KARA
Korea Anti Ransomware Alliance

2023.01.

KARA 랜섬웨어 동향 보고서

KARA 랜섬웨어 동향 보고서

■ 랜섬웨어 트렌드

✓ 랜섬웨어 트렌드 분석

최근 랜섬웨어는 Ransomware-as-a-Service(RaaS) 발전으로 세분화되고 조직화되어 활동을 하는 Lockbit, Royal, BlackCat(Alphv), Bianlian, BlackBasta와 같은 대형 그룹들이 가장 많은 활동과 피해를 입히고 있다. 이들 그룹은 서비스형 랜섬웨어로 다양한 공격자에 의해 하나의 수익 모델로 사용되어 끊임없는 공격을 수행하고 있다. 특히 Lockbit 랜섬웨어는 '22년 9월경 내부 개발자에 의해 빌드 툴이 유출되었으며 이를 활용한 Bl00dy 랜섬웨어가 발견되기도 하였다. 이러한 대형 그룹들의 공격이 활발하게 활동하고 있는 가운데 새로운 랜섬웨어 그룹, 기존 랜섬웨어의 변종들이 새로운 공격을 위해 우후죽순 생겨나고 있다.

신규 랜섬웨어 및 그룹 활동

4분기에 새로 발견된 그룹 중 ProjectRelic, Qilin, FreeCivilian, Play 랜섬웨어는 다크웹에서 이중 협박 전략을 채택하여 파일 암호화 및 유출된 정보를 게시하여 협박을 시도하고 있으며 10월에 발견된 Endurance 랜섬웨어는 포럼 사이트에서 미국 정부 관련 데이터를 포함한 총 18건의 게시를 통해 유출 데이터를 판매하고 있는 것이 확인되었다. 해당 랜섬웨어는 다크웹 사이트 운영 준비와 Endurance 랜섬웨어의 연장선으로 보이는 Endurance-Wiper를 오픈소스로 제작하는 등 다양한 활동과 활성화를 예시하는 듯한 정황이 확인되었다. 11월 중순 이후 새로운 유출 데이터에 대한 게시물이 없고 다크웹 사이트 접속이 불가하여 추가적인 활동 정황이 발견되지 않았지만 12월 말경 새로운 유출 대상을 공개하며 Endurance 랜섬웨어를 통한 공격이 지속되고 있는 것을 확인할 수 있다.

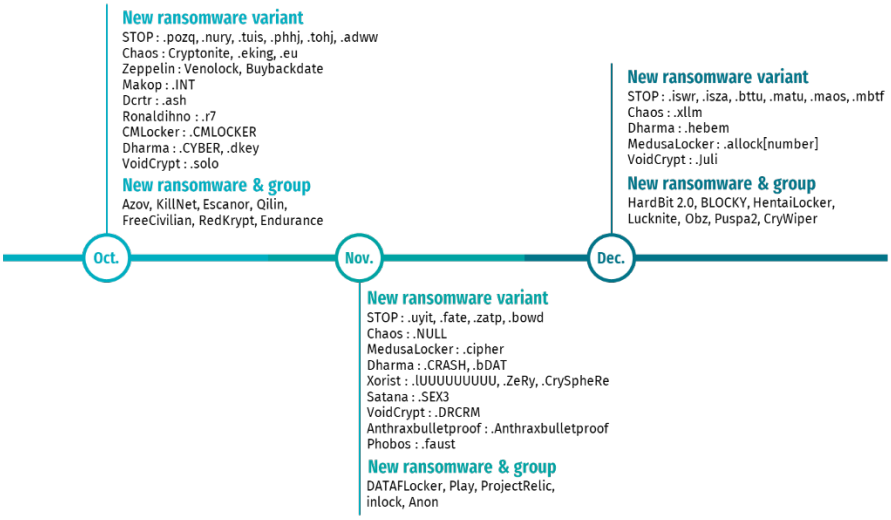


그림 1. 신규/변종 랜섬웨어 활동

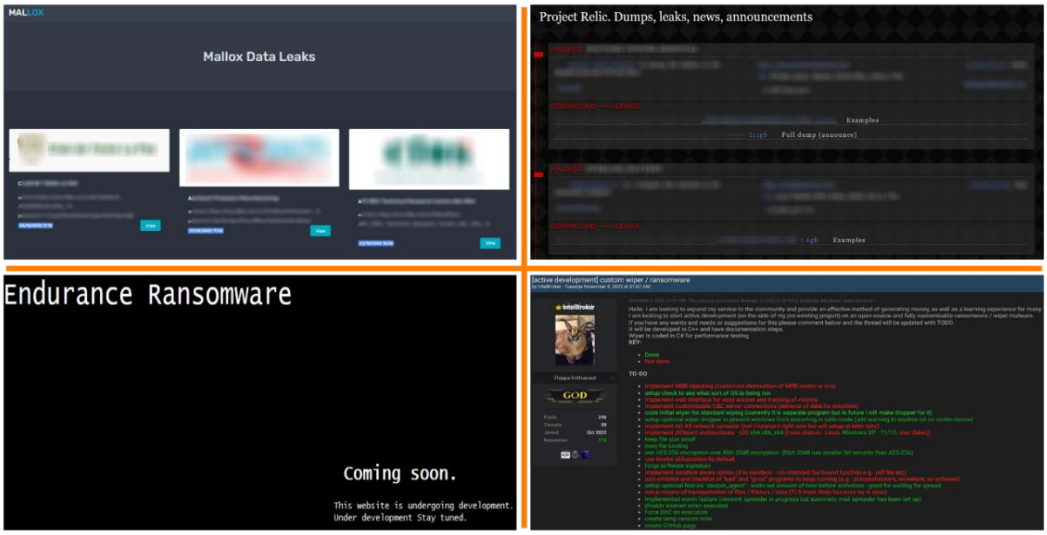


그림 2. 신규 랜섬웨어 다크웹 활동

랜섬웨어 공격 그룹 트렌드

랜섬웨어는 안정적인 수익 모델을 위한 다양한 전략과 탐지 회피 기법을 적용하여 공격을 시도하고 있으며 공격 대상을 선정하기 위한 정찰 단계와 공격을 수행하기 위한 각종 수집, 스캔, 원격 접속 등의 도구 개발 및 침투 전략을 수립하는데 상당한 공을 들이고 있다. 고도화된 랜섬웨어 제작부터 수준 높은 해킹 기술을 보유한 랜섬웨어 공격 그룹들의 활동이 지속되고 있으며 치밀하게 계획한 침투 전략과 세분화된 조직을 통해 정확하고 빠르게 공격을 수행하여 다량의 피해가 발생하고 있다.

변화하는 랜섬웨어

이러한 고도화된 타겟형 랜섬웨어 공격 이외에도 하반기 및 4분기에 발견되는 랜섬웨어는 조금씩 변화의 흐름을 보이기 시작했다. RansomExx 랜섬웨어는 Rust 기반으로 개발된 버전으로 업데이트 되었으며 이는 BlackCat, Hive, Luna 랜섬웨어 다음으로 발견된 Rust 기반 랜섬웨어로 조금씩 새로운 언어를 통해 개발된 경우가 발견되고 있다. 또한 Wiper(데이터 파괴형) 악성코드인 Azov, BlackCat(Alphv) 그룹의 자체 제작 툴인 ExMatter의 파일 파괴 기능이 추가된 업데이트, 데이터베이스 서버를 노리는 GlobeImposter, Mallox, Masscan 등의 랜섬웨어 공격이 증가하기 시작했다. Wiper 악성코드는 지정학적인 문제와 사회/정치/외교적 문제 등으로 금전적 이득이 아닌 특정 악의적인 목적에 치중되어있다. 취약한 데이터베이스 서버를 노리는 랜섬웨어 공격은 예전부터 지속적으로 발견되어 왔지만 최근 국내 감염 사례가 증가하고 있어 주의와 관심이 필요하다.

1. 랜섬웨어 그룹 활동 및 통계

최근 3개월간의 랜섬웨어 그룹의 활동을 살펴보면 LockBit 랜섬웨어가 가장 활발한 활동을 보였으며 Royal, BlackCat(Alphv), Bianlian, BlackBasta 랜섬웨어 순으로 랜섬웨어에 공격당한 피해자를 확인할 수 있다. 이들 상위 그룹의 랜섬웨어는 모두 RaaS 형태로 조직화된 그룹들의 활동은 여전히 위협적인 모습을 보이고 있다. 또한 제조/서비스 환경의 지속적인 랜섬웨어 공격과 IT, 유통, 의료 관련 산업에 대한 공격도 많은 것을 확인할 수 있다.

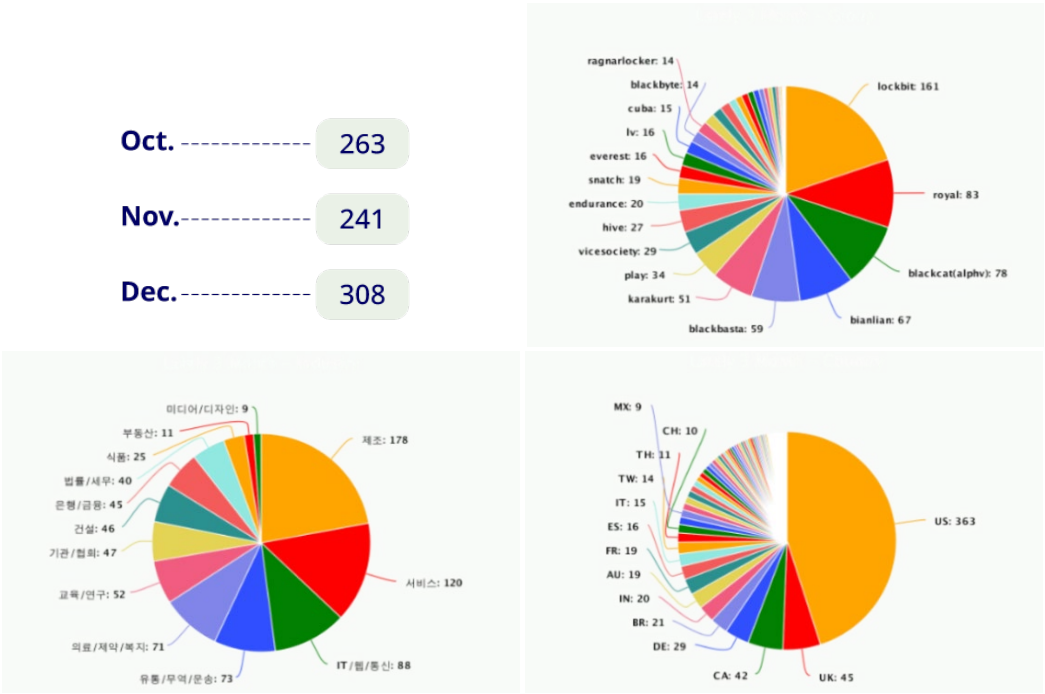


그림 3. 랜섬웨어 그룹 활동

2. 데이터 파괴형 랜섬웨어

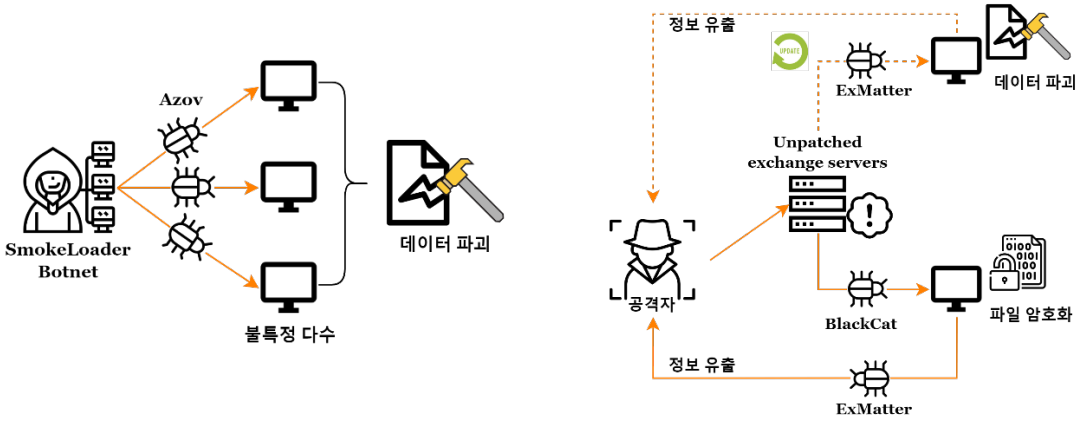


그림 4. Azov 랜섬웨어(좌) / ExMatter(우) 공격 패턴

10월경 Wiper(데이터 파괴형) 악성코드인 Azov가 등장하게 되는데 단순히 데이터 파괴만을 수행하며 사회/정치/외교적 이슈, 혼란 야기, 사이버 전쟁 등 특수한 목적을 위해 수행된 공격이다. 사실상 Wiper 악성코드와 랜섬웨어는 엄밀히 말하면 다른 악성코드이다. 우선 궁극적인 목적이 다르다. Wiper 악성코드는 오로지 파괴만을 위해 사용되고 랜섬웨어는 금전적인 이득을 위해 파일을 암호화하여 인질로 삼는다. 그러나 여기서 주목할 점은 궁극적인 목적은 다르지만 일부 전략의 유사성을 볼 수 있다는 점이다. 공격 대상 선정, 최초 침투, 탐지 회피 기법 등 다양한 부분을 공유하고 있으며 Wiper, 랜섬웨어 악성코드 모두 정상적인 서비스 유지, 중요 파일에 대한 접근 등을 못하게 공격하여 타겟 대상을 마비시키는 악성 행위를 수행한다. 물론 여기서 악성 행위가 종료되면 궁극적인 목표가 다르기 때문에 Wiper와 랜섬웨어는 다른 분류로만 구분하는 것이 맞을 것이다. 하지만 추가적으로 포착한 정황을 바탕으로 이야기를 조금 확장할 수 있다.

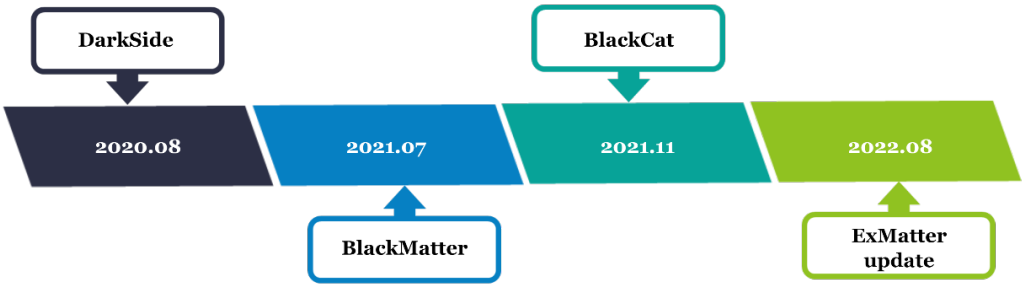
위의 이야기에 덧붙여 BlackCat(Alphv) 랜섬웨어를 추가적으로 살펴볼 필요가 있다. Alphv 그룹의 자체 제작 툴인 ExMatter 정보 유출 툴은 BlackCat 랜섬웨어가 암호화를 수행하기 전 2중 협박을 위해 정보 유출을 목적으로 사용한다. 최근 해당 툴의 업데이트를 통해 다양한 기능이 추가되었는데 그 중 자료 유출 후 파일을 파괴하는 형태의 기능을 추가하였다. 이러한 형태의 공격은 다음과 같은 시나리오를 생각할 수 있다.

1차적으로 데이터를 유출하고 2차적인 공격으로 데이터를 파괴 후 유출한 데이터를 이용하여 협박을 수행할 수 있다. 협박을 통해 성공적으로 수익을 얻게 된다면 암호화 알고리즘에 의존하지 않아도 되는 구조 및 공격 전략을 수행할 수 있다.

암호화 알고리즘을 제외하고 데이터 파괴형으로 변화할 경우 공격 그룹은 새로운 모델과 전략을 수행할 수 있으며 기존에 존재하던 여러 위험 요소를 제거할 수 있게 된다. 암호화를 위한 알고리즘의 취약점 혹은 복잡도에 따른 결함과 이슈가 발생하여 복호화 툴이 개발되거나 수익 모델을 잃는 경우도 사라지게 될 것이다. 또한 대부분의 랜섬웨어가 RaaS 형태인 점을 보면 개발자와의 수익 배분 구조도 변경이 가능하여 공격 그룹 입장에서는 더 많은 수익을 얻을 수 있게 된다. 암호화 방식을 사용하지 않음으로써 조직화된 랜섬웨어 그룹의 구조가 변할 수 있어 변화의 움직임에 관심을 기울이고 살펴볼 필요가 있다.

✓ BlackCat 랜섬웨어 – ExMatter

1) Background



- BlackCat 랜섬웨어는 Alphv 랜섬웨어 그룹에서 사용하고 있는 최신 버전의 랜섬웨어이며 RaaS(Ransomware-as-a-Service)로 서비스형 랜섬웨어에 속한다.
- 2020 년 8 월에 최초 발견된 DarkSide, 2021 년 7 월에 발견된 BlackMatter 를 거쳐 Re-Branding 된 랜섬웨어로 2021 년 11 월에 BlackCat 으로 바뀐 이후 현재까지 꾸준히 활동하고 있다.
- Alphv 그룹의 최초 랜섬웨어인 DarkSide 는 2021 년 5 월 미국의 Colonial Pipeline 을 공격하여 인프라를 마비시켰으며 해당 사건으로 FBI 의 지속적인 추적을 통해 운영을 중단하였다.
- 이후 2021 년 7 월 BlackMatter 로 이름을 변경하여 활동을 재개하였으며 DarkSide 의 암호화 알고리즘인 Custom Salsa20 을 사용하고 유출 사이트의 문구가 유사한 점 등을 바탕으로 Alphv 그룹의 Re-Branding 된 랜섬웨어로 확인됐다. 2021 년 9 월 Olympus 를 공격한 이력이 있으며 정부 및 수사 기관의 지속적인 압력으로 또 다시 운영을 중단하게 된다.
- 마지막 버전인 BlackCat 랜섬웨어는 2021 년 11 월 활동을 재개하였으며 Rust 기반으로 작성된 최초의 랜섬웨어이다. BlackMatter 운영 중 사용했던 자체 제작한 정보 유출 툴인 Fendr 공격 도구를 재사용하였다. Fendr 혹은 ExMatter 로 불리는 정보 유출 툴은 꾸준히 기능을 업데이트하며 실제 공격에 사용되고 있다.
- 2022 년 8 월 ExMatter 의 다양한 기능이 추가되었으며 업데이트된 기능 중 파일 및 정보를 유출한 뒤 파일을 파괴하는 형태의 기능이 확인되었다.

2) 특징

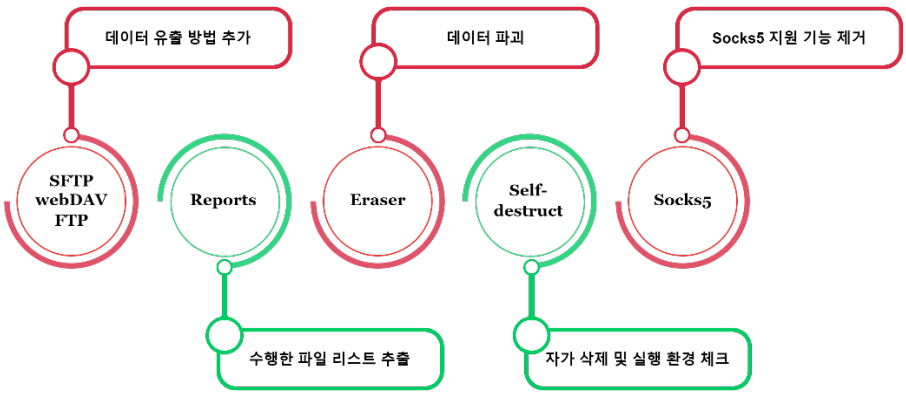


그림 5. ExMatter 기능 업데이트

- 데이터 유출 후 파일을 파괴하는 형태의 기능을 업데이트하여 파일 암호화가 아닌 파일을 파괴하는 형태의 새로운 전략을 사용한다.
- 데이터 유출 방법으로 FTP 를 통한 업로드 기능이 추가되었다.
- 핵심 정보만 추출하여 빠르게 유출 작업을 수행하기위해 특정 확장자만 수집하도록 변경하였으며 특정 폴더 명을 포함하는 경우 제외 후 데이터 유출 및 파괴를 위한 파일 리스트를 생성한다. 생성한 리스트를 추출할 수 있는 report 기능 또한 추가되었다.
- 업데이트 기능 중 데이터를 파괴하는 형태의 핵심 기능이 추가되었으며 리스트화 된 파일들의 데이터를 파괴한다.
- 실행된 툴이 종료되기 전 파워쉘 명령어를 통해 프로세스 종료 후 툴을 파괴하며 Commercial 도메인이 아닌 경우에도 실행된 툴을 파괴한다.
- 마지막으로 Socks5 프록시 지원 기능이 삭제되었다.

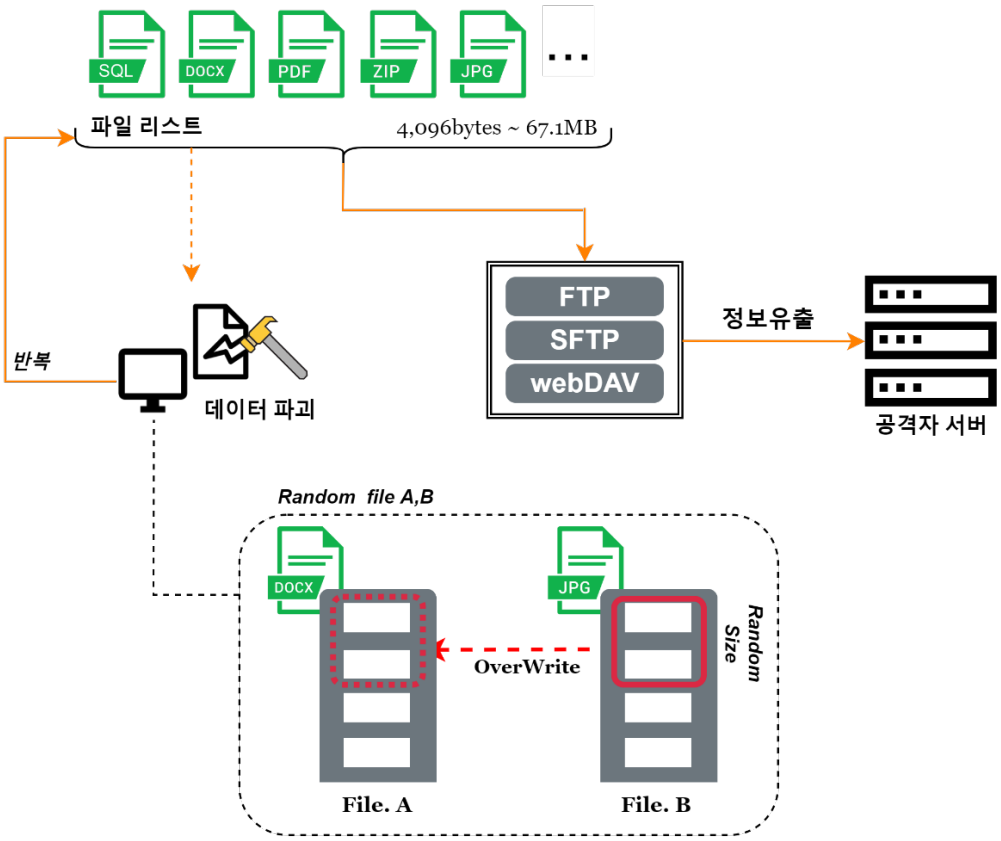


그림 6. 정보 유출 및 데이터 파괴 동작

- 파일 크기가 4,096 bytes ~ 약 67.1MB 인 경우 특정 확장자(pdf, doc, png, sql 등)를 포함하면서 특정 폴더 이름(Windows, Program Files 등)을 포함하고 있는 경우는 제외한 파일 유출 대상 리스트를 생성한다.
- 유출 방법으로는 sftp, ftp, webDAV 를 이용하며 전송되는 서버에 유출 대상의 호스트 이름으로 생성된 폴더에 업로드 된다.
- 서버에 모든 전송이 끝나면 파일을 파괴하는 작업을 수행한다. 생성한 파일 유출 리스트에서 무작위로 2 개의 파일을 선택 후 덮어씌우기위한 랜덤 사이즈를 채택하고 선택된 두 번째 파일의 시작 부분부터 선정한 랜덤 사이즈의 데이터를 읽어 첫번째 파일의 첫 부분부터 데이터를 덮어 씌어 파일을 파괴하며 해당 행위를 반복 수행한다.
- 랜덤한 파일을 선택하고 랜덤한 사이즈를 채택하여 파일 파괴 작업을 진행하기 때문에 파괴되지 않는 파일 혹은 여러 번 파괴되는 경우의 파일이 발생할 수 있다.

3) IoC

SHA256	FD102A2D650E12121782E63BE11DC189FC6361C77B683A8D447C97357C071861 5ED16FD24FBADB1DB96A2291E83427E8CB20D6C173C6A48A3C5C21182DEBF4A0 66607276117C3C4E7B3CBDACFC5A5D6BAFBDF124A807EB4B5624309514EAAA02
File name	sync.exe, sync2.exe, sync_enc.exe, indexhost.exe, bbio.nl.exe
IPv4	20.99.133.109 20.99.184.37 23.216.147.64 23.216.147.76

3. 데이터베이스 타겟형 랜섬웨어

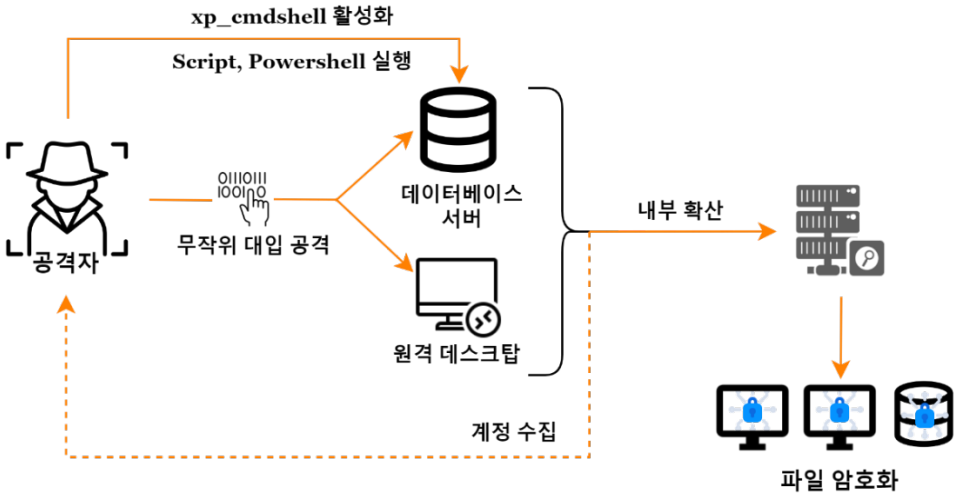


그림 7. 취약한 데이터베이스 공격 패턴

취약한 데이터베이스를 노린 랜섬웨어 공격은 매년 크고 작은 사고가 발생하고 있다. 데이터베이스는 각 기업들이 정상적인 서비스 제공을 위해 반드시 필요한 중요한 시스템 중 하나이다. 웹 서버나 PC 등을 공격한 경우와 데이터베이스를 노린 공격은 피해 규모가 확연히 차이가 난다. 데이터베이스가 암호화되면 기업에서 제공하는 대부분의 정상적인 서비스가 불가능하며 암호화된 파일을 복호화 해야할 경우 1순위로 복구를 해야하는 시스템이다. 또한 취약한 데이터베이스를 선정하여 공격하는 경우는 이미 오래전에 알려진 취약점과 기본적인 보안 사항을 조치하지 않은 서버로 공격자 입장에서 손쉽게 침투할 수 있어 꾸준히 공격 방법으로 이용되고 있다.

공격자들은 이런 점을 노려 외부에 노출된 취약한 데이터베이스 서버를 확인하여 공격을 시도하며 원격 데스크톱 서비스가 열려 있는 경우 혹은 외부에 노출된 데이터베이스에 무작위 대입 공격과 사전 공격을 수행하여 침투를 한다.

최초 침투 후 관리자 계정을 타깃으로 무작위 대입 공격 혹은 사전 공격을 수행하여 계정을 수집한다. 수집된 계정 정보를 이용하여 운영체제 명령을 수행할 수 있는 'xp_cmdshell'을 활성화하고 스크립트 파일 혹은 파워쉘 명령어 실행을 통해 추가적인 악성행위를 수행한다. 내부 네트워크를 탐색하고 공격 거점을 만들기 위해 각종 수집, 스캔, 원격 접속을 위한 도구를 사용한다. 침투 후 모든 준비가 끝나면 마지막으로 랜섬웨어를 실행하고 내부 이동을 통해 다수의 서버 혹은 PC를 감염시킨다.

취약한 MS-SQL 서버를 노리는 GlobeImposter, Mallox(Fargo), Masscan 랜섬웨어가 최근 가장 활발히 활동하고 있는 것으로 확인된다. GlobeImposter 랜섬웨어는 앞서 언급한 3가지 랜섬웨어 중 가장 오래된 랜섬웨어이다. 2017년 최초로 발견되었으며 2019년 다양한 기능을 업데이트 후 미국, 유럽, 아시아 등의 지역을 대상으로 공격을 시도하였으며 주로 피싱 메일 혹은 RDP를 통한 침투를 통해 랜섬웨어를 감염시켰으나 최근 MS-SQL 서버를 대상으로 공격 및 감염 사례가 꾸준히 발견되고 있다.

다음으로 Mallox 랜섬웨어는 2021년 최초로 발견되었으며 SQL 계정 관련 공격을 통해 서버에 접속 후 추가로 설치한 원격 프로그램을 통해 랜섬웨어 공격을 시도하거나 SQL을 통해 스크립트 혹은 파워쉘 명령어를 통해 랜섬웨어 공격을 수행한다. mallox로 불리는 랜섬웨어는 TargetCompany 랜섬웨어 그룹에서 사용한 랜섬웨어로 감염 후 변경되는 확장자가 .mallox, .FARGO, .FARGO2, .FARGO3 등으로 여러 변종이 발견되었으며 암호화 제외 대상을 확인하기위한 확장자 체크 리스트에 GlobeImposter 랜섬웨어의 최신 변종의 확장자가 포함되어 있어 일부 연관성이 확인된다.

마지막으로 Masscan 랜섬웨어는 올해 하반기 본격적으로 활동을 시작했으며 활동과 동시에 많은 감염 사례와 피해를 입혔다. 주로 외부에 노출된 취약한 데이터베이스를 공격하였으며 무작위 공격, 사전 공격 등을 수행하여 계정을 탈취하고 이를 통해 원격 접속 도구를 사용하여 랜섬웨어 공격을 수행하는 전략을 주로 사용하였다.

데이터베이스를 노린 공격은 다양한 형태와 방법으로 과거부터 꾸준히 존재해왔으며 랜섬웨어 공격이 증가하면서 이를 이용한 공격이 수면위로 드러나게 되었고 과거부터 존재해왔던 공격 방법을 통해 랜섬웨어 공격이 현재까지도 지속되고 있다. 외부에 노출된 취약한 데이터베이스가 여전히 존재하고 적절한 보안 조치가 이루어지지 않는 상황이 지속되고 있어 데이터베이스 관련 공격으로 인한 랜섬웨어 피해 사례가 증가하고 있으며 이를 예방하기 위해 사고 발생 전 외부에 노출된 취약한 데이터베이스 서버에 대한 적절한 보호 조치가 필요하다.

✓ Masscan 랜섬웨어

1) Background

그림 8. Masscan 랜섬웨어 감염 사례

- Masscan 랜섬웨어는 기본 포트(TCP: 1433)를 사용하는 취약한 MS-SQL 데이터베이스 서버를 대상으로 공격을 시도하며 외부에 노출된 서버를 조사하여 공격 대상을 선정한다.
- 공격 대상을 선정 후 데이터베이스에 무작위 공격을 시도하여 SA 계정 혹은 취약한 관리자 계정을 획득하고 xp_cmdshell[1], sqlps.exe[2]를 이용하여 공격에 필요한 명령어를 실행한다. 이 후 계정 생성 혹은 권한 상승, 원격 제어 도구 등을 사용하여 내부 침투를 시도하며 최종적으로 랜섬웨어를 실행하여 서버 및 PC를 암호화한다.
- MS-SQL 데이터베이스는 Microsoft 社에서 개발한 데이터베이스 서버로 'sqlps.exe' 툴을 이용한 공격의 급증을 경고하기도 했다. 'sqlps.exe' 툴은 SQL 서버에서 사용되는 공식 PowerShell 유틸리티로 cmdlet(Native PowerShell 명령어)을 사용할 수 있도록 도와준다. 공식 유틸리티를 사용함으로써 흔적이 남지 않도록 명령을 수행할 수 있게 된다.

---

[1] MS-SQL 서버에서 Windows Command 명령을 수행할 수 있는 프로시저

[2] MS-SQL 서버에서 사용되는 공식 PowerShell 유틸리티

- 2022년 6월 국내에서 첫 발견된 랜섬웨어로 해외에서 발견된 사례는 없으며 국내의 취약한 데이터베이스 서버를 대상으로 타겟형 공격을 시도한 것으로 확인된다.
- 최초 발견된 6월 이후 Masscan 랜섬웨어에 감염된 피해 기업은 수십 건으로 확인되고 있으며 제약, 바이오 등 다양한 업종에서 감염 사례가 발생하고 있다. 업종에 관계없이 외부에 노출된 취약한 데이터베이스 서버를 보유한 기업을 선정하여 공격 수행한다.
- 2022년 7월에는 콜택시 서버 운영 업체의 랜섬웨어 감염으로 강원, 부산, 대전 등의 약 18개 시, 군 지역에서 택시 호출 서비스가 중단되었으며 피해가 급증하여 공격자에게 비용을 지불하여 복구 한 사례가 있다.

2) 특징

- Masscan 랜섬웨어는 .NET 언어로 개발되었으며 실행 시 설정 값을 포함하는 파일(Encrypt.exe.config or Encrypt.app.config or *.config)이 있어야 정상 실행이 된다. 설정 값 내용으로는 변경 확장자, 공용 키, 랜섬노트 내용 등을 포함하고 있다.

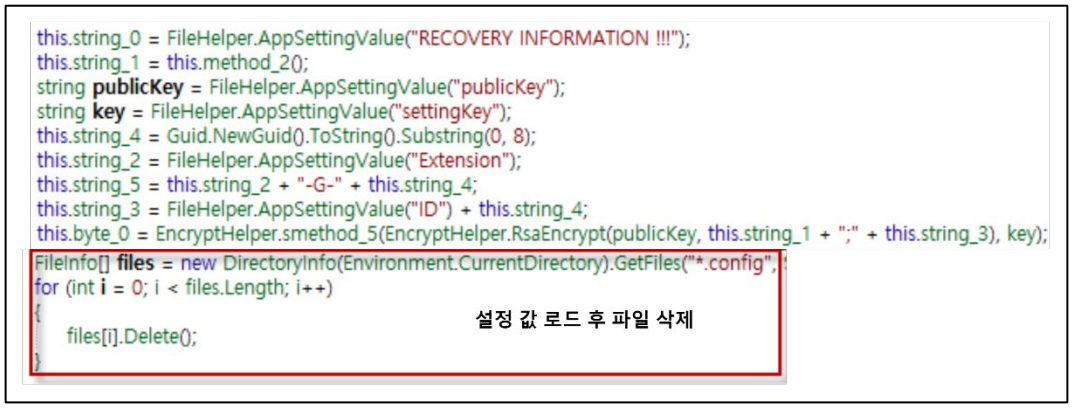


그림 9. 설정 값 로드

- 최초 발견시 변경되는 확장자는 .masscan-F-{id값} 형태로 변경되었으며 이 후 식별 값이 F, R, G 순으로 변경되어 최근에 발견되는 랜섬웨어는 확장자를 .masscan-G-{id값}으로 변경한다.

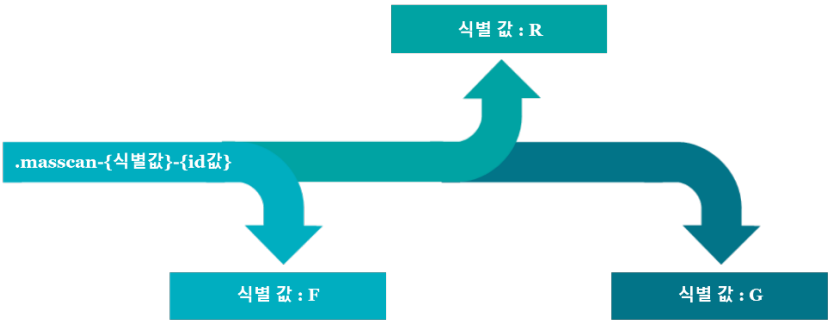


그림 10. Masscan 확장자 변경

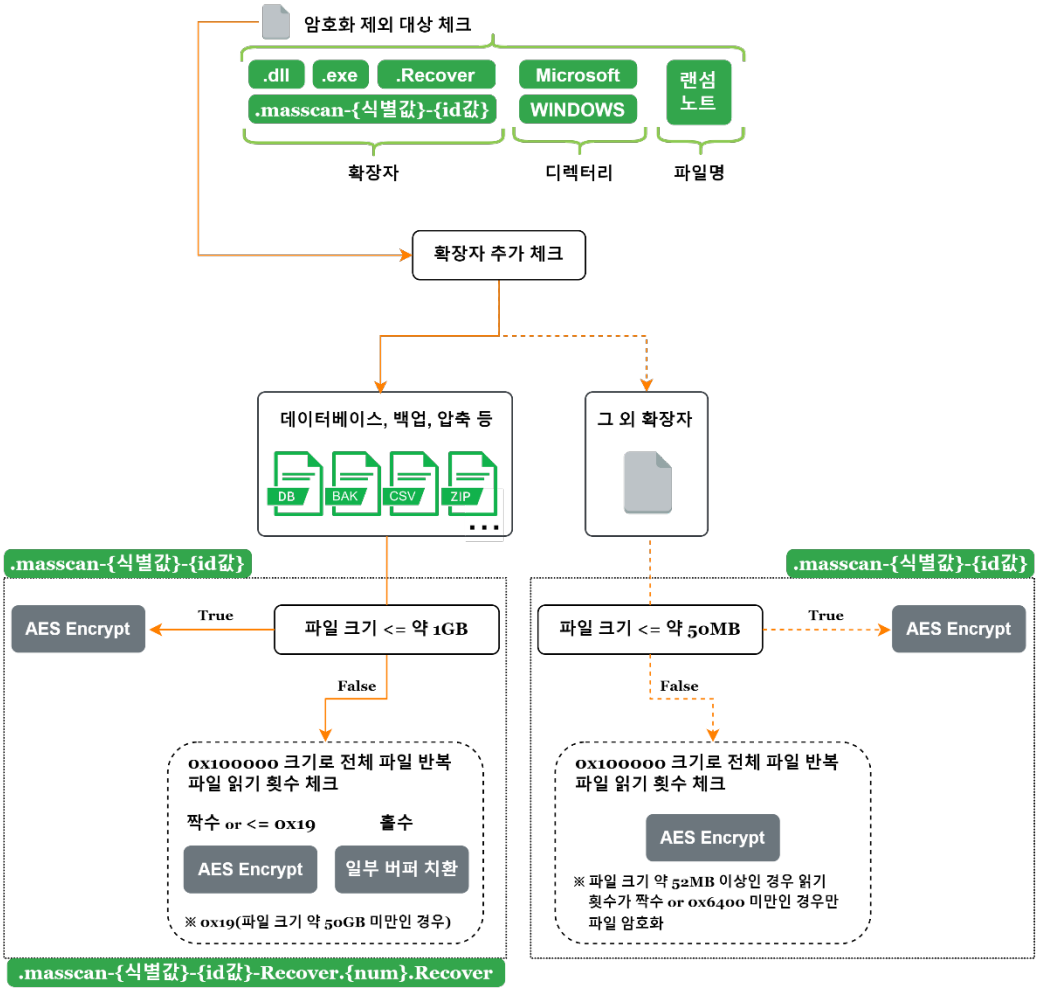


그림 11. Masscan 암호화 로직

- 파일 암호화 전 시스템 구동 및 복호화 방법을 정상적으로 안내하기위해 파일의 확장자 및 파일명을 체크하며 .dll, .exe, .Recover 확장자, 랜섬노트 파일명의 파일은 암호화 대상에서 제외된다. 데이터베이스 관련 파일, 백업 파일, 압축 파일 등을 체크하여 리스트와 동일한 경우 기존에 변경되는 확장자 뒤에 '-Recover.{Round number}.Recover' 문자열을 추가한 별도의 파일을 생성한다. 해당 파일은 추가적인 식별자를 포함하는 것으로 보이지만 파일을 삭제하고 있어 확인 목적으로 사용했을 가능성이 존재한다.
- 가장 최근에 수정된 파일을 우선순위로 암호화 대상 리스트를 생성하고 암호화 대상이 되는 파일의 크기를 체크하여 일정 크기 이상일 경우 파일의 일부분만 암호화하여 다수의 파일을 빠르게 암호화하는 로직을 사용하며 스레드를 통해 로컬 및 네트워크 드라이브의 파일 암호화 작업을 동시에 수행한다.

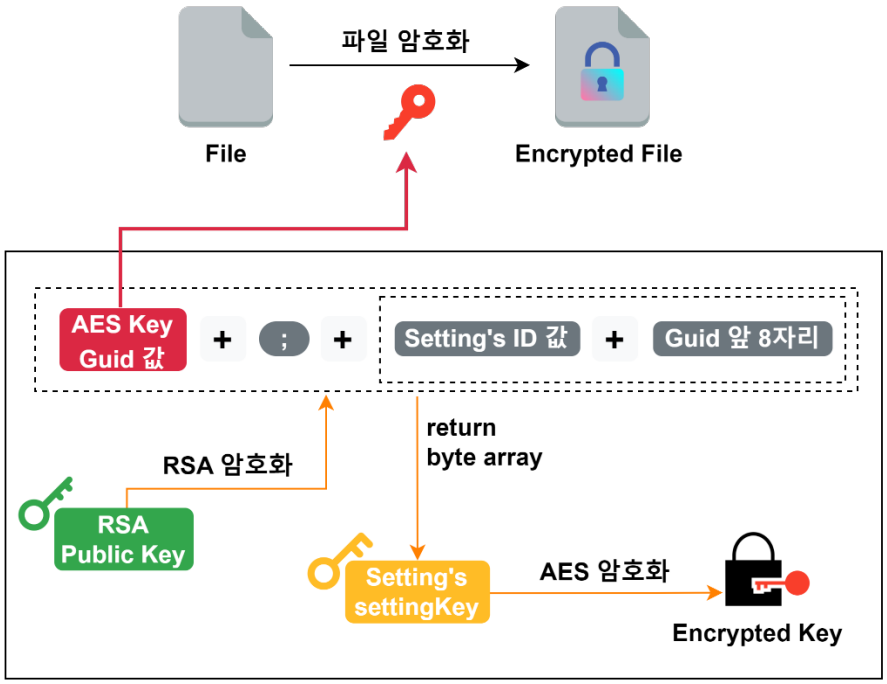


그림 12. 암호화 방식 및 암호화 키 값 보호

- 암호화에 사용된 알고리즘은 AES 대칭 키 방식을 사용하며 암호화 전 설정 값 로드 시 사용될 키 값을 불러온 뒤 RSA 암호화 알고리즘을 통해 키를 보호한다. 랜섬웨어 주요 동작을 수행하기 전 설정 값이 있는 파일로부터 필요한 값들을 로드 후 바로 삭제하기 때문에 공격자의 개인 키를 통해서만 복호화가 가능하다.
- 암호화 로직 중 파일 크기가 작은 경우에만 보호된 키 값을 파일 첫 부분에 저장을 하고 파일 크기가 큰 경우에는 저장하지 않는다. 한번 생성한 AES 대칭 키를 재사용하기때문에 빠른 작업을 위해 선택한 방식으로 보여진다.
- 탐지 및 사고 분석을 회피하기 위한 방법으로 앞서 언급한 config 파일 사용과 이벤트 로그를 삭제하고 공격에 사용한 도구 및 계정들을 삭제하여 흔적을 지운다.

3) IoC

SHA256	3E2B2F7E72226F935B4672A850A814E23C189830169B86073787BC7522C514BD 9B2DD07AEFB4FF495D876B23E8EF9D39B62B1385B82AF68D158006B9E1FE9A3F A9CAA7F0590C71C6FAF49E745347912C120C33AE2B57F0A9BC8CF001B08B7896 3F4B88A22813F7F808C4DB09093B6192F72B4AAD831A00607F6937505646A359
File name	EnCrypt.exe RunExe.exe
IPv4	23.216.147.64 23.216.147.76 20.99.133.109

■ 랜섬웨어 Mitigations

공격자는 공격대상을 선정하기위해 공격자 그룹이 수립한 전략을 통해 다양한 방법으로 정찰을 수행하며 이후 내부 인프라에 침입하여 파일을 암호화 시키고 자산을 위협하며 데이터 유출을 통한 협박을 시도한다. 이러한 피해를 예방하기위해 타겟형 APT 공격에 대한 대비와 침입에 대한 각 단계별 적절한 보안 요소 및 프로세스를 마련하여 공격자 그룹이 목표를 달성하기 전에 탐지하고 차단할 필요가 있다.

이를 위해 SK쉴더스 랜섬웨어 대응센터와 KARA는 랜섬웨어 대응 종합컨설팅이 가능한 One-Stop 서비스를 운영하고 있고, 현재 보안 수준을 확인하기 위한 무료 컨설팅도 제공하고 있다.

안녕을 지키는 기술 | SK 쉴더스

SK쉴더스㈜ 13486 경기도 성남시 분당구 판교로227번길 23, 4&5층
https://www.skshieldus.com

발행인 : SK쉴더스 EQST사업그룹 & KARA(Korea Anti Ransomware Alliance)
제　작 : SK쉴더스 커뮤니케이션그룹