MALICIOUS

Classifications: Backdoor | Spyware | Injector | Keylogger

Threat Names: QuasarRAT | QuasarRAT.v1 | AZORult | Mal/HTMLGen-A | xRAT | Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**Adobe Download Manager.exe**
ID	#9843023
MD5	e74b9ed601a42abe59c15e702103f25b
SHA1	ffcb43160db6ddc9bb62c85c420672de30b609d5
SHA256	27e5ab1169ea020b4f9f3bd3b1f176f0a64f3751942f2a544d0a14006076dd16
File Size	2063.55 KB
Report Created	2024-02-08 00:08 (UTC+1)
Target Environment	windows 10 (64bit TH2 -EN- MSO_2016) | exe

OVERVIEW

VMRay Threat Identifiers (31 rules, 73 matches)

Score	Category	Operation	Count	Classification
5/5	Extracted Configuration	QuasarRAT configuration was extracted	1	Backdoor
	• A configuration for QuasarRAT was extracted from artifacts of the dynamic analysis.			
5/5	YARA	Malicious content matched by YARA rules	10	Spyware
	• YARA detected "Azorult_Generic" from ruleset "Malware" in memory dump data from (process #5) adobe download manager.exe. • YARA detected "QuasarRAT" from ruleset "RATs" in the sample file C:\Users\RDhJ0CNFevzX\Desktop\Adobe Download Manager.exe. • YARA detected "Azorult_Generic" from ruleset "Malware" in memory dump data from (process #1) adobe download manager.exe. • YARA detected "QuasarRAT" from ruleset "RATs" in memory dump data from (process #4) windef.exe. • YARA detected "xRAT_1" from ruleset "RATs" in memory dump data from (process #4) windef.exe. • YARA detected "QuasarRAT" from ruleset "RATs" in memory dump data from (process #5) adobe download manager.exe. • YARA detected "QuasarRAT" from ruleset "RATs" in memory dump data from (process #1) adobe download manager.exe. • YARA detected "Azorult_Generic" from ruleset "Malware" in code dump data from (process #1) adobe download manager.exe. • YARA detected "xRAT_1" from ruleset "RATs" in process image data from (process #1) adobe download manager.exe. • YARA detected "QuasarRAT" from ruleset "RATs" in process image data from (process #1) adobe download manager.exe.		
5/5	Discovery	Combination of other detections shows configuration discovery	1	-
	• Sample enumerates processes, collects hardware information and queries network configuration which indicates system fingerprinting.			
5/5	Data Collection	Combination of other detections shows multiple input capture behaviors	1	Spyware
	• (Process #12) winsock.exe logs keys and potentially exfiltrates data.			
4/5	Defense Evasion	Obscures a file's origin	3	-
	• (Process #4) windef.exe tries to delete zone identifier of file "C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe". • (Process #4) windef.exe tries to delete zone identifier of file "C:\Users\RDhJ0CNFevzX\AppData\Roaming\SubDir\winsock.exe". • (Process #12) winsock.exe tries to delete zone identifier of file "C:\Users\RDhJ0CNFevzX\AppData\Roaming\SubDir\winsock.exe".			
4/5	Injection	Writes into the memory of another process	1	Injector
	• (Process #2) vnc.exe modifies memory of (process #3) svchost.exe.			
4/5	Injection	Modifies control flow of another process	1	-
	• (Process #2) vnc.exe alters context of (process #3) svchost.exe.			
4/5	Reputation	Malicious file detected via reputation	3	-
	• The sample itself is a known malicious file. • Reputation analysis labels embedded file "C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe" as Mal/Generic-S. • Embedded file "C:\Users\RDHJ0C~1\AppData\Local\Temp\vnc.exe" is a known malicious file.			
4/5	Reputation	Malicious host or URL detected via reputation	3	-
	• Reputation analysis labels the URL "hxxp://0x21[.]in:8000/_az/" which was contacted by (process #5) adobe download manager.exe as Mal/HTMLGen-A. • Reputation analysis labels the resolved domain "0x21.in" as Mal/HTMLGen-A. • Reputation analysis labels the contacted IP address 5.8.88.191 as Mal/HTMLGen-A.			
3/5	Input Capture	Monitors keyboard input	1	Keylogger

Score	Category	Operation	Count	Classification
	• (Process #12) winsock.exe installs system wide "WH_KEYBOARD_LL" hook(s) to monitor keystrokes.			
3/5	Injection	Injects a file into another process	1	-
	• (Process #12) winsock.exe injects file into (process #15) run-service-who.exe.			
2/5	Anti Analysis	Tries to detect debugger	1	-
	• (Process #1) adobe download manager.exe tries to detect a debugger via API "IsDebuggerPresent".			
2/5	Discovery	Queries OS version via WMI	2	-
	• (Process #4) windef.exe queries OS version via WMI query: SELECT Caption FROM Win32_OperatingSystem. • (Process #12) winsock.exe queries OS version via WMI query: SELECT Caption FROM Win32_OperatingSystem.			
2/5	Discovery	Reads network adapter information	2	-
	• (Process #4) windef.exe reads the network adapters' addresses by API. • (Process #12) winsock.exe reads the network adapters' addresses by API.			
2/5	Hide Tracks	Hides files	2	-
	• (Process #4) windef.exe hides the file "C:\Users\RDhJ0CNFevzX\AppData\Roaming\SubDir\winsock.exe" by setting its "hidden" attribute. • (Process #12) winsock.exe hides the file "C:\Users\RDhJ0CNFevzX\AppData\Roaming\SubDir\winsock.exe" by setting its "hidden" attribute.			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	1	-
	• (Process #1) adobe download manager.exe modifies memory of (process #5) adobe download manager.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
	• (Process #1) adobe download manager.exe alters context of (process #5) adobe download manager.exe.			
2/5	Task Scheduling	Schedules task	3	-
	• Schedules task for command "C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe", to be triggered by LOGON. • Schedules task for command "C:\Users\RDhJ0CNFevzX\AppData\Roaming\SubDir\winsock.exe", to be triggered by LOGON. • Schedules task for command "C:\Users\RDhJ0CNFevzX\btpanui\SystemPropertiesPerformance.exe", to be triggered by TIME. Task has been rescheduled by the analyzer.			
2/5	Task Scheduling	Schedules task via schtasks	2	-
	• Schedules task "win defender run" via the schtasks command line utility. • Schedules task "RtkAudioService64" via the schtasks command line utility.			
1/5	Mutex	Creates mutex	4	-
	• (Process #1) adobe download manager.exe creates mutex with name "runas". • (Process #4) windef.exe creates mutex with name "QSR_MUTEX_0kBRNrRz5TDLEQoul0". • (Process #12) winsock.exe creates mutex with name "QSR_MUTEX_0kBRNrRz5TDLEQoul0". • (Process #5) adobe download manager.exe creates mutex with name "A743A547-9C1AFDB0-AEA27C97-73E39B07-D5BBC660F".			
1/5	Discovery	Enumerates running processes	1	-
	• (Process #1) adobe download manager.exe enumerates running processes.			
1/5	Hide Tracks	Creates process with hidden window	6	-

Score	Category	Operation	Count	Classification
		• (Process #2) vnc.exe starts (process #3) svchost.exe with a hidden window. • (Process #1) adobe download manager.exe starts (process #5) adobe download manager.exe with a hidden window. • (Process #4) windef.exe starts (process #10) schtasks.exe with a hidden window. • (Process #4) windef.exe starts (process #12) winsock.exe with a hidden window. • (Process #12) winsock.exe starts (process #13) schtasks.exe with a hidden window. • (Process #1) adobe download manager.exe starts (process #78) schtasks.exe with a hidden window.		
1/5	Obfuscation	Creates a page with write and execute permissions	3	-
		• (Process #3) svchost.exe changes the protection of a page in a foreign process from writable ("PAGE_READWRITE") to executable ("PAGE_EXECUTE_READ"). • (Process #2) vnc.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code. • (Process #1) adobe download manager.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.		
1/5	Obfuscation	Reads from memory of another process	1	-
		• (Process #1) adobe download manager.exe reads from (process #5) adobe download manager.exe.		
1/5	Privilege Escalation	Enables process privileges	1	-
		• (Process #12) winsock.exe enables process privilege "SeDebugPrivilege".		
1/5	Discovery	Reads system data	1	-
		• (Process #5) adobe download manager.exe reads the cryptographic machine GUID from registry.		
1/5	Network Connection	Performs DNS request	2	-
		• (Process #5) adobe download manager.exe fails to resolve hostname "0x21.in" • (Process #4) windef.exe resolves hostname "ip-api.com" to IP "208.95.112.1".		
1/5	Network Connection	Connects to remote host	3	-
		• (Process #12) winsock.exe opens an outgoing TCP connection to host "208.95.112.1:80". • (Process #4) windef.exe opens an outgoing TCP connection to host "208.95.112.1:80". • (Process #12) winsock.exe opens an outgoing TCP connection to host "5.8.88.191:443".		
1/5	Obfuscation	Resolves API functions dynamically	5	-
		• (Process #1) adobe download manager.exe resolves 55 API functions by name. • (Process #3) svchost.exe resolves 237 API functions by name. • (Process #4) windef.exe resolves 49 API functions by name. • (Process #12) winsock.exe resolves 50 API functions by name. • (Process #5) adobe download manager.exe resolves 85 API functions by name.		
1/5	Execution	Drops PE file	3	-
		• (Process #1) adobe download manager.exe drops file "C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe". • (Process #1) adobe download manager.exe drops file "C:\Users\RDhJ0CNFevzX\btpanui\SystemPropertiesPerformance.exe". • (Process #1) adobe download manager.exe drops file "C:\Users\RDHJ0C~1\AppData\Local\Temp\vnc.exe".		
1/5	Execution	Executes dropped PE file	3	-
		• Executes dropped file "C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe". • Executes dropped file "C:\Users\RDhJ0CNFevzX\btpanui\SystemPropertiesPerformance.exe". • Executes dropped file "C:\Users\RDHJ0C~1\AppData\Local\Temp\vnc.exe".		

Malware Configuration: QuasarRAT

Metadata	Key	Extracted Value
Version	Value	1.3.0.0
Socket	Address Port Network Protocol C2 Listen Address Port Network Protocol C2 Listen	5.8.88.191 443 tcp ✔ ✖ sockartek.icu 443 tcp ✔ ✖
Path	Tags Path Is Dir Tags Path Is Dir Tags Path Is Dir Tags Path Is Dir	Special Folder %appdata% ✔ Install Folder SubDir ✔ Install Name winsock.exe ✖ Log Directory Logs ✔
Mutex	Value	QSR_MUTEX_0kBRNrRz5TDLEQoul0
Mission ID	Value	EbayProfiles
Interval	Tags Value	Reconnect Delay 3000.0
Other: Salt	Value	v+seVvvNlzuyGQlkMKV4QwA9VkTSHmK51PGA5+bDOUE=
Other: Key	Tags Value	PBKDF2 Input Password MWhG6wsCIMX8aJM2CVXT
Other: Startup Key	Value	win defender run
Other: Install Enabled	Value	✔
Other: Startup Enabled	Value	✔
Other: Hide File	Value	✔
Other: Hide Install Directory	Value	✔
Other: Logger Enabled	Value	✔
Other: Hide Log Directory	Value	✔
Other: Client Key	Value	q/M9YOfM0QDY+acgy4plEQ==
Other: Client Auth Key	Value	iwb/FVEFSrvXyRpBxbtrAvdMlxa7+ov04yp0i3czHSu4tv1s4GZ3EJzmAGkSQNOaN8kB3o9RFUbfJZJcB+hSpA==

Mitre ATT&CK Matrix

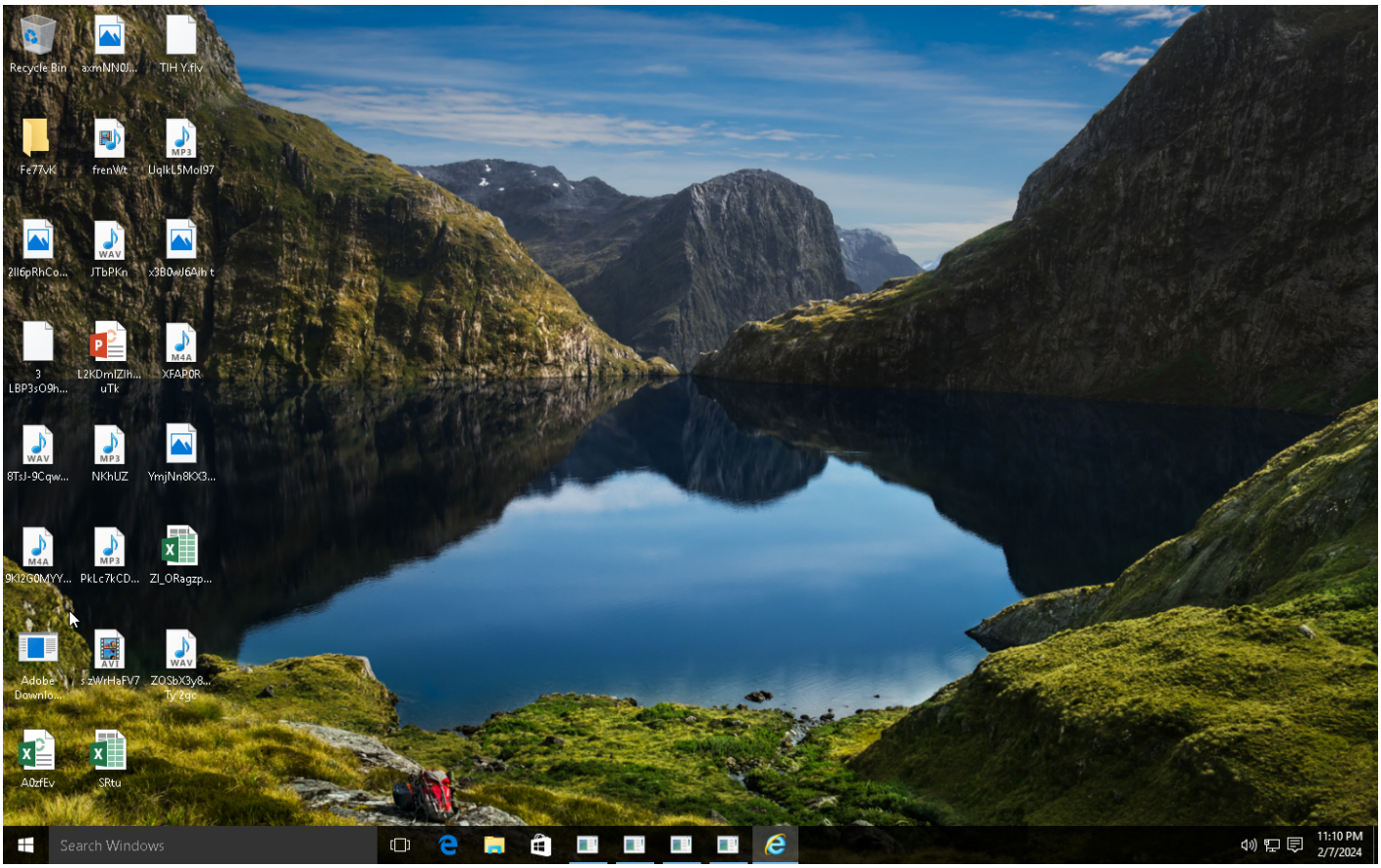
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation	#T1158 Hidden Files and Directories	#T1179 Hooking	#T1143 Hidden Window	#T1056 Input Capture	#T1057 Process Discovery		#T1056 Input Capture			
	#T1053 Scheduled Task	#T1179 Hooking	#T1055 Process Injection	#T1045 Software Packing	#T1179 Hooking	#T1082 System Information Discovery		#T1119 Automated Collection			
		#T1053 Scheduled Task	#T1053 Scheduled Task	#T1096 NTFS File Attributes		#T1016 System Network Configuration Discovery					
				#T1158 Hidden Files and Directories		#T1012 Query Registry					
				#T1055 Process Injection							

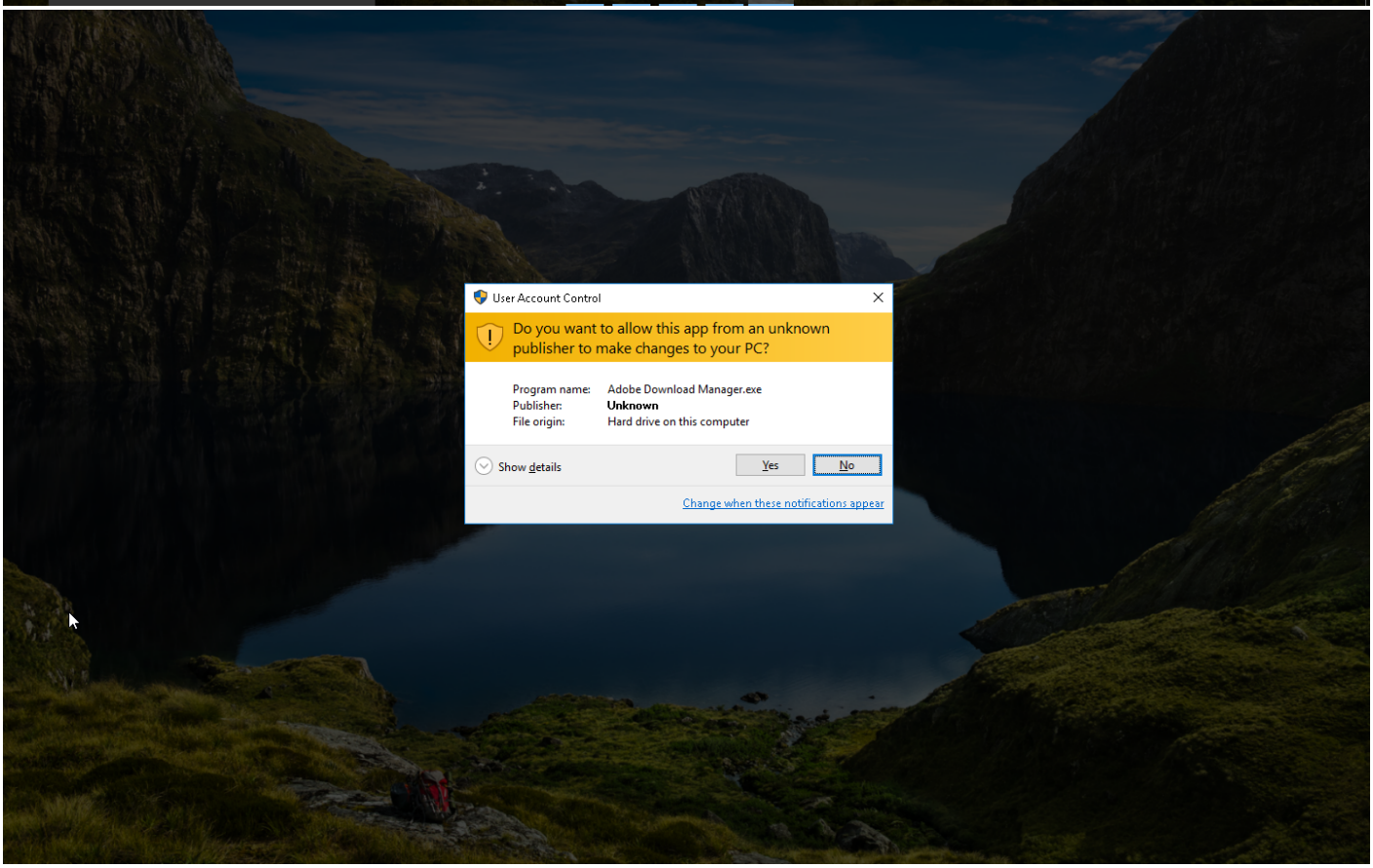
Sample Information

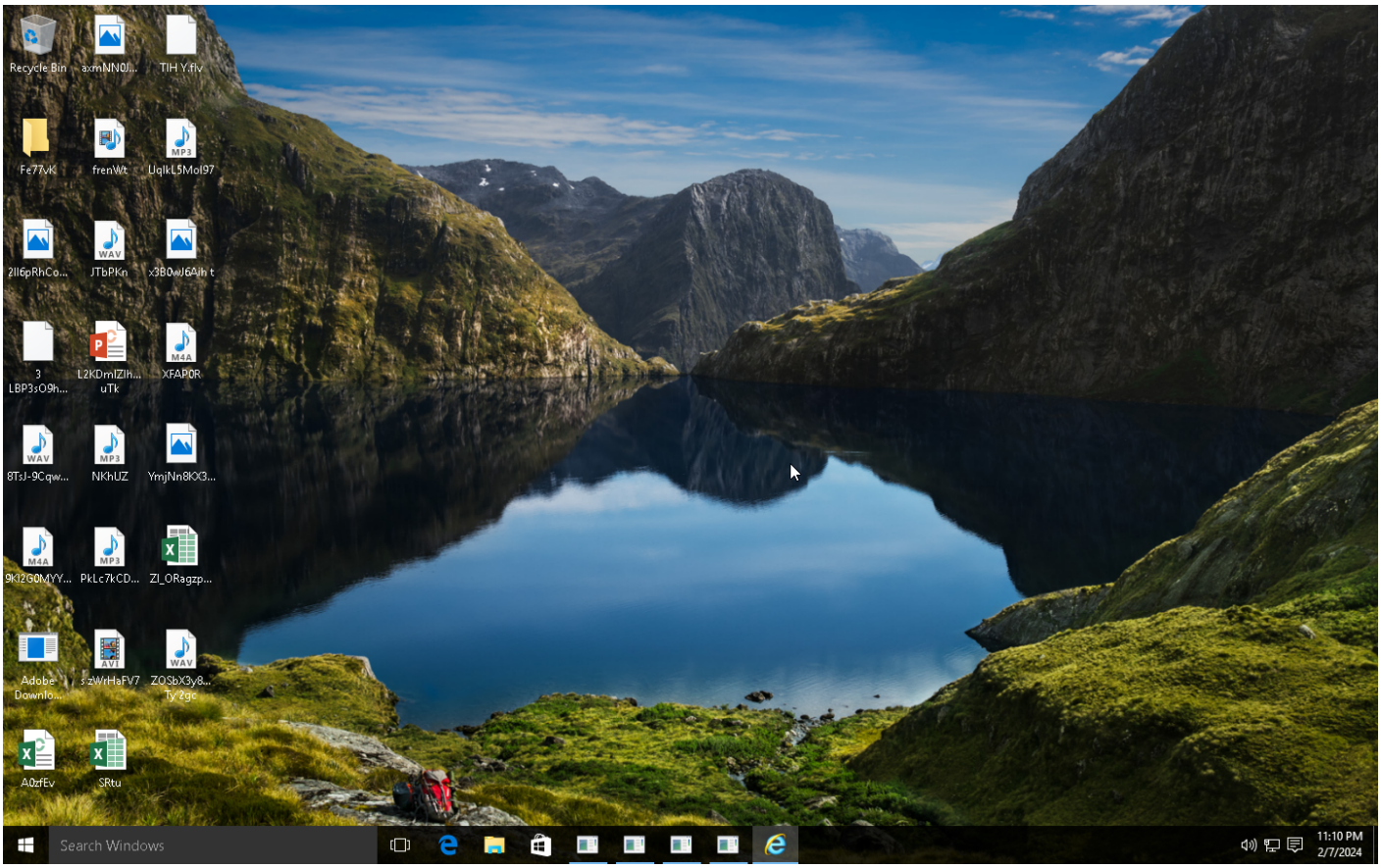
ID	#9843023
MD5	e74b9ed601a42abe59c15e702103f25b
SHA1	ffcb43160db6ddc9bb62c85c420672de30b609d5
SHA256	27e5ab1169ea020b4f9f3bd3b1f176f0a64f3751942f2a544d0a14006076dd16
SSDeep	24576:su6J33O0c+JY5UZ+XC0kGso6Fal1lXgM6YmenKKSUlmDaGJTA4Pqa6jUvOkQwKY1:2u0c++OCvkGs9Fap5aLKLkDl+dUvO9Yn
ImpHash	afcdf79be1557326c854b6e20cb900a7
File Name	Adobe Download Manager.exe
File Size	2063.55 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

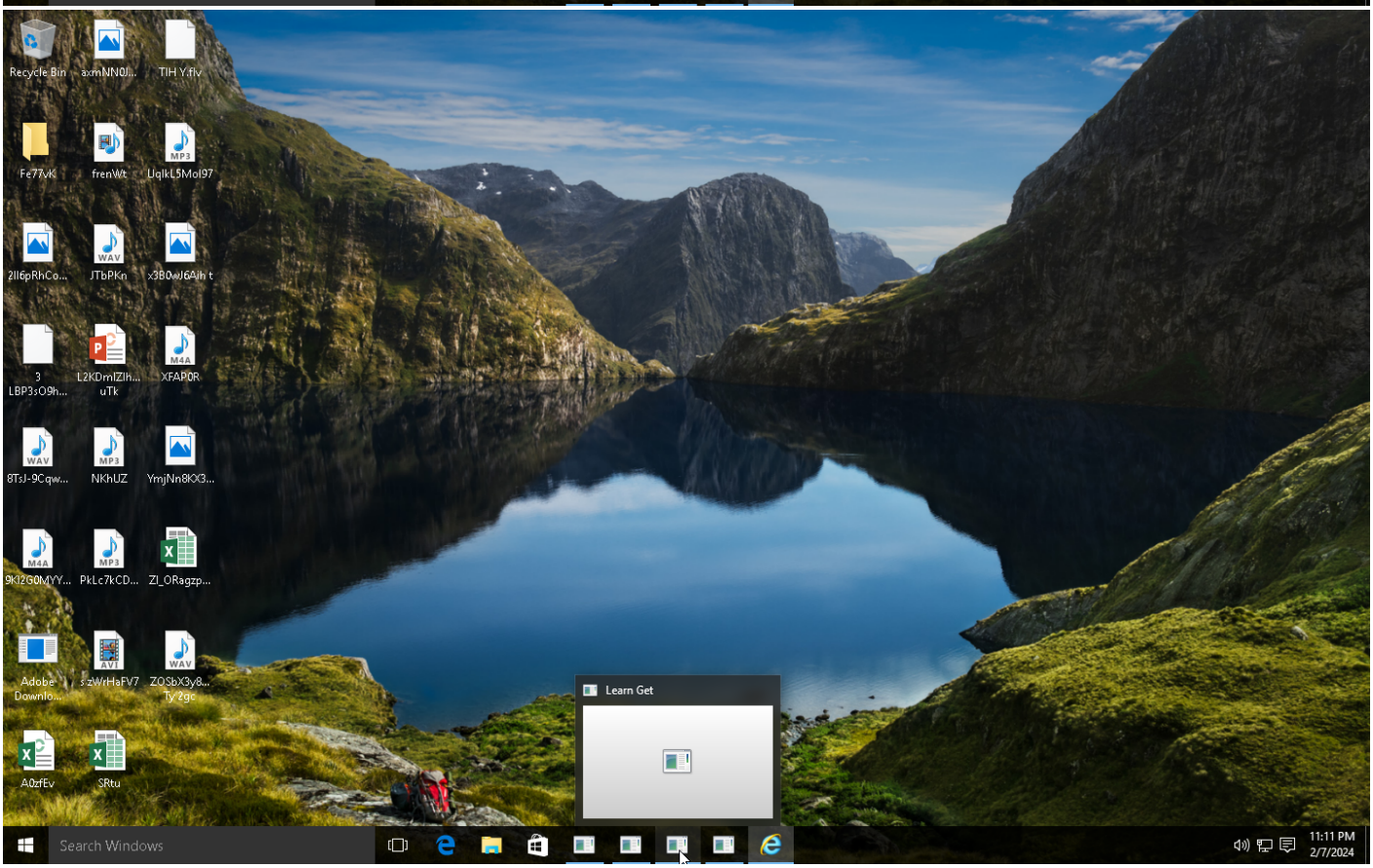
Analysis Information

Creation Time	2024-02-08 00:08 (UTC+1)
Analysis Duration	00:03:17
Termination Reason	Timeout
Number of Monitored Processes	77
Execution Successful	True
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	22


Recycle Bin
axmNN0l...
TIH Y.flv
Fe77vK
frenWt
UqIkL5Mol97
2lI6pRhCo...
JTbPKn
x3B0wJ6Ajh t
3 LBP3sO9h...
L2KDmIZIh... uTk
XFAP0R
8TsJ-9Cqw...
NKhUZ
YmjNn8lO3...
9KI2G0MYY...
PkLc7kCD...
ZI_ORagzp...
Adobe Downlo...
szWrHaFV7
ZOSbX3y8... Ty 2gc
A0zfEv
SRtu
Search Windows
11:10 PM
2/7/2024


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: Adobe Download Manager.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear





Screenshots truncated

NETWORK

General

3.67 KB total sent

3.10 KB total received

4 ports 80, 443, 53, 445

3 contacted IP addresses

3 URLs extracted

0 files downloaded

2 malicious hosts detected

DNS

3 DNS requests for 2 domains

1 nameservers contacted

2 total requests returned errors

HTTP/S

0 URLs contacted, 0 servers

2 sessions, 0 bytes sent, 0 bytes received

HTTP Requests

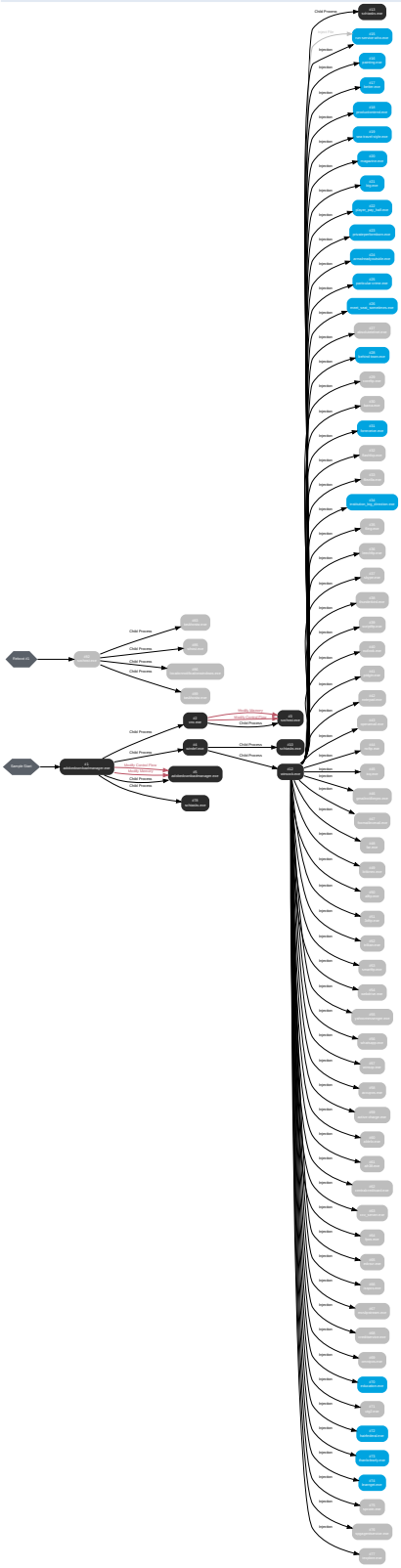
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
POST	hxxp://0x21[.]in:8000/_az/	-	-	-	0 bytes	MALICIOUS

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	0x21[.]in	NX_DOMAIN	-	-	MALICIOUS
A	ip-api[.]com	NO_ERROR	208.95.112.1	-	CLEAN

BEHAVIOR

Process Graph



Process #1: adobe download manager.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\adobe download manager.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\Adobe Download Manager.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 124875, Reason: Analysis Target
Unmonitor End Time	End Time: 195862, Reason: Terminated
Monitor duration	70.99s
Return Code	1073807364
PID	4484
Parent PID	1656
Bitness	32 Bit

Dropped Files (3)

File Name	File Size	SHA256	YARA Match
C:\Users\RDHJ0C~1\AppData\Local\Temp\vnc.exe	405.50 KB	4e8a99cd33c9e5c747a3ce8f1a3e17824846f4a8f7cb0631aebd0815db2ce3a4	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\windef.exe	349.00 KB	7050608d53f80269df951d00883ed79815c060ce7678a76b5c3f6a2a985beea9	✔
C:\Users\RDhJ0CNFevzX\btpanui\SystemPropertiesPerformance.exe	2063.56 KB	25000160aa1a06fd370be2a5cabce36c80fb12fbb1817e6ac67847dca7586295	✔

Host Behavior

Type	Count
Module	106
File	59
Environment	2
System	2281
Registry	3
-	1
Window	2
Mutex	1
Process	211
-	3
-	11

Process #2: vnc.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\appdata\local\temp\vnc.exe
Command Line	"C:\Users\RDHJ0C~1\AppData\Local\Temp\vnc.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 134822, Reason: Child Process
Unmonitor End Time	End Time: 168493, Reason: Terminated
Monitor duration	33.67s
Return Code	0
PID	668
Parent PID	4484
Bitness	32 Bit

Host Behavior

Type	Count
Module	50
System	3
Process	1
-	8
-	7

Process #3: svchost.exe

ID	3
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 135657, Reason: Child Process
Unmonitor End Time	End Time: 194017, Reason: Terminated
Monitor duration	58.36s
Return Code	1073807364
PID	4212
Parent PID	668
Bitness	64 Bit

Injection Information (5)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\users\rdhj0cnfevzx\appdata\local\temp\vnc.exe	0x1110	0x7ff65b183980(140696066996608)	0x4	✔	1
Modify Memory	#2: c:\users\rdhj0cnfevzx\appdata\local\temp\vnc.exe	0x1110	0x400000(4194304)	0x9c000	✔	1
Modify Memory	#2: c:\users\rdhj0cnfevzx\appdata\local\temp\vnc.exe	0x1110	0x4a0000(4849664)	0x318	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\appdata\local\temp\vnc.exe	0x1110 / 0x810	0x1cb0f000(481357824)	-	✔	1
Modify Memory	#2: c:\users\rdhj0cnfevzx\appdata\local\temp\vnc.exe	0x1110	0x7ff65b183980(140696066996608)	0x4	✔	1

Host Behavior

Type	Count
Module	259

Process #4: windef.exe

ID	4
File Name	c:\users\rdhj0cnfevzx\appdata\local\temp\windef.exe
Command Line	"C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 135825, Reason: Child Process
Unmonitor End Time	End Time: 156267, Reason: Terminated
Monitor duration	20.44s
Return Code	0
PID	636
Parent PID	4484
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Roaming\SubDir\winsock.exe	349.00 KB	7050608d53f80269df951d00883ed79815c060ce7678a76b5c3f6a2a985beea9	✔

Host Behavior

Type	Count
Registry	22
-	8
-	12
COM	4
Module	56
-	1
Mutex	1
File	28
System	3
Environment	4
-	1
Process	2

Network Behavior

Type	Count
DNS	1
TCP	1

Process #5: adobe download manager.exe

ID	5
File Name	c:\users\rdhj0cnfevzx\desktop\adobe download manager.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\Adobe Download Manager.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 140870, Reason: Child Process
Unmonitor End Time	End Time: 172109, Reason: Terminated
Monitor duration	31.24s
Return Code	0
PID	4668
Parent PID	4484
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\adobe download manager.exe	0x117c	0x1000000(16777216)	0x20000	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\adobe download manager.exe	0x117c	0x77c008(7847944)	0x4	✔	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\adobe download manager.exe	0x117c / 0x127c	0x77298fe0(1999212512)	-	✔	1

Host Behavior

Type	Count
Module	106
Keyboard	2
System	4
Registry	8
User	2
Mutex	1
-	1

Network Behavior

Type	Count
HTTP	1
DNS	1
TCP	1

Process #10: schtasks.exe

ID	10
File Name	c:\windows\syswow64\schtasks.exe
Command Line	"schtasks" /create /tn "win defender run" /sc ONLOGON /tr "C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe" /rl HIGHEST /f
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 152708, Reason: Child Process
Unmonitor End Time	End Time: 155553, Reason: Terminated
Monitor duration	2.85s
Return Code	0
PID	4616
Parent PID	636
Bitness	32 Bit

Host Behavior

Type	Count
Module	3
System	3
COM	1
File	6

Process #12: winsock.exe

ID	12
File Name	c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe
Command Line	"C:\Users\RDhJ0CNFevzX\AppData\Roaming\SubDir\winsock.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 153765, Reason: Child Process
Unmonitor End Time	End Time: 195860, Reason: Terminated
Monitor duration	42.09s
Return Code	1073807364
PID	4856
Parent PID	636
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Logs\02-07-2024	224 bytes	acce7bf50072acc7fd91ba76beec9c319c9673ad8244acb3b29605424ad721f9	✖

Host Behavior

Type	Count
Registry	25
-	9
-	12
COM	4
Module	62
-	1
Mutex	1
File	34
System	16
Environment	4
-	1
Process	1
User	1
Window	3
Keyboard	5

Network Behavior

Type	Count
TCP	2

Process #13: schtasks.exe

ID	13
File Name	c:\windows\syswow64\schtasks.exe
Command Line	"schtasks" /create /tn "win defender run" /sc ONLOGON /tr "C:\Users\RDhJ0CNFevzX\AppData\Roaming\SubDir\winsock.exe" /rl HIGHEST /f
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 163031, Reason: Child Process
Unmonitor End Time	End Time: 165903, Reason: Terminated
Monitor duration	2.87s
Return Code	0
PID	4944
Parent PID	4856
Bitness	32 Bit

Host Behavior

Type	Count
Module	3
System	3
COM	1
File	6

Process #15: run-service-who.exe

ID	15
File Name	c:\program files (x86)\windows defender\run-service-who.exe
Command Line	"C:\Program Files (x86)\Windows Defender\run-service-who.exe"
Initial Working Directory	C:\Program Files (x86)\Windows Defender\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 193707, Reason: Terminated
Monitor duration	29.20s
Return Code	1073807364
PID	3432
Parent PID	4856
Bitness	32 Bit

Injection Information (1)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Inject File	#12: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe	0xa0c / 0xd6c		-	✖	1

Process #16: painting.exe

ID	16
File Name	c:\program files (x86)\microsoft office\painting.exe
Command Line	"C:\Program Files (x86)\Microsoft Office\painting.exe"
Initial Working Directory	C:\Program Files (x86)\Microsoft Office\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194200, Reason: Terminated
Monitor duration	29.69s
Return Code	1073807364
PID	3484
Parent PID	4856
Bitness	32 Bit

Process #17: better.exe

ID	17
File Name	c:\program files (x86)\windows defender\better.exe
Command Line	"C:\Program Files (x86)\Windows Defender\better.exe"
Initial Working Directory	C:\Program Files (x86)\Windows Defender\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194349, Reason: Terminated
Monitor duration	29.84s
Return Code	1073807364
PID	3420
Parent PID	4856
Bitness	32 Bit

Process #18: production tend.exe

ID	18
File Name	c:\program files\windows nt\production tend.exe
Command Line	"C:\Program Files\Windows NT\production tend.exe"
Initial Working Directory	C:\Program Files\Windows NT\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194378, Reason: Terminated
Monitor duration	29.87s
Return Code	1073807364
PID	3468
Parent PID	4856
Bitness	32 Bit

Process #19: sea-travel-style.exe

ID	19
File Name	c:\program files (x86)\msbuild\sea-travel-style.exe
Command Line	"C:\Program Files (x86)\MSBuild\sea-travel-style.exe"
Initial Working Directory	C:\Program Files (x86)\MSBuild\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 195065, Reason: Terminated
Monitor duration	30.56s
Return Code	1073807364
PID	3536
Parent PID	4856
Bitness	32 Bit

Process #20: magazine.exe

ID	20
File Name	c:\program files (x86)\mozilla firefox\magazine.exe
Command Line	"C:\Program Files (x86)\Mozilla Firefox\magazine.exe"
Initial Working Directory	C:\Program Files (x86)\Mozilla Firefox\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194333, Reason: Terminated
Monitor duration	29.82s
Return Code	1073807364
PID	3412
Parent PID	4856
Bitness	32 Bit

Process #21: big.exe

ID	21
File Name	c:\program files\windows defender\big.exe
Command Line	"C:\Program Files\Windows Defender\big.exe"
Initial Working Directory	C:\Program Files\Windows Defender\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194365, Reason: Terminated
Monitor duration	29.86s
Return Code	1073807364
PID	3444
Parent PID	4856
Bitness	32 Bit

Process #22: player_pay_half.exe

ID	22
File Name	c:\program files\microsoft sql server\player_pay_half.exe
Command Line	"C:\Program Files\Microsoft SQL Server\player_pay_half.exe"
Initial Working Directory	C:\Program Files\Microsoft SQL Server\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194197, Reason: Terminated
Monitor duration	29.69s
Return Code	1073807364
PID	3560
Parent PID	4856
Bitness	32 Bit

Process #23: privateperformborn.exe

ID	23
File Name	c:\program files\windows nt\privateperformborn.exe
Command Line	"C:\Program Files\Windows NT\privateperformborn.exe"
Initial Working Directory	C:\Program Files\Windows NT\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 195031, Reason: Terminated
Monitor duration	30.52s
Return Code	1073807364
PID	3576
Parent PID	4856
Bitness	32 Bit

Process #24: armalreadyoutside.exe

ID	24
File Name	c:\program files\windows photo viewer\armalreadyoutside.exe
Command Line	"C:\Program Files\Windows Photo Viewer\armalreadyoutside.exe"
Initial Working Directory	C:\Program Files\Windows Photo Viewer\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 195088, Reason: Terminated
Monitor duration	30.58s
Return Code	1073807364
PID	3516
Parent PID	4856
Bitness	32 Bit

Process #25: particular-crime.exe

ID	25
File Name	c:\program files (x86)\common files\particular-crime.exe
Command Line	"C:\Program Files (x86)\Common Files\particular-crime.exe"
Initial Working Directory	C:\Program Files (x86)\Common Files\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 195052, Reason: Terminated
Monitor duration	30.54s
Return Code	1073807364
PID	3524
Parent PID	4856
Bitness	32 Bit

Process #26: meet_seat_sometimes.exe

ID	26
File Name	c:\program files (x86)\windows multimedia platform\meet_seat_sometimes.exe
Command Line	"C:\Program Files (x86)\Windows Multimedia Platform\meet_seat_sometimes.exe"
Initial Working Directory	C:\Program Files (x86)\Windows Multimedia Platform\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194968, Reason: Terminated
Monitor duration	30.46s
Return Code	1073807364
PID	3600
Parent PID	4856
Bitness	32 Bit

Process #27: absolutetelnet.exe

ID	27
File Name	c:\program files\microsoft office\absolutetelnet.exe
Command Line	"C:\Program Files\Microsoft Office\absolutetelnet.exe"
Initial Working Directory	C:\Program Files\Microsoft Office\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194877, Reason: Terminated
Monitor duration	30.37s
Return Code	1073807364
PID	3636
Parent PID	4856
Bitness	32 Bit

Process #28: behind-town.exe

ID	28
File Name	c:\program files (x86)\windows media player\behind-town.exe
Command Line	"C:\Program Files (x86)\Windows Media Player\behind-town.exe"
Initial Working Directory	C:\Program Files (x86)\Windows Media Player\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 195033, Reason: Terminated
Monitor duration	30.52s
Return Code	1073807364
PID	3544
Parent PID	4856
Bitness	32 Bit

Process #29: coreftp.exe

ID	29
File Name	c:\program files\java\coreftp.exe
Command Line	"C:\Program Files\Java\coreftp.exe"
Initial Working Directory	C:\Program Files\Java\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194817, Reason: Terminated
Monitor duration	30.31s
Return Code	1073807364
PID	3684
Parent PID	4856
Bitness	32 Bit

Process #30: barca.exe

ID	30
File Name	c:\program files\uninstall information\barca.exe
Command Line	"C:\Program Files\Uninstall Information\barca.exe"
Initial Working Directory	C:\Program Files\Uninstall Information\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194849, Reason: Terminated
Monitor duration	30.34s
Return Code	1073807364
PID	3660
Parent PID	4856
Bitness	32 Bit

Process #31: for receive.exe

ID	31
File Name	c:\program files\microsoft office\for receive.exe
Command Line	"C:\Program Files\Microsoft Office\for receive.exe"
Initial Working Directory	C:\Program Files\Microsoft Office\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194990, Reason: Terminated
Monitor duration	30.48s
Return Code	1073807364
PID	3584
Parent PID	4856
Bitness	32 Bit

Process #32: flashfxp.exe

ID	32
File Name	c:\program files\windows mail\flashfxp.exe
Command Line	"C:\Program Files\Windows Mail\flashfxp.exe"
Initial Working Directory	C:\Program Files\Windows Mail\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194752, Reason: Terminated
Monitor duration	30.24s
Return Code	1073807364
PID	3716
Parent PID	4856
Bitness	32 Bit

Process #33: filezilla.exe

ID	33
File Name	c:\program files\windows sidebar\filezilla.exe
Command Line	"C:\Program Files\Windows Sidebar\filezilla.exe"
Initial Working Directory	C:\Program Files\Windows Sidebar\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194770, Reason: Terminated
Monitor duration	30.26s
Return Code	1073807364
PID	3708
Parent PID	4856
Bitness	32 Bit

Process #34: institution_big_direction.exe

ID	34
File Name	c:\program files\msbuild\institution_big_direction.exe
Command Line	"C:\Program Files\MSBuild\institution_big_direction.exe"
Initial Working Directory	C:\Program Files\MSBuild\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194922, Reason: Terminated
Monitor duration	30.41s
Return Code	1073807364
PID	3608
Parent PID	4856
Bitness	32 Bit

Process #35: fling.exe

ID	35
File Name	c:\program files\windows journal\fling.exe
Command Line	"C:\Program Files\Windows Journal\fling.exe"
Initial Working Directory	C:\Program Files\Windows Journal\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194739, Reason: Terminated
Monitor duration	30.23s
Return Code	1073807364
PID	3732
Parent PID	4856
Bitness	32 Bit

Process #36: leechftp.exe

ID	36
File Name	c:\program files (x86)\windows portable devices\leechftp.exe
Command Line	"C:\Program Files (x86)\Windows Portable Devices\leechftp.exe"
Initial Working Directory	C:\Program Files (x86)\Windows Portable Devices\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194302, Reason: Terminated
Monitor duration	29.79s
Return Code	1073807364
PID	3780
Parent PID	4856
Bitness	32 Bit

Process #37: skype.exe

ID	37
File Name	c:\program files (x86)\microsoft office\skype.exe
Command Line	"C:\Program Files (x86)\Microsoft Office\skype.exe"
Initial Working Directory	C:\Program Files (x86)\Microsoft Office\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194617, Reason: Terminated
Monitor duration	30.11s
Return Code	1073807364
PID	3860
Parent PID	4856
Bitness	32 Bit

Process #38: thunderbird.exe

ID	38
File Name	c:\program files\common files\thunderbird.exe
Command Line	"C:\Program Files\Common Files\thunderbird.exe"
Initial Working Directory	C:\Program Files\Common Files\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194555, Reason: Terminated
Monitor duration	30.05s
Return Code	1073807364
PID	3880
Parent PID	4856
Bitness	32 Bit

Process #39: scriptftp.exe

ID	39
File Name	c:\program files (x86)\microsoft office\scriptftp.exe
Command Line	"C:\Program Files (x86)\Microsoft Office\scriptftp.exe"
Initial Working Directory	C:\Program Files (x86)\Microsoft Office\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194598, Reason: Terminated
Monitor duration	30.09s
Return Code	1073807364
PID	3852
Parent PID	4856
Bitness	32 Bit

Process #40: outlook.exe

ID	40
File Name	c:\program files\internet explorer\outlook.exe
Command Line	"C:\Program Files\Internet Explorer\outlook.exe"
Initial Working Directory	C:\Program Files\Internet Explorer\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194628, Reason: Terminated
Monitor duration	30.12s
Return Code	1073807364
PID	3828
Parent PID	4856
Bitness	32 Bit

Process #41: pidgin.exe

ID	41
File Name	c:\program files (x86)\windows mail\pidgin.exe
Command Line	"C:\Program Files (x86)\Windows Mail\pidgin.exe"
Initial Working Directory	C:\Program Files (x86)\Windows Mail\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194568, Reason: Terminated
Monitor duration	30.06s
Return Code	1073807364
PID	3836
Parent PID	4856
Bitness	32 Bit

Process #42: notepad.exe

ID	42
File Name	c:\program files (x86)\microsoft analysis services\notepad.exe
Command Line	"C:\Program Files (x86)\Microsoft Analysis Services\notepad.exe"
Initial Working Directory	C:\Program Files (x86)\Microsoft Analysis Services\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194658, Reason: Terminated
Monitor duration	30.15s
Return Code	1073807364
PID	3804
Parent PID	4856
Bitness	32 Bit

Process #43: operamail.exe

ID	43
File Name	c:\program files (x86)\microsoft sql server\operamail.exe
Command Line	"C:\Program Files (x86)\Microsoft SQL Server\operamail.exe"
Initial Working Directory	C:\Program Files (x86)\Microsoft SQL Server\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194646, Reason: Terminated
Monitor duration	30.14s
Return Code	1073807364
PID	3812
Parent PID	4856
Bitness	32 Bit

Process #44: ncftp.exe

ID	44
File Name	c:\program files (x86)\windows multimedia platform\ncftp.exe
Command Line	"C:\Program Files (x86)\Windows Multimedia Platform\ncftp.exe"
Initial Working Directory	C:\Program Files (x86)\Windows Multimedia Platform\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194676, Reason: Terminated
Monitor duration	30.17s
Return Code	1073807364
PID	3788
Parent PID	4856
Bitness	32 Bit

Process #45: icq.exe

ID	45
File Name	c:\program files\windows mail\icq.exe
Command Line	"C:\Program Files\Windows Mail\icq.exe"
Initial Working Directory	C:\Program Files\Windows Mail\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194689, Reason: Terminated
Monitor duration	30.18s
Return Code	1073807364
PID	3764
Parent PID	4856
Bitness	32 Bit

Process #46: gmailnotifierpro.exe

ID	46
File Name	c:\program files (x86)\windows mail\gmailnotifierpro.exe
Command Line	"C:\Program Files (x86)\Windows Mail\gmailnotifierpro.exe"
Initial Working Directory	C:\Program Files (x86)\Windows Mail\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194708, Reason: Terminated
Monitor duration	30.20s
Return Code	1073807364
PID	3756
Parent PID	4856
Bitness	32 Bit

Process #47: foxmailincmail.exe

ID	47
File Name	c:\program files\uninstall information\foxmailincmail.exe
Command Line	"C:\Program Files\Uninstall Information\foxmailincmail.exe"
Initial Working Directory	C:\Program Files\Uninstall Information\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194721, Reason: Terminated
Monitor duration	30.21s
Return Code	1073807364
PID	3740
Parent PID	4856
Bitness	32 Bit

Process #48: far.exe

ID	48
File Name	c:\program files\windows journal\far.exe
Command Line	"C:\Program Files\Windows Journal\far.exe"
Initial Working Directory	C:\Program Files\Windows Journal\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194784, Reason: Terminated
Monitor duration	30.27s
Return Code	1073807364
PID	3692
Parent PID	4856
Bitness	32 Bit

Process #49: bitkinex.exe

ID	49
File Name	c:\program files\msbuild\bitkinex.exe
Command Line	"C:\Program Files\MSBuild\bitkinex.exe"
Initial Working Directory	C:\Program Files\MSBuild\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194802, Reason: Terminated
Monitor duration	30.29s
Return Code	1073807364
PID	3668
Parent PID	4856
Bitness	32 Bit

Process #50: alftp.exe

ID	50
File Name	c:\program files\uninstall information\alftp.exe
Command Line	"C:\Program Files\Uninstall Information\alftp.exe"
Initial Working Directory	C:\Program Files\Uninstall Information\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194864, Reason: Terminated
Monitor duration	30.36s
Return Code	1073807364
PID	3644
Parent PID	4856
Bitness	32 Bit

Process #51: 3dftp.exe

ID	51
File Name	c:\program files (x86)\mozilla firefox\3dftp.exe
Command Line	"C:\Program Files (x86)\Mozilla Firefox\3dftp.exe"
Initial Working Directory	C:\Program Files (x86)\Mozilla Firefox\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 193989, Reason: Terminated
Monitor duration	29.48s
Return Code	1073807364
PID	3620
Parent PID	4856
Bitness	32 Bit

Process #52: trillian.exe

ID	52
File Name	c:\program files\microsoft.net\trillian.exe
Command Line	"C:\Program Files\Microsoft.NET\trillian.exe"
Initial Working Directory	C:\Program Files\Microsoft.NET\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194533, Reason: Terminated
Monitor duration	30.02s
Return Code	1073807364
PID	3900
Parent PID	4856
Bitness	32 Bit

Process #53: smartftp.exe

ID	53
File Name	c:\program files (x86)\microsoft sql server\smartftp.exe
Command Line	"C:\Program Files (x86)\Microsoft SQL Server\smartftp.exe"
Initial Working Directory	C:\Program Files (x86)\Microsoft SQL Server\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 195098, Reason: Terminated
Monitor duration	30.59s
Return Code	1073807364
PID	3872
Parent PID	4856
Bitness	32 Bit

Process #54: webdrive.exe

ID	54
File Name	c:\program files\java\webdrive.exe
Command Line	"C:\Program Files\Java\webdrive.exe"
Initial Working Directory	C:\Program Files\Java\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194529, Reason: Terminated
Monitor duration	30.02s
Return Code	1073807364
PID	3912
Parent PID	4856
Bitness	32 Bit

Process #55: yahoomessenger.exe

ID	55
File Name	c:\program files\uninstall information\yahoomessenger.exe
Command Line	"C:\Program Files\Uninstall Information\yahoomessenger.exe"
Initial Working Directory	C:\Program Files\Uninstall Information\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 195131, Reason: Terminated
Monitor duration	30.62s
Return Code	1073807364
PID	3952
Parent PID	4856
Bitness	32 Bit

Process #56: whatsapp.exe

ID	56
File Name	c:\program files\microsoft.net\whatsapp.exe
Command Line	"C:\Program Files\Microsoft.NET\whatsapp.exe"
Initial Working Directory	C:\Program Files\Microsoft.NET\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194505, Reason: Terminated
Monitor duration	30.00s
Return Code	1073807364
PID	3924
Parent PID	4856
Bitness	32 Bit

Process #57: winscp.exe

ID	57
File Name	c:\program files\windows multimedia platform\winscp.exe
Command Line	"C:\Program Files\Windows Multimedia Platform\winscp.exe"
Initial Working Directory	C:\Program Files\Windows Multimedia Platform\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 195114, Reason: Terminated
Monitor duration	30.61s
Return Code	1073807364
PID	3944
Parent PID	4856
Bitness	32 Bit

Process #58: accupos.exe

ID	58
File Name	c:\program files (x86)\windows portable devices\accupos.exe
Command Line	"C:\Program Files (x86)\Windows Portable Devices\accupos.exe"
Initial Working Directory	C:\Program Files (x86)\Windows Portable Devices\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194080, Reason: Terminated
Monitor duration	29.57s
Return Code	1073807364
PID	3980
Parent PID	4856
Bitness	32 Bit

Process #59: active-charge.exe

ID	59
File Name	c:\program files\microsoft analysis services\active-charge.exe
Command Line	"C:\Program Files\Microsoft Analysis Services\active-charge.exe"
Initial Working Directory	C:\Program Files\Microsoft Analysis Services\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194489, Reason: Terminated
Monitor duration	29.98s
Return Code	1073807364
PID	3964
Parent PID	4856
Bitness	32 Bit

Process #60: aldelo.exe

ID	60
File Name	c:\program files\microsoft.net\aldelo.exe
Command Line	"C:\Program Files\Microsoft.NET\aldelo.exe"
Initial Working Directory	C:\Program Files\Microsoft.NET\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194459, Reason: Terminated
Monitor duration	29.95s
Return Code	1073807364
PID	4000
Parent PID	4856
Bitness	32 Bit

Process #61: afr38.exe

ID	61
File Name	c:\program files\windows mail\afr38.exe
Command Line	"C:\Program Files\Windows Mail\afr38.exe"
Initial Working Directory	C:\Program Files\Windows Mail\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194471, Reason: Terminated
Monitor duration	29.96s
Return Code	1073807364
PID	3988
Parent PID	4856
Bitness	32 Bit

Process #62: centralcreditcard.exe

ID	62
File Name	c:\program files (x86)\windows mail\centralcreditcard.exe
Command Line	"C:\Program Files (x86)\Windows Mail\centralcreditcard.exe"
Initial Working Directory	C:\Program Files (x86)\Windows Mail\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194427, Reason: Terminated
Monitor duration	29.92s
Return Code	1073807364
PID	4024
Parent PID	4856
Bitness	32 Bit

Process #63: ccv_server.exe

ID	63
File Name	c:\program files (x86)\windowspowershell\ccv_server.exe
Command Line	"C:\Program Files (x86)\WindowsPowerShell\ccv_server.exe"
Initial Working Directory	C:\Program Files (x86)\WindowsPowerShell\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194442, Reason: Terminated
Monitor duration	29.93s
Return Code	1073807364
PID	4016
Parent PID	4856
Bitness	32 Bit

Process #64: fpos.exe

ID	64
File Name	c:\program files\common files\fpos.exe
Command Line	"C:\Program Files\Common Files\fpos.exe"
Initial Working Directory	C:\Program Files\Common Files\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 316955, Reason: Terminated by timeout
Monitor duration	152.45s
Return Code	Unknown
PID	4056
Parent PID	4856
Bitness	32 Bit

Process #65: edcsvr.exe

ID	65
File Name	c:\program files\windows nt\edcsvr.exe
Command Line	"C:\Program Files\Windows NT\edcsvr.exe"
Initial Working Directory	C:\Program Files\Windows NT\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194409, Reason: Terminated
Monitor duration	29.90s
Return Code	1073807364
PID	4048
Parent PID	4856
Bitness	32 Bit

Process #66: isspos.exe

ID	66
File Name	c:\program files (x86)\windows multimedia platform\isspos.exe
Command Line	"C:\Program Files (x86)\Windows Multimedia Platform\isspos.exe"
Initial Working Directory	C:\Program Files (x86)\Windows Multimedia Platform\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 192172, Reason: Terminated
Monitor duration	27.66s
Return Code	1073807364
PID	4072
Parent PID	4856
Bitness	32 Bit

Process #67: mxslipstream.exe

ID	67
File Name	c:\program files\microsoft office\mxslipstream.exe
Command Line	"C:\Program Files\Microsoft Office\mxslipstream.exe"
Initial Working Directory	C:\Program Files\Microsoft Office\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 316955, Reason: Terminated by timeout
Monitor duration	152.45s
Return Code	Unknown
PID	4080
Parent PID	4856
Bitness	32 Bit

Process #68: creditservice.exe

ID	68
File Name	c:\program files\windows journal\creditservice.exe
Command Line	"C:\Program Files\Windows Journal\creditservice.exe"
Initial Working Directory	C:\Program Files\Windows Journal\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 194395, Reason: Terminated
Monitor duration	29.89s
Return Code	1073807364
PID	4036
Parent PID	4856
Bitness	32 Bit

Process #69: omnipos.exe

ID	69
File Name	c:\program files\windowspowershell\omnipos.exe
Command Line	"C:\Program Files\WindowsPowerShell\omnipos.exe"
Initial Working Directory	C:\Program Files\WindowsPowerShell\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 316955, Reason: Terminated by timeout
Monitor duration	152.45s
Return Code	Unknown
PID	1080
Parent PID	4856
Bitness	32 Bit

Process #70: education.exe

ID	70
File Name	c:\program files (x86)\windows sidebar\education.exe
Command Line	"C:\Program Files (x86)\Windows Sidebar\education.exe"
Initial Working Directory	C:\Program Files (x86)\Windows Sidebar\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 316955, Reason: Terminated by timeout
Monitor duration	152.45s
Return Code	Unknown
PID	4124
Parent PID	4856
Bitness	32 Bit

Process #71: utg2.exe

ID	71
File Name	c:\program files\windowspowershell\utg2.exe
Command Line	"C:\Program Files\WindowsPowerShell\utg2.exe"
Initial Working Directory	C:\Program Files\WindowsPowerShell\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 316955, Reason: Terminated by timeout
Monitor duration	152.45s
Return Code	Unknown
PID	4116
Parent PID	4856
Bitness	32 Bit

Process #72: hairfederal.exe

ID	72
File Name	c:\program files (x86)\mozilla firefox\hairfederal.exe
Command Line	"C:\Program Files (x86)\Mozilla Firefox\hairfederal.exe"
Initial Working Directory	C:\Program Files (x86)\Mozilla Firefox\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 316955, Reason: Terminated by timeout
Monitor duration	152.45s
Return Code	Unknown
PID	4140
Parent PID	4856
Bitness	32 Bit

Process #73: thankclearly.exe

ID	73
File Name	c:\program files\windowspowershell\thankclearly.exe
Command Line	"C:\Program Files\WindowsPowerShell\thankclearly.exe"
Initial Working Directory	C:\Program Files\WindowsPowerShell\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 316955, Reason: Terminated by timeout
Monitor duration	152.45s
Return Code	Unknown
PID	4148
Parent PID	4856
Bitness	32 Bit

Process #74: learnget.exe

ID	74
File Name	c:\program files (x86)\windows multimedia platform\learnget.exe
Command Line	"C:\Program Files (x86)\Windows Multimedia Platform\learnget.exe"
Initial Working Directory	C:\Program Files (x86)\Windows Multimedia Platform\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 316955, Reason: Terminated by timeout
Monitor duration	152.45s
Return Code	Unknown
PID	4160
Parent PID	4856
Bitness	32 Bit

Process #75: spcwin.exe

ID	75
File Name	c:\program files\internet explorer\spcwin.exe
Command Line	"C:\Program Files\Internet Explorer\spcwin.exe"
Initial Working Directory	C:\Program Files\Internet Explorer\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 316955, Reason: Terminated by timeout
Monitor duration	152.45s
Return Code	Unknown
PID	3404
Parent PID	4856
Bitness	32 Bit

Process #76: spgagentservice.exe

ID	76
File Name	c:\program files\windows multimedia platform\spgagentservice.exe
Command Line	"C:\Program Files\Windows Multimedia Platform\spgagentservice.exe"
Initial Working Directory	C:\Program Files\Windows Multimedia Platform\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 316955, Reason: Terminated by timeout
Monitor duration	152.45s
Return Code	Unknown
PID	4104
Parent PID	4856
Bitness	32 Bit

Process #77: iexplore.exe

ID	77
File Name	c:\program files (x86)\internet explorer\iexplore.exe
Command Line	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:2284 CREDAT:82945 /prefetch:2
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 164509, Reason: Injection
Unmonitor End Time	End Time: 316955, Reason: Terminated by timeout
Monitor duration	152.45s
Return Code	Unknown
PID	4220
Parent PID	4856
Bitness	32 Bit

Process #78: schtasks.exe

ID	78
File Name	c:\windows\syswow64\schtasks.exe
Command Line	"C:\Windows\SysWOW64\schtasks.exe" /create /tn RtkAudioService64 /tr "C:\Users\RDhJ0CNFevzX\btpanui\SystemPropertiesPerformance.exe" /sc minute /mo 1 /F
Initial Working Directory	C:\Windows\SysWOW64\
Monitor Start Time	Start Time: 169598, Reason: Child Process
Unmonitor End Time	End Time: 173234, Reason: Terminated
Monitor duration	3.64s
Return Code	0
PID	4860
Parent PID	4484
Bitness	32 Bit

Host Behavior

Type	Count
Module	3
System	3
COM	1
File	6

Process #82: svchost.exe

ID	82
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: 216895, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 316955, Reason: Terminated by timeout
Monitor duration	100.06s
Return Code	Unknown
PID	864
Parent PID	4860
Bitness	64 Bit

Process #83: taskhostw.exe

ID	83
File Name	c:\windows\system32\taskhostw.exe
Command Line	taskhostw.exe SYSTEM
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 246126, Reason: Child Process
Unmonitor End Time	End Time: 316955, Reason: Terminated by timeout
Monitor duration	70.83s
Return Code	Unknown
PID	1084
Parent PID	864
Bitness	64 Bit

Process #85: sihost.exe

ID	85
File Name	c:\windows\system32\sihost.exe
Command Line	sihost.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 260155, Reason: Child Process
Unmonitor End Time	End Time: 316955, Reason: Terminated by timeout
Monitor duration	56.80s
Return Code	Unknown
PID	1328
Parent PID	864
Bitness	64 Bit

Process #86: locationnotificationwindows.exe

ID	86
File Name	c:\windows\system32\locationnotificationwindows.exe
Command Line	C:\Windows\System32\LocationNotificationWindows.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 261900, Reason: Child Process
Unmonitor End Time	End Time: 316955, Reason: Terminated
Monitor duration	55.05s
Return Code	0
PID	1420
Parent PID	864
Bitness	64 Bit

Process #89: taskhostw.exe

ID	89
File Name	c:\windows\system32\taskhostw.exe
Command Line	taskhostw.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 284851, Reason: Child Process
Unmonitor End Time	End Time: 316955, Reason: Terminated by timeout
Monitor duration	32.10s
Return Code	Unknown
PID	1864
Parent PID	864
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
27e5ab1169ea020b4f9f3bd3b1f176f0a64f3751942f2a544d0a14006076dd16	C:\Users\RDhJ0CNFevzX\Desktop\Adobe Download Manager.exe	Sample File	2063.55 KB	application/vnd.microsoft.portable-executable	Access, Read	MALICIOUS
4e8a99cd33c9e5c747a3ce8f1a3e17824846f4a8f7cb0631aebd0815db2ce3a4	C:\Users\RDHJ0C~1\AppData\Local\Temp\vnc.exe	Dropped File	405.50 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
7050608d53f80269df951d00883ed79815c060ce7678a76b5c3f6a2a985beea9	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\windef.exe, C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe, C:\Users\RDhJ0CNFevzX\AppData\Roaming\SubDir\winsock.exe	Dropped File	349.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
25000160aa1a06fd370be2a5cabce36c80fb12fbb1817e6ac67847dca7586295	C:\Users\RDhJ0CNFevzX\btpanui\SystemPropertiesPerformance.exe, SystemPropertiesPerformance.exe	Dropped File	2063.56 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
23e00bc877d9dfc46cd2d915c83c60eb4e81ba26cb01b098f5d76921f155bee1	-	Memory Dump	2088.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
5d495b339155370c29b067db8079388631ccfce4543292ca9b7efe300494491c	-	Code Dump File	128.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
aa3ed654344922ca23f929fd789aad9882cccb375057f389fa31889340972416	-	Memory Dump	2088.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
e1ef8d708f7b799e15d68c8597d1c9c587e9b99caa3eac3a8b5613e121a177f5	-	Memory Dump	376.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
0fe774d249d7c3093dd6b8de1c9c045f6efd4553710d877828e871e1be0e54f4	-	Memory Dump	112.50 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
8fc1fbdf1a853a4588481515d2d4b57d30df0f81bff1fa02fbc882ca75aa57c2	-	Memory Dump	2088.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
aaea59fe3efcda5715dd4e19a95c1ab792d720eaef875a29e371f1b7fa690b95	-	Memory Dump	128.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
c287e02efbd76af057f666b61d55d12cba8f519097eada47a402f8344f943779	-	Memory Dump	128.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
4ffda485cbcf2693a98dc2aabbd417fe4bb21e6a9b76feddea54b6f218bd1d30	-	Memory Dump	128.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
a4df02aab13454210ad5a90ca400154cab5f3c8df213ddeb12dff8b0dc8cb8ba	-	Memory Dump	128.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
a827628cc9c96987810eea5d946f6803a0bbbc61f0c097b56a29ca81a8b5912a	-	Memory Dump	128.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
b74e49e4781c980e1c4cc10692624c7bdf93656b299ca6f8089d01c4d084695e	-	Memory Dump	128.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
e079b0b40d4c7c4c73cdd75e926309dd2a9087851bc81ff032aba661972e4017	-	Memory Dump	128.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
76020f9d9d2b98191e5489bef6a663b9fc7973207c91ab361202b74f6b9af8c6	-	Memory Dump	128.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
7a2ca0af2e7f805f8d97ad4d845d75e02f31284670878113a7c16dff1bd0267b	-	Memory Dump	128.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
dceb6fa694b65604c4c44d7ca6fabed0d5ea3c7fca449e553365ff62f20b06ab	-	Memory Dump	128.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
f92993ca366d96e280cc56453ea4a389b44b3a1d50be6551de20bde6d658e894	-	Memory Dump	128.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
28b90965d78cbc8579bf8678d31d9d6b3886ec11e34030ad978e137f0696d263	-	Extracted File	13.47 KB	image/png	-	CLEAN
acce7bf50072acc7fd91ba76beec9c319c9673ad8244acb3b29605424ad721f9	C:\Users\RDhJ0CNFevzX\AppData\Roaming\Logs\02-07-2024	Dropped File	224 bytes	application/octet-stream	Access, Create, Write	CLEAN
c2d814a34b184b7cdf10e4e7a4311ff15db99326d6dd8d328b53bf9e19ccf858	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\counters.dat	Modified File	128 bytes	application/octet-stream	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\Adobe Download Manager.exe	Accessed File, Sample File	Access, Read	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Roaming\SubDir\winsock.exe	Accessed File, Dropped File, Extracted File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Logs	Accessed File	Access, Create	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\windef.exe	Accessed File, Dropped File, Extracted File	Access, Create, Write	SUSPICIOUS
C:\Users\RDhJ0CNFevzX\btpanui\SystemPropertiesPerformance.exe	Accessed File, Dropped File	Access, Create, Write	SUSPICIOUS
C:\Users\RDHJ0C~1\AppData\Local\Temp\vnc.exe	Accessed File, Dropped File, Extracted File	Access, Create, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Logs\02-07-2024	Accessed File, Dropped File	Access, Create, Write	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\counters.dat	Modified File	-	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\Adobe Download Manager.exe:Zone.Identifier	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\windef.exe.config	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe:Zone.Identifier	Accessed File	Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\SubDir	Accessed File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\schtasks.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\SubDir\winsock.exe:Zone.Identifier	Accessed File	Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\SubDir\winsock.exe.config	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\btpanui	Accessed File	Access, Create	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxp://0x21[.]jin:8000/_az/	Extracted	-	-	-	MALICIOUS
hxxp://5[.]8[.]88[.]191:443	Extracted	5.8.88.191	Russia	-	MALICIOUS
hxxp://sockartek[.]icu:443	Extracted	-	-	-	MALICIOUS

Domain

Domain	IP Address	Country	Protocols	Verdict
0x21[.]in	-	-	-	MALICIOUS
ip-api[.]com	208.95.112.1	United States	TCP, DNS, HTTP	CLEAN
sockartek[.]icu	-	-	-	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
5.8.88.191	-	Russia	TCP	MALICIOUS
208.95.112.1	ip-api[.]com	United States	TCP, DNS, HTTP	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
QSR_MUTEX_0kBRNrRz5TDLEQoul0	access	windef.exe, winsock.exe	MALICIOUS
runas	access	adobe download manager.exe	CLEAN
A743A547-9C1AFDB0-AEA27C97-73E39B07-D5BBC660F	access	adobe download manager.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Control Panel\Mouse	access	adobe download manager.exe	CLEAN
HKEY_CURRENT_USER\Control Panel\Mouse\SwapMouseButtons	access, read	adobe download manager.exe	CLEAN
HKEY_CURRENT_USER\Software\AutoIt v3\AutoIt	access	adobe download manager.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	windef.exe, winsock.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	windef.exe, winsock.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	access, read	windef.exe, winsock.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	windef.exe, winsock.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	windef.exe, winsock.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	access	windef.exe, winsock.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework	access	windef.exe, winsock.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\LegacyWPADSupport	access, read	windef.exe, winsock.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	windef.exe, winsock.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	access, read	windef.exe, winsock.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	windef.exe, winsock.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	access, read	windef.exe, winsock.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	access, read	windef.exe, winsock.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	access, read	windef.exe, winsock.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	windef.exe, winsock.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	access, read	windef.exe, winsock.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	winsock.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	access, read	winsock.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	access, read	winsock.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography	access	adobe download manager.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid	access, read	adobe download manager.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	access, create	adobe download manager.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName	access, read	adobe download manager.exe	CLEAN

Process

Process Name	Commandline	Verdict
adobe download manager.exe	"C:\Users\RDhJ0CNFevzX\Desktop\Adobe Download Manager.exe"	MALICIOUS
vnc.exe	"C:\Users\RDHJ0C~1\AppData\Local\Temp\vnc.exe"	MALICIOUS
windef.exe	"C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe"	MALICIOUS
adobe download manager.exe	"C:\Users\RDhJ0CNFevzX\Desktop\Adobe Download Manager.exe"	MALICIOUS
winsock.exe	"C:\Users\RDhJ0CNFevzX\AppData\Roaming\SubDir\winsock.exe"	MALICIOUS
schtasks.exe	"schtasks" /create /tn "win defender run" /sc ONLOGON /tr "C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe" /rl HIGHEST /f	SUSPICIOUS
schtasks.exe	"schtasks" /create /tn "win defender run" /sc ONLOGON /tr "C:\Users\RDhJ0CNFevzX\AppData\Roaming\SubDir\winsock.exe" /rl HIGHEST /f	SUSPICIOUS
schtasks.exe	"C:\Windows\SysWOW64\schtasks.exe" /create /tn RtkAudioService64 /tr "C:\Users\RDhJ0CNFevzX\btpanui\SystemPropertiesPerformance.exe" /sc minute /mo 1 /F	SUSPICIOUS
magazine.exe	"C:\Program Files (x86)\Mozilla Firefox\magazine.exe"	CLEAN
better.exe	"C:\Program Files (x86)\Windows Defender\better.exe"	CLEAN
run-service-who.exe	"C:\Program Files (x86)\Windows Defender\run-service-who.exe"	CLEAN
big.exe	"C:\Program Files\Windows Defender\big.exe"	CLEAN
production tend.exe	"C:\Program Files\Windows NT\production tend.exe"	CLEAN
painting.exe	"C:\Program Files (x86)\Microsoft Office\painting.exe"	CLEAN
armalreadyoutside.exe	"C:\Program Files\Windows Photo Viewer\armalreadyoutside.exe"	CLEAN
particular-crime.exe	"C:\Program Files (x86)\Common Files\particular-crime.exe"	CLEAN
sea-travel-style.exe	"C:\Program Files (x86)\MSBuild\sea-travel-style.exe"	CLEAN
behind-town.exe	"C:\Program Files (x86)\Windows Media Player\behind-town.exe"	CLEAN
player_pay_half.exe	"C:\Program Files\Microsoft SQL Server\player_pay_half.exe"	CLEAN
privateperformborn.exe	"C:\Program Files\Windows NT\privateperformborn.exe"	CLEAN
for receive.exe	"C:\Program Files\Microsoft Office\for receive.exe"	CLEAN
meet_seat_sometimes.exe	"C:\Program Files (x86)\Windows Multimedia Platform\meet_seat_sometimes.exe"	CLEAN

Process Name	Commandline	Verdict
institution_big_direction.exe	"C:\Program Files\MSBuild\institution_big_direction.exe"	CLEAN
3dftp.exe	"C:\Program Files (x86)\Mozilla Firefox\3dftp.exe"	CLEAN
absolutetelnet.exe	"C:\Program Files\Microsoft Office\absolutetelnet.exe"	CLEAN
alftp.exe	"C:\Program Files\Uninstall Information\alftp.exe"	CLEAN
barca.exe	"C:\Program Files\Uninstall Information\barca.exe"	CLEAN
bitkinex.exe	"C:\Program Files\MSBuild\bitkinex.exe"	CLEAN
coreftp.exe	"C:\Program Files\Java\coreftp.exe"	CLEAN
far.exe	"C:\Program Files\Windows Journal\far.exe"	CLEAN
filezilla.exe	"C:\Program Files\Windows Sidebar\filezilla.exe"	CLEAN
flashfxp.exe	"C:\Program Files\Windows Mail\flashfxp.exe"	CLEAN
fling.exe	"C:\Program Files\Windows Journal\fling.exe"	CLEAN
foxmailincmail.exe	"C:\Program Files\Uninstall Information\foxmailincmail.exe"	CLEAN
gmailnotifierpro.exe	"C:\Program Files (x86)\Windows Mail\gmailnotifierpro.exe"	CLEAN
icq.exe	"C:\Program Files\Windows Mail\icq.exe"	CLEAN
leechftp.exe	"C:\Program Files (x86)\Windows Portable Devices\leechftp.exe"	CLEAN
ncftp.exe	"C:\Program Files (x86)\Windows Multimedia Platform\ncftp.exe"	CLEAN
notepad.exe	"C:\Program Files (x86)\Microsoft Analysis Services\notepad.exe"	CLEAN
operamail.exe	"C:\Program Files (x86)\Microsoft SQL Server\operamail.exe"	CLEAN
outlook.exe	"C:\Program Files\Internet Explorer\outlook.exe"	CLEAN
pidgin.exe	"C:\Program Files (x86)\Windows Mail\pidgin.exe"	CLEAN
scriptftp.exe	"C:\Program Files (x86)\Microsoft Office\scriptftp.exe"	CLEAN
skype.exe	"C:\Program Files (x86)\Microsoft Office\skype.exe"	CLEAN
smartftp.exe	"C:\Program Files (x86)\Microsoft SQL Server\smartftp.exe"	CLEAN
thunderbird.exe	"C:\Program Files\Common Files\thunderbird.exe"	CLEAN
trillian.exe	"C:\Program Files\Microsoft.NET\trillian.exe"	CLEAN
webdrive.exe	"C:\Program Files\Java\webdrive.exe"	CLEAN
whatsapp.exe	"C:\Program Files\Microsoft.NET\whatsapp.exe"	CLEAN
winscp.exe	"C:\Program Files\Windows Multimedia Platform\winscp.exe"	CLEAN
yahoomessenger.exe	"C:\Program Files\Uninstall Information\yahoomessenger.exe"	CLEAN
active-charge.exe	"C:\Program Files\Microsoft Analysis Services\active-charge.exe"	CLEAN
accupos.exe	"C:\Program Files (x86)\Windows Portable Devices\accupos.exe"	CLEAN
afr38.exe	"C:\Program Files\Windows Mail\afr38.exe"	CLEAN
aldelo.exe	"C:\Program Files\Microsoft.NET\aldelo.exe"	CLEAN
ccv_server.exe	"C:\Program Files (x86)\WindowsPowerShell\ccv_server.exe"	CLEAN
centralcreditcard.exe	"C:\Program Files (x86)\Windows Mail\centralcreditcard.exe"	CLEAN
creditservice.exe	"C:\Program Files\Windows Journal\creditservice.exe"	CLEAN

Process Name	Commandline	Verdict
edcsvr.exe	"C:\Program Files\Windows NT\edcsvr.exe"	CLEAN
fpos.exe	"C:\Program Files\Common Files\fpos.exe"	CLEAN
isspos.exe	"C:\Program Files (x86)\Windows Multimedia Platform\isspos.exe"	CLEAN
mxslipstream.exe	"C:\Program Files\Microsoft Office\mxslipstream.exe"	CLEAN
omnipos.exe	"C:\Program Files\WindowsPowerShell\omnipos.exe"	CLEAN
spcwin.exe	"C:\Program Files\Internet Explorer\spcwin.exe"	CLEAN
spgagentservice.exe	"C:\Program Files\Windows Multimedia Platform\spgagentservice.exe"	CLEAN
utg2.exe	"C:\Program Files\WindowsPowerShell\utg2.exe"	CLEAN
education.exe	"C:\Program Files (x86)\Windows Sidebar\education.exe"	CLEAN
hairfederal.exe	"C:\Program Files (x86)\Mozilla Firefox\hairfederal.exe"	CLEAN
thankclearly.exe	"C:\Program Files\WindowsPowerShell\thankclearly.exe"	CLEAN
learnget.exe	"C:\Program Files (x86)\Windows Multimedia Platform\learnget.exe"	CLEAN
iexplore.exe	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:2284 CREDAT:82945 /prefetch:2	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
taskhostw.exe	taskhostw.exe SYSTEM	CLEAN
sihost.exe	sihost.exe	CLEAN
locationnotificationwindows.exe	C:\Windows\System32\LocationNotificationWindows.exe	CLEAN
taskhostw.exe	taskhostw.exe	CLEAN

YARA / AV

YARA (22)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	Azorult_Generic	Azorult v2 and v3	Memory Dump	-	Spyware	5/5
RATs	QuasarRAT	QuasarRAT	Sample File	C:\Users\RDhJ0CNFevzX\Desktop\Adobe Download Manager.exe	Backdoor	5/5
Malware	Azorult_Generic	Azorult v2 and v3	Memory Dump	-	Spyware	5/5
Malware	Azorult_Generic	Azorult v2 and v3	Memory Dump	-	Spyware	5/5
Malware	Azorult_Generic	Azorult v2 and v3	Memory Dump	-	Spyware	5/5
Malware	Azorult_Generic	Azorult v2 and v3	Memory Dump	-	Spyware	5/5
Malware	Azorult_Generic	Azorult v2 and v3	Memory Dump	-	Spyware	5/5
Malware	Azorult_Generic	Azorult v2 and v3	Memory Dump	-	Spyware	5/5
Malware	Azorult_Generic	Azorult v2 and v3	Memory Dump	-	Spyware	5/5
RATs	QuasarRAT	QuasarRAT	Memory Dump	-	Backdoor	5/5
RATs	xRAT_1	xRAT malware	Memory Dump	-	Backdoor	5/5
RATs	QuasarRAT	QuasarRAT	Memory Dump	-	Backdoor	5/5
RATs	QuasarRAT	QuasarRAT	Memory Dump	-	Backdoor	5/5
RATs	QuasarRAT	QuasarRAT	Memory Dump	-	Backdoor	5/5
Malware	Azorult_Generic	Azorult v2 and v3	Memory Dump	-	Spyware	5/5
Malware	Azorult_Generic	Azorult v2 and v3	-	-	Spyware	5/5
RATs	xRAT_1	xRAT malware	Dropped File	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\windef.exe	Backdoor	5/5
RATs	QuasarRAT	QuasarRAT	Dropped File	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\windef.exe	Backdoor	5/5
Malware	Azorult_Generic	Azorult v2 and v3	Memory Dump	-	Spyware	5/5
Malware	Azorult_Generic	Azorult v2 and v3	Memory Dump	-	Spyware	5/5
Malware	Azorult_Generic	Azorult v2 and v3	Memory Dump	-	Spyware	5/5
RATs	QuasarRAT	QuasarRAT	Dropped File	C:\Users\RDhJ0CNFevzX\btpanui\SystemPropertiesPerformance.exe	Backdoor	5/5

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_mso2016
Description	windows 10 (64bit TH2 -EN- MSO_2016)
Architecture	x86 64-bit
Operating System	Windows 10 Threshold 2
Kernel Version	10.0.10586.0 (0de6dc23-8e19-4bb7-8608-d54b1e6fa379)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	2024.1.0
Dynamic Engine Version	2024.1.0 / 01/04/2024 17:31
Static Engine Version	2024.1.0.0 / 2024-01-04 16:05:55
AV Exceptions Version	2024.1.2.19 / 2024-01-30 23:09:03
Link Detonation Heuristics Version	2024.1.2.20 / 2024-02-01 16:04:36
Smart Memory Dumping Rules Version	2024.1.2.19 / 2024-01-30 23:09:03
Config Extractors Version	2024.1.2.20 / 2024-02-01 16:04:36
Signature Trust Store Version	2024.1.2.19 / 2024-01-30 23:09:03
VMRay Threat Identifiers Version	2024.1.2.20 / 2024-02-01 16:04:36
YARA Built-in Ruleset Version	2024.1.2.21

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1001
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	11.0.10586.0
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	8.0.1710.11

System Information

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

System Root	C:\Windows