Malware Analysis Monthly Report (2018-01)

Cryptocurrency Mining Malware Analysis

SOOSAN INT Security Laboratory (CERT)

2018. 01. 19

The report describes Cryptocurrency mining malware.
It was made by SOOSAN INT's Security Laboratory, and we allows you to use it for research purpose. But we decline all responsibility by the rest of use. Please keep in mind that you have the responsibility in that case.

You can reach us via CERT members' mail (SungMin.Rue@soosan.co.kr / KimNamGuy@soosan.co.kr)

SOOSAN INT

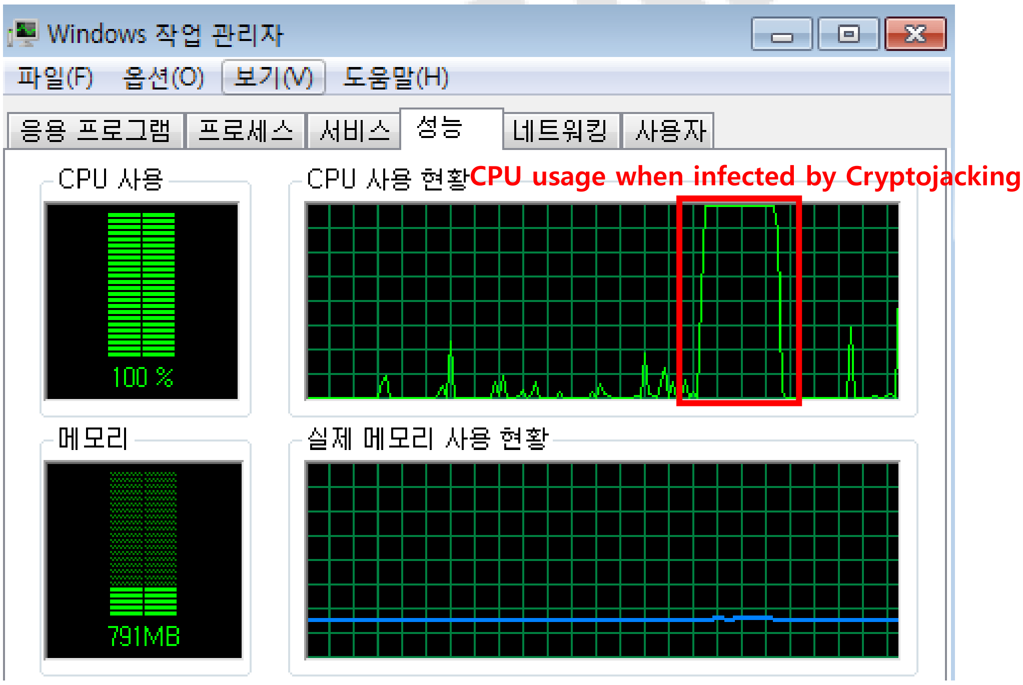
Contents

1. Abstract

In 2017, crytocurrency was remarked because crytocurrency price was skyrocketed. In January 2017, Bitcoin price was about 1,000 dollars; in December 2017, Bitcoin was jumped up to more than 18,000 dollars. Today, Bitcoin is in downturn, but still Bitcoin price is high.

The cryptocurrency's skyrocketing has been getting hackers to make the malware for cryptocurrency acquisition. Especially, it showed up 'Cryptojacking' which is to hack the device and abuse it for coin mining without permission. In cyber security, the Cryptojacking has been issued. According to SK inforsec, 40% of 40 cyber-attacks were the Cryptojacking[1]. So, we analyzed it for cyber security.

In this report, I'm going to introduce Cryptojacking. In section 2, I am going to explain the general principle for coin mining and Cryptojacking. And then I am going to describe its case study done by us.



[1] 서울경제 (2018. 01. 19), "지난 10월부터 가상화폐 마이너 급증...올해 사이버 공격 더 지능화 http://www.sedaily.com/NewsView/1RUHL1JRKE

2. Cryptocurrency Mining Malware (Cryptojacking)

2.1 Cryptocurrency Mining and Cryptojacking

While state money is issued by central bank, cryptocurrency is issued by mining. The mining is the process that the participants (Nodes) get the coin when they solve the problem presented by a mining administrator. In most case, the process is as follow: "encrypted letters (Hash) are given. And the coin is given to the person (or miner) who decrypt it first". The Bitcon's mining process is summarized as below:

1. "8a3a41b85b8b29ad444def299fee21793cd8b9e567eab02cd81" Hash is given.
2. Miner tries to decrypt the hash with brutal force.
3. In requital of the decryption, miner can get the coin.

To decrypt the hash, miner has no option but putting the letter one by one. As a result, the only earliest miner can get the coin. In other words, the main to get the coin is dependent on the computing power. In other words, the more computing power has, the more miner has the possibility to get the coin. For this reason, this is the trend that miners use the multiple computing powers (i.e. PCs) to get the coin. For reference, the location is called "Mining Pool" where the mining computers are congregated.

For example, Bitmain corporation in China uses thousands of computers for mining. Electrical charge per day is 40,000 dollars. It's the amazing number with considering China price. In another case, some mining pools utilize hydroelectric power generation to reduce the electrical charge[2]. In Korea, there are many mining pools[3]. Because of this trend, shortage of GPU happened in Korea. Furthermore, there are some issues that mining pool

[2] 중앙일보 (2017. 08. 31), "하루 전기료만 4400만원...비트코인 캐는 사람들", http://news.joins.com/article/21892530

[3] 머니투데이 (2017. 10. 25), "가상화폐 채굴장 왜 강원도에? 현장 가보니", http://news.mt.co.kr/mtview.php?no=2017102515072025656

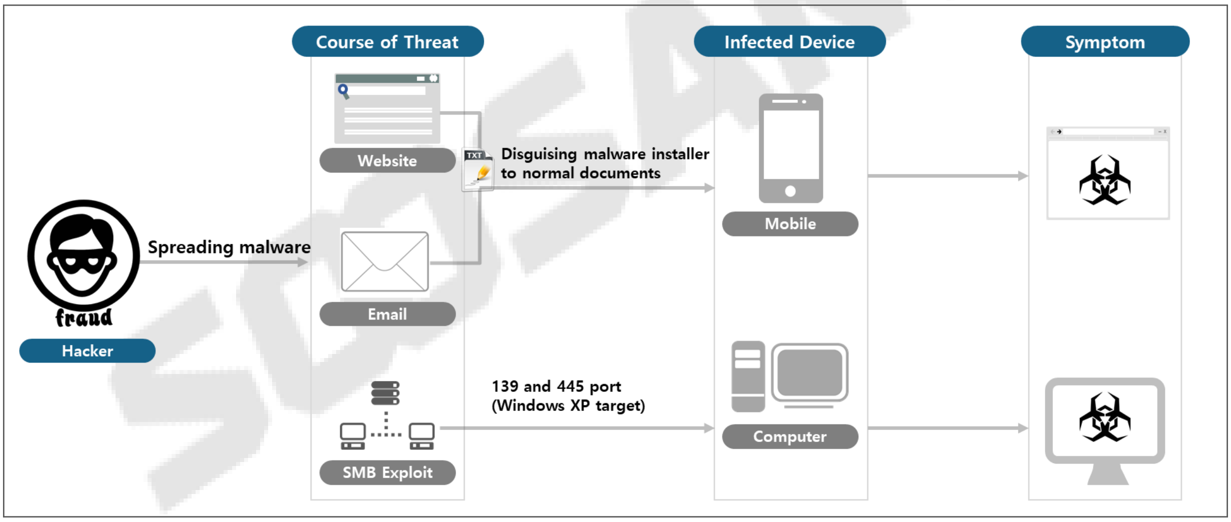
is ruining environments.

Especially in the case of Bitcoin, the issue amount is limited to 21 million coins. And in 24th December, it became known that 80% (16 million bitcoin) had been mined so that the remain coin is small. Thus, the competition for Bitcoin acquisition is fierce.

Currently, cryptocurreny's price is dropping. But still, the price is too high. So, to get the coin, Crytojacking was shown up. It's still widespread[4]. As I said before, Crytojacking makes hackers surreptitiously abuse user's PC for getting coin. Thanks to it, hacker costs nothing. Then see its principle and symptom.

2.2 Cryptojacking Intro

Cryptojacking's principle is as follows:



2.2.1 Threat Course

According to our research, the Hackers spread Cryptojacking with three methods. Firstly, they can spread it by watering hole. Watering hole infects malware via web site. Hackers

[4] Fortune (October 23, 2017), "Why Cryptojacking Is The Next Big Cybersecurity Threat", http://fortune.com/2017/10/23/bitcoin-monero-cryptocurrency-mining-security-threat/

can put malware file in website by abusing website's exploit. Its method has been mostly used because it's the best way to spread it. Most site visitors will be infected by malicious site. Please keep in mind that the success criteria are not to infect specific target but anyone; in other words, the number of infected is important. The more infected, the more easily hackers can get the coin by mining. Secondly, they can use malicious mail to spread Cryptojacking. They can induce mail readers to download malicious files, disgusting it to the normal document. If the readers download it, the installer hidden in the file will be executed and install the Cryptojacking in their PC. Lastly, the hackers can spread the Cryptojacking with SMB (Server Messaging Block) exploit. For reference, SMB is the network protocol to share files. Its port is 139 and 445. In a word, this method is included in zero-day attack. EthernalBlue is the tool to find and less Window XP version because SMB exploit is only founded and less Window XP version. If that version is founded, DoublePulsar put the Cryptojacking to the exploited PC.

2.2.2 Infection Symptom

The Cryptojacking infected device is mostly PC. However recently, it was reported that mobile can be infected. This case has not yet been founded; but it can fully happen. The Cryptojacking symptom can be divided to two types. Cryptojacking can create the hidden folder and abuse the victim PC for mining. Or Cryptojacking can put malicious java script to normal site, discussing adware (in fact, that adware abuses victim PC for mining).

The Cryptojacking was examined. In fact, it's not too risky because it just impacts the victim's device performance. But we should not ignore because it can cause another risk. The most Crytpjacking is networked-based (C&C); so, hackers use it as attack path. To put simply, the Cryptojacking can play role as malware spread path.

3. Case Study (ActivateDesktop)

SOOSAN INT Cert has analyzed the Crytojacking for several times. We are going to introduce the representative case among them.

3.1 Analyzed Malicious File Info

The file name which we analyzed is "ActiveDesktop.exe". The file hash is as follows:

- MD5: 54b6b09962cbede423af9ac3f881117a
- SHA-1: 0004fabc375205237a74b86a94ef9bb3941b505a
- SHA-256: 07dd567986e5acbb4ff2e29099bf994ca2eaa726b3c4a59276628e39d3e54용

We found C&C[5] trace in that file. "http:// 1.lalkaboy.z8.ru" domain was identified as C&C. We analyzed more detailed; that domain was C&C server address of attacker. And we found the dropper site[6]. "http://1.lalkaboy.z8.ru/tools/RegWriter.exe.raum_encrypted" is identified as dropper site.

For reference, the below folder and files were created If you run "ActiveDesktop.exe".

Division	Name (File Location)
Created Folder	.Trash-100 (C:W)
	db (C:₩.Trash-100)
	version (C:₩.Trash-100₩db)
Created File	ActivateDesktop.exe (C:₩.Trash-100)
	framework_exe (C:₩.Trash-100₩db)

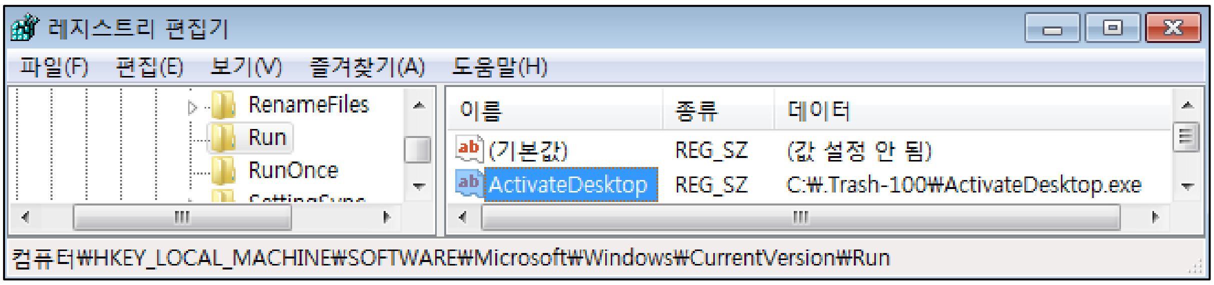
[5] C&C (Command & Control): It's the technology for a hacker to remotely control malware.

[6] Dropper: It's application to site to play role as malware installer.

3.2 Infection Symptom

Automatic running registry is added. It is automatically re-run after restart

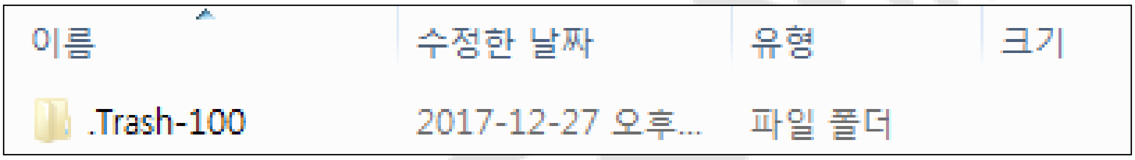
Running ➔ regedit ➔ You can find ActivateDesktop in "HKEY_LOCAL_MACHINE₩SOFTWARE ₩Microsoft₩Windows₩CurrentVersion₩Run"



이름	종류	데이터
(기본값)	REG_SZ	(값 설정 안 됨)
ActivateDesktop	REG_SZ	C:₩.Trash-100₩ActivateDesktop.exe

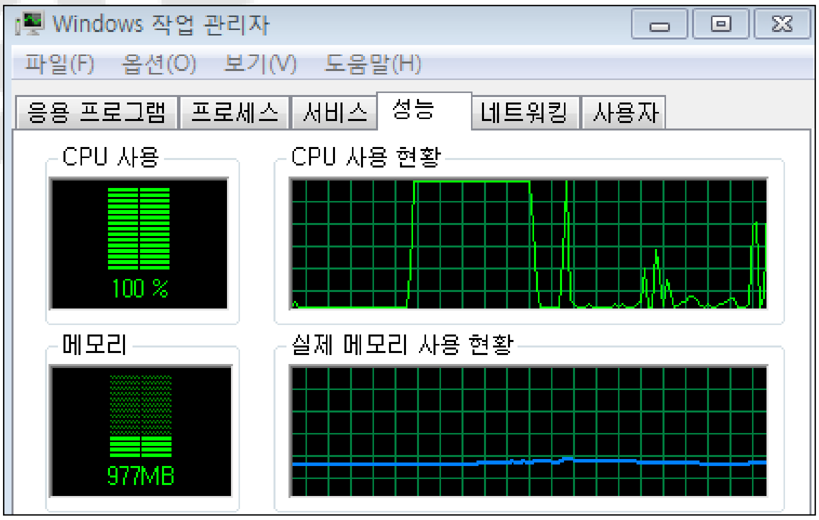
컴퓨터₩HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run

C:₩.Trash-100 Hidden folder is created



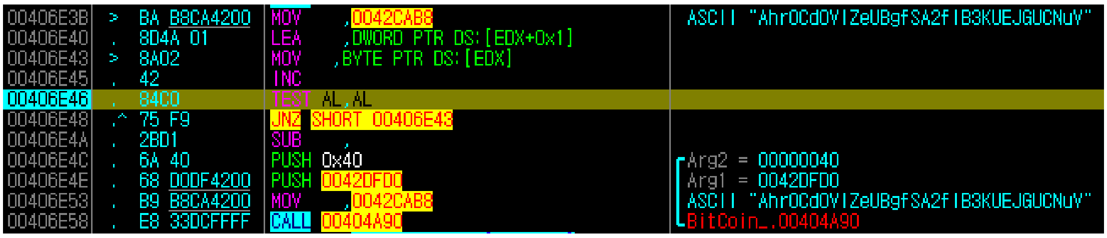
이름	수정한 날짜	유형	크기
.Trash-100	2017-12-27 오후...	파일 폴더	

The symptom is CPU's usage is increased because of the Cryptojacking which is running background environment.



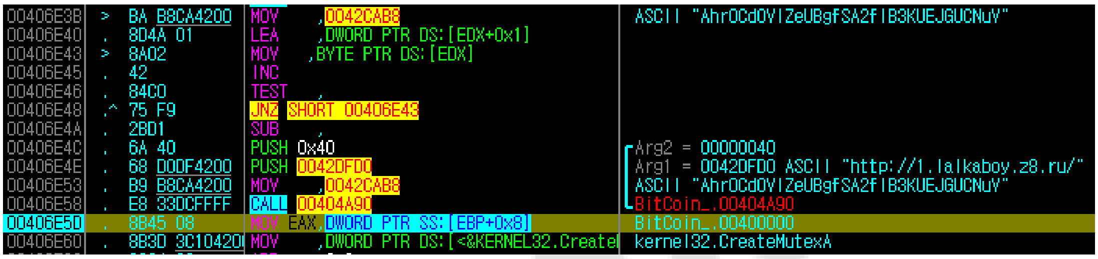
3.3 Analysis Result (Behavior Process)

1. C&C checking: It uses the domain “ru”, the code is obfuscated.



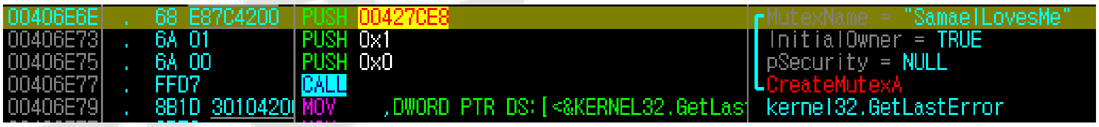
```
00406E3B  >  BA B8CA4200  MOV     ,0042CAB8                    ASCII "AhrOCdOVIZeUBgfSA2fIB3KUEJGUCNuV"
00406E40  .  8D4A 01      LEA     ,DWORD PTR DS:[EDX+0x1]
00406E43  >  8A02         MOV    ,BYTE PTR DS:[EDX]
00406E45  .  42           INC
00406E46  .  84C0         TEST AL,AL
00406E48  .^ 75 F9        JNZ SHORT 00406E43
00406E4A  .  2BD1         SUB     ,
00406E4C  .  6A 40        PUSH 0x40                           ┌Arg2 = 00000040
00406E4E  .  68 D0DF4200  PUSH 0042DFD0                       │Arg1 = 0042DFD0
00406E53  .  B9 B8CA4200  MOV     ,0042CAB8                   │ASCII "AhrOCdOVIZeUBgfSA2fIB3KUEJGUCNuV"
00406E58  .  E8 33DCFFFF  CALL 00404A90                       └BitCoin_.00404A90
```

2. When we decrypted it with CALL 00404A90 call, we could find “http://1.lalkaboy.z8.ru/” domain.

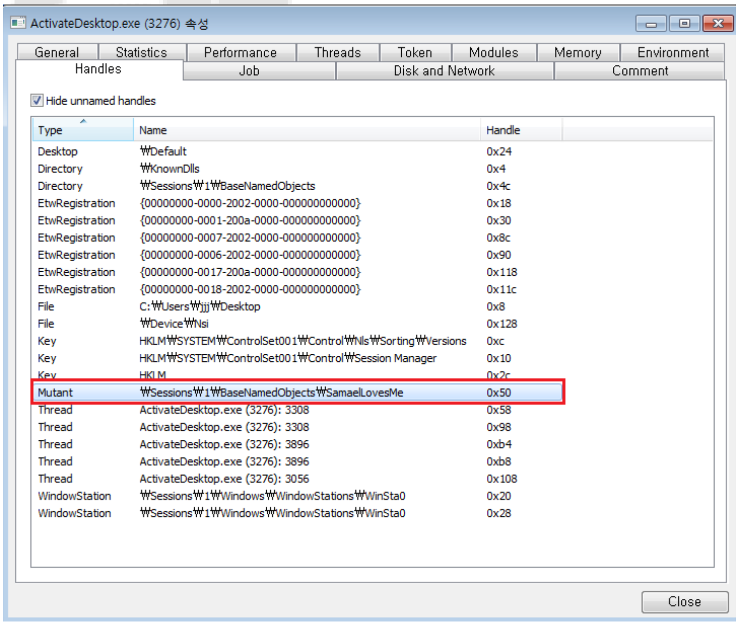


```
00406E3B  >  BA B8CA4200  MOV     ,0042CAB8                    ASCII "AhrOCdOVIZeUBgfSA2fIB3KUEJGUCNuV"
00406E40  .  8D4A 01      LEA     ,DWORD PTR DS:[EDX+0x1]
00406E43  >  8A02         MOV    ,BYTE PTR DS:[EDX]
00406E45  .  42           INC
00406E46  .  84C0         TEST    ,
00406E48  .^ 75 F9        JNZ SHORT 00406E43
00406E4A  .  2BD1         SUB     ,
00406E4C  .  6A 40        PUSH 0x40                           ┌Arg2 = 00000040
00406E4E  .  68 D0DF4200  PUSH 0042DFD0                       │Arg1 = 0042DFD0 ASCII "http://1.lalkaboy.z8.ru/"
00406E53  .  B9 B8CA4200  MOV     ,0042CAB8                   │ASCII "AhrOCdOVIZeUBgfSA2fIB3KUEJGUCNuV"
00406E58  .  E8 33DCFFFF  CALL 00404A90                       └BitCoin_.00404A90
00406E5D  .  8B45 08      MOV EAX,DWORD PTR SS:[EBP+0x8]       BitCoin_.00400000
00406E60  .  8B3D 3C10420 MOV     ,DWORD PTR DS:[<&KERNEL32.Create  kernel32.CreateMutexA
```

3. “SamaelLovesMe” was also found. That file is checking whether the Cryptojacking is run with duplication.



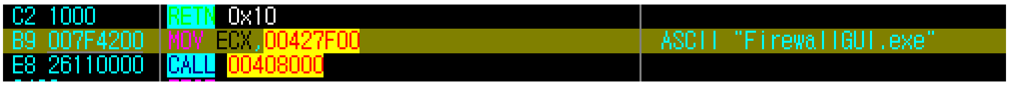
```
00406E6E  .  68 E87C4200  PUSH 00427CE8                        ┌MutexName = "SamaelLovesMe"
00406E73  .  6A 01        PUSH 0x1                             │InitialOwner = TRUE
00406E75  .  6A 00        PUSH 0x0                             │pSecurity = NULL
00406E77  .  FFD7         CALL                                 └CreateMutexA
00406E79  .  8B1D 3010420 MOV      ,DWORD PTR DS:[<&KERNEL32.GetLas  kernel32.GetLastError
```



☑ Hide unnamed handles

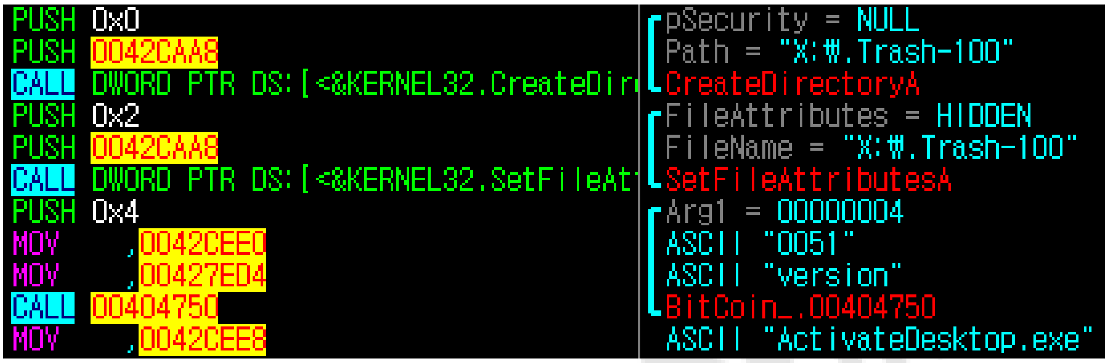
Type	Name	Handle
Desktop	₩Default	0x24
Directory	₩KnownDlls	0x4
Directory	₩Sessions₩1₩BaseNamedObjects	0x4c
EtwRegistration	{00000000-0000-2002-0000-000000000000}	0x18
EtwRegistration	{00000000-0001-200a-0000-000000000000}	0x30
EtwRegistration	{00000000-0007-2002-0000-000000000000}	0x8c
EtwRegistration	{00000000-0006-2002-0000-000000000000}	0x90
EtwRegistration	{00000000-0017-200a-0000-000000000000}	0x118
EtwRegistration	{00000000-0018-2002-0000-000000000000}	0x11c
File	C:₩Users₩jjj₩Desktop	0x8
File	₩Device₩Nsi	0x128
Key	HKLM₩SYSTEM₩ControlSet001₩Control₩Nls₩Sorting₩Versions	0xc
Key	HKLM₩SYSTEM₩ControlSet001₩Control₩Session Manager	0x10
Key	HKLM	0x2c
Mutant	₩Sessions₩1₩BaseNamedObjects₩SamaelLovesMe	0x50
Thread	ActivateDesktop.exe (3276): 3308	0x58
Thread	ActivateDesktop.exe (3276): 3308	0x98
Thread	ActivateDesktop.exe (3276): 3896	0xb4
Thread	ActivateDesktop.exe (3276): 3896	0xb8
Thread	ActivateDesktop.exe (3276): 3056	0x108
WindowStation	₩Sessions₩1₩Windows₩WindowStations₩WinSta0	0x20
WindowStation	₩Sessions₩1₩Windows₩WindowStations₩WinSta0	0x28

4. We did CALL for 00408000 address function, and we checked whether FirewallGUI.exe file was run. If that file was run, we stopped that process.



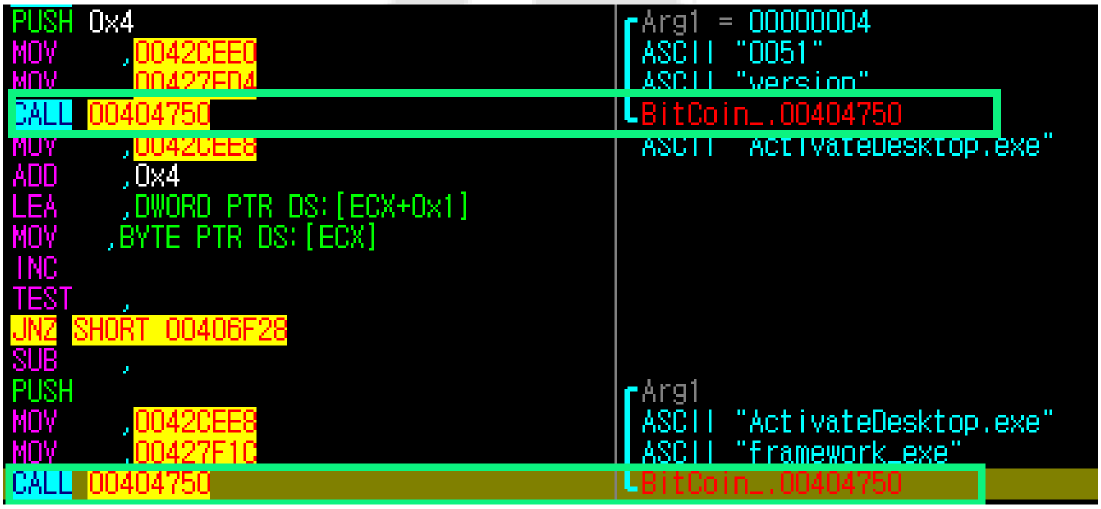
```
C2 1000       RETN 0x10
B9 007F4200   MOV ECX,00427F00                          ASCII "FirewallGUI.exe"
E8 26110000   CALL 00408000
```

5. We were able to find that “C:₩.Trash-100” hidden folder was created by using CreateDirectoryA Function if FirewallGUI.exe was not run.



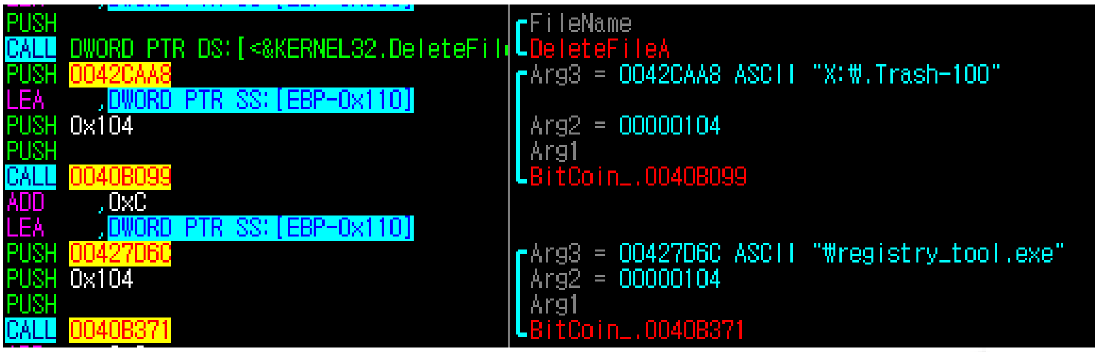
```
PUSH 0x0                                      pSecurity = NULL
PUSH 0042CAA8                                 Path = "X:₩.Trash-100"
CALL DWORD PTR DS:[<&KERNEL32.CreateDir      CreateDirectoryA
PUSH 0x2                                      FileAttributes = HIDDEN
PUSH 0042CAA8                                 FileName = "X:₩.Trash-100"
CALL DWORD PTR DS:[<&KERNEL32.SetFileAt      SetFileAttributesA
PUSH 0x4                                      Arg1 = 00000004
MOV     ,0042CEE0                             ASCII "0051"
MOV     ,00427ED4                             ASCII "version"
CALL 00404750                                 BitCoin_.00404750
MOV     ,0042CEE8                             ASCII "ActivateDesktop.exe"
```

6. After “C:₩.Trash-100” folder creation, the file additionally created “db” folder. And then framework_exe was created.



```
PUSH 0x4                                      Arg1 = 00000004
MOV     ,0042CEE0                             ASCII "0051"
MOV     ,00427ED4                             ASCII "version"
CALL 00404750                                 BitCoin_.00404750
MOV     ,0042CEE8                             ASCII "ActivateDesktop.exe"
ADD     ,0x4
LEA     ,DWORD PTR DS:[ECX+0x1]
MOV    ,BYTE PTR DS:[ECX]
INC
TEST    ,
JNZ SHORT 00406F28
SUB     ,
PUSH                                          Arg1
MOV     ,0042CEE8                             ASCII "ActivateDesktop.exe"
MOV     ,00427F1C                             ASCII "framework_exe"
CALL 00404750                                 BitCoin_.00404750
```

7. We could find the info to create file name and folder name, in ASCII. And CALL 00404750 address became included in ASII stack. Finally, ActivateDesktop.exe file was registered in registry; we found that automatic starting of mining behavior after restart.



```
PUSH                                      FileName
CALL  DWORD PTR DS:[<&KERNEL32.DeleteFil  DeleteFileA
PUSH  0042CAA8                            Arg3 = 0042CAA8 ASCII "X:₩.Trash-100"
LEA    ,DWORD PTR SS:[EBP-0x110]
PUSH  0x104                               Arg2 = 00000104
PUSH                                      Arg1
CALL  0040B099                            BitCoin_.0040B099
ADD    ,0xC
LEA    ,DWORD PTR SS:[EBP-0x110]
PUSH  00427D6C                            Arg3 = 00427D6C ASCII "₩registry_tool.exe"
PUSH  0x104                               Arg2 = 00000104
PUSH                                      Arg1
CALL  0040B371                            BitCoin_.0040B371
```

3.4 Recommendations

We recommend 3 things for you to prevent Cryptojacking infection. It's as follows"

1. **Malicious site prevention with eWalker solution.** The main point to avoid the Cryptojacking infection is not to visit the malicious sites. But it's difficult. So, I would like to recommend our web security solution **"eWalker". eWalker has more than 400K malicious site DataBase (DB). So, if you use eWalker, you can be safe from Cryptojacking malware by watering hole. For refence, we are already ready to prevent Cryptojacking including ActiveDesktop.exe. In the case of C&C domain, eWalker already prevents it.**

C&C Server (Domain & IP)	
1	http:// 1.lalkaboy.z8.ru (80.93.62.207)
2	http:// http://1.lalkaboy.z8.ru/tools/RegWriter.exe.raum_encrypted

2. **OS update is also important** because SMB exploit attack was found.
3. **It's also important to be cautions of reading unknown email**. As we said before, hackers use the mail as malware spreading path. So, you have to be cautions when you receive the unknown mails.

End of Documents

SOOSAN INT

#3F, Suseo Hyundai Venture-ville, 10, Bamgogae-ro 1-gil, Gangnam-gu, Seoul, Korea 06349
Tel +82-2-541-0073 | **Fax** +82-2-541-0204
E-mail sungmin.rue@soosan.co.kr
HP http://www.soosanint.com