MALICIOUS

Classifications: -

Threat Names: Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe**
ID	#5069215
MD5	0d32ff3680a716fd66cb9ab0e3ebc763
SHA1	2aa356f14a156bf56efc66e39e0654bddb4fd95a
SHA256	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71
File Size	2526.00 KB
Report Created	2022-08-05 20:28 (UTC+2)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (14 rules, 75 matches)

Score	Category	Operation	Count	Classification
4/5	Defense Evasion	Bypasses Windows User Account Control (UAC)	1	-
	• (Process #1) 21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe disables UAC dialog via registry.			
4/5	Masquerade	Creates a new process masquerading as a system process	1	-
	• (Process #56) cmd.exe creates a process named explorer.exe.			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as Mal/Generic-S.			
2/5	_data_collection	Reads sensitive application data	1	-
	• (Process #1) 21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe tries to read sensitive data of application "git" by file.			
2/5	Anti Analysis	Creates an unusually large number of processes	1	-
	• Above average number of processes were monitored.			
2/5	Task Scheduling	Schedules task	28	-
	• Schedules task for command ""C:\Program Files (x86)\Windows Portable Devices\yahoomessenger.exe"", to be triggered by LOGON.			
	• Schedules task for command ""C:\Users\kEecfMwgj\Downloads\System.exe"", to be triggered by LOGON.			
	• Schedules task for command ""C:\Users\kEecfMwgj\NetHood\fling.exe"", to be triggered by LOGON.			
	• Schedules task for command ""C:\Boot\ko-KR\WmiPrvSE.exe"", to be triggered by LOGON.			
	• Schedules task for command ""C:\Users\All Users\Microsoft\WwanSvc\fling.exe"", to be triggered by LOGON.			
	• Schedules task for command ""C:\Boot\de-DE\lsm.exe"", to be triggered by LOGON.			
	• Schedules task for command ""C:\Program Files (x86)\MSBuild\Microsoft\explorer.exe"", to be triggered by LOGON.			
	• Schedules task for command ""C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\smartftp.exe"", to be triggered by LOGON.			
	• Schedules task for command ""C:\MSOCache\All Users\lsass.exe"", to be triggered by LOGON.			
	• Schedules task for command ""C:\Windows\en-US\flashfxp.exe"", to be triggered by LOGON.			
	• Schedules task for command ""C:\Windows\Help\Windows\isspos.exe"", to be triggered by LOGON.			
	• Schedules task for command ""C:\Windows\Offline Web Pages\smartftp.exe"", to be triggered by LOGON.			
	• Schedules task for command ""C:\Program Files\Windows Defender\en-US\WmiPrvSE.exe"", to be triggered by LOGON.			
	• Schedules task for command ""C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\congress.exe"", to be triggered by LOGON.			
	• Schedules task for command ""C:\Program Files (x86)\Windows Portable Devices\yahoomessenger.exe"", to be triggered by TIME. Task has been rescheduled by the analyzer.			
	• Schedules task for command ""C:\Users\kEecfMwgj\Downloads\System.exe"", to be triggered by TIME. Task has been rescheduled by the analyzer.			
	• Schedules task for command ""C:\Users\kEecfMwgj\NetHood\fling.exe"", to be triggered by TIME. Task has been rescheduled by the analyzer.			
	• Schedules task for command ""C:\Boot\ko-KR\WmiPrvSE.exe"", to be triggered by TIME. Task has been rescheduled by the analyzer.			
	• Schedules task for command ""C:\Users\All Users\Microsoft\WwanSvc\fling.exe"", to be triggered by TIME. Task has been rescheduled by the analyzer.			
	• Schedules task for command ""C:\Boot\de-DE\lsm.exe"", to be triggered by TIME. Task has been rescheduled by the analyzer.			
	• Schedules task for command ""C:\Program Files (x86)\MSBuild\Microsoft\explorer.exe"", to be triggered by TIME. Task has been rescheduled by the analyzer.			
	• Schedules task for command ""C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\smartftp.exe"", to be triggered by TIME. Task has been rescheduled by the analyzer.			
	• Schedules task for command ""C:\MSOCache\All Users\lsass.exe"", to be triggered by TIME. Task has been rescheduled by the analyzer.			
	• Schedules task for command ""C:\Windows\en-US\flashfxp.exe"", to be triggered by TIME. Task has been rescheduled by the analyzer.			
	• Schedules task for command ""C:\Windows\Help\Windows\isspos.exe"", to be triggered by TIME. Task has been rescheduled by the analyzer.			
	• Schedules task for command ""C:\Windows\Offline Web Pages\smartftp.exe"", to be triggered by TIME. Task has been rescheduled by the analyzer.			
	• Schedules task for command ""C:\Program Files\Windows Defender\en-US\WmiPrvSE.exe"", to be triggered by TIME. Task has been rescheduled by the analyzer.			
	• Schedules task for command ""C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\congress.exe"", to be triggered by TIME. Task has been rescheduled by the analyzer.			

Score	Category	Operation	Count	Classification
2/5	Task Scheduling	Schedules task via schtasks	22	-

- Schedules task "yahoomessengery" via the schtasks command line utility.
- Schedules task "yahoomessenger" via the schtasks command line utility.
- Schedules task "SystemS" via the schtasks command line utility.
- Schedules task "System" via the schtasks command line utility.
- Schedules task "flingf" via the schtasks command line utility.
- Schedules task "fling" via the schtasks command line utility.
- Schedules task "WmiPrvSEW" via the schtasks command line utility.
- Schedules task "WmiPrvSE" via the schtasks command line utility.
- Schedules task "lsml" via the schtasks command line utility.
- Schedules task "lsm" via the schtasks command line utility.
- Schedules task "explorere" via the schtasks command line utility.
- Schedules task "explorer" via the schtasks command line utility.
- Schedules task "smartftps" via the schtasks command line utility.
- Schedules task "smartftp" via the schtasks command line utility.
- Schedules task "lsassl" via the schtasks command line utility.
- Schedules task "lsass" via the schtasks command line utility.
- Schedules task "flashfxpf" via the schtasks command line utility.
- Schedules task "flashfxp" via the schtasks command line utility.
- Schedules task "issposi" via the schtasks command line utility.
- Schedules task "isspos" via the schtasks command line utility.
- Schedules task "congressc" via the schtasks command line utility.
- Schedules task "congress" via the schtasks command line utility.

1/5	Privilege Escalation	Enables process privilege	2	-

- (Process #1) 21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe enables process privilege "SeDebugPrivilege".
- (Process #60) explorer.exe enables process privilege "SeDebugPrivilege".

1/5	Mutex	Creates mutex	2	-

- (Process #1) 21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe creates mutex with name "Local\d728178a8bc9e72dab6d832d7b41df6e8cb9b01e".
- (Process #60) explorer.exe creates mutex with name "Local\d728178a8bc9e72dab6d832d7b41df6e8cb9b01e".

1/5	System Modification	Modifies application directory	6	-

- (Process #1) 21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe modifies "C:\Program Files (x86)\Windows Portable Devices\yahoomessenger.exe".
- (Process #1) 21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe modifies "C:\Program Files (x86)\Windows Portable Devices\8503bace434a30".
- (Process #1) 21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe modifies "C:\Program Files (x86)\MSBuild\Microsoft\explorer.exe".
- (Process #1) 21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe modifies "C:\Program Files (x86)\MSBuild\Microsoft\7a0fd90576e088".
- (Process #1) 21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe modifies "C:\Program Files\Windows Defender\en-US\WmiPrvSE.exe".
- (Process #1) 21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe modifies "C:\Program Files\Windows Defender\en-US\24dbde2999530e".

1/5	System Modification	Modifies operating system directory	6	-

- (Process #1) 21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe creates file "C:\Windows\en-US\flashfxp.exe" in the OS directory.
- (Process #1) 21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe creates file "C:\Windows\en-US\b064723b75e933" in the OS directory.
- (Process #1) 21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe creates file "C:\Windows\Help\Windows\isspos.exe" in the OS directory.
- (Process #1) 21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe creates file "C:\Windows\Help\Windows\4863bbf8905744" in the OS directory.
- (Process #1) 21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe creates file "C:\Windows\Offline Web Pages\smartftp.exe" in the OS directory.
- (Process #1) 21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe creates file "C:\Windows\Offline Web Pages\757a39080a2975" in the OS directory.

1/5	Hide Tracks	Writes an unusually large amount of data to the registry	1	-

Score	Category	Operation	Count	Classification
		• (Process #1) 21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe hides 2114 bytes in "HKEY_CURRENT_USER\Software\c0c40df0fc4d1585d5de603ec4f3d9f726afeeba\16211b4c33c8ccf43124ddbe6c57634ab86b6ebc".		
1/5	Hide Tracks	Creates process with hidden window	1	-
		• (Process #1) 21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe starts (process #56) cmd.exe with a hidden window.		
1/5	Obfuscation	Resolves API functions dynamically	2	-
		• (Process #1) 21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe resolves 48 API functions by name. • (Process #3) wmiprvse.exe resolves 25 API functions by name.		

Mitre ATT&CK Matrix

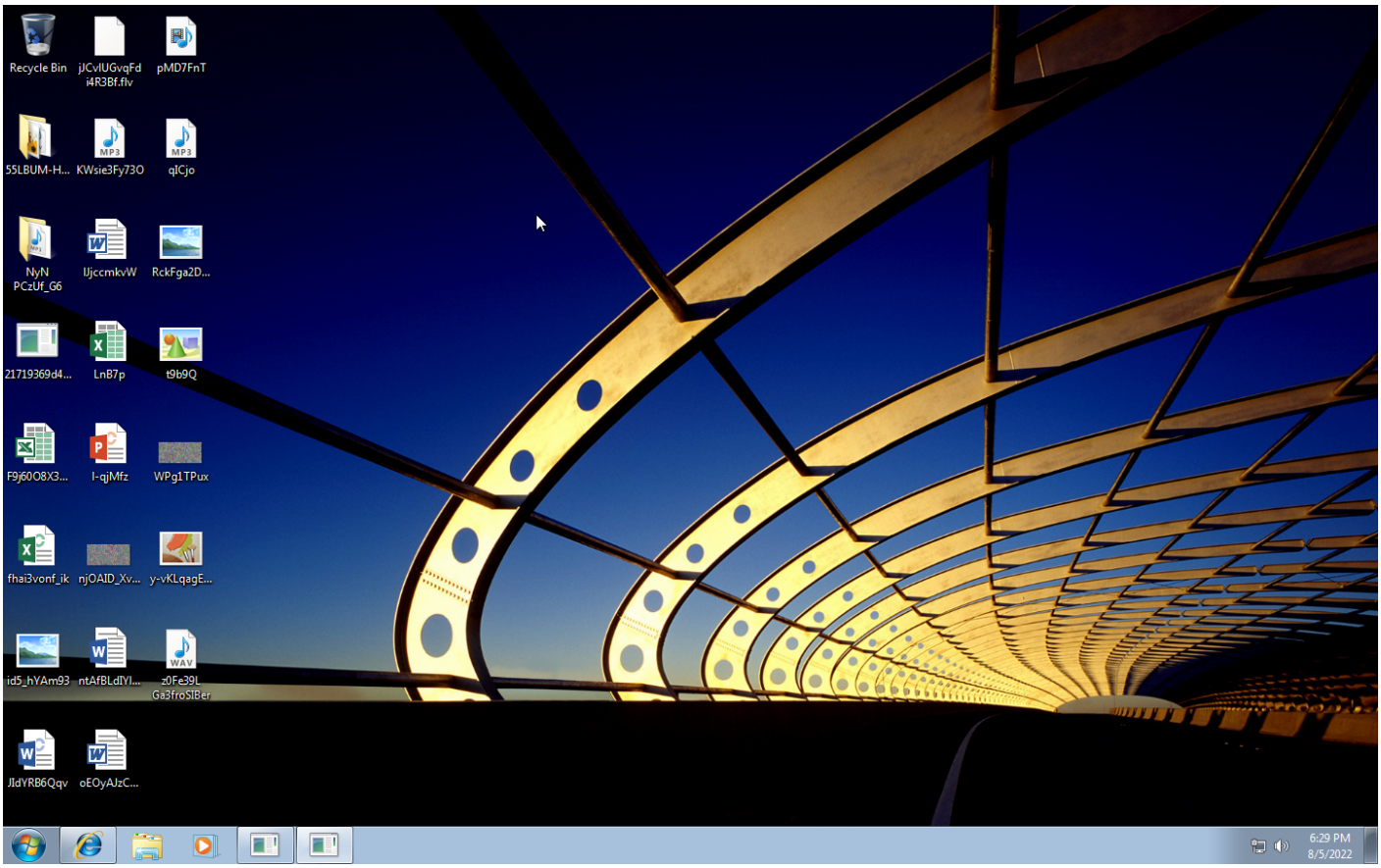
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1112 Modify Registry	#T1081 Credentials in Files	#T1083 File and Directory Discovery		#T1119 Automated Collection			
				#T1143 Hidden Window				#T1005 Data from Local System			
				#T1045 Software Packing							

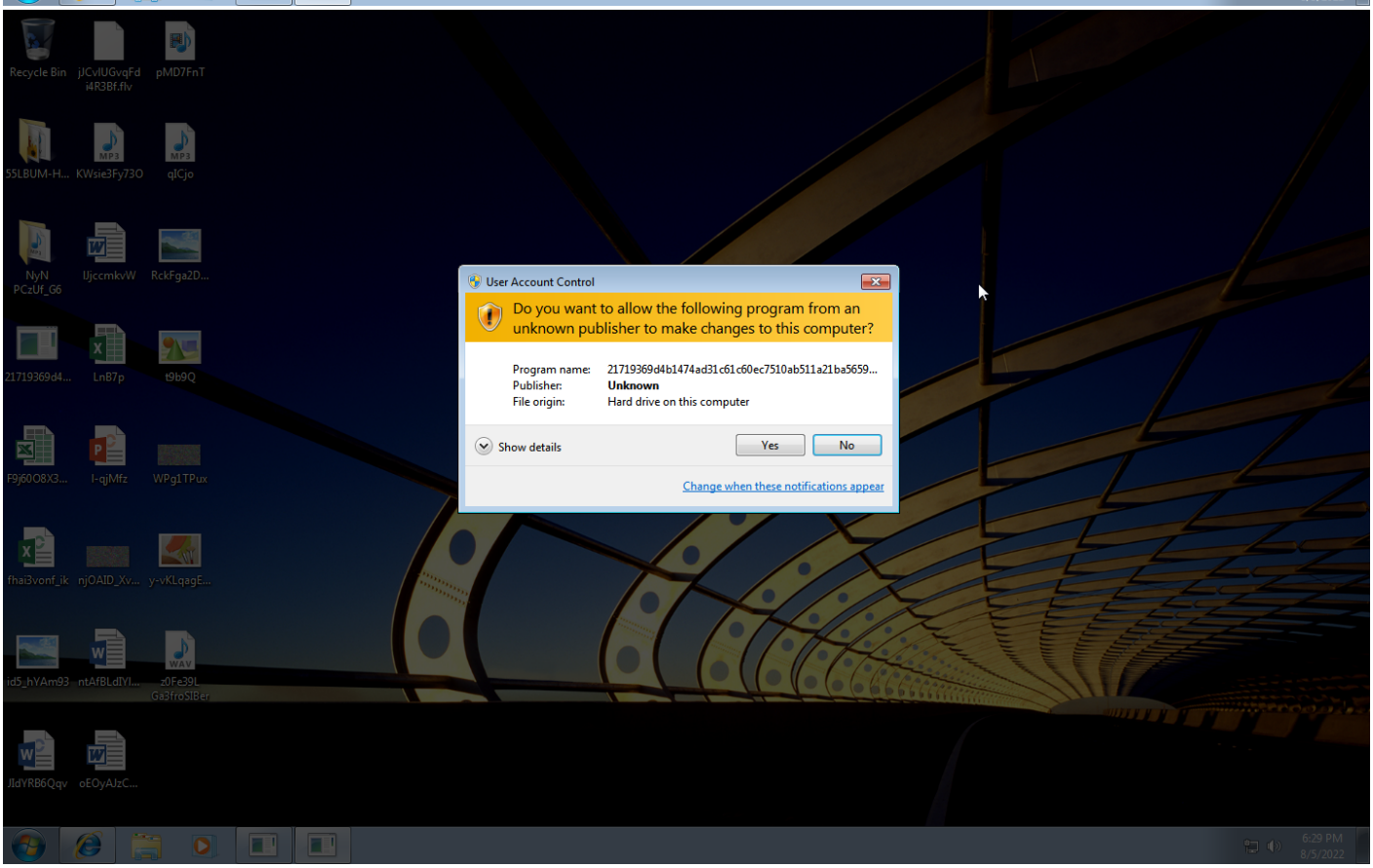
Sample Information

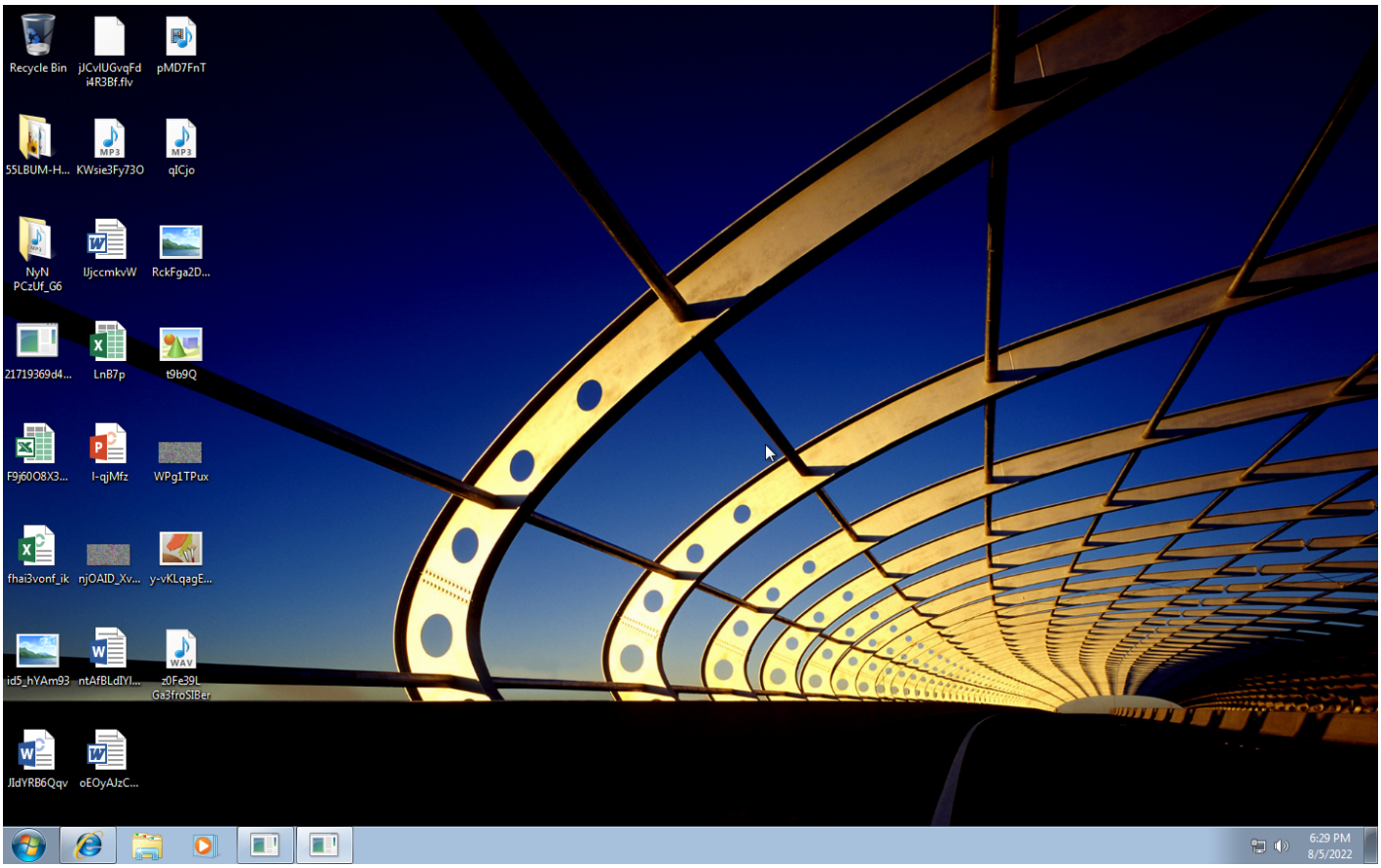
ID	#5069215
MD5	0d32ff3680a716fd66cb9ab0e3ebc763
SHA1	2aa356f14a156bf56efc66e39e0654bddb4fd95a
SHA256	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71
SSDeep	49152:5Ad/na1hwN3zHvJB4x365neVoe51QDr67tUKR8jJLYPYI553bpGes:5cG6N3kBoi1QDr6RwjNYP15VVs
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe
File Size	2526.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

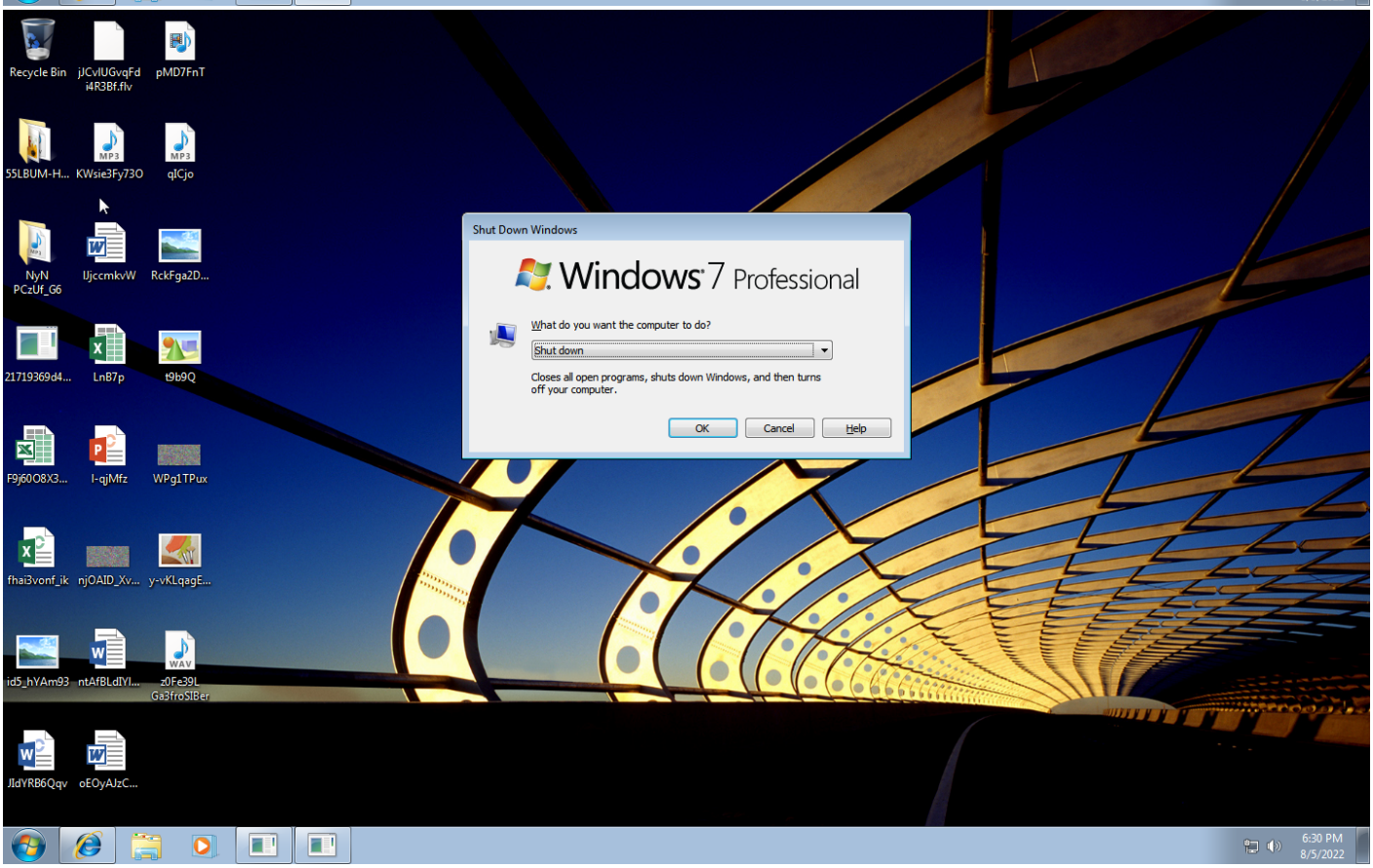
Analysis Information

Creation Time	2022-08-05 20:28 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	60
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	0


Recycle Bin
jJCvIUGvqFd i4R3Bf.flv
pMD7FnT
55LBUM-H...
KWsie3Fy73O
qICjo
NyN PCzUf_G6
IJjccmkvW
RckFga2D...
21719369d4...
Ln87p
t9b9Q
F9j60O8X3...
I-qjMfz
WPg1TPux
fhai3vonf_ik
njOAID_Xv...
y-vKLqagE...
id5_hYAm93
ntAfBLdIYI...
z0Fe39L Ga3froSIBer
JIdYRB6Qqv
oEOyAJzC...
6:29 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: 21719369d4b1474ad31c61c60ec7510ab511a21ba5659...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear





Screenshots truncated

NETWORK

General

0 bytes total sent

0 bytes total received

0 ports

0 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

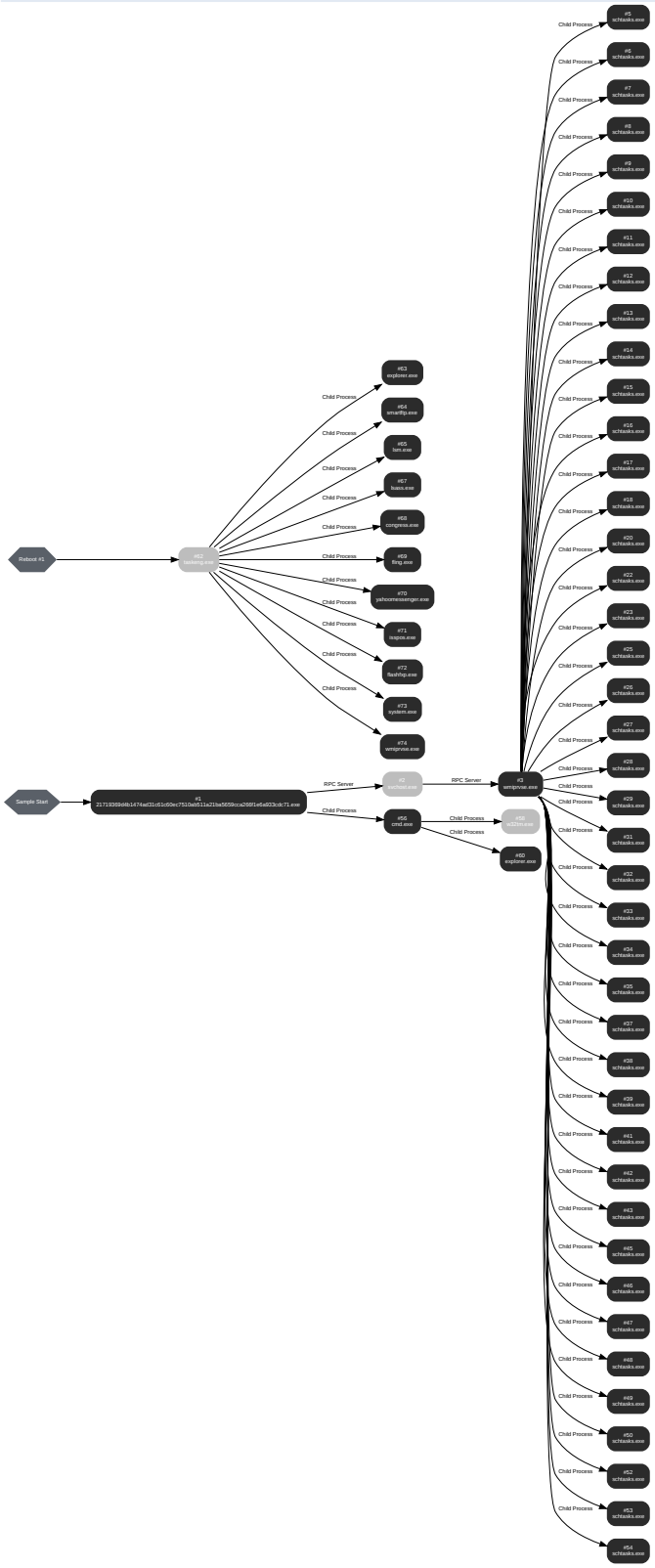
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: 21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 48683, Reason: Analysis Target
Unmonitor End Time	End Time: 140317, Reason: Terminated
Monitor duration	91.63s
Return Code	0
PID	3908
Parent PID	1916
Bitness	64 Bit

Dropped Files (17)

File Name	File Size	SHA256	YARA Match
C:\Windows\Help\Windows\4863bbf8905744	544 bytes	a1fa33ef6a682ce950587050813c6f58ec6b7a30391745620f68b78637d1bbdd	✖
C:\Windows\en-US\b064723b75e933	397 bytes	848e8f3a5d639cafbef893e4d594f88882fd0ea3a92117c5f8b4abbd26087514	✖
C:\Users\kEecfMwgj\AppData\Local\Temp\Tp6OfGWybr	25 bytes	d5a613b8e51b850cf2311fc221b1197ccd361f1f5dc35dcf15dcae9bc48a57f1	✖
C:\Program Files (x86)\MSBuild\Microsoft\7a0fd90576e088	128 bytes	f154ae8288d916f7aea0445e8215c9a211d5d46b0c163fd916356a7a6d54a74b	✖
C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\757a39080a2975	652 bytes	5424a5ea68f81e5bb924f102d0fe12d286b86f23f295effd53e412f24e79c19c	✖
C:\MSOCache\All Users\6203df4a6bafc7	516 bytes	c1a005bd4328774a62eb5d3dc1ad6ac3b87799a5686b90f841c6cb804b7317e7	✖
-	793 bytes	03ddbf1a49253e134c529a5d836e6b74959ab2de0a76019c66721d0549ab0999	✖
C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\61ed18144b6802	782 bytes	e174bb4a62d510f5a7afa7fed5f7c53b761a1d7704c9bdde98ac374ebd592f6b	✖
C:\Program Files (x86)\Windows Portable Devices\8503bace434a30	235 bytes	371c25fa18cf4776c46acfd7f0a47a2214b51bdc35e13e52e5778c0b20ab4559	✖
C:\Boot\de-DE\101b941d020240	289 bytes	f60254afe03838f420c7f07154b05f216870df73378c1541b95b331c2a9ce009	✖
C:\Boot\ko-KR\WmiPrvSE.exe	2526.00 KB	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71	✖
C:\Program Files\Windows Defender\en-US\24dbde2999530e	872 bytes	7732116ddb03778e4b052165d462fb0673b11169c67ae7cbca1d52a7e50e9a83	✖
C:\Windows\Offline Web Pages\757a39080a2975	982 bytes	dab1a4d6da339000497233a4edd5a801b9a9f30bb0e84e7a5845a11920fc77b9	✖
-	854 bytes	56bfed37762cb01dcf9f5c0e4191b7a258d73240d7262facc182daff386b0fe5	✖
C:\Users\kEecfMwgj\Downloads\27d1bcfc3c54e0	917 bytes	b96d8300249cdc7be3c1e21fe180660217309fff9cf7bf86399315f38b511b00	✖
C:\Users\kEecfMwgj\AppData\Local\Temp\\UiqPJstYE1.bat	222 bytes	21097d3c6c5c521832c7f7900f7ae9a6d32e5f1ee71f389759894fe3dc4125c7	✖
C:\Boot\ko-KR\24dbde2999530e	424 bytes	47930e02683a6fc28edeab00d9a4bc2517a9ec2f220b6b354ca39fb8ef16d6cb	✖

Host Behavior

Type	Count
Registry	60
-	3
File	143
User	2
Module	70
System	19
Mutex	2
COM	631
Process	21

Process #2: svchost.exe

ID	2
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k netsvcs
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 87389, Reason: RPC Server
Unmonitor End Time	End Time: 288728, Reason: Terminated by timeout
Monitor duration	201.34s
Return Code	Unknown
PID	872
Parent PID	3908
Bitness	64 Bit

Process #3: wmiprvse.exe

ID	3
File Name	c:\windows\system32\wbem\wmiprvse.exe
Command Line	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 87389, Reason: RPC Server
Unmonitor End Time	End Time: 288728, Reason: Terminated by timeout
Monitor duration	201.34s
Return Code	Unknown
PID	3296
Parent PID	872
Bitness	64 Bit

Host Behavior

Type	Count
Module	987
System	291
Process	42
Registry	1

Process #5: schtasks.exe

ID	5
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "yahoomessengery" /sc MINUTE /mo 8 /tr "'C:\Program Files (x86)\Windows Portable Devices\yahoomessenger.exe'" /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 88969, Reason: Child Process
Unmonitor End Time	End Time: 92675, Reason: Terminated
Monitor duration	3.71s
Return Code	0
PID	4012
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #6: schtasks.exe

ID	6
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "yahoomessenger" /sc ONLOGON /tr "'C:\Program Files (x86)\Windows Portable Devices\yahoomessenger.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 89689, Reason: Child Process
Unmonitor End Time	End Time: 93484, Reason: Terminated
Monitor duration	3.79s
Return Code	0
PID	4020
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #7: schtasks.exe

ID	7
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "yahoomessengery" /sc MINUTE /mo 14 /tr "'C:\Program Files (x86)\Windows Portable Devices\yahoomessenger.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 90885, Reason: Child Process
Unmonitor End Time	End Time: 93487, Reason: Terminated
Monitor duration	2.60s
Return Code	0
PID	4036
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #8: schtasks.exe

ID	8
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "SystemS" /sc MINUTE /mo 14 /tr "'C:\Users\kEecfMwgj\Downloads\System.exe'" /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 93489, Reason: Child Process
Unmonitor End Time	End Time: 94698, Reason: Terminated
Monitor duration	1.21s
Return Code	0
PID	4052
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #9: schtasks.exe

ID	9
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "System" /sc ONLOGON /tr "'C:\Users\kEecfMwgj\Downloads\System.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 94037, Reason: Child Process
Unmonitor End Time	End Time: 95786, Reason: Terminated
Monitor duration	1.75s
Return Code	0
PID	4068
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #10: schtasks.exe

ID	10
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "SystemS" /sc MINUTE /mo 8 /tr "'C:\Users\kEecfMwgj\Downloads\System.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 94699, Reason: Child Process
Unmonitor End Time	End Time: 96386, Reason: Terminated
Monitor duration	1.69s
Return Code	0
PID	4080
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #11: schtasks.exe

ID	11
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "flingf" /sc MINUTE /mo 14 /tr "'C:\Users\kEecfMwgj\NetHood\fling.exe'" /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 95788, Reason: Child Process
Unmonitor End Time	End Time: 98051, Reason: Terminated
Monitor duration	2.26s
Return Code	0
PID	4092
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #12: schtasks.exe

ID	12
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "fling" /sc ONLOGON /tr "'C:\Users\kEecfMwgj\NetHood\fling.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 96389, Reason: Child Process
Unmonitor End Time	End Time: 98209, Reason: Terminated
Monitor duration	1.82s
Return Code	0
PID	3000
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #13: schtasks.exe

ID	13
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "flingf" /sc MINUTE /mo 11 /tr "'C:\Users\kEecfMwgj\NetHood\fling.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 97162, Reason: Child Process
Unmonitor End Time	End Time: 98734, Reason: Terminated
Monitor duration	1.57s
Return Code	0
PID	2988
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #14: schtasks.exe

ID	14
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "WmiPrvSEW" /sc MINUTE /mo 8 /tr "'C:\Boot\ko-KR\WmiPrvSE.exe'" /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 98210, Reason: Child Process
Unmonitor End Time	End Time: 100600, Reason: Terminated
Monitor duration	2.39s
Return Code	0
PID	2952
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #15: schtasks.exe

ID	15
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "WmiPrvSE" /sc ONLOGON /tr "'C:\Boot\ko-KR\WmiPrvSE.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 98736, Reason: Child Process
Unmonitor End Time	End Time: 101451, Reason: Terminated
Monitor duration	2.71s
Return Code	0
PID	2940
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #16: schtasks.exe

ID	16
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "WmiPrvSEW" /sc MINUTE /mo 14 /tr "'C:\Boot\ko-KR\WmiPrvSE.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 99736, Reason: Child Process
Unmonitor End Time	End Time: 100999, Reason: Terminated
Monitor duration	1.26s
Return Code	0
PID	2924
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #17: schtasks.exe

ID	17
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "flingf" /sc MINUTE /mo 9 /tr "'C:\Users\All Users\Microsoft\WwanSvc\fling.exe'" /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 101001, Reason: Child Process
Unmonitor End Time	End Time: 103813, Reason: Terminated
Monitor duration	2.81s
Return Code	0
PID	2972
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #18: schtasks.exe

ID	18
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "fling" /sc ONLOGON /tr "'C:\Users\All Users\Microsoft\WwanSvc\fling.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 101746, Reason: Child Process
Unmonitor End Time	End Time: 104928, Reason: Terminated
Monitor duration	3.18s
Return Code	0
PID	2960
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #20: schtasks.exe

ID	20
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "flingf" /sc MINUTE /mo 11 /tr "'C:\Users\All Users\Microsoft\WwanSvc\fling.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 103144, Reason: Child Process
Unmonitor End Time	End Time: 105619, Reason: Terminated
Monitor duration	2.48s
Return Code	0
PID	308
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #22: schtasks.exe

ID	22
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "lsml" /sc MINUTE /mo 14 /tr "'C:\Boot\de-DE\lsm.exe'" /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 104930, Reason: Child Process
Unmonitor End Time	End Time: 108134, Reason: Terminated
Monitor duration	3.20s
Return Code	0
PID	3056
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #23: schtasks.exe

ID	23
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "lsm" /sc ONLOGON /tr "'C:\Boot\de-DE\lsm.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 105622, Reason: Child Process
Unmonitor End Time	End Time: 109074, Reason: Terminated
Monitor duration	3.45s
Return Code	0
PID	3060
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #25: schtasks.exe

ID	25
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "lsml" /sc MINUTE /mo 8 /tr "'C:\Boot\de-DE\lsm.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 107344, Reason: Child Process
Unmonitor End Time	End Time: 110042, Reason: Terminated
Monitor duration	2.70s
Return Code	0
PID	2368
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #26: schtasks.exe

ID	26
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "explorere" /sc MINUTE /mo 6 /tr "'C:\Program Files (x86)\MSBuild\Microsoft\explorer.exe'" /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 109098, Reason: Child Process
Unmonitor End Time	End Time: 111713, Reason: Terminated
Monitor duration	2.62s
Return Code	0
PID	2060
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #27: schtasks.exe

ID	27
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "explorer" /sc ONLOGON /tr "'C:\Program Files (x86)\MSBuild\Microsoft\explorer.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 110466, Reason: Child Process
Unmonitor End Time	End Time: 112042, Reason: Terminated
Monitor duration	1.58s
Return Code	0
PID	2100
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #28: schtasks.exe

ID	28
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "explorere" /sc MINUTE /mo 10 /tr "'C:\Program Files (x86)\MSBuild\Microsoft\explorer.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 111056, Reason: Child Process
Unmonitor End Time	End Time: 113388, Reason: Terminated
Monitor duration	2.33s
Return Code	0
PID	3396
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #29: schtasks.exe

ID	29
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "smartftps" /sc MINUTE /mo 10 /tr "'C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\smartftp.exe'" /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 112044, Reason: Child Process
Unmonitor End Time	End Time: 114387, Reason: Terminated
Monitor duration	2.34s
Return Code	0
PID	3356
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #31: schtasks.exe

ID	31
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "smartftp" /sc ONLOGON /tr "'C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\smartftp.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 112786, Reason: Child Process
Unmonitor End Time	End Time: 114488, Reason: Terminated
Monitor duration	1.70s
Return Code	0
PID	3184
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #32: schtasks.exe

ID	32
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "smartftps" /sc MINUTE /mo 13 /tr "'C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\smartftp.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 113500, Reason: Child Process
Unmonitor End Time	End Time: 115412, Reason: Terminated
Monitor duration	1.91s
Return Code	0
PID	1976
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #33: schtasks.exe

ID	33
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "lsassl" /sc MINUTE /mo 6 /tr "'C:\MSOCache\All Users\lsass.exe'" /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 114490, Reason: Child Process
Unmonitor End Time	End Time: 116027, Reason: Terminated
Monitor duration	1.54s
Return Code	0
PID	3444
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #34: schtasks.exe

ID	34
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "lsass" /sc ONLOGON /tr "'C:\MSOCache\All Users\lsass.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 115009, Reason: Child Process
Unmonitor End Time	End Time: 116885, Reason: Terminated
Monitor duration	1.88s
Return Code	0
PID	3436
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #35: schtasks.exe

ID	35
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "lsassl" /sc MINUTE /mo 5 /tr "'C:\MSOCache\All Users\lsass.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 116029, Reason: Child Process
Unmonitor End Time	End Time: 118415, Reason: Terminated
Monitor duration	2.39s
Return Code	0
PID	3404
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #37: schtasks.exe

ID	37
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "flashfxpf" /sc MINUTE /mo 5 /tr "'C:\Windows\en-US\flashfxp.exe'" /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 117260, Reason: Child Process
Unmonitor End Time	End Time: 119715, Reason: Terminated
Monitor duration	2.46s
Return Code	0
PID	3504
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #38: schtasks.exe

ID	38
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "flashfxp" /sc ONLOGON /tr "'C:\Windows\en-US\flashfxp.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 118168, Reason: Child Process
Unmonitor End Time	End Time: 120153, Reason: Terminated
Monitor duration	1.99s
Return Code	0
PID	3496
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #39: schtasks.exe

ID	39
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "flashfxpf" /sc MINUTE /mo 5 /tr "'C:\Windows\en-US\flashfxp.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 118749, Reason: Child Process
Unmonitor End Time	End Time: 121083, Reason: Terminated
Monitor duration	2.33s
Return Code	0
PID	3560
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #41: schtasks.exe

ID	41
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "issposi" /sc MINUTE /mo 8 /tr "'C:\Windows\Help\Windows\isspos.exe'" /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 120155, Reason: Child Process
Unmonitor End Time	End Time: 122094, Reason: Terminated
Monitor duration	1.94s
Return Code	0
PID	3548
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #42: schtasks.exe

ID	42
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "isspos" /sc ONLOGON /tr "'C:\Windows\Help\Windows\isspos.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 120760, Reason: Child Process
Unmonitor End Time	End Time: 123266, Reason: Terminated
Monitor duration	2.51s
Return Code	0
PID	3520
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #43: schtasks.exe

ID	43
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "issposi" /sc MINUTE /mo 10 /tr "'C:\Windows\Help\Windows\isspos.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 121350, Reason: Child Process
Unmonitor End Time	End Time: 123818, Reason: Terminated
Monitor duration	2.47s
Return Code	0
PID	3600
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #45: schtasks.exe

ID	45
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "smartftps" /sc MINUTE /mo 9 /tr "'C:\Windows\Offline Web Pages\smartftp.exe'" /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 122497, Reason: Child Process
Unmonitor End Time	End Time: 124851, Reason: Terminated
Monitor duration	2.35s
Return Code	0
PID	3640
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #46: schtasks.exe

ID	46
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "smartftp" /sc ONLOGON /tr "'C:\Windows\Offline Web Pages\smartftp.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 123268, Reason: Child Process
Unmonitor End Time	End Time: 125523, Reason: Terminated
Monitor duration	2.25s
Return Code	0
PID	3636
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #47: schtasks.exe

ID	47
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "smartftps" /sc MINUTE /mo 14 /tr "'C:\Windows\Offline Web Pages\smartftp.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 124035, Reason: Child Process
Unmonitor End Time	End Time: 126168, Reason: Terminated
Monitor duration	2.13s
Return Code	0
PID	3620
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #48: schtasks.exe

ID	48
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "WmiPrvSEW" /sc MINUTE /mo 5 /tr "'C:\Program Files\Windows Defender\en-US\WmiPrvSE.exe'" /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 125047, Reason: Child Process
Unmonitor End Time	End Time: 126380, Reason: Terminated
Monitor duration	1.33s
Return Code	0
PID	3676
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #49: schtasks.exe

ID	49
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "WmiPrvSE" /sc ONLOGON /tr "'C:\Program Files\Windows Defender\en-US\WmiPrvSE.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 125525, Reason: Child Process
Unmonitor End Time	End Time: 128287, Reason: Terminated
Monitor duration	2.76s
Return Code	0
PID	3656
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #50: schtasks.exe

ID	50
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "WmiPrvSEW" /sc MINUTE /mo 5 /tr "'C:\Program Files\Windows Defender\en-US\WmiPrvSE.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 126381, Reason: Child Process
Unmonitor End Time	End Time: 128934, Reason: Terminated
Monitor duration	2.55s
Return Code	0
PID	3684
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #52: schtasks.exe

ID	52
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "congressc" /sc MINUTE /mo 11 /tr "'C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\congress.exe'" /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 127534, Reason: Child Process
Unmonitor End Time	End Time: 129660, Reason: Terminated
Monitor duration	2.13s
Return Code	0
PID	2372
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #53: schtasks.exe

ID	53
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "congress" /sc ONLOGON /tr "'C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\congress.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 128290, Reason: Child Process
Unmonitor End Time	End Time: 130474, Reason: Terminated
Monitor duration	2.18s
Return Code	0
PID	2384
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #54: schtasks.exe

ID	54
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "congressc" /sc MINUTE /mo 10 /tr "'C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\congress.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 128936, Reason: Child Process
Unmonitor End Time	End Time: 131032, Reason: Terminated
Monitor duration	2.10s
Return Code	0
PID	2412
Parent PID	3296
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	9
COM	1
User	1
File	2

Process #56: cmd.exe

ID	56
File Name	c:\windows\system32\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C "C:\Users\kEecfMwgj\AppData\Local\Temp\UiqPJstYE1.bat"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 137919, Reason: Child Process
Unmonitor End Time	End Time: 145777, Reason: Terminated
Monitor duration	7.86s
Return Code	1
PID	2700
Parent PID	3908
Bitness	64 Bit

Host Behavior

Type	Count
Module	5
Environment	12
File	77
Process	2
-	1

Process #58: w32tm.exe

ID	58
File Name	c:\windows\system32\w32tm.exe
Command Line	w32tm /stripchart /computer:localhost /period:5 /dataonly /samples:2
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 138729, Reason: Child Process
Unmonitor End Time	End Time: 145590, Reason: Terminated
Monitor duration	6.86s
Return Code	0
PID	2772
Parent PID	2700
Bitness	64 Bit

Process #60: explorer.exe

ID	60
File Name	c:\program files (x86)\msbuild\microsoft\explorer.exe
Command Line	"C:\Program Files (x86)\MSBuild\Microsoft\explorer.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 144607, Reason: Child Process
Unmonitor End Time	End Time: 288728, Reason: Terminated by timeout
Monitor duration	144.12s
Return Code	Unknown
PID	2912
Parent PID	2700
Bitness	64 Bit

Host Behavior

Type	Count
Registry	54
-	2
File	20
User	2
Module	19
System	5
Mutex	2

Process #62: taskeng.exe

ID	62
File Name	c:\windows\system32\taskeng.exe
Command Line	taskeng.exe {1202B463-65FD-4008-AD56-FFB42ECEBA22} S-1-5-21-4219442223-4223814209-3835049652-1000:Q9IATRKPRH\kEecfMwgj:Interactive:[1]
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 224529, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 288728, Reason: Terminated by timeout
Monitor duration	64.20s
Return Code	Unknown
PID	1236
Parent PID	2412
Bitness	64 Bit

Process #63: explorer.exe

ID	63
File Name	c:\program files (x86)\msbuild\microsoft\explorer.exe
Command Line	"C:\Program Files (x86)\MSBuild\Microsoft\explorer.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 226077, Reason: Child Process
Unmonitor End Time	End Time: 288728, Reason: Terminated by timeout
Monitor duration	62.65s
Return Code	Unknown
PID	1372
Parent PID	1236
Bitness	64 Bit

Host Behavior

Type	Count
Registry	1

Process #64: smartftp.exe

ID	64
File Name	c:\windows\offline web pages\smartftp.exe
Command Line	"C:\Windows\Offline Web Pages\smartftp.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 226151, Reason: Child Process
Unmonitor End Time	End Time: 288728, Reason: Terminated by timeout
Monitor duration	62.58s
Return Code	Unknown
PID	1380
Parent PID	1236
Bitness	64 Bit

Host Behavior

Type	Count
Registry	1

Process #65: lsm.exe

ID	65
File Name	c:\boot\de-de\lsm.exe
Command Line	C:\Boot\de-DE\lsm.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 226192, Reason: Child Process
Unmonitor End Time	End Time: 288728, Reason: Terminated by timeout
Monitor duration	62.54s
Return Code	Unknown
PID	1388
Parent PID	1236
Bitness	64 Bit

Host Behavior

Type	Count
Registry	1

Process #67: lsass.exe

ID	67
File Name	c:\msocache\all users\lsass.exe
Command Line	"C:\MSOCache\All Users\lsass.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 226255, Reason: Child Process
Unmonitor End Time	End Time: 288728, Reason: Terminated by timeout
Monitor duration	62.47s
Return Code	Unknown
PID	1400
Parent PID	1236
Bitness	64 Bit

Host Behavior

Type	Count
Registry	1

Process #68: congress.exe

ID	68
File Name	c:\recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\congress.exe
Command Line	C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\congress.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 226262, Reason: Child Process
Unmonitor End Time	End Time: 288728, Reason: Terminated by timeout
Monitor duration	62.47s
Return Code	Unknown
PID	1408
Parent PID	1236
Bitness	64 Bit

Host Behavior

Type	Count
Registry	1

Process #69: fling.exe

ID	69
File Name	c:\users\all users\microsoft\wwansvc\fling.exe
Command Line	"C:\Users\All Users\Microsoft\WwanSvc\fling.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 226301, Reason: Child Process
Unmonitor End Time	End Time: 288728, Reason: Terminated by timeout
Monitor duration	62.43s
Return Code	Unknown
PID	1416
Parent PID	1236
Bitness	64 Bit

Host Behavior

Type	Count
Registry	1

Process #70: yahoomessenger.exe

ID	70
File Name	c:\program files (x86)\windows portable devices\yahoomessenger.exe
Command Line	"C:\Program Files (x86)\Windows Portable Devices\yahoomessenger.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 226407, Reason: Child Process
Unmonitor End Time	End Time: 288728, Reason: Terminated by timeout
Monitor duration	62.32s
Return Code	Unknown
PID	1432
Parent PID	1236
Bitness	64 Bit

Host Behavior

Type	Count
Registry	1

Process #71: isspos.exe

ID	71
File Name	c:\windows\help\windows\isspos.exe
Command Line	C:\Windows\Help\Windows\isspos.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 226494, Reason: Child Process
Unmonitor End Time	End Time: 288728, Reason: Terminated by timeout
Monitor duration	62.23s
Return Code	Unknown
PID	1440
Parent PID	1236
Bitness	64 Bit

Host Behavior

Type	Count
Registry	1

Process #72: flashfxp.exe

ID	72
File Name	c:\windows\en-us\flashfxp.exe
Command Line	C:\Windows\en-US\flashfxp.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 226532, Reason: Child Process
Unmonitor End Time	End Time: 288728, Reason: Terminated by timeout
Monitor duration	62.20s
Return Code	Unknown
PID	1448
Parent PID	1236
Bitness	64 Bit

Host Behavior

Type	Count
Registry	1

Process #73: system.exe

ID	73
File Name	c:\users\keecfmwgj\downloads\system.exe
Command Line	C:\Users\kEecfMwgj\Downloads\System.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 226668, Reason: Child Process
Unmonitor End Time	End Time: 288728, Reason: Terminated by timeout
Monitor duration	62.06s
Return Code	Unknown
PID	1460
Parent PID	1236
Bitness	64 Bit

Host Behavior

Type	Count
Registry	1

Process #74: wmiprvse.exe

ID	74
File Name	c:\program files\windows defender\en-us\wmiprvse.exe
Command Line	"C:\Program Files\Windows Defender\en-US\WmiPrvSE.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 226746, Reason: Child Process
Unmonitor End Time	End Time: 288728, Reason: Terminated by timeout
Monitor duration	61.98s
Return Code	Unknown
PID	1476
Parent PID	1236
Bitness	64 Bit

Host Behavior

Type	Count
Registry	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71	C:\Boot\ko-KR\WmiPrvSE.exe, C:\MSOCache\All Users\lsass.exe, C:\Users\kEecfMwgj\Desktop\21719369d4b1474ad31c61c60ec7510ab511a21ba5... ...:\Users\kEecfMwgj\NetHood\fling.exe, C:\Program Files\Windows Defender\en-US\WmiPrvSE.exe, C:\Users\kEecfMwgj\Downloads\System.exe	Sample File	2526.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
a1fa33ef6a682ce9505870508 13c6f58ec6b7a30391745620f68b78637d1bbdd	C:\Windows\Help\Windows\4863bbf8905744	Dropped File	544 bytes	text/plain	Access, Create, Write	CLEAN
848e8f3a5d639cafbef893e4d594f88882fd0ea3a92117c5f8b4abbd26087514	C:\Windows\en-US\b064723b75e933	Dropped File	397 bytes	text/plain	Access, Create, Write	CLEAN
d5a613b8e51b850cf2311fc221b1197ccd361f1f5dc35dcf15dcae9bc48a57f1	C:\Users\kEecfMwgj\AppData\Local\Temp\Tp6OfGWybr	Dropped File	25 bytes	text/plain	Access, Create, Delete, Write	CLEAN
f154ae8288d916f7aea0445e8215c9a211d5d46b0c163fd916356a7a6d54a74b	C:\Program Files (x86)\MSBuild\Microsoft\7a0fd90576e088	Dropped File	128 bytes	text/plain	Access, Create, Write	CLEAN
5424a5ea68f81e5bb924f102d0fe12d286b86f23f295effd53e412f24e79c19c	C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\757a39080a2975	Dropped File	652 bytes	text/plain	Access, Create, Write	CLEAN
c1a005bd4328774a62eb5d3dc1ad6ac3b87799a5686b90f841c6cb804b7317e7	C:\MSOCache\All Users\6203df4a6bafc7	Dropped File	516 bytes	text/plain	Access, Create, Write	CLEAN
03ddbf1a49253e134c529a5d836e6b74959ab2de0a76019c66721d0549ab0999	-	Dropped File	793 bytes	text/plain	-	CLEAN
e174bb4a62d510f5a7afa7fed5f7c53b761a1d7704c9bdde98ac374ebd592f6b	C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\61ed18144b6802	Dropped File	782 bytes	text/plain	Access, Create, Write	CLEAN
371c25fa18cf4776c46acfd7f0a47a2214b51bdc35e13e52e5778c0b20ab4559	C:\Program Files (x86)\Windows Portable Devices\8503bace434a30	Dropped File	235 bytes	text/plain	Access, Create, Write	CLEAN
f60254afe03838f420c7f07154b05f216870df73378c1541b95b331c2a9ce009	C:\Boot\de-DE\101b941d020240	Dropped File	289 bytes	text/plain	Access, Create, Write	CLEAN
7732116ddb03778e4b052165d462fb0673b11169c67ae7cbca1d52a7e50e9a83	C:\Program Files\Windows Defender\en-US\24dbde2999530e	Dropped File	872 bytes	text/plain	Access, Create, Write	CLEAN
dab1a4d6da339000497233a4edd5a801b9a9f30bb0e84e7a5845a11920fc77b9	C:\Windows\Offline Web Pages\757a39080a2975	Dropped File	982 bytes	text/plain	Access, Create, Write	CLEAN
56bfed37762cb01dcf9f5c0e4191b7a258d73240d7262facc182daff386b0fe5	-	Dropped File	854 bytes	text/plain	-	CLEAN
b96d8300249cdc7be3c1e21fe180660217309fff9cf7bf86399315f38b511b00	C:\Users\kEecfMwgj\Downloads\27d1bcfc3c54e0	Dropped File	917 bytes	text/plain	Access, Create, Write	CLEAN
21097d3c6c5c521832c7f7900f7ae9a6d32e5f1ee71f389759894fe3dc4125c7	C:\Users\kEecfMwgj\AppData\Local\Temp\\UiqPJstYE1.bat, C:\Users\kEecfMwgj\AppData\Local\Temp\UiqPJstYE1.bat	Dropped File	222 bytes	text/x-msdos-batch	Access, Create, Delete, Read, Write	CLEAN
47930e02683a6fc28edeab00d9a4bc2517a9ec2f220b6b354ca39fb8ef16d6cb	C:\Boot\ko-KR\24dbde2999530e	Dropped File	424 bytes	text/plain	Access, Create, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Windows\Help\Windows\isspos.exe	Dropped File, Accessed File, VM File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
C:\Windows\Offline Web Pages\smartftp.exe	Dropped File, Accessed File, VM File	Access, Create, Write	MALICIOUS
C:\Users\All Users\Microsoft\WwanSvc\fling.exe	Accessed File	Access, Create, Write	MALICIOUS
C:\Boot\de-DE\lsm.exe	Dropped File, Accessed File, VM File	Access, Create, Write	MALICIOUS
C:\Windows\en-US\flashfxp.exe	Dropped File, Accessed File, VM File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Windows Portable Devices\yahoomessenger.exe	Dropped File, Accessed File, VM File	Access, Create, Write	MALICIOUS
C:\Boot\ko-KR\WmiPrvSE.exe	Dropped File, Accessed File, VM File	Access, Create, Write	MALICIOUS
C:\MSOCache\All Users\lsass.exe	Dropped File, Accessed File, VM File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe	Sample File, Accessed File, VM File	Access	MALICIOUS
C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\smartftp.exe	Dropped File, Accessed File, VM File	Access, Create, Write	MALICIOUS
C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\congress.exe	Dropped File, Accessed File, VM File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\MSBuild\Microsoft\explorer.exe	Dropped File, Accessed File, VM File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Downloads\System.exe	Dropped File, Accessed File, VM File	Access, Create, Write	MALICIOUS
C:\Program Files\Windows Defender\en-US\WmiPrvSE.exe	Dropped File, Accessed File, VM File	Access, Create, Write	MALICIOUS
c:\programdata\microsoft\wwansvc\fling.exe	Dropped File, VM File	-	MALICIOUS
C:\Users\kEecfMwgj\NetHood\fling.exe	Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\network shortcuts\fling.exe	Dropped File, VM File	-	MALICIOUS
C:\Windows\en-US\b064723b75e933	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\\UiqPJstYE1.bat	Dropped File, Accessed File	Access, Create, Delete, Read, Write	CLEAN
C:\Users\kEecfMwgj\Desktop\21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe.config	Accessed File	Access	CLEAN
C:\Program Files\Windows Defender\en-US\24dbde2999530e	Dropped File, Accessed File	Access, Create, Write	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\61ed18144b6802	Dropped File, Accessed File	Access, Create, Write	CLEAN
nul	Accessed File	Access, Create	CLEAN
C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\757a39080a2975	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\Program Files (x86)\MSBuild\Microsoft\explorer.exe.config	Accessed File	Access	CLEAN
C:\Users\All Users\Microsoft\WwanSvc\bceae2a2bde6c4	Accessed File	Access, Create, Write	CLEAN
c:\programdata\microsoft\wwansvc\bceae2a2bde6c4	Dropped File	-	CLEAN
C:\Windows\Help\Windows\4863bbf8905744	Dropped File, Accessed File	Access, Create, Write	CLEAN
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\network shortcuts\bceae2a2bde6c4	Dropped File	-	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\Tp6OfGWybr	Dropped File, Accessed File	Access, Create, Delete, Write	CLEAN
C:\Windows\system32\schtasks.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\MSBuild\Microsoft\7a0fd90576e088	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\Boot\de-DE\101b941d020240	Dropped File, Accessed File	Access, Create, Write	CLEAN

File Name	Category	Operations	Verdict
C:\MSOCache\All Users\6203df4a6bafc7	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\NetHood\bceae2a2bde6c4	Accessed File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\\	Accessed File	Access	CLEAN
C:\Boot\ko-KR\24dbde2999530e	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\Desktop\253dafe4483684	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\Downloads\27d1bcfc3c54e0	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	Accessed File	Access, Read	CLEAN
C:\Program Files (x86)\Windows Portable Devices\8503bace434a30	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\Windows\Offline Web Pages\757a39080a2975	Dropped File, Accessed File	Access, Create, Write	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
Local\d728178a8bc9e72dab6d832d7b41df6e8cb9b01e	access	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe, explorer.exe	CLEAN
d728178a8bc9e72dab6d832d7b41df6e8cb9b01e	access	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe, explorer.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA	read, access, write	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe, explorer.exe	MALICIOUS
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	read, access	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseSafeSynchronousClose	read, access	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\Full	access	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\PromptOnSecureDesktop	read, access, write	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseHttpPipeliningAndBufferPooling	read, access	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe, explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\c0c40df0fc4d1585d5de603ec4f3d9f726afeeba\16211b4c33c8ccf43124ddbe6c57634ab86b6ebc	read, access, write	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchSendAuxRecord	read, access	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Uri.UseStrictIPv6AddressParsing	access	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	access	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorAdmin	read, access, write	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System	access	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.UseSafeSynchronousClose	access	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\WMIDisableCOMSecurity	read, access	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Uri.AllowAllUriEncodingExpansion	access	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe, explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\AllowAllUriEncodingExpansion	read, access	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SchSendAuxRecord	access	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseStrictRfcInterimResponseHandling	read, access	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.RequireCertificateEKUs	access	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SystemDefaultTlsVersions	read, access	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe, explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Action Center\Checks\{C8E6F269-B90A-4053-A3BE-499AFCEC98C4}.check.0\CheckSetting	read, access, write	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Uri.AllowDangerousUnicodeDecompositions	access	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	read, access	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.UseStrictRfcInterimResponseHandling	access	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	explorer.exe, isspos.exe, fling.exe, lsm.exe, 21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe, lsass.exe, yahoomessenger.exe, flashfxp.exe, congress.exe, wmiprvse.exe, system.exe, smartftp.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\Full\Release	read, access	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe, explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Action Center\Checks\{C8E6F269-B90A-4053-A3BE-499AFCEC98C4}.check.0	access	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe, explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\c0c40df0fc4d1585d5de603ec4f3d9f726afeeba	create, access	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	read, access	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\RequireCertificateEKUs	read, access	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName	read, access	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.UseHttpPipeliningAndBufferPooling	access	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\AllowDangerousUnicodeDecompositions	read, access	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseStrictIPv6AddressParsing	read, access	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe, explorer.exe	CLEAN

Process

Process Name	Commandline	Verdict
21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe	"C:\Users\kEecfMwgj\Desktop\21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71.exe"	MALICIOUS
explorer.exe	"C:\Program Files (x86)\MSBuild\Microsoft\explorer.exe"	MALICIOUS
schtasks.exe	schtasks.exe /create /tn "yahoomessengery" /sc MINUTE /mo 8 /tr "'C:\Program Files (x86)\Windows Portable Devices\yahoomessenger.exe'" /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "yahoomessenger" /sc ONLOGON /tr "'C:\Program Files (x86)\Windows Portable Devices\yahoomessenger.exe'" /rl HIGHEST /f	SUSPICIOUS

Process Name	Commandline	Verdict
schtasks.exe	schtasks.exe /create /tn "SystemS" /sc MINUTE /mo 14 /tr "'C:\Users\kEecfMwgj\Downloads\System.exe'" /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "System" /sc ONLOGON /tr "'C:\Users\kEecfMwgj\Downloads\System.exe'" /rl HIGHEST /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "flingf" /sc MINUTE /mo 14 /tr "'C:\Users\kEecfMwgj\NetHood\fling.exe'" /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "fling" /sc ONLOGON /tr "'C:\Users\kEecfMwgj\NetHood\fling.exe'" /rl HIGHEST /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "WmiPrvSEW" /sc MINUTE /mo 8 /tr "'C:\Boot\ko-KR\WmiPrvSE.exe'" /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "WmiPrvSE" /sc ONLOGON /tr "'C:\Boot\ko-KR\WmiPrvSE.exe'" /rl HIGHEST /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "flingf" /sc MINUTE /mo 9 /tr "'C:\Users\All Users\Microsoft\WwanSvc\fling.exe'" /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "fling" /sc ONLOGON /tr "'C:\Users\All Users\Microsoft\WwanSvc\fling.exe'" /rl HIGHEST /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "lsml" /sc MINUTE /mo 14 /tr "'C:\Boot\de-DE\lsm.exe'" /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "lsm" /sc ONLOGON /tr "'C:\Boot\de-DE\lsm.exe'" /rl HIGHEST /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "explorere" /sc MINUTE /mo 6 /tr "'C:\Program Files (x86)\MSBuild\Microsoft\explorer.exe'" /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "explorer" /sc ONLOGON /tr "'C:\Program Files (x86)\MSBuild\Microsoft\explorer.exe'" /rl HIGHEST /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "smartftps" /sc MINUTE /mo 10 /tr "'C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\smartftp.exe'" /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "smartftp" /sc ONLOGON /tr "'C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\smartftp.exe'" /rl HIGHEST /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "lsassl" /sc MINUTE /mo 6 /tr "'C:\MSOCache\All Users\lsass.exe'" /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "lsass" /sc ONLOGON /tr "'C:\MSOCache\All Users\lsass.exe'" /rl HIGHEST /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "flashfxpf" /sc MINUTE /mo 5 /tr "'C:\Windows\en-US\flashfxp.exe'" /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "flashfxp" /sc ONLOGON /tr "'C:\Windows\en-US\flashfxp.exe'" /rl HIGHEST /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "issposi" /sc MINUTE /mo 8 /tr "'C:\Windows\Help\Windows\isspos.exe'" /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "isspos" /sc ONLOGON /tr "'C:\Windows\Help\Windows\isspos.exe'" /rl HIGHEST /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "smartftps" /sc MINUTE /mo 9 /tr "'C:\Windows\Offline Web Pages\smartftp.exe'" /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "smartftp" /sc ONLOGON /tr "'C:\Windows\Offline Web Pages\smartftp.exe'" /rl HIGHEST /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "WmiPrvSEW" /sc MINUTE /mo 5 /tr "'C:\Program Files\Windows Defender\en-US\WmiPrvSE.exe'" /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "WmiPrvSE" /sc ONLOGON /tr "'C:\Program Files\Windows Defender\en-US\WmiPrvSE.exe'" /rl HIGHEST /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "congressc" /sc MINUTE /mo 11 /tr "'C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\congress.exe'" /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "congress" /sc ONLOGON /tr "'C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\congress.exe'" /rl HIGHEST /f	SUSPICIOUS
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "yahoomessengery" /sc MINUTE /mo 14 /tr "'C:\Program Files (x86)\Windows Portable Devices\yahoomessenger.exe'" /rl HIGHEST /f	CLEAN
schtasks.exe	schtasks.exe /create /tn "SystemS" /sc MINUTE /mo 8 /tr "'C:\Users\kEecfMwgj\Downloads\System.exe'" /rl HIGHEST /f	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN

Process Name	Commandline	Verdict
schtasks.exe	schtasks.exe /create /tn "flingf" /sc MINUTE /mo 11 /tr "'C:\Users\kEecfMwgj\NetHood\fling.exe'" /rl HIGHEST /f	CLEAN
schtasks.exe	schtasks.exe /create /tn "WmiPrvSEW" /sc MINUTE /mo 14 /tr "'C:\Boot\ko-KR\WmiPrvSE.exe'" /rl HIGHEST /f	CLEAN
schtasks.exe	schtasks.exe /create /tn "flingf" /sc MINUTE /mo 11 /tr "'C:\Users\All Users\Microsoft\WwanSvc\fling.exe'" /rl HIGHEST /f	CLEAN
schtasks.exe	schtasks.exe /create /tn "lsmI" /sc MINUTE /mo 8 /tr "'C:\Boot\de-DE\lsm.exe'" /rl HIGHEST /f	CLEAN
schtasks.exe	schtasks.exe /create /tn "explorere" /sc MINUTE /mo 10 /tr "'C:\Program Files (x86)\MSBuild\Microsoft\explorer.exe'" /rl HIGHEST /f	CLEAN
schtasks.exe	schtasks.exe /create /tn "smartftps" /sc MINUTE /mo 13 /tr "'C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\smartftp.exe'" /rl HIGHEST /f	CLEAN
schtasks.exe	schtasks.exe /create /tn "lsassl" /sc MINUTE /mo 5 /tr "'C:\MSOCache\All Users\lsass.exe'" /rl HIGHEST /f	CLEAN
schtasks.exe	schtasks.exe /create /tn "flashfxpf" /sc MINUTE /mo 5 /tr "'C:\Windows\en-US\flashfxp.exe'" /rl HIGHEST /f	CLEAN
schtasks.exe	schtasks.exe /create /tn "issposi" /sc MINUTE /mo 10 /tr "'C:\Windows\Help\Windows\isspos.exe'" /rl HIGHEST /f	CLEAN
schtasks.exe	schtasks.exe /create /tn "smartftps" /sc MINUTE /mo 14 /tr "'C:\Windows\Offline Web Pages\smartftp.exe'" /rl HIGHEST /f	CLEAN
schtasks.exe	schtasks.exe /create /tn "WmiPrvSEW" /sc MINUTE /mo 5 /tr "'C:\Program Files\Windows Defender\en-US\WmiPrvSE.exe'" /rl HIGHEST /f	CLEAN
schtasks.exe	schtasks.exe /create /tn "congressc" /sc MINUTE /mo 10 /tr "'C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\congress.exe'" /rl HIGHEST /f	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /C "C:\Users\kEecfMwgj\AppData\Local\Temp\UiqPJstYE1.bat"	CLEAN
w32tm.exe	w32tm /stripchart /computer:localhost /period:5 /dataonly /samples:2	CLEAN
taskeng.exe	taskeng.exe {1202B463-65FD-4008-AD56-FFB42ECEBA22} S-1-5-21-4219442223-4223814209-3835049652-1000:Q9IATRKPRH\kEecfMwgj:Interactive:[1]	CLEAN
smartftp.exe	"C:\Windows\Offline Web Pages\smartftp.exe"	CLEAN
explorer.exe	"C:\Program Files (x86)\MSBuild\Microsoft\explorer.exe"	CLEAN
lsm.exe	C:\Boot\de-DE\lsm.exe	CLEAN
congress.exe	C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\congress.exe	CLEAN
lsass.exe	"C:\MSOCache\All Users\lsass.exe"	CLEAN
fling.exe	"C:\Users\All Users\Microsoft\WwanSvc\fling.exe"	CLEAN
yahoomessenger.exe	"C:\Program Files (x86)\Windows Portable Devices\yahoomessenger.exe"	CLEAN
isspos.exe	C:\Windows\Help\Windows\isspos.exe	CLEAN
flashfxp.exe	C:\Windows\en-US\flashfxp.exe	CLEAN
system.exe	C:\Users\kEecfMwgj\Downloads\System.exe	CLEAN
wmiprvse.exe	"C:\Program Files\Windows Defender\en-US\WmiPrvSE.exe"	CLEAN

YARA / AV

No YARA or AV matches available.

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