Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 14, Issue. 1, January 2025, pg.1 – 10

Monitoring Invisible Remote Activity (MIRA) – A Persistent Stealthy Attack Script for Collecting Network Traffic, Keystrokes and Screenshots of Victim Windows Machines

Michael Gabriel A. Del Rosario

College of Computer Studies, De La Salle – Manila, Philippines
delrosariomichaelgabriel@gmail.com

DOI: https://doi.org/10.47760/ijcsmc.2025.v14i01.001

Abstract: ***Digitalization has interwoven the systems of various industries and rendered them interdependent, for the sake of the convenience of consumers in their products and services. Significantly however, this is accompanied by the increasing exploitations of their vulnerabilities, with financial and political motives. Microsoft Windows remains to be the most popular operating system, with a market share of 80.38% and 83% of malware targeting it, as of 2021. A Cyberattack is any unauthorized action that compromises the virtual assets and services of a system. It is pivotal for organization to understand these attacks to impede its increase and improve their responses and measures. The Windows Registry is a database that stores configuration and information regarding a Windows system. This is often abused by attackers by malicious configurations to conduct an attack. The MITRE ATT&CK framework is a knowledge base of tactics employed throughout a whole Cyberattack; it is particularly useful for organizations in understanding such. This manuscript evaluates and discusses an attack script that synthesizes various tactics of the MITRE ATT&CK framework regarding its effectivity across different metrics and applicability in understanding various tactics of a Cyberattack, which may contribute to the discussed improvements of an organization's responses, measures, and prevention.***

Keywords: Attack Script, Collection, MITRE ATT&CK Framework, Registry, Windows

© 2025, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden

I. INTRODUCTION

Thanks to digitalization, various industries' systems have been interwoven and rendered interdepended on each other to provide consumers with convenience in their products and services. Significantly however, this comes with the increasing exploitations of their vulnerabilities, stemming from political and financial motives [2].

Microsoft Windows remains to be the most popular operating system (OS). As of 2021, the OS has a remarkable market share of 80.38% among the desktop Oses, which can be seen in Fig. 1. Detrimentally, this makes it a common target for Cyberattacks, with 83% of malware targeting it [1].

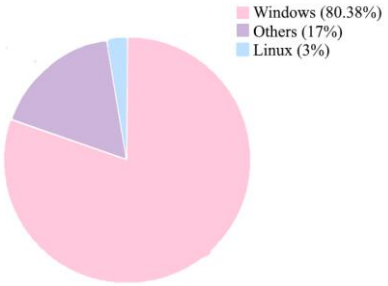

Fig. 1 Windows Market Share

A Cyberattack is defined as any unauthorized action that aims to violate the security of virtual assets or disrupting its correlated services, with the former notably being through data theft and accessing of potentially sensitive information. Typically, attackers follow certain characteristics to achieve their goal of exfiltrating an organization's data, which can be seen in Table I [3].

TABLE I
CHARACTERISTICS FOR CYBERATTACKS

Characteristic	Description
Harmonized	A system's process must be harmonized and predictable to synchronize the steps for data collection.
Organized	Logical organization of methods for efficient results expected by the attacker.
Enormous	Intends to collect large scales of data.
Regimented	Organize with perfect sequence, with enough impact to compromise an organization.
Not Spontaneous	Occurrence that are deliberate in nature, paired with careful planning.
Demanding Time and Resource	Advanced planning necessitating time and resources.

It is a pivotal strategy for organizations to learn from Cyberattacks to improve security measure, awareness, and graceful response. This can be conducted by understanding the causes and natures of these attacks, ultimately leading to the impediment of their increase [2].

II. OBJECTIVE

The objective of this manuscript is to evaluate a persistent stealthy attack script for Monitoring Invisible Remote Activity (MIRA), for its effectivity in exfiltrating information about activities within a victim machine, using the metrics defined in subsection C. or Verification in the Methodology section. Specifically, network packets, keystrokes, and screenshots of the current screen are collected. The script's alignment with the tactics of the MITRE ATT&CK framework and its fulfillment of certain Cyberattack characteristics shall also be discussed.

III. REVIEW OF RELATED LITERATURE

A. *Windows Registry*

The Windows Registry is a hierarchical database that stores system information and configurations for Windows systems. Some of this information includes that of the OS and the installed software, defining their functionality and nature with regards to the system.

© 2025, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden

The information within the Registry is stored in their respective hives, which are defined by the type and nature of the information. The major hives and their descriptions can be seen in Table II [5]. Parsing software exist to translate the information encompassed within these hives into a format readable by humans [6].

TABLE II
WINDOWS REGISTRY MAJOR HIVES

Hive	Description
HKEY_LOCAL_MACHINE	This contains all the configuration settings of a computer. It contains the sub-hives: HARDWARE: Stores information about hardware devices detected upon startup. SAM: Stores sensitive information about users and work groups. SECURITY: Stores local security database in SAM and management of user access to the database. SOFTWARE: Stores configurations of programs. SYSTEM: Stores configurations of hardware drivers and services.
HKEY_USERS	Contains information and configurations for individual users within the system.
HKEY_CLASSES_ROOT	Contains information on the registration class and file associations of the system and individual users.
HKEY_CURRENT_USER	Store information and configuration regarding the Environment, Identities, Network, Software, and Volatile Environment of a particular user. Programs may create, access, and modify such information.
HKEY_CURRENT_CONFIG	Image of the hardware configuration profiles.

Registry keys compose the hives, these contain the pertinent information and configurations regarding the hive it is situated in. Precisely, this information is stored as values in keys with corresponding name, data, and type of which [6].

The Registry is often exploited by attackers in order to maliciously configure a victim Windows system to conduct a Cyberattack [6]. Security sensitive keys are defined in a study as those that could lead to the compromise of a Windows system's security upon the change in the name and data. One of which are startup keys which include Run and RunOnce, these are often abused to automatically execute malicious code upon the startup of a Windows system [7].

B. MITRE ATT&CK Framework

The MITRE ATT&CK framework serves as a knowledge base for Cyber-adversary behaviors, which are observed in the continuously evolving Cyber-landscape. At the time of writing, it has at least 122 threat groups, reports for detection and analysis of intrusions. It contains tactics which compose a whole Cyberattack, with various techniques for each tactic, Table III shows these tactics [8].

TABLE III
MITRE ATT&CK TACTICS

Tactic	Description
Reconnaissance	Gathering of information for planning future operations.
Resource Development	Establishing resources to support operations.
Initial Access	Attempt to access the victim's network.
Execution	Attempt to execute the pertinent malicious code.
Persistence	Attempt to maintain foothold within the victim's system.
Privilege Escalation	Attempt to gain higher-level privileges or permission.
Défense Evasion	Attempt to avoid detection.
Credential Access	Attempt to steal account names and passwords.
Discovery	Attempt to contextualize the victim's environment.
Lateral Movement	Attempt to traverse the victim's environment.
Collection	Attempt to gather data of interest to a goal.
Command and Control	Attempt to communicate with compromised system to control them.
Exfiltration	Attempt to steal victim's data.
Impact	Attempt to interrupt, manipulate, or destroy victim's systems and data.

© 2025, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden

This framework is particularly useful for organizations in identifying and understanding the behaviors of a Cyberattack to detect and defend themselves from such. Threat detection controls and prevention measures may be developed through its use [8].

C. *Keyloggers, Screenloggers, and Packet Sniffing*

Collection of victim's data can take various forms and contexts or use cases. The banking industry heavily involves privileges and credentials for which in its various operations that may significantly impact financial assets. Collection of such credentials to gain access of these privileges are typically conducted through keyloggers and screenloggers. These are software that captures and saves keystrokes and screenshots into files and sends them to the attacker without the victim's knowledge, many of which attempt to conceal themselves [9].

Packet sniffing is the technique of monitoring the packets that come across a network, allowing for the collection of network traffic and data carried by such packets, which may include clear-text passwords, usernames, and other confidential information. Packet sniffers are software that enable this, they are generally impossible to detect as they are inherently passive [10].

Currently, there exists various software for keylogging, screenlogging, and packet sniffing, which are used for malicious monitoring and logging within the attacker's remote system [11][10]. However, there exists an opportunity to combine all of which into one attack script for employing the tactic of Collection and integrate Persistence and Defense Evasion tactics. This may serve for simulating these tactics and understanding their behavior, to help organizations in detecting and defending themselves from such, as discussed previously [8].

IV. METHODOLOGY

A. *Hardware Resources*

Two physical Windows machines will be utilized for this manuscript's experimentation. Table IV shows the victim machine's specifications, whereas Table V shows those of the attacking machine. The victim machine shall have its activity, and the pertinent information of which, collected and transmitted to the attacking machine upon the activation of the remote listener which it stores. The activity to be simulated within the victim machine is discussed in subsection B. or Procedures. It is notable that Windows Security and firewall of the victim machine are activated, with only inbound connections that do not match a rule being blocked.

TABLE IV
VICTIM MACHINE'S SPECIFICATIONS

Item	Value
OS Name	Microsoft Windows 11 Home Single Language
System Type	X64-based PC
Processor	Intel Core i5-9400, 2900 Mhz, 6 Core(s), 6 Logical Processor(s)
Total Physical Memory	10.1 GB
Total Virtual Memory	16.3 GB
Programs	Python, Registry Editor

TABLE V
ATTACKING MACHINE'S SPECIFICATIONS

Item	Value
OS Name	Microsoft Windows 11 Home Single Language
System Type	x64-based PC
Processor	AMD Ryzen 9 5900HX with Radeon Graphics, 3301 Mhz, 8 Core(s), 16 Logical Processor(s)
Total Physical Memory	15.4 GB
Total Virtual Memory	21.6 GB
Programs	Python

B. *Procedures*

The steps for conducting the experimentation of the script can be seen in Table VI. Steps 1 to 4 sets up the script for the actual experimentation, whereas observation and evaluation will be conducted upon step 5 where the script is to proceed with its primary functions.

© 2025, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden

TABLE VI
SCRIPT EVALUATION STEPS

Step	Description
Transfer Script to Victim Machine	Transfer using USB device.
Determine Time Intervals for Each Type of Collected Data	Utilize a random number generator ranging from 0 to 60.
Set Time Intervals	Utilize the randomly generated values.
Reboot The Victim Machine	Proceed with experimentation proper.
Observe the Change of the Script's Filename	The script shall imitate an existing filename in its directory.
Observe the Update of the Corresponding Value in the Run Key	The data field of the corresponding value in the Run key shall refer to the new filename of the script.
Activate Remote Listener in Attacking Machine	The attacking machine will now accept transmitted collected data.
Experiment Participant Attempts to Log into a Dummy Google Account	A non-researcher human participant will attempt to log into a dummy Google account.
Determine Login Activity and Credentials	Evaluate collected data to observe the activity of logging in at certain times of capture, and credentials of the dummy Google account.
Observe Restoration of Corresponding Value in the Run Key	The corresponding value in the Run key shall be deleted and restored automatically.

The technical mechanism of the script and its listener can be seen in Fig. 2. Generally, once the script has been implanted into the victim machine to execute upon startup, it will attempt to transmit the collected data once its corresponding interval has passed. For the attacking machine to receive the data, the remote listener shall foremost be executed within.

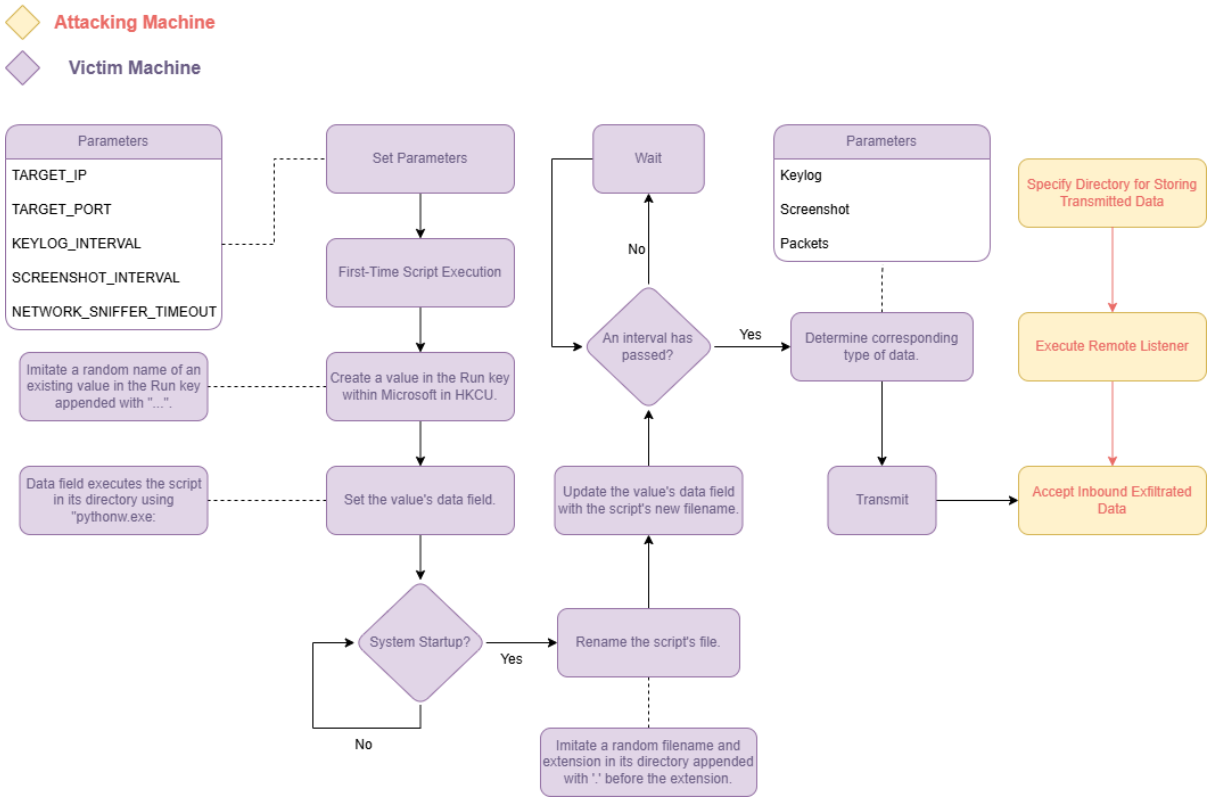

Fig. 2 MIRA's Flowchart

© 2025, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden

Fig. 3 MIRA's Logo

C. Verification

The script was evaluated according to the technical metrics defined in Table VII. Generally, these will be used to fulfill the defined objective of this manuscript regarding its effectivity in exfiltrating the network packets, keystrokes, and screenshots of the victim machine.

TABLE VII
METRICS FOR VERIFICATION IN THE SCRIPT'S EVALUATION

Metric	Goal
Stealth	The script's filename imitates another existing file in its directory. The script's corresponding Value imitates another existing Value in the Run key.
Persistence	A Value in the Run Key of HKCU: Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run has successfully been created with the Data field set to execute the script through Python upon startup. The corresponding Value of the script is restored upon deletion. The Data field of the corresponding Value of the script is updated according to the new filename of the script.
Keylogging Accuracy	All keystrokes of the victim machine are logged during the specified time interval.
Packet Sniffing	Packets from the network activity of the victim machine are collected during the specified time interval.
Screenshotting	Screenshots of the current screen of the victim machine are collected for every passing of the specified time interval.

Moreover, the script's capacity to simulate the tactics: Persistence, Defense Evasion, and Collection shall be discussed relative to its use for understanding the aspects of Cyberattacks against Windows systems, alongside its fulfillment of the various characteristics of a Cyberattack. The collection of the dummy Google account's credentials using the collected data will also be consolidated.

© 2025, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden

V. RESULTS AND DISCUSSION

A. *Network Traffic*

The network traffic of the victim machine was successfully collected with a time interval of 32, particularly the packets that were sniffed from which and transmitted to the specified directory in the attacking machine. A sample text file for the collected packets from the experimentation can be seen in Fig. 4.

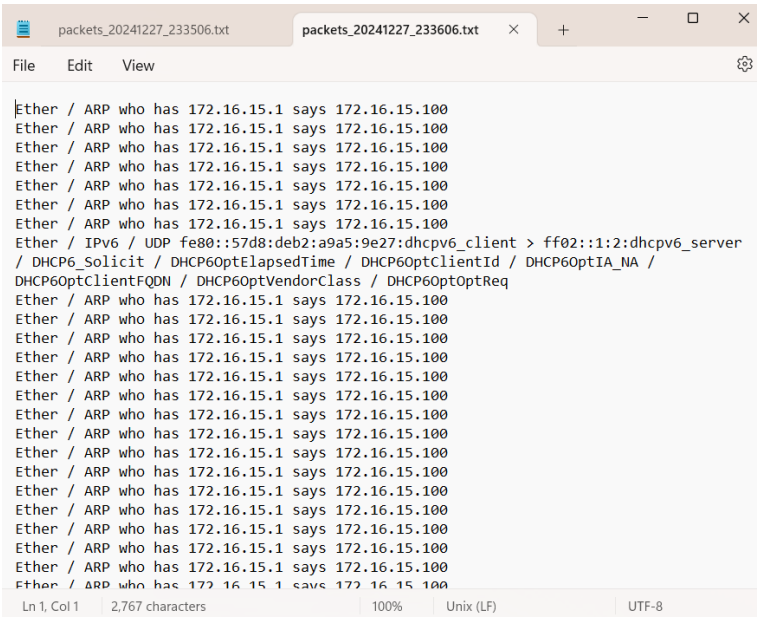

Fig. 4 Sample of Collected Packets from the Victim Machine

B. *Keystrokes*

The keystrokes of the victim machine were successfully collected with a time interval of 57 and transmitted to the attacking machine. Notably, the credentials “okingarud” of the dummy Google account “facundosalaysay@gmail.com” were extracted from logging into within the victim machine during the experimentation, being derived from the keystrokes seen in Fig. 5.

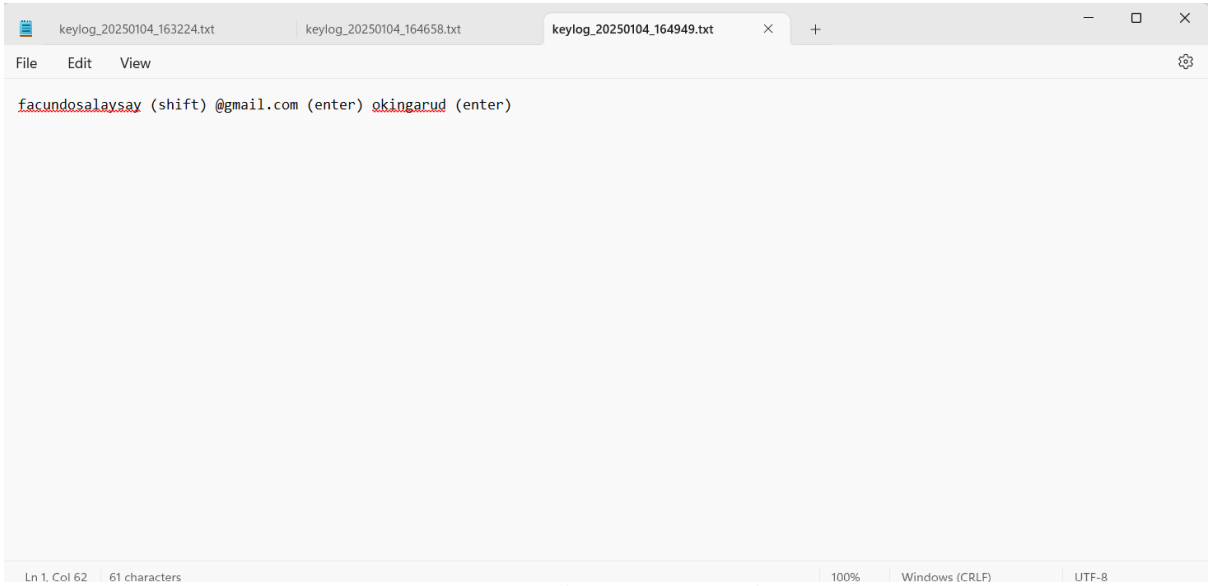

Fig. 5 Keystrokes with Credentials of the Google Account from the Victim Machine

© 2025, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden

C. *Screenshots*

Screenshots from the victim machine were successfully collected with a time interval of 15 and transmitted to the attacking machine, these indicate the activities within the victim machine at certain times in which the screenshots are taken. A sample screenshot that indicates the activity of logging into the dummy Google account during the experimentation can be seen in Fig. 6.

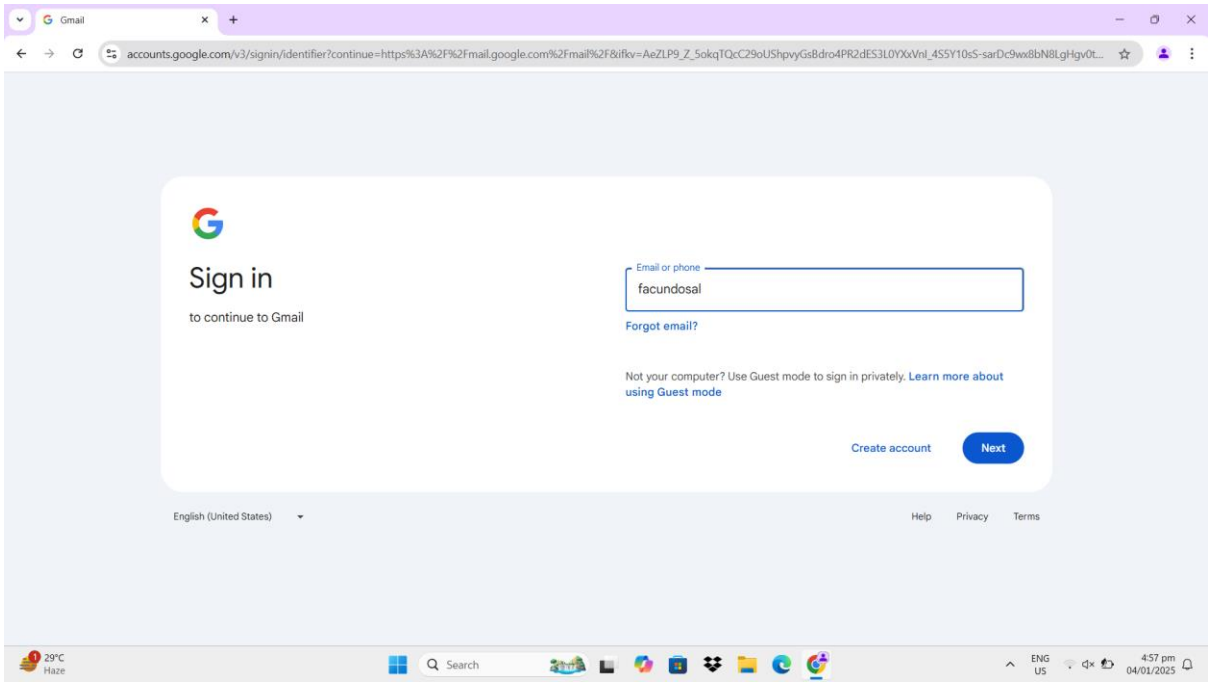

Fig. 6 Sample Screenshot of Google Login Activity from the Victim Machine

D. *Evaluation of the Attack Script*

The script is measured relative to the defined metrics in subsection C. or Verification in the Methodology section, the fulfillment of each metric can be seen in Table VIII. All metrics were fulfilled given the results of the script's experimentation.

TABLE VIII
SCRIPT'S EVALUATION ACCORDING TO METRICS

Metric	Fulfilled?	Details
Stealth	Yes	A name of an existing value in the Run key was successfully imitated. Filename and extension of an existing file in the script's directory was successfully imitated.
Persistence	Yes	The script and its data collection activity persist after the reboot of the victim machine. The corresponding value in the Run key was restored upon deletion.
Keylogging Accuracy	Yes	All keystrokes of the victim machine were logged respective to the corresponding time interval. Credentials "okingarud" of the dummy Google account "facundosalaysay@gmail.com" were extracted using the combined collected keystrokes.
Packet Sniffing	Yes	Packets from the victim machine were collected.
Screenshotting	Yes	Screenshots of the victim machine were collected. The activity of logging into the dummy Google account was observed from the screenshots.

Given that it is possible for a computer to be connected to two networks concurrently, the attack script's packet sniffing from the victim machine and exfiltrating its pertinent information provides the capacity to gather packets of all networks that the victim machine is connected to. This is opposed to merely capturing packets from the same or common network that the attacker and victim machines are connected to, providing a richer overview of the network traffic from the perspective of the victim machine.

© 2025, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden

The evaluation of the script's alignment to the characteristics for a Cyberattack, defined in the related literature, can be seen in Table IX. This is relative to the script's functionality with regards to the fulfillment of the employed details of each characteristic.

TABLE IX
SCRIPT'S EVALUATION ACCORDING TO CHARACTERISTICS

Characteristic	Fulfilled?	Details
Harmonized	Yes	Fulfilled by the initialization of the script by system's startup, and by timed data collection (i.e. activating the remote listener, setting the time intervals) according to the appropriate schedule.
Organized	Yes	Time intervals for data collection is set and fixed, with the activation of the remote listener left to the attacker's discretion.
Enormous	Variable	Dependent on the attacker's planned scale (i.e. minimal time intervals set for high frequency of data collection, exfiltrating data from multiple victim systems).
Regimented	Variable	Fulfilled by the sequence executed by the attacker as the whole of a Cyberattack is conducted, the script serves as a utility for probing the activities within a victim system, which can be utilized in a perfectly sequenced attack.
Not Spontaneous	Yes	Utilization of the script is dependent on the activation of the remote listener, whenever desired and appropriate.
Demanding Time and Resource	Yes	The implantation of the script and activation of the remote listener must be appropriately timed and planned, where it is dependent on the quality of a whole attack.

E. The Script for Attack Simulation

The evaluation of the script's alignment to certain MITRE ATT&CK tactics can be seen in Table X. Multiple techniques among the tactics: Persistence, Defense Evasion, and Collection were found to be employed by or similar to the script's capabilities.

TABLE X
SCRIPT'S EVALUATION ACCORDING TO MITRE ATT&CK TACTICS

Tactic	Alignment
Persistence	Technique T1547.001 "Registry Run Keys / Startup Folder" is employed by the script by creating a value in the HKCU's Run key within Microsoft, enabling it to execute upon startup.
Defense Evasion	Technique T1036.006 "Space after Filename" is similar to the script's imitation of an existing file's filename and extension within its directory upon every startup, using '.' Instead of a space or ' '. Technique T1036.008 "Masquerade File Type" is similar to the script's nature which imitates different files and types of which, while retaining the malicious executable code as its content.
Collection	Technique T1056.001 "Keylogging" is employed by the script simply through its keylogging capacity. Technique T1113 "Screen Capture" is employed by the script simply through its screenshotting capacity. Technique T1557 "Adversary-in-the-Middle" is similar to the script's positioning within the victim machine for network sniffing, using the sniffed network traffic from the victim machine.

VI. CONCLUSIONS

The understanding of the nature and causes of various Cyberattacks is indeed pivotal for the future prevention of and graceful recovery from which, as employed by the reviewed literatures. The MITRE ATT&CK framework helps in such a process by simulating various tactics of Cyberattacks through different individual techniques. The attack script MIRA was evaluated to fulfill certain characteristics of a Cyberattack as defined by a related literature [3] and verified to be effective. It was also observed to employ or be similar to various techniques among the MITRE ATT&CK tactics: Persistence, Defense Evasion, and Collection, serving as a synthesis of such tactics. With this, the script can be utilized to simulate aspects of a Cyberattack, particularly the three tactics and its techniques that either perfectly align or are similar to its capabilities. This would then contribute to the discussed understanding of Cyberattacks for an organization's preparedness and prevention.

© 2025, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden

ACKNOWLEDGEMENT

The author would like to acknowledge Jerome E. Gutierrez for continuously providing meaningful insights into the writing process and the fundamentals of Cybersecurity.

REFERENCES

[1] Luo L., Zou C., Narain S., and Fu X. (2022). On Teaching Malware Analysis on Latest Windows

[2] Patterson C. M., Nurse J. R. C.. and Franqueira V. N. L. (2023). Learning from cyber security incidents: A systematic review and future research agenda. Computers & Security, vol. 32, p. 103309

[3] Uma M. and Padmavathi G. (2011). A Survey on Various Cyber Attacks and Their Classification. International Journal of Network Security. vol. 15, p. 390-396

[4] Rosli N., Yassin W., MA F., and Rahayu S. (2019). Clustering Analysis for Malware Behavior Detection using Registry Data. International Journal of Advanced Computer Science and Applications. vol. 10

[5] Saidi R.M., Ahmad S., Noor N., and Yunos R. (2013). Windows registry analysis for forensic investigation. Windows Registry Analysis for Forensic Investigation

[6] Del Rosario M.G. (2024). PARSNIP: Parsing Registry Hives from Snip-Snapped Shadow Copies with Timelining and Timsort. International Journal of Computer Science and Mobile Computing. vol 13, p. 76-85

[7] Singh J. and Singh J. (2021). A survey on machine learning-based malware detection in executable files. Journal of Systems Architecture. vol. 112

[8] Rajesh P., Alam M., Tahernezhadi M., Monika A., and Chanakya G. (2022). Analysis Of Cyber Threat Detection And Emulation Using MITRE Attack Framework. International Conference on Intelligent Data Science Technologies and Applications

[9] Sbai H., Goldsmith M., Meftali S., and Happa J. (2018). A Survey of Keylogger and Screenlogger Attacks in the Banking Sector and Countermeasures to Them

[10] Belbase S. (2020). Detection of Intrusion Using Packet Sniffer. International Journal of Innovative Research in Technology. vol. 7

[11] Adhikary N., Shrivastava R., Kumar A., Verma S.K., Bag M., and Singh V. (2012). Battering Keyloggers and Screen Recording Software by Fabricating Passwords. International Journal of Computer Network and Information Security. vol. 5, p. 13-21

© 2025, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden