



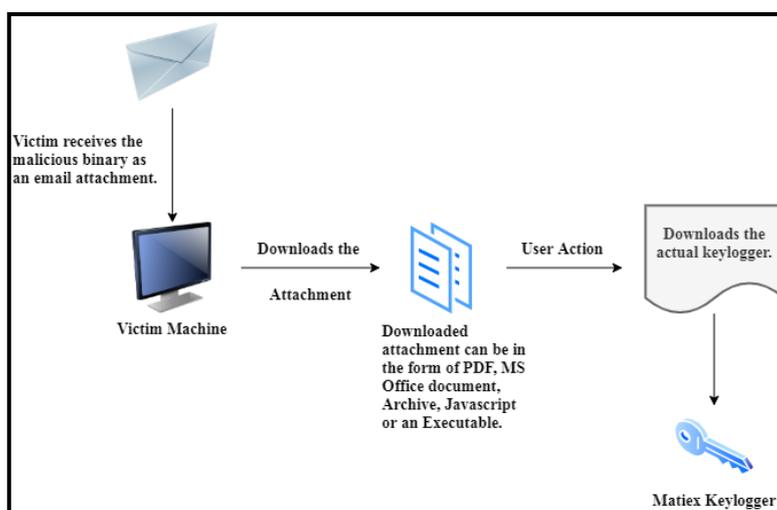
Matiex Keylogger Threat Report

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).

```

.text:0046BA20 dd 204F2D4Ch, 20452D47h, 202D2D52h, 412D4D2Dh,
.text:0046BA20 dd 582D452Dh, 204B2D2Dh, 2D592D45h, 2D4F2D4Ch,
.text:0046BA20 dd 322D2D52h, 0A085E16Ah
.text:0046B8B4 aMATIEXKEYLOGGER_1086 db '--M-A-T-I-E-X--K-E-Y-L-O-G-E-R--',0
.text:0046B8B5 aWebhook_0 db 'Webhook',0
.text:0046BADD aProfilepicture_0 db 'ProfilePicture',0
.text:0046BAEC aNativeclipboa db 'NativeClipboard',0
.text:0046BAFC aGetclipboardda db 'GetClipboardData',0
.text:0046BB00 aUFormat db 'uFormat',0
.text:0046BB15 aIsclipboardfor db 'IsClipboardFormatAvailable',0
.text:0046BB30 aFormat db 'format',0
.text:0046BB37 aOpenclipboard db 'OpenClipboard',0
.text:0046BB45 aHwndnewowner db 'hwndNewOwner',0
.text:0046BB52 aCloseclipboard db 'CloseClipboard',0
.text:0046BB61 aGloballock db 'GlobalLock',0
.text:0046BB6C aHmem db 'hMem',0
.text:0046BB71 aGlobalunlock db 'GlobalUnlock',0
.text:0046BB7E aGetclipboard db 'GetClipboard',0
.text:0046BB88 db 2Dh
.text:0046BB8C db 2Dh ; -
.text:0046BB8D db 4Dh, 2Dh, 41h

```

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).

```

0046536C aSqlitehandler db 'SQLiteHandler',0
0046537A aDbBytes db 'db_bytes',0
00465383 aPageSize db 'page_size',0
0046538D aEncoding_0 db 'encoding',0
00465396 aMasterTableEnt db 'master_table_entries',0
004653AB aSqldatatype siz db 'SQLDataTypesize',0
004653BB aTableEntries db 'table_entries',0
004653C9 aFieldNames db 'field_names',0
004653D5 aGvl db 'GVL',0
004653D9 aStartindex db 'startIndex',0
004653E4 aCvl db 'CVL',0
004653E8 aEndindex db 'endIndex',0
004653F1 aIsodd db 'IsOdd',0
004653F7 aConverttointeg db 'ConvertToInteger',0
00465408 aSize db 'Size',0
0046540D aReadmastertabl db 'ReadMasterTable',0
0046541D aOffset db 'Offset',0
00465424 aReadtablefromo db 'ReadTableFromOffset',0
00465438 aReadtable db 'ReadTable',0
00465442 aTableName db 'TableName',0
0046544C aGetrowcount db 'GetRowCount',0
00465458 aGetvalue db 'GetValue',0
00465461 aRowNum db 'row_num',0
00465469 aField db 'field',0
0046546F aGettablenames db 'GetTableNames',0

```

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.

00452445	aGetStringvalue	db	'get_StringValue',0
00452455	aKey_0	db	'key',0
00452459	aStringValue_1	db	'StringValue',0
00452465	aKeylogger	db	'KeyLogger',0
0045246F	aIDisposable_0	db	'IDisposable',0
0045247B	aHookcallback	db	'_hookCallback',0
00452489	aNewwindow	db	'_newwindow',0
00452494	aKeyDownevent	db	'KeyDownEvent',0
004524A1	aKeyupevent	db	'KeyUpEvent',0
004524AC	aSethook	db	'SetHook',0
004524B4	aSetwindowshook	db	'SetWindowsHookExA',0
004524C6	aHook_0	db	'hook',0
004524CB	aKeydelegate	db	'KeyDelegate',0
004524D7	aHmod	db	'HMod',0
004524DC	aThreadId	db	'ThreadId',0
004524E5	aCallnexthook	db	'CallNextHook',0
004524F2	aCallnexthooke	db	'CallNextHookEx',0
00452501	aCode	db	'code',0
00452506	aDirection	db	'direction',0
00452510	aUnhook	db	'UnHook',0
00452517	aUnhookwindowsh	db	'UnhookWindowsHookEx',0
0045252B	aAddKeydown	db	'add_KeyDown',0
00452537	aObj	db	'obj',0
0045253B	aRemoveKeydown	db	'remove_KeyDown',0
0045254A	aAddKeyup	db	'add_KeyUp',0
00452554	aRemoveKeyup	db	'remove_KeyUp',0
00452561	aGetCurrentwind	db	'get_CurrentWindow',0
00452573	aProcesskey	db	'ProcessKey',0
0045257E	aIdentifykey	db	'IdentifyKey',0
0045258A	aVkcodetounicod	db	'VKCodeToUnicode',0
0045259A	aVkcode	db	'VKCode',0
004525A1	aInitializecapt	db	'InitializeCaptionLogging',0

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.

:0046041	aGetOsfullname	db	'get_OSFullName',0
:0046042	aGetOsplatform	db	'get_OSPlatform',0
:0046043	aGetOsversion	db	'get_OSVersion',0
:0046044	aGetTotalphysic	db	'get_TotalPhysicalMemory',0
:0046046	aGetsystemwebpr	db	'GetSystemWebProxy',0
:0046047	aCredentialcach	db	'CredentialCache',0
:0046048	aGetDefaultnetw	db	'get_DefaultNetworkCredentials',0
:004604A	aNetworkcredent	db	'NetworkCredential',0
:004604B	aSetCredentials	db	'set_Credentials',0
:004604C	aICredentials	db	'ICredentials',0
:004604D	aSetProxy	db	'set_Proxy',0
:004604E	aReplace	db	'Replace',0
:004604F	aLatecall	db	'LateCall',0
:0046050	aGetelementsbyt	db	'GetElementsByTagName',0
:0046051	aXmlNodeList	db	'XmlNodeList',0
:0046052	aGetInnertext	db	'get_InnerText',0
:0046053	aGetAscii_0	db	'get_ASCII',0
:0046054	aGetClipboard	db	'Clipboard',0
:0046055	aClipboardproxy	db	'ClipboardProxy',0
:0046056	aGettext	db	'GetText',0
:0046057	aContains	db	'Contains',0
:0046058	aGetName	db	'set_Name',0
:0046059	aSetMethod	db	'set_Method',0
:0046060	aSetContentleng	db	'set_ContentLength',0
:0046061	aGetrequeststre	db	'GetRequestStream',0
:0046062	aWrite	db	'Write',0
:0046063	aMailaddress	db	'MailAddress',0
:0046064	aSetFrom	db	'set_From',0
:0046065	aGetTo	db	'get_To',0
:0046066	aMailaddresscol	db	'MailAddressCollection',0
:0046067	aSetSubject	db	'set_Subject',0
:0046068	aSetBody	db	'set_Body',0
:0046069	aGetAttachments	db	'get_Attachments',0
:0046070	aAttachmentcoll	db	'AttachmentCollection',0
:0046071	aSetEnablessl	db	'set_EnableSsl',0
:0046072	aSetPort	db	'set_Port',0
:0046073	aICredentialsby	db	'ICredentialsByHost',0
:0046074	aSend	db	'Send',0
:0046075	aReadallbytes	db	'ReadAllBytes',0
:0046076	aDelete	db	'Delete',0
:0046077	aGetAudio	db	'get_Audio',0
:0046078	aAudio	db	'Audio',0
:0046079	aStop	db	'Stop',0
:0046080	aGetfiles_0	db	'GetFiles',0
:0046081	aEndswith	db	'EndsWith',0
:0046082	aFilesysteminfo	db	'FileSystemInfo',0
:0046083	aGetFullname	db	'get_FullName',0
:0046084	aSubstring	db	'Substring',0
:0046085	aSplit	db	'Split',0
:0046086	aJoin	db	'Join',0
:0046087	aGet	db	'Get',0
:0046088	aConditionalcom	db	'ConditionalCompareObjectEqual',0
:0046089	aStartswith	db	'StartsWith',0
:0046090	aConvert_0	db	'Convert',0
:0046091	aSetInterval	db	'set_Interval',0
:0046092	aSetattributes	db	'SetAttributes',0
:0046093	aGetRegistry	db	'get_Registry',0
:0046094	aRegistryproxy	db	'RegistryProxy',0
:0046095	aGetenvironment_0	db	'GetEnvironmentVariable',0
:0046096	aCopy_0	db	'Copy',0
:0046097	aGetFolderPath_0	db	'GetFolderPath',0

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.

```

:0046CEB1 aFileStream db 'FileStream',0
:0046CEBC aBoolean db 'Boolean',0
:0046CEC4 aByte_0 db 'Byte',0
:0046CEC9 aToLower db 'ToLower',0
:0046CED1 aGetNow db 'get_Now',0
:0046CED9 aGetMillisecond db 'get_Millisecond',0
:0046CEE9 aStream db 'Stream',0
:0046CF00 aGetTicks db 'get_Ticks',0
:0046CEFA aInt64 db 'Int64',0
:0046CF00 aGetHeaders db 'get_Headers',0
:0046CF0C aWebheadercolle db 'WebHeaderCollection',0
:0046CF20 aAdd_0 db 'Add',0
:0046CF24 aFormat_0 db 'Format',0
:0046CF2B aGetEncoding db 'get_Encoding',0
:0046CF3B aEncoding_1 db 'Encoding',0
:0046CF41 aGetbytes db 'GetBytes',0
:0046CF44 aUploaddata db 'UploadData',0
:0046CF55 aFile_0 db 'File',0
:0046CF5A aReadalltext db 'ReadAllText',0
:0046CF66 aGetString_0 db 'GetString',0
:0046CF70 aHttpwebrequest db 'HttpWebRequest',0
:0046CF71 aWebresponse db 'WebResponse',0
:0046CF8B aStreamreader_0 db 'StreamReader',0
:0046CF9B aWebexception db 'WebException',0
:0046CFAS aWebrequest db 'WebRequest',0
:0046CFB0 aMds db 'MDS',0
:0046CFB4 aAppend db 'Append',0
:0046CFBB aNewlatebinding db 'NewLateBinding',0
:0046B1C3 aCredentialmode_0 db 'CredentialModel',0
:0046B1D3 aUrl_3 db '_Url',0
:0046B1D8 aUsername_1 db '_Username',0
:0046B1E2 aPassword_2 db '_Password',0
:0046B1EC aGetUrl_3 db 'get_Url',0
:0046B1F4 aSetUrl_3 db 'set_Url',0
:0046B1FC aGetUsername_1 db 'get_Username',0
:0046B209 aSetUsername_1 db 'set_Username',0
:0046B216 aUrl_4 db 'Url',0
:0046B21A aUsername_2 db 'Username',0
:0046B223 aDcwebhook db 'DcWebHook',0
:0046B22D aWebhook db 'WebHook',0
:0046B236 aUsername_3 db '_UserName',0
:0046B240 aProfilepicture db 'ProfilePicture',0
:0046B250 aDwebclient db 'dwebClient',0
:0046B258 aWebclient db 'WebClient',0
:0046B265 aDiscordvalues db 'discordValues',0
:0046B273 aNamevaluecolle db 'NameValueCollection',0
:0046B287 aSystemcollecti_2 db 'System.Collections.Specialized',0
:0046B2A6 aGetWebhook db 'get_WebHook',0
:0046B2B2 aSetWebhook db 'set_WebHook',0
:0046B2BE aGetProfilepict db 'get_ProfilePicture',0
:0046B2D1 aSetProfilepict db 'set_ProfilePicture',0
:0046B2E4 aSendMessage db 'SendMessage',0
:0046B2F0 aMsgsend db 'msgSend',0

```

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.

```

:00426278 aGetTimepasswor db 'get_timePasswordChanged',0
:00426290 aSetTimepasswor db 'set_timePasswordChanged',0
:004262A8 aGetTimesused db 'get_timesUsed',0
:004262B6 aSetTimesused db 'set_timesUsed',0
:004262C4 aGetTimeLastuse db 'get_timeLastUsed',0
:004262D5 aSetTimeLastuse db 'set_timeLastUsed',0
:004262E6 aGetIsdisposed db 'get_IsDisposed',0
:004262F5 aGetTimecreated db 'get_timeCreated',0
:00426305 aSetTimecreated db 'set_timeCreated',0
:00426315 aMFormbeingcrea db 'm_FormBeingCreated',0
:00426328 aSynchronized db 'Synchronized',0
:00426335 aGetId db 'get_id',0
:0042633C aSetId db 'set_id',0
:00426343 aGetGuid db 'get_guid',0
:0042634C aSetGuid db 'set_guid',0
:00426355 aGetPasswordfie db 'get_passwordField',0
:00426367 aSetPasswordfie db 'set_passwordField',0
:00426379 aGetUsernamefie db 'get_usernameField',0
:0042638B aSetUsernamefie db 'set_usernameField',0
:0042639D aReadtoend db 'ReadToEnd',0
:004263A7 aTargetmethod db 'TargetMethod',0
:004263B4 aMethod db 'method',0
:004263B8 aOriginalThunder db 'Original_Thunderbird',0
:004263CF aGetPassword db 'get_Password',0
:004263DC aSetPassword db 'set_Password',0
:004263E9 aGetEncrypteddpa db 'get_encryptedPassword',0
:004263FF aSetEncrypteddpa db 'set_encryptedPassword',0
:0046E6B0 aScreenshotlogge db 'screenshotLoggerTimer',0
:0046E6C1 align 2
:0046E6C4 dw 110h
:0046E6C7 db 0
:0046E6CC db 16h, 43h, 6Ch
:0046E6D0 aIpbboardreplace db 'ipboardReplacerTimer',0
:0046E6E1 align 2
:0046E6E4 dw 110h
:0046E6E7 db 0
:0046E6EC db 16h, 43h, 6Ch
:0046E6F0 aIpbboardloggert db 'ipboardLoggerTimer',0
:0046E6F3 align 10h
:0046E6F6 db 10h
:0046E6F9 db 1, 0, 00h
:0046E704 aKillertimer_1 db 'KillerTimer',0
:0046E707 db 0
:0046E710 db 16h, 1, 0
:0046E713 db 11h
:0046E716 aVoicerecordlog_1 db 'voiceRecordLogger',0
:0046E721 align 4
:0046E724 dd 0000113h, 50656854h, 53445753h, 65646E65h, 7372h, 13000110h
:0046E727 dd 14700h
:0046E740 aProcesshacker_1 db 'processhackerFucked',0
:0046E754 db 0
:0046E755 db 1Ah, 1, 0
:0046E758 db 15h
:0046E759 aRemotedestruct_2 db 'RemoteDestructChecker',0
:0046E76F align 10h
:0046E770 dd 1700011Ch
:0046E774 aDatetimedestru_1 db 'DateTimeDestructChecker',0
:0046E78C dd 14700h
:0046E790 aBPleaseRefacto db 'BPlease refactor calling code to use normal Visual Basic as
:0046E793 db 'nt',0
:0046E796 dd 1200680h, 00B1101h, 2000108h, 0

```

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.