MALICIOUS

Classifications: Spyware

Threat Names: AgentTesla AgentTesla.v3

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe**
ID	#4023226
MD5	189ad2733ba3c8baa0d9fb41e4223d92
SHA1	90d2762579dfd97d7b767662566f3a623766dd0a
SHA256	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b
File Size	434.50 KB
Report Created	2022-04-07 20:10 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (21 rules, 66 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	2	Spyware
	• Rule "AgentTesla_HTML_Message" from ruleset "Malware" has matched on layer 4 network traffic to IP "207.148.117.199:587". • Rule "AgentTesla_StringDecryption_v3" from ruleset "Malware" has matched on a memory dump for (process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe.			
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: Ipswitch WS_FTP, Internet Download Manager, Cyberfox, IncrediMail, SeaMonkey, Pocomail, FileZilla... ..., FTP Navigator, Opera Mail, Postbox, CoreFTP, BlackHawk, Internet Explorer / Edge, TigerVNC, Comodo IceDragon, Microsoft Outlook.			
2/5	Data Collection	Reads sensitive browser data	9	-
	• (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to read sensitive data of web browser "Opera" by file. • (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to read sensitive data of web browser "BlackHawk" by file. • (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to read sensitive data of web browser "k-Meleon" by file. • (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to read sensitive data of web browser "Cyberfox" by file. • (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to read sensitive data of web browser "Mozilla Firefox" by file. • (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file. • (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to read sensitive data of web browser "Comodo IceDragon" by file. • (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to read sensitive data of web browser "Flock" by file. • (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to read credentials of web browser "Internet Explorer" by reading from the system's credential vault.		
2/5	Data Collection	Reads sensitive application data	6	-
	• (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to read sensitive data of application "SeaMonkey" by file. • (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to read sensitive data of application "Internet Download Manager" by registry. • (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to read sensitive data of application "OpenVPN" by registry. • (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to read sensitive data of application "WinSCP" by registry. • (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to read sensitive data of application "TightVNC" by registry. • (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to read sensitive data of application "TigerVNC" by registry.		
2/5	Data Collection	Reads sensitive ftp data	4	-
	• (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to read sensitive data of ftp application "CoreFTP" by registry. • (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to read sensitive data of ftp application "FTP Navigator" by file. • (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to read sensitive data of ftp application "Ipswitch WS_FTP" by file. • (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to read sensitive data of ftp application "FileZilla" by file.		
2/5	Data Collection	Reads sensitive mail data	7	-
	• (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to read sensitive data of mail application "Mozilla Thunderbird" by file. • (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to read sensitive data of mail application "Postbox" by file. • (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to read sensitive data of mail application "Microsoft Outlook" by registry. • (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to read sensitive data of mail application "Pocomail" by file. • (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to read sensitive data of mail application "IncrediMail" by registry. • (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to read sensitive data of mail application "The Bat!" by file. • (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to read sensitive data of mail application "Opera Mail" by file.		
2/5	Discovery	Queries OS version via WMI	1	-

Score	Category	Operation	Count	Classification
	• (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe queries OS version via WMI.			
2/5	Discovery	Executes WMI query	2	-
	• (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe executes WMI query: select * from Win32_OperatingSystem. • (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe executes WMI query: SELECT * FROM Win32_Processor.			
2/5	Discovery	Collects hardware properties	1	-
	• (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe queries hardware properties via WMI.			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	1	-
	• (Process #1) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe modifies memory of (process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
	• (Process #1) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe alters context of (process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe.			
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #1) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe starts (process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe with a hidden window.			
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #1) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe reads from (process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.			
1/5	Privilege Escalation	Enables process privilege	1	-
	• (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe enables process privilege "SeDebugPrivilege".			
1/5	Discovery	Possibly does reconnaissance	22	-

Score	Category	Operation	Count	Classification
		• (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to gather information about application "icecat" by file.		
		• (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to gather information about application "SeaMonkey" by file.		
		• (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to gather information about application "Postbox" by file.		
		• (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to gather information about application "Foxmail" by registry.		
		• (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to gather information about application "blackHawk" by file.		
		• (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to gather information about application "WinSCP" by registry.		
		• (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to gather information about application "FTP Navigator" by file.		
		• (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to gather information about application "WS_FTP" by file.		
		• (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to gather information about application "k-Meleon" by file.		
		• (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to gather information about application "Cyberfox" by file.		
		• (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to gather information about application "Pocomail" by file.		
		• (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to gather information about application "RealVNC" by registry.		
		• (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to gather information about application "TightVNC" by registry.		
		• (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to gather information about application "TigerVNC" by registry.		
		• (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to gather information about application "Mozilla Firefox" by file.		
		• (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to gather information about application "Comodo IceDragon" by file.		
		• (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to gather information about application "Flock" by file.		
		• (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to gather information about application "FileZilla" by file.		
		• (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to gather information about application "Qualcomm Eudora" by registry.		
		• (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to gather information about application "FlashFXP" by file.		
		• (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to gather information about application "The Bat!" by file.		
		• (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to gather information about application "Opera Mail" by file.		
1/5	Execution	Executes itself	1	-
		• (Process #1) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe executes a copy of the sample at C:\Users\RDhJ0CNFevzX\Desktop\d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe.		
1/5	Network Connection	Performs DNS request	1	-
		• (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe resolves host name "mail.safalaw.com.ph" to IP "207.148.117.199".		
1/5	Network Connection	Connects to remote host	1	-
		• (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe opens an outgoing TCP connection to host "207.148.117.199:587".		
1/5	Network Connection	Tries to connect using an uncommon port	1	-
		• (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe tries to connect to TCP port 587 at 207.148.117.199.		
1/5	Obfuscation	Resolves API functions dynamically	1	-
		• (Process #2) d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe resolves 51 API functions by name.		

Mitre ATT&CK Matrix

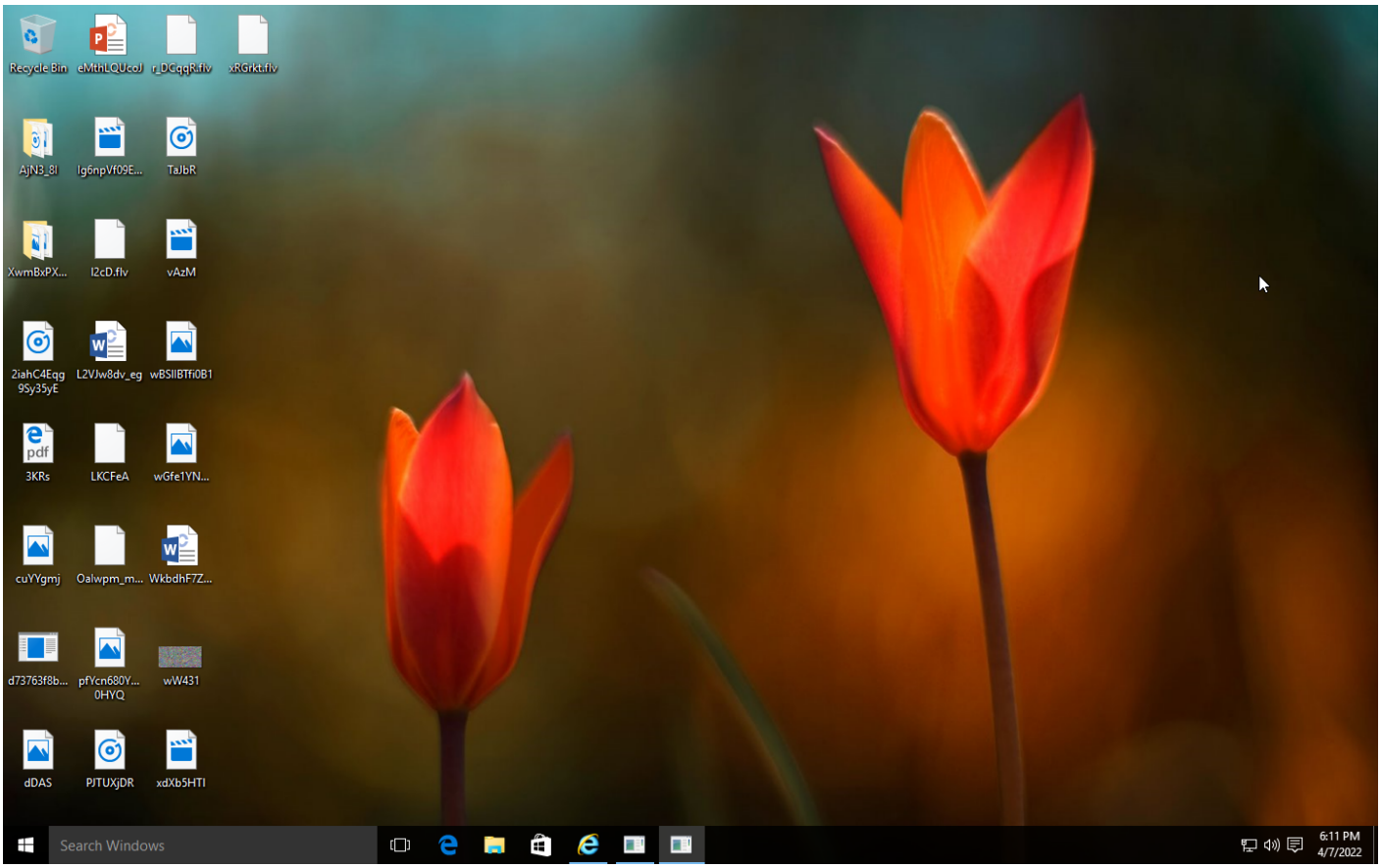
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation			#T1143 Hidden Window	#T1081 Credentials in Files	#T1083 File and Directory Discovery		#T1119 Automated Collection	#T1065 Uncommonly Used Port		
				#T1045 Software Packing	#T1214 Credentials in Registry	#T1012 Query Registry		#T1005 Data from Local System			
					#T1003 Credential Dumping	#T1082 System Information Discovery					

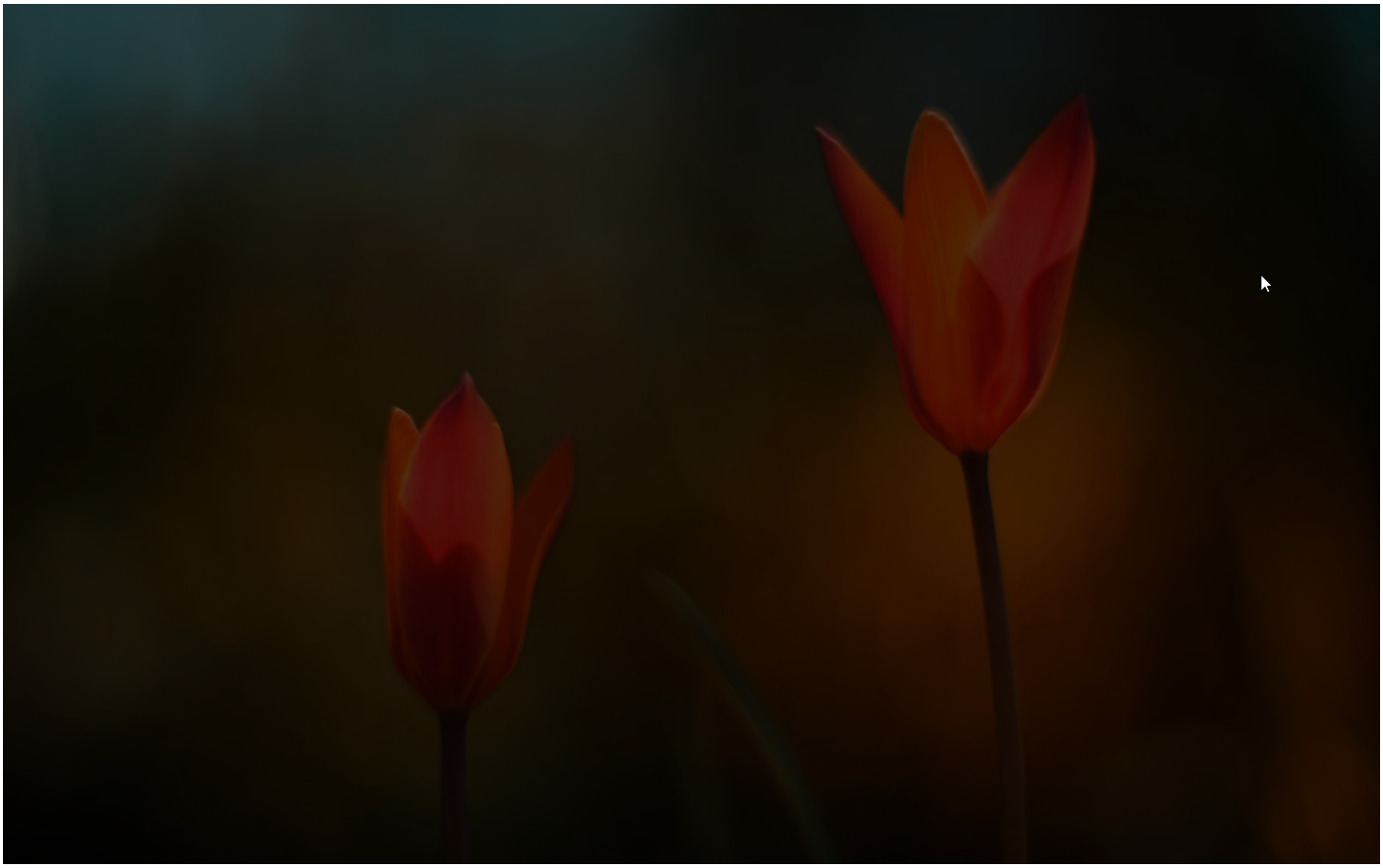
Sample Information

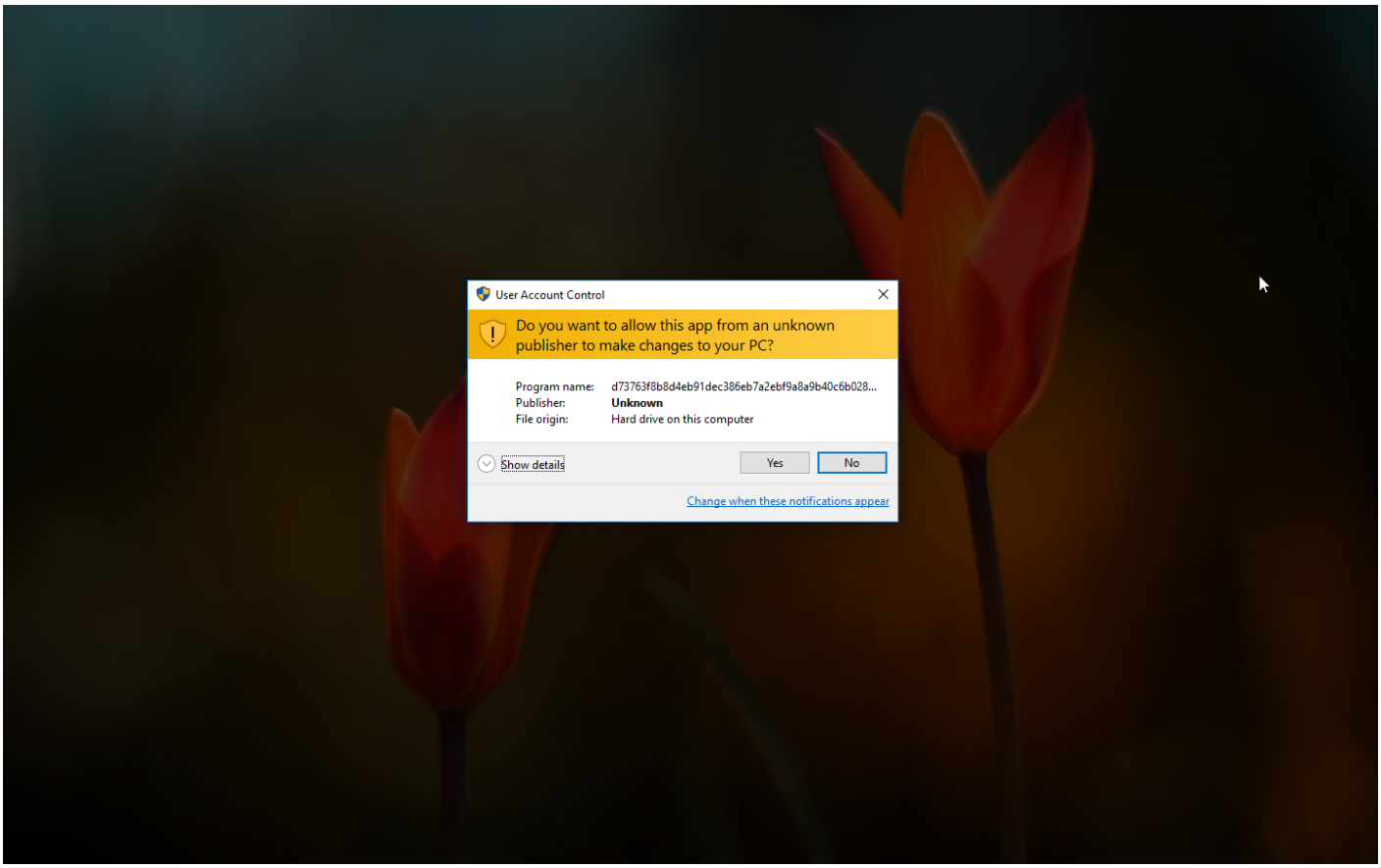
ID	#4023226
MD5	189ad2733ba3c8baa0d9fb41e4223d92
SHA1	90d2762579dfd97d7b767662566f3a623766dd0a
SHA256	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b
SSDeep	12288:wJrxvRltNiL65tlekTAEr4xwWEL9KHHvxosMKnd:8fsiL65t7kT1rjhKHH5os
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe
File Size	434.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

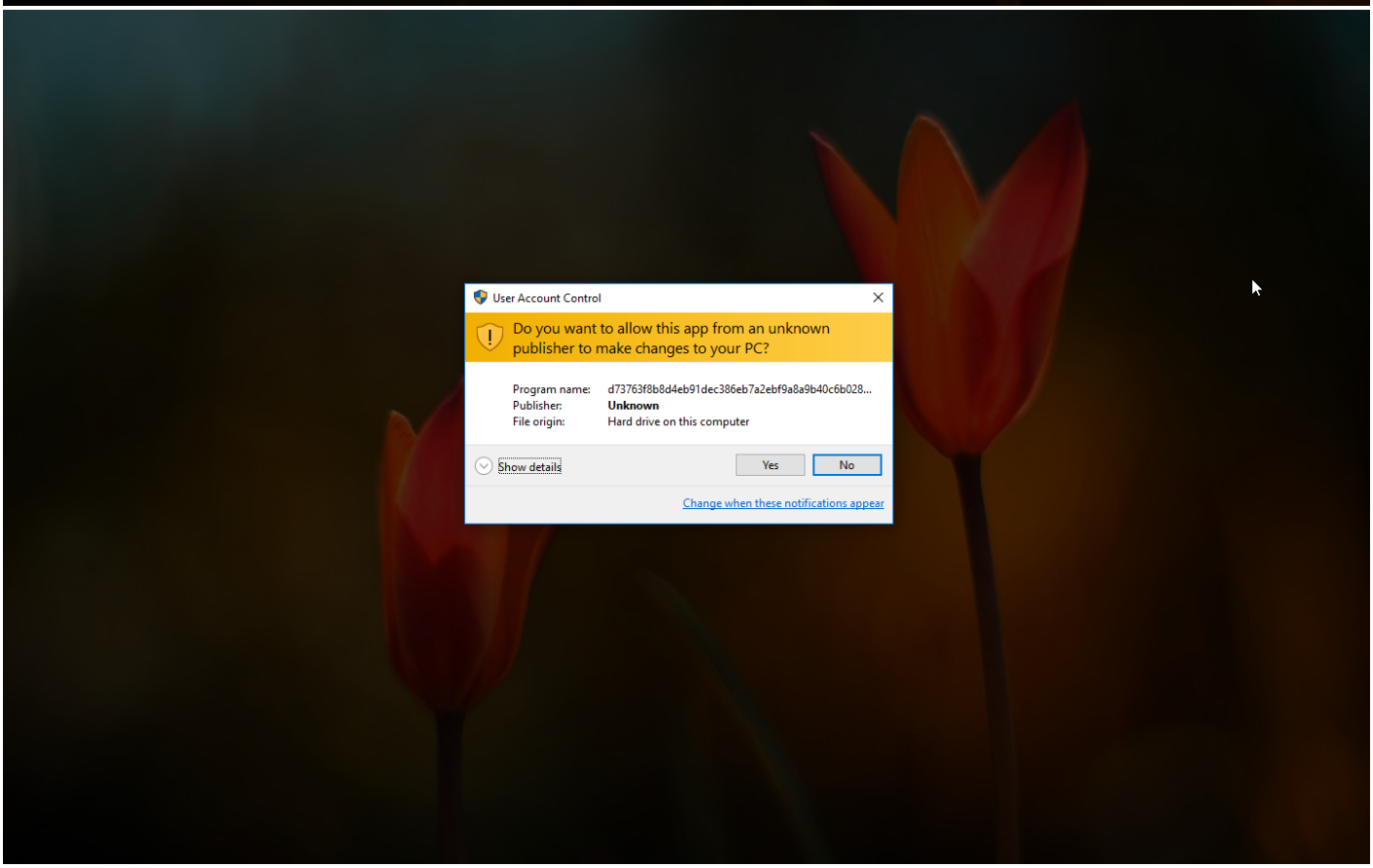
Analysis Information

Creation Time	2022-04-07 20:10 (UTC+2)
Analysis Duration	00:03:59
Termination Reason	Timeout
Number of Monitored Processes	2
Execution Successful	False
Reputation Enabled	✓
WHOIS Enabled	✓
Built-in AV Enabled	✗
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	3


Recycle Bin
eMthLQUcoJ
r_DCqqR.flv
xRGrkt.flv
AjN3_8I
lg6npVf09E...
TaJbR
XwmBxPX...
l2cD.flv
vAzM
2iahC4Eqg 9Sy35yE
L2VJw8dv_eg
wBSIIBTfi0B1
3KRs
LKCFeA
wGfe1YN...
cuYYgmj
Oalwpm_m...
WkbdhF7Z...
d73763f8b...
pfYcn680Y... 0HYQ
wW431
dDAS
PJTUXjDR
xdXb5HTI
Search Windows
6:11 PM
4/7/2022







Screenshots truncated

NETWORK

General

1.62 KB total sent

6.51 KB total received

1 ports 587

2 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

1 DNS requests for 1 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	mail.safalaw.com.ph	NoError	207.148.117.199		NA

BEHAVIOR

Process Graph

Process #1: d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 84045, Reason: Analysis Target
Unmonitor End Time	End Time: 174659, Reason: Terminated
Monitor duration	90.61s
Return Code	0
PID	3716
Parent PID	1184
Bitness	32 Bit

Host Behavior

Type	Count
Module	50
Window	6
Registry	3
File	1
Process	1
-	3
-	7

Process #2: d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe
Command Line	"{path}"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 172036, Reason: Child Process
Unmonitor End Time	End Time: 314084, Reason: Terminated by Timeout
Monitor duration	142.05s
Return Code	Unknown
PID	4088
Parent PID	3716
Bitness	32 Bit

Injection Information (6)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	0xe58	0x400000(4194304)	0x200	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	0xe58	0x402000(4202496)	0x33c00	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	0xe58	0x436000(4415488)	0x600	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	0xe58	0x438000(4423680)	0x200	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	0xe58	0x210008(2162696)	0x4	✓	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	0xe58 / 0xcf4		-	✓	1

Host Behavior

Type	Count
-	21
Registry	92
File	136
User	4
System	31
Module	63
COM	33
Environment	27

Type	Count
-	2
Mutex	2
Window	3

Network Behavior

Type	Count
DNS	1
TCP	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b	C:\Users\RDhJ0CNFevzX\Desktop\d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	Sample File	434.50 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS

Filename

File Name	Category	Operations	Verdict
System Paging File	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe.config	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	Accessed File	Read, Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\config\machine.config	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Epic Privacy Browser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\BraveSoftware\Brave-Browser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Yandex\YandexBrowser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Coowon\Coowon\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Elements Browser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Sputnik\Sputnik\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\QIP Surf\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chromium\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Vivaldi\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CocCoc\Browser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\MapleStudio\ChromePlus\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chedot\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Iridium\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\liebao\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\360Chrome\Chrome\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\7Star\7Star\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CatalinaGroup\Citrio\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Kometa\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CentBrowser\User Data	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Local\Orbitum\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Amigo\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\uCozMedia\Uran\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Comodo\Dragon\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Software\Opera Stable	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Torch\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\icecat\profiles.ini	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Apple\Apple Application Support\plutil.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\SeaMonkey\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Trillian\users\global\accounts.dat	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Moonchild Productions\Pale Moon\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Claws-mail	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Claws-mail\clawsrc	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Thunderbird\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Postbox\profiles.ini	Accessed File	Access	CLEAN
C:\Storage\	Accessed File	Access	CLEAN
C:\mail\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\VirtualStore\Program Files\Foxmail\mail\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\VirtualStore\Program Files (x86)\Foxmail\mail\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\Folder.lst	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\NETGATE Technologies\BlackHawk\profiles.ini	Accessed File	Access	CLEAN
C:\cftp\Ftplist.txt	Accessed File	Access	CLEAN
C:\Program Files\Private Internet Access\data	Accessed File	Access	CLEAN
C:\Private Internet Access\data	Accessed File	Access	CLEAN
C:\FTP Navigator\Ftplist.txt	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Ipswitch\WS_FTP\Sites\ws_ftp.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Waterfox\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Tencent\QQBrowser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Tencent\QQBrowser\User Data\Default\EncryptedStorage	Accessed File	Access	CLEAN
C:\Program Files (x86)\jDownloader\config\database.script	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\MySQL\Workbench\workbench_user_data.dat	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Roaming\eM Client	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\NordVPN	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\K-Meleon\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\8pecxstudios\Cyberfox\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Mailbird\Store\Store.db	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Pocomail\accounts.ini	Accessed File	Access	CLEAN
C:\Program Files (x86)\uvnc bvba\UltraVNC\ultravnc.ini	Accessed File	Access	CLEAN
C:\Program Files (x86)\UltraVNC\ultravnc.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\Firefox\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Credentials\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Credentials\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	Accessed File	Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Protect\S-1-5-21-1560258661-3990802383-1811730007-1000\26d4f968-a540-431b-ab1b-a50e9bbda5d1	Accessed File	Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Comodo\IceDragon\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\FTPGetter\servers.xml	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome\User Data\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Flock\Browser\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Psi\profiles	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Psi+\profiles	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\FileZilla\recentservers.xml	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\falkon\profiles\profiles.ini	Accessed File	Access	CLEAN
C:\ProgramData\FlashFXP\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\FlashFXP\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\The Bat!	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Edge\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Mail\Opera Mail\wand.dat	Accessed File	Access	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
mail.safalaw.com.ph	207.148.117.199	-	DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
192.168.0.1	-	-	UDP, DNS	CLEAN

IP Address	Domains	Country	Protocols	Verdict
207.148.117.199	mail.safalaw.com.ph	Singapore	TCP, DNS	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	read, access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	read, access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_PERFORMANCE_DATA	access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	read, access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	read, access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting	access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Impersonation Level	read, access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Namespace	read, access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_CURRENT_USER\Software\DownloadManager\Passwords	access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\FTPWare\COREFTP\Sites	access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_CURRENT_USER\Software\Aerofox\FoxmailPreview	access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_CURRENT_USER\Software\Aerofox\Foxmail\V3.1	access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_CURRENT_USER\Software\RimArts\B2\Settings	access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_CURRENT_USER\Software\OpenVPN-GUI\configs	access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Martin Prikryl\WinSCP 2\Sessions	access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Messaging Subsystem\Profiles\9375CFF0413111d3B88A00104B2A6676	access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001	access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Email	read, access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP Password	read, access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 Password	read, access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTP Password	read, access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP Password	read, access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002	access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Email	read, access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password	read, access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password	read, access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP Password	read, access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password	read, access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Server	read, access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003	access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\Email	read, access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP Password	read, access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3 Password	read, access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTP Password	read, access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP Password	read, access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\RealVNC\WinVNC4	access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Wow6432Node\RealVNC\WinVNC4	access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\vncserver	access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\RealVNC\vncserver	access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4	access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\RealVNC\WinVNC4	access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\ORL\WinVNC3	access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\ORL\WinVNC3	access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\TightVNC\Server	access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_CURRENT_USER\Software\TightVNC\Server	access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\TigerVNC\Server	access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_CURRENT_USER\Software\TigerVNC\Server	access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	read, access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	read, access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	read, access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	read, access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_CURRENT_USER\Software\IncrediMail\Identities	access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_CURRENT_USER\Software\Qualcomm\Eudora\CommandLine	access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	read, access	d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	CLEAN

Process

Process Name	Commandline	Verdict
d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	"{path}"	MALICIOUS
d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe	"C:\Users\RDhJ0CNFevzX\Desktop\d73763f8b8d4eb91dec386eb7a2ebf9a8a9b40c6b028d57e6144ed74551d460b.exe"	SUSPICIOUS

YARA / AV

YARA (3)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	AgentTesla_HTML_Message	Agent Tesla html-formatted message	Web Request	-	Spyware	5/5
Malware	AgentTesla_HTML_Message	Agent Tesla html-formatted message	Web Request	-	Spyware	5/5
Malware	AgentTesla_StringDecryption_v3	Agent Tesla v3 string decryption	Memory Dump	-	Spyware	5/5

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_mso2016
Description	win10_64_th2_en_mso2016
Architecture	x86 64-bit
Operating System	Windows 10 Threshold 2
Kernel Version	10.0.10586.0 (0de6dc23-8e19-4bb7-8608-d54b1e6fa379)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	4.4.1
Dynamic Engine Version	4.4.1 / 01/14/2022 05:06
Static Engine Version	4.4.1.0 / 2022-01-14 04:00:58
AV Exceptions Version	4.4.1.6 / 2021-12-14 15:06:27
Link Detonation Heuristics Version	4.4.1.16 / 2022-03-11 16:16:43
Smart Memory Dumping Rules Version	4.4.1.6 / 2021-12-14 15:06:27
Signature Trust Store Version	4.4.1.6 / 2021-12-14 15:06:27
VMRay Threat Identifiers Version	4.4.1.19 / 2022-03-31 10:55:59
YARA Built-in Ruleset Version	4.4.1.19

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1003
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	11.0.10586.0
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed

System Information

Sample Directory	C:\Users\RDhJ0CNFevzX\Desktop
Computer Name	XC64ZB
User Domain	XC64ZB
User Name	RDhJ0CNFevzX
User Profile	C:\Users\RDhJ0CNFevzX
Temp Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp
System Root	C:\Windows