Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.778138

CAPABILITY ANALYSIS OF ATM MALWARE USING THE CAPA FOR FORENSIC INVESTIGATIONS

Kiranbhai R Dodiya[1], Dr. Kapil Kumar[2]*

[1]Research Scholar, Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad, Gujarat-380009, India.

[2]*Associate Professor, Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad, Gujarat-380009, India

***CORRESPONDING AUTHOR: -** Dr. Kapil Kumar

*Associate Professor, Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad, Gujarat-380009, India

Abstract

The current Digital Age has seen an unprecedented shift in how people live, work and communicate owing to rapid technological progressions. Yet, this evolution also brings unique challenges, mainly concentrating on enhancing cybersecurity measures. ATM malware is a significant challenge due to its polymorphic nature. ATMs enable global financial transactions. However, ATMs lure crooks with financial gain. ATM malware has advanced recently, posing severe dangers to financial institutions and customers. This study analyses ATM malware capabilities using CAPA. ATM malware can be analyzed using CAPA. CAPA is applied to ATM malware types to investigate attackers' methods for stealing cash or sensitive financial data. Accurate CAPA analysis and ATM malware samples are the study techniques. The investigation examines the malware's code entry, card skimming, cash-out techniques, and network exploitation. ATM malware evasion tactics are also discussed. This analysis shows how ATM malware operates and evolves. ATM malware techniques and capabilities must be understood to improve ATM security. This research will help financial institutions and ATM designers stay ahead of hackers and improve safety. This study analyses ATM malware capabilities using CAPA. Examining real-world ATM malware samples helps researchers, security professionals, and industry stakeholders understand the evolving threat landscape. This study allows initiative-taking defences against ATM hacks, improving ATM system security and dependability.

Keywords: ATM-Malware, Network, Cyber-criminal, CAPA, Capability, Enhancing

1. Introduction

Malicious software called ATM malware, or ATM skimming, is intended to steal financial and personal information from Automated Teller Machines (ATMs). ATM malware is designed to capture and gather confidential information from unaware ATM users, including PIN codes and credit card details. The primary attack technique is reading and recording the data on the magnetic stripe of the user's card with skimming devices mounted to the ATM's card reader. The malware may also be injected into the ATM's operating system, giving attackers remote access and the ability to view confidential data. Once the attacker obtains the required information, they may use it to conduct numerous types of fraud, such as credit card fraud, identity theft, and unauthorized withdrawals. Financial institutions all around the globe are

becoming more concerned about the use of ATM malware since it may lead to significant financial losses and harm to their brand. [1]

1.1 Exploration of ATM-based malware:

The target and mode of attack are the primary distinctions between ATM malware and regular malware. When compared to ATM malware, which is specially designed to target automated teller machines, daily malware is created to infect and corrupt home computers or mobile devices. Because it must get past the security precautions put in place on ATMs, which are often more robust and safer than those found on personal devices, ATM malware is more complicated and sophisticated than ordinary malware. Malware for ATMs may be planted both physically on the ATM and remotely on the ATM's operating system. Common malware often aims to steal critical financial or personal information from the infected device or to use it as a springboard for other assaults on other systems. In contrast, ATM malware aims to gather consumers' financial and personal data for economic advantages, such as credit card fraud or identity theft. The amount of skill needed to produce and use one sort of malware differs from the other. While anybody with a rudimentary grasp of coding can create and disseminate regular malware, developing ATM malware requires more excellent skill and familiarity with ATM systems and security protocols [2].

1.2 Types of ATM Malware

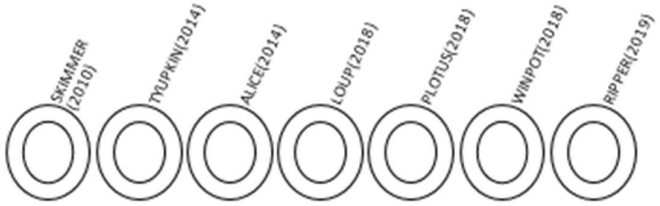


Figure 1 Types of ATM malware

1. Skimmer (2010): Skimmer is a type of malware that targets point-of-sale (POS) or ATM payment card terminals to steal sensitive data. Skimmers, like card numbers and PINs, are frequently used to collect credit card data, which could be used fraudulently.
2. Tyupkin (2014): Tyupkin was a type of financial malware that mainly targeted ATMs in Europe and allowed criminals to steal money from compromised devices. The virus required physical access to the ATM to take over the machine and make cash withdrawals. It used a series of codes and orders to do this.
3. ALICE (2014): 2014 a new banking Trojan named ALICE was released, targeting South Korean financial institutions. The virus attempted to steal banking passwords and other confidential information from affected P.Cs. Alice has sophisticated abilities, such as getting around security measures and permitting remote access.
4. LOUP (2018): The word "LOUP" is less well-known and has nothing to do with a virus or other cyber threat that is frequently discussed. It could be a word used in a particular region or a specific piece of malware.

PLOTUS, short for "Platinum Loader of the United States," is a banking Trojan linked to the hacking group Platinum. Despite having a particular interest in hacking American banks, PLOTUS primarily targeted financial institutions in Southeast Asia. The malware attempted to gain unauthorized access to banking systems to steal sensitive information and facilitate financial fraud.

6. WinPot (2018): WinPot is a specific type of malware that targets ATMs. Once attached to an ATM, a perpetrator could force the machine to print money against its will. A USB drive or other physical access device is frequently used to introduce the virus into the ATM. Even though it has primarily been studied in Mexico, its use may be every day abroad.

7. RIPPER (2019): Since its release in 2018, RIPPER, sometimes referred to as "Ryuk," has been a well-known ransomware variant. It is often disseminated through exploit kits and targeted phishing efforts. After infecting a system, RIPPER encrypts data, making them unavailable, and requests a Bitcoin ransom in exchange for their decryption. RIPPER is one of the most financially devastating ransomware families due to its substantial ransom demands. [10]

Literature Review:

In the field of malware analysis, the main two methods are static and dynamic malware analysis. Many researchers have published research papers on the static and dynamic analysis of malware.

"Malware Analysis: Tools and Techniques," by Kunwar et al. [11], describes malware analysis tools. This article summarises malware analysis methods, tools, and methodologies. Malware—viruses, worms, Trojans, and rootkits—is defined and explained in this research. Malware analysis helps understand malware activity and develop countermeasures. This study discusses static, dynamic, and hybrid malware analyses. He describes each method's pros and cons and shows its tools. The study discusses malware analysis tools such as disassemblers, debuggers, sandboxes, and memory analysis tools.

"Framework to detect malicious codes embedded with JPEG images over social networking sites" by Kunwar et al. proposes a framework for detecting malicious programs hidden in JPEG photos on social media. The study then proposes a way to detect malicious JPEG images. Pre-processing, feature extraction, classification, and post-processing comprise the framework. The writers explain and demonstrate how to use each component [12].

Malware analysis and detection using reverse engineering techniques (2018) S. Megira et al. work on VMware as virtualization and how malware works with This technical combination with dynamic gives a more accurate result and gives an idea of the different tools and techniques used for the analysis of the malware and the critical functions of the tools and techniques. [13]

"Emerging Malware Analysis Techniques and Tools: A Comparative Analysis" compares malware analysis techniques and technologies. The paper begins with malware and its growing sophistication. They then discuss how good malware analysis methods and tools can detect and mitigate malware. The study examines static, dynamic, hybrid, machine learning-based, and sandboxing malware analysis methods. The writers compare each method and tool's pros and cons [14].

CrowdStrike's "Ploutus ATM Malware Case Study: Automated Deobfuscation of a Strongly Obfuscated.NET Binary" examines the family. The document introduces the Ploutus malware's origins, capabilities, and targets. Next, Ploutus malware deobfuscation is automated via reflection-based metadata extraction. Ploutus deobfuscation was reported. The Ploutus malware's deobfuscation is discussed. The report displays its novel automatic deobfuscation approach. "Ploutus ATM Malware Case Study: Automated Deobfuscation of a Strongly Obfuscated.NET Binary" helps security researchers examine the family. The report discusses malware deobfuscation. The report displays its novel automatic deobfuscation approach. Tech findings: Ploutus wins ATM cassettes for all bills. Ploutus decompiles.NET Malware hides. Reflection decrypts malware. This discovery concerns ATM malware researchers and security experts. Ploutus malware deobfuscation is addressed. The report displays its innovative automatic deobfuscation [15].

The Tyupkin ATM virus is modular. Microsoft.NET decompiles efficiently. Malware is obfuscated—unauthorized cash dispensing ATM setup Security disablement 4. The Tyupkin virus endangers ATMs. Moreover, reports ATM operators should be aware of the malware, protect their ATMs, and emphasize the Tyupkin malware analysis's significant technical findings: Modular malware is removable. Malware analysis and ATM eradication are complex. Malware obfuscates its code: random functions, encrypted text, and variable names. Malware can contact a C&C server. This C&C server will enable hackers to command malware. ATM malware leverages multiple vulnerabilities. Malware may control ATMs and perpetrate crimes. [16]

"North Korean Remote Access Tool: FAST CASH for Windows" by the Cybersecurity and Infrastructure Security Agency (CISA) describes North Korean government-used RAT malware. The research says FastCash may steal data, install new malware, and stay on target networks. FBI and DoD analysts created the paper to help FASTCASH-infected organizations mitigate and respond. U.S. government partners recognized FastCash as North Korean RAT malware. The FBI believes HIDDEN COBRA operators use FAST CASH and proxy servers to stay on victim networks and abuse them. The report helps companies concerned about North Korean cyberattacks. Fast cash may compromise victim networks, according to the study. The study recommends FastCash and other RAT malware mitigation solutions for enterprises. Report results: The North Korean government employs FASTCASH RAT. FastCash takes data, infects networks, and remains. [17]

Payments Cards & Mobile's "ATM Hacking Report: Scenarios from 2018 ATM Hacks" investigates ATM hacking. The paper lists standard methods: Malware: Malware infects systems. Phishing emails, USB devices, and rogue websites can compromise ATMs. Social engineering: tricking someone into revealing personal information or harming themselves or their company. Social engineering impersonates customer service professionals to acquire ATM passwords or pins. ATM attacks. Physical attacks can install malware, steal cash, or turn off ATMs. Lists hackable ATMs. Vulnerable ATMs lack secure networks and maintenance. ATM security recommendations conclude the report. These tips: ATM upkeep: Refresh ATM security. ATMs need network security. ATMs need strong passwords. ATM staff should report suspicious activity. The study provides critical ATM hacking and protection information. Police, ATMs, and banks can use the report—more findings: Malware infects ATMs. Social

engineering hacks ATMs. Physical attacks install malware, steal cash, and turn off ATMs. Unprotected ATMs get hacked. Maintenance, connectivity, secure passwords, and training can prevent ATM hacking. [18]

Cyware Alerts' article "ATM Malware FiXS Targets Mexican Banks to Dispense Quick Money" outlines a new ATM malware strain named FiXS. Modular malware can steal money from ATMs and install and control other malware. It currently targets ATMs in Mexico but may target ATMs in other countries. ATMs can be protected from FiXS and other ATM malware by updating security patches, using strong passwords and multi-factor authentication, monitoring for suspicious activity, and using a security solution to detect and block malware. Financial institutions and law enforcement are needed to fight ATM malware [19].

Many researchers have worked on malware techniques using static and dynamic analysis using different tools and techniques. However, more work needs to be done on the capability of ATM malware, which is now a growing problem for the investigation agency, so here we attempt to examine the ATM malware using the CAPA. The main objective of the research is to analyze the ATM malicious code for forensic investigation using the CAPA. The REMnux tool CAPA analyses ATM malware to understand how it works and how it was deployed and to find indicators of compromise (IOCs) that can be used to identify and prevent future attacks. Studying malicious code can reveal how attackers break into ATMs and steal data. They can determine how the malware exploited hardware or software weaknesses to seize control of the ATM and how it communicates with the attacker's server to exfiltrate data.

This study uses the CAPA tool to evaluate malware behaviour and features. It may help investigators understand the malware's structure and purpose and locate its modules and functions.

2. METHODOLOGY

The open-source program CAPA demonstrates proficiency in the static evaluation of PE files; nonetheless, it has limitations in several dimensions compared to more thorough malware analysis tools. The primary emphasis of this software is on static analysis, with a notable absence of comprehensive signature-based detection often observed in commercial antivirus solutions. Furthermore, it specializes in PE file formats, which restricts its suitability to a broader array of file types. Although the tool incorporates YARA rules to enable configurable detection and is cost-effective as an open-source solution, it may require a higher skill level. It often has a smaller user community and less extensive documentation than user-friendly commercial alternatives offering dynamic analytic capabilities.

Sample size - 48 (ATM Malware)

SR.NO	NAME OF MALWARE	NUMBER OF SAMPLES
1	**Alice**	**06**
2	**Loup**	**01**

3	**Plotus**	**14**
4	**Skimmer**	**14**
5	**Tyupkin**	**06**
6	**Ripper**	**07**
Total number of samples - 48		

Table 2 Sample collection

Sample Collection: ATM Malware Family Download ATM malware from the malware research facility for research. Install REMnux virtualized the malware sample includes the Linux-based REMnux system for malware analysis. If packaged with the default password "infected," the malware sample must be unzipped before the examination.

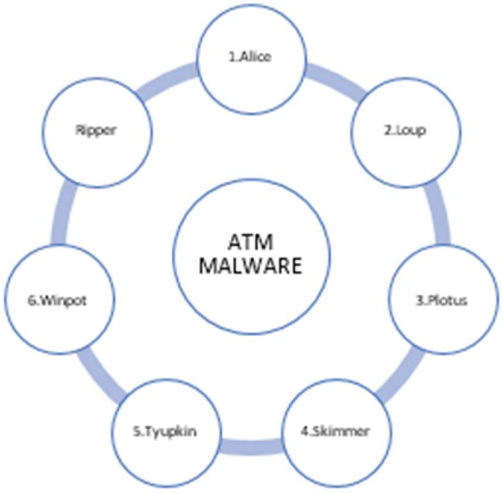


Figure 2 ATM Malware Family

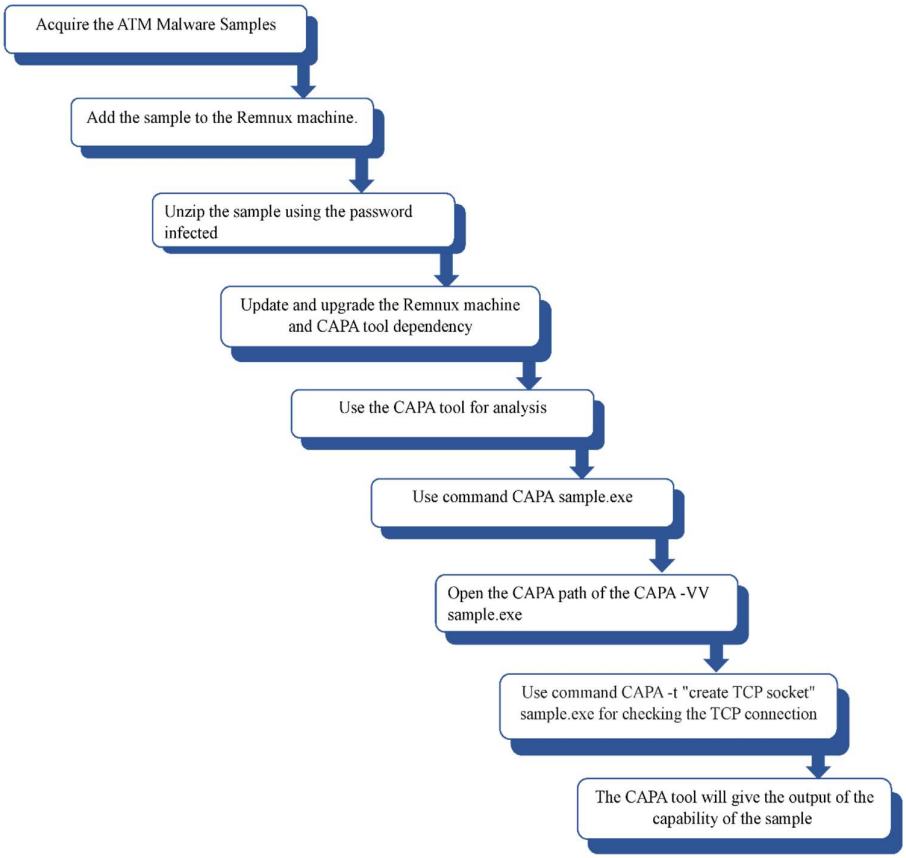


Figure 3 Flow Chart of CAPA Working Mechanisms

2.1 About the CAPA Tool

FireEye created the open-source CAPA (Comprehensive, Automated, and Parallel Analysis) program to do static analysis on malware samples. The Linux distribution REMnux, intended for malware analysis and reverse engineering, comes with CAPA.

CAPA employs sophisticated algorithms and heuristics to analyze malware and identify its capabilities, such as its ability for network interaction or system retention. Executable files, libraries, and scripts are just a few file types it can examine. It also produces a thorough report on its results.

The following are some CAPA features:

1. Analyzing malware based on its capabilities, such as networking, code injection, or persistence, is what CAPA does.
2. Detection of new, previously unknown threats and recognized malware families: CAPA can detect known and undiscovered threats.
3. Support for several file types, including executable files, DLLs, scripts, and more, is provided by CAPA.
4. Rule-based analysis: CAPA analyses malware and produces a report on its capabilities using a set of specified rules.

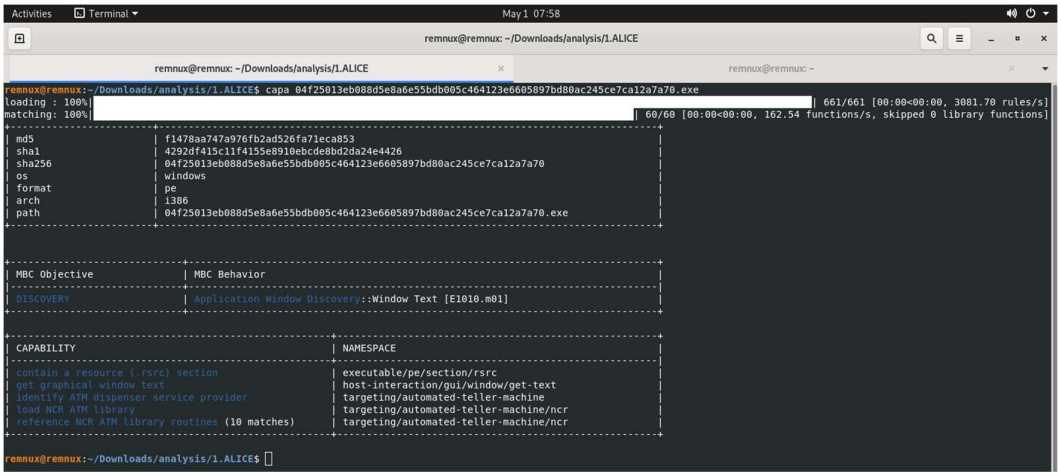
5. Integration with other tools: Virus Total, Cuckoo Sandbox, and other malware analysis platforms may all be integrated with CAPA.

2. SAMPLE ANALYSIS

Download ATM malware from the malware research facility for research.
Install REMnux virtualized. The malware sample includes the Linux-based REMnux system for malware analysis. If packaged with the default password "infected," the malware sample must be unzipped before the examination. Upgrade REMnux and CAPA tool dependency: Malware analysis requires the REMnux machine and CAPA tool to have the latest patches and dependencies.
A study using CAPA analysis: CAPA analyses malware capabilities via static analysis. It can evaluate ATM malware.
1."CAPA path of sample.exe": CAPA starts using this command on ATM malware. “Capa -vv sample.exe": When applying the "-vv" option, the CAPA program can disclose ATM malware sample characteristics and abilities.
capa -t "create TCP socket: This command checks the ATM malware's TCP connection. It shows a malware sample's connection, which could reveal the attacker's command and control locations.

3. Result and Discussion

1. capa sample.exe



The usage of the CAPA tool on the REMnux machine to analyze a sample malware file with the name "04f25013eb088d5e8a6e55bdb005c464123e6605897bd80ac245ce7ca12a7a70.exe" is shown in the activity log. The MBC (Malware Behaviour Classification) finds the window text in [E1010.mo1] during malware analysis requires an executable file with an ATM resource section (.rsrc). Malware acts as follows:

Discovery: ATM malware detects and identifies the window text.

Capability: Malware must contain a resource section (.rsrc) in its executable file to retrieve graphical window text. The ATM malware grabs window text from the host system's GUI and targets ATM dispenser service providers.

2. capa -V.V. sample path sample.exe

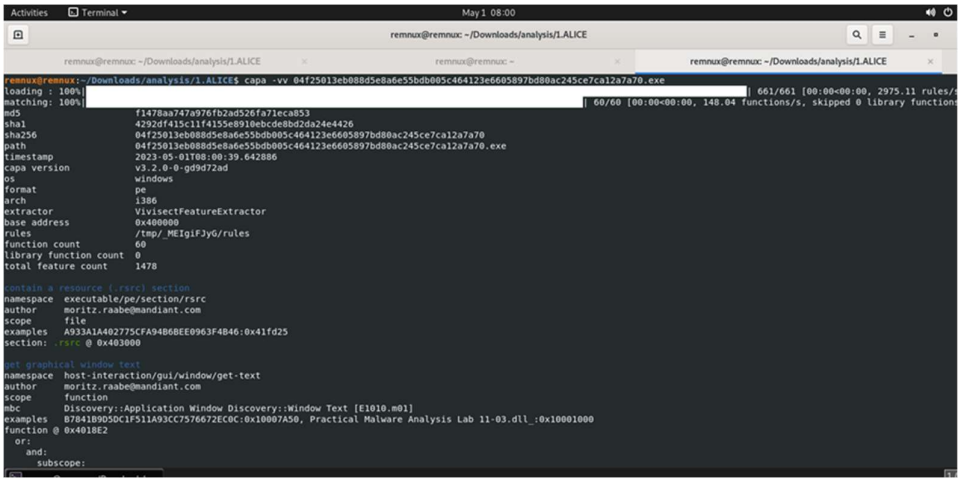


Figure 5 Verbose output

It consists of numerous actions and commands entering the terminal. A breakdown of several significant passages is provided below:

Working directories for the user are "/Downloads/analysis/1.ALICE," including "msxfs. WFSStartUp," "mixes. WFSCleanUp," "mixes. WFSFreeResult," "mixes. WFSLock," and "mixes. WFSGetInfo," among other API calls and methods. There are references to namespaces, authors, and scopes connected to the NCR ATM library and automated teller machine (ATM). With the "-vv" option, which denotes verbose output, the "capa" tool is used to analyze a file with the name "04f25013eb88d5e8a6e55bdb05c464123e6605897bdBoac245ce7cal2a7ar0.exe". The log records operations involving various commands and tools in analyzing and examining executable files. Information about API calls, functions, namespaces, and pointers to pertinent sites is included.

3. capa -t "create TCP socket" sample path sample.exe

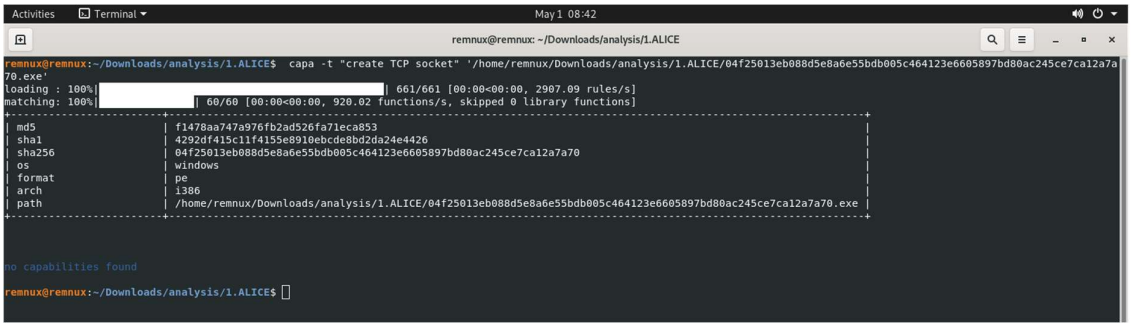


Figure 6 TCP connection

Whenever the tool Capa was used for analyzing a binary file with the name "04f25013eb088d5e8a6e55bdb005c464123e6605897bd80ac245ce7ca12a7a70.exe" to look for the capability "create TCP socket," it did not find any matches in the binary. This parameter indicates that this sample is not transmitting data to its command-and-control center.

4. Conclusion

This study discusses the forensics analysis of ATM malware using the CAPA tool. The research examines ATM malware varieties, their characteristics, and how the CAPA tool can find and analyze them. This study will illuminate the research emphasizing the need for timely ATM malware analysis and forensic investigation to avert financial losses and protect banks' reputations. This research provides security experts and enforcement organizations with an easy-to-follow process for employing the CAPA tool in ATM malware forensics. This study expands knowledge of ATM malware analysis and CAPA use. Keep up with ATM malware and other cybercrimes. This study emphasizes the need for continual research and developing new methodologies and technologies.

5. FUTURE SCOPE

Creating advanced tools: The study stresses the need for forensic tools to identify and analyze ATM malware. Future research may build faster, more accurate ATM malware detection and evaluation methods. Given ATM malware's complexity, advanced machine learning and A.I. methods are needed to detect and analyze such threats. Future research may focus on ATM malware-detecting machine learning and A.I. models. The study stresses the need for law enforcement and banking institutions to work together to combat ATM malware. Future research may focus on improving data exchange among these organizations to avoid and detect ATM malware. The research recommends software updates, system upgrades, and employee training to prevent ATM malware assaults. ATM malware hazards in financial institutions may be addressed in future studies.

REFERENCES

1. “Malware-based attacks on ATMs – A summary – NVISO Labs.” https://blog.nviso.eu/2023/01/10/malware-based-attacks-on-atms-a-summary/ (accessed May 15, 2023).
2. “What Is the Difference Between Malware and a Virus? | Trellix.” https://www.trellix.com/en-us/security-awareness/ransomware/malware-vs-viruses.html (accessed May 15, 2023).
3. “Everything You Need to Know About the ‘Alice’ ATM Malware - PSafe Blog.” https://www.psafe.com/en/blog/everything-need-know-alice-atm-malware/ (accessed May 15, 2023).
4. “Loup Malware Removal Report.” https://www.enigmasoftware.com/loupmalware-removal/ (accessed May 15, 2023).
5. “Jackpotting malware | Infosec Resources.” https://resources.infosecinstitute.com/topic/jackpotting-malware/ (accessed May 15, 2023).

6. "ATM is a New Skimmer: Crooks Bring ATMs on Their Side | Kaspersky." https://www.kaspersky.com/about/press-releases/2016_atm-is-a-new-skimmer-crooks-bring-atms-on-their-side (accessed May 15, 2023).
7. "Tyupkin Virus (Malware) | ATM Machine Security | Virus Definition." https://www.kaspersky.com/resource-center/threats/tyupkin-malware-atm-security-malware (accessed May 15, 2023).
8. "WinPot Malware Uses Slot Machine-Like Interface to Empty ATMs." https://securityintelligence.com/news/winpot-malware-uses-slot-machine-like-interface-to-empty-atms/ (accessed May 15, 2023).
9. D. Sancho and N. Huq, "Cashing in on ATM Malware: a Comprehensive Look at Various Attack Types." [Online]. Available: www.europol.europa.eu
10. "10 years of virtual dynamite: A high-level retrospective of ATM malware." https://blog.talosintelligence.com/10-years-of-virtual-dynamite/ (accessed May 15, 2023).
11. R. S. Kunwar and P. Sharma, "Malware analysis: Tools and techniques," *ACM International Conference Proceeding Series*, vol. 04-05-March-2016, Mar. 2016, doi: 10.1145/2905055.2905361.
12. R. S. Kunwar and P. Sharma, "Framework to detect malicious codes embedded with JPEG images over social networking sites," *Proceedings of 2017 International Conference on Innovations in Information, Embedded and Communication Systems, ICIIECS 2017*, vol. 2018-January, pp. 1–4, Jan. 2018, doi: 10.1109/ICIIECS.2017.8276144.
13. S. Megira, A. R. Pangesti, and F. W. Wibowo, "Malware Analysis and Detection Using Reverse Engineering Technique," *J Phys Conf Ser*, vol. 1140, no. 1, p. 012042, Dec. 2018, doi: 10.1088/1742-6596/1140/1/012042.
14. "(PDF) An Emerging Malware Analysis Techniques and Tools: A Comparative Analysis." https://www.researchgate.net/publication/350886133_An_Emerging_Malware_Analysis_Techniques_and_Tools_A_Comparative_Analysis#fullTextFileContent (accessed May 15, 2023).
15. "Automated Deobfuscation of Ploutus ATM Malware | CrowdStrike." https://www.crowdstrike.com/blog/ploutus-atm-malware-deobfuscation-case-study/ (accessed May 24, 2023).
16. "Tyupkin ATM Malware Analysis | Infosec Resources." https://resources.infosecinstitute.com/topic/tyupkin-atm-malware-analysis/ (accessed May 24, 2023).
17. "MAR-10257062-1. v2 - North Korean Remote Access Tool: FASTCASH for Windows | CISA." https://www.cisa.gov/news-events/analysis-reports/ar20-239c (accessed May 24, 2023).
18. "ATM hacking report: Scenarios from 2018 ATM hacks." https://www.paymentscardsandmobile.com/atm-hacking-report/ (accessed May 24, 2023).

19. “ATM Malware FiXS Targets Mexican Banks to Dispense Quick Money | Cyware Alerts - Hacker News.” https://cyware.com/news/atm-malware-fixs-targets-mexican-banks-to-dispense-quick-money-9d39c87c (accessed May 24, 2023).