Dridex Malware Analysis Report

By: Mustafa Hussien

Sep 2020

E-mail: Mustafa12hussien@gmail.com

## TABLE OF CONTENTS

- Dridex malware is a sophisticated strain of banking malware that targets the Windows platform, delivering spam campaigns to infect computers and steal banking credentials and other personal information to facilitate fraudulent money transfer Functionality.
- The main goal of Dridex malware to collect and gather important of the user and send it to the attacker.

MITRE ATT&CK: TOOLS AND ATTACK TECHNIQUES' CLASSIFICATION

- The MITRE ATT&CK™ framework is a comprehensive matrix of tactics and techniques to better classify attacks and assess an organization's risk.
- As you can see, here are possible tactics and techniques that used by Dridex malware.
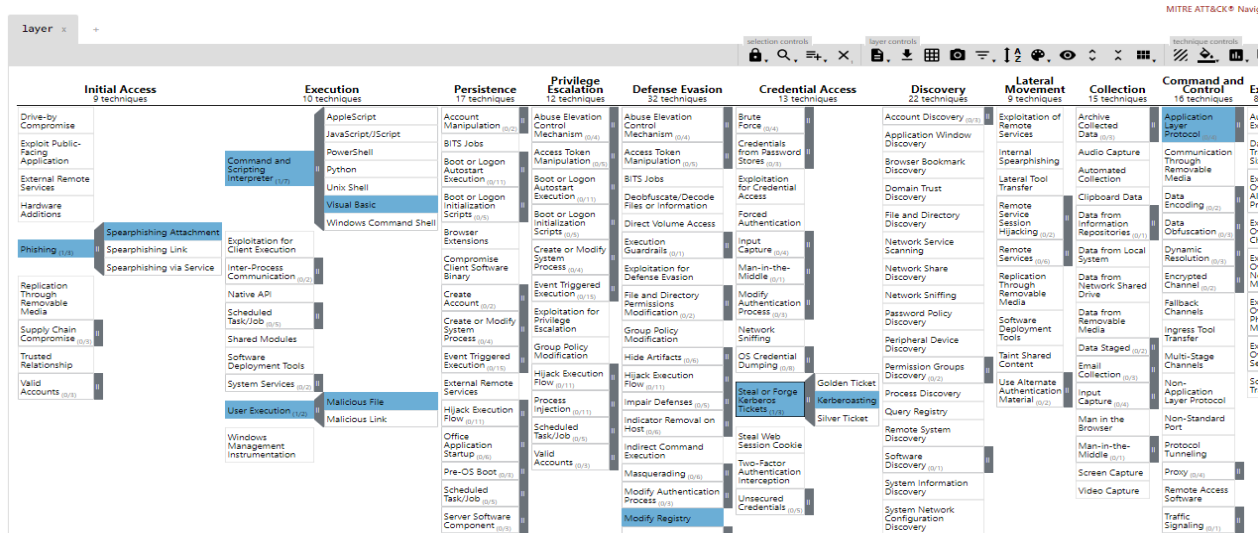
Technique ID	Tactic Name	Technique Name	Description
T1566	Initial Access	Spear-phishing Attachment	Sending a spear-phishing email with a malicious document
T1204	Execution	User Execution-Malicious File	Malicious document executes macro code (VBScript)
T1137	Persistence	Office Template Macro	The VBScript executes downloading Dridex Payload without need to click any button in the excel file.
T1112	Defense Evasion	Modify Registry	Modifying some important registries and trying to create files.
T1558 T1539	Credential Access	- Steal or Forge Kerberos Tickets (Kerberoasting). - Steal Web Session Cookies	It's trying to check web cookies and steal it also checking the Kerberos details between the user and the server.
T1087	Discovery	Account Discovery	Trying to steal user account's information and send it to the C&C server.
T1071	Command and Control	Application layer protocol	Using normal communication with the attacker through DNS protocol.

INITIAL ACCESS

In this section, we will mention the technique the attackers used to get their initial access to the company machines and internal network.

The attacker used Spear-phishing to gain access into the internal environment.

- Spear-phishing email with malicious Excel File (document with a macros).
- When the victim opens the excel file the security warning appears.
- Once the victim enables the content, the malicious content will be loaded and run automatically
- The victim clicks on content "**ALL-Open and Pay**" button then VBA code will run and using Regsvr32.exe to communicate and download the Dridex payload.
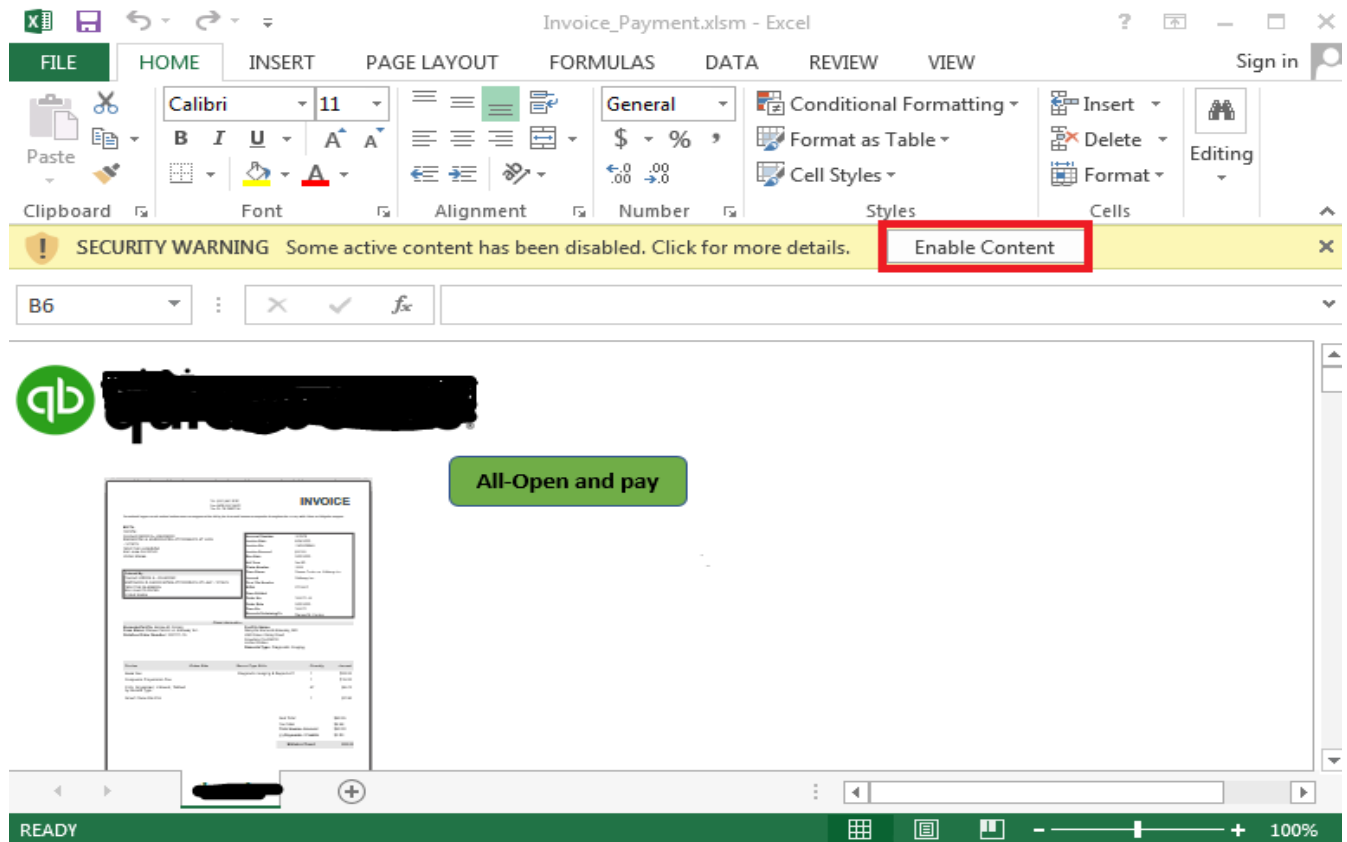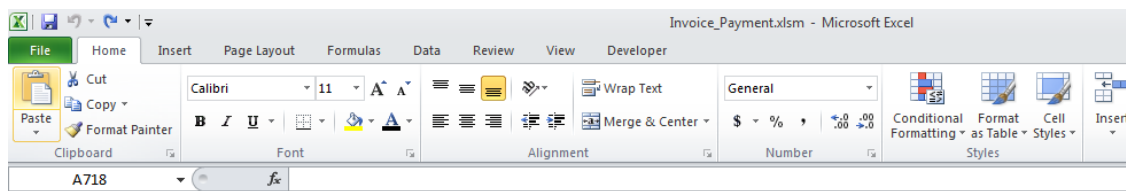
- The VBA code has protection which prevent showing the code, when the user tries to view the VBA project, it pops up a warning message.

  After I analyzed the VBA code, I found that it is able to decode and run a piece of dynamic VBA code containing a URL randomly picked from around 290 encoded download URLs.
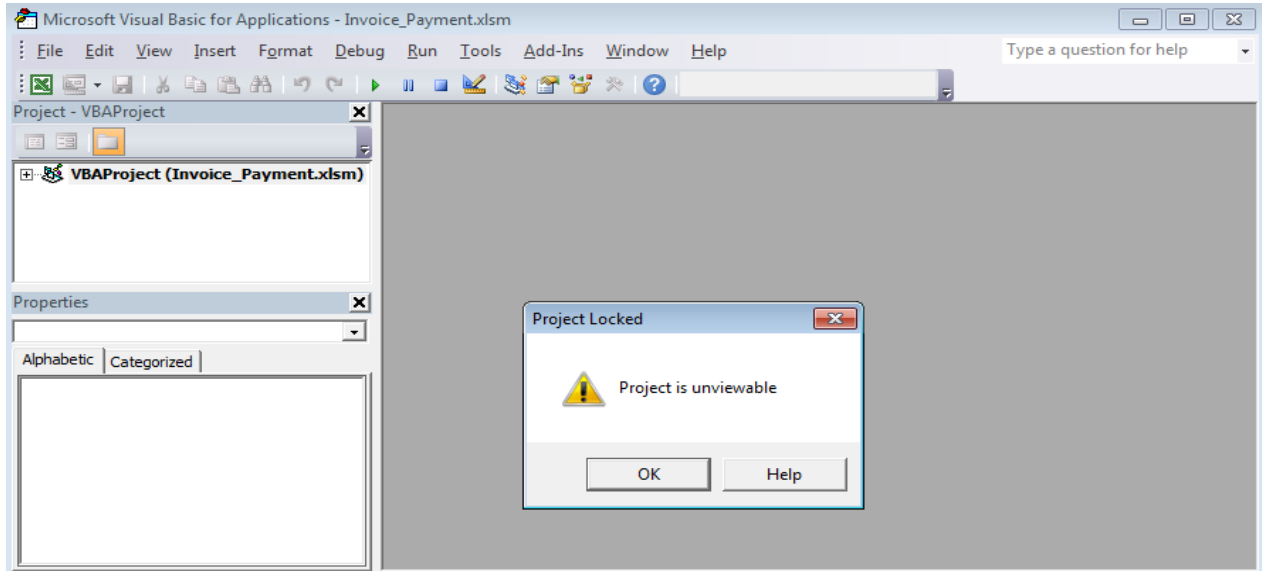
- These download URLs are encoded and hidden (their font color was set to white, the same as the background color) in the first sheet of the Excel document.
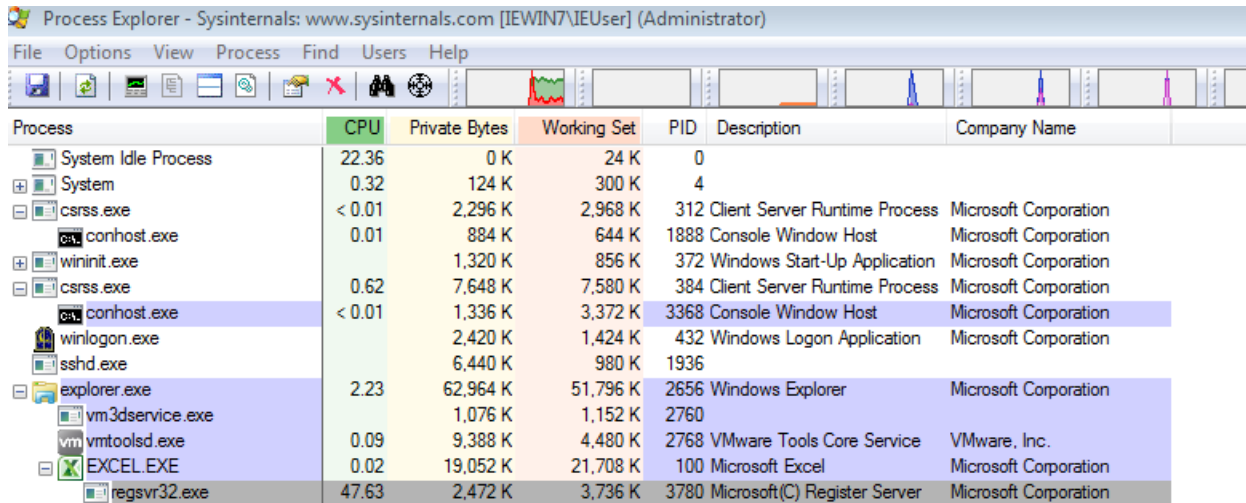
01: DROPPER

The malicious Excel-file works as a downloader for the Dridex-Payload and it starts the downloaded file using the process "regsvr32.exe" with the parameter "-s.
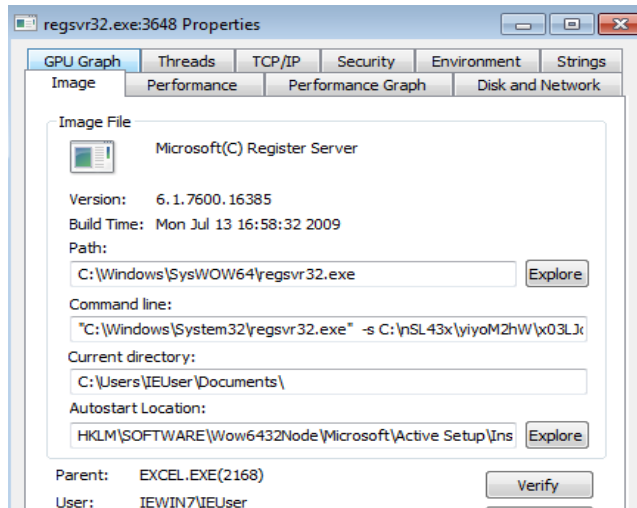

- The hash of malicious Excel-File:

Filename	MD5	Size (in Bytes)	Description
Invoice_Payment.xlsm	36d6caa7639fa761ec5408b1cdc8cad7	56150	Type of the malware: Dropper

02: DROPPED SAMPLE

It uses a fixed path to be saved under C:\ (Random Name) generated each time that user click the malicious button in the Excel-file.

downloaded file is the payload file of Dridex. Therefore, the Excel document is used as a Dridex downloader.

and here are some Http Socket communications generated by regsvr32.exe:

```
55032   HTTP_QueryLocalAddress
55033   HTTP_QueryClientIpAddress
55034   HTTP_QueryClientId
55035   HTTP_QueryClientAddress
55036   HTTP_Open
55037   HTTP_Initialize
55038   HTTP_FreeResolverHint
55039   HTTP_CopyResolverHint
55040   HTTP_Close
55041   HTTP_Abort
55042   HTTP2WinHttpDirectSend
55043   HTTP2WinHttpDirectReceive
55044   HTTP2WinHttpDelayedReceive
55045   HTTP2TimerReschedule
55046   HTTP2TestHook
55047   HTTP2SocketTransportChannel__SendComplete
55048   HTTP2SocketTransportChannel__ReceiveComplete
55049   HTTP2RecycleChannel
55050   HTTP2ProcessRuntimePostedEvent
55051   HTTP2ProcessComplexTSend
55052   HTTP2ProcessComplexTReceive
55053   HTTP2PlugChannelDirectSend
55054   HTTP2IISSenderDirectSend
55055   HTTP2IISDirectReceive
55056   HTTP2GetRpcConnectionTransport
55057   HTTP2FlowControlChannelDirectSend
55058   HTTP2EpRecvFailed
55059   HTTP2DirectReceive
```

- So, let's represent the hashe and TimeDateStamp which is a value representing the time the file was created of the downloaded file (C:\nSL43x\yiyoM2hW\x03LJcZI.exe)

Filename	MD5	PE Timestamp	Size (in Bytes)	Description
x03LJcZI.exe	82da83b56600cbab28b678998d63312f	0x5F18A78E (Wed Jul 22 13:54:38 2020)	303104	Type of the malware: Backdoor, 32 bits

03: FUNCTIONALITY

The malicious Excel-file has a downloader functionality:

- The main goal of the malicious Excel-file which contains VBA code to communicate and download the Trojan file and that works in the 1st stage of the apt attack.
- Once the user enables the content, VBA code will run and use regsvr32.exe to communicate, Then Dridex_Payload downloaded.
- Here we go in the 2nd stage of the attack which will contain different actions:
- Working as a Keylogger, trying to record each keystroke that user clicking and get info.

- The malicious excel file and Regsvr.exe include functions which keylogger uses like (**GetForegroundWindow**) This function returns a handle to the window currently in the foreground of the desktop. Keyloggers commonly use this function to determine in which window the user is entering his keystrokes. And (**GetAsyncKeyState)** This function is used to determine whether a particular key is being pressed. Malware sometimes uses this function to implement a keylogger**.**

  also (**AttachThreadInput**) This function attaches the input processing from one thread to another so that the second thread receives input events such as keyboard and mouse events. Keyloggers and other spyware use this function:

- Then we go to the 3rd stage of exfiltrating the data he collected from the victim and send it to the attacker(C&C) server
- Trying to steal web cookies.
- Trying to steal the victim's account information.
- Communicate with different IPs and malicious domains that encoded and hidden in the malicious excel-file which also decoded by a function in the VBA code called (ExecuteExcel4Macro) Function:

FILESYSTEM CHANGES

Filename	Change Type	Description
C:\nSL43x\yiyoM2hW\x03LJcZI	Created	Downloaded Dridex-Payload

- Every time the victim clicks "All-open and Pay" button, automatically download the Dridex-Payload with a name generated randomly under C:\nsl43X.
- The Dridex-Payload downloaded with random name and without extension (will be described in static analysis section).

- list of Files which payload tries to download:

Hostname	File name	File size	Hash
gds-korea.com	W2coij.pdf	548 bytes	370E16C3B7DBA286CFF055F93B9A94D8
gds-korea.com	9zjyth.txt	548 bytes	370E16C3B7DBA286CFF055F93B9A94D8
gds-korea.com	J7sumb.txt	548 bytes	370E16C3B7DBA286CFF055F93B9A94D8

PROCESSES AND MEMORY CHANGES

Process	Change Type	Description
regsvr32.exe	Created/Service	Dridex is executed in the regsvr32.exe process, which is a command-line utility process of Microsoft Windows used for registering and unregistering DLLs and ActiveX controls in the operating system Registry. The downloaded Dridex payload file is one of these DLL files

- This section for all changes that happened in the registry by the malicious Excel-File:

REGISTRY CHANGES

Here are all the registry changes including:

- Registry changes by the excel.exe which contains query for regsvr.exe process in registry path HKCU\Software\Microsoft\Windows\CurrentVersion\App Paths\regsvr32.exe:

- This malware also modifies "**HKCU\Software\Classes\exefile\shell\open\Drop Target**" registry path which means "**Registry Shell Spawning**", This Registry shell spawning procedure spawns a child process to execute a command or series of commands. so that it will automatically execute every time an .EXE, .COM, .PIF, .BAT, .HT or .HTA file is opened or executed, the malware file will be executed first

- Also, it tries to edit and collect info about all installed softwares, this path contains a lot of information like:
  - DisplayName
  - Display Version
  - Publisher
  - Version Minor
  - Version Major
  - Version

```
2837385  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{92FB6C44-E685-45AD-9B20-CADF4CABA132}.KB4503575
2837386  mInstalledByr
2837387  IEUser
2837388  tInstalledDateu
2837389  9/29/2019
2837390  Update
2837391  InstallerName
2837392  Windows Installer
2837393  iInstallerVersion
2837394  5.00
2837395  Version
```

for example:
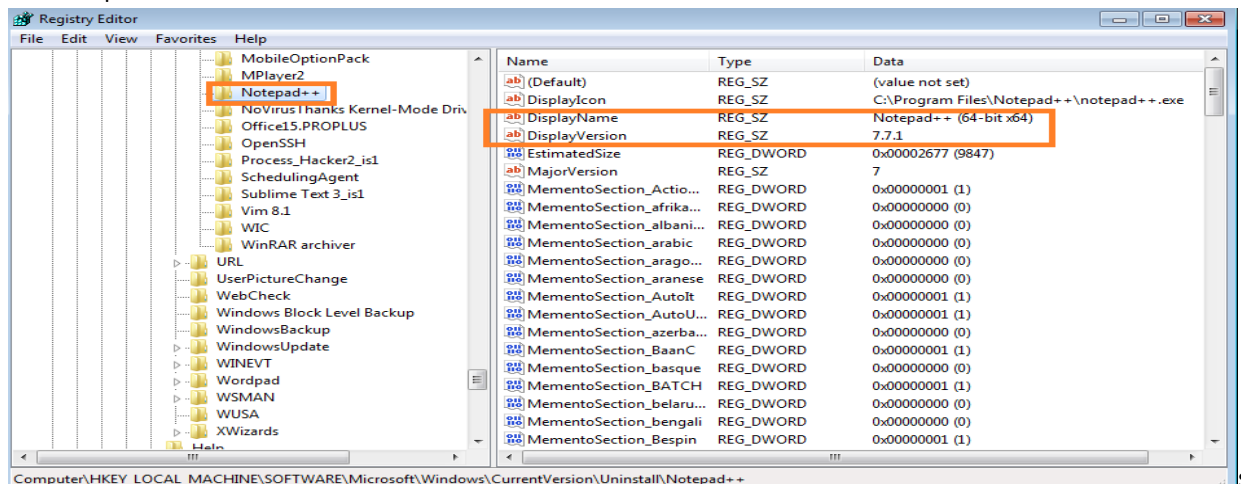
MAINTAINING PERSISTENCE

The regsvr32.exe trying to modify the registry HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Exection Options:

- Image File Execution Options:
  is a Windows registry key which enables Windows to open the door for persistence and code execution will achieved and the trigger will be either the creation of a process or the exit of an application.

COMMAND & CONTROL (C&C)

Here, we will present all information about the communications with C&C servers

- • Communication to multiple malicious domains trying to get C&C commands and other related samples to be downloaded.

DOMAINS AND IPS

Here, you will give an overview on how the communication with the attacker works. Is it

- • Once you click "**ALL-Open and Pay**" button at the same time you observe the analysis tool, you figure out there connections initiated with those domains and IPs:

Domain	IP
Umeskin*com	35.189.52.116
Juiceslam*com	35.246.124.74
www.Ayobergerak*id	159.89.195.219
Bobbydhillonfilmdirector*com	167.172.49.193
Caissefamilylaw*com	35.231.194.169
Limitlessadvisor*com	34.196.61.233
Dreamers*com	206.189.134.108
Musei*basilicate.beniculturali*it	2.42.229.67
Letsencrypt*org	134.209.226.211
Malaysia*hadatha*net	198.50.219.219
Lovecryst*com	149.28.51.189
Zajacwogrodzie*pl	87.98.235.184
Lescousettesdewouavie*com	92.222.139.190
Fastrxsupply*su	79.172.193.55
Plasconpackaging*co*uk	130.211.75.145
Helasverigesamlas*se	164.90.180.213
m.am-clinica*ru	188.120.230.79
Satyasumamarketers*in	81.16.28.177
Nativated*com	35.197.254.151
Mengshuzhai*com	104.18.52.21
	87.98.235.184
	62.240.108.16
	79.172.193.55
	164.90.180.213
	206.189.134.108
	172.67.219.50
	104.18.52.21
	199.66.90.63

ANTI-REVERSING TECHNIQUES

The Dridex malware is Generating an Exception to the Call API

- It tries anti-reversing technique to bypass the analysis has a function based on conditions related to the upper one.
- It has (int 3) value when it hits during running in debugger working as a trap for debuggers then execution will be ended.
- Using exception handler when calling these APIs. it has the "int 3" code at the bottom, which generates an exception with code 80000003 (the BREAKPOINT trap). It interrupts execution and waits until the exception is processed.
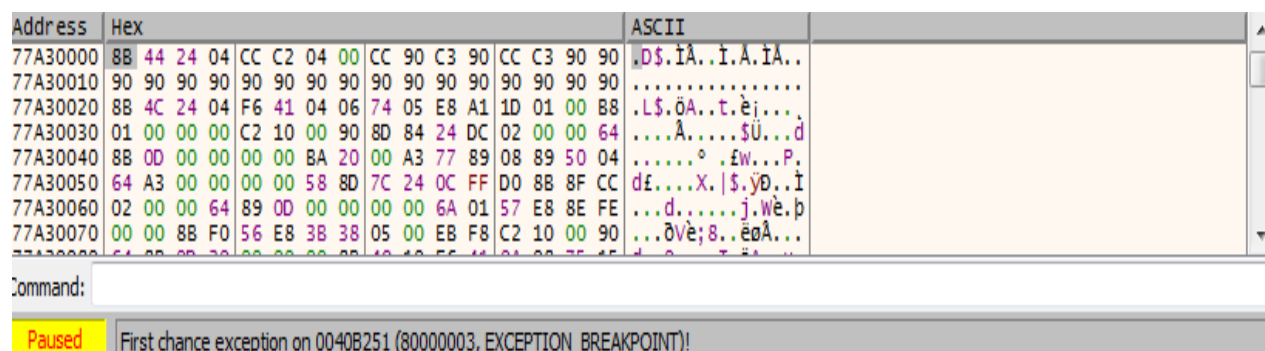
RECOMMENDED ACTIONS

- Enterprises should have email security solution keeping it up to date with online updates of antivirus and IPS definitions.
- Using HIPS solution to monitor a single host for suspicious activity by analyzing events occurring within that host, If the attack is trying to exploit an unknown vulnerability, the anti-virus will not stop it if it doesn't have the signature for it. Host Intrusion Prevention System solutions take a different approach to PC protection than traditional signature anti-malware – HIPS takes control of application integrity rather than trying to match signatures from among the millions of malware examples out there.

CONCLUSION

We explained how Dridex malware getting into the environment and it's different to be techniques obfuscated using phishing emails to infect the internal user with protected VBA code collecting his important information trying to grab it and communicate with the attacker to send him the collected data.

REFERENCES

- Here are References:
  - https://www.fortinet.com/blog/threat-research/hundreds-of-urls-inside-microsoft-excel-spreads-new-dridex-trojan-variant
  - https://en.wikipedia.org/wiki/Dridex
  - https://us-cert.cisa.gov/ncas/alerts/aa19-339a
  - https://www.aha.org/system/files/media/file/2020/06/hc3-cyber-threat-briefing-tlp-white-dridex%20malware-6-25-2020.pdf
  - https://threatresearch.ext.hp.com/dridex-threat-analysis-july-2019-variant/