

JOeSandbox Cloud BASIC



ID: 356212

Sample Name:

SecuriteInfo.com.Heur.15528.xls

Cookbook:

defaultwindowsofficecookbook.jbs

Time: 19:19:33

Date: 22/02/2021

Version: 31.0.0 Emerald

Table of Contents

Table of Contents	2
Analysis Report SecuriteInfo.com.Heur.15528.xls	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Startup	4
Malware Configuration	4
Yara Overview	4
Initial Sample	4
Sigma Overview	4
System Summary:	5
Signature Overview	5
AV Detection:	5
Compliance:	5
Software Vulnerabilities:	5
System Summary:	5
HIPS / PFW / Operating System Protection Evasion:	5
Mitre Att&ck Matrix	5
Behavior Graph	6
Screenshots	6
Thumbnails	6
Antivirus, Machine Learning and Genetic Malware Detection	7
Initial Sample	7
Dropped Files	7
Unpacked PE Files	7
Domains	7
URLs	7
Domains and IPs	9
Contacted Domains	9
URLs from Memory and Binaries	9
Contacted IPs	13
Public	13
General Information	13
Simulations	14
Behavior and APIs	15
Joe Sandbox View / Context	15
IPs	15
Domains	15
ASN	15
JA3 Fingerprints	15
Dropped Files	16
Created / dropped Files	16
Static File Info	18
General	18
File Icon	18
Static OLE Info	18
General	18
OLE File "SecuriteInfo.com.Heur.15528.xls"	18
Indicators	18
Summary	18
Document Summary	19
Streams	19
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096	19
General	19
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096	19
General	19

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 83229	19
General	19
Macro 4.0 Code	19
Network Behavior	20
Network Port Distribution	20
TCP Packets	20
UDP Packets	20
DNS Queries	22
DNS Answers	22
HTTPS Packets	22
Code Manipulations	22
Statistics	22
Behavior	22
System Behavior	22
Analysis Process: EXCEL.EXE PID: 2576 Parent PID: 792	23
General	23
File Activities	23
File Created	23
File Deleted	24
Registry Activities	24
Key Created	24
Key Value Created	24
Analysis Process: rundll32.exe PID: 6196 Parent PID: 2576	24
General	24
File Activities	25
Disassembly	25
Code Analysis	25

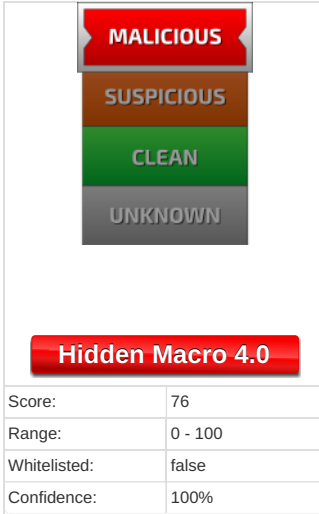
Analysis Report SecuriteInfo.com.Heur.15528.xls

Overview

General Information

Sample Name:	SecuriteInfo.com.Heur.15.28.xls
Analysis ID:	356212
MD5:	5a75c6184001a6..
SHA1:	b3ec9fbbc5e96c4..
SHA256:	c71bd3833fbb10c..
Most interesting Screenshot:	

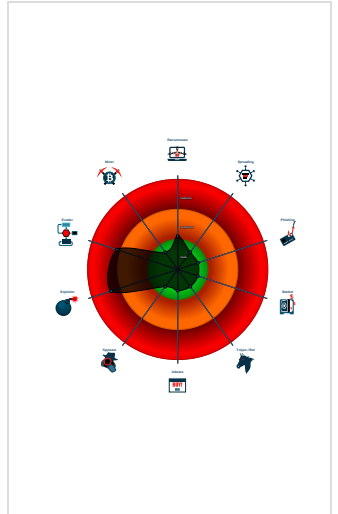
Detection



Signatures

- Multi AV Scanner detection for subm...
- Office document tries to convince vi...
- Document exploit detected (UrlDown...
- Document exploit detected (process...
- Found Excel 4.0 Macro with suspicio...
- Sigma detected: Microsoft Office Pr...
- Yara detected hidden Macro 4.0 in E...
- Document contains embedded VBA ...
- JA3 SSL client fingerprint seen in co...
- Potential document exploit detected ...
- Potential document exploit detected ...
- Potential document exploit detected ...

Classification



Startup

- System is w10x64
-  EXCEL.EXE (PID: 2576 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
 -  rundll32.exe (PID: 6196 cmdline: rundll32 .\rieurow.vnt,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- cleanup

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
SecuriteInfo.com.Heur.15528.xls	SUSP_EnableContent_String_Gen	Detects suspicious string that asks to enable active content in Office Doc	Florian Roth	0x11da3:\$e1: Enable Editing 0x11e18:\$e2: Enable Content
SecuriteInfo.com.Heur.15528.xls	SUSP_Excel4Macro_Auto Open	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	0x0:\$header_docf: D0 CF 11 E0 0x148a2:\$s1: Excel 0x15906:\$s1: Excel 0x3802:\$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 01 3A
SecuriteInfo.com.Heur.15528.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

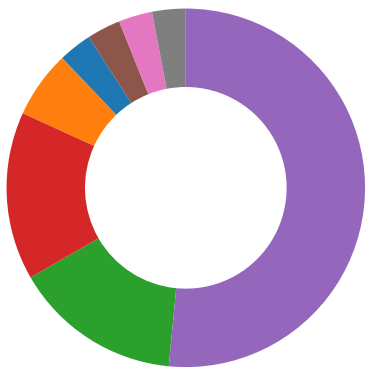
Sigma Overview

System Summary:



Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



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

Click to jump to signature section

AV Detection:



Multi AV Scanner detection for submitted file

Compliance:



Uses new MSVCR DLLs

Uses secure TLS version for HTTPS connections

Software Vulnerabilities:



Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:



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:



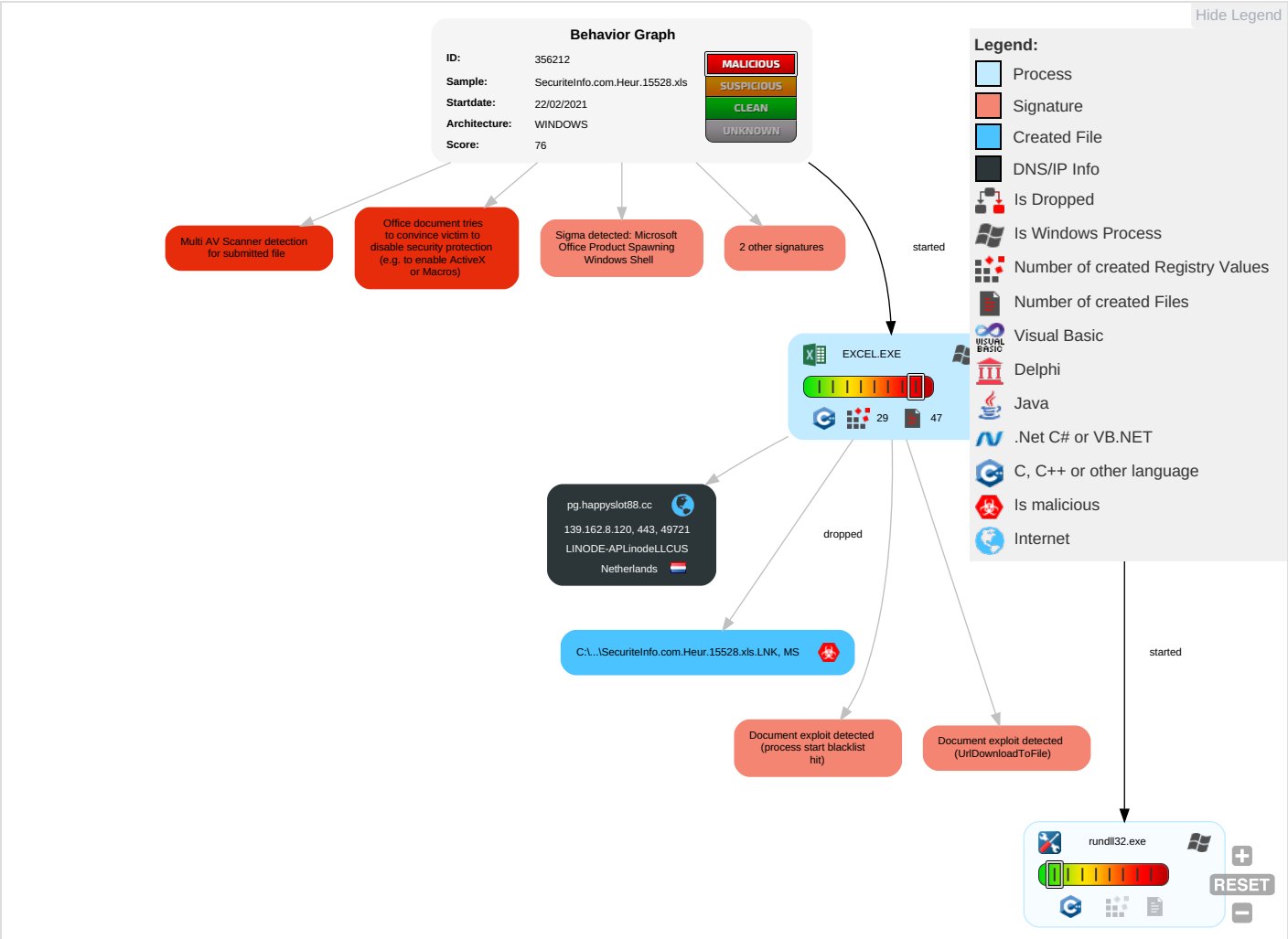
Yara detected hidden Macro 4.0 in Excel

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 1 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
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 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Disruption of Local Operations
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 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Disruption of Local Operations
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Compromise of Confidentiality
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 1 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Malicious Activity or Data Breach

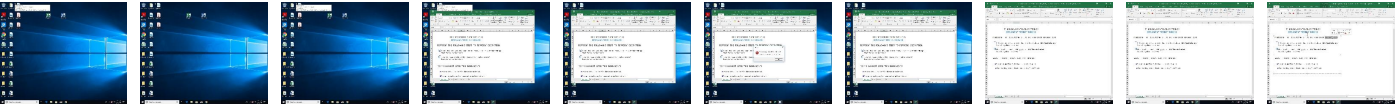
Behavior Graph

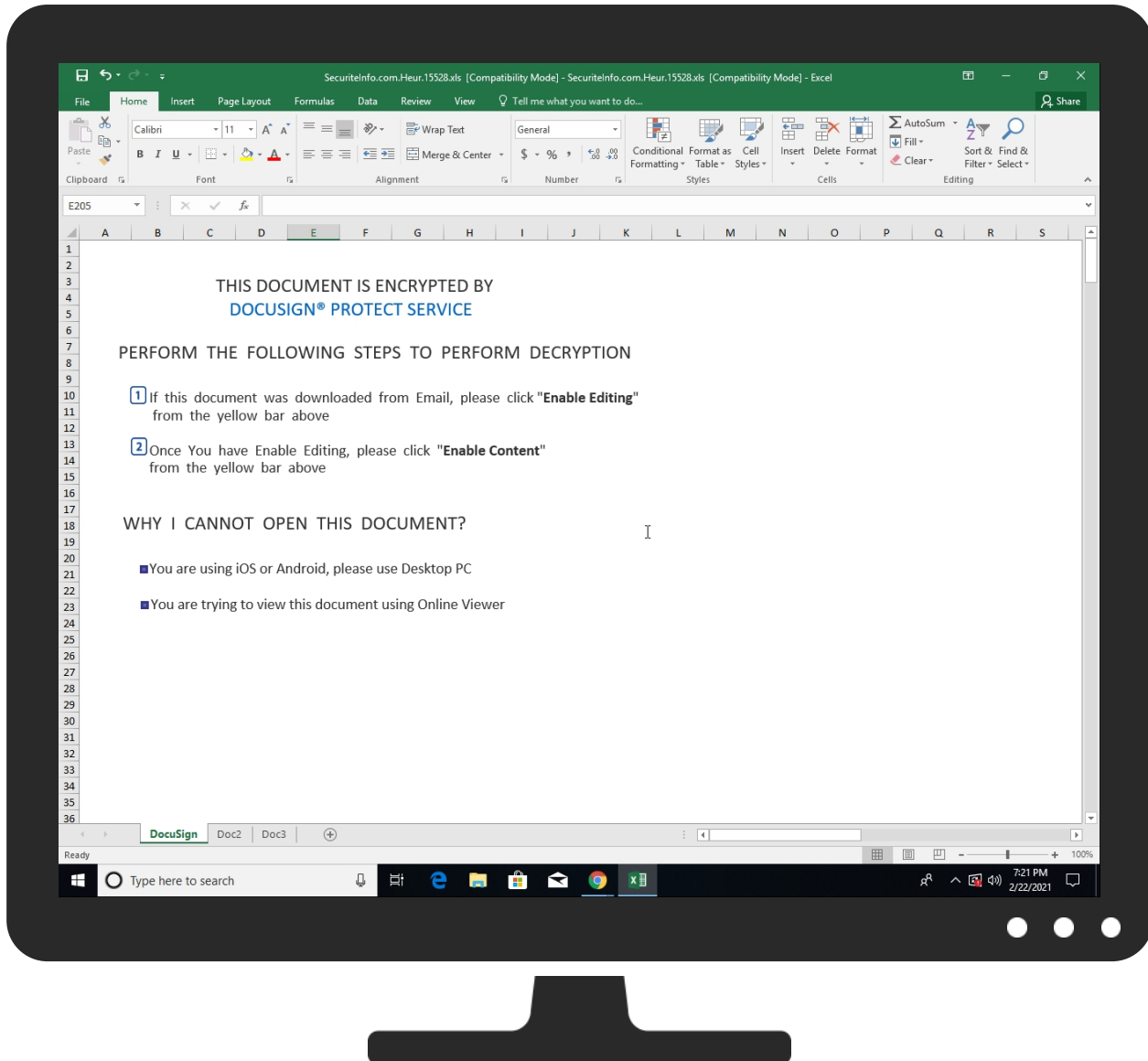
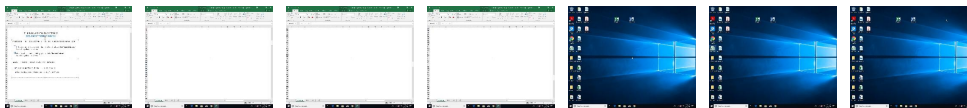


Screenshots

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
SecuriteInfo.com.Heur.15528.xls	10%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
pg.happyslot88.cc	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	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://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	

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://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://asgmsproxyapi.azurewebsites.net/	0%	Virustotal		Browse
http://https://asgmsproxyapi.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://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://api.cortana.ai	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://https://staging.cortana.ai	0%	URL Reputation	safe	
http://https://staging.cortana.ai	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
pg.happyslot88.cc	139.162.8.120	true	false	1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticsdf.office.com	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://login.microsoftonline.com/	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://shell.suite.office.com:1443	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://autodiscover-s.outlook.com/	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://cdn.entity.	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.addins.omex.office.net/appinfo/query	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://wus2-000.contentsync.	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.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	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://powerlift.acompli.net	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://https://rpticket.partnerservices.getmicrosoftkey.com	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://cortana.ai	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.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	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://entitlement.diagnosticsdf.office.com	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://api.aadrm.com/	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false	0%, Virustotal, Browse - Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://api.microsoftstream.com/api/	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://cr.office.com	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://graph.ppe.windows.net	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://https://tasks.office.com	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false	0%, Virustotal, Browse - Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://store.office.cn/addinstemplate	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.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.	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.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=	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://web.microsoftstream.com/video/	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://graph.windows.net	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://dataservice.o365filtering.com/	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://weather.service.msn.com/data.aspx	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://apis.live.net/v5.0/	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.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	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://autodiscover.s.outlook.com/autodiscover/autodiscover.xml	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://management.azure.com	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://incidents.diagnostics.office.com	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://insertmedia.bing.office.net/odc/insertmedia	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://api.office.net	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://incidents.diagnosticsdf.office.com	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://asgmsproxyapi.azurewebsites.net/	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false	0%, Virustotal, Browse - Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://entitlement.diagnostics.office.com	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://outlook.office.com/	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://templatelogging.office.com/client/log	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://outlook.office365.com/	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://webshell.suite.office.com	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://management.azure.com/	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://ncus-000.contentsync	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://https://graph.windows.net/	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://devnull.onenote.com	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://messaging.office.com/	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://augloop.office.com/v2	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://skyapi.live.net/Activity/	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.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	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://dataservice.o365filtering.com	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://https://api.cortana.ai	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://onedrive.live.com	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false	Avira URL Cloud: safe	unknown
http://https://visio.uservice.com/forums/368202-visio-on-devices	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://directory.services.	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false		high
http://https://staging.cortana.ai	69F6F346-5229-46C6-AF0A-021EDB BC41A1.0.dr	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
139.162.8.120	unknown	Netherlands		63949	LINODE-APLinodeLLCUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356212
Start date:	22.02.2021
Start time:	19:19:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Heur.15528.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@3/6@1/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 52.255.188.83, 204.79.197.200, 13.107.21.200, 52.147.198.201, 13.88.21.125, 52.109.76.68, 52.109.88.39, 52.109.76.34, 52.109.12.24, 51.104.139.180, 23.210.248.85, 20.54.26.129, 93.184.221.240, 51.103.5.186, 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, wu.azureedge.net, wns.notify.trafficmanager.net, www.bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.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, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, www.bing.com, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, prod.configsvc1.live.com.akadns.net, wu.ec.azureedge.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skype.dataprddcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skype.dataprddcoleus17.cloudapp.net, a-0001.a-fdentry.net.trafficmanager.net, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, skype.dataprddcolwus15.cloudapp.net, europe.configsvc1.live.com.akadns.net, vip2-par02p.wns.notify.trafficmanager.net

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
139.162.8.120	SecuriteInfo.com.Heur.15528.xls	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LINODE-APLinodeLLCUS	SecuriteInfo.com.Heur.15528.xls	Get hash	malicious	Browse	139.162.8.120
	Drawings2.exe	Get hash	malicious	Browse	45.56.79.23
	Sign-1870635479_637332644.xls	Get hash	malicious	Browse	176.58.123.25
	SecuriteInfo.com.Exploit.Siggen3.10350.26515.xls	Get hash	malicious	Browse	176.58.123.25
	SecuriteInfo.com.Heur.1476.xls	Get hash	malicious	Browse	176.58.123.25
	Sign-92793351_1597657581.xls	Get hash	malicious	Browse	176.58.123.25
	Invoice467972.jar	Get hash	malicious	Browse	23.239.31.129
	Invoice467972.jar	Get hash	malicious	Browse	23.239.31.129
	SecuriteInfo.com.Heur.22173.xls	Get hash	malicious	Browse	176.58.123.25
	Deposit_50%PAYMENT TERM -PO09-excel.htm	Get hash	malicious	Browse	45.79.77.20
	Sign_1229872171-1113140666(1).xls	Get hash	malicious	Browse	176.58.123.25
	IU-8549 Medical report COVID-19.doc	Get hash	malicious	Browse	172.104.97.173
	SecuriteInfo.com.Exploit.Siggen3.10048.24657.xls	Get hash	malicious	Browse	176.58.123.25
	SecuriteInfo.com.Exploit.Siggen3.10048.15397.xls	Get hash	malicious	Browse	176.58.123.25
	Invoice#6026115.xls	Get hash	malicious	Browse	172.104.247.192
	index_2021-02-17-11_45.dll	Get hash	malicious	Browse	176.58.123.25
	MT0128.jar	Get hash	malicious	Browse	23.239.31.129
	MT0128.jar	Get hash	malicious	Browse	23.239.31.129
	v.dll	Get hash	malicious	Browse	172.104.247.192
	SecuriteInfo.com.Exploit.Siggen3.10048.426.xls	Get hash	malicious	Browse	176.58.123.25

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	Muligheds.exe	Get hash	malicious	Browse	139.162.8.120
	DHL_6368638172 documento de recibo.pdf.exe	Get hash	malicious	Browse	139.162.8.120
	PDF.exe	Get hash	malicious	Browse	139.162.8.120
	pagamento.exe	Get hash	malicious	Browse	139.162.8.120
	message_zdm (2).html	Get hash	malicious	Browse	139.162.8.120
	Statement-ID28865611496334.vbs	Get hash	malicious	Browse	139.162.8.120
	Statement-ID21488878391791.vbs	Get hash	malicious	Browse	139.162.8.120
	frank_2021-02-22_02-03.exe	Get hash	malicious	Browse	139.162.8.120
	Statement-ID72347595684775.vbs	Get hash	malicious	Browse	139.162.8.120
	MR52.vbs	Get hash	malicious	Browse	139.162.8.120
	Scan_medcal equipment sample_pdf.exe	Get hash	malicious	Browse	139.162.8.120
	rfq02212021.exe	Get hash	malicious	Browse	139.162.8.120
	RE ICA 40 Sdn Bhd- Purchase Order#6769704.exe	Get hash	malicious	Browse	139.162.8.120
	RFQ-#09503.exe	Get hash	malicious	Browse	139.162.8.120
	RFQ_1101983736366355_1101938377388.exe	Get hash	malicious	Browse	139.162.8.120
	Offer Request 6100003768.exe	Get hash	malicious	Browse	139.162.8.120
	124992436.docx	Get hash	malicious	Browse	139.162.8.120

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	scarf.exe	Get hash	malicious	Browse	139.162.8.120
	Copy_remittnce.exe	Get hash	malicious	Browse	139.162.8.120
	document-1900770373.xls	Get hash	malicious	Browse	139.162.8.120

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\69F6F346-5229-46C6-AF0A-021EDBBC41A1	
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):	5.375859108438167
Encrypted:	false
SSDEEP:	1536:lcQceNquBXA3gBwJpQ9DQW+zA9H34ZldpKWxboOilXNErLdzEh:xcQ9DQW+z0XiK
MD5:	DDDC6EBF2C098002BEDC3A69DDA8090D
SHA1:	F27D835B94574B0DD8BF640B2C6DF277DDC87D79
SHA-256:	5AE1CC3C503F396754EB466F6CB5D696EB2672766782A0FCC674BF47652DE65C
SHA-512:	B747B86A760E9E03301AB2BEF7D1EF89DF5A745182D1034859A33776DC1D92E81FBE33B9598030FA5D3B259DE9C20A2B6F43562BE74EBB2B3AFDADA46313483C
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="2021-02-22T18:20:26">..Build: 16.0.13817.30529->..<o:default>..<o:ticket o:headerName="Authorization" o:headerValue="{}" />..</o:default>..<o:service o:name="Research">..<o:url>https://rr.office.microsoft.com/research/query.aspx</o:url>..</o:service>..<o:service o:name="ORedir">..<o:url>https://o15.officedir.microsoft.com/r</o:url>..</o:service>..<o:service o:name="ORedirSSL">..<o:url>https://o15.officedir.microsoft.com/r</o:url>..</o:service>..<o:service o:name="CViewClientHelpd">..<o:url>https://[MAX.BaseHost]/client/results</o:url>..</o:service>..<o:service o:name="CViewClientHome">..<o:url>https://[MAX.BaseHost]/client/results</o:url>..</o:service>..<o:service o:name="CViewClientTemplate">..<o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>..</o:service>..<o:

C:\Users\user\AppData\Local\Temp\F9810000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	64846
Entropy (8bit):	7.693818560967215
Encrypted:	false
SSDEEP:	1536:OfmFcq+nbub6aJpa/h/9g/W/iuz9c9ZJRf9wx8fkocM/WWL:5cbueaJpaZlgulEZJRlwWWO
MD5:	4A8836C1D581711F0D530F622117F7C5
SHA1:	37FC14F2BB14A9B0372DFD55065C686284E910AF
SHA-256:	DAED0EDCAB1C1E81FAF7D3157FBA7EFBED6B86FD57CBDDDB4B297FBACB0F315E1
SHA-512:	F3512C1960EF32A0D72AE8A021D6177C21444FBBED2C20ECC16111E2F560F10518C0C9A098C29BEA81A9B0974839963A28D9F1350E835B98663B3D6A9CAD1EE
Malicious:	false
Reputation:	low
Preview:	.U.N.0....;D....j....x..=M.:e.h~.n.*.U+qi.8....r....]P.....R..f.....m..l..].N~L...CAh.j....~s.D....:4....H?}...%4..'......hb....M....t..Wt{...W..T.T...>..+....i% R4.l..[.].@i.SGf..<.-b.t"...c.*'.u.O.."d6.Z...)BZy..T=.6.+...x...W..X..[.v..j.P.J..r....FZ.e^..P....._....d...wo..O...?.....b.....&.....o@.....nH.[(.#.....r...^....9...hDW..W-M.#.?...)..t.x....N.....p...f.H....9.r.6.....PK.....!...l.....[Content_Types].xml ...(.....).....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 16:19:49 2019, mtime=Tue Feb 23 02:20:28 2021, atime=Tue Feb 23 02:20:28 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.672786196074765
Encrypted:	false
SSDEEP:	12:8RNNcXUMuEIPCH2YgprAK1Yj89xA+WrijAZ/2bDxLLC5Lu4t2Y+xlBjKZm:8RNXgZr48X6AZiDxy87aB6m
MD5:	0A15C3DA04BCC961BA88053586D8C843
SHA1:	BED9207E685BF68E9595952601FAA9F564B13CA3
SHA-256:	958E487DB9BA6CA60BC9D09A3A97977DAA67460DB5E56973CC78FA4C2E28EEAF

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
SHA-512:	73E2BEAE5587B6006A7D7895254EB2E830C4A9E45833B843988D8F0B5087833A9B682E1C71AD0E8581F90AD58D9689840C11CB3941E012B60768CFA7ED824B74
Malicious:	false
Reputation:	low
Preview:	L.....F.....N.....u...P.O. :i....+00.../C:\.....x.1.....N....Users.d.....L.WR.....:.....qj..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,- .2.1.8.1.3.....P.1.....>Qxx..user.<.....Ny.WR.....S.....i.h.a.r.d.z....~.1.....WR....Desktop.h.....Ny.WR.....Y.....>.....[.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-2.1 .7.6.9.....E.....D.....>S.....C:\Users\user\Desktop.....\.....\.....\.....\D.e.s.k.t.o.p.....(LB.)...As..`.....X.....210979.....!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\SecuriteInfo.com.Heur.15528.xls.LNK		
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE	
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 14:03:44 2020, mtime=Tue Feb 23 02:20:28 2021, atime=Tue Feb 23 02:20:28 2021, length=93696, window=hide	
Category:	dropped	
Size (bytes):	2280	
Entropy (8bit):	4.697000249744024	
Encrypted:	false	
SSDEEP:	48:80/GU7hHKU5zAHhHKlu9B6p0/GU7hHKU5zAHhHKlu9B6:80/7dKbKlu9K0/7dKbKlu9	
MD5:	05CB1CC58914F998F59F45D189A8F831	
SHA1:	3F8A9AB7D307E9E3A9252904F01EF7CCF500934D	
SHA-256:	1D0BD92D4159412152A474A35150B6F76CC608F23358B6F937AF3221B98F695	
SHA-512:	6AF74E6EEF7E9C3A6FBB5AE7D3798E0C70402CF003C5758D6C77B95ABF04269ED16A0FACF89765F19EB1B56F1D05A828EF59606B75958BB7AA04C967296ECF53	
Malicious:	true	
Reputation:	low	
Preview:	L.....F.....1.(:.....n.....P.O. :i....+00.../C:\.....x.1.....N....Users.d.....L.WR.....:.....qj..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,- .2.1.8.1.3.....P.1.....>Qxx..user.<.....Ny.WR.....S.....i.h.a.r.d.z....~.1.....>Qyx..Desktop.h.....Ny.WR.....Y.....>.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,- .2.1.7.6.9.....2..n..WR...SECURI~1.XLS.p.....>QwxWR.....h.....S.e.c.u.r.i.t.e.I.n.f.o..c.o.m...H.e.u.r...1.5.5.2.8...x.l.s.....e.....d.....>S.. ...C:\Users\user\Desktop\SecuriteInfo.com.Heur.15528.xls..6.....\.....\.....\.....\D.e.s.k.t.o.p.\S.e.c.u.r.i.t.e.I.n.f.o..c.o.m...H.e.u.r...1.5.5.2.8...x.l.s.....(LB.)...As..`..... .X.....210979.....!a.%.H.VZAj...0.-.....-!a.%.H.VZAj...0.-.....-.....1SPS.XF.L8C....&m.q...../...S.-.1.-.5.-2.1.-3.8.5.3	

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):	146
Entropy (8bit):	4.804842734194581
Encrypted:	false
SSDEEP:	3:oyBVomM0bMp1uscbMp1mM0bMp1v:dj60Qp+Qph0Qpl
MD5:	5B7147D888D64DA59D28E0B4595D9A2B
SHA1:	EB08786BFCC87F5C6B4224D27834720ECC70928C
SHA-256:	EFC0834821A3BA16E9130839385399219C55CDC39EC65E831B069A2F705B0130
SHA-512:	57A08E9A1043188F6C02351DC31CDA62291EF7BA36F8BBE36776631D37138BD1051CDC28BDAA2573505C09950C681BC77B0920E48042FB2B31E5689D6B91847C
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..SecuriteInfo.com.Heur.15528.xls.LNK=0..SecuriteInfo.com.Heur.15528.xls.LNK=0..[xls]..SecuriteInfo.com.Heur.15528.xls.LNK=0..

C:\Users\user\Desktop\DA810000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	127348
Entropy (8bit):	4.307100638025005
Encrypted:	false
SSDEEP:	3072:YJxEtjPOtioVjDGUU1qfDlaGGx+cL2QnAFVZXUImJxEtjPOtioVjDGUU1qfDlaGn:yxEtjPOtioVjDGUU1qfDlavx+W2QnAFk
MD5:	5CB47404307BB610062A933364E351D1
SHA1:	78BC0D9AE60DA4483B6625EAE254B8C32026946D
SHA-256:	3C8FEE25D10CD4E03E4243434AE14DB408C50C4E88F863558BC9AFB464DDFF8A
SHA-512:	EC90A506107B0935B3E795D9733FF5B27CD03ACD3C485D7BEA183CE93E35A99EB753CFD5B8979D9010016B7536A81B28AB920AF6E39359F49F8C57436DFDC9E
Malicious:	false
Reputation:	low

C:\Users\user\Desktop\DA810000	
Preview:	T8.....\p... B....a.....=.....=...i.9J.8.....X.@. ".....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.....,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.....?.....,C.a.l.i.b.r.i.1.....4.....,C.a.l.i.b.r.i.1.....8.....,C.a.l.i.b.r.i.1.....8.....,C.a.l.i.b.r.i.1.....8.....,C.a.l.i.b.r.i.1.....8.....,C.a.l.i.b.r.i.1.....h...8.....,C.a.m.b.r.i.a.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.....

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: Mon Feb 22 11:58:55 2021, Security: 0
Entropy (8bit):	3.473104569518557
TrID:	- Microsoft Excel sheet (30009/1) 78.94% - Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	SecuriteInfo.com.Heur.15528.xls
File size:	93696
MD5:	5a75c6184001a6b8785206f1e2121290
SHA1:	b3ec9fbcc5e96c45e74d503210a51a7ee5ce8132
SHA256:	c71bd3833fbb10cd2f845c83a6ed957f3243990de48a74b4d5cf1602303f4bb1
SHA512:	d1d29f02ae53f7fe04ebab4e628d0e30f0f9f4c1bbe58ef3eed9bc3f44d0b2af4b8df2b81fbc75ba083f77c52a7827cbb6b089382f3d8c9d6aae12bf8cf2760
SSDEEP:	1536:ca7uDpHYHceXVhca+fMHLtyeGxcl8O9pTi4XUXmRgb05SXw1OTsRKvoNGrEJcQ:ca7uDpHYHceXVhca+fMHLtyeGxcl8O9v
File Content Preview:	>.....

File Icon

	
Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General	
Document Type:	OLE
Number of OLE Files:	1

OLE File "SecuriteInfo.com.Heur.15528.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

Summary	
Last Saved Time:	2021-02-22 11:58:55
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:	0.337819969156
Base64 Encoded:	False
Data ASCII:	<pre>+,...0.....H.....P.... .X.....`.....h.....p.....x.....DocuSign.....Doc2.....Doc3.....Doc1 </pre>
Data Raw:	<pre> fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 01 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 e8 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 a8 00 00 00 02 00 00 00 e3 04 00 00 </pre>

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

General

General	
Stream Path:	\\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.250492291218
Base64 Encoded:	False
Data ASCII:	O h.....+'...0.....@.....H.. ...T.....`.....x..... ...Microsoft Excel.@..... .##...@.....)'.....
Data Raw:	fe ff 00 00 06 02 02 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: 83229

General

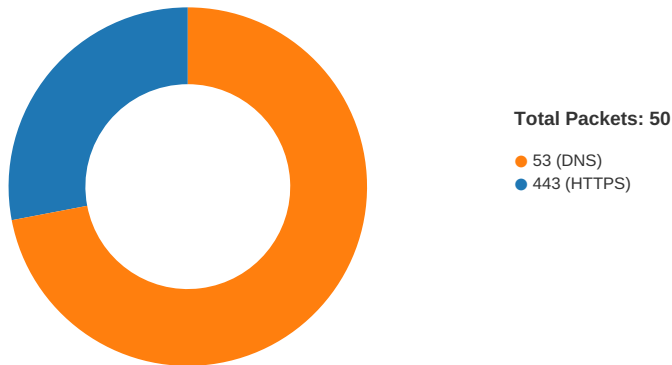
General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	83229
Entropy:	3.67638531123
Base64 Encoded:	True
Data ASCII:	<pre> g 2 \ . p . . . B a = i . . J . 8 X . @ " </pre>
Data Raw:	<pre> 09 08 10 00 00 06 05 00 67 32 cd 07 c9 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 20 </pre>

[illegible][illegible]

[illegible]

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 19:20:28.945894957 CET	49721	443	192.168.2.3	139.162.8.120
Feb 22, 2021 19:20:29.167375088 CET	443	49721	139.162.8.120	192.168.2.3
Feb 22, 2021 19:20:29.167481899 CET	49721	443	192.168.2.3	139.162.8.120
Feb 22, 2021 19:20:29.168451071 CET	49721	443	192.168.2.3	139.162.8.120
Feb 22, 2021 19:20:29.389699936 CET	443	49721	139.162.8.120	192.168.2.3
Feb 22, 2021 19:20:29.392009974 CET	443	49721	139.162.8.120	192.168.2.3
Feb 22, 2021 19:20:29.392064095 CET	443	49721	139.162.8.120	192.168.2.3
Feb 22, 2021 19:20:29.392096043 CET	443	49721	139.162.8.120	192.168.2.3
Feb 22, 2021 19:20:29.392148018 CET	49721	443	192.168.2.3	139.162.8.120
Feb 22, 2021 19:20:29.392211914 CET	49721	443	192.168.2.3	139.162.8.120
Feb 22, 2021 19:20:29.392219067 CET	49721	443	192.168.2.3	139.162.8.120
Feb 22, 2021 19:20:29.406243086 CET	49721	443	192.168.2.3	139.162.8.120
Feb 22, 2021 19:20:29.628897905 CET	443	49721	139.162.8.120	192.168.2.3
Feb 22, 2021 19:20:29.629467010 CET	443	49721	139.162.8.120	192.168.2.3
Feb 22, 2021 19:20:29.629607916 CET	49721	443	192.168.2.3	139.162.8.120
Feb 22, 2021 19:20:29.630937099 CET	49721	443	192.168.2.3	139.162.8.120
Feb 22, 2021 19:20:29.852118015 CET	443	49721	139.162.8.120	192.168.2.3
Feb 22, 2021 19:20:30.522454977 CET	443	49721	139.162.8.120	192.168.2.3
Feb 22, 2021 19:20:30.522802114 CET	49721	443	192.168.2.3	139.162.8.120
Feb 22, 2021 19:20:30.525335073 CET	49721	443	192.168.2.3	139.162.8.120
Feb 22, 2021 19:20:30.535044909 CET	443	49721	139.162.8.120	192.168.2.3
Feb 22, 2021 19:20:30.535351992 CET	443	49721	139.162.8.120	192.168.2.3
Feb 22, 2021 19:20:30.540003061 CET	49721	443	192.168.2.3	139.162.8.120
Feb 22, 2021 19:20:30.540625095 CET	49721	443	192.168.2.3	139.162.8.120
Feb 22, 2021 19:20:30.748271942 CET	443	49721	139.162.8.120	192.168.2.3
Feb 22, 2021 19:20:30.748473883 CET	49721	443	192.168.2.3	139.162.8.120

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 19:20:13.536171913 CET	64938	53	192.168.2.3	8.8.8.8
Feb 22, 2021 19:20:13.589221001 CET	53	64938	8.8.8.8	192.168.2.3
Feb 22, 2021 19:20:13.652007103 CET	60152	53	192.168.2.3	8.8.8.8
Feb 22, 2021 19:20:13.720706940 CET	53	60152	8.8.8.8	192.168.2.3
Feb 22, 2021 19:20:14.366910934 CET	57544	53	192.168.2.3	8.8.8.8
Feb 22, 2021 19:20:14.417426109 CET	53	57544	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 19:20:15.299793959 CET	55984	53	192.168.2.3	8.8.8.8
Feb 22, 2021 19:20:15.351500034 CET	53	55984	8.8.8.8	192.168.2.3
Feb 22, 2021 19:20:16.055807114 CET	64185	53	192.168.2.3	8.8.8.8
Feb 22, 2021 19:20:16.104733944 CET	53	64185	8.8.8.8	192.168.2.3
Feb 22, 2021 19:20:16.864917994 CET	65110	53	192.168.2.3	8.8.8.8
Feb 22, 2021 19:20:16.916476011 CET	53	65110	8.8.8.8	192.168.2.3
Feb 22, 2021 19:20:19.264467955 CET	58361	53	192.168.2.3	8.8.8.8
Feb 22, 2021 19:20:19.313463926 CET	53	58361	8.8.8.8	192.168.2.3
Feb 22, 2021 19:20:24.550055981 CET	63492	53	192.168.2.3	8.8.8.8
Feb 22, 2021 19:20:24.599874020 CET	53	63492	8.8.8.8	192.168.2.3
Feb 22, 2021 19:20:25.660494089 CET	60831	53	192.168.2.3	8.8.8.8
Feb 22, 2021 19:20:25.710973024 CET	53	60831	8.8.8.8	192.168.2.3
Feb 22, 2021 19:20:26.040143967 CET	60100	53	192.168.2.3	8.8.8.8
Feb 22, 2021 19:20:26.113622904 CET	53	60100	8.8.8.8	192.168.2.3
Feb 22, 2021 19:20:26.557635069 CET	53195	53	192.168.2.3	8.8.8.8
Feb 22, 2021 19:20:26.632488012 CET	53	53195	8.8.8.8	192.168.2.3
Feb 22, 2021 19:20:27.288362980 CET	50141	53	192.168.2.3	8.8.8.8
Feb 22, 2021 19:20:27.345408916 CET	53	50141	8.8.8.8	192.168.2.3
Feb 22, 2021 19:20:27.573331118 CET	53195	53	192.168.2.3	8.8.8.8
Feb 22, 2021 19:20:27.633255959 CET	53	53195	8.8.8.8	192.168.2.3
Feb 22, 2021 19:20:28.589118958 CET	53195	53	192.168.2.3	8.8.8.8
Feb 22, 2021 19:20:28.658246040 CET	53	53195	8.8.8.8	192.168.2.3
Feb 22, 2021 19:20:28.884668112 CET	53023	53	192.168.2.3	8.8.8.8
Feb 22, 2021 19:20:28.943761110 CET	53	53023	8.8.8.8	192.168.2.3
Feb 22, 2021 19:20:29.453006029 CET	49563	53	192.168.2.3	8.8.8.8
Feb 22, 2021 19:20:29.504666090 CET	53	49563	8.8.8.8	192.168.2.3
Feb 22, 2021 19:20:30.586302042 CET	53195	53	192.168.2.3	8.8.8.8
Feb 22, 2021 19:20:30.643656015 CET	53	53195	8.8.8.8	192.168.2.3
Feb 22, 2021 19:20:30.688621044 CET	51352	53	192.168.2.3	8.8.8.8
Feb 22, 2021 19:20:30.740325928 CET	53	51352	8.8.8.8	192.168.2.3
Feb 22, 2021 19:20:31.581621885 CET	59349	53	192.168.2.3	8.8.8.8
Feb 22, 2021 19:20:31.630434990 CET	53	59349	8.8.8.8	192.168.2.3
Feb 22, 2021 19:20:32.360450983 CET	57084	53	192.168.2.3	8.8.8.8
Feb 22, 2021 19:20:32.409260988 CET	53	57084	8.8.8.8	192.168.2.3
Feb 22, 2021 19:20:33.146677971 CET	58823	53	192.168.2.3	8.8.8.8
Feb 22, 2021 19:20:33.203701019 CET	53	58823	8.8.8.8	192.168.2.3
Feb 22, 2021 19:20:34.309154987 CET	57568	53	192.168.2.3	8.8.8.8
Feb 22, 2021 19:20:34.357893944 CET	53	57568	8.8.8.8	192.168.2.3
Feb 22, 2021 19:20:34.711848974 CET	53195	53	192.168.2.3	8.8.8.8
Feb 22, 2021 19:20:34.769081116 CET	53	53195	8.8.8.8	192.168.2.3
Feb 22, 2021 19:20:35.913816929 CET	50540	53	192.168.2.3	8.8.8.8
Feb 22, 2021 19:20:35.962596893 CET	53	50540	8.8.8.8	192.168.2.3
Feb 22, 2021 19:20:37.668611050 CET	54366	53	192.168.2.3	8.8.8.8
Feb 22, 2021 19:20:37.718168020 CET	53	54366	8.8.8.8	192.168.2.3
Feb 22, 2021 19:20:38.598248959 CET	53034	53	192.168.2.3	8.8.8.8
Feb 22, 2021 19:20:38.648453951 CET	53	53034	8.8.8.8	192.168.2.3
Feb 22, 2021 19:20:47.300442934 CET	57762	53	192.168.2.3	8.8.8.8
Feb 22, 2021 19:20:47.351907969 CET	53	57762	8.8.8.8	192.168.2.3
Feb 22, 2021 19:20:50.563761950 CET	55435	53	192.168.2.3	8.8.8.8
Feb 22, 2021 19:20:50.623769045 CET	53	55435	8.8.8.8	192.168.2.3
Feb 22, 2021 19:21:07.490240097 CET	50713	53	192.168.2.3	8.8.8.8
Feb 22, 2021 19:21:07.558243036 CET	53	50713	8.8.8.8	192.168.2.3
Feb 22, 2021 19:21:08.928632975 CET	56132	53	192.168.2.3	8.8.8.8
Feb 22, 2021 19:21:08.980113029 CET	53	56132	8.8.8.8	192.168.2.3
Feb 22, 2021 19:21:10.731972933 CET	58987	53	192.168.2.3	8.8.8.8
Feb 22, 2021 19:21:10.785418034 CET	53	58987	8.8.8.8	192.168.2.3
Feb 22, 2021 19:21:12.184909105 CET	56579	53	192.168.2.3	8.8.8.8
Feb 22, 2021 19:21:12.238502026 CET	53	56579	8.8.8.8	192.168.2.3
Feb 22, 2021 19:21:17.196134090 CET	60633	53	192.168.2.3	8.8.8.8
Feb 22, 2021 19:21:17.257117033 CET	53	60633	8.8.8.8	192.168.2.3
Feb 22, 2021 19:21:50.932719946 CET	61292	53	192.168.2.3	8.8.8.8
Feb 22, 2021 19:21:50.981904984 CET	53	61292	8.8.8.8	192.168.2.3
Feb 22, 2021 19:21:51.519282103 CET	63619	53	192.168.2.3	8.8.8.8
Feb 22, 2021 19:21:51.576239109 CET	53	63619	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 19:22:14.238630056 CET	64938	53	192.168.2.3	8.8.8.8
Feb 22, 2021 19:22:14.291295052 CET	53	64938	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 22, 2021 19:20:28.884668112 CET	192.168.2.3	8.8.8.8	0x12d8	Standard query (0)	pg.happyslot88.cc	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 19:20:28.943761110 CET	8.8.8.8	192.168.2.3	0x12d8	No error (0)	pg.happyslot88.cc		139.162.8.120	A (IP address)	IN (0x0001)

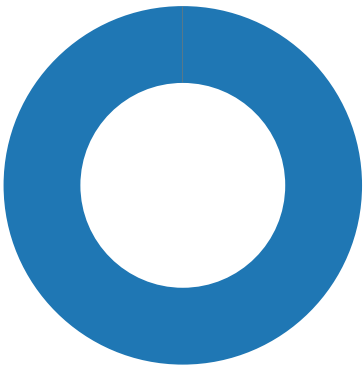
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 22, 2021 19:20:29.392064095 CET	139.162.8.120	443	192.168.2.3	49721	CN=pg.happyslot88.cc 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.	Mon Feb 01 08:41:15 CET 2021	Sun May 02 09:41:15 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		

Code Manipulations

Statistics

Behavior



● EXCEL.EXE
● rundll32.exe



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2576 Parent PID: 792

General

Start time:	19:20:24
Start date:	22/02/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0x1140000
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	16CF643	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	16CF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\I\NetCache	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	16CF643	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	16CF643	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	16CF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\I\NetCookies	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	16CF643	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	16CF643	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	16CF643	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\I\NetCookies	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	16CF643	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	16CF643	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	16CF643	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	16CF643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\I\NetCache\Content.MSO\750DEE41.tmp	success or wait	1	12B495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\I\NetCache\Content.MSO\2344F88C.tmp	success or wait	1	12B495B	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	11B20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	11B211C	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	11B213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	11B213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 6196 Parent PID: 2576

General

Start time:	19:20:30
Start date:	22/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true

Commandline:	rundll32 ..\rieuro.vnt,DllRegisterServer
Imagebase:	0xf10000
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