VMRAY

DYNAMIC ANALYSIS REPORT

#10762756

MALICIOUS

Classifications: Spyware Injector

Threat Names: Mal/Generic-S AgentTesla.v3

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe**
ID	#5007300
MD5	9cef8265c679bafb06f885678ceab7bd
SHA1	ac7faaa7e8439951eaafd8e02007f33a555cd01b
SHA256	18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90
File Size	625.50 KB
Report Created	2022-07-27 01:23 (UTC+2)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (26 rules, 81 matches)

Score	Category	Operation	Count	Classification
5/5	Extracted Configuration	Agent Tesla configuration was extracted	1	Spyware
	• A configuration for Agent Tesla was extracted from artifacts of the dynamic analysis.			
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 #4) installutil.exe.			
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: TigerVNC, FileZilla, OpenVPN, The Bat!, Mozilla Thunderbird, Mozilla Firefox, Internet Explorer, ...l, Cyberfox, Opera Mail, Ipswitch WS_FTP, FTP Navigator, WinSCP, Postbox, TightVNC, SeaMonkey, Microsoft Outlook, Flock, Pocomail.			
4/5	Defense Evasion	Obscures a file's origin	1	-
	• (Process #4) installutil.exe tries to delete zone identifier of file "C:\Users\kEecfMwgj\AppData\Roaming\Acrobat\Acrobat.exe".			
4/5	Injection	Writes into the memory of another process	1	Injector
	• (Process #3) geater.exe modifies memory of (process #4) installutil.exe.			
4/5	Injection	Modifies control flow of another process	1	-
	• (Process #3) geater.exe alters context of (process #4) installutil.exe.			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as Mal/Generic-S.			
2/5	Defense Evasion	Sends control codes to connected devices	7	-
	• (Process #6) wmiprvse.exe controls device "\\.\{71F897D7-EB7C-4D8D-89DB-AC80D9DD2270}" through API DeviceIOControl. • (Process #6) wmiprvse.exe controls device "\\.\{29898C9D-B0A4-4FEF-BDB6-57A562022CEE}" through API DeviceIOControl. • (Process #6) wmiprvse.exe controls device "\\.\{DF4A9D2C-8742-4EB1-8703-D395C4183F33}" through API DeviceIOControl. • (Process #6) wmiprvse.exe controls device "\\.\{8E301A52-AFFA-4F49-B9CA-C79096A1A056}" through API DeviceIOControl. • (Process #6) wmiprvse.exe controls device "\\.\{D798E63F-0CBA-45D6-AA42-58A00E60B2E0}" through API DeviceIOControl. • (Process #6) wmiprvse.exe controls device "\\.\{78032B7E-4968-42D3-9F37-287EA86C0AAA}" through API DeviceIOControl. • (Process #6) wmiprvse.exe controls device "\\.\{68F1467C-143D-484A-87A1-65BCBB1B2D48}" through API DeviceIOControl.			
2/5	Data Collection	Reads sensitive browser data	9	-
	• (Process #4) installutil.exe tries to read sensitive data of web browser "Opera" by file. • (Process #4) installutil.exe tries to read sensitive data of web browser "BlackHawk" by file. • (Process #4) installutil.exe tries to read credentials of web browser "Internet Explorer" by reading from the system's credential vault. • (Process #4) installutil.exe tries to read sensitive data of web browser "k-Meleon" by file. • (Process #4) installutil.exe tries to read sensitive data of web browser "Comodo IceDragon" by file. • (Process #4) installutil.exe tries to read sensitive data of web browser "Flock" by file. • (Process #4) installutil.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file. • (Process #4) installutil.exe tries to read sensitive data of web browser "Cyberfox" by file. • (Process #4) installutil.exe tries to read sensitive data of web browser "Mozilla Firefox" by file.			
2/5	Data Collection	Reads sensitive mail data	7	-

Score	Category	Operation	Count	Classification
	• (Process #4) installutil.exe tries to read sensitive data of mail application "Mozilla Thunderbird" by file. • (Process #4) installutil.exe tries to read sensitive data of mail application "Postbox" by file. • (Process #4) installutil.exe tries to read sensitive data of mail application "Microsoft Outlook" by registry. • (Process #4) installutil.exe tries to read sensitive data of mail application "Opera Mail" by file. • (Process #4) installutil.exe tries to read sensitive data of mail application "The Bat!" by file. • (Process #4) installutil.exe tries to read sensitive data of mail application "IncrediMail" by registry. • (Process #4) installutil.exe tries to read sensitive data of mail application "Pocomail" by file.			
2/5	Data Collection	Reads sensitive application data	6	-
	• (Process #4) installutil.exe tries to read sensitive data of application "Internet Download Manager" by registry. • (Process #4) installutil.exe tries to read sensitive data of application "SeaMonkey" by file. • (Process #4) installutil.exe tries to read sensitive data of application "OpenVPN" by registry. • (Process #4) installutil.exe tries to read sensitive data of application "TightVNC" by registry. • (Process #4) installutil.exe tries to read sensitive data of application "TigerVNC" by registry. • (Process #4) installutil.exe tries to read sensitive data of application "WinSCP" by registry.			
2/5	Data Collection	Reads sensitive ftp data	4	-
	• (Process #4) installutil.exe tries to read sensitive data of ftp application "CoreFTP" by registry. • (Process #4) installutil.exe tries to read sensitive data of ftp application "Ipswitch WS_FTP" by file. • (Process #4) installutil.exe tries to read sensitive data of ftp application "FTP Navigator" by file. • (Process #4) installutil.exe tries to read sensitive data of ftp application "FileZilla" by file.			
2/5	Discovery	Queries OS version via WMI	1	-
	• (Process #4) installutil.exe queries OS version via WMI.			
2/5	Discovery	Executes WMI query	2	-
	• (Process #4) installutil.exe executes WMI query: select * from Win32_OperatingSystem. • (Process #4) installutil.exe executes WMI query: SELECT * FROM Win32_Processor.			
2/5	Discovery	Collects hardware properties	1	-
	• (Process #4) installutil.exe queries hardware properties via WMI.			
1/5	Privilege Escalation	Enables process privilege	3	-
	• (Process #1) 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe enables process privilege "SeDebugPrivilege". • (Process #3) geater.exe enables process privilege "SeDebugPrivilege". • (Process #4) installutil.exe enables process privilege "SeDebugPrivilege".			
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #3) geater.exe starts (process #3) geater.exe with a hidden window.			
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #3) geater.exe reads from (process #3) geater.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #3) geater.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.			
1/5	Persistence	Installs system startup script or application	1	-
	• (Process #4) installutil.exe adds "C:\Users\kEecfMwgj\AppData\Roaming\Acrobat\Acrobat.exe" to Windows startup via registry.			

Score	Category	Operation	Count	Classification
1/5	Discovery	Possibly does reconnaissance	22	-
	• (Process #4) installutil.exe tries to gather information about application "Postbox" by file. • (Process #4) installutil.exe tries to gather information about application "SeaMonkey" by file. • (Process #4) installutil.exe tries to gather information about application "Opera Mail" by file. • (Process #4) installutil.exe tries to gather information about application "blackHawk" by file. • (Process #4) installutil.exe tries to gather information about application "FlashFXP" by file. • (Process #4) installutil.exe tries to gather information about application "Qualcomm Eudora" by registry. • (Process #4) installutil.exe tries to gather information about application "icecat" by file. • (Process #4) installutil.exe tries to gather information about application "k-Meleon" by file. • (Process #4) installutil.exe tries to gather information about application "RealVNC" by registry. • (Process #4) installutil.exe tries to gather information about application "TightVNC" by registry. • (Process #4) installutil.exe tries to gather information about application "TigerVNC" by registry. • (Process #4) installutil.exe tries to gather information about application "WS_FTP" by file. • (Process #4) installutil.exe tries to gather information about application "Foxmail" by registry. • (Process #4) installutil.exe tries to gather information about application "Comodo IceDragon" by file. • (Process #4) installutil.exe tries to gather information about application "FTP Navigator" by file. • (Process #4) installutil.exe tries to gather information about application "Flock" by file. • (Process #4) installutil.exe tries to gather information about application "The Bat!" by file. • (Process #4) installutil.exe tries to gather information about application "WinSCP" by registry. • (Process #4) installutil.exe tries to gather information about application "Cyberfox" by file. • (Process #4) installutil.exe tries to gather information about application "Mozilla Firefox" by file. • (Process #4) installutil.exe tries to gather information about application "FileZilla" by file. • (Process #4) installutil.exe tries to gather information about application "Pocomail" by file.			
1/5	Network Connection	Performs DNS request	2	-
	• (Process #1) 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe resolves host name "www.google.com" to IP "142.250.185.68". • (Process #4) installutil.exe resolves host name "multimetals.cfd" to IP "192.185.37.183".			
1/5	Network Connection	Connects to remote host	3	-
	• (Process #3) geater.exe opens an outgoing TCP connection to host "142.250.185.68:443". • (Process #4) installutil.exe opens an outgoing TCP connection to host "192.185.37.183:587". • (Process #1) 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe opens an outgoing TCP connection to host "142.250.185.68:443".			
1/5	Network Connection	Tries to connect using an uncommon port	1	-
	• (Process #4) installutil.exe tries to connect to TCP port 587 at 192.185.37.183.			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #4) installutil.exe resolves 53 API functions by name.			
1/5	Execution	Executes dropped PE file	1	-
	• Executes dropped file "C:\Users\kEecfMwgj\AppData\Roaming\Acrobat\Acrobat.exe".			
-	Trusted	Known clean file	1	-
	• File "C:\Users\kEecfMwgj\AppData\Roaming\Acrobat\Acrobat.exe" is a known clean file.			
-	Trusted	File has embedded known clean URL	1	-
	• Extracted URL "https://translate.google.de/?hl=de&tab=wT" is a known clean URL.			

Malware Configuration: AgentTesla

Metadata	Key	Extracted Value
Email Address	Tags	Sender
	Value	logs@multimetals.cfd
	Tags	Recipient
	Value	logs@multimetals.cfd
URL	Url	asset@multimetals.cfd
	Tags	SMTP Server
	Username	logs@multimetals.cfd
	Password	multimetals.cfd
Encryption Key	Key	qg==
	Algorithm	XOR

Mitre ATT&CK Matrix

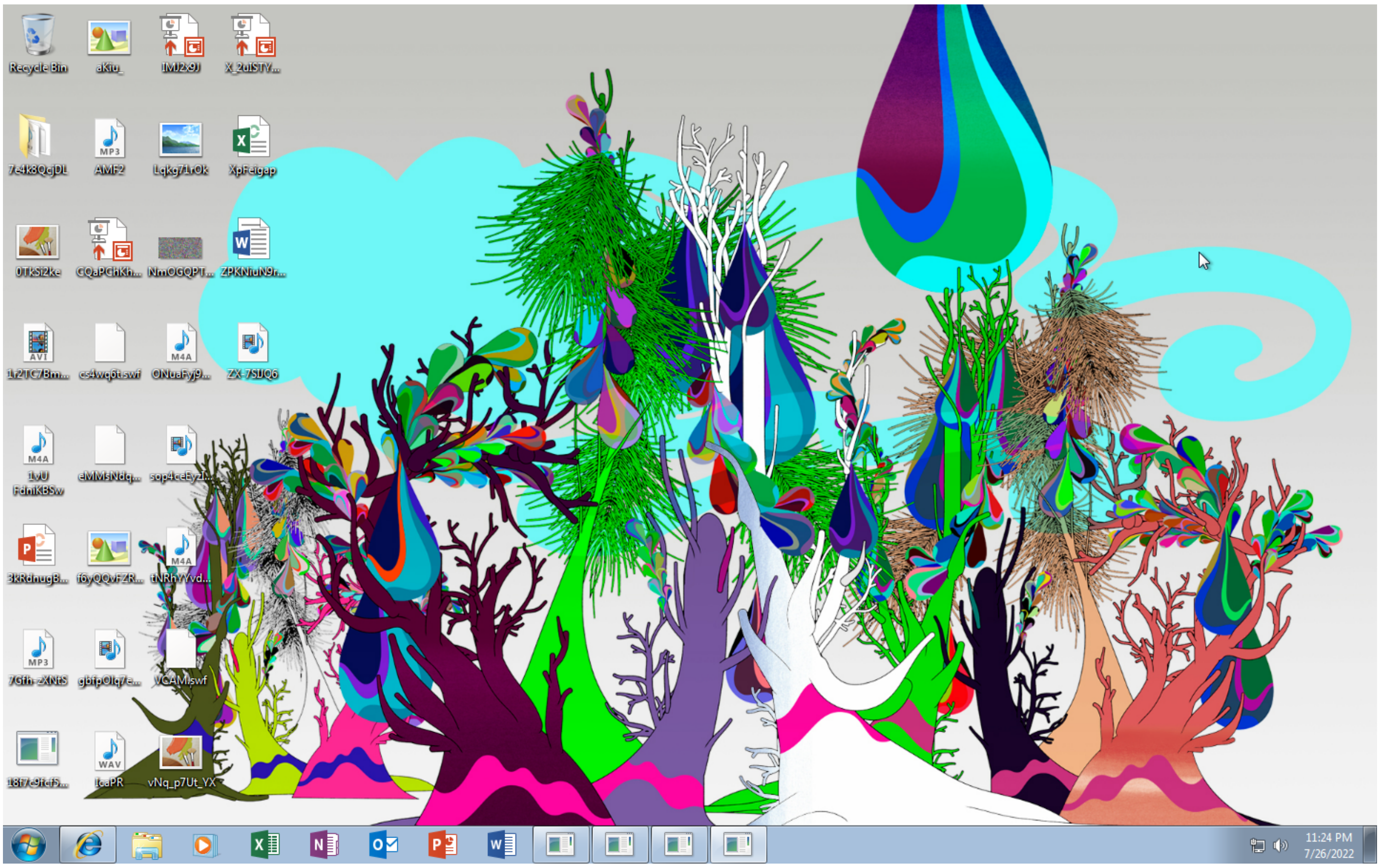
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation	#T1060 Registry Run Keys / Startup Folder		#T1143 Hidden Window	#T1081 Credentials in Files	#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			
				#T1112 Modify Registry	#T1003 Credential Dumping	#T1082 System Information Discovery					
				#T1096 NTFS File Attributes							

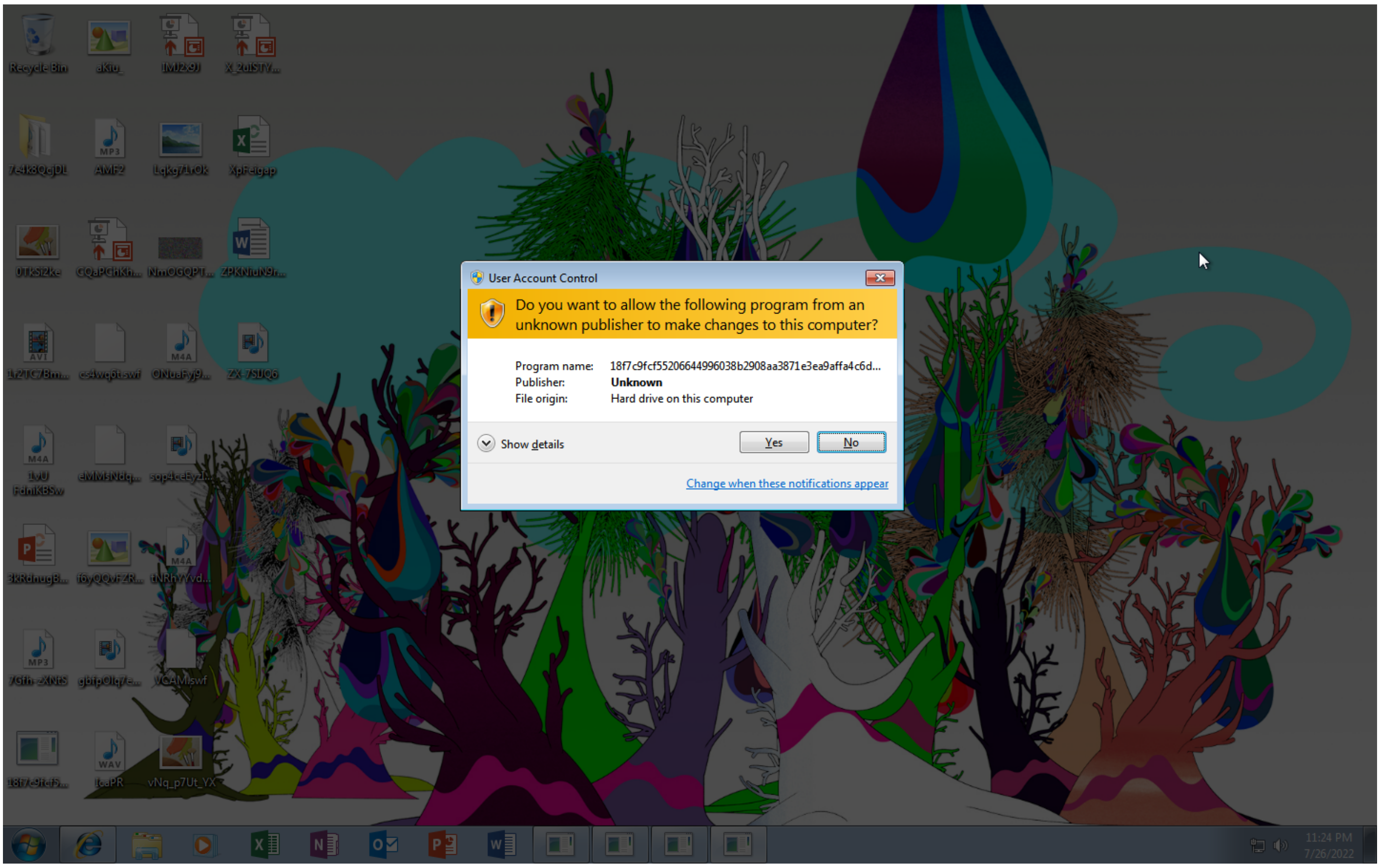
Sample Information

ID	#5007300
MD5	9cef8265c679bafb06f885678ceab7bd
SHA1	ac7faaa7e8439951eaafd8e02007f33a555cd01b
SHA256	18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90
SSDeep	12288:7yJTxDWRQLg9r91BXxQ/q22ZzGSf1q6B0sQuc9G:7ynWRQerDxxs32NG61q6PQuc
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe
File Size	625.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2022-07-27 01:23 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	6
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	2

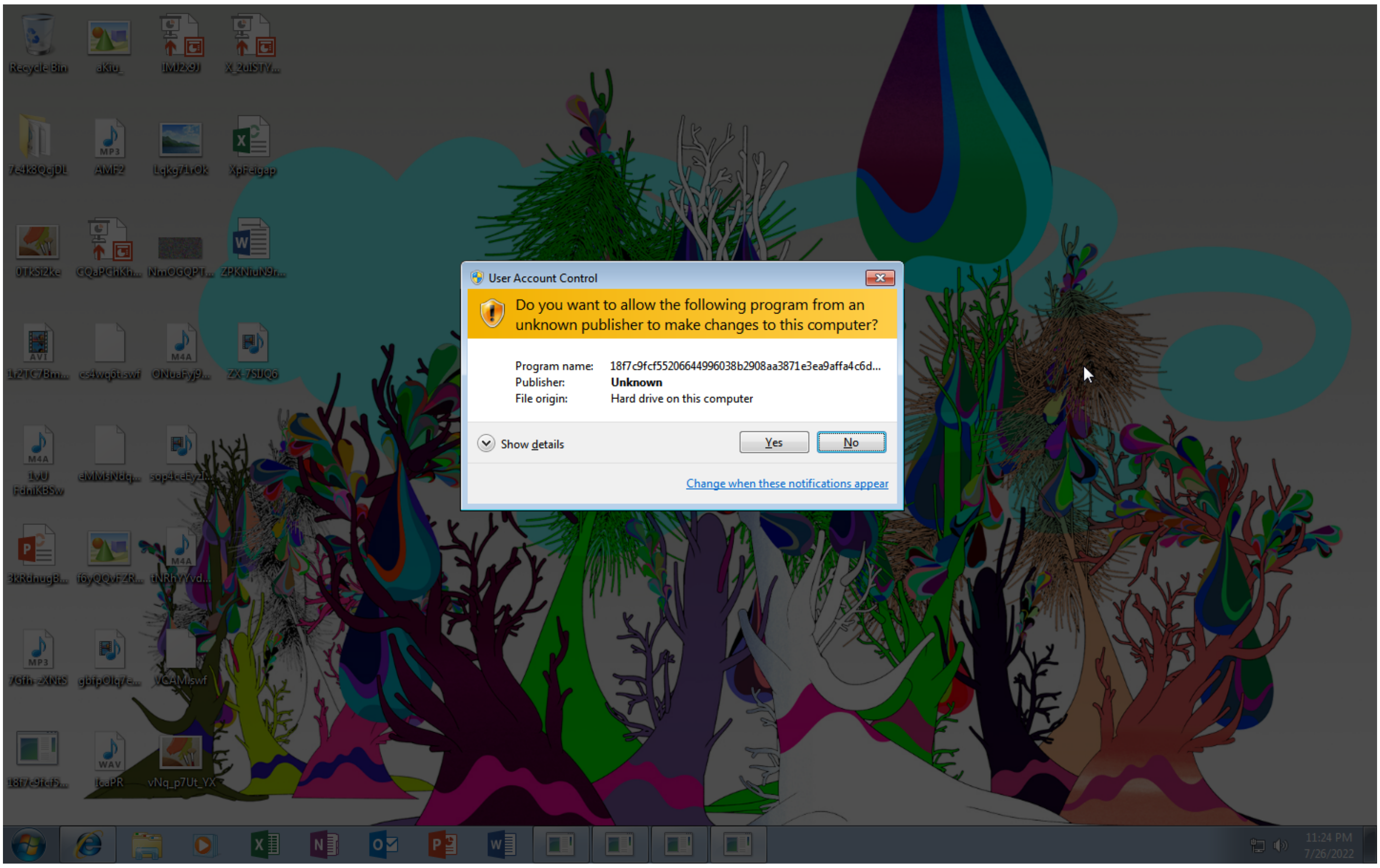




User Account Control

Do you want to allow the following program from an unknown publisher to make changes to this computer?

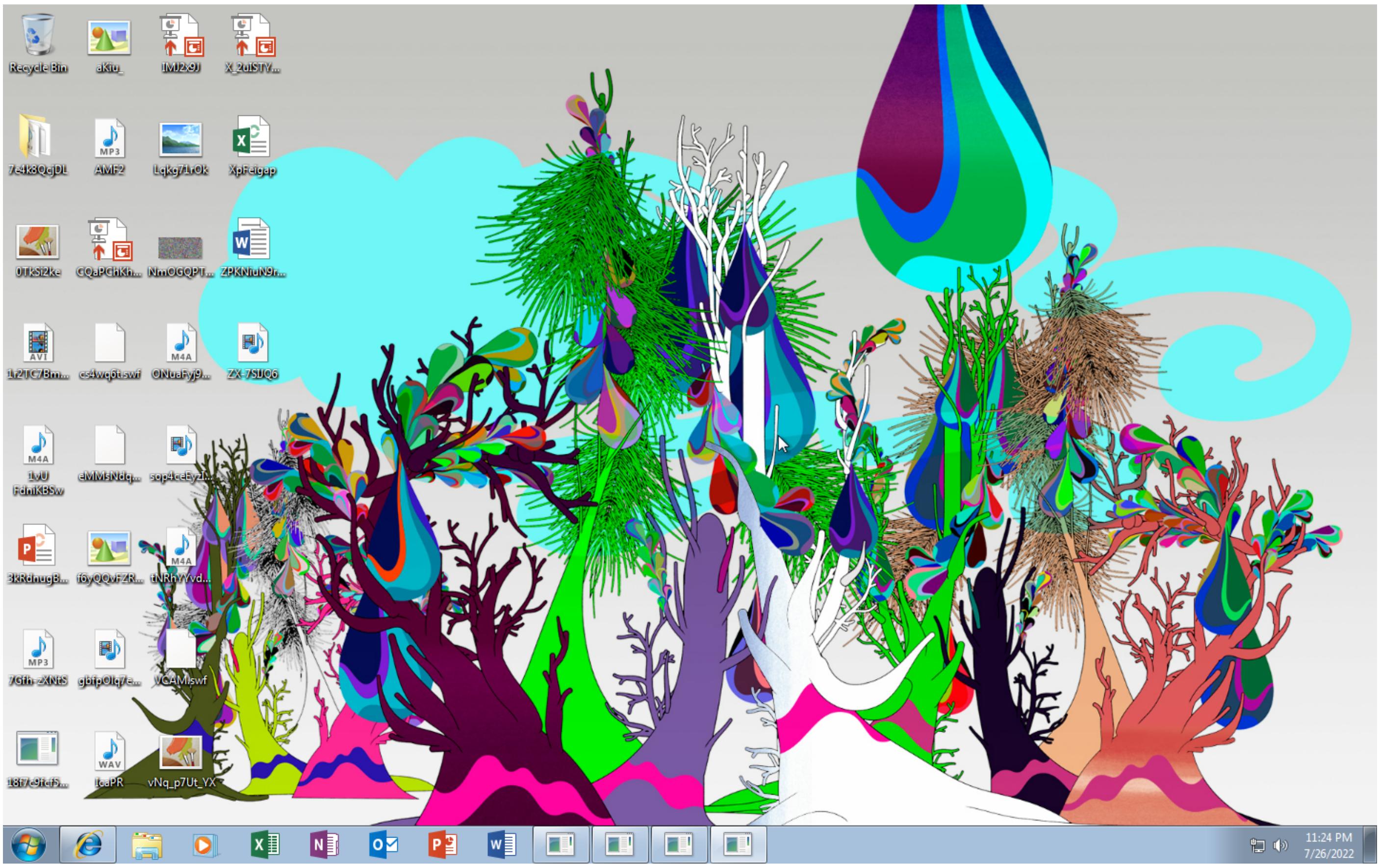
Program name: 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d...
Publisher: **Unknown**
File origin: Hard drive on this computer



User Account Control

Do you want to allow the following program from an unknown publisher to make changes to this computer?

Program name: 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d...
Publisher: **Unknown**
File origin: Hard drive on this computer



Screenshots truncated

NETWORK

General

4.33 KB total sent

117.53 KB total received

4 ports 53, 587, 443, 445

3 contacted IP addresses

29 URLs extracted

2 files downloaded

0 malicious hosts detected

DNS

2 DNS requests for 2 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

1 URLs contacted, 1 servers

2 sessions, 2.03 KB sent, 115.42 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://video.google.de/?hl=de&tab=wv	-	-		0 bytes	NA
GET	http://www.google.de/history/optout?hl=de	-	-		0 bytes	NA
GET	http://www.google.de/preferences?hl=de	-	-		0 bytes	NA
GET	https://accounts.google.com/ServiceLogin?hl=de&passive=true&continue=https://www.google.com/&ec=GAZAAQ	-	-		0 bytes	NA
GET	https://drive.google.com/?tab=wo	-	-		0 bytes	NA
GET	https://mail.google.com/mail/?tab=wm	-	-		0 bytes	NA
GET	https://news.google.com/?tab=wn	-	-		0 bytes	NA
GET	https://www.blogger.com/?tab=wj	-	-		0 bytes	NA
GET	https://plusone.google.com/u/0	-	-		0 bytes	NA
GET	https://www.google.com/setprefdomain?prefdom=DE&prev=https://www.google.de/&sig=K_T2w9tLOZa98tlBqgTOW3r-7Gz8c%3D	-	-		0 bytes	NA
GET	https://www.google.com/finance?tab=we	-	-		0 bytes	NA
GET	https://www.google.com/setprefdomain?prefdom=DE&prev=https://www.google.de/&sig=K_XUe_WfBa4scu8otld0a1lCf7fHs%3D	-	-		0 bytes	NA
GET	https://maps.google.de/maps?hl=de&tab=wl	-	-		0 bytes	NA
GET	https://docs.google.com/document/?usp=docs_alc	-	-		0 bytes	NA
GET	https://photos.google.com/?tab=wq&pageId=none	-	-		0 bytes	NA
GET	https://lh3.googleusercontent.com/ogw/default-user=s96	-	-		0 bytes	NA

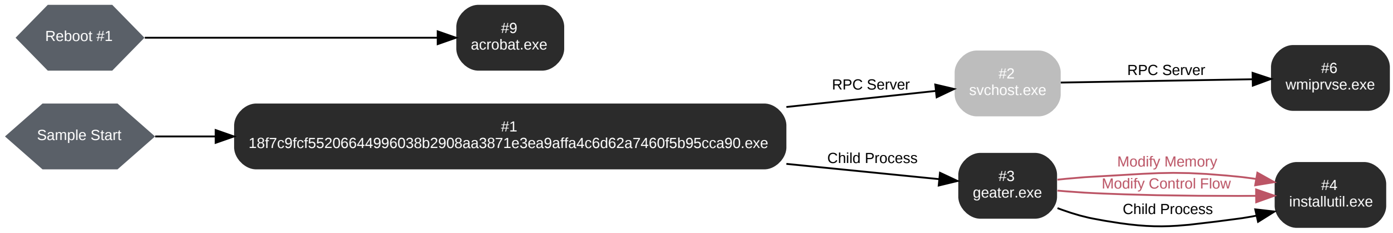
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	https://lh3.googleusercontent.com/ogw/default-user=s24	-	-		0 bytes	NA
GET	https://www.google.de/shopping?hl=de&source=og&tab=wf	-	-		0 bytes	NA
GET	https://www.google.de/intl/de/about/products?tab=wh	-	-		0 bytes	NA
GET	https://www.google.de/webhp?tab=ww	-	-		0 bytes	NA
GET	https://www.google.de/imghp?hl=de&tab=wi	-	-		0 bytes	NA
GET	https://translate.google.de/?hl=de&tab=wT	-	-		0 bytes	NA
GET	https://books.google.de/?hl=de&tab=wp	-	-		0 bytes	NA
GET	https://apis.google.com	-	-		0 bytes	NA
GET	https://www.youtube.com/?gl=DE&tab=w1	-	-		0 bytes	NA
GET	https://calendar.google.com/calendar?tab=wc	-	-		0 bytes	NA
GET	https://www.gstatic.com	-	-		0 bytes	NA
GET	https://play.google.com/?hl=de&tab=w8	-	-		0 bytes	NA
GET	https://www.google.com	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	www.google.com	NO_ERROR	142.250.185.68		NA
A	multimetals.cfd	NO_ERROR	192.185.37.183		NA

BEHAVIOR

Process Graph



Process #1: 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 44712, Reason: Analysis Target
Unmonitor End Time	End Time: 110483, Reason: Terminated
Monitor duration	65.77s
Return Code	0
PID	4028
Parent PID	1928
Bitness	32 Bit

Dropped Files (3)

File Name	File Size	SHA256	YARA Match
-	108.45 KB	61602c8a9d8f81c3d33068c5fc846c4cddb9cd00ed033a0f8a456dfd32582629	✖
C:\Users\kEecfMwgj\Desktop\18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	625.50 KB	18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90	✖
-	8.03 KB	790a6af00576b6ee07663cf571a92e5b72379c9d24f3599af1fa9fec8aeb168a	✖

Host Behavior

Type	Count
Registry	56
File	28
-	10
User	1
Module	29
System	47
Environment	9
-	1
Window	6
Process	1

Network Behavior

Type	Count
HTTPS	1
DNS	1
TCP	1

Process #2: svchost.exe

ID	2
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k netsvcs
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 80613, Reason: RPC Server
Unmonitor End Time	End Time: 289902, Reason: Terminated by timeout
Monitor duration	209.29s
Return Code	Unknown
PID	864
Parent PID	4028
Bitness	64 Bit

Process #3: geater.exe

ID	3
File Name	c:\users\keecfmwgj\appdata\local\temp\geater.exe
Command Line	"C:\Users\kEecfMwgj\AppData\Local\Temp\geater.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 108718, Reason: Child Process
Unmonitor End Time	End Time: 196669, Reason: Terminated
Monitor duration	87.95s
Return Code	0
PID	2704
Parent PID	4028
Bitness	32 Bit

Host Behavior

Type	Count
Registry	56
File	31
-	13
User	1
Module	931
System	49
Environment	12
-	1
Window	6
Process	1
-	3
-	9

Network Behavior

Type	Count
HTTPS	1
TCP	1

Process #4: installutil.exe

ID	4
File Name	c:\windows\microsoft.net\framework\v4.0.30319\installutil.exe
Command Line	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 152576, Reason: Child Process
Unmonitor End Time	End Time: 235445, Reason: Terminated
Monitor duration	82.87s
Return Code	1073807364
PID	2856
Parent PID	2704
Bitness	32 Bit

Injection Information (6)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#3: c:\users\keecfmwgj\appdata\local\temp\geater.exe	0xa94	0x400000(4194304)	0x200	✔	1
Modify Memory	#3: c:\users\keecfmwgj\appdata\local\temp\geater.exe	0xa94	0x402000(4202496)	0x33e00	✔	1
Modify Memory	#3: c:\users\keecfmwgj\appdata\local\temp\geater.exe	0xa94	0x436000(4415488)	0x600	✔	1
Modify Memory	#3: c:\users\keecfmwgj\appdata\local\temp\geater.exe	0xa94	0x438000(4423680)	0x200	✔	1
Modify Memory	#3: c:\users\keecfmwgj\appdata\local\temp\geater.exe	0xa94	0x7efde008(2130567176)	0x4	✔	1
Modify Control Flow	#3: c:\users\keecfmwgj\appdata\local\temp\geater.exe	0xa94 / 0xb2c	0x435d3e(4414782)	-	✔	1

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\AppData\Roaming\Acrobat\Acrobat.exe	40.15 KB	af5cbd35c7d8dea7d879113fda61b0f64ac6618bcdae15c0c732a018babf68ee	✖

Host Behavior

Type	Count
-	32
Registry	126
File	198
User	4
Module	73
System	13
COM	44
Environment	37
-	2

Type	Count
Mutex	2
-	1
Window	3

Network Behavior

Type	Count
DNS	1
TCP	1

Process #6: wmiprvse.exe

ID	6
File Name	c:\windows\system32\wbem\wmiprvse.exe
Command Line	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 199253, Reason: RPC Server
Unmonitor End Time	End Time: 289902, Reason: Terminated by timeout
Monitor duration	90.65s
Return Code	Unknown
PID	3332
Parent PID	864
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Registry	4
Module	39
File	15
-	14

Process #9: acrobat.exe

ID	9
File Name	c:\users\keecfmwgj\appdata\roaming\acrobat\acrobat.exe
Command Line	"C:\Users\kEecfMwgj\AppData\Roaming\Acrobat\Acrobat.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 276441, Reason: Autostart
Unmonitor End Time	End Time: 283624, Reason: Terminated
Monitor duration	7.18s
Return Code	4294967295
PID	1876
Parent PID	1740
Bitness	32 Bit

Host Behavior

Type	Count
Registry	1
File	31
Module	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90	C:\Users\kEecfMwgj\Desktop\18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe, C:\Users\kEecfMwgj\AppData\Local\Temp\geater.exe	Sample File	625.50 KB	application/vnd.microsoft.portable-executable	Access, Create, Delete, Write	MALICIOUS
61602c8a9d8f81c3d33068c5fc846c4cddb9cd00ed033a0f8a456dfd32582629	-	Dropped File	108.45 KB	application/octet-stream	-	CLEAN
790a6af00576b6ee07663cf571a92e5b72379c9d24f3599af1fa9fec8aeb168a	-	Dropped File	8.03 KB	application/octet-stream	-	CLEAN
2ab43247d3d367bcfb779e1e167b252a3f54e7046dad71abc2bd4c2d66e16c7d	-	Downloaded File	49.02 KB	text/html	-	CLEAN
af5cbd35c7d8dea7d879113fda61b0f64ac6618bcdae15c0c732a018babf68ee	C:\Users\kEecfMwgj\AppData\Roaming\Acrobat\Acrobat.exe	Dropped File	40.15 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	CLEAN
3a45c4ff7bc28dc34f596e124dae411940e2215b6ce74bef76c9a5a005f80dc4	-	Downloaded File	49.11 KB	text/html	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\AppData\Local\Temp\geater.exe	Dropped File, Accessed File, VM File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	Sample File, Accessed File, VM File	Access, Delete	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Flock\Browser\	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\96f7edb07b12303f0ec2595c7f3778c7\System.Configuration.ni.dll	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\ntdll.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Acrobat\Acrobat.exe.config	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\c9a4cbc00f690a9e3cddfc400f6e85bb\System.Windows.Forms.ni.dll	Accessed File	Access	CLEAN
\\.\{2CAA64ED-BAA3-4473-B637-DEC65A14C8AA}	Accessed File	Access	CLEAN
C:\Program Files (x86)\uvnc bvba\UltraVNC\ultravnc.ini	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Web\8e86e9948f7dcebce93d5df6073700ba\System.Web.ni.dll	Accessed File	Access	CLEAN
C:\Storage\	Accessed File	Access	CLEAN
C:\Windows\System32\wshtcpip.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WINNSI.DLL	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\bcryptprimitives.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Elements Browser\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Moonchild Productions\Pale Moon\profiles.ini	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\AppData\Roaming\Mozilla\icecat\profiles.ini	Accessed File	Access	CLEAN
C:\Windows\system32\USERENV.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Tencent\QQBrowser\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Coowon\Coowon\User Data	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clrjit.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Chromium\User Data	Accessed File	Access	CLEAN
C:\Windows\syswow64\psapi.dll	Accessed File	Access	CLEAN
C:\Windows\system32\winhttp.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\Desktop\Folder.lst	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\7Star\7Star\User Data	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\FTPGetter\servers.xml	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\The Bat!	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\360Chrome\Chrome\User Data	Accessed File	Access	CLEAN
C:\Windows\system32\IPHLPAPI.DLL	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Trillian\users\global\accounts.dat	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\15af16d373cf0528cb74fc73d365fdbf\System.Xml.ni.dll	Accessed File	Access	CLEAN
C:\Windows\syswow64\MSCTF.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Torch\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\K-Meleon\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Postbox\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\geater.exe.config	Accessed File	Access	CLEAN
C:\Windows\system32\IMM32.DLL	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\liebao\User Data	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\schannel.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Mailbird\Store\Store.db	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\K-Meleon\profiles.ini	Accessed File	Access	CLEAN
\\.\{DF4A9D2C-8742-4EB1-8703-D395C4183F33}	Accessed File	Access	CLEAN
C:\Windows\system32\rasadhlp.dll	Accessed File	Access	CLEAN
C:\Windows\system32\api-ms-win-core-synch-l1-2-0.DLL	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll	Accessed File	Access	CLEAN
\\.\{9A399D81-2EAD-4F23-BCDD-637FC13DCD51}	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\AppData\Local\Comodo\Dragon\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Comodo\IceDragon\profiles.ini	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsCodecs.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Tencent\QQBrowser\User Data\Default\EncryptedStorage	Accessed File	Access	CLEAN
C:\Windows\syswow64\USER32.dll	Accessed File	Access	CLEAN
C:\Windows\syswow64\WS2_32.dll	Accessed File	Access	CLEAN
C:\Windows\system32\dhcpcsvc.DLL	Accessed File	Access	CLEAN
C:\Windows\syswow64\MSASN1.dll	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\sechost.dll	Accessed File	Access	CLEAN
C:\Windows\system32\dhcpcsvc6.DLL	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\FileZilla\recentservers.xml	Accessed File	Access	CLEAN
\\.\{E43D242B-9EAB-4626-A952-46649FBB939A}	Accessed File	Access	CLEAN
C:\ProgramData\FlashFXP\	Accessed File	Access	CLEAN
C:\Windows\system32\VCRUNTIME140_CLR0400.dll	Accessed File	Access	CLEAN
C:\Windows\syswow64\OLEAUT32.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\MSCOREE.DLL	Accessed File	Access	CLEAN
\\.\{71F897D7-EB7C-4D8D-89DB-AC80D9DD2270}	Accessed File	Access	CLEAN
C:\Windows\system32\credssp.dll	Accessed File	Access	CLEAN
\\.\{5C264C78-4D74-46FF-BC21-C933DE51C5DF}	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\QIP Surf\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\NETGATE Technologies\BlackHawk\	Accessed File	Access	CLEAN
C:\Windows\syswow64\USP10.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Postbox\profiles.ini	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	Accessed File	Access, Read	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\36eaccfde177c2e7b93b8dbdde4e012a\mscorlib.ni.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\a891970b44db9e340c3ef3efa95b793c\Microsoft.VisualBasic.ni.dll	Accessed File	Access	CLEAN
\\.\{954905E5-5ED1-4BAF-AC14-2C2B8B445E08}	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Iridium\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\falkon\profiles\profiles.ini	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Acrobat	Accessed File	Access, Create	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.Config	Accessed File	Access, Read	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\31fae3290fad30c31c98651462d22724\System.Core.ni.dll	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\geater.exe\:Zone.Identifier	Accessed File	Access, Delete	CLEAN
C:\Windows\system32\RpcRtRemote.dll	Accessed File	Access	CLEAN
C:\Windows\system32\rsaenh.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\VirtualStore\Program Files\Foxmail\mail\	Accessed File	Access	CLEAN
\\.\{68F1467C-143D-484A-87A1-65BCBB1B2D48}	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Vivaldi\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Pocomail\accounts.ini	Accessed File	Access	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Sputnik\Sputnik\User Data	Accessed File	Access	CLEAN
C:\mail\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Comodo\IceDragon\	Accessed File	Access	CLEAN
\\.\{8E301A52-AFFA-4F49-B9CA-C79096A1A056}	Accessed File	Access	CLEAN
\\.\{2E05A730-9200-401C-93EB-834FDA0A8400}	Accessed File	Access	CLEAN
C:\Windows\system32\webio.dll	Accessed File	Access	CLEAN
C:\Windows\system32\secur32.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\BraveSoftware\Brave-Browser\User Data	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\2c3c912ea8f058f9d04c4650128feb3f\System.ni.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\FlashFXP\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Google\Chrome\User Data\	Accessed File	Access	CLEAN
C:\Windows\syswow64\ole32.dll	Accessed File	Access	CLEAN
C:\Windows\system32\rasman.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Amigo\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Mozilla\Firefox\profiles.ini	Accessed File	Access	CLEAN
C:\Windows\syswow64\LPK.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Orbitum\User Data	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Opera Software\Opera Stable	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\f7568d7f1b9d356f64779b4c0927cfb3\System.Drawing.ni.dll	Accessed File	Access	CLEAN
C:\Windows\system32\rtutils.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Psi+\profiles	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\CocCoc\Browser\User Data	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\syswow64\RPCRT4.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Kometa\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Psi\profiles	Accessed File	Access	CLEAN
C:\Windows\system32\CRYPTSP.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\uCozMedia\Uran\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Ipswitch\WS_FTP\Sites\ws_ftp.ini	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Credentials\	Accessed File	Access	CLEAN
C:\Windows\system32\bcrypt.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Moonchild Productions\Pale Moon\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\8pecxstudios\Cyberfox\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\MapleStudio\ChromePlus\User Data	Accessed File	Access	CLEAN
C:\Program Files (x86)\UltraVNC\ultravnc.ini	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\CentBrowser\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp	Accessed File	Access	CLEAN
C:\Program Files\Private Internet Access\data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\VirtualStore\Program Files (x86)\Foxmail\mail\	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\nlssorting.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Mozilla\icecat\	Accessed File	Access	CLEAN
C:\Windows\syswow64\KERNEL32.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\NordVPN	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Edge\User Data	Accessed File	Access	CLEAN
C:\Windows\system32\ucrtbase_clr0400.dll	Accessed File	Access	CLEAN
C:\Windows\system32\ncrypt.dll	Accessed File	Access	CLEAN
C:\Windows\system32\profapi.dll	Accessed File	Access	CLEAN
C:\Windows\system32\api-ms-win-core-xstate-l2-1-0.dll	Accessed File	Access	CLEAN
C:\Windows\system32\mswsock.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\UCBrowser\	Accessed File	Access	CLEAN
C:\Windows\syswow64\SspiCli.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Mozilla\SeaMonkey\profiles.ini	Accessed File	Access	CLEAN
c:\users\keecfmwgj\appdata\local\gdipfontcachev1.dat	Dropped File	-	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Claws-mail\clawsrc	Accessed File	Access	CLEAN
C:\Windows\System32\wship6.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Waterfox\profiles.ini	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\Desktop\18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe\:Zone.Identifier	Accessed File	Access, Delete	CLEAN

Reduced dataset

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://play.google.com/?hl=de&tab=w8	-	-	-	-	CLEAN
https://books.google.de/?hl=de&tab=wp	-	-	-	-	CLEAN
https://www.blogger.com/?tab=wj	-	-	-	-	CLEAN
https://www.google.com	-	142.250.185.68	-	GET	CLEAN
https://www.gstatic.com	-	-	-	-	CLEAN
https://www.google.de/intl/de/about/products?tab=wh	-	-	-	-	CLEAN
https://www.google.com/finance?tab=we	-	142.250.185.68	-	-	CLEAN
https://www.google.de/shopping?hl=de&source=og&tab=wf	-	-	-	-	CLEAN
https://news.google.com/?tab=wn	-	-	-	-	CLEAN
https://www.youtube.com/?gl=DE&tab=w1	-	-	-	-	CLEAN
https://translate.google.de/?hl=de&tab=wT	-	-	-	-	CLEAN
https://lh3.googleusercontent.com/ogw/default-user=s24	-	-	-	-	CLEAN
https://apis.google.com	-	-	-	-	CLEAN
http://video.google.de/?hl=de&tab=wv	-	-	-	-	CLEAN
https://calendar.google.com/calendar?tab=wc	-	-	-	-	CLEAN
http://www.google.de/preferences?hl=de	-	-	-	-	CLEAN
https://www.google.de/webhp?tab=ww	-	-	-	-	CLEAN
http://asset@multimetals.cfd	-	192.185.37.183	-	-	CLEAN
https://drive.google.com/?tab=wo	-	-	-	-	CLEAN
https://lh3.googleusercontent.com/ogw/default-user=s96	-	-	-	-	CLEAN
http://www.google.de/history/optout?hl=de	-	-	-	-	CLEAN
https://docs.google.com/document/?usp=docs_alc	-	-	-	-	CLEAN
https://accounts.google.com/ServiceLogin?hl=de&passive=true&continue=https://www.google.com/&ec=GAZAAQ	-	-	-	-	CLEAN
https://maps.google.de/maps?hl=de&tab=wl	-	-	-	-	CLEAN
https://plusone.google.com/u/0	-	-	-	-	CLEAN
https://www.google.de/imghp?hl=de&tab=wi	-	-	-	-	CLEAN
https://www.google.com/setprefdomain?prefdom=DE&prev=https://www.google.de/&sig=K_T2w9tLOZa98tlBqgTOW3r-7Gz8c%3D	-	142.250.185.68	-	-	CLEAN
https://www.google.com/setprefdomain?prefdom=DE&prev=https://www.google.de/&sig=K_XUe_WfBa4scu8otId0a1ICf7fHs%3D	-	142.250.185.68	-	-	CLEAN
https://photos.google.com/?tab=wq&pageId=none	-	-	-	-	CLEAN
https://mail.google.com/mail/?tab=wm	-	-	-	-	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
docs.google.com	-	-	-	CLEAN
maps.google.de	-	-	-	CLEAN
drive.google.com	-	-	-	CLEAN
news.google.com	-	-	-	CLEAN
photos.google.com	-	-	-	CLEAN
accounts.google.com	-	-	-	CLEAN
www.blogger.com	-	-	-	CLEAN
www.google.de	-	-	-	CLEAN
multimetals.cfd	192.185.37.183	-	TCP, DNS	CLEAN
lh3.googleusercontent.com	-	-	-	CLEAN
calendar.google.com	-	-	-	CLEAN
www.youtube.com	-	-	-	CLEAN
apis.google.com	-	-	-	CLEAN
www.google.com	142.250.185.68	-	TCP, HTTPS, DNS	CLEAN
play.google.com	-	-	-	CLEAN
video.google.de	-	-	-	CLEAN
books.google.de	-	-	-	CLEAN
www.gstatic.com	-	-	-	CLEAN
translate.google.de	-	-	-	CLEAN
mail.google.com	-	-	-	CLEAN
plusone.google.com	-	-	-	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
192.185.37.183	multimetals.cfd	United States	TCP, DNS	CLEAN
142.250.185.68	www.google.com	United States	TCP, HTTPS, DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
-	access, delete	installutil.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\TigerVNC\Server	access	installutil.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTP Password	read, access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	installutil.exe, geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\TightVNC\Server	access	installutil.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	access	geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\XML	access	geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\AllowAllUriEncodingExpansion	read, access	installutil.exe, geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_CURRENT_USER\Software\RimArts\B2\Settings	access	installutil.exe	CLEAN
HKEY_CURRENT_USER\Software\ORL\WinVNC3	access	installutil.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP Password	read, access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SystemDefaultTlsVersions	read, access	installutil.exe, geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Server	read, access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	read, access	installutil.exe, geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.UseSafeSynchronousClose	access	installutil.exe, geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	installutil.exe, geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_CURRENT_USER\Software\OpenVPN-GUI\configs	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SchSendAuxRecord	access	installutil.exe, geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseSafeSynchronousClose	read, access	installutil.exe, geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.UseStrictRfcInterimResponseHandling	access	installutil.exe, geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Uri.AllowDangerousUnicodeDecompositions	access	installutil.exe, geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	read, access	installutil.exe, geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP Password	read, access	installutil.exe	CLEAN
HKEY_CURRENT_USER\Software\TightVNC\Server	access	installutil.exe	CLEAN
HKEY_CURRENT_USER\Software\Qualcomm\Eudora\CommandLine	access	installutil.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Acrobat	read, access, delete, write	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\ORL\WinVNC3	access	installutil.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	access	installutil.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password	read, access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\RequireCertificateEKUs	read, access	installutil.exe, geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Messaging Subsystem\Profiles\9375CFF0413111d3B88A00104B2A6676	access	installutil.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTP Password	read, access	installutil.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3 Password	read, access	installutil.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Email	read, access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	installutil.exe, geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\FTPWare\COREFTP\Sites	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework	access	geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Uri.AllowAllUriEncodingExpansion	access	installutil.exe, geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	installutil.exe, geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	read, access	installutil.exe, geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Uri.UseStrictIPv6AddressParsing	access	installutil.exe, geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	installutil.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe, geater.exe, acrobat.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP Password	read, access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.UseHttpPipeliningAndBufferPooling	access	installutil.exe, geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_CURRENT_USER\Software\Aerofox\FoxmailPreview	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\LegacyWPADSupport	read, access	geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\vncserver	access	installutil.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Wow6432Node\RealVNC\WinVNC4	access	installutil.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP Password	read, access	installutil.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\Email	read, access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	read, access	installutil.exe, geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\SOFTWARE\RealVNC\vncserver	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchSendAuxRecord	read, access	installutil.exe, geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseStrictIPv6AddressParsing	read, access	installutil.exe, geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4	access	installutil.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002	access	installutil.exe	CLEAN
HKEY_CURRENT_USER\Software\DownloadManager\Passwords	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\RealVNC\WinVNC4	access	installutil.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 Password	read, access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	read, access	installutil.exe, geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	installutil.exe, geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Impersonation Level	read, access	installutil.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	read, access	installutil.exe, geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_CURRENT_USER\Software\Aerofox\Foxmail\V3.1	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SecurityProtocol	access	geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	read, access	installutil.exe, geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	read, access	installutil.exe, geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	read, access	installutil.exe, geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\WMIDisableCOMSecurity	read, access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseHttpPipeliningAndBufferPooling	read, access	installutil.exe, geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP Password	read, access	installutil.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\TigerVNC\Server	access	installutil.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\SOFTWARE\Martin Prikryl\WinSCP 2\Sessions	access	installutil.exe	CLEAN
HKEY_CURRENT_USER\Software\IncrediMail\Identities	access	installutil.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseStrictRfcInterimResponseHandling	read, access	installutil.exe, geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.RequireCertificateEKUs	access	installutil.exe, geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003	access	installutil.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password	read, access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Namespace	read, access	installutil.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Email	read, access	installutil.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password	read, access	installutil.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	access	installutil.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\AllowDangerousUnicodeDecompositions	read, access	installutil.exe, geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\.NETFramework\XML	access	geater.exe, 18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\RealVNC\WinVNC4	access	installutil.exe	CLEAN

Process

Process Name	Commandline	Verdict
18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe	"C:\Users\kEecfMwgj\Desktop\18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90.exe"	MALICIOUS
geater.exe	"C:\Users\kEecfMwgj\AppData\Local\Temp\geater.exe"	MALICIOUS
installutil.exe	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe"	SUSPICIOUS
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	SUSPICIOUS
acrobat.exe	"C:\Users\kEecfMwgj\AppData\Roaming\Acrobat\Acrobat.exe"	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN

YARA / AV

YARA (2)

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
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	VPN DE starvpn
Network Config Name	VPN DE starvpn

Platform Information

Platform Version	4.6.0
Dynamic Engine Version	4.6.0 / 07/08/2022 04:26
Static Engine Version	4.6.0.0 / 2022-07-08 03:00:22
AV Exceptions Version	4.6.0.1 / 2022-07-04 05:54:12
Link Detonation Heuristics Version	4.6.0.3 / 2022-07-11 12:34:44
Smart Memory Dumping Rules Version	4.6.0.1 / 2022-07-04 05:54:12
Config Extractors Version	4.6.0.5 / 2022-07-18 16:31:08
Signature Trust Store Version	4.6.0.1 / 2022-07-04 05:54:12
VMRay Threat Identifiers Version	4.6.0.5 / 2022-07-18 16:31:08
YARA Built-in Ruleset Version	4.6.0.5

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