MALICIOUS

Classifications: -

Threat Names: Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**05379ea4600304f51cffa8d1ee9e3b2931a69129f6bed14d45a500d966a71fca.exe**
ID	#5071275
MD5	54172888b473f2515b13fe1e2032a112
SHA1	fc4ff4d53a1ea6cfee9265840bfc1dda0ee8c1e6
SHA256	05379ea4600304f51cffa8d1ee9e3b2931a69129f6bed14d45a500d966a71fca
File Size	1203.65 KB
Report Created	2022-08-06 04:17 (UTC+2)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (14 rules, 101 matches)

Score	Category	Operation	Count	Classification
4/5	Masquerade	Creates a new process masquerading as a system process	1	-
	• (Process #76) taskeng.exe creates a process named explorer.exe.			
4/5	Reputation	Known malicious file	2	-
	• Reputation analysis labels the sample itself as Mal/Generic-S. • Reputation analysis labels file "C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\absolutetelnet.exe" as Mal/Generic-S.			
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	32	-
	• Schedules task for command ""C:\comproviderRuntimecommon\whatever_only.exe"", to be triggered by LOGON. • Schedules task for command ""C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\RedistList\spcwin.exe"", to be triggered by LOGON. • Schedules task for command ""C:\Boot\ru-RU\but inside save.exe"", to be triggered by LOGON. • Schedules task for command ""C:\Boot\es-ES\Idle.exe"", to be triggered by LOGON. • Schedules task for command ""C:\Boot\pl-PL\operamail.exe"", to be triggered by LOGON. • Schedules task for command ""C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\explorer.exe"", to be triggered by LOGON. • Schedules task for command ""C:\Program Files (x86)\Microsoft OneDrive\omnipos.exe"", to be triggered by LOGON. • Schedules task for command ""C:\Program Files\Reference Assemblies\taskhost.exe"", to be triggered by LOGON. • Schedules task for command ""C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\absolutetelnet.exe"", to be triggered by LOGON. • Schedules task for command ""C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\services.exe"", to be triggered by LOGON. • Schedules task for command ""C:\Users\Default\Recent\iexplore.exe"", to be triggered by LOGON. • Schedules task for command ""C:\Windows\SysWOW64\winrm\0409\fpos.exe"", to be triggered by LOGON. • Schedules task for command ""C:\comproviderRuntimecommon\but inside save.exe"", to be triggered by LOGON. • Schedules task for command ""C:\Users\Default\spoolsv.exe"", to be triggered by LOGON. • Schedules task for command ""C:\Program Files\Windows NT\Accessories\en-US\yardadultbehind.exe"", to be triggered by LOGON. • Schedules task for command ""C:\Users\Default User\flashfxp.exe"", to be triggered by LOGON. • Schedules task for command ""C:\comproviderRuntimecommon\whatever_only.exe"", to be triggered by TIME. Task has been rescheduled by the analyzer. • Schedules task for command ""C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\RedistList\spcwin.exe"", to be triggered by TIME. Task has been rescheduled by the analyzer. • Schedules task for command ""C:\Boot\ru-RU\but inside save.exe"", to be triggered by TIME. Task has been rescheduled by the analyzer. • Schedules task for command ""C:\Boot\es-ES\Idle.exe"", to be triggered by TIME. Task has been rescheduled by the analyzer. • Schedules task for command ""C:\Boot\pl-PL\operamail.exe"", to be triggered by TIME. Task has been rescheduled by the analyzer. • Schedules task for command ""C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\explorer.exe"", to be triggered by TIME. Task has been rescheduled by the analyzer. • Schedules task for command ""C:\Program Files (x86)\Microsoft OneDrive\omnipos.exe"", to be triggered by TIME. Task has been rescheduled by the analyzer. • Schedules task for command ""C:\Program Files\Reference Assemblies\taskhost.exe"", to be triggered by TIME. Task has been rescheduled by the analyzer. • Schedules task for command ""C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\absolutetelnet.exe"", to be triggered by TIME. Task has been rescheduled by the analyzer. • Schedules task for command ""C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\services.exe"", to be triggered by TIME. Task has been rescheduled by the analyzer. • Schedules task for command ""C:\Users\Default\Recent\iexplore.exe"", to be triggered by TIME. Task has been rescheduled by the analyzer. • Schedules task for command ""C:\Windows\SysWOW64\winrm\0409\fpos.exe"", to be triggered by TIME. Task has been rescheduled by the analyzer. • Schedules task for command ""C:\comproviderRuntimecommon\but inside save.exe"", to be triggered by TIME. Task has been rescheduled by the analyzer. • Schedules task for command ""C:\Users\Default\spoolsv.exe"", to be triggered by TIME. Task has been rescheduled by the analyzer. • Schedules task for command ""C:\Program Files\Windows NT\Accessories\en-US\yardadultbehind.exe"", to be triggered by TIME. Task has been rescheduled by the analyzer. • Schedules task for command ""C:\Users\Default User\flashfxp.exe"", to be triggered by TIME. Task has been rescheduled by the analyzer.			
2/5	Task Scheduling	Schedules task via schtasks	30	-

Score	Category	Operation	Count	Classification
		• Schedules task "whatever_onlyw" via the schtasks command line utility. • Schedules task "whatever_only" via the schtasks command line utility. • Schedules task "spcwins" via the schtasks command line utility. • Schedules task "spcwin" via the schtasks command line utility. • Schedules task "but inside saveb" via the schtasks command line utility. • Schedules task "but inside save" via the schtasks command line utility. • Schedules task "Idlel" via the schtasks command line utility. • Schedules task "Idle" via the schtasks command line utility. • Schedules task "operamailo" via the schtasks command line utility. • Schedules task "operamail" 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 "omniposo" via the schtasks command line utility. • Schedules task "omnipos" via the schtasks command line utility. • Schedules task "taskhostt" via the schtasks command line utility. • Schedules task "taskhost" via the schtasks command line utility. • Schedules task "absolutetelneta" via the schtasks command line utility. • Schedules task "absolutetelnet" via the schtasks command line utility. • Schedules task "servicess" via the schtasks command line utility. • Schedules task "services" via the schtasks command line utility. • Schedules task "iexplorei" via the schtasks command line utility. • Schedules task "iexplore" via the schtasks command line utility. • Schedules task "fposf" via the schtasks command line utility. • Schedules task "fpos" via the schtasks command line utility. • Schedules task "spoolsvs" via the schtasks command line utility. • Schedules task "spoolsv" via the schtasks command line utility. • Schedules task "yardadultbehindy" via the schtasks command line utility. • Schedules task "yardadultbehind" via the schtasks command line utility. • Schedules task "flashfxpf" via the schtasks command line utility. • Schedules task "flashfxp" via the schtasks command line utility.		
1/5	Hide Tracks	Creates process with hidden window	2	-
		• (Process #2) wscript.exe starts (process #3) cmd.exe with a hidden window. • (Process #4) chainsavesref.exe starts (process #68) cmd.exe with a hidden window.		
1/5	Privilege Escalation	Enables process privilege	1	-
		• (Process #4) chainsavesref.exe enables process privilege "SeDebugPrivilege".		
1/5	Mutex	Creates mutex	1	-
		• (Process #4) chainsavesref.exe creates mutex with name "Local\a662db5313495af89c12e9daf05e137fcad6fcec".		
1/5	System Modification	Modifies operating system directory	4	-
		• (Process #4) chainsavesref.exe creates file "C:\Windows\schemas\EAPMethods\csrss.exe" in the OS directory. • (Process #4) chainsavesref.exe creates file "C:\Windows\SysWOW64\winrm\0409\fpos.exe" in the OS directory. • (Process #4) chainsavesref.exe creates file "C:\Windows\SysWOW64\winrm\0409\2cfdd657e33eed" in the OS directory. • (Process #4) chainsavesref.exe creates file "C:\Windows\CSC\v2.0.6\far.exe" in the OS directory.		
1/5	System Modification	Modifies application directory	8	-

Score	Category	Operation	Count	Classification
		• (Process #4) chainsavesref.exe modifies "C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\RedistList\spcwin.exe". • (Process #4) chainsavesref.exe modifies "C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\RedistList\dea609c9470f15". • (Process #4) chainsavesref.exe modifies "C:\Program Files (x86)\Microsoft OneDrive\omnipos.exe". • (Process #4) chainsavesref.exe modifies "C:\Program Files (x86)\Microsoft OneDrive\9a9ef8f6a80f81". • (Process #4) chainsavesref.exe modifies "C:\Program Files\Reference Assemblies\taskhost.exe". • (Process #4) chainsavesref.exe modifies "C:\Program Files\Reference Assemblies\b75386f1303e64". • (Process #4) chainsavesref.exe modifies "C:\Program Files\Windows NT\Accessories\en-US\yardadultbehind.exe". • (Process #4) chainsavesref.exe modifies "C:\Program Files\Windows NT\Accessories\en-US\ac6c4644f9bcea".		
1/5	Hide Tracks	Writes an unusually large amount of data to the registry	1	-
		• (Process #4) chainsavesref.exe hides 2418 bytes in "HKEY_CURRENT_USER\Software\caa6004a855dece65e49fdcfb42785d36f42888b\437b07143d558f8f987cd92e573298e152164cb4".		
1/5	Obfuscation	Resolves API functions dynamically	3	-
		• (Process #1) 05379ea4600304f51cffa8d1ee9e3b2931a69129f6bed14d45a500d966a71fca.exe resolves 49 API functions by name. • (Process #4) chainsavesref.exe resolves 41 API functions by name. • (Process #6) wmiprvse.exe resolves 25 API functions by name.		
1/5	Execution	Drops PE file	14	-
		• (Process #4) chainsavesref.exe drops file "C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\absolutetelnet.exe". • (Process #4) chainsavesref.exe drops file "C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\explorer.exe". • (Process #4) chainsavesref.exe drops file "C:\Boot\es-ES\Idle.exe". • (Process #4) chainsavesref.exe drops file "C:\comproviderRuntimecommon\whatever_only.exe". • (Process #4) chainsavesref.exe drops file "C:\Program Files\Reference Assemblies\taskhost.exe". • (Process #4) chainsavesref.exe drops file "C:\Program Files (x86)\Microsoft OneDrive\omnipos.exe". • (Process #4) chainsavesref.exe drops file "C:\Boot\pl-PL\operamail.exe". • (Process #4) chainsavesref.exe drops file "C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\RedistList\spcwin.exe". • (Process #4) chainsavesref.exe drops file "C:\Windows\SysWOW64\winrm\0409\fpos.exe". • (Process #4) chainsavesref.exe drops file "C:\Program Files\Windows NT\Accessories\en-US\yardadultbehind.exe". • (Process #4) chainsavesref.exe drops file "C:\Boot\ru-RU\but inside save.exe". • (Process #4) chainsavesref.exe drops file "C:\Users\Default\spoolsv.exe". • (Process #4) chainsavesref.exe drops file "C:\comproviderRuntimecommon\but inside save.exe". • (Process #4) chainsavesref.exe drops file "C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\services.exe".		
1/5	Execution	Executes dropped PE file	1	-
		• Executes dropped file "C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\absolutetelnet.exe".		
-	Trusted	Known clean file	1	-
		• Embedded file "" is a known clean file.		

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	#T1143 Hidden Window							
				#T1112 Modify Registry							
				#T1045 Software Packing							

Sample Information

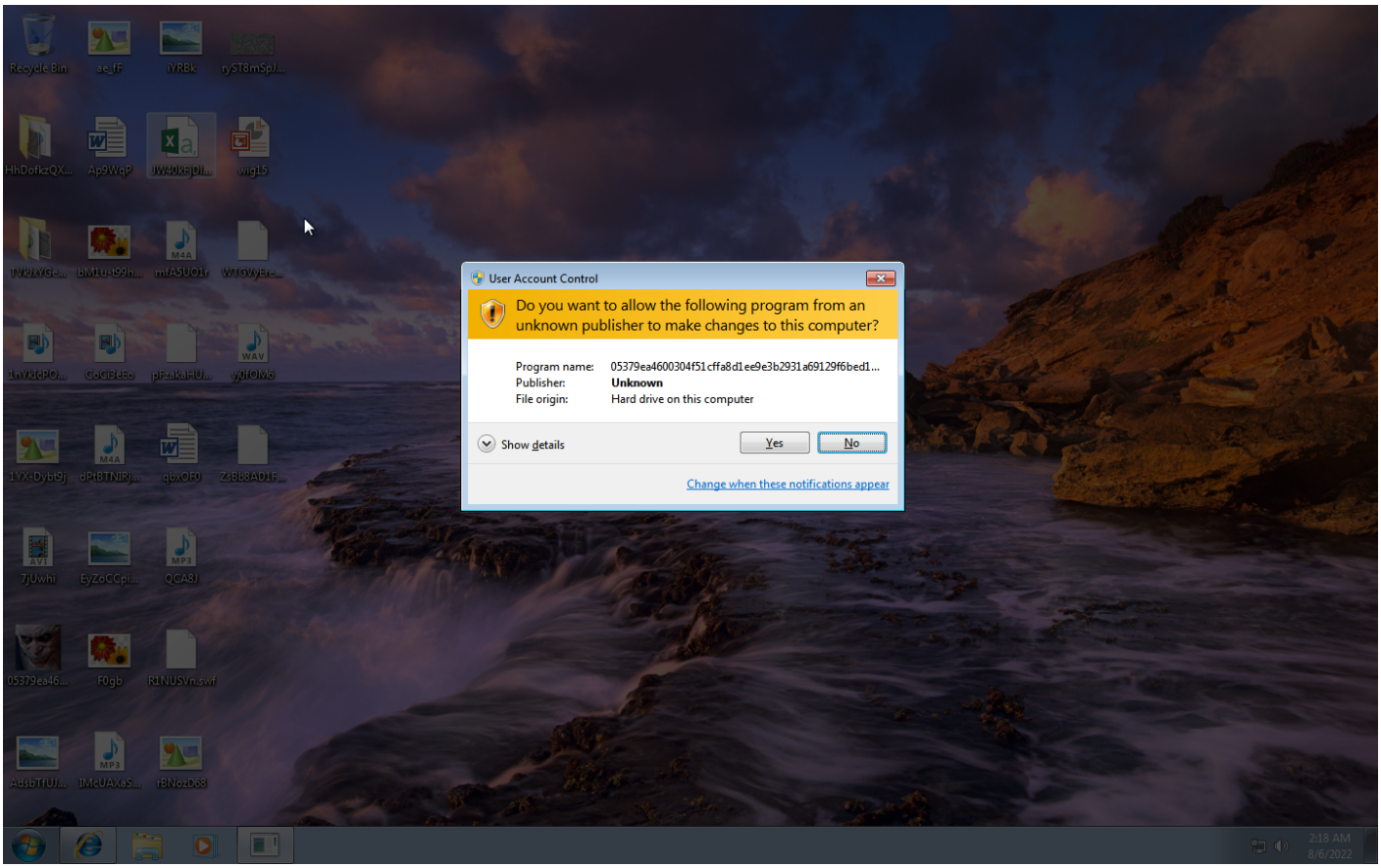
ID	#5071275
MD5	54172888b473f2515b13fe1e2032a112
SHA1	fc4ff4d53a1ea6cfee9265840bfc1dda0ee8c1e6
SHA256	05379ea4600304f51cffa8d1ee9e3b2931a69129f6bed14d45a500d966a71fca
SSDeep	12288:WRZ+IoG/n9lQxW3OBseWyx/bl84s165YnPKDGWcvOarVwvZDyg7VGNtlmleJS:Q2G/nvxW3Ww4DW1lDGWcmarVKFPJS
ImpHash	fcf1390e9ce472c7270447fc5c61a0c1
File Name	05379ea4600304f51cffa8d1ee9e3b2931a69129f6bed14d45a500d966a71fca.exe
File Size	1203.65 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2022-08-06 04:17 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	73
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
ae_fF
iYRBk
ryST8mSpJ...
HhDofkzQX...
Ap9WqP
JW40kFjDI...
wig15
TVkJxYGe...
bM1u-t99h...
mfA5UO1r
WTGVyEre...
1nYklcPO...
CoCiBeEo
pFzakaHU...
yj0fOM6
1YX-Dybt9j
dPtBTNIRj...
qbxOF0
ZsBb8AD1F...
7jUwhi
EyZoCCpi...
QCA8J
05379ea46...
F0gb
R1NUSVn.swf
AdsbTfUJ...
lMcUAXaS...
rBNozD68
2:18 AM
8/6/2022

Recycle Bin
ae_fF
iYRBk
ryST8mSpJ...
HhDofkzQX...
Ap9WqP
JW40kFjDI...
wig15
TVkJxYGe...
bM1u-t99h...
mfA5UO1r
WTGVyEre...
1nYklcPO...
CoCiBeEo
pFzakaHU...
yj0fOM6
1YX-Dybt9j
dPtBTNIRj...
qbxOF0
ZsBb8AD1F...
7jUwhi
EyZoCCpi...
QCA8J
05379ea46...
F0gb
R1NUSVn.swf
AdsbTfUJ...
lMcUAXaS...
rBNozD68
2:18 AM
8/6/2022



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

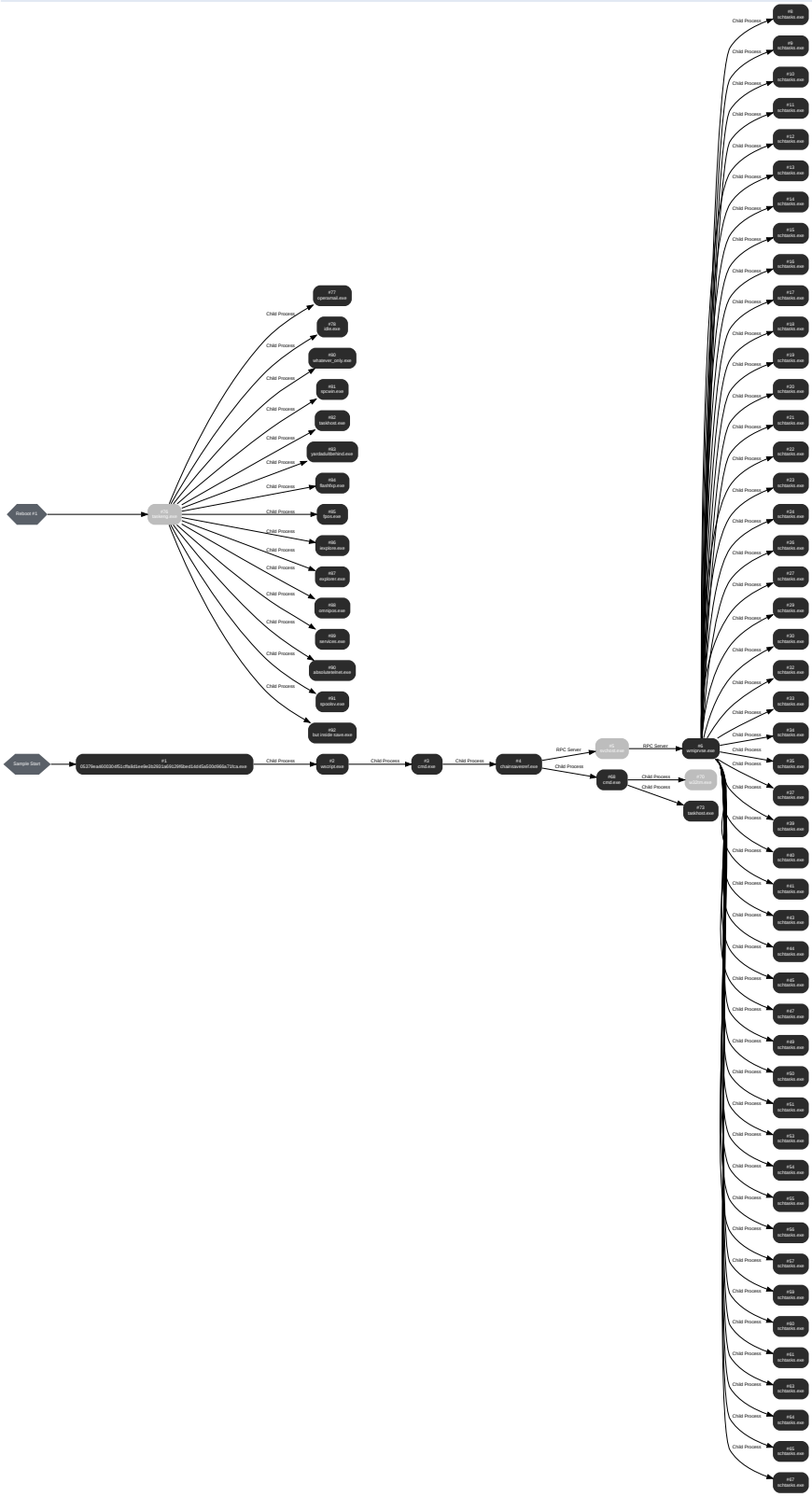
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: 05379ea4600304f51cffa8d1ee9e3b2931a69129f6bed14d45a500d966a71fca.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\05379ea4600304f51cffa8d1ee9e3b2931a69129f6bed14d45a500d966a71fca.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\05379ea4600304f51cffa8d1ee9e3b2931a69129f6bed14d45a500d966a71fca.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 50883, Reason: Analysis Target
Unmonitor End Time	End Time: 83721, Reason: Terminated
Monitor duration	32.84s
Return Code	0
PID	3588
Parent PID	1916
Bitness	32 Bit

Dropped Files (4)

File Name	File Size	SHA256	YARA Match
C:\comproviderRuntimecommon\DLLiR59GMmL352HHbgfc.bat	47 bytes	09c3e02a4caad39e7c91f0ba1cc93c8c727d23b306da9129cca1d0955880c33e	✖
chainsavesref.exe	828.50 KB	b570e2028088759d02ea13f7646bf7aca78865d55f7fd8e2efaeec45c670e9ff	✖
C:\comproviderRuntimecommon\et1pu6VAlkUOY7GuC90A.vbe	221 bytes	0864baa556adddc451e8ad0acbdfbaf692a7371a5cbb8ef2b2b83aa05c56fb39	✖
__tmp_rar_sfx_access_check_20445881	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
System	16
Module	86
File	130
Environment	5
Window	2
-	1
Process	1

Process #2: wscript.exe

ID	2
File Name	c:\windows\syswow64\wscript.exe
Command Line	"C:\Windows\System32\WScript.exe" "C:\comproviderRuntimecommon\et1pu6VAlkUOY7GuC90A.vbe"
Initial Working Directory	C:\comproviderRuntimecommon\
Monitor Start Time	Start Time: 81630, Reason: Child Process
Unmonitor End Time	End Time: 94359, Reason: Terminated
Monitor duration	12.73s
Return Code	0
PID	3612
Parent PID	3588
Bitness	32 Bit

Host Behavior

Type	Count
System	17
Module	25
Registry	27
-	1
Window	2
COM	7
File	4
Process	1

Process #3: cmd.exe

ID	3
File Name	c:\windows\syswow64\cmd.exe
Command Line	C:\Windows\system32\cmd.exe /c ""C:\comproviderRuntimecommon\DLLiR59GMmL352HHbgfc.bat" "
Initial Working Directory	C:\comproviderRuntimecommon\
Monitor Start Time	Start Time: 92633, Reason: Child Process
Unmonitor End Time	End Time: 176843, Reason: Terminated
Monitor duration	84.21s
Return Code	0
PID	3656
Parent PID	3612
Bitness	32 Bit

Host Behavior

Type	Count
Module	5
File	52
Environment	10
Process	1

Process #4: chainsavesref.exe

ID	4
File Name	c:\comproviderruntimecommon\chainsavesref.exe
Command Line	"C:\comproviderRuntimecommon\chainsavesref.exe"
Initial Working Directory	C:\comproviderRuntimecommon\
Monitor Start Time	Start Time: 93661, Reason: Child Process
Unmonitor End Time	End Time: 175828, Reason: Terminated
Monitor duration	82.17s
Return Code	0
PID	3680
Parent PID	3656
Bitness	64 Bit

Dropped Files (19)

File Name	File Size	SHA256	YARA Match
C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\c5b4cb5e9653cc	447 bytes	3e6d9b2b18eee239c9ec1f5fc1a29c02bc1f9b18d59d20cd6a4a84bacadcd710	✖
C:\Windows\SysWOW64\winrm\0409\2cfdd657e33eed	900 bytes	100f3958bd7e682bf500ed0effade3dec6a741bafda3987ae159ad9932683ae4	✖
C:\Program Files\Reference Assemblies\b75386f1303e64	908 bytes	d67ca00c04545c3ac50cbdaf0eb69e9c9a2a75879b4700c165da1d53298fa0d7	✖
C:\comproviderRuntimecommon\c34a7c10ac282e	322 bytes	ea5e14d8ddabbab9797ca1d20e0ad93ced8f2c2507834a704d6ae9b1d592267b	✖
C:\Boot\pl-PL\172e128c88b792	382 bytes	53f23b0c58e94f8b4dc161bd51c8cbddea365e1cd183a846d07ac366b0de59d7	✖
C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\RedistList\dea609c9470f15	478 bytes	60eedcadb8fc106e4ac1028bfc61c649eaec2247dc9c217272f265420afbb7a5	✖
C:\Users\kEecfMwgj\AppData\Local\Temp\1fgVzmzb1s	25 bytes	478547b4f458ac74edd4bb6b634a3b3d75ccbfae4567ec48782911d15d21a304	✖
C:\Users\kEecfMwgj\AppData\Local\Temp\GYwzkQocQK.bat	219 bytes	a2d04dd6baa82f73d47208295e5352ed4877c1b8ca45afbc624d4f60d04c8a75	✖
C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\7a0fd90576e088	64 bytes	1795bc9fc79dc8f4707197ec13aa0a07572fd226c0f94d5def68ec7c3e17e692	✖
C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\9e3bd0c464004d	731 bytes	8e68e8c091974947b89d092faee94cbd7e15f7ff1dc331b181287a036575a667	✖
C:\Boot\es-ES\6ccacd8608530f	691 bytes	bd034e99db8f96b343f84cee052fcf96394f2fb2ef77f468f2c82b80af97fee2	✖
C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\absolutetelnet.exe	828.50 KB	b570e2028088759d02ea13f7646bf7aca78865d55f7fd8e2efaeec45c670e9ff	✖
C:\Program Files (x86)\Microsoft OneDrive\9a9ef8f6a80f81	386 bytes	321b7f25ff2c1757c483153a8244e40e550fa09b1a10bed6acd8ad59053a6348	✖
-	948 bytes	586e9359009845126614ca003f3862e4f72f9994b91e86a521aa1d425c37db89	✖
C:\comproviderRuntimecommon\e76e23195dba9d	988 bytes	4b8e865b614cb8abf63cd9c71866454c2c03da9c7ca21ce2c7ac7b149105bb44	✖
-	132 bytes	b7a4ead73182d3ee99a9211111579e48f5ac3a0078a6d33515a558705de4e973	✖
C:\Users\Default\f3b6ecef712a24	943 bytes	9c80f368adba592c1c87ac0e1fecceaf2fce232f14351df983291aa1a595f629	✖
C:\Boot\ru-RU\e76e23195dba9d	257 bytes	ec2b285db6f6baebf02c715c81db5a0af407ac21a6be3026faba0d1df0364226	✖
C:\Program Files\Windows NT\Accessories\en-US\ac6c4644f9bcea	965 bytes	c402b2e2e0bc9ed750d76511b0c23d464c5c616a9d9ada5e2eeec35a08936522	✖

Host Behavior

Type	Count
Registry	48
-	3
File	168
User	2
Module	51
System	23
Mutex	1
Process	39
COM	721

Process #5: svchost.exe

ID	5
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: 124567, Reason: RPC Server
Unmonitor End Time	End Time: 290916, Reason: Terminated by timeout
Monitor duration	166.35s
Return Code	Unknown
PID	872
Parent PID	3680
Bitness	64 Bit

Process #6: wmiprvse.exe

ID	6
File Name	c:\windows\system32\wbem\wmiprvse.exe
Command Line	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 124567, Reason: RPC Server
Unmonitor End Time	End Time: 290916, Reason: Terminated by timeout
Monitor duration	166.35s
Return Code	Unknown
PID	2948
Parent PID	872
Bitness	64 Bit

Host Behavior

Type	Count
Module	1131
System	360
Process	48
Registry	1

Process #8: schtasks.exe

ID	8
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "whatever_onlyw" /sc MINUTE /mo 11 /tr "'C:\comproviderRuntimecommon\whatever_only.exe'" /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 126068, Reason: Child Process
Unmonitor End Time	End Time: 129735, Reason: Terminated
Monitor duration	3.67s
Return Code	0
PID	3748
Parent PID	2948
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 "whatever_only" /sc ONLOGON /tr "'C:\comproviderRuntimecommon\whatever_only.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 126765, Reason: Child Process
Unmonitor End Time	End Time: 129842, Reason: Terminated
Monitor duration	3.08s
Return Code	0
PID	3756
Parent PID	2948
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 "whatever_onlyw" /sc MINUTE /mo 5 /tr "'C:\comproviderRuntimecommon\whatever_only.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 127417, Reason: Child Process
Unmonitor End Time	End Time: 129221, Reason: Terminated
Monitor duration	1.80s
Return Code	0
PID	3772
Parent PID	2948
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 "spcwins" /sc MINUTE /mo 8 /tr "'C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\RedistList\spcwin.exe'" /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 129222, Reason: Child Process
Unmonitor End Time	End Time: 130436, Reason: Terminated
Monitor duration	1.21s
Return Code	0
PID	3784
Parent PID	2948
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 "spcwin" /sc ONLOGON /tr "'C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\RedistList\spcwin.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 129737, Reason: Child Process
Unmonitor End Time	End Time: 131194, Reason: Terminated
Monitor duration	1.46s
Return Code	0
PID	3796
Parent PID	2948
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 "spcwins" /sc MINUTE /mo 5 /tr "'C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\RedistList\spcwin.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 130438, Reason: Child Process
Unmonitor End Time	End Time: 131830, Reason: Terminated
Monitor duration	1.39s
Return Code	0
PID	3808
Parent PID	2948
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 "but inside saveb" /sc MINUTE /mo 8 /tr "'C:\Boot\ru-RU\but inside save.exe'" /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 131196, Reason: Child Process
Unmonitor End Time	End Time: 132448, Reason: Terminated
Monitor duration	1.25s
Return Code	0
PID	3820
Parent PID	2948
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 "but inside save" /sc ONLOGON /tr "'C:\Boot\ru-RU\but inside save.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 131831, Reason: Child Process
Unmonitor End Time	End Time: 133188, Reason: Terminated
Monitor duration	1.36s
Return Code	0
PID	3836
Parent PID	2948
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 "but inside saveb" /sc MINUTE /mo 12 /tr "'C:\Boot\ru-RU\but inside save.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 132449, Reason: Child Process
Unmonitor End Time	End Time: 134495, Reason: Terminated
Monitor duration	2.05s
Return Code	0
PID	3848
Parent PID	2948
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 "Idlel" /sc MINUTE /mo 6 /tr "'C:\Boot\es-ES\Idle.exe'" /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 133190, Reason: Child Process
Unmonitor End Time	End Time: 134436, Reason: Terminated
Monitor duration	1.25s
Return Code	0
PID	3860
Parent PID	2948
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 "Idle" /sc ONLOGON /tr "'C:\Boot\es-ES\Idle.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 133721, Reason: Child Process
Unmonitor End Time	End Time: 135634, Reason: Terminated
Monitor duration	1.91s
Return Code	0
PID	3872
Parent PID	2948
Bitness	64 Bit

Host Behavior

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

Process #19: schtasks.exe

ID	19
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "Idlel" /sc MINUTE /mo 9 /tr "'C:\Boot\es-ES\Idle.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 134439, Reason: Child Process
Unmonitor End Time	End Time: 136186, Reason: Terminated
Monitor duration	1.75s
Return Code	0
PID	3884
Parent PID	2948
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 "operamailo" /sc MINUTE /mo 10 /tr "'C:\Boot\pl-PL\operamail.exe'" /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 135231, Reason: Child Process
Unmonitor End Time	End Time: 136970, Reason: Terminated
Monitor duration	1.74s
Return Code	0
PID	3896
Parent PID	2948
Bitness	64 Bit

Host Behavior

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

Process #21: schtasks.exe

ID	21
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "operamail" /sc ONLOGON /tr "'C:\Boot\pl-PL\operamail.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 135636, Reason: Child Process
Unmonitor End Time	End Time: 137624, Reason: Terminated
Monitor duration	1.99s
Return Code	0
PID	3908
Parent PID	2948
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 "operamailo" /sc MINUTE /mo 13 /tr "'C:\Boot\pl-PL\operamail.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 136272, Reason: Child Process
Unmonitor End Time	End Time: 138368, Reason: Terminated
Monitor duration	2.10s
Return Code	0
PID	3920
Parent PID	2948
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 "explorere" /sc MINUTE /mo 13 /tr "'C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\explorer.exe'" /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 137053, Reason: Child Process
Unmonitor End Time	End Time: 138356, Reason: Terminated
Monitor duration	1.30s
Return Code	0
PID	3932
Parent PID	2948
Bitness	64 Bit

Host Behavior

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

Process #24: schtasks.exe

ID	24
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "explorer" /sc ONLOGON /tr "'C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\explorer.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 137626, Reason: Child Process
Unmonitor End Time	End Time: 139922, Reason: Terminated
Monitor duration	2.30s
Return Code	0
PID	3944
Parent PID	2948
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 5 /tr "'C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\explorer.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 138369, Reason: Child Process
Unmonitor End Time	End Time: 140330, Reason: Terminated
Monitor duration	1.96s
Return Code	0
PID	3968
Parent PID	2948
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 "omniposo" /sc MINUTE /mo 14 /tr "'C:\Program Files (x86)\Microsoft OneDrive\omnipos.exe'" /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 139924, Reason: Child Process
Unmonitor End Time	End Time: 141186, Reason: Terminated
Monitor duration	1.26s
Return Code	0
PID	4004
Parent PID	2948
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 "omnipos" /sc ONLOGON /tr "'C:\Program Files (x86)\Microsoft OneDrive\omnipos.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 140656, Reason: Child Process
Unmonitor End Time	End Time: 142133, Reason: Terminated
Monitor duration	1.48s
Return Code	0
PID	4024
Parent PID	2948
Bitness	64 Bit

Host Behavior

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

Process #30: schtasks.exe

ID	30
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "omniposo" /sc MINUTE /mo 12 /tr "'C:\Program Files (x86)\Microsoft OneDrive\omnipos.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 141188, Reason: Child Process
Unmonitor End Time	End Time: 143176, Reason: Terminated
Monitor duration	1.99s
Return Code	0
PID	4036
Parent PID	2948
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 "taskhostt" /sc MINUTE /mo 6 /tr "'C:\Program Files\Reference Assemblies\taskhost.exe'" /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 142140, Reason: Child Process
Unmonitor End Time	End Time: 143940, Reason: Terminated
Monitor duration	1.80s
Return Code	0
PID	4060
Parent PID	2948
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 "taskhost" /sc ONLOGON /tr "'C:\Program Files\Reference Assemblies\taskhost.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 142671, Reason: Child Process
Unmonitor End Time	End Time: 144904, Reason: Terminated
Monitor duration	2.23s
Return Code	0
PID	4068
Parent PID	2948
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 "taskhostt" /sc MINUTE /mo 6 /tr "'C:\Program Files\Reference Assemblies\taskhost.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 143238, Reason: Child Process
Unmonitor End Time	End Time: 145534, Reason: Terminated
Monitor duration	2.30s
Return Code	0
PID	4084
Parent PID	2948
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 "absolutetelneta" /sc MINUTE /mo 6 /tr "'C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\absolutetelnet.exe'" /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 143942, Reason: Child Process
Unmonitor End Time	End Time: 146318, Reason: Terminated
Monitor duration	2.38s
Return Code	0
PID	2148
Parent PID	2948
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 "absolutetelnet" /sc ONLOGON /tr "'C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\absolutetelnet.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 145134, Reason: Child Process
Unmonitor End Time	End Time: 148204, Reason: Terminated
Monitor duration	3.07s
Return Code	0
PID	3076
Parent PID	2948
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 "absolutetelneta" /sc MINUTE /mo 12 /tr "'C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\absolutetelnet.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 146320, Reason: Child Process
Unmonitor End Time	End Time: 149171, Reason: Terminated
Monitor duration	2.85s
Return Code	0
PID	924
Parent PID	2948
Bitness	64 Bit

Host Behavior

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

Process #40: schtasks.exe

ID	40
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "servicess" /sc MINUTE /mo 5 /tr "'C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\services.exe'" /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 147231, Reason: Child Process
Unmonitor End Time	End Time: 150287, Reason: Terminated
Monitor duration	3.06s
Return Code	0
PID	3164
Parent PID	2948
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 "services" /sc ONLOGON /tr "'C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\services.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 149174, Reason: Child Process
Unmonitor End Time	End Time: 151427, Reason: Terminated
Monitor duration	2.25s
Return Code	0
PID	3160
Parent PID	2948
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 "servicess" /sc MINUTE /mo 11 /tr "'C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\services.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 150195, Reason: Child Process
Unmonitor End Time	End Time: 151949, Reason: Terminated
Monitor duration	1.75s
Return Code	0
PID	3188
Parent PID	2948
Bitness	64 Bit

Host Behavior

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

Process #44: schtasks.exe

ID	44
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "iexplorei" /sc MINUTE /mo 10 /tr "'C:\Users\Default\Recent\iexplore.exe'" /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 151429, Reason: Child Process
Unmonitor End Time	End Time: 154030, Reason: Terminated
Monitor duration	2.60s
Return Code	0
PID	3232
Parent PID	2948
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 "iexplore" /sc ONLOGON /tr "'C:\Users\Default\Recent\iexplore.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 151951, Reason: Child Process
Unmonitor End Time	End Time: 154812, Reason: Terminated
Monitor duration	2.86s
Return Code	0
PID	3220
Parent PID	2948
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 "iexplorei" /sc MINUTE /mo 9 /tr "'C:\Users\Default\Recent\iexplore.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 153070, Reason: Child Process
Unmonitor End Time	End Time: 155343, Reason: Terminated
Monitor duration	2.27s
Return Code	0
PID	3288
Parent PID	2948
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 "fposf" /sc MINUTE /mo 14 /tr "'C:\Windows\SysWOW64\winrm\0409\fpos.exe'" /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 154813, Reason: Child Process
Unmonitor End Time	End Time: 156657, Reason: Terminated
Monitor duration	1.84s
Return Code	0
PID	3248
Parent PID	2948
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 "fpos" /sc ONLOGON /tr "'C:\Windows\SysWOW64\winrm\0409\fpos.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 155345, Reason: Child Process
Unmonitor End Time	End Time: 157295, Reason: Terminated
Monitor duration	1.95s
Return Code	0
PID	3320
Parent PID	2948
Bitness	64 Bit

Host Behavior

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

Process #51: schtasks.exe

ID	51
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "fposf" /sc MINUTE /mo 11 /tr "'C:\Windows\SysWOW64\winrm\0409\fpos.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 156022, Reason: Child Process
Unmonitor End Time	End Time: 157980, Reason: Terminated
Monitor duration	1.96s
Return Code	0
PID	3308
Parent PID	2948
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 "but inside saveb" /sc MINUTE /mo 6 /tr "'C:\comproviderRuntimecommon\but inside save.exe'" /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 156713, Reason: Child Process
Unmonitor End Time	End Time: 158870, Reason: Terminated
Monitor duration	2.16s
Return Code	0
PID	3340
Parent PID	2948
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 "but inside save" /sc ONLOGON /tr "'C:\comproviderRuntimecommon\but inside save.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 157297, Reason: Child Process
Unmonitor End Time	End Time: 159727, Reason: Terminated
Monitor duration	2.43s
Return Code	0
PID	2908
Parent PID	2948
Bitness	64 Bit

Host Behavior

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

Process #55: schtasks.exe

ID	55
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "but inside saveb" /sc MINUTE /mo 6 /tr "'C:\comproviderRuntimecommon\but inside save.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 157991, Reason: Child Process
Unmonitor End Time	End Time: 160026, Reason: Terminated
Monitor duration	2.04s
Return Code	0
PID	1896
Parent PID	2948
Bitness	64 Bit

Host Behavior

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

Process #56: schtasks.exe

ID	56
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "spoolsvs" /sc MINUTE /mo 13 /tr "'C:\Users\Default\spoolsv.exe'" /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 159036, Reason: Child Process
Unmonitor End Time	End Time: 160194, Reason: Terminated
Monitor duration	1.16s
Return Code	0
PID	2224
Parent PID	2948
Bitness	64 Bit

Host Behavior

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

Process #57: schtasks.exe

ID	57
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "spoolsv" /sc ONLOGON /tr "'C:\Users\Default\spoolsv.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 159729, Reason: Child Process
Unmonitor End Time	End Time: 161594, Reason: Terminated
Monitor duration	1.86s
Return Code	0
PID	2236
Parent PID	2948
Bitness	64 Bit

Host Behavior

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

Process #59: schtasks.exe

ID	59
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "spoolsvs" /sc MINUTE /mo 5 /tr "'C:\Users\Default\spoolsv.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 160195, Reason: Child Process
Unmonitor End Time	End Time: 162016, Reason: Terminated
Monitor duration	1.82s
Return Code	0
PID	2300
Parent PID	2948
Bitness	64 Bit

Host Behavior

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

Process #60: schtasks.exe

ID	60
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "yardadultbehindy" /sc MINUTE /mo 8 /tr "'C:\Program Files\Windows NT\Accessories\en-US\yardadultbehind.exe'" /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 161079, Reason: Child Process
Unmonitor End Time	End Time: 162181, Reason: Terminated
Monitor duration	1.10s
Return Code	0
PID	2312
Parent PID	2948
Bitness	64 Bit

Host Behavior

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

Process #61: schtasks.exe

ID	61
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "yardadultbehind" /sc ONLOGON /tr "'C:\Program Files\Windows NT\Accessories\en-US\yardadultbehind.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 161596, Reason: Child Process
Unmonitor End Time	End Time: 162862, Reason: Terminated
Monitor duration	1.27s
Return Code	0
PID	2324
Parent PID	2948
Bitness	64 Bit

Host Behavior

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

Process #63: schtasks.exe

ID	63
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "yardadultbehindy" /sc MINUTE /mo 10 /tr "'C:\Program Files\Windows NT\Accessories\en-US\yardadultbehind.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 162182, Reason: Child Process
Unmonitor End Time	End Time: 163701, Reason: Terminated
Monitor duration	1.52s
Return Code	0
PID	2600
Parent PID	2948
Bitness	64 Bit

Host Behavior

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

Process #64: schtasks.exe

ID	64
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "flashfxpf" /sc MINUTE /mo 9 /tr "'C:\Users\Default User\flashfxp.exe'" /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 162864, Reason: Child Process
Unmonitor End Time	End Time: 165215, Reason: Terminated
Monitor duration	2.35s
Return Code	0
PID	2612
Parent PID	2948
Bitness	64 Bit

Host Behavior

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

Process #65: schtasks.exe

ID	65
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "flashfxp" /sc ONLOGON /tr "'C:\Users\Default User\flashfxp.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 163702, Reason: Child Process
Unmonitor End Time	End Time: 165867, Reason: Terminated
Monitor duration	2.17s
Return Code	0
PID	2624
Parent PID	2948
Bitness	64 Bit

Host Behavior

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

Process #67: schtasks.exe

ID	67
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /create /tn "flashfxpf" /sc MINUTE /mo 13 /tr "'C:\Users\Default User\flashfxp.exe'" /rl HIGHEST /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 164307, Reason: Child Process
Unmonitor End Time	End Time: 166469, Reason: Terminated
Monitor duration	2.16s
Return Code	0
PID	2648
Parent PID	2948
Bitness	64 Bit

Host Behavior

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

Process #68: cmd.exe

ID	68
File Name	c:\windows\system32\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C "C:\Users\kEecfMwgj\AppData\Local\Temp\GYwzkQocQK.bat"
Initial Working Directory	C:\comproviderRuntimecommon\
Monitor Start Time	Start Time: 174885, Reason: Child Process
Unmonitor End Time	End Time: 183792, Reason: Terminated
Monitor duration	8.91s
Return Code	1
PID	2672
Parent PID	3680
Bitness	64 Bit

Host Behavior

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

Process #70: w32tm.exe

ID	70
File Name	c:\windows\system32\w32tm.exe
Command Line	w32tm /stripchart /computer:localhost /period:5 /dataonly /samples:2
Initial Working Directory	C:\comproviderRuntimecommon\
Monitor Start Time	Start Time: 175832, Reason: Child Process
Unmonitor End Time	End Time: 183791, Reason: Terminated
Monitor duration	7.96s
Return Code	0
PID	2712
Parent PID	2672
Bitness	64 Bit

Process #73: taskhost.exe

ID	73
File Name	c:\program files\reference assemblies\taskhost.exe
Command Line	"C:\Program Files\Reference Assemblies\taskhost.exe"
Initial Working Directory	C:\comproviderRuntimecommon\
Monitor Start Time	Start Time: 181975, Reason: Child Process
Unmonitor End Time	End Time: 188815, Reason: Terminated
Monitor duration	6.84s
Return Code	1073807364
PID	3440
Parent PID	2672
Bitness	64 Bit

Host Behavior

Type	Count
Registry	4
-	2
File	6

Process #76: taskeng.exe

ID	76
File Name	c:\windows\system32\taskeng.exe
Command Line	taskeng.exe {6CDE4FA8-8AE9-4DFE-886C-F817993F890F} S-1-5-21-4219442223-4223814209-3835049652-1000:Q9IATRKPRH\kEecfMwgj:Interactive:Highest[1]
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 231282, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 290916, Reason: Terminated by timeout
Monitor duration	59.63s
Return Code	Unknown
PID	1256
Parent PID	2648
Bitness	64 Bit

Process #77: operamail.exe

ID	77
File Name	c:\boot\pl-pl\operamail.exe
Command Line	C:\Boot\pl-PL\operamail.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 232519, Reason: Child Process
Unmonitor End Time	End Time: 290916, Reason: Terminated by timeout
Monitor duration	58.40s
Return Code	Unknown
PID	1344
Parent PID	1256
Bitness	64 Bit

Host Behavior

Type	Count
Registry	1

Process #78: idle.exe

ID	78
File Name	c:\boot\es-es\idle.exe
Command Line	C:\Boot\es-ES\Idle.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 232580, Reason: Child Process
Unmonitor End Time	End Time: 290916, Reason: Terminated by timeout
Monitor duration	58.34s
Return Code	Unknown
PID	1352
Parent PID	1256
Bitness	64 Bit

Host Behavior

Type	Count
Registry	1

Process #80: whatever_only.exe

ID	80
File Name	c:\comproviderruntimecommon\whatever_only.exe
Command Line	C:\comproviderRuntimecommon\whatever_only.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 232659, Reason: Child Process
Unmonitor End Time	End Time: 290916, Reason: Terminated by timeout
Monitor duration	58.26s
Return Code	Unknown
PID	1360
Parent PID	1256
Bitness	64 Bit

Host Behavior

Type	Count
Registry	1

Process #81: spcwin.exe

ID	81
File Name	c:\program files\reference assemblies\microsoft\framework\v3.0\redistlist\spcwin.exe
Command Line	"C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\RedistList\spcwin.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 232746, Reason: Child Process
Unmonitor End Time	End Time: 290916, Reason: Terminated by timeout
Monitor duration	58.17s
Return Code	Unknown
PID	1388
Parent PID	1256
Bitness	64 Bit

Host Behavior

Type	Count
Registry	1

Process #82: taskhost.exe

ID	82
File Name	c:\program files\reference assemblies\taskhost.exe
Command Line	"C:\Program Files\Reference Assemblies\taskhost.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 232782, Reason: Child Process
Unmonitor End Time	End Time: 290916, Reason: Terminated by timeout
Monitor duration	58.13s
Return Code	Unknown
PID	1396
Parent PID	1256
Bitness	64 Bit

Host Behavior

Type	Count
Registry	1

Process #83: yardadultbehind.exe

ID	83
File Name	c:\program files\windows nt\accessories\en-us\yardadultbehind.exe
Command Line	"C:\Program Files\Windows NT\Accessories\en-US\yardadultbehind.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 232835, Reason: Child Process
Unmonitor End Time	End Time: 290916, Reason: Terminated by timeout
Monitor duration	58.08s
Return Code	Unknown
PID	1404
Parent PID	1256
Bitness	64 Bit

Host Behavior

Type	Count
Registry	1

Process #84: flashfxp.exe

ID	84
File Name	c:\users\default user\flashfxp.exe
Command Line	"C:\Users\Default User\flashfxp.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 232904, Reason: Child Process
Unmonitor End Time	End Time: 290916, Reason: Terminated by timeout
Monitor duration	58.01s
Return Code	Unknown
PID	1412
Parent PID	1256
Bitness	64 Bit

Host Behavior

Type	Count
Registry	1

Process #85: fpos.exe

ID	85
File Name	c:\windows\syswow64\winrm\0409\fpos.exe
Command Line	C:\Windows\SysWOW64\winrm\0409\fpos.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 232910, Reason: Child Process
Unmonitor End Time	End Time: 290916, Reason: Terminated by timeout
Monitor duration	58.01s
Return Code	Unknown
PID	1420
Parent PID	1256
Bitness	64 Bit

Host Behavior

Type	Count
Registry	1

Process #86: iexplore.exe

ID	86
File Name	c:\users\default\recent\iexplore.exe
Command Line	C:\Users\Default\Recent\iexplore.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 232937, Reason: Child Process
Unmonitor End Time	End Time: 290916, Reason: Terminated by timeout
Monitor duration	57.98s
Return Code	Unknown
PID	1432
Parent PID	1256
Bitness	64 Bit

Host Behavior

Type	Count
Registry	1

Process #87: explorer.exe

ID	87
File Name	c:\recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\explorer.exe
Command Line	C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\explorer.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 233055, Reason: Child Process
Unmonitor End Time	End Time: 290916, Reason: Terminated by timeout
Monitor duration	57.86s
Return Code	Unknown
PID	1456
Parent PID	1256
Bitness	64 Bit

Host Behavior

Type	Count
Registry	1

Process #88: omnipos.exe

ID	88
File Name	c:\program files (x86)\microsoft onedrive\omnipos.exe
Command Line	"C:\Program Files (x86)\Microsoft OneDrive\omnipos.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 233112, Reason: Child Process
Unmonitor End Time	End Time: 290916, Reason: Terminated by timeout
Monitor duration	57.80s
Return Code	Unknown
PID	1476
Parent PID	1256
Bitness	64 Bit

Host Behavior

Type	Count
Registry	1

Process #89: services.exe

ID	89
File Name	c:\recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\services.exe
Command Line	C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\services.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 233177, Reason: Child Process
Unmonitor End Time	End Time: 290916, Reason: Terminated by timeout
Monitor duration	57.74s
Return Code	Unknown
PID	1484
Parent PID	1256
Bitness	64 Bit

Host Behavior

Type	Count
Registry	1

Process #90: absolutetelnet.exe

ID	90
File Name	c:\recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\absolutetelnet.exe
Command Line	C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\absolutetelnet.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 233277, Reason: Child Process
Unmonitor End Time	End Time: 290916, Reason: Terminated by timeout
Monitor duration	57.64s
Return Code	Unknown
PID	1500
Parent PID	1256
Bitness	64 Bit

Host Behavior

Type	Count
Registry	1

Process #91: spoolsv.exe

ID	91
File Name	c:\users\default\spoolsv.exe
Command Line	C:\Users\Default\spoolsv.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 233317, Reason: Child Process
Unmonitor End Time	End Time: 290916, Reason: Terminated by timeout
Monitor duration	57.60s
Return Code	Unknown
PID	1512
Parent PID	1256
Bitness	64 Bit

Host Behavior

Type	Count
Registry	1

Process #92: but inside save.exe

ID	92
File Name	c:\comproviderruntimecommon\but inside save.exe
Command Line	"C:\comproviderRuntimecommon\but inside save.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 233404, Reason: Child Process
Unmonitor End Time	End Time: 290916, Reason: Terminated by timeout
Monitor duration	57.51s
Return Code	Unknown
PID	1524
Parent PID	1256
Bitness	64 Bit

Host Behavior

Type	Count
Registry	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
05379ea4600304f51cffa8d1ee9e3b2931a69129f6bed14d45a500d966a71fca	C:\Users\kEecfMwgj\Desktop\05379ea4600304f51cffa8d1ee9e3b2931a69129f6bed14d45a500d966a71fca.exe	Sample File	1203.65 KB	application/vnd.microsoft.portable-executable	Access, Read	MALICIOUS
b570e2028088759d02ea13f7646bf7aca78865d55f7fd8e2efaeec45c670e9ff	C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\absolutetelnet.exe, C:\Users\Default User\flashfxp.exe, C:\Recovery\d327d5c2-7147... ...C:\Windows\CSC\v2.0.6\far.exe, C:\Users\Default\Recent\iexplore.exe, C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\services.exe	Dropped File	828.50 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
a91f4373ceebadfc70b3bd0758848918f928c3c76562e3d9d531574796fd9e9c	-	Extracted File	2.82 KB	image/png	-	CLEAN
3e6d9b2b18eee239c9ec1f5fc1a29c02bc1f9b18d59d20cd6a4a84bacadcd710	C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\c5b4cb5e9653cc	Dropped File	447 bytes	text/plain	Access, Create, Write	CLEAN
100f3958bd7e682bf500ed0efade3dec6a741bafda3987ae159ad9932683ae4	C:\Windows\SysWOW64\winrm\0409\2cfdd657e33eed	Dropped File	900 bytes	text/plain	Access, Create	CLEAN
d67ca00c04545c3ac50cbdaf0eb69e9c9a2a75879b4700c165da1d53298fa0d7	C:\Program Files\Reference Assemblies\b75386f1303e64	Dropped File	908 bytes	text/plain	Access, Create, Write	CLEAN
ea5e14d8ddabbab9797ca1d20e0ad93ced8f2c2507834a704d6ae9b1d592267b	C:\comproviderRuntimecommon\c34a7c10ac282e	Dropped File	322 bytes	text/plain	Access, Create, Write	CLEAN
53f23b0c58e94f8b4dc161bd51c8cbddea365e1cd183a846d07ac366b0de59d7	C:\Boot\pl-PL\172e128c88b792	Dropped File	382 bytes	text/plain	Access, Create, Write	CLEAN
d1f53a003519e193da97f0b2114dab9ec90283d8058fb5b8a9a5bed86f159593	-	Extracted File	5.27 KB	image/png	-	CLEAN
09c3e02a4caad39e7c91f0ba1cc93c8c727d23b306da9129cca1d0955880c33e	C:\comproviderRuntimecommon\DLLiR59GMmL352HHbgfc.bat, DLLiR59GMmL352HHbgfc.bat, \\?\C:\comproviderRuntimecommon\DLLiR59GMmL352HHbgfc.bat	Dropped File	47 bytes	text/plain	Access, Create, Read, Write	CLEAN
60eedcadb8fc106e4ac1028bfc61c649eaec2247dc9c217272f265420afbb7a5	C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\RedistList\dea609c9470f15	Dropped File	478 bytes	text/plain	Access, Create, Write	CLEAN
478547b4f458ac74edd4bb6b634a3b3d75ccbfae4567ec48782911d15d21a304	C:\Users\kEecfMwgj\AppData\Local\Temp\1fgVzmzb1s	Dropped File	25 bytes	text/plain	Access, Create, Delete, Write	CLEAN
a2d04dd6baa82f73d47208295e5352ed4877c1b8ca45afbc624d4f60d04c8a75	C:\Users\kEecfMwgj\AppData\Local\Temp\GYwzkQocQK.bat, C:\Users\kEecfMwgj\AppData\Local\Temp\\GYwzkQocQK.bat	Dropped File	219 bytes	text/x-msdos-batch	Access, Create, Delete, Read, Write	CLEAN
1795bc9fc79dc8f4707197ec13aa0a07572fd226c0f94d5def68ec7c3e17e692	C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\7a0fd90576e088	Dropped File	64 bytes	text/plain	Access, Create, Write	CLEAN
8e68e8c091974947b89d092faee94cbd7e15f7ff1dc331b181287a036575a667	C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\9e3bd0c464004d	Dropped File	731 bytes	text/plain	Access, Create, Write	CLEAN
27d3a1a2da49dc535cc10806abaae9dfa49e4f5f44a40540ead50e065b99ca68	-	Extracted File	5.42 KB	image/png	-	CLEAN
bd034e99db8f96b343f84cee052fcf96394f2fb2ef77f468f2c82b80af97fee2	C:\Boot\es-ES\6ccacd8608530f	Dropped File	691 bytes	text/plain	Access, Create, Write	CLEAN
321b7f25ff2c1757c483153a8244e40e550fa09b1a10bed6acd8ad59053a6348	C:\Program Files (x86)\Microsoft OneDrive\9a9ef8f6a80f81	Dropped File	386 bytes	text/plain	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
586e9359009845126614ca003f3862e4f72f9994b91e86a521aa1d425c37db89	-	Dropped File	948 bytes	text/plain	-	CLEAN
4b8e865b614cb8abf63cd9c71866454c2c03da9c7ca21ce2c7ac7b149105bb44	C:\comproviderRuntimecommon\e76e23195dba9d	Dropped File	988 bytes	text/plain	Access, Create, Write	CLEAN
b7a4ead73182d3ee99a9211111579e48f5ac3a0078a6d33515a558705de4e973	-	Dropped File	132 bytes	text/plain	-	CLEAN
0864baa556adddc451e8ad0acbdfbaf692a7371a5cbb8ef2b2b83aa05c56fb39	C:\comproviderRuntimecommon\et1pu6VAlkUOY7GuC90A.vbe, et1pu6VAlkUOY7GuC90A.vbe, \\?\C:\comproviderRuntimecommon\et1pu6VAlkUOY7GuC90A.vbe	Dropped File	221 bytes	application/octet-stream	Access, Create, Write	CLEAN
9c80f368adba592c1c87ac0e1fecceaf2fce232f14351df983291aa1a595f629	C:\Users\Default\f3b6ecef712a24	Dropped File	943 bytes	text/plain	Access, Create, Write	CLEAN
ec2b285db6f6baebf02c715c81db5a0af407ac21a6be3026faba0d1df0364226	C:\Boot\ru-RU\e76e23195dba9d	Dropped File	257 bytes	text/plain	Access, Create, Write	CLEAN
c402b2e2e0bc9ed750d76511b0c23d464c5c616a9d9ada5e2eeec35a08936522	C:\Program Files\Windows NT\Accessories\en-US\ac6c4644f9bcea	Dropped File	965 bytes	text/plain	Access, Create, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Desktop\05379ea4600304f51cffa8d1ee9e3b2931a69129f6bed14d45a500d966a71fca.exe	Sample File, Accessed File, VM File	Access, Read	MALICIOUS
C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\absolutetelnet.exe	Dropped File, Accessed File	Access, Create, Write	SUSPICIOUS
C:\Users\Default User\flashfxp.exe	Accessed File	Access, Create, Write	SUSPICIOUS
C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\explorer.exe	Dropped File, Accessed File	Access, Create, Write	SUSPICIOUS
C:\Boot\es-ES\ldle.exe	Dropped File, Accessed File	Access, Create, Write	SUSPICIOUS
C:\comproviderRuntimecommon\whatever_only.exe	Dropped File, Accessed File	Access, Create, Write	SUSPICIOUS
C:\Program Files\Reference Assemblies\taskhost.exe	Dropped File, Accessed File	Access, Create, Write	SUSPICIOUS
C:\Program Files (x86)\Microsoft OneDrive\omnipos.exe	Dropped File, Accessed File	Access, Create, Write	SUSPICIOUS
C:\Boot\pl-PL\operamail.exe	Dropped File, Accessed File	Access, Create, Write	SUSPICIOUS
C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\RedistList\spcwin.exe	Dropped File, Accessed File	Access, Create, Write	SUSPICIOUS
C:\Windows\SysWOW64\winrm\0409\fpos.exe	Dropped File, Accessed File	Access, Create, Write	SUSPICIOUS
C:\Program Files\Windows NT\Accessories\en-US\yardadultbehind.exe	Dropped File, Accessed File	Access, Create, Write	SUSPICIOUS
C:\Boot\ru-RU\but inside save.exe	Dropped File, Accessed File	Access, Create, Write	SUSPICIOUS
C:\comproviderRuntimecommon\but inside save.exe	Dropped File, Accessed File	Access, Create, Write	SUSPICIOUS
C:\Users\Default\spoolsv.exe	Dropped File, Accessed File	Access, Create, Write	SUSPICIOUS
C:\Users\Default\Recent\iexplore.exe	Accessed File	Access, Create, Write	SUSPICIOUS
C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\services.exe	Dropped File, Accessed File	Access, Create, Write	SUSPICIOUS
C:\comproviderRuntimecommon\et1pu6VAlkUOY7GuC90A.vbe	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\Users\Default\f3b6ecef712a24	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\Program Files\Windows NT\Accessories\en-US\ac6c4644f9bcea	Dropped File, Accessed File	Access, Create, Write	CLEAN

File Name	Category	Operations	Verdict
"C:\comproviderRuntimecommon\chainsavesref.exe"	Accessed File	Access	CLEAN
C:\Users\Default\Recent\9db6e019d4f04e	Accessed File	Access, Create, Write	CLEAN
C:\Program Files\Reference Assemblies\b75386f1303e64	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\Users\Default User\b064723b75e933	Accessed File	Access, Create, Write	CLEAN
C:\comproviderRuntimecommon\chainsavesref.exe.config	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\WScript.exe	Accessed File	Access	CLEAN
C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\7a0fd90576e088	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\Boot\pl-PL\172e128c88b792	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\c5b4cb5e9653cc	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\Boot\es-ES\6ccacd8608530f	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\Desktop\DXGIDebug.dll	Accessed File	Access	CLEAN
C:\Windows\schemas\EAPMethods\csrss.exe	Accessed File	Access, Create, Write	CLEAN
C:\Windows\system32\schtasks.exe	Accessed File	Access	CLEAN
C:\Windows\CSC\v2.0.6\far.exe	Accessed File	Access, Create, Write	CLEAN
__tmp_rar_sfx_access_check_20445881	Dropped File, Accessed File, Not Extracted	Access, Create, Delete	CLEAN
DLLiR59GMmL352HHbgfc.bat	Accessed File	Access	CLEAN
c:\users\default\appdata\roaming\microsoft\windows\recent\iexplore.exe	Dropped File	-	CLEAN
chainsavesref.exe	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\1fgVzmzb1s	Dropped File, Accessed File	Access, Create, Delete, Write	CLEAN
nul	Accessed File	Access, Create	CLEAN
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\config\machine.config	Accessed File	Access, Read	CLEAN
"C:\comproviderRuntimecommon\DLLiR59GMmL352HHbgfc.bat"	Accessed File	Access	CLEAN
et1pu6VAlkUOY7GuC90A.vbe	Accessed File	Access	CLEAN
C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\RedistList\dea609c9470f15	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\Program Files (x86)\Microsoft OneDrive\9a9ef8f6a80f81	Dropped File, Accessed File	Access, Create, Write	CLEAN
c:\users\default\flashfxp.exe	Dropped File	-	CLEAN
c:\users\default\b064723b75e933	Dropped File	-	CLEAN
chainsavesref.exe	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\comproviderRuntimecommon\DLLiR59GMmL352HHbgfc.bat	Dropped File, Accessed File	Access, Create, Read, Write	CLEAN
C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\9e3bd0c464004d	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\Windows\SysWOW64\winrm\0409\2cfdd657e33eed	Dropped File, Accessed File, Modified File	Access, Create	CLEAN
C:/comproviderRuntimecommon	Accessed File	Access, Create	CLEAN
C:/comproviderRuntimecommon	Accessed File	Access	CLEAN
C:\Boot\ru-RU\e76e23195dba9d	Dropped File, Accessed File	Access, Create, Write	CLEAN

File Name	Category	Operations	Verdict
c:\users\default\appdata\roaming\microsoft\windows\recent\9db6e019d4f04e	Dropped File	-	CLEAN
C:\comproviderRuntimecommon\c34a7c10ac282e	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\GYwzkQocQK.bat	Dropped File, Accessed File	Access, Create, Delete, Read, Write	CLEAN
C:\comproviderRuntimecommon\e76e23195dba9d	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\comproviderRuntimecommon\0d92ca00b4a11c	Accessed File	Access	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
Local\a662db5313495af89c12e9daf05e137fcad6fcec	access	chainsavesref.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\AllowDangerousUnicodeDecompositions	read, access	chainsavesref.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\DisplayLogo	read, access	wscript.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SchSendAuxRecord	access	chainsavesref.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseHttpPipeliningAndBufferPooling	read, access	chainsavesref.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\WMIDisableCOMSecurity	read, access	chainsavesref.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\Enabled	read, access	wscript.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\LogSecuritySuccesses	read, access	wscript.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	but inside save.exe, yardadultbehind.exe, whatever_only.exe, spcwin.exe, iexplore.exe, services.exe, flashfxp.exe, spoolsv.exe, fpos.exe, explorer.exe, taskhost.exe, omnipos.exe, idle.exe, absolutetelnet.exe, chainsavesref.exe, operamail.exe	CLEAN
HKEY_CLASSES_ROOT\.vbe	read, access	wscript.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\LogSecuritySuccesses	read, access	wscript.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\RequireCertificateEKUs	read, access	chainsavesref.exe	CLEAN
HKEY_CURRENT_USER\Software\caa6004a855dece65e49fdcfb42785d36f42888b	create, access	chainsavesref.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Uri.AllowAllUriEncodingExpansion	access	chainsavesref.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Uri.AllowDangerousUnicodeDecompositions	access	chainsavesref.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SystemDefaultTlsVersions	read, access	chainsavesref.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseSafeSynchronousClose	read, access	chainsavesref.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.UseHttpPipeliningAndBufferPooling	access	chainsavesref.exe	CLEAN
HKEY_CURRENT_USER\Software\caa6004a855dece65e49fdcfb42785d36f42888b\437b07143d558f8f987cd92e573298e152164cb4	write, read, access	chainsavesref.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	access	chainsavesref.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings	create, access	wscript.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseStrictRfcInterimResponseHandling	read, access	chainsavesref.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	read, access	chainsavesref.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Uri.UseStrictIPv6AddressParsing	access	chainsavesref.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchSendAuxRecord	read, access	chainsavesref.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\Enabled	read, access	wscript.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseStrictIPv6AddressParsing	read, access	chainsavesref.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\Timeout	read, access	wscript.exe	CLEAN
HKEY_CLASSES_ROOT\VBEFile\ScriptEngine	read, access	wscript.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\TrustPolicy	read, access	wscript.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\Full\Release	read, access	chainsavesref.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	chainsavesref.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\Full	access	chainsavesref.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings	create, access	wscript.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName	read, access	chainsavesref.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\UseWINSAFER	read, access	wscript.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.RequireCertificateEKUs	access	chainsavesref.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	read, access	chainsavesref.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\AllowAllUriEncodingExpansion	read, access	chainsavesref.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\Timeout	read, access	wscript.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	chainsavesref.exe, taskhost.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\DisplayLogo	read, access	wscript.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\TrustPolicy	read, access	wscript.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	read, access	chainsavesref.exe, taskhost.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\UseWINSAFER	read, access	wscript.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\IgnoreUserSettings	read, access	wscript.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.UseStrictRfcInterimResponseHandling	access	chainsavesref.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.UseSafeSynchronousClose	access	chainsavesref.exe	CLEAN

Process

Process Name	Commandline	Verdict
05379ea4600304f51cffa8d1ee9e3b2931a69129f6bed14d45a500d966a71fca.exe	"C:\Users\kEecfMwgj\Desktop\05379ea4600304f51cffa8d1ee9e3b2931a69129f6bed14d45a500d966a71fca.exe"	MALICIOUS
chainsavesref.exe	"C:\comproviderRuntimecommon\chainsavesref.exe"	MALICIOUS
schtasks.exe	schtasks.exe /create /tn "whatever_onlyw" /sc MINUTE /mo 11 /tr "'C:\comproviderRuntimecommon\whatever_only.exe'" /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "whatever_only" /sc ONLOGON /tr "'C:\comproviderRuntimecommon\whatever_only.exe'" /rl HIGHEST /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "spcwins" /sc MINUTE /mo 8 /tr "'C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\RedistList\spcwin.exe'" /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "spcwin" /sc ONLOGON /tr "'C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\RedistList\spcwin.exe'" /rl HIGHEST /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "but inside saveb" /sc MINUTE /mo 8 /tr "'C:\Boot\ru-RU\but inside save.exe'" /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "IdleI" /sc MINUTE /mo 6 /tr "'C:\Boot\es-ES\Idle.exe'" /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "Idle" /sc ONLOGON /tr "'C:\Boot\es-ES\Idle.exe'" /rl HIGHEST /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "but inside save" /sc ONLOGON /tr "'C:\Boot\ru-RU\but inside save.exe'" /rl HIGHEST /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "operamailo" /sc MINUTE /mo 10 /tr "'C:\Boot\pl-PL\operamail.exe'" /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "operamail" /sc ONLOGON /tr "'C:\Boot\pl-PL\operamail.exe'" /rl HIGHEST /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "explorere" /sc MINUTE /mo 13 /tr "'C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\explorer.exe'" /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "explorer" /sc ONLOGON /tr "'C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\explorer.exe'" /rl HIGHEST /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "omniposo" /sc MINUTE /mo 14 /tr "'C:\Program Files (x86)\Microsoft OneDrive\omnipos.exe'" /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "omnipos" /sc ONLOGON /tr "'C:\Program Files (x86)\Microsoft OneDrive\omnipos.exe'" /rl HIGHEST /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "taskhostt" /sc MINUTE /mo 6 /tr "'C:\Program Files\Reference Assemblies\taskhost.exe'" /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "taskhost" /sc ONLOGON /tr "'C:\Program Files\Reference Assemblies\taskhost.exe'" /rl HIGHEST /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "absolutetelneta" /sc MINUTE /mo 6 /tr "'C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\absolutetelnet.exe'" /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "absolutetelnet" /sc ONLOGON /tr "'C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\absolutetelnet.exe'" /rl HIGHEST /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "servicess" /sc MINUTE /mo 5 /tr "'C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\services.exe'" /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "services" /sc ONLOGON /tr "'C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\services.exe'" /rl HIGHEST /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "iexplorei" /sc MINUTE /mo 10 /tr "'C:\Users\Default\Recent\iexplore.exe'" /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "iexplore" /sc ONLOGON /tr "'C:\Users\Default\Recent\iexplore.exe'" /rl HIGHEST /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "fposf" /sc MINUTE /mo 14 /tr "'C:\Windows\SysWOW64\winrm\0409\fpos.exe'" /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "fpos" /sc ONLOGON /tr "'C:\Windows\SysWOW64\winrm\0409\fpos.exe'" /rl HIGHEST /f	SUSPICIOUS

Process Name	Commandline	Verdict
schtasks.exe	schtasks.exe /create /tn "but inside saveb" /sc MINUTE /mo 6 /tr "'C:\comproviderRuntimecommon\but inside save.exe'" /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "but inside save" /sc ONLOGON /tr "'C:\comproviderRuntimecommon\but inside save.exe'" /rl HIGHEST /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "spoolsvs" /sc MINUTE /mo 13 /tr "'C:\Users\Default\spoolsv.exe'" /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "spoolsv" /sc ONLOGON /tr "'C:\Users\Default\spoolsv.exe'" /rl HIGHEST /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "yardadultbehindy" /sc MINUTE /mo 8 /tr "'C:\Program Files\Windows NT\Accessories\en-US\yardadultbehind.exe'" /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "yardadultbehind" /sc ONLOGON /tr "'C:\Program Files\Windows NT\Accessories\en-US\yardadultbehind.exe'" /rl HIGHEST /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "flashfxpf" /sc MINUTE /mo 9 /tr "'C:\Users\Default User\flashfxp.exe'" /f	SUSPICIOUS
schtasks.exe	schtasks.exe /create /tn "flashfxp" /sc ONLOGON /tr "'C:\Users\Default User\flashfxp.exe'" /rl HIGHEST /f	SUSPICIOUS
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	SUSPICIOUS
but inside save.exe	"C:\comproviderRuntimecommon\but inside save.exe"	CLEAN
wscript.exe	"C:\Windows\System32\WScript.exe" "C:\comproviderRuntimecommon\et1pu6VAlkUOY7GuC90A.vbe"	CLEAN
cmd.exe	C:\Windows\system32\cmd.exe /c ""C:\comproviderRuntimecommon\DLLiR59GMmL352HHbgfc.bat" "	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
schtasks.exe	schtasks.exe /create /tn "whatever_onlyw" /sc MINUTE /mo 5 /tr "'C:\comproviderRuntimecommon\whatever_only.exe'" /rl HIGHEST /f	CLEAN
schtasks.exe	schtasks.exe /create /tn "spcwins" /sc MINUTE /mo 5 /tr "'C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\RedistList\spcwin.exe'" /rl HIGHEST /f	CLEAN
schtasks.exe	schtasks.exe /create /tn "but inside saveb" /sc MINUTE /mo 12 /tr "'C:\Boot\ru-RU\but inside save.exe'" /rl HIGHEST /f	CLEAN
schtasks.exe	schtasks.exe /create /tn "Idlel" /sc MINUTE /mo 9 /tr "'C:\Boot\es-ES\Idle.exe'" /rl HIGHEST /f	CLEAN
schtasks.exe	schtasks.exe /create /tn "operamailo" /sc MINUTE /mo 13 /tr "'C:\Boot\pl-PL\operamail.exe'" /rl HIGHEST /f	CLEAN
schtasks.exe	schtasks.exe /create /tn "explorere" /sc MINUTE /mo 5 /tr "'C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\explorer.exe'" /rl HIGHEST /f	CLEAN
schtasks.exe	schtasks.exe /create /tn "omniposo" /sc MINUTE /mo 12 /tr "'C:\Program Files (x86)\Microsoft OneDrive\omnipos.exe'" /rl HIGHEST /f	CLEAN
schtasks.exe	schtasks.exe /create /tn "taskhostt" /sc MINUTE /mo 6 /tr "'C:\Program Files\Reference Assemblies\taskhost.exe'" /rl HIGHEST /f	CLEAN
schtasks.exe	schtasks.exe /create /tn "absolutetelneta" /sc MINUTE /mo 12 /tr "'C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\absolutetelnet.exe'" /rl HIGHEST /f	CLEAN
schtasks.exe	schtasks.exe /create /tn "servicess" /sc MINUTE /mo 11 /tr "'C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\services.exe'" /rl HIGHEST /f	CLEAN
schtasks.exe	schtasks.exe /create /tn "iexplorei" /sc MINUTE /mo 9 /tr "'C:\Users\Default\Recent\iexplore.exe'" /rl HIGHEST /f	CLEAN
schtasks.exe	schtasks.exe /create /tn "fposf" /sc MINUTE /mo 11 /tr "'C:\Windows\SysWOW64\winrm\0409\fpos.exe'" /rl HIGHEST /f	CLEAN
schtasks.exe	schtasks.exe /create /tn "but inside saveb" /sc MINUTE /mo 6 /tr "'C:\comproviderRuntimecommon\but inside save.exe'" /rl HIGHEST /f	CLEAN
schtasks.exe	schtasks.exe /create /tn "spoolsvs" /sc MINUTE /mo 5 /tr "'C:\Users\Default\spoolsv.exe'" /rl HIGHEST /f	CLEAN
schtasks.exe	schtasks.exe /create /tn "yardadultbehindy" /sc MINUTE /mo 10 /tr "'C:\Program Files\Windows NT\Accessories\en-US\yardadultbehind.exe'" /rl HIGHEST /f	CLEAN
schtasks.exe	schtasks.exe /create /tn "flashfxpf" /sc MINUTE /mo 13 /tr "'C:\Users\Default User\flashfxp.exe'" /rl HIGHEST /f	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /C "C:\Users\kEecfMwgj\AppData\Local\Temp\GYwzkQocQK.bat"	CLEAN

Process Name	Commandline	Verdict
w32tm.exe	w32tm /stripchart /computer:localhost /period:5 /dataonly /samples:2	CLEAN
taskhost.exe	"C:\Program Files\Reference Assemblies\taskhost.exe"	CLEAN
explorer.exe	C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\explorer.exe	CLEAN
taskeng.exe	taskeng.exe {6CDE4FA8-8AE9-4DFE-886C-F817993F890F} S-1-5-21-4219442223-4223814209-3835049652-1000:Q9IATRKPRH\kEecfMwgj:Interactive:Highest[1]	CLEAN
operamail.exe	C:\Boot\pl-PL\operamail.exe	CLEAN
idle.exe	C:\Boot\es-ES\Idle.exe	CLEAN
whatever_only.exe	C:\comproviderRuntimecommon\whatever_only.exe	CLEAN
spcwin.exe	"C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\RedistList\spcwin.exe"	CLEAN
taskhost.exe	"C:\Program Files\Reference Assemblies\taskhost.exe"	CLEAN
yardadultbehind.exe	"C:\Program Files\Windows NT\Accessories\en-US\yardadultbehind.exe"	CLEAN
flashfxp.exe	"C:\Users\Default User\flashfxp.exe"	CLEAN
fpos.exe	C:\Windows\SysWOW64\winrm\0409\fpos.exe	CLEAN
iexplore.exe	C:\Users\Default\Recent\iexplore.exe	CLEAN
omnipos.exe	"C:\Program Files (x86)\Microsoft OneDrive\omnipos.exe"	CLEAN
services.exe	C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\services.exe	CLEAN
absolutetelnet.exe	C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\absolutetelnet.exe	CLEAN
spoolsv.exe	C:\Users\Default\spoolsv.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