon, and S. Lee. Analysis of Remote Update Vulnerabilities of IoT Healthcare Devices. Journal of KIIT, Vol. 19, No. 1, pp. 87-97, 2021.
[69] Espressif. [Online]. Available : https://www.espressif.com/
[70] Espressif. ESP32-S2 Series Datasheet. [Online]. Available : https://www.espressif.com/en/products/devkits.
[71] O. Barybin, E. Zaitseva, and V. Brazhnyi. Testing the Security ESP32 Internet of Things Devices. 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), 2019.
[72] Z. Li, H. Ren, E. Chou, X. Liu, and C. D. McAllister, Retrieving Forensically Sound Evidence from the ESP Series of IoT Devices. IEEE Internet of Things Journal, Vol. 9, No.15, pp. 13144-13152, 2022.
[73] Aircrack-Ng. [Online]. Available : https://www.kali.org/tools/aircrack-ng/
[74] Wordlists. [Online]. Available : https://www.kali.org/tools/wordlists/
[75] Ettercap Project. [Online]. Available : https://www.ettercap-project.org/
[76] Wireshark. [Online]. Available : https://www.wireshark.org.
[77] Hping3. [Online]. Available : https://www.kali.org/tools/hping3/
[78] Espressif. ESP32-WROOM-32 Datasheet. 2023.
[79] Espressif. Esptool.py Documentation. [Online]. Available: https://docs.espressif.com/projects/esptool/en/latest/esp32/
[80] Espressif. ESP-IDF API Guides. [Online]. Available : https://docs.espressif.com/projects/esp-idf/en/latest/esp32/api-guides/partition-tables.html.
[81] Espressif. ESP32 Tutorials. [Online]. Available : http://www.lucadentella.it/en/2016/12/22/esp32-4-flash-bootloader-e-freertos/
[82] B. Pearson, L. Luo, Y. Zhang, R. Dey, Z. Ling, M. Bassiouni, and X. Fu. On Misconception of Hardware and Cost in IoT Security and Privacy. In ICC 2019-2019 IEEE International Conference on Communications (ICC), 2019.
[83] WinMerge. https://winmerge.org/
[84] Espressif. ESP32 Networking APIs. [Online] Available: https://docs.espressif.com/projects/esp-idf/en/latest/esp32/api-reference/network/esp_wifi.html

논문 개요

4차산업혁명 사회에서 차세대 ICT 기술은 금융, 교통, 공공기관 등 다양한 분야에서 필수적인 요소로 자리 잡고 있다. 일례로 블록체인 기술은 익명성, 신뢰성, 보안성 등을 바탕으로 암호화폐나 탈중앙화 거래소를 비롯하여 여러 기술에 접목되고 있으며, 사물인터넷(Internet of Things, IoT) 또한 스마트홈, 커넥티드카, 드론 등의 형태로 초연결사회의 주요 요소로써 활용되고 있다. 그러나, 이러한 보편성에도 불구하고 여전히 해당 기술들에 대한 보안성 점검 및 검토의 필요성이 요구되는 실정이다. 특히, 랜섬웨어 또는 크립토마이너 (crypto-miner)와 같이 암호화폐를 악용하는 악성코드가 증가하면서, IoT를 비롯한 차세대 ICT 기술들에도 영향을 미치고 있다.

본 연구는 암호화폐로 수익을 창출하는 악성코드를 APT (Advanced Persistent Threats)와 non-APT로 분류하고, 각 악성코드의 암호화폐 악용 및 피해 규모 측면을 중점으로 분석하여 각각의 특징을 도출한다. 또한, IoT 드론을 선정하여 원격 업데이트 기술에 대한 모의 공격 시나리오를 구현하고, 최종적으로 OTA 업데이트를 지연시켜 IoT 기기의 최신 펌웨어 패치를 방해하는 연구를 수행한다. 이후, 메모리 포렌식 관점에서 공격 흔적을 도출하여 향후 공격에 대한 포렌식 가능성을 보인다.