ID: 357325
Sample Name: purchase order_2242021.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 13:05:58
Date: 24/02/2021
Version: 31.0.0 Emerald

Table of Contents

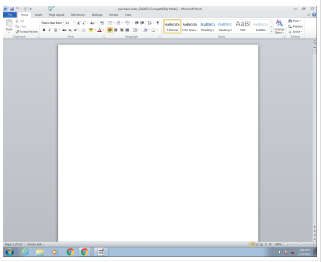
Analysis Report purchase order_2242021.doc

Overview

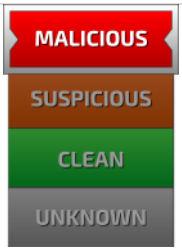
General Information

Sample Name:	purchase order_2242021.doc
Analysis ID:	357325
MD5:	f0c779ec7573308..
SHA1:	6934649699360c..
SHA256:	fe38000650bb91c..
Tags:	doc
Infos:	

Most interesting Screenshot:



Detection



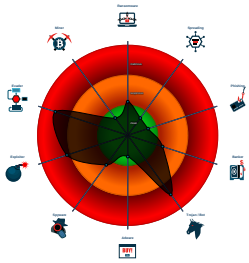
AgentTesla GuLoader

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

Signatures

- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Yara detected AgentTesla
- Yara detected GuLoader
- Connects to a URL shortener service
- Detected RDTSC dummy instruction…
- Drops PE files to the user root direc…
- Hides threads from debuggers
- Office equation editor drops PE file
- Office equation editor starts process…
- Sigma detected: Executables Starte…

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 2276 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- EQNEDT32.EXE (PID: 2368 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - 69577.exe (PID: 2484 cmdline: C:\Users\Public\69577.exe MD5: 5D2D34449323C67BA1F5EC7561DF2204)
    - RegAsm.exe (PID: 2464 cmdline: C:\Users\Public\69577.exe MD5: 246BB0F8D68A463FD17C235DEB5491C0)
      - dw20.exe (PID: 2248 cmdline: dw20.exe -x -s 1612 MD5: FBA78261A16C65FA44145613E3669E6E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.2355136875.000000001E5A1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.2355136875.000000001E5A1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000005.00000002.2351330528.0000000000092000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
Process Memory Space: RegAsm.exe PID: 2464	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: RegAsm.exe PID: 2464	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: EQNEDT32.EXE connecting to internet

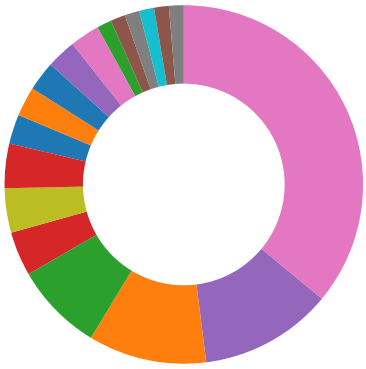
Sigma detected: File Dropped By EQNEDT32EXE

Sigma detected: Executables Started in Suspicious Folder

Sigma detected: Execution in Non-Executable Folder

Sigma detected: Suspicious Program Location Process Starts

Signature Overview



- AV Detection
- Exploits
- Compliance
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Exploits:

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

Compliance:

Uses new MSVCR Dlls

Networking:

Connects to a URL shortener service

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:

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect Any.run

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

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected AgentTesla

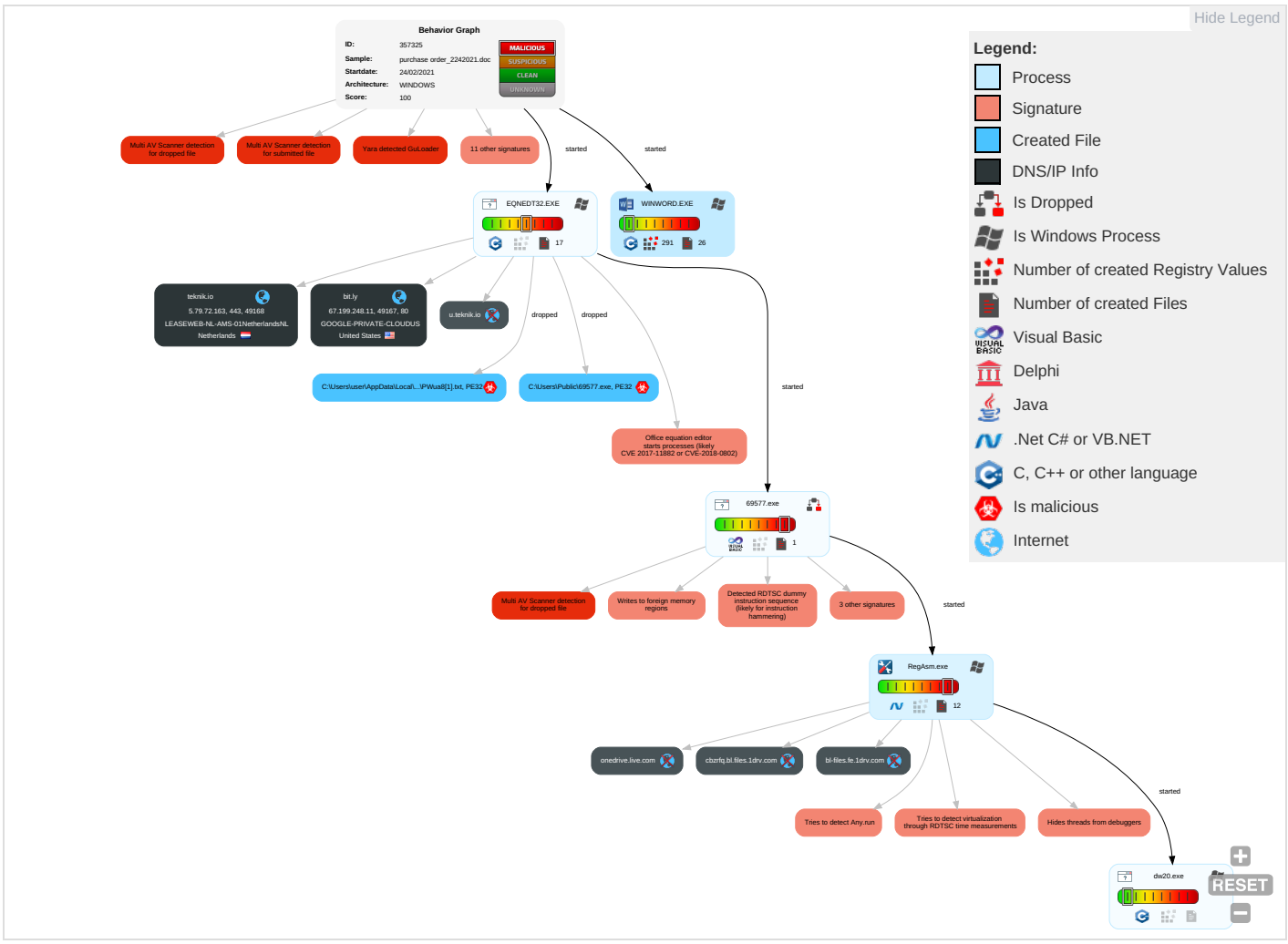
Remote Access Functionality:

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
Spearphishing Link 1	Exploitation for Client Execution 1 3	Path Interception	Access Token Manipulation 1	Masquerading 1 2 1	OS Credential Dumping	Query Registry 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eave Insec Netw Comi
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Virtualization/Sandbox Evasion 2 2	LSASS Memory	Security Software Discovery 6 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 2	Explo Redir Calls
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1 1	Security Account Manager	Virtualization/Sandbox Evasion 2 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Explo Track Local
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM (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	Mani Devic Comi
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamr Denia Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 2 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce

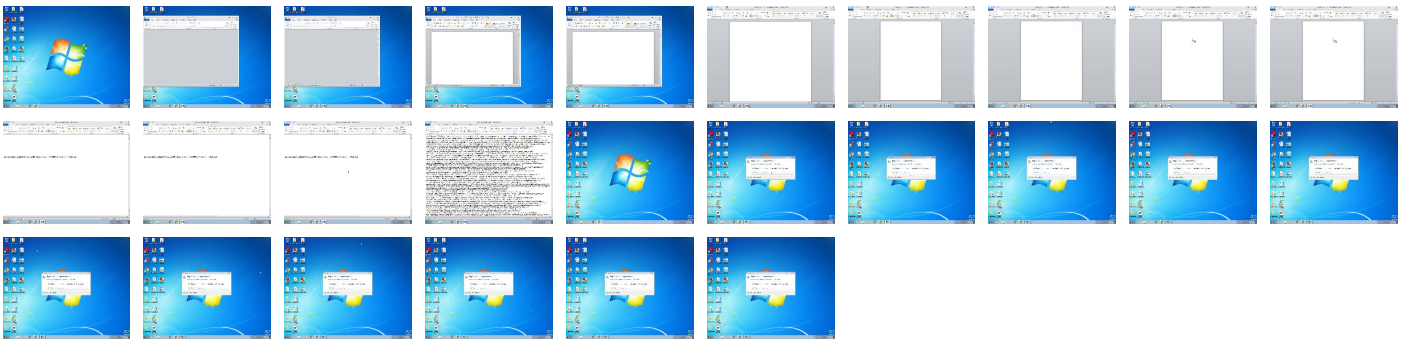
Behavior Graph

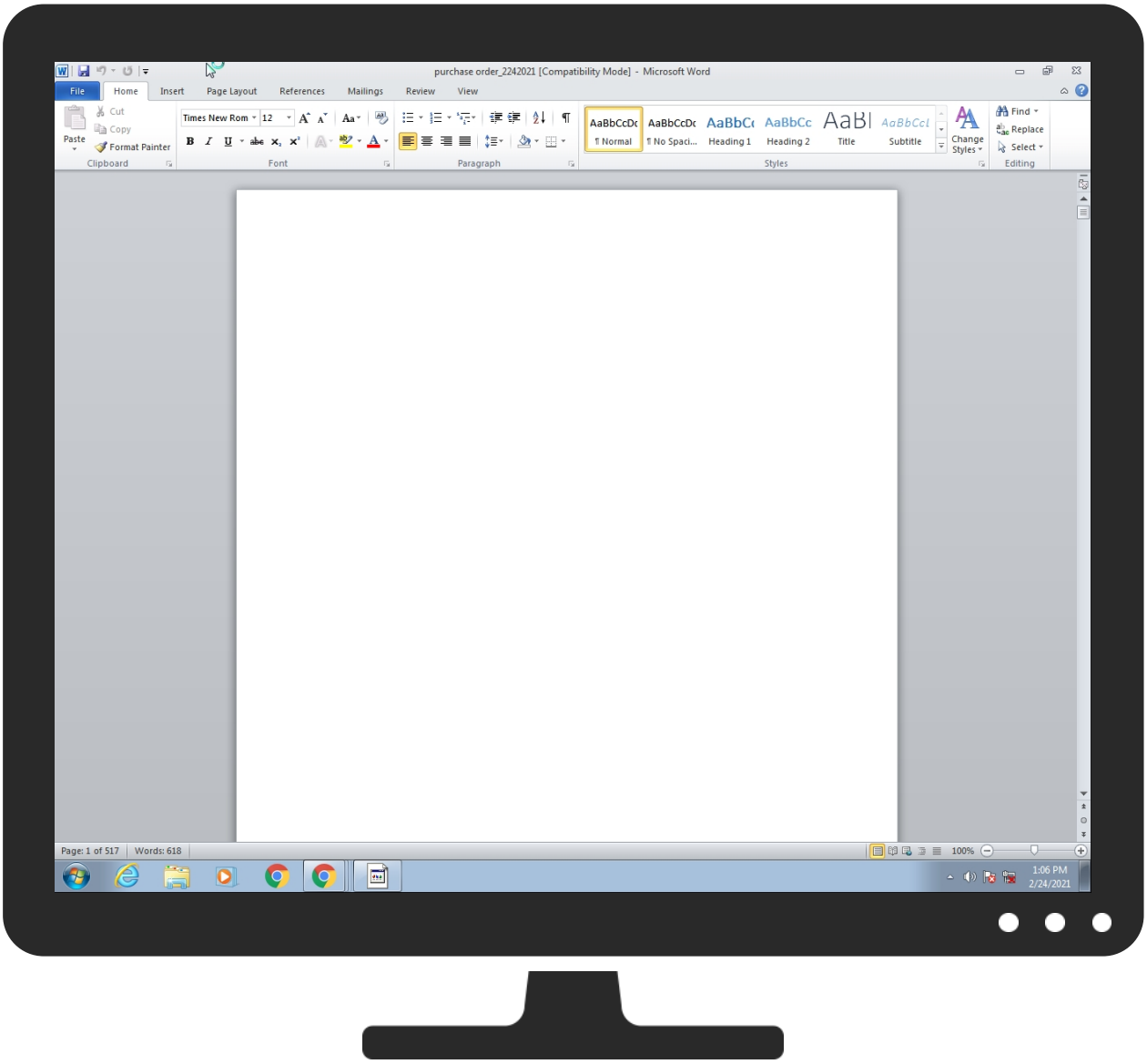


Screenshots

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
purchase order_2242021.doc	43%	Virustotal		Browse
purchase order_2242021.doc	28%	ReversingLabs	Document-Office.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\PWua8[1].txt	12%	ReversingLabs	Win32.Trojan.Remcos	
C:\Users\Public\69577.exe	12%	ReversingLabs	Win32.Trojan.Remcos	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://JSQBKI.com	0%	Avira URL Cloud	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
bit.ly	67.199.248.11	true	false		high
teknik.io	5.79.72.163	true	false		high
onedrive.live.com	unknown	unknown	false		high
cbzrfq.bl.files.1drv.com	unknown	unknown	false		high
u.teknik.io	unknown	unknown	false		high

Contacted URLs

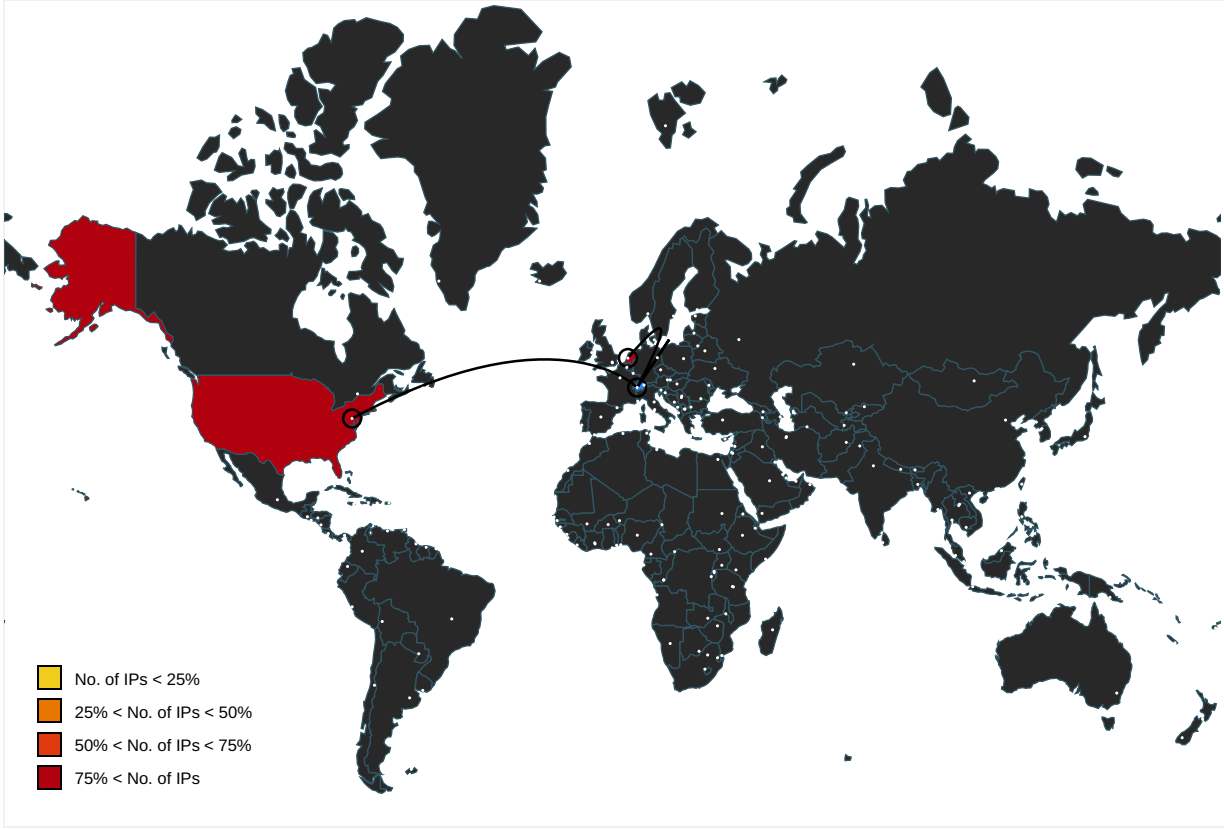
Name	Malicious	Antivirus Detection	Reputation
http://bit.ly/3qO7045	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	RegAsm.exe, 00000005.00000002.2355136875.000000001E5A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	RegAsm.exe, 00000005.00000002.2355136875.000000001E5A1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	RegAsm.exe, 00000005.00000002.2351501536.00000000005EB000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	RegAsm.exe, 00000005.00000002.2351812250.0000000002750000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.entrust.net/server1.crl0	RegAsm.exe, 00000005.00000002.2351501536.00000000005EB000.00000004.00000020.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	RegAsm.exe, 00000005.00000002.2355136875.000000001E5A1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://JSQBKI.com	RegAsm.exe, 00000005.00000002.2355136875.000000001E5A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.entrust.net03	RegAsm.exe, 00000005.00000002.2351501536.00000000005EB000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/download?cid=F57CEB019EB26E7D&resid=F57CEB019EB26E7D%21108&authkey=AN1oxHG	RegAsm.exe, RegAsm.exe, 00000005.00000002.2351501536.00000000005EB000.00000004.00000020.sdmp, RegAsm.exe, 00000005.00000002.2351491082.00000000005D8000.00000004.00000020.sdmp	false		high
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	RegAsm.exe, 00000005.00000002.2351501536.00000000005EB000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	RegAsm.exe, 00000005.00000002.2355136875.000000001E5A1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.%s.comPA	RegAsm.exe, 00000005.00000002.2351812250.0000000002750000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.diginotar.nl/cps/pkioverheid0	RegAsm.exe, 00000005.00000002.2351501536.00000000005EB000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cbzrfq.bl.files.1drv.com/	RegAsm.exe, 00000005.00000002.2351532072.0000000000663000.00000004.00000020.sdmp	false		high
http://https://cbzrfq.bl.files.1drv.com/D	RegAsm.exe, 00000005.00000002.2351532072.0000000000663000.00000004.00000020.sdmp	false		high
http://ocsp.entrust.net0D	RegAsm.exe, 00000005.00000002.2351501536.00000000005EB000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://secure.comodo.com/CPS0	RegAsm.exe, 00000005.00000002.2351501536.00000000005EB000.00000004.00000020.sdmp	false		high
http://crl.entrust.net/2048ca.crl0	RegAsm.exe, 00000005.00000002.2351501536.00000000005EB000.00000004.00000020.sdmp	false		high
http://https://onedrive.live.com/	RegAsm.exe, 00000005.00000002.2351474503.00000000005BD000.00000004.00000020.sdmp	false		high
http://https://u.teknik.io/PWua8.txt	3qO7045[1].htm.2.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
67.199.248.11	unknown	United States		396982	GOOGLE-PRIVATE-CLOUDUS	false
5.79.72.163	unknown	Netherlands		60781	LEASEWEB-NL-AMS-01NetherlandsNL	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	357325
Start date:	24.02.2021
Start time:	13:05:58
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	purchase order_2242021.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (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:	10
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.winDOC@8/19@4/2

EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 79% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 192.35.177.64, 23.0.174.185, 23.0.174.187, 67.26.17.254, 8.238.85.126, 8.248.137.254, 8.250.159.254, 8.241.90.126, 13.107.42.13, 13.107.42.12 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, odc-web-brs.onedrive.akadns.net, odc-web-geo.onedrive.akadns.net, bl-files.ha.1drv.com.l-0003.dc-msedge.net.l-0003.l-msedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, l-0004.l-msedge.net, odwebpl.trafficmanager.net.l-0004.dc-msedge.net.l-0004.l-msedge.net, l-0003.l-msedge.net, audownload.windowsupdate.nsatc.net, apps.digsigtrust.com, odc-bl-files-brs.onedrive.akadns.net, auto.au.download.windowsupdate.com.c.footprint.net, odc-bl-files-geo.onedrive.akadns.net, apps.identrust.com, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:06:38	API Interceptor	47x Sleep call for process: EQNEDT32.EXE modified
13:07:56	API Interceptor	78x Sleep call for process: 69577.exe modified
13:08:01	API Interceptor	629x Sleep call for process: RegAsm.exe modified
13:08:11	API Interceptor	296x Sleep call for process: dw20.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
67.199.248.11	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909yy.doc	Get hash	malicious	Browse	• bit.ly/3kijui1
	QUOTE.doc	Get hash	malicious	Browse	• bit.ly/2P3CMwd
	IMG_61061_SCANNED.doc	Get hash	malicious	Browse	• bit.ly/2ZElo32
	SWIFT Payment W0301.doc	Get hash	malicious	Browse	• bit.ly/3dyLFYN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Quotation408S_A02021_AHYAN_group_of_companies.doc	Get hash	malicious	Browse	• bit.ly/2O MPBuy
	YOUR PRODUCT.doc	Get hash	malicious	Browse	• bit.ly/2LVhrUo
	Invoice.doc	Get hash	malicious	Browse	• bit.ly/3a msMGn
	Purchase order.doc	Get hash	malicious	Browse	• bit.ly/3q m8NNO
	IMG_04779.doc	Get hash	malicious	Browse	• bit.ly/3dffBt0
	INV00004423.doc	Get hash	malicious	Browse	• bit.ly/3aLXmrV
	PO_Scanned_06387.doc	Get hash	malicious	Browse	• bit.ly/3rwUfef
	IMG_Scanned_3062.doc	Get hash	malicious	Browse	• bit.ly/2YXPr5o
	INV00004423.doc	Get hash	malicious	Browse	• bit.ly/2MvEzt1
	DTBT760087673.doc	Get hash	malicious	Browse	• bit.ly/3arM6Rr
	IMG_59733.doc	Get hash	malicious	Browse	• bit.ly/3rf1U0L
	IMG_804941.doc	Get hash	malicious	Browse	• bit.ly/3cyMT5V
	IMG_0916.doc	Get hash	malicious	Browse	• bit.ly/3pFy7y3
	SOA 2.doc	Get hash	malicious	Browse	• bit.ly/3cxhzEz
	Quotation Ref FP-299318.doc	Get hash	malicious	Browse	• bit.ly/3a nMC2V
	PO 9174-AR.doc	Get hash	malicious	Browse	• bit.ly/2LcGNNi
5.79.72.163	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909yy.doc	Get hash	malicious	Browse	
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	
	PO AAN2102002-V020.doc	Get hash	malicious	Browse	
	PO55004.doc	Get hash	malicious	Browse	
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	
	RFQ Document.doc	Get hash	malicious	Browse	
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909_RAW.doc	Get hash	malicious	Browse	
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	
	QUOTATION44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCK.doc	Get hash	malicious	Browse	
	Quotation408S_A02021_AHYAN_group_of_companies.doc	Get hash	malicious	Browse	
	tcwO1bua5E.exe	Get hash	malicious	Browse	
	87e8ff5c51e0.xls	Get hash	malicious	Browse	
	Request for Quote_SEKOLAH TUNAS BAKTI SG.doc__.rtf	Get hash	malicious	Browse	
	hvEUyC1xKe.exe	Get hash	malicious	Browse	
	NEW_QUOTATION_mp20201126_Quotation_20P6200829_sup_mpjxPriceInquiry_1606406420424.doc	Get hash	malicious	Browse	
	Purchase Order.doc	Get hash	malicious	Browse	
	CAz0v9shg2.rtf	Get hash	malicious	Browse	
	pGSheevuq8.rtf	Get hash	malicious	Browse	
	wtYnMaD8Bg.rtf	Get hash	malicious	Browse	
	Wines list12.12.2020.doc	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
bit.ly	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909yy.doc	Get hash	malicious	Browse	• 67.199.248.11
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 67.199.248.10
	PO AAN2102002-V020.doc	Get hash	malicious	Browse	• 67.199.248.11
	PO55004.doc	Get hash	malicious	Browse	• 67.199.248.10
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 67.199.248.10
	RFQ Document.doc	Get hash	malicious	Browse	• 67.199.248.10
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909_RAW.doc	Get hash	malicious	Browse	• 67.199.248.10
	Order.doc	Get hash	malicious	Browse	• 67.199.248.10
	QUOTE.doc	Get hash	malicious	Browse	• 67.199.248.11
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_57109_Scanned.doc	Get hash	malicious	Browse	• 67.199.248.10
	Deadly Variants of Covid 19.doc	Get hash	malicious	Browse	• 67.199.248.10

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	swift payment.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_61061_SCANNED.doc	Get hash	malicious	Browse	• 67.199.248.11
	IMG_6078_SCANNED.doc	Get hash	malicious	Browse	• 67.199.248.11
	IMG_01670_Scanned.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_7742_Scanned.doc	Get hash	malicious	Browse	• 67.199.248.10
	SWIFT Payment W0301.doc	Get hash	malicious	Browse	• 67.199.248.11
	_a6590.docx	Get hash	malicious	Browse	• 67.199.248.11
	Statement-ID28865611496334.vbs	Get hash	malicious	Browse	• 67.199.248.10

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LEASEWEB-NL-AMS-01NetherlandsNL	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909yy.doc	Get hash	malicious	Browse	• 5.79.72.163
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 5.79.72.163
	PO AAN2102002-V020.doc	Get hash	malicious	Browse	• 5.79.72.163
	PO55004.doc	Get hash	malicious	Browse	• 5.79.72.163
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 5.79.72.163
	RFQ Document.doc	Get hash	malicious	Browse	• 5.79.72.163
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909_RAW.doc	Get hash	malicious	Browse	• 5.79.72.163
	SecuriteInfo.com.Trojan.PackedNET.540.1271.exe	Get hash	malicious	Browse	• 213.227.154.188
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 5.79.72.163
	MV9tCJw8Xr.exe	Get hash	malicious	Browse	• 5.79.70.250
	QUOTATION44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCK.doc	Get hash	malicious	Browse	• 5.79.72.163
	Quotation408S_A02021_AHYAN_group_of_companies.doc	Get hash	malicious	Browse	• 5.79.72.163
	Request For Quotation.PDF.exe	Get hash	malicious	Browse	• 212.32.237.101
	PO#652.exe	Get hash	malicious	Browse	• 5.79.87.207
	Parcel _009887 .exe	Get hash	malicious	Browse	• 212.32.237.92
	PO 20211602.xlsm	Get hash	malicious	Browse	• 82.192.82.225
	6d0000.exe	Get hash	malicious	Browse	• 213.227.133.129
	SecuriteInfo.com.Trojan.PackedNET.541.9005.exe	Get hash	malicious	Browse	• 62.212.86.139
	New Order 83329 PDF.exe	Get hash	malicious	Browse	• 95.211.208.58
	YTDSetup.exe	Get hash	malicious	Browse	• 82.192.80.226
GOOGLE-PRIVATE-CLOUDUS	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909yy.doc	Get hash	malicious	Browse	• 67.199.248.11
	Offerte aanvragen 22-02-2021.ppt	Get hash	malicious	Browse	• 67.199.248.16
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 67.199.248.10
	PO AAN2102002-V020.doc	Get hash	malicious	Browse	• 67.199.248.10
	PO55004.doc	Get hash	malicious	Browse	• 67.199.248.10
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 67.199.248.10
	RFQ Document.doc	Get hash	malicious	Browse	• 67.199.248.10
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909_RAW.doc	Get hash	malicious	Browse	• 67.199.248.10
	Order.doc	Get hash	malicious	Browse	• 67.199.248.10
	QUOTE.doc	Get hash	malicious	Browse	• 67.199.248.11
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_57109_Scanned.doc	Get hash	malicious	Browse	• 67.199.248.10
	Deadly Variants of Covid 19.doc	Get hash	malicious	Browse	• 67.199.248.10
	swift payment.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_61061_SCANNED.doc	Get hash	malicious	Browse	• 67.199.248.11
	IMG_6078_SCANNED.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_01670_Scanned.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_7742_Scanned.doc	Get hash	malicious	Browse	• 67.199.248.10
	SWIFT Payment W0301.doc	Get hash	malicious	Browse	• 67.199.248.11
	_a6590.docx	Get hash	malicious	Browse	• 67.199.248.11

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8efIqigYDff:RN7MlanAQwEIztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....T.....R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.....\|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n-.....D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay.....n/R... ._.+..<....Am.t.<. ..V..y`.yO..e@../...<#..#.....dju*..B.....8..H'..lr.....I.I6/..d.].xIX<...&U...GD..Mn.y&.[<(tk.....%B.b;/..`.#h....C.P...B..8d.F...D.k..... 0..w...@(.. @K....?.)ce.....\.\.....I.....Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a.,...E5 X..i.d..w.....#o*+.....X.P...k...V.$...X.r.e....9E.x..=\...Km.....B...Ep...xI@@c1.....p?...d.{EYN.K.X>D3..Z..q.] .Mq.....L.n}.....+/I\.cDB0.'.Y...r.[.....vM...o.=....zK..r.. I..>B....U..3....Z...ZjS...wZ.M...IW;..e.L...zC.wBtQ..&.Z.Fv+..G9.8..!..\T:K`.....m.....9T.u..3h.....{...d[...@...Q.?..p.e.t[.%7.....^.....s.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	data
Category:	dropped
Size (bytes):	893
Entropy (8bit):	7.366016576663508
Encrypted:	false
SSDEEP:	24:hBntmDvKUQQDvKUr7C5fpqp8gPvXHmXvponXux:3ntmD5QQD5XC5RqHHXmXvp++x
MD5:	D4AE187B4574036C2D76B6DF8A8C1A30
SHA1:	B06F409FA14BAB33CBAF4A37811B8740B624D9E5
SHA-256:	A2CE3A0FA7D2A833D1801E01EC48E35B70D84F3467CC9F8FAB370386E13879C7
SHA-512:	1F44A360E8BB8ADA22BC5BFE001F1BABB4E72005A46BC2A94C33C4BD149FF256CCE6F35D65CA4F7FC2A5B9E15494155449830D2809C8CF218D0B9196EC646BC
Malicious:	false
Reputation:	high, very likely benign file
Preview:	0..y..*.H.....j0..f...1.0...*.H.....N0..J0..2.....D...'..09...@k0...*.H.....0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30...0009302112192..210930140115Z0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30.."0...*.H.....0.....P..W..be.....,k0.[...}.@.....3vI*.?!I..N..>H.e...!.e.*.2....w..{.....s.z..2..~..0....*8.y.1.P..e.Qc...a.Ka..Rk...K.(.H.....>.... .[.*....p....%.tr.{j.4.0...h.{T....Z...=d.....Ap..r.&.8U9C....\@.....%.....:..n.>..\..<.i....*.)W..=....]..... B0@0...U.....0....0...U.....0....0...U.....{,q...K.u...`...0...*.H.....,...\...(f7:...?K.... ]..YD.>.>..K.t.....t..~.....K. D....}..j.....N..:.pI.....:^H...X._..Z.....Y..n.....f3.Y[...sG.+..7H..VK....r2...D.SrmC.&H.Rg.X..gvqx...V..9$1....Z0G..P.....dc`.....}...=2.e..|.Wv..(9..e...w.j..w.....)...55.1.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.090852246460565
Encrypted:	false
SSDEEP:	6:kKLRgVpbqoN+SkQlPlEGYRMY9z+4KlDA3RUeKlF+adAlf:jRr3kPlE99SNxAhUeo+aKt
MD5:	06D163042F0078DA3522C50E90975E28
SHA1:	2173031E7AC39CA991EA0C7D992E1F4BEA3DE2A8
SHA-256:	E6E0D52FF25A5EAC6B21282081AA15C511FB0666EEF3B0D91F90F0E114ECB98A
SHA-512:	DE2171EBF28792ADE6A7BE0646575C31FBD2577283AC83737DC4BF7AA1577C797DD789AD45B6F5D584F3D7BAE958FB3A86065D5081C55D674D7E3F4A47E0F1D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Preview:	p..... .....4.....(..... ....&.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.e.b.b.a.e.1.d.7.e.a.d.6.1.:.0."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	3.0215269645321685
Encrypted:	false
SSDEEP:	3:kkFklMdUtXfllXIE/QhzllPlzRkwWBARLNDU+ZMlKlBkvclcMlVHblB1UAYpFit:kKX8JliBAIdQZV7eAYLit
MD5:	418E33A6103113CCFF36E4BE556E8261
SHA1:	D33A2F7A96B8FAA2121BDDEC0D2F3DF3961B1419
SHA-256:	2C2AFE1975A6CA6A7BD38F5954DD86E72B5D1289212A8BB3328317BDB1977E6E
SHA-512:	143B2A4378B9572E4DB1532F732DA5146EBAD0814875DA732A7AB1D0FBB17F3F45A6F5E8D2482427BDFE00C2A98DA90968F63394F58D16A8C890782E1AF64B37
Malicious:	false
Reputation:	low
Preview:	p..... ....`.....(..... .....u.....(.....}...h.t.t.p.:././.a.p.p.s...i.d.e.n.t.r.u.s.t...c.o.m./.r.o.o.t.s./.d.s.t.r.o.o.t.c.a.x.3...p.7.c...".3.7.d.-.5.9.e.7.6.b.3.c.6.4.b.c.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\PWua8[1].txt	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	131072
Entropy (8bit):	4.79650156443488
Encrypted:	false
SSDEEP:	1536:HWWTwV4fVhuy/kysvxhG7NuX40vbyovaWm5vj2kht/uxVQwV4MjW:7wVUPsyChtX40Tyova75vj2mt/QqwV
MD5:	5D2D34449323C67BA1F5EC7561DF2204
SHA1:	A48C7F51DB44CA8A2B0240D9C57C1983AC5D75DD
SHA-256:	95A1FF3F5D08AC3D0DFE64300EEC668FA0C78BDB7DA395F1D91735C5A0AEF8A5
SHA-512:	28B4C6DF609084045F866686E559C7771B6455BC8FDE56942F9422265C6ED2ACFE12EF383C23225AD171D9D7BA22EFC9EF7137C069070812AF798EDAA8AE6D7
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 12%
Reputation:	low
IE Cache URL:	http://https://u.teknik.io/PWua8.txt
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1...1...1....0...~..0.....0...Rich1.....PE..L...n\RK.....P.....`....@.....J.....R..(....p.....(... .....text...DF.....P.....`.data.....`.....`.....@....rsrc.....p.....p.....@..@...I.....MSVBVM60.DLL.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\3qO7045[1].htm	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	116
Entropy (8bit):	4.555420363401828
Encrypted:	false
SSDEEP:	3:qVvzLURODccZ/vXbvx9nDyZHL+dEJRTHsIkFSXbKFvNGb:qFzLIeco3XLx92ZHqGJVMIMSLWQb
MD5:	5430FAE62906F346226C0F6B7EDB2505
SHA1:	1CAB9FF7715955A9BD0C3702AF5152353BAA6901
SHA-256:	104F6C00E1E641D26F8F4E324B88FFA7A6A825FA195DBBABA775BBD8F86EC554
SHA-512:	FBEF7B1D0A394927CAEFF28C56E9F0ED1F59949BB964D3BC1B5C197128BC2F08FFFD97A3FA68145FD0534ABC2253277797C68A9710D605D747D7388924302EF
Malicious:	false
Reputation:	low
Preview:	<html>.<head><title>Bitly</title></head>.<body>moved here</body>.</html>

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{96CDA2CA-B597-4160-9AA2-9325CEFB4D67}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{96CDA2CA-B597-4160-9AA2-9325CEFB4D67}.tmp	
Entropy (8bit):	1.3573187972516119
Encrypted:	false
SSDEEP:	3:Iiiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlbf:IiiiiiiiifdLloZQc8++lsJe1MzM
MD5:	ADEECB285197F0DA2AC8593087E205A2
SHA1:	78E89DAF70658C478C753D50D4C39755F5CDCA84
SHA-256:	4FE2B6146A5F8F2641F78A01D06063848F0790082776D94ADACD89D9A462E0E1
SHA-512:	307F3F8621F1B9FF604041D8BC7746BBAC8C706537797E40F910625D0882BED9E2EAEEB78D801850F79EDA41D550670C72F4DE363EAE7F84E67BA93458C0CFE
Malicious:	false
Reputation:	low
Preview:	..(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A.. ...."...&...*.......:..>... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{9A867ADF-3614-4635-BFBB-6C9AC8D8FC42}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	3498022
Entropy (8bit):	4.142539932120983
Encrypted:	false
SSDEEP:	24576:FDKMKEUMKOyMKwpMKMlMYkKMGMKt1MKohMHwKMe9KM6MKo9MwheQ:vQ
MD5:	A1F0AB1026D7BD370F80083BBA7CE963
SHA1:	32BC747DED3B2018E0856E759FF03ADEA33BF5EE
SHA-256:	C6E3761741B575DD410FD2C5857E950F1A15F4C515FE5D32BBDA920AE9FD8B79
SHA-512:	5493327842E3569752958E78F948FC08811790F81746834547C1BD8AA005D36C6D5C9E1ECEB12363CBF6ABBEFA61AC75354A237A493FB732F91FA0E1B5EF7E5C
Malicious:	false
Reputation:	low
Preview:	..@.A.p.J.n.b.S.m.E.I.k.B.Y.w.P.B.r.@.-.D.y.s.i.v.y.j.z.Z.m.o.I.e.C.P.i.F.<.e.h.&.&.0._.M.-.C._.g.-.-._.-.d.,.6.4.>.3.2.9.9.7.$.C.v.>.y.t.=.n.5.|.:.%._.>.j.n.8.%.b.m.;.=.u...2.8..... . . . .

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B6618253-1CF8-4E74-AA78-05F4F57053A0}.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
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Temp\Cab78C9.tmp	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8efIqigYDff:RN7MlanAQwEIztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F

C:\Users\user\AppData\Local\Temp\Cab78C9.tmp	
Malicious:	false
Preview:	MSCF.....,.....I.....T.....R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.....\|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n-.....D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay.....n/R... ._.+..<...Am.t.<. ..V..y`.yO..e@../...<#..#.....dju*..B.....8..H'..lr.....l.I6/..d.].xIX<...&U...GD..Mn.y&.[<(tk.....%B.b;./..`.#h....C.P...B..8d.F...D.k..... 0..w...@(.. @K....?.)ce.....\.\.....l.....Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a.,...E5 X..i.d..w.....#o*+.....X.P...k...V.$...X.r.e....9E.x..=\...Km.....B...Ep...xI@@c1.....p?...d.{EYN.K.X>D3..Z..q.] .Mq.....L.n}.....+/I\.cDB0.'.Y...r.[.....vM...o.=....zK..r.. I..>B....U..3....Z...ZjS...wZ.M...IW;..e.L...zC.wBtQ..&.Z.Fv+..G9.8..!..\T:K`.....m.....9T.u..3h.....{...d[...@...Q.?..p.e.t[.%7.....^.....s.

C:\Users\user\AppData\Local\Temp\Tar78CA.tmp	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	data
Category:	dropped
Size (bytes):	152788
Entropy (8bit):	6.316654432555028
Encrypted:	false
SSDEEP:	1536:WIA6c7RbAh/E9nF2hspNuc8odv+1//FnzAYtYyjCQxSMnl3xlUwg:WAmfF3pNuc7v+ltjCQSMnnSx
MD5:	64FEDADE4387A8B92C120B21EC61E394
SHA1:	15A2673209A41CCA2BC3ADE90537FE676010A962
SHA-256:	BB899286BE1709A14630DC5ED80B588FDD872DB361678D3105B0ACE0D1EA6745
SHA-512:	655458CB108034E46BCE5C4A68977DCBF77E20F4985DC46F127ECBDE09D6364FE308F3D70295BA305667A027AD12C952B7A32391EFE4BD5400AF2F4D0D83087
Malicious:	false
Preview:	0..T...*.H.....T.0..T....1.0...`.H.e.....0..D...+.....7.....D.0..D.0...+.....7.....R19%..210115004237Z0...+.....0..D.0..*....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0 ...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a. t.e. .A.u.t.h.o.r.i.t.y...0.,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00. .+.....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[....J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

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):	104
Entropy (8bit):	4.477506521672235
Encrypted:	false
SSDEEP:	3:M16NKRAX6XDEd6lNC9KRAX6XDEd6lmX16NKRAX6XDEd6lv:M4NAAXwEAfC9AAXwEAvNAAXwEA1
MD5:	319E61C883692B7358D466E3AD6A8B01
SHA1:	5DD6A28A69BCFE9050F178FC3E0BA82E9E1E9CB9
SHA-256:	FA9F64C6A6A7A55D1C25A0431BD0AFA9D82CFD15920E1142CD63A282E8939A85
SHA-512:	2D17CE30A4187D7B32EB69A31BF983099AD433750B74183A4F7AE411EE419E669AF4EA8F0B0B1605144F875CB1B4D1CDA190C2AC01713F6A4752BAD17AB3431
Malicious:	false
Preview:	[doc]..purchase order_2242021.LNK=0..purchase order_2242021.LNK=0..[doc]..purchase order_2242021.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\purchase order_2242021.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=Wed Aug 26 14:08:18 2020, mtime=Wed Aug 26 14:08:18 2020, atime=Wed Feb 24 20:06:36 2021, length=1797651, window=hide
Category:	dropped
Size (bytes):	2148
Entropy (8bit):	4.558495707581942
Encrypted:	false
SSDEEP:	48:8n/XT0ZVXb+2Cw4+Qh2n/XT0ZVXb+2Cw4+Q/:8n/XuVXbM+Qh2n/XuVXbM+Q/
MD5:	B17CF01EAFABBDBC92CA93B98A73A27E
SHA1:	226FEC551A3022DD9EC31C81D152DB512465853C
SHA-256:	6AE2076101B206082430CBC6AC9EE18396AB47F62953D9D24AB1C5A9E80E7C8B
SHA-512:	4FDDC21D95242B07FDB7038FB8CEC50E25274E09093ACD08CD9C4436B769938E290BD24A58E14F5833AB31C0C45D4F5C3176D3B5D12DB8402833292952FBD22
Malicious:	false
Preview:	L.....F.... ....P.{...P.{.....n.....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.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7 .6.9.....~.2..n..XR. .PURCHA~1.DOC..b.....Q.y.Q.y*...8.....p.u.r.c.h.a.s.e. .o.r.d.e.r._.2.2.4.2.0.2.1...d.o.c.....-...8...[.....?J.....C:\Users\..#..... .....\\061544\Users.user\Desktop\purchase order_2242021.doc.1.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.p.u.r.c.h.a.s.e. .o.r.d.e.r._.2.2.4.2.0.2.1...d.o.c.....:..,.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.....061544....

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

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVy3KGcils6w7Adtln:vdsCkWthGciWfQl
MD5:	4A5DFFE330E8BBBF59615CB0C71B87BE
SHA1:	7B896C17F93ECFC9B69E84FC1EADEDD9DA550C4B
SHA-256:	D28616DC54FDEF1FF5C5BA05A77F178B7E3304493BAF3F4407409F2C84F4F215
SHA-512:	3AA160CB89F4D8393BCBF9FF4357FFE7AE00663F21F436D341FA4F5AD4AEDC737092985EB4A94A694A02780597C6375D1615908906A6CEC6D7AB616791B6285C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Preview:	..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\HDGNLTQS.txt	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	ASCII text
Category:	downloaded
Size (bytes):	90
Entropy (8bit):	4.294724337284533
Encrypted:	false
SSDEEP:	3:jvdiE1C7i2JLJdvglvPRdWFYIS/n:kE1ki2JLTvgliFJn
MD5:	60C5107F8B85546339B0AF38B517DD85
SHA1:	4C7E105169D3E3C2608F917EEB0A76AC70247D7F
SHA-256:	14DDA52EF4808BBBF1D30E95609E89C4E36D030D772A128405B58AA1D8F0E965
SHA-512:	7F15E78260E2DC398DFCD0BD0054EBBF250193873B610BA668565DAA5DAA35C05EDE12696108DD019CEED954AFB5336B5674B1323D3C43AFC335ECE1EB767E FB
Malicious:	false
IE Cache URL:	bit.ly/
Preview:	_bit.l1oc6O-1f1018e00109e7d832-00p.bit.ly/.1536.1517611264.30906391.1555483204.30870257.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\JOHDAECH.txt	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	64
Entropy (8bit):	4.1123437507738325
Encrypted:	false
SSDEEP:	3:vpqMLJUQ2arRTTG4WT/nx3SyS/n:vEMWXo1TG4UJSpn
MD5:	52D117091370D78E57A45347984C82A7
SHA1:	B88EAFFA9FC3F0B37D88CA795DAB3F572EE601AF
SHA-256:	0BE8ADA46BA469AA2021090A2188B15F58BE7E1935353887AB6828EA482548F1
SHA-512:	16A12CDCE6B48FEF53897D51A9D16AE36DD22AA730404019765140069581EA30917B0711C148008286542CE0FF83E8F2949A7770D56591967781F67E2CCC202B
Malicious:	false
IE Cache URL:	live.com/
Preview:	wla42..live.com/.1536.3819446656.30871589.3600096691.30870257.*.

C:\Users\user\Desktop\~$rchase order_2242021.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

C:\Users\user\Desktop\~$rchase order_2242021.doc	
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVy3KGcils6w7Adtln:vdsCkWthGciWfQl
MD5:	4A5DFFE330E8BBBF59615CB0C71B87BE
SHA1:	7B896C17F93ECFC9B69E84FC1EADEDD9DA550C4B
SHA-256:	D28616DC54FDEF1FF5C5BA05A77F178B7E3304493BAF3F4407409F2C84F4F215
SHA-512:	3AA160CB89F4D8393BCBF9FF4357FFE7AE00663F21F436D341FA4F5AD4AEDC737092985EB4A94A694A02780597C6375D1615908906A6CEC6D7AB616791B6285C
Malicious:	false
Preview:	.user...A.l.b.u.s.............p.......................................P.....................z...............x...

C:\Users\Public\69577.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	131072
Entropy (8bit):	4.79650156443488
Encrypted:	false
SSDEEP:	1536:HWWTwV4fVhuy/kysvxhG7NuX40vbyovaWm5vj2kht/uxVQwV4MjW:7wVUPsyChtX40Tyova75vj2mt/QqwV
MD5:	5D2D34449323C67BA1F5EC7561DF2204
SHA1:	A48C7F51DB44CA8A2B0240D9C57C1983AC5D75DD
SHA-256:	95A1FF3F5D08AC3D0DFE64300EEC668FA0C78BDB7DA395F1D91735C5A0AEF8A5
SHA-512:	28B4C6DF609084045F866686E559C7771B6455BC8FDE56942F9422265C6ED2ACFE12EF383C23225AD171D9D7BA22EFC9EF7137C069070812AF798EDAA8AE6D7
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 12%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......u...1...1...1.....0...~..0......0...Rich1...........PE..L...n\RK.................P ....`....@..................................J.......................................R..(....p....................................................................(... ...................................text...DF.......P................. ..`.data........`.......`.............@....rsrc.......p.......p.............@..@...I...........MSVBVM60.DLL...

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	6.29966086098654
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	purchase order_2242021.doc
File size:	1797651
MD5:	f0c779ec7573308d5c5bbf15762391d5
SHA1:	6934649699360c8cf7a0d8dee37c994082268054
SHA256:	fe38000650bb91c8e0d5aee0a0bff8136d849d58dc6f7d9f35d33788abd9a799
SHA512:	d4adf951d8c57f8a63c0a5f9cbbb8ba56fe6820669159e879e5d29e390571c57c651f3457df60ae85e4b40fedb1d3f870af333aa4e50ad136a4f027ebe1aeede
SSDEEP:	12288:VZQgZQgZQgZQgZQgZQgZQgZQgZQgZQgZQgZQgZQgZQgZQgZQgZQgZQgZQgZQgZQgZQC:V/////////////////////////o545h
File Content Preview:	{\rtf51437\page11419927264400464@ApJnbSmElkBYwPBr@-DysivyjzZmoIeCPiF<eh&&0_M-C_g--_-d,64>32997$Cv>yt=n5|:%_>jn8%bm\mklP;=u\m3699.28........ ....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

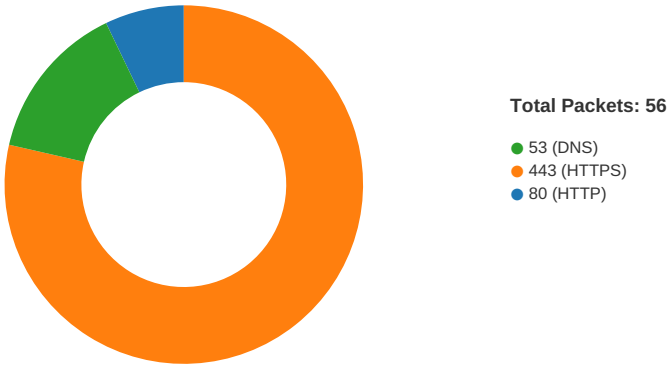
Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	001A47FFh								no

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 13:06:50.302928925 CET	49167	80	192.168.2.22	67.199.248.11
Feb 24, 2021 13:06:50.315180063 CET	80	49167	67.199.248.11	192.168.2.22
Feb 24, 2021 13:06:50.315296888 CET	49167	80	192.168.2.22	67.199.248.11
Feb 24, 2021 13:06:50.315624952 CET	49167	80	192.168.2.22	67.199.248.11
Feb 24, 2021 13:06:50.327708006 CET	80	49167	67.199.248.11	192.168.2.22
Feb 24, 2021 13:06:50.422799110 CET	80	49167	67.199.248.11	192.168.2.22
Feb 24, 2021 13:06:50.422919989 CET	49167	80	192.168.2.22	67.199.248.11
Feb 24, 2021 13:06:50.496206045 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:50.531502962 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:50.531634092 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:50.541237116 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:50.578671932 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:50.578704119 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:50.578797102 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:50.592158079 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:50.628480911 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:50.628570080 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.005666018 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.139710903 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.847400904 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.847433090 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.847618103 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.847687006 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.847713947 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.847758055 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.847774029 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.847784996 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.847820044 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.848287106 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.848365068 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.848552942 CET	443	49168	5.79.72.163	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 13:06:52.848614931 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.848623037 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.848666906 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.848833084 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.848856926 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.848906994 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.848911047 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.848978996 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.849313974 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.849390984 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.849493027 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.849565029 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.855420113 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.882944107 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.882980108 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.882997036 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.883011103 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.883027077 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.883121967 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.883284092 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.883326054 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.883354902 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.883378029 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.883398056 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.883415937 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.883425951 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.883449078 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.883467913 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.883522034 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.883725882 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.883748055 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.883776903 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.883791924 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.883889914 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.883954048 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.883956909 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.884004116 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.884007931 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.884049892 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.884109974 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.884141922 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.884159088 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.884188890 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.884274960 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.884299040 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.884325027 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.884341002 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.884404898 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.884459972 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.884481907 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.884540081 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.885004997 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.885207891 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.885236025 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.885276079 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.885294914 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.918937922 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.918989897 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.919028044 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.919066906 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.919104099 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.919142008 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.919189930 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.919209957 CET	49168	443	192.168.2.22	5.79.72.163

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 13:06:52.919233084 CET	443	49168	5.79.72.163	192.168.2.22
Feb 24, 2021 13:06:52.919253111 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.919260025 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.919265032 CET	49168	443	192.168.2.22	5.79.72.163
Feb 24, 2021 13:06:52.919271946 CET	49168	443	192.168.2.22	5.79.72.163

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 13:06:50.275626898 CET	52197	53	192.168.2.22	8.8.8.8
Feb 24, 2021 13:06:50.288167953 CET	53	52197	8.8.8.8	192.168.2.22
Feb 24, 2021 13:06:50.472788095 CET	53099	53	192.168.2.22	8.8.8.8
Feb 24, 2021 13:06:50.494493961 CET	53	53099	8.8.8.8	192.168.2.22
Feb 24, 2021 13:06:50.935065031 CET	52838	53	192.168.2.22	8.8.8.8
Feb 24, 2021 13:06:50.947669029 CET	53	52838	8.8.8.8	192.168.2.22
Feb 24, 2021 13:06:50.951725006 CET	61200	53	192.168.2.22	8.8.8.8
Feb 24, 2021 13:06:50.964308977 CET	53	61200	8.8.8.8	192.168.2.22
Feb 24, 2021 13:06:51.469333887 CET	49548	53	192.168.2.22	8.8.8.8
Feb 24, 2021 13:06:51.487565041 CET	53	49548	8.8.8.8	192.168.2.22
Feb 24, 2021 13:06:51.490777969 CET	55627	53	192.168.2.22	8.8.8.8
Feb 24, 2021 13:06:51.503056049 CET	53	55627	8.8.8.8	192.168.2.22
Feb 24, 2021 13:08:14.036895037 CET	56009	53	192.168.2.22	8.8.8.8
Feb 24, 2021 13:08:14.049120903 CET	53	56009	8.8.8.8	192.168.2.22
Feb 24, 2021 13:08:15.175936937 CET	61865	53	192.168.2.22	8.8.8.8
Feb 24, 2021 13:08:15.239042044 CET	53	61865	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 24, 2021 13:06:50.275626898 CET	192.168.2.22	8.8.8.8	0x26d4	Standard query (0)	bit.ly	A (IP address)	IN (0x0001)
Feb 24, 2021 13:06:50.472788095 CET	192.168.2.22	8.8.8.8	0x437e	Standard query (0)	u.teknik.io	A (IP address)	IN (0x0001)
Feb 24, 2021 13:08:14.036895037 CET	192.168.2.22	8.8.8.8	0x1e5e	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Feb 24, 2021 13:08:15.175936937 CET	192.168.2.22	8.8.8.8	0x60f4	Standard query (0)	cbzrfq.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
Feb 24, 2021 13:06:50.288167953 CET	8.8.8.8	192.168.2.22	0x26d4	No error (0)	bit.ly		67.199.248.11	A (IP address)	IN (0x0001)
Feb 24, 2021 13:06:50.288167953 CET	8.8.8.8	192.168.2.22	0x26d4	No error (0)	bit.ly		67.199.248.10	A (IP address)	IN (0x0001)
Feb 24, 2021 13:06:50.494493961 CET	8.8.8.8	192.168.2.22	0x437e	No error (0)	u.teknik.io	teknik.io		CNAME (Canonical name)	IN (0x0001)
Feb 24, 2021 13:06:50.494493961 CET	8.8.8.8	192.168.2.22	0x437e	No error (0)	teknik.io		5.79.72.163	A (IP address)	IN (0x0001)
Feb 24, 2021 13:08:14.049120903 CET	8.8.8.8	192.168.2.22	0x1e5e	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Feb 24, 2021 13:08:15.239042044 CET	8.8.8.8	192.168.2.22	0x60f4	No error (0)	cbzrfq.bl.files.1drv.com	bl-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Feb 24, 2021 13:08:15.239042044 CET	8.8.8.8	192.168.2.22	0x60f4	No error (0)	bl-files.fe.1drv.com	odc-bl-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- bit.ly

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	67.199.248.11	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 24, 2021 13:06:50.315624952 CET	0	OUT	GET /3qO7045 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: bit.ly Connection: Keep-Alive
Feb 24, 2021 13:06:50.422799110 CET	1	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Wed, 24 Feb 2021 12:06:50 GMT Content-Type: text/html; charset=utf-8 Content-Length: 116 Cache-Control: private, max-age=90 Location: https://u.teknik.io/PWua8.txt Set-Cookie: _bit=l1oc6O-1f1018e00109e7d832-00p; Domain=bit.ly; Expires=Mon, 23 Aug 2021 12:06:50 GMT Via: 1.1 google Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 42 69 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 75 2e 74 65 6b 6e 69 6b 2e 69 6f 2f 50 57 75 61 38 2e 74 78 74 22 3e 6d 6f 76 65 64 20 68 65 72 65 3c 2f 61 3e 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e Data Ascii: <html><head><title>Bitly</title></head><body>moved here</body></html>

Code Manipulations

Statistics

Behavior

- WINWORD.EXE
- EQNEDT32.EXE
- 69577.exe
- RegAsm.exe
- dw20.exe

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2276 Parent PID: 584

General

Start time:	13:06:36

Start date:	24/02/2021
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:	0x13f990000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE92726B4	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FEE963EB92	CreateFileW

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	unknown	2	ff fe	..	success or wait	1	7FEE963ECEB	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	7FEE963EC53	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	7FEE9646CAC	ReadFile
C:\Program Files\Microsoft Office\Office14\PROOF\MSSP7EN.dub	unknown	310	success or wait	1	7FEE8A7E8B7	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	unknown	1	end of file	1	7FEE963EC53	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	unknown	4096	success or wait	1	7FEE9646CAC	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	unknown	1	success or wait	1	7FEE8A70793	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	unknown	4096	success or wait	1	7FEE8ADAD58	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	7FEE8A70793	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	7FEE8ADAD58	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{9A867ADF-3614-4635-BFBB-6C9AC8D8FC42}.tmp	unknown	512	success or wait	1	7FEE9199AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{9A867ADF-3614-4635-BFBB-6C9AC8D8FC42}.tmp	unknown	512	success or wait	2751	7FEE9199AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE91AE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE91AE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE91AE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE9199AC0	unknown

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE9199AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE9199AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\FD79A	success or wait	1	7FEE9199AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\FD79A	FD79A	binary	04 00 00 00 E4 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 18 3B 5D 19 F1 0A D7 01 9A D7 0F 00 9A D7 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE9199AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF				

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1381498926	1381498927	success or wait	1	7FEE9199AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1381498927	1381498928	success or wait	1	7FEE9199AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\FD79A	FD79A	binary	04 00 00 00 E4 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 18 3B 5D 19 F1 0A D7 01 9A D7 0F 00 9A D7 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00 00 00 E4 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 9A D7 0F 00 9A D7 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE9199AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF				

Analysis Process: EQNEDT32.EXE PID: 2368 Parent PID: 584

General

Start time:	13:06:38
Start date:	24/02/2021
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options	success or wait	1	41369F	RegCreateKeyExA

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: 69577.exe PID: 2484 Parent PID: 2368

General

Start time:	13:06:41

Start date:	24/02/2021
Path:	C:\Users\Public\69577.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\69577.exe
Imagebase:	0x400000
File size:	131072 bytes
MD5 hash:	5D2D34449323C67BA1F5EC7561DF2204
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Antivirus matches:	• Detection: 12%, ReversingLabs
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RegAsm.exe PID: 2464 Parent PID: 2484

General

Start time:	13:07:56
Start date:	24/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\69577.exe
Imagebase:	0x1340000
File size:	53248 bytes
MD5 hash:	246BB0F8D68A463FD17C235DEB5491C0
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: 00000005.00000002.2355136875.000000001E5A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.2355136875.000000001E5A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 00000005.00000002.2351330528.0000000000092000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	94400	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	94400	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	94400	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	94400	InternetOpenUrlA
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	94400	InternetOpenUrlA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	94400	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	94400	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	94400	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	94400	InternetOpenUrlA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\JOHDAECH.txt	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	94400	InternetOpenUrlA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	73FFD6F0	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	73FFD6F0	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFD6F0	ReadFile

Registry Activities

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: dw20.exe PID: 2248 Parent PID: 2464

General

Start time:	13:08:11
Start date:	24/02/2021

Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
Wow64 process (32bit):	true
Commandline:	dw20.exe -x -s 1612
Imagebase:	0x10000000
File size:	33936 bytes
MD5 hash:	FBA78261A16C65FA44145613E3669E6E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis