



ID: 339441
Sample Name: sample1.bin
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 03:30:32
Date: 14/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report sample1.bin 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Startup 5
Malware Configuration 5
Yara Overview 5
Sigma Overview 5
Signature Overview 6
AV Detection: 6
Networking: 6
System Summary: 6
Persistence and Installation Behavior: 6
Boot Survival: 6
Hooking and other Techniques for Hiding and Protection: 6
Lowering of HIPS / PFW / Operating System Security Settings: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 10
Domains and IPs 11
Contacted Domains 11
URLs from Memory and Binaries 11
Contacted IPs 15
Public 15
Private 15
General Information 15
Simulations 16
Behavior and APIs 16
Joe Sandbox View / Context 17
IPs 17
Domains 17
ASN 17
JA3 Fingerprints 17
Dropped Files 17
Created / dropped Files 17
Static File Info 25
General 25
File Icon 26
Static OLE Info 26
General 26
OLE File "sample1.doc" 26
Indicators 26
Summary 26
Document Summary 27
Streams with VBA 27
VBA File Name: ThisDocument.cls, Stream Size: 3696 27
General 27

VBA Code Keywords 27
VBA Code 28
Streams 28
Stream Path: \x1CompObj, File Type: data, Stream Size: 114 28
General 28
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096 28
General 28
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096 28
General 28
Stream Path: 1Table, File Type: data, Stream Size: 7386 28
General 28
Stream Path: Data, File Type: data, Stream Size: 187989 29
General 29
Stream Path: Macros/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 367 29
General 29
Stream Path: Macros/PROJECTwm, File Type: data, Stream Size: 41 29
General 29
Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 2845 29
General 29
Stream Path: Macros/VBA/dir, File Type: data, Stream Size: 513 30
General 30
Stream Path: WordDocument, File Type: data, Stream Size: 627764 30
General 30
Network Behavior 30
Snort IDS Alerts 30
UDP Packets 30
DNS Queries 31
DNS Answers 32
Code Manipulations 32
Statistics 32
Behavior 32
System Behavior 32
Analysis Process: WINWORD.EXE PID: 1536 Parent PID: 792 32
General 32
File Activities 33
File Created 33
File Deleted 33
File Moved 33
File Written 34
File Read 44
Registry Activities 44
Key Created 45
Key Value Created 45
Key Value Modified 49
Analysis Process: svchost.exe PID: 1004 Parent PID: 568 55
General 55
File Activities 55
Analysis Process: svchost.exe PID: 6192 Parent PID: 568 55
General 55
File Activities 56
Registry Activities 56
Analysis Process: svchost.exe PID: 6588 Parent PID: 568 56
General 56
File Activities 56
Analysis Process: svchost.exe PID: 6684 Parent PID: 568 56
General 56
Analysis Process: svchost.exe PID: 6720 Parent PID: 568 57
General 57
File Activities 57
Analysis Process: svchost.exe PID: 6776 Parent PID: 568 57
General 57
File Activities 57
Analysis Process: svchost.exe PID: 6792 Parent PID: 568 57
General 57
Analysis Process: svchost.exe PID: 6880 Parent PID: 568 58
General 58
Analysis Process: SgrmBroker.exe PID: 6944 Parent PID: 568 58
General 58
Analysis Process: svchost.exe PID: 6976 Parent PID: 568 58
General 58
Registry Activities 59
Analysis Process: certutil.exe PID: 6392 Parent PID: 4940 59
General 59
File Activities 59
Registry Activities 59

Analysis Process: conhost.exe PID: 6372 Parent PID: 6392 59
General 59
Disassembly 60
Code Analysis 60

Copyright null 2021

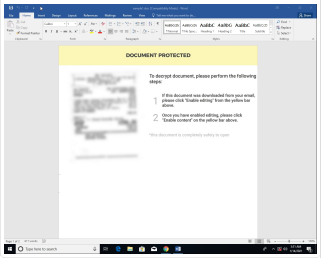
Analysis Report sample1.bin

Overview

General Information

Sample Name:	sample1.bin (renamed file extension from bin to doc)
Analysis ID:	339441
MD5:	7dbd8ecfada1d39.
SHA1:	0d21e2742204d1..
SHA256:	dc40e48d2eb0e5..

Most interesting Screenshot:



Detection

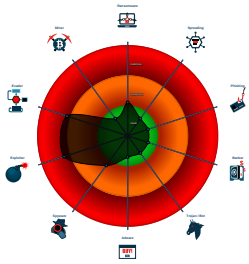


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Snort IDS alert for network traffic (e….
- Changes security center settings (no…
- Creates and opens a fake document…
- Creates processes via WMI
- Document contains an embedded VB…
- Drops PE files to the user root direc…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…

Classification



Startup

- **System is w10x64**
- WINWORD.EXE (PID: 1536 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
- svchost.exe (PID: 1004 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6192 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6588 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6684 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6720 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6776 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6792 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6880 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 6944 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 6976 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- certutil.exe (PID: 6392 cmdline: Certutil -decode C:\Users\Public\Ksh1.xls C:\Users\Public\Ksh1.pdf MD5: EB199893441CED4BBBCB547FE411CF2D)
  - conhost.exe (PID: 6372 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

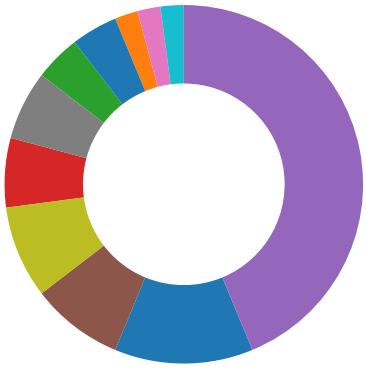
No yara matches

Sigma Overview

No Sigma rule has matched

Copyright null 2021

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- System Summary
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings

Click to jump to signature section

AV Detection:



Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

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)

Document contains an embedded VBA macro with suspicious strings

Persistence and Installation Behavior:



Creates processes via WMI

Boot Survival:



Drops PE files to the user root directory

Hooking and other Techniques for Hiding and Protection:



Creates and opens a fake document (probably a fake document to hide exploiting)

Lowering of HIPS / PFW / Operating System Security Settings:



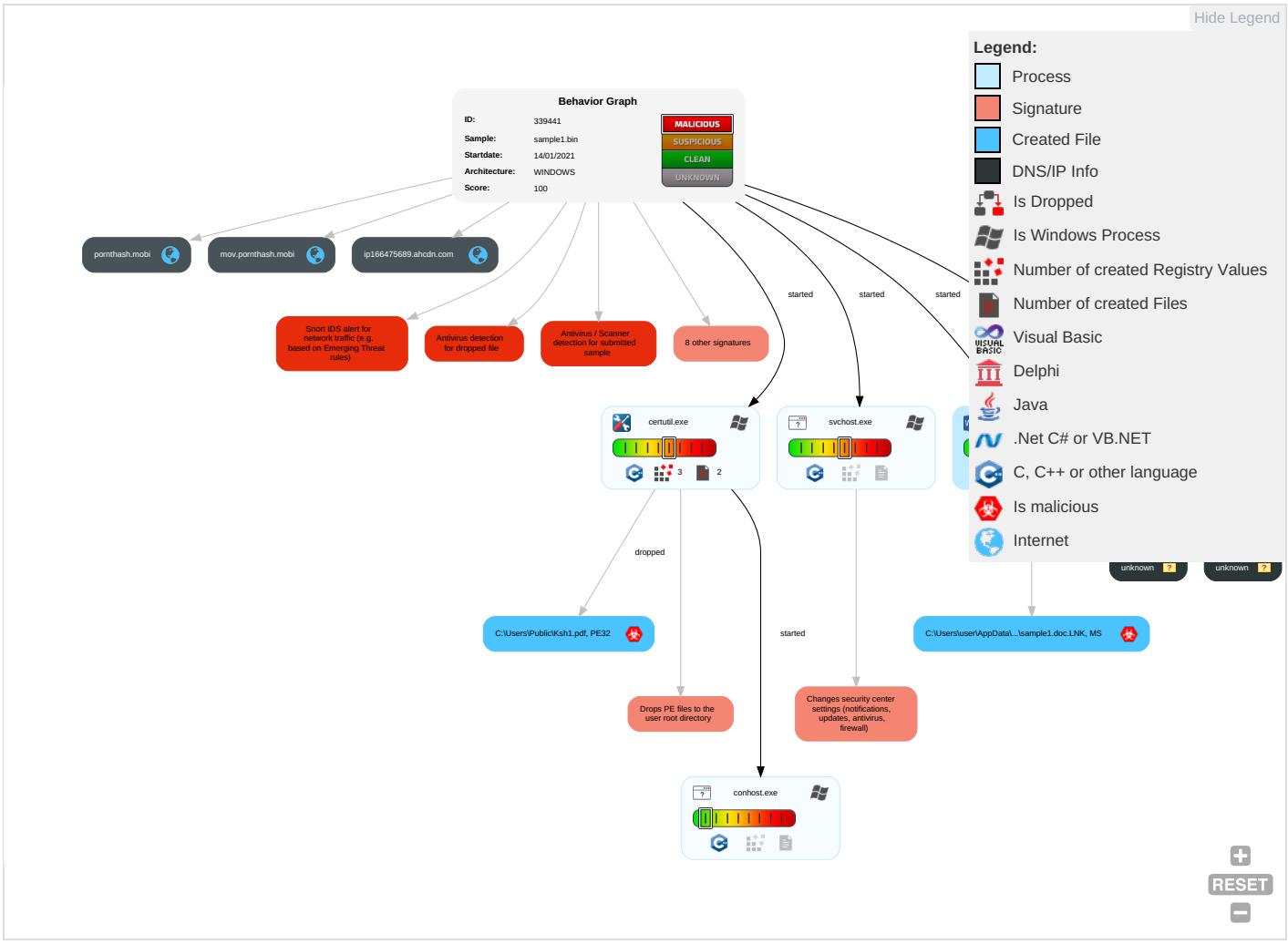
Changes security center settings (notifications, updates, antivirus, firewall)

Mitre Att&ck Matrix

Copyright null 2021

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Net Effe
Valid Accounts	Windows Management Instrumentation 1 1 1	DLL Side-Loading 1	Process Injection 1	Masquerading 1 3 1	OS Credential Dumping	Security Software Discovery 1 2 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 1	Eav Inse Net Cor
Default Accounts	Scripting 1 2	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 2	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exp Rec Cal
Domain Accounts	Exploitation for Client Execution 1 1	Logon Script (Windows)	Extra Window Memory Injection 1	Virtualization/Sandbox Evasion 2	Security Account Manager	Remote System Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exp Tra Loc
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 1 2	LSA Secrets	System Information Discovery 2 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Mar Dev Cor
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jam Der Ser
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rog Acc
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Extra Window Memory Injection 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dov Inse Pro

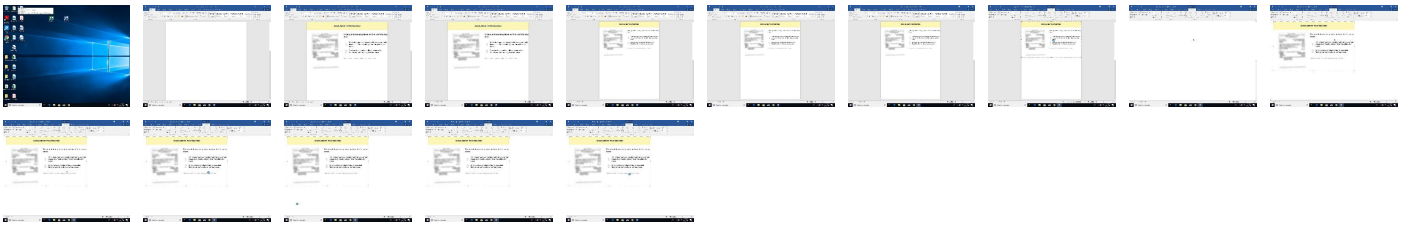
Behavior Graph

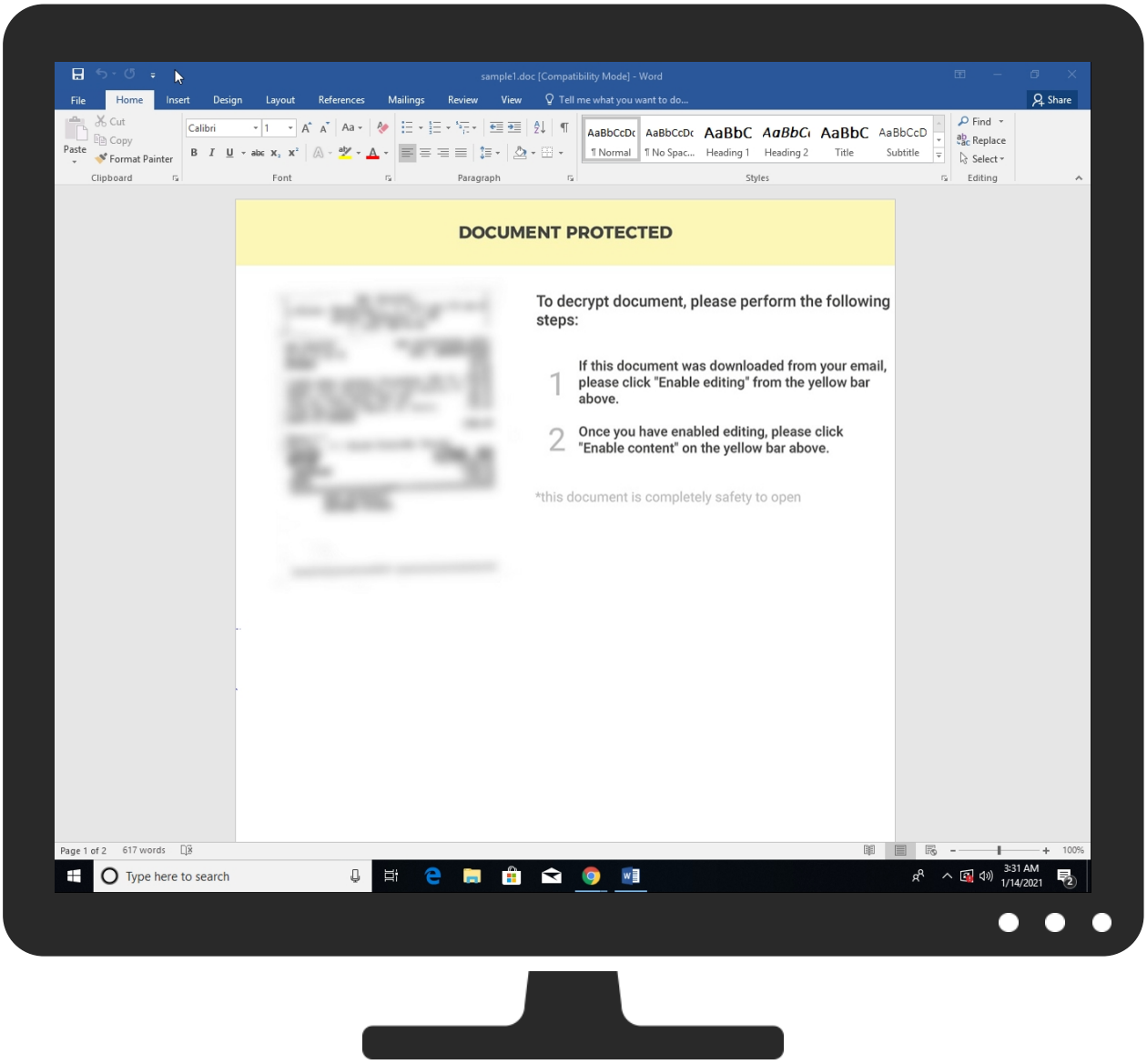


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
sample1.doc	62%	Virustotal		Browse
sample1.doc	46%	Metadefender		Browse
sample1.doc	72%	ReversingLabs	Document-Word.Trojan.Valyria	
sample1.doc	100%	Avira	HEUR/Macro.Downloader.MRYT.Gen	
sample1.doc	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\Ksh1.pdf	100%	Avira	TR/Casdet.xqfgu	
C:\Users\Public\Ksh1.pdf	100%	Joe Sandbox ML		
C:\Users\Public\Ksh1.pdf	41%	Metadefender		Browse
C:\Users\Public\Ksh1.pdf	64%	ReversingLabs	Win32.Trojan.Malrep	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
mov.pornthash.mobi	0%	Virustotal		Browse
pornthash.mobi	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Virustotal		Browse
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Virustotal		Browse
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	

Copyright null 2021

Source	Detection	Scanner	Label	Link
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ip166475689.ahcdn.com	188.209.213.202	true	false		high
mov.pornthash.mobi	104.21.4.61	true	false	• 0%, Virustotal, Browse	unknown
pornthash.mobi	104.21.4.61	true	false	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://login.microsoftonline.com/	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://shell.suite.office.com:1443	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 0000000D.00000002.312307229.0000022F0143D000.00000004.00000001.sdmp	false		high
http://https://autodiscover-s.outlook.com/	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://dev.ditu.live.com/REST/v1/Traffic/Incidents/	svchost.exe, 0000000D.00000003.308691668.0000022F0145A000.00000004.00000001.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 0000000D.00000002.312540794.0000022F0144E000.00000004.00000001.sdmp	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://cdn.entity.	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://wus2-000.contentsync.	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high

Copyright null 2021

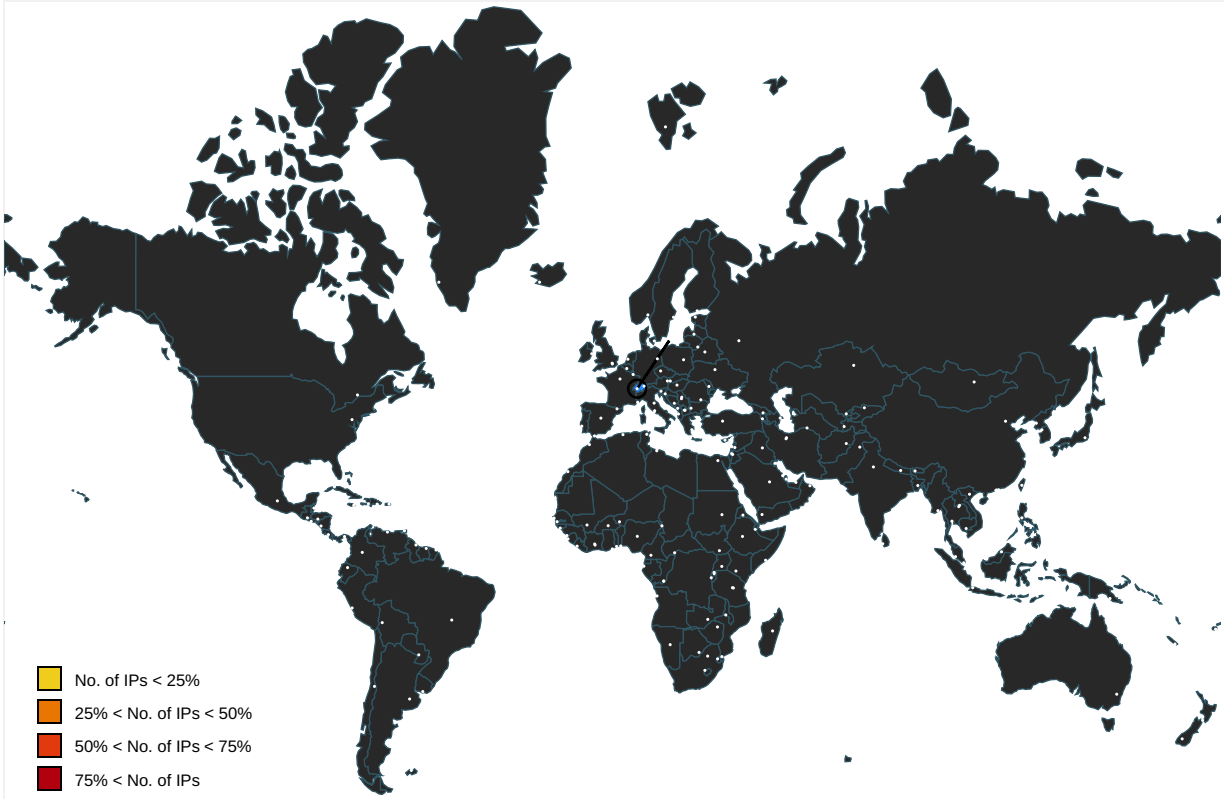
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 0000000D.00000003.308679000.0000022F01461000.00000004.00000001.sdmp	false		high
http://https://powerlift.acompli.net	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://cortana.ai	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://api.aadrm.com/	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 0000000D.00000003.308691668.0000022F0145A000.00000004.00000001.sdmp	false		high
http://https://ofcrecsvcapi-int.azurewebsites.net/	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 0000000D.00000002.312354867.0000022F01442000.00000004.00000001.sdmp	false		high
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://api.microsoftstream.com/api/	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://cr.office.com	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://appexmapsappupdate.blob.core.windows.net	svchost.exe, 0000000D.00000003.308679000.0000022F01461000.00000004.00000001.sdmp	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://www.bingmapsportal.com	svchost.exe, 0000000D.00000002.309801474.0000022F01413000.00000004.00000001.sdmp	false		high
http://https://ecs.office.com/config/v2/Office	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://graph.ppe.windows.net	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://store.office.cn/addinstemplate	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 0000000D.00000003.309006862.0000022F01445000.00000004.00000001.sdmp	false		high
http://https://wus2-000.pagecontentsync.	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 0000000D.00000002.312307229.0000022F0143D000.00000004.00000001.sdmp	false		high
http://https://globaldisco.crm.dynamics.com	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://web.microsoftstream.com/video/	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 0000000D.00000002.312307229.0000022F0143D000.00000004.00000001.sdmp, svchost.exe, 0000000D.00000002.309801474.0000022F01413000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Locations	svchost.exe, 0000000D.00000003.308679000.0000022F01461000.00000004.00000001.sdmp	false		high
http://https://graph.windows.net	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://dataservice.o365filtering.com/	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 0000000D.00000003.286866511.0000022F01431000.00000004.00000001.sdmp	false		high
http://https://officesetup.getmicrosoftkey.com	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 0000000D.00000003.308691668.0000022F0145A000.00000004.00000001.sdmp	false		high
http://https://outlook.office365.com/autodiscover/autodiscover.json	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dynamic.t	svchost.exe, 0000000D.00000003.308667722.0000022F01464000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 0000000D.00000003.308679000.0000022F01461000.00000004.00000001.sdmp	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://weather.service.msn.com/data.aspx	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://apis.live.net/v5.0/	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 0000000D.00000003.308691668.0000022F0145A000.00000004.00000001.sdmp	false		high
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://dev.ditu.live.com/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 0000000D.00000003.308691668.0000022F0145A000.00000004.00000001.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 0000000D.00000003.308691668.0000022F0145A000.00000004.00000001.sdmp	false		high
http://https://management.azure.com	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://incidents.diagnostics.office.com	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 0000000D.00000003.308679000.0000022F01461000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 0000000D.00000002.312307229.0000022F0143D000.00000004.00000001.sdmp	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://api.office.net	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://entitlement.diagnostics.office.com	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 0000000D.00000002.312354867.0000022F01442000.00000004.00000001.sdmp	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://outlook.office.com/	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 0000000D.00000003.308679000.0000022F01461000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 0000000D.00000003.286866511.0000022F01431000.00000004.00000001.sdmp	false		high
http://https://templatelogging.office.com/client/log	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high
http://https://outlook.office365.com/	C8E730CE-6109-4C50-987F-9ABD6FDBDF02.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339441
Start date:	14.01.2021
Start time:	03:30:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	sample1.bin (renamed file extension from bin to doc)
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211

Copyright null 2021

Number of analysed new started processes analysed:	20
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 • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.expl.evad.winDOC@13/28@3/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe • Excluded IPs from analysis (whitelisted): 40.88.32.150, 168.61.161.212, 52.109.88.177, 52.109.76.36, 51.104.139.180, 2.20.84.85, 92.122.213.247, 92.122.213.194, 20.54.26.129, 2.20.142.209, 2.20.142.210, 51.11.168.160 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, officeclient.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, europe.configsvc1.live.com.akadns.net • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
03:31:46	API Interceptor	2x Sleep call for process: svchost.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	0.5952333925020915
Encrypted:	false
SSDEEP:	6:0FsWv0k1GaD0JOCEfMuaaD0JOCEfMKQmDFWv2Al/gz2cE0fMbhEZolrRSQ2hyYl8:0+o7GaD0JcaaD0JwQQFo2Ag/0bjSQJ
MD5:	E3708C8D87BB674A73482801402474E3
SHA1:	1A8D2302B3B042C763528D0CBB69D8B32E5768E7
SHA-256:	78C9AA6D0570C9B49AE1CFC3B608B30FFC8809896D74C59F45016618EE04402A
SHA-512:	1C658EDABBE854C41C322A5609FAD1213E8F6A8EC13344DD19443D1CA8731F11D063747676D8112A6FA8826B83D7DC0DFE1B7774E4C9299A280E4D3CD17FE4
Malicious:	false
Reputation:	low
Preview:	.....:{..(.....y..... ..1C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....y.....&.....e.f.3...w.....3...w.....h..C.:.\.P.r.o.g.r.a.m .D.a.t.a.\.M.i.c.r.o.s.o.f.t.\.N.e.t.w.o.r.k.\.D.o.w.n.l.o.a.d.e.r.\.q.m.g.r...d.b...G..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0xae16a304, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.09580686296721547
Encrypted:	false
SSDEEP:	12:Wzc0+VaO4bl93N+sKozc0+VaO4bl93N+sK:6TjTTj
MD5:	F53ACAEFC5B0D6FA3CAD9BF844F56527
SHA1:	235FDA870F3985D2B06591F1A801429DFC8B7D95
SHA-256:	36D0D2B2DE84A519775E95168C7917292840B9E2F85E159479E627E49DDAAD93
SHA-512:	8DD00AEBF88957E4E3C334C54890270AB8A1449F55C3E1A6D10B78146D17937186E0F9CC1D58C5BA726EC1C5C3B89A6EE5F6CA62072E80ACAAEA0321DF92DA 57
Malicious:	false
Reputation:	low
Preview:	....e.f.3...w.....&.....w.....y..h.(.....3...w.....B.....@..... ....3...w..... .....1.....ywk.....B.e.....y..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.11193516914275213
Encrypted:	false
SSDEEP:	3:+9EvLRV8vAxXl/bJdAtiQu8v/tall:+Yr8vAJt4A8vQ
MD5:	D0E53B0EC516725F17F6813C5587E2CF
SHA1:	E68A9E8F8825657423F377CCAFE9B9D5A4A2BDB4
SHA-256:	00B2DBA055649AAB282B7266498110A79F6DDA6450384FD2DBC87E11A608233A
SHA-512:	8D76613AF2D0CC3555DE2CFFFECB4C73CCB38F021D43FA2526BE8F01BA2465F472DA5BAE6738BCBA179F910A0C1475B6415B9448B8AD9C959E0D5A978DE5C 9B
Malicious:	false
Preview:	d\.U.....3...w.....y.....w.....w.....w....:O.....w.....B.e.....y..... ....

C:\Users\Public\Ksh1.pdf	
Process:	C:\Windows\System32\certutil.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	446976
Entropy (8bit):	7.675102075961339
Encrypted:	false
SSDEEP:	12288:NWSikkQXsGOCAStP1W+TXPc9JXvaWv7j3:ESiL5Sp1W+TYfHj
MD5:	706EA7F029E6BC4DBF845DB3366F9A0E
SHA1:	942443DFB8784066523DB761886115E08C99575F
SHA-256:	FB07F875DC45E6045735513E75A83C50C78154851BD23A645D43EA853E6800AC
SHA-512:	036D5DE7E732302EF81989FBA62ABB1375119FC8141748D6548ED2310E95BDC07468ADA5CBF06C4F721B2B95CAF51E3267D4EF6DB2A2031CF5C8B2ABEE1C15 3
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 41%, Browse • Antivirus: ReversingLabs, Detection: 64%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....)N(.m/F.m/F.m/F....g/F...../F....u/F.?GC.M/F.?GB.b/F.?GE.~/F.d W..h/F.m/G../F..FO.l/F..FF.l/F..F..l/F.m/..l/F..FD.l/F.Richm/F.....PE..L...+._.....!.....d}.....0.....@.....H...X...<.....PB..... .....0|..8.....h|..@.....0..8.....text...g..... ..`.rdata..d\...0...^.....@..@.data.....v.....@....rsrc...PB.. .....D...~.....@..@.reloc.....@..B..... .....

C:\Users\Public\~$Ksh1.doc	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.468762537539322
Encrypted:	false
SSDEEP:	3:Rl/ZdazGlmPREl9lnlt1olF4ditr:RtZu+lHlYBR
MD5:	61CCB0AE1C8D3B3D7D8D942BBA014043
SHA1:	2BC241C791ACAA6CCC41E6F9D0BD1C03E49633F6
SHA-256:	D45E84624442FE9ED3005AE828C8E49FEA3C8D4677AC12F5D58B63FD198D39DB
SHA-512:	E2B419E3A461D7A0196A9D34F4369CD8C94C31905D2886A3B9DABAC56527477A0746E9725F1177725B0C408044A1E989DDEB66BD32C859DD32A4D100F8478AB
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....[...9..x..t`..tP..t.....[...:.....[...;.....T...

C:\Users\Public\~$Ksh1.xls	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.468762537539322
Encrypted:	false
SSDEEP:	3:Rl/ZdazGlmPREl9lnlt1olF4ditr:RtZu+lHlYBR

C:\Users\Public\~$Ksh1.xls	
MD5:	61CCB0AE1C8D3B3D7D8D942BBA014043
SHA1:	2BC241C791ACAA6CCC41E6F9D0BD1C03E49633F6
SHA-256:	D45E84624442FE9ED3005AE828C8E49FEA3C8D4677AC12F5D58B63FD198D39DB
SHA-512:	E2B419E3A461D7A0196A9D34F4369CD8C94C31905D2886A3B9DABAC56527477A0746E9725F1177725B0C408044A1E989DDEB66BD32C859DD32A4D100F8478AB
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....[...9..x..t`..tP..t.....[...:.....[...;.....T...

C:\Users\Public\~WRD0000.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	595972
Entropy (8bit):	5.85065356609278
Encrypted:	false
SSDEEP:	12288:FmkTbAui+yjlKtAMgWffRtpqgnydr6YqVPCY:FmkvVW9gnyQxt9
MD5:	D631AB4CEFF199B52FF4E4B7AAD0199D
SHA1:	F30002C31BF32184507182100942A2012F0B8703
SHA-256:	9DE083F693C144A38D697089F6560A2EFE81B1AD1C5385EC07D6B41BB54B8FFE
SHA-512:	56B3941CD93658F7DF8976213E2DFD5CB74E7ABB651AD26FDA9B7191E675E03289366B32EEDF68D139562A88DBBAE2589FDA8ABBDB756C43E2E605863459A16 2
Malicious:	false
Preview:	TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAA

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\C8E730CE-6109-4C50-987F-9ABD6FDBDF02	
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-01-14T02:31:22">.. Build: 16.0.13712.30526-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRD0001.doc	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	598272
Entropy (8bit):	5.856822353998229
Encrypted:	false
SSDEEP:	12288:FmkwUHZaSyYGKFaaGXuG7ttehnyragYqyPhU:FmkVZm2hnyDxAC
MD5:	7E9AB23E4F7C98AF0A03B64E3C14D7F6
SHA1:	BAD0DC91FB2929FDBF66E569257BABA97E1EC233
SHA-256:	532A6B3137804F51266923EBB06FA6DE43022C2B14F14F6785DDFDA8CA4238EE
SHA-512:	014420FD9C97DBCFF01E11E385E392D8F9AB91D238A418E76C72CD1CD191D2BEE17E7442398C20BA229AD25B0461778F76A88039B1810E20E88A0FE58C43478
Malicious:	false
Preview:	TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAA

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRD0003.doc	
Preview:	TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAA

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRD0497.doc	
Preview:	TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAA

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.1125937326451811
Encrypted:	false
SSDEEP:	12:NCjXm/Ey6q9995+iUl71miM3qQ10nMCldimE8eawHza1miIbMP:Nnl68Cp1tMLyMCldzE9BHza1tII
MD5:	B2C26F4E7D63823BACCFBED8A4F234C0
SHA1:	CF64A7A23F44D0FA20673456F7C8AAB96ED6F045
SHA-256:	27E0AF7C33CA7069BDDF351C871A38E5AA37C232C9879E44ED0EF825BD03DB0D
SHA-512:	F111F19D85AA53C4F090E07A6CB2F3325A37228A1995BE68E80974E2E5DE081ED16A6AEBD2E076ACB1DC5789CA5614F98D627C275DDC8EC1B9493506925FE9F
Malicious:	false
Preview:	.....x...j.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....}I.g0..... .....h.....U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c. a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...e.t.l.....P.P.....x...Z..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11240451627438612
Encrypted:	false
SSDEEP:	12:7jXm/Ey6q9995+iNl71mK2P3qQ10nMCldimE8eawHza1mKk7tsP:Wl68zp1iPLyMCldzE9BHza1AJc
MD5:	C0B0B8426F83EF2F8A60DBF14BE87297
SHA1:	71C06754571BC5D8086EC6A1510E07613FC3CC21
SHA-256:	038D6DC1A0C8E20DC41857093EEBFDFD635CFB4B4272520CAE67817110475267
SHA-512:	AF49F2DAA2511724E57C2702580E84E3CF25C9BEF3E8425A4358DA3B6F57068587A43D6CDCBC7933F9FBBED361D446B8FE7E3D387C74B15AE7F480F64E794A6A
Malicious:	false
Preview:	.....x...rC.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....}I.g0..... .....h.....U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c. a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...e.t.l.....P.P.....x....J..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Ksh1.doc.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Thu Jan 14 10:32:15 2021, mtime=Thu Jan 14 10:32:15 2021, atime=Thu Jan 14 10:32:15 2021, length=595972, window=hide
Category:	dropped
Size (bytes):	1872
Entropy (8bit):	4.595377904117475
Encrypted:	false
SSDEEP:	24:88YOlHDIBAXL+vNx7aB6my8YOlHDIBAXL+vNx7aB6m:8HOljISXLO8B6pHOljISXLO8B6
MD5:	9D3C1C4DB5B591B8D47852847E19FF04
SHA1:	5DA05072C70C918D4C5F8463E64A5E60993F0277
SHA-256:	1BAA0597E24756A8FBBF5563AFF17F2BB0D328158ED40221D4D50CEC9271D335
SHA-512:	20BF966A5547013B5AE089C5FBF0BC968B9FF0610D372E63392A3A4C44BC3E9EE795071F12A338E3DBD1DD176BBA703DD1CA581646FB8F35A40AED5CE0DE89B
Malicious:	false
Preview:	L.....F.... .....i.h...tZ..h...tZ..h.....}....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.[.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1 .8.1.3.....|.1.....R.\..Public..f.....L..R.\.....<.....P.u.b.l.i.c...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.6.....Z.2.....R.\ .Ksh1.doc..B.....R.\.R.\.....h.....K.s.h.1.. .d.o.c.....G.....-.....F.....>.S.....C:\Users\Public\Ksh1.doc..!.....\.....\.....\.....\.....\.....\.P.u.b.l.i.c.\.K.s.h.1...d.o.c.....v..*.cM.jVD.Es.!...`.....X.....377142..... ...!a..%.H.VZAj.....-.....-..!a..%.H.VZAj.....-.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.- .1.0.0.2.....9...1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....L.....F.... .....i.h...tZ..h...tZ..h.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Ksh1.xls.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Thu Jan 14 10:32:13 2021, mtime=Thu Jan 14 10:32:14 2021, atime=Thu Jan 14 10:32:14 2021, length=595972, window=hide
Category:	dropped
Size (bytes):	1872
Entropy (8bit):	4.6054989632820185

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Ksh1.xls.LNK	
Encrypted:	false
SSDEEP:	24:8f2VYOlzIKtSUAXzkF3vTz7aB6myf2VYOlzIKtSUAXzkF3vTz7aB6m:8uqOl1tSjXeLqB6puqOl1tSjXeLqB6
MD5:	623DBB8DBBCA4AAA84C9D0B51D2294AA
SHA1:	ED9CF95C49771F3F4BA706367FDF131F3536EDF8
SHA-256:	869594510F0C7C4AA0B36EC430A5565D02D1228D6FC8357079F83AAA87E79727
SHA-512:	CF1E69A0AC8207A82DF21752018105620BCDD641DE3CADED9FC0F18F2659DA0F2FB4F23F4992103FA3A29D962CD47F53981BAE59BB510D7D8AE28C65C6F1AA6
Malicious:	false
Preview:	L.....F.... ...f...h....V.h....V.h.....}....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.[.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....|.1.....R.\..Public..f.....L..R.\.....<.....&W..P.u.b.l.i.c...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.6.....Z.2.....R.\ .Ksh1.xls..B.....R.\.R.\.....R.....&W..K.s.h.1...x.l.s.....G.....-.....F.....>.S.....C:\Users\Public\Ksh1.xls..!.....\.....\.....\.....\.....\.....\.P.u.b.l.i.c.\.K.s.h.1...x.l.s.....v..*.cM.jVD.Es.!...`.....X.....377142.....!a..%.H.VZAj...~..-.....-..!a..%.H.VZAj...~..-.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9...1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....L.....F.... ...f...h....V.h....V.h.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Public.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Wed Apr 11 22:38:20 2018, mtime=Thu Jan 14 10:32:13 2021, atime=Thu Jan 14 10:32:13 2021, length=4096, window=hide
Category:	dropped
Size (bytes):	1638
Entropy (8bit):	4.631801277891009
Encrypted:	false
SSDEEP:	24:8nEJOMW8As7Rvmi7aB6mySOMW8As7Rvmi7aB6m:8nEJOMCsEzB6pSOMCsEzB6
MD5:	D20EC39F272E325460490D56EB95738F
SHA1:	5B40AEB7E5FBB6C34A62808981C94D7B95E92A68
SHA-256:	B91AEE090146F1DAED24BB4148EF9B471834012BBB1E89223522F82A5CC3E33E
SHA-512:	C7666B9A7BC9205DD57B875DEA7B2DA81DCDCFF1A1CB2E332E16AE61F32ADE62314C1C2EA7B6EA559941D3B86E4F2A415865417E384C8EF0F73DA8ECE7C25936
Malicious:	false
Preview:	L.....F.....,....f...h...f...h.....#....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.[.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....|.1.....Nlv..Public..f.....L..R.[.....<.....o2.P.u.b.l.i.c...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.6.....>.....-.....=.....>.S.....C:\Users\Public.....\....\....\....\....\....\.P.u.b.l.i.c.....v..*.cM.jVD.Es.!...`.....X.....377142.....!a..%.H.VZAj...{..-.....-..!a..%.H.VZAj...{..-.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9...1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....L.....F.....,....ztb.h....V.h.....#....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.[.....:.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	447
Entropy (8bit):	4.3899967917411375
Encrypted:	false
SSDEEP:	12:MWXVqsogWEBIogWEBIogWCogWE+ogWE+qG+ogWC:FXVqs8EBI8EBI8C8E+8E+qG+8C
MD5:	FD72007F8A3EB8088D84D55642E4BD50
SHA1:	E4EA33BEAB25EFE67858F1935F8D5F0BACA65E4B
SHA-256:	51DF55852A44D725F534237277FCF0FC82A78A17E0ABB73ADDBB4F870B075948
SHA-512:	ACEDFBD511ABA21CE1C36E0A404884E0FD250DE10E52B5D0D593ABA14E6C27444EEED66E8D74385134BD8012D32F9982B9EA757346541A94EE3B167D380B7AF4
Malicious:	false
Preview:	[doc]..sample1.doc.LNK=0..sample1.doc.LNK=0..[doc]..sample1.doc.LNK=0..Public.LNK=0..[doc]..sample1.doc.LNK=0..[xls]..Ksh1.xls.LNK=0..Ksh1.xls.LNK=0..[doc]..sample1.doc.LNK=0..[xls]..Ksh1.xls.LNK=0..Ksh1.xls.LNK=0..[doc]..sample1.doc.LNK=0..[xls]..Ksh1.xls.LNK=0..Public.LNK=0..[doc]..sample1.doc.LNK=0..[xls]..Ksh1.xls.LNK=0..Ksh1.doc.LNK=0..[xls]..Ksh1.xls.LNK=0..Ksh1.doc.LNK=0..[doc]..sample1.doc.LNK=0..Ksh1.doc.LNK=0..[xls]..Ksh1.xls.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\sample1.doc.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Thu Jan 14 10:31:16 2021, mtime=Thu Jan 14 10:31:22 2021, atime=Thu Jan 14 10:31:19 2021, length=856064, window=hide
Category:	dropped
Size (bytes):	2076
Entropy (8bit):	4.666899485134856
Encrypted:	false
SSDEEP:	24:84PGKCWv88lQAVKHJlfDLx7aB6my4PGKCWv88lQAVKHJlfDLx7aB6m:84PLlnVKHJlH8B6p4PLlnVKHJlH8B6
MD5:	BD2560F66385CC85CDA44422341BE635
SHA1:	F4066416295028DA67836117A585CEBF2161F96C
SHA-256:	4DB40943AADE005210F9B32BB7C34F9C2986801F3FFAE0A0CC71A70E13D8B3D1
SHA-512:	C772B4A63539F1D005C5427C20D9955468E50DA38DFF66E4241EEEC9852AACBBC54C0F37676FFBD6FE9276B3F5DBE89C6470500B29C6768FA71FDCEC8A6BAFE

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\sample1.doc.LNK	
Malicious:	**true**
Preview:	L.....F.... ... ..h....*.h...g8..h.....P.O. ..:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.[.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qvx..user.<.....Ny..R.[.....S.....,Q.h.a.r.d.z.....~.1.....R.[..Desktop.h.....Ny..R.[.....Y.....>.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9....b.2.....R.[.sample1.doc.H.....R.[.R.[.....].....s.a.m.p.l.e.1...d.o.c.....Q.....-.....P.....>.S.....C:\Users\user\Desktop\sample1.doc..".....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.s.a.m.p.l.e.1...d.o.c.....:..,.LB.)...As...`.....X.....377142.....!a..%.H.VZAj..._..-.....-..!a..%.H.VZAj..._..-.....-.....1SPS.XF.L8C....&.m.q......./...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9...1SPS..mD..pH.H@..=x....

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.468762537539322
Encrypted:	false
SSDEEP:	3:Rl/ZdazGlmPREl9lnlt1olF4ditr:RtZu+lHlYBR
MD5:	61CCB0AE1C8D3B3D7D8D942BBA014043
SHA1:	2BC241C791ACAA6CCC41E6F9D0BD1C03E49633F6
SHA-256:	D45E84624442FE9ED3005AE828C8E49FEA3C8D4677AC12F5D58B63FD198D39DB
SHA-512:	E2B419E3A461D7A0196A9D34F4369CD8C94C31905D2886A3B9DABAC56527477A0746E9725F1177725B0C408044A1E989DDEB66BD32C859DD32A4D100F8478AB
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....[...9..x..t`..tP..t.....[...:.....[...;.....T...

C:\Users\user\Desktop\~$ample1.doc	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.468762537539322
Encrypted:	false
SSDEEP:	3:Rl/ZdazGlmPREl9lnlt1olF4ditr:RtZu+lHlYBR
MD5:	61CCB0AE1C8D3B3D7D8D942BBA014043
SHA1:	2BC241C791ACAA6CCC41E6F9D0BD1C03E49633F6
SHA-256:	D45E84624442FE9ED3005AE828C8E49FEA3C8D4677AC12F5D58B63FD198D39DB
SHA-512:	E2B419E3A461D7A0196A9D34F4369CD8C94C31905D2886A3B9DABAC56527477A0746E9725F1177725B0C408044A1E989DDEB66BD32C859DD32A4D100F8478AB
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....[...9..x..t`..tP..t.....[...:.....[...;.....T...

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBA A
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

Static File Info

General

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Author: User, Template: Normal.dotm, Last Saved By: kirin, Revision Number: 7, Name of Creating Application: Microsoft Office Word, Total Editing Time: 20:00, Create Time/Date: Sun May 10 01:31:00 2020, Last Saved Time/Date: Wed Oct 28 04:44:00 2020, Number of Pages: 2, Number of Words: 89482, Number of Characters: 510049, Security: 0
Entropy (8bit):	6.919205506848504
TrID:	• Microsoft Word document (32009/1) 54.23% • Microsoft Word document (old ver.) (19008/1) 32.20% • Generic OLE2 / Multistream Compound File (8008/1) 13.57%
File name:	sample1.doc
File size:	850432
MD5:	7dbd8ecfada1d39a81a58c9468b91039
SHA1:	0d21e2742204d1f98f6fcabe0544570fd6857dd3
SHA256:	dc40e48d2eb0e57cd16b1792bdccc185440f632783c7bcc87c955e1d4e88fc95
SHA512:	a851ac80b43ebdb8e990c2eb3daabb456516fc40bb43c9f76d0112674dbd6264efce881520744f0502f2962fc0bb4024e7d73ea66d56bc87c0cc6dfde2ab869a
SSDEEP:	12288:emkTbAui+yjlKtAMgWffRtpqgnydr6YqVPCspBZZLFLIx/mBDOq1a:emkvVW9gnyQxtN9eEBDOQa
File Content Preview:	.....>.....g.....j.....Z...[...\...]...^..._...`...a...b...c...d...e...f.....

File Icon

Icon Hash:	74f4c4c6c1cac4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "sample1.doc"

Indicators

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

Summary

Code Page:	1252
Title:	
Subject:	
Author:	User
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	kirin
Revion Number:	7
Total Edit Time:	1200
Create Time:	2020-05-10 00:31:00
Last Saved Time:	2020-10-28 04:44:00

Summary	
Number of Pages:	2
Number of Words:	89482
Number of Characters:	510049
Creating Application:	Microsoft Office Word
Security:	0

Document Summary	
Document Code Page:	1252
Number of Lines:	4250
Number of Paragraphs:	1196
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	1048576

Streams with VBA

VBA File Name: ThisDocument.cls, Stream Size: 3696

General	
Stream Path:	Macros/VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	3696
Data ASCII:	. . . . . { . . . . . ' E . . . . . (. . . . . 2 . . . . . S l e e p . . . . . x . . . . . M E . .
Data Raw:	01 16 03 00 00 18 01 00 00 dc 06 00 00 fc 00 00 00 02 02 00 00 ff ff ff ff e3 06 00 00 7b 0b 00 00 00 00 00 00 01 00 00 00 f1 27 45 f5 00 00 ff ff a3 01 00 00 88 00 00 00 b6 00 ff ff 01 01 28 00 00 00 00 00 32 02 20 00 00 00 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 53 6c 65 70 00 00 00 00 ff ff ff ff 01 00 00 00 ff ff ff ff ff 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
#Else
VB_Name
VB_Creatable
".pdf"):
SetTask(Task
VB_Exposed
Null,
Form_Close()
("doc"):
Formt,
VB_TemplateDerived
Function
(ByVal
String
Right(Range.Text,
String)
Form_Close
Long)
Long,
VB_Customizable
Task,
("xls"):
FileName:=STP
".xls
PtrSafe
Left(ActiveDocument.Paragraphs(One).Range.Text,
Declare
"ThisDocument"
SetTask
False

Keyword
FileFormat:=wdFormatText
Attribute
Private
VB_PredeclaredId
Sleep
VB_GlobalNameSpace
VB_Base
".pdf,In")
Document_Close()

VBA Code

Streams

Stream Path: \x1CompObj, File Type: data, Stream Size: 114

General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	114
Entropy:	4.2359563651
Base64 Encoded:	True
Data ASCII:	. . . . . F . . . M i c r o s o f t W o r d 9 7 - 2 0 0 3 D o c u m e n t . . . . . M S W o r d D o c . . . . . W o r d . D o c u m e n t . 8 . . 9 . q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 06 09 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 20 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 57 6f 72 64 20 39 37 2d 32 30 30 33 20 44 6f 63 75 6d 65 6e 74 00 0a 00 00 00 4d 53 57 6f 72 64 44 6f 63 00 10 00 00 00 57 6f 72 64 2e 44 6f 63 75 6d 65 6e 74 2e 38 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.25569624217
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . h . . . . . p . . . . . | . . . . . ? ! . . . . .
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 e8 00 00 00 0c 00 00 00 01 00 00 00 68 00 00 00 0f 00 00 00 70 00 00 00 05 00 00 00 7c 00 00 00 06 00 00 00 84 00 00 00 11 00 00 00 8c 00 00 00 17 00 00 00 94 00 00 00 0b 00 00 00 9c 00 00 00 10 00 00 00 a4 00 00 00 13 00 00 00 ac 00 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.473780805052
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . l . . . . . (. . . . . 4 . . . . . @ . . . . . L . . . . . T . . . . . \\ . . . . . d . . . . . U s e r . . . . .
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 6c 01 00 00 11 00 00 00 01 00 00 00 90 00 00 00 02 00 00 00 98 00 00 00 03 00 00 00 a4 00 00 00 04 00 00 00 b0 00 00 00 05 00 00 00 c0 00 00 00 06 00 00 00 cc 00 00 00 07 00 00 00 d8 00 00 00 08 00 00 00 ec 00 00 00 09 00 00 00 fc 00 00 00

Stream Path: 1Table, File Type: data, Stream Size: 7386

General	
Stream Path:	1Table
File Type:	data

General	
Stream Size:	7386
Entropy:	5.92077573609
Base64 Encoded:	True
Data ASCII:	. . . . . x . . . . . 6 . . . 6 . . . 6 . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . 6 . . . 6 . . 6 . . . 6 . . . 6 . . . 6 . . . > . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . .
Data Raw:	1e 06 0f 00 12 00 01 00 78 01 0f 00 07 00 03 00 03 00 03 00 00 00 04 00 08 00 00 00 98 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00

Stream Path: Data, File Type: data, Stream Size: 187989

General	
Stream Path:	Data
File Type:	data
Stream Size:	187989
Entropy:	7.97862280177
Base64 Encoded:	True
Data ASCII:	U . . . D . d . . . . . 1 . . . . . N . . . . . C . . . * . . . . A . . . . . t . e . m . p . l . a . t . e . . . . . b . . . . . b r . . . . 7 . a . _ . . . . . D . . . . . n . . . . . b r . . . . 7 . a . _ . . . . P N G . . . . . I H D R . . . O . . . . . 3 0 . u
Data Raw:	55 de 02 00 44 00 64 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 a3 31 e3 1d c3 03 c3 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0f 00 04 f0 4e 00 00 00 b2 04 0a f0 08 00 00 00 01 04 00 00 00 0a 00 00 43 00 0b f0 2a 00 00 00 04 41 01 00 00 00 05 c1 12 00 00 00 06 01 02 00 00 00 ff 01 00 00 08 00 74 00 65 00

Stream Path: Macros/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 367

General	
Stream Path:	Macros/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	367
Entropy:	5.29037636248
Base64 Encoded:	True
Data ASCII:	I D = " { D 4 7 2 8 3 5 A - 3 8 9 1 - 4 D B 9 - 8 6 F 0 - 0 C 1 2 4 A F F D 6 E 1 } " . . D o c u m e n t = T h i s D o c u m e n t / & H 0 0 0 0 0 0 0 0 . . N a m e = " P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " 0 8 0 A E 9 E F E D E F E D E F E D E F E D " . . D P B = " 9 6 9 4 7 7 F B 8 B 0 7 1 8 0 8 1 8 0 8 1 8 " . . G C = " 2 4 2 6 C 5 8 9 D D 1 6 D E 1 6 D E E 9 " . . . . [H o s t E x t e n d e r I n f o]
Data Raw:	49 44 3d 22 7b 44 34 37 32 38 33 35 41 2d 33 38 39 31 2d 34 44 42 39 2d 38 36 46 30 2d 30 43 31 32 34 41 46 46 44 36 45 31 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 44 6f 63 75 6d 65 6e 74 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4e 61 6d 65 3d 22 50 72 6f 6a 65 63 74 22 0d 0a 48 65 6c 70 43 6f 6e 74 65 78 74 49 44 3d 22 30 22 0d 0a 56 65 72 73 69 6f 6e 43 6f 6d 70 61 74 69

Stream Path: Macros/PROJECTwm, File Type: data, Stream Size: 41

General	
Stream Path:	Macros/PROJECTwm
File Type:	data
Stream Size:	41
Entropy:	3.07738448508
Base64 Encoded:	False
Data ASCII:	T h i s D o c u m e n t . T . h . i . s . D . o . c . u . m . e . n . t . . . . .
Data Raw:	54 68 69 73 44 6f 63 75 6d 65 6e 74 00 54 00 68 00 69 00 73 00 44 00 6f 00 63 00 75 00 6d 00 65 00 6e 00 74 00 00 00 00 00

Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 2845

General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	2845
Entropy:	4.32828178006
Base64 Encoded:	False

General	
Data ASCII:	. a . . .

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 03:31:20.493016005 CET	60100	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:31:20.552378893 CET	53	60100	8.8.8.8	192.168.2.3
Jan 14, 2021 03:31:22.347606897 CET	53195	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:31:22.404367924 CET	53	53195	8.8.8.8	192.168.2.3
Jan 14, 2021 03:31:22.934644938 CET	50141	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:31:22.995167971 CET	53	50141	8.8.8.8	192.168.2.3
Jan 14, 2021 03:31:23.446079969 CET	53023	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:31:23.494133949 CET	53	53023	8.8.8.8	192.168.2.3
Jan 14, 2021 03:31:23.939429045 CET	50141	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:31:23.998469114 CET	53	50141	8.8.8.8	192.168.2.3
Jan 14, 2021 03:31:24.955398083 CET	50141	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:31:25.014638901 CET	53	50141	8.8.8.8	192.168.2.3
Jan 14, 2021 03:31:26.955465078 CET	50141	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:31:27.014661074 CET	53	50141	8.8.8.8	192.168.2.3
Jan 14, 2021 03:31:30.971551895 CET	50141	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:31:31.023490906 CET	53	50141	8.8.8.8	192.168.2.3
Jan 14, 2021 03:31:43.270042896 CET	49563	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:31:43.318037033 CET	53	49563	8.8.8.8	192.168.2.3
Jan 14, 2021 03:31:43.455792904 CET	51352	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:31:43.503793955 CET	53	51352	8.8.8.8	192.168.2.3
Jan 14, 2021 03:31:44.264404058 CET	59349	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:31:44.312263012 CET	53	59349	8.8.8.8	192.168.2.3
Jan 14, 2021 03:31:45.099395990 CET	57084	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:31:45.155900955 CET	53	57084	8.8.8.8	192.168.2.3
Jan 14, 2021 03:31:45.982577085 CET	58823	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:31:46.030450106 CET	53	58823	8.8.8.8	192.168.2.3
Jan 14, 2021 03:31:46.783137083 CET	57568	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:31:46.831110954 CET	53	57568	8.8.8.8	192.168.2.3
Jan 14, 2021 03:31:47.558320999 CET	50540	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:31:47.609205961 CET	53	50540	8.8.8.8	192.168.2.3
Jan 14, 2021 03:31:48.325836897 CET	54366	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:31:48.373833895 CET	53	54366	8.8.8.8	192.168.2.3
Jan 14, 2021 03:31:49.091344118 CET	53034	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:31:49.147531986 CET	53	53034	8.8.8.8	192.168.2.3
Jan 14, 2021 03:31:50.035516977 CET	57762	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:31:50.093086004 CET	53	57762	8.8.8.8	192.168.2.3
Jan 14, 2021 03:31:52.749440908 CET	55435	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:31:52.818248034 CET	53	55435	8.8.8.8	192.168.2.3
Jan 14, 2021 03:32:04.694058895 CET	50713	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:32:04.760720015 CET	53	50713	8.8.8.8	192.168.2.3
Jan 14, 2021 03:32:05.598315001 CET	56132	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:32:05.659096956 CET	53	56132	8.8.8.8	192.168.2.3
Jan 14, 2021 03:32:19.660710096 CET	58987	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:32:19.708764076 CET	53	58987	8.8.8.8	192.168.2.3
Jan 14, 2021 03:32:21.869105101 CET	56579	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:32:21.936005116 CET	53	56579	8.8.8.8	192.168.2.3
Jan 14, 2021 03:32:23.872899055 CET	60633	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:32:23.939750910 CET	53	60633	8.8.8.8	192.168.2.3
Jan 14, 2021 03:32:24.422291994 CET	61292	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:32:24.517784119 CET	53	61292	8.8.8.8	192.168.2.3
Jan 14, 2021 03:32:24.752584934 CET	63619	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:32:24.800654888 CET	53	63619	8.8.8.8	192.168.2.3
Jan 14, 2021 03:32:54.230439901 CET	64938	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:32:54.278379917 CET	53	64938	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2021 03:32:23.872899055 CET	192.168.2.3	8.8.8.8	0x9b6d	Standard query (0)	pornthash.mobi	A (IP address)	IN (0x0001)
Jan 14, 2021 03:32:24.422291994 CET	192.168.2.3	8.8.8.8	0xd192	Standard query (0)	mov.pornthash.mobi	A (IP address)	IN (0x0001)
Jan 14, 2021 03:32:24.752584934 CET	192.168.2.3	8.8.8.8	0xe98e	Standard query (0)	ip166475689.ahcdn.com	A (IP address)	IN (0x0001)

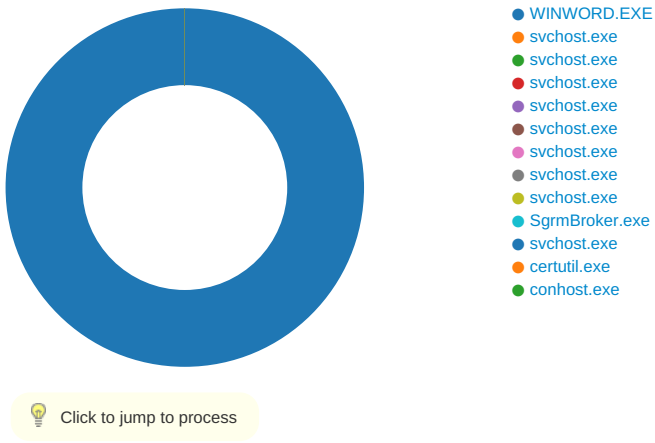
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2021 03:32:23.939750910 CET	8.8.8.8	192.168.2.3	0x9b6d	No error (0)	pornthash.mobi		104.21.4.61	A (IP address)	IN (0x0001)
Jan 14, 2021 03:32:23.939750910 CET	8.8.8.8	192.168.2.3	0x9b6d	No error (0)	pornthash.mobi		172.67.154.11	A (IP address)	IN (0x0001)
Jan 14, 2021 03:32:24.517784119 CET	8.8.8.8	192.168.2.3	0xd192	No error (0)	mov.pornthash.mobi		104.21.4.61	A (IP address)	IN (0x0001)
Jan 14, 2021 03:32:24.517784119 CET	8.8.8.8	192.168.2.3	0xd192	No error (0)	mov.pornthash.mobi		172.67.154.11	A (IP address)	IN (0x0001)
Jan 14, 2021 03:32:24.800654888 CET	8.8.8.8	192.168.2.3	0xe98e	No error (0)	ip166475689.ahcdn.com		188.209.213.202	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 1536 Parent PID: 792

General

Start time:	03:31:20
Start date:	14/01/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x350000
File size:	1937688 bytes
MD5 hash:	0B9AB9B9C4DE429473D6450D4297A123
Has elevated privileges:	true
Has administrator privileges:	true

Copyright null 2021

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\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	66AD977C	unknown
C:\Users\user\AppData\Local\Temp\~DF79ACFDBB249F05E2.TMP	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	66A05805	unknown
C:\Users\Public\~WRD0000.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	66A22C2C	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRD0001.doc	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	66A22C2C	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRD0002.doc	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	66A22C2C	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRD0003.doc	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	66A22C2C	unknown
C:\Users\Public\~$Ksh1.xls	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	66A22C2C	unknown
C:\Users\Public\~WRD0004.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	66A22C2C	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRD0005.doc	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	66A22C2C	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRD0364.doc	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	66A22C2C	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRD0497.doc	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	66A22C2C	unknown
C:\Users\Public\~$Ksh1.doc	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	66A22C2C	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DF79ACFDBB249F05E2.TMP	success or wait	1	66A05805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRD0001.doc	success or wait	1	66A22C2C	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRD0003.doc	success or wait	1	66A22C2C	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRD0002.doc	success or wait	1	66A22C2C	unknown
C:\Users\user\AppData\Local\Temp\~$imgs.htm	success or wait	1	66A22C2C	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRD0005.doc	success or wait	1	66A22C2C	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRD0497.doc	success or wait	1	66A22C2C	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRD0364.doc	success or wait	1	66A22C2C	unknown
C:\Users\Public\~$Ksh1.xls	success or wait	1	66A22C2C	unknown

File Moved

Copyright null 2021

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\Public\~WRD0000.tmp	C:\Users\Public\Ksh1.xls	success or wait	1	66A22C2C	unknown
C:\Users\Public\~WRD0004.tmp	C:\Users\Public\Ksh1.doc	success or wait	1	66A22C2C	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRD0002.doc	unknown	26112	54 00 56 00 71 00 51 00 41 00 41 00 4d 00 41 00 41 00 41 00 41 00 45 00 41 00 41 00 41 00 41 00 2f 00 2f 00 38 00 41 00 41 00 4c 00 67 00 41 00 41 00 41 00 41 00 41 00 41 00 41 00 41 00 41 00 51 00 41 00 41 00 41 00 41 00 41 00 41 00 41 00 41 00 41

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRD0002.doc	unknown	26112	78 00 34 00 5a 00 6b 00 44 00 51 00 41 00 41 00 41 00 41 00 41 00 41 00 4d 00 65 00 47 00 61 00 41 00 30 00 41 00 41 00 41 00 41 00 41 00 41 00 41 00 44 00 48 00 68 00 6d 00 77 00 4e 00 41 00 41 00 41 00 41 00 41 00 41 00 41 00 41 00 41 00 41 00 78 00 34 00 5a 00 77 00 44 00 51 00 41 00 41 00 41 00 41 00 41 00 41 00 41 00 41 00 4d 00 65 00 47 00 64 00 41 00 30 00 41 00 41 00 41 00 41 00 41 00 41 00 44 00 48 00 68 00 6e 00 67 00 4e 00 41 00 41 00 41 00 41 00 41 00 41 00 41 00 41 00 78 00 34 00 5a 00 38 00 44 00 51 00 41 00 41 00 41 00 41 00 41 00 41 00 41 00 4d 00 65 00 47 00 67 00 41 00 30 00 41 00 41 00 41 00 41 00 41 00 41 00 44 00 48 00 68 00 6f 00 51 00 4e 00 41 00 41 00 41 00 41 00 41 00 41 00 41 00 41 00 78 00 34 00 61 00 49 00 44 00 51 00 41 00 41	x.4.Z.k.D.Q.A.A.A.A.A.A.A.M.e.G.a.A.0.A.A.A.A.A.A.A.D.H.h.m.w.N.A.A.A.A.A.A.A.A.x.4.Z.w.D.Q.A.A.A.A.A.A.M.e.G.d.A.0.A.A.A.A.A.A.D.H.h.n.g.N.A.A.A.A.A.A.A.A.x.4.Z.8.D.Q.A.A.A.A.A.A.M.e.G.g.A.0.A.A.A.A.A.A.D.H.h.o.Q.N.A.A.A.A.A.A.A.A.x.4.a.I.D.Q.A.A	success or wait	41	66A22C2C	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRD0001.doc	unknown	15360	78 34 62 6b 46 41 41 41 41 41 41 41 41 4d 65 47 36 42 51 41 41 41 41 41 41 41 41 44 48 68 75 77 55 41 41 41 41 41 41 41 41 78 34 62 77 46 41 41 41 41 41 41 41 41 4d 65 47 39 42 51 41 41 41 41 41 41 41 44 48 68 76 67 55 41 41 41 41 41 41 41 78 34 62 38 46 41 41 41 41 41 41 41 41 4d 65 47 41 42 55 41 41 41 41 41 41 41 44 48 68 67 51 56 41 41 41 41 41 41 41 41 78 34 59 49 46 51 41 41 41 41 41 41 41 4d 65 47 44 42 55 41 41 41 41 41 41 41 44 48 68 68 41 56 41 41 41 41 41 41 41 78 34 59 55 46 51 41 41 41 41 41 41 41 4d 65 47 47 42 55 41 41 41 41 41 41 41 44 48 68 68 77 56 41 41 41 41 41 41 41 78 34 59 67 46 51 41 41 41 41 41 41 41 4d 65 47 4a 42 55 41 41 41 41 41 41 41 44 48 68 69 67 56 41 41 41 41 41 41 41 78 34 59 73 46 51 41 41 41 41 41 41 41 4d 65	x4bkFAAAAAAAAMeG6BQAAAAAAADHhuwUAAAAAAAAx4bwFAAAAAAAAMeG9BQAAAAAAADHhvgUAAAAAAAAx4b8FAAAAAAAAMeGABUAAAAAAADHhgQVAAAAAAAAx4YIFQAAAAAAAMeGDBUAAAAAAADHhhAVAAAAAAAAx4YUFQAAAAAAAMeGGBUAAAAAAADHhhwVAAAAAAAAx4YgFQAAAAAAAMeGJBUAAAAAAADHhigVAAAAAAAAx4YsFQAAAAAAAMe	success or wait	41	66A22C2C	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRD0002.doc	unknown	28160	57 00 56 00 6d 00 46 00 77 00 48 00 51 00 6e 00 67 00 33 00 67 00 6b 00 41 00 48 00 77 00 68 00 78 00 30 00 58 00 38 00 2f 00 76 00 2f 00 2f 00 2f 00 37 00 41 00 42 00 36 00 78 00 2b 00 4c 00 52 00 65 00 79 00 4c 00 41 00 44 00 50 00 4a 00 67 00 54 00 67 00 46 00 41 00 41 00 44 00 41 00 44 00 35 00 54 00 42 00 69 00 38 00 48 00 44 00 69 00 32 00 58 00 6f 00 78 00 30 00 58 00 38 00 2f 00 76 00 2f 00 2f 00 2f 00 2f 00 7a 00 4c 00 41 00 69 00 30 00 33 00 77 00 5a 00 49 00 6b 00 4e 00 41 00 41 00 41 00 41 00 41 00 46 00 6c 00 66 00 58 00 6c 00 76 00 4a 00 77 00 31 00 57 00 4c 00 37 00 4f 00 6a 00 51 00 42 00 41 00 41 00 41 00 68 00 63 00 42 00 30 00 44 00 34 00 42 00 39 00 43 00 41 00 42 00 31 00 43 00 54 00 50 00 41 00 75 00 51 00 79 00 59 00 41 00 52 00 43 00 48	W.V.m.F.w.H.Q.n.g.3.g.k.A.H.w. h.x.0.X.8./.v./././.7.A.B.6.x. +.L.R.e.y.L.A.D.P.J.g.T.g.F.A. A.D.A.D.5.T.B.i.8.H.D.i.2.X.o. x.0.X.8./.v./././.z.L.A.i.0.3. w.Z.I.k.N.A.A.A.A.A.A.F.I.f.X.l. v.J.w.1.W.L.7.O.j.Q.B.A.A.A.h. c.B.0.D.4.B.9.C.A.B.1.C.T.P.A.u.Q.y.Y.A.R.C.H	success or wait	1	66A22C2C	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRD0002.doc	unknown	5640	4f 00 44 00 49 00 38 00 4d 00 6b 00 41 00 79 00 52 00 44 00 4a 00 49 00 4d 00 6b 00 77 00 79 00 55 00 44 00 4a 00 55 00 4d 00 6c 00 67 00 79 00 58 00 44 00 4a 00 67 00 4d 00 6d 00 51 00 79 00 61 00 44 00 4a 00 73 00 4d 00 6e 00 41 00 79 00 64 00 44 00 4a 00 34 00 4d 00 6e 00 77 00 79 00 67 00 44 00 4b 00 45 00 4d 00 6f 00 67 00 79 00 6a 00 44 00 4b 00 51 00 4d 00 70 00 51 00 79 00 6d 00 44 00 4b 00 63 00 4d 00 71 00 41 00 79 00 70 00 44 00 4b 00 6f 00 4d 00 71 00 77 00 79 00 73 00 44 00 4b 00 30 00 4d 00 72 00 67 00 79 00 76 00 44 00 4c 00 41 00 4d 00 73 00 51 00 79 00 79 00 44 00 4c 00 4d 00 4d 00 74 00 41 00 79 00 31 00 44 00 4c 00 59 00 4d 00 74 00 77 00 79 00 34 00 44 00 4c 00 6b 00 4d 00 75 00 67 00 79 00 37 00 44 00 4c 00 77 00 4d 00 76 00 51 00 79	O.D.I.8.M.k.A.y.R.D.J.I.M.k.w. y.U.D.J.U.M.I.g.y.X.D.J.g.M.m. Q.y.a.D.J.s.M.n.A.y.d.D.J.4.M. n.w.y.g.D.K.E.M.o.g.y.j.D.K.Q. M.p.Q.y.m.D.K.c.M.q.A.y.p.D.K. o.M.q.w.y.s.D.K.0.M.r.g.y.v.D. L.A.M.s.Q.y.y.D.L.M.M.t.A.y.1. D.L.Y.M.t.w.y.4.D.L.k.M.u.g.y.7.D.L.w.M.v.Q.y	success or wait	1	66A22C2C	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRD0003.doc	unknown	32256	54 56 71 51 41 41 4d 41 41 41 41 45 41 41 41 41 2f 2f 38 41 41 4c 67 41 41 41 41 41 41 41 41 41 41 51 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 43 41 45 41 41 41 34 66 75 67 34 41 74 41 6e 4e 49 62 67 42 54 4d 30 68 56 47 68 70 63 79 42 77 63 6d 39 6e 63 6d 46 74 49 47 4e 68 62 6d 35 76 64 43 42 69 5a 53 42 79 64 57 34 67 61 57 34 67 52 45 39 54 49 47 31 76 5a 47 55 75 44 51 30 4b 4a 41 41 41 41 41 41 41 41 41 41 41 70 54 69 69 6a 62 53 39 47 38 47 30 76 52 76 42 74 4c 30 62 77 32 62 4f 33 38 47 63 76 52 76 44 5a 73 37 58 77 47 69 39 47 38 4e 6d 7a 74 50 42 31 4c 30 62 77 50 30 64 44 38 55 30 76 52 76 41 2f 52 30 4c 78 59 69 39 47 38 44 39 48 52 66 46 2b 4c 30 62	TVqQAAMAAAAEAAAA//8AALgAAAAAAA AAQAAAAAAAAAAAAAA AAAAAAAAAAAA AAAAAAAAAAAAAAAAAA AACAEAAA4fug 4AtAnNIbgBTM0hVGhpcy Bwcm9ncmFt IGNhbm5vdCBiZSBydW4g aW4gRE9TIG 1vZGUuDQ0KJAAAAAAA AAApTiijbS9G 8G0vRvBtL0bw2bO38Gcv RvDZs7XwGi 9G8NmztPB1L0bwP0dD8 U0vRvA/R0Lx Yi9G8D9HRfF+L0b	success or wait	36	66A22C2C	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRD0003.doc	unknown	15364	53 66 42 34 34 2f 53 33 39 2f 4c 55 76 55 5a 33 53 61 46 73 32 6f 5a 73 33 63 70 4e 73 47 57 78 4c 66 46 66 53 45 78 5a 73 73 59 5a 32 77 76 38 65 54 6f 6c 34 63 35 62 4f 6b 41 58 57 75 36 66 39 4b 2b 54 48 74 67 65 4d 65 46 6a 30 71 4f 4b 64 51 53 6f 54 4c 2b 57 67 6a 69 69 32 41 51 6c 75 30 6a 66 31 43 36 42 42 6e 5a 46 73 32 4b 34 65 41 32 75 47 63 4f 57 53 69 6c 31 39 33 5a 65 61 75 35 50 59 6f 4a 6c 76 76 4a 78 2f 69 50 66 4d 48 67 4f 43 57 32 37 73 70 79 55 4a 6f 57 48 79 6a 4f 49 41 73 5a 6f 61 30 76 7a 4e 54 78 4b 33 65 58 6a 56 73 71 70 35 39 55 73 61 77 6a 7a 4f 42 44 59 48 2f 30 61 46 71 33 6c 4f 54 78 45 69 56 4b 52 41 6d 43 36 49 4e 6f 45 63 78 73 62 39 43 2f 56 33 4e 75 42 34 41 56 54 4a 55 6f 70 31 41 41 70 50 7a 69 62 49 4e 68 70 35 59	SfB44/S39/LUvUZ3SaFs2oZs3cpNsG WxLfFfSExZssYZ2wv8eTol4c5bOkAX Wu6f9K+THtgeMeFj0qOKdQSoTL+Wgj ii2AQlu0jf1C6BBnZFs2K4eA2uGcOW Silj193Zeau5PYoJlvvJx/iPfMHgOC W27spyUJoWHyjOIAsZoa0vzNTxK3eX jVsqp59UsawjzOBDYH/0aFq3lOTxEi VKRAmC6INoEcxsb9C/V3NuB4AVTJUo p1AApPzibINhp5Y	success or wait	1	66A22C2C	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\~WRD0000.tmp	unknown	32256	54 56 71 51 41 41 4d 41 41 41 41 45 41 41 41 41 2f 2f 38 41 41 4c 67 41 41 41 41 41 41 41 41 41 41 51 41 41 41 41 41 41 41 41 41 41

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\~$Ksh1.xls	unknown	108	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 00 00 00 00 01 00 00 00 ee 5b 9f ec 00 39 00 8c 78 8f d4 74 60 8f d4 74 50 8f d4 74 01 00 00 00 00 00 00 00 80 00 00 00 ea 5b 9b ec 00 3a 00 88 00 00 00 00 00 00 00 00 05 00 00 00 18 00 00 00 00 00 00 00 01 00 00 00 f6 5b 87 ec 00 3b 00 8c 00 00 00 00 00 00 00 00 54 00 00 00	..p.r.a.t.e.s.h.....[...9 ..x..t`..tP..t.....[.. .:.....[...;.....T...	success or wait	1	66A22C2C	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRD0364.doc	unknown	26112	54 00 56 00 71 00 51 00 41 00 41 00 4d 00 41 00 41 00 41 00 41 00 45 00 41 00 41 00 41 00 41 00 2f 00 2f 00 38 00 41 00 41 00 4c 00 67 00 41 00 41 00 41 00 41 00 41 00 41 00 41 00 41 00 41 00 41 00 51 00 41 00 41 00 41 00 41 00 41 00 41 00 41 00 41 00 41 00 41

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRD0005.doc	unknown	19456	54 56 71 51 41 41 4d 41 41 41 41 45 41 41 41 41 2f 2f 38 41 41 4c 67 41 41 41 41 41 41 41 41 41 41 51 41 41 41 41 41 41 41 41 41 41

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRD0005.doc	unknown	15360	78 34 62 6b 46 41 41 41 41 41 41 41 41 4d 65 47 36 42 51 41 41 41 41 41 41 41 44 48 68 75 77 55 41 41 41 41 41 41 41 41 78 34 62 77 46 41 41 41 41 41 41 41 41 4d 65 47 39 42 51 41 41 41 41 41 41 41 44 48 68 76 67 55 41 41 41 41 41 41 41 41 78 34 62 38 46 41 41 41 41 41 41 41 41 4d 65 47 41 42 55 41 41 41 41 41 41 41 44 48 68 67 51 56 41 41 41 41 41 41 41 41 78 34 59 49 46 51 41 41 41 41 41 41 41 4d 65 47 44 42 55 41 41 41 41 41 41 41 44 48 68 68 41 56 41 41 41 41 41 41 41 41 78 34 59 55 46 51 41 41 41 41 41 41 41 4d 65 47 47 42 55 41 41 41 41 41 41 41 44 48 68 68 77 56 41 41 41 41 41 41 41 41 78 34 59 67 46 51 41 41 41 41 41 41 41 4d 65 47 4a 42 55 41 41 41 41 41 41 41 44 48 68 69 67 56 41 41 41 41 41 41 41 41 78 34 59 73 46 51 41 41 41 41 41 41 41 4d 65	x4bkFAAAAAAAAMeG6BQAAAAAADHhuwUAAAAAAAAx4bwFAAAAAAAMeG9BQAAAAAADHhvgUAAAAAAAAx4b8FAAAAAAAMeGABUAAAAAAADHhgQVAAAAAAAAx4YlFQAAAAAAAMeGDBUAAAAAADHhhAVAAAAAAAAx4YUFQAAAAAAAMeGGBUAAAAAADHhhwVAAAAAAAAx4YgFQAAAAAAAMeGJBUAAAAAADHhigVAAAAAAAAx4YsFQAAAAAAAMe	success or wait	41	66A22C2C	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRD0364.doc	unknown	28160	57 00 56 00 6d 00 46 00 77 00 48 00 51 00 6e 00 67 00 33 00 67 00 6b 00 41 00 48 00 77 00 68 00 78 00 30 00 58 00 38 00 2f 00 76 00 2f 00 2f 00 2f 00 37 00 41 00 42 00 36 00 78 00 2b 00 4c 00 52 00 65 00 79 00 4c 00 41 00 44 00 50 00 4a 00 67 00 54 00 67 00 46 00 41 00 41 00 44 00 41 00 44 00 35 00 54 00 42 00 69 00 38 00 48 00 44 00 69 00 32 00 58 00 6f 00 78 00 30 00 58 00 38 00 2f 00 76 00 2f 00 2f 00 2f 00 7a 00 4c 00 41 00 69 00 30 00 33 00 77 00 5a 00 49 00 6b 00 4e 00 41 00 41 00 41 00 41 00 41 00 46 00 6c 00 66 00 58 00 6c 00 76 00 4a 00 77 00 31 00 57 00 4c 00 37 00 4f 00 6a 00 51 00 42 00 41 00 41 00 41 00 68 00 63 00 42 00 30 00 44 00 34 00 42 00 39 00 43 00 41 00 42 00 31 00 43 00 54 00 50 00 41 00 75 00 51 00 79 00 59 00 41 00 52 00 43 00 48	W.V.m.F.w.H.Q.n.g.3.g.k.A.H.w.h.x.0.X.8./.v././.7.A.B.6.x.+.L.R.e.y.L.A.D.P.J.g.T.g.F.A.A.D.A.D.5.T.B.i.8.H.D.i.2.X.o.x.0.X.8./.v././.z.L.A.i.0.3.w.Z.I.k.N.A.A.A.A.A.F.I.f.X.I.v.J.w.1.W.L.7.O.j.Q.B.A.A.A.h.c.B.0.D.4.B.9.C.A.B.1.C.T.P.A.u.Q.y.Y.A.R.C.H	success or wait	1	66A22C2C	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRD0364.doc	unknown	5640	4f 00 44 00 49 00 38 00 4d 00 6b 00 41 00 79 00 52 00 44 00 4a 00 49 00 4d 00 6b 00 77 00 79 00 55 00 44 00 4a 00 55 00 4d 00 6c 00 67 00 79 00 58 00 44 00 4a 00 67 00 4d 00 6d 00 51 00 79 00 61 00 44 00 4a 00 73 00 4d 00 6e 00 41 00 79 00 64 00 44 00 4a 00 34 00 4d 00 6e 00 77 00 79 00 67 00 44 00 4b 00 45 00 4d 00 6f 00 67 00 79 00 6a 00 44 00 4b 00 51 00 4d 00 70 00 51 00 79 00 6d 00 44 00 4b 00 63 00 4d 00 71 00 41 00 79 00 70 00 44 00 4b 00 6f 00 4d 00 71 00 77 00 79 00 73 00 44 00 4b 00 30 00 4d 00 72 00 67 00 79 00 76 00 44 00 4c 00 41 00 4d 00 73 00 51 00 79 00 79 00 44 00 4c 00 4d 00 4d 00 74 00 41 00 79 00 31 00 44 00 4c 00 59 00 4d 00 74 00 77 00 79 00 34 00 44 00 4c 00 6b 00 4d 00 75 00 67 00 79 00 37 00 44 00 4c 00 77 00 4d 00 76 00 51 00 79	O.D.I.8.M.k.A.y.R.D.J.I.M.k.w. y.U.D.J.U.M.l.g.y.X.D.J.g. M.m. Q.y.a.D.J.s.M.n.A.y.d.D.J. 4.M. n.w.y.g.D.K.E.M.o.g.y.j.D. K.Q. M.p.Q.y.m.D.K.c.M.q.A.y.p .D.K. o.M.q.w.y.s.D.K.0.M.r.g.y.v .D. L.A.M.s.Q.y.y.D.L.M.M.t.A. y.1. D.L.Y.M.t.w.y.4.D.L.k.M.u. g.y.7.D.L.w.M.v.Q.y	success or wait	1	66A22C2C	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRD0497.doc	unknown	32256	54 56 71 51 41 41 4d 41 41 41 41 45 41 41 41 41 2f 2f 38 41 41 4c 67 41 41 41 41 41 41 41 41 41 51 41 41 41 41 41 41 41 41 41

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRD0497.doc	unknown	15364	53 66 42 34 34 2f 53 33 39 2f 4c 55 76 55 5a 33 53 61 46 73 32 6f 5a 73 33 63 70 4e 73 47 57 78 4c 66 46 66 53 45 78 5a 73 73 59 5a 32 77 76 38 65 54 6f 6c 34 63 35 62 4f 6b 41 58 57 75 36 66 39 4b 2b 54 48 74 67 65 4d 65 46 6a 30 71 4f 4b 64 51 53 6f 54 4c 2b 57 67 6a 69 69 32 41 51 6c 75 30 6a 66 31 43 36 42 42 6e 5a 46 73 32 4b 34 65 41 32 75 47 63 4f 57 53 69 49 6a 31 39 33 5a 65 61 75 35 50 59 6f 4a 6c 76 76 4a 78 2f 69 50 66 4d 48 67 4f 43 57 32 37 73 70 79 55 4a 6f 57 48 79 6a 4f 49 41 73 5a 6f 61 30 76 7a 4e 54 78 4b 33 65 58 6a 56 73 71 70 35 39 55 73 61 77 6a 7a 4f 42 44 59 48 2f 30 61 46 71 33 6c 4f 54 78 45 69 56 4b 52 41 6d 43 36 49 4e 6f 45 63 78 73 62 39 43 2f 56 33 4e 75 42 34 41 56 54 4a 55 6f 70 31 41 41 70 50 7a 69 62 49 4e 68 70 35 59	SfB44/S39/LUvUZ3SaFs2oZs3cpNsGWxLfFfSExZssYZ2wv8eTol4c5bOkAXWu6f9K+THtgeMeFj0qOKdQSoTL+Wgjii2AQlu0jf1C6BBnZFs2K4eA2uGcOWSilj193Zeau5PYoJlvvJx/iPfMHgOCW27spyUJoWHyjOIAsZoa0vzNTxK3eXjVsqp59UsawjzOBDYH/0aFq3lOTxEiVKRAmC6INoEcxsb9C/V3NuB4AVTJUop1AApPzibINhp5Y	success or wait	1	66A22C2C	unknown
C:\Users\Public\~WRD0004.tmp	unknown	32256	54 56 71 51 41 41 4d 41 41 41 41 45 41 41 41 41 2f 2f 38 41 41 4c 67 41 41 41 41 41 41 41 41 41 51 41 41 41 41 41 41 41 41 41

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\~WRD0004.tmp	unknown	6148	43 69 41 67 49 43 41 67 49 44 77 76 63 6d 56 78 64 57 56 7a 64 47 56 6b 55 48 4a 70 64 6d 6c 73 5a 57 64 6c 63 7a 34 4e 43 69 41 67 49 43 41 38 4c 33 4e 6c 59 33 56 79 61 58 52 35 50 67 30 4b 49 43 41 38 4c 33 52 79 64 58 4e 30 53 57 35 6d 62 7a 34 4e 43 6a 77 76 59 58 4e 7a 5a 57 31 69 62 48 6b 2b 44 51 6f 41 41 41

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	66A18A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	66A18A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	66A18A84	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\1F096	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery	success or wait	2	66A22C2C	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\2454D	success or wait	1	66A22C2C	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 1	success or wait	1	66A22C2C	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\248F7	success or wait	1	66A22C2C	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 2	success or wait	1	66A22C2C	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Name	unicode	Recover Text from Any File	success or wait	1	66A05805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Path	unicode	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\RECOVR32.CNV	success or wait	1	66A05805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	*	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cambria Math	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\1F096	1F096	binary	04 00 00 00 00 06 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 68 00 61 00 72 00 64 00 7A 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 08 00 00 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 01 00 00 00 00 00 00 00 C2 71 70 DB 68 EA D6 01 96 F0 01 00 96 F0 01 00 00 00 00 00 DB 04 00 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 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 1	File Path	unicode	C:\Users\Public\Ksh1.xls	success or wait	1	66A22C2C	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 1	Datetime	unicode	2021-01-14T03:32	success or wait	1	66A22C2C	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 1	Position	unicode	0 0	success or wait	1	66A22C2C	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\File MRU	Item 22	unicode	[F00000000][T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\5622580005.docx	success or wait	1	66A22C2C	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\248F7	248F7	binary	04 00 00 00 00 06 00 00 18 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 50 00 75 00 62 00 6C 00 69 00 63 00 5C 00 4B 00 73 00 68 00 31 00 2E 00 64 00 6F 00 63 00 08 00 00 00 4B 00 73 00 68 00 31 00 2E 00 64 00 6F 00 63 00 00 00 00 00 01 00 00 00 00 00 00 00 74 5A EA E8 68 EA D6 01 F7 48 02 00 F7 48 02 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			68 00 74 00 6D 00 08 00 00 00 68 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 01 00 00 00 00 00 00 00 C2 71 70 DB 68 EA D6 01 96 F0 01 00 96 F0 01 00 00 00 00 00 DB 04 00 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 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\File MRU	Item 8	unicode	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\6483516391.docx	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\1244065654.docx	success or wait	1	66A22C2C	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\File MRU	Item 9	unicode	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\3677062445.docx	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\6483516391.docx	success or wait	1	66A22C2C	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\File MRU	Item 10	unicode	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\9106464316.docx	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\3677062445.docx	success or wait	1	66A22C2C	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\File MRU	Item 11	unicode	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\2265465471.docx	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\9106464316.docx	success or wait	1	66A22C2C	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\File MRU	Item 12	unicode	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\0666563528.docx	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\2265465471.docx	success or wait	1	66A22C2C	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\File MRU	Item 13	unicode	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\1343496627.docx	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\0666563528.docx	success or wait	1	66A22C2C	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\File MRU	Item 14	unicode	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\8784112376.docx	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\1343496627.docx	success or wait	1	66A22C2C	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\File MRU	Item 15	unicode	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\8995528179.docx	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\8784112376.docx	success or wait	1	66A22C2C	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\File MRU	Item 16	unicode	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\7155756679.docx	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\8995528179.docx	success or wait	1	66A22C2C	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\File MRU	Item 17	unicode	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\7011884383.docx	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\7155756679.docx	success or wait	1	66A22C2C	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\File MRU	Item 18	unicode	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\7245361316.docx	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\7011884383.docx	success or wait	1	66A22C2C	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\File MRU	Item 19	unicode	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\2265332024.docx	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\7245361316.docx	success or wait	1	66A22C2C	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\File MRU	Item 20	unicode	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\5622580005.docx	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\2265332024.docx	success or wait	1	66A22C2C	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\File MRU\Change	ChangeId	dword	1953171221	1494287124	success or wait	1	66A22C2C	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\2454D	2454D	binary	04 00 00 00 00 06 00 00 18 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 50 00 75 00 62 00 6C 00 69 00 63 00 5C 00 4B 00 73 00 68 00 31 00 2E 00 78 00 6C 00 73 00 08 00 00 00 4B 00 73 00 68 00 31 00 2E 00 78 00 6C 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 DA 88 56 E8 68 EA D6 01 4D 45 02 00 4D 45 02 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\File MRU	Item 15	unicode	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\8784112376.docx	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\1343496627.docx	success or wait	1	66A22C2C	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\File MRU	Item 16	unicode	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\8995528179.docx	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\8784112376.docx	success or wait	1	66A22C2C	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\File MRU	Item 17	unicode	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\7155756679.docx	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\8995528179.docx	success or wait	1	66A22C2C	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\File MRU	Item 18	unicode	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\7011884383.docx	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\7155756679.docx	success or wait	1	66A22C2C	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\File MRU	Item 19	unicode	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\7245361316.docx	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\7011884383.docx	success or wait	1	66A22C2C	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\File MRU	Item 20	unicode	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\2265332024.docx	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\7245361316.docx	success or wait	1	66A22C2C	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\File MRU	Item 21	unicode	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\5622580005.docx	[F00000000] [T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\2265332024.docx	success or wait	1	66A22C2C	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\File MRU\Change	ChangeId	dword	1494287124	107157759	success or wait	1	66A22C2C	unknown

Analysis Process: svchost.exe PID: 1004 Parent PID: 568

General

Start time:	03:31:42
Start date:	14/01/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6192 Parent PID: 568

General

Start time:	03:31:46
Start date:	14/01/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff7488e0000
File size:	51288 bytes

MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6588 Parent PID: 568

General

Start time:	03:31:56
Start date:	14/01/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6684 Parent PID: 568

General

Start time:	03:31:57
Start date:	14/01/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright null 2021

Reputation:	high

Analysis Process: svchost.exe PID: 6720 Parent PID: 568

General

Start time:	03:31:58
Start date:	14/01/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6776 Parent PID: 568

General

Start time:	03:31:58
Start date:	14/01/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k unistacksvcgroup
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6792 Parent PID: 568

General

Start time:	03:31:58
Start date:	14/01/2021
Path:	C:\Windows\System32\svchost.exe

Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 6880 Parent PID: 568

General

Start time:	03:31:59
Start date:	14/01/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: SgrmBroker.exe PID: 6944 Parent PID: 568

General

Start time:	03:31:59
Start date:	14/01/2021
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff673870000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 6976 Parent PID: 568

General

Start time:	03:32:00
Start date:	14/01/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false

Copyright null 2021

Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

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

Analysis Process: certutil.exe PID: 6392 Parent PID: 4940

General

Start time:	03:32:16
Start date:	14/01/2021
Path:	C:\Windows\System32\certutil.exe
Wow64 process (32bit):	false
Commandline:	Certutil -decode C:\Users\Public\Ksh1.xls C:\Users\Public\Ksh1.pdf
Imagebase:	0x7ff6b94e0000
File size:	1557504 bytes
MD5 hash:	EB199893441CED4BBBCB547FE411CF2D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6372 Parent PID: 6392

General

Start time:	03:32:16
Start date:	14/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Copyright null 2021

Disassembly

Code Analysis