ID: 626277
Sample Name:
SecuriteInfo.com.Variant.Jaik.72878.26055.480
Cookbook: default.jbs
Time: 19:42:14
Date: 13/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

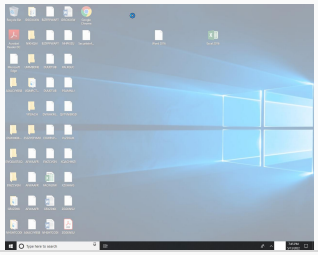
Windows Analysis Report

SecuriteInfo.com.Variant.Jaik.72878.26055.480

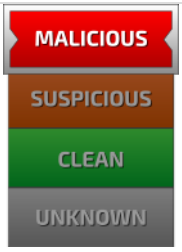
Overview

General Information

Sample Name:	SecuriteInfo.com.Variant.Jaik.72878.26055.480 (renamed file extension from 480 to exe)
Analysis ID:	626277
MD5:	029bbe98a21641.
SHA1:	a24173f1daf45d7.
SHA256:	e73b7de7723536.
Tags:	exe
Infos:	



Detection



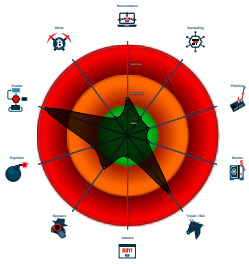
FormBook

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for drop…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Machine Learning detection for sam…
- Injects a PE file into a foreign proce…
- Found evasive API chain (may stop…

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.Variant.Jaik.72878.26055.exe (PID: 7156 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.Variant.Jaik.72878.26055.exe" MD5: 029BBE98A216416EB698CA543A5C0830)
  - idcqz.exe (PID: 5444 cmdline: C:\Users\user\AppData\Local\Temp\idcqz.exe C:\Users\user\AppData\Local\Temp\dknqrab MD5: 51F62DEF6DC686B87CC0BAFC31685546)
    - idcqz.exe (PID: 5408 cmdline: C:\Users\user\AppData\Local\Temp\idcqz.exe C:\Users\user\AppData\Local\Temp\dknqrab MD5: 51F62DEF6DC686B87CC0BAFC31685546)
      - explorer.exe (PID: 3688 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - cmstp.exe (PID: 6488 cmdline: C:\Windows\SysWOW64\cmstp.exe MD5: 4833E65ED211C7F118D4A11E6FB58A09)
          - cmd.exe (PID: 3252 cmdline: /c del "C:\Users\user\AppData\Local\Temp\idcqz.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
            - conhost.exe (PID: 6920 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - explorer.exe (PID: 6668 cmdline: "C:\Windows\explorer.exe" /LOADSAVEDWINDOWS MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.cortesdisenosroutercnc.com/itq4/"
  ],
  "decoy": [
    "worklocalcortland.com",
    "hostydom.tech",
    "ittakegenius.com",
    "clarisfixion.com",
    "totalzerosband.com",
    "shop-for-432.club",
    "exploremytruth.com",
    "skarpaknivar.com",
    "teknikunsur.net",
    "shoppingclick.online",
    "808gang.net",
    "solobookings.com",
    "mikunandina.com",
    "insumedkap.com",
    "kingdomcell.com",
    "qabetalive838475.com",
    "foxyreal.website",
    "filmweltruhr.com",
    "pokibar.com",
    "girassolpresentes.com",
    "rprent.com",
    "klatch22.com",
    "qam3.com",
    "bbuur.com",
    "grandmino.com",
    "windowcontractor.info",
    "myownstack.com",
    "suprebahia.com",
    "amaliebeac.space",
    "rugggedclassicvinyl.com",
    "thevillagetour.com",
    "obsoletely.xyz",
    "fintell.online",
    "mychianfts.net",
    "skillingyousoftly.com",
    "mejicat.com",
    "tntpowerspeedagility.com",
    "richardklewis.store",
    "yourdmvhometeam.com",
    "citestaccnt1631545392.com",
    "weddingbyneus.com",
    "mbkjewelry.com",
    "shubhamsports.com",
    "bountyhub.xyz",
    "heritage.solar",
    "vitalorganicbarsoap.com",
    "cloandjoe.com",
    "royalluxextensions.com",
    "lbrzandvoort.com",
    "knowmust.xyz",
    "okpu.top",
    "balanz.kitchen",
    "buggy4t.com",
    "gownstevensond.com",
    "f4w6.claims",
    "workingfromgarden.com",
    "foryourtinyhuman.com",
    "preventbiotech.com",
    "happyklikshop.com",
    "tuyenxanh.com",
    "lift2.cloud",
    "skazhiraku.net",
    "purpleatticexperiment.com",
    "freebtc.pro"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.649764201.0000000000410000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000C.00000002.649764201.0000000000410000.00000040.80000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000C.00000002.649764201.0000000000410000.00000040.80000000.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ad9:$sqlite3step: 68 34 1C 7B E1 • 0x16bec:$sqlite3step: 68 34 1C 7B E1 • 0x16b08:$sqlite3text: 68 38 2A 90 C5 • 0x16c2d:$sqlite3text: 68 38 2A 90 C5 • 0x16b1b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c43:$sqlite3blob: 68 53 D8 7F 8C
00000003.00000002.385147934.0000000001870000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000003.00000002.385147934.0000000001870000.00000004.00001000.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 28 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.idcqz.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.idcqz.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7808:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7ba2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1261c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9332:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18da7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
4.2.idcqz.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15cd9:$sqlite3step: 68 34 1C 7B E1 • 0x15dec:$sqlite3step: 68 34 1C 7B E1 • 0x15d08:$sqlite3text: 68 38 2A 90 C5 • 0x15e2d:$sqlite3text: 68 38 2A 90 C5 • 0x15d1b:$sqlite3blob: 68 53 D8 7F 8C • 0x15e43:$sqlite3blob: 68 53 D8 7F 8C
4.0.idcqz.exe.400000.8.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
4.0.idcqz.exe.400000.8.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 22 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Networking

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion

Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information

Yara detected FormBook

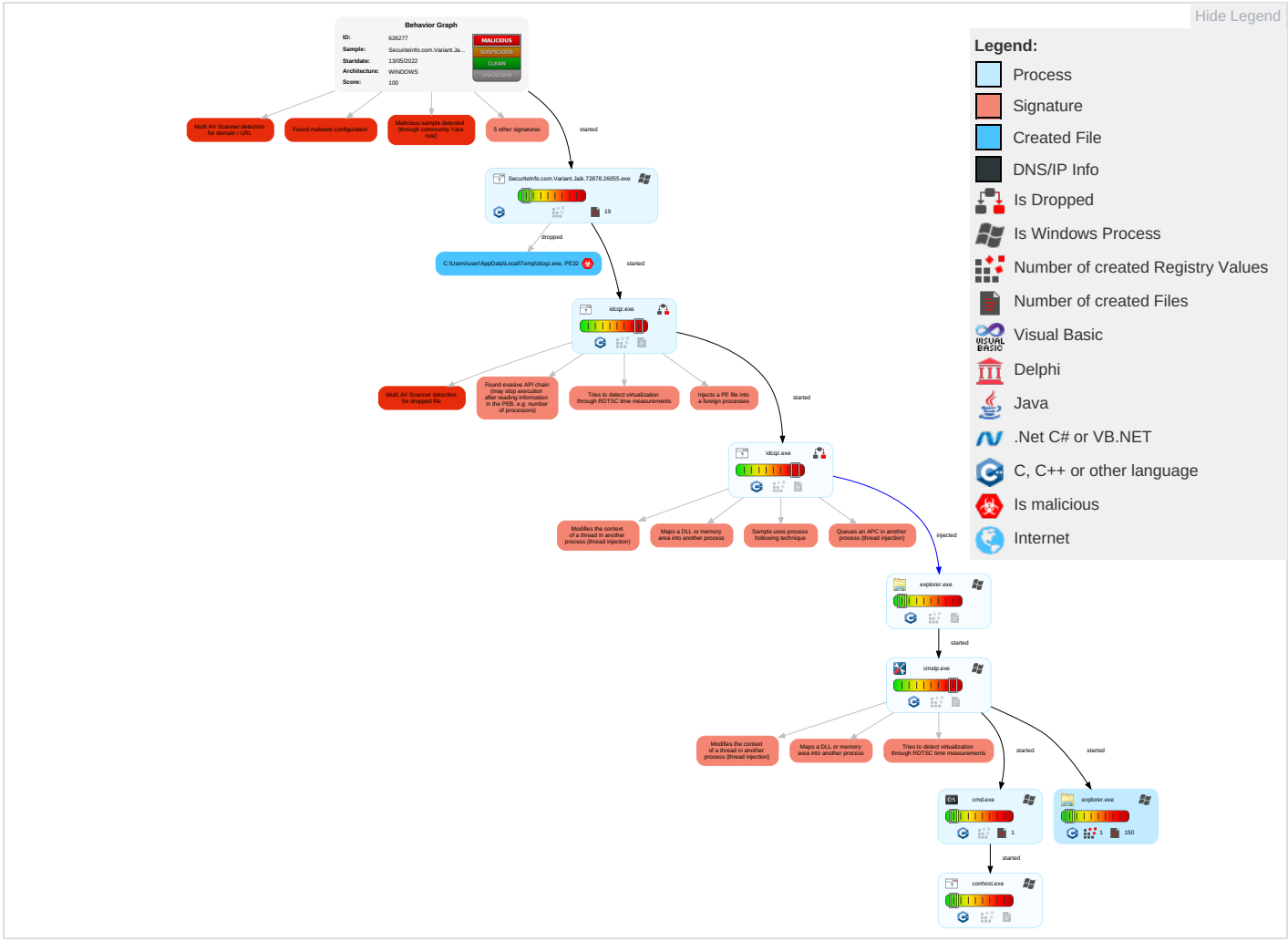
Remote Access Functionality

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 1 Native API	Path Interception	1 Access Token Manipulation	1 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 Shared Modules	Boot or Logon Initialization Scripts	5 1 2 Process Injection	2 Virtualization/Sandbox Evasion	LSASS Memory	1 Query Registry	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Access Token Manipulation	Security Account Manager	2 7 1 Security Software Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	5 1 2 Process Injection	NTDS	2 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	2 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 Obfuscated Files or Information	Cached Domain Credentials	2 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Software Packing	DCSync	1 1 4 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

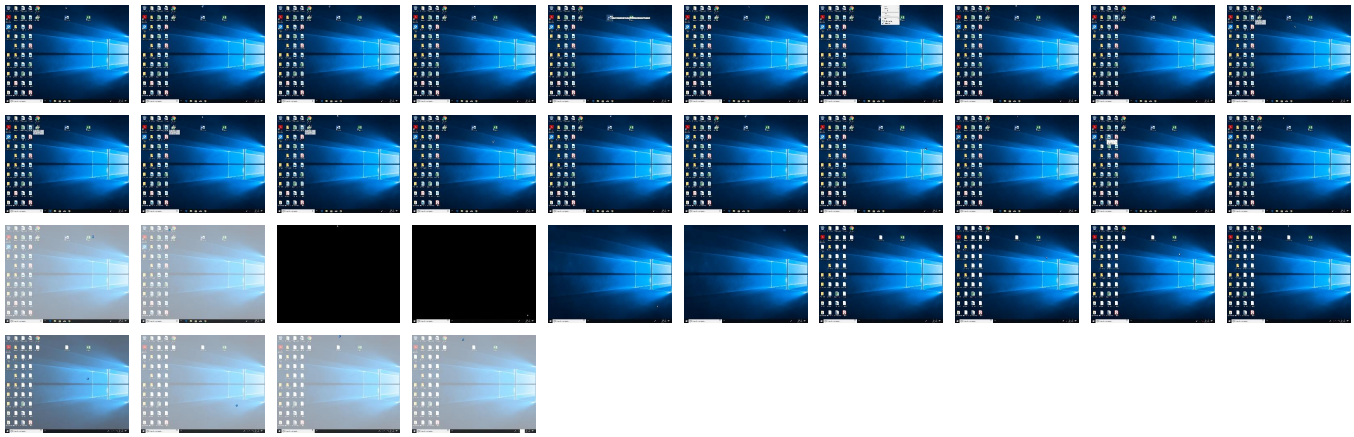
Behavior Graph



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
SecuriteInfo.com.Variant.Jaik.72878.26055.exe	49%	Virustotal		Browse
SecuriteInfo.com.Variant.Jaik.72878.26055.exe	51%	ReversingLabs	Win32.Trojan.FormBook	
SecuriteInfo.com.Variant.Jaik.72878.26055.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\idcqz.exe	15%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\idcqz.exe	22%	ReversingLabs	Win32.Trojan.Pwsx	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.idcqz.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
12.2.cmstp.exe.8b0000.1.unpack	100%	Avira	HEUR/AGEN.1234539		Download File
4.0.idcqz.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
4.2.idcqz.exe.3340000.5.unpack	100%	Avira	HEUR/AGEN.1234539		Download File
3.2.idcqz.exe.1870000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.0.idcqz.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.0.idcqz.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
12.0.cmstp.exe.8b0000.0.unpack	100%	Avira	HEUR/AGEN.1234539		Download File
4.2.idcqz.exe.fa4630.2.unpack	100%	Avira	HEUR/AGEN.1234539		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
www.cortesdisenosroutercnc.com/itq4/	10%	Virustotal		Browse
www.cortesdisenosroutercnc.com/itq4/	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.cortesdisenosroutercnc.com/itq4/	true	• 10%, Virustotal, Browse • Avira URL Cloud: malware	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	SecuriteInfo.com.Variant.Jaik.72878.26055.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626277
Start date and time: 13/05/202219:42:14	2022-05-13 19:42:14 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Variant.Jaik.72878.26055.480 (renamed file extension from 480 to 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:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@10/4@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 47.7% (good quality ratio 45%) • Quality average: 76.8% • Quality standard deviation: 29.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SearchUI.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, ShellExperienceHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, mobsync.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 40.125.122.176, 52.152.110.14, 20.223.24.244, 52.242.101.226
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, e12564.dspb.akamaiedge.net, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtEnumerateKey calls found.
- Report size getting too big, too many NtEnumerateValueKey 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 NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:44:55	API Interceptor	118x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\bn5z71pvulub10vjar

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Jaik.72878.26055.exe
File Type:	data
Category:	dropped
Size (bytes):	167423
Entropy (8bit):	**7.991030598002282**
Encrypted:	**true**
SSDEEP:	3072:z1F74Q5ZD00MiVOYj9zJCzR9WNT6E2CA22/VG6QF574Br1q:z1FkqlVOUlzAZzaVGRGBr1q
MD5:	40FF96237005585BB3469F7844D579EA
SHA1:	CB38299275DA36B767A8EDD8AF4546CF0165B6D6
SHA-256:	81B2280B25F3F4BEF5A87D35291A9D6FD9D57E754FFDE05628663AC65F324257
SHA-512:	52E449F89A8F97696A96C98142D01AC9C34753DECFC24365AB0FBD820E54482C1C61A8A05E69D21D77F32099C831355EB24F5196BF3CCF91CE3A5F4383C6446
Malicious:	false
Reputation:	low
Preview:	....?.V.*...t...c...u.2.. ..l...q.&.m..3...%.....E.~..#...u....x.P..g9..Xq.....pi..@.|.6.}..&...J.7.'...^....K#.....D..tqv...<..AH99y.....bH...]../.e.....U^..t....^.'d....>#....2.O.-..*.K..3N.7. :.Z/d.Q4.,.SZ....[..U`..l'.#....9.A.....g~..C.?.V.h#..e.....-...ha.l.....m..3.....%.....E.~.....VP...Rx:,..T.1...v.?.5.e.F....$.y...z1....JZ...q.....D.....x4....xj.u..Zl....z..l.u...Fl...e. ..R..J?.....'dk.L.....k....-..*.d...TOy.".sd.Q4.,.,....H[.....I.#x.....A.....g0..C.?.V....Ne.....ha.l...q.&.m..3...%.....E.~.....VP...Rx:,..T.1...v.?.5.e.F....$.y...z1....JZ...q.... .D.....x4....xj.u..Zl....z..l.u...Fl...e...R..J?.....^.'d.g....._...O.-..*.d...TOy.:./d.Q4.,.,....H[.....I.#x.....A.....g0..C.?.V....Ne.....ha.l...q.&.m..3...%.....E.~.....VP...Rx:,..T .1...v.?.5.e.F....$.y...z1....JZ...q.....D.....x4....xj.u..Zl....z..l.u...Fl...e...R..J?.....^.'d.g....._...O.-..*.d...TOy.:./d.Q4.,.,....H[.

C:\Users\user\AppData\Local\Temp\dknqrab

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Jaik.72878.26055.exe
File Type:	data
Category:	dropped
Size (bytes):	5418
Entropy (8bit):	6.08058386157834
Encrypted:	false
SSDEEP:	96:v5fm8CsQMHXy2ZcUqP0PkvET4Ua36tHDp22n2CXn23PNYi7JArcUN9zB+v0QUe6S:hfQ03pQvESkHc22823PNMr/99+vh6S
MD5:	05102B10AF50DD080DF138356B05637D
SHA1:	BFB1ABB77EA1CE16E41D207C10FF31D6509558AB
SHA-256:	865D3959F838A6F4D41B9CF369C5863A10CD322A5F0410FD03A577890166D891
SHA-512:	2318CD339F1F65991D59A43E2C30368AA1DBEE674A8149D21DC5E56C8274CFA01AAEEBECC44043E82B6DA804F01DBDB05D4180115FC9073967C1F11CC7416E BE
Malicious:	false
Preview:	.....u..[..k.o[E..'o.`'+e.'o.`'+e.[E..e."...[E...U&.U*.e.j.....e..u..U&.U*.e.j.....e.u..U&.U*.e.j....e..u..U&.U*.e.j....e..u.[]*.p.D..C...e&..e..u..e*[....e.m.e.m....D*y..e..u...e.o..E.[..D..... [.>%..E..U.y.U.t.U....U..y.U.w.U.x..N*...&....f.:[..U..U...t.e.'%.e..E.....>.;...[.>-.E.xw.e.wxs.&.u....'o.`'+e.e...e&K:.e..m*.....u.e.e....m...e.u..&.b..W.L....b.....b`..W.z.....b- v.W.h.....u..[.'"o.`'+e.e.*...e..e.[]..N.e...e...e.e...e.....%...N..e.D.yC...-..n-..e.D.y....-..n-.D.D..C...%.jb`..W.....j.....e..'.e.j.U..d...e.[]..N.[E....e.....e....u..[..'o.`'+e.e."...e..e.[]..N.e. ..e...e.e...e.....'^....e.D.yC...-..n-..e&.D.y....-..n-..e*.D.y...-..n-..e...D.tC...5..f5..e.D.y....-..n-.D%D..C...%.jb..W.....j.....e.[]..N.e.m.../.U..U..U*.U&.U.....e.[]..N.[E....e.....e....u..[.6.e.*...e..e.[]..N.e...e..e.e...e.....N..e.D.yC...-..n-.e&.D.y....-..n-.D.D..C...%.jb-v.W.....j.....e..(.U&.U....

C:\Users\user\AppData\Local\Temp\idcqz.exe

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Jaik.72878.26055.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	80384
Entropy (8bit):	6.294165791913379
Encrypted:	false
SSDEEP:	1536:jugTaC+v1eUfr0oxAomP3cX/4pi2sWjcdQQI:Na5UUD1/ui5QL
MD5:	51F62DEF6DC686B87CC0BAFC31685546
SHA1:	C99222ABD6547D34DED56B44CC5818675D902F07
SHA-256:	9E398BB06FD1CBF54E40BFB36211CBD5C73AF57E652603C9B6A37A70DAB5AF4D
SHA-512:	1D4933E4C6BA61833174819B34F59C266B2CFD5B4DA3ED36DD9C2FB8AC047EF0C76B4DE173432E1451D7CD3A489511EA4223B8941EF5FAED0EB09E7A921CBI 76

Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 15%, Browse • Antivirus: ReversingLabs, Detection: 22%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....w...w...w...%`..w...%^..w...%a.w.....w...w..w..p....w..p.~..w..p... .w..Rich.w.....PE..L....?~b.....7.....@.....@.....$.....p.....T.....@..... .....text...U..... ..`.rdata...N.....P.....@..@.data... 1...0.....@....rsrc.....p.....*.....@..@.reloc.....,..... ..@..B..... .....

C:\Users\user\AppData\Local\Temp\nsrF91A.tmp	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Jaik.72878.26055.exe
File Type:	data
Category:	dropped
Size (bytes):	263211
Entropy (8bit):	7.569144130803792
Encrypted:	false
SSDEEP:	3072:i1F74Q5ZD00MiVOYj9zJCzR9WNT6E2CA22/VG6QF574Br1X7a5UUD1/ui5QL:i1FkqlVOUIzAZzaVGRGBr1QUQU
MD5:	6EFB91B44285F8050C8CBCC272E54FDB
SHA1:	2B6B1160680ACA8809287FE2D055BA30963A04EE
SHA-256:	54719DDAC4D092D918795FD291A01E1F03A203C49AE742D6077D201E2622BFE5
SHA-512:	8AB0FB7A8751E406E164DCB3DE836558D7A9ACD3EC18700BC580535C8EC61B16657C304BDB303D34639847FA8F3510DFA9EFC5F890B53807714C700A8267541
Malicious:	false
Preview:	.&.....,.....O.....(&.....&..... .....G.....j..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.906288840175113
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • 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:	SecuriteInfo.com.Variant.Jaik.72878.26055.exe
File size:	255769
MD5:	029bbe98a216416eb698ca543a5c0830
SHA1:	a24173f1daf45d7444e3c698c3ae09a540a818dd
SHA256:	e73b7de772353638addd480041e90a67f27d8d5b087bf222b1c6649c54b9cc57
SHA512:	684acd7f2302c8deae1fc81ec9e5811588692ba0f8a080fe26a959dbde8159bafd4906684ade4639051abaf563b4438f8bd99b115ab5d668a845a4de9d2830bc
SSDEEP:	6144:LOtlOtWQ/YWOXDYv0RgaJ1LULzHgpZQR7ZnbpEBb7TLwV1Azo:LOLtX/DOEMRgUa8M1cbfLwDj
TLSH:	B8441301AF08C47BDAB34A331D7B54525ABED51A10D44ACB5340A3DEFD663C2EA9F293
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!`G.@...@...@../OQ..@...@..I@../OS..@...c>..@..+F...@..Rich.@.....PE..L.....Oa.....h....:....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x403646
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:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614F9AA9 [Sat Sep 25 21:54:49 2021 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:	61259b55b8912888e90f516ca08dc514

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A230h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080C8h]
mov esi, dword ptr [004080CCh]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007F63D0A9EA0Ah
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007F63D0A9E9DAh
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [007A8B58h], eax
xor eax, eax

Instruction
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3b9000	0xa50	.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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.rdata
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	0x67c4	0x6800	False	0.675180288462	data	6.49518266675	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.4498046875	data	5.14106681717	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x39ebb8	0x600	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x3a9000	0x10000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x3b9000	0xa50	0xc00	False	0.401692708333	data	4.18753619353	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3b9190	0x2e8	data	English	United States
RT_DIALOG	0x3b9478	0x100	data	English	United States
RT_DIALOG	0x3b9578	0x11c	data	English	United States
RT_DIALOG	0x3b9698	0x60	data	English	United States
RT_GROUP_ICON	0x3b96f8	0x14	data	English	United States
RT_MANIFEST	0x3b9710	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, CreateFileW, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Possible Origin

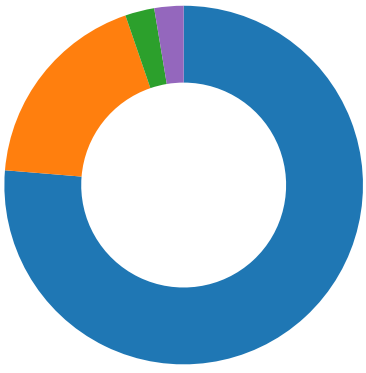
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior



- SecuriteInfo.com.Variant.Jaik.7287…
- idcqz.exe
- idcqz.exe
- explorer.exe
- cmstp.exe
- cmd.exe
- conhost.exe
- explorer.exe

Click to jump to process

System Behavior

Analysis Process: SecuriteInfo.com.Variant.Jaik.72878.26055.exe PID: 7156, Parent PID: 5048

General

Target ID:	0
Start time:	19:43:29
Start date:	13/05/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Jaik.72878.26055.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.Variant.Jaik.72878.26055.exe"
Imagebase:	0x400000
File size:	255769 bytes
MD5 hash:	029BBE98A216416EB698CA543A5C0830
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: idcqz.exe PID: 5444, Parent PID: 7156

General

Target ID:	3
Start time:	19:43:30
Start date:	13/05/2022
Path:	C:\Users\user\AppData\Local\Temp\idcqz.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\idcqz.exe C:\Users\user\AppData\Local\Temp\dknqrab
Imagebase:	0xa70000
File size:	80384 bytes
MD5 hash:	51F62DEF6DC686B87CC0BAFC31685546
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.385147934.0000000001870000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.385147934.0000000001870000.00000004.00001000.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.385147934.0000000001870000.00000004.00001000.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 15%, Virustotal, Browse • Detection: 22%, ReversingLabs
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\dknqrab	unknown	4096	success or wait	1	A72C9C	ReadFile
C:\Users\user\AppData\Local\Temp\dknqrab	unknown	4096	success or wait	1	A72C9C	ReadFile
C:\Users\user\AppData\Local\Temp\bn5z71pvulub10vjar	unknown	167423	success or wait	1	1860A1E	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	186051C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	186051C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	186051C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	186051C	ReadFile

Analysis Process: idcqz.exe PID: **5408**, Parent PID: **5444**

General

Target ID:	4
Start time:	19:43:32
Start date:	13/05/2022
Path:	C:\Users\user\AppData\Local\Temp\idcqz.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\idcqz.exe C:\Users\user\AppData\Local\Temp\dknqrab
Imagebase:	0xa70000
File size:	80384 bytes
MD5 hash:	51F62DEF6DC686B87CC0BAFC31685546
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: 00000004.00000002.465827211.0000000001450000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.465827211.0000000001450000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.465827211.0000000001450000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.383459730.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.383459730.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.383459730.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.465393336.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.465393336.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.465393336.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.382002117.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.382002117.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.382002117.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.467817917.00000000017B0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.467817917.00000000017B0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.467817917.00000000017B0000.00000040.10000000.00040000.00000000.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	4186D7	NtReadFile

Analysis Process: explorer.exe PID: **3688**, Parent PID: **5408**

General

Target ID:	7
Start time:	19:43:37
Start date:	13/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff77c400000
File size:	3933184 bytes

MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
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: 00000007.00000000.453411186.000000000F07E000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.453411186.000000000F07E000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.453411186.000000000F07E000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.429389252.000000000F07E000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.429389252.000000000F07E000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.429389252.000000000F07E000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

Analysis Process: cmstp.exe PID: **6488**, Parent PID: **3688**

General

Target ID:	12
Start time:	19:44:09
Start date:	13/05/2022
Path:	C:\Windows\SysWOW64\cmstp.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmstp.exe
Imagebase:	0x8b0000
File size:	82944 bytes
MD5 hash:	4833E65ED211C7F118D4A11E6FB58A09
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: 0000000C.00000002.649764201.0000000000410000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.649764201.0000000000410000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.649764201.0000000000410000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.650352103.00000000006B0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.650352103.00000000006B0000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.650352103.00000000006B0000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.650320550.0000000000680000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.650320550.0000000000680000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.650320550.0000000000680000.00000040.10000000.00040000.00000000.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	4286D7	NtReadFile

Analysis Process: cmd.exe PID: **3252**, Parent PID: **6488**

General

Target ID:	14

Start time:	19:44:14
Start date:	13/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\AppData\Local\Temp\idcqz.exe"
Imagebase:	0xed0000
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **6920**, Parent PID: **3252**

General

Target ID:	15
Start time:	19:44:15
Start date:	13/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: explorer.exe PID: **6668**, Parent PID: **5380**

General

Target ID:	23
Start time:	19:44:54
Start date:	13/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\explorer.exe" /LOADSAVEDWINDOWS
Imagebase:	0x7ff77c400000
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly