악성코드 및 패커 탐지를 이용한 공격 그룹 판별

Identification of Attack Group using Malware and Packer Detection

저자 (Authors)

문해은, 성준영, 이현식, 장경익, 곽기용, 우상태

Heaeun Moon, Joonyoung Sung, Hyunsik Lee, Gyeongik Jang, Kiyong Kwak, Sangtae Woo

출처 (Source)

정보과학회논문지 45(2), 2018.2, 106-112 (7 pages)

Journal of KIISE 45(2), 2018.2, 106-112 (7 pages)

발행처 (Publisher)

한국정보과학회

KOREA INFORMATION SCIENCE SOCIETY

URL

http://www.dbpia.co.kr/Article/NODE07367765

APA Style

문해은, 성준영, 이현식, 장경익, 곽기용, 우상태 (2018). 악성코드 및 패커 탐지를 이용한 공격 그룹 판별. 정보과학회논문지, 45(2), 106-112.

ISSN 2383-630X(Print) / ISSN 2383-6296(Online)
Journal of KIISE, Vol. 45, No. 2, pp. 106-112, 2018. 2
https://doi.org/10.5626/JOK.2018.45.2.106

악성코드 및 패커 탐지를 이용한 공격 그룹 판별

(Identification of Attack Group using Malware and Packer Detection)

문 해 은 [†] (Heaeun Moon)
성 준 영 [††] (Joonyoung Sung)
이 현 식 [†††] (Hyunsik Lee)
장 경 익 [††††] (Gyeongik Jang)
곽 기 용 [††††] (Kiyong Kwak)
우 상 태 [†††††] (Sangtae Woo)

요 약 최근 악성코드를 이용한 사이버 공격이 급증하고 있다. 피해가 늘어남에 따라 수 년간 다양한 방식의 악성코드 탐지 기법들이 연구되고 있으며, 최근 공격 그룹 판별을 위한 다양한 프로파일링 등장하고 있다. 본 논문은 악성코드 탐지가 아닌 특정 악성코드를 사용하는 공격 그룹에 대한 판별을 주목적으로 하며, 판별에 각 공격 그룹이 사용하는 악성코드에 대한 문자열 및 코드 시그니처를 이용한다. 탐지 기법을 구현하기 위해 야라(Yara)를 사용하였으며, 공격 그룹에서 주로 사용되는 원격 관리 도구(RAT, Remote Access Tool)를 대상으로 연구를 진행했다. 또한 탐지율 증가를 위하여 악성코드 패킹 여부 확인 및 해제 기술을 추가하였다. 본 논문은 최근 공격 그룹들이 주로 사용하는 원격 관리 도구를 대상으로 악성코드와 패커의 주요 특징 시그니처를 이용해 룰셋(Ruleset)을 작성하고 작성한 룰셋을 기반으로 원격 관리 도구 탐지 및 공격 그룹 판별 가능성에 대해 다룬다.

키워드: 원격 관리 도구, RAT, 패커, 야라, 코드 시그니처, 탐지

Abstract Recently, the number of cyber attacks using malicious code has increased. Various types of malicious code detection techniques have been researched for several years as the damage has increased. In recent years, profiling techniques have been used to identify attack groups. This paper focuses on the identification of attack groups using a detection technique that does not involve malicious code detection. The attacker is identified by using a string or a code signature of the malicious code. In addition, the detection rate is increased by adding a technique to confirm the packing file. We use Yara as a detection technique. We have research about RAT (remote access tool) that is mainly used in attack groups. Further, this paper develops a ruleset using malicious code and packer main feature signatures for RAT which is mainly used by the attack groups. It is possible to detect the attacker by detecting RAT based on the newly created ruleset.

Keywords: remote access tool, RAT, packer, yara, code signature, detection

· 이 논문은 2017년 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(No. 2016-0-00081, 악성코드 全 생명주기 통합 프로파일링 및 공격그룹 식별 기술 개발)
· 이 논문은 2017 한국컴퓨터종합학술대회에서 '코드 시그니처를 이용한 악성코드 및 패커 탐지'의 제목으로 발표된 논문을 확장한 것임

† 비 회 원 : NSHC RedAlert 팀장
hemoon@nshc.net
†† 비 회 원 : NSHC 커뮤니티 이사
jysung@nshc.net
††† 정 회 원 : NSHC RedAlert 연구원(NSHC)
hslee@nshc.net
(Corresponding author임)
†††† 비 회 원 : NSHC RedAlert 연구원
kijang@nshc.net
kykwak@nshc.net
††††† 비 회 원 : NSHC 컨설팅 연구원
stwoo@nshc.net

논문접수 : 2017년 8월 21일
(Received 21 August 2017)
논문수정 : 2017년 11월 9일
(Revised 9 November 2017)
심사완료 : 2017년 11월 21일
(Accepted 21 November 2017)

정보과학회논문지 제45권 제2호(2018. 2)

1. 서 론

최근 많은 공격 그룹들은 맞춤형 악성코드를 개발하기보단 기존 악성코드를 위·변조하여 가공하는 방식을 사용한다. 수많은 공격 그룹이 동일 원격 관리 도구를 사용하여 악성코드를 생성한 후 가공하는 방식을 사용하기 때문에 방어자는 공격 주체를 특정 APT 공격 그룹으로 한정하는데 어려움을 겪는다[1]. 본 연구에서는 공격 그룹 판별을 위해 원격 관리 도구의 시그니처를 사용한다. 대상이 되는 원격 관리 도구의 모듈들은 C&C 서버 주소, 기능 활성화 및 비활성화에 따라 해시(Hash)값이 변하기 때문에 행위 기반의 탐지가 필요하며, 모듈 내에 존재하는 데이터를 야라에 적용해 탐지하고자 한다.

1.1 원격 관리 도구(RAT, Remote Access Tool)

RAT는 많은 공격자들이 사용하는 도구로 대상 시스템을 감염시킨 후 원격에서 제어하기 위해 사용된다. 감염을 위해 모듈(Module)을 생성하며, 모듈이 시스템에서 실행되면 공격자는 대상 시스템을 원격에서 제어할 수 있게 된다. 대표적인 RAT 도구로는 프랑스에서 크게 이슈가 되었던 다크코멧(DarkComet)이 존재하며, 싱가포르에서 JAR 파일 형태로 활동하며 윈도우(Windows), 리눅스(Linux), macOS, 안드로이드(Android)를 지원하는 Adwind RAT가 있다. 이뿐만 아니라 Black Shades, JSpy, Pussy, Bozok, Poison, njRAT, DameWare 등등 많은 RAT 도구들이 존재한다. 이러한 RAT 도구들은 공통으로 원격 접속 환경을 만들어 주는 모듈을 생성하며 설정한 URL에서 파일을 내려받는 다운로더(Downloader) 또한 생성 가능하다. RAT는 감염된 사용자의 PC 정보를 간편하게 확인할 수 있으며 모니터링과 키로거와 같은 정보 탈취 기능을 가지고 있는 경우가 대부분이다. RAT는 사용하기 편리한 인터페이스를 제공하는 만큼 능숙하지 않은 공격자도 쉽게 공격에 사용할 수 있다. 보통 RAT에서 생성된 모듈들은 이메일에 첨부하여 전송되거나 웹 사이트의 취약점을 이용해 드라이브 바이 다운로드(Drive By Download, DBD) 공격으로 사용자들을 감염시킨다.

1.2 패커(Packer)

패커는 실행 파일을 압축하여 용량을 줄이는 데 사용되지만 악성코드에선 실행 파일의 용량을 줄일 뿐만 아니라 파일 내부의 코드와 리소스를 감추기 위해 사용된다. 일반적으로 패커는 프로그램이 악의적으로 수정되는 것을 막기 위한 목적을 갖지만 분석가 입장에서의 패커는 악성코드의 리소스 및 코드를 보호하는 기법이다. 패킹된 악성코드를 실행할 경우 패킹된 코드가 해제되면서 메모리에 로드 된다. 이는 실행에 아무런 지장을 주지 않지만 분석을 위한 파일의 원본 코드 확인은 어렵게 된다.

1.3 야라(Yara)

야라는 문자열이나 시그니처 패턴을 기반으로 악성코드를 검색하여 분류할 수 있는 도구다. 이는 C 언어 또는 파이썬(Python) 언어와 비슷한 문법을 사용하기 때문에 룰셋(Ruleset) 작성이 쉽다. 야라는 윈도우, 리눅스, macOS 등 다양한 시스템에서 지원하며 직접 소스코드를 컴파일 하거나 실행 파일을 사용해 설치할 수 있다. 야라는 파이썬 모듈을 지원하기 때문에 이를 이용한 고도화 작업이 가능하다. 야라의 룰셋은 '설명', '룰셋명', '문자열', '참/거짓 판단 조건'으로 나뉘어 정의되며, 파일 분류 시 단순한 문자열이나 시그니처 패턴뿐만이 아닌 대상 파일 엔트리 포인트(Entry Point) 값 지정, 파일 오프셋(File Offset), 가상 메모리 주소(Virtual Memory Address)를 지정할 수 있다. 야라 작성 시 정규표현식을 함께 사용할 경우 더욱 효율적인 패턴 작성이 가능하다.

1.4 가상 머신(Virtual machine, VM)

가상 머신은 컴퓨팅 환경을 소프트웨어로 구현한 것으로, 컴퓨터를 애뮬레이션 하는 소프트웨어다. 이는 가상 머신 내부에 운영 체제 또는 응용 프로그램을 설치 및 실행할 수 있는 환경을 제공한다. 가상 머신은 가상 머신 응용소프트웨어, 하드웨어 가상 머신 소프트웨어, 운영 체제 수준의 가상화 소프트웨어로 나뉘며 연구 진행 중 사용되는 가상 머신은 하드웨어 가상 머신 소프트웨어이다. 하드웨어 가상 머신 소프트웨어에는 대표적으로 VMware, 버추얼박스(Virtual Box), 페러렐즈(Parallels), QEMU 등이 있으며, 이들 중 연구에는 버추얼박스를 사용했다. 버추얼박스는 현재 오라클에서 개발 중인 소프트웨어로 클로즈드(closed) 버전과 오픈 소스 버전이 존재한다. 버추얼박스는 VBoxmanage 명령어를 통해 기능 제어가 가능하기 때문에 자동화 작업을 수행하는데 좀 더 편리하다. 패킹된 악성코드는 메모리 로드 시 패킹 해제 코드를 실행하기 때문에 본 연구에서는 패킹 해제된 악성코드 메모리 덤프 파일을 얻기 위해 가상 머신 환경을 이용하였다.

1.5 메모리 포렌식(Memory Forensic)

메모리 포렌식은 APT(Advanced Persistent Threat) 공격 또는 악성코드(Malware, Malicious Software)로 인한 침해 사고에서 공격당한 PC의 중요한 데이터를 확인하는데 핵심적인 역할을 한다. 메모리 포렌식은 여러 가지 포렌식 소프트웨어를 이용해 물리적인 램(RAM)을 분석하는 일련의 과정이며 분석 대상인 램은 메모리의 한 종류로 컴퓨터 시스템 중앙처리장치(CPU, Central Processing Unit)에 의한 소프트웨어 연산 결

과 데이터 및 코드를 적재하는 장소이다. 컴퓨터 시스템의 특성 상 중앙처리장치에서 연산을 처리하기 때문에 메모리에는 하드디스크에 저장되는 정보와 다른 유형의 값들이 저장되며, 주로 소프트웨어 및 파일의 실행 과정 또는 실행 시 사용되었던 특징적인 정보가 존재한다. 메모리 포렌식을 통해 프로세스 및 쓰레드 정보, 모듈 및 라이브러리 정보, 실행된 파일 및 소켓 정보를 포함하는 다양한 데이터 구조 정보를 획득할 수 있다. 메모리 포렌식에 사용되는 도구는 각각 다른 특징과 장점을 가지며 사용되는 도구로는 Win(32/64)dd.exe와 Dumplt.exe, FTK Imager Lite, 볼라틸리티(Volatility), 보라폭스(Volafox)가 있다. 해당 연구에서는 메모리 포렌식을 위해 볼라틸리티를 사용하였다.

2. RAT 및 패커 특징 분석 및 기술

다양한 종류의 RAT 중 다크코멧(DarkComet), njRAT, 판도라(Pandora)를 대상으로 연구를 진행하였으며 각 RAT에서 주로 사용하는 패커인 UPX, FSG, MPRESS의 특징을 분석하였다. 각 패커의 패킹 기술을 해제하기 위해 메모리 포렌식 기술을 사용하였으며 이 장에서는 패킹이 해제된 파일을 획득하기 위해 사용한 기술에 대해 정리한다.

2.1 RAT 특징 분석

RAT 도구는 일반적으로 다운로더(Downloader) 생성 기능을 제공하며 실행 시 사용할 뮤텍스 명 설정, 감염 시스템의 키로그를 탈취하기 위한 키로거, 다양한 플러그인, 정상 프로그램으로 위장하기 위한 아이콘 이미지 변경, 안티 바이러스 프로그램 우회 등 다양한 기능을 제공한다. RAT에서 가장 기본적으로 사용되는 모듈 생성 기능을 파악하기 위해서 다크코멧의 빠른 모듈 생성(Minimalist(Quick)) 탭을 확인하였으며 다음은 해당 탭의 화면 구성이다. 설정을 통해 감염 시스템에서 실행될 모듈(실행 파일) 명을 지정 할 수 있으며, 감염 PC ID, 감염 시 연결될 IP 주소, 포트 번호, 설치 될 장소, 실행 파일 아이콘을 지정할 수 있다(그림 1).

RAT는 모듈 생성 기능 외 감염 시스템 모니터링 기능 등의 폭 넓은 기능을 제공한다. 연구 대상 중 njRAT는 닷넷(.NET) 기반의 RAT로 S.K.Y.P.E/Tagged 그룹에서 주로 사용하는 도구로 유명하다.

2.2 패커 특징 분석

본 연구에서 수집한 RAT는 주로 UPX, FSG, MPRESS와 같이 상용화된 패커를 사용한다. 이러한 패커들은 고유한 시그니처를 가지고 있으며 각 패커 별로 언패킹을 위한 코드를 가지고 있다. UPX 패커로 패킹된 파일에는 패커가 생성한 섹션인 UPX0, UPX1이 존재하며, 다음과 같은 정적 데이터를 확인할 수 있다(그림 1).

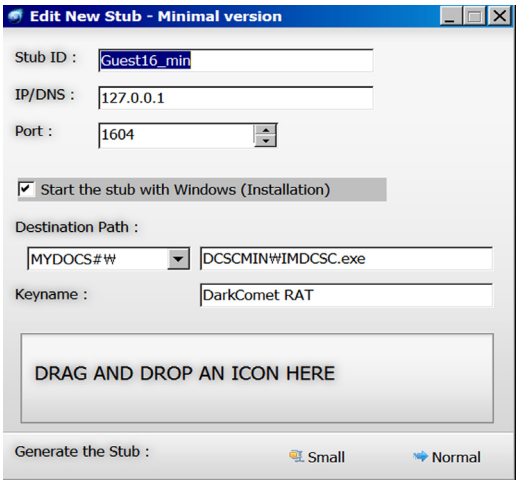

그림 1 다크코멧 모듈 빌더 화면 구성
Fig. 1 Darkcomet Module builder configuration

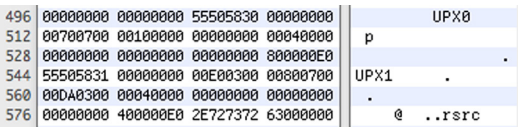

그림 2 UPX 패커 탐지 시 사용될 수 있는 데이터
Fig. 2 UPX packer detection data

2.3 탐지에 활용되는 데이터

패킹되지 않은 RAT에서 생성한 모듈을 분석하면 고유한 문자열과 코드 시그니처를 확인할 수 있다. 각각 모듈에서 다음과 같은 데이터를 확인할 수 있다(표 1).

또한, 패킹된 RAT 실행 파일에서 아래와 같이 각 패커와 관련된 시그니처와 문자열 데이터를 확인할 수 있다(표 2).

이렇게 추출한 데이터를 이용하여 각 RAT에 대한 야라 룰셋을 작성하고 탐지 시스템에 적용할 수 있다. 야라 룰셋이 적용된 탐지 시스템은 룰셋에 해당하는 파일을 검색하여 탐지된 파일이 매칭되는 RAT 룰셋명을 확인할 수 있고 그에 따른 RAT 종류를 확인할 수 있다.

표 1 모듈에서 사용할 수 있는 데이터
Table 1 Detection data in the module

DarkComet	[ESC], [<-], [NUM_LOCK], [DEL], [INS], [SNAPSHOT], [LEFT], [RIGHT], [DOWN], [UP], …
njRAT	{6e 00 65 00 74 00 73 00 68 00 20 00 66 00 69 00 72 00 65 00 77 00 61 00 6c 00 6c 00 20 00 64 00 65 00 6c 00 65 00 74 00 65 00 20 00 61 00 6c 00 6c 00 6f 00 77 00 65 00 64 00 70 00 72 00 6f 00 67 00 72 00 61 00 6d 00}
Pandora	{00 00 48 69 64 69 6e 67 20 64 65 73 6b 74 6f 70 20 69 63 6f 6e 73 2e 2e 2e 00}

표 2 패킹된 모듈을 탐지할 때 사용되는 데이터
Table 2 Data used detect to the packed module

UPX	UPX0, UPX1, UPX!, {57 FF D5 58 61 8D 44 24 80 6A 00 39 C4 75 FA 83 EC 80 E9}
FSG	FSG!, {87 25 ?? ?? ?? ?? 61 94 55 A4 B6 80 FF 13}, {78 F3 75 03 FF 63 0C}
MPRESS	MPRESS1, .MPRESS2, {60 BE 00 [2] 00 8D BE 00 [2] FF [1-12] EB 1? 90 90 90 90 90 [1-3] 8A 06 46 88 07 47 01 DB 75 07 8B 1E 83 EE FC 11 DB 72 ED B8 01}

2.4 볼라틸리티(Volatility) 활용 기술

[2] 볼라틸리티는 다양한 플랫폼과 플러그인을 제공하는 메모리 포렌식 도구로 다음과 같이 여러 프로세스 분석 플러그인을 제공한다(표 3).

표 3 볼라틸리티 플러그인
Table 3 Volatility Plugin Table

Plugin name	contents
pslist	Running process information.
psscan	Running process information and already terminated process information.
psxview	Compares the process information identified by pslist and psscan, and hidden process information.
pstress	Displays information similar to pslist, correlates Parent process and Child process.
procexedump	Extract binaries from the memory area of the process without including empty space(slack space).
volshell	Analyze memory dump files in a command format similar to WinDbg.

위 플러그인 중 pslist, psxview, procexedump는 주로패킹된 파일로부터 원본 코드를 추출할 시 사용된다. psxview를 사용하는 이유는 다른 프로세스 확인 플러그인들과는 다르게 은닉된 프로세스들도 확인할 수 있기 때문이다. 하지만 속도가 pslist에 비해 느리므로 상황에 따라 사용한다. 또한 procexedump(procdump)는 메모리상의 프로세스를 획득할 때 사용된다. 다음은 메모리 포렌식을 이용한 언패킹 과정이다(그림 3).

3. 악성코드 탐지 방법

이 장에서는 악성코드를 탐지하기 위해 사용된 탐지 기법과 탐지 연구 결과에 대해 다룬다.

3.1 탐지 방법

RAT에서 생성되는 모듈은 대부분 PE 파일 구조로

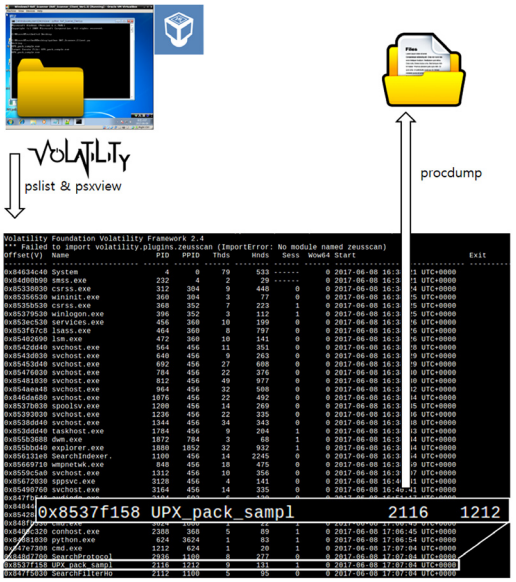

그림 3 메모리포렌식을 이용한 덤프 과정
Fig. 3 Dump process using memory forensics

되어 있다. 텍스트(.text) 섹션에서 각 모듈에서 사용하는 특정 문자열을 확인할 수 있으며 역공학(Reversing Engineering) 과정을 통해 모듈에서 악성 행위와 관련된 코드 시그니처(Code signature)를 추출할 수 있다. RAT는 패커를 지원하는 경우도 있기 때문에 RAT에서 사용하는 패커의 특징을 분석하여 룰셋을 작성한다면 사용된 패커 정보에 대해서도 확인이 가능하다. 패킹된 파일 탐지 시 패킹을 해제한 원본 파일을 추출하고 그에 대한 탐지를 진행한다면 패킹된 파일이더라도 RAT에서 생성된 모듈 여부를 판단할 수 있게 된다. 다음 그림 4는 연구의 전체적인 탐지 흐름도다.

3.2 스트링을 이용한 탐지 기법

스트링 시그니처를 사용한 탐지 기법은 strings 유틸리티를 사용해 흔히 사용되지 않는 문자, 바이너리에서 사용되는 DLL, API 이름을 추출하여 탐지에 사용할 수 있다[3]. 예로 아래 문자열을 들 수 있다(표 4).

위의 문자열은 다크코멧에서 생성된 모듈에서 발견할 수 있는 문자열로 흔히 정상 실행 파일에서는 볼 수 없는 문자열이다.

표 4 탐지에 이용되는 문자열
Table 4 Strings used for detection

Strings info	DCDATA, GENCODE, .dcp, NETDATA, SID, COMBOPATH, netsh firewall delete allowedprogram, ##password##, ##0##0##0##Victim##0##0##0##PAD&

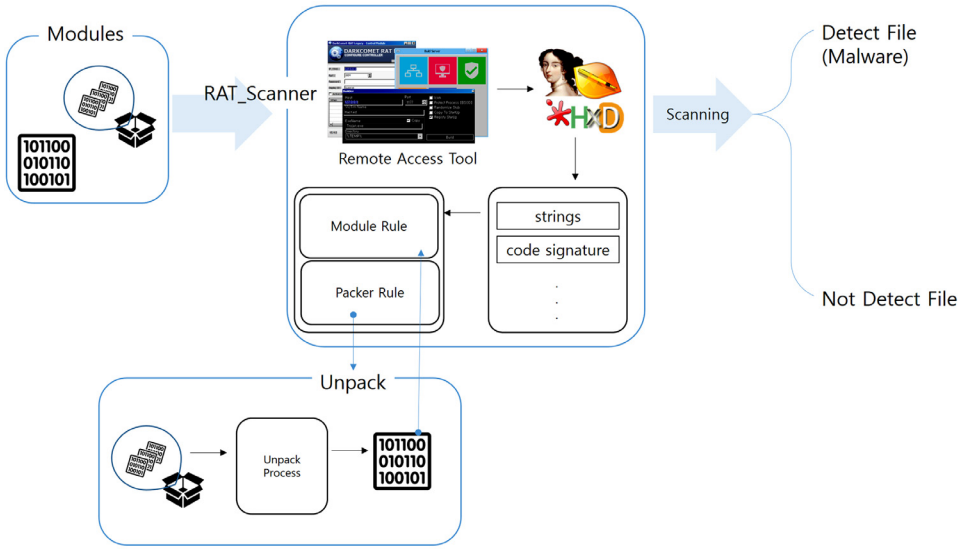

그림 4 탐지 방법
Fig. 4 Detection process

3.3 코드 시그니처를 이용한 탐지 기법

역공학 과정을 통해 각 모듈에서 블록 단위의 코드 시그니처를 획득할 수 있다. 역공학을 통해 패킹 해제 코드 시그니처를 추출하거나 각 모듈의 경고문 생성, 원격 접속과 같은 코드 시그니처를 추출하여 야라 룰셋 작성에 이용할 수 있다. 코드 시그니처 탐지 기법 예시는 그림 5와 같다.

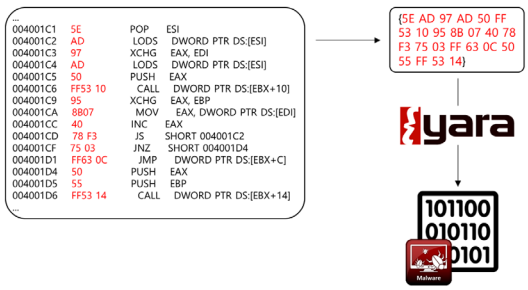

그림 5 코드 시그니처 탐지 예시
Fig. 5 Example of code signature detection

다음과 같은 코드 시그니처는 탐지 기술에도 중요하게 사용될 수 있지만, 공격그룹을 추적할 때 사용될 수 있는 중요 데이터가 된다.

3.4 탐지 기술에 대한 상세 설명

스트링과 코드 시그니처는 야라에서 탐지를 위해 사용되는 데이터로, 야라의 상태(condition) 필드가 추가된다. 본 연구를 진행할 때는 오탐을 줄이기 위해 상태는 모든 조건이 맞을 때 탐지하도록 작성하였으며 탐지 기술의 전체적인 상세 흐름도는 그림 6과 같다.

상세 탐지 흐름도를 보면 메인으로 실행되고 있는 RAT Scanner와 VirtualBox에서 실행되는 RAT Scanner Client가 존재한다. RAT Scanner는 대상 샘플 중에 미리 작성된 룰셋에 해당하는 샘플들을 확인하며, 그중 패킹된 샘플들은 패커 탐지 룰셋을 사용하여 따로 분류한다. 그 후 패커에 대한 분류가 완료되면, 패킹된 샘플들을 RAT Scanner Client에게 전달한다. RAT Scanner Client는 분류 대상인 RAT를 실행하여 가상머신 메모리에 업로드한다. 이후 RAT Scanner는 가상 머신의 메모리에서 패킹이 해제된 실행 파일을 획득하여 RAT 룰셋으로 재 탐지 하는 작업을 실행한다.

3.5 야라를 사용한 탐지 결과

다음은 다크코멧 버전 4와 버전 5에서 제공하는 여러 옵션을 서로 다르게 적용하여 모듈을 생성한 후 탐지 시스템에서 탐지율을 확인한 결과이다. 다음은 패커 탐지 룰셋 적용 전의 탐지율이다(표 5).

다음은 RAT Scanner에 패커에 탐지 룰셋 적용 후

표 5 각 모듈 별 결과 1
Table 5 Results for module 1

	DarkComet	
	Version 4.x	Version 5.x
Create Module	18	25
Detect Module	16	23
Detect rate	88%	92%

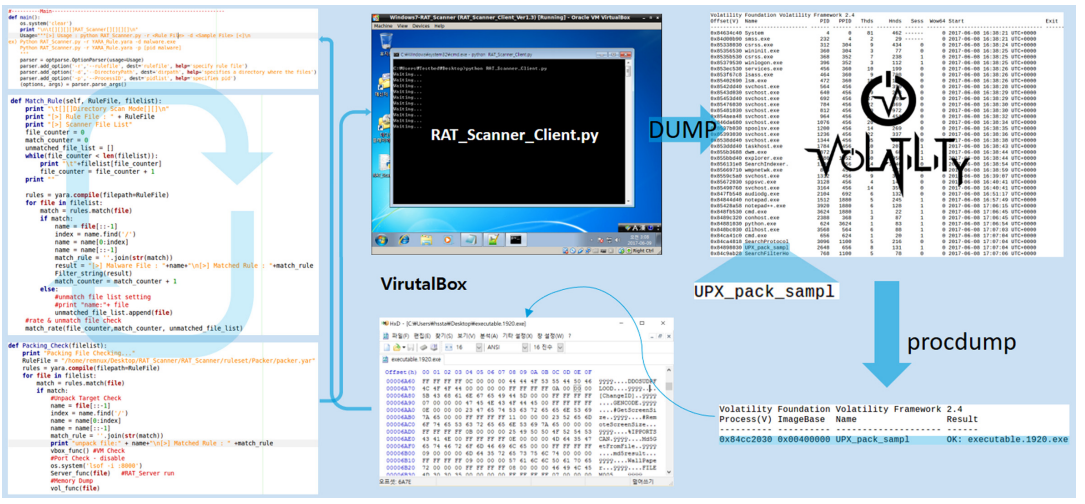

그림 6 상세 탐지 흐름도
Fig. 6 Detailed detection flow

표 6 각 모듈 별 결과
Table 6 Results for module 2

	DarkComet	
	Version 4.x	Version 5.x
Create Module	18	25
Detect Module	18	25
Detect rate	100%	100%

재탐지 코드 사용 시 탐지율은 표 6과 같다.

패킹을 해제하고 재탐지하는 코드를 추가했을 뿐인데 탐지율이 각 88%, 92%에서 100%로 증가한 것을 확인할 수 있다.

4. 결론 및 향후 연구

본 논문은 RAT에서 생성된 모듈을 대상으로 분석하고 분석한 데이터를 기반으로 야라 룰셋을 작성해 악성코드를 탐지하는 기법을 제안하고 있다. 제안하는 방법은 모듈의 중요 코드 시그니처를 잘 정의한다면 아주 적은 오탐율(False Positive Rate)을 가지는 탐지 기법이며 야라 룰셋 작성에 사용된 데이터는 역공학 과정을 통해 쉽게 추출할 수 있어 자동화에도 매우 편리하다.

과거 포이즌 아이비(Poison IVY) 그룹이 PlugX RAT 도구를 사용해 APT 공격을 시도한 사례와 같이 최근 많은 APT 공격 그룹들이 특정 공격 그룹 판별을 우회하기 위해 공격에 원격 관리 도구인 RAT를 많이 사용하고 있다. 공개되어 있는 RAT가 아닌 알려지지 않은 커스텀 RAT(Custom RAT)를 사용한 APT 공격도 다수 존재하지만 이러한 APT 공격은 본 논문에서 다루는 탐지 연구 중 룰셋 고도화 작업을 통해 커스텀 RAT에 대한 사전 탐지가 가능할 것이다. 단, 현재 진행한 연구는 수 많은 RAT 중 일부에 불과하여 야라 룰셋 작성에 사용할 데이터가 부족하며, 알려지지 않은 공격자 및 공격 그룹으로 인한 예외 경의가 발생할 수 있으므로 본 탐지 기법의 탐지율을 증가시키기 위해서 추가적인 RAT 의 특징 분석 및 탐지 룰셋 작성에 대한 고도화 연구가 필요하다.

References

[1] Juan Anres Guerrero-Saade, GReAT, (2015.Nov.17) D. Kaspersky Security Bulletin. Previsioni per il 2016 [Online]. Available: https://securelist.it/kaspersky-security-bulletin-2016-predictions/59176/ (2014. Jan. 31)

[2] Volatility Foundation, "Volatility," [Online]. Available: http://www.volatilityfoundation.org/, (2017.01.03).

[3] Ronghua Tian, Lynn Batten, Rafiqul Islam, Steve Versteeg, "An automated classification system based on the strings of trojan and virus families," *Journal of IEEE : Malicious Unwanted Software (MALWARE)*, pp. 23-30, Oct. 2009. (in Canada)

문 해 은
2002년 영남대학교 정보통신공학 졸업(석사). 2002년 3월~2014년 2월 (주)넷맨 수석연구원/연구소장. 2014년 8월 (주)NSHC Red Alert 팀장. 관심분야는 OS, 소프트웨어 공학, 인공지능, 정보보안

성 준 영

2005년 충북대학교 정보통신공학과 졸업(학사). 2005년~현재 (주)NSHC 이사. 관심분야는 정보보안, 컴퓨터 이론

이 현 식

2008년 강원대학교 컴퓨터정보통신공학과 졸업(학사). 2016년~현재 (주)NSHC Red Alert 연구원, 관심분야는 OS, 컴퓨터 이론, 정보보안

장 경 익

2008년 서울호서전문학교 컴퓨터공학과 졸업(학사). 2012년~현재 (주)NSHC Red Alert 주임 연구원. 관심분야는 OS, 컴퓨터 이론. 관심분야는 OS, 컴퓨터 이론

곽 기 용

2017년 국가평생교육진흥원 컴퓨터 공학 졸업(학사). 2013년 11월~현재 (주)NSHC Red Alert 주임 연구원. 관심분야는 인공지능, 정보보안, 소프트웨어 공학

우 상 태

2004년 충북대학교 정보통신공학과 졸업(학사). 2005년~현재 (주)NSHC 연구원. 관심분야는 정보보안, 유무선네트워크