ID: 358179
Sample Name:
QUOTATIONs44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCKs.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 07:28:29
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

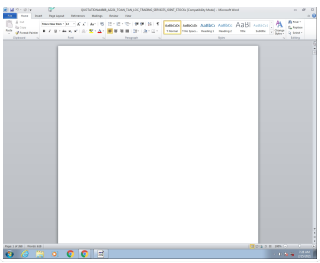
Analysis Report QUOTATIONs44888_A2221_TOAN_TAN…

Overview

General Information

Sample Name:	QUOTATIONs44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCKs.doc
Analysis ID:	358179
MD5:	bc1c94e783483f1..
SHA1:	7747c98d3d2da1..
SHA256:	d1e84cab5bf5ead.
Tags:	doc
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

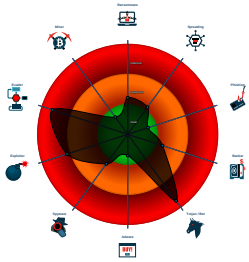
Nanocore GuLoader

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e.…
- Yara detected GuLoader
- Yara detected Nanocore RAT
- C2 URLs / IPs found in malware con…
- Connects to a URL shortener service
- Detected RDTSC dummy instruction

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 2200 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- EQNEDT32.EXE (PID: 2308 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - 69577.exe (PID: 2680 cmdline: C:\Users\Public\69577.exe MD5: A6AD1C3046A3CF0C6992507F2886AAB3)
    - RegAsm.exe (PID: 2916 cmdline: C:\Users\Public\69577.exe MD5: 246BB0F8D68A463FD17C235DEB5491C0)
    - RegAsm.exe (PID: 2488 cmdline: C:\Users\Public\69577.exe MD5: 246BB0F8D68A463FD17C235DEB5491C0)
      - schtasks.exe (PID: 3060 cmdline: 'schtasks.exe' /create /f /tn 'SMTP Service' /xml 'C:\Users\user\AppData\Local\Temp\tmp9445.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
      - schtasks.exe (PID: 2276 cmdline: 'schtasks.exe' /create /f /tn 'SMTP Service Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp80F5.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
- taskeng.exe (PID: 2272 cmdline: taskeng.exe {DA6299CA-95CA-4E9D-8945-2CC05321254C} S-1-5-21-966771315-3019405637-367336477-1006:user-PC\user:Interactive:[1] MD5: 65EA57712340C09B1B0C427B4848AE05)
  - RegAsm.exe (PID: 1904 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe 0 MD5: 246BB0F8D68A463FD17C235DEB5491C0)
  - smtpsvc.exe (PID: 2348 cmdline: 'C:\Program Files (x86)\SMTP Service\smtpsvc.exe' 0 MD5: 246BB0F8D68A463FD17C235DEB5491C0)
- filename1.exe (PID: 1552 cmdline: 'C:\Users\user\subfolder1\filename1.exe' MD5: A6AD1C3046A3CF0C6992507F2886AAB3)
- smtpsvc.exe (PID: 2560 cmdline: 'C:\Program Files (x86)\SMTP Service\smtpsvc.exe' MD5: 246BB0F8D68A463FD17C235DEB5491C0)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "92421eeb-c456-44c2-ab8d-5a66d7e5ab97",
  "Group": "Company",
  "Domain1": "194.5.98.202",
  "Domain2": "",
  "Port": 4488,
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.2371344330.000000000140000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
00000006.00000002.2371344330.000000000140000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
00000006.00000002.2371344330.000000000140000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000006.00000002.2371329317.000000000130000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000006.00000002.2371329317.000000000130000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost

Click to see the 5 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.RegAsm.exe.130000.1.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
6.2.RegAsm.exe.130000.1.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
6.2.RegAsm.exe.144629.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb184:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost
6.2.RegAsm.exe.144629.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xb184:$x2: NanoCore.ClientPluginHost • 0xc25f:$s4: PipeCreated • 0xb19e:$s5: IClientLoggingHost
6.2.RegAsm.exe.144629.2.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

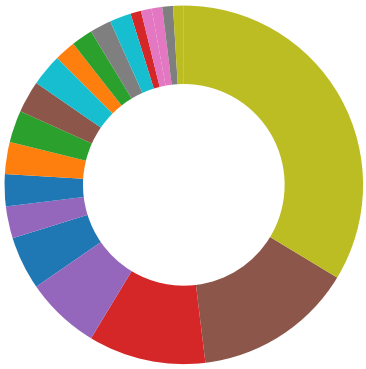
Source	Rule	Description	Author	Strings
Click to see the 20 entries				

Sigma Overview

System Summary:

- Sigma detected: Droppers Exploiting CVE-2017-11882
- Sigma detected: EQNEDT32.EXE connecting to internet
- Sigma detected: File Dropped By EQNEDT32EXE
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file as task from temp location
- Sigma detected: Executables Started in Suspicious Folder
- Sigma detected: Execution in Non-Executable Folder
- Sigma detected: Suspicious Program Location Process Starts

Signature Overview



- AV Detection
- Exploits
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- 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:

- Found malware configuration
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Yara detected Nanocore RAT

Exploits:

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

Compliance:

- Uses new MSVCR Dlls
- Binary contains paths to debug symbols

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

Connects to a URL shortener service

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

Data Obfuscation:

Yara detected GuLoader

Boot Survival:

Drops PE files to the user root directory

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

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect Any.run

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

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

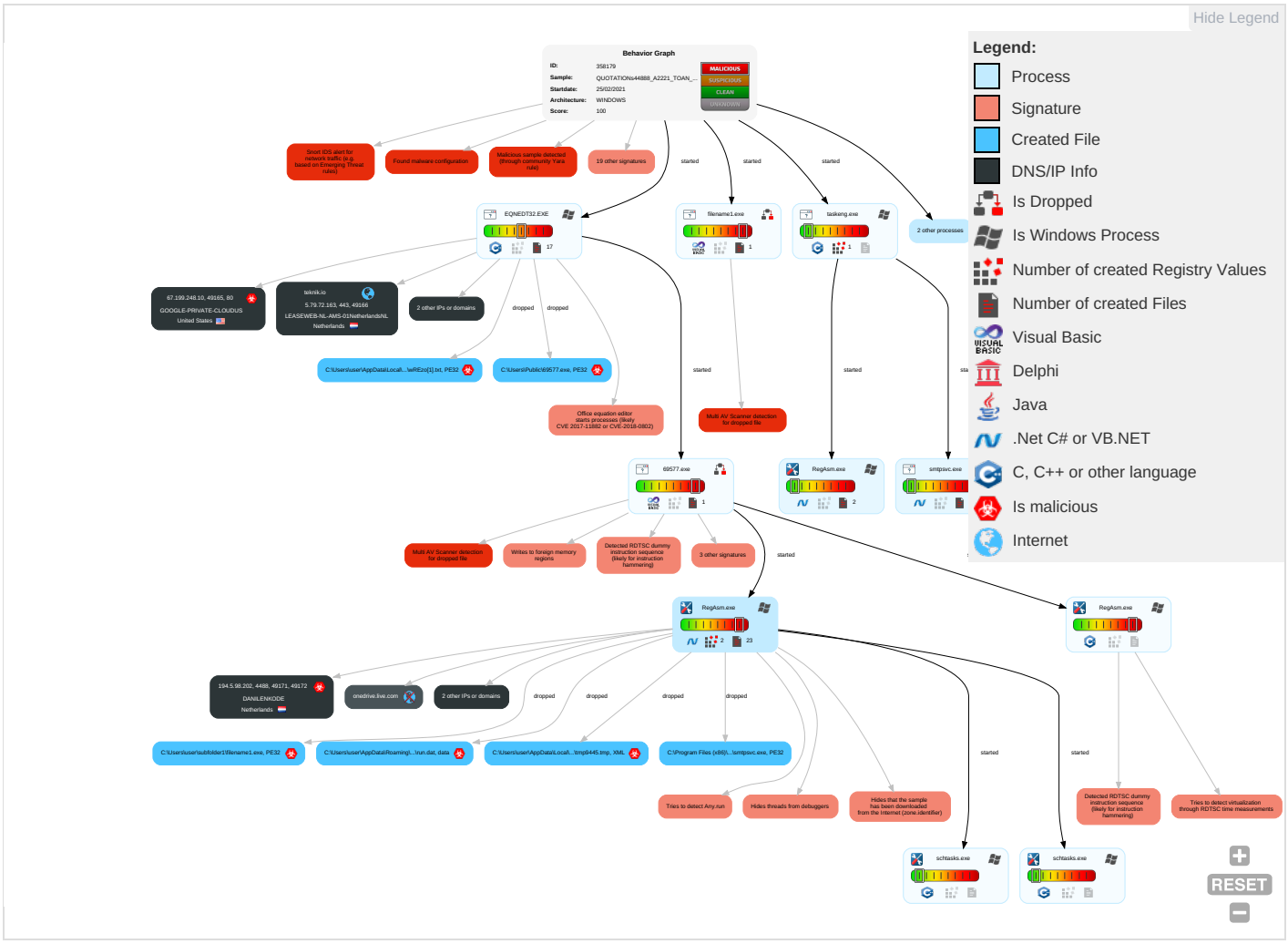
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Spearphishing Link 1	Exploitation for Client Execution 1 3	Scheduled Task/Job 1	Access Token Manipulation 1	Disable or Modify Tools 1 1	Input Capture 1 1	File and Directory Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 3
Default Accounts	Command and Scripting Interpreter 1	Registry Run Keys / Startup Folder 1	Process Injection 1 1 2	Obfuscated Files or Information 1	LSASS Memory	System Information Discovery 2 4	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Encrypted Channel 1 2
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Scheduled Task/Job 1	Software Packing 1	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Standard Port 1
Local Accounts	At (Windows)	Logon Script (Mac)	Registry Run Keys / Startup Folder 1	Masquerading 1 2 2	NTDS	Security Software Discovery 6 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Remote Access Software 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 2 3	LSA Secrets	Virtualization/Sandbox Evasion 2 3	SSH	Keylogging	Data Transfer Size Limits	Non-Application Layer Protocol 2
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Access Token Manipulation 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Application Laye Protocol 1 1 3
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Laye Protocol

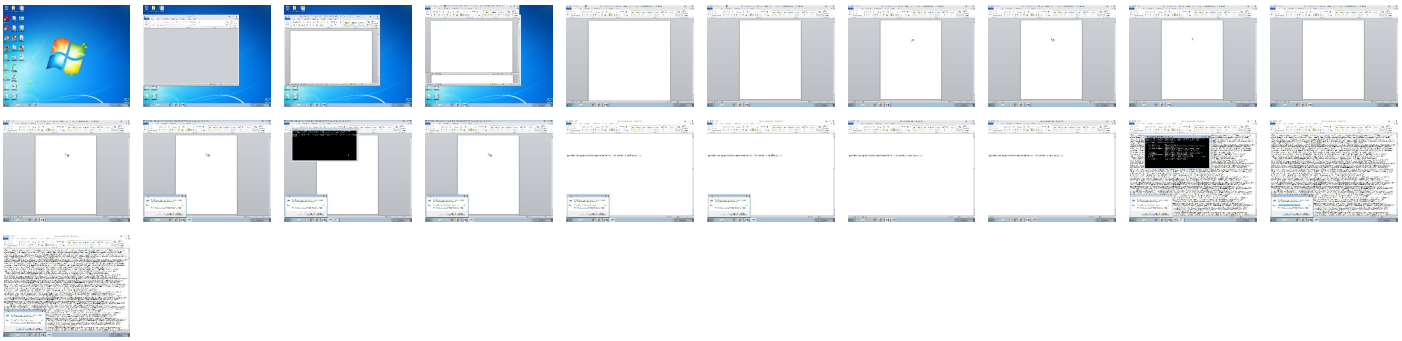
Behavior Graph

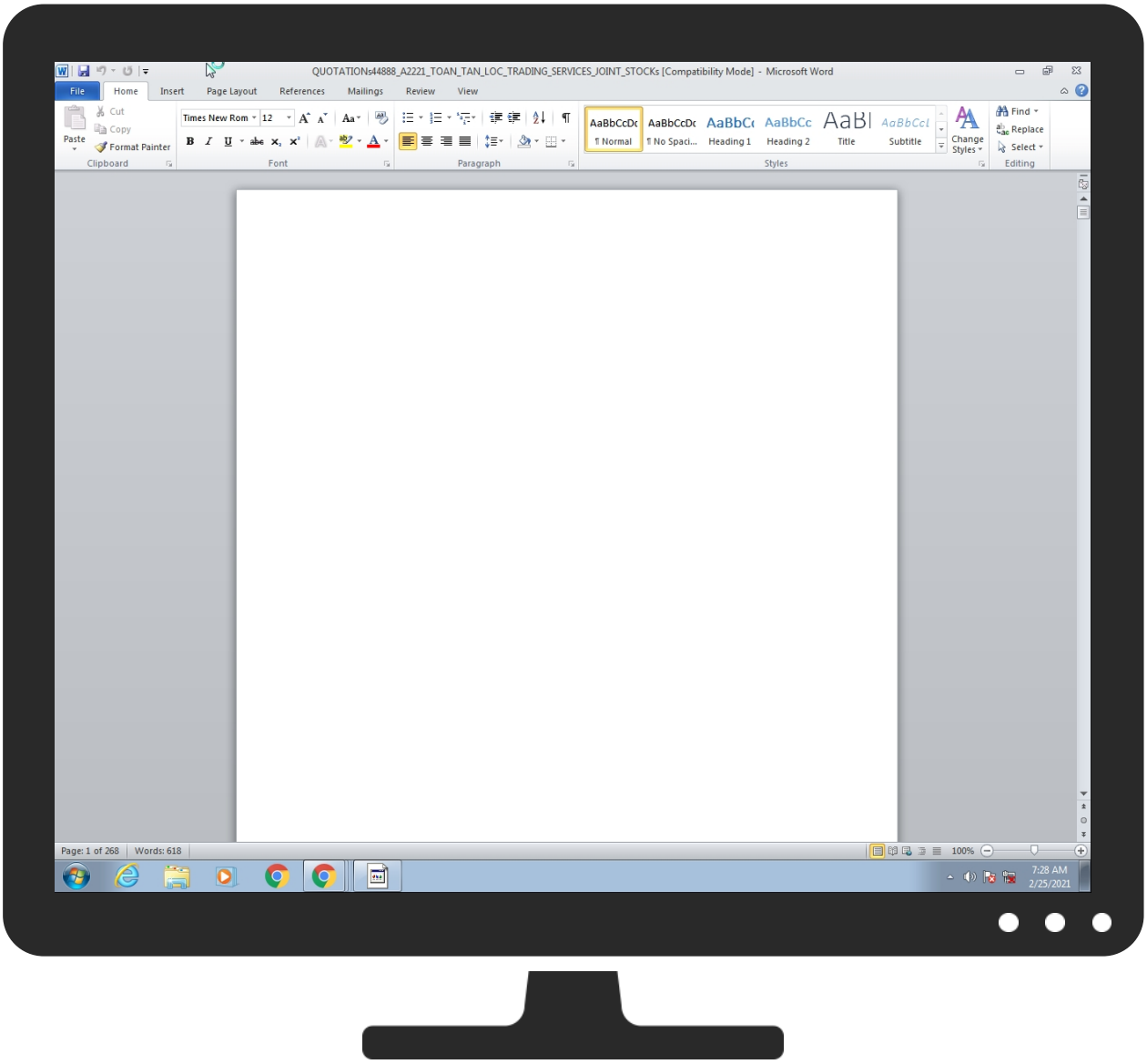


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
QUOTATIONs44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCKs.doc	39%	Virustotal		Browse
QUOTATIONs44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCKs.doc	25%	ReversingLabs	Document-RTF.Exploit.MathType	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	0%	Virustotal		Browse
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	0%	Metadefender		Browse
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JW C\wREzo[1].txt	42%	Virustotal		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JW C\wREzo[1].txt	28%	ReversingLabs	Win32.Trojan.Guloader	
C:\Users\user\subfolder1\filename1.exe	28%	ReversingLabs	Win32.Trojan.Guloader	
C:\Users\Public\69577.exe	28%	ReversingLabs	Win32.Trojan.Guloader	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.RegAsm.exe.140000.3.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://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	
194.5.98.202	0%	Virustotal		Browse
194.5.98.202	0%	Avira URL Cloud	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
bit.ly	67.199.248.11	true	false		high
teknik.io	5.79.72.163	true	false		high
onedrive.live.com	unknown	unknown	false		high
ibkebw.dm.files.1drv.com	unknown	unknown	false		high
u.teknik.io	unknown	unknown	false		high

Contacted URLs

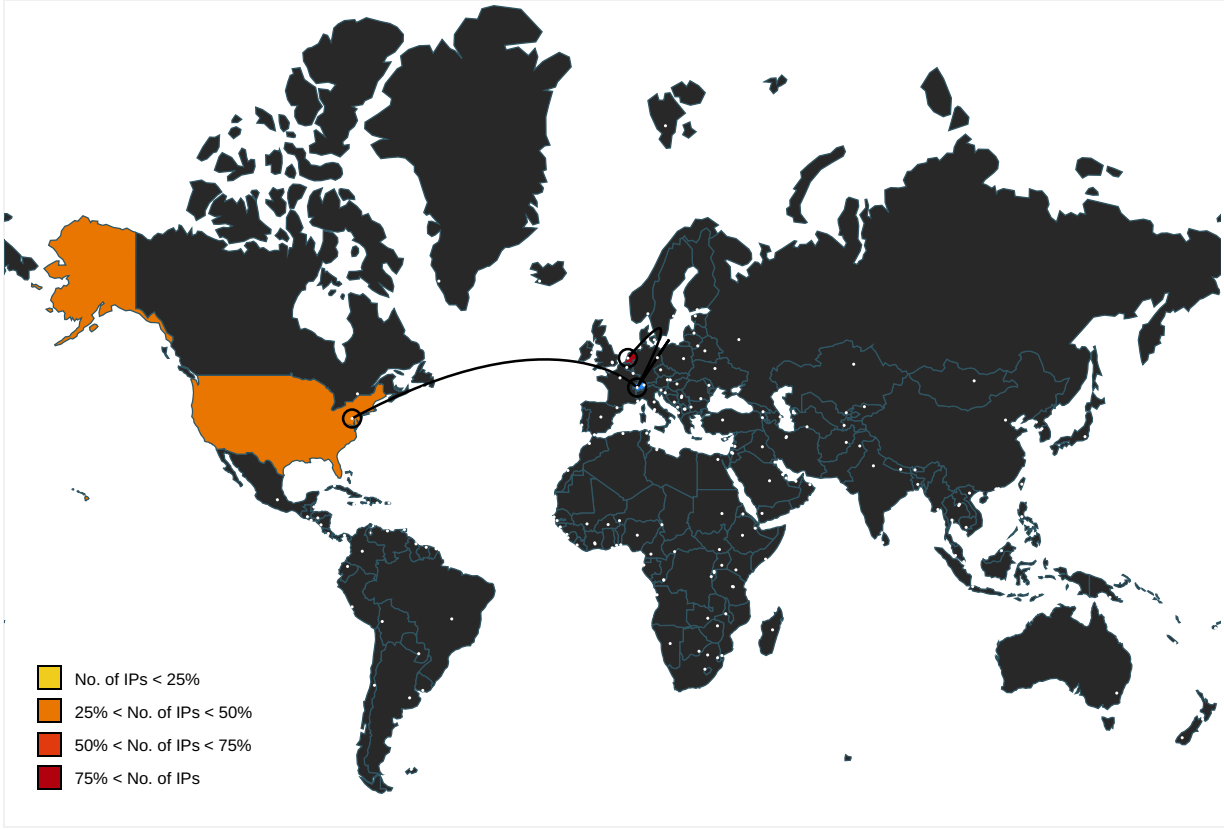
Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
194.5.98.202	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://bit.ly/2ZKf4aq	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	RegAsm.exe, 00000006.00000002.2372026516.00000000008CC000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	RegAsm.exe, 00000006.00000002.2372610828.0000000002790000.00000002.00000001.sdmp, taskeng.exe, 0000000C.00000002.2371587310.0000000001BE0000.00000002.00000001.sdmp, RegAsm.exe, 00000000F.00000002.2323283664.0000000002500000.00000002.00000001.sdmp	false		high
http://crl.entrust.net/server1.crl0	RegAsm.exe, 00000006.00000002.2372026516.00000000008CC000.00000004.00000020.sdmp	false		high
http://ocsp.entrust.net03	RegAsm.exe, 00000006.00000002.2372026516.00000000008CC000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/E	RegAsm.exe, 00000006.00000002.2371947778.000000000085A000.00000004.00000020.sdmp	false		high
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	RegAsm.exe, 00000006.00000002.2372026516.00000000008CC000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	RegAsm.exe, 00000006.00000002.2372610828.0000000002790000.00000002.00000001.sdmp, taskeng.exe, 0000000C.00000002.2371587310.0000000001BE0000.00000002.00000001.sdmp, RegAsm.exe, 00000000F.00000002.2323283664.0000000002500000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.diginotar.nl/cps/pkioverheid0	RegAsm.exe, 00000006.00000002.2372026516.00000000008CC000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://u.teknik.io/wREzo.txt	2ZKf4aq[1].htm.2.dr	false		high
http://https://ibkebw.dm.files.1drv.com/y	RegAsm.exe, 00000006.00000002.2382485610.000000001DC80000.00000004.00000001.sdmp	false		high
http://ocsp.entrust.net0D	RegAsm.exe, 00000006.00000002.2372026516.00000000008CC000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ibkebw.dm.files.1drv.com/	RegAsm.exe, 00000006.00000002.2371947778.000000000085A000.00000004.00000020.sdmp	false		high
http://https://secure.comodo.com/CPS0	RegAsm.exe, 00000006.00000002.2372026516.00000000008CC000.00000004.00000020.sdmp	false		high
http://https://onedrive.live.com/download?cid=802AC8A73EEC8C8E&resid=802AC8A73EEC8C8E%21110&authkey=AK1w6-P	RegAsm.exe, RegAsm.exe, 00000006.00000002.2371992276.000000000089A000.00000004.00000020.sdmp	false		high
http://crl.entrust.net/2048ca.crl0	RegAsm.exe, 00000006.00000002.2372026516.00000000008CC000.00000004.00000020.sdmp	false		high
http://https://ibkebw.dm.files.1drv.com/y4mkt1ePYl5p-A97ciot0bQ59hcBfLkczVR077g5LVTnsSoRxe1bs39ErOjDRD_qmHQ	RegAsm.exe, 00000006.00000002.2371992276.000000000089A000.00000004.00000020.sdmp, RegAsm.exe, 00000006.00000002.2382485610.000000001DC80000.00000004.00000001.sdmp	false		high
http://https://onedrive.live.com/	RegAsm.exe, 00000006.00000002.2371947778.000000000085A000.00000004.00000020.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
67.199.248.10	unknown	United States		396982	GOOGLE-PRIVATE-CLOUDUS	true
5.79.72.163	unknown	Netherlands		60781	LEASEWEB-NL-AMS-01NetherlandsNL	false
194.5.98.202	unknown	Netherlands		208476	DANILENKODE	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358179
Start date:	25.02.2021
Start time:	07:28:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	QUOTATIONs44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCKs.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:	22
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.expl.evad.winDOC@19/25@6/3
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 192.35.177.64, 2.20.142.209, 2.20.142.210, 13.107.42.13, 13.107.42.12 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, odc-web-brs.onedrive.akadns.net, odc-dm-files-geo.onedrive.akadns.net, odc-dm-files-brs.onedrive.akadns.net, odc-web-geo.onedrive.akadns.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, l-0004.l-msedge.net, odwebpl.trafficmanager.net.l-0004.dc-msedge.net.l-0004.l-msedge.net, odc-dm-files.onedrive.akadns.net.l-0003.dc-msedge.net.l-0003.l-msedge.net, l-0003.l-msedge.net, audownload.windowsupdate.nsatc.net, apps.digsigtrust.com, apps.identrust.com, au-bg-shim.trafficmanager.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 NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
07:28:32	API Interceptor	46x Sleep call for process: EQNEDT32.EXE modified
07:30:17	API Interceptor	77x Sleep call for process: 69577.exe modified
07:30:25	API Interceptor	570x Sleep call for process: RegAsm.exe modified
07:30:28	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce Startup key C:\Users\user\subfolder1\filename1.exe
07:30:29	Task Scheduler	Run new task: SMTP Service path: "C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe" s>$(Arg0)
07:30:29	API Interceptor	2x Sleep call for process: schtasks.exe modified
07:30:29	API Interceptor	189x Sleep call for process: taskeng.exe modified
07:30:31	Task Scheduler	Run new task: SMTP Service Task path: "C:\Program Files (x86)\SMTP Service\smtpsvc.exe" s>$(Arg0)
07:30:36	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run SMTP Service C:\Program Files (x86)\SMTP Service\smtpsvc.exe
07:30:45	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce Startup key C:\Users\user\subfolder1\filename1.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
67.199.248.10	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• bit.ly/3aLCPVF
	PO AAN2102002-V020.doc	Get hash	malicious	Browse	• bit.ly/3pNzHgj
	PO55004.doc	Get hash	malicious	Browse	• bit.ly/3kioaoe
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• bit.ly/2NUvTNf
	RFQ Document.doc	Get hash	malicious	Browse	• bit.ly/3qOyCWN
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909_RAW.doc	Get hash	malicious	Browse	• bit.ly/3qN5fEA
	Order.doc	Get hash	malicious	Browse	• bit.ly/3boWBW4
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• bit.ly/2NScGvD
	IMG_57109_Scanned.doc	Get hash	malicious	Browse	• bit.ly/3kemdsK
	Deadly Variants of Covid 19.doc	Get hash	malicious	Browse	• bit.ly/2Me6ei3
	swift payment.doc	Get hash	malicious	Browse	• bit.ly/2NmOCRI
	IMG_6078_SCANNED.doc	Get hash	malicious	Browse	• bit.ly/3qIRVRz
	IMG_01670_Scanned.doc	Get hash	malicious	Browse	• bit.ly/3duA4tQ
	IMG_7742_Scanned.doc	Get hash	malicious	Browse	• bit.ly/3sdTreK
	QUOTATION44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCK.doc	Get hash	malicious	Browse	• bit.ly/3dCBRgm
	DHL Shipment Notification 7465649870.doc	Get hash	malicious	Browse	• bit.ly/3bhrITG
	Quote QU038097.doc	Get hash	malicious	Browse	• bit.ly/3aom5Uu
	IMG_51067.doc__.rtf	Get hash	malicious	Browse	• bit.ly/3djdyUC
	IMG_123773.doc	Get hash	malicious	Browse	• bit.ly/2Nsv9ym
	B62672021 PRETORIA.doc	Get hash	malicious	Browse	• bit.ly/3jOWhDW

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
bit.ly	CsmBq6KLHu.doc	Get hash	malicious	Browse	• 67.199.248.11
	purchase order_2242021.doc	Get hash	malicious	Browse	• 67.199.248.11
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909yy.doc	Get hash	malicious	Browse	• 67.199.248.11
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 67.199.248.10
	PO AAN2102002-V020.doc	Get hash	malicious	Browse	• 67.199.248.11
	PO55004.doc	Get hash	malicious	Browse	• 67.199.248.10
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 67.199.248.10
	RFQ Document.doc	Get hash	malicious	Browse	• 67.199.248.10
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909_RAW.doc	Get hash	malicious	Browse	• 67.199.248.10
	Order.doc	Get hash	malicious	Browse	• 67.199.248.10
	QUOTE.doc	Get hash	malicious	Browse	• 67.199.248.11
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_57109_Scanned.doc	Get hash	malicious	Browse	• 67.199.248.10
	Deadly Variants of Covid 19.doc	Get hash	malicious	Browse	• 67.199.248.10
	swift payment.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_61061_SCANNED.doc	Get hash	malicious	Browse	• 67.199.248.11
	IMG_6078_SCANNED.doc	Get hash	malicious	Browse	• 67.199.248.11
	IMG_01670_Scanned.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_7742_Scanned.doc	Get hash	malicious	Browse	• 67.199.248.10
	SWIFT Payment W0301.doc	Get hash	malicious	Browse	• 67.199.248.11

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LEASEWEB-NL-AMS-01NetherlandsNL	purchase order_2242021.doc	Get hash	malicious	Browse	• 5.79.72.163
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909yy.doc	Get hash	malicious	Browse	• 5.79.72.163
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 5.79.72.163

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO AAN2102002-V020.doc	Get hash	malicious	Browse	• 5.79.72.163
	PO55004.doc	Get hash	malicious	Browse	• 5.79.72.163
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 5.79.72.163
	RFQ Document.doc	Get hash	malicious	Browse	• 5.79.72.163
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909_RAW.doc	Get hash	malicious	Browse	• 5.79.72.163
	SecuriteInfo.com.Trojan.PackedNET.540.1271.exe	Get hash	malicious	Browse	• 213.227.154.188
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 5.79.72.163
	MV9tCJw8Xr.exe	Get hash	malicious	Browse	• 5.79.70.250
	QUOTATION44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCK.doc	Get hash	malicious	Browse	• 5.79.72.163
	Quotation408S_A02021_AHYAN_group_of_companies.doc	Get hash	malicious	Browse	• 5.79.72.163
	Request For Quotation.PDF.exe	Get hash	malicious	Browse	• 212.32.237.101
	PO#652.exe	Get hash	malicious	Browse	• 5.79.87.207
	Parcel _009887 .exe	Get hash	malicious	Browse	• 212.32.237.92
	PO 20211602.xlsm	Get hash	malicious	Browse	• 82.192.82.225
	6d0000.exe	Get hash	malicious	Browse	• 213.227.133.129
	SecuriteInfo.com.Trojan.PackedNET.541.9005.exe	Get hash	malicious	Browse	• 62.212.86.139
	New Order 83329 PDF.exe	Get hash	malicious	Browse	• 95.211.208.58
GOOGLE-PRIVATE-CLOUDUS	CsmBq6KLHu.doc	Get hash	malicious	Browse	• 67.199.248.11
	Details van vereiste.pps	Get hash	malicious	Browse	• 67.199.248.16
	purchase order_2242021.doc	Get hash	malicious	Browse	• 67.199.248.11
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909yy.doc	Get hash	malicious	Browse	• 67.199.248.11
	Offerte aanvragen 22-02-2021.ppt	Get hash	malicious	Browse	• 67.199.248.16
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 67.199.248.10
	PO AAN2102002-V020.doc	Get hash	malicious	Browse	• 67.199.248.10
	PO55004.doc	Get hash	malicious	Browse	• 67.199.248.10
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 67.199.248.10
	RFQ Document.doc	Get hash	malicious	Browse	• 67.199.248.10
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909_RAW.doc	Get hash	malicious	Browse	• 67.199.248.10
	Order.doc	Get hash	malicious	Browse	• 67.199.248.10
	QUOTE.doc	Get hash	malicious	Browse	• 67.199.248.11
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_57109_Scanned.doc	Get hash	malicious	Browse	• 67.199.248.10
	Deadly Variants of Covid 19.doc	Get hash	malicious	Browse	• 67.199.248.10
	swift payment.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_61061_SCANNED.doc	Get hash	malicious	Browse	• 67.199.248.11
	IMG_6078_SCANNED.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_01670_Scanned.doc	Get hash	malicious	Browse	• 67.199.248.10
DANILENKODE	swift006.pdf.exe	Get hash	malicious	Browse	• 194.5.97.116
	neue bestellung.PDF.exe	Get hash	malicious	Browse	• 194.5.97.48
	m72OvSF7e5.exe	Get hash	malicious	Browse	• 194.5.98.202
	neue bestellung.PDF.exe	Get hash	malicious	Browse	• 194.5.97.48
	Eingang.Jpg.exe	Get hash	malicious	Browse	• 194.5.97.116
	V33QokMrIv.exe	Get hash	malicious	Browse	• 194.5.98.202
	3Fv4j323nj.exe	Get hash	malicious	Browse	• 194.5.98.182
	scan09e8902093922023ce.exe	Get hash	malicious	Browse	• 194.5.98.46
	PO AAN2102002-V020.doc	Get hash	malicious	Browse	• 194.5.98.182
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909_RAW.doc	Get hash	malicious	Browse	• 194.5.98.202
	neue bestellung.PDF.exe	Get hash	malicious	Browse	• 194.5.97.48
	Orderoffer.exe	Get hash	malicious	Browse	• 194.5.98.66
	neue bestellung.PDF.exe	Get hash	malicious	Browse	• 194.5.97.48
	OrderSuppliesQuote0817916.exe	Get hash	malicious	Browse	• 194.5.97.248
	DHL_6368638172 documento de recibo,pdf.exe	Get hash	malicious	Browse	• 194.5.97.244
	QuotationInvoices.exe	Get hash	malicious	Browse	• 194.5.97.248
	PAYMENT_.EXE	Get hash	malicious	Browse	• 194.5.98.211
	payment.exe	Get hash	malicious	Browse	• 194.5.98.66

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RFQ_1101983736366355 1101938377388.exe	Get hash	malicious	Browse	• 194.5.98.21
	Slip copy .xls.exe	Get hash	malicious	Browse	• 194.5.97.116

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	PO AAN2102002-V020.doc	Get hash	malicious	Browse	
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909_RAW.doc	Get hash	malicious	Browse	
	RFQ # TSI2202708.doc	Get hash	malicious	Browse	
	rfq_20712557-20200308 Order.doc	Get hash	malicious	Browse	
	31RFQ 49177 PO-DM-11-2018-109159.exe	Get hash	malicious	Browse	
	69shipment Details...exe	Get hash	malicious	Browse	
	64RFQ#4500052988_AHBGroup_01734221347210 3_20181024.exe	Get hash	malicious	Browse	
	22RFQ#4500052988_AHBGroup_01734221347210 3_20181024.exe	Get hash	malicious	Browse	
	41COSCO TBN FULLY SIGNED CPFN.exe	Get hash	malicious	Browse	
	19Request for Quote_Goedeker_6397_3 01-2_12137018.exe	Get hash	malicious	Browse	
	72Payment....exe	Get hash	malicious	Browse	
	832238740303837363.exe	Get hash	malicious	Browse	
	35Request for Quote_SOSi_6397_3 01-2_12137018.exe	Get hash	malicious	Browse	
	61Request for Quote_SOSi_6397_3 01-2_12137018.exe	Get hash	malicious	Browse	
	17Request for Quote_SOSi_6397_3 01-2_12137018.exe	Get hash	malicious	Browse	
	59Doc_RFQ Roccia s.r.l. 180001899918 & 500037221 (1).exe	Get hash	malicious	Browse	
	71RFQ Ganix Global-180001899918 & 500037221.exe	Get hash	malicious	Browse	
	81PAYMENT.exe	Get hash	malicious	Browse	
	59Doc_RFQ Roccia s.r.l. 180001899918 & 500037221.exe	Get hash	malicious	Browse	
	2810010518.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Program Files (x86)\SMTP Service\smtpsvc.exe

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	53248
Entropy (8bit):	4.48905382202799
Encrypted:	false
SSDEEP:	768:GP2Bbv+VazyoD2z9TU//1mz1+M9GnLEu+2hhFRJS8AW:tJv46yoD2BTNz1+M9GLfvw8AW
MD5:	246BB0F8D68A463FD17C235DEB5491C0
SHA1:	63F237F94EAB14CB4DCA7ACB5817644D4428873A
SHA-256:	32B60D7BBA22CC1682F4BA651D86C9FB357BDC82E9A284AB9668E5446BD24BB3
SHA-512:	187D08DF6563739A3A537439F313D9F4D53001FA8A9CD146986DAB3C1168E25E210771AFC2A7D6C2A88EB44F0EEF2E91DDCEA8ABD86742AD0E6D78F07BDF796
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Program Files (x86)\SMTP Service\smtpsvc.exe	
Joe Sandbox View:	• Filename: PO AAN2102002-V020.doc, Detection: malicious, Browse • Filename: DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909_RAW.doc, Detection: malicious, Browse • Filename: RFQ # TSI2202708.doc, Detection: malicious, Browse • Filename: rfq_20712557-20200308 Order.doc, Detection: malicious, Browse • Filename: 31RFQ 49177 PO-DM-11-2018-109159.exe, Detection: malicious, Browse • Filename: 69shipment Details...exe, Detection: malicious, Browse • Filename: 64RFQ#4500052988_AHBGroup_017342213472103_20181024.exe, Detection: malicious, Browse • Filename: 22RFQ#4500052988_AHBGroup_017342213472103_20181024.exe, Detection: malicious, Browse • Filename: 41COSCO TBN FULLY SIGNED CPFN.exe, Detection: malicious, Browse • Filename: 19Request for Quote_Goedeker_6397_3 01-2_12137018.exe, Detection: malicious, Browse • Filename: 72Payment....exe, Detection: malicious, Browse • Filename: 832238740303837363.exe, Detection: malicious, Browse • Filename: 35Request for Quote_SOSi_6397_3 01-2_12137018.exe, Detection: malicious, Browse • Filename: 61Request for Quote_SOSi_6397_3 01-2_12137018.exe, Detection: malicious, Browse • Filename: 17Request for Quote_SOSi_6397_3 01-2_12137018.exe, Detection: malicious, Browse • Filename: 59Doc_RFQ Roccia s.r.l. 180001899918 & 500037221 (1).exe, Detection: malicious, Browse • Filename: 71RFQ Ganix Global-180001899918 & 500037221.exe, Detection: malicious, Browse • Filename: 81PAYMENT.exe, Detection: malicious, Browse • Filename: 59Doc_RFQ Roccia s.r.l. 180001899918 & 500037221.exe, Detection: malicious, Browse • Filename: 2810010518.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...,..S..... ....@.. ..... .@.....O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B..... .....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8eflqigYDff:RN7MlanAQwElztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
Reputation:	high, very likely benign file
Preview:	MSCF.....,.....I.....T.....R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.....\|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n-.....D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay.....n/R... ._.+..<...Am.t.<. ..V..y`.yO..e@../...<#..#.....dju*..B.....8..H'..Ir.....I.I6/..d.].xIX<...&U...GD..Mn.y&.[<(tk.....%B.b;/..`.#h....C.P...B..8d.F...D.k..... 0..w...@(.. @K....?.)ce.....\.\.....I.....Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a..,...E5X..i.d..w.....#o*+.....X.P...k...V.$...X.r.e....9E.x..=\...Km.....B...Ep...xl@@c1.....p?...d.{EYN.K.X>D3..Z..q.] .Mq.....L.n}.....+/l\.cDB0.'.Y...r.[.....vM...o.=....zK..r..I..>B....U..3....Z...ZjS...wZ.M...IW;..e.L...zC.wBtQ..&.Z.Fv+..G9.8..!..\T:K`.....m.....9T.u..3h.....{...d[...@...Q.?..p.e.t[.%7.....^.....s.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	data
Category:	dropped
Size (bytes):	893
Entropy (8bit):	7.366016576663508
Encrypted:	false
SSDEEP:	24:hBntmDvKUQQDvKUr7C5fpqp8gPvXHmXvponXux:3ntmD5QQD5XC5RqHHXmXvp++x
MD5:	D4AE187B4574036C2D76B6DF8A8C1A30
SHA1:	B06F409FA14BAB33CBAF4A37811B8740B624D9E5
SHA-256:	A2CE3A0FA7D2A833D1801E01EC48E35B70D84F3467CC9F8FAB370386E13879C7
SHA-512:	1F44A360E8BB8ADA22BC5BFE001F1BABB4E72005A46BC2A94C33C4BD149FF256CCE6F35D65CA4F7FC2A5B9E15494155449830D2809C8CF218D0B9196EC646BC
Malicious:	false
Reputation:	high, very likely benign file
Preview:	0..y..*.H.....j0..f...1.0...*.H.....N0..J0..2.....D....'..09...@k0...*.H.....0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30...000930211219Z..210930140115Z0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30.."0...*.H.....0.....P..W..be.....,k0.[...}.@.....3vl*.?!I..N..>H.e...!.e.*.2....w..{.....s.z..2..~..0....*8.y.1.P..e.Qc...a.Ka..Rk...K.(.H.....>.... .[.*....p....%.tr.{j.4.0...h.{T....Z...=d.....Ap..r.&.8U9C....\@.....%.....:..n.>..\..<.i....*.)W..=....]......B0@0...U.....0....0...U.....0...U.....{,q...K.u...`...0...*.H.....,...\...(f7:...?K.... ]..YD.>.>..K.t.....t..~.....K. D....}..j.....N..:.pI.....:^H...X._..Z.....Y..n.....f3.Y[...sG.+..7H..VK....r2...D.SrmC.&H.Rg.X..gvqx...V..9$1....Z0G..P.....dc`.....}...=2.e..|.Wv..(9..e...w.j..w.....)...55.1.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	data
Category:	dropped

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Size (bytes):	328
Entropy (8bit):	3.080958610796429
Encrypted:	false
SSDEEP:	6:kKLKEbqoN+SkQlPlEGYRMY9z+4KlDA3RUeKlF+adAlf:jM3kPlE99SNxAhUeo+aKt
MD5:	AD9008ACF5082FA8EB71D2E8C5BD9B96
SHA1:	11394AD7642601A83B356A265AC805C5E28A27AC
SHA-256:	4EE9FB4CE3E871D63A19C36B13F3AD281EB17EEAE99A9C13EC45CCC220B6DBCB
SHA-512:	B44C0F7E414E3405AA0DF081E723086E5FB08A622DF2BCDCEEBCC19C77C97D3946A7FB7D7EC34DF1DED51A28EDDA3432B2D206053A89BF5E5431E29974642E12
Malicious:	false
Preview:	p..... .....b.....(..... .....&.....h.t.t.p.:./.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.e.b.b.a.e.1.d.7.e.a.d.6.1.:.0."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	3.0294634724686764
Encrypted:	false
SSDEEP:	3:kkFklA9M1fllXlE/QhzllPlzRkwWBARLNDU+ZMlKlBkvclcMlVHblB1UAYpFit:kK5QliBAIdQZV7eAYLit
MD5:	030E777529B43E0D9FED41EFFE564B26
SHA1:	80E57C39FC84DC03AFC464FF6E0E9D66239F1BD3
SHA-256:	88ABA1A4879A359E121690E3BBC990017F6C45ABBA1EB0FDAF3DFAAD07A5BE61
SHA-512:	75E8FEA934E26617B9E933794507CF9FA2ADD1AFF10000D35652F468742F4B4AE2B33A1447138A70BA9F9045F84C31E63E38D59CDAC4BB2B9C0C80FFEC12BB2C
Malicious:	false
Preview:	p..... ....`....SJ.....(..... .....u.....(.....}...h.t.t.p.:./.a.p.p.s...i.d.e.n.t.r.u.s.t...c.o.m./.r.o.o.t.s./.d.s.t.r.o.o.t.c.a.x.3...p.7.c...".3.7.d.-.5.9.e.7.6.b.3.c.6.4.b.c.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\wREzo[1].txt	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	131072
Entropy (8bit):	4.856871861209239
Encrypted:	false
SSDEEP:	3072:6wVUP1A3a64iOR/VfgmLQPDBZByQqFXrMQqwV:6wVUPH6GfgmLQPDBZByQqFXIQqwV
MD5:	A6AD1C3046A3CF0C6992507F2886AAB3
SHA1:	8024E4315C4BD196F1531E08C541359DBAC70A39
SHA-256:	CEF944407A26C3C148AFBF8253BAA55AEE7CDFAEC17B5A158831574245BAC8AD
SHA-512:	A5C0796BCCE3CEDE14CC02915A4A0A55AEEAFD0B0675AF8FE395905F9ED78A58CBDCED5EE89CFBDD7E55B90A5AED2D647C76EE3BB9DD35E778DA1968076F21A
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 42%, Browse • Antivirus: ReversingLabs, Detection: 28%
IE Cache URL:	http://https://u.teknik.io/wREzo.txt
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1...1...1.....0...~..0.....0...Rich1.....PE..L.....Y.....P.....`....@.....tY..(....p.....(... .....text....M.....P.....`.data.....`.....`.....@....rsrc.....p.....p.....@..@...I.....MSVBVM60.DLL.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\2ZKf4aq[1].htm	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	116
Entropy (8bit):	4.572661742712173
Encrypted:	false
SSDEEP:	3:qVvzLURODccZ/vXbvx9nDyZHL+E8IkFSXbKFvNGb:qFzLIeco3XLx92ZHqHIMSLWQb
MD5:	64D298FA5892D258CB4465CD14478454
SHA1:	0BBAEB8DBA81A7861C1AAFBAB629538937594658
SHA-256:	89007ADC49FABF9602747C7FA654CC9174D9FE25FD1CBF9DBA800329AAEBF36B
SHA-512:	C717A6A0C3811DC77B485D9D70159EE277970D213F456BC6F79FA0910E249BEC845E61CA24B6F48A73EEE15130743C27781A35610C945018BBC9B81BC9A1AC4

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\2ZKf4aq[1].htm	
Malicious:	false
Preview:	<html>.<head><title>Bitly</title></head>.<body>moved here</body>.</html>

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{0863C5D3-5908-4917-8F28-8909E0160183}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1834894
Entropy (8bit):	4.020416000417094
Encrypted:	false
SSDEEP:	12288:DoINuEINuEINuEINuVINuEwNuEINueINuEINuEINuEINtEINuEINuEINuEIX:k
MD5:	BCAEE394FB7661B22A808356CABD3615
SHA1:	E9252AC0D9998D3E8EAB95CF0153A29852A756A4
SHA-256:	1D0BF7198BD288E1276088B92D41C342A575DA7C2AB9085BF47A3A5C6843D175
SHA-512:	84EF925747D34DFEDFCE70B97A2FE525FBF5FD844B3368395FE9773E282AB561ACAA755D519ACE34A3CDDD402FD29B6696CCD161C6869573FB7BCF5A1AE1A(E6
Malicious:	false
Preview:	..@.m.4.2.J.E.U.a.4.S.r.c.I.Z.j.j.E.@.-.K.I.2.W.T.Y.r.C.C.I.Y.w.a.u.Z.0.C.<.e.h.&.&.7._.M.-.C._.D.-.-._.-.V.,.6.4.>.8.8.9.6.4.$.C.v.>.y.t.=.n.6.|.:.%._.>.j.n.8.%.b.m.;.=.u...1.4..... . . . .

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{24864F90-30CA-4646-ACFF-79FC9E14ADCB}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28B A4
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{C2D3EB9C-AB70-4784-8852-5C03B64EE05D}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3568273340340575
Encrypted:	false
SSDEEP:	3:liiiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlbQ:liiiiiiiiifdLloZQc8++lsJe1Mzb
MD5:	C990C02C26800951CBF8B0581C7AAC39
SHA1:	9768AA8776819BD7E836740634B596D46FFA8303
SHA-256:	0DDDB3264217F403F4D0D5791562DDA835E42E9592B1BCE42E6F1076F31F7AC3
SHA-512:	CC236BE11D2BAB46160A6AE3C01168B6B92A2DD5A77E027D561E00B5A5A617045008E975C6E54D73D3E6BFF5B7B499AFD560FDEFCA7B1FBCCBFB95436BE02 B2
Malicious:	false
Preview:	..(...(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A.....

C:\Users\user\AppData\Local\Temp\CabBF0C.tmp	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134

C:\Users\user\AppData\Local\Temp\CabBF0C.tmp	
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8efIqigYDff:RN7MlanAQwEIztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
Preview:	MSCF.....,.....I.....T.....R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.....\|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n-.....D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay.....n/R... ._.+..<...Am.t.<. ..V..y`.yO..e@../...<#..#.....dju*..B.....8..H'..lr.....l.I6/..d.].xIX<...&U...GD..Mn.y&.[<(tk.....%B.b;./...`.#h....C.P...B..8d.F...D.k..... 0..w...@(.. @K....?.)ce.....\.\.....l.....Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a..,...E5X..i.d..w.....#o*+.....X.P...k...V.$...X.r.e....9E.x..=\...Km.....B...Ep...xI@@c1.....p?...d.{EYN.K.X>D3..Z..q.] .Mq.....L.n}.....+/l\.cDB0.'.Y...r.[.....vM...o.=....zK..r..I..>B....U..3....Z...ZjS...wZ.M...IW;..e.L...zC.wBtQ..&.Z.Fv+..G9.8..!..\T:K`.....m.....9T.u..3h.....{...d[...@...Q.?..p.e.t[.%7.....^.....s.

C:\Users\user\AppData\Local\Temp\TarBF0D.tmp	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	data
Category:	dropped
Size (bytes):	152788
Entropy (8bit):	6.316654432555028
Encrypted:	false
SSDEEP:	1536:WIA6c7RbAh/E9nF2hspNuc8odv+1//FnzAYtYyjCQxSMnl3xlUwg:WAmfF3pNuc7v+ltjCQSMnnSx
MD5:	64FEDADE4387A8B92C120B21EC61E394
SHA1:	15A2673209A41CCA2BC3ADE90537FE676010A962
SHA-256:	BB899286BE1709A14630DC5ED80B588FDD872DB361678D3105B0ACE0D1EA6745
SHA-512:	655458CB108034E46BCE5C4A68977DCBF77E20F4985DC46F127ECBDE09D6364FE308F3D70295BA305667A027AD12C952B7A32391EFE4BD5400AF2F4D0D83087
Malicious:	false
Preview:	0..T...*.H.....T.0..T....1.0...`.H.e.....0..D...+.....7.....D.0..D.0...+.....7.....R19%..210115004237Z0...+.....0..D.0..*....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0.,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00.+.....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Local\Temp\tmp80F5.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.1063907901076036
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Rl4xtn:cbk4oL600QydbQxIYODOLedq3Sl4j
MD5:	CFAE5A3B7D8AA9653FE2512578A0D23A
SHA1:	A91A2F8DAEF114F89038925ADA6784646A0A5B12
SHA-256:	2AB741415F193A2A9134EAC48A2310899D18EFB5E61C3E81C35140A7EFEA30FA
SHA-512:	9DFD7ECA6924AE2785CE826A447B6CE6D043C552FBD3B8A804CE6722B07A74900E703DC56CD4443CAE9AB9601F21A6068E29771E48497A9AE434096A11814E8
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmp9445.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1319
Entropy (8bit):	5.133606110275315
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0mne5xtn:cbk4oL600QydbQxIYODOLedq3Ze5j
MD5:	C6F0625BF4C1CDFB699980C9243D3B22
SHA1:	43DE1FE5805769355163 27F17B5DA0C656C72851
SHA-256:	8DFC4E937F0B2374E3CED25FCE344B0731CF44B8854625B318D50ECE2DA8F576
SHA-512:	9EF2DBD4142AD0E1E6006929376ECB8011E7FFC801EE2101E906787D70325AD82752DF65839DE9972391FA52E1E5974EC1A5C7465A88AA56257633EBB7D70969

C:\Users\user\AppData\Local\Temp\tmp9445.tmp

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 />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\catalog.dat

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	data
Category:	dropped
Size (bytes):	928
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	24:IQnybgCUtvd7xCFhwUuQnybgCUtvd7xCFhwUuQnybgCUtvd7xCFhwUuQnybgCUtw:Ik/lCrwfk/lCrwfk/lCrwfk/lCrw8
MD5:	CCB690520E68EE385ACC0ACFE759AFFC
SHA1:	33F0DA3F55E5B3C5AC19B61D31471CB60BCD5C96
SHA-256:	166154225DAB5FCB79C1CA97D371B159D37B83FBC0ADABCD8EBA98FA113A7A3B
SHA-512:	AC4F3CF1F8F460745D37E6350861C2FBCDDCC1BBDE0A48FB361BFBF5B1EBF10A05F798A72CE413FCA073FF8108955353DDBCBD9D50CED6CDAE231C67A28FDA3
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.....@.3..{...grv+V...B.......].P...W.4C}uL.....s~..F...}......E......E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.....@.3..{...grv+V...B.......].P...W.4C}uL.....s~..F...}......E......E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.....@.3..{...grv+V...B.......].P...W.4C}uL.....s~..F...}......E......E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.....@.3..{...grv+V...B.......].P...W.4C}uL.....s~..F...}......E......E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:xt:r
MD5:	3ABB7239389DBB84935EC98902664658
SHA1:	85EF47D1F243C052DA1C993B9A5F0D953AEB04EE
SHA-256:	C56B2DE67DFEBED5A8C2EAEC31498AD5E2AC6586A6C15EA6E82AB708FE8EBFC7
SHA-512:	BA77692928043D117C69ABCB3ADEE4F90E23AF8F30FEA996E3746F4971EEB030DBED26F535EEA1AF377E7DCB83911E977C0490C9C6923EC27BB025AD4B988FB6
Malicious:	**true**
Preview:	..x....H

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\QUOTATIONs44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCKs.LNK

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:13 2020, mtime=Wed Aug 26 14:08:13 2020, atime=Thu Feb 25 14:28:30 2021, length=967360, window=hide
Category:	dropped
Size (bytes):	2568
Entropy (8bit):	4.577226214280601
Encrypted:	false
SSDEEP:	48:8QQY/XT3IkMbi1c42IQh2QQY/XT3IkMbi1c42IQ/:8QQY/XLIkMzpIQh2QQY/XLIkMzpIQ/
MD5:	2FF98281FD0929741EEB9C54BF54DB9B
SHA1:	C7F911DBA118EE784BB739A68E8F3798C8CB8A71
SHA-256:	7A1350716802EDF98667519C211D93E8B01CBA0016E0988EB36016D93F20F795
SHA-512:	5494D271B997819243119463B6DB88DC2F1D6E7EB9CD4F990B200116643DF201C6C39ADD17CA552C7A080F3617DE03CD28AED54293CDDC929C7929E3A6BE4EE
Malicious:	false
Preview:	L.................F.... ...u....{..u....{..ym...........................;....P.O. .:i.....+00.../C:\.................t.1.....QK.X..Users.`.......:..QK.X*..................6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1......Q.y..user.8......QK.X.Q.y*...&=....U..............A.l.b.u.s.....z.1......Q.y..Desktop.d......QK.X.Q.y*..._=.............:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.......2.....YR.{ .QUOTAT~1.DOC..........Q.y.Q.y*...8....................Q.U.O.T.A.T.I.O.N.s.4.4.8.8.8._.A.2.2.2.1._.T.O.A.N._.T.A.N._.L.O.C._.T.R.A.D.I.N.G._.S.E.R.V.I.C.E.S._.J.O.I.N.T._.S.T.O.C.K.s...d.o.c......................-...8...[............?J......C:\Users\..#..................\\936905\Users.user\Desktop\QUOTATIONs44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCKs.doc.[.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.Q.U.O.T.A.T.I.O.N.s.4.4.8.8.8._.A.2.2.2.1._.T.O.A.N._.T.A.N._.L.O.C._.T.R.A.D.I.N.G._.S.E.R.V.I.C.E.S._.J.O.I.N.T._.S.T.O.C.K.s..

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):	230
Entropy (8bit):	4.619567959906291
Encrypted:	false
SSDEEP:	6:M7qjk8A2zDKnKqjk8A2zDKjqjk8A2zDKs:Md87anY87aV87as
MD5:	8164887DD336F403637A7B7C1135A1DA
SHA1:	0D2E021E54D11E130E87026854D6D8367BC65052
SHA-256:	8617F63E83B01A5499DAB372DFB16503950187DFD4C82A4485F137476564F204
SHA-512:	9E8A0BCB48782714F3DE01F8482DB2B913DB7213334353C4A2B43B0B12AD5D56BEF8756A42746CA1537CFD56DEEE7A5ACCC1D56E22B8CE44A7DF0EE02D8F9A F6
Malicious:	false
Preview:	[doc]..QUOTATIONs44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCKs.LNK=0..QUOTATIONs44888_A2221_TOAN_TAN_LOC_TRADIN G_SERVICES_JOINT_STOCKs.LNK=0..[doc]..QUOTATIONs44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCKs.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:vrJlaCkWtVyzALORwObGUXKbylln:vdsCkWtJLObyvb+l
MD5:	6AF5EAEBE6C935D9A5422D99EEE6BEF0
SHA1:	6FE25A65D5CC0D4F989A1D79DF5CE1D225D790EC
SHA-256:	CE916A38A653231ED84153C323027AC4A0695E0A7FB7CC042385C96FA6CB4719
SHA-512:	B2F51A8375748037E709D75C038B48C69E0F02D2CF772FF355D7203EE885B5DB9D1E15DA2EDB1C1E2156A092F315EB9C069B654AF39B7F4ACD3EFEFF1F8CAE 0
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....^.....^.....P.^.....^.....z.....^.....x...

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Preview:	..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\LIP8714C.txt	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	64
Entropy (8bit):	4.030028124459133
Encrypted:	false
SSDEEP:	3:vpqMLJUQ2ciiZ/YXvWVt2X:vEMWXcijWVM
MD5:	25EDED50548FE4FFF3119179E391DD16
SHA1:	73D001FDD077A3066DB93CC0EF438BC51D2C20F0
SHA-256:	2CDCAB99426A62F6722A1704DE32D7B9BB8925A45B767D0934A1365A1578B1F1
SHA-512:	D85614C03EC7E9636E32AC05386752A76B2B330742DB6F6BC3A68EB566B94CE77ABA70E6A737E0EFAAADCE832289C4D623488DCA099765AF710ADA007793530 0
Malicious:	false
IE Cache URL:	live.com/

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\LIP8714C.txt	
Preview:	wla42..live.com/.1536.4124483072.30871743.3006855612.30870411.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\Y5D8BEZV.txt	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	ASCII text
Category:	downloaded
Size (bytes):	89
Entropy (8bit):	4.3519817792342295
Encrypted:	false
SSDEEP:	3:jviOdjc3SQBI6LJci2JQdYVO2O2LGWTW3SVy2X:uOdg3SQI69ci2J53OyTXf
MD5:	BE6FA4005BF612690EEE1ECDD31EE976
SHA1:	883ACE9B58936BEE7163C278302FDD324127848A
SHA-256:	A05E2DC449119D274ED9B43B253ACD75E696BCE9AD895B8D8393B538560A28B1
SHA-512:	DC1C24E681E21D645F5CD3BE083F27DC4E4C9CC275BBD51A3D8B6205FC46EBD63DF0DC7857A16665BD82CFBF234DFBC56B48CCC57ABA89A59E7367D6F07884C
Malicious:	false
IE Cache URL:	bit.ly/
Preview:	_bit.l1p6te-b37a8979adaf075f5e-00T.bit.ly/.1536.1532647680.30906545.667713608.30870411.*.

C:\Users\user\Desktop\~$OTATIONs44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCKs.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:vrJlaCkWtVyzALORwObGUXKbylln:vdsCkWtJLObyvb+l
MD5:	6AF5EAEBE6C935D9A5422D99EEE6BEF0
SHA1:	6FE25A65D5CC0D4F989A1D79DF5CE1D225D790EC
SHA-256:	CE916A38A653231ED84153C323027AC4A0695E0A7FB7CC042385C96FA6CB4719
SHA-512:	B2F51A8375748037E709D75C038B48C69E0F02D2CF772FF355D7203EE885B5DB9D1E15DA2EDB1C1E2156A092F315EB9C069B654AF39B7F4ACD3EFEFF1F8CAE0
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....^.....^.....P.^.....^.....z.....^.....x...

C:\Users\user\subfolder1\filename1.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	4.856871861209239
Encrypted:	false
SSDEEP:	3072:6wVUP1A3a64iOR/VfgmLQPDBZByQqFXrMQqwV:6wVUPH6GfgmLQPDBZByQqFXIQqwV
MD5:	A6AD1C3046A3CF0C6992507F2886AAB3
SHA1:	8024E4315C4BD196F1531E08C541359DBAC70A39
SHA-256:	CEF944407A26C3C148AFBF8253BAA55AEE7CDFAEC17B5A158831574245BAC8AD
SHA-512:	A5C0796BCCE3CEDE14CC02915A4A0A55AEEAFD0B0675AF8FE395905F9ED78A58CBDCED5EE89CFBDD7E55B90A5AED2D647C76EE3BB9DD35E778DA1968076F21A
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 28%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1...1...1.....0...~..0.....0...Rich1.....PE..L.....Y.....P. .....`....@.....tY..(....p.....(... .....text....M.....P..... ..`.data.....`.....`.....@....rsrc.....p.....p.....@..@...I.....MSVBVM60.DLL..... ....

C:\Users\Public\69577.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	131072
Entropy (8bit):	4.856871861209239
Encrypted:	false

C:\Users\Public\69577.exe	
SSDEEP:	3072:6wVUP1A3a64iOR/VfgmLQPDBZByQqFXrMQqwV:6wVUPH6GfgmLQPDBZByQqFXIQqwV
MD5:	A6AD1C3046A3CF0C6992507F2886AAB3
SHA1:	8024E4315C4BD196F1531E08C541359DBAC70A39
SHA-256:	CEF944407A26C3C148AFBF8253BAA55AEE7CDFAEC17B5A158831574245BAC8AD
SHA-512:	A5C0796BCCE3CEDE14CC02915A4A0A55AEEAFD0B0675AF8FE395905F9ED78A58CBDCED5EE89CFBDD7E55B90A5AED2D647C76EE3BB9DD35E778DA1968076F21A
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 28%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1...1...1....0...~..0.....0...Rich1.....PE..L.....Y.....P. .....`....@.....tY..(....p.....(... .....text....M.....P..... ..`.data.....`.....`.....@....rsrc.....p.....p.....@..@...I.....MSVBVM60.DLL..... ....

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	6.068615237294724
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	QUOTATIONs44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCKs.doc
File size:	967360
MD5:	bc1c94e783483f1c218efb5dcaf5f67e
SHA1:	7747c98d3d2da16f6e8b2fc56bd0e84532e3a543
SHA256:	d1e84cab5bf5eadd159b04374dce5a78a0e93156086475d41ad86665357dfc66
SHA512:	e399eeecd3067441e52ddcbb394a8547e1ed20fb262a8c70ffc37ac49b6854410011e23d1405c94d6aded1ca32627b8a1f27bf35c7d2d1767dfffbbf3f3a7f17
SSDEEP:	24576:X67676767676767676767676767676767676767676767676q5j:quuuuuuuuuuuuuuuuuuuuuuus
File Content Preview:	{\rtf33843\page51787859448176035@m42JEUa4SrclZjjE@-KI2WTYrCCIYwauZ0C<eh&&7_M-C_D--_-V,64>88964$Cv>yt=n6|:%_>jn8%bm\mklP;=u\k6588.14.... ....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	000D9BB0h								no

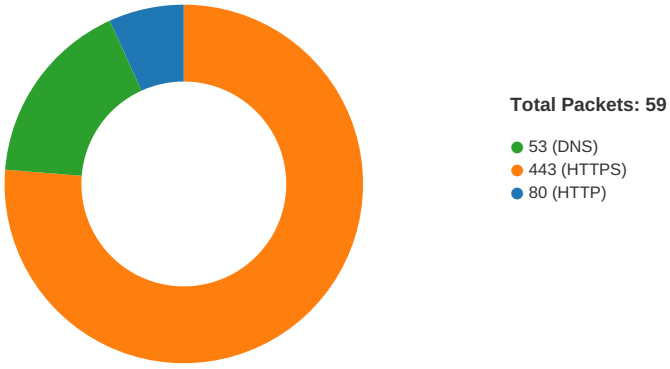
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/25/21-07:31:12.865275	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49171	4488	192.168.2.22	194.5.98.202
02/25/21-07:31:18.959312	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49172	4488	192.168.2.22	194.5.98.202

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/25/21-07:31:26.516121	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49173	4488	192.168.2.22	194.5.98.202
02/25/21-07:31:32.853198	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49174	4488	192.168.2.22	194.5.98.202
02/25/21-07:31:39.738064	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49175	4488	192.168.2.22	194.5.98.202

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 07:29:14.575544119 CET	49165	80	192.168.2.22	67.199.248.10
Feb 25, 2021 07:29:14.626983881 CET	80	49165	67.199.248.10	192.168.2.22
Feb 25, 2021 07:29:14.627127886 CET	49165	80	192.168.2.22	67.199.248.10
Feb 25, 2021 07:29:14.627883911 CET	49165	80	192.168.2.22	67.199.248.10
Feb 25, 2021 07:29:14.679239988 CET	80	49165	67.199.248.10	192.168.2.22
Feb 25, 2021 07:29:14.770637989 CET	80	49165	67.199.248.10	192.168.2.22
Feb 25, 2021 07:29:14.770742893 CET	49165	80	192.168.2.22	67.199.248.10
Feb 25, 2021 07:29:14.934967041 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:14.986754894 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:14.987035036 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:15.002682924 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:15.057116032 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:15.057153940 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:15.057266951 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:15.057316065 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:15.069318056 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:15.124504089 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:15.124650002 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:16.673723936 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:16.754147053 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:16.999515057 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:16.999567032 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:16.999798059 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:16.999907970 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:16.999948025 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:16.999984980 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:16.999989986 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:17.000025034 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:17.000046015 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:17.000701904 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:17.000741959 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:17.000777006 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:17.000799894 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:17.000830889 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:17.001118898 CET	443	49166	5.79.72.163	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 07:29:17.001157999 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:17.001193047 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:17.001195908 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:17.001216888 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:17.001255989 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:17.001569986 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:17.001612902 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:17.001647949 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:17.001668930 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:17.008138895 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:17.051927090 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:17.051981926 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:17.052119017 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:17.052165985 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:17.052170992 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:17.052200079 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:17.052217007 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:17.052244902 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:17.052256107 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:17.052284956 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:17.052297115 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:17.052316904 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:17.052345037 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:17.052361012 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:17.052386045 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:17.052406073 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:17.052426100 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:17.052454948 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:17.052464962 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:17.052479029 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:17.052512884 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:17.052530050 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:17.052557945 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:17.052572966 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:17.052617073 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:17.052823067 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:17.052864075 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:17.052885056 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:17.052902937 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:17.052908897 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:17.052941084 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:17.052961111 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:17.052979946 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:17.052989960 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:17.053019047 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:17.053040981 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:17.053081036 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:17.053147078 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:17.053188086 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:17.053210974 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:17.053231955 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:17.053481102 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:17.053522110 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:17.053548098 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:17.053575039 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:17.055668116 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:17.104232073 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:17.104295969 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:17.104334116 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:17.104377031 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:17.104413986 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:17.104461908 CET	443	49166	5.79.72.163	192.168.2.22
Feb 25, 2021 07:29:17.104470968 CET	49166	443	192.168.2.22	5.79.72.163
Feb 25, 2021 07:29:17.104502916 CET	49166	443	192.168.2.22	5.79.72.163

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 07:29:17.104506016 CET	443	49166	5.79.72.163	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 07:29:14.461078882 CET	52197	53	192.168.2.22	8.8.8.8
Feb 25, 2021 07:29:14.511269093 CET	53	52197	8.8.8.8	192.168.2.22
Feb 25, 2021 07:29:14.511475086 CET	52197	53	192.168.2.22	8.8.8.8
Feb 25, 2021 07:29:14.561319113 CET	53	52197	8.8.8.8	192.168.2.22
Feb 25, 2021 07:29:14.812344074 CET	53099	53	192.168.2.22	8.8.8.8
Feb 25, 2021 07:29:14.872477055 CET	53	53099	8.8.8.8	192.168.2.22
Feb 25, 2021 07:29:14.872773886 CET	53099	53	192.168.2.22	8.8.8.8
Feb 25, 2021 07:29:14.932527065 CET	53	53099	8.8.8.8	192.168.2.22
Feb 25, 2021 07:29:15.402287006 CET	52838	53	192.168.2.22	8.8.8.8
Feb 25, 2021 07:29:15.451178074 CET	53	52838	8.8.8.8	192.168.2.22
Feb 25, 2021 07:29:15.456893921 CET	61200	53	192.168.2.22	8.8.8.8
Feb 25, 2021 07:29:15.514120102 CET	53	61200	8.8.8.8	192.168.2.22
Feb 25, 2021 07:29:16.026027918 CET	49548	53	192.168.2.22	8.8.8.8
Feb 25, 2021 07:29:16.087656021 CET	53	49548	8.8.8.8	192.168.2.22
Feb 25, 2021 07:29:16.093247890 CET	55627	53	192.168.2.22	8.8.8.8
Feb 25, 2021 07:29:16.154942989 CET	53	55627	8.8.8.8	192.168.2.22
Feb 25, 2021 07:31:07.850161076 CET	56009	53	192.168.2.22	8.8.8.8
Feb 25, 2021 07:31:07.904503107 CET	53	56009	8.8.8.8	192.168.2.22
Feb 25, 2021 07:31:08.949430943 CET	61865	53	192.168.2.22	8.8.8.8
Feb 25, 2021 07:31:09.023087978 CET	53	61865	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 07:29:14.461078882 CET	192.168.2.22	8.8.8.8	0x7e45	Standard query (0)	bit.ly	A (IP address)	IN (0x0001)
Feb 25, 2021 07:29:14.511475086 CET	192.168.2.22	8.8.8.8	0x7e45	Standard query (0)	bit.ly	A (IP address)	IN (0x0001)
Feb 25, 2021 07:29:14.812344074 CET	192.168.2.22	8.8.8.8	0xef41	Standard query (0)	u.teknik.io	A (IP address)	IN (0x0001)
Feb 25, 2021 07:29:14.872773886 CET	192.168.2.22	8.8.8.8	0xef41	Standard query (0)	u.teknik.io	A (IP address)	IN (0x0001)
Feb 25, 2021 07:31:07.850161076 CET	192.168.2.22	8.8.8.8	0xbe16	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Feb 25, 2021 07:31:08.949430943 CET	192.168.2.22	8.8.8.8	0xbf16	Standard query (0)	ibkebw.dm.files.1drv.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 07:29:14.511269093 CET	8.8.8.8	192.168.2.22	0x7e45	No error (0)	bit.ly		67.199.248.11	A (IP address)	IN (0x0001)
Feb 25, 2021 07:29:14.511269093 CET	8.8.8.8	192.168.2.22	0x7e45	No error (0)	bit.ly		67.199.248.10	A (IP address)	IN (0x0001)
Feb 25, 2021 07:29:14.561319113 CET	8.8.8.8	192.168.2.22	0x7e45	No error (0)	bit.ly		67.199.248.10	A (IP address)	IN (0x0001)
Feb 25, 2021 07:29:14.561319113 CET	8.8.8.8	192.168.2.22	0x7e45	No error (0)	bit.ly		67.199.248.11	A (IP address)	IN (0x0001)
Feb 25, 2021 07:29:14.872477055 CET	8.8.8.8	192.168.2.22	0xef41	No error (0)	u.teknik.io	teknik.io		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 07:29:14.872477055 CET	8.8.8.8	192.168.2.22	0xef41	No error (0)	teknik.io		5.79.72.163	A (IP address)	IN (0x0001)
Feb 25, 2021 07:29:14.932527065 CET	8.8.8.8	192.168.2.22	0xef41	No error (0)	u.teknik.io	teknik.io		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 07:29:14.932527065 CET	8.8.8.8	192.168.2.22	0xef41	No error (0)	teknik.io		5.79.72.163	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 07:31:07.904503107 CET	8.8.8.8	192.168.2.22	0xbe16	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 07:31:09.023087978 CET	8.8.8.8	192.168.2.22	0xbf16	No error (0)	ibkebw.dm.files.1drv.com	dm-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 07:31:09.023087978 CET	8.8.8.8	192.168.2.22	0xbf16	No error (0)	dm-files.fe.1drv.com	odc-dm-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- bit.ly

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	67.199.248.10	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

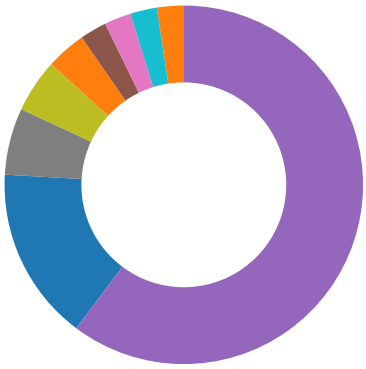
Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 07:29:14.627883911 CET	0	OUT	GET /2ZKf4aq HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: bit.ly Connection: Keep-Alive
Feb 25, 2021 07:29:14.770637989 CET	1	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Thu, 25 Feb 2021 06:29:14 GMT Content-Type: text/html; charset=utf-8 Content-Length: 116 Cache-Control: private, max-age=90 Location: https://u.teknik.io/wREzo.txt Set-Cookie: _bit=l1p6te-b37a8979adaf075f5e-00T; Domain=bit.ly; Expires=Tue, 24 Aug 2021 06:29:14 GMT Via: 1.1 google Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 42 69 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 75 2e 74 65 6b 6e 69 6b 2e 69 6f 2f 77 52 45 7a 6f 2e 74 78 74 22 3e 6d 6f 76 65 64 20 68 65 72 65 3c 2f 61 3e 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e Data Ascii: <html><head><title>Bitly</title></head><body>moved here</body></html>

Code Manipulations

Statistics

Behavior

- WINWORD.EXE
- EQNEDT32.EXE
- 69577.exe
- RegAsm.exe
- RegAsm.exe
- schtasks.exe
- schtasks.exe
- taskeng.exe
- RegAsm.exe
- smtpsvc.exe
- filename1.exe
- smtpsvc.exe



Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2200 Parent PID: 584

General

Start time:	07:28:30
Start date:	25/02/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13f320000
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	7FEE8F826B4	CreateDirectoryA

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{0863C5D3-5908-4917-8F28-8909E0160183}.tmp	unknown	512	success or wait	147	7FEE8DE0172	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE8EBE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE8EBE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE8EBE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE8EA9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE8EA9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE8EA9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\1096C3	success or wait	1	7FEE8EA9AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Mic rosoft\Office\14.0\Word\Resili ency\DocumentRecovery\1096C3	1096C3	binary	04 00 00 00 98 08 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 67 C4 1F 29 8B 0B D7 01 C3 96 10 00 C3 96 10 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	success or wait	1	7FEE8EA9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF				

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1381564462	1381564463	success or wait	1	7FEE8EA9AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1381564463	1381564464	success or wait	1	7FEE8EA9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\1096C3	1096C3	binary	04 00 00 00 98 08 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 67 C4 1F 29 8B 0B D7 01 C3 96 10 00 C3 96 10 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	04 00 00 00 98 08 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 C3 96 10 00 C3 96 10 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	success or wait	1	7FEE8EA9AC0	unknown

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

Analysis Process: EQNEDT32.EXE PID: 2308 Parent PID: 584

General

Start time:	07:28:32
Start date:	25/02/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

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

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

Analysis Process: 69577.exe PID: 2680 Parent PID: 2308

General

Start time:	07:28:35
Start date:	25/02/2021
Path:	C:\Users\Public\69577.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\69577.exe
Imagebase:	0x400000
File size:	131072 bytes
MD5 hash:	A6AD1C3046A3CF0C6992507F2886AAB3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Antivirus matches:	• Detection: 28%, ReversingLabs
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RegAsm.exe PID: 2916 Parent PID: 2680

General

Start time:	07:30:17
Start date:	25/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\Public\69577.exe
Imagebase:	0xbf0000
File size:	53248 bytes
MD5 hash:	246BB0F8D68A463FD17C235DEB5491C0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: RegAsm.exe PID: 2488 Parent PID: 2680

General

Start time:	07:30:22
Start date:	25/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\69577.exe
Imagebase:	0xbf0000
File size:	53248 bytes
MD5 hash:	246BB0F8D68A463FD17C235DEB5491C0
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.2371344330.0000000000140000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.2371344330.0000000000140000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.2371344330.0000000000140000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.2371329317.0000000000130000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.2371329317.0000000000130000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 00000006.00000002.2371533870.0000000000282000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.2382867266.000000001F3FF000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\subfolder1	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	281A17	SHCreateDirectoryExW
C:\Users\user\subfolder1\filename1.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	28799F	CreateFileW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	284570	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	284570	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	284570	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	284570	InternetOpenUrlA
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	284570	InternetOpenUrlA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	284570	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	284570	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	284570	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	284570	InternetOpenUrlA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\LIP8714C.txt	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	284570	InternetOpenUrlA
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7B07A1	CreateDirectoryW
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file | open no recall	success or wait	1	7B089B	CreateFileW
C:\Program Files (x86)\SMTP Service	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7B07A1	CreateDirectoryW
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	read data or list directory | read attributes | delete | synchronize | generic write	device | sparse file	sequential only | non directory file	success or wait	1	7B0B20	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp9445.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	7B0D1C	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp80F5.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	7B0D1C	GetTempFileNameW
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\Logs	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7B07A1	CreateDirectoryW
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\Logs\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7B07A1	CreateDirectoryW
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\catalog.dat	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file | open no recall	success or wait	1	7B089B	CreateFileW

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\subfolder1\filename1.exe	unknown	131072	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 75 9f f9 db 31 fe 97 88 31 fe 97 88 31 fe 97 88 b2 e2 99 88 30 fe 97 88 7e dc 9e 88 30 fe 97 88 07 d8 9a 88 30 fe 97 88 52 69 63 68 31 fe 97 88 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 04 c3 ba 59 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 50 01 00 00 a0 00 00 00 00 00 00 dc 13 00 00 00 10 00 00 00 60 01 00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 00 00 01 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......u...1...1...1.......0. ..~...0.......0...Rich1....... ....PE..L......Y............. ...P...................`....@.	success or wait	1	281C68	WriteFile
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat	unknown	8	1c 1d 78 fa a2 d9 d8 48	..x....H	success or wait	1	7B0A53	WriteFile
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	0	53248	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 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 2c 00 0f 53 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 08 00 00 a0 00 00 00 20 00 00 00 00 00 00 de b7 00 00 00 20 00 00 00 c0 00 00 00 00 40 00 00 20 00 00 00 10 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00 01 00 00 10 00 00 9f e8 00 00 03 00 40 05 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	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...,..S.......... ....@.. ....@.................	success or wait	1	7B0B20	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp9445.tmp	unknown	1319	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 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	7B0A53	WriteFile
C:\Users\user\AppData\Local\Temp\tmp80F5.tmp	unknown	1310	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 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	7B0A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc d5 c2 a4 ed f2 80 40 dc 33 8c a4 7b 0c cc 1c 67 72 76 2b 56 81 e7 f3 bf b9 42 19 0e 82 0d c5 eb 15 5d f3 50 8b f6 16 57 df 34 43 7d 75 4c 1e b2 93 0b a6 73 7e 82 c7 46 04 b7 fb 7d 99 ad 83 81 ed 81 00 45 f9 c7 db f0 db f0 45 f9 14 f3 b4 36 45 8f 94 b5 81 a3 7b d9 9f 05 18 7b ed a9 79 53 82 bd bf 37 fa c4 22 16 68 4b d7 21 03 78 86 32 be 99 69 df a3 8f 7a 4a d5 da bb fa 20 fc b4 c0 c0 66 d0 dd a7 3f c0 5f 0b e4 fb a3 30 ca 3a 65 5b 37 77 7b 31 81 21 de 34 a9 bb 99 d3 ca 26 b9	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h...t .+..Z\.. .i.....@.3..{...grv +V.....B.....].P...W.4C}uL.. ...s~..F...}.....E.....E... .6E.....{....{..yS...7..".hK.! .x.2..i...zJ.... ....f...?._.. ..0.:e[7w{1.!.4.....&.	success or wait	1	7B0A53	WriteFile
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc d5 c2 a4 ed f2 80 40 dc 33 8c a4 7b 0c cc 1c 67 72 76 2b 56 81 e7 f3 bf b9 42 19 0e 82 0d c5 eb 15 5d f3 50 8b f6 16 57 df 34 43 7d 75 4c 1e b2 93 0b a6 73 7e 82 c7 46 04 b7 fb 7d 99 ad 83 81 ed 81 00 45 f9 c7 db f0 db f0 45 f9 14 f3 b4 36 45 8f 94 b5 81 a3 7b d9 9f 05 18 7b ed a9 79 53 82 bd bf 37 fa c4 22 16 68 4b d7 21 03 78 86 32 be 99 69 df a3 8f 7a 4a d5 da bb fa 20 fc b4 c0 c0 66 d0 dd a7 3f c0 5f 0b e4 fb a3 30 ca 3a 65 5b 37 77 7b 31 81 21 de 34 a9 bb 99 d3 ca 26 b9	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h...t .+..Z\.. .i.....@.3..{...grv +V.....B.....].P...W.4C}uL.. ...s~..F...}.....E.....E... .6E.....{....{..yS...7..".hK.! .x.2..i...zJ.... ....f...?._.. ..0.:e[7w{1.!.4.....&.	success or wait	3	7B0A53	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\69577.exe	unknown	131072	success or wait	1	28799F	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	73FFD6F0	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	73FFD6F0	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFD6F0	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	74034496	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	74034496	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe	unknown	4096	success or wait	1	74034496	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe	unknown	512	success or wait	1	74034496	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7B0A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7B0A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4096	success or wait	1	7B0A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4096	end of file	1	7B0A53	ReadFile
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	74034496	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	74034496	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	Startup key	unicode	C:\Users\user\subfolder1\filename1.exe	success or wait	1	28185B	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run	SMTP Service	unicode	C:\Program Files (x86)\SMTP Service\smtpsvc.exe	success or wait	1	7B0C12	RegSetValueExW

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

Analysis Process: schtasks.exe PID: 3060 Parent PID: 2488

General

Start time:	07:30:28
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'SMTP Service' /xml 'C:\Users\user\AppData\Local\Temp\tmp9445.tmp'
Imagebase:	0x2c0000
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\tmp9445.tmp	unknown	2	success or wait	1	2C8F47	ReadFile
C:\Users\user\AppData\Local\Temp\tmp9445.tmp	unknown	1320	success or wait	1	2C900C	ReadFile

Analysis Process: schtasks.exe PID: 2276 Parent PID: 2488

General

Start time:	07:30:29
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true

Commandline:	'schtasks.exe' /create /f /tn 'SMTP Service Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp80F5.tmp'
Imagebase:	0x2c0000
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\tmp80F5.tmp	unknown	2	success or wait	1	2C8F47	ReadFile
C:\Users\user\AppData\Local\Temp\tmp80F5.tmp	unknown	1311	success or wait	1	2C900C	ReadFile

Analysis Process: taskeng.exe PID: 2272 Parent PID: 860

General

Start time:	07:30:29
Start date:	25/02/2021
Path:	C:\Windows\System32\taskeng.exe
Wow64 process (32bit):	false
Commandline:	taskeng.exe {DA6299CA-95CA-4E9D-8945-2CC05321254C} S-1-5-21-966771315-3019405637-367336477-1006:user-PC\user:Interactive:[1]
Imagebase:	0xff9c0000
File size:	464384 bytes
MD5 hash:	65EA57712340C09B1B0C427B4848AE05
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\Tasks\SMTP Service	unknown	2	success or wait	1	FF9C433D	ReadFile
C:\Windows\System32\Tasks\SMTP Service	unknown	2718	success or wait	1	FF9C43A4	ReadFile
C:\Windows\System32\Tasks\SMTP Service Task	unknown	2	success or wait	1	FF9C433D	ReadFile
C:\Windows\System32\Tasks\SMTP Service Task	unknown	2700	success or wait	1	FF9C43A4	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\Handshake\{DA6299CA-95CA-4E9D-8945-2CC05321254C}	data	binary	4D 45 4F 57 01 00 00 00 E4 B7 BD 92 8B F2 A0 46 B5 51 45 A5 2B DD 51 25 00 00 00 00 00 00 00 00 2F 33 AA 2B A6 BA 7C 97 EF 31 93 7F 37 C2 21 27 01 CC 00 00 E0 08 00 00 B1 9C F9 9F 0C 35 14 45 00 00 00 00	success or wait	1	FF9D2CB8	RegSetValueExW

Analysis Process: RegAsm.exe PID: 1904 Parent PID: 2272

General

Start time:	07:30:30
Start date:	25/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe 0
Imagebase:	0xbf0000
File size:	53248 bytes
MD5 hash:	246BB0F8D68A463FD17C235DEB5491C0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	73FFA4FC	unknown

Analysis Process: smtpsvc.exe PID: 2348 Parent PID: 2272

General

Start time:	07:30:31
Start date:	25/02/2021
Path:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\SMTP Service\smtpsvc.exe' 0
Imagebase:	0xd90000
File size:	53248 bytes
MD5 hash:	246BB0F8D68A463FD17C235DEB5491C0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Virustotal, Browse • Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73FFA4FC	unknown

Analysis Process: filename1.exe PID: 1552 Parent PID: 1388

General

Start time:	07:30:36
Start date:	25/02/2021
Path:	C:\Users\user\subfolder1\filename1.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\subfolder1\filename1.exe'
Imagebase:	0x400000
File size:	131072 bytes
MD5 hash:	A6AD1C3046A3CF0C6992507F2886AAB3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Antivirus matches:	• Detection: 28%, ReversingLabs
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: smtpsvc.exe PID: 2560 Parent PID: 1388

General

Start time:	07:30:45
Start date:	25/02/2021
Path:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\SMTP Service\smtpsvc.exe'
Imagebase:	0x1240000
File size:	53248 bytes
MD5 hash:	246BB0F8D68A463FD17C235DEB5491C0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73FFA4FC	unknown

Disassembly

Code Analysis