MALICIOUS

Classifications: Spyware, Keylogger

Threat Names: Agent Tesla v3, Mal/Generic-S, Mal/HTMLGen-A

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**b0a10bd27d48fea4e569797829057892.virus.exe**
ID	#2779368
MD5	b0a10bd27d48fea4e569797829057892
SHA1	5909c3383e27a1c5e7edcadd5319b31d2813df12
SHA256	4e63cadd6aa91bc65755bd2b4035a3451cbc4854ed2817ac08941919f892f7e7
File Size	861.50 KB
Report Created	2021-09-27 13:18 (UTC+2)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (25 rules, 70 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	1	Spyware
	• Rule "AgentTesla_StringDecryption_v3" from ruleset "Malware" has matched on a memory dump for (process #2) b0a10bd27d48fea4e569797829057892.virus.exe.			
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: BlackHawk, TigerVNC, Pocomail, Opera, Flock, CoreFTP, FTP Navigator, The Bat!, Opera Mail, SeaMon... ... Ipswitch WS_FTP, Comodo IceDragon, FileZilla, Postbox, OpenVPN, Internet Explorer, Internet Download Manager, Cyberfox, k-Meleon.			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as "Mal/Generic-S".			
4/5	Reputation	Resolves known malicious domain	1	-
	• Reputation analysis labels the resolved domain "mail.airseaalliance.com" as "Mal/HTMLGen-A".			
3/5	Input Capture	Monitors keyboard input	1	Keylogger
	• (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe installs system wide "WH_KEYBOARD_LL" hook(s) to monitor keystrokes.			
2/5	Data Collection	Reads sensitive browser data	9	-
	• (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to read sensitive data of web browser "Opera" by file. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to read sensitive data of web browser "Comodo IceDragon" by file. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to read sensitive data of web browser "Flock" by file. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to read sensitive data of web browser "Cyberfox" by file. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to read credentials of web browser "Internet Explorer" by reading from the system's credential vault. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to read sensitive data of web browser "k-Meleon" by file. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to read sensitive data of web browser "Mozilla Firefox" by file. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to read sensitive data of web browser "BlackHawk" by file.			
2/5	Data Collection	Reads sensitive ftp data	5	-
	• (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to read sensitive data of ftp application "FTP Navigator" by file. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to read sensitive data of ftp application "FileZilla" by file. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to read sensitive data of ftp application "Ipswitch WS_FTP" by file. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to read sensitive data of ftp application "CoreFTP" by file. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to read sensitive data of ftp application "CoreFTP" by registry.			
2/5	Data Collection	Reads sensitive mail data	7	-
	• (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to read sensitive data of mail application "Opera Mail" by file. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to read sensitive data of mail application "The Bat!" by file. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to read sensitive data of mail application "IncrediMail" by registry. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to read sensitive data of mail application "Pocomail" by file. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to read sensitive data of mail application "Microsoft Outlook" by registry. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to read sensitive data of mail application "Mozilla Thunderbird" by file. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to read sensitive data of mail application "Postbox" by file.			
2/5	Data Collection	Reads sensitive application data	6	-

Score	Category	Operation	Count	Classification
	• (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to read sensitive data of application "Internet Download Manager" by registry. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to read sensitive data of application "WinSCP" by registry. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to read sensitive data of application "SeaMonkey" by file. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to read sensitive data of application "TightVNC" by registry. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to read sensitive data of application "TigerVNC" by registry. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to read sensitive data of application "OpenVPN" by registry.		
2/5	Discovery	Queries OS version via WMI	1	-
	• (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe queries OS version via WMI.			
2/5	Discovery	Executes WMI query	2	-
	• (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe executes WMI query: select * from Win32_OperatingSystem. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe executes WMI query: SELECT * FROM Win32_Processor.			
2/5	Discovery	Collects hardware properties	1	-
	• (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe queries hardware properties via WMI.			
2/5	Anti Analysis	Tries to detect virtual machine	1	-
	• Multiple processes are possibly trying to detect a VM via rdtsc.			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	1	-
	• (Process #1) b0a10bd27d48fea4e569797829057892.virus.exe modifies memory of (process #2) b0a10bd27d48fea4e569797829057892.virus.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
	• (Process #1) b0a10bd27d48fea4e569797829057892.virus.exe alters context of (process #2) b0a10bd27d48fea4e569797829057892.virus.exe.			
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #1) b0a10bd27d48fea4e569797829057892.virus.exe starts (process #2) b0a10bd27d48fea4e569797829057892.virus.exe with a hidden window.			
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #1) b0a10bd27d48fea4e569797829057892.virus.exe reads from (process #2) b0a10bd27d48fea4e569797829057892.virus.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) b0a10bd27d48fea4e569797829057892.virus.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) b0a10bd27d48fea4e569797829057892.virus.exe enables process privilege "SeDebugPrivilege".			
1/5	Discovery	Possibly does reconnaissance	22	-

Score	Category	Operation	Count	Classification
	• (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to gather information about application "FTP Navigator" by file. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to gather information about application "Opera Mail" by file. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to gather information about application "The Bat!" by file. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to gather information about application "Comodo IceDragon" by file. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to gather information about application "Qualcomm Eudora" by registry. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to gather information about application "Flock" by file. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to gather information about application "FileZilla" by file. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to gather information about application "icecat" by file. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to gather information about application "Cyberfox" by file. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to gather information about application "Pocomail" by file. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to gather information about application "k-Meleon" by file. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to gather information about application "WS_FTP" by file. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to gather information about application "WinSCP" by registry. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to gather information about application "SeaMonkey" by file. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to gather information about application "Foxmail" by registry. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to gather information about application "Postbox" by file. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to gather information about application "Mozilla Firefox" by file. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to gather information about application "RealVNC" by registry. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to gather information about application "TightVNC" by registry. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to gather information about application "TigerVNC" by registry. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to gather information about application "blackHawk" by file. • (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to gather information about application "CoreFTP" by file.		
1/5	Execution	Executes itself	1	-
	• (Process #1) b0a10bd27d48fea4e569797829057892.virus.exe executes a copy of the sample at C:\Users\kEecfMwgj\Desktop\b0a10bd27d48fea4e569797829057892.virus.exe.			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe resolves 53 API functions by name.			
1/5	Network Connection	Performs DNS request	1	-
	• (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe resolves host name "mail.airseaalliance.com" to IP "135.181.211.109".			
1/5	Network Connection	Connects to remote host	1	-
	• (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe opens an outgoing TCP connection to host "135.181.211.109:587".			
1/5	Network Connection	Tries to connect using an uncommon port	1	-
	• (Process #2) b0a10bd27d48fea4e569797829057892.virus.exe tries to connect to TCP port 587 at 135.181.211.109.			

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	#T1179 Hooking	#T1179 Hooking	#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			
				#T1497 Virtualization/ Sandbox Evasion	#T1003 Credential Dumping	#T1082 System Information Discovery		#T1056 Input Capture			
					#T1056 Input Capture	#T1497 Virtualization/ Sandbox Evasion					
					#T1179 Hooking	#T1124 System Time Discovery					

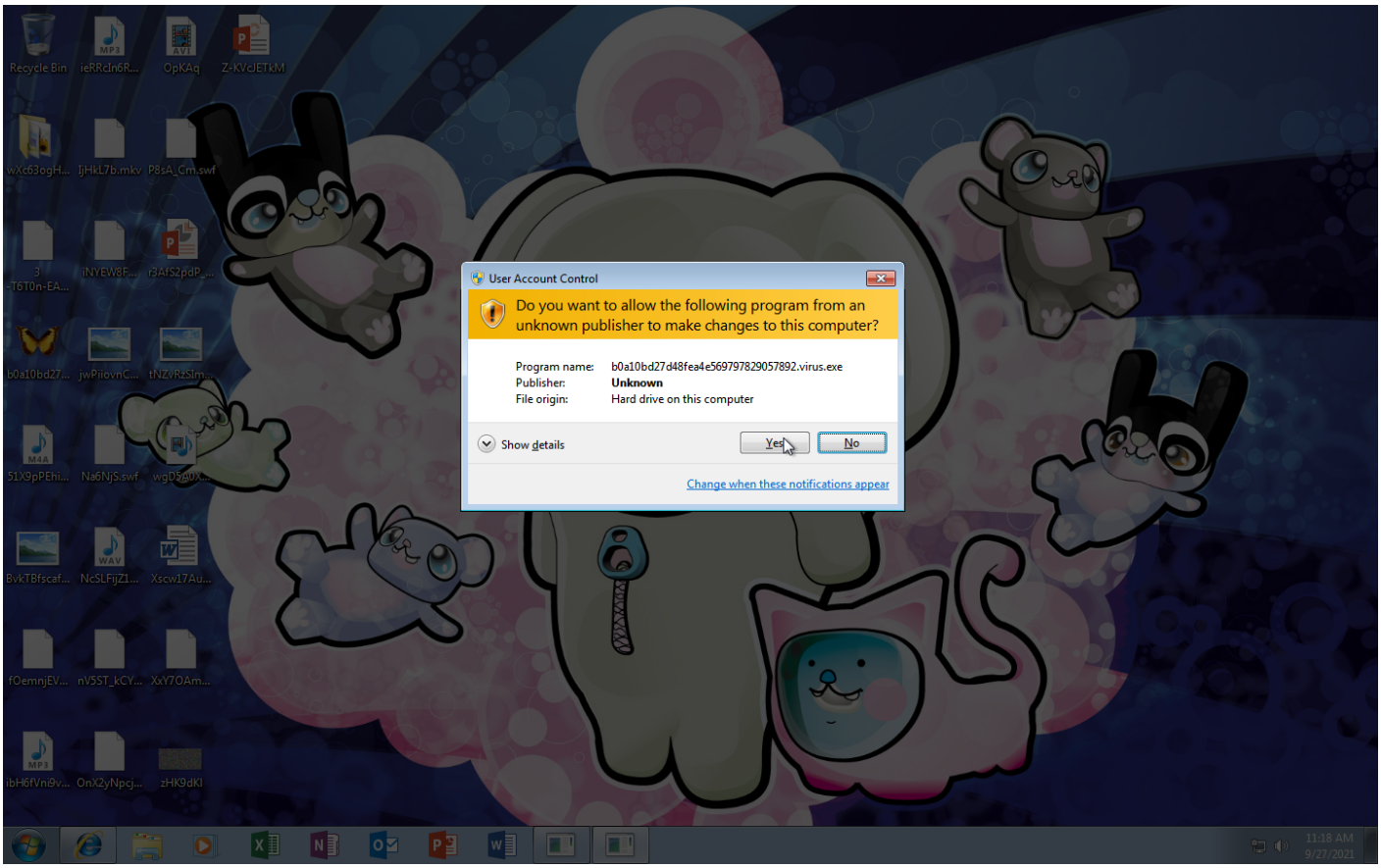
Sample Information

ID	#2779368
MD5	b0a10bd27d48fea4e569797829057892
SHA1	5909c3383e27a1c5e7edcadd5319b31d2813df12
SHA256	4e63cadd6aa91bc65755bd2b4035a3451cbc4854ed2817ac08941919f892f7e7
SSDeep	12288:fycRcIcGRiuoBQnxcsDA7Mg+Svq4DPp9KDwu43oO3yYeQEi2RA/2xYBSzz2DNBcF:n2lFjF+3e+vms2bC/UP1QHeF+G
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	b0a10bd27d48fea4e569797829057892.virus.exe
File Size	861.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2021-09-27 13:18 (UTC+2)
Analysis Duration	00:04:00
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	1


Recycle Bin
ieRRcIn6R...
OpKAq
Z-KVcJETkM
wXc63ogH...
IjHkL7b.mkv
P8sA_Cm.swf
iNYEW8F...
r3AfS2pdP_...
b0a10bd27...
jwPiiovnC...
tNZvRzSIm...
51X9pPEhi...
Na6NjS.swf
BvkTBfscaf...
NcSLFijZ1...
Xscw17Au...
fOemnjEV...
nV5ST_kCY...
XxY7OAm...
ibH6fVni9v...
OnX2yNpcj...
zHK9dKl
11:18 AM
9/27/2021


User Account Control
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Program name: b0a10bd27d48fea4e569797829057892.virus.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear

NETWORK

General

1.23 KB total sent

1.00 KB total received

1 ports 587

2 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

2 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.airseaalliance.com, airseaalliance.com	NoError	135.181.211.109	airseaalliance.com	NA
-	mail.airseaalliance.com	-	135.181.211.109		NA

BEHAVIOR

Process Graph

Process #1: b0a10bd27d48fea4e569797829057892.virus.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\b0a10bd27d48fea4e569797829057892.virus.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\b0a10bd27d48fea4e569797829057892.virus.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 42887, Reason: Analysis Target
Unmonitor End Time	End Time: 132694, Reason: Terminated
Monitor duration	89.81s
Return Code	0
PID	3796
Parent PID	1116
Bitness	32 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
-	8.03 KB	790a6af00576b6ee07663cf571a92e5b72379c9d24f3599af1fa9fec8aeb168a	✕
-	108.45 KB	4d55a3a562da4193c4f052457deead562b2b4b326d9ed8a1ceb0b58e36c41687	✕

Host Behavior

Type	Count
Registry	4
Process	1
File	20
Module	33
Window	6
-	3
-	7

Process #2: b0a10bd27d48fea4e569797829057892.virus.exe

ID	2
File Name	c:\users\keecfmwgj\desktop\b0a10bd27d48fea4e569797829057892.virus.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\b0a10bd27d48fea4e569797829057892.virus.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 130605, Reason: Child Process
Unmonitor End Time	End Time: 282949, Reason: Terminated by Timeout
Monitor duration	152.34s
Return Code	Unknown
PID	3924
Parent PID	3796
Bitness	32 Bit

Injection Information (6)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\keecfmwgj\desktop\b0a10bd27d48fea4e569797829057892.virus.exe	0xed8	0x400000(4194304)	0x200	✓	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\b0a10bd27d48fea4e569797829057892.virus.exe	0xed8	0x402000(4202496)	0x35600	✓	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\b0a10bd27d48fea4e569797829057892.virus.exe	0xed8	0x438000(4423680)	0x600	✓	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\b0a10bd27d48fea4e569797829057892.virus.exe	0xed8	0x43a000(4431872)	0x200	✓	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\b0a10bd27d48fea4e569797829057892.virus.exe	0xed8	0x7efde008(2130567176)	0x4	✓	1
Modify Control Flow	#1: c:\users\keecfmwgj\desktop\b0a10bd27d48fea4e569797829057892.virus.exe	0xed8 / 0xf58		-	✓	1

Host Behavior

Type	Count
Registry	124
File	132
Module	75
Window	6
System	18
User	4
-	31
COM	53
Environment	26
-	2
Mutex	2

Network Behavior

Type	Count
DNS	2
TCP	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
4e63cadd6aa91bc65755bd2b4035a3451cbc4854ed2817ac08941919f892f7e7	C:\Users\kEecfMwgj\Desktop\b0a10bd27d48fea4e569797829057892.virus.exe	Sample File	861.50 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
790a6af00576b6ee07663cf571a92e5b72379c9d24f3599af1fa9fec8aeb168a	c:\users\keecfmwgj\appdata\local\gdipfontcachev1.dat	Dropped File	8.03 KB	application/octet-stream	-	CLEAN
4d55a3a562da4193c4f052457deead562b2b4b326d9ed8a1ceb0b58e36c41687	c:\users\keecfmwgj\appdata\local\gdipfontcachev1.dat	Dropped File	108.45 KB	application/octet-stream	-	CLEAN

Filename

File Name	Category	Operations	Verdict
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\kEecfMwgj\Desktop\b0a10bd27d48fea4e569797829057892.virus.exe.config	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\Desktop\b0a10bd27d48fea4e569797829057892.virus.exe	Sample File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Iridium\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\uCozMedia\Uran\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Opera Software\Opera Stable	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\7Star\7Star\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Coowon\Coowon\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\MapleStudio\ChromePlus\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\CocCoc\Browser\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Yandex\YandexBrowser\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\CatalinaGroup\Citrio\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\360Chrome\Chrome\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Sputnik\Sputnik\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Torch\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\QIP Surf\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Chedot\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\liebao\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Orbitum\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Kometa\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Vivaldi\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\CentBrowser\User Data	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\AppData\Local\Elements Browser\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Amigo\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\BraveSoftware\Brave-Browser\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Epic Privacy Browser\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Comodo\Dragon\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Chromium\User Data	Accessed File	Access	CLEAN
C:\FTP Navigator\Ftplist.txt	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Opera Mail\Opera Mail\wand.dat	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\The Bat!	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Waterfox\profiles.ini	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Comodo\IceDragon\profiles.ini	Accessed File	Access	CLEAN
C:\cftp\Ftplist.txt	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\FTPGetter\servers.xml	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Flock\Browser\profiles.ini	Accessed File	Access	CLEAN
C:\Users\All Users\AppData\Roaming\FlashFXP\3quick.dat	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\FileZilla\recentservers.xml	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\eM Client	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Mozilla\icecat\profiles.ini	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Moonchild Productions\Pale Moon\profiles.ini	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\falkon\profiles\profiles.ini	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\8pecxstudios\Cyberfox\profiles.ini	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Apple\Apple Application Support\plutil.exe	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\NordVPN	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Google\Chrome\User Data\	Accessed File	Access	CLEAN
C:\Program Files (x86)\jDownloader\config\database.script	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Edge\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Tencent\QQBrowser\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Tencent\QQBrowser\User Data\Default\EncryptedStorage	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Pocomail\accounts.ini	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\K-Meleon\profiles.ini	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Ipswitch\WS_FTP\Sites\ws_ftp.ini	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Psi\profiles	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\AppData\Roaming\Psi+\profiles	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Mozilla\SeaMonkey\profiles.ini	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:\Users\kEecfMwgj\Desktop\Folder.lst	Accessed File	Access	CLEAN
C:\Storage\	Accessed File	Access	CLEAN
C:\mail\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\VirtualStore\Program Files\Foxmail\mail\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\VirtualStore\Program Files (x86)\Foxmail\mail\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Thunderbird\profiles.ini	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Postbox\profiles.ini	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Mozilla\Firefox\profiles.ini	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Trillian\users\global\accounts.dat	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Credentials\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Credentials\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Mailbird\Store\Store.db	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\kEecfMwgj\AppData\Roaming\NETGATE Technologies\BlackHawk\profiles.ini	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\MySQL\Workbench\workbench_user_data.dat	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Claws-mail	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Claws-mail\clawsrc	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\CoreFTP\sites.idx	Accessed File	Access	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
mail.airseaalliance.com	135.181.211.109	-	DNS	MALICIOUS
airseaalliance.com	135.181.211.109	-	DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
192.168.0.1	-	-	UDP, DNS	CLEAN
135.181.211.109	airseaalliance.com, mail.airseaalliance.com	Finland	DNS, TCP	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_PERFORMANCE_DATA	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.UseHttpPipeliningAndBufferPooling	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseHttpPipeliningAndBufferPooling	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.UseSafeSynchronousClose	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseSafeSynchronousClose	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.UseStrictRfcInterimResponseHandling	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseStrictRfcInterimResponseHandling	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Uri.AllowDangerousUnicodeDecompositions	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\AllowDangerousUnicodeDecompositions	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Uri.UseStrictIPv6AddressParsing	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseStrictIPv6AddressParsing	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Uri.AllowAllUriEncodingExpansion	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\AllowAllUriEncodingExpansion	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SchSendAuxRecord	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchSendAuxRecord	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SystemDefaultTlsVersions	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.RequireCertificateEKUs	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\RequireCertificateEKUs	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Impersonation Level	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Namespace	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\WMIDisableCOMSecurity	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\Software\DownloadManager\Passwords	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\Software\Qualcomm\Eudora\CommandLine	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\Software\IncrediMail\Identities	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Martin Prikryl\WinSCP 2\Sessions	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\Software\RimArts\B2\Settings	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Messaging Subsystem\Profiles\9375CFF0413111d3B88A00104B2A6676	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Email	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP Password	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 Password	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTP Password	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP Password	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Email	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP Password	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Server	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\Email	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP Password	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3 Password	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTP Password	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP Password	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\Software\Aerofox\FoxmailPreview	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\Software\Aerofox\Foxmail\V3.1	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\RealVNC\WinVNC4	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Wow6432Node\RealVNC\WinVNC4	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\vncserver	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\RealVNC\vncserver	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\RealVNC\WinVNC4	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\ORL\WinVNC3	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\Software\ORL\WinVNC3	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\TightVNC\Server	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\Software\TightVNC\Server	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\TigerVNC\Server	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\Software\TigerVNC\Server	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\Software\OpenVPN-GUI\configs	access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
HKEY_CURRENT_USER\Software\FTPWare\COREFTP\Sites\Host	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
\HKEY_CURRENT_USERSoftwareFTPWareCOREFTPSitesPort	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
\HKEY_CURRENT_USERSoftwareFTPWareCOREFTPSitesUser	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
\HKEY_CURRENT_USERSoftwareFTPWareCOREFTPSitesPW	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN
\HKEY_CURRENT_USERSoftwareFTPWareCOREFTPSitesName	read, access	b0a10bd27d48fea4e569797829057892.virus.exe	CLEAN

Process

Process Name	Commandline	Verdict
b0a10bd27d48fea4e569797829057892.virus.exe	"C:\Users\kEecfMwgj\Desktop\b0a10bd27d48fea4e569797829057892.virus.exe"	MALICIOUS
b0a10bd27d48fea4e569797829057892.virus.exe	"C:\Users\kEecfMwgj\Desktop\b0a10bd27d48fea4e569797829057892.virus.exe"	MALICIOUS

YARA / AV

YARA (1)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	AgentTesla_StringDecryption_v3	Agent Tesla v3 string decryption	Memory Dump	-	Spyware	5/5

ENVIRONMENT

Virtual Machine Information

Name	win7_64_sp1_en_mso2016
Description	win7_64_sp1_en_mso2016
Architecture	x86 64-bit
Operating System	Windows 7
Kernel Version	6.1.7601.18741 (2e37f962-d699-492c-aaf3-f9f4e9770b1d)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	4.3.0
Dynamic Engine Version	4.3.0 / 09/20/2021 03:59
Static Engine Version	4.3.0.0 / 2021-09-20 03:00:12
AV Exceptions Version	4.3.0.0 / 2021-09-20 03:00:12
Link Detonation Heuristics Version	4.3.0.4 / 2021-09-16 11:30:34
Signature Trust Store Version	4.3.0.0 / 2021-09-20 03:00:12
VMRay Threat Identifiers Version	4.3.1.7 / 2021-09-22 10:00:51
YARA Built-in Ruleset Version	4.3.0.5

Anti Virus Information

Built-in AV Version	AVCORE v2.2 Linux/x86_64 11.0.1.19 (March 15, 2021)
Built-in AV Database Update Release Date	2021-09-27 07:10:04+00:00
Built-in AV Database Records	10465270

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	8.0.7601.17514
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed

System Information

Sample Directory	C:\Users\kEecfMwgj\Desktop
Computer Name	Q9IATRKPRH
User Domain	Q9IATRKPRH

User Name	kEecfMwgj
User Profile	C:\Users\kEecfMwgj
Temp Directory	C:\Users\KEECFM~1\AppData\Local\Temp
System Root	C:\Windows