ID: 411767
Sample Name:
ox87DNNM8d.exe
Cookbook: default.jbs
Time: 06:27:57
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

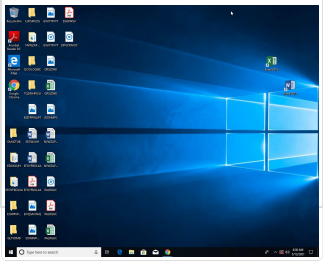
Analysis Report ox87DNNM8d.exe

Overview

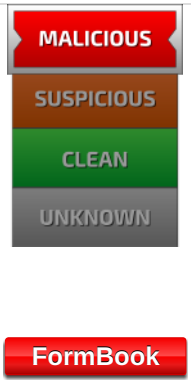
General Information

Sample Name:	ox87DNNM8d.exe
Analysis ID:	411767
MD5:	41e38bcd6f5f300..
SHA1:	2f3b2173d7a5a3a.
SHA256:	4e2b4396335fc6d.
Infos:	

Most interesting Screenshot:



Detection

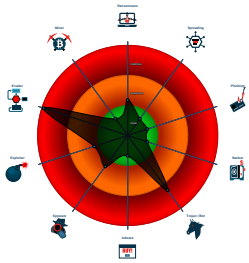


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- System process connects to networ…
- Yara detected AntiVM3
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Injects a PE file into a foreign proce…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…
- Queues an APC in another process …

Classification



Startup

- **System is w10x64**
- ox87DNNM8d.exe (PID: 4368 cmdline: 'C:\Users\user\Desktop\ox87DNNM8d.exe' MD5: 41E38BCD6F5F3001C2E4F08EBCD2396C)
  - ox87DNNM8d.exe (PID: 5656 cmdline: C:\Users\user\Desktop\ox87DNNM8d.exe MD5: 41E38BCD6F5F3001C2E4F08EBCD2396C)
    - explorer.exe (PID: 3472 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - systray.exe (PID: 6544 cmdline: C:\Windows\SysWOW64\systray.exe MD5: 1373D481BE4C8A6E5F5030D2FB0A0C68)
        - cmd.exe (PID: 6824 cmdline: /c del 'C:\Users\user\Desktop\ox87DNNM8d.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6876 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.panda810.com/sve/"
  ],
  "decoy": [
    "rockouqe.com",
    "secureproductsolutions.net",
    "josephserino.com",
    "operationstrategy.com",
    "umrohalfatih.com",
    "humanityenlightened.com",
    "taylorxgroup.com",
    "francescopetroni.net",
    "anaume-kun.com",
    "galleryalireza.com",
    "alimamavn.com",
    "tym0769.com",
    "trendselection.club",
    "warmupspod.com",
    "v-work.xyz",
    "aclmspecialmeeting2020.com",
    "youporn-live.net",
    "germinatebio.net",
    "hempnseeds.com",
    "ezfto.com",
    "pengruncapital.com",
    "voxitor.com",
    "hempdivasmag.com",
    "everydayleadershipinstitute.com",
    "biking-division.com",
    "livingstonemoments.com",
    "vstarfireworks.com",
    "abilitybrazil.com",
    "gixaa.com",
    "kp-dental.com",
    "developmentignited.com",
    "8155a.com",
    "petylook.com",
    "agrogroupkz.com",
    "germsbuzzter.com",
    "valley-bitcoin.com",
    "dcsdeliveryaz.website",
    "elitefriendlies.com",
    "pinoywebtools.com",
    "circuleather.com",
    "mioskinplus.info",
    "tamaraog.com",
    "maxfelicitavideo.com",
    "americacivics.com",
    "shebawatches.com",
    "meisammirhashemi.com",
    "nelivo.com",
    "real-dating-clubs2.com",
    "poishem.directory",
    "geminein.club",
    "soundalchemyadvanced.com",
    "kidswrtingpadstore.com",
    "cya-wonder.club",
    "tuqof.com",
    "showbizpr.com",
    "homo-nomad.com",
    "bcc-cbd.com",
    "papayacrisp.com",
    "paymentink.gold",
    "purejoyclothing.com",
    "newsadvices.com",
    "gungalmata.com",
    "viewsfromthedriversseat.com",
    "techriew.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.280873290.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000002.280873290.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000003.00000002.280873290.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x183f9:$sqlite3step: 68 34 1C 7B E1 • 0x1850c:$sqlite3step: 68 34 1C 7B E1 • 0x18428:$sqlite3text: 68 38 2A 90 C5 • 0x1854d:$sqlite3text: 68 38 2A 90 C5 • 0x1843b:$sqlite3blob: 68 53 D8 7F 8C • 0x18563:$sqlite3blob: 68 53 D8 7F 8C
00000003.00000002.281369748.0000000001730000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000003.00000002.281369748.0000000001730000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

Unpacked PEs

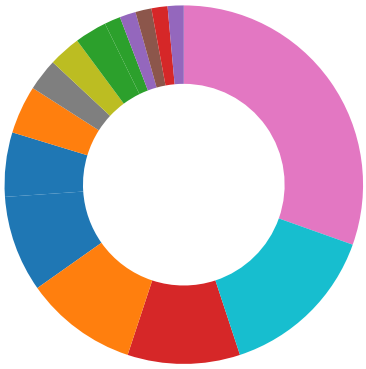
Source	Rule	Description	Author	Strings
3.2.ox87DNNM8d.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.ox87DNNM8d.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.2.ox87DNNM8d.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x183f9:$sqlite3step: 68 34 1C 7B E1 • 0x1850c:$sqlite3step: 68 34 1C 7B E1 • 0x18428:$sqlite3text: 68 38 2A 90 C5 • 0x1854d:$sqlite3text: 68 38 2A 90 C5 • 0x1843b:$sqlite3blob: 68 53 D8 7F 8C • 0x18563:$sqlite3blob: 68 53 D8 7F 8C
1.2.ox87DNNM8d.exe.400dbc8.3.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
1.2.ox87DNNM8d.exe.400dbc8.3.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x12fd98:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x130002:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15c3b8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15c622:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13bb25:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x168145:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13b611:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x167c31:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13bc27:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x168247:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13bd9f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x1683bf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x130a1a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x15d03a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x13a88c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x166eac:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x131713:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x15dd33:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1417c7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x16dde7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1427ca:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 4 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection:

Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

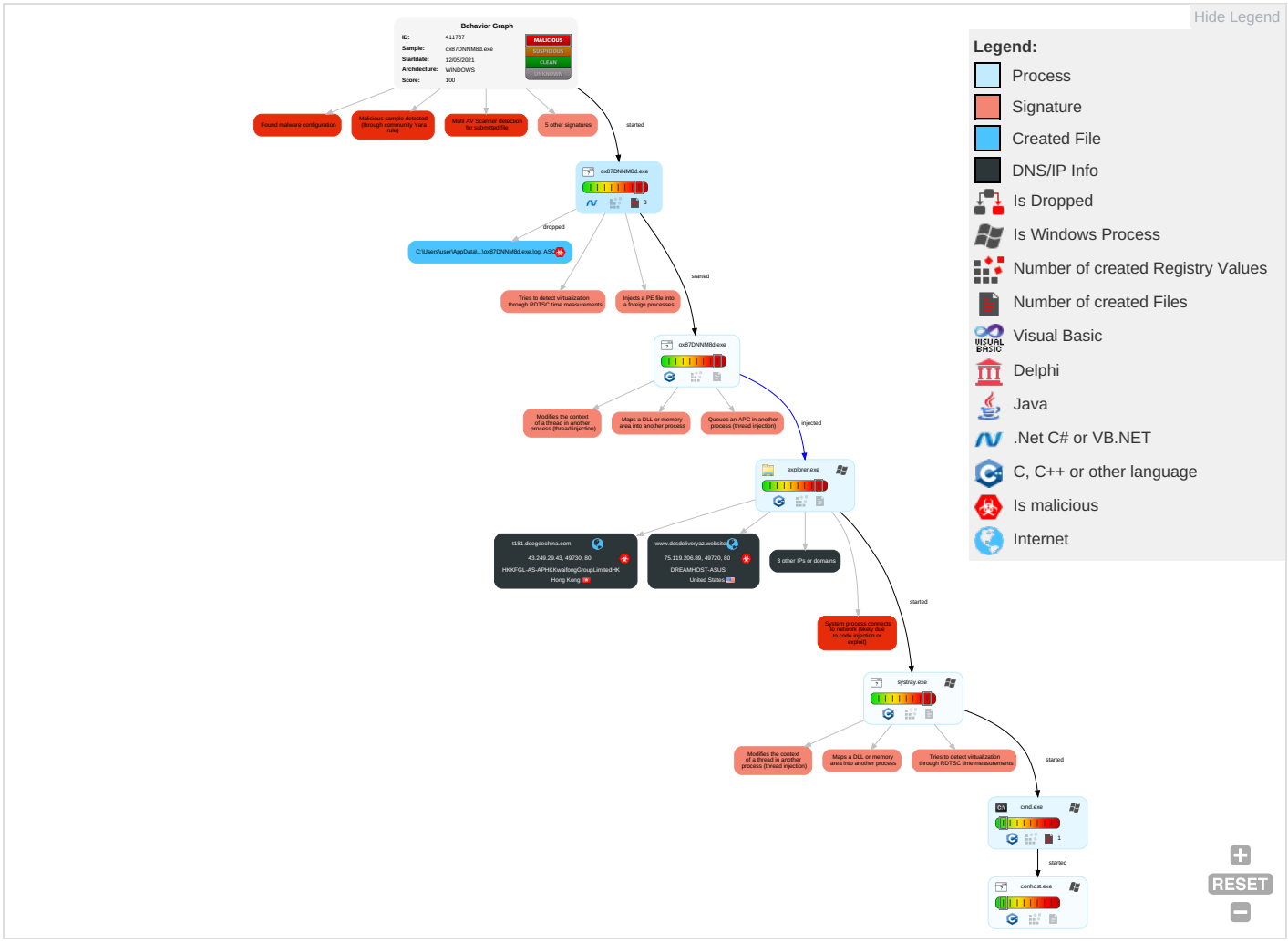
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 5 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 2 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communi
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	Input Capture 1	Process Discovery 2	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS Redirect F Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS Track Dev Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 3 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 5 1 2	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulat Device Communi

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

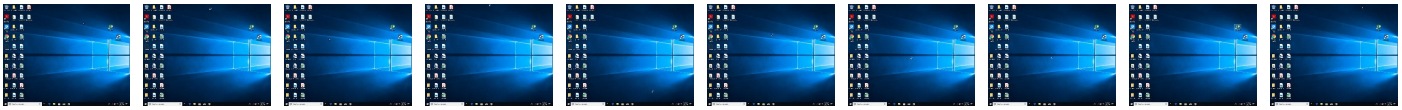
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
ox87DNNM8d.exe	57%	Virustotal		Browse
ox87DNNM8d.exe	41%	Metadefender		Browse
ox87DNNM8d.exe	66%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.ox87DNNM8d.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
t181.deegeechina.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.vstarfireworks.com/sve/?B6Ah=2mSxzHKvGhdVKk9ZF/49Uvkx+tNG2gtFJsc3MZrG0ttjvP+42CyBXtijrWDGJsqiNYNw&8pW=2dUh0da	0%	Avira URL Cloud	safe	
http://www.americacivics.com/sve/?8pW=2dUh0da&B6Ah=pTnyDIvt+g7sdgQmMg9D2FnTPO22hVGFgxtUPmNZyFP4G/454L1vxjiDnOTVCmVO7LzE	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
www.panda810.com/sve/	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.dcsdeliveryaz.website/sve/?B6Ah=exmy3Nx7PpUJKJt1HtiGWNpuQz3EYRIgq3k+uiZc9JLQuvdlfCRkPG1S5SdPXsQAS6a5&8pW=2dUh0da	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.americacivics.com	35.186.238.101	true	false		unknown
t181.deegeechina.com	43.249.29.43	true	true	• 0%, Virustotal, Browse	unknown
www.dcsdeliveryaz.website	75.119.206.89	true	true		unknown
www.secureproductsolutions.net	unknown	unknown	true		unknown
www.vstarfireworks.com	unknown	unknown	true		unknown

Contacted URLs

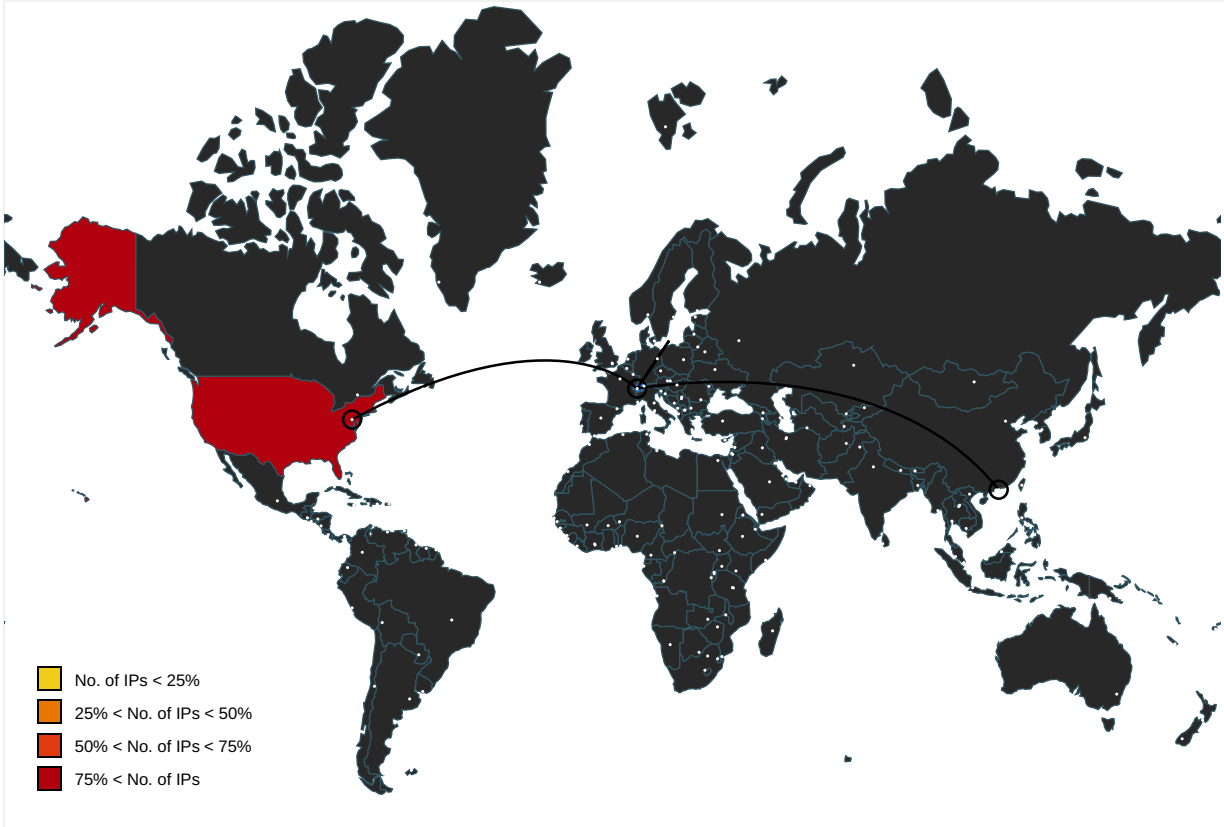
Name	Malicious	Antivirus Detection	Reputation
http://www.vstarfireworks.com/sve/?B6Ah=2mSxzHKvGhdVKk9ZF/49Uvkx+tNG2gtFJsc3MZrG0ttjvP+42CyBXtijrWDGJsqiNYNw&8pW=2dUh0da	true	• Avira URL Cloud: safe	unknown
http://www.americacivics.com/sve/?8pW=2dUh0da&B6Ah=pTnyDIvt+g7sdgQmMg9D2FnTPO22hVGFgxtUPmNZyFP4G/454L1vxjiDnOTVCmVO7LzE	false	• Avira URL Cloud: safe	unknown
www.panda810.com/sve/	true	• Avira URL Cloud: safe	low
http://www.dcsdeliveryaz.website/sve/?B6Ah=exmy3Nx7PpUJKJt1HtiGWNpuQz3EYRIgq3k+uiZc9JLQuvdlfCRkPG1S5SdPXsQAS6a5&8pW=2dUh0da	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000004.00000000.263514865.000000000BC36000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000004.00000000.263514865.000000000BC36000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000004.00000000.263514865.000000000BC36000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000004.00000000.263514865.000000000BC36000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000004.00000000.263514865.000000000BC36000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000004.00000000.263514865.000000000BC36000.00000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000004.00000000.263514865.000000000BC36000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000004.00000000.263514865.000000000BC36000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000004.00000000.263514865.000000000BC36000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	ox87DNNM8d.exe, 00000001.00000002.234229050.0000000002FC7000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	explorer.exe, 00000004.00000000.263514865.000000000BC36000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000004.00000000.263514865.000000000BC36000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000004.00000000.263514865.000000000BC36000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000004.00000000.263514865.000000000BC36000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000004.00000000.263514865.000000000BC36000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000004.00000000.263514865.000000000BC36000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000004.00000000.263514865.000000000BC36000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn	explorer.exe, 00000004.0000000 0.263514865.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000004.0000000 0.263514865.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000004.0000000 0.263514865.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000004.0000000 0.263514865.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000004.0000000 0.263514865.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000004.0000000 0.263514865.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000004.0000000 0.263514865.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000004.0000000 0.263514865.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000004.0000000 0.263514865.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	ox87DNNM8d.exe, 00000001.00000 002.234176049.0000000002F71000 .00000004.00000001.sdmp	false		high
http://www.sakkal.com	explorer.exe, 00000004.0000000 0.263514865.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
35.186.238.101	www.americacivics.com	United States		15169	GOOGLEUS	false
75.119.206.89	www.dcsdeliveryaz.website	United States		26347	DREAMHOST-ASUS	true
43.249.29.43	t181.deegeechina.com	Hong Kong		133115	HKKFGL-AS-APHKKwaifongGroupLimitedHK	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	411767
Start date:	12.05.2021
Start time:	06:27:57
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ox87DNNM8d.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	28
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.evad.winEXE@7/1@4/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 28% (good quality ratio 25.8%) • Quality average: 69.6% • Quality standard deviation: 31.7%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Simulations

Behavior and APIs

Time	Type	Description
06:28:47	API Interceptor	1x Sleep call for process: ox87DNNM8d.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DREAMHOST-ASUS	ENCORE.docx	Get hash	malicious	Browse	• 64.90.45.190
	4GGwmv0AJm.exe	Get hash	malicious	Browse	• 69.163.200.146
	documents-857527454.xlsm	Get hash	malicious	Browse	• 67.205.36.230
	documents-857527454.xlsm	Get hash	malicious	Browse	• 67.205.36.230
	70pGP1JaCf6M0kf.exe	Get hash	malicious	Browse	• 173.236.15 2.151
	documents-1509207685.xlsm	Get hash	malicious	Browse	• 67.205.36.230
	documents-1509207685.xlsm	Get hash	malicious	Browse	• 67.205.36.230
	documents-1576257262.xlsm	Get hash	malicious	Browse	• 67.205.36.230
	documents-1576257262.xlsm	Get hash	malicious	Browse	• 67.205.36.230
	documents-26926602.xlsm	Get hash	malicious	Browse	• 67.205.36.230
	documents-26926602.xlsm	Get hash	malicious	Browse	• 67.205.36.230
	documents-26926602.xlsm	Get hash	malicious	Browse	• 67.205.36.230
	documents-26926602.xlsm	Get hash	malicious	Browse	• 67.205.36.230
	documents-192987462.xlsm	Get hash	malicious	Browse	• 67.205.36.230
	documents-192987462.xlsm	Get hash	malicious	Browse	• 67.205.36.230
	documents-1926412023.xlsm	Get hash	malicious	Browse	• 67.205.36.230
	documents-1926412023.xlsm	Get hash	malicious	Browse	• 67.205.36.230
	documents-102763662.xlsm	Get hash	malicious	Browse	• 67.205.36.230
	documents-102763662.xlsm	Get hash	malicious	Browse	• 67.205.36.230
	Financial Results April 21.pptx (9,753K).exe	Get hash	malicious	Browse	• 66.33.210.242
HKKFGL-AS-APHKKwaifongGroupLimitedHK	bt.apk	Get hash	malicious	Browse	• 39.109.113.244
	#U6e05#U65b0#U59b9#U5a9a#U7167#U9a97@16.exe	Get hash	malicious	Browse	• 110.92.66.233
	#U5e74#U7ec8#U63d0#U6210#U5206#U7ea2#U6838#U5bf9#U8868@i4.exe	Get hash	malicious	Browse	• 110.92.66.246
	insz.exe	Get hash	malicious	Browse	• 88.218.145.49
	DOCUMENTO_MEDICO.doc	Get hash	malicious	Browse	• 154.221.28.167
	NI3651011817UL.doc	Get hash	malicious	Browse	• 103.210.23 7.241
	BAL_46979369.doc	Get hash	malicious	Browse	• 103.210.23 7.241
	427424855528075826480424.doc	Get hash	malicious	Browse	• 103.210.23 7.241
	FILE_81380052.doc	Get hash	malicious	Browse	• 103.210.23 7.241
	FILE_PO_09152020EX.doc	Get hash	malicious	Browse	• 103.210.23 7.241
	DOC_PO_09152020EX.doc	Get hash	malicious	Browse	• 103.210.23 7.241
	KH3117818420XX.doc	Get hash	malicious	Browse	• 103.210.23 7.241
	XCP_87353228.doc	Get hash	malicious	Browse	• 103.210.23 7.241
	BAL_PO_09152020EX.doc	Get hash	malicious	Browse	• 103.210.23 7.241
	IO3812758081JW.doc	Get hash	malicious	Browse	• 103.210.23 7.241
	BAL_53345761.doc	Get hash	malicious	Browse	• 103.210.23 7.241
	FILE_PO_09152020EX.doc	Get hash	malicious	Browse	• 103.210.23 7.241
	FILE_YZGLOSASM.doc	Get hash	malicious	Browse	• 103.210.23 7.241
	BAL_3105782760272.doc	Get hash	malicious	Browse	• 103.210.23 7.241
	VCG4PMFIB0AR.doc	Get hash	malicious	Browse	• 103.210.23 7.241

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ox87DNNM8d.exe.log	
Process:	C:\Users\user\Desktop\ox87DNNM8d.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.613842542238479
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	ox87DNNM8d.exe
File size:	840704
MD5:	41e38bcd6f5f3001c2e4f08ebcd2396c
SHA1:	2f3b2173d7a5a3a19e8a73d5fbfde7abc1836909
SHA256:	4e2b4396335fc6d3e6ff8c19b326f0f6342f537ba026ce1901d2122b2c7b3e4c
SHA512:	20c03ac7e5647f2140f9c969046fd9aa86e18b352387e52238a1f652694a40a374aa499309827f71599de6cad89937a373bc9d3d1cc83e7ed8a37593d386bd4
SSDEEP:	24576:cAXIVpK3/ZWzEtY+i+/+He2yjmfNRp+n6:9EpK3/ZWYtYv0+He2emV+6
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....0.....O... ...`....@.. ....@.....

File Icon

Icon Hash:	f8ce929a929a92d4

Static PE Info

General	
Entrypoint:	0x4b4fb2
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60948AF6 [Fri May 7 00:33:58 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb4f58	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb8000	0x19eb8	.rsrc

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb6000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xb2fb8	0xb3000	False	0.92964112692	data	7.93204508639	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.reloc	0xb6000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0xb8000	0x19eb8	0x1a000	False	0.0641432542067	data	2.31358815064	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xb8220	0xac5	PNG image data, 256 x 256, 8-bit gray+alpha, non-interlaced		
RT_ICON	0xb8ce8	0xb20	data		
RT_ICON	0xb9808	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 16777215, next used block 16777215		
RT_ICON	0xbbdb0	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 16777215, next used block 16777215		
RT_ICON	0xbce58	0x10828	data		
RT_ICON	0xcd680	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 16777215, next used block 16777215		
RT_GROUP_ICON	0xd18a8	0x5a	data		
RT_VERSION	0xd1904	0x400	data		
RT_MANIFEST	0xd1d04	0x1b4	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

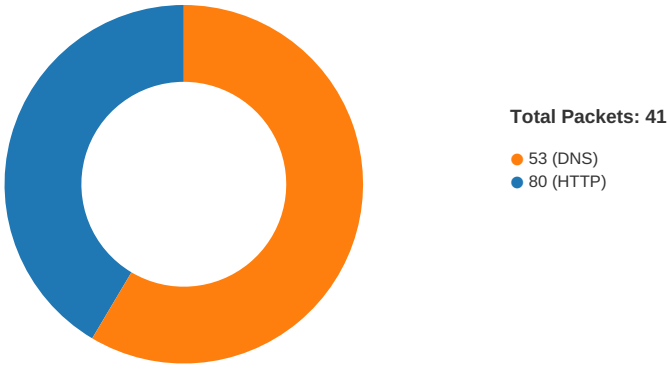
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Crowbar 2015. This software is licensed under the GNU General Public License v3.0 or above.
Assembly Version	1.0.0.0
InternalName	DateTimeNative.exe
FileVersion	1.0.0.0
CompanyName	Crowbar
LegalTrademarks	
Comments	Awesome clipboard manager.
ProductName	Clippy
ProductVersion	1.0.0.0
FileDescription	Clippy
OriginalFilename	DateTimeNative.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/12/21-06:30:28.857747	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49728	35.186.238.101	192.168.2.5

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 06:30:08.731209040 CEST	49720	80	192.168.2.5	75.119.206.89
May 12, 2021 06:30:08.932468891 CEST	80	49720	75.119.206.89	192.168.2.5
May 12, 2021 06:30:08.932590961 CEST	49720	80	192.168.2.5	75.119.206.89
May 12, 2021 06:30:08.932787895 CEST	49720	80	192.168.2.5	75.119.206.89
May 12, 2021 06:30:09.134083986 CEST	80	49720	75.119.206.89	192.168.2.5
May 12, 2021 06:30:09.236999989 CEST	80	49720	75.119.206.89	192.168.2.5
May 12, 2021 06:30:09.238914967 CEST	49720	80	192.168.2.5	75.119.206.89
May 12, 2021 06:30:09.240603924 CEST	80	49720	75.119.206.89	192.168.2.5
May 12, 2021 06:30:09.241219997 CEST	49720	80	192.168.2.5	75.119.206.89
May 12, 2021 06:30:09.441761017 CEST	80	49720	75.119.206.89	192.168.2.5
May 12, 2021 06:30:28.676335096 CEST	49728	80	192.168.2.5	35.186.238.101
May 12, 2021 06:30:28.720247984 CEST	80	49728	35.186.238.101	192.168.2.5
May 12, 2021 06:30:28.721172094 CEST	49728	80	192.168.2.5	35.186.238.101
May 12, 2021 06:30:28.721317053 CEST	49728	80	192.168.2.5	35.186.238.101
May 12, 2021 06:30:28.762145996 CEST	80	49728	35.186.238.101	192.168.2.5
May 12, 2021 06:30:28.857747078 CEST	80	49728	35.186.238.101	192.168.2.5
May 12, 2021 06:30:28.858009100 CEST	49728	80	192.168.2.5	35.186.238.101
May 12, 2021 06:30:28.858123064 CEST	80	49728	35.186.238.101	192.168.2.5
May 12, 2021 06:30:28.858201027 CEST	49728	80	192.168.2.5	35.186.238.101
May 12, 2021 06:30:28.898891926 CEST	80	49728	35.186.238.101	192.168.2.5
May 12, 2021 06:30:51.399552107 CEST	49730	80	192.168.2.5	43.249.29.43
May 12, 2021 06:30:51.676214933 CEST	80	49730	43.249.29.43	192.168.2.5
May 12, 2021 06:30:51.676359892 CEST	49730	80	192.168.2.5	43.249.29.43
May 12, 2021 06:30:51.676578999 CEST	49730	80	192.168.2.5	43.249.29.43
May 12, 2021 06:30:51.971482038 CEST	80	49730	43.249.29.43	192.168.2.5
May 12, 2021 06:30:51.971520901 CEST	80	49730	43.249.29.43	192.168.2.5
May 12, 2021 06:30:51.971709967 CEST	49730	80	192.168.2.5	43.249.29.43
May 12, 2021 06:30:52.173600912 CEST	49730	80	192.168.2.5	43.249.29.43
May 12, 2021 06:30:52.250524998 CEST	80	49730	43.249.29.43	192.168.2.5
May 12, 2021 06:30:52.250617981 CEST	49730	80	192.168.2.5	43.249.29.43
May 12, 2021 06:30:52.452609062 CEST	80	49730	43.249.29.43	192.168.2.5
May 12, 2021 06:30:52.452783108 CEST	49730	80	192.168.2.5	43.249.29.43

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 06:28:38.799510002 CEST	64344	53	192.168.2.5	8.8.8.8
May 12, 2021 06:28:38.854988098 CEST	53	64344	8.8.8.8	192.168.2.5
May 12, 2021 06:28:39.447067976 CEST	62060	53	192.168.2.5	8.8.8.8
May 12, 2021 06:28:39.520203114 CEST	53	62060	8.8.8.8	192.168.2.5
May 12, 2021 06:28:40.034023046 CEST	61805	53	192.168.2.5	8.8.8.8
May 12, 2021 06:28:40.090976954 CEST	53	61805	8.8.8.8	192.168.2.5
May 12, 2021 06:28:41.152870893 CEST	54795	53	192.168.2.5	8.8.8.8
May 12, 2021 06:28:41.201633930 CEST	53	54795	8.8.8.8	192.168.2.5
May 12, 2021 06:28:41.601744890 CEST	49557	53	192.168.2.5	8.8.8.8
May 12, 2021 06:28:41.662442923 CEST	53	49557	8.8.8.8	192.168.2.5
May 12, 2021 06:28:45.705430031 CEST	61733	53	192.168.2.5	8.8.8.8
May 12, 2021 06:28:45.756230116 CEST	53	61733	8.8.8.8	192.168.2.5
May 12, 2021 06:28:47.224498987 CEST	65447	53	192.168.2.5	8.8.8.8
May 12, 2021 06:28:47.273613930 CEST	53	65447	8.8.8.8	192.168.2.5
May 12, 2021 06:28:48.591703892 CEST	52441	53	192.168.2.5	8.8.8.8
May 12, 2021 06:28:48.651035070 CEST	53	52441	8.8.8.8	192.168.2.5
May 12, 2021 06:28:50.457161903 CEST	62176	53	192.168.2.5	8.8.8.8
May 12, 2021 06:28:50.505949020 CEST	53	62176	8.8.8.8	192.168.2.5
May 12, 2021 06:28:51.592045069 CEST	59596	53	192.168.2.5	8.8.8.8
May 12, 2021 06:28:51.640861988 CEST	53	59596	8.8.8.8	192.168.2.5
May 12, 2021 06:28:53.460700989 CEST	65296	53	192.168.2.5	8.8.8.8
May 12, 2021 06:28:53.512550116 CEST	53	65296	8.8.8.8	192.168.2.5
May 12, 2021 06:28:54.732152939 CEST	63183	53	192.168.2.5	8.8.8.8
May 12, 2021 06:28:54.782819033 CEST	53	63183	8.8.8.8	192.168.2.5
May 12, 2021 06:29:07.680038929 CEST	60151	53	192.168.2.5	8.8.8.8
May 12, 2021 06:29:07.741580963 CEST	53	60151	8.8.8.8	192.168.2.5
May 12, 2021 06:29:25.114991903 CEST	56969	53	192.168.2.5	8.8.8.8
May 12, 2021 06:29:25.180248976 CEST	53	56969	8.8.8.8	192.168.2.5
May 12, 2021 06:29:46.937997103 CEST	55161	53	192.168.2.5	8.8.8.8
May 12, 2021 06:29:46.999602079 CEST	53	55161	8.8.8.8	192.168.2.5
May 12, 2021 06:29:48.188477993 CEST	54757	53	192.168.2.5	8.8.8.8
May 12, 2021 06:29:48.268415928 CEST	53	54757	8.8.8.8	192.168.2.5
May 12, 2021 06:29:59.183288097 CEST	49992	53	192.168.2.5	8.8.8.8
May 12, 2021 06:29:59.251389980 CEST	53	49992	8.8.8.8	192.168.2.5
May 12, 2021 06:30:08.481898069 CEST	60075	53	192.168.2.5	8.8.8.8
May 12, 2021 06:30:08.707669020 CEST	53	60075	8.8.8.8	192.168.2.5
May 12, 2021 06:30:13.955764055 CEST	55016	53	192.168.2.5	8.8.8.8
May 12, 2021 06:30:14.014740944 CEST	53	55016	8.8.8.8	192.168.2.5
May 12, 2021 06:30:18.336004019 CEST	64345	53	192.168.2.5	8.8.8.8
May 12, 2021 06:30:18.397649050 CEST	53	64345	8.8.8.8	192.168.2.5
May 12, 2021 06:30:28.614039898 CEST	57128	53	192.168.2.5	8.8.8.8
May 12, 2021 06:30:28.675231934 CEST	53	57128	8.8.8.8	192.168.2.5
May 12, 2021 06:30:48.976097107 CEST	54791	53	192.168.2.5	8.8.8.8
May 12, 2021 06:30:49.052944899 CEST	53	54791	8.8.8.8	192.168.2.5
May 12, 2021 06:30:51.048041105 CEST	50463	53	192.168.2.5	8.8.8.8
May 12, 2021 06:30:51.398247957 CEST	53	50463	8.8.8.8	192.168.2.5
May 12, 2021 06:30:51.405097961 CEST	50394	53	192.168.2.5	8.8.8.8
May 12, 2021 06:30:51.478733063 CEST	53	50394	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 06:29:48.188477993 CEST	192.168.2.5	8.8.8.8	0x9fe0	Standard query (0)	www.secure productsol utions.net	A (IP address)	IN (0x0001)
May 12, 2021 06:30:08.481898069 CEST	192.168.2.5	8.8.8.8	0xba98	Standard query (0)	www.dcsdel iveryaz.website	A (IP address)	IN (0x0001)
May 12, 2021 06:30:28.614039898 CEST	192.168.2.5	8.8.8.8	0x26ee	Standard query (0)	www.americ acivics.com	A (IP address)	IN (0x0001)
May 12, 2021 06:30:51.048041105 CEST	192.168.2.5	8.8.8.8	0x89c	Standard query (0)	www.vstarf ireworks.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 06:29:48.268415928 CEST	8.8.8.8	192.168.2.5	0x9fe0	Name error (3)	www.secure productsol utions.net	none	none	A (IP address)	IN (0x0001)
May 12, 2021 06:30:08.707669020 CEST	8.8.8.8	192.168.2.5	0xba98	No error (0)	www.dcsdel iveryaz.website		75.119.206.89	A (IP address)	IN (0x0001)
May 12, 2021 06:30:28.675231934 CEST	8.8.8.8	192.168.2.5	0x26ee	No error (0)	www.americ acivics.com		35.186.238.101	A (IP address)	IN (0x0001)
May 12, 2021 06:30:51.398247957 CEST	8.8.8.8	192.168.2.5	0x89c	No error (0)	www.vstarf ireworks.com	t181.deegeechina.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 06:30:51.398247957 CEST	8.8.8.8	192.168.2.5	0x89c	No error (0)	t181.deege echina.com		43.249.29.43	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.dcsdeliveryaz.website
- www.americacivics.com
- www.vstarfireworks.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49720	75.119.206.89	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 06:30:08.932787895 CEST	1393	OUT	GET /sve/?B6Ah=exmy3Nx7PpUJKJt1HtiGWNpuQz3EYRIgq3k+uiZc9JLQuvdlfCRkPG1S5SdPXsQAS6a5&8pW=2dUh0da HTTP/1.1 Host: www.dcsdeliveryaz.website Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 06:30:09.236999989 CEST	1394	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 12 May 2021 04:30:09 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 Upgrade: h2 Connection: Upgrade, close Location: http://dcsdeliveryaz.website/sve/?B6Ah=exmy3Nx7PpUJKJt1HtiGWNpuQz3EYRIgq3k+uiZc9JLQuvdlfCRkPG1S5SdPXsQAS6a5&8pW=2dUh0da Vary: User-Agent Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49728	35.186.238.101	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 06:30:28.721317053 CEST	4707	OUT	GET /sve/?8pW=2dUh0da&B6Ah=pTnyDIvt+g7sdgQmMg9D2FnTPO22hVGFgxtUPmNZyFP4G/454L1vxjiDnOTVCmVO7LzE HTTP/1.1 Host: www.americacivics.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 06:30:28.857747078 CEST	4707	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 12 May 2021 04:30:28 GMT Content-Type: text/html Content-Length: 275 ETag: "6099a39b-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49730	43.249.29.43	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 06:30:51.676578999 CEST	4725	OUT	GET /sve/?B6Ah=2mSxzHKvGhdVKk9ZF/49Uvkx+tNG2gtFJsc3MZrG0ttjvP+42CyBXtijrWDGJsqiNYNw&8pW=2dUh0da HTTP/1.1 Host: www.vstarfireworks.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 06:30:51.971482038 CEST	4727	IN	HTTP/1.1 404 Not Found Cache-Control: no-store Pragma: no-cache Content-Type: text/html Server: IIS X-Powered-By: WAF/2.0 Date: Wed, 12 May 2021 05:07:40 GMT Connection: close Content-Length: 1163 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 67 62 32 33 31 32 22 2f 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 d5 d2 bb b5 bd ce c4 bc fe bb f2 c4 bf c2 bc a1 a3 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 3c 21 2d 2d 0d 0a 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 2d 73 69 Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=gb2312"/><title>404 - </title><style type="text/css">...body{margin:0;font-si

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

Processes

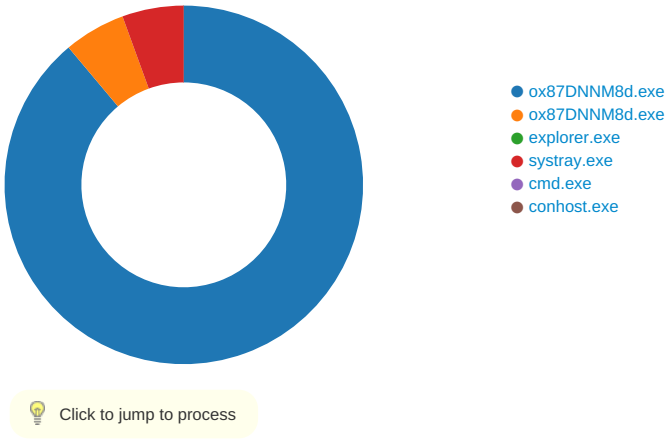
Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x81 0x1E 0xEC

Function Name	Hook Type	New Data
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x89 0x9E 0xEC
GetMessageW	INLINE	0x48 0x8B 0xB8 0x89 0x9E 0xEC
GetMessageA	INLINE	0x48 0x8B 0xB8 0x81 0x1E 0xEC

Statistics

Behavior



System Behavior

Analysis Process: ox87DNNM8d.exe PID: 4368 Parent PID: 5700

General

Start time:	06:28:46
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\ox87DNNM8d.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ox87DNNM8d.exe'
Imagebase:	0xb50000
File size:	840704 bytes
MD5 hash:	41E38BCD6F5F3001C2E4F08EBCD2396C
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: 00000001.00000002.234588732.0000000003F79000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.234588732.0000000003F79000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.234588732.0000000003F79000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.234229050.0000000002FC7000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DCCCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DCCCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ox87DNNM8d.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DFDC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ox87DNNM8d.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6DFDC907	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	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB11B4F	ReadFile

Analysis Process: ox87DNNM8d.exe PID: 5656 Parent PID: 4368

General

Start time:	06:28:49
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\ox87DNNM8d.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\ox87DNNM8d.exe
Imagebase:	0xfb0000
File size:	840704 bytes
MD5 hash:	41E38BCD6F5F3001C2E4F08EBCD2396C
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: 00000003.00000002.280873290.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.280873290.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.280873290.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.281369748.0000000001730000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.281369748.0000000001730000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.281369748.0000000001730000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.281290291.00000000015E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.281290291.00000000015E0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.281290291.00000000015E0000.00000040.00000001.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	1622408	success or wait	1	419E47	NtReadFile

Analysis Process: explorer.exe PID: 3472 Parent PID: 5656

General

Start time:	06:28:52
Start date:	12/05/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true

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

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: systray.exe PID: 6544 Parent PID: 3472

General

Start time:	06:29:10
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\systray.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\systray.exe
Imagebase:	0x7ff797770000
File size:	9728 bytes
MD5 hash:	1373D481BE4C8A6E5F5030D2FB0A0C68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.493625427.0000000000AA0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.493625427.0000000000AA0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.493625427.0000000000AA0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.492941508.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.492941508.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.492941508.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.492525761.0000000000170000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.492525761.0000000000170000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.492525761.0000000000170000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	189E47	NtReadFile

Analysis Process: cmd.exe PID: 6824 Parent PID: 6544

General

Start time:	06:29:15
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe

Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\ox87DNNM8d.exe'
Imagebase:	0xf60000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6876 Parent PID: 6824

General

Start time:	06:29:15
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis