ID: 458678
Sample Name: moni $@.exe
Cookbook: default.jbs
Time: 16:36:35
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

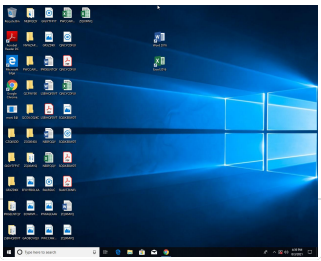
Windows Analysis Report moni $@.exe

Overview

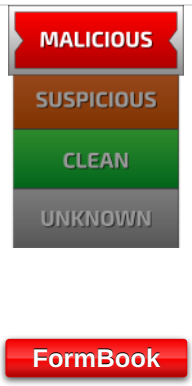
General Information

Sample Name:	moni $@.exe
Analysis ID:	458678
MD5:	1e46a61b2d491a..
SHA1:	5bb236d5c49991..
SHA256:	b07a33b6e6d800..
Tags:	exe null
Infos:	

Most interesting Screenshot:



Detection



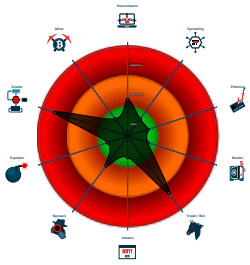
FormBook

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

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Detected unpacking (overwrites its o…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Yara detected AntiVM3
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Machine Learning detection for samp…
- Sigma detected: Suspicious Proces…

Classification



Process Tree

- **System is w10x64**
- moni $@.exe (PID: 3516 cmdline: 'C:\Users\user\Desktop\moni $@.exe' MD5: 1E46A61B2D491A15952BD579210ECB8F)
  - RegSvcs.exe (PID: 5996 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegSvcs.exe MD5: 59FCE79E9D81AB9E2ED4C3561205F5DF)
  - RegSvcs.exe (PID: 6000 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegSvcs.exe MD5: 59FCE79E9D81AB9E2ED4C3561205F5DF)
  - RegSvcs.exe (PID: 404 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegSvcs.exe MD5: 59FCE79E9D81AB9E2ED4C3561205F5DF)
  - RegSvcs.exe (PID: 6060 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegSvcs.exe MD5: 59FCE79E9D81AB9E2ED4C3561205F5DF)
  - RegSvcs.exe (PID: 6028 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegSvcs.exe MD5: 59FCE79E9D81AB9E2ED4C3561205F5DF)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.panyu-qqbaby.com/weni/"
  ],
  "decoy": [
    "sdmdwang.com",
    "konversationswithkoshie.net",
    "carap.club",
    "eagldeream.com",
    "856380585.xyz",
    "elgallocoffee.com",
    "magetu.info",
    "lovertons.com",
    "theichallenge.com",
    "advancedautorepairsonline.com",
    "wingsstyling.info",
    "tapdaugusta.com",
    "wiloasbanhsgtarewdasc.solutions",
    "donjrisdumb.com",
    "experienceddoctor.com",
    "cloverhillconsultants.com",
    "underwear.show",
    "karensgonewild2020.com",
    "arodsr.com",
    "thefucktardmanual.com",
    "712kenwood.info",
    "telecompink.com",
    "ebizkendra.com",
    "kitkatmp3.com",
    "utformehagen.com",
    "profitsnavigator.com",
    "kathyharvey.com",
    "tongaoffshore.com",
    "vrpreservation.com",
    "hy7128.com",
    "nicolettejohnsonphotography.com",
    "rating.travel",
    "visualartcr.com",
    "nationalbarista.com",
    "lovecartoonforever.com",
    "koimkt.com",
    "directpractice.pro",
    "blockchaincloud360.com",
    "queverenbuenosaires.com",
    "coachmyragolden.com",
    "awree.com",
    "facebookipl.com",
    "rcheapwdbuy.com",
    "trinspinsgreen.com",
    "voxaide.com",
    "ecorner.online",
    "mattvickery.com",
    "regarta.com",
    "fknprfct.com",
    "theessentialstore.net",
    "sunilpsingh.com",
    "ovtnywveba.club",
    "optimalgafa.com",
    "awdjob.info",
    "humachem.com",
    "southeasternsteakcompany.com",
    "centerevents.net",
    "warrenswindowcleans.co.uk",
    "lebullterrier.com",
    "thecxchecker.com",
    "formerknown.com",
    "pupbutler.com",
    "tincanphones.com",
    "tgeuuy.cool"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.249181885.0000000013221000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.249181885.0000000013221000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x59470:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x5980a:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x6551d:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x65009:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x6561f:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x65797:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x5a222:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x64284:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x5af9a:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x6a60f:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x6b6b2:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000000.00000002.249181885.0000000013221000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x67541:$sqlite3step: 68 34 1C 7B E1 • 0x67654:$sqlite3step: 68 34 1C 7B E1 • 0x67570:$sqlite3text: 68 38 2A 90 C5 • 0x67695:$sqlite3text: 68 38 2A 90 C5 • 0x67583:$sqlite3blob: 68 53 D8 7F 8C • 0x676ab:$sqlite3blob: 68 53 D8 7F 8C
00000000.00000002.247523574.000000000328E000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Process Memory Space: moni $@.exe PID: 3516	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Suspicious Process Start Without DLL

Sigma detected: Possible Applocker Bypass

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Compliance:

Detected unpacking (overwrites its own PE header)

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Detected unpacking (overwrites its own PE header)

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Stealing of Sensitive Information:

Yara detected FormBook

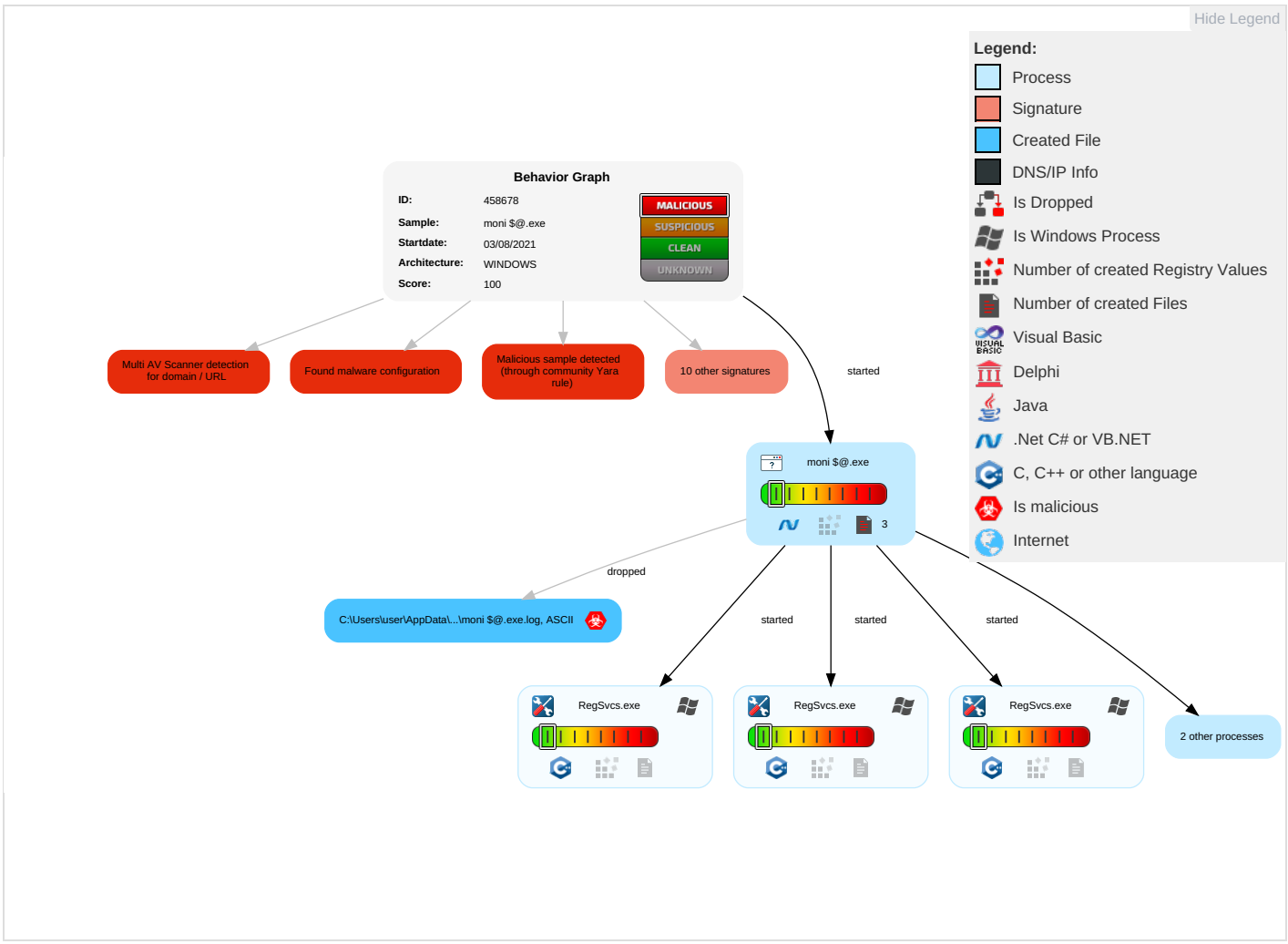
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop or Insecure Network Communicati
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 t Redirect Pho Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 t Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 2	NTDS	System Information Discovery 1 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicati
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

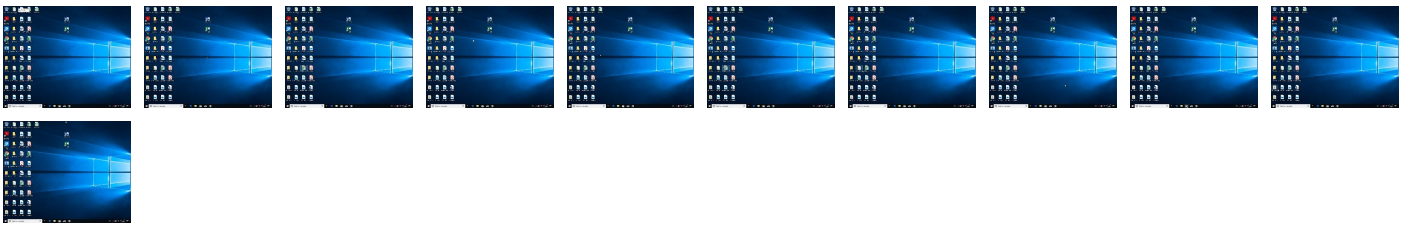
Behavior Graph



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
moni $@.exe	39%	Virustotal		Browse
moni $@.exe	35%	ReversingLabs	Win32.Trojan.Swotter	
moni $@.exe	100%	Avira	HEUR/AGEN.1142734	
moni $@.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.moni $@.exe.ff0000.0.unpack	100%	Avira	HEUR/AGEN.1142734		Download File
0.2.moni $@.exe.ff0000.0.unpack	100%	Avira	HEUR/AGEN.1142734		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
www.panyu-qqbaby.com/weni/	7%	Virustotal		Browse
www.panyu-qqbaby.com/weni/	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.panyu-qqbaby.com/weni/	true	• 7%, Virustotal, Browse • Avira URL Cloud: malware	low

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458678
Start date:	03.08.2021
Start time:	16:36:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	moni $@.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:	31
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@11/1@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 2% (good quality ratio 1.6%) • Quality average: 51.6% • Quality standard deviation: 32.9%
HCA Information:	• Successful, ratio: 86% • 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

Simulations

Behavior and APIs

Time	Type	Description
16:37:30	API Interceptor	1x Sleep call for process: moni $@.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\moni $@.exe.log	
Process:	C:\Users\user\Desktop\moni $@.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1742
Entropy (8bit):	5.381353871108486
Encrypted:	false
SSDEEP:	48:MxHKEYHKGD8Ao6+vxpNl1qHGiD0HKeGitHTG1hAHKKPJAmHKoA9:iqEYqGgAo9ZPlwml0qertzG1eqKPJ/qT
MD5:	978918F6120A43D1FA5899938A5A542F
SHA1:	6567A2E687B40BFD3A46246F51F4C89D93D89455
SHA-256:	F814F290A540B3FD755D05F3434317D7B26F2C33D2087F9E63233CD88AB510FC
SHA-512:	1DF2AF5A3F8212BF591AAA366FE96F167F3E6D43746E07B7CD44F1B2F06C63B1D290412891AD0B4D0A82D1DFD6EB2EB7D70981C35941F370DC97729E9205DD5
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll",0..3,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.V9921e851#\f2e0589ed6d670f264a5f65dd0ad000f\Microsoft.VisualBasic.ni.dll",0..3,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll",0..3,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_6

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.904280766447238
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:	moni $@.exe
File size:	680960
MD5:	1e46a61b2d491a15952bd579210ecb8f
SHA1:	5bb236d5c49991298040dd88b4b83c4cb21e148a
SHA256:	b07a33b6e6d8007b04f1f4a78cd8be773506bbf6b60ed0227665188d57e82a15
SHA512:	022f35d056e6e1856b9c57e7d96ed63b221ad961d0d55085f26bceeb5659bb652cb2bf2e294e4a2c830a3aae67f7ecbcf57021990939b28d771d8afbbc247eb4
SSDEEP:	12288:YBg2LBBBBBBBBBBXBBBBBBBBBBRqLHPmm9SrzQnD+rdhpAUh7qIe6YHedKhBg/:YZmvmYSwSpFZi+dKbgwtGJl+KP3hv
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....X.....Jw... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4a774a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61089407 [Tue Aug 3 00:55:35 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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xa5750	0xa5800	False	0.918747639728	data	7.91066136918	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.reloc	0xa8000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0xaa000	0x61c	0x800	False	0.33740234375	data	4.62076178534	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: moni $@.exe PID: 3516 Parent PID: 5680

General

Start time:	16:37:26
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\moni $@.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\moni $@.exe'
Imagebase:	0xff0000
File size:	680960 bytes
MD5 hash:	1E46A61B2D491A15952BD579210ECB8F
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: 00000000.00000002.249181885.0000000013221000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.249181885.0000000013221000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.249181885.0000000013221000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.247523574.000000000328E000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: RegSvcs.exe PID: 5996 Parent PID: 3516

General

Start time:	16:37:32
Start date:	03/08/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegSvcs.exe
Imagebase:	0x1ea58910000
File size:	44640 bytes
MD5 hash:	59FCE79E9D81AB9E2ED4C3561205F5DF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: RegSvcs.exe PID: 6000 Parent PID: 3516

General

Start time:	16:37:32
Start date:	03/08/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegSvcs.exe
Imagebase:	0x1fc30120000
File size:	44640 bytes
MD5 hash:	59FCE79E9D81AB9E2ED4C3561205F5DF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: RegSvcs.exe PID: 404 Parent PID: 3516

General

Start time:	16:37:33
Start date:	03/08/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegSvcs.exe
Imagebase:	0x25f29860000
File size:	44640 bytes
MD5 hash:	59FCE79E9D81AB9E2ED4C3561205F5DF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: RegSvcs.exe PID: 6060 Parent PID: 3516

General

Start time:	16:37:33
Start date:	03/08/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegSvcs.exe
Imagebase:	0x17f6b7a0000
File size:	44640 bytes
MD5 hash:	59FCE79E9D81AB9E2ED4C3561205F5DF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: RegSvcs.exe PID: 6028 Parent PID: 3516

General

Start time:	16:37:33
Start date:	03/08/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegSvcs.exe
Imagebase:	0x1f4cfd30000
File size:	44640 bytes
MD5 hash:	59FCE79E9D81AB9E2ED4C3561205F5DF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis