ID: 482227
Sample Name: eb70000.dll
Cookbook: default.jbs
Time: 15:02:46
Date: 13/09/2021
Version: 33.0.0 White Diamond

Table of Contents

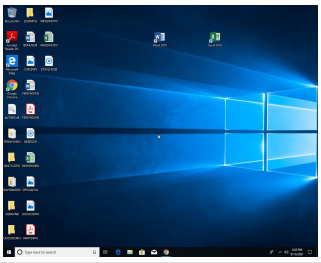
Windows Analysis Report eb70000.dll

Overview

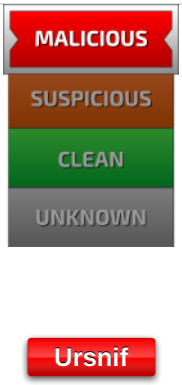
General Information

Sample Name:	eb70000.dll
Analysis ID:	482227
MD5:	9ba0a5c4d18333..
SHA1:	453b87bb4014df0.
SHA256:	1ea68b94b55aab..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



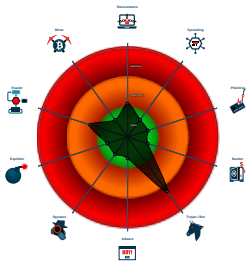
Ursnif

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Found malware configuration
- Yara detected Ursnif
- PE file does not import any functions
- Tries to load missing DLLs
- Program does not show much activi…
- Creates a process in suspended mo…
- Checks if the current process is bein…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 5764 cmdline: loaddll64.exe 'C:\Users\user\Desktop\eb70000.dll' MD5: A84133CCB118CF35D49A423CD836D0EF)
  - cmd.exe (PID: 3324 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\eb70000.dll',#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 5600 cmdline: rundll32.exe 'C:\Users\user\Desktop\eb70000.dll',#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6040 cmdline: rundll32.exe C:\Users\user\Desktop\eb70000.dll,#1 MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "RSA Public Key":
"IAZ1zSJ38XVO1Dw8H0aujdSn7vlA7+ZcfD37AAPhGBwxHfljiWFzy/k/JsiLQibgTFoRNYR0WicFP9oKT10dWk3vlFdDCgh6WbcCOrRnKCiGetdT32V7hiEb2Y2ASaCB+MOiO4CORC2a4Y0DzkToBON/xdWf8i0d0JAA4RDvGSLkccMQ
KtPjl5Uzec2vvxTerDsrfVA/n1vguo9nj9ViSeEtzUdiinf4UKBAit3GBDA77QYvMJljeCu6NuSNPN5bb87iygT/5x/ExMqtsnwUnL65cMos70g6xDPQGfQWuVBJMUHMwBIIKn5DVdSpeVkTs2cGy/RBUet/N6d4xUrvU0AdovS/dRY0E
0Ee0Eenz4s=",
  "c2_domain": [
    "art.microsoftsofymicrosoftsoft.at",
    "apr.intoolkom.at",
    "r23cirt55ysvtdvl.onion",
    "gta5.fifatalk.at",
    "pop.biopiof.at",
    "l46t3vgvmtx5wxe6.onion",
    "v10.avyanok.com",
    "free.monotreener.com",
    "sam.fafona.at"
  ],
  "ip_check_url": [
    "curlmyip.net",
    "ident.me",
    "l2.io/ip",
    "whatismyip.akamai.com"
  ],
  "serpent_key": "rQH4gusjF0tL2dQz",
  "server": "580",
  "sleep_time": "5",
  "SetWaitableTimer_value(CRC_CONFIGTIMEOUT)": "600",
  "time_value": "600",
  "SetWaitableTimer_value(CRC_TASKTIMEOUT)": "240",
  "SetWaitableTimer_value(CRC_SENDTIMEOUT)": "300",
  "SetWaitableTimer_value(CRC_KNOCKERTIMEOUT)": "240",
  "not_use(CRC_BCTIMEOUT)": "10",
  "botnet": "2500",
  "SetWaitableTimer_value": "60"
}
```


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
eb70000.dll	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Found malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Stealing of Sensitive Information:

Yara detected Ursnif

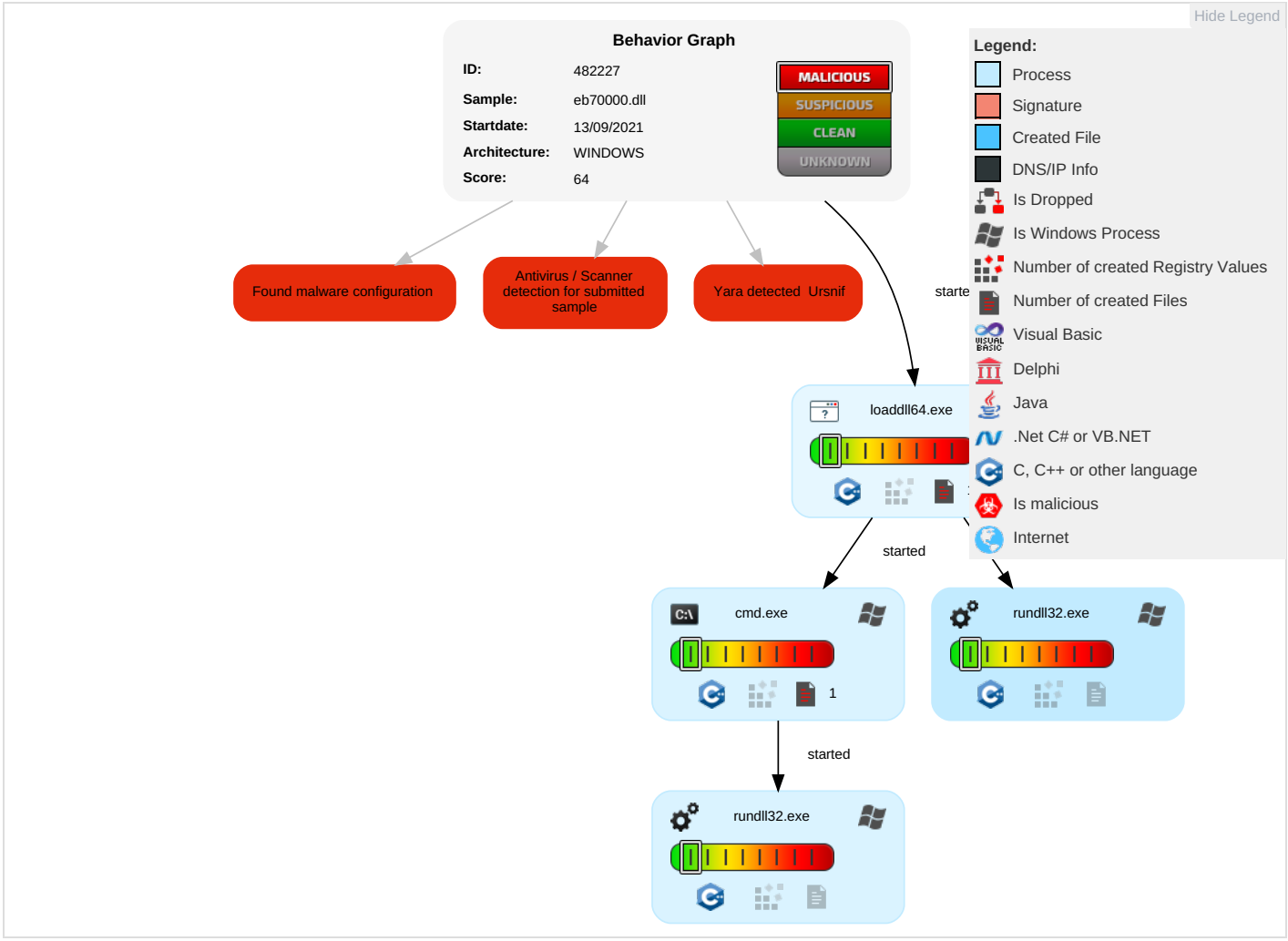
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	DLL Side-Loading 1	Process Injection 1 1	Virtualization/Sandbox Evasion 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Rundll32 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1	Security Account Manager	System Information Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	DLL Side-Loading 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap

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
eb70000.dll	100%	Avira	HEUR/AGEN.1108168	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

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:	33.0.0 White Diamond
Analysis ID:	482227
Start date:	13.09.2021
Start time:	15:02:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	eb70000.dll
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:	4
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:	mal64.troj.winDLL@7/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll • Stop behavior analysis, all processes terminated
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	MS-DOS executable
Entropy (8bit):	6.444528625389228
TrID:	• Win64 Dynamic Link Library (generic) (102004/3) 84.88% • Win64 Executable (generic) (12005/4) 9.99% • DOS Executable Borland Pascal 7.0x (2037/25) 1.69% • Generic Win/DOS Executable (2004/3) 1.67% • DOS Executable Generic (2002/1) 1.67%
File name:	eb70000.dll
File size:	247808
MD5:	9ba0a5c4d18333344e8063c003d3a514
SHA1:	453b87bb4014df0619d9014a9cc0ef97965fa82e
SHA256:	1ea68b94b55aabf5b922923b8ab7e44af4dda2b0a6af1d8 37904468269192e8c
SHA512:	66a9ad56f394e48118269eff00f0530478dc59b8eb9d3d4f 66ab3b09d4d0a66358d4f8dc9bf91d4b37c700478653b8 ac41d86212ca7c04f10505aaed54a36ea
SSDEEP:	6144:tmnZO0GDlypHAT/cxkDyPFXkfh+3m33c5TWjak4 S2S83x:tMZOrEpHAT/cLPF0Im3s5TWjaCb8
File Content Preview:	MZ..... ....PE..d..

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x18002acf4
Entrypoint Section:	.text
Digitally signed:	false

General

Imagebase:	0x180000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, DLL, LARGE_ADDRESS_AWARE
DLL Characteristics:	
Time Stamp:	0x61126E40 [Tue Aug 10 12:17:04 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:	

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2fbbc	0x2fc00	False	0.579500368128	zlib compressed data	6.39419710487	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x31000	0x6837	0x6a00	False	0.372457252358	data	5.25962089647	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x38000	0x1e40	0x1800	False	0.3359375	lif file	3.97256092254	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x3a000	0x1908	0x1a00	False	0.527644230769	data	5.34903211258	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bss	0x3c000	0x1f50	0x2000	False	0.964111328125	data	7.89630830869	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x3e000	0x1000	0xc00	False	0.533528645833	data	4.90522921984	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll64.exe PID: 5764 Parent PID: 3540

General

Start time:	15:03:41
Start date:	13/09/2021
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe 'C:\Users\user\Desktop\eb70000.dll'
Imagebase:	0x7ff7d4800000
File size:	140288 bytes
MD5 hash:	A84133CCB118CF35D49A423CD836D0EF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 3324 Parent PID: 5764

General

Start time:	15:03:42
Start date:	13/09/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\eb70000.dll',#1
Imagebase:	0x7ff7180e0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 6040 Parent PID: 5764

General

Start time:	15:03:42
Start date:	13/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\eb70000.dll,#1
Imagebase:	0x7ff7f82a0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 5600 Parent PID: 3324

General

Start time:	15:03:42
Start date:	13/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe 'C:\Users\user\Desktop\eb70000.dll',#1
Imagebase:	0x7ff7f82a0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Disassembly

Code Analysis