ID: 441923
Sample Name: statistic-1496367785.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 17:46:18
Date: 29/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

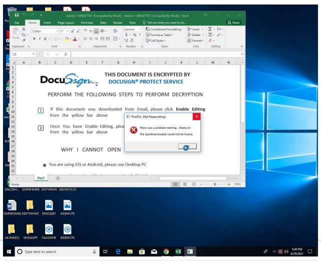
Windows Analysis Report statistic-1496367785.xls

Overview

General Information

Sample Name:	statistic-1496367785.xls
Analysis ID:	441923
MD5:	7fb48e03b899f79..
SHA1:	55445d13cd4331..
SHA256:	1c818433e1ca49..
Infos:	

Most interesting Screenshot:



statistic-1496367785 [Compatibility Mode] - statistic-1496367785 [Compatibility Mode] - Excel

THIS DOCUMENT IS ENCRYPTED BY
DOCUSIGN® PROTECT SERVICE

PERFORM THE FOLLOWING STEPS TO PERFORM DECRYPTION

1 If this document was downloaded from Email, please click **Enable Editing** from the yellow bar above

2 Once You have Enable Editing, plea… from the yellow bar above

WHY I CANNOT OPEN

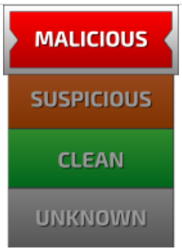
You are using iOS or Android, please use Desktop PC

RunDLL (Not Responding)

There was a problem starting ..\flamo.vir

The specified module could not be found.

Detection



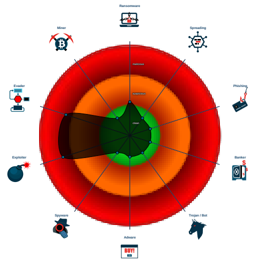
Hidden Macro 4.0

Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- Found abnormal large hidden Excel …
- Sigma detected: Microsoft Office Pr…
- Yara detected hidden Macro 4.0 in E…
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…
- Potential document exploit detected…
- Potential document exploit detected…

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 6844 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 5304 cmdline: rundll32 ..\flamo.vir,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5428 cmdline: rundll32 ..\flamo.vir1,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
statistic-1496367785.xls	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	
statistic-1496367785.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

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

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

Found abnormal large hidden Excel 4.0 Macro sheet

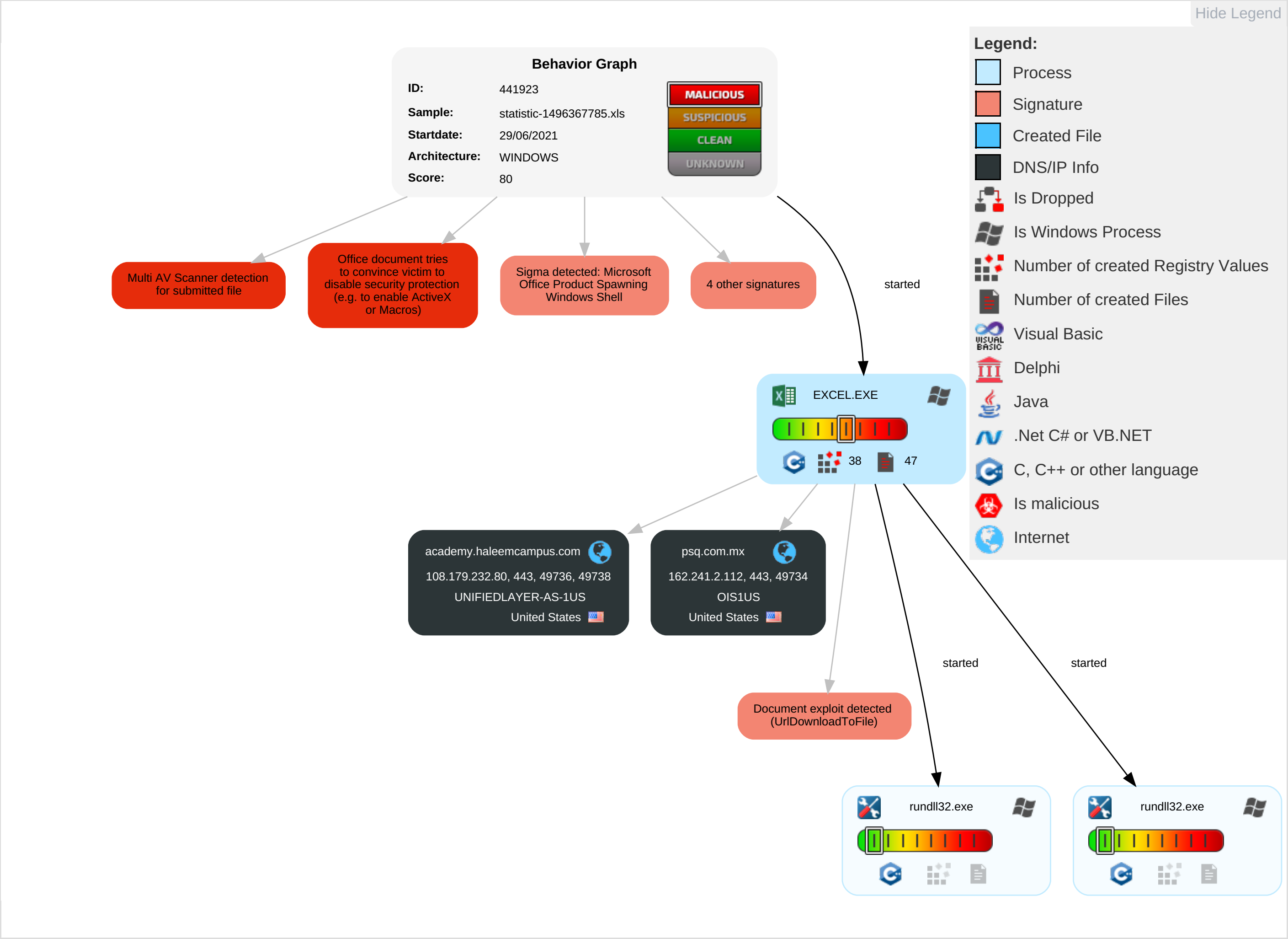
HIPS / PFW / Operating System Protection Evasion:

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	In
Valid Accounts	Scripting 2	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 Sy Pa
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	De Lo
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	De De Da
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		Ca Bi Fr
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		M Ap Ra or

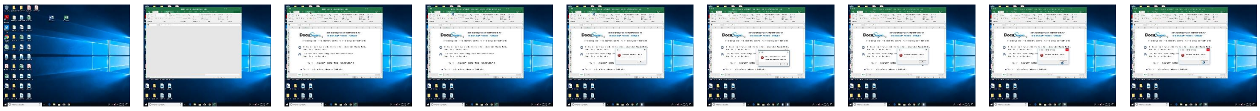
Behavior Graph

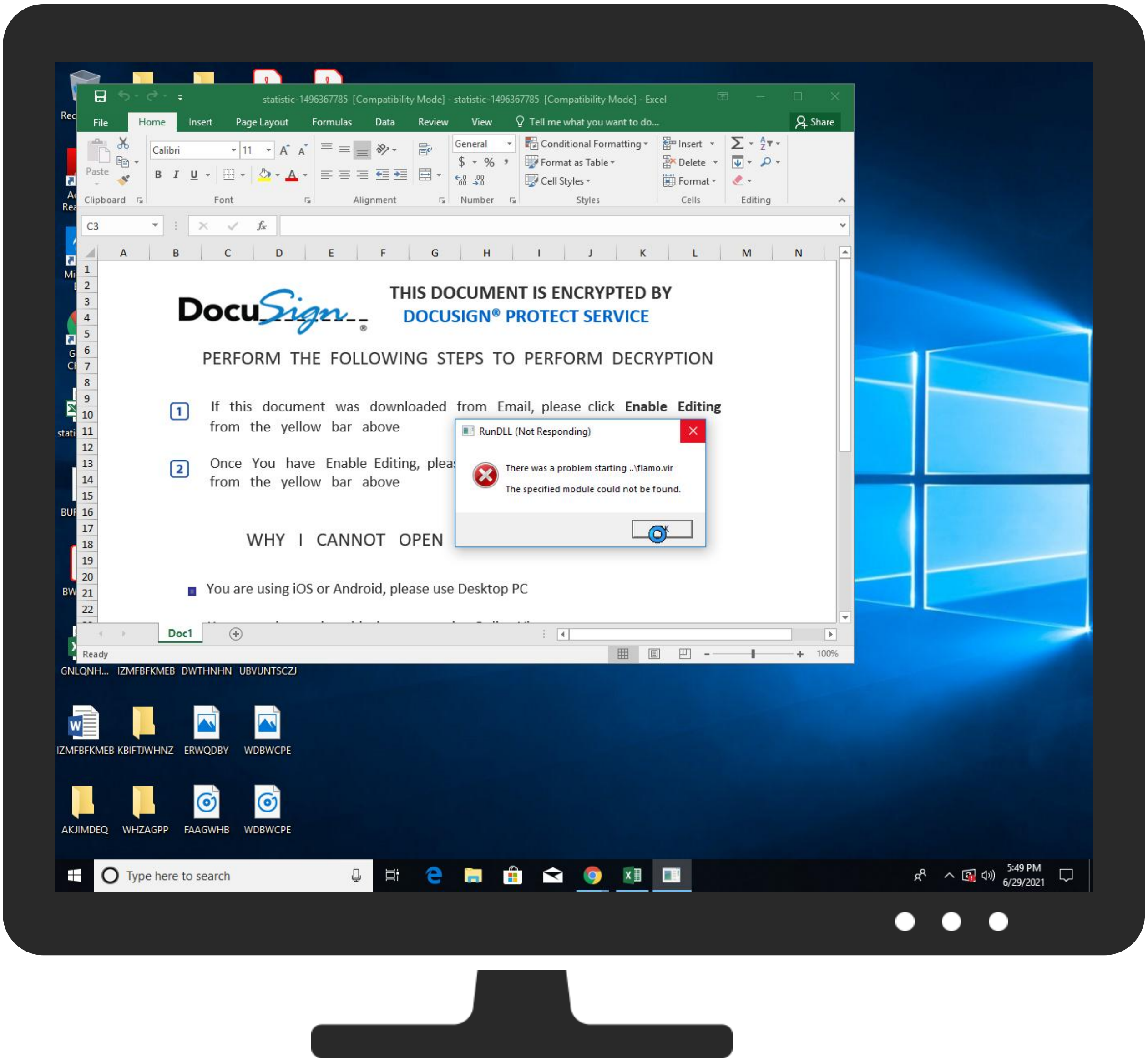


Screenshots

Thumbnails

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





statistic-1496367785 [Compatibility Mode] - statistic-1496367785 [Compatibility Mode] - Excel

THIS DOCUMENT IS ENCRYPTED BY
DOCUSIGN® PROTECT SERVICE

PERFORM THE FOLLOWING STEPS TO PERFORM DECRYPTION

1 If this document was downloaded from Email, please click **Enable Editing** from the yellow bar above

2 Once You have Enable Editing, pleas from the yellow bar above

WHY I CANNOT OPEN

- You are using iOS or Android, please use Desktop PC

RunDLL (Not Responding)

There was a problem starting ..\flamo.vir

The specified module could not be found.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
statistic-1496367785.xls	38%	Virustotal		Browse
statistic-1496367785.xls	35%	ReversingLabs	Document-Excel.Trojan.Woreflint	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
academy.haleemcampus.com	1%	Virustotal		Browse
psq.com.mx	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://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://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	
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://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Virustotal		Browse
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	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%	Virustotal		Browse
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://directory.services.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
academy.haleemcampus.com	108.179.232.80	true	false	• 1%, Virustotal, Browse	unknown
psq.com.mx	162.241.2.112	true	false	• 1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
108.179.232.80	academy.haleemcampus.com	United States	🇺🇸	46606	UNIFIEDLAYER-AS-1US	false
162.241.2.112	psq.com.mx	United States	🇺🇸	26337	OIS1US	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	441923
Start date:	29.06.2021
Start time:	17:46:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	statistic-1496367785.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:	17
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:	mal80.expl.evad.winXLS@5/7@2/2
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 • Found warning dialog • Click Ok
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
108.179.232.80	statistic-1496367785.xls	Get hash	malicious	Browse	
	33c179ca_by_Libranalysis.xls	Get hash	malicious	Browse	
	33c179ca_by_Libranalysis.xls	Get hash	malicious	Browse	
	7fb953aa_by_Libranalysis.xls	Get hash	malicious	Browse	
	7fb953aa_by_Libranalysis.xls	Get hash	malicious	Browse	
	statistic-462462953.xls	Get hash	malicious	Browse	
	statistic-462462953.xls	Get hash	malicious	Browse	
	statistic-1403316517.xls	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	statistic-1403316517.xls	Get hash	malicious	Browse	
	statistic-260077031.xls	Get hash	malicious	Browse	
	statistic-260077031.xls	Get hash	malicious	Browse	
	5c89f585_by_Libranalysis.xls	Get hash	malicious	Browse	
	5c89f585_by_Libranalysis.xls	Get hash	malicious	Browse	
	statistic-1066846651.xls	Get hash	malicious	Browse	
	statistic-1066846651.xls	Get hash	malicious	Browse	
162.241.2.112	statistic-1496367785.xls	Get hash	malicious	Browse	
	33c179ca_by_Libranalysis.xls	Get hash	malicious	Browse	
	33c179ca_by_Libranalysis.xls	Get hash	malicious	Browse	
	7fb953aa_by_Libranalysis.xls	Get hash	malicious	Browse	
	7fb953aa_by_Libranalysis.xls	Get hash	malicious	Browse	
	statistic-462462953.xls	Get hash	malicious	Browse	
	statistic-462462953.xls	Get hash	malicious	Browse	
	statistic-1403316517.xls	Get hash	malicious	Browse	
	statistic-1403316517.xls	Get hash	malicious	Browse	
	statistic-260077031.xls	Get hash	malicious	Browse	
	statistic-260077031.xls	Get hash	malicious	Browse	
	5c89f585_by_Libranalysis.xls	Get hash	malicious	Browse	
	5c89f585_by_Libranalysis.xls	Get hash	malicious	Browse	
	statistic-1066846651.xls	Get hash	malicious	Browse	
	statistic-1066846651.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
psq.com.mx	statistic-1496367785.xls	Get hash	malicious	Browse	• 162.241.2.112
	33c179ca_by_Libranalysis.xls	Get hash	malicious	Browse	• 162.241.2.112
	33c179ca_by_Libranalysis.xls	Get hash	malicious	Browse	• 162.241.2.112
	7fb953aa_by_Libranalysis.xls	Get hash	malicious	Browse	• 162.241.2.112
	7fb953aa_by_Libranalysis.xls	Get hash	malicious	Browse	• 162.241.2.112
	statistic-462462953.xls	Get hash	malicious	Browse	• 162.241.2.112
	statistic-462462953.xls	Get hash	malicious	Browse	• 162.241.2.112
	statistic-1403316517.xls	Get hash	malicious	Browse	• 162.241.2.112
	statistic-1403316517.xls	Get hash	malicious	Browse	• 162.241.2.112
	statistic-260077031.xls	Get hash	malicious	Browse	• 162.241.2.112
	statistic-260077031.xls	Get hash	malicious	Browse	• 162.241.2.112
	5c89f585_by_Libranalysis.xls	Get hash	malicious	Browse	• 162.241.2.112
	5c89f585_by_Libranalysis.xls	Get hash	malicious	Browse	• 162.241.2.112
	statistic-1066846651.xls	Get hash	malicious	Browse	• 162.241.2.112
	statistic-1066846651.xls	Get hash	malicious	Browse	• 162.241.2.112
academy.haleemcampus.com	33c179ca_by_Libranalysis.xls	Get hash	malicious	Browse	• 108.179.232.80
	33c179ca_by_Libranalysis.xls	Get hash	malicious	Browse	• 108.179.232.80
	7fb953aa_by_Libranalysis.xls	Get hash	malicious	Browse	• 108.179.232.80
	7fb953aa_by_Libranalysis.xls	Get hash	malicious	Browse	• 108.179.232.80
	statistic-462462953.xls	Get hash	malicious	Browse	• 108.179.232.80
	statistic-462462953.xls	Get hash	malicious	Browse	• 108.179.232.80
	statistic-1403316517.xls	Get hash	malicious	Browse	• 108.179.232.80
	statistic-1403316517.xls	Get hash	malicious	Browse	• 108.179.232.80
	statistic-260077031.xls	Get hash	malicious	Browse	• 108.179.232.80
	statistic-260077031.xls	Get hash	malicious	Browse	• 108.179.232.80
	5c89f585_by_Libranalysis.xls	Get hash	malicious	Browse	• 108.179.232.80
	5c89f585_by_Libranalysis.xls	Get hash	malicious	Browse	• 108.179.232.80
	statistic-1066846651.xls	Get hash	malicious	Browse	• 108.179.232.80
	statistic-1066846651.xls	Get hash	malicious	Browse	• 108.179.232.80

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OIS1US	statistic-1496367785.xls	Get hash	malicious	Browse	• 162.241.2.112
	Purchase Order.exe	Get hash	malicious	Browse	• 162.241.85.212
	DHL DOCUMENTS.exe	Get hash	malicious	Browse	• 162.241.85.210
	New_PO#98202139.xll	Get hash	malicious	Browse	• 162.241.2.66
	Payment_Swift00987.exe	Get hash	malicious	Browse	• 162.241.2.50

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Payment_Advice.exe	Get hash	malicious	Browse	• 162.241.2.50
	PO#8076.exe	Get hash	malicious	Browse	• 162.241.2.239
	New_Order.xll	Get hash	malicious	Browse	• 162.241.2.66
	PO36782110.xll	Get hash	malicious	Browse	• 162.241.2.66
	Product_Inquiry.xll	Get hash	malicious	Browse	• 162.241.2.66
	Request for quotation,PDF.exe	Get hash	malicious	Browse	• 162.241.203.147
	Request for quotation,PDF.exe	Get hash	malicious	Browse	• 162.241.203.147
	CARGO ARRIVAL NOTICE-MEDICOM AWB.exe	Get hash	malicious	Browse	• 162.241.85.231
	Payment_Advice.exe	Get hash	malicious	Browse	• 162.241.2.50
	ZRvY1UrHuF.xls	Get hash	malicious	Browse	• 162.241.203.185
	PO_no52071.exe	Get hash	malicious	Browse	• 162.241.2.122
	33c179ca_by_Libranalysis.xls	Get hash	malicious	Browse	• 162.241.2.112
	33c179ca_by_Libranalysis.xls	Get hash	malicious	Browse	• 162.241.2.112
	7fb953aa_by_Libranalysis.xls	Get hash	malicious	Browse	• 162.241.2.112
	7fb953aa_by_Libranalysis.xls	Get hash	malicious	Browse	• 162.241.2.112
UNIFIEDLAYER-AS-1US	statistic-1496367785.xls	Get hash	malicious	Browse	• 108.179.232.80
	4dvYb6Nq3y.exe	Get hash	malicious	Browse	• 50.87.238.189
	Remittance.xls	Get hash	malicious	Browse	• 162.241.120.180
	SecuriteInfo.com.Trojan.Win32.Save.a.27842.exe	Get hash	malicious	Browse	• 192.185.164.148
	SEOCHANG INDUSTRY Co., Ltd..exe	Get hash	malicious	Browse	• 162.241.24.206
	7R9igRpuL4.msi	Get hash	malicious	Browse	• 192.185.0.218
	nxinF8KuKS.exe	Get hash	malicious	Browse	• 192.185.16.56
	242jQP4mQP.exe	Get hash	malicious	Browse	• 50.87.248.20
	Halkbank.exe	Get hash	malicious	Browse	• 192.185.0.218
	HBenKsn2R8.exe	Get hash	malicious	Browse	• 96.125.162.104
	DC Viet Nam Order list 6-25-21.exe	Get hash	malicious	Browse	• 162.144.0.158
	Minutes of Meeting 22062021.exe	Get hash	malicious	Browse	• 108.167.156.42
	plan-1053707320.xlsb	Get hash	malicious	Browse	• 50.116.92.246
	plan-1053707320.xlsb	Get hash	malicious	Browse	• 50.116.92.246
	factura y factura de la v#U00eda a#U00e9rea.exe	Get hash	malicious	Browse	• 74.220.199.6
	T5gtQGRL8u.exe	Get hash	malicious	Browse	• 162.241.135.156
	PO 74230360.xlsb	Get hash	malicious	Browse	• 162.241.114.107
	PO 74230360.xlsb	Get hash	malicious	Browse	• 162.241.114.107
	PO 74230360.xlsb	Get hash	malicious	Browse	• 162.241.114.107
	plan-930205822.xlsb	Get hash	malicious	Browse	• 50.116.92.246

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	Bank_ details.exe	Get hash	malicious	Browse	• 108.179.232.80 • 162.241.2.112
	prijenos SWIFT za partiju 220000000001182910.exe	Get hash	malicious	Browse	• 108.179.232.80 • 162.241.2.112
	PO29012021,pdf.ppam	Get hash	malicious	Browse	• 108.179.232.80 • 162.241.2.112
	OFfcxY5xia.exe	Get hash	malicious	Browse	• 108.179.232.80 • 162.241.2.112
	k72fFnCoEX.exe	Get hash	malicious	Browse	• 108.179.232.80 • 162.241.2.112
	DWJn18MuX6.exe	Get hash	malicious	Browse	• 108.179.232.80 • 162.241.2.112
	sp7UUM849P.exe	Get hash	malicious	Browse	• 108.179.232.80 • 162.241.2.112
	CL2SJ8-LYGF7Z-SEJ2QPPAPL.htm	Get hash	malicious	Browse	• 108.179.232.80 • 162.241.2.112
	AqZrR9upiM.exe	Get hash	malicious	Browse	• 108.179.232.80 • 162.241.2.112
	iduD2A1.dll	Get hash	malicious	Browse	• 108.179.232.80 • 162.241.2.112

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	E6973qZ1cV.exe	Get hash	malicious	Browse	108.179.232.80 162.241.2.112
	97FC461FD24104740310BD741F7F8EBF489E640AA93A0.exe	Get hash	malicious	Browse	108.179.232.80 162.241.2.112
	Tu33yM3ZKj.exe	Get hash	malicious	Browse	108.179.232.80 162.241.2.112
	BNK1135000001.docx	Get hash	malicious	Browse	108.179.232.80 162.241.2.112
	message_zdm.html	Get hash	malicious	Browse	108.179.232.80 162.241.2.112
	Financial Statements.html	Get hash	malicious	Browse	108.179.232.80 162.241.2.112
	Wilson-McShane Corporation ACH.xlsx	Get hash	malicious	Browse	108.179.232.80 162.241.2.112
	Dfdvfczl_Signed_.exe	Get hash	malicious	Browse	108.179.232.80 162.241.2.112
	9irkb5Rbn8.exe	Get hash	malicious	Browse	108.179.232.80 162.241.2.112
	kgx2fkTmpa.exe	Get hash	malicious	Browse	108.179.232.80 162.241.2.112

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\0A8CE175-D39D-43AE-8F1B-CA84388C02A0

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):	135209
Entropy (8bit):	5.363078467391509
Encrypted:	false
SSDEEP:	1536:pcQIKNgeBTA3gBwlpQ9DQW+zoY34ZliKWXboOidX5E6LWME9:9EQ9DQW+zwXO1
MD5:	F36D695FFC65C02CF6642D107DE3436E
SHA1:	A6E39AE62834265B4937B554FF799614E6CBD2BC
SHA-256:	0A1F0B3E72F02FBF65827B4356D516DA6D321ACB4EB356F16657728C82584E94
SHA-512:	E21B9C58D9A8AE3B1CA665CB890568370C080F42E41072CED05ED5CA5C4A7507ADF0AC349300276F24EC4CDCE5BFB3D88FF53AB15A14443EFB4FE6D5D3BD950
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="2021-06-29T15:47:13">.. Build: 16.0.14228.30525-->.. <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\BDB40000

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	82869
Entropy (8bit):	7.897086363765867
Encrypted:	false
SSDEEP:	1536:ILMCBgFqO57Lav5F/U2SiwFNfZ7pjS8ZiYhuiNde9kJY:04qO5PWzUWwtNm8ZUmY
MD5:	30C64BA689D114C1B1F07726F4B0F643
SHA1:	6E453A1835195371901BDEC66BDDE4EAAC7B0DD2
SHA-256:	E9806EDFE4032C38F466EC4CB002167D14B5076F4197EBE861053E1A3BE5ECC9
SHA-512:	A285BEF29AB022AC67BB0E0D55E0A9DD1E04F16D301C5EA081AC7B7D6AA598875692E742FCAB3285A61BA2C51EC632AE8BAC04CE5E1BE2603899763B4512510E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\BDB40000

Preview:	.U.N.0.}G.....J\@Z!....w.`?....U..1..=c7..JK)...'s.3.x|...z.....7#V..^i....u}.*L.)a...-.......n..+.v.>.p.9......p...hE.... .\t.OF._\z...:e.6._.L.T]-hy.d...~...T-.!.-E"....w$......%..C....H.4!jb.......o...{.m..7gD0......2K)..?...r.c........T7".?.[|a......f;H6.b....).5V........Y.......?A.v.l._.....Qt.B....b........c..t........\..g..a'...........6..].k..:T..Y.....}...K3.&..4.#....D..u .I.z.m..kF......@m...<.......PK..........!.[:..............[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 17:12:41 2019, mtime=Tue Jun 29 14:47:14 2021, atime=Tue Jun 29 14:47:14 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.655853070338881
Encrypted:	false
SSDEEP:	12:8vVCXUM7t7gcduCH2BvOpM4IiujBF+WrjAZ/DYbDMSeuSeL44t2Y+xIBjKZm:8W9qmpTyVAZbcDG7aB6m
MD5:	C28D5CC4959D0E1E0857E734A7985781
SHA1:	02DD24C036CD987F04E14B31EF9ECDEDF4B75E50
SHA-256:	E1050433736C4F3D25755ECD8A6E34798FA29A618D0A58BC759B4D208756C19A
SHA-512:	B48A5C3C3280FD958E5042B35A152E976770ED7C9AD959048870DF6790740DF9007302E66BDEDCBC0D33523995DDF3E74172DA641AC48EDB37D7638D779DD2
Malicious:	false
Reputation:	low
Preview:	L..................F.............-..1?r..l....o..l...0......................u....P.O. .:i.....+00.../C:\..................x.1......N....Users.d......L...R.}...................:......;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Q}<..user.<.......N...R.}....#J........................j.o.n.e.s.....~.1......R.}..Desktop.h.......N...R.}.....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.......820094...........!a..%.H.VZAj...m<..............!a..%.H.VZAj...m<.........................1SPS.XF.L8C....&.m.q............/...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.........9...1SPS..mD..pH.H@..=x.....h....H......K*..@.A..7sFJ............

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	113
Entropy (8bit):	4.71317481637129
Encrypted:	false
SSDEEP:	3:oyBVomMnUTWeS4UOytUTWeS4UmMnUTWeS4Uv:dj6nUTL8tUTLinUTLK
MD5:	827572951026F0F9437E31D866B8FF08
SHA1:	0B6A363D618B5E1D031EE6E5DCE5C18A9B13BBE6
SHA-256:	493A258224290D5C5BB92DC4C57E3B8E36D4BE213CC9F3744D69D345F03B843B
SHA-512:	F224FE824B181BEA88A282AFDD4528CF59F8952BD571C595AC6E6E3F2E7E9FA499B9E8FC5DE623B02501C0D341A82B3A7053B7550746CA36CDC6EBF1FBA662B
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..statistic-1496367785.LNK=0..statistic-1496367785.LNK=0..[xls]..statistic-1496367785.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\statistic-1496367785.LNK

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 06:35:54 2020, mtime=Tue Jun 29 14:47:15 2021, atime=Tue Jun 29 14:47:15 2021, length=176128, window=hide
Category:	modified
Size (bytes):	2210
Entropy (8bit):	4.704393826342388
Encrypted:	false
SSDEEP:	48:8Ogw9qmp5Y5MiWlOkMkBB6pOgw9qmp5Y5MiWlOkMkBB6:8hcZiWlOdwKhcZiWlOdw
MD5:	1DBF118D07425F742972F80B6F479464
SHA1:	348393828935581579897E182E3872D7033C7054
SHA-256:	8996BA14F72BBE59CC466D0F4AB1911D640C453A9EC210C47DD791D3301037AB
SHA-512:	9A2021007A4621460404B0BDC89CC20E55E35F7F26F6F4AAAFD5F3961AA10539D9D8122016337C16769CE55F360D49B2CF54EF351A671C799CA325D283135453
Malicious:	false
Reputation:	low
Preview:	L..................F.... ....\T........l......l...............................P.O. .:i.....+00.../C:\..................x.1......N....Users.d......L...R.}...................:......;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Q}<..user.<.......N...R.}....#J........................j.o.n.e.s.....~.1.....>Q.<..Desktop.h.......N...R.}.....Y.............>......T..D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....~.2......R.} .STATIS~1.XLS..b......>Q|<.R.}.....V.....................a..s.t.a.t.i.s.t.i.c.-.1.4.9.6.3.6.7.7.8.5...x.l.s.......^...............-.......]...........>.S......C:\Users\user\Desktop\statistic-1496367785.xls../.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.s.t.a.t.i.s.t.i.c.-.1.4.9.6.3.6.7.7.8.5...x.l.s.........:..,.LB.)...As...`.......X.......820094...........!a..%.H.VZAj...Z................!a..%.H.VZAj...Z..........................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.

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	dropped
Size (bytes):	22
Entropy (8bit):	2.9808259362290785
Encrypted:	false
SSDEEP:	3:QAlX0Gn:QKn
MD5:	7962B839183642D3CDC2F9CEBDBF85CE
SHA1:	2BE8F6F309962ED367866F6E70668508BC814C2D
SHA-256:	5EB8655BA3D3E7252CA81C2B9076A791CD912872D9F0447F23F4C4AC4A6514F6
SHA-512:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB 342
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\7EB40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	222635
Entropy (8bit):	5.628519548551312
Encrypted:	false
SSDEEP:	6144:a8rmdAIByzElbSRg3WCbgBeP5NmPTdbsizCnQC6VqCJ6KS8rmdAIByzElbSRg3WS:uLnQC6sCRY
MD5:	6F378E0FCB99595324566C5A91985656
SHA1:	9059F775A49511C7A614F831EC90841008171C0D
SHA-256:	3026EAEDD6AFA59DF4C54D4CF1E1EE6A4891F32CC83B2B1AA95426B0F6458763
SHA-512:	467D5668E72E6D3B891D261512CDDC4A53742B06E2D345BA8180F46FEFA23958BD77D0D6E188624B3F0132A3DB738C108BF774BD918A3571F55CFB98E9B42C0
Malicious:	false
Reputation:	low
Preview:	........T8..........................\.p....pratesh B.....a.........=..=........V..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.......6...........C.a.l.i.b.r.i.1.......4..........C.a.l.i.b.r.i.1.*.h...6..........C.a.l.i.b.r.i. .L.i.g.h.t.1...,...6...........C.a.l.i.b.r.i.1.......6....... ....C.a.l.i.b.r.i.1.......6...........C.a.l.i.b.r.i.1.................C.a.l.i.b.r.i.1.................C.a.l.i.b.r.i.1.................C.a.l.i.b.r.i.1.......4..........C.a.l.i.b.r.i.1.................C.a.l.i.b.r.i.1............ ......C.a.l.i.b.r.i.1.................C.a.l.i.b.r.i.

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Author: van-van, Last Saved By: Grog, Name of Creating Application: Microsoft Excel, Create Time/Date: Fri Jun 5 19:17:20 2015, Last Saved Time/Date: Fri May 21 09 :07:02 2021, Security: 0
Entropy (8bit):	2.0857713013138395
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	statistic-1496367785.xls
File size:	536064
MD5:	7fb48e03b899f792be6c3118a46c5c8f
SHA1:	55445d13cd433121c6c2bfb31414b08e31e28a65
SHA256:	1c818433e1ca49729f987b3f060b2133c8375f8164181c4 684600a278ee6033f
SHA512:	e950fe3278277996dbfb9f7f80bd03976793ba4967f27261 2f901eea83e1284a512104348ab14d3028dcac0ef9cd527 dde9ce22323c90fa080fae3fcdc79905f
SSDEEP:	6144:C6tIrWqrY5O3NMHGRYc9u/YRTP85XbDu1XYiXx y:Ru1XPE
File Content Preview:	........................>... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "statistic-1496367785.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:	False

Summary

Code Page:	1251
Author:	van-van
Last Saved By:	Grog
Create Time:	2015-06-05 18:17:20
Last Saved Time:	2021-05-21 08:07:02
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Document Code Page:	1251
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False

Streams

Macro 4.0 Code

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 29, 2021 17:47:16.690315008 CEST	192.168.2.4	8.8.8.8	0xe30f	Standard query (0)	psq.com.mx	A (IP address)	IN (0x0001)
Jun 29, 2021 17:47:18.234659910 CEST	192.168.2.4	8.8.8.8	0x544f	Standard query (0)	academy.haleemcampus.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 29, 2021 17:47:16.874973059 CEST	8.8.8.8	192.168.2.4	0xe30f	No error (0)	psq.com.mx		162.241.2.112	A (IP address)	IN (0x0001)
Jun 29, 2021 17:47:18.292426109 CEST	8.8.8.8	192.168.2.4	0x544f	No error (0)	academy.haleemcampus.com		108.179.232.80	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
Jun 29, 2021 17:47:17.197526932 CEST	162.241.2.112	443	192.168.2.4	49734	CN=psq.com.mx CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Tue Jul 28 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018	Thu Jul 29 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
Jun 29, 2021 17:47:18.617918968 CEST	108.179.232.80	443	192.168.2.4	49736	CN=www.academy.haleemcampus.com CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue May 25 09:21:24 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Mon Aug 23 09:21:24 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	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=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 6844 Parent PID: 800

General

Start time:	17:47:10
Start date:	29/06/2021
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:	0xe40000
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

Show Windows behavior

File Created

File Deleted

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: rundll32.exe PID: 5304 Parent PID: 6844

General

Start time:	17:49:08
Start date:	29/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\flamo.vir,DllRegisterServer
Imagebase:	0x20000
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

Show Windows behavior

Analysis Process: rundll32.exe PID: 5428 Parent PID: 6844

General

Start time:	17:49:09
Start date:	29/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\flamo.vir1,DllRegisterServer

Imagebase:	0x20000
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

Show Windows behavior

Disassembly

Code Analysis