**252 – Password Stealer**

|  |
| --- |
| **Team Information** |

**Team Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Team Member \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Email Address \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |
| --- |
| **Instructions** |

**Description** Kim was using a password management tool recommended by an Information Security Specialist. One day, Kim found out through an email that account was stolen. Kim asked a Digital Forensics Specialist to analyze Kim's PC. Analyze Kim's PC to determine the cause.

|  |  |
| --- | --- |
| Target | Hash (MD5) |
| KimPC\_64GB\_NVME.E01 | 56E911E8F845A484D4AC7FA67BCFBC0A |

**Questions**

1. What is the name and version of the password management tool that Kim used? (20 points)
2. Submit SHA1 of the malware used in the attack. (30 points)
3. How many PCs were attacked in total? (50 points)
4. What is the ID and password that Kim saved using the password management tool? (150 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: |  | Publisher**:** |  |
| Version: |  | | |
| URL: |  | | |

|  |
| --- |
| **Step-by-step methodology:** |

1. What is the name and version of the password management tool that Kim used? (20 points)

(FTK Imager의 캡처가 정상 동작하지 않아 글로 대체한다.)

[KimPC\_64GB\_NVME.E01\Basic data partition (3)\NONAME\root\Users\ppp\Downloads]에 위치해 있는 KeePass-2.53.1-Setup.exe 파일을 발견했다.

[KimPC\_64GB\_NVME.E01\Basic data partition (3)\NONAME\root\Windows\Prefetch]에 위치해 있는 KEEPASS-2.53 1-SETUP.EXE와 KEEPASS-2.53 1-SETUP.TMP 파일을 발견했다.

구글링을 해 본 결과, KeePass password safe는 무료 오픈 소스 비밀번호 관리자이다.

**KeePass 2.53.2**

2. Submit SHA1 of the malware used in the attack. (30 points)

[KimPC\_64GB\_NVME.E01\Basic data partition (3)\NONAME\root\Users\ppp\Downloads] 위치에 있었던 파일들을 하나씩 export(우클릭-Export Files) 해보던 와중 viewer.exe파일을 윈도우 보안 시스템이 계속해서 삭제한다는 사실을 발견했다.

악성코드인지 파악하기 위해 Virustotal에 업로드하였다.

텍스트, 스크린샷, 소프트웨어, 멀티미디어 소프트웨어이(가) 표시된 사진

자동 생성된 설명

악성코드로 판단하였다.

텍스트, 스크린샷, 소프트웨어, 폰트이(가) 표시된 사진

자동 생성된 설명

이 파일의 SHA-1은 **fc8113603a8f611ddfd964ffefdec674f9f2367a**이다.

3. How many PCs were attacked in total? (50 points)

텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진

자동 생성된 설명

viewer.exe 파일을 HXD로 살펴보면 PYINSTALLER라는 텍스트가 보인다.

이는 파이썬으로 작성된 py 파일이 아닐까 의심이 들어, pyinstxtractor라는 툴을 다운받았다.

텍스트, 폰트, 스크린샷, 화이트이(가) 표시된 사진

자동 생성된 설명

기존의 파일과 툴을 같은 폴더에 위치시킨 후, cmd창을 켜준다.

텍스트, 스크린샷이(가) 표시된 사진

자동 생성된 설명

**python pyinstxtractor.py viewer.exe** 라는 명령어를 입력하면 extracted된 폴더가 생긴다.

텍스트, 스크린샷, 메뉴, 번호이(가) 표시된 사진

자동 생성된 설명

폴더를 살펴보다가 대부분이 파이썬 프로그램이거나, 확장자가 존재하는데 mal, struct는 유독 파일이 깨끗해 보여서 HXD로 열어보았다.

텍스트, 스크린샷, 번호, 폰트이(가) 표시된 사진

자동 생성된 설명

struct에는 별다른 점이 없다.

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

자동 생성된 설명

mal 파일에는 <http://43.202.32.232/page> 라는 url이 있었다.

텍스트, 스크린샷, 폰트이(가) 표시된 사진

자동 생성된 설명

상단의 url대로 접속해보았지만 연결이 불가능했다.

4. What is the ID and password that Kim saved using the password management tool? (150 points)

**The deadline for this problem is July 31.**

**Please do not post your write-up before the deadline for fair competition!**

**\* Delete this box when submitting your answer.**