ID: 339452
Sample Name: Incaseformat
Cookbook: default.jbs
Time: 04:19:24
Date: 14/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

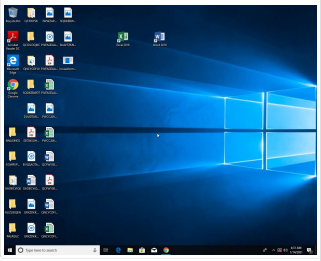
Analysis Report Incaseformat

Overview

General Information

Sample Name:	Incaseformat (renamed file extension from none to exe)
Analysis ID:	339452
MD5:	1ea8bea4055adc..
SHA1:	300b32ae0a70e8..
SHA256:	3c8c16428fe5b2d..

Most interesting Screenshot:



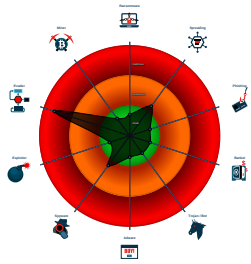
Detection

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

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Detected unpacking (changes PE se…
- Detected unpacking (creates a PE fi…
- Detected unpacking (overwrites its o…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Creates an undocumented autostart …
- Drops executable to a common third…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Antivirus or Machine Learning detec…
- Contains functionality to check if a d…

Classification



Startup

- **System is w10x64**
- Incaseformat.exe (PID: 3504 cmdline: 'C:\Users\user\Desktop\Incaseformat.exe' MD5: 1EA8BEA4055ADC9EDF91E03B0C80E68A)
- lvrslql.exe (PID: 5264 cmdline: C:\PROGRA~3\Mozilla\lvrslql.exe -ddeznal MD5: 0174F8B5E7DD2E44B57EBBE3742B216F)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

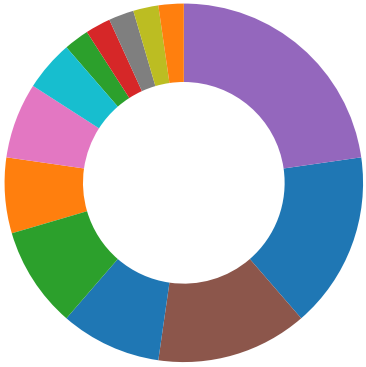
Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Compliance
- Spreading
- Key, Mouse, Clipboard, Microphone and Screen Capturing

Copyright null 2021



- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- 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

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Compliance:

Detected unpacking (creates a PE file in dynamic memory)

Detected unpacking (overwrites its own PE header)

Data Obfuscation:

Detected unpacking (changes PE section rights)

Detected unpacking (creates a PE file in dynamic memory)

Detected unpacking (overwrites its own PE header)

Persistence and Installation Behavior:

Drops executable to a common third party application directory

Boot Survival:

Creates an undocumented autostart registry key

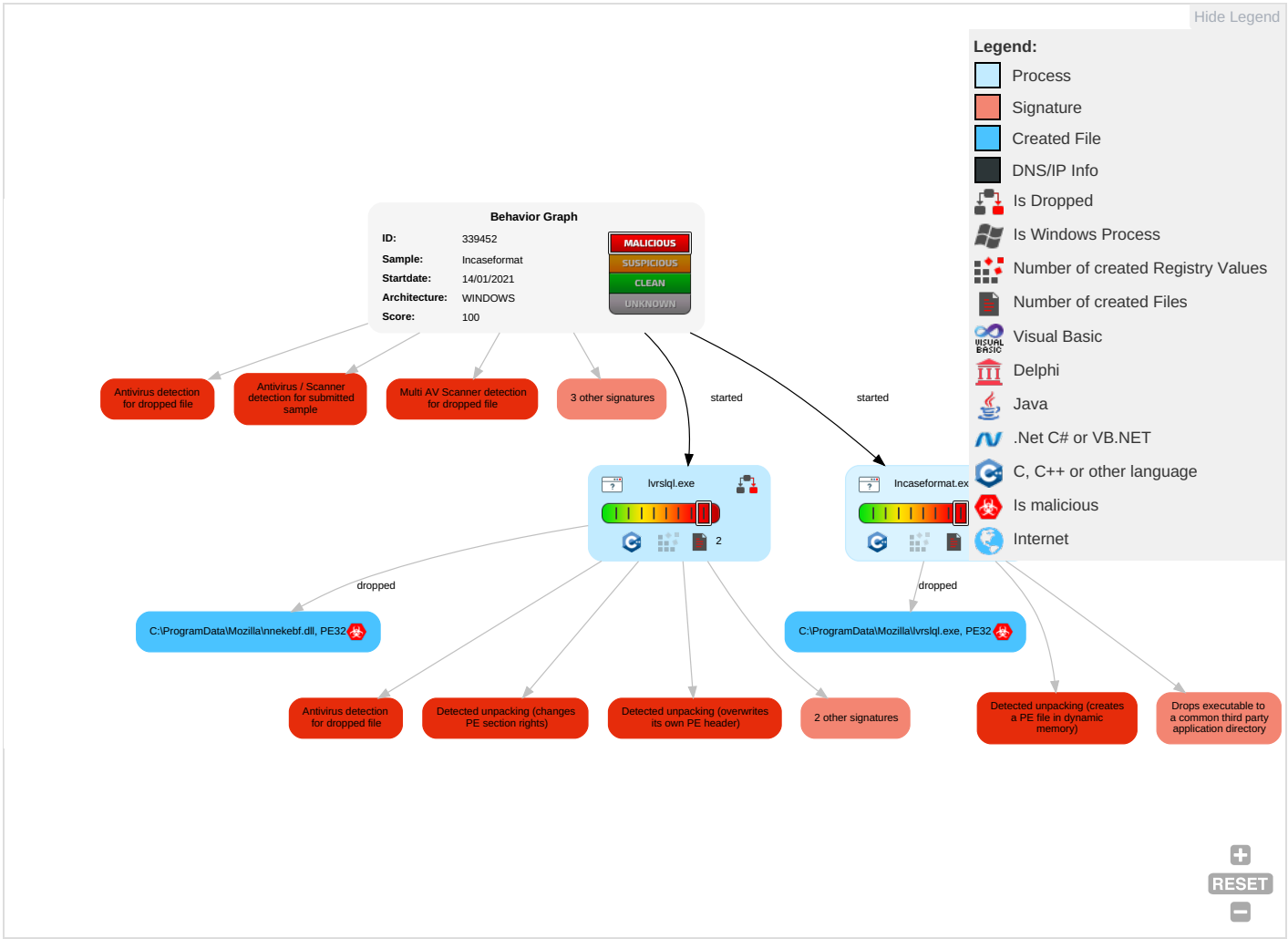
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Exploitation for Privilege Escalation 1	Masquerading 1	Input Capture 1	System Time Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Default Accounts	Native API 2	Registry Run Keys / Startup Folder 1	Process Injection 1	Process Injection 1	LSASS Memory	Security Software Discovery 1 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization

Copyright null 2021

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Obfuscated Files or Information 2	Security Account Manager	Account Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Registry Run Keys / Startup Folder 1	Software Packing 3 3	NTDS	System Owner/User Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	System Information Discovery 4	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.


No bigger version


Recycle Bin
QCFWYSK
NVWZAP...
SQSJKEBW...
Acrobat Reader DC
QCOILOQIKC
PIVFAGEAA...
SUAVTZKN...
Excel 2016
Word 2016
Microsoft Edge
QNCYCDFIJJ
PIVFAGEAA...
Incaseform...
Google Chrome
SQSJKEBWDT
PIVFAGEAA...
DUUDTUB...
PWCCAW...
BNAGMGS
EEGWXUH...
PWCCAW...
EOWRVP...
EIVQSAOTA...
QCFWYSK...
GAOBCVIQJ
GAOBCVIQ...
QCFWYSK...
KLIZUSIQEN
GRXZDKK...
QNCYCDFI...
PALRGUC
GRXZDKK...
QNCYCDFI...
Type here to search
4:31 AM
1/14/2021

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Incaseformat.exe	83%	Virustotal		Browse
Incaseformat.exe	100%	ReversingLabs	Win32.Dropper.GepSys	
Incaseformat.exe	100%	Avira	TR/Dropper.Gen	
Incaseformat.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\ProgramData\Mozilla\lvrslql.exe	100%	Avira	TR/Dropper.Gen	
C:\ProgramData\Mozilla\nnekebf.dll	100%	Avira	TR/ATRAPS.Gen4	
C:\ProgramData\Mozilla\lvrslql.exe	100%	Joe Sandbox ML		
C:\ProgramData\Mozilla\nnekebf.dll	100%	Joe Sandbox ML		
C:\ProgramData\Mozilla\nnekebf.dll	76%	Virustotal		Browse
C:\ProgramData\Mozilla\nnekebf.dll	55%	Metadefender		Browse
C:\ProgramData\Mozilla\nnekebf.dll	84%	ReversingLabs	Win32.Trojan.Zeus	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.Incaseformat.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
0.2.Incaseformat.exe.400000.0.unpack	100%	Avira	TR/Gepys.aouma		Download File
1.2.lvrslql.exe.df0000.1.unpack	100%	Avira	TR/Gepys.aouma		Download File
0.2.Incaseformat.exe.2150000.1.unpack	100%	Avira	TR/Gepys.aouma		Download File
1.0.lvrslql.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
1.2.lvrslql.exe.400000.0.unpack	100%	Avira	TR/Gepys.aouma		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339452
Start date:	14.01.2021
Start time:	04:19:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 11s
Hypervisor based Inspection enabled:	false

Copyright null 2021

Report type:	light
Sample file name:	Incaseformat (renamed file extension from none 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:	39
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.evad.winEXE@2/2@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 31% (good quality ratio 28.6%) • Quality average: 80.4% • Quality standard deviation: 29.8%
HCA Information:	• Successful, ratio: 52% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Max analysis timeout: 720s exceeded, the analysis took too long • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, MusNotifyIcon.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe

Simulations

Behavior and APIs

Time	Type	Description
04:20:19	Task Scheduler	Run new task: uihuovc path: C:\PROGRA~3\Mozilla\lvrslql.exe s>-ddeznal

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Mozilla\lvrslql.exe	
Process:	C:\Users\user\Desktop\Incaseformat.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	386118
Entropy (8bit):	7.757548173569129
Encrypted:	false
SSDEEP:	6144:flzoa7yNgAIQo8OLamr3RLzRnHhq92gkqnC2v7LA+Fq3PTzhVaY:ftB7yNgD83m3fE92TqC25sPPKY
MD5:	0174F8B5E7DD2E44B57EBBE3742B216F
SHA1:	182A5FA3FA20939D1646A8BB2D5D99D358AB0C67
SHA-256:	E2830DBE2A0C182413532707C4A1D0005BF77F5A4275D743C40DBC5CD257AD01
SHA-512:	D094657C9FD11DC9D4E909AFB0E8C7A1F21038189D49EBD4C749E9FE508DBDEE76BC68A6C478B38CCE8F5C13FB76CE0CB7E3CC5924507C8FADAA003A6982 2D
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....=..S..S..S..v(..S..R..S.1.A..S..S..S.....S....S.....S.Rich.S..... PE..L..."..Q.....@.....d.....text...F... ....`.rdata.....@..@.data.....@....rsrc.....@..@..... ....

C:\ProgramData\Mozilla\nnekebf.dll	
Process:	C:\ProgramData\Mozilla\lvrslql.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	23040
Entropy (8bit):	6.549949874024087
Encrypted:	false
SSDEEP:	384:ucR0NobYoT7lP/uy4rKTFBYFk64owOCjxXfr6ftakRl:ue0OHlz4EVhTPjxXz6T
MD5:	186E739497337C4C3084CE81279271D4
SHA1:	2A31C24432B259926A7E5E33F7EB8C9AE57A517B
SHA-256:	33F74F3530AF748C84DDDE066BF29E347BDA982FE81C742773951B1FF286CC0B
SHA-512:	B9AAC441ECD2055BE2A2407299243357BD6A28A39309D5FF7463EAAAD46FC8A565C35379C7CCFD0579EC0EFB3DF7A16D1E46D595D9F380995B7F327D95B29E 4
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 76%, Browse • Antivirus: Metadefender, Detection: 55%, Browse • Antivirus: ReversingLabs, Detection: 84%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....=..S..S..S..v(..S..R..S.1.A..S.....S..S..S.....S.....S.Rich.S..... PE..L...!..Q.....!.....D.....`.....`.....`..d.....`.....t ext...XC.....D..... ..`.rdata.....`.....H.....@..@.data...L....p.....L.....@....rsrc.....N.....@..@.reloc.....V.....@..B..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.75753941681381

General

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:	Incaseformat.exe
File size:	386110
MD5:	1ea8bea4055adc9edf91e03b0c80e68a
SHA1:	300b32ae0a70e86eecbccc2b850d783ded5a0f69
SHA256:	3c8c16428fe5b2d67ed59d543805e5ec63b3565f05305cbc193c961107e56f1d
SHA512:	28e9af00495f838562d8ee67ab3521baea93f8b0360505cd0cbd40b40ad14b7e365ae7c71599fe5d05c539c106323021890a16c97c19770fda1bb5a01131b0bf
SSDEEP:	6144:flzoa7yNgAIQo8OLamr3RLzRnHhq92gkqnC2v7LA+Fq3PTzhVap:ftB7yNgD83m3fE92TqC25sPPKp
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....=...S...S...S..v(...S...R...S.1.A...S...S...S.....S.....S.....S.Rich.S.....PE..L..."..Q.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x42c0f0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x51829C22 [Thu May 2 17:02:26 2013 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	b40c457657c59e9d515f1130618a2f1e

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 50h
lea eax, dword ptr [ebp-50h]
push eax
call dword ptr [0042D034h]
push 0000019Ch
push 00000000h
call dword ptr [0042D070h]
test eax, eax
je 00007F4F08AE7696h
xor eax, eax
jmp 00007F4F08AE76E9h
push 00007F00h
push 00000000h

Instruction
call dword ptr [0042D070h]
test eax, eax
jne 00007F4F08AE7696h
xor eax, eax
jmp 00007F4F08AE76D4h
push ebp
mov eax, eax
mov eax, eax
mov eax, eax
mov eax, eax
mov eax, eax
mov eax, eax
mov eax, eax
mov eax, eax
mov eax, eax
mov eax, eax
mov eax, eax
mov eax, eax
mov eax, eax
mov eax, eax
mov eax, eax
mov eax, eax
mov eax, eax
mov eax, eax
mov eax, eax
mov eax, eax
mov eax, eax
mov eax, eax
mov eax, eax
mov eax, eax
mov eax, eax
mov eax, eax
mov eax, eax
mov eax, eax
mov eax, eax
call 00007F4F08AE7089h
mov esp, ebp
pop ebp
ret
push ebp
mov ebp, esp
sub esp, 0000021Ch
mov eax, dword ptr [ebp+08h]
mov dword ptr [ebp-0000020Ch], eax
mov ecx, dword ptr [ebp+0Ch]
mov dword ptr [ebp-0000021Ch], ecx
mov dword ptr [ebp-00000218h], 00000005h
mov dword ptr [ebp-00000210h], 0042E0E0h
mov edx, dword ptr [ebp-0000020Ch]
cmp edx, dword ptr [ebp-0000021Ch]
jnc 00007F4F08AE76A6h
mov dword ptr [ebp-00000218h], 00000005h

Rich Headers

Programming Language:	[IMP] VS2005 build 50727 [RES] VS2008 build 21022 [LNK] VS2008 build 21022 [C] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2d094	0x64	.rdata

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2f000	0x790	.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	0x2d000	0x94	.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	0x2b346	0x2b400	False	0.853814803107	data	7.66572568976	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x2d000	0x3b4	0x400	False	0.5078125	data	4.79024068833	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x2e000	0x118	0x200	False	0.263671875	data	2.00112152127	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2f000	0x2b790	0x800	False	0.3037109375	data	2.76533518439	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x2f0d0	0x188	Alpha compressed COFF	Russian	Russia
None	0x2f268	0x526	PC bitmap, Windows 3.x format, 160 x 15 x 4	Russian	Russia
None	0x2f258	0xb	PGP Secret Sub-key (v4) - 0b created on Tue Jul 14 05:20:16 1970 - unknown (pub 0) Plaintext or unencrypted data	Russian	Russia

Imports

DLL	Import
KERNEL32.dll	ReadFile, CreateFileA, GetTickCount, GetModuleHandleA, GetCommandLineA, GetProcAddress, GetStartupInfoA, ExitProcess
USER32.dll	GetSystemMetrics, LoadBitmapA, GetMessageA, LoadIconA, LoadMenuA, PostQuitMessage, RegisterClassExA, ReleaseDC, SetMenu, ShowWindow, TranslateMessage, UpdateWindow, LoadIconW, GetDC, EndPaint, DispatchMessageA, DefWindowProcA, CreateWindowExA, BeginPaint, LoadCursorA
GDI32.dll	SelectObject, DeleteDC, CreateCompatibleDC, BitBlt
ADVAPI32.dll	RegOpenKeyA

Version Infos

Description	Data
FileDescription	
CompanyName	
Translation	0x0419 0x04b0

Possible Origin

Language of compilation system	Country where language is spoken	Map
Russian	Russia	

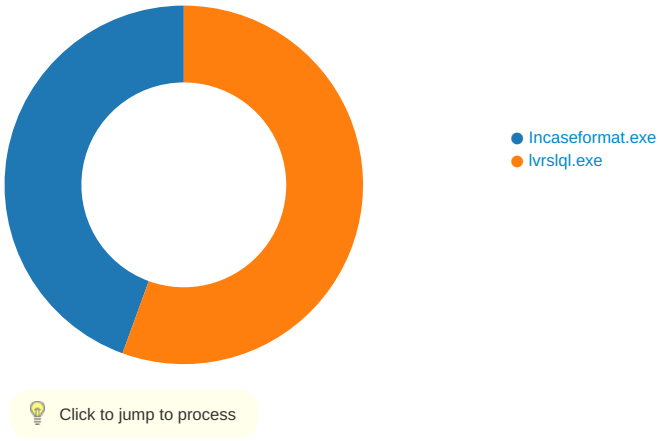
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Incaseformat.exe PID: 3504 Parent PID: 5656

General

Start time:	04:20:13
Start date:	14/01/2021
Path:	C:\Users\user\Desktop\Incaseformat.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Incaseformat.exe'
Imagebase:	0x400000
File size:	386110 bytes
MD5 hash:	1EA8BEA4055ADC9EDF91E03B0C80E68A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Mozilla\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	402401	CreateDirectoryW
C:\PROGRA~3\Mozilla\lvrslql.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	401FB7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Mozilla\lvrslql.exe	unknown	386118	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 89 d1 3d d0 cd b0 53 83 cd b0 53 83 cd b0 53 83 ea 76 28 83 c4 b0 53 83 cd b0 52 83 ec b0 53 83 31 90 41 83 cc b0 53 83 cd b0 53 83 cc b0 53 83 d3 e2 d0 83 cc b0 53 83 d3 e2 c7 83 cc b0 53 83 d3 e2 c2 83 cc b0 53 83 52 69 63 68 cd b0 53 83 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 22 9c 82 51 00 00 00 00 00 00 00 00 e0 00 03 01 0b 01 09 00 00 b4 02 00 00 0e 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.........=...S...S...S..v(... S...R...S.1.A...S...S...S..... ..S.......S.......S.Rich..S... ......PE..L...\"..Q...........	success or wait	1	40209F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Incaseformat.exe	unknown	386110	success or wait	1	401F1B	ReadFile

Analysis Process: lvrslql.exe PID: 5264 Parent PID: 528

General

Start time:	04:20:18
Start date:	14/01/2021
Path:	C:\ProgramData\Mozilla\lvrslql.exe
Wow64 process (32bit):	true
Commandline:	C:\PROGRA~3\Mozilla\lvrslql.exe -ddeznal
Imagebase:	0x400000
File size:	386118 bytes
MD5 hash:	0174F8B5E7DD2E44B57EBBE3742B216F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Mozilla\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	402401	CreateDirectoryW
C:\PROGRA~3\Mozilla\nnekebf.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4014D1	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Mozilla\nnekebf.dll	unknown	23040	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 89 d1 3d d0 cd b0 53 83 cd b0 53 83 cd b0 53 83 ea 76 28 83 c4 b0 53 83 cd b0 52 83 ec b0 53 83 31 90 41 83 cc b0 53 83 d3 e2 d0 83 cc b0 53 83 cd b0 53 83 cc b0 53 83 d3 e2 c7 83 cc b0 53 83 d3 e2 c2 83 cc b0 53 83 52 69 63 68 cd b0 53 83 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 21 9c 82 51 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 09 00 00 44 00 00 00 12 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....=...S...S...S..v(... S...R...S.1.A...S.....S...S. ..S.....S.....S.Rich..S... ......PE..L...!..Q.....! .....D.....	success or wait	1	4014EE	WriteFile

Registry Activities

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Windows	AppInit_DLLs	unicode		C:\PROGRA~3\Mozilla\nnekebf.dll	success or wait	1	401413	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Windows	LoadAppInit_DLLs	dword	0	1	success or wait	1	401433	RegSetValueExW

Disassembly

Code Analysis