Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

Unmasking the Threat: Exploring Effective Techniques for Investigating ATM Malware Through Digital Forensic Analyses

Kiranbhai R Dodiya1, Kashyap Joshi2, Dr. Kapil Kumar3*

1,2Research Scholar, Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad, Gujarat-380009, India.
3*Associate Professor, Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad, Gujarat-380009, India, E-mail: - kkforensic@gmail.com

*Corresponding Author- Dr. Kapil Kumar
Associate Professor, Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad, Gujarat-380009, India, E-mail: - kkforensic@gmail.com

Abstract:
Hackers have developed new techniques to directly breach a system or device, responding to the surge in numerous cybercrimes. Criminals frequently attack automated teller machines (ATMs) because of the vulnerabilities they present. ATM security must monitor and investigate these attacks because ATMs may contain and manage enormous sums of cash, making them good targets for hackers. Because of this, ATM security needs to monitor and investigate these assaults. Because automated teller machines may hold and handle significant quantities of money, the security at ATMs needs to monitor and analyze assaults of this kind. In the present study, using Studio to analyze ATM malware is essential to identifying malware signatures and behaviours that can improve ATM security. Banks and ATM manufacturers must implement specific measures to prevent ATM malware attacks. Based on present research on ATM malware analysis, researchers have uncovered critical insights that are highly beneficial for those seeking to investigate Malware aimed at breaching automated teller machines (ATMs). It is an invaluable tool for conducting such investigations. This paper will serve as a means of sharing insightful findings and aiding others in deepening their understanding of this crucial topic.

Keywords: ATM Malware, Investigation, Cyber-Attack, Analysis

1. Introduction:

ATM malware is malicious software or code designed to target automated teller machines (ATMs) to carry out unauthorized activities for financial gain. This type of malware is crafted to exploit ATM system vulnerabilities and compromise security measures (“Hacking ATMs: The New Wave of Malware | Infosec Resources,” n.d.). Malware-based ATM assaults have increased due to attacker sophistication and simple dark web access to resources and information. Hackers are finding more sophisticated ways to attack ATMs using Malware to win jackpots and control cash extraction (“Malware-based attacks on ATMs – A summary – NVISO Labs,” n.d.). ATM skimming steals credit card information through a hidden camera that records the victim's PIN and lets fraudsters clone their credit card and make illicit purchases. ATM malware comprises cash trapping and network-based attacks that exploit ATM network connection weaknesses (“What Is ATM Skimming and How to Spot a Skimmer | Avast,” n.d.).

Banks and ATM manufacturers must implement strict access limits, frequent software and hardware updates, and regular security assessments to prevent ATM malware attacks. Users should also be aware of suspected ATM activity and protect themselves by covering the keypad when entering their PIN and regularly checking their bank records for unauthorized transactions (“ATM Malware: The Next Generation of ATM Attacks,” n.d.).

ATM malware may be categorized into several types according to its functions, installation procedures, and the attackers’ objectives (“ATM logic attacks: vulnerabilities and security risks of ATMs,” n.d.). Figure 1 shows a few common types of ATM malware.

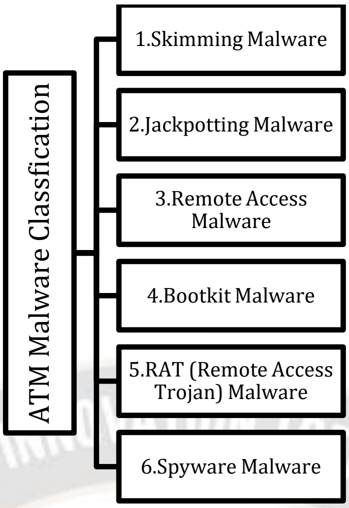


***Figure 1**: Classification of ATM Malware Based on the Mode of Operation*

The first category of malware is "skimming malware," which tries to intercept card information by installing tools or messing with an ATM's card reader ("ATM is a New Skimmer: Crooks Bring ATMs on Their Side | Kaspersky," n.d.). This malware gathers data from a debit or credit card's magnetic stripe or chip. The second category of malware is jackpotting malware, which modifies the hardware or software of the ATM to release cash without permission ("Jackpotting malware | Infosec Resources," n.d.). The third type of Malware is "Remote access" malware, which allows hackers to acquire unauthorized control over ATMs by exploiting poor network security or software flaws ("What is Remote Access Trojan (RAT)? - Check Point Software," n.d.). The fourth type of malware, known as a "Bootkit," infects the ATM's boot process and gives attackers ongoing access to the system ("Bootkit | Malwarebytes Labs," n.d.). The sixth sort of malware, RAT (Remote Access Trojan), gives hackers remote access to the compromised ATM, allowing them to conduct unauthorized acts ("FIN7 Hackers Load New RAT Malware Into ATM Maker's Software," n.d.). Finally, the sixth type of malware is spyware, which monitors and records ATM activity, such as keystrokes or screenshots, to steal sensitive information ("All you need to know about the spyware in ATMs that can steal your money from the bank - iPleaders," n.d.).

This research article aims to contribute to ATM malware analysis by expanding our understanding of investigative procedures for examining malicious software targeting automated teller machines (ATMs). With the rising sophistication of attacks on ATMs, we must enhance our knowledge of practical techniques for uncovering and analyzing ATM malware.

2. Material and Methodology:

2.1 Sample Collection:

This study examined 35 ATM malware of 5 families from different online sources. Among the analyzed ATM malware samples, the first malware, Alice, comprises six models, whereas a single piece represents Loup. Notably, Plotus demonstrates the very best wide variety of portions, amounting to fourteen, accompanied by means of Skimmer and Tyupkin, which encompass nine and 5 samples, respectively. The array of ATM malware variations offers a treasured opportunity to very well look at their precise traits, behaviours, and potential affects. This complete evaluation contributes to more sturdy statistics at the evolving hazard panorama within the banking region. By cautiously studying these malware samples, it becomes possible to increase effective countermeasures, bolstering the safety of ATM systems and minimizing the dangers posed with the aid of these trendy attack

2.2 New technique for category of ATM Malware:

The accrued samples of ATM malware had been systematically classified based on their fantastic assault mechanisms. This kind lets in a extra profound knowledge of the various techniques employed using attackers in compromising ATM systems. By ordering the samples, researchers can come to be aware of patterns and traits that indicate the capability of new procedures or emerging strategies utilized by ATM malware in virtual forensics. The accrued samples of ATM malware were systematically labeled primarily based on their wonderful attack mechanisms. This classification permits a deeper information of the diverse strategies employed by using attackers in compromising ATM systems. By categorizing the samples, researchers can perceive styles and traits that can imply capability new approaches or rising strategies utilized by ATM malware in virtual forensics.

2.2 Tool used for evaluation:

PEStudio is a critical device employed on this have a look at to conduct an in-intensity evaluation of Windows executable files, in particular the ones containing malicious code. Using PEStudio, researchers can study the import and export capabilities, become aware of aid strings, and establish associations with malicious code. Without charge, PEStudio can perform a static evaluation on diverse Windows executable files, including malware, trojans, and viruses. This function is worthwhile for safety researchers, malware analysts, and reverse engineers, allowing them to successfully find out and compare probably risky code within those files. By leveraging the competencies of PEStudio, professionals inside the field can efficaciously pick out and assess the character of ability threats, contributing to the continuing efforts to beautify cybersecurity measures. PEStudio analyses the header, resources, imports, exports, and metadata to comprehend the file. It also indicates malware-like code or language. Malware makers use packers, cryptos, and other obfuscations to hide. PEStudio's simple interface reveals much about executable files. Custom searches, filtering, and exporting data for research are also available.

2.3 Analysis workflow in PEStudio for ATM Malware:

A systematic approach is essential for malware analysis to comprehend its functionality and potential risks. Security experts can explore the subtle complexities of a malware sample by going through a set of procedures while using specialized tools like PEStudio. The first step is to obtain the malware sample and set up PEStudio, a potent software program for looking at Windows executable files. After loading the model into PEStudio, the analysis goes through several steps, including Virus total scanning, looking into blocked libraries, self-modifying potential, finding stopped strings, and looking closely at suspicious imports and exports. Each meticulously planned procedure helps to reveal the inner workings and purposes of the malware under study ("Pestudio: Initial Malware Assessment Made Simple - Security Investigation," n.d.).

Acquire malware sample

Download and install PE studio

Add the executable sample

Analyze the Malware using different functions of PEstudio

Analysis using virustotal score

Analysis of blacklisted library

Analysis of self modifying capabilities

Analysis of blacklisted strings

Analysis of suspicious imports and exports

***Figure 2:** Analysis Workflow in PEStudio for ATM Malware*

3 Results:

3.1 Classification of ATM Malware:

By studying these distinct types of ATM malware, security experts and financial institutions can effectively enhance their defence mechanisms and develop efficient responses to counter these threats. The classification in Table 1 offers an overview of the different types of ATM malware based on their specific functionalities.

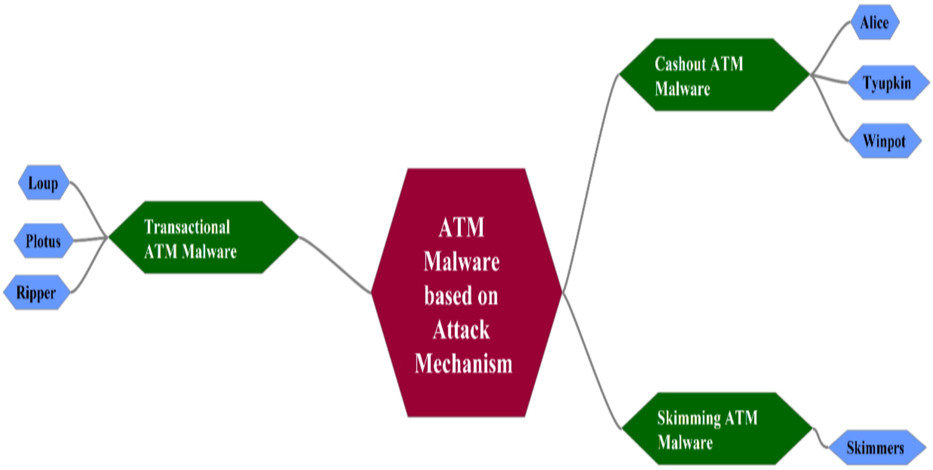
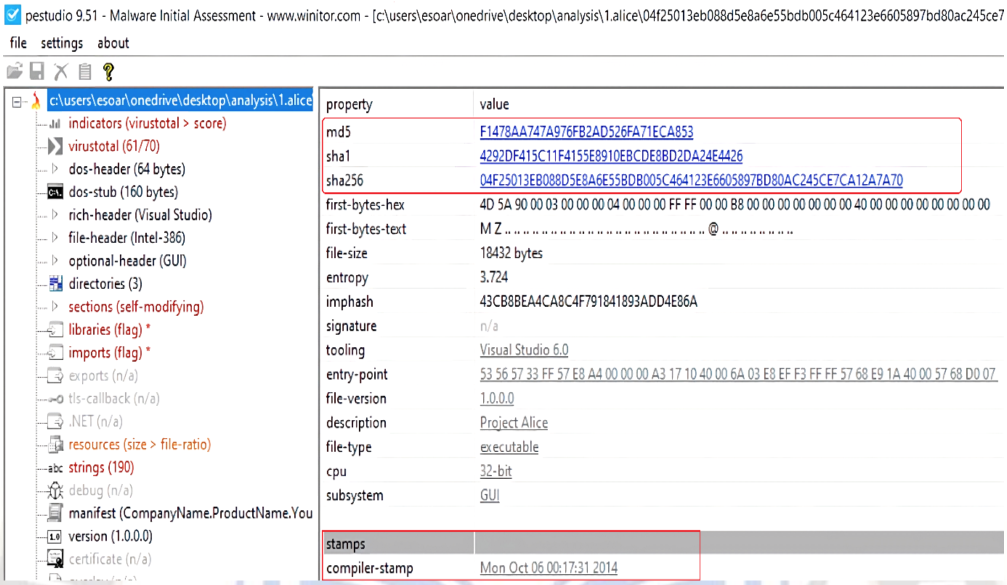


***Figure 3** Classification of ATM Malware*

Analysis of ATM Malware:

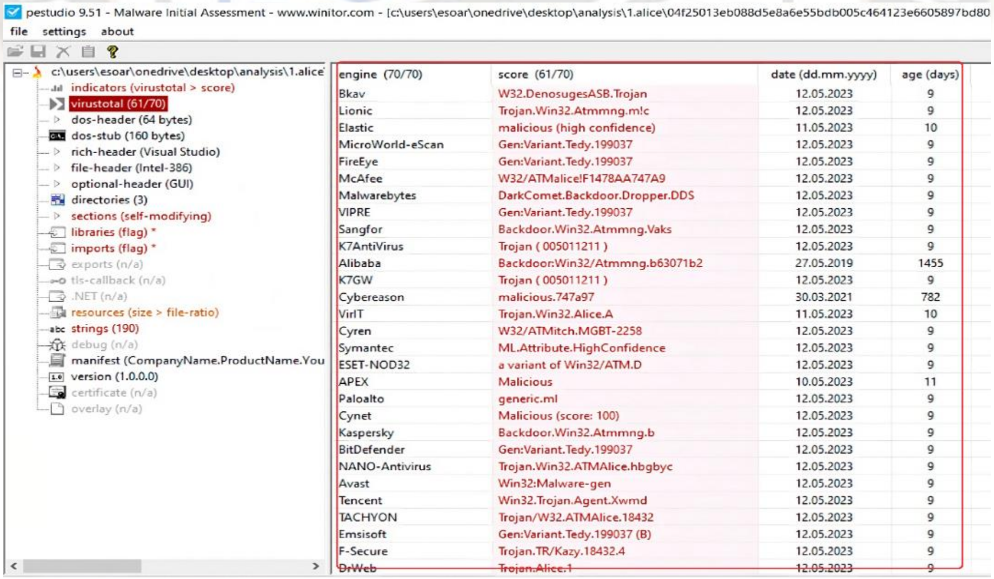
The executable's MD5, SHA1, and SHA256 results from PEStudio will help identify the ATM malware's signature. The first byte's hex will help determine the origin file type because malware authors often employ obfuscation to disguise suspicious behaviour. (Fig.3) Shannon entropy values indicate suspicious activity between 0 and 8 and above 7.2. Time stamps help identify file origin, executable tempering, and threat development.


pestudio 9.51 - Malware Initial Assessment - www.winitor.com - [c:\users\esoar\onedrive\desktop\analysis\1.alice\04f25013eb088d5e8a6e55bdb005c464123e6605897bd80ac245ce7
file settings about
c:\users\esoar\onedrive\desktop\analysis\1.alice
indicators (virustotal > score)
virustotal (61/70)
dos-header (64 bytes)
dos-stub (160 bytes)
rich-header (Visual Studio)
file-header (Intel-386)
optional-header (GUI)
directories (3)
sections (self-modifying)
libraries (flag) *
imports (flag) *
exports (n/a)
tls-callback (n/a)
.NET (n/a)
resources (size > file-ratio)
strings (190)
debug (n/a)
manifest (CompanyName.ProductName.You
version (1.0.0.0)
certificate (n/a)

property	value
md5	F1478AA747A976FB2AD526FA71ECA853
sha1	4292DF415C11F4155E8910EBCDE8BD2DA24E4426
sha256	04F25013EB088D5E8A6E55BDB005C464123E6605897BD80AC245CE7CA12A7A70
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00
first-bytes-text	M Z .. .. @ .. ..
file-size	18432 bytes
entropy	3.724
imphash	43CB8BEA4CA8C4F791841893ADD4E86A
signature	n/a
tooling	Visual Studio 6.0
entry-point	53 56 57 33 FF 57 E8 A4 00 00 00 A3 17 10 40 00 6A 03 E8 EF F3 FF FF 57 68 E9 1A 40 00 57 68 D0 07
file-version	1.0.0.0
description	Project Alice
file-type	executable
cpu	32-bit
subsystem	GUI
stamps	
compiler-stamp	Mon Oct 06 00:17:31 2014

__Figure 4:__ Snapshot of the Basic Indicator of ATM Malware

While examining a PE file, the Virus Total API plugin in PE Studio is used to scan the Virus Total detection rate of the file. The plugin will display the detection rate as a number, indicating how many antivirus engines out of all those that scanned it determined the file to be harmful. That specific antivirus search engine could not identify this malware code.

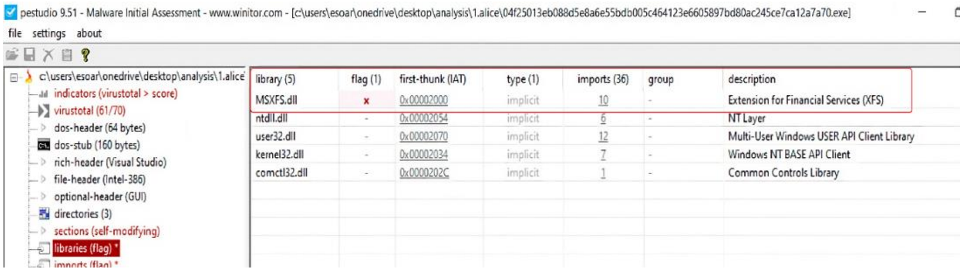

pestudio 9.51 - Malware Initial Assessment - www.winitor.com - [c:\users\esoar\onedrive\desktop\analysis\1.alice\04f25013eb088d5e8a6e55bdb005c464123e6605897bd80
file settings about
c:\users\esoar\onedrive\desktop\analysis\1.alice
indicators (virustotal > score)
virustotal (61/70)
dos-header (64 bytes)
dos-stub (160 bytes)
rich-header (Visual Studio)
file-header (Intel-386)
optional-header (GUI)
directories (3)
sections (self-modifying)
libraries (flag) *
imports (flag) *
exports (n/a)
tls-callback (n/a)
.NET (n/a)
resources (size > file-ratio)
strings (190)
debug (n/a)
manifest (CompanyName.ProductName.You
version (1.0.0.0)
certificate (n/a)
overlay (n/a)

engine (70/70)	score (61/70)	date (dd.mm.yyyy)	age (days)
Bkav	W32.DenosugesASB.Trojan	12.05.2023	9
Lionic	Trojan.Win32.Atmmng.m!c	12.05.2023	9
Elastic	malicious (high confidence)	11.05.2023	10
MicroWorld-eScan	Gen:Variant.Tedy.199037	12.05.2023	9
FireEye	Gen:Variant.Tedy.199037	12.05.2023	9
McAfee	W32/ATMalice!F1478AA747A9	12.05.2023	9
Malwarebytes	DarkComet.Backdoor.Dropper.DDS	12.05.2023	9
VIPRE	Gen:Variant.Tedy.199037	12.05.2023	9
Sangfor	Backdoor.Win32.Atmmng.Vaks	12.05.2023	9
K7AntiVirus	Trojan (005011211)	12.05.2023	9
Alibaba	Backdoor:Win32/Atmmng.b63071b2	27.05.2019	1455
K7GW	Trojan (005011211)	12.05.2023	9
Cybereason	malicious.747a97	30.03.2021	782
VirIT	Trojan.Win32.Alice.A	11.05.2023	10
Cyren	W32/ATMitch.MGBT-2258	12.05.2023	9
Symantec	ML.Attribute.HighConfidence	12.05.2023	9
ESET-NOD32	a variant of Win32/ATM.D	12.05.2023	9
APEX	Malicious	10.05.2023	11
Paloalto	generic.ml	12.05.2023	9
Cynet	Malicious (score: 100)	12.05.2023	9
Kaspersky	Backdoor.Win32.Atmmng.b	12.05.2023	9
BitDefender	Gen:Variant.Tedy.199037	12.05.2023	9
NANO-Antivirus	Trojan.Win32.ATMAlice.hbgbyc	12.05.2023	9
Avast	Win32:Malware-gen	12.05.2023	9
Tencent	Win32.Trojan.Agent.Xwmd	12.05.2023	9
TACHYON	Trojan/W32.ATMAlice.18432	12.05.2023	9
Emsisoft	Gen:Variant.Tedy.199037 (B)	12.05.2023	9
F-Secure	Trojan.TR/Kazy.18432.4	12.05.2023	9
DrWeb	Trojan.Alice.1	12.05.2023	9

__Figure 5:__ Virus Total Indicator of ATM Malware

The fact that the MSXFS.dll file was classified as harmful in this portion of the library analysis implies that it could be compromised. Figure 5, which illustrates the presence of malicious code using this component within the library, supports the suspicions raised by earlier analysis and further helps them.

Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*



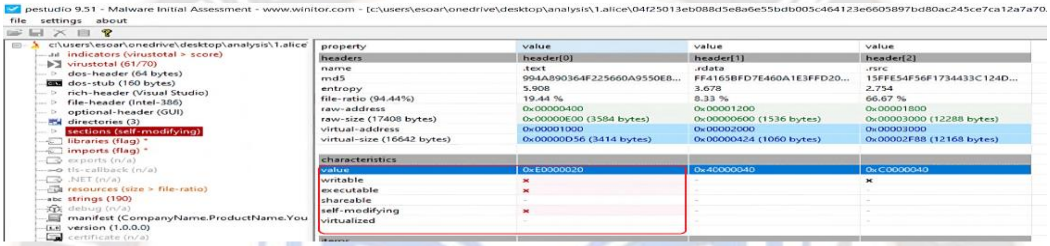
pestudio 9.51 - Malware Initial Assessment - www.winitor.com - [c:\users\esoar\onedrive\desktop\analysis\1.alice\04f25013eb088d5e8a6e55bdb005c464123e6605897bd80ac245ce7ca12a7a70.exe]

- c:\users\esoar\onedrive\desktop\analysis\1.alice
- indicators (virustotal > score)
- virustotal (61/70)
- dos-header (64 bytes)
- dos-stub (160 bytes)
- rich-header (Visual Studio)
- file-header (Intel-386)
- optional-header (GUI)
- directories (3)
- sections (self-modifying)
- libraries (flag) *
- imports (flag) *

library (5)	flag (1)	first-thunk (IAT)	type (1)	imports (36)	group	description
MSXFS.dll	x	0x00002000	implicit	10	-	Extension for Financial Services (XFS)
ntdll.dll	-	0x00002054	implicit	6	-	NT Layer
user32.dll	-	0x00002070	implicit	12	-	Multi-User Windows USER API Client Library
kernel32.dll	-	0x00002034	implicit	7	-	Windows NT BASE API Client
comctl32.dll	-	0x0000202C	implicit	1	-	Common Controls Library

Figure 6 *shows the malicious library (flag).*

Section (self-modifying)" usually refers to malicious code that alters itself during execution. Malware authors may use self-modifying code to evade security measures or make reverse engineering harder. Self-modifying code may dynamically produce or change memory instructions, making signature-based malware detection more challenging. PEStudio analyses Windows executables and lists "Sections (self-modifying)" in its report. This information can help analysts understand how the virus works and improve detection and mitigation measures.



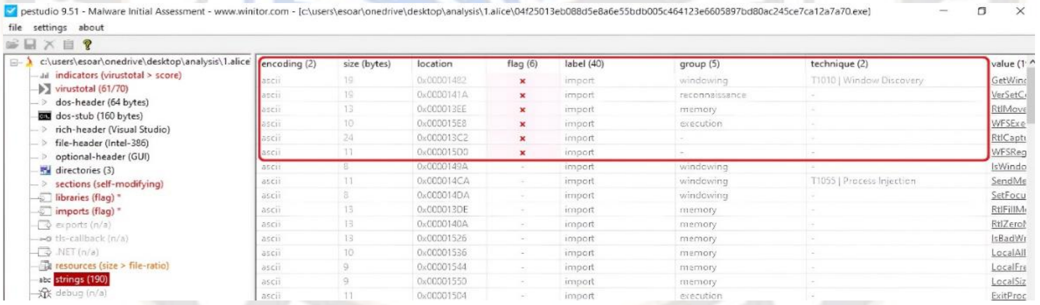
pestudio 9.51 - Malware Initial Assessment - www.winitor.com - [c:\users\esoar\onedrive\desktop\analysis\1.alice\04f25013eb088d5e8a6e55bdb005c464123e6605897bd80ac245ce7ca12a7a70.

- c:\users\esoar\onedrive\desktop\analysis\1.alice
- indicators (virustotal > score)
- virustotal (61/70)
- dos-header (64 bytes)
- dos-stub (160 bytes)
- rich-header (Visual Studio)
- file-header (Intel-386)
- optional-header (GUI)
- directories (3)
- sections (self-modifying)
- libraries (flag) *
- imports (flag) *
- exports (n/a)
- tls-callback (n/a)
- .NET (n/a)
- resources (size > file-ratio)
- strings (190)
- debug (n/a)
- manifest (CompanyName.ProductName.You
- version (1.0.0.0)
- certificate (n/a)

property	value	value	value
headers	header[0]	header[1]	header[2]
name	.text	.rdata	.rsrc
md5	994A890364F225660A9550E8...	FF4165BFD7E460A1E3FFD20...	15FFE54F56F1734433C124D...
entropy	5.908	3.678	2.754
file-ratio (94.44%)	19.44 %	8.33 %	66.67 %
raw-address	0x00000400	0x00001200	0x00001800
raw-size (17408 bytes)	0x00000E00 (3584 bytes)	0x00000600 (1536 bytes)	0x00003000 (12288 bytes)
virtual-address	0x00001000	0x00002000	0x00003000
virtual-size (16642 bytes)	0x00000D56 (3414 bytes)	0x00000424 (1060 bytes)	0x00002F88 (12168 bytes)
characteristics			
value	0xE0000020	0x40000040	0xC0000040
writable	x	-	x
executable	x	-	-
shareable	-	-	-
self-modifying	x	-	-
virtualized	-	-	-

Figure 7 *shows the analysis of the Section (self-modifying capability).*

The flag library list contains intriguing functionality and flag strings that provide insight into what malware attempts to perform in the ATM. In Figure 7, the malware attempts to run instructions in the WFS framework and import data from the WFS register.



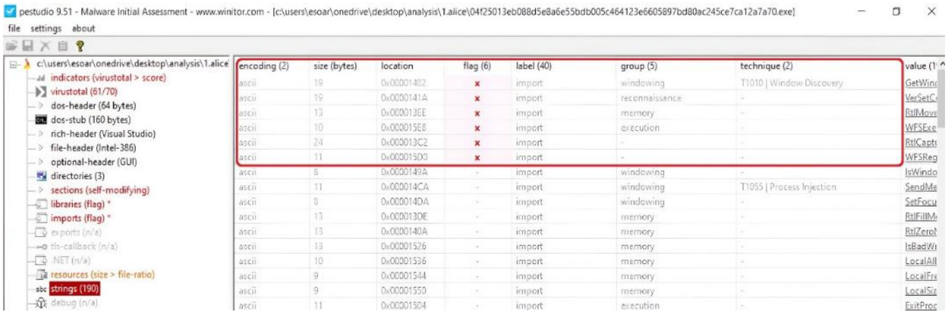
pestudio 9.51 - Malware Initial Assessment - www.winitor.com - [c:\users\esoar\onedrive\desktop\analysis\1.alice\04f25013eb088d5e8a6e55bdb005c464123e6605897bd80ac245ce7ca12a7a70.exe]

- c:\users\esoar\onedrive\desktop\analysis\1.alice
- indicators (virustotal > score)
- virustotal (61/70)
- dos-header (64 bytes)
- dos-stub (160 bytes)
- rich-header (Visual Studio)
- file-header (Intel-386)
- optional-header (GUI)
- directories (3)
- sections (self-modifying)
- libraries (flag) *
- imports (flag) *
- exports (n/a)
- tls-callback (n/a)
- .NET (n/a)
- resources (size > file-ratio)
- strings (190)
- debug (n/a)

encoding (2)	size (bytes)	location	flag (6)	label (40)	group (5)	technique (2)	value (1
ascii	19	0x00001482	x	import	windowing	T1010 | Window Discovery	GetWind
ascii	19	0x0000141A	x	import	reconnaissance	-	VerSetC
ascii	13	0x000013EE	x	import	memory	-	RtlMove
ascii	10	0x000015E8	x	import	execution	-	WFSExe
ascii	24	0x000013C2	x	import	-	-	RtlCaptu
ascii	11	0x000015D0	x	import	-	-	WFSReg
ascii	8	0x0000149A	-	import	windowing	-	IsWindo
ascii	11	0x000014CA	-	import	windowing	T1055 | Process Injection	SendMe
ascii	8	0x000014DA	-	import	windowing	-	SetFocu
ascii	13	0x000013DE	-	import	memory	-	RtlFillM
ascii	13	0x0000140A	-	import	memory	-	RtlZeroM
ascii	13	0x00001526	-	import	memory	-	IsBadWr
ascii	10	0x00001536	-	import	memory	-	LocalAll
ascii	9	0x00001544	-	import	memory	-	LocalFre
ascii	9	0x00001550	-	import	memory	-	LocalSiz
ascii	11	0x00001504	-	import	execution	-	ExitProc

Figure 8 *shows the analysis of code strings.*

The "Import" component in PEStudio malware analysis refers to a Windows executable's or DLL file's imported functions from other systems or third-party libraries. In Figure 8, this section may assist in identifying the malware's external resources and suspicious APIs.



pestudio 9.51 - Malware Initial Assessment - www.winitor.com - [c:\users\esoar\onedrive\desktop\analysis\1.alice\04f25013eb088d5e8a6e55bdb005c464123e6605897bd80ac245ce7ca12a7a70.exe]

- c:\users\esoar\onedrive\desktop\analysis\1.alice
- indicators (virustotal > score)
- virustotal (61/70)
- dos-header (64 bytes)
- dos-stub (160 bytes)
- rich-header (Visual Studio)
- file-header (Intel-386)
- optional-header (GUI)
- directories (3)
- sections (self-modifying)
- libraries (flag) *
- imports (flag) *
- exports (n/a)
- tls-callback (n/a)
- .NET (n/a)
- resources (size > file-ratio)
- strings (190)
- debug (n/a)

encoding (2)	size (bytes)	location	flag (6)	label (40)	group (5)	technique (2)	value (1
ascii	19	0x00001482	x	import	windowing	T1010 | Window Discovery	GetWind
ascii	19	0x0000141A	x	import	reconnaissance	-	VerSetC
ascii	13	0x000013EE	x	import	memory	-	RtlMove
ascii	10	0x000015E8	x	import	execution	-	WFSExe
ascii	24	0x000013C2	x	import	-	-	RtlCaptu
ascii	11	0x000015D0	x	import	-	-	WFSReg
ascii	8	0x0000149A	-	import	windowing	-	IsWindo
ascii	11	0x000014CA	-	import	windowing	T1055 | Process Injection	SendMe
ascii	8	0x000014DA	-	import	windowing	-	SetFocu
ascii	13	0x000013DE	-	import	memory	-	RtlFillM
ascii	13	0x0000140A	-	import	memory	-	RtlZeroM
ascii	13	0x00001526	-	import	memory	-	IsBadWr
ascii	10	0x00001536	-	import	memory	-	LocalAll
ascii	9	0x00001544	-	import	memory	-	LocalFre
ascii	9	0x00001550	-	import	memory	-	LocalSiz
ascii	11	0x00001504	-	import	execution	-	ExitProc

Figure 9 *shows the analysis of imports used by malicious code.*

In ATM malware analysis, the suspected files noted are compared to specific ATM malware families. Here's an explanation of the associated ATM malware family and the range of occurrences.

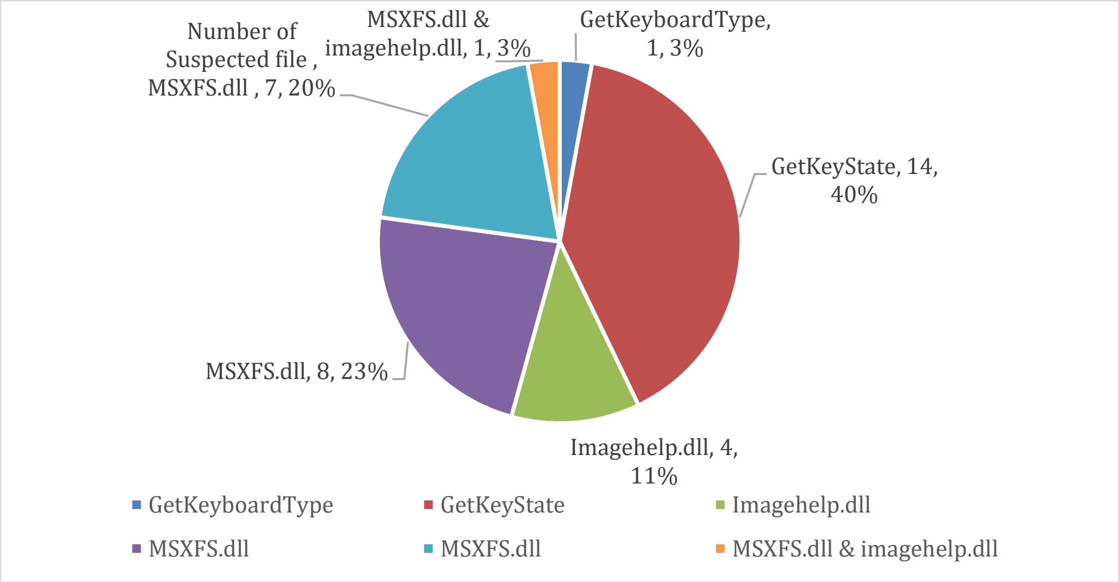


***Fig 10**. Comparative Study of ATM Malware Family*

The Skimmer malware family is well-known for its ability to collect and steal sensitive data from ATM consumers. It is connected to the Plotus malware family, which may also employ keylogging methods to collect user credentials. Imagehelp.Dll is a Dynamic Link Library (DLL) record used to govern executable documents intently related to the Skimmer malware circle of relatives. MSXFS.Dll is a DLL report linked with the Microsoft Extended Financial Services (XFS) framework related to the Alice and Skimmer malware families. MSXFS.Dll is connected to the Tyupkin malware own family, that's notorious for compromising ATMs and allowing illegal coin withdrawals.MSXFS.Dll & imagehelp.Dll is a mash-up of the MSXFS.Dll and imagehlp.Dll files, each of which might be related to the Skimmer malware circle of relatives. Analysts may additionally get insights into the frequency and relevance of awesome ATM malware households via analyzing the diversity of suspicious files approximately every malware family. The provided information shows the wide variety of suspected files associated with extraordinary ATM malware families. These include GetKeyboardType (Skimmer, one count), GetKeyState (Plotus, 14 counts), Imagehelp.dll (Skimmer, four counts), MSXFS.Dll (Alice, Skimmer, eight counts), MSXFS.dll (Tyupkin, seven counts) and MSXFS.dll & imagehlp.dll (Skimmer, one count number). These statistics provide insights into the relative occurrence of different ATM malware families within the analyzed ATMs, allowing researchers and security specialists to develop suitable strategies and countermeasures to guard against those threats.

Discussion:

In-depth malware detection and prevention literature reveals the limits of present technologies and the need for new ones. The authors advise redirecting suspicious code to the honeypot's virtual machine. The host system can safely inspect the code. The investigation analyses ATM malware analysis, detection, and prevention, showing existing limitations and proposing new ones. Next, transmit suspicious code to a honeypot host virtual machine. The host system may safely analyze the analysis (Kumar and Pant, 2009)("(PDF) Malware Analysis & its Application to Digital Forensic," n.d.).Signature-based malware detection is not useful; hence, the authors advocate generating new addresses for security. The framework's base is a better static analysis of the malware code's PE header. The method discovers complex malware with low false positives and high detection rates. The authors' behavioural detection technique analyses malware code activity instead of structure. The behaviour detection approach uses a set of parameters to detect suspicious behaviour, such as attempts to access or alter sensitive data or system files (Louk et al., 2015). The research employs both analytical approaches to better fathom malware characteristics, discusses static, dynamic, and combined analysis techniques, and focuses on malware analysis time, precision, and profundity. A similar study uses sandboxes, debuggers, network sniffers, disassemblers, decompiles, and hex editors. Academics examine malware analysis trends using machine learning and AI for autonomous malware analysis and categorization. They argue that manual research and human capabilities are needed to thoroughly grasp and analyze the complicated operation of modern malware (YusirwanS et al., 2015). The article "New Malware Analysis Method on Digital Forensics" provides a registry analysis approach for discovering and analyzing malware on Windows systems. It emphasizes the limitations of current malware analysis

***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

techniques and proposes this unique strategy to overcome them. It recommends procedures for live Windows computers to scan the registry for malware and preserve volatile data on a live Windows machine during live forensics investigations. According to the authors, this technique is not a checklist and may need to be adapted for unique situations(and Lee, 2015). A study stresses malware analysis and detection for cyber security and reverses engineering, ATM malware analysis, and its benefits and downsides. Dynamic, static, and reverse engineering increase malware detection and analysis. It can locate intricate and obfuscated code that the malware analysis method cannot(Sunghyuck and Lee, n.d.) Megira et al., 2018). The paper "An Effective Malware Detection Method Using Hybrid Feature Selection and Machine Learning Algorithms" proposes a singular malware detection technique for Windows structures based on API calls, feature selection, and device getting to know algorithms. The authors first extract a fixed of API calls from malware samples. Then, they use a hybrid feature choice method to select the most applicable functions. Finally, they use machine gaining knowledge of algorithms to train a classifier to distinguish among malicious and benign samples. The outcomes of the studies show that the counseled approach may also as it should be identify malware (Dabas et al., 2022). This study tests a completely unique malware that combines injection assaults and obfuscation techniques in opposition to Android anti-malware systems. According to the authors, most anti-virus applications couldn't recognize the malware, even when deployed with other spells. This indicates that anti-malware systems need to be up to date to stumble on better this new kind of malware(Derhab et al., 2016a). The look at "Performance Evaluation of CNN and Pre-educated Models for Malware Classification" assesses how well convolutional neural networks (CNNs) and pre-skilled models carry out in classifying malware**.** On various malware datasets, the authors found that CNNs ought to outperform pre-skilled models in accuracy. This indicates that CNNs are a promising method for identifying malware(Habibi et al., 2023). Ahmad and associates advocate a unique approach for detecting malware on Android smartphones that makes use of a bio-stimulated set of rules and a system gaining knowledge of classifier. They reveal that the recommended technique can produce high detection rates with little fake fantastic interest. The counseled approach has yet to be made into a commercial product and is best examined on a dataset of Android packages. The examine notably contributes to malware detection normal (Derhab et al., 2016b). Vinod et al. Advise an empirical assessment of a machine name-based totally Android malware detector, which uses a dataset of malicious and benign Android packages to extract gadget calls and use a gadget learning classifier to become aware of malicious programs. This paper proposes a new approach for detecting metamorphic malware, that is a type of malware that can change its code to keep away from detection. The proposed approach uses a heterogeneous opcode area, combining one of a kind opcodes, which includes branch opcodes, unigrams, and bigrams. A device gaining knowledge of classifier changed into used to train a model to hit upon metamorphic malware, which performed an accuracy of ninety nine.Eight% with a fake tremendous price of zero.2%. The approach is likewise effective towards 0-day malware, which has but to be seen through anti-virus software program(Vinod and Viswalakshmi, 2018). Discovering and assessing dangerous codes in an ATM system is feasible.

Conclusion

ATM malware code written with PEStudio grows increasingly sophisticated and is difficult to stop from a digital forensic standpoint. PEStudio helped analyze malware code and identify vulnerabilities. The research underlines the need to secure ATM networks and prevent unauthorized access to personal financial data. Identify and eradicate threats, analyze software updates and system logs, and use powerful malware analysis products. ATM malware contains msxfs.dll, a malicious code in the executable file that causes hazardous operations. The study demonstrates the importance of digital forensic techniques in combating cybercrime and the necessity for ongoing research and innovative approaches and tools to manage the evolving threat landscape. Organizations may better defend their systems and data against malicious attacks by implementing PEStudio and taking the initiative to secure it.

4 Future advancement of malware analysis in forensic

Hackers constantly create new ATM malware versions, endangering the banking sector. ATM malware research may advance. ATM malware continually changes, making signature-based malware analysis worthless. ATM malware behavioural analysis looks for unusual behaviours that may indicate an assault. This approach finds new malware strains and exploits. Machine learning can detect suspicious activity by training algorithms to understand ATM network circulation trends and changes. These systems can detect and destroy new threats by learning from prior attacks. Modern malware detection methods help find and remove ATM malware. These advances can check ATM systems and update potentially harmful software quickly. ATM makers and other firms may anticipate assaults by sharing threat information. This knowledge allows the creation of new security measures to stop assaults before they cause system harm. IoT devices like cameras and sensors help improve ATM network security. Devices may monitor the ATM's surroundings for illegal activities or unauthorized entrances.

References

[1]. All you need to know about the spyware in ATMs that can steal your money from the bank - iPleaders [WWW Document], n.d. URL https:// blog. ipleaders.in/all-you-need-to-know-about-the-spyware-in-atm-machines-that-can-steal-your-money-from-the-bank/ (accessed 5.28.23).

[2]. ATM is a New Skimmer: Crooks Bring ATMs on Their Side | Kaspersky [WWW Document], n.d. URL

https://www.kaspersky.com/about/press-releases/ 2016_atm-is-a-new-skimmer-crooks-bring-atms-on-their-side (accessed 5.15.23).

[3]. ATM logic attacks: vulnerabilities and security risks of ATMs [WWW Document], n.d. URL https://www.ptsecurity.com/ww-en/analytics/atm-vulnerabilities-2018/ (accessed 6.20.23).

[4]. ATM Malware: The Next Generation of ATM Attacks [WWW Document], n.d. URL https:// security intelligence.com/atm-malware-the-next-generation-of-atm-attacks/ (accessed 5.28.23).

[5]. Bootkit | Malwarebytes Labs [WWW Document], n.d. URL https://www.malwarebytes.com/ blog/ detections/bootkit (accessed 5.28.23).

[6]. Dabas, N., Ahlawat, P., Sharma, P., 2022. An Effective Malware Detection Method Using Hybrid Feature Selection and Machine Learning Algorithms. Arab J Sci Eng 1–19.

[7]. Derhab, A., Saleem, K., Youssef, A., Guerroumi, M., 2016a. Preventive Policy Enforcement with Minimum User Intervention Against SMS Malware in Android Devices. Arab J Sci Eng 41, 479–493.

[8]. Derhab, A., Saleem, K., Youssef, A., Guerroumi, M., 2016b. Preventive Policy Enforcement with Minimum User Intervention Against SMS Malware in Android Devices. Arab J Sci Eng 41, 479–493.

[9]. FIN7 Hackers Load New RAT Malware Into ATM Maker's Software [WWW Document], n.d. URL https://www.bleepingcomputer.com/news/security/fin7-hackers-load-new-rat-malware-into-atm-makers-software/ (accessed 5.28.23).

[10]. Habibi, O., Chemmakha, M., Lazaar, M., 2023. Performance Evaluation of CNN and Pre-trained Models for Malware Classification. Arab J Sci Eng 1–15.

[11]. Hacking ATMs: The New Wave of Malware | Infosec Resources [WWW Document], n.d. URL https:// resources. infosecinstitute.com/ topic/ hacking-atms-new-wave-malware/ (accessed 6.20.23).

[12]. Jackpotting malware | Infosec Resources [WWW Document], n.d. URL https://resources. infosecinstitute. com/topic/ jackpotting-malware/ (accessed 5.15.23).

[13]. Kumar, S., Pant, D., 2009. Detection and Prevention of New and Unknown Malware using Honeypots, International Journal on Computer Science and Engineering.

[14]. Louk, M., Lim, H., Lee, H., Atiquzzaman, M., 2015. A practical framework of behaviour detection-advanced static analysis for malware detection. 14th International Communications and Information Technologies Symposium, ISCIT 2014 361–365.

[15]. Malware-based attacks on ATMs – A summary – NVISO Labs [WWW Document], n.d. URL https://blog.nviso.eu/2023/01/10/malware-based-attacks-on-atms-a-summary/ (accessed 6.20.23).

[16]. Megira, S., Pangesti, A.R., Wibowo, F.W., 2018. Malware Analysis and Detection Using Reverse Engineering Technique. J Phys Conf Ser 1140.

[17]. (PDF) Malware Analysis & its Application to Digital Forensic [WWW Document], n.d. URL https://www .researchgate.net/publication/268423577_Malware_ Analysis_its_Application_to_Digital_Forensic (accessed 6.6.23).

[18]. Pestudio: Initial Malware Assessment Made Simple - Security Investigation [WWW Document], n.d. URL https://www. socinvestigation.c om/pestudio-initial-malware-assessment-made-simple/ (accessed 6.20.23).

[19]. Sunghyuck, H., Lee, S., n.d. New Malware Analysis Method on Digital Forensics.

[20]. Sunghyuck.hong@gmail.com, S.H., Lee, S., 2015. New Malware Analysis Method on Digital Forensics. Indian J Sci Technol 8.

[21]. Vinod, P., Viswalakshmi, P., 2018. Empirical Evaluation of a System Call-Based Android Malware Detector. Arab J Sci Eng 43, 6751–6770.

[22]. What Is ATM Skimming and How to Spot a Skimmer | Avast [WWW Document], n.d. URL https://www. avast.com/c-atm-skimmer (accessed 6.20.23).

[23]. What is a Remote Access Trojan (RAT)? - Check Point Software [WWW Document], n.d. URL https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-remote-access-trojan/ (accessed 5.17.23).

[24]. YusirwanS, S., Prayudi, Y., Riadi, I., 2015. Implementation of Malware Analysis using Static and Dynamic Analysis Methods. Int J Comput Appl 117, 11–15.