2020-09

「Tactics, Techniques, Procedures」

【특징정보(Feature) 기반】

TTPs#3 : 공격자의 악성코드 활용 전략 분석

인터넷침해대응센터
KrCERT/CC
KOREA INTERNET SECURITY CENTER

과학기술정보통신부

KISA 한국인터넷진흥원

CONTENTS

집　　필 : 침해사고분석단 종합분석팀
한상원 선임, 김병재 선임,
이재광 팀장

감　　수 : 신대규 본부장, 이동근 단장

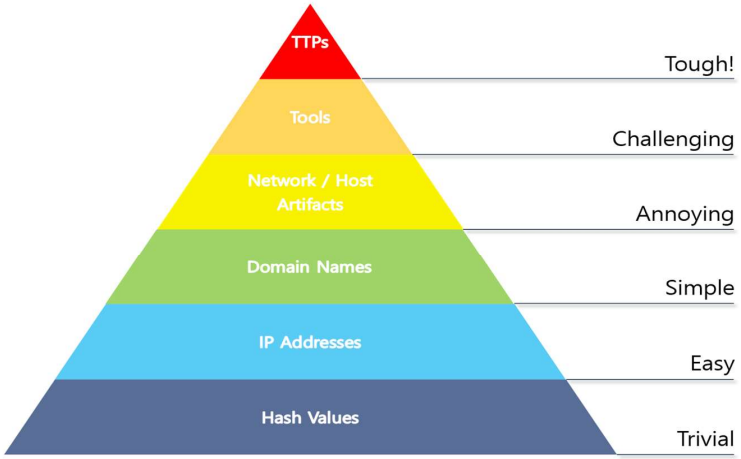
KISC KrCERT/CC KOREA INTERNET SECURITY CENTER

인터넷침해대응센터
KrCERT/CC
KOREA INTERNET SECURITY CENTER

Ⅰ. 서론

o 해킹 사고가 지속 발생함에 따라 보안 요구 사항은 점점 더 까다로워지고 있으며 방어 시스템의 기능은 매우 높은 수준으로 발전하고 있다. 그렇지만, **과거의 침해사고들이 현재에도 여전히 발생하고 있으며, 방어 체계를 잘 갖춘 기업도 전혀 예외가 아니다.**

o 사이버보안에서 유명한 고통의 피라미드(The Pyramid of Pain)는 방어자가 TTP(공격자의 전략과 전술, 그리고 그 과정)를 이해하고 방어 체계를 운영하는 것이 가장 효과적임을 잘 표현하고 있다. **보안은 공격자를 Tough!한 단계로 끌고 가는 것이다.**



각 지표 별 대응 시 공격자가 받는 스트레스, David J Bianco

o 여전히, IoC(Indicator of compromise, 악성IP · 악성 도메인 등 단순 지표) 기반의 방어 체계는 매우 유용하다. 다만, **공격자는 단순 지표와 관련된 공격 인프라를 쉽게 확보하고 버린다.**

o TTP는 다르다. **공격자는 TTP를 쉽게 확보하거나 버릴 수 없다.** 타깃이 정해진 공격자는 타깃의 방어 환경을 무력화하기 위해 많은 시간을 들여서 TTP를 학습하고 연습한다. 그리고, 확보된 TTP를 지속 활용할 수 있는 대상들이 새로운 타깃이 된다.

o 공격자의 TTP는 언제나 방어 환경의 특성과 맞물려 있다. 그래서, 방어자는 방어 환경에 대해 정확히 이해하고 있어야 하며, 공격의 흐름과 과정을 패턴이나 기법이 아닌 전략·전술 관점으로 보아야 한다. **방어자의 환경과 공격자의 TTP는 함께 이야기 되어야 한다.**

o TTP를 이해한 방어자는 2가지를 설명할 수 있어야 한다. '공격자의 TTP가 방어자 환경에 유효한 것인지 여부', '유효하다면 TTP를 무력화할 수 있는 방어 전략은 무엇인지'

o 한국인터넷진흥원(이하 KISA)은 침해사고 대응 과정을 통해 공격자의 TTP를 파악하고 있으며, 그 과정 및 대응방안을 ATT&CK Framework[1] 기반으로 작성하여 배포한다. 보고서에 포함되어 있는 TTP와 관련된 다양한 흔적들(Artifacts)은 TTP에 대한 이해를 돕는 보조 수단일 뿐이다.

1) 실제 공격에 사용된 전술 및 기술과 그에 대한 대응방안을 나타낸 매트릭스

Ⅱ. 개요

o KISA는 2020년 상반기에 수집된 악성코드를 대상으로 특징정보(Feature)를 추출하여 악성코드 별 TTPs를 분석하였고 ATT&CK Matrix 전술별 통계를 도출하였다. 각각의 비율은 전체 악성코드의 TTPs를 추출하여 전술별로 그룹핑을 하고, 각 전술 내에서의 기술사용 빈도를 나타낸 것이다.

< 악성코드 특징정보(Feature) >

악성코드가 각각 가지고 있는 고유의 분석 결과 정보를 뜻하며, 아래와 같은 정보를 포함하고 있다.

- 레지스트리 행위 정보 : 특정 레지스트리 생성 및 변조 행위 정보(Path, name)
- 프로세스 행위 정보 : CMD, Powershell 등을 포함한 프로세스 실행 및 변조 행위 정보(name, parameter)
- 동적 및 정적 분석 정보 : API의 실행 순서, 문자열 정보, 메타데이터 정보 등

o TTPs의 각 전술에는 다양한 기술들이 존재하지만 악성코드가 사용하는 기술들은 각 전술별로 Top3 정도에 밀집되어 있는 것을 알 수 있었다. 방어자는 악성코드에 의해 사용되는 주요 기술들을 파악하고 공격이 완성되는 최종 단계 이전에 악성코드를 탐지하여 무력화 할 수 있도록 노력하는 것이 매우 중요하다.

o TTPs 통계를 기반으로 확인된 가장 일반적인 악성코드 감염 활동은 아래와 같다. 기본적으로 공격자는 서비스와 레지스트리를 이용해 악성코드 실행과 지속성을 유지하며, 악성코드의 피해를 확산시키기 위해 권한을 상승한다. 이후 감염 시스템에서 수집한 내부 정보를 암호화 하고, 네트워크 프로토콜을 이용해 C2와 통신하게 된다.

[악성코드 감염 활동]

Ⅲ. ATT&CK Matrix

Execution
- Service Execution (33.8%)
- Scripting (21.5%)
- Command-Line Interface (18.3%)

Persistence
- Registry Run Keys/ Startup Folder (30.5%)
- Modify Existing Service (25.0%)
- New Service (19.8%)

Privilege Escalation
- Process Injection (78.2%)
- New Service (11.3%)
- Valid Accounts (4.3%)

Defense Evasion
- Obfuscated Files or Information (42.7%)
- Process Injection (31.5%)
- Disabling Security Tools (12.5%)

Credential Access
- Input Capture (83.7%)
- Hooking (10.6%)
- Credentials in Files (3.5%)

Discovery
- Security Software Discovery (32.5%)
- System Information Discovery (31.3%)
- Remote System Discovery (10.5%)

Lateral Movement
- Replication Through Removable Media (64.6%)
- Taint Shared Content (31.3%)
- Exploitation of Remote Services (4.0%)

Collection
- Input Capture (42.2%)
- Clipboard Data (33.6%)
- Data from Local System (15.6%)

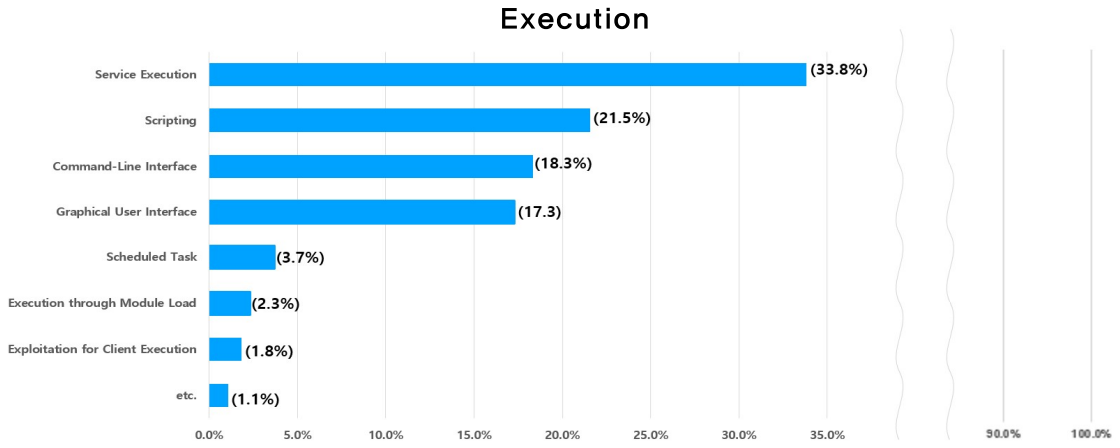
Command and Control
- Standard Cryptographic Protocol (38.3%)
- Standard Application Layer Protocol(24.4%)
- Standard Non-Application Layer Protocol (24.2%)

Exfiltration
- Data Encrypted (94.4%)
- Exfiltration Over Other Network Medium (2.9%)
- Exfiltration Over Command and Control Channel(2.6%)

* 각 기술 별 대응전략은 MITRE 홈페이지에서 제시한 내용을 반영

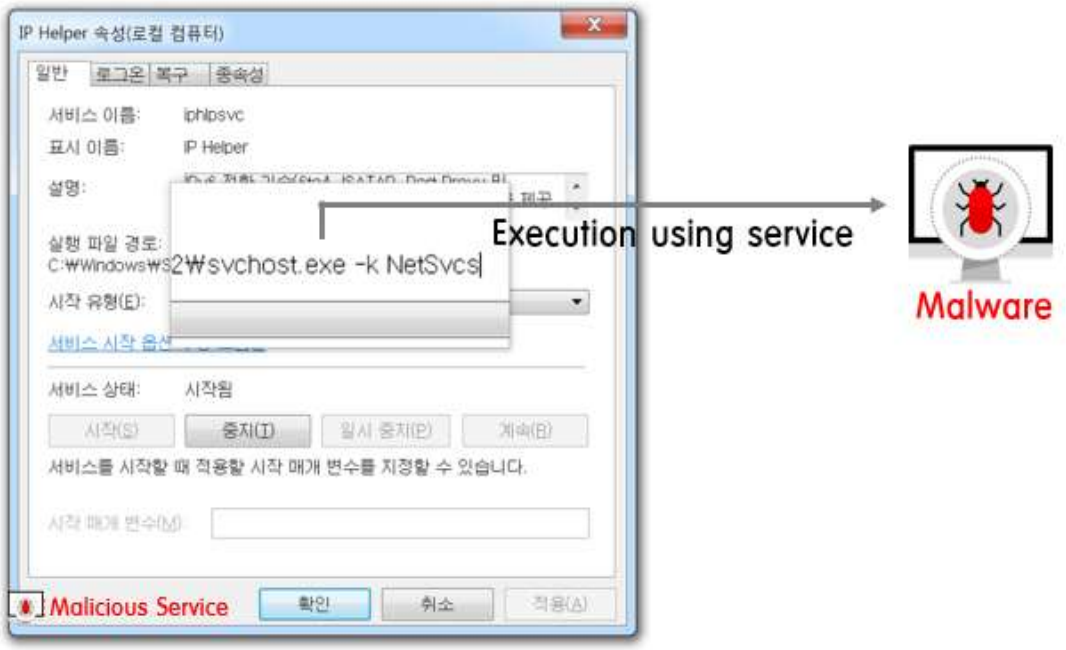
[전술별 기술사용 빈도]

1 Execution : 실행



가. Service Execution(33.8%) : 윈도우 서비스를 통해 악성코드 실행

공격자 또는 사전에 감염된 악성코드는 SC 및 Net 등의 윈도우 명령어를 통해 서비스를 등록 및 실행 할 수 있으며, 서비스 실행 시 실행파일 경로의 악성코드가 실행된다.

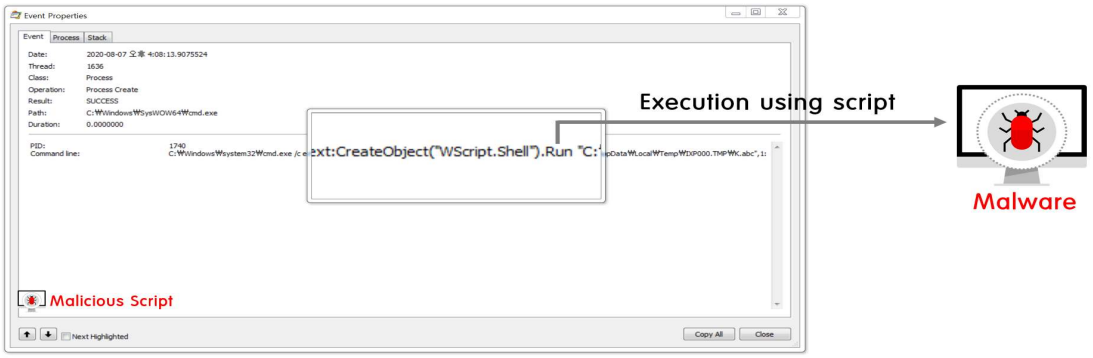


대응 전략	
계정 권한 관리	낮은 권한을 가진 사용자가 더 높은 권한 수준에서 실행되는 서비스를 만들거나 수정 할 수 있는 권한이 있는지 확인한다.
시스템 로그 확인	시스템 로그의 신규 서비스 등록을 모니터링 하여 비정상적인 서비스를 식별한다.

※ 각 기술 별 대응전략은 MITRE 홈페이지에 제시한 내용을 반영

나. Scripting(21.54%) : 스크립트를 통해 악성코드 실행

일반적으로 악성 문서 또는 사전에 감염된 악성코드와 연결된 C2에서 추가적으로 스크립트를 전달받아 실행되며, 스크립트 실행 시 악성코드가 실행된다.

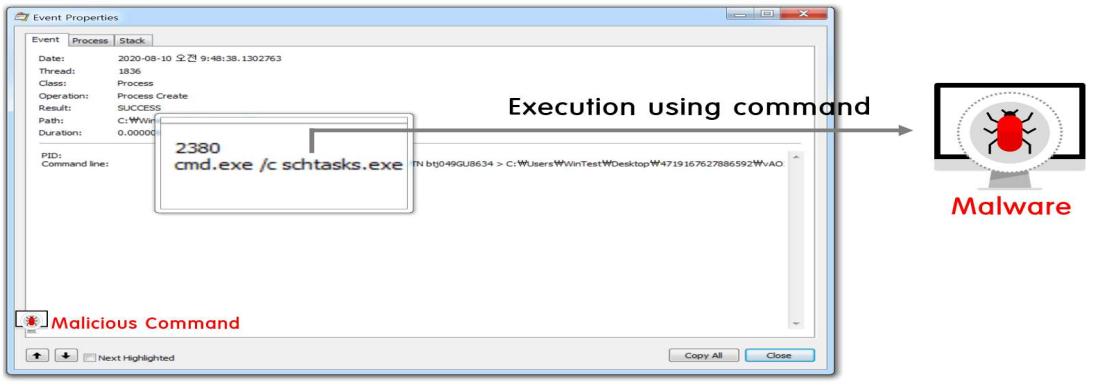


대응 전략	
코드 서명	코드 서명이 된 스크립트의 실행만 허용한다.
권한 있는 계정 관리	PowerShell이 필요한 경우 PowerShell 실행 정책을 관리자로 제한한다.
웹 기반 콘텐츠 제한	스크립트 차단 확장 프로그램을 통해 악성 스크립트 및 HTA 파일의 실행을 방지한다.

※ 각 기술 별 대응전략은 MITRE 홈페이지에 제시한 내용을 반영

다. Command-Line Interface(18.32%) : 콘솔 인터페이스를 사용하여 악성코드 실행

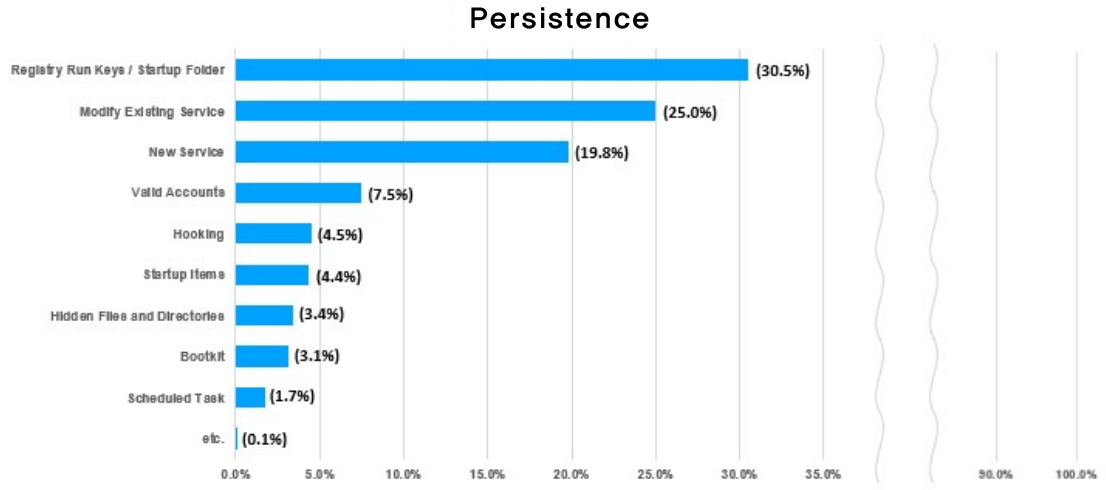
공격자 또는 사전에 감염된 악성코드는 Windows 명령 쉘(cmd.exe)의 "cmd.exe /c" 명령을 이용하여 악성코드를 실행한다.



대응 전략	
안티 바이러스 / 멀웨어	백신을 설치하여 의심스러운 파일 삭제 및 탐지 활성화한다.
명령 실행 비활성화	AppLocker 및 Windows Defender Application Control 등을 통해 불필요한 명령 실행을 차단하거나 소프트웨어 제한 정책을 사용한다.

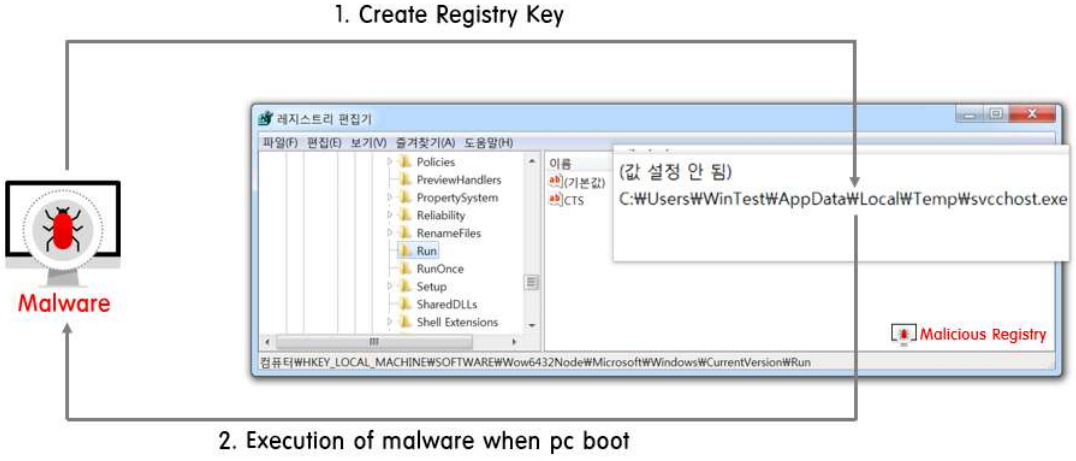
※ 각 기술 별 대응전략은 MITRE 홈페이지에 제시한 내용을 반영

2 Persistence : 지속성 유지



가 Registry Run Keys / Startup Folder(31.4%) : 자동 실행 레지스트리 또는 시작 프로그램 등록

악성코드 실행 시 특정 레지스트리 또는 시작프로그램에 악성코드를 등록하여 PC 부팅시 마다 악성코드가 자동으로 실행되어 지속성을 유지한다.



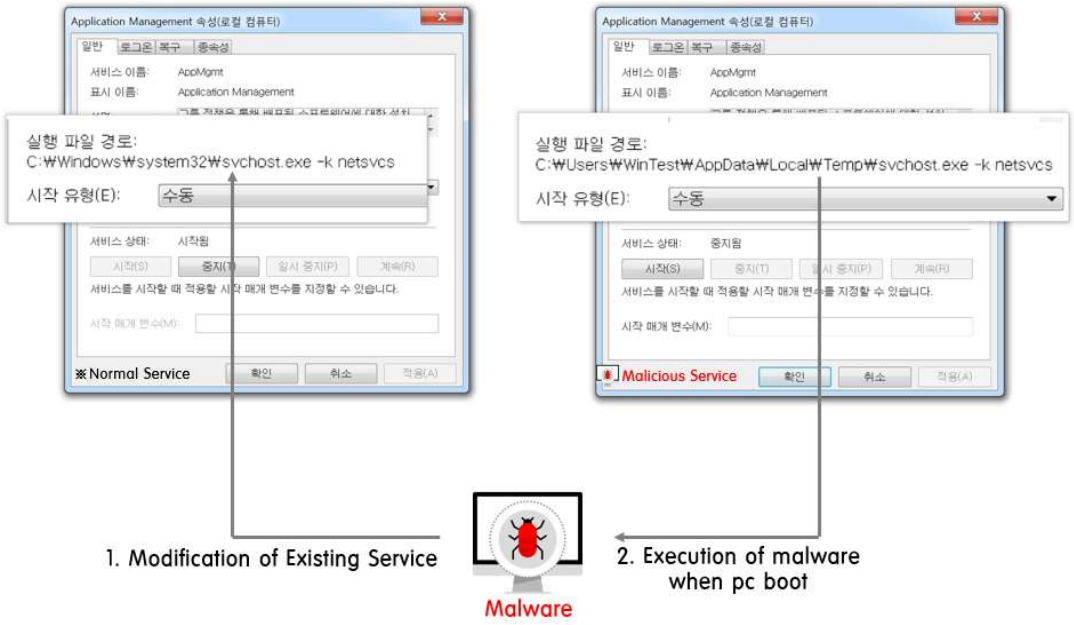
대응 전략

시작 프로그램 폴더 경로 및 시작 프로그램으로 등록된 프로그램의 모니터링이 필요하다.
(C:₩Users₩[유저 명]₩AppData₩Roaming₩Microsoft₩Windows₩Start Menu₩Programs₩Startup₩)

※ 각 기술 별 대응전략은 MITRE 홈페이지에 제시한 내용을 반영

나. Modify Existing Service(25.74%) : 기존 사용 중인 서비스 변조

악성코드 실행 시 기존 윈도우 서비스를 확인 후 레지스트리 변경을 통해 실행 파일 경로의 내용을 변조한다. PC 부팅시마다 변조된 서비스에 의해 악성코드가 실행되어 지속성을 유지한다.

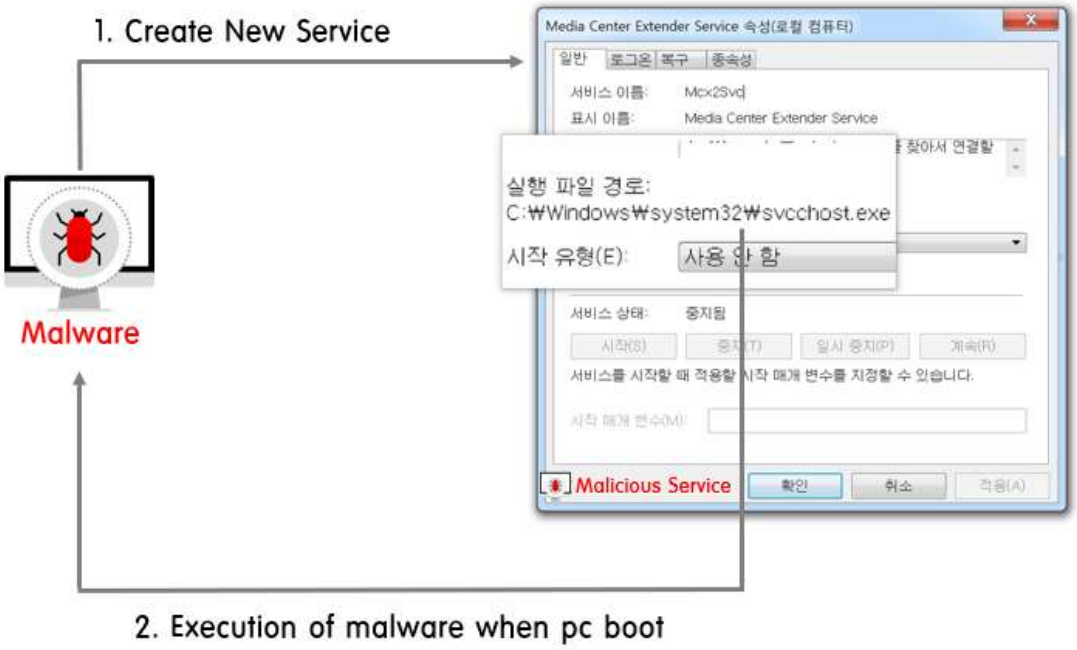


대응 전략	
계정 권한 관리	낮은 권한을 가진 사용자가 더 높은 권한 수준에서 실행되는 서비스를 만들거나 수정 할 수 있는 권한이 있는지 확인한다.
시스템 로그 확인	시스템 로그의 신규 서비스 등록을 모니터링 하여 비정상적인 서비스를 식별한다.

※ 각 기술 별 대응전략은 MITRE 홈페이지에 제시한 내용을 반영

다. New Service(20.39%) : 서비스 생성

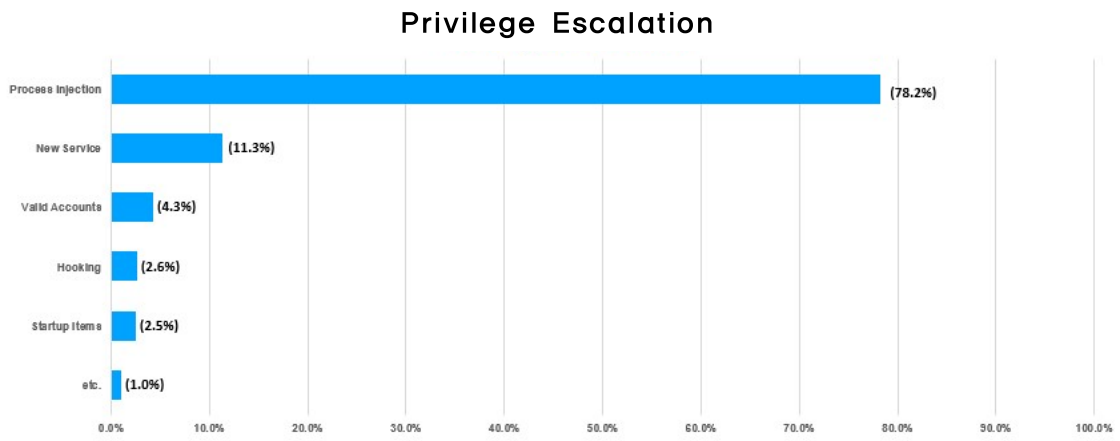
악성코드 실행 시 윈도우 서비스를 신규로 생성하며, PC 부팅시마다 생성된 서비스에 의해 악성코드가 실행되어 지속성을 유지한다.



대응 전략	
계정 권한 관리	낮은 권한을 가진 사용자가 더 높은 권한 수준에서 실행되는 서비스를 생성하거나 수정 가능한 권한이 있는지 확인한다.
시스템 로그 확인	시스템 로그의 신규 서비스 등록을 모니터링 하여 비정상적인 서비스를 식별한다.

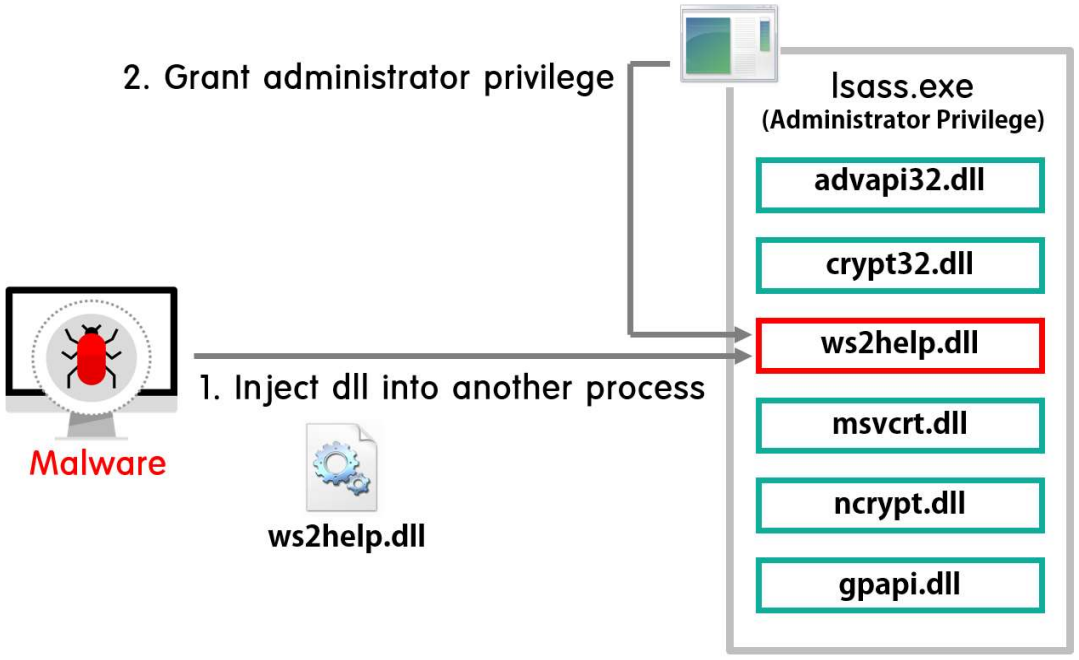
※ 각 기술 별 대응전략은 MITRE 홈페이지에 제시한 내용을 반영

3 Privilege Escalation : 권한 상승



가. Process Injection(78.22%) : 특정 프로세스에 코드 삽입

악성코드는 현재 실행되고 있는 관리자권한의 프로세스를 탐색하여 해당 프로세스에 DLL 악성코드(Dynamic Link Library)를 주입한다. 주입된 악성 DLL은 관리자 권한을 부여받아 실행 될 수 있다.



대응 전략	
안티 바이러스 / 멀웨어	백신을 설치하여 의심스러운 파일 삭제 및 탐지 활성화한다.
권한 있는 계정 관리(Linux)	ptrace의 사용을 권한이 있는 사용자로만 제한하여 ptrace기반 프로세스 인젝션을 완화한다.(Linux)

※ 각 기술 별 대응전략은 MITRE 홈페이지에 제시한 내용을 반영

나. New Service(11.35%) : 서비스 생성

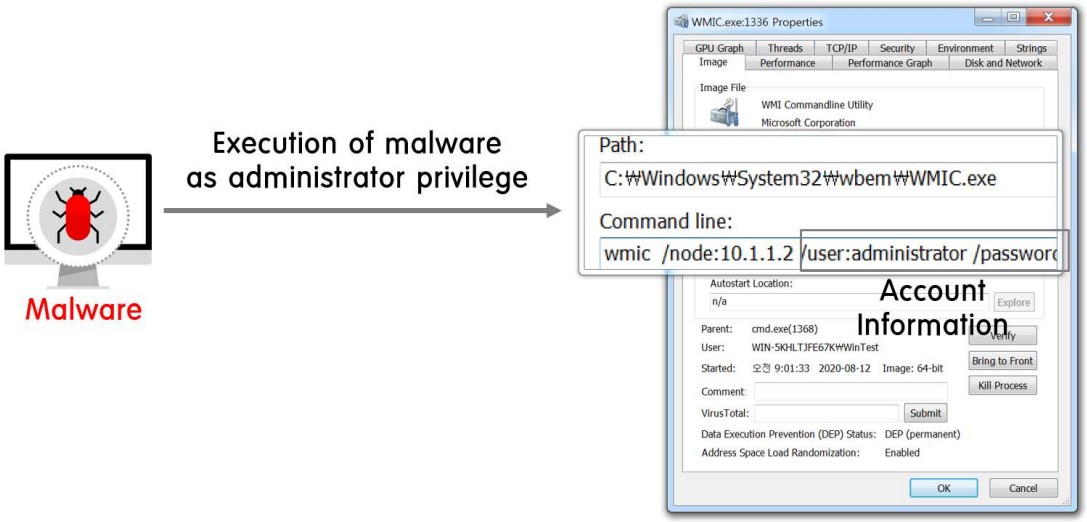
악성코드 실행 시 윈도우 서비스를 신규로 생성하며, 서비스를 이용하여 악성코드를 실행할 경우 악성코드는 SYSTEM 권한을 가진다.

대응 전략	
계정 권한 관리	낮은 권한을 가진 사용자가 더 높은 권한 수준에서 실행되는 서비스를 생성하거나 수정 가능한 권한이 있는지 확인한다.
시스템 로그 확인	시스템 로그의 신규 서비스 등록을 모니터링 하여 비정상적인 서비스를 식별한다.

※ 각 기술 별 대응전략은 MITRE 홈페이지에 제시한 내용을 반영

다. Valid Accounts(4.29%) : 유효한 계정 정보 활용

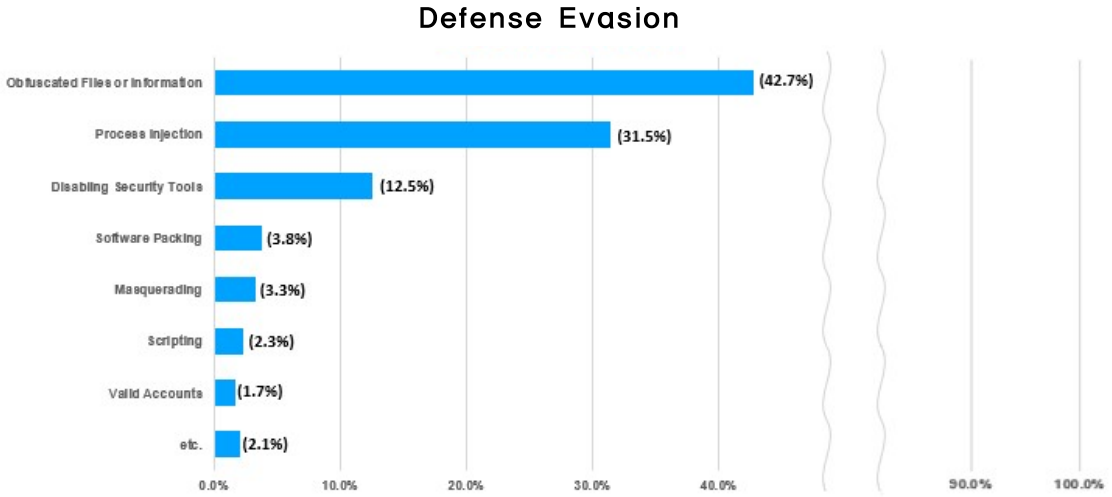
관리자 권한으로 악성코드를 실행시키기 위해 wmic 등의 명령어를 활용하여 사전에 수집한 계정정보를 통해 악성코드를 실행한다.



대응 전략	
접속 제한	IP별 사용자 접속을 제한한다.
비밀번호 정책	기본 계정의 비밀번호는 주기적으로 변경한다.
권한 있는 계정 관리	관리자 계정(Administrator) 비활성화 등 로컬 계정에 대한 권한 및 액세스를 최소화 하고, 관리자 그룹 계정의 UAC(User Access Control)를 설정하여 악용으로 인한 영향을 제한한다.

※ 각 기술 별 대응전략은 MITRE 홈페이지에 제시한 내용을 반영

4 Defense Evasion : 방어 회피



가. Obfuscated Files or Information(40.03%) : 파일 또는 정보 난독화

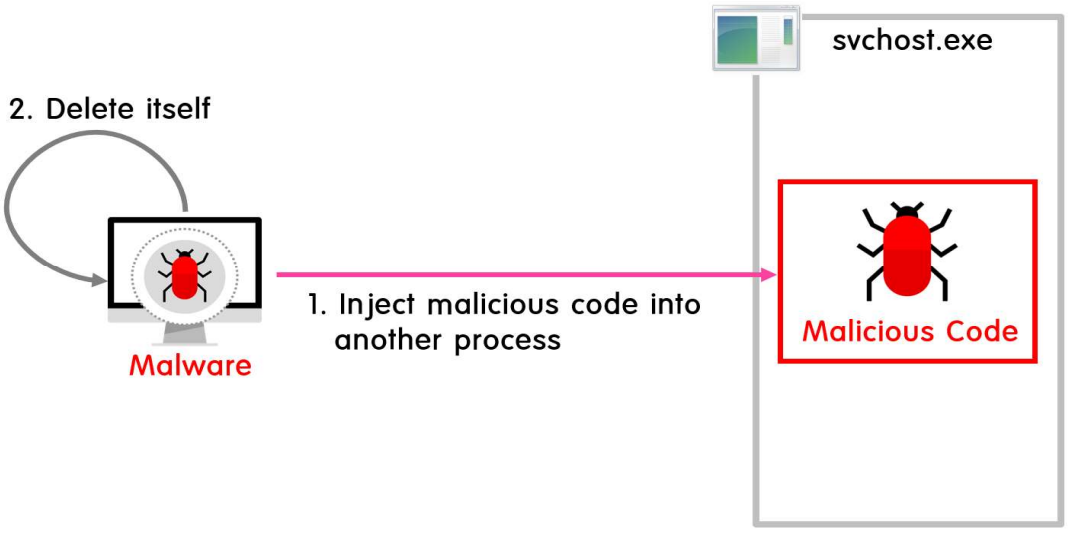
악성코드는 백신 등 보안 장비 및 소프트웨어의 탐지를 회피하기 위해 악성행위를 하는 페이로드 또는 추가 생성한 악성코드를 난독화하여 저장한다.

대응 전략	
안티 바이러스 / 멀웨어	백신을 설치하여 의심스러운 파일 삭제 및 탐지 활성화한다.

※ 각 기술 별 대응전략은 MITRE 홈페이지에 제시한 내용을 반영

나. Process Injection(31.7%) : 특정 프로세스에 코드 삽입

악성코드는 백신의 탐지를 회피하기 위해 현재 실행중인 정상 프로세스에 악성행위를 하는 코드 일부 또는 전체를 삽입해 은닉되어 동작한다.

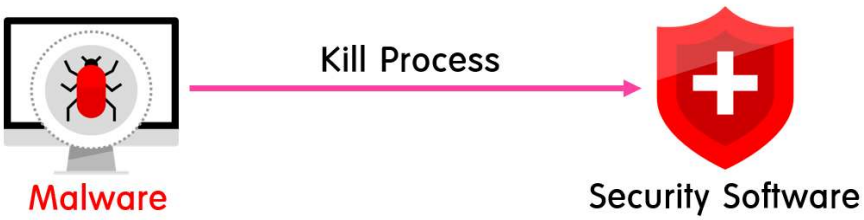


대응 전략	
안티 바이러스 / 멀웨어	백신을 설치하여 의심스러운 파일 삭제 및 탐지 활성화한다.
권한 있는 계정 관리(Linux)	ptrace의 사용을 권한이 있는 사용자로만 제한하여 ptrace기반 프로세스 인젝션을 완화한다.(Linux)

※ 각 기술 별 대응전략은 MITRE 홈페이지에 제시한 내용을 반영

다. Disabling Security Tools(12.61%) : 백신 등 보안 소프트웨어 무력화

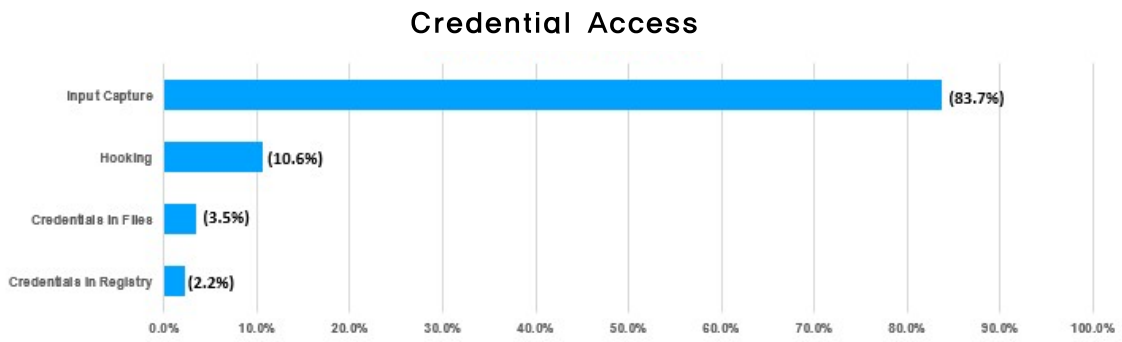
악성코드를 탐지하고 치료하는 백신 등 보안 소프트웨어의 프로세스를 탐색하여 프로세스를 종료하는 것뿐만 아니라, 해당 소프트웨어를 삭제하거나 변조한다.



대응 전략	
계정 권한 제한	공격자가 백신 등 보안 소프트웨어를 비활성화하거나 무력화 하지 않도록 프로세스, 레지스트리, 사용자 계정 권한을 확인한다.

※ 각 기술 별 대응전략은 MITRE 홈페이지에 제시한 내용을 반영

5 Credential Access : 계정정보 접근



가. Input Capture(83.69%) : 키로깅을 통한 사용자 계정 정보 수집

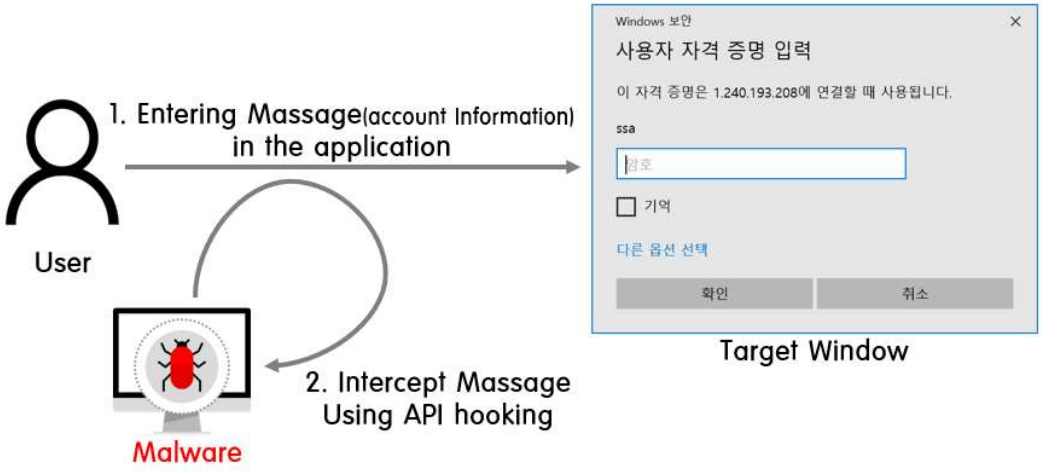
악성코드는 목표 시스템의 계정 및 사용자 정보를 탈취하기 위해 사용자가 키보드로 입력하는 데이터를 중간에서 파일로 로깅하여 수집한다.

대응 전략	
안티 바이러스 / 멀웨어	백신을 설치하여 의심스러운 파일 삭제 및 탐지 활성화한다.

※ 각 기술 별 대응전략은 MITRE 홈페이지에 제시한 내용을 반영

나. Hooking(10.63%) : 프로시저, IAT 등 후킹

악성코드는 사용자가 특정 어플리케이션에 입력하는 메시지를 API Hooking 기술 등을 통해 중간에서 가로챈다.

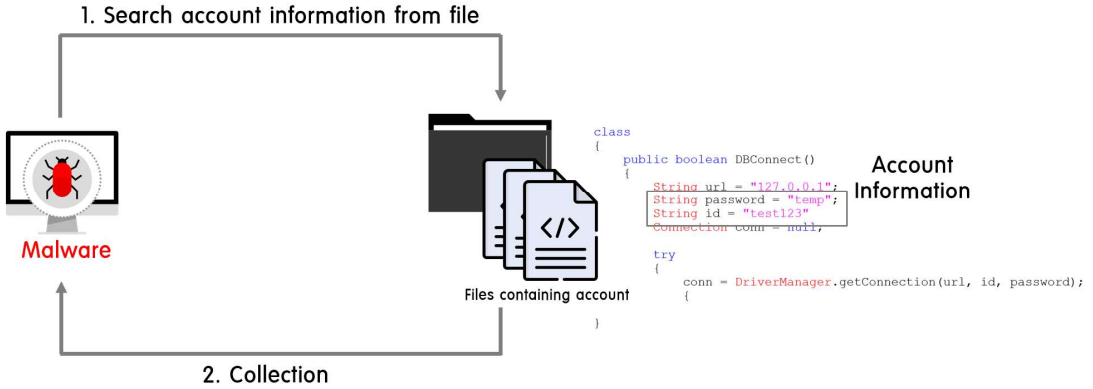


대응 전략	
안티 바이러스 / 멀웨어	백신을 설치하여 의심스러운 파일 삭제 및 탐지 활성화한다.

※ 각 기술 별 대응전략은 MITRE 홈페이지에 제시한 내용을 반영

다. Credentials in Files(3.61%) : 저장된 계정정보 덤프 및 수집

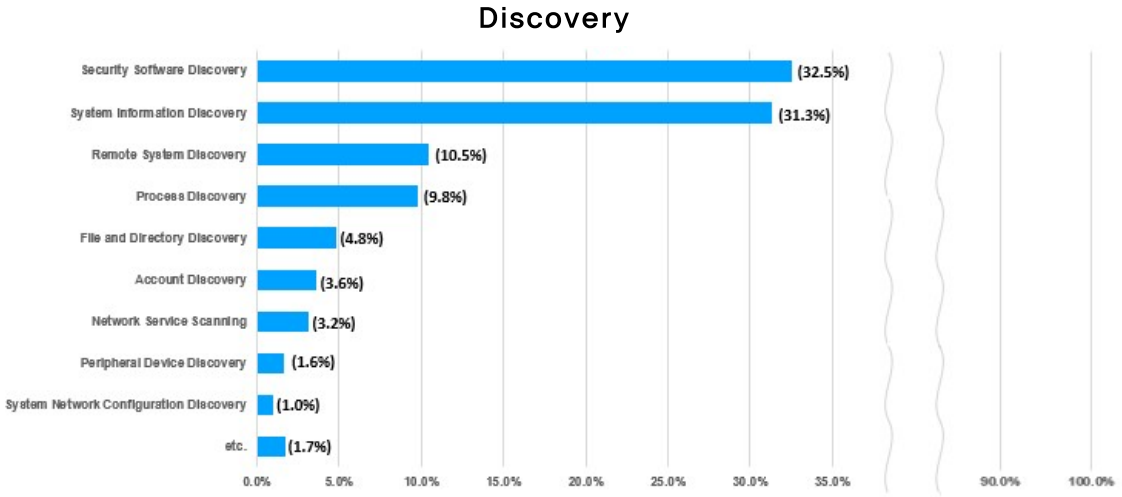
악성코드는 시스템 내 파일들 중 특정 문자열이 포함되어있는 파일을 수집하여 공격자가 원하는 계정정보를 획득한다.



대응 전략	
사용자 교육	시스템 및 서비스의 패스워드를 파일로 저장하는 것을 자제하고 특정 권한을 가진 사용자만 열람할 수 있게 제한한다.

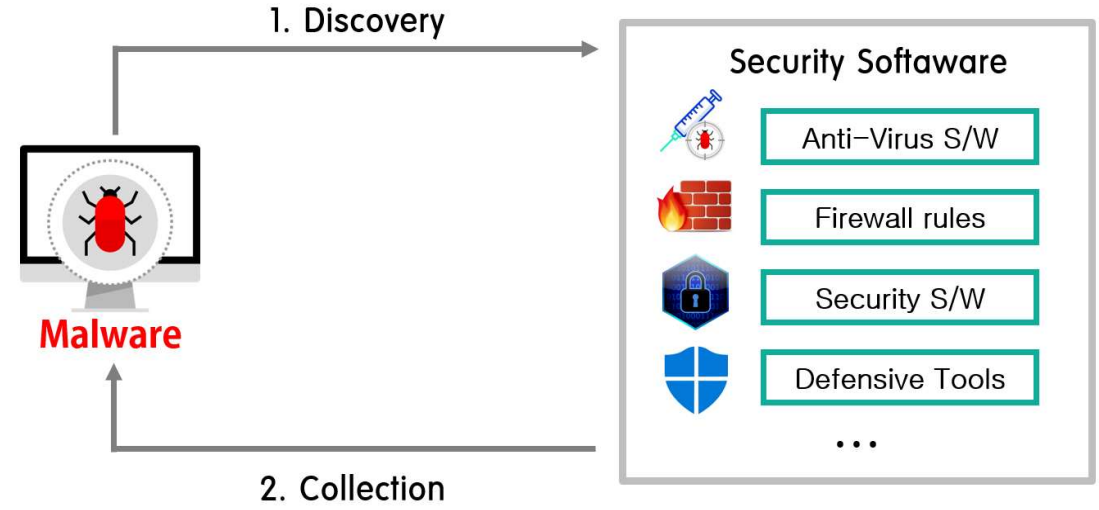
※ 각 기술 별 대응전략은 MITRE 홈페이지에 제시한 내용을 반영

6 Discovery : 탐색



가. Security Software Discovery(32.53%) : 보안 프로그램 등 탐색

악성코드 실행 시 윈도우 관리 도구(WMI)를 이용하여 시스템 내 설치된 백신 프로그램, 방화벽 규칙 등 보안 소프트웨어를 탐색하고 정보를 수집한다.

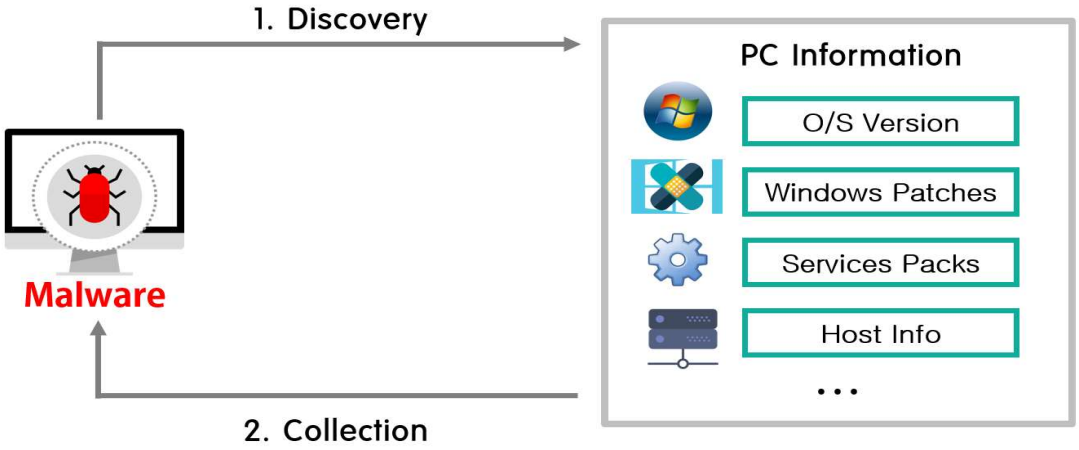


대응 전략	
WMI 비활성화	시스템에서 윈도우 관리 도구(WMI)를 사용하지 않을 경우 비활성화 한다.
안티 바이러스 / 멀웨어	백신을 설치하여 의심스러운 파일 삭제 및 탐지 활성화 한다.

※ 각 기술 별 대응전략은 MITRE 홈페이지에 제시한 내용을 반영

나. System Information Discovery(31.37%) : 시스템 정보 탐색

악성코드 실행 시 systeminfo와 같은 명령어를 통해 감염 시스템의 버전, 서비스팩, 아키텍처 등을 포함한 운영체제 및 하드웨어 정보를 탐색하고 수집한다.

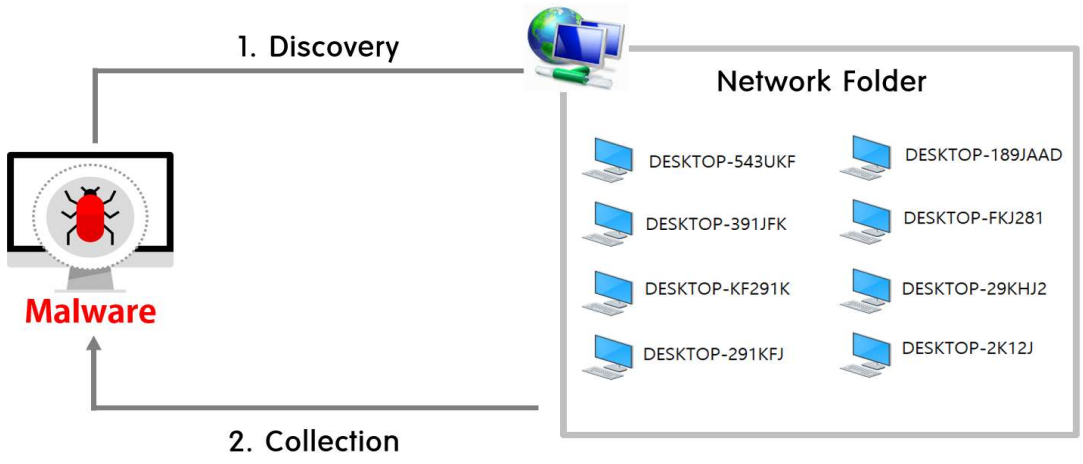


대응 전략	
안티 바이러스 / 멀웨어	백신을 설치하여 의심스러운 파일 삭제 및 탐지 활성화한다.

※ 각 기술 별 대응전략은 MITRE 홈페이지에 제시한 내용을 반영

다. Remote System Discovery(10.48%) : 네트워크의 다른 시스템 탐색

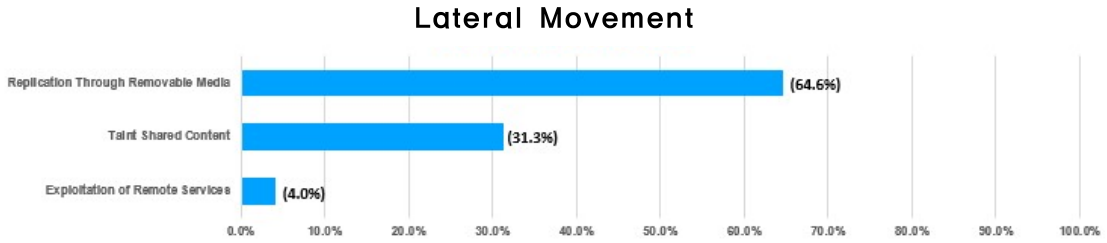
악성코드 실행 시 net view와 같은 명령어를 통해 감염 시스템과 동일한 네트워크에 연결된 다른 시스템 목록을 탐색하고 정보를 수집한다.



대응 전략	
안티 바이러스 / 멀웨어	백신을 설치하여 의심스러운 파일 삭제 및 탐지 활성화한다.

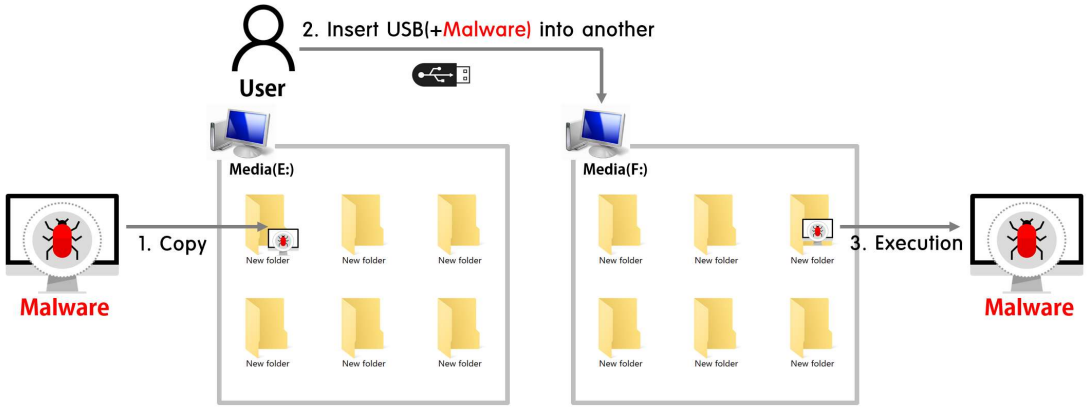
※ 각 기술 별 대응전략은 MITRE 홈페이지에 제시한 내용을 반영

7 Lateral Movement : 시스템 내부 이동



가. Replication Through Removable Media(64.72%) : 이동식 매체 이용

악성코드를 이동식 매체에 복사하고 해당 매체를 다른 시스템에 삽입하였을 때 악성코드가 Autorun을 통해 자동으로 실행되거나, 정상 파일처럼 보이도록 파일명을 수정하여 다른 시스템에서 실행하도록 유도한다.

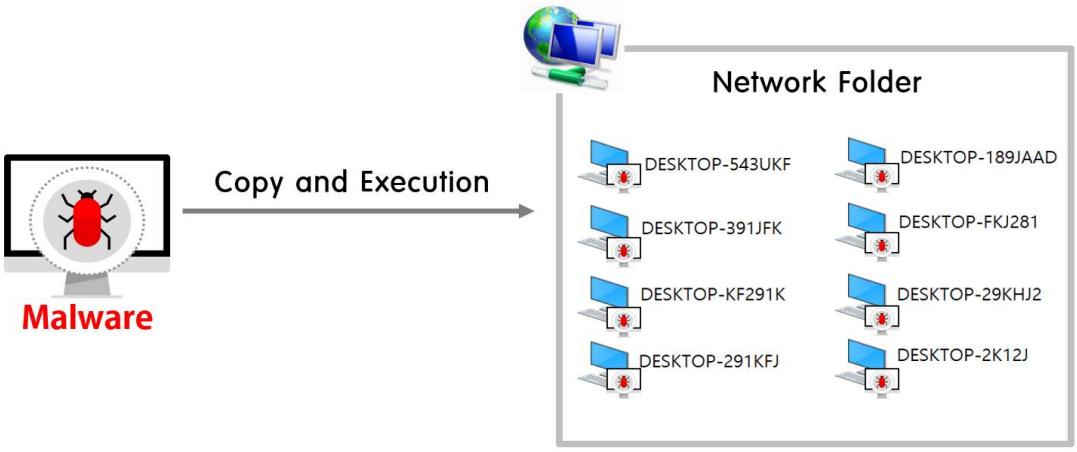


대응 전략	
프로그램 제거 / 비활성화	필요하지 않은 경우 자동 실행을 비활성화 하고, 이동식 미디어를 허용하지 않거나 제한한다.
안티 바이러스 / 멀웨어	백신을 설치하여 의심스러운 파일 삭제 및 탐지 활성화한다.

※ 각 기술 별 대응전략은 MITRE 홈페이지에 제시한 내용을 반영

나. Taint Shared Content(31.41%) : 공유 네트워크 등에 감염된 콘텐츠를 통한 감염

악성코드 실행 시 감염 시스템과 동일한 네트워크에 있는 다른 시스템들로 전파되어 피해를 확산시킨다.

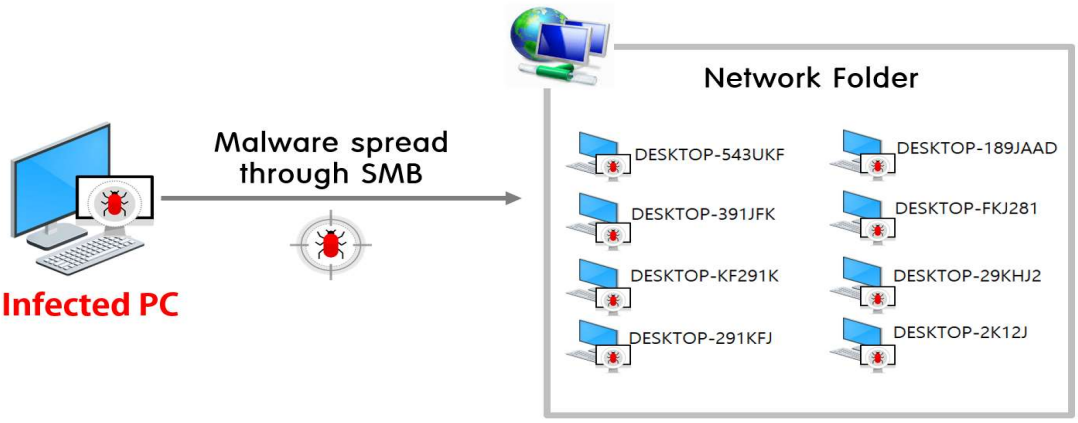


대응 전략	
하드웨어 설치 제한	네트워크 내에서 USB 등의 이동식 미디어의 사용을 제한한다.

※ 각 기술 별 대응전략은 MITRE 홈페이지에 제시한 내용을 반영

다. Exploitation of Remote Services(4.15%) : SMB, RDP 등 원격 서비스 취약점 공격

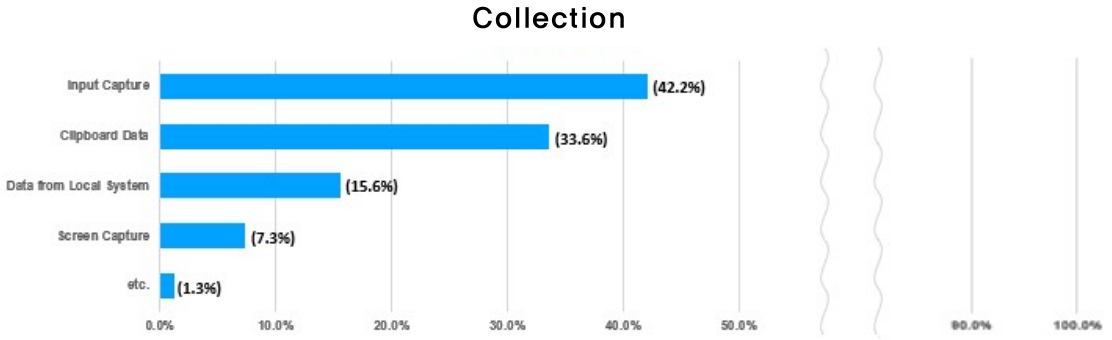
공격자는 악성코드에 감염된 PC를 통해 원격 서비스 프로토콜(SMB, RDP 등)을 악용하여 동일한 네트워크 내부 시스템에 접근하고 악성코드를 전파시켜 피해를 확산시킨다.



대응 전략	
정기적 업데이트	운영체제 및 소프트웨어의 최신 업데이트를 유지하여 취약점 공격에 예방한다.
권한 있는 계정 관리	관리자 계정(Administrator) 비활성화 등 로컬 계정에 대한 권한 및 액세스 최소화

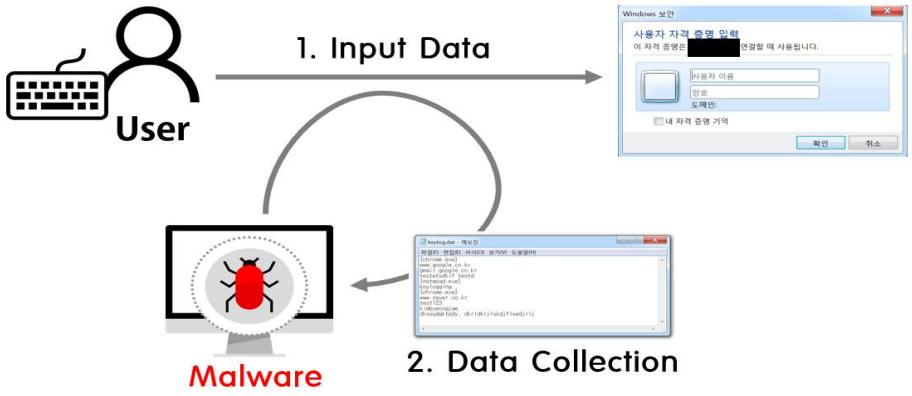
※ 각 기술 별 대응전략은 MITRE 홈페이지에 제시한 내용을 반영

8 Collection : 정보 수집



가. Input Capture(42.17%) : 키로깅을 통한 정보 수집

악성코드 실행 시 키로깅 기법을 통해 관리자 및 사용자가 입력한 계정정보, 개인정보 등의 데이터를 수집한다.

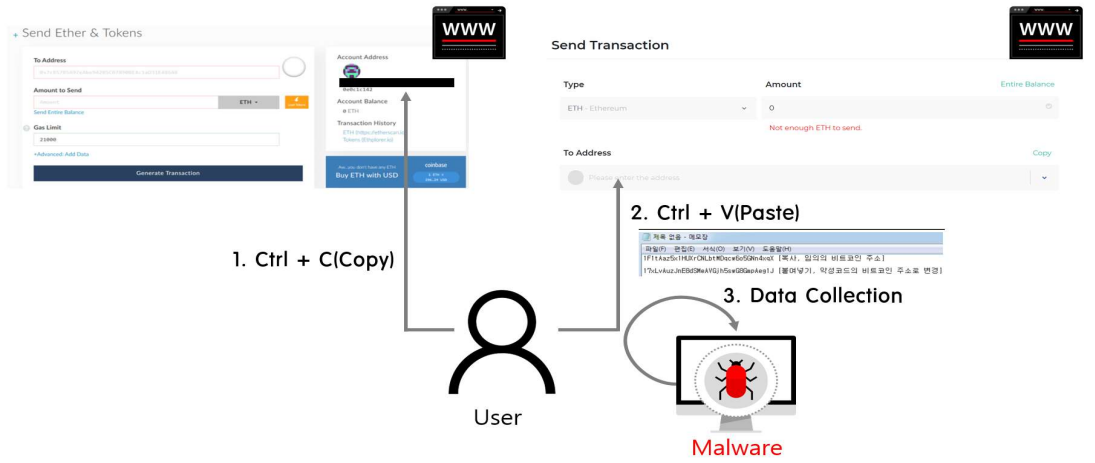


대응 전략	
안티 바이러스 / 멀웨어	백신을 설치하여 의심스러운 파일 삭제 및 탐지 활성화한다.

※ 각 기술 별 대응전략은 MITRE 홈페이지에 제시한 내용을 반영

나. Clipboard Data(33.62%) : 클립보드 데이터 수집

악성코드 실행 시 클립보드를 확인하는 코드를 통해 사용자가 복사한 텍스트를 수집한다. 이를 이용하여 수집한 텍스트 중 사용자가 복사한 비트코인 주소를 붙여놓기 할 때 자신의 주소가 붙여놓기 하게 만든다.

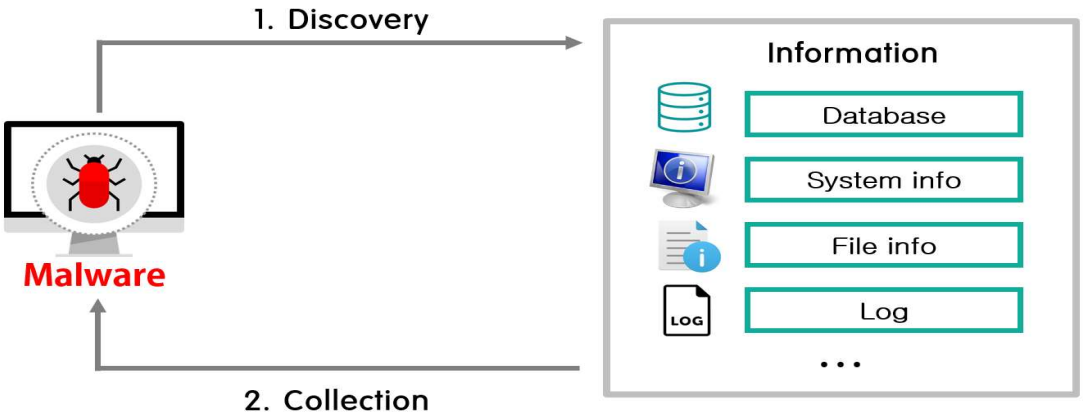


대응 전략	
안티 바이러스 / 멀웨어	백신을 설치하여 의심스러운 파일 삭제 및 탐지 활성화한다.

※ 각 기술 별 대응전략은 MITRE 홈페이지에 제시한 내용을 반영

다. Data from Local System(15.55%) : DB 등 로컬 시스템 정보 수집

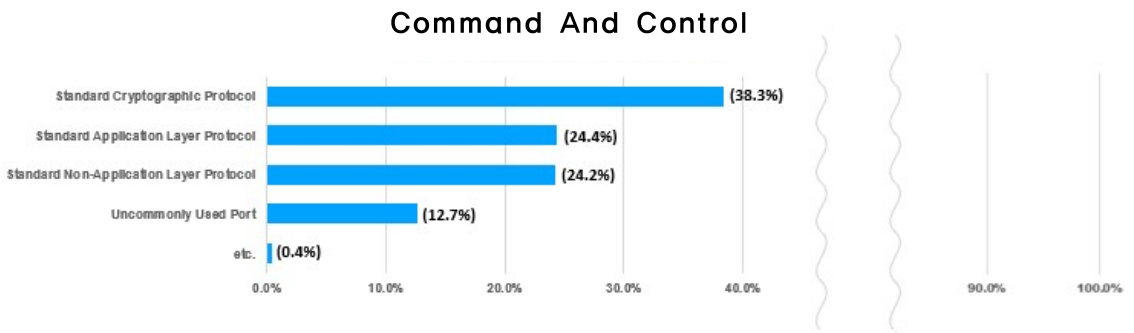
악성코드 실행 시 감염 시스템에서 데이터베이스 설정 정보(ID, Password, Port 등), 로그 정보(웹로그, 브라우저 로그 등), 파일 정보와 같은 로컬 시스템 정보를 탐색하고 수집한다.



대응 전략	
문서 보안	중요 정보는 별도 분리 보관 및 암호설정을 하고, 기업 문서 보안솔루션(DRM) 도입 검토한다.

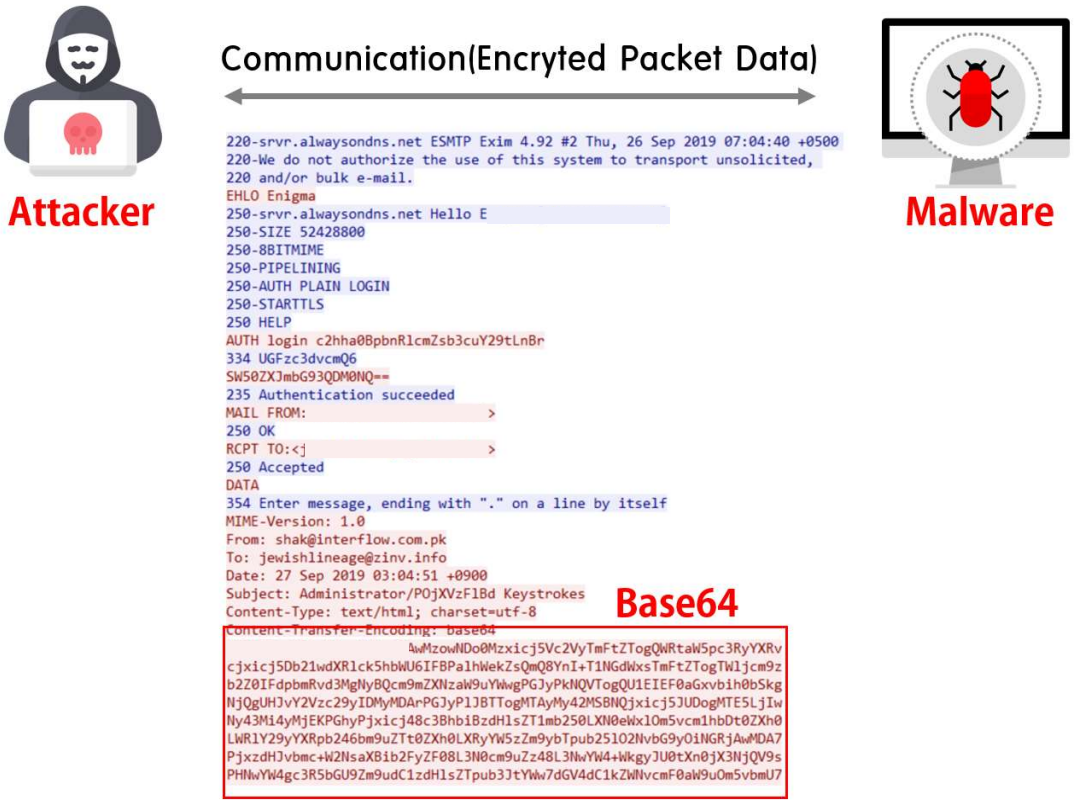
※ 각 기술 별 대응전략은 MITRE 홈페이지에 제시한 내용을 반영

9 Command and Control : 명령제어



가. Standard Cryptographic Protocol(38.59%) : 알려진 암호화 알고리즘을 이용하여 통신

공격자는 명령어를 숨기고 트래픽 탐지를 우회하기 위해 RC4, Base64 등 알려진 암호화 알고리즘으로 데이터를 인코딩 및 암호화하여 통신한다.

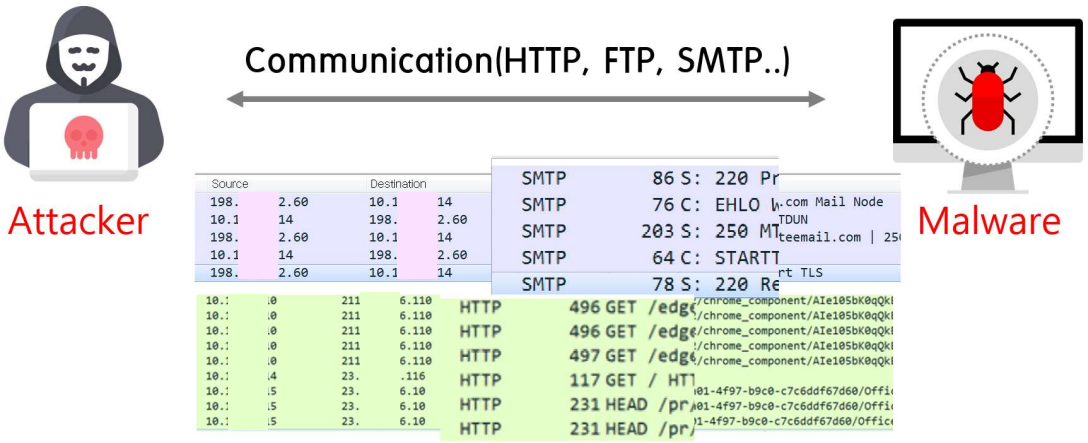


대응 전략	
네트워크 침입 방지	네트워크 보안장비(UTM,IPS)를 통해 악의적인 트래픽을 식별하고 차단하여 네트워크 침입 및 C2통신을 방지한다.
네트워크 포트 비활성화	불필요한 네트워크 포트를 비활성화하고 네트워크 설정 변경사항을 모니터링 한다.

※ 각 기술 별 대응전략은 MITRE 홈페이지에 제시한 내용을 반영

나. Standard Application Layer Protocol(24.54%) : 응용 계층 프로토콜을 사용하여 통신

공격자는 네트워크 필터링 및 탐지를 피하기 위해 주로 응용 계층 프로토콜(HTTP, FTP, SMTP 등)을 사용하여 C2서버 및 감염 시스템과 통신한다.

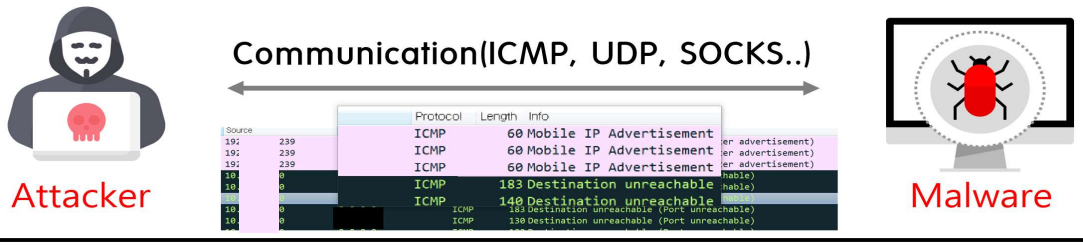


대응 전략	
네트워크 침입 방지	네트워크 보안장비(UTM,IPS)를 통해 악의적인 트래픽을 식별하고 차단하여 네트워크 침입 및 C2통신을 방지한다.
네트워크 포트 비활성화	불필요한 네트워크 포트를 비활성화하고 네트워크 설정 변경사항을 모니터링 한다.

※ 각 기술 별 대응전략은 MITRE 홈페이지에 제시한 내용을 반영

다. Standard Non-Application Layer Protocol(24.42%) : 응용 계층이 아닌 프로토콜을 사용하여 통신

공격자는 응용 계층뿐만 아니라 네트워크 계층(ICMP), 전송 계층(UDP), 세션계층(SOCKS) 등 비 응용 계층을 사용하여 C2서버 및 감염 시스템과 통신할 수 있다.



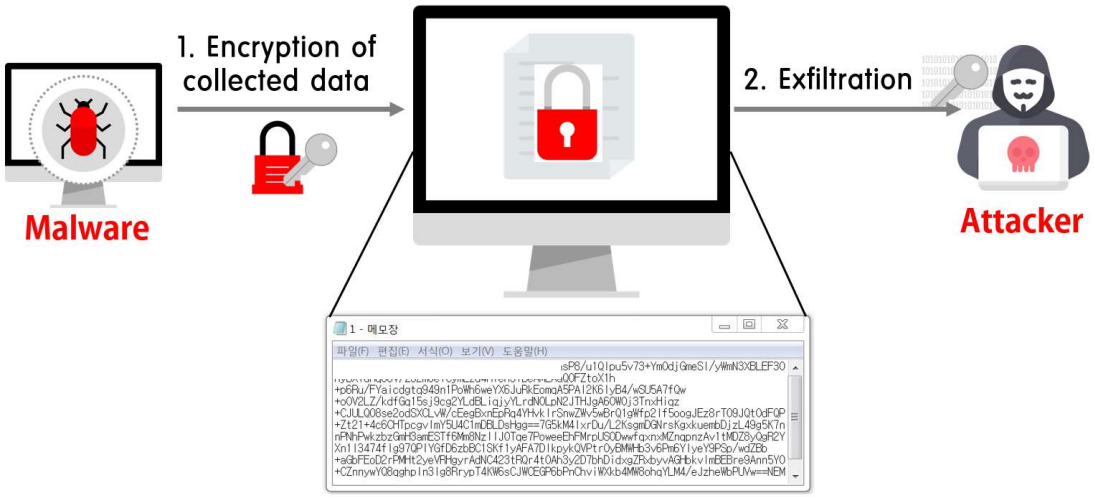
대응 전략	
네트워크 침입 방지	네트워크 보안장비(UTM,IPS)를 통해 악의적인 트래픽을 식별하고 차단하여 네트워크 침입 및 C2통신을 방지한다.
네트워크 포트 비활성화	불필요한 네트워크 포트를 비활성화하고 네트워크 설정 변경사항을 모니터링 한다.

※ 각 기술 별 대응전략은 MITRE 홈페이지에 제시한 내용을 반영

⑩ Exfiltration : 정보 유출

가. Data Encrypted(94.39%) : 데이터를 암호화하여 유출

악성코드는 감염 시스템에서 수집한 정보 및 파일을 인코딩, 압축 라이브러리 등을 이용해 데이터를 암호화 하여 유출한다.



대응 전략	
안티 바이러스 / 멀웨어	백신을 설치하여 의심스러운 파일 삭제 및 탐지 활성화한다.

※ 각 기술 별 대응전략은 MITRE 홈페이지에 제시한 내용을 반영

Ⅳ. 결론

【Defender's Insight】

사이버 공격 대부분은 악성코드를 통해 이루어지기 때문에 공격자는 방어 환경을 우회하고 탐지를 회피하기 위해 악성코드를 지속 고도화해 나가고 있다.

KISA에서는 공격에 이용된 악성코드를 단순히 기능 중심으로 파악하는 것을 탈피하고 악성코드가 가지고 있는 특징들을 전략과 전술 관점에서 분석해 보았다. 그 결과, 악성코드들의 활동이 ATT&CK 매트릭스에 명시된 다양한 기술들 중 몇 가지 주요 기술들을 중심으로 이루어지는 것을 파악할 수 있었다.

기업에서 악성코드를 선제적으로 대응하기 위해서는 PC 및 서버에서 아래와 같은 행위들을 수집하고 모니터링 할 수 있는 체계가 필요하다.

- 윈도우 서비스 생성 및 변조
- 시작 프로그램 등록을 위한 레지스트리 생성
- 코드 서명이 불분명한 프로그램 또는 스크립트 실행
- 의심스러운 windows 명령 쉘 실행
- 프로세스 변조 및 생성
- 계정의 비정상적인 사용 여부
- 백신 등 보안제품 작동 상태 변경 여부
- 미미카츠와 같은 계정정보 수집 및 탈취행위 여부
- 비정상적인 네트워크 공유 폴더 사용
- 네트워크 정보 등 시스템 정보 수집

이러한 노력을 통해 악성코드에 대한 방어 전략을 잘 갖추게 된다면 많은 악성코드 공격을 탐지하고 무력화 할 수 있을 것이라 생각한다.

KISA는 향후 공격 기술별로 주요 사용된 악성 서비스 경로 및 파일명, 악성코드 실행에 주요 사용된 악성 명령어 등 상세한 내용을 추가적으로 공개할 예정이다.