SUBEX

Matiex Keylogger Threat Report

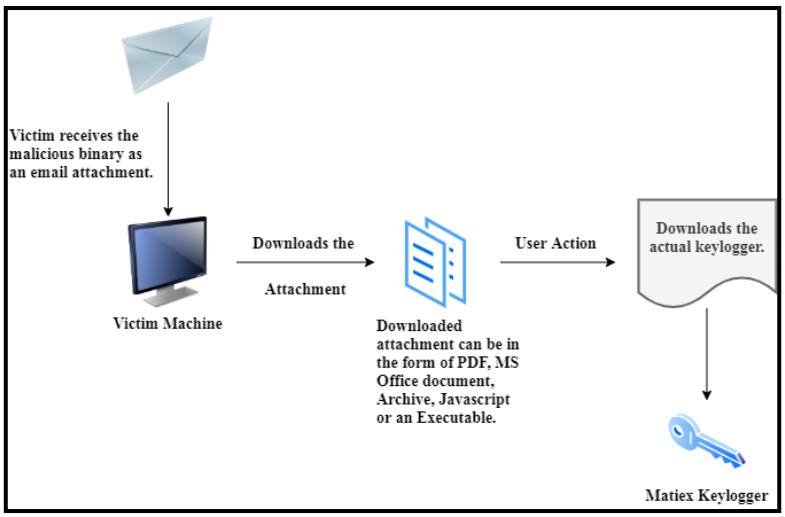
Date: **08/01/2021**

Krupa Gajjar,
Sampada Kanitkar

Keylogger or keylogging is a technique of capturing and recording the user input from the keyboard. Keylogging is mostly carried covertly without the person knowing about it that the keystrokes are being recorded. Nowadays such programs are mostly used for stealing confidential information such as credit card information, passwords, etc.

Overview

The sample intercepted here is a keylogger known as Matiex Keylogger. The functionality of this keylogger encompasses taking screenshots, sound recording via computer microphone, capturing clipboard data, and stealing other sensitive information stored on the victim machine. The attacker can access the recorded input via SMTP, FTP, Telegram and Discord. This keylogger is even capable of generating fake messages that includes self-destruction feature which allows it to uninstall itself from the victim machine any time.



Infection Flow

Technical Analysis

Matiex is propagated via email chain attachments, online advertisements i.e., via social engineering techniques or via software cracks. When distributed via email attachments the files can be in any format such as:

- PDF
- Microsoft Office documents
- JavaScript
- Archives
- Any form of executable, etc.

Hence, luring the victim into downloading and executing these attachments. By loading the executable in any disassembler anyone can identify the name of the keylogger (Fig 1).

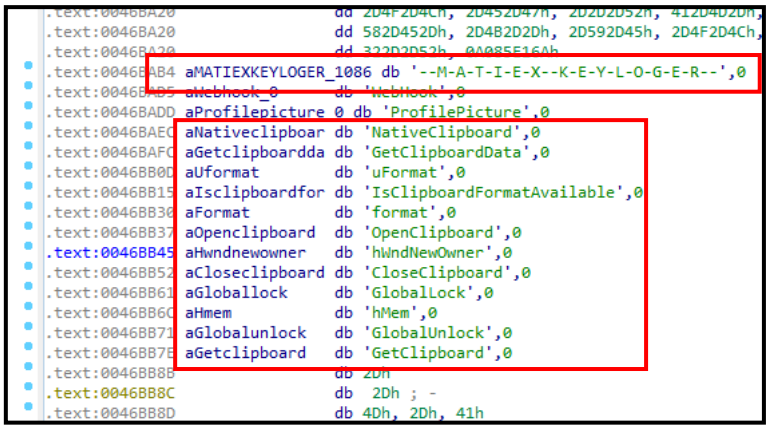


Fig 1

Matiex binary retrieves all the data from the clipboard in a specified format. Further, it opens the clipboard for examination, thereby preventing other applications from modifying the clipboard data until the keylogger finishes reading and recording all the information.

Further analyzing the executable shows that the keylogger tries to identify any SQLite database and read all the stored information from it (Fig 2).

Fig 2

The binary records various key up and down movements and tries to manipulate those events. Disassembled code of the keylogger shows that it also installs application-defined hooking procedure to monitor the victim machine system for certain types of event. Here it tries to monitor its own keylogging functionality.

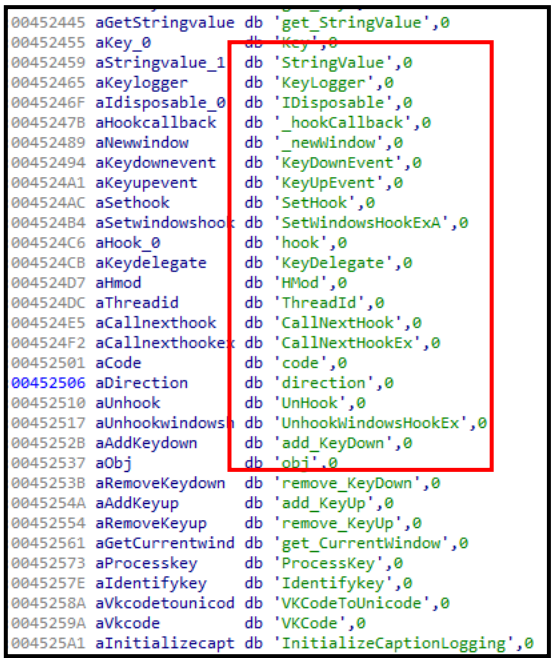


Fig 3

Matiex keylogger steals system information such as:

- OS Name
- Platform
- Version
- Total Physical Memory
- Network Credentials
- Registry information
- Audio
- Different folder paths

It also collects various mailing address, subject, various attachments, File system information etc.

Fig 4

Matiex sends all the recorded and captured sensitive information via Discord which is a free VoIP application. First, the keylogger steals the username and password of the application and using the hooking technique, the binary sends the message and uploads the data.

Fig 5

This keylogger checks for how many times passwords and usernames have been changed, how many times a password has been used and the last username and password that is used, it also checks for various email clients the victim uses on the machine. Also, the binary tries to capture the screenshot of the victim machine, record IP address and voice via the device's microphone.

Fig 6

File Hash: 5f3cd5647257d60a7b6607bc02af4c8f

IOCs:

1af8e9543d441af0c1812b1c68e81e3b

MITRE Techniques:

T1010 – Application Window Discovery	T1057 - Process Discovery
T1033 - System Owner/User Discovery	T1082 - System Information Discovery
T1071 - Application Layer Protocol	T1083 – File and Directory Discovery
T1115 – Clipboard Data	T1087 – Account Discovery
T1056.001 - Keylogging	T1124 – System Time Discovery
T1056.004 – Credential API Hooking	

Subex Secure Protection
Subex Secure detects the malware as '`SS_Gen_Matiex_PE_A`'.

OUR HONEYPOT NETWORK

This report has been prepared from the threat intelligence gathered by our honeypot network. This honeypot network is today operational in 62 cities across the world. These cities have at least one of the following attributes:

- Are landing centers for submarine cables
- Are internet traffic hotspots
- House multiple IoT projects with a high number of connected endpoints
- House multiple connected critical infrastructure projects
- Have academic and research centers focusing on IoT
- Have the potential to host multiple IoT projects across domains in the future

Over 3.5 million attacks a day are being registered across this network of individual Honeypots. These attacks are studied, analyzed, categorized, and marked according to a threat rank index, a priority assessment framework that we have developed within Subex. The honeypot network includes over 4000 physical and virtual devices covering over 400 device architectures and varied connectivity mediums globally. These devices are grouped based on the sectors they belong to for purposes of understanding sectoral attacks. Thus, a layered flow of threat intelligence is made possible.