

7주차 스터디

6주차 문제 풀이, 악성코드 유사도 분석

6주차 문제 풀이

- [WDF 디지털 포렌식 챌린지](#)
 - 주어진 이미지 파일을 분석하고 시나리오에서 요구하는 내용 찾아보기
- [Forensic CTF: Baud.. James Baud..](#)
 - [CTF Questions](#)에서 요구하는 정답 찾아보기

WDF 디지털 포렌식 챌린지

최고수 분석관은 디지털 포렌식 경력 7년차의 팀장이다. 그는 며칠 전 성범죄 수사전담반의 나 강력 수사관부터 디지털 포렌식 분석 의뢰를 받았다.

나강력 수사관으로부터 확인된 내용은 다음과 같다.

- 최근 불법 음란물 온라인 판매에 대한 단속을 강화하고 있는 가운데, 인터넷 커뮤니티 D 사이트로부터 수사의뢰를 받음
- 아이피 추적 결과 (주)투스타커피에서 음란물 판매 관련 글을 게시한 것으로 확인되어, 압수수색을 실시함
- 압수수색 결과, 문제의 글을 게시한 날짜(2020년 10월 21일)에는 전직 직원이었던 ‘홍길동’만 사무실에 근무하였던 것으로 확인됨
- 홍길동이 사용하였던 노트북은 회사 기밀 유출 건과 관련하여 민간 포렌식 업체에서 분석을 수행한 바 있으며, 포렌식 분석 이후에는 해당 노트북을 중고시장에 매각하여 그 행방을 알 수 없음
- 다만 이전에 분석을 담당하였던 민간 포렌식 업체에 분석 결과물이 남아 있음을 확인하고, 추가 압수수색을 실시하여 당시 분석 결과물 중에 하나인 가상머신에 관한 컨테이너 파일을 확보 함

최고수 팀장은 위 가상머신 컨테이너 파일에 대한 분석을 디지털 포렌식 경력 2년차인 김신참 분석관에게 배정하였다.

WDF 디지털 포렌식 챌린지

김신참 분석관은 나강력 수사관과 혐의자 홍길동에 대한 조사 상황을 확인하였고, 다음과 같은 사실을 확인하였다.

- 홍길동은 현재 인터넷 도박 혐의로 구속되어 수감중인 상태이며, 관련 건으로 수사중인 상태임
- 홍길동은 과거 (주)투스타커피에 직원으로 근무한 바 있었으며, 경쟁회사에 재취업하면서 회사 기밀을 유출하여 형사처벌을 받은 사실 있음
- 홍길동은 평소 IT쪽에 관심이 많아 가상머신을 공부한 적이 있으나, 주로 퇴근 후에 IT 공부 차원에서 사용하였을 뿐, 근무시간에 가상머신을 사용한 적은 없다고 주장함
- 홍길동은 문제가 된 음란물을 인터넷 커뮤니티에 게시한 사실이 전혀 없다고 주장함

참고 : 고양이 그림 --> 아동 음란물, 토끼 그림 --> 성인음란물

나강력 수사관의 분석요구사항은 다음과 같다.

- 가상머신의 실제 사용자 확인
- 2020년 10월 21일 전후의 혐의자의 컴퓨터 사용 이력 분석
- 아동 음란물 등 음란물 유포, 판매 등 흔적 확인
- 기타 혐의자와 관련된 특이정황

Forensic CTF: Baud.. James Baud..

SCENARIO: You're on deck to investigate the high profile hack of a celebrity. Your client provided two screenshots of pop-up message boxes he saw on his system, after which he noticed several vital files were deleted from his system.

1. Whose computer is this evidence from?
2. Who is the other actor?
3. What email service are they using (include TLD)?
4. What makes this email service difficult to analyze?
5. What is the email address of the user?
6. What email address does he correspond with?
7. What type of file is the payload?
8. What is the first Google search the user made about the other individual?
9. What is the second Google search the user made about the other individual?
10. What is the third Google search the user made about the other individual?
11. What IP address was used by the attacker for C2?
12. What is the exact name of the payload?
13. What is the first time the user logged into their email (MM/DD/YYYY H:MM:SS AM/PM)?
14. What is the mail server name used to send these messages?
15. What is the UTC time of the initial email (as stated in the email header)?
16. What is the email subject of the first threatening email sent by the user?
17. What insult does the other individual use in his response?

Forensic CTF: Baud.. James Baud..

- todo

Forensic CTF: Baud.. James Baud..

- todo

정적 분석, 동적 분석

- 정적 분석¹: 실행 없이 소프트웨어를 분석하는 것
 - 소스코드 기반²: code smell³이나 문제가 될 수 있는 소스코드를 탐지
 - 바이너리 기반: 바이너리에 존재하는 어셈블리 코드를 분석
 - [IDA Pro](#), [Binary Ninja](#), [Cutter](#), [Ghidra](#), [Decompiler Explorer](#) 외에도 [bytecode-viewer](#), [jd-gui](#), [jadx](#), [dnSpy](#), [CyberChef](#), [SSView](#) 등 분석 타겟, 용도에 따라서 사용하는 도구가 다르다.
- 동적 분석⁴⁵: 실제 또는 가상 환경에서 프로그램을 실행하여 행위 분석
 - 자동 분석: [cuckoo sandbox](#), [CAPEv2](#), [hybrid-analysis](#), [intezer](#) 등 - [malware-tools](#) 참고
 - 수동 분석: [IDA Pro](#), [x64dbg](#), [ollydbg](#), [Immunity Debugger](#), [Sysinternals](#), [SysmonTools](#) 등
- 개발, 보안 관점에 따라서 해석이 조금 다를 수 있지만 기본적인 개념은 같다.

¹ https://en.wikipedia.org/wiki/Static_program_analysis

² https://owasp.org/www-community/controls/Static_Code_Analysis

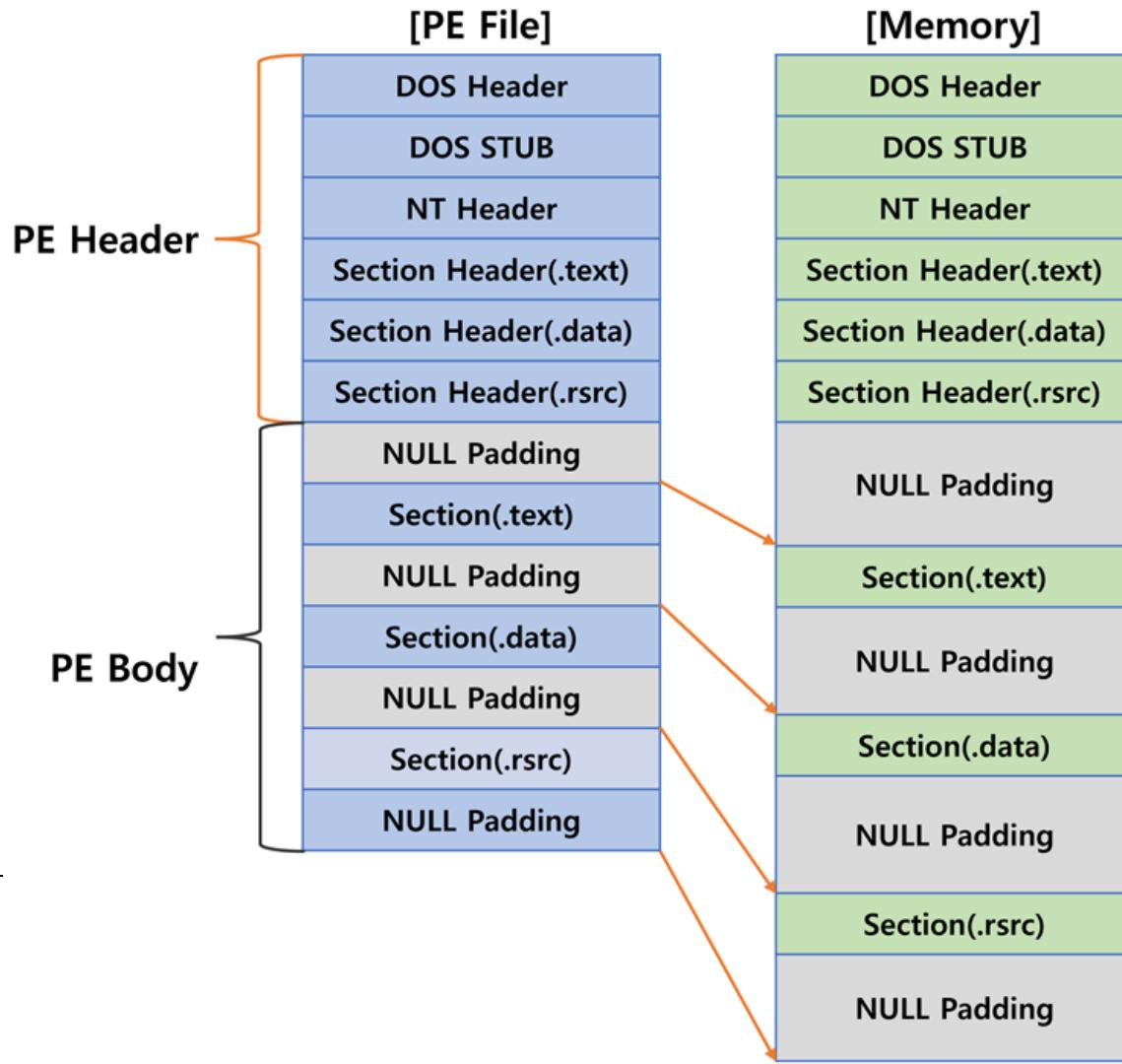
³ https://en.wikipedia.org/wiki/Code_smell

⁴ https://en.wikipedia.org/wiki/Dynamic_program_analysis

⁵ <https://www.vmray.com/glossary/dynamic-analysis/>

PE (Portable Executable)¹

- 윈도우 운영체제에서 사용되는 실행 파일, DLL 등을 위한 파일 형식²
- 파일의 어느 청크가 메모리 어디 부분에 적재되어야 하는지, 프로그램 코드 중 어느 부분에서 프로그램 실행을 시작해야 하는지 등을 정의하고 있다.⁴
- .text 섹션에 있는 프로그램 코드로 리버싱을 진행 한다.
- IAT²를 분석하여 어떤 API가 사용되는지 확인하는 것도 의미있는 분석이 될 수 있다.



¹ <https://learn.microsoft.com/en-us/windows/win32/debug/pe-format>

² https://ko.wikipedia.org/wiki/PE_포맷

³ <https://hwanstory.kr/@kim-hwan/posts/Windows-Portable-Executable-File-Format>

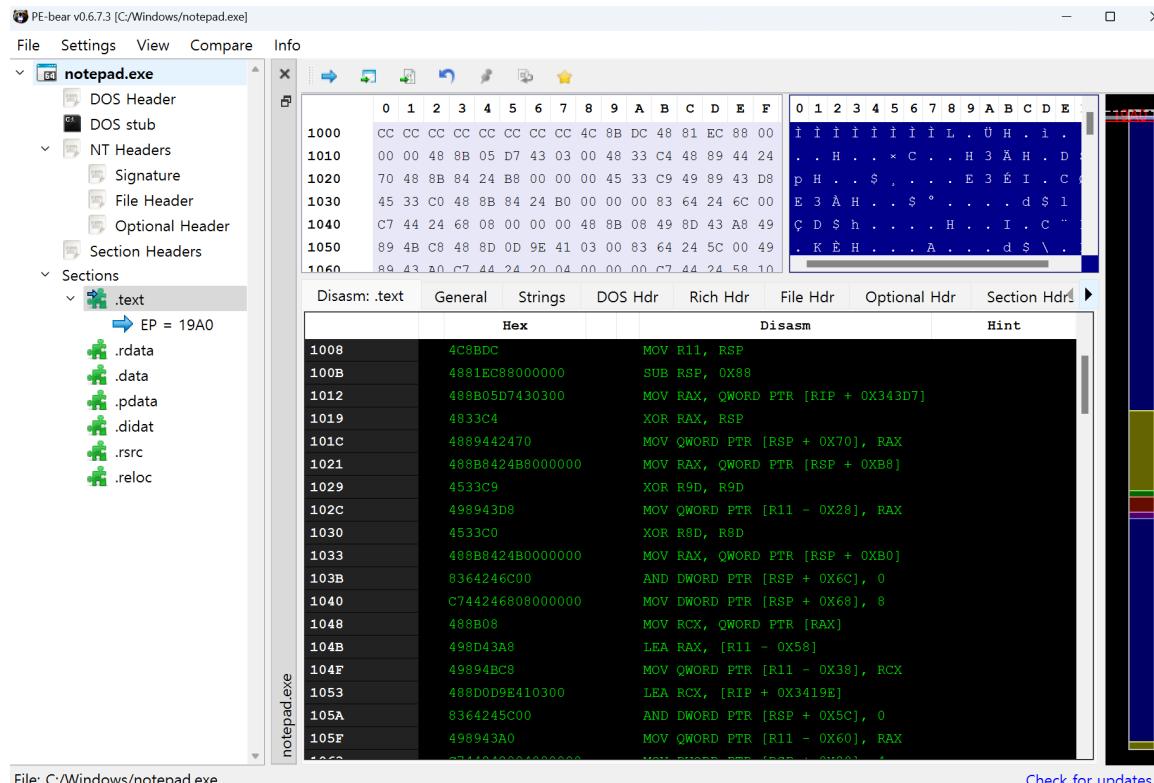
⁴ 멀웨어 데이터 과학 - p2

PE (Portable Executable)

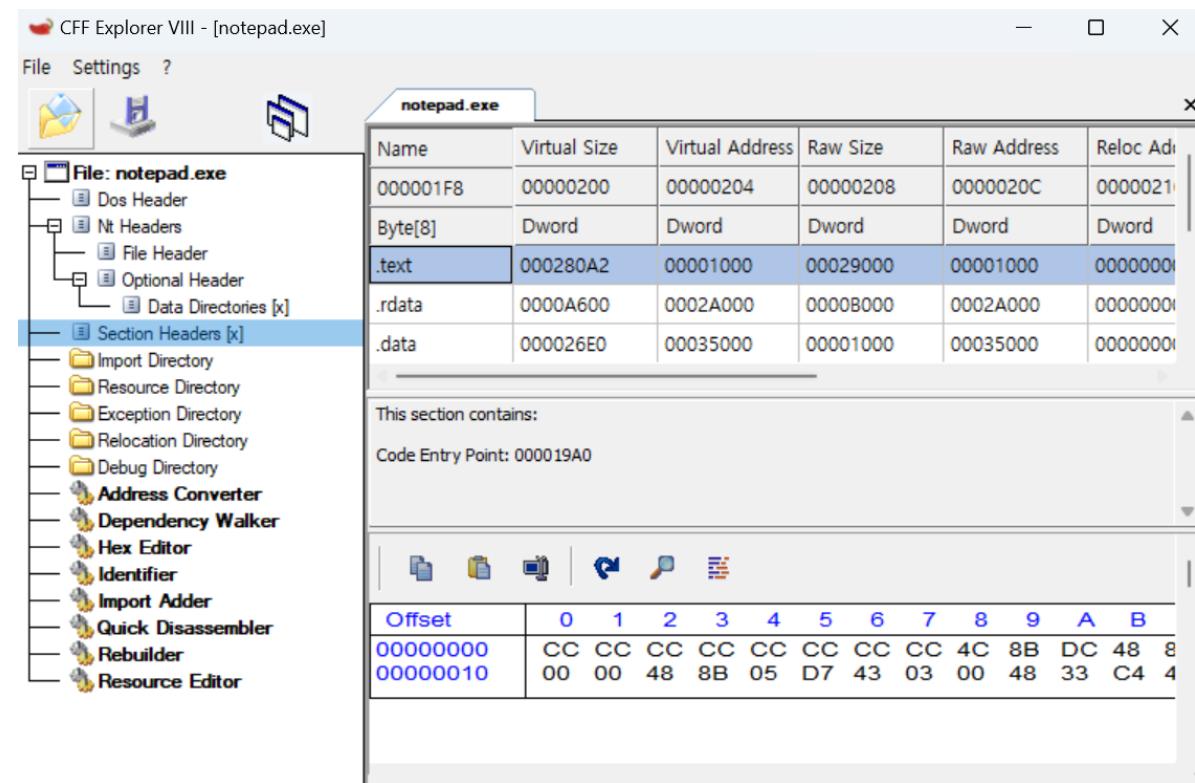
¹ <https://github.com/corkami/pics/blob/master/binary/pe101/pe101ko.png>

PE (Portable Executable)

- PE-bear, CFF Explorer, PEView, FileInsight-plugins, PEStudio

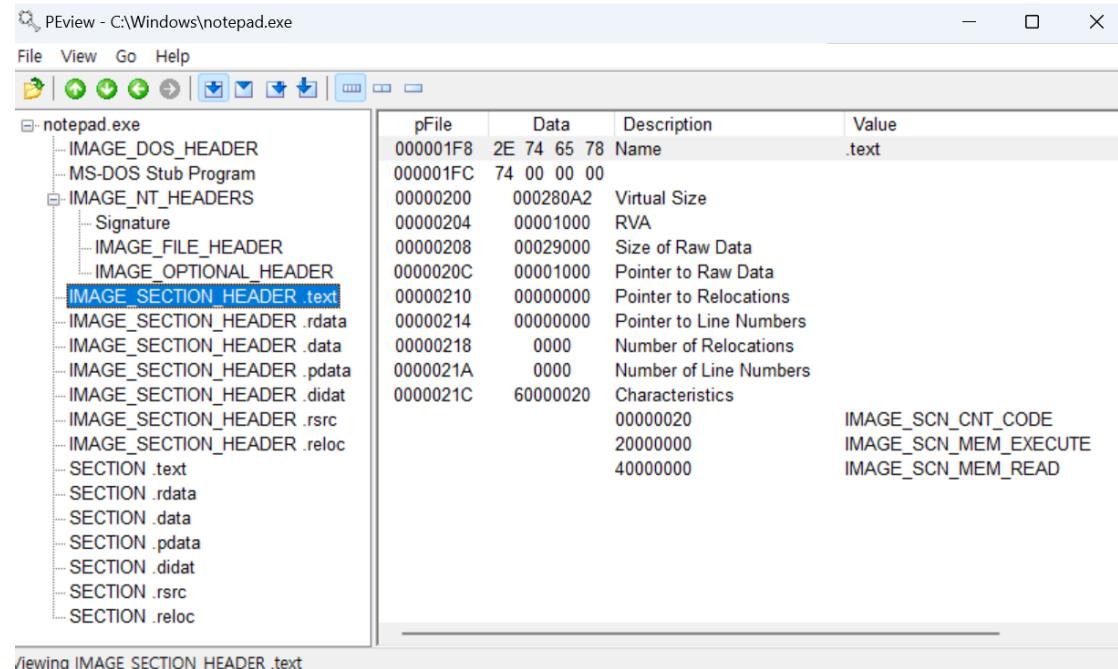


PE-bear

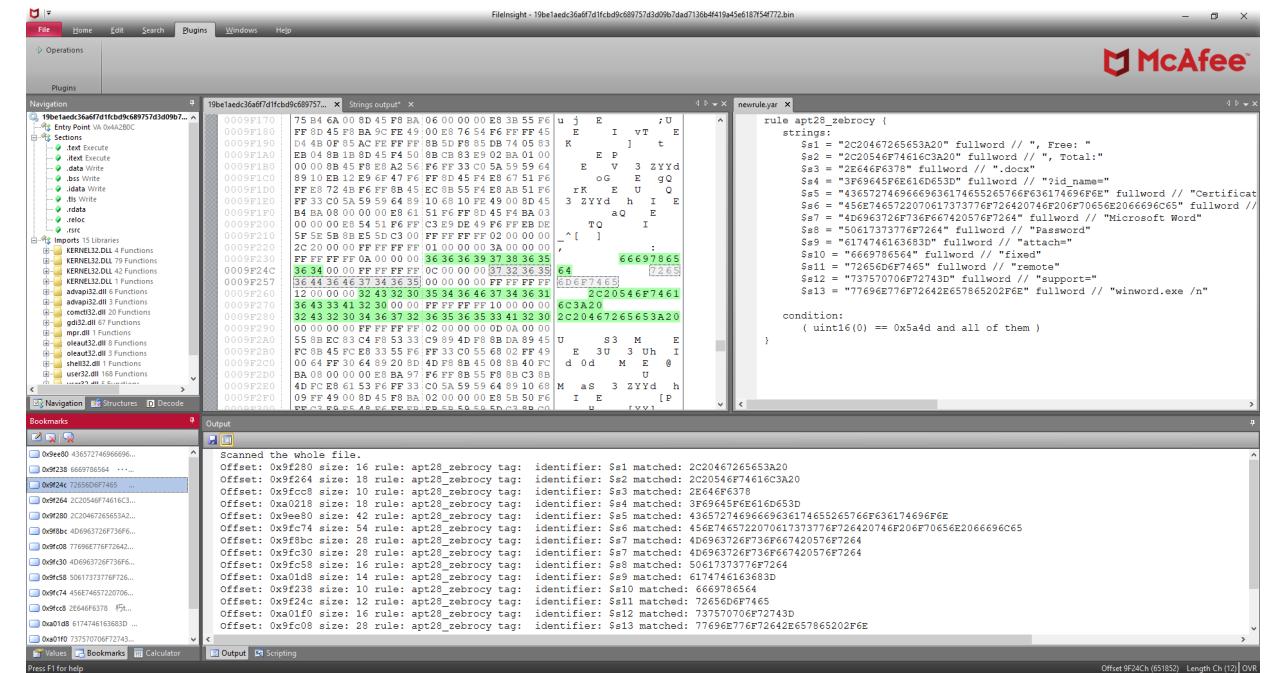


CFF Explorer

PE (Portable Executable)



PEView



FileInsight-plugins

pefile

```
pip install pefile
```

```
import pefile
pe = pefile.PE('sample.exe')
for section in pe.sections:
    print(section.Name, hex(section.VirtualAddress),
          hex(section.Misc_VirtualSize), section.SizeOfRawData)
```

```
import pefile
for entry in pe.DIRECTORY_ENTRY_IMPORT:
    print(entry.dll)
    for imp in entry.imports:
        print('\t', hex(imp.address), imp.name)
```

- PE 파일의 section들의 데이터를 출력하는 코드, 사용하는 API들을 출력하는 코드

¹ <https://pefile.readthedocs.io/en/latest/usage/UsageExamples.html#iterating-through-the-sections>

² <https://pefile.readthedocs.io/en/latest/usage/UsageExamples.html#listing-the-imported-symbols>

패커 (Packer), 프로텍터 (Protector)

- 패커: 실행 파일을 압축한 후 실행될 때 메모리에 스스로 압축을 풀어서 원본 코드를 다시 만드는 방법
 - 리버싱을 어렵게 한다는 점에서 프로텍터와의 구분이 모호한 경우도 있다.
 - 대부분 악의적인 목적으로 사용된다고 한다.¹
- 프로텍터: 프로그램 변조, 리버싱 등을 방지하기 위한 방법
 - 일반적으로 패킹, 난독화 기법³들이 모두 포함되어 있다.¹
- Detect It Easy, Exeinfo PE, PEID 등의 도구를 사용하여 패커, 프로텍터 적용 유무를 확인할 수 있다.
- UniExtract2, VMUnpacker 등 언패커를 사용하는 방법도 있지만 실패한다면 수동으로 메모리 덤프를 통해 추출해야 한다.

¹ <https://www.malwarebytes.com/blog/news/2017/03/explained-packer-crypter-and-protector>

² https://en.wikipedia.org/wiki/Executable_compression

³ [https://en.wikipedia.org/wiki/Obfuscation_\(software\)](https://en.wikipedia.org/wiki/Obfuscation_(software))

패커 (Packer), 프로텍터 (Protector)

- Themida Protector를 사용하는 카카오톡

The screenshot shows the 'Detect It Easy v3.09 [Windows 10 Version 2009] (x86_64)' interface. The file path is 'C:\Program Files (x86)\Kakao\KakaoTalk\KakaoTalk.exe'. The file type is 'PE32' and the size is '24.85 MiB'. The search mode is set to '자동적 인' (Automatic). The analysis results for the PE32 section include:

- 운영 시스템: Windows(Vista)[I386, 32비트, GUI]
- 링커: Microsoft Linker(14.33.31629)
- 컴파일러: Microsoft Visual C/C++(19.33.31630)[C++]
- 언어: C/C++
- 도구: Visual Studio(2022 version 17.3)
- 서명 도구: Windows Authenticode(2.0)[PKCS #7]
- 프로텍터: Themida/Winlicense(3.XX)

Under the '오버레이: Binary' section, it lists:

- 인증서: WinAuth(2.0)[PKCS #7]

¹ <https://hummingbird.tistory.com/6468>

악성코드 스캔

- [Virustotal](#)에서 확인하기
 - 무작정 Virustotal에 업로드하는 것은 좋지 않다.
 - [Virustotal Intelligence](#)^{1,2}에서 누구나 샘플을 다운로드할 수 있기 때문
 - [OpenHashTab](#), [HashMyFiles](#), [Quickhash-GUI](#) 등 해시값(MD5, SHA1, ...) 생성 도구를 사용하여 해시값을 검색해보고, 업로드가 안된 파일이면 경우에 따라서 업로드 유무 판단
 - [PEStudio](#)가 해시값으로 Virustotal에 조회해서 보여준다.

The screenshot shows two side-by-side windows of the PESuite application. Both windows have the title 'pestudio 9.58 - Malware Initial Assessment - www.winitor.com (read-only)'.
The left window displays a table of analysis results for the file 'c:\#users\hyuunnnn\desktop\kape\kape.exe'. The table has four columns: engine (70/70), score (0/70), date (dd.mm.yyyy), and age (days). The data is as follows:

engine (70/70)	score (0/70)	date (dd.mm.yyyy)	age (days)
ALYac	-	04.12.2023	72
APEX	-	28.11.2023	78
AVG	-	04.12.2023	72
Acronis	-	28.08.2023	170
AhnLab-V3	-	04.12.2023	72
Alibaba	-	27.05.2019	1724

The right window shows a detailed analysis of the same file. It lists indicators (count > 3), strings (count > 2), footprints (count > 1), and a 'virustotal' section. The 'virustotal' section indicates that the item was not found at Virustotal and provides a link to 'open Virustotal in your Web browser'.

¹ <https://www.virustotal.com/gui/intelligence-overview>

² <https://docs.virustotal.com/docs/virustotal-intelligence-introduction>

악성코드 스캔

- Microsoft Defender 활용하기
 - 이전에 포렌식 문제에서 랜섬웨어 추출과 동시에 Defender가 잡아줬던 것처럼 탐지율이 준수하다.
 - 그러나 Defender가 잡았다는 것은 백신 서버에 파일이 저장된 것이기 때문에 악성코드 공유 문제 발생
- ClamAV^{1,2} 활용하기
 - 시그니처 데이터베이스를 활용하여 악성코드 패턴을 탐지한다.

```
C:\Users\hyuunnnn\Desktop\clamav-1.3.0.win.x64>freshclam.exe
ClamAV update process started at Thu Feb 15 06:31:10 2024
daily.cvd database is up-to-date (version: 27185, sigs: 2053392, f-level: 90, builder: raynman)
main.cvd database is up-to-date (version: 62, sigs: 6647427, f-level: 90, builder: sigmgr)
bytecode.cvd database is up-to-date (version: 334, sigs: 91, f-level: 90, builder: anvilleg)
```

- 오픈소스이며 PC 내부에서 동작하기 때문에 외부로 업로드되지 않는다.
- 상용엔진에 비해 많이 부족한 것은 사실이다. ClamAV는 단순히 스캐너일 뿐이다.³

```
C:\Users\hyuunnnn\Desktop\clamav-1.3.0.win.x64>clamscan.exe "C:\Users\hyuunnnn\Desktop\test\test\240103, P3"
Loading:   14s, ETA:   0s [=====] 8.69M/8.69M sigs
Compiling:  3s, ETA:   0s [=====] 41/41 tasks
```

¹ <https://docs.clamav.net>

² <https://youtu.be/9gQXBUJ0sHE>

³ <https://blog.clamav.net/2011/03/top-5-misconceptions-about-clamav.html>

FLOSS STACK STRINGS (3)

```
ROOT\CIMV2  
DeviceId  
SELECT * FROM Win32_PnPEntity
```

FLOSS TIGHT STRINGS (0)

FLOSS DECODED STRINGS (31)

```
[\@HTP(LPH  
AXeA  
paAXeA  
pbA8  
Kern  
el32.dll  
GetS  
tartupInfoA  
Heap  
Create  
Exit  
Process  
GetP  
rocessHeap
```

문자열 검사

- 문자열을 추출하여 어떤 기능을 하는지 유추 가능
 - strings**: 바이너리 파일에서 ascii, unicode 문자를 추출한다.
 - floss**: **strings** 기능에 더하여 난독화된 문자열을 탐지하고 복호화 루틴을 찾아서 에뮬레이팅하는 과정을 수행한다.
→ 탐지율이 높진 않은 것 같다. (그래도 의미있는 정보를 얻을 가능성도 있기 때문에 밀쳐야 본전 마인드로 사용하면 되겠다.)

The screenshot shows two panels from the NetworkMiner tool. The left panel, titled 'Network Communication', displays 'IP Traffic' with three entries: 113.160.112.125:443 (TCP), 196.45.177.52:8080 (TCP), and 213.210.194.59:8443 (TCP). Below it, under 'Memory Pattern IPs', are three entries: 113.160.112.125, 196.45.177.52, and 213.210.194.59. The right panel, titled 'FLOSS STACK STRINGS (6)', lists the following strings:
113.160.112.125
213.210.194.59
196.45.177.52
199.26.11.18
SOVA?0VAK
EDf3

9394078671922de6b5cd194e3581ec46¹

¹ [HiddenCobra_BANKSHOT - AdobeARM.exe](#)

문자열 검사

- **CAPA**: 실행 파일의 기능, 행위를 탐지해주는 기능 → 특정 API 사용 여부나 payload 등을 탐지하여 어떤 행위가 예상되는지 알려준다.

```
self delete
namespace anti-analysis/anti-forensic/self-deletion
author michael.hunhoff@mandiant.com, @mr-tz
scope function
att&ck Defense Evasion::Indicator Removal::File Deletion [T1070.004]
mbc Defense Evasion::Self Deletion::COMSPEC Environment Variable [F0007.001]
function @ 0x4027B0
and:
or:
match: host-interaction/process/create @ 0x4028AF
or:
api: CreateProcess @ 0x402914
or:
regex: /del\s*\S/
- "@echo off\r\n:D1\r\n\ndel /a %1\r\nif exist %1 goto D1\r\n\ndel /a %0" @ 0x4028B5

receive data (3 matches)
namespace communication
author william.ballenthin@mandiant.com
scope function
mbc Command and Control::C2 Communication::Receive Data [B0030.002]
description all known techniques for receiving data from a potential C2 server
function @ 0x401B4D
or:
match: receive data on socket @ 0x401B4D
or:
api: recv @ 0x401B7D
api: recv @ 0x401B7D
```

```
    strcpy(Destination, aEchoOffD1DelA1);
v1 = strlen(Destination);
WriteFile(FileA, Destination, v1, &NumWritten);
CloseHandle(FileA);
memset(&StartupInfo, 0, sizeof(StartupInfo));
StartupInfo.dwFlags = 1;
StartupInfo.wShowWindow = 0;
CreateProcessA(0, CommandLine, 0, 0, 0,
0, 0, 0, 0, &StartupInfo, &ProcessHandle, &ThreadHandle);
}
return 1;
}
000028B5 sub_4027B0:49 (4028B5)
aEchoOffD1DelA1 db '@echo off',0Dh,0Ah ; DATA XREF
db ':D1',0Dh,0Ah
db 'del /a %1',0Dh,0Ah
db 'if exist %1 goto D1',0Dh,0Ah
db 'del /a %0',0Dh,0Ah
align 4
```

¹ Backdoor - Joanap

7FE80CEE04003FED91C02E3A372F4B01¹

	Talos Group	Dell Secure W	Other Name 1	Other Name 2	Other Name 3	Other Name 4	Other Name 5	Other Name 6	Other Name 7	Other Name 8	Rep. of Korea	MITRE AT&CK	Operation 1	Operation 2	Op
Chollima	Group 77	Hastati Group	121,BeagleBoyzBureau121,BeagleBoyz	Unit 121,Unit121	Whois Hacking Team,WHOis Team	NewRomanic Cyber Army Team	ZINC,APT-C-26,UNC2970,UNC577,UNC4736	Appleworm,NICKEL GLADSTONE,COVELLITE,ATK3	Hidden Cobra,Diamond Sleet,Black Artemis,	Nickel Academy,LolZarus		G0032	Troy	Blockbuster	D
hollima	Group 123	ScarCruft	APT37	Red Eyes	Reaper	Venus 121(금성121)	THALLIUM				G0067	Reaper	Erebus	G	
lima			DEV-0530,DEV0530	DarkSeoul,Dark Seoul	PLUTONIUM	Guardian of Peace	GOP	Onyx Sleet	Storm-0530	H0lyGh0st	Andariel	G0138	Dark Hotel	DesertWolf	V
llima														Campaign	

위협 인텔리전스 팀은 악성코드 분석에서 파악한 식별자를 사용해 공격을 분류하고 알려진 위협과 구분 짓는다.
악성코드 분석을 공격 배후에 누가(경쟁자, 국가 지원 공격 그룹 등) 있는지에 대한 정보를 얻는 데 도움을 준다.

악성코드 분석 시작하기 - p33

			APT38										G0082		
hollima			APT38	ElectricFish	BlueNoroff	TA444 (Proofpoint)	COPERNICIUM	TAG-71 (Microsoft)				G0082		Far Eastern I	
o														Honeybee	

¹ APT Groups and Operations

² https://en.wikipedia.org/wiki/List_of_hacker_groups

유사도 분석을 왜 할까?

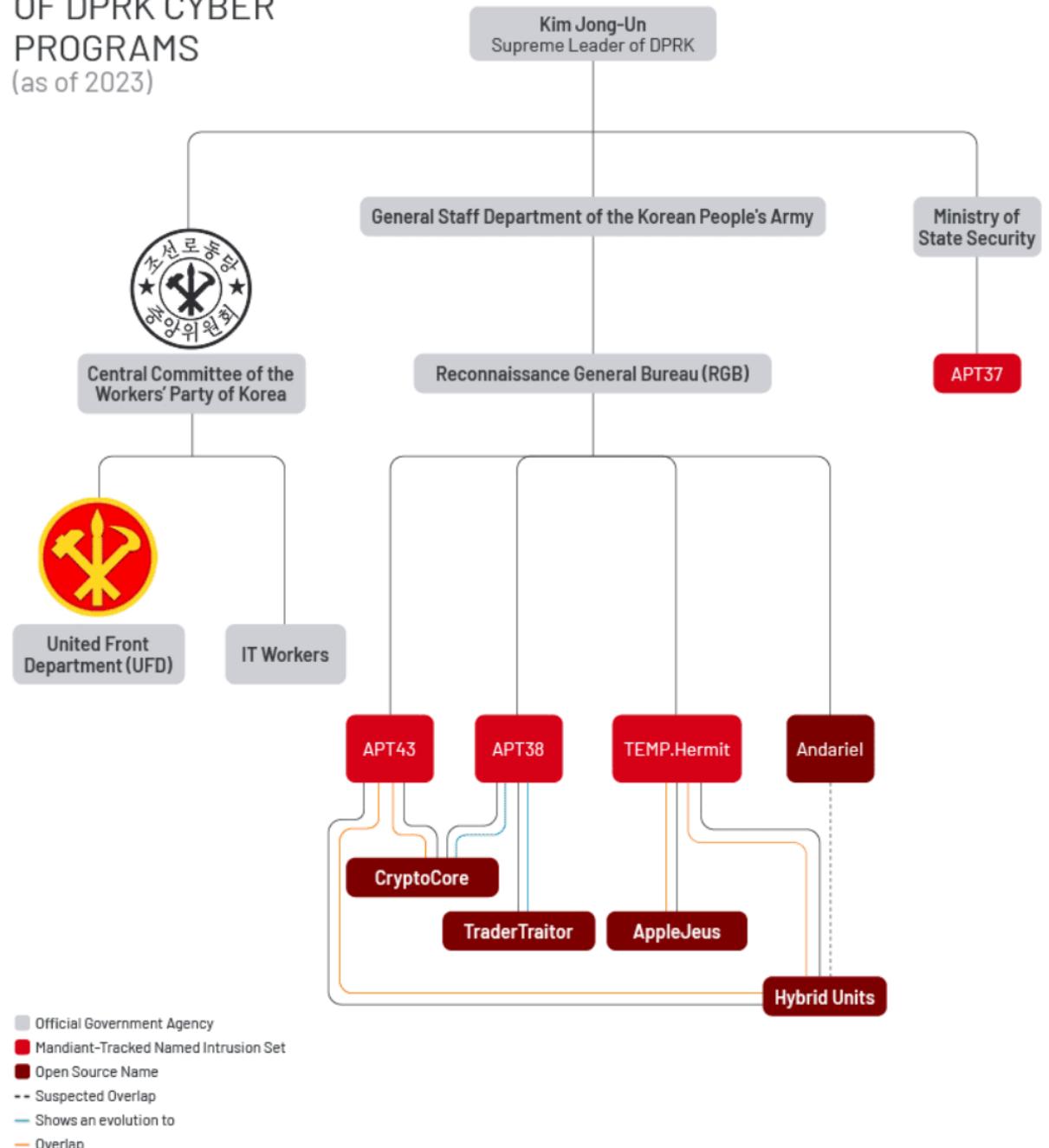
Table 1: CISA and Joint CISA Publications

Publication Date	Title	Description
February 9, 2023	#StopRansomware: Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities	The NSA, FBI, CISA, Department of Health and Human Services, the Republic of Korea (ROK) National Intelligence Service, and the ROK Defense Security Agency issued a joint Cybersecurity Advisory to highlight ongoing ransomware activity against Healthcare and Public Health Sector organizations and other critical infrastructure sector entities.
July 6, 2022	Joint FBI-CISA-Treasury CSA: North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector	The FBI, CISA, and the Department of the Treasury issued a joint Cybersecurity Advisory to provide information on Maui ransomware, which has been used by North Korean state-sponsored cyber actors since at least May 2021 to target Healthcare and Public Health (HPH) Sector organizations.

¹ <https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/north-korea>

² <https://www.mandiant.com/resources/blog/north-korea-cyber-structure-alignment-2023>

ASSESSED STRUCTURE OF DPRK CYBER PROGRAMS (as of 2023)



유사도 분석을 왜 할까?

북한



WinRAR 취약점(CVE-2023-38831) 분석
보고서

2024.01.26



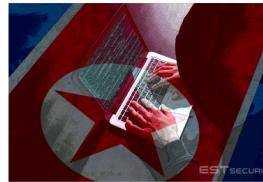
2024년 보안 위협 전망 및 2023년 주요 보안
이슈 회고

2024.01.02



ESRC 주간 Email 위협 통계 (11월 넷째주)

2023.11.28



'금성121' APT 조직, 국내 정치사회적 이슈를
악용한 공격 진행중!

2023.09.19



자산 관리 프로그램을 악용한 공격 정황 포착 (Andariel 그룹)

Posted By song.th , 2023년 11월 10일

ASEC 분석팀은 Lazarus 그룹과 협력 관계이거나 하위 조직으로 알려진 Andariel 위협 그룹이 최근 특정 자산 관리 프로그램을 이용한 공격을 통해 악성코드를 유포하고 있는 정황을 확인하였다. Andariel 그룹은 최초 침투 과정에서 주로 스파이 피싱 공격이나 워터링 툴 공격 그리고 공급망 공격을 이용하며, 이외에도 악성코드 설치 과정에서 중앙 관리 솔루션을 악용하는 사례도 존재한다. 최근에는 Log4shell 및 InnoRox Agent 등 여러 프로그램에 대한 취약점을 이용하여 국내 다양한 기업군에 공격을 해오고 있다. [1] 이번에 확인된 공격은 국내의 또 다른 자산 관리 프로그램이 사용되었으며, 이외에도...



김수키(Kimsuky)조직의 'Mail Online Security' 프로그램 위장 공격 주의!

2023.06.02



한미(韓美) 합동 보안권고문 : 북한 김수키(Kimsuky) 조직의 싱크탱크, 핵계, 미디어 대...

2023.06.02



북한 사이버 공격의 현주소와 그 대응 방법

2023.05.26



ESRC 주간 Email 위협 통계 (5월 셋째주)

2023.05.23



Lazarus 조직의 Operation Dream Magic

Posted By securityresponseteam , 2023년 10월 13일

Lazarus 조직은 국가가 배후인 것으로 알려진 해킹 조직으로 금전적인 이득, 자료 탈취 등의 목적으로 전세계를 대상으로 꾸준히 해킹하고 있습니다. Lazarus 조직의 이니세이프 취약점을 악용한 워터링 툴을 간단하게 정리하면 언론사의 특정 기사에 악성 링크 삽입, 해당 기사를 클릭하는 기업, 기관이 해킹 대상, 국내 취약한 홈페이지를 C2로 악용 그리고 제한된 범위의 해킹을 위해서 IP 필터링 등을 사용

- 국내 뿐만 아니라 외국에서도 악성코드를 분석하고 리포트를 작성하여 공유하고 있다.

¹ <https://blog.alyac.co.kr/search/ 북한>

² <https://asec.ahnlab.com/ko/>

유사도 분석을 왜 할까?

Hacks, Thefts, and Total Amounts Stolen

This Repo	Value Stolen	Incidents		Chainalysis	Value Stolen	Incidents		TRM	Value Stolen	Incidents
2023	\$649,889,146	20		2023	\$1,000,000,000	20		2023	\$600,000,000	?
2022	\$767,638,000	9		2022	\$1,650,000,000	15		2022	\$850,000,000	?
2021	\$317,050,000	13		2021	\$428,800,000	9		2021	\$250,000,000	?
2020	\$307,726,000	8		2020	\$300,000,000	5		2020	\$290,000,000	?
2019	\$191,794,000	9		2019	\$271,000,000	9		2019	\$200,000,000	?
2018	\$430,265,000	15		2018	\$522,000,000	10		2018	\$400,000,000	?
2017	\$109,490,000	6		2017	\$29,000,000	4		2017	\$100,000,000	?
2016	0	0		2016	\$1,500,000	1		2016	0	?
Total:	\$2,773,852,146	80		Total:	\$4,202,300,000	73		Total:	\$2,690,000,000	0

¹ <https://github.com/tayvano/lazarus-bluenoroff-research>

[bindiff](#), [diaphora](#), [veles - blog](#), [cantordust - blog](#), [binocle](#), [binvis](#) 등

IOC(Indicator Of Compromise, 침해지표)

- todo

<https://maj3sty.tistory.com/1066>

```

def get_imphash(self):
    impstrs = []
    exts = ["ocx", "sys", "dll"]
    if not hasattr(self, "DIRECTORY_ENTRY_IMPORT"):
        return ""
    for entry in self.DIRECTORY_ENTRY_IMPORT:
        if isinstance(entry.dll, bytes):
            libname = entry.dll.decode().lower()
        else:
            libname = entry.dll.lower()
        parts = libname.rsplit(".", 1)
        if len(parts) > 1 and parts[1] in exts:
            libname = parts[0]

        entry_dll_lower = entry.dll.lower()
        for imp in entry.imports:
            funcname = None
            if not imp.name:
                funcname = ordlookup.ordLookup(
                    entry_dll_lower, imp.ordinal, make_name=True
                )
            if not funcname:
                raise PEFormatError(
                    f"Unable to look up ordinal {entry.dll}:{imp.ordinal:04x}"
                )
            else:
                funcname = imp.name

            if not funcname:
                continue

            if isinstance(funcname, bytes):
                funcname = funcname.decode()
            impstrs.append("%s.%s" % (libname.lower(), funcname.lower()))

    return md5(",".join(impstrs).encode()).hexdigest()

```

imphash (import hashing)

- 실행 파일에 있는 라이브러리/임포트 함수 이름과 특유의 순서를 바탕으로 해시값을 생성하는 방법¹
- IAT에서 라이브러리 이름과 API 이름을 리스트에 append하고 마지막에 , 를 기준으로 join 한 문자의 조합을 md5로 변환하는 방식으로 구현하고 있다.

¹ 악성코드 분석 시작하기 - p91

² pefile - get_imphash

fuzzy hash

Fuzzy hashing

Forensic Malware Analysis: The Value of Fuzzy Hashing Algorithms in Identifying Similarities

A Ransomware Detection Method Using Fuzzy Hashing for Mitigating the Risk of Occlusion of Information Systems

Fuzzy-Import Hashing: A Malware Analysis Approach

[How To] Fuzzy Hashing with SSDEEP (similarity matching)

How to Identify Malware Similarities with Fuzzy Hashing

FUZZY HASHES

ssdeep

ssdeep - pypi

Playbook of the Week: Uncovering Unknown Malware Using SSDeep

ssdc

impfuzzy

- todo

PDB (Program Data Base)

- PDB path는 디버그 모드로 빌드할 때 생성된다. 이때 프로젝트명은 무엇인지, 제작자는 누구인지 등 악성코드에 대한 정보를 얻을 수 있다.
- KEEPER CTF IR-1 문제의 랜섬웨어 파일에 PDB path를 통해 제작자와 랜섬웨어 이름 확인 가능
 - CAPA를 사용한 결과이며, `strings` 명령어를 통해서도 확인할 수 있다.

```
contains PDB path
namespace executable/pe/pdb
author moritz.raabe@mandiant.com
scope file
regex: /:\\.*/.pdb/
- "C:\\Users\\hyuunnnn\\Downloads\\hidden-tear-master\\hidden-tear-master\\hidden-tear\\hidden-tear\\obj\\Debug\\hidden-tear.pdb" @ file+0x1AAD8
```

```
lSystem.Resources.ResourceReader, mscorelib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet
PADPAPD
RSDS[
C:\Users\hyuunnnn\Downloads\hidden-tear-master\hidden-tear-master\hidden-tear\hidden-tear\obj\Debug\hidden-tear.pdb
_CorExeMain
mscoree.dll
```

¹ Visual Studio 디버거에서 기호 파일(.pdb) 및 소스 파일 지정(C#, C++, Visual Basic, F#)

² <https://www.mandiant.com/resources/blog/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware>

Rich header^{1 2}

- todo

¹ Rich Headers: leveraging this mysterious artifact of the PE format

² The devil's in the Rich header

yara

yara

awesome-yara

<https://github.com/Neo23x0/Loki>

<https://github.com/DissectMalware/yaradb-g-backend>

<https://github.com/DissectMalware/yaradb-g-frontend>

<https://ieeexplore.ieee.org/document/9289501>

<https://youtu.be/fu71CljrxsU>

yara

- 구글이 인수한 `virustotal`에서 만든 유사도 탐지 도구
- 텍스트 또는 패턴을 기반으로 악성코드를 식별하고 분류하기 위해 만들었다고 한다.

```
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        threat_level = 3
        in_the_wild = true

    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"

    condition:
        $a or $b or $c
}
```

- `strings`에서 제작한 rule을 기반으로 `condition` 영역에 탐지 조건을 정의한다.

¹ <https://virustotal.github.io/yara/>

yara

```
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        threat_level = 3
        in_the_wild = true

    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"

    condition:
        $a or $b or $c
}
```

- `meta` : rule에 대한 설명, 언제 만들었는지, 제작자 이름 등을 적는 공간이다.
- `strings` : 탐지해야 하는 데이터를 정의하는 공간이다.
- `condition` : `strings`에서 정의한 rule들의 탐지 조건을 정의하는 공간이다.

yara

rule 옵션	설명
wide	문자가 2바이트로 인코딩된 문자열을 검색할 때 사용
ascii	todo
nocase	todo
fullword	todo

yara

- 왜 유사도 분석 쪽에서 사용되는 걸까?
 - [Virustotal Intelligence \(VTI\)](#)라는 시스템에서 yara rule을 활용하여 `virustotal`에 업로드된 파일들을 실시간으로 탐지할 수 있다.
 - 이전에 만들었던 rule에 탐지된 파일이 새로운 악성코드인지, 재사용되는 코드는 없는지 등 분석¹
 - 유사도 분야의 일을 하는 회사라면 대부분 `virustotal`을 사용하며, rule 또한 SNS, Github 등에서 매우 활발하게 공유되고 있다. - [awesome-yara](#)
 - 분석 리포트, 블로그 등에도 yara rule을 올려주는 경우도 많다.²

[Introduction to YARA - OALabs](#)

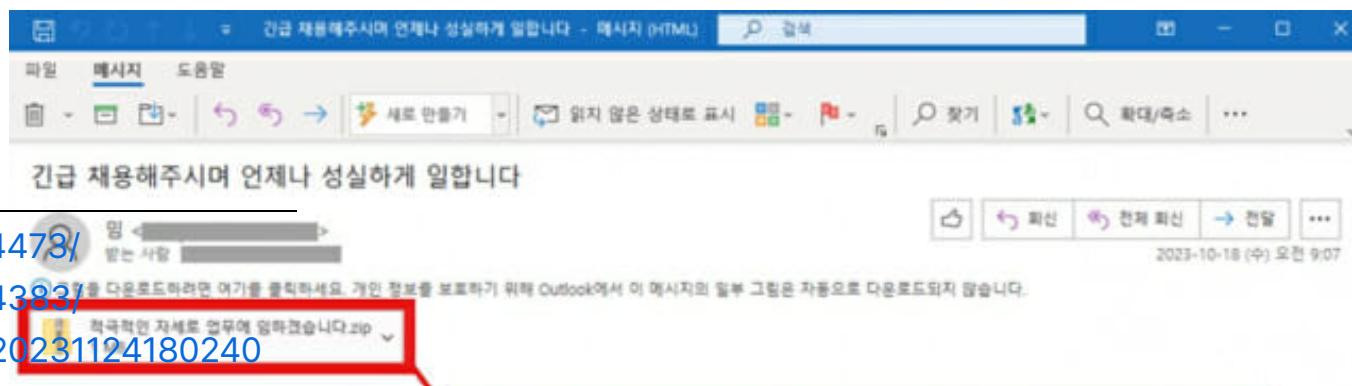
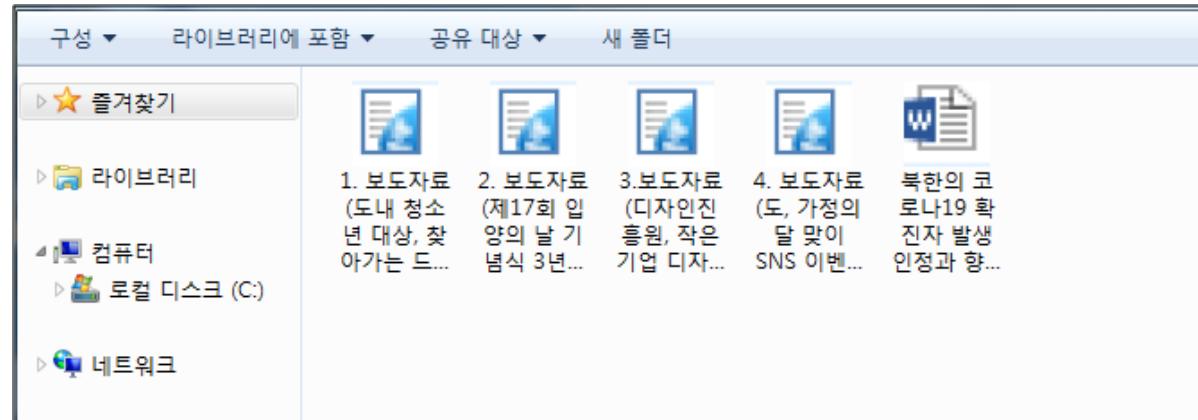
¹ <https://intezer.com/blog/threat-hunting/turning-open-source-against-malware/>

² [HIDDEN COBRA – North Korean Remote Administration Tool: FALLCHILL](#)

정상파일 위치 - 아이콘, 확장자 수정

이름	원본 크기	압축 크기	압축률	종류	수정한 날짜
readme.txt	95	96	-1%	텍스트 문서	2023-06-15 오전 9:38
개인정보유출내역.zip	82,320	81,675	1%	ZIP 파일	2023-06-15 오전 10:07

이름	원본 크기	압축 크기	압축률	종류	수정한 날짜
개인정보유출내역.hwp	...	299,520	81,624	73% 응용 프로그램	2023-06-15 오전 10:02



¹ <https://asec.ahnlab.com/ko/54473/>

² <https://asec.ahnlab.com/ko/34383/>

³ <https://znet.co.kr/view/?no=20231124180240>

- Magniber , Hermes , GandCrab 랜섬웨어가 유사하다는 사례가 있다.¹



Kay Kyoung-ju Kwak

@kjkwak12

...

#Matrix, #Magniber, #Hermes, #GlobeImposter, #GandCrab use exactly same icons, similar loader and decryption algorithm.

Below is yararule to detect some of icons

pastebin.com/fXjgs39A

Any feedback welcome.

DeepL로 번역 ⚙

게시물 번역하기

0AA2B07C743DF99246A1A0C068...	0AC758D0E65C3B3E13B1D5EF475...	0ADD59B2AA11F5C7863DC0A368...	0AEDA9B5709BD21460CEA52353...
0AFC1D09E8D8812847DEFE212B8...	0B1AB78C01D5705956DE9E9E97F...	0B3E2C54516553A2B2F92D4055A...	0B50731FAED2020C1987C93A8B2...
0BAC7387B68DEBD6E2322985352...	0BD060C28955F9AA73848881EA1...	0BF814FDEEC0A91222806888413...	0C8DDF3FFB34FD8D7406B0822E...
0CA17828E917C357A9878528692...	0C786148924948B68AC8ABA8C7...	0CD3AAC4948F1638F5BFEEA482C...	0CD581E4ADD1F26B06406A8AF...
0CDFB347DA5883435D28E28D79...	0D03D8FD85122C7E54CF598ECD...	0D61B1A97C8AD401CCD9719087...	0D282F3A041173F0CE9E7F31D51...
0DA17F7A6103078FDCB826AF66...	0DC5421DA605C917D073C6EC81...	0DE0E085728370A6B298EA53E3EB...	0E260122E91CC995086FF54508...
0E69866174BC8C0F0D92838F872...	0E592792068872A36868A1C1C36...	0EC7E0B859489257D43A21021E8A...	0EF1F26F35DDD50AAE83F412777...
0FOF02DDF2DF8DE6258954E972...	0F3FB53DA8381A58CAA526808FF...	0F4A699E555E0DF97388945321D...	0F88FE21AA99E58E744E84183362...
0FD1133BE84A4CCCCB8CA401416...	0FE477DAE2491C08888951BCA68...	0FF7CF52F315D36759E144D3FC9...	1A4E57D98C8C383929E1E6D0E45...
1A3146D80871AF6CD637898F8E1...	1A9509A49F57DC0812FCAF3F2F5...	1AC09D5884FCDF039FE850A7E4...	1ACC82D681BFF883076FC2C88FB...
1AD0EAA20942A28F45071B9828E...	1AE2EB46C40BAE6A5C4A6CCE77...	1AE9155C07066428C226035ABC9...	1AE861F902C86D058AA838F87D...
182F5DBBE559FCB3A6A524D13...	1B69C44E43F2605843F36518ABC...	1B891E68CD236885F069A84E1116...	1B14476E43578CAEFB274627FA...
1B1879472ABCBD0529877094C...	1B8252A673E8BBF2940DEE370DB...	1BBB7B990F20DAC43CA39C09CA...	1BDBAE8600383CE9313ABFE46F...
1B843E1937911586435F690886C...	1C8F59222F28F9AACCE95C9F6DF9...	1C988AB20F0E63E98C8510F1107...	1C608FA84C83E178CFEC8744C4...
1C84F1C1C9276604A0DD723069...	1C1498A4F6658D4798A7800CD2...	1C4845840A4E2984C78D463C0C...	1CA50EABD77D880298A3862148...
1CDC8C94F6758116002A5A650D...	1CF32C65E212F0A109776E545AF...	1D2EE78D9F2DA29CD5E17A299A...	1D642C94A970F883C13B0DADD7...
1DC9C6BA3387CEBD48558F3A5F...	1E82184C8C39D14F98EB258075D...	1E505795291F2AE647CC97D88A8...	1EEDFDA42538E04FCE341AC5F98...
1F28435840B895AC441FFBD9E75...	1F6F7C27892902D1E9E48E1853F0...	1F064C3F670388536720E988832...	1F735C5822B971F721D9A445CF7...
1F851DF370A007E253C21DC87D...	1O2AF91983763048208868C3A80E...	02B67F98AB0A0C8652781A4F01...	02C7600DD7390896BCEBF836189...
2A30058683729E8729B548D5E4C...	2AA29ECC2C9D71E6D3305EC508...	2A531E626DFF9E09474CC46FAB5...	2AA162135E4E69E3F1CB0C6C22E...
2A46C86BA487A8902D0D78E449...	2B0A006F6A8DED4086B51C06857...	2B2DACC55DD8BA2EEFC585F8ED...	2B92C2F5E7364F1EF4B51005A671...
2B2F4A2C37A24FFB0C8C1F1BC55...	2B10E2B86D8D3F6CFA58FF9F987...	2B9467DD63F3D79339A77EB879...	

¹ <https://twitter.com/kjkwak12/status/980708057037467648>

yara

- todo

¹ <https://ahnlabasec.tistory.com/1124>

² 국내를 타깃으로 하는 위협그룹 프로파일링 - 2017 사이버 위협 인텔리전스 보고서

- GTFOBins , LOLBAS

<https://github.com/JPCERTCC/jpcert-yara>

시스템에 있는 기본 도구를 사용하는 공격자들을 'living off the land'라고 한다.

대상 운영체제에 포함된 도구에 대해 철저하고 정통한 지식을 갖고 있으면
공격자는 자신의 도구를 모두 가지고 다닐 필요 없이 '가벼운 여행'을 할 수 있다.

net.exe 명령어의 사용을 통해 시스템에 사용자 계정이 추가됐다는 점은
공격자가 획득한 접근 수준과 사용한 방법을 알려준다.

사용자 프로파일의 shellbag 아티팩트를 조사한 결과
사용자를 추가하기 위해 제어판에 액세스한 적이 있음을 알게 되면
터미널 서비스를 통해 GUI 셸과 상호작용할 수 있는 셸 기반 액세스 권한이 있음을 알 수 있다.

[Windows 환경에서 침해 시스템 분석하기 - p160, Eng](#)

악성코드 샘플

[awesome-malware-analysis](#), [theZoo](#), malware samples & writeup - 1 2 3 4 5 6 7 8 9,

[Ultimate-RAT-Collection](#), [malware-traffic-analysis](#), [hybrid-analysis](#), [virusshare](#), [vx-underground](#)

[malware-study](#), [malware-tools](#), [Reverse Engineering tools](#), [Reverse-Engineering](#),
[reverseengineering-reading-list](#)

[exploitation-course](#), [레드팀 플레이북](#), [Win32_Offensive_Cheatsheet](#)

[linux-re-101](#), [osx-re-101](#), [RE-iOS-Apps](#), [AndroidAppRE](#)

참고자료

멀웨어 데이터 과학

악성코드 분석 시작하기

국내를 타깃으로 하는 위협그룹 프로파일링 - 2017 사이버 위협 인텔리전스 보고서

악성코드 중심의 침해대응 매트릭스 모델링 - 2019 인텔리전스 보고서