MALICIOUS

Classifications: Spyware

Threat Names: Agent Tesla v3 | C2/Generic-A | Gen:Variant.Bulz.766082

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe**
ID	#2780378
MD5	22a2657bb48e3303f6f0a0fd1fdfe441
SHA1	d6a230a732f3d691a7fce60081f30627ffabd33d
SHA256	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac
File Size	862.00 KB
Report Created	2021-09-27 18:15 (UTC+2)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (28 rules, 82 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 #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.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	System Modification	Modifies network configuration	1	-
	• (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe modifies the host.conf file, probably to redirect network traffic.			
4/5	Reputation	Contacts known malicious IP address	1	-
	• Reputation analysis labels the contacted IP address 208.91.198.143 as "C2/Generic-A".			
4/5	Antivirus	Malicious content was detected by heuristic scan	1	-
	• Built-in AV detected the sample itself as "Gen:Variant.Bulz.766082".			
2/5	Anti Analysis	Tries to detect virtual machine	3	-
	• (Process #1) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe reads out system information, commonly used to detect "VirtualBox" via registry. (Key is "HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\VirtualBox Guest Additions"). • (Process #1) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe reads out system information, commonly used to detect "VMware" via registry. (Key is "HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Tools"). • Multiple processes are possibly trying to detect a VM via rdtsc.			
2/5	Anti Analysis	Tries to detect application sandbox	1	-
	• (Process #1) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to detect "wine" by calling GetProcAddress() on "wine_get_unix_file_name".			
2/5	Discovery	Executes WMI query	3	-
	• (Process #1) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe executes WMI query: SELECT * FROM Win32_VideoController. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe executes WMI query: select * from Win32_OperatingSystem. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe executes WMI query: SELECT * FROM Win32_Processor.			
2/5	Discovery	Collects hardware properties	2	-
	• (Process #1) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe queries hardware properties via WMI. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe queries hardware properties via WMI.			
2/5	Data Collection	Reads sensitive browser data	9	-

Score	Category	Operation	Count	Classification
		• (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to read sensitive data of web browser "Opera" by file. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to read sensitive data of web browser "Cyberfox" by file. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to read sensitive data of web browser "Flock" by file. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to read sensitive data of web browser "k-Meleon" by file. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to read sensitive data of web browser "Mozilla Firefox" by file. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to read sensitive data of web browser "BlackHawk" by file. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to read sensitive data of web browser "Comodo IceDragon" by file. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to read credentials of web browser "Internet Explorer" by reading from the system's credential vault.		
2/5	Data Collection	Reads sensitive ftp data	5	-
		• (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to read sensitive data of ftp application "CoreFTP" by file. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to read sensitive data of ftp application "CoreFTP" by registry. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to read sensitive data of ftp application "FTP Navigator" by file. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to read sensitive data of ftp application "FileZilla" by file. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to read sensitive data of ftp application "Ipswitch WS_FTP" by file.		
2/5	Data Collection	Reads sensitive mail data	7	-
		• (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to read sensitive data of mail application "Microsoft Outlook" by registry. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to read sensitive data of mail application "Pocomail" by file. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to read sensitive data of mail application "Opera Mail" by file. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to read sensitive data of mail application "Postbox" by file. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to read sensitive data of mail application "The Bat!" by file. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to read sensitive data of mail application "Mozilla Thunderbird" by file. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to read sensitive data of mail application "IncrediMail" by registry.		
2/5	Data Collection	Reads sensitive application data	6	-
		• (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to read sensitive data of application "TightVNC" by registry. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to read sensitive data of application "TigerVNC" by registry. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to read sensitive data of application "WinSCP" by registry. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to read sensitive data of application "Internet Download Manager" by registry. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to read sensitive data of application "OpenVPN" by registry. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to read sensitive data of application "SeaMonkey" by file.		
2/5	Discovery	Queries OS version via WMI	1	-
		• (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe queries OS version via WMI.		
2/5	Injection	Writes into the memory of a process started from a created or modified executable	1	-
		• (Process #1) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe modifies memory of (process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe.		
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
		• (Process #1) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe alters context of (process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe.		
1/5	Hide Tracks	Creates process with hidden window	3	-

Score	Category	Operation	Count	Classification
	• (Process #1) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe starts (process #2) powershell.exe with a hidden window. • (Process #1) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe starts (process #6) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe with a hidden window. • (Process #1) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe starts (process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe with a hidden window.		
1/5	Obfuscation	Reads from memory of another process	2	-
	• (Process #1) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe reads from (process #6) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe. • (Process #1) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe reads from (process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe.		
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.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	2	-
	• (Process #1) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe enables process privilege "SeDebugPrivilege". • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe enables process privilege "SeDebugPrivilege".		
1/5	Discovery	Enumerates running processes	1	-
	• (Process #1) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe enumerates running processes.		
1/5	System Modification	Modifies operating system directory	1	-
	• (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe creates file "C:\Windows\system32\drivers\etc\hosts" in the OS directory.		
1/5	Discovery	Possibly does reconnaissance	22	-
	• (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to gather information about application "Cyberfox" by file. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to gather information about application "CoreFTP" by file. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to gather information about application "Pocomail" by file. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to gather information about application "FTP Navigator" by file. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to gather information about application "icecat" by file. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to gather information about application "FileZilla" by file. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to gather information about application "Opera Mail" by file. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to gather information about application "Foxmail" by registry. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to gather information about application "Postbox" by file. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to gather information about application "Flock" by file. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to gather information about application "RealVNC" by registry. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to gather information about application "TightVNC" by registry. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to gather information about application "TigerVNC" by registry. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to gather information about application "k-Meleon" by file. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to gather information about application "WinSCP" by registry. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to gather information about application "The Bat!" by file. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to gather information about application "Mozilla Firefox" by file. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to gather information about application "WS_FTP" by file. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to gather information about application "blackHawk" by file. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to gather information about application "SeaMonkey" by file. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to gather information about application "Qualcomm Eudora" by registry. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to gather information about application "Comodo IceDragon" by file.		
1/5	Obfuscation	Resolves API functions dynamically	2	-

Score	Category	Operation	Count	Classification
	• (Process #1) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe resolves 63 API functions by name. • (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe resolves 53 API functions by name.			
1/5	Network Connection	Performs DNS request	1	-
	• (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe resolves host name "smtp.zfftcn.com" to IP "208.91.199.225".			
1/5	Network Connection	Connects to remote host	1	-
	• (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe opens an outgoing TCP connection to host "208.91.199.225:587".			
1/5	Network Connection	Tries to connect using an uncommon port	1	-
	• (Process #7) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe tries to connect to TCP port 587 at 208.91.199.225.			
1/5	Execution	Executes itself	1	-
	• (Process #1) 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe executes a copy of the sample at C:\Users\kEecfMwgj\Desktop\85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe.			

Mitre ATT&CK Matrix

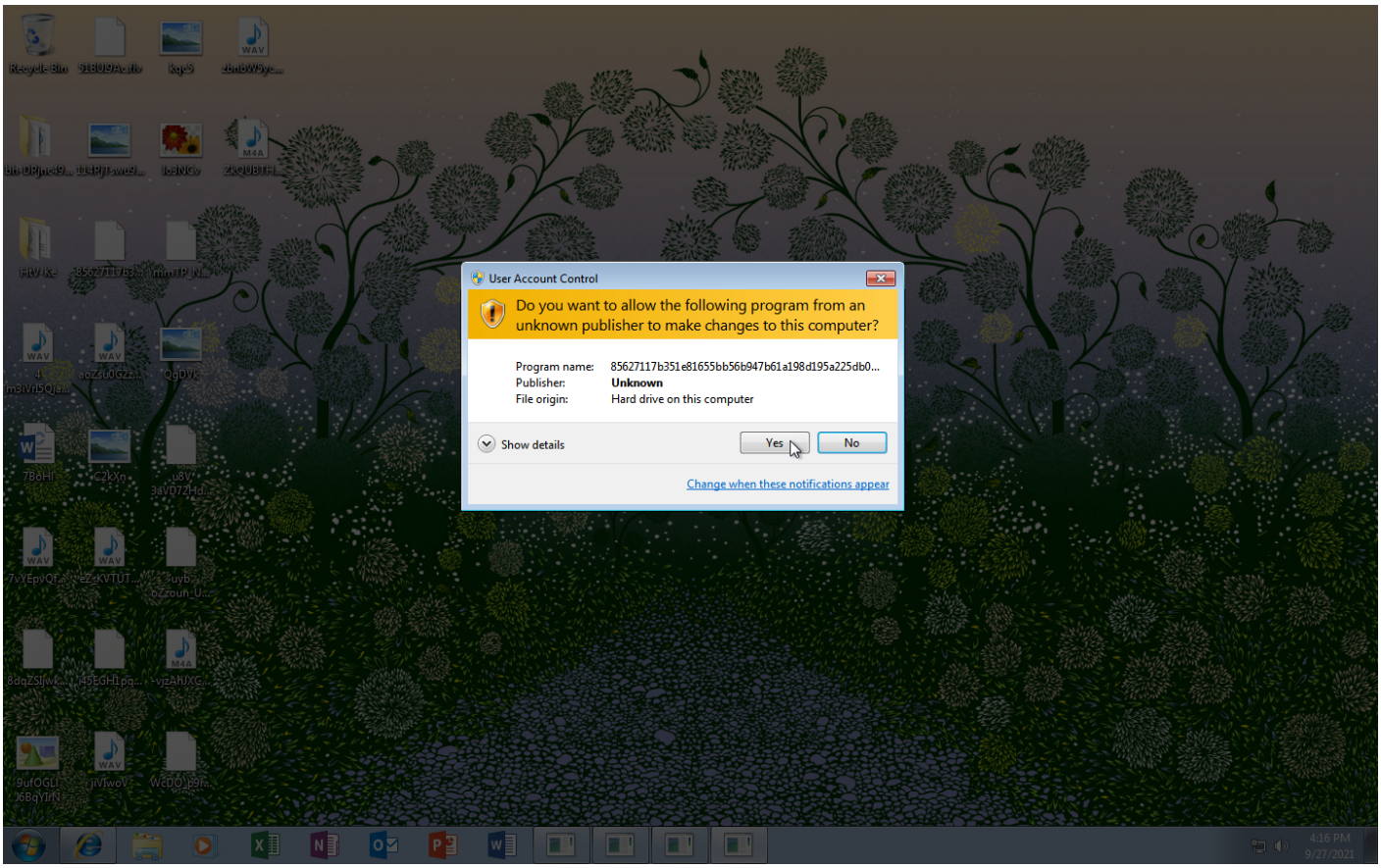
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation			#T1143 Hidden Window	#T1081 Credentials in Files	#T1497 Virtualization/ Sandbox Evasion		#T1119 Automated Collection	#T1090 Connection Proxy		
				#T1497 Virtualization/ Sandbox Evasion	#T1214 Credentials in Registry	#T1012 Query Registry		#T1005 Data from Local System	#T1065 Uncommonly Used Port		
				#T1045 Software Packing	#T1003 Credential Dumping	#T1082 System Information Discovery					
						#T1057 Process Discovery					
						#T1083 File and Directory Discovery					
						#T1124 System Time Discovery					

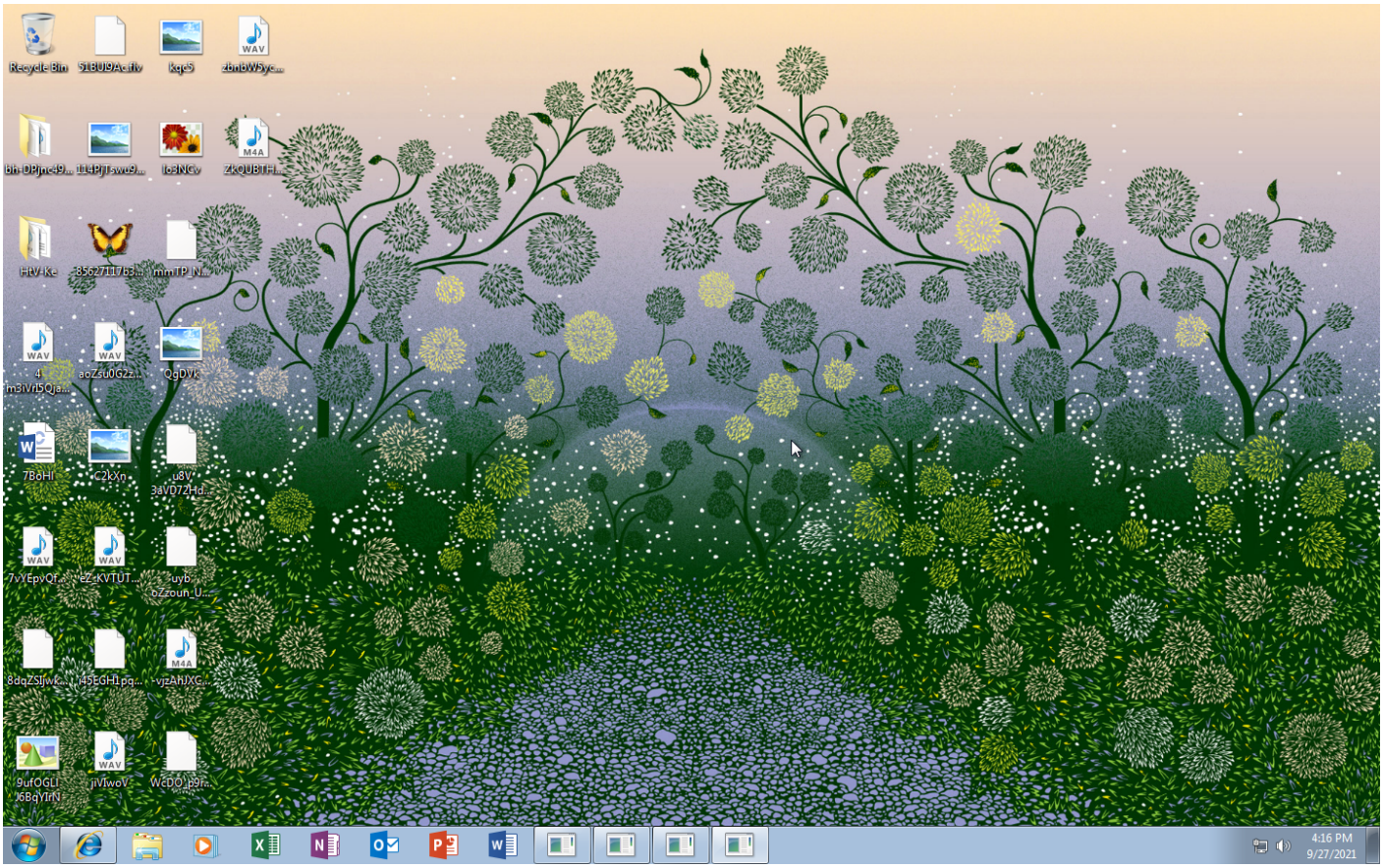
Sample Information

ID	#2780378
MD5	22a2657bb48e3303f6f0a0fd1fdfe441
SHA1	d6a230a732f3d691a7fce60081f30627ffabd33d
SHA256	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac
SSDeep	12288:X52s002Ce2nsnG3/TEbszQ4yejelxJjtaTXOYVgqrmYBF0yl9STO3AbX8bwtxTse:zTIFMF+wGyVDidkAFjHoSa8F+2
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe
File Size	862.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2021-09-27 18:15 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	4
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	1
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	1


User Account Control
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Program name: 85627117b351e81655bb56b947b61a198d195a225db0...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear



NETWORK

General

1.19 KB total sent

891 bytes 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

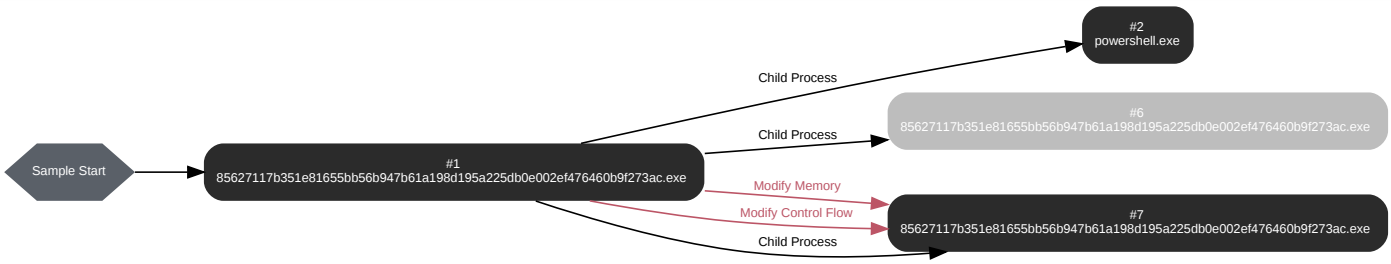
0 sessions, 0 bytes sent, 0 bytes received

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	smtp.zfftcn.com, us2.smtp.mailhostbox.com	NoError	208.91.199.225, 208.91.198.143, 208.91.199.223, 208.91.199.224	us2.smtp.mailhostbox.com	NA
-	smtp.zfftcn.com	-	208.91.199.225, 208.91.198.143, 208.91.199.223, 208.91.199.224		NA

BEHAVIOR

Process Graph



Process #1: 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 49181, Reason: Analysis Target
Unmonitor End Time	End Time: 147498, Reason: Terminated
Monitor duration	98.32s
Return Code	0
PID	3908
Parent PID	1116
Bitness	32 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
-	8.03 KB	790a6af00576b6ee07663cf571a92e5b72379c9d24f3599af1fa9fec8aeb168a	✗
-	108.45 KB	3834c58cec46747331b7e675f28dc2d7498faade8ca3c52b8993203165fcb14e	✗

Host Behavior

Type	Count
Registry	43
Process	6
File	20
Module	87
Window	6
-	3
COM	5
-	1
-	4
-	9
User	1

Process #2: powershell.exe

ID	2
File Name	c:\windows\syswow64\windowspowershell\v1.0\powershell.exe
Command Line	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\kEecfMwgj\Desktop\85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 133413, Reason: Child Process
Unmonitor End Time	End Time: 188932, Reason: Terminated
Monitor duration	55.52s
Return Code	1
PID	4020
Parent PID	3908
Bitness	32 Bit

Host Behavior

Type	Count
System	44
Module	4
File	795
Environment	30
Registry	54
-	39

Process #6: 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe

ID	6
File Name	c:\users\keecfmwgj\desktop\85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 145220, Reason: Child Process
Unmonitor End Time	End Time: 146359, Reason: Terminated
Monitor duration	1.14s
Return Code	4294967295
PID	2756
Parent PID	3908
Bitness	32 Bit

Process #7: 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe

ID	7
File Name	c:\users\keecfmwgj\desktop\85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 145361, Reason: Child Process
Unmonitor End Time	End Time: 290238, Reason: Terminated by Timeout
Monitor duration	144.88s
Return Code	Unknown
PID	2748
Parent PID	3908
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\85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	0xf48	0x400000(4194304)	0x200	✓	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	0xf48	0x402000(4202496)	0x35600	✓	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	0xf48	0x438000(4423680)	0x400	✓	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	0xf48	0x43a000(4431872)	0x200	✓	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	0xf48	0x7efde008(2130567176)	0x4	✓	1
Modify Control Flow	#1: c:\users\keecfmwgj\desktop\85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	0xf48 / 0xab8		-	✓	1

Host Behavior

Type	Count
Registry	124
File	136
Module	75
Window	6
System	16
User	4
-	30
COM	53

Type	Count
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
85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac	C:\Users\kEecfMwgj\Desktop\85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	Sample File	862.00 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
9b13a3ea948a1071a81787aac1930b89e30df22ce13f8ff751f31b5d83e79ffb	C:\Windows\system32\drivers\etc\hosts	Modified File	835 bytes	text/plain	Create, Write, Access	CLEAN
790a6af00576b6ee07663cf571a92e5b72379c9d24f3599af1fa9fec8aeb168a	c:\users\keecfmwgj\appdata\local\gdipfontcachev1.dat	Dropped File	8.03 KB	application/octet-stream	-	CLEAN
3834c58cec46747331b7e675f28dc2d7498faade8ca3c52b8993203165fcb14e	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\85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe.config	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\Desktop\85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	Sample File	Access	CLEAN
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\Desktop\%SystemRoot%\system32\WindowsPowerShell\v1.0\	Accessed File	Access	CLEAN
C:\Windows\system32	Accessed File	Access	CLEAN
C:\Windows	Accessed File	Access	CLEAN
C:\Windows\System32\Wbem	Accessed File	Access	CLEAN
C:\Windows\System32\WindowsPowerShell\v1.0\	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Modules.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Modules.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Modules.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Modules.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Modules.ni.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Modules.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	Accessed File	Read, Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.ni.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.ni.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\Documents\WindowsPowerShell\Modules	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\Modules.psd1	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\Modules.psm1	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\Modules.cdxml	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\Modules.xaml	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\Modules.ni.dll	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\Modules.dll	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	Accessed File	Read, Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\PackageManagement.psd1	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\PackageManagement.psm1	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\PackageManagement.cdxml	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\PackageManagement.xaml	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\PackageManagement.ni.dll	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\PackageManagement.dll	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	Accessed File	Read, Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\en-US\PowerShellGet.psd1	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\en\PowerShellGet.psd1	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	Accessed File	Read, Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSGet.Format.ps1xml	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSGet.Resource.psd1	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSGetModuleInfo.xml	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.psd1	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.psm1	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.cdxml	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.xaml	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.ni.dll	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Modules.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Modules.psm1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Modules.cdxml	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Modules.xaml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Modules.ni.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Modules.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\ISE	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\TroubleshootingPack	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	Accessed File	Read, Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	Accessed File	Read, Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	Accessed File	Read, Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\en-US\Microsoft.PowerShell.Management.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\en\Microsoft.PowerShell.Management.psd1	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\PSGetModuleInfo.xml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Commands.Management.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Commands.Management.dll\Microsoft.PowerShell.Commands.Management.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Commands.Management	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Commands.Management\Microsoft.PowerShell.Commands.Management.dll	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Commands.Management	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Commands.Management\Microsoft.PowerShell.Commands.Management.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Commands.Management	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Commands.Management\Microsoft.PowerShell.Commands.Management.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\en-US\BitsTransfer.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\en\BitsTransfer.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.Format.ps1xml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\PSGetModuleInfo.xml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\Microsoft.BackgroundIntelligentTransfer.Management	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\Microsoft.BackgroundIntelligentTransfer.Management.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\Microsoft.BackgroundIntelligentTransfer.Management.psm1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\Microsoft.BackgroundIntelligentTransfer.Management.cdxml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\Microsoft.BackgroundIntelligentTransfer.Management.xaml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\Microsoft.BackgroundIntelligentTransfer.Management.ni.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\Microsoft.BackgroundIntelligentTransfer.Management.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\Microsoft.BackgroundIntelligentTransfer.Management\Microsoft.BackgroundIntelligentTransfer.Management.psd1	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\Microsoft.BackgroundIntelligentTransfer.Management\Microsoft.BackgroundIntelligentTransfer.Management.psm1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\Microsoft.BackgroundIntelligentTransfer.Management\Microsoft.BackgroundIntelligentTransfer.Management.cdxml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\Microsoft.BackgroundIntelligentTransfer.Management\Microsoft.BackgroundIntelligentTransfer.Management.xaml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\Microsoft.BackgroundIntelligentTransfer.Management\Microsoft.BackgroundIntelligentTransfer.Management.ni.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\Microsoft.BackgroundIntelligentTransfer.Management\Microsoft.BackgroundIntelligentTransfer.Management.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.BackgroundIntelligentTransfer.Management	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.BackgroundIntelligentTransfer.Management\Microsoft.BackgroundIntelligentTransfer.Management.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.BackgroundIntelligentTransfer.Management\Microsoft.BackgroundIntelligentTransfer.Management.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.BackgroundIntelligentTransfer.Management\Microsoft.BackgroundIntelligentTransfer.Management.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.BackgroundIntelligentTransfer.Management\Microsoft.BackgroundIntelligentTransfer.Management.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.BackgroundIntelligentTransfer.Management\Microsoft.BackgroundIntelligentTransfer.Management.ni.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.BackgroundIntelligentTransfer.Management\Microsoft.BackgroundIntelligentTransfer.Management.dll	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.BackgroundIntelligentTransfer.Management	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.BackgroundIntelligentTransfer.Management\Microsoft.BackgroundIntelligentTransfer.Management.psd1	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.BackgroundIntelligentTransfer.Management\Microsoft.BackgroundIntelligentTransfer.Management.psm1	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.BackgroundIntelligentTransfer.Management\Microsoft.BackgroundIntelligentTransfer.Management.cdxml	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.BackgroundIntelligentTransfer.Management\Microsoft.BackgroundIntelligentTransfer.Management.xaml	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.BackgroundIntelligentTransfer.Management\Microsoft.BackgroundIntelligentTransfer.Management.ni.dll	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.BackgroundIntelligentTransfer.Management\Microsoft.BackgroundIntelligentTransfer.Management.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.BackgroundIntelligentTransfer.Management	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.BackgroundIntelligentTransfer.Management\Microsoft.BackgroundIntelligentTransfer.Management.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.BackgroundIntelligentTransfer.Management\Microsoft.BackgroundIntelligentTransfer.Management.psm1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.BackgroundIntelligentTransfer.Management\Microsoft.BackgroundIntelligentTransfer.Management.cdxml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.BackgroundIntelligentTransfer.Management\Microsoft.BackgroundIntelligentTransfer.Management.xaml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.BackgroundIntelligentTransfer.Management\Microsoft.BackgroundIntelligentTransfer.Management.ni.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.BackgroundIntelligentTransfer.Management\Microsoft.BackgroundIntelligentTransfer.Management.dll	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	Accessed File	Read, Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\ISE\ISE.psd1	Accessed File	Read, Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\Microsoft.PowerShell.Archive.psd1	Accessed File	Read, Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\Microsoft.PowerShell.Diagnostics.psd1	Accessed File	Read, Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\Microsoft.PowerShell.Host.psd1	Accessed File	Read, Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\Microsoft.PowerShell.ODataUtils.psd1	Accessed File	Read, Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security\Microsoft.PowerShell.Security.psd1	Accessed File	Read, Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\Microsoft.WSMan.Management.psd1	Accessed File	Read, Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\PSDesiredStateConfiguration.psd1	Accessed File	Read, Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\PSDiagnostics.psd1	Accessed File	Read, Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\en-US\PSDiagnostics.psd1	Accessed File	Access	CLEAN

Reduced dataset

Domain

Domain	IP Address	Country	Protocols	Verdict
smtp.zfftcn.com	208.91.199.223, 208.91.198.143, 208.91.199.224, 208.91.199.225	-	DNS	CLEAN
us2.smtp.mailhostbox.com	208.91.198.143, 208.91.199.223, 208.91.199.224, 208.91.199.225	-	DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
208.91.198.143	smtp.zfftcn.com, us2.smtp.mailhostbox.com	United States	DNS	MALICIOUS
192.168.0.1	-	-	UDP, DNS	CLEAN
208.91.199.225	smtp.zfftcn.com, us2.smtp.mailhostbox.com	United States	DNS, TCP	CLEAN
208.91.199.223	smtp.zfftcn.com, us2.smtp.mailhostbox.com	United States	DNS	CLEAN
208.91.199.224	smtp.zfftcn.com, us2.smtp.mailhostbox.com	United States	DNS	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	powershell.exe, 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE	access	powershell.exe, 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\HARDWARE\DEVICEMAP\Scsi\Scsi Port 0\Scsi Bus 0\Target Id 0\Logical Unit Id 0	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\HARDWARE\Description\System	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\HARDWARE\Description\System\SystemBiosVersion	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\HARDWARE\Description\System\VideoBiosVersion	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\VirtualBox Guest Additions	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Tools	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\HARDWARE\DEVICEMAP\Scsi\Scsi Port 1\Scsi Bus 0\Target Id 0\Logical Unit Id 0	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\HARDWARE\DEVICEMAP\Scsi\Scsi Port 2\Scsi Bus 0\Target Id 0\Logical Unit Id 0	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Disk\Enum	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Disk\Enum\0	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{4D36E968-E325-11CE-BFC1-08002BE10318}\0000	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{4D36E968-E325-11CE-BFC1-08002BE10318}\0000\DriverDesc	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{4D36E968-E325-11CE-BFC1-08002BE10318}\0000\Settings	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{4D36E968-E325-11CE-BFC1-08002BE10318}\0000\Settings\Device Description	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\WMIDisableCOMSecurity	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_PERFORMANCE_DATA	access	powershell.exe, 85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.UseHttpPipeliningAndBufferPooling	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseHttpPipeliningAndBufferPooling	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.UseSafeSynchronousClose	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseSafeSynchronousClose	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.UseStrictRfcInterimResponseHandling	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseStrictRfcInterimResponseHandling	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Uri.AllowDangerousUnicodeDecompositions	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\AllowDangerousUnicodeDecompositions	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Uri.UseStrictIPv6AddressParsing	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseStrictIPv6AddressParsing	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Uri.AllowAllUriEncodingExpansion	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\AllowAllUriEncodingExpansion	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SchSendAuxRecord	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchSendAuxRecord	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SystemDefaultTlsVersions	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.RequireCertificateEKUs	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\RequireCertificateEKUs	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Impersonation Level	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Namespace	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging	access	powershell.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Environment	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Environment__PSLockdownPolicy	read, access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\PowerShell\3\PowerShellEngine	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\PowerShell\3\PowerShellEngine\ApplicationBase	read, access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_CURRENT_USER\Software\FTPWare\COREFTP\Sites\Host	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
\HKEY_CURRENT_USERSoftwareFTPWareCOREFTPSitesPort	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
\HKEY_CURRENT_USERSoftwareFTPWareCOREFTPSitesUser	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
\HKEY_CURRENT_USERSoftwareFTPWareCOREFTPSitesPW	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
\HKEY_CURRENT_USERSoftwareFTPWareCOREFTPSitesName	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Messaging Subsystem\Profiles\9375CFF0413111d3B88A00104B2A6676	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Email	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP Password	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 Password	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTP Password	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP Password	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Email	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP Password	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Server	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\Email	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP Password	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3 Password	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTP Password	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP Password	read, access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_CURRENT_USER\Software\Aerofox\FoxmailPreview	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_CURRENT_USER\Software\Aerofox\Foxmail\V3.1	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\RealVNC\WinVNC4	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Wow6432Node\RealVNC\WinVNC4	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\vncserver	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\RealVNC\vncserver	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\RealVNC\WinVNC4	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\ORL\WinVNC3	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_CURRENT_USER\Software\ORL\WinVNC3	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\TightVNC\Server	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\TightVNC\Server	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\TigerVNC\Server	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_CURRENT_USER\Software\TigerVNC\Server	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Martin Prikryl\WinSCP 2\Sessions	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_CURRENT_USER\Software\RimArts\B2\Settings	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_CURRENT_USER\Software\DownloadManager\Passwords	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_CURRENT_USER\Software\OpenVPN-GUI\configs	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_CURRENT_USER\Software\IncrediMail\Identities	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN
HKEY_CURRENT_USER\Software\Qualcomm\Eudora\CommandLine	access	85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	CLEAN

Process

Process Name	Commandline	Verdict
85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	"C:\Users\kEecfMwgj\Desktop\85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe"	MALICIOUS
85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	"C:\Users\kEecfMwgj\Desktop\85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe"	MALICIOUS
powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\kEecfMwgj\Desktop\85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe"	CLEAN

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

Antivirus (1)

File Type	Threat Name	File Name	Verdict
Sample File	Gen:Variant.Bulz.766082	C:\Users\kEecfMwgj\Desktop\85627117b351e81655bb56b947b61a198d195a225db0e002ef476460b9f273ac.exe	MALICIOUS

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 13:37:06+00:00
Built-in AV Database Records	10469506

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