151 – Malicious Service

Team Information

Team Name: DogeCoin

Team Member: Dongbin Oh, Donghyun Kim, Donghyun Kim, Yeongwoong Kim

Email Address: dfc-dogecoin@naver.com

Instructions

Description It appears that an attacker has installed a malicious service on the system. Investigate artifacts related to the malicious service.

Target	Hash (MD5)
Windows.7z	C5B3E6D65D8B9F7FAAF8FB90B6227A57

Questions

1. What is the ServiceName and BinaryPathName of the malicious service installed by the attacker? (100 points)
2. When did the attacker install the malicious service? (50 points)

Teams must:

- Develop and document the step-by-step approach used to solve this problem to allow another examiner to replicate team actions and results.
- Specify all tools used in deriving the conclusion(s).

Tools used:

Name:	REGA	Publisher:	DFRC
Version:	1.5.3.0		
URL:	http://forensic.korea.ac.kr/tools.html		

Name:	Registry Explorer	Publisher:	Eric Zimmerman
Version:	1.6.0.0		
URL:	https://ericzimmerman.github.io/#!index.md		

Name:	RegRipper	Publisher:	keydet89
Version:	3.0		
URL:	https://github.com/keydet89/RegRipper3.0		

Name:	RegSize	Publisher:	Bridgey
Version:	-		
URL:	https://github.com/bridgeythegeek/regsize		

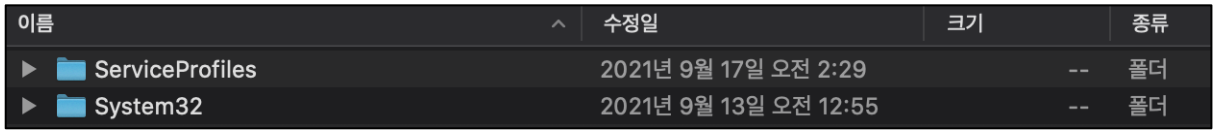
Step-by-step methodology:

1. What is the ServiceName and BinaryPathName of the malicious service installed by the attacker? (100 points)

주어진 시나리오를 확인하게 되면, 공격자가 악성 서비스를 시스템에 설치한 것으로 추정된다. 공격자는 악의적인 페이로드나 악성코드의 지속성 (Persistence)을 유지하기 위해 다양한 기법을 사용하는데 그 중 하나인 Windows Service를 이용할 수 있다. Windows Service에 특정 페이로드/바이너리 경로를 등록하게 되면 Windows 부팅 시점부터 백그라운드에서 실행됨으로 악성 행위를 지속할 수 있게 된다.

해당 서비스를 등록/관리하는 방법은 sc.exe, Registry, PowerShell Command 등으로 다양하게 존재하며, 탐지 분석을 어렵게 하기 위해 기존의 운영체제에 존재하는 서비스를 수정하거나 정상적인 소프트웨어의 이름으로 위장하는 경우가 많다.[1]

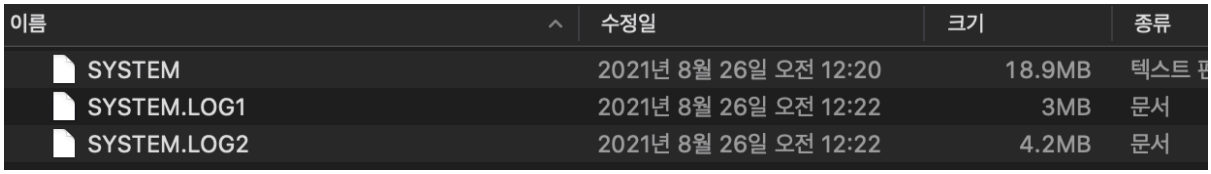
이러한 사실에 기반하여 공격자가 설치한 것으로 추정되는 서비스를 추적한 결과는 아래와 같다.



[그림 1] 윈도우 레지스트리 파일

압축 파일 내부를 확인한 결과, "SYSTEM" 레지스트리 하이브와 "NTUSER" 레지스트리 하이브 파일이 저장되어 있음을 확인할 수 있었다.

SYSTEM 하이브 분석



[그림 2] 시스템 하이브 파일

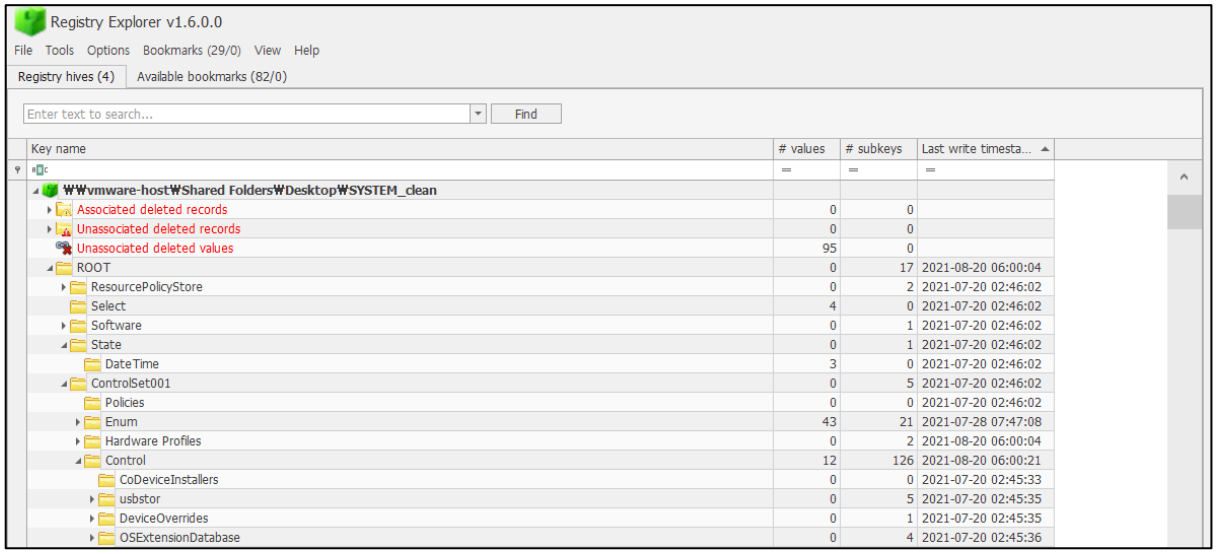
먼저 SYSTEM 하이브를 먼저 분석하였다. 폴더 내부에는 해당 하이브 파일과 하이브의 트랜잭션이 포함된 로그 파일을 같이 확인할 수 있다.

레지스트리 트랜잭션 로그 파일[2]은 데이터가 레지스트리 하이브에 기록되기 전에 임시로 데이터를 저장하는 저널 역할을 하고 있다. 이에 레지스트리 하이브에는 존재하지 않고 로그에만 데이터가 존재할 수 있으므로 이 둘을 취합해서 분석해야한다.

[1] https://attack.mitre.org/techniques/T1543/003/

[2] https://www.fireeye.com/blog/threat-research/2019/01/digging-up-the-past-windows-registry-forensics-revisited.html

Registry Explorer는 하이브 파일과, 트랜잭션 로그 파일을 취합해서 분석할 수 있는 기능을 지원한다. 이에 해당 파일들을 대상으로 확인한 결과, 아래의 키들을 확인할 수 있었다.



[그림 3] Registry Explorer로 확인한 SYSTEM 하이브

특히 해당 SYSTEM 하이브에서 시스템에 등록된 Windows Service Key, Value 데이터를 확인할 수 있는데 그 경로는 다음과 같다.

[표 1] Windows Service 레지스트리 경로

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

해당 경로의 Key, Value를 통해 Windows에 등록된 서비스를 파악할 수 있지만, 대부분의 악성코드들이 교묘하게 정상적인 서비스와 유사한 이름의 서비스를 가지는 등 다양한 방법으로 위장하므로 여러 관점에서 레지스트리 하이브를 분석하였다.

Default Service Diff 관점

첫번째로는 정상적인 시스템에 등록된 서비스와 주어진 레지스트리 하이브에 기록된 서비스의 서비스 명과 주요한 설정 값들을 비교하였다. (ImagePath, DisplayName 등)

Diffing하여 기본 서비스 외에 새롭게 등록된 서비스이거나 기존에 설정된 서비스와 주요 설정 값이 다른 서비스를 나열한 결과는 아래와 같다.

[표 2] 기본 서비스 외에 새롭게 등록된 서비스 및 설정 값이 다른 서비스

서비스 명	실행 경로
AdobeARMservice	"C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe"

AESMService	"C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe"
AirModeBtn	\SystemRoot\System32\drivers\AirModeBtn.sys
aspnet_staters	-
BthHFAud	\SystemRoot\System32\drivers\BthHfAud.sys
ClickToRunSvc	"C:\Program Files\Common Files\ Microsoft Shared\ClickToRun\OfficeClickToRun.exe" /service
Clr_optimization_v2.0.50727_32	-
Clr_optimization_v2.0.50727_64	-
CnxtHdAudService	\SystemRoot\system32\drivers\CHDRT64.sys
cplspconc	%SystemRoot%\System32\DriverStore\FileRepository\ iigd_dch.inf_amd64_18b9147b1f53b9f9\IntelCpHDCPSvc.exe
dpdf_acpi	\SystemRoot\System32\DriverStore\FileRepository\ dptf_acpi.inf_amd64_5989fd2721678bab\dptf_acpi.sys
dptf_cpu	\SystemRoot\System32\DriverStore\FileRepository\ dptf_cpu.inf_amd64_4a3ae74cfa6c37d6\dptf_cpu.sys
DtsApp4Service	%SystemRoot%\System32\DTS\PC\APO4x\DtsApo4Service.exe
FileSyncHelper	"C:\Program Files (x86)\ Microsoft OneDrive\21.150.0725.0001\FileSyncHelper.exe"
FontCache3.0.0.0	%systemroot%\Microsoft.Net\Framework64\v3.0\WPF\ PresentationFontCache.exe
HAM501	\SystemRoot\System32\Drivers\HAM501.sys
HAM501C	\SystemRoot\System32\Drivers\HAM501C.sys
hcmon	\SystemRoot\system32\DRIVERS\hcmon.sys
iaLPSS2_SPI	\SystemRoot\System32\DriverStore\FileRepository\ ialpss2_spi_icl.inf_amd64_f47170929a096263\iaLPSS2_SPI.sys
iaLPSS2_UART2	\SystemRoot\System32\DriverStore\FileRepository\ ialpss2_uart2_icl.inf_amd64_2fd93d380196ad59\iaLPSS2_UART2.sys
ibtusb	\SystemRoot\System32\DriverStore\FileRepository\ ibtusb.inf_amd64_1699b3a6d53419b4\ibtusb.sys
igccservice	%SystemRoot%\System32\DriverStore\FileRepository\ igcc_dch.inf_amd64_20131b732500f04d\OneApp.IGCC.WinService.exe
igfxCUIService2.0.0.0	%SystemRoot%\System32\DriverStore\FileRepository\ cui_dch.inf_amd64_165e58a7838ac336\igfxCUIServiceN.exe
igfxn	\SystemRoot\System32\DriverStore\FileRepository\ iigd_dch.inf_amd64_18b9147b1f53b9f9\igdkmdn64.sys
IntcDAud	\SystemRoot\System32\DriverStore\FileRepository\ intcdaud.inf_amd64_903eba7571a52ae1\IntcDAud.sys
Intel(R) Capability Licensing Service TCP IP Interface	%SystemRoot%\System32\DriverStore\FileRepository\ iclsclient.inf_amd64_75ffca5eec865b4b\lib\SocketHeciServer.exe

Intel(R) TPM Provisioning Service	%SystemRoot%\System32\DriverStore\FileRepository\ iclsclient.inf_amd64_75ffca5eec865b4b\lib\TPMProvisioningService.exe
MSDTC Bridge 3.0.0.0	-
Netaapi	\SystemRoot\System32\drivers\netaapl64.sys
NetAdapterCx	system32\drivers\NetAdapterCx.sys
Netwtw08	\SystemRoot\System32\drivers\Netwtw08.sys
nhi	\SystemRoot\System32\drivers\TbtBusDrv.sys
OneDrive Updater Service	"C:\Program Files (x86)\ Microsoft OneDrive\21.150.0725.0001\OneDriveUpdaterService.exe"
PlatformMgrService	%SystemRoot%\System32\DriverStore\FileRepository\ platmgrsvc.inf_amd64_8f224c030b55d621\PlatformMgrService.exe
PlatMgr	\SystemRoot\System32\drivers\PlatMgr.sys
rtux62w10	\SystemRoot\System32\drivers\rtux64w10.sys
SAService	C:\Program Files\WindowsApps\ 22094synapticsincorporate.smartaudio2_1.1.51.0_x86__qt57b6kdvhcfw\ SAII\SASrv.exe
ServiceModelEndpoint 3.0.0.0	-
SerivceModelOperation 3.0.0.0	-
ServiceModelService 3.0.0.0	-
SMSvcHost 3.0.0.0	-
ss_conn_launcher_service	%SystemRoot%\System32\Samsung\EasySetup\ss_conn_launcher.exe
ss_conn_usb_driver2	\SystemRoot\System32\Drivers\ss_conn_usb_driver2.sys
ssudmdm	\SystemRoot\system32\DRIVERS\ssudmdm.sys
ssudqcfilter	\SystemRoot\System32\drivers\ssudqcfilter.sys
SynaAssist	"%SystemRoot%\System32\SynaAssist64.exe"
TbtHostControllerService	%SystemRoot%\ThunderboltService.exe
VMAuthdService	"C:\Program Files (x86)\VMware\VMware Player\vmware-authd.exe"
vwifimp	\SystemRoot\System32\drivers\vwifimp.sys
WDC_SAM	\SystemRoot\System32\drivers\wdcsam64.sys
xnotepep	System32\drivers\xnotepep.sys

대부분의 서비스들이 Drive와 관련되거나 사용자 어플리케이션과 관련된 정상 서비스임을 확인할 수 있었다. 그러나 “aspnet_staters”라는 특이 서비스 명과 Value를 가지는 특이 서비스를 확인할 수 있었다.

Hidden Key/Value 탐색

세번째로 확인한 요소는 숨겨지거나 인코딩 된 Key/Value를 식별하는 것이다. 일부 악성코드 및 파일리스 멀웨어의 경우 서비스 등록과 같은 Persistent 유지 시 Reigstry를 사용하는데 이때 사용자에게 노출되지 않도록 Key/Value를 숨기거나 인코딩하여 특수한 형태로 저장한다는 특징을 가진다.[3]

해당 내역을 확인하기 위해 RegSize라는 도구를 일부 수정 (REG_SZ 검색, Value Data를 실제보다 2배 출력되는 것을 수정) 하여 숨겨지거나 인코딩 된 것으로 추정되는Key/Value까지 모두 표시토록 하였다.

[표 3] 수정된 RegSize 수행 결과

```
✗ dhyun@gimdonghyeon-ui-MacBookPro  ~/regsize    master ± open .
 dhyun@gimdonghyeon-ui-MacBookPro  ~/regsize    master ± python2 regsize.py
target SYSTEM
[SYSTEM]
2785    3.52077
ControlSet001\Services\Eaphost\Methods\311\21\WLANProfileCreationUXAuth\13\WLANP
rofileTemplate
2552    3.55591
ControlSet001\Services\RasMan\PPP\EAP\25\WLANProfileCreationUXAuth\13\WLANProfil
eTemplate
2552    3.55591
ControlSet001\Services\RasMan\PPP\EAP\25\WLANProfileCreationUXAuth\26\WLANProfil
eTemplate
2247    3.53538
ControlSet001\Services\Eaphost\Methods\311\21\WLANProfileCreationUXAuth\26\WLANP
rofileTemplate
1864    3.52292 ControlSet001\Services\RasMan\PPP\EAP\13\WLANProfileTemplate
1598    3.54833
ControlSet001\Services\Eaphost\Methods\311\21\WLANProfileCreationUXAuth\1028\WLA
NProfileTemplate
1493    3.54712
ControlSet001\Services\Eaphost\Methods\311\21\WLANProfileCreationUXAuth\1027\WLA
NProfileTemplate
1491    3.54594
ControlSet001\Services\Eaphost\Methods\311\21\WLANProfileCreationUXAuth\1026\WLA
NProfileTemplate
1490    3.54489
ControlSet001\Services\Eaphost\Methods\311\21\WLANProfileCreationUXAuth\1025\WLA
NProfileTemplate
1429    3.56774
ControlSet001\Services\Eaphost\Methods\311\50\WLANProfileTemplate
1361    3.56374
ControlSet001\Services\Eaphost\Methods\311\18\WLANProfileTemplate
1313    3.56514
ControlSet001\Services\Eaphost\Methods\311\23\WLANProfileTemplate
```

[3] https://www.slideshare.net/F-INSIGHT/160820-fitalk-fileless-malware-forensics

```
916     3.64893 ControlSet001\Services\mpssvc\Parameters\AppCs\AppCs\S-1-15-2-
2551677095-2355568638-4209445997-2436930744-3692183382-387691378-1866284433S-1-
5-21-2949964769-1086094253-4195774485-1001
907     3.73676
ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices
\AppIso\FirewallRules\{96608C96-AA5F-40C4-A9CA-65D921FED5CD}
906     3.73686
ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices
\AppIso\FirewallRules\{026E8023-D790-4E77-B630-BA681204ECAA}
895     3.73891
ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices
\AppIso\FirewallRules\{D7FED75E-3CE8-40C3-ACCB-3120097E3BAB}
894     3.73997
ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices
\AppIso\FirewallRules\{33D8952B-682D-4531-B127-3ECC76D849AC}
894     3.73893
ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices
\AppIso\FirewallRules\{63016D1C-F12D-43DA-BACE-90796C4BD984}
894     3.73950
ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices
\AppIso\FirewallRules\{910CF1DB-B084-4902-8E5A-AEA5BD5FD3E0}
893     3.73992
ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices
\AppIso\FirewallRules\{905F4786-16D2-4C00-980E-C21109F69F7D}
120     3.10212
DriverDatabase\DriverPackages\microsoft_bluetooth_hfp_ag.inf_amd64_d2736f1d9bc81
5e1\Configurations\BthHfEnum_Ag_Install\Driver\Security
120     3.10212
DriverDatabase\DriverPackages\microsoft_bluetooth_hfp_hf.inf_amd64_0c00f8f3a465c
9a4\Configurations\BthHfEnum_Hf_Install\Driver\Security
113     3.39547 DriverDatabase\DriverPackages\icelakepch-
lpsystem.inf_amd64_6571fea8dac56998\Strings\pci\ven_8086&dev_3481desc
112     3.36338 DriverDatabase\DriverPackages\icelakepch-
lpsystem.inf_amd64_6571fea8dac56998\Strings\pci\ven_8086&dev_3482desc
101     3.34146
DriverDatabase\DriverPackages\tbthostcontrollerextension.inf_amd64_d1a1c65d4f6d4
d6e\OemPath
83      3.41066
DriverDatabase\DriverPackages\xnotepep.inf_amd64_6ea3529718e30820\OemPath
83      3.45415 HardwareConfig\{e4da51c4-74d8-145b-8725-
6f2fdc7e72d8}\ComputerIds\{8cd8be08-fb49-5f32-8650-24f09a0c811b}
74      3.45742 HardwareConfig\{e4da51c4-74d8-145b-8725-
6f2fdc7e72d8}\ComputerIds\{5cc0cc70-f829-5379-8f9b-a61916aea542}
62      3.12263
DriverDatabase\DriverPackages\vmci.inf_amd64_5e38a278d114b813\OemPath
62      3.38845 Setup\FirstBoot\OnError\0
56      3.14352
DriverDatabase\DriverPackages\vmusb.inf_amd64_c603306f7f2b335a\OemPath
21      2.43108 WaaS\WaaSMedic\State\TimeSyncPlugin\LastDetectionRunTime


✗ dhyun@gimdonghyeon-ui-MacBookPro  ~/regsize    master ±  python2
regsize.py target NTUSER.DAT
```

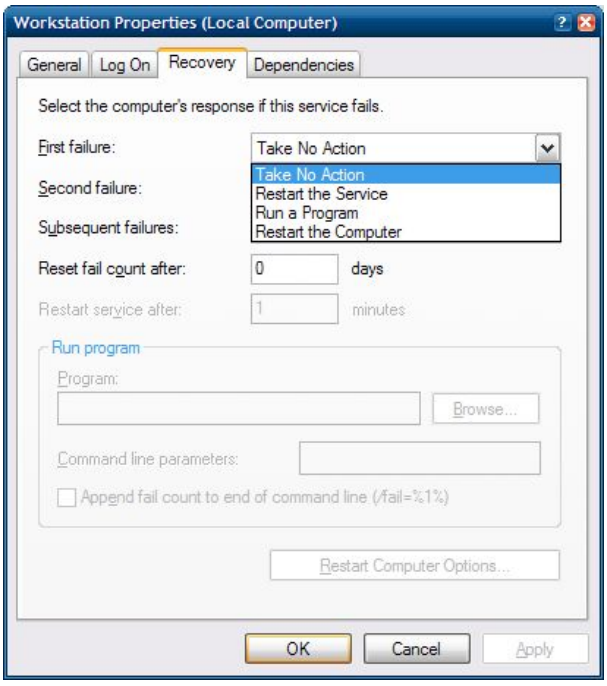
```
[NTUSER.DAT]
1404     3.82696 SOFTWARE\Microsoft\AuthCookies\Live\Default\DIDC\Data
145      3.03216 Control Panel\PowerCfg\PowerPolicies\3\Description
119      3.04452 SOFTWARE\Microsoft\AuthCookies\Live\Default\DIDC\P3P
95       2.94522 Control Panel\PowerCfg\PowerPolicies\0\Description
86       3.01679 Control Panel\PowerCfg\PowerPolicies\1\Description
76       3.30739 SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell
Folders\Startup
73       2.98146 Control Panel\PowerCfg\PowerPolicies\4\Description
68       3.32837 SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell
Folders\Programs
66       3.38582 SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell
Folders\NetHood
66       3.34533 SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell
Folders\PrintHood
65       3.08405 SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell
Folders\!Do not use this registry key
60       3.19965
SOFTWARE\Google\Chrome\NativeMessagingHosts\com.microsoft.browsercore\(default)
59       3.33783 SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell
Folders\Start Menu
59       3.05232
SOFTWARE\Microsoft\Windows\CurrentVersion\Themes\LastHighContrastTheme
58       2.90138 Control Panel\PowerCfg\PowerPolicies\2\Description
58       3.33027 SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell
Folders\Cookies
58       3.33677 SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell
Folders\Templates
57       3.31318 SOFTWARE\Microsoft\Windows\CurrentVersion\Lock
Screen\LockAppAumId
56       3.34669 SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell
Folders\Cache
39       1.40236
SOFTWARE\Microsoft\Wisp\Pen\SysEventParameters\FlickCommands\upRight
 dhyun@gimdonghyeon-ui-MacBookPro  ~/regsize    master ± python2 regsize.py
target NTUSER.DAT
[NTUSER.DAT]
1396     3.82472 SOFTWARE\Microsoft\AuthCookies\Live\Default\DIDC\Data
145      3.03216 Control Panel\PowerCfg\PowerPolicies\3\Description
119      3.04452 SOFTWARE\Microsoft\AuthCookies\Live\Default\DIDC\P3P
95       2.94522 Control Panel\PowerCfg\PowerPolicies\0\Description
86       3.01679 Control Panel\PowerCfg\PowerPolicies\1\Description
76       3.30739 SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell
Folders\Startup
73       2.98146 Control Panel\PowerCfg\PowerPolicies\4\Description
68       3.32837 SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell
Folders\Programs
66       3.38582 SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell
Folders\NetHood
```

```
66      3.34533 SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell
Folders\PrintHood
65      3.08405 SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell
Folders\!Do not use this registry key
60      3.19965
SOFTWARE\Google\Chrome\NativeMessagingHosts\com.microsoft.browsercore\(default)
59      3.33783 SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell
Folders\Start Menu
59      3.05232
SOFTWARE\Microsoft\Windows\CurrentVersion\Themes\LastHighContrastTheme
58      2.90138 Control Panel\PowerCfg\PowerPolicies\2\Description
58      3.33027 SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell
Folders\Cookies
58      3.33677 SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell
Folders\Templates
57      3.31318 SOFTWARE\Microsoft\Windows\CurrentVersion\Lock
Screen\LockAppAumId
56      3.34669 SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell
Folders\Cache
39      1.40236
SOFTWARE\Microsoft\Wisp\Pen\SysEventParameters\FlickCommands\upRight
```

해당 결과를 분석해보았으나 Service 와 관련된 유의미한 결과는 찾을 수 없었다.

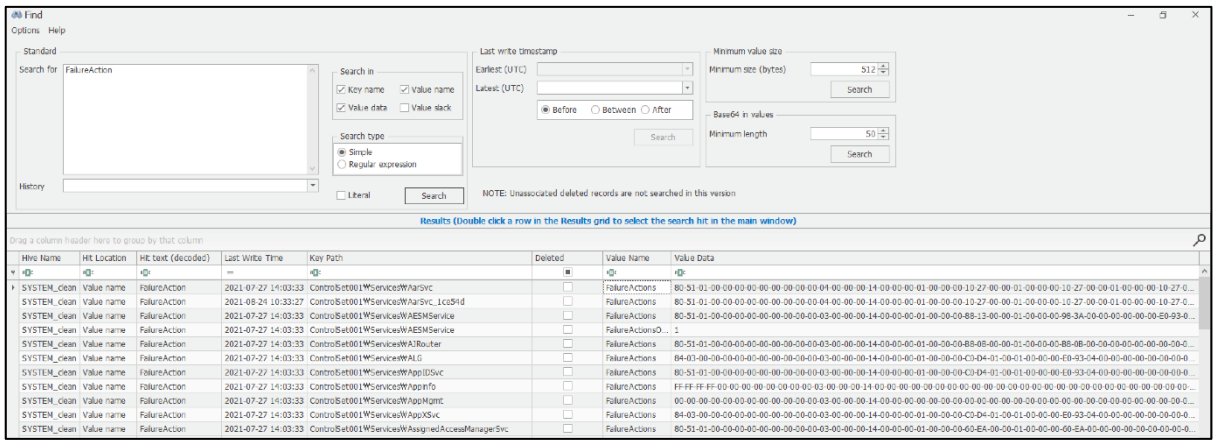
FailureAction 관점

세번째로 확인한 요소는 FailuerAction이다. FailureAction은 레지스트리에 등록된 서비스가 설정된 Binary Path가 존재하지 않거나 할 때 오류가 발생하고, 대체할 수 있는 행위를 설정할 수 있는 기능이다. 아래와 같이 First failure와 Second Failure 등을 통해 Service 실행 실패 시 행위를 설정할 수 있다.



[그림 4] Failure Action 설정 화면

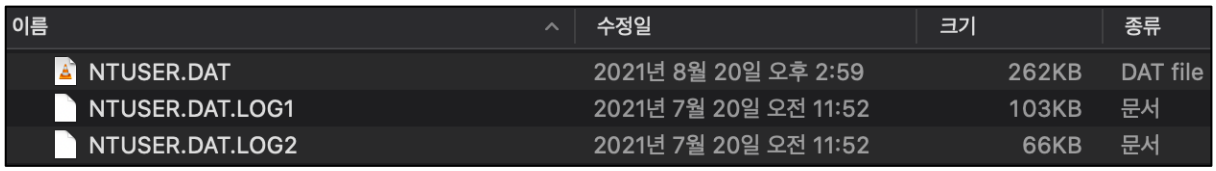
일부 악성코드에서 Run a Program 기능을 이용해 기존 Service에 지정된 Path 이외에 별도의 지정된 Path의 Binary를 실행시킬 수 있다. Mamba Ransomware[4] 악성코드가 이러한 기능을 사용하는 대표적인 예이다. 이를 조사하기 위해서 Registry Explorer를 이용하여 FailureActions 라는 키워드로 Value Name을 검색하였다. 결과는 아래와 같다.



[그림 5] FailureAction 조사 결과

Value Data를 해석하기 위해서는 다음 Stack Overflow[5]를 참고하였다. 그러나 조사 결과 FailureAction 중 Run a program과 같은 설정을 가지고 있는 Service는 존재하지 않았다.

NTUSER.DAT 하이브 분석



[그림 6] NTUSER 하이브

이외에 동봉된 NTUSER.DAT 파일은 LocalService, NetworkService 두 폴더에 존재하였는데 이 또한 SYSTEM HIVE와 동일하게 Reigstry Explorer로 Transaction Log를 포함해 분석하였으나 악성 서비스와 관련된 것으로 보이는 유의미한 결과를 확인하지 못하였다. (Run Key 등, Service 형태가 아닌 Persistent 관련 요소 추가 확인)

Privilege 관점 분석

Least privilege는 정보보안에 있어서 요구되는 원칙 중 하나로 사용자/프로세스/서비스가 행위를 함에 있어서 요구되는 최소한의 privilege만 부여되어야 한다는 의미이다.[6] 레지스트리는 이러한 privilege를 Group으로 관리하며 NT AUTHORITY\SYSTEM과 같은 권한이 그 예이다. 악성코드의 경우 키보드 입력 탈취 등 높은 권한을 필

4 https://logrhythm.com/blog/mamba-ransomware-analysis/

5 https://stackoverflow.com/questions/36462623/what-reg-binary-to-set-for-failureaction-for-

6 https://en.wikipedia.org/wiki/Principle_of_least_privilege

요로 하는 행위를 할 수 있다. 이에 몇몇 악성코드는 높은 권한을 레지스트리 서비스 기능을 이용해 탈취하곤 한다. 아래의 그림과 같이 Service binary를 replace하여 정상 바이너리처럼 보이게 할 수 있다.

```
PS C:\Windows\system32> Get-ModifiableServiceFile | more


ServiceName                   : AeLookupSvc
Path                          : C:\Windows\system32\svchost.exe -k netsvcs
ModifiableFile                : C:\Windows\system32
ModifiableFilePermissions     : GenericAll
ModifiableFileIdentityReference : BUILTIN\Administrators
StartName                     : localSystem
AbuseFunction                 : Install-ServiceBinary -Name 'AeLookupSvc'
CanRestart                    : True

ServiceName                   : AeLookupSvc
Path                          : C:\Windows\system32\svchost.exe -k netsvcs
ModifiableFile                : C:\Windows\system32
ModifiableFilePermissions     : {ReadAttributes, ReadControl, Execute/Travers
                                e, WriteAttributes...}
ModifiableFileIdentityReference : BUILTIN\Administrators
StartName                     : localSystem
AbuseFunction                 : Install-ServiceBinary -Name 'AeLookupSvc'
CanRestart                    : True

ServiceName                   : Apache
Path                          : "C:\xampp\apache\bin\httpd.exe" -k runservice
ModifiableFile                : C:\xampp\apache\bin\httpd.exe
ModifiableFilePermissions     : {ReadAttributes, ReadControl, Execute/Travers
                                e, DeleteChild...}
ModifiableFileIdentityReference : BUILTIN\Users
StartName                     : LocalSystem
AbuseFunction                 : Install-ServiceBinary -Name 'Apache'
CanRestart                    : True
```

[그림 7] Apache Service의 LocalSystem 권한

위의 그림은 httpd가 LocalSystem 권한을 가지고 있고 일반 유저가 Service binary를 수정할 수 있는 권한을 가지고 있어 참고 자료[7]에서는 결국 Powersploit을 이용해 httpd service를 이용한 reverse TCP connection을 성공하였다. 비슷한 방법으로 Regripper의 svc 플러그인을 이용해 분석한 결과를 이용해 LocalSystem 권한을 가진 102개의 결과를 발견할 수 있었다.

```
2021-08-19
00:32:36Z,pmem,pmem,\??\C:\Users\FORENS~1\AppData\Local\Temp\pme86A8.tmp,Kernel
driver,Manual,,@%SystemRoot%\system32\umpnpmgr.dll,-101
2021-08-18 23:53:19Z,GoogleChromeElevationService,Google Chrome Elevation Service
(GoogleChromeElevationService),"C:\Program Files\Google\Chrome\Application\92.0.45
15.159\elevation_service.exe",Own_Process,Manual,LocalSystem,@%SystemRoot%\system3
2\drivers\fvevol.sys,-100
2021-08-17 13:38:31Z,FileSyncHelper,FileSyncHelper,"C:\Program Files (
LocalSystem,                                                    Find  Find Prev  Find
```

[그림 8] LocalSystem 권한 분석

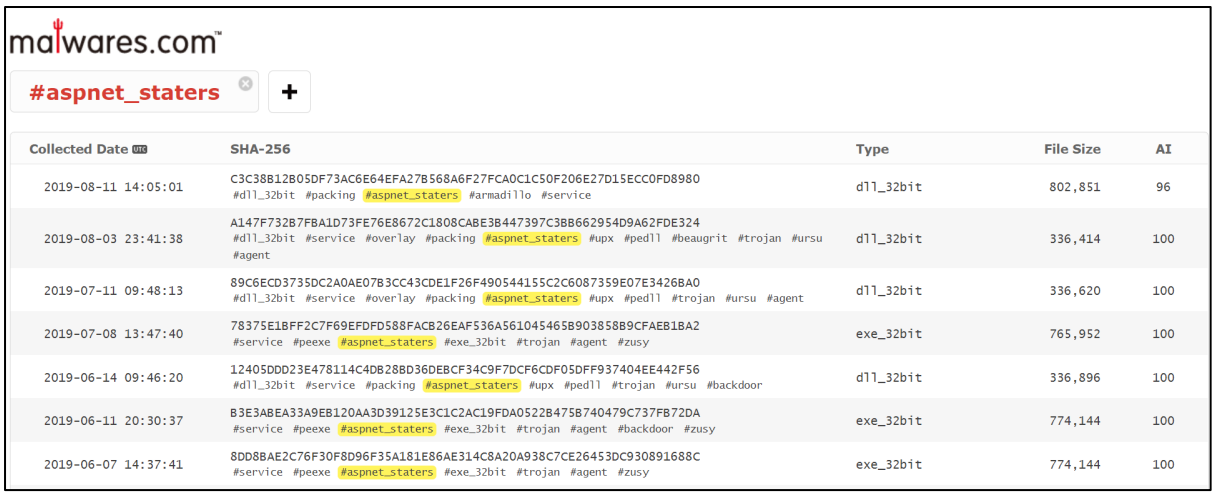
그러나 102개의 결과를 모두 살펴보아도 악성코드의 흔적으로 보이는 경로 등을 발생할 수 없었고 또한 least privilege를 만족하지 못하는 서비스가 있더라도, 이를 악성 service로 단정짓기에는 논리적 비약이 존재하기 때문에 추가적인 privilege 관점 분석을 진행할 수 없었다. 또한 NT AUTHORITY 권한을 가진 43개의 Service 역시 동일한 결과를 나타내었다.

7 https://pentestlab.blog/2017/03/30/weak-service-permissions/

유사 악성코드 조사

비정상적인 서비스는 식별하였으나 어떠한 목적을 가진 서비스인지, 서비스 내부에 기록된 Value들의 의미를 파악하기 위해 서비스 명을 기반으로 유사한 악성코드를 조사하였다.

"aspnet_staters" 라는 Key에 서비스를 등록하는 악성코드는 많은 것으로 확인되었다[8] [9] [10] [11] [12] [13]. 악성코드 검색 서비스를 제공하는 malwares.com에서도 #aspnet_staters 태그가 있을 정도로 해당 이름의 서비스를 등록하는 악성코드가 다 수 존재한다. [14].

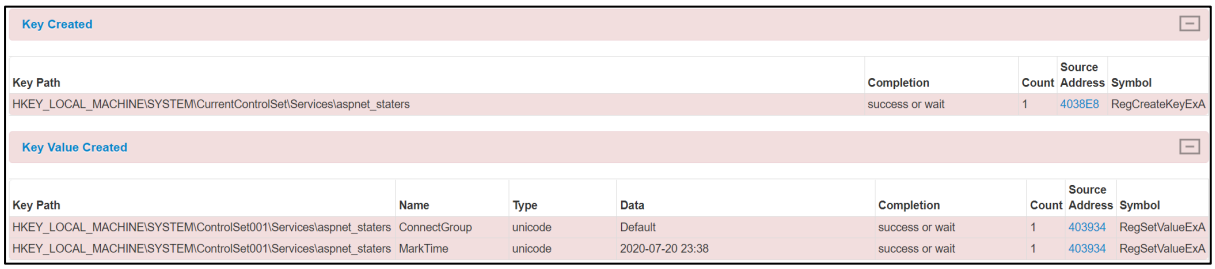

malwares.com

#aspnet_staters +

Collected Date	SHA-256	Type	File Size	AI
2019-08-11 14:05:01	C3C38B12B05DF73AC6E64EFA27B568A6F27FCA0C1C50F206E27D15ECC0FD8980 #dll_32bit #packing #aspnet_staters #armadillo #service	dll_32bit	802,851	96
2019-08-03 23:41:38	A147F732B7FBA1D73FE76E8672C1808CABE3B447397C3BB662954D9A62FDE324 #dll_32bit #service #overlay #packing #aspnet_staters #upx #pedll #beaugrit #trojan #ursu #agent	dll_32bit	336,414	100
2019-07-11 09:48:13	89C6ECD3735DC2A0AE07B3CC43CDE1F26F4905441555C2C6087359E07E3426BA0 #dll_32bit #service #overlay #packing #aspnet_staters #upx #pedll #trojan #ursu #agent	dll_32bit	336,620	100
2019-07-08 13:47:40	78375E1BFF2C7F69EFDFD588FACB26EAF536A561045465B903858B9CFAEB1BA2 #service #peexe #aspnet_staters #exe_32bit #trojan #agent #zusy	exe_32bit	765,952	100
2019-06-14 09:46:20	12405DDD23E478114C4DB28BD36DEBCF34C9F7DCF6CDF05DFF937404EE442F56 #dll_32bit #service #packing #aspnet_staters #upx #pedll #trojan #ursu #backdoor	dll_32bit	336,896	100
2019-06-11 20:30:37	B3E3ABEA33A9EB120AA3D39125E3C1C2AC19FDA0522B475B740479C737FB72DA #service #peexe #aspnet_staters #exe_32bit #trojan #agent #backdoor #zusy	exe_32bit	774,144	100
2019-06-07 14:37:41	8DD8BAE2C76F30F8D96F35A181E86AE314C8A20A938C7CE26453DC930891688C #service #peexe #aspnet_staters #exe_32bit #trojan #agent #zusy	exe_32bit	774,144	100

[그림 9] "aspnet_staters" 키워드 기반으로 악성코드 검색 결과

aspnet_staters 서비스를 등록하는 악성코드 중에서, ConnectGroup과 MarkTime Value를 생성하는 악성코드 5종을 발견했다. 해당 악성코드의 서비스 등록 흔적은 공개된 동적 분석 웹사이트의 분석 보고서를 통해 확인하였다.


Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\aspnet_staters	success or wait	1	4038E8	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\aspnet_staters	ConnectGroup	unicode	Default	success or wait	1	403934	RegSetValueExA
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\aspnet_staters	MarkTime	unicode	2020-07-20 23:38	success or wait	1	403934	RegSetValueExA

aspent_staters Key와 ConnectGroup 및 MarkTime Value를 생성하는 악성코드 (1) [15]

[8] http://malwarefixit.com/backdoor/backdoor-pcclient-6543-1-dll.htm
[9] https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/Worm.PS1.LEMONDUCK.YCAC-A/
[10] https://www.joesandbox.com/analysis/248050/0/html#
[11] https://otx.alienvault.com/indicator/file/62674c1310cae0c3881551a81ee0d88dde6cce6635d16de9f22902491e2ea62a
[12] https://tria.ge/200721-f9vv25stwj/behavioral2#report
[13] https://shorturl.at/bjwBY
[14] https://www.malwares.com/search/tag?tag=aspnet_staters
[15] https://www.joesandbox.com/analysis/248050/0/html#1852FA6C268A5B5BDA067A901764D203D433

Registry

Total	Read	Write	Delete
5	3	2	0

STATUS	KEY
Read	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
Read	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
Read	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
Write	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\aspnet_staters\ConnectGroup
Write	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\aspnet_staters\MarkTime

aspent_staters Key와 ConnectGroup 및 MarkTime Value를 생성하는 악성코드 (2) [16]

Registry Write	process:	svchost.exe	op:	SetValueKeyStr	status:	0x00000000
	path:	HKLM₩SYSTEM₩ControlSet001₩Services₩aspnet_staters₩ConnectGroup				
Registry Create	process:	svchost.exe	op:	CreateKeyEx	status:	0x00000104
	path:	HKLM₩SYSTEM₩ControlSet001₩Services₩aspnet_staters				
Registry Create	process:	svchost.exe	op:	CreateKeyEx	status:	0x00000000
	path:	HKLM₩SYSTEM₩ControlSet001₩Services₩aspnet_staters				
Registry Read	process:	svchost.exe	op:	OpenKeyEx	status:	0x00000104
	path:	HKLM₩SYSTEM₩ControlSet001₩Services₩aspnet_staters				
Registry Read	process:	svchost.exe	op:	OpenKeyEx	status:	0x00000000
	path:	HKLM₩SYSTEM₩ControlSet001₩Services₩aspnet_staters				
Registry Read	process:	svchost.exe	op:	QueryKey	status:	0x00000000
	path:	HKLM₩SYSTEM₩ControlSet001₩Services₩aspnet_staters				
Registry Write	process:	svchost.exe	op:	SetValueKeyStr	status:	0x00000000
	path:	HKLM₩SYSTEM₩ControlSet001₩Services₩aspnet_staters₩MarkTime				

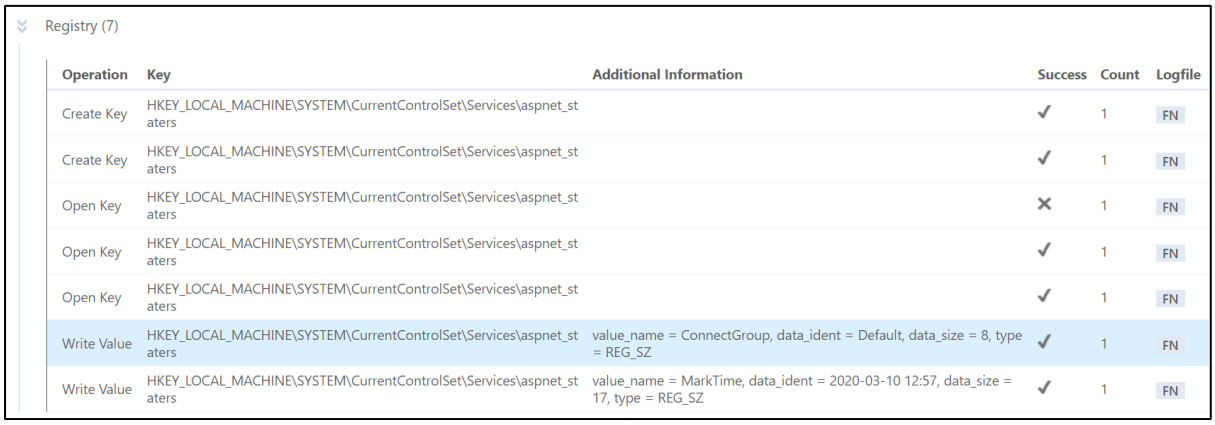
aspent_staters Key와 ConnectGroup 및 MarkTime Value를 생성하는 악성코드 (3) [17]

18）设置注册表数据,主要是设置aspnet_staters服务的相关信息，以便其他样本读取，并判断是否被感染

```
v32 = 1886744434;                       // ConnectGroup
LOBYTE(v33) = 0;
GetInforOfReg_Services((int)&ServiceName, (LPCSTR)&ServiceStartTable, &String, 0x400u);//
                                        // 获取SYSTEM\CurrentControlSet\Services\aspnet_staters的Data
if ( !lstrlenA(&String) )
{
  RegSetValueEx_((int)&ServiceName, &byte_407482);// 设置Services\aspnet_staters键值"ConnectGroup"内容为"MS-SQL
  RegSetValueEx_1((int)&ServiceName);   // 设置aspnet_staters键值MarkTime
}
```

aspent_staters Key와 ConnectGroup 및 MarkTime Value를 생성하는 악성코드 (4) [18]

[16] https://otx.alienvault.com/indicator/file/62674c1310cae0c3881551a81ee0d88dde6cce6635d16de9f22902491e2ea62a
[17] https://tria.ge/200721-f9vv25stwj/behavioral2#q=aspnet_staters
[18] https://shorturl.at/bjwBY

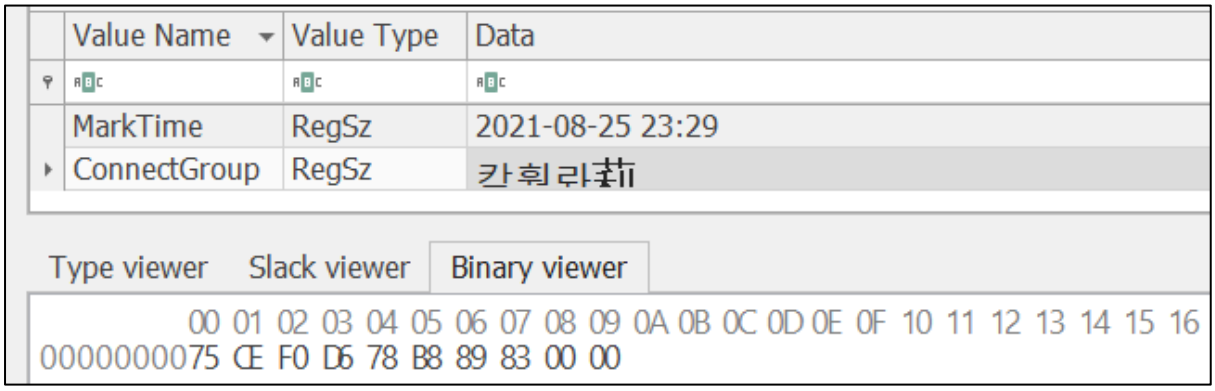


Registry (7)

Operation	Key	Additional Information	Success	Count	Logfile
Create Key	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\aspnet_staters		✓	1	FN
Create Key	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\aspnet_staters		✓	1	FN
Open Key	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\aspnet_staters		✗	1	FN
Open Key	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\aspnet_staters		✓	1	FN
Open Key	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\aspnet_staters		✓	1	FN
Write Value	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\aspnet_staters	value_name = ConnectGroup, data_ident = Default, data_size = 8, type = REG_SZ	✓	1	FN
Write Value	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\aspnet_staters	value_name = MarkTime, data_ident = 2020-03-10 12:57, data_size = 17, type = REG_SZ	✓	1	FN

aspent_staters Key와 ConnectGroup 및 MarkTime Value를 생성하는 악성코드 (5) [19]

악성코드 5 종에 대해 직접 샘플을 구하여, ConnectGroup 의 값이 75CEF0D678B889830000 인 샘플이 있는지 확인하려 하였지만 실패하였다. 샘플들은 최소 1 년 이상 지났기 때문에 C&C 서버 통신 문제 등으로 서비스 등록하는 루틴에 도달하기 전에 종료되는 것으로 추정된다. 이러한 이유로 본 시나리오와 같은 ConnectGroup 의 Data 를 등록하는 악성코드를 재현하지 못하였다.



[그림 10] MarkTime, ConnectGroup Value 확인

하지만, 많은 악성코드에서 aspnet_staters 라는 이름으로 서비스 Key 에다 등록하는 악성코드가 많은 것을 확인할 수 있다. 더 나아가서 ConnectGroup 과 MarkTime 이라는 Value 를 등록하는 악성코드도 실제로 발견하였으므로, aspnet_staters 는 비정상적인 서비스로 추정할 수 있다.

서비스 실행 경로 (Binary Path)

Registry Explorer로는 ImagePath나 ServiceDll을 확인할 수 없었으나 Reg Ripper의 SVC 플러그인 결과를 통해 서비스 실행 경로를 확인하였다.

19 https://www.vmray.com/analyses/ca938d15fcf7/report/behavior_grouped.html#gfn_644

해당 결과에 따르면 “aspnet_staters” 서비스의 실행 경로는

@%SystemRoot%\system32\appxdeploymentserver.dll로 추정된다.

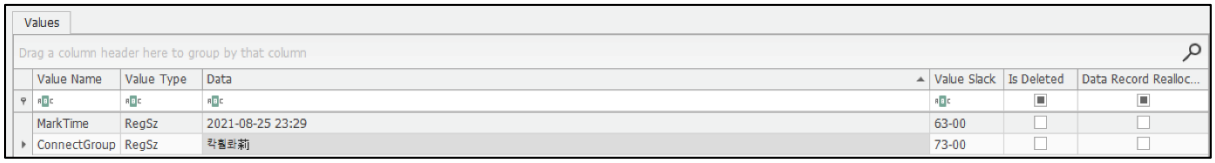
```
svc v.20200525
(System) Lists Services key contents by LastWrite time (CSV)

Time,Name,DisplayName,ImagePath/ServiceDll,Type,Start,ObjectName
2021-08-25 14:51:02Z,BITS,@%SystemRoot%\system32\qmgr.dll;-1000,%SystemRoot%\System32\svchost.exe -k netsvcs -p,Shar
2021-08-25 14:42:34Z,USBSTOR,@usbstor.inf;%USBSTOR.SvcDesc%;USB Mass Storage Driver,\SystemRoot\System32\drivers\USB
2021-08-25 14:42:34Z,WpdUpFltr,@%systemroot%\System32\drivers\WpdUpFltr.sys;-100,System32\drivers\WpdUpFltr.sys,Kern
2021-08-25 14:42:34Z,WUDFWpdFs,@wpdfs.inf;%WPDFS_SvcName%;WPD 파일 시스템 드라이버,\SystemRoot\system32\DRIVERS\WUDF
2021-08-25 14:29:22Z,aspnet_staters,,,,,,@%SystemRoot%\system32\appxdeploymentserver.dll,-2
2021-08-24 10:34:39Z,MicrosoftEdgeElevationService,Microsoft Edge Elevation Service (MicrosoftEdgeElevationService),
```

[그림 11] Reg Ripper로 수집한 서비스 실행 경로

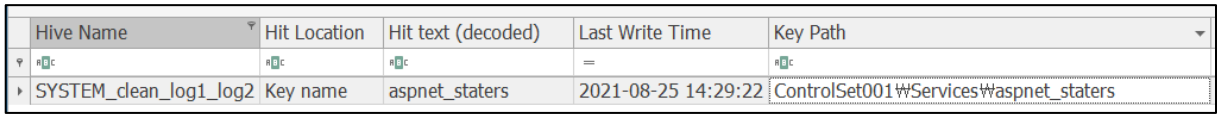
2. When did the attacker install the malicious service? (50 points)

aspnet_staters의 Key의 Last Written 시각과 MarkTime Value에 기록된 시간을 확인하였다. 보통 Service의 설치 시각은 "서비스명" Key의 Last Written 시각이 된다.

Last Written 시각은 2021-08-25 23:29:22 (UTC+0), MarkTime 시각은 2021-08-25 23:29 (UTC+0) 이다. MarkTime은 초를 확인할 수는 없었지만, Last Written 시각의 시간/분이 같은 것을 확인하였다.

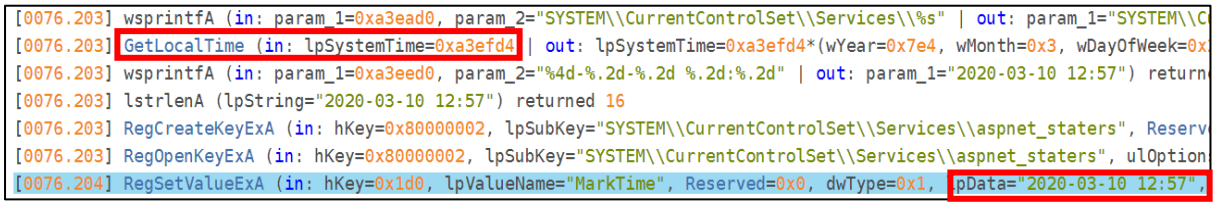


[그림 12] aspnet_staters의 MarkTime Value 확인



[그림 13] aspnet_staters의 Last Write Time

본 시나리오에서 aspnet_staters를 등록한 악성 파일을 확인할 수 없었지만, ConnectGroup과 MarkTime Value를 등록하는 비슷한 악성 코드의 동적 분석 결과[20]를 통해 MarkTime에 기록된 시간 값의 의미를 확인하였다.



[그림 14] MarkTime 데이터에 대한 기록 시점 분석

MarkTime에 기록되는 값은 악성코드가 실행 중인 현재 시각 (정확히는 GetLocalTime 함수가 호출되는 시각)인 것을 확인하였다. 따라서, 유사한 악성코드가 많은 본 시나리오의 악성코드도 MarkTime에 현재 시각을 기록했을 것으로 추정된다.

Last Written 시각과 MarkTime의 시각은 거의 비슷한 시점이므로, 서비스가 등록된 이후 서비스에 해당하는 Registry Key가 변경되지 않았다. 따라서, Last Written 시각이 서비스의 설치 시각이며, 2021-08-25 23:29:22 (UTC+9) 이다.

[20] https://www.vmray.com/analyses/ca938d15fcf7/report/behavior_grouped.html#gfn_644