MALICIOUS

Classifications: Backdoor

Threat Names: NanoCore, Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe**
ID	#5067790
MD5	583524e79bf439fe42fc992fea5d75f9
SHA1	433e13004fc64ef09412e0ac57cc42492eb9b327
SHA256	fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18
File Size	782.00 KB
Report Created	2022-08-05 15:28 (UTC+2)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (19 rules, 24 matches)

Score	Category	Operation	Count	Classification
5/5	Extracted Configuration	NanoCore configuration was extracted	1	Backdoor
	• A configuration for NanoCore was extracted from artifacts of the dynamic analysis.			
5/5	YARA	Malicious content matched by YARA rules	2	Backdoor
	• Rule "NanoCoreRAT" from ruleset "RATs" has matched on a code dump for (process #1) fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe. • Rule "NanoCoreRAT" from ruleset "RATs" has matched on a memory dump for (process #4) fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe.			
4/5	Defense Evasion	Obscures a file's origin	1	-
	• (Process #4) fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe tries to delete zone identifier of file "C:\Users\kEecfMwgj\Desktop\fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe".			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as Mal/Generic-S.			
2/5	Hide Tracks	Deletes file after execution	1	-
	• (Process #4) fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe deletes executed executable "C:\Program Files (x86)\AGP Subsystem\agpss.exe".			
2/5	Network Connection	Sets up server that accepts incoming connections	1	Backdoor
	• (Process #4) fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe starts a TCP server listening on port 49159.			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	1	-
	• (Process #1) fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe modifies memory of (process #4) fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
	• (Process #1) fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe alters context of (process #4) fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe.			
2/5	Task Scheduling	Schedules task	2	-
	• Schedules task for command "C:\Users\kEecfMwgj\AppData\Roaming\nFxloujoILCO.exe", to be triggered by LOGON. • Schedules task for command "C:\Users\kEecfMwgj\AppData\Roaming\nFxloujoILCO.exe", to be triggered by REGISTRATION.			
1/5	Hide Tracks	Creates process with hidden window	4	-
	• (Process #1) fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe starts (process #2) powershell.exe with a hidden window. • (Process #1) fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe starts (process #3) schtasks.exe with a hidden window. • (Process #1) fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe starts (process #1) fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe with a hidden window. • (Process #4) fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe starts (process #4) fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe with a hidden window.			
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #1) fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe reads from (process #1) fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-

Score	Category	Operation	Count	Classification
	• (Process #1) fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.			
1/5	Mutex	Creates mutex	1	-
	• (Process #4) fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe creates mutex with name "Global\{7492bd48-e55d-4165-b6f8-ba286e7dc450}".			
1/5	Discovery	Reads system data	1	-
	• (Process #4) fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe reads the cryptographic machine GUID from registry.			
1/5	Persistence	Installs system startup script or application	1	-
	• (Process #4) fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe adds "C:\Program Files (x86)\AGP Subsystem\agpss.exe" to Windows startup via registry.			
1/5	Privilege Escalation	Enables process privilege	1	-
	• (Process #4) fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe enables process privilege "SeDebugPrivilege".			
1/5	Discovery	Enumerates running processes	1	-
	• (Process #4) fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe enumerates running processes.			
1/5	Network Connection	Connects to remote host	1	-
	• (Process #4) fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe opens an outgoing TCP connection to host "79.134.225.53:7171".			
1/5	Network Connection	Tries to connect using an uncommon port	1	-
	• (Process #4) fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe tries to connect to TCP port 7171 at 79.134.225.53.			

Malware Configuration: NanoCore

Metadata	Key	Extracted Value
Version	Value	1.2.2.0
Mutex	Value	7492bd48-e55d-4165-b6f8-ba286e7dc450
Socket	Address Port C2	79.134.225.53 7171 ✔
Interval	Tags Value	ConnectDelay 4000.0
	Tags Value	RestartDelay 5000.0
	Tags Value	RunDelay 0.0
	Tags Value	TimeoutInterval 5000.0
Other: RunOnStartup	Value	✔
Other: RequestElevation	Value	✖
Other: BypassUAC	Value	✔
Other: ClearZoneIdentifier	Value	✔
Other: ClearAccessControl	Value	✖
Other: SetCriticalProcess	Value	✖
Other: PreventSystemSleep	Value	✔
Other: EnableDebugMode	Value	✖

Mitre ATT&CK Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1053 Scheduled Task	#T1060 Registry Run Keys / Startup Folder	#T1053 Scheduled Task	#T1143 Hidden Window		#T1082 System Information Discovery			#T1065 Uncommonly Used Port		
		#T1053 Scheduled Task		#T1045 Software Packing		#T1012 Query Registry					
				#T1112 Modify Registry		#T1057 Process Discovery					
				#T1096 NTFS File Attributes							

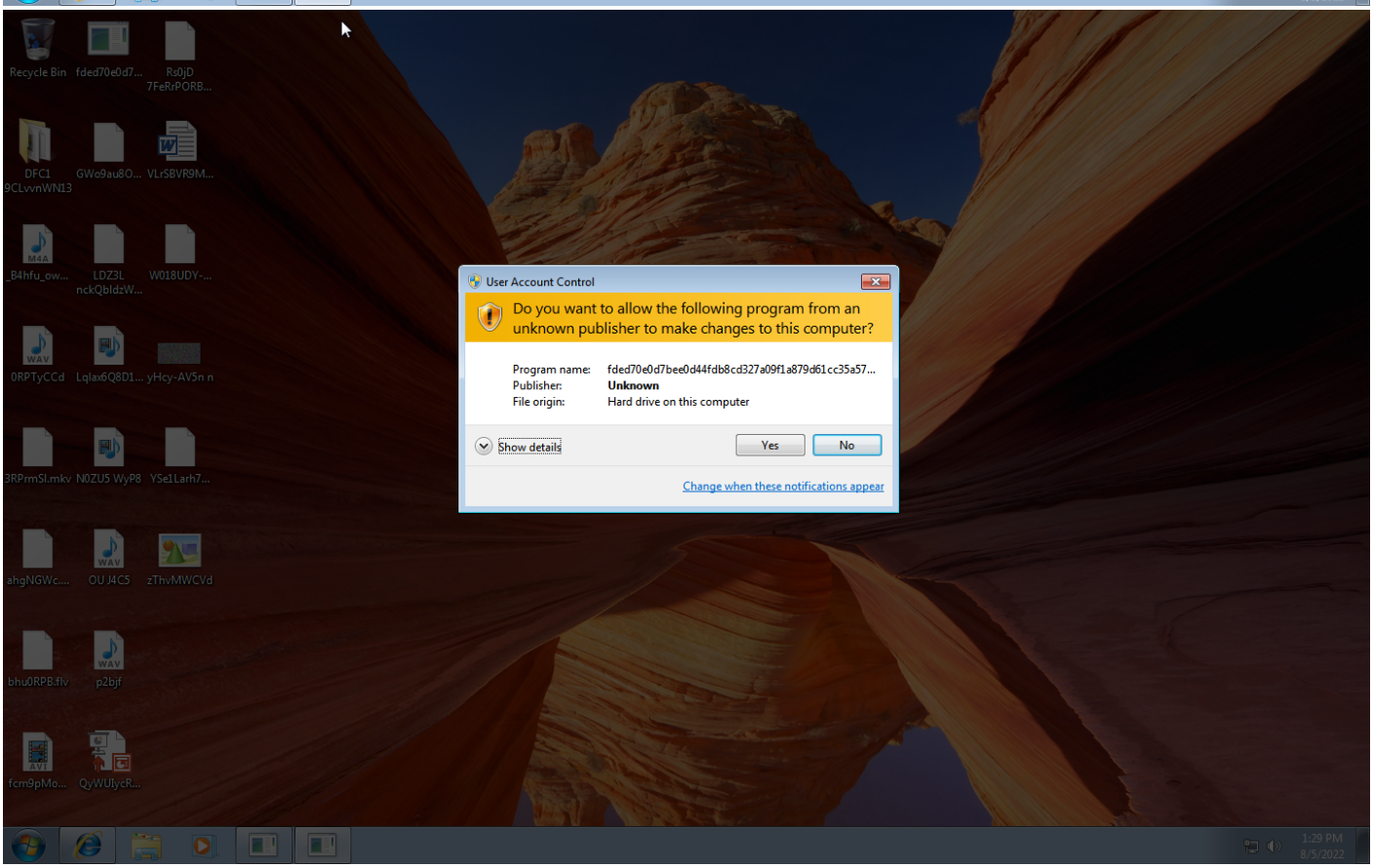
Sample Information

ID	#5067790
MD5	583524e79bf439fe42fc992fea5d75f9
SHA1	433e13004fc64ef09412e0ac57cc42492eb9b327
SHA256	fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18
SSDeep	24576:/l4lNIPllllplUIlllllllllllllIUlUUPllllUlUllbUllbT9dDZH1m3q+lVKbk0Q:/l4lNIPllllplUIlllllllllllllIUlUUt
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe
File Size	782.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2022-08-05 15:28 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	9
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


Recycle Bin
fded70e0d7...
Rs0jD
7FeRrPORB...
DFC1
9CLvvnWN13
GWo9au8O...
VLrSBVR9M...
_B4hfu_ow...
LDZ3L
nckQbIdzW...
W018UDY-...
0RPTyCCd
Lqlax6Q8D1...
yHcy-AV5n n
3RPrmSl.mkv
N0ZU5 WyP8
YSe1Larh7...
ahgNGWc....
OU J4C5
zThvMWCVd
bhu0RPB.flv
p2bjf
fcm9pMo...
QyWUlycR...
1:29 PM
8/5/2022


User Account Control
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Program name: fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear

Screenshots truncated

NETWORK

General

152 bytes total sent

120 bytes total received

1 ports 7171

1 contacted IP addresses

1 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

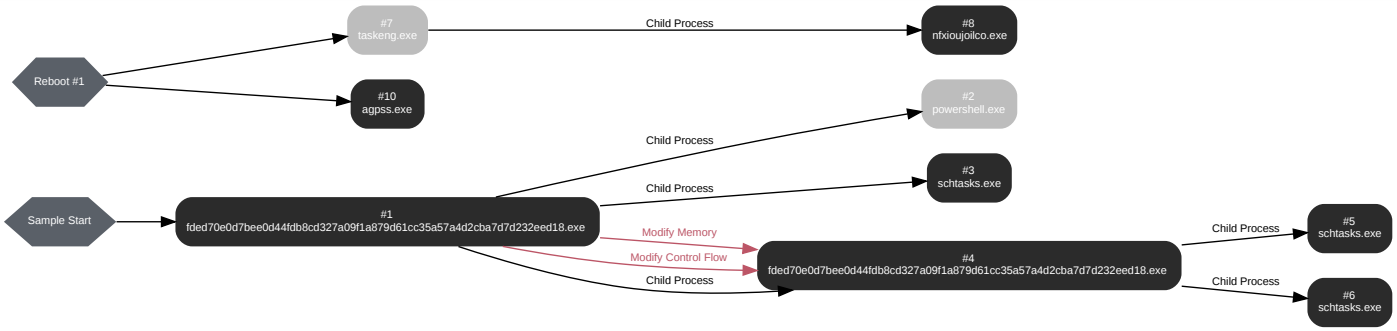
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 45977, Reason: Analysis Target
Unmonitor End Time	End Time: 159096, Reason: Terminated
Monitor duration	113.12s
Return Code	0
PID	3936
Parent PID	1916
Bitness	32 Bit

Dropped Files (4)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\Desktop\fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe	782.00 KB	fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18	✖
C:\Users\kEecfMwgj\AppData\Local\Temp\tmpC690.tmp	1.56 KB	19655acbfeaf3c70e713a44fa36beca214ce51283e6a777d83ae76bcd8b91399	✖
-	8.03 KB	c5e68bc6ec9388f0b0be98a6100459c5573044e269a87f804dac29c025505f52	✖
-	108.54 KB	7d41c8cc04967418bc2d9f627955932ad8b9069cfd79e6a97016f9146e578c41	✖

Host Behavior

Type	Count
Registry	4
File	29
Module	37
Window	6
User	1
Process	3
-	3
-	7

Process #2: powershell.exe

ID	2
File Name	c:\windows\syswow64\windowspowershell\v1.0\powershell.exe
Command Line	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\kEecfMwgj\AppData\Roaming\nFxloujolLCO.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 152143, Reason: Child Process
Unmonitor End Time	End Time: 181272, Reason: Terminated
Monitor duration	29.13s
Return Code	1073807364
PID	4040
Parent PID	3936
Bitness	32 Bit

Process #3: schtasks.exe

ID	3
File Name	c:\windows\syswow64\schtasks.exe
Command Line	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\nFxIoujoILCO" /XML "C:\Users\kEecfMwgj\AppData\Local\Temp\tmpC690.tmp"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 152666, Reason: Child Process
Unmonitor End Time	End Time: 156007, Reason: Terminated
Monitor duration	3.34s
Return Code	0
PID	4060
Parent PID	3936
Bitness	32 Bit

Host Behavior

Type	Count
System	2
Module	7
COM	1
File	9

Process #4: fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe

ID	4
File Name	c:\users\keecfmwgj\desktop\fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 156820, Reason: Child Process
Unmonitor End Time	End Time: 181089, Reason: Terminated
Monitor duration	24.27s
Return Code	1073807364
PID	2096
Parent PID	3936
Bitness	32 Bit

Injection Information (6)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\keecfmwgj\desktop\fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe	0xf64	0x400000(4194304)	0x200	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe	0xf64	0x402000(4202496)	0x1c800	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe	0xf64	0x420000(4325376)	0x200	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe	0xf64	0x422000(4333568)	0x16000	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe	0xf64	0x7efde008(2130567176)	0x4	✔	1
Modify Control Flow	#1: c:\users\keecfmwgj\desktop\fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe	0xf64 / 0x5c0	0x41e792(4319122)	-	✔	1

Dropped Files (6)

File Name	File Size	SHA256	YARA Match
C:\Program Files (x86)\AGP Subsystem\agpss.exe	782.00 KB	fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18	✖
C:\Users\kEecfMwgj\AppData\Roaming\B9C8F16E-2E51-4052-9ECB-F86AE5D96EF6\run.dat	8 bytes	bb32e00d8f24fef8c0672fe8781f2be4a46f50f5fd78421e6210b436b58f9fc8	✖
C:\Users\kEecfMwgj\AppData\Roaming\B9C8F16E-2E51-4052-9ECB-F86AE5D96EF6\task.dat	95 bytes	610fcf9c824091895c008cc9d998a23401ca21d2ad1355fc4a0c093a48eb5cda	✖
C:\Users\kEecfMwgj\AppData\Local\Temp\tmpFD29.tmp	1.33 KB	b29e7f9a093d2f3d64f6ac96b4ec8b34a9db2c05c45058af547e926438e3ba08	✖
C:\Users\kEecfMwgj\AppData\Roaming\B9C8F16E-2E51-4052-9ECB-F86AE5D96EF6\settings.bin	8 bytes	3c099e8a656f6d63978ecb6dd8d4c8eacdb689bb2f748314550dc78a05f30d95	✖

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp17.tmp	1.28 KB	ccd9d374a356e8635fe06015e07c986fb0e6f71099234ddc2935a6cb5e1571ac	✖

Host Behavior

Type	Count
Registry	25
File	71
Module	20
Window	14
System	76
Mutex	1
Process	9
User	4
Keyboard	10
Environment	2

Network Behavior

Type	Count
TCP	1

Process #5: schtasks.exe

ID	5
File Name	c:\windows\syswow64\schtasks.exe
Command Line	"schtasks.exe" /create /f /tn "AGP Subsystem" /xml "C:\Users\kEecfMwgj\AppData\Local\Temp\tmpFD29.tmp"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 169301, Reason: Child Process
Unmonitor End Time	End Time: 170972, Reason: Terminated
Monitor duration	1.67s
Return Code	0
PID	2000
Parent PID	2096
Bitness	32 Bit

Host Behavior

Type	Count
System	2
Module	7
COM	1
File	9

Process #6: schtasks.exe

ID	6
File Name	c:\windows\syswow64\schtasks.exe
Command Line	"schtasks.exe" /create /f /tn "AGP Subsystem Task" /xml "C:\Users\kEecfMwgj\AppData\Local\Temp\tmp17.tmp"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 170023, Reason: Child Process
Unmonitor End Time	End Time: 171828, Reason: Terminated
Monitor duration	1.80s
Return Code	0
PID	1504
Parent PID	2096
Bitness	32 Bit

Host Behavior

Type	Count
System	2
Module	7
COM	1
File	9

Process #7: taskeng.exe

ID	7
File Name	c:\windows\system32\taskeng.exe
Command Line	taskeng.exe {6D9545EF-31E1-4286-8B8C-42C7F98001F2} S-1-5-21-4219442223-4223814209-3835049652-1000:Q9IATRKPRH\kEecfMwgj:Interactive:LUA[1]
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 222756, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 285985, Reason: Terminated by timeout
Monitor duration	63.23s
Return Code	Unknown
PID	1232
Parent PID	1504
Bitness	64 Bit

Process #8: nfxioujoilco.exe

ID	8
File Name	c:\users\keecfmwgj\appdata\roaming\nfxioujoilco.exe
Command Line	C:\Users\kEecfMwgj\AppData\Roaming\nFxIoujoILCO.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 229023, Reason: Child Process
Unmonitor End Time	End Time: 285985, Reason: Terminated by timeout
Monitor duration	56.96s
Return Code	Unknown
PID	1328
Parent PID	1232
Bitness	32 Bit

Host Behavior

Type	Count
Registry	4
File	20
Module	11
Window	4

Process #10: agpss.exe

ID	10
File Name	c:\program files (x86)\agp subsystem\agpss.exe
Command Line	"C:\Program Files (x86)\AGP Subsystem\agpss.exe"
Initial Working Directory	C:\Windows\SysWOW64\
Monitor Start Time	Start Time: 246823, Reason: Autostart
Unmonitor End Time	End Time: 285985, Reason: Terminated by timeout
Monitor duration	39.16s
Return Code	Unknown
PID	1836
Parent PID	2096
Bitness	32 Bit

Host Behavior

Type	Count
Registry	4
File	20
Module	11
Window	4

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18	C:\Program Files (x86)\AGP Subsystem\agpss.exe, C:\Users\kEecfMwgj\Desktop\fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe, C:\Users\kEecfMwgj\AppData\Roaming\nFxloujolLCO.exe	Sample File	782.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Delete, Write	MALICIOUS
bb32e00d8f24fef8c0672fe8781f2be4a46f50f5fd78421e6210b436b58f9fc8	C:\Users\kEecfMwgj\AppData\Roaming\B9C8F16E-2E51-4052-9ECB-F86AE5D96EF6\run.dat	Dropped File	8 bytes	text/plain	Access, Create, Write	CLEAN
19655acbfeaf3c70e713a44fa36beca214ce51283e6a777d83ae76bcd8b91399	C:\Users\kEecfMwgj\AppData\Local\Temp\tmpC690.tmp	Dropped File	1.56 KB	text/xml	Access, Create, Delete, Read, Write	CLEAN
610fcf9c824091895c008cc9d998a23401ca21d2ad1355fc4a0c093a48eb5cda	C:\Users\kEecfMwgj\AppData\Roaming\B9C8F16E-2E51-4052-9ECB-F86AE5D96EF6\task.dat	Dropped File	95 bytes	text/plain	Access, Create, Write	CLEAN
37af1cc5a7606c4cce476c2324b066c3a7f625eee010baf8347937ad13fd4081	-	Extracted File	851 bytes	image/png	-	CLEAN
c5e68bc6ec9388f0b0be98a6100459c5573044e269a87f804dac29c025505f52	-	Dropped File	8.03 KB	application/octet-stream	-	CLEAN
b29e7f9a093d2f3d64f6ac96b4ec8b34a9db2c05c45058af547e926438e3ba08	C:\Users\kEecfMwgj\AppData\Local\Temp\tmpFD29.tmp	Dropped File	1.33 KB	text/xml	Access, Create, Delete, Read, Write	CLEAN
3c099e8a656f6d63978ecb6dd8d4c8eacdb689bb2f748314550dc78a05f30d95	C:\Users\kEecfMwgj\AppData\Roaming\B9C8F16E-2E51-4052-9ECB-F86AE5D96EF6\settings.bin	Dropped File	8 bytes	application/octet-stream	Access, Create, Write	CLEAN
ccd9d374a356e8635fe06015e07c986fb0e6f71099234ddc2935a6cb5e1571ac	C:\Users\kEecfMwgj\AppData\Local\Temp\tmp17.tmp	Dropped File	1.28 KB	text/xml	Access, Create, Delete, Read, Write	CLEAN
7d41c8cc04967418bc2d9f627955932ad8b9069cfd79e6a97016f9146e578c41	-	Dropped File	108.54 KB	application/octet-stream	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Desktop\fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe	Sample File, Accessed File, VM File	Access	MALICIOUS
C:\Program Files (x86)\AGP Subsystem\agpss.exe	Dropped File, Accessed File, VM File	Access, Create, Delete, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\nFxloujolLCO.exe	Dropped File, Accessed File, VM File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\B9C8F16E-2E51-4052-9ECB-F86AE5D96EF6\storage.dat	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\B9C8F16E-2E51-4052-9ECB-F86AE5D96EF6\Exceptions\1.2.2.0	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\B9C8F16E-2E51-4052-9ECB-F86AE5D96EF6\task.dat	Dropped File, Accessed File	Access, Create, Write	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\tmpFD29.tmp	Dropped File, Accessed File	Access, Create, Delete, Read, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\AppData\Roaming\B9C8F16E-2E51-4052-9ECB-F86AE5D96EF6\Logs\kEecfMwgj	Accessed File	Access, Create	CLEAN
C:\Windows\SysWOW64\schtasks.exe	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\Desktop\fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe.config	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\tmpC690.tmp	Dropped File, Accessed File	Access, Create, Delete, Read, Write	CLEAN
C:\Users\kEecfMwgj\Desktop\fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe:Zone.Identifier	Accessed File	Access, Delete	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\B9C8F16E-2E51-4052-9ECB-F86AE5D96EF6\run.dat	Dropped File, Accessed File	Access, Create, Write	CLEAN
c:\users\keecfmwgj\appdata\local\gdipfontcachev1.dat	Dropped File	-	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\B9C8F16E-2E51-4052-9ECB-F86AE5D96EF6\catalog.dat	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\B9C8F16E-2E51-4052-9ECB-F86AE5D96EF6	Accessed File	Access, Create	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\B9C8F16E-2E51-4052-9ECB-F86AE5D96EF6\settings.bak	Accessed File	Access, Delete	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\nFxIoujoILCO.exe.config	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	Accessed File	Access, Read	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\B9C8F16E-2E51-4052-9ECB-F86AE5D96EF6\Logs	Accessed File	Access, Create	CLEAN
C:\Program Files (x86)\AGP Subsystem\agpss.exe.config	Accessed File	Access	CLEAN
C:\Program Files (x86)	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\B9C8F16E-2E51-4052-9ECB-F86AE5D96EF6\AGP Subsystem\agpss.exe	Accessed File	Access, Delete	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\B9C8F16E-2E51-4052-9ECB-F86AE5D96EF6\settings.bin	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\Program Files (x86)\AGP Subsystem	Accessed File	Access, Create	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp17.tmp	Dropped File, Accessed File	Access, Create, Delete, Read, Write	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://79.134.225.53	-	79.134.225.53	-	-	MALICIOUS

IP

IP Address	Domains	Country	Protocols	Verdict
79.134.225.53	-	Switzerland	TCP	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
7492bd48-e55d-4165-b6f8-ba286e7dc450	-	-	MALICIOUS

Name	Operations	Parent Process Name	Verdict
Global\{7492bd48-e55d-4165-b6f8-ba286e7dc450}	access	fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System	access	fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	read, access	agpss.exe, fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe, nfxioujoilco.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	access	fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	agpss.exe, fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe, nfxioujoilco.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid	read, access	fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	agpss.exe, fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe, nfxioujoilco.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run	access	fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	read, access	fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	read, access	agpss.exe, fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe, nfxioujoilco.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\AGP Subsystem	read, access, write	fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	read, access	fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	read, access	fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	read, access	fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography	access	fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA	read, access	fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\AGP Subsystem	read, access	fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe	CLEAN

Process

Process Name	Commandline	Verdict
fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe	"C:\Users\kEecfMwgj\Desktop\fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe"	MALICIOUS
schtasks.exe	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\nFxIoujoILCO" /XML "C:\Users\kEecfMwgj\AppData\Local\Temp\tmpC690.tmp"	SUSPICIOUS
fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe	"C:\Users\kEecfMwgj\Desktop\fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18.exe"	SUSPICIOUS
powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\kEecfMwgj\AppData\Roaming\nFxIoujoILCO.exe"	CLEAN

Process Name	Commandline	Verdict
schtasks.exe	"schtasks.exe" /create /f /tn "AGP Subsystem" /xml "C:\Users\kEecfMwgj\AppData\Local\Temp\tmpFD29.tmp"	CLEAN
taskeng.exe	taskeng.exe {6D9545EF-31E1-4286-8B8C-42C7F98001F2} S-1-5-21-4219442223-4223814209-3835049652-1000:Q9IATRKPRH\kEecfMwgj:Interactive:LUA[1]	CLEAN
schtasks.exe	"schtasks.exe" /create /f /tn "AGP Subsystem Task" /xml "C:\Users\kEecfMwgj\AppData\Local\Temp\tmp17.tmp"	CLEAN
nfxioujoilco.exe	C:\Users\kEecfMwgj\AppData\Roaming\nFxIoujoILCO.exe	CLEAN
agpss.exe	"C:\Program Files (x86)\AGP Subsystem\agpss.exe"	CLEAN

YARA / AV

YARA (2)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
RATs	NanoCoreRAT	NanoCore RAT	-	-	Backdoor	5/5
RATs	NanoCoreRAT	NanoCore RAT	Memory Dump	-	Backdoor	5/5

ENVIRONMENT

Virtual Machine Information

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

Platform Information

Platform Version	4.6.0
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	4.6.1.9 / 2022-07-29 14:01:00
Link Detonation Heuristics Version	4.6.1.9 / 2022-07-29 14:01:00
Smart Memory Dumping Rules Version	4.6.1.9 / 2022-07-29 14:01:00
Config Extractors Version	4.6.1.12 / 2022-08-02 11:53:09
Signature Trust Store Version	4.6.1.9 / 2022-07-29 14:01:00
VMRay Threat Identifiers Version	4.6.1.14 / 2022-08-03 12:19:21
YARA Built-in Ruleset Version	4.6.1.10

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	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