**ID:** 481181
**Sample Name:**
start[2021.09.09_15-26].vbs
**Cookbook:** default.jbs
**Time:** 13:48:06
**Date:** 10/09/2021
**Version:** 33.0.0 White Diamond

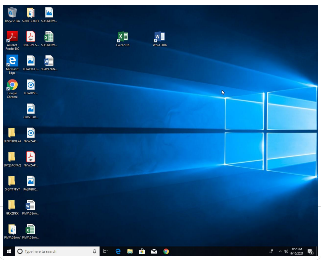
# Table of Contents

# Windows Analysis Report start[2021.09.09_15-26].vbs

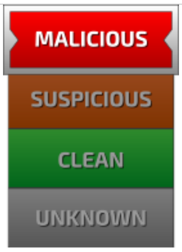
## Overview

### General Information

| | |
|---|---|
| Sample Name: | start[2021.09.09_15-26].vbs |
| Analysis ID: | 481181 |
| MD5: | 3959f76d91c30f3.. |
| SHA1: | 2c918bff7f90737… |
| SHA256: | 1d02060d7493d2.. |
| Infos: | |
| Most interesting Screenshot: | |



### Detection



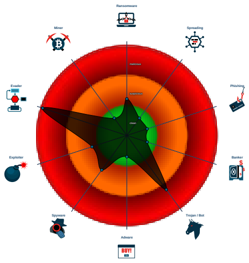
Ursnif

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

### Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- Benign windows process drops PE f…
- VBScript performs obfuscated calls …
- Yara detected Ursnif
- System process connects to networ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Tries to detect sandboxes and other…
- Creates processes via WMI

### Classification



## Process Tree

- **System is w10x64**
- wscript.exe (PID: 3840 cmdline: C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\start[2021.09.09_15-26].vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- WmiPrvSE.exe (PID: 1304 cmdline: C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding MD5: A782A4ED336750D10B3CAF776AFE8E70)
  - rundll32.exe (PID: 2396 cmdline: rundll32 C:\Users\user\AppData\Local\Temp\fum.cpp,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
    - rundll32.exe (PID: 5236 cmdline: rundll32 C:\Users\user\AppData\Local\Temp\fum.cpp,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- WmiPrvSE.exe (PID: 1848 cmdline: C:\Windows\sysWOW64\wbem\wmiprvse.exe -secured -Embedding MD5: 7AB59579BA91115872D6E51C54B9133B)
- **cleanup**

## Malware Configuration

### Threatname: Ursnif

```
{
  "lang_id": "RU, CN",
  "RSA Public Key":
"IAodzSkRRXZVbpA8JuABjuUBQvpHiTpdg9dOAQp7bBw4t0xkkPvGywDaeciS3HngU/RkNYsOricM2S0LVvdwWlSJ6FdKpFt6YFFWOrsBfCiNFCtU5v/Ohii1LI6H4/OB/132O4comC2he+ED1d47BeoZGdamjIEdPypU4ReJbSLrCxcR
MW03mJzNzM22WWjes9V+fVfZ8lvnVONnlm+2SejHIEhpJMv4VzqUiuRgWDBCh1ovNzO3eDJUiuSU1jFcdmg2ywuZOyDLXh6uuRZonMVTxMoziZw6y80jGvuwDFFQy5TMx6xbKoXdqNSwE60TugFay/vbpOuG0fp4zORCVEe39fTGD2o0G
ttx0E5BI4w=",
  "c2_domain": [
    "atl.bigbigpoppa.com",
    "pop.urlovedstuff.com"
  ],
  "botnet": "2500",
  "server": "580",
  "serpent_key": "Do9L8DmcVMtyFi6j",
  "sleep_time": "5",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "1"
}
```

## Yara Overview

### Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000017.00000003.607221952.00000000050C8000.00000004.00000040.sdmp | JoeSecurity_Ursnif | Yara detected Ursnif | Joe Security | |
| 00000017.00000003.607028050.00000000050C8000.00000004.00000040.sdmp | JoeSecurity_Ursnif | Yara detected Ursnif | Joe Security | |
| 00000017.00000003.606994412.00000000050C8000.00000004.00000040.sdmp | JoeSecurity_Ursnif | Yara detected Ursnif | Joe Security | |
| 00000017.00000003.607255595.00000000050C8000.00000004.00000040.sdmp | JoeSecurity_Ursnif | Yara detected Ursnif | Joe Security | |
| 00000017.00000003.607169997.00000000050C8000.00000004.00000040.sdmp | JoeSecurity_Ursnif | Yara detected Ursnif | Joe Security | |
| Click to see the 5 entries | | | | |

## Sigma Overview

**No Sigma rule has matched**

## Jbx Signature Overview

Click to jump to signature section

### AV Detection:

**Found malware configuration**

**Multi AV Scanner detection for submitted file**

**Antivirus detection for URL or domain**

**Multi AV Scanner detection for domain / URL**

**Multi AV Scanner detection for dropped file**

### Networking:

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

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

### Key, Mouse, Clipboard, Microphone and Screen Capturing:

**Yara detected Ursnif**

### E-Banking Fraud:

**Yara detected Ursnif**

### System Summary:

**Writes registry values via WMI**

### Data Obfuscation:

**VBScript performs obfuscated calls to suspicious functions**

### Persistence and Installation Behavior:

**Creates processes via WMI**

## Hooking and other Techniques for Hiding and Protection:

**Yara detected Ursnif**

**Deletes itself after installation**

## Malware Analysis System Evasion:

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

**Found evasive API chain (may stop execution after checking system information)**

## Anti Debugging:

**Found API chain indicative of debugger detection**

## HIPS / PFW / Operating System Protection Evasion:

**Benign windows process drops PE files**

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

## Stealing of Sensitive Information:

**Yara detected Ursnif**

## Remote Access Functionality:

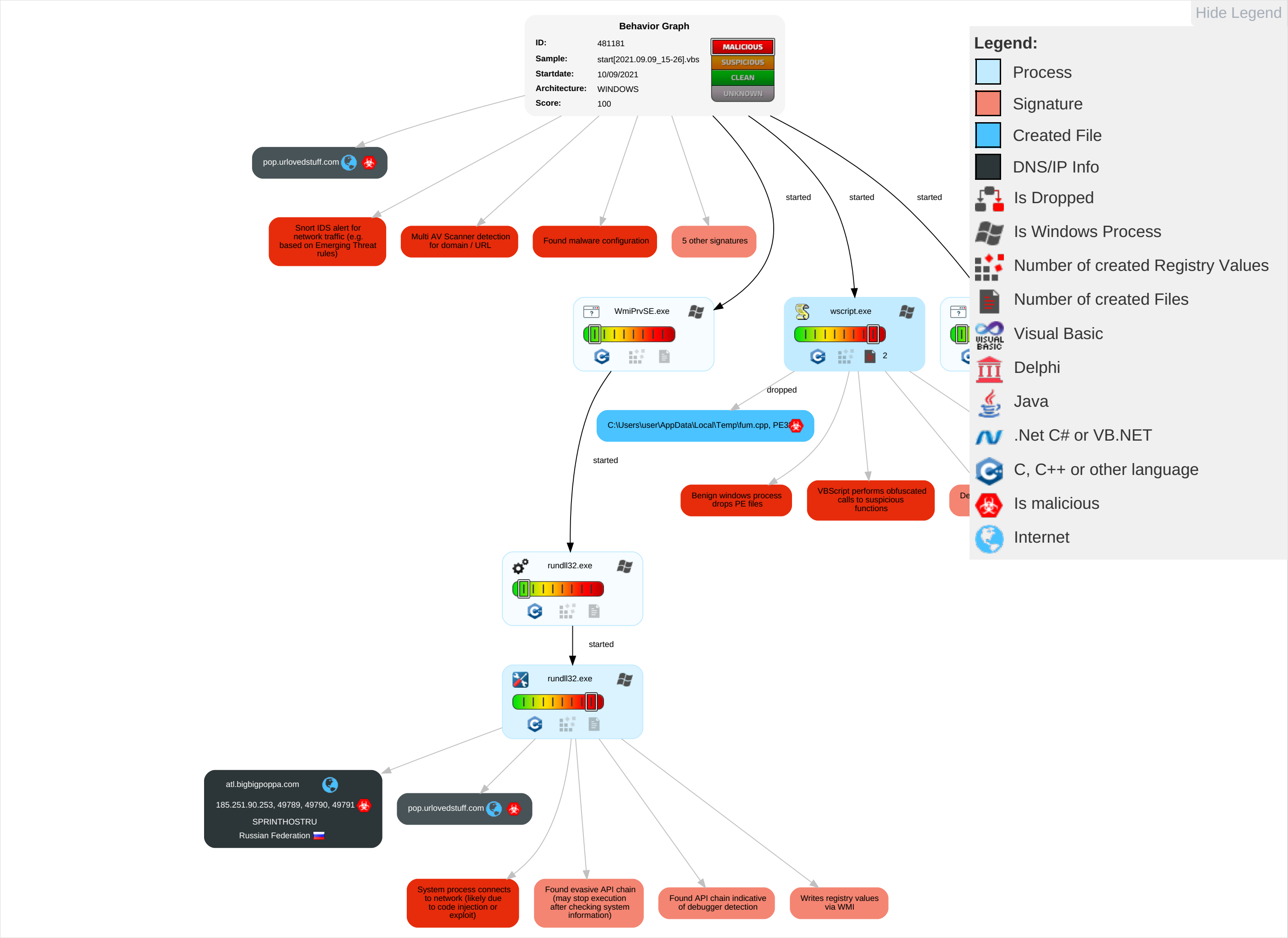
**Yara detected Ursnif**

# Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Com and ( |
|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Windows Management Instrumentation 2 2 1 | Path Interception | Process Injection 1 2 | Disable or Modify Tools 1 | OS Credential Dumping | System Time Discovery 1 | Remote Services | Archive Collected Data 1 1 | Exfiltration Over Other Network Medium | Ingre Trans |
| Default Accounts | Scripting 1 2 1 | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Scripting 1 2 1 | LSASS Memory | Account Discovery 1 | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | Encry Chan |
| Domain Accounts | Native API 1 2 | Logon Script (Windows) | Logon Script (Windows) | Obfuscated Files or Information 2 | Security Account Manager | File and Directory Discovery 1 | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Non- Appli Layer Proto |
| Local Accounts | Exploitation for Client Execution 1 | Logon Script (Mac) | Logon Script (Mac) | File Deletion 1 | NTDS | System Information Discovery 1 4 5 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Appli Layer Proto |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | Masquerading 1 | LSA Secrets | Query Registry 1 | SSH | Keylogging | Data Transfer Size Limits | Fallba Chan |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | Virtualization/Sandbox Evasion 1 3 | Cached Domain Credentials | Security Software Discovery 3 5 1 | VNC | GUI Input Capture | Exfiltration Over C2 Channel | Multib Comr |
| External Remote Services | Scheduled Task | Startup Items | Startup Items | Process Injection 1 2 | DCSync | Virtualization/Sandbox Evasion 1 3 | Windows Remote Management | Web Portal Capture | Exfiltration Over Alternative Protocol | Comr Used |
| Drive-by Compromise | Command and Scripting Interpreter | Scheduled Task/Job | Scheduled Task/Job | Rundll32 1 | Proc Filesystem | Process Discovery 2 | Shared Webroot | Credential API Hooking | Exfiltration Over Symmetric Encrypted Non-C2 Protocol | Appli Layer |

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Com and ( |
|---|---|---|---|---|---|---|---|---|---|---|
| Exploit Public-Facing Application | PowerShell | At (Linux) | At (Linux) | Masquerading | /etc/passwd and /etc/shadow | System Owner/User Discovery 1 | Software Deployment Tools | Data Staged | Exfiltration Over Asymmetric Encrypted Non-C2 Protocol | Web |
| Supply Chain Compromise | AppleScript | At (Windows) | At (Windows) | Invalid Code Signature | Network Sniffing | Remote System Discovery 1 | Taint Shared Content | Local Data Staging | Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol | File T Proto |

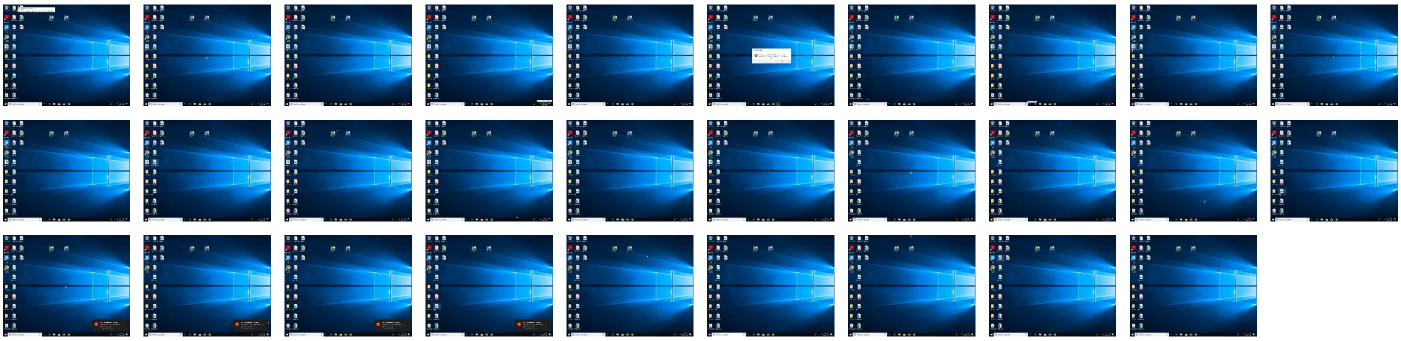
## Behavior Graph

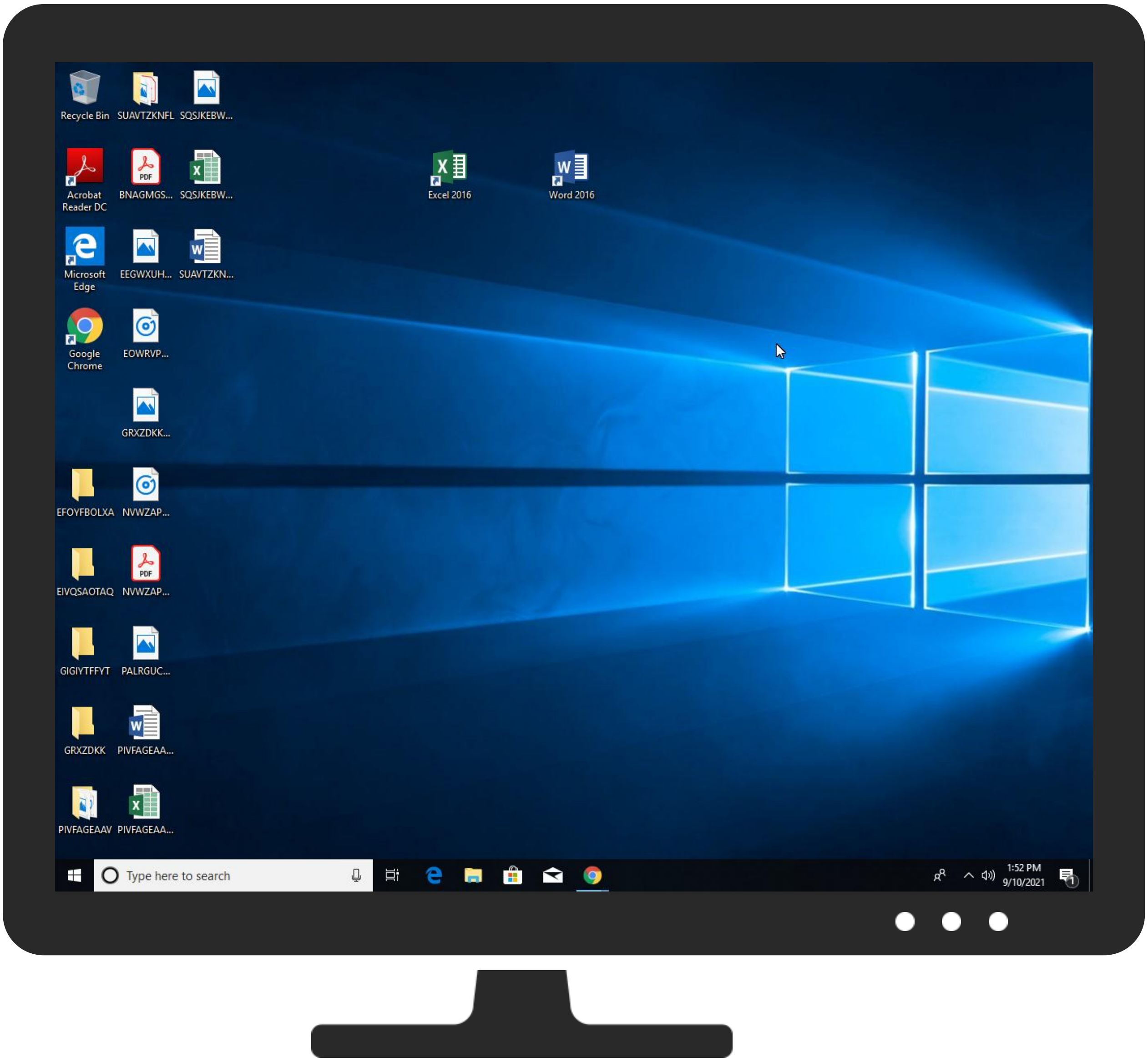

Hide Legend
Behavior Graph
ID: 481181
Sample: start[2021.09.09_15-26].vbs
Startdate: 10/09/2021
Architecture: WINDOWS
Score: 100
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
pop.urlovedstuff.com
Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
Multi AV Scanner detection for domain / URL
Found malware configuration
5 other signatures
started
started
started
WmiPrvSE.exe
wscript.exe
2
dropped
C:\Users\user\AppData\Local\Temp\fum.cpp, PE32
started
Benign windows process drops PE files
VBScript performs obfuscated calls to suspicious functions
De
rundll32.exe
started
rundll32.exe
atl.bigbigpoppa.com
185.251.90.253, 49789, 49790, 49791
SPRINTHOSTRU
Russian Federation
pop.urlovedstuff.com
System process connects to network (likely due to code injection or exploit)
Found evasive API chain (may stop execution after checking system information)
Found API chain indicative of debugger detection
Writes registry values via WMI
Legend:
Process
Signature
Created File
DNS/IP Info
Is Dropped
Is Windows Process
Number of created Registry Values
Number of created Files
Visual Basic
Delphi
Java
.Net C# or VB.NET
C, C++ or other language
Is malicious
Internet

## 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 |
|---|---|---|---|---|
| start[2021.09.09_15-26].vbs | 10% | Virustotal | | Browse |

## Dropped Files

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\fum.cpp | 13% | ReversingLabs | Win32.Worm.Cridex | |

## Unpacked PE Files

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 23.2.rundll32.exe.c20000.0.unpack | 100% | Avira | HEUR/AGEN.1108168 | | Download File |

## Domains

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| pop.urlovedstuff.com | 9% | Virustotal | | Browse |
| atl.bigbigpoppa.com | 9% | Virustotal | | Browse |

## URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://atl.bigbigpoppa.com/ | 100% | Avira URL Cloud | malware | |
| http://pop.urlovedstuff.com/FYLjL0FWG/A8A_2Fylls_2BN6G7XZV/uXdtwH9ZjhHPJVfO4Ke/_2B2DA3Bxr3hT97jg6X5cf/HmT9c0wd9uTFE/mjIXEmZg/7w1x_2BJ7UrOUMBuwkzmQs_/2B_2B90mhB/GdhMF2xI5ZZQZOsRZ/w8ERaF_2FKjr/oJe_2BmPqxj/UioALST3UPW_2B/x25T0SA4ncGBrSmoWvhyD/GJA93v_2Bs5_2FOu/bRGYPwsER1HateV/PYXudbMJvsQ83oCtuH/3_2FsJC5W/WltZ3WhV77sZrxWGfR6s/bNzIeDiXMV8LnHFQlB1/BK37js8oH2L1YJRuiB3U5s/fOdLI1WLm_2Bt/WCukq3AFEXzr/kh2 | 100% | Avira URL Cloud | malware | |
| http://atl.bigbigpoppa.com/R4Q64ljn5F0AeB0LyB/NuqzcVKz_/2FKpDeUm0fBCI1AQABSO/SrwJzbiGX2y5piswKvk/JCT | 100% | Avira URL Cloud | malware | |
| http://pop.bigbigpoppa.com/ | 100% | Avira URL Cloud | malware | |
| http://pop.urlovedstuff.com/FYLjL0FWG/A8A_2Fylls_2BN6G7XZV/uXdtwH9ZjhHPJVfO4Ke/_2B2DA3Bxr3hT97jg6X5c | 100% | Avira URL Cloud | malware | |
| http://atl.bigbigpoppa.com/0su8VV6_2B3_2B/puf6UG3h9deC_2Ft6TxKM/_2FYbenbgPpDMagU/M3qvcdiaQn_2FfY/O5d | 100% | Avira URL Cloud | malware | |

# Domains and IPs

## Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| pop.urlovedstuff.com | 185.251.90.253 | true | true | • 9%, Virustotal, Browse | unknown |
| atl.bigbigpoppa.com | 185.251.90.253 | true | true | • 9%, Virustotal, Browse | unknown |

## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://pop.urlovedstuff.com/FYLjL0FWG/A8A_2Fylls_2BN6G7XZV/uXdtwH9ZjhHPJVfO4Ke/_2B2DA3Bxr3hT97jg6X5cf/HmT9c0wd9uTFE/mjIXEmZg/7w1x_2BJ7UrOUMBuwkzmQs_/2B_2B90mhB/GdhMF2xI5ZZQZOsRZ/w8ERaF_2FKjr/oJe_2BmPqxj/UioALST3UPW_2B/x25T0SA4ncGBrSmoWvhyD/GJA93v_2Bs5_2FOu/bRGYPwsER1HateV/PYXudbMJvsQ83oCtuH/3_2FsJC5W/WltZ3WhV77sZrxWGfR6s/bNzIeDiXMV8LnHFQlB1/BK37js8oH2L1YJRuiB3U5s/fOdLI1WLm_2Bt/WCukq3AFEXzr/kh2 | true | • Avira URL Cloud: malware | unknown |

## URLs from Memory and Binaries

## Contacted IPs

## Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 185.251.90.253 | pop.urlovedstuff.com | Russian Federation | 🇷🇺 | 35278 | SPRINTHOSTRU | true |

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 33.0.0 White Diamond |
| Analysis ID: | 481181 |
| Start date: | 10.09.2021 |
| Start time: | 13:48:06 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 8m 24s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | start[2021.09.09_15-26].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: | 31 |

| | |
|---|---|
| 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: | mal100.troj.evad.winVBS@7/2@4/1 |
| EGA Information: | • Successful, ratio: 100% |
| HDC Information: | • Successful, ratio: 21.2% (good quality ratio 20.6%)<br>• Quality average: 80.8%<br>• Quality standard deviation: 27.2% |
| HCA Information: | • Successful, ratio: 71%<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<br>• Override analysis time to 240s for JS/VBS files not yet terminated |
| Warnings: | Show All |

# Simulations

## Behavior and APIs

| Time | Type | Description |
|---|---|---|
| 13:51:30 | API Interceptor | 1x Sleep call for process: wscript.exe modified |
| 13:52:04 | API Interceptor | 3x Sleep call for process: rundll32.exe modified |

# Joe Sandbox View / Context

## IPs

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 185.251.90.253 | sample.vbs | Get hash | malicious | Browse | |
| | 345678.vbs | Get hash | malicious | Browse | |
| | start[526268].vbs | Get hash | malicious | Browse | |
| | URS8.VBS | Get hash | malicious | Browse | |
| | documentation_446618.vbs | Get hash | malicious | Browse | |
| | start_information[754877].vbs | Get hash | malicious | Browse | |
| | start[873316].vbs | Get hash | malicious | Browse | |
| | documentation[979729].vbs | Get hash | malicious | Browse | |
| | run_documentation[820479].vbs | Get hash | malicious | Browse | |
| | run[476167].vbs | Get hash | malicious | Browse | |
| | run_presentation[645872].vbs | Get hash | malicious | Browse | |
| | documentation[979729].vbs | Get hash | malicious | Browse | |

## Domains

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| atl.bigbigpoppa.com | sample.vbs | Get hash | malicious | Browse | • 185.251.90.253 |
| | 345678.vbs | Get hash | malicious | Browse | • 185.251.90.253 |
| | start[526268].vbs | Get hash | malicious | Browse | • 185.251.90.253 |
| | URS8.VBS | Get hash | malicious | Browse | • 185.251.90.253 |
| | documentation_446618.vbs | Get hash | malicious | Browse | • 185.251.90.253 |
| | start_information[754877].vbs | Get hash | malicious | Browse | • 185.251.90.253 |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | start[873316].vbs | Get hash | malicious | Browse | • 185.251.90.253 |
| | documentation[979729].vbs | Get hash | malicious | Browse | • 185.251.90.253 |
| | run_documentation[820479].vbs | Get hash | malicious | Browse | • 185.251.90.253 |
| | run[476167].vbs | Get hash | malicious | Browse | • 185.251.90.253 |
| | run_presentation[645872].vbs | Get hash | malicious | Browse | • 185.251.90.253 |
| | documentation[979729].vbs | Get hash | malicious | Browse | • 185.251.90.253 |
| pop.urlovedstuff.com | URS8.VBS | Get hash | malicious | Browse | • 185.251.90.253 |
| | documentation[979729].vbs | Get hash | malicious | Browse | • 185.251.90.253 |

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| SPRINTHOSTRU | sample.vbs | Get hash | malicious | Browse | • 185.251.90.253 |
| | 345678.vbs | Get hash | malicious | Browse | • 185.251.90.253 |
| | start[526268].vbs | Get hash | malicious | Browse | • 185.251.90.253 |
| | ZaRfpqeOYY.apk | Get hash | malicious | Browse | • 141.8.192.169 |
| | URS8.VBS | Get hash | malicious | Browse | • 185.251.90.253 |
| | h4AjR43abb.exe | Get hash | malicious | Browse | • 185.251.88.208 |
| | documentation_446618.vbs | Get hash | malicious | Browse | • 185.251.90.253 |
| | start_information[754877].vbs | Get hash | malicious | Browse | • 185.251.90.253 |
| | dAmDdz0YVv.exe | Get hash | malicious | Browse | • 185.251.88.208 |
| | start[873316].vbs | Get hash | malicious | Browse | • 185.251.90.253 |
| | documentation[979729].vbs | Get hash | malicious | Browse | • 185.251.90.253 |
| | run_documentation[820479].vbs | Get hash | malicious | Browse | • 185.251.90.253 |
| | run[476167].vbs | Get hash | malicious | Browse | • 185.251.90.253 |
| | run_presentation[645872].vbs | Get hash | malicious | Browse | • 185.251.90.253 |
| | yXf9mhlpKV.exe | Get hash | malicious | Browse | • 185.251.88.208 |
| | mgdL2TD6Dg.exe | Get hash | malicious | Browse | • 185.251.88.208 |
| | documentation[979729].vbs | Get hash | malicious | Browse | • 185.251.90.253 |
| | Pi2KyLAg44.exe | Get hash | malicious | Browse | • 185.251.88.208 |
| | oClF50dZRG.exe | Get hash | malicious | Browse | • 185.251.88.208 |
| | 2K5KXrsoLH.exe | Get hash | malicious | Browse | • 185.251.88.208 |

## JA3 Fingerprints

**No context**

## Dropped Files

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\fum.cpp | sample.vbs | Get hash | malicious | Browse | |
| | 345678.vbs | Get hash | malicious | Browse | |
| | start[526268].vbs | Get hash | malicious | Browse | |

# Created / dropped Files

| **C:\Users\user\AppData\Local\Temp\adobe.url** | |
|---|---|
| Process: | C:\Windows\System32\wscript.exe |
| File Type: | MS Windows 95 Internet shortcut text (URL=<https://adobe.com/>), ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 108 |
| Entropy (8bit): | 4.699454908123665 |
| Encrypted: | false |
| SSDEEP: | 3:J25YdimVVG/VClAWPUyxAbABGQEZapfpgtovn:J254vVG/4xPpuFJQxHvn |
| MD5: | 99D9EE4F5137B94435D9BF49726E3D7B |
| SHA1: | 4AE65CB58C311B5D5D963334F1C30B0BD84AFC03 |
| SHA-256: | F5BC6CF90B739E9C70B6EA13F5445B270D8F5906E199270E22A2F685D989211E |
| SHA-512: | 7B8A65FE6574A80E26E4D7767610596FEEA1B5225C3E8C7E105C6AC83F5312399EDB4E3798C3AF4151BCA8EF84E3D07D1ED1C5440C8B66B2B8041408F0F2E4F |
| Malicious: | false |
| Reputation: | moderate, very likely benign file |
| Preview: | [{000214A0-0000-0000-C000-000000000046}]..Prop3=19,11..[InternetShortcut]..IDList=..URL=https://adobe.com/.. |

### C:\Users\user\AppData\Local\Temp\fum.cpp

| | |
|---|---|
| Process: | C:\Windows\System32\wscript.exe |
| File Type: | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows |
| Category: | dropped |
| Size (bytes): | 387072 |
| Entropy (8bit): | 6.617827225958404 |
| Encrypted: | false |
| SSDEEP: | 6144:kZv2xLg5Ema5+kMLdcW2Ipsk0AOIjlllll/lllllWQO+XK+Mtw:kn5AUkaqIpWylllll/lllll7O+XLMtw |
| MD5: | D48EBF7B31EDDA518CA13F71E876FFB3 |
| SHA1: | C72880C38C6F1A013AA52D032FC712DC63FE29F1 |
| SHA-256: | 8C5BA29FBEEDF62234916D84F3A857A3B086871631FD87FABDFC0818CF049587 |
| SHA-512: | 59CBBD4ADA4F51650380989A6A024600BB67982255E9F8FFBED14D3A723471B02DAF53A0A05B2E6664FF35CB4C224F9B209FB476D6709A7B33F0A9C060973FB8 |
| Malicious: | **true** |
| Antivirus: | • Antivirus: ReversingLabs, Detection: 13% |
| Joe Sandbox View: | • Filename: sample.vbs, Detection: malicious, Browse<br>• Filename: 345678.vbs, Detection: malicious, Browse<br>• Filename: start[526268].vbs, Detection: malicious, Browse |
| Reputation: | low |
| Preview: | MZ......................@...............................................!..L.!This program cannot be run in DOS mode....$.......\|...8st.8st.8st....st...9st...#st...+st.8su..st...2st...?st...9st...st...9st...9st .Rich8st.........................PE..L......Y...........!.....,..........9........@......................................%O....@.................................p...d................................%..`...T...............................@.. ..........@................................text....*.......,.................. ..`.rdata...~...@.......0.............@..@.data..............................@....gfids.............................@..@.reloc...%.......&.......... .......@..B...................................................................................................................................................................................................................... ....................................... |

## Static File Info

### General

| | |
|---|---|
| File type: | ASCII text, with very long lines, with CRLF line t erminators |
| Entropy (8bit): | 4.847598444077791 |
| TrID: | |
| File name: | start[2021.09.09_15-26].vbs |
| File size: | 1393062 |
| MD5: | 3959f76d91c30f3c14916f80a6c4cf23 |
| SHA1: | 2c918bff7f9073762308af3876777afc8507e3a8 |
| SHA256: | 1d02060d7493d25e46e7cdf76fc05aa6c80493f40db75d4<br>8700f1eb17431191d |
| SHA512: | 5e74bc0322cbec0d955395f9cb43345bc6d40c2ead457a<br>bf5a83a859097327220d7d23d73e8f9a4bbe967a5b73d0<br>a5e522d090f1bcd39cb3f168b4a9a7a14fd |
| SSDEEP: | 12288:SfCepvwq9BTH3FEN9cy59WSpU9lAR4lYtE9E5r<br>f99bh:ipvp9BT1U9cyjUAvmEZbh |
| File Content Preview: | IHGsfsedgfssd = Timer()..For hjdHJGASDF = 1 to 7..W<br>Script.Sleep 1000:..Next..frjekgJHKasd = Timer()..if frjek<br>gJHKasd - IHGsfsedgfssd < 5 Then..Do: KJHSGDflkjsd<br>= 4: Loop..End if ..const VSE = 208..const Aeq = 94..pg<br>oTH = Array(UGM,DP,wy,2,yt,2,2,2,vy,2,2, |

### File Icon

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

## Network Behavior

### Snort IDS Alerts

| Timestamp | Protocol | SID | Message | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|---|---|---|
| 09/10/21-13:52:04.105913 | TCP | 2033204 | ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F) | 49789 | 80 | 192.168.2.3 | 185.251.90.253 |

| Timestamp | Protocol | SID | Message | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|---|---|---|
| 09/10/21-13:52:04.105913 | TCP | 2033203 | ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) | 49789 | 80 | 192.168.2.3 | 185.251.90.253 |
| 09/10/21-13:52:25.037475 | TCP | 2033204 | ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F) | 49790 | 80 | 192.168.2.3 | 185.251.90.253 |
| 09/10/21-13:52:25.037475 | TCP | 2033203 | ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) | 49790 | 80 | 192.168.2.3 | 185.251.90.253 |
| 09/10/21-13:52:46.068609 | TCP | 2033204 | ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F) | 49791 | 80 | 192.168.2.3 | 185.251.90.253 |
| 09/10/21-13:52:46.068609 | TCP | 2033203 | ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) | 49791 | 80 | 192.168.2.3 | 185.251.90.253 |

## Network Port Distribution

## TCP Packets

## UDP Packets

## DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| Sep 10, 2021 13:52:03.637804985 CEST | 192.168.2.3 | 8.8.8.8 | 0x7952 | Standard query (0) | atl.bigbigpoppa.com | A (IP address) | IN (0x0001) |
| Sep 10, 2021 13:52:24.674542904 CEST | 192.168.2.3 | 8.8.8.8 | 0xf4a6 | Standard query (0) | pop.urlovedstuff.com | A (IP address) | IN (0x0001) |
| Sep 10, 2021 13:52:45.707376957 CEST | 192.168.2.3 | 8.8.8.8 | 0xf1f6 | Standard query (0) | atl.bigbigpoppa.com | A (IP address) | IN (0x0001) |
| Sep 10, 2021 13:53:06.561090946 CEST | 192.168.2.3 | 8.8.8.8 | 0x7fa9 | Standard query (0) | pop.urlovedstuff.com | A (IP address) | IN (0x0001) |

## DNS Answers

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Sep 10, 2021 13:52:04.017317057 CEST | 8.8.8.8 | 192.168.2.3 | 0x7952 | No error (0) | atl.bigbigpoppa.com | | 185.251.90.253 | A (IP address) | IN (0x0001) |
| Sep 10, 2021 13:52:24.976217031 CEST | 8.8.8.8 | 192.168.2.3 | 0xf4a6 | No error (0) | pop.urlovedstuff.com | | 185.251.90.253 | A (IP address) | IN (0x0001) |
| Sep 10, 2021 13:52:46.013231993 CEST | 8.8.8.8 | 192.168.2.3 | 0xf1f6 | No error (0) | atl.bigbigpoppa.com | | 185.251.90.253 | A (IP address) | IN (0x0001) |
| Sep 10, 2021 13:53:06.865139961 CEST | 8.8.8.8 | 192.168.2.3 | 0x7fa9 | No error (0) | pop.urlovedstuff.com | | 185.251.90.253 | A (IP address) | IN (0x0001) |

## HTTP Request Dependency Graph

- atl.bigbigpoppa.com
- pop.urlovedstuff.com

## HTTP Packets

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 0 | 192.168.2.3 | 49789 | 185.251.90.253 | 80 | C:\Windows\SysWOW64\rundll32.exe |

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

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Sep 10, 2021 13:52:04.105912924 CEST | 5011 | OUT | GET /R4Q64ljn5F0AeB0LyB/NuqzcVKz_/2FKpDeUm0fBCI1AQABSO/SrwJzbiGX2y5piswKvk/JCT7aFfMHddlV3_2FIkW8P/ayLC_2Bshelva/2X_2Bg56/7jrpWKChL2MGyrBCg5dLHkp/afoZMxsy1T/Wp7_2FPeXCx8Q_2BZ/qOUTFrHwatL_/2B9CZYfq_2B/hvctvVLoqJu_2B/vpIx1k_2FVAj6zT_2F3t3/6fHnbpgCWlIc40kF/GNgoS4_2BmIaDcC/8SXP0dHgwB95tBuoyP/x_2BcO7Jg/2OPTdoZOpI7RlGA8Y18Y/JYFZfFiYFwCa3nBrqzw/H_2B8_2FkkexIGmoFzmcpf/7smS06LtDXKEe/c HTTP/1.1<br>Cache-Control: no-cache<br>Connection: Keep-Alive<br>Pragma: no-cache<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:90.0) Gecko/20100101 Firefox/90.0<br>Host: atl.bigbigpoppa.com |
| Sep 10, 2021 13:52:04.548911095 CEST | 5011 | IN | HTTP/1.1 404 Not Found<br>Server: nginx<br>Date: Fri, 10 Sep 2021 11:52:04 GMT<br>Content-Type: text/html; charset=utf-8<br>Content-Length: 146<br>Connection: close<br>Vary: Accept-Encoding<br>Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a<br>Data Ascii: <html><head><title>404 Not Found</title></head><body><center><h1>404 Not Found</h1></center><hr><center>nginx</center></body></html> |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 1 | 192.168.2.3 | 49790 | 185.251.90.253 | 80 | C:\Windows\SysWOW64\rundll32.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Sep 10, 2021 13:52:25.037475109 CEST | 5012 | OUT | GET /FYLjL0FWG/A8A_2FylIs_2BN6G7XZV/uXdtwH9ZjhHPJVfO4Ke/_2B2DA3Bxr3hT97jg6X5cf/HmT9c0wd9uTFE/mjIXEmZg/7w1x_2BJ7UrOUMBuwkzmQs_/2B_2B90mhB/GdhMF2xI5ZZQZOsRZ/w8ERaF_2FKjr/oJe_2BmPqxj/UioALST3UPW_2B/x25T0SA4ncGBrSmoWvhyD/GJA93v_2Bs5_2FOu/bRGYPwsER1HateV/PYXudbMJvsQ83oCtuH/3_2FsJC5W/WltZ3WhV77sZrxWGfR6s/bNzIeDiXMV8LnHFQlB1/BK37js8oH2L1YJRuiB3U5s/fOdLI1WLm_2Bt/WCukq3AFEXzr/kh2 HTTP/1.1<br>Cache-Control: no-cache<br>Connection: Keep-Alive<br>Pragma: no-cache<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:90.0) Gecko/20100101 Firefox/90.0<br>Host: pop.urlovedstuff.com |
| Sep 10, 2021 13:52:25.510382891 CEST | 5013 | IN | HTTP/1.1 404 Not Found<br>Server: nginx<br>Date: Fri, 10 Sep 2021 11:52:25 GMT<br>Content-Type: text/html; charset=utf-8<br>Content-Length: 146<br>Connection: close<br>Vary: Accept-Encoding<br>Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a<br>Data Ascii: <html><head><title>404 Not Found</title></head><body><center><h1>404 Not Found</h1></center><hr><center>nginx</center></body></html> |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 2 | 192.168.2.3 | 49791 | 185.251.90.253 | 80 | C:\Windows\SysWOW64\rundll32.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Sep 10, 2021 13:52:46.068608999 CEST | 5014 | OUT | GET /0su8VV6_2B3_2B/puf6UG3h9deC_2Ft6TxKM/_2FYbenbgPpDMagU/M3qvcdiaQn_2FfY/O5d7t6b51CsWR3vpDy/zU3pR9vjY/lPgvi3S86qplQEaQf_2B/jxDYlqt8BjtcOWY_2FN/ohwhXl17Lh66734_2Fqn_2/FgCM3Tnuck0nF/J0S1YKxS/oTav10uGKUAnWla7FsZqe_2/BIXpQqvfaR/nMso0hdyU8dnVmjyD/LLoIt20KVY7z/9GJ5tvt7Ozs/NXB1gCveQulFzL/ZrjIdUFvH1uWGi_2BuvX_/2BGZEq0uPSkXlrhP/QwzrBUc1U9Q1ZY4/HzIgE26R/E HTTP/1.1<br>Cache-Control: no-cache<br>Connection: Keep-Alive<br>Pragma: no-cache<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:90.0) Gecko/20100101 Firefox/90.0<br>Host: atl.bigbigpoppa.com |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Sep 10, 2021 13:52:46.509069920 CEST | 5014 | IN | HTTP/1.1 404 Not Found<br>Server: nginx<br>Date: Fri, 10 Sep 2021 11:52:46 GMT<br>Content-Type: text/html; charset=utf-8<br>Content-Length: 146<br>Connection: close<br>Vary: Accept-Encoding<br>Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a<br>Data Ascii: <html><head><title>404 Not Found</title></head><body><center><h1>404 Not Found</h1></center><hr><center>nginx</center></body></html> |

# Code Manipulations

# Statistics

## Behavior

Click to jump to process

# System Behavior

## Analysis Process: wscript.exe PID: 3840 Parent PID: 3388

### General

| | |
|---|---|
| Start time: | 13:48:57 |
| Start date: | 10/09/2021 |
| Path: | C:\Windows\System32\wscript.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\start[2021.09.09_15-26].vbs' |
| Imagebase: | 0x7ff6d0c20000 |
| 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

Show Windows behavior

### File Deleted

## Analysis Process: WmiPrvSE.exe PID: 1304 Parent PID: 792

### General

| | |
|---|---|
| Start time: | 13:51:29 |
| Start date: | 10/09/2021 |

| | |
|---|---|
| Path: | C:\Windows\System32\wbem\WmiPrvSE.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding |
| Imagebase: | 0x7ff66d5c0000 |
| File size: | 488448 bytes |
| MD5 hash: | A782A4ED336750D10B3CAF776AFE8E70 |
| Has elevated privileges: | true |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |
| Reputation: | moderate |

## Analysis Process: rundll32.exe PID: 2396 Parent PID: 1304

### General

| | |
|---|---|
| Start time: | 13:51:29 |
| Start date: | 10/09/2021 |
| Path: | C:\Windows\System32\rundll32.exe |
| Wow64 process (32bit): | false |
| Commandline: | rundll32 C:\Users\user\AppData\Local\Temp\fum.cpp,DllRegisterServer |
| Imagebase: | 0x7ff665ad0000 |
| File size: | 69632 bytes |
| MD5 hash: | 73C519F050C20580F8A62C849D49215A |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

Show Windows behavior

### File Read

## Analysis Process: rundll32.exe PID: 5236 Parent PID: 2396

### General

| | |
|---|---|
| Start time: | 13:51:30 |
| Start date: | 10/09/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32 C:\Users\user\AppData\Local\Temp\fum.cpp,DllRegisterServer |
| Imagebase: | 0x1370000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

| | |
|---|---|
| Yara matches: | - Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000017.00000003.607221952.00000000050C8000.00000004.00000040.sdmp, Author: Joe Security<br>- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000017.00000003.607028050.00000000050C8000.00000004.00000040.sdmp, Author: Joe Security<br>- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000017.00000003.606994412.00000000050C8000.00000004.00000040.sdmp, Author: Joe Security<br>- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000017.00000003.607255595.00000000050C8000.00000004.00000040.sdmp, Author: Joe Security<br>- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000017.00000003.607169997.00000000050C8000.00000004.00000040.sdmp, Author: Joe Security<br>- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000017.00000003.607202425.00000000050C8000.00000004.00000040.sdmp, Author: Joe Security<br>- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000017.00000003.607241313.00000000050C8000.00000004.00000040.sdmp, Author: Joe Security<br>- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000017.00000003.607113605.00000000050C8000.00000004.00000040.sdmp, Author: Joe Security<br>- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000017.00000002.735811134.00000000050C8000.00000004.00000040.sdmp, Author: Joe Security |
| Reputation: | high |

### File Activities

Show Windows behavior

## Analysis Process: WmiPrvSE.exe PID: 1848 Parent PID: 792

### General

| | |
|---|---|
| Start time: | 13:52:02 |
| Start date: | 10/09/2021 |
| Path: | C:\Windows\SysWOW64\wbem\WmiPrvSE.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\sysWOW64\wbem\wmiprvse.exe -secured -Embedding |
| Imagebase: | 0xec0000 |
| File size: | 426496 bytes |
| MD5 hash: | 7AB59579BA91115872D6E51C54B9133B |
| Has elevated privileges: | true |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |
| Reputation: | moderate |

### Registry Activities

Show Windows behavior

# Disassembly

## Code Analysis

Joe Sandbox Cloud Basic 33.0.0 White Diamond