KARA
Korea Anti Ransomware Alliance

2023.07.

KARA 랜섬웨어 동향 보고서

KARA 랜섬웨어 동향 보고서

■ 랜섬웨어 트렌드

✓ 랜섬웨어 트렌드 분석

랜섬웨어 그룹들은 지속적으로 공격을 수행하기 위해 새로운 랜섬웨어를 개발 및 테스트하고 있으며 데이터 탈취를 위한 도구를 제작해 활발한 공격을 수행하고 있다. 그 중 Play 그룹은 네트워크를 스캔하고 데이터를 탈취하는 Grixba, VSS[1]에서 파일을 탈취할 수 있는 VSS Copying Tool을 자체적으로 개발해 공격에 사용하기도 했다. 지속적인 위협세를 보이고 있는 LockBit 그룹은 4월에 Mac운영체제를 타깃으로 하는 랜섬웨어를 개발하고 곧이어 다크웹을 통해 QA(Quality Assurance) 테스터를 구하는 게시글을 올리기도 했다. 또한 6월 말에는 세계적인 반도체 기업 TSMC의 민감 데이터를 탈취했다고 주장했으나 TSMC 측에서는 서버 설정 및 구성 정보들이 유출되었다며 민감데이터는 유출되지 않았다고 밝혔다. 해당 사건에서 LockBit 그룹이 제시한 협상 금액은 현재까지 확인된 LockBit 그룹의 협상 금액 중 최고치인 7천만 달러(한화 기준 920억)이며 LockBit 그룹의 주장이 사실이라면 상당한 규모의 피해가 발생할 것으로 예상된다. IAB와의 협업을 통해 활발하게 활동중인 그룹들도 확인할 수 있었는데, 특히 지난 1분기에 공개적으로 IAB를 구인한 Bl00dy 그룹이 2분기에는 미국의 교육 분야를 타깃으로 다수의 피해를 입힌데 이어 BlackCat, LockBit 그룹들도 IAB와의 협업을 통해 지속적인 공격을 수행하고 있다. 한편 짧은 시간에 다수의 기업들을 공격하기위해 기업에서 많이 사용하는 소프트웨어들의 취약점을 찾아내고 이를 악용해 대규모 공격을 수행하는 Clop, Malas 그룹의 활동이 지속되고 있다. 특히 Clop 그룹은 2020년 12월에 대규모 공격을 수행한데 이어 올해 상반기에도 두 번에 걸쳐 대규모 공격을 수행하며 다수의 기업에 피해를 입혔다.

신규 랜섬웨어 및 그룹 활동

2분기에는 Akira, DarkAngels(DungHill), CryptNet, CrossLock, BlackSuit, Rancoz, Ra group, MalasLocker, WiperLeak, 8base, Shadow, Rhysida, Darkrace, Lapiovra, Noescape 총 15개의 랜섬웨어 그룹이 다크웹을 운영하며 이중 협박 전략을 사용하기 시작했다. 이 중 일부 그룹은 유출된 랜섬웨어의 소스코드 혹은 빌더를 사용한 것으로 보이는데, CryptNet 그룹은 Chaos 랜섬웨어, Shadow 그룹은 LockBit3.0 랜섬웨어, Lapiovra 그룹은 REvil/Sodinokibi 랜섬웨어, Ra group은 Babuk 랜섬웨어의 소스코드 및 빌더를 사용한 것으로 확인된다. 또한 BlackSuit 랜섬웨어는 Royal 랜섬웨어와 코드 및 동작 방식이 상당 부분 유사하여 리브랜딩이 아닌 그룹에서 새롭게 사용하기 시작한 서브 개념의 활동으로 보인다. Rancoz와 Vicesociety 랜섬웨어는 유출 사이트, 랜섬노트 등

[1] VSS : Volume Shadow Copy의 약자, 특정 시점의 데이터를 담고있는 스냅샷 또는 복원 지점

일부 유사성이 존재하는데 직접적인 관계를 나타내는 요소는 부족하여 그룹을 연관 짓기는 어렵다.

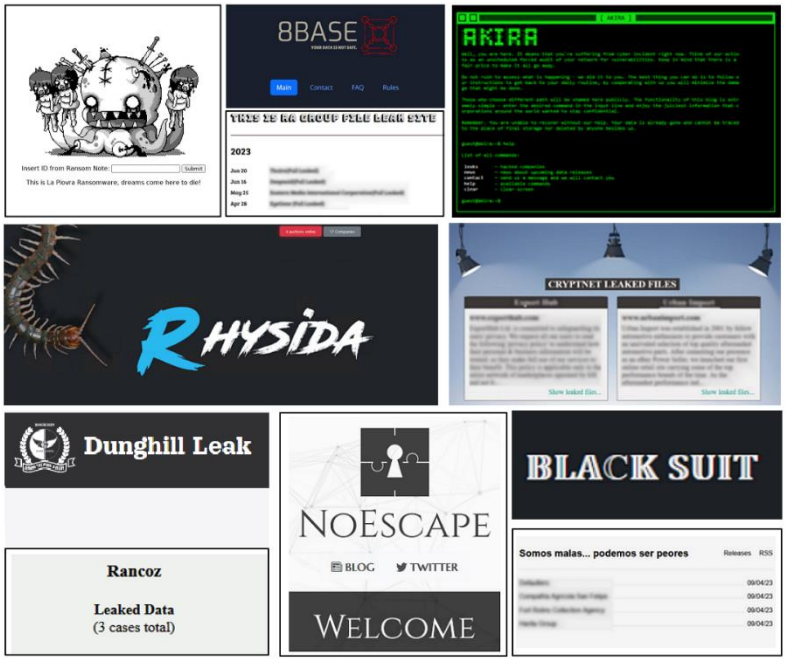


그림 1. 신규 랜섬웨어 다크웹 활동

기존에 활동을 해오던 랜섬웨어 그룹들이 새로운 다크웹을 운영하는 사례도 확인됐다. 2022년 5월부터 활동을 시작한 DarkAngels 그룹은 4월경 다크웹 유출사이트 DungHill을 운영하기 시작하였으며 8Base 그룹은 올해 5월부터 다크웹 운영을 시작함과 동시에 66건의 데이터를 게시하였는데 2022년 4월부터 게시한 데이터가 포함되어 있어 지속적인 활동을 이어오다 5월부터 이중 협박 전략을 시작한 것으로 보인다. 한편 8Base 그룹의 다크웹이 RansomHouse 그룹의 다크웹과 비슷해 일각에서는 RansomHouse 에서 비롯된 것으로 추측하고 있으나 일부 공격에 사용된 랜섬웨어는 Phobos 랜섬웨어의 변종 중 하나로 다양한 그룹의 랜섬웨어를 제공 받아 사용하는 것으로 보인다.

5월에 발견된 Malas 그룹은 취약한 Zimbra Collaboration Suite 소프트웨어를 사용하는 기업을 타깃으로 단기간에 171개의 기업의 네트워크에 침투하고 다크웹에 게시하는 등 대규모 공격을 수행해 다수의 피해자들을 협박하기 시작했다. 또한 일반적인 금전 갈취 방식과는 다르게 비영리 자선단체에 기부를 요구하는 것이 특징인데, 특히 랜섬 노트에는 공격 그룹의 이득이 아닌 기업과 경제적 불평등을 싫어한다는 이유로 자선단체 기부를 요구하는 내용이 포함되어 있으며 이는 단순 파괴, 암호 화폐 요구와는 사뭇 다른 의적처럼 보이는 협박이지만 실제 기부 후 정상적으로 복구 될지는 확신할 수 없다.

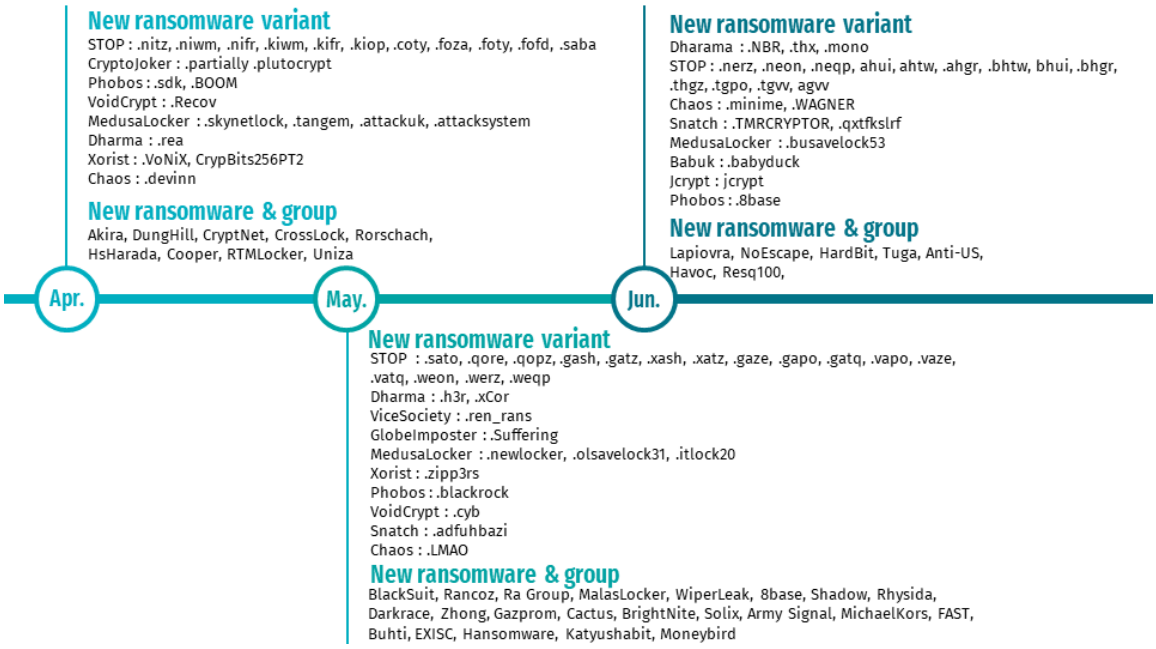


그림 2. 신규/변종 랜섬웨어 활동

4월 중순에는 LockBit 그룹에서 Mac운영체제를 타깃으로 하는 랜섬웨어를 개발 및 테스트하며 지속적인 활동을 이어갔다. 한편 같은 시기에 Rorschach 랜섬웨어가 발견됐는데, 해당 랜섬웨어는 Babuk 및 LockBit2.0과 코드가 유사해 BabLock(Babuk+LockBit)으로도 불리고 있다. 또한 현재까지 발견된 랜섬웨어 중 가장 빠른 암호화 알고리즘을 사용하고 있으며 발견되는 변종 마다 Yanluowang, DarkSide의 랜섬노트가 생성 되는 등 다양한 랜섬웨어로 보인다는 특징이 있다. Rorschach 랜섬웨어는 다크웹 운영, 버그 바운티, 다양한 홍보활동 등 공개적인 활동을 이어가는 LockBit 그룹과 상반되게 피해자와 직접 연락하고 대외활동을 하지 않는 등 은밀하게 활동하며 기업들을 타깃으로 공격을 수행하여 뒤늦게 그 존재가 밝혀지게 되었다.

랜섬웨어 공격 그룹 트렌드

지난 2월 취약한 ESXi서버를 노린 ESXiArgs 랜섬웨어의 여파로 전세계적으로 3,800개 이상의 서버가 감염되는 사례가 발생했으며 같은 달 파일 전송 소프트웨어 GoAnyWhere MFT(Managed File Transfer Software) 의 취약점(CVE-2023-0669)[2]을 악용한 Clop 그룹의 대규모 공격으로 인해 130개의 기업에 침해사고가 발생했다. 이어서 2분기에는 5월에 등장한 Malas 그룹이 이메일 및 협업

[2] CVE-2023-0669 : GoAnyWhere MTF 관리자 패널에서 발생하는 원격 코드 실행 취약점

소프트웨어 Zimbra Collaboration Suite의 취약점(CVE-2022-24682)[3]을 악용해 침투한 171개의 기업의 명단을 게시했으며 Clop 그룹은 파일 전송 소프트웨어 MOVEIt MFT의 취약점(CVE-2023-34362)[4]을 악용해 다시 한번 대규모 공격을 수행했다. 특히 Clop 그룹의 MOVEit 대규모 공격으로 인해 수백곳의 기업에 피해가 발생하였으며 6월에 그칠 줄 알았던 데이터 게시가 7월까지 지속되며 피해자가 계속해서 발견되고 있다. 이처럼 대규모 랜섬웨어 공격이 1분기와 2분기에 걸쳐 지속적으로 발생하고 있으며 공격자 및 그룹들은 기업에서 사용도가 높은 소프트웨어 및 솔루션들의 취약점을 악용해 광범위한 공격을 수행하고 있어 많은 피해가 발생하고 있다.

한편 국내에서는 BlackCat, BianLian, Ra group 등의 그룹에 의해 데이터가 유출되는 사고가 발생했으며, 일부 중소기업들이 Phobos 랜섬웨어에 감염되는 사례도 확인됐다. 특히 Phobos 랜섬웨어의 공격자들은 피해자에게 금액을 지불 받은 후에도 동일한 금액을 재 요구하는 등 공개적으로 활동하며 신뢰도를 쌓아가는 랜섬웨어 그룹과는 사뭇 다른 악질적인 행태를 보이고 있다.

대규모 공격

5월 27일, Progress 社의 파일 전송 소프트웨어 MOVEit에서 발견된 제로데이 취약점(CVE-2023-34362) 이 공격에 활발하게 쓰이는 정황이 확인됐다. 공격에 활용된 취약점은 운영체제의 명령어를 실행할 수 있는 SQL 인젝션 취약점으로 공격자는 이를 악용해 다수의 기업에서 데이터를 탈취한것으로 알려졌는데, 얼마 지나지 않아 Clop 그룹은 다크웹을 통해 해당 공격의 배후라고 밝혔으며 협상에 응하지 않은 기업들의 데이터를 6월 14일부터 공개할 것이라고 예고하였고 약 300여개의 기업에서 탈취한 데이터를 보유하고 있다고 밝혔다. Clop 그룹은 2020년 12월 Accellion FTA(File Transfer Appliance) 소프트웨어의 취약점을 악용해 100개의 기업에 공격을 수행한데 이어 2023년 2월에는 GoAnyWhere MFT 소프트웨어의 취약점을 통해 130개의 기업에 데이터를 탈취했으며, 5월 말부터는 MOVEit 소프트웨어의 취약점을 악용해 다수의 기업 데이터를 탈취하는 등 지속적으로 대규모 공격을 수행하고 있다.

[3] CVE-2022-24682 : 유효성 검사가 이루어지지 않아 Cross-Site-Scripting(XSS)이 발생하는 취약점

[4] CVE-2023-34362 : SQL 인젝션을 통해 운영체제의 명령어를 실행 할 수 있는 취약점

1. 랜섬웨어 그룹 활동 및 통계

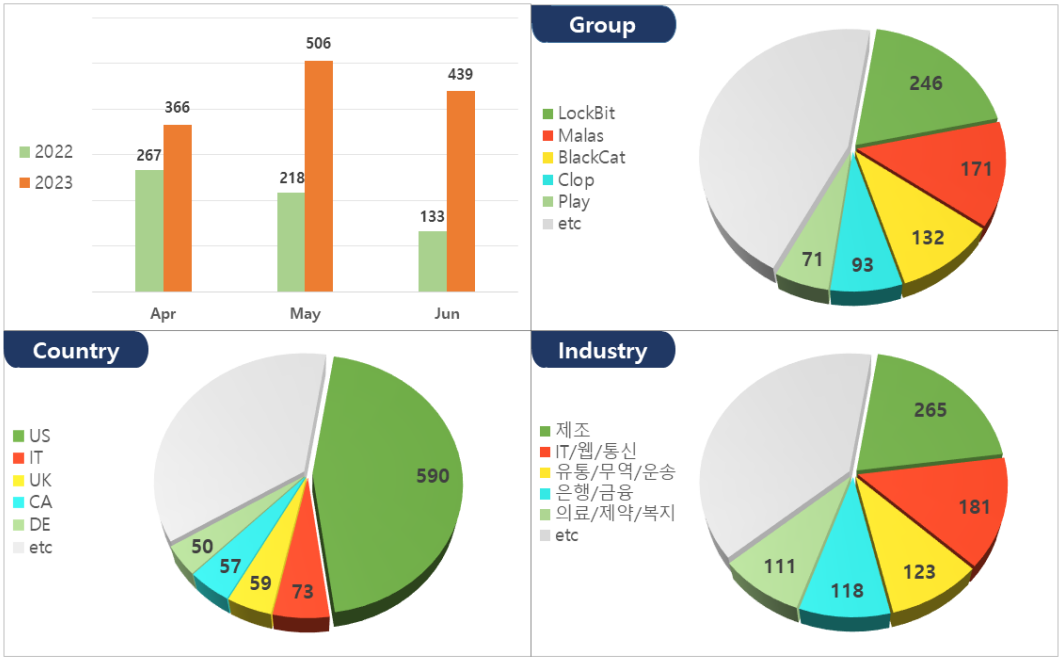


그림 3. 랜섬웨어 그룹 활동

랜섬웨어 피해가 작년에 비해 평균적으로 증가한 것을 확인 할 수 있다. 특히 5월과 6월에는 신규 랜섬웨어 그룹의 공격이 다수 발견되었고 Malas 그룹 및 Clop 그룹의 대규모 공격으로 인해 많은 사고 사례가 확인되었다. Malas 그룹은 5월부터 활동을 시작함과 동시에 Zimbra Collaboration Suite 소프트웨어의 취약점을 악용해 171개의 기업에서 탈취한 데이터를 유출했으며 4, 5월 동안 큰 활동을 보이지 않던 Clop 그룹은 MOVEit 취약점을 통해 탈취한 기업들의 데이터를 6월 14일부터 게시하기 시작했는데 6월 한달 동안 89개의 기업에서 탈취한 데이터를 다크웹에 게시했다. Clop 그룹에서 약 300여개의 기업에 공격을 수행했다고 공표한 만큼 추가적인 데이터 공개가 지속될 것으로 보인다. 또한 5월부터 다크웹을 운영한 8Base 그룹도 6월 한달 간 47개의 기업 데이터를 유출하는 등 활발한 활동을 보이고 있다. 한편 LockBit 그룹은 1분기에 비해 활동의 감소세를 보였는데, 랜섬웨어를 배포하는 데 관여한 혐의로 LockBit 계열사 일부가 체포되는 등 수사기관의 압박을 피하는 의도 혹은 대규모 공격으로 이목이 집중된 Clop 그룹을 의식해서 데이터 공개를 미루는 등 다양한 추론이 가능하다. 이어서 BlackCat, Play 그룹들은 기업을 타깃으로 지속적으로 피해를 입히고 있으며 피해국은 미국, 이탈리아, 영국 순으로, 산업군은 제조, IT, 유통업 순으로 피해가 발생하고 있다.

2. History of Clop

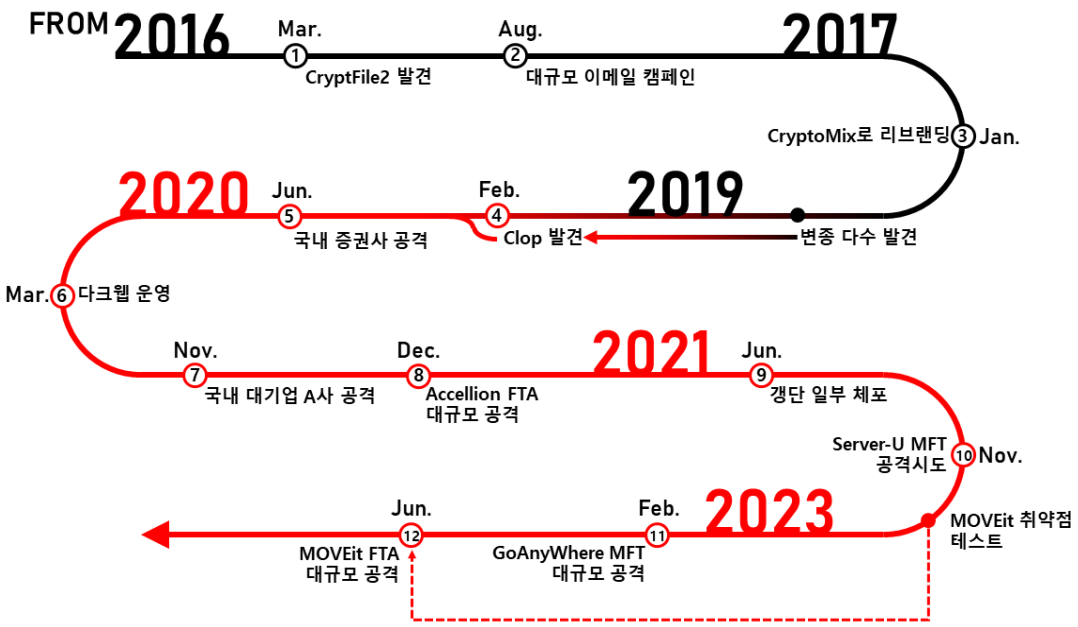


그림 4. Clop 연대기

Clop 랜섬웨어는 CryptoMix 의 변종으로부터 파생되었으며 최초 시작점을 살펴보면 2016 년 CryptFile2 랜섬웨어로부터 지속적인 리브랜딩을 통해 탄생되었다. 여기서 Clop(klop)은 러시아어로 인간과 동물의 피를 빨아먹는 벌레를 뜻하며 러시아 정부의 지원을 받는 TA-505 해킹 조직에서 운용중인것으로 알려져 있다.

Clop 랜섬웨어는 기존의 CryptoMix 랜섬웨어와 다르게 안티바이러스 우회, 특정 프로세스 종료, 유효한 디지털 서명을 포함 하는 등 여러 기능들이 추가되며 발전하기 시작했으며 기업들을 타깃으로 한 공격에 사용되기 시작했다. 또한 2020 년 3 월부터는 다크웹을 운영하며 이중 협박 전략을 사용하기 시작했는데, 같은 해 11 월에 국내 대기업 A 사에 공격을 수행하고 탈취한 데이터를 다크웹을 통해 유출하기도 했다.

2020 년 11 월, Clop 그룹은 파일 전송 프로그램 Accellion FTA 의 제로데이 취약점을 악용해 100 개 이상의 기업에 침투해 대규모 공격을 수행하는 등 활발한 활동을 이어갔다. 하지만 2021 년 6 월 한국, 우크라이나, 미국 경찰의 협력으로 Clop 그룹의 일부 구성원이 체포되면서 일각에서 Clop 활동에 차질이 생길 것이라 추측했으나 해당 사건 직후에도 다크웹을 통해 지속적으로 피해자들의 데이터를 게시하며 행보를 이어 나갔으며, 2023 년 1 월에는 GoAnyWhere MFT

소프트웨어의 취약점을 악용해 130 개의 기업에 피해를 입힌데 이어 5 월 말 부터는 MOVEit MFT 취약점을 통해 대규모 공격을 수행하는 등 현재까지 지속적인 위협세를 이어가고 있다.

- **Clop 리브랜딩**

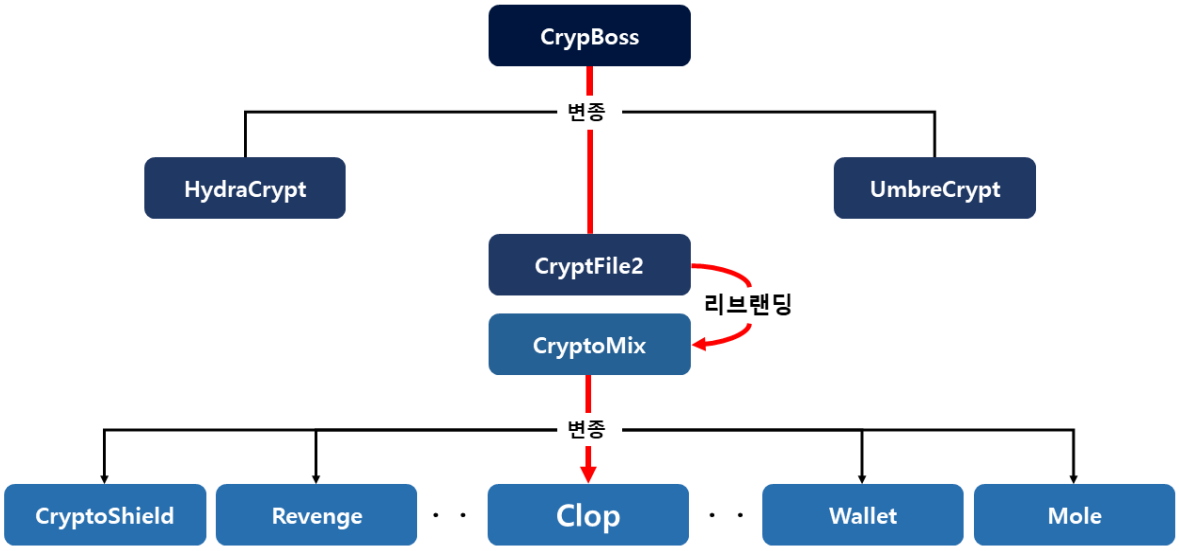


그림 5. Clop 가계도

CryptFile2 랜섬웨어

CryptFile2 랜섬웨어는 2016 년 3 월부터 Nuclear, Neutrino 등의 Exploit Kit[5]을 통해 유포되기 시작했으며 2016 년 8 월 미국의 정부기관 및 교육기관을 타깃으로 한 대규모 이메일 공격에서 사용되기도 했다. CryptFile2 랜섬웨어는 CrypBoss 의 변종인 HydraCrypt 랜섬웨어와 코드가 유사할 뿐 만 아니라 협상 시 사용되던 이메일 주소가 CrypBoss 의 변종인 HydraCrypt, UmbreCrypt 랜섬웨어에도 사용되었기 때문에 CrypBoss 의 변종으로 추측됐으며, 협상 금액은 0.5~1.5 비트코인(당시 원화기준 20 만원~60 만원)으로 알려져 있다.

CryptoMix 랜섬웨어

2017 년 1 월, CryptFile2 랜섬웨어가 CryptoMix 랜섬웨어로 리브랜딩 되었다. 여기서 CryptoMix 는 CryptoWall 과 CryptXXX 랜섬웨어에서 파생된 것으로 추측되며 그 이유는 CryptoMix 랜섬웨어

[5] Exploit Kit : 다양한 소프트웨어들의 취약점을 이용해 악성코드를 유포하는 도구

실행 시 생성되는 2 개의 랜섬노트가 각각 CryptoWall 과 CryptXXX 의 랜섬노트와 같았기 때문이다. 협상 금액은 5 비트코인(당시 원화기준 400 만원) 이였으며 2019 년 4 월까지 CryptoShield, Revenge, Wallet, Mole 등 다수의 변종이 발견된 가운데 2019 년 2 월에 Clop 이라는 이름의 변종이 발견되었다.

- **Clop 그룹, 서막을 올리다**

2019 년 2 월, CryptoMix 랜섬웨어의 변종으로 발견된 Clop 랜섬웨어는 안티바이러스 우회, 특정 프로세스 종료, 유효한 디지털 서명을 포함 하는 등 다양한 기능들을 추가하며 발전하기 시작했다. Clop 랜섬웨어는 국내 뿐만 아니라 전세계를 타깃으로 한 피싱 캠페인에 사용되기 시작했는데 해당 피싱 공격은 공격 대상을 명확히 지정하고 수신자의 언어에 맞춰 정교하게 작성한 메일로 스피어 피싱 공격을 수행했다는 점, PC 에서 러시아어를 사용중인 경우 암호화를 하지 않는 점, 첨부 파일 실행 시 TA-505 조직에서 제작한 RAT[6] 악성코드 SDBBot, FlawedGrace 가 실행된다는 점에서 러시아 배후 해킹 조직 TA-505 에서 운용중인 랜섬웨어 그룹으로 알려져 있다.

1) Clop 랜섬웨어의 진화

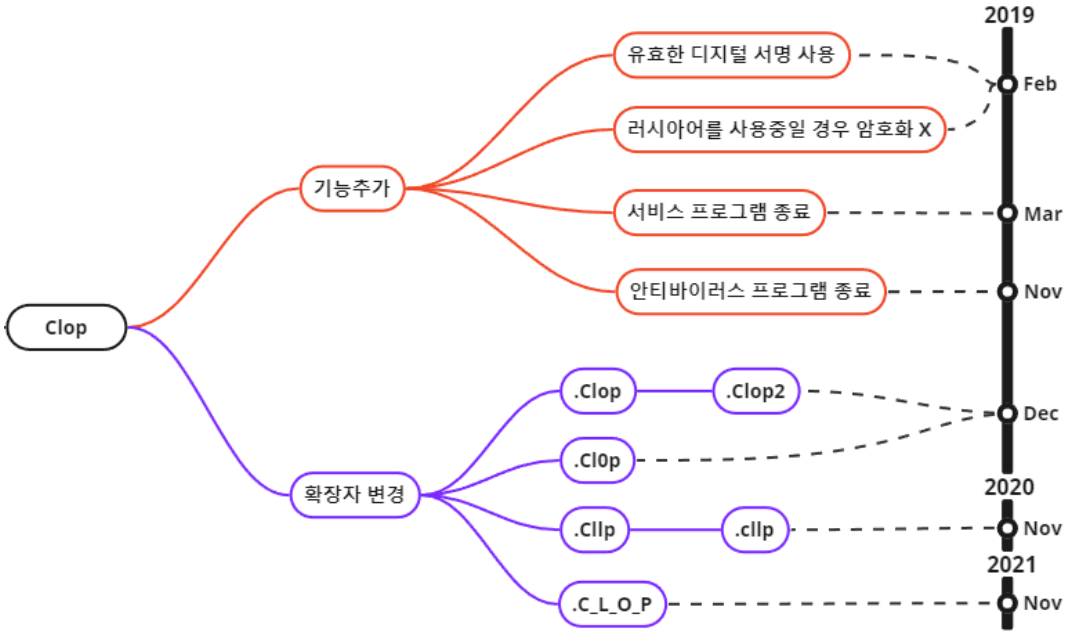


그림 6. Clop 랜섬웨어의 진화

[6] RAT : Remote Access Trojan의 줄임말으로, 원격으로 컴퓨터를 제어하는 악성코드의 일종

Clop 랜섬웨어는 기존 CryptoMix 랜섬웨어와 다르게 다양한 기능들이 추가되며 발전하기 시작했다. 특히 Microsoft SQL Service, MySQL, BackupExec와 같은 특정 서비스 프로그램 및 Kaspersky, Window Defender와 같은 안티바이러스 제품을 종료 시키는 루틴이 추가되었고, 실행중인 PC에서 사용중인 언어를 확인해 러시아어를 사용하는 경우 데이터를 암호화하지 않고 종료하는 기능이 추가 되었다.

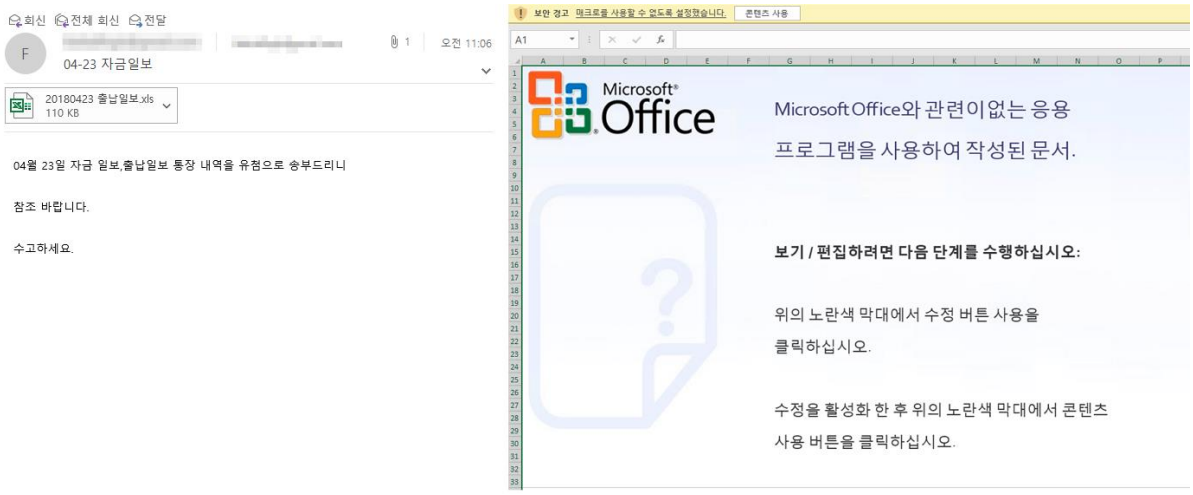


그림 7. 스피어 피싱 메일 및 악성 파일

이렇게 발전한 Clop 랜섬웨어는 2019년 2월부터 스피어 피싱을 통한 공격에 사용되기 시작했다. 공격자들은 공격 대상을 명확하게 지정한 뒤 본문 내용 또한 수신자의 언어에 맞춰 정교하게 작성해 공격을 수행했다. 또한 공격 과정 중 시스템이 Active Directory[7](AD) 환경일 경우 추가로 악성코드를 다운받는 DownLoader 악성코드가 발견되었는데, AD는 주로 기업에서 사용하는 환경으로써 공격자들이 기업을 타깃으로 공격을 준비한 것을 알 수 있다. 해당 스피어 피싱 공격 사례는 국내에서도 다수 확인됐으며 국세청 홈텍스, e-티켓을 위장한 공격자들의 이메일들이 발견되기도 했다.

[7] Active Directory : 기업 네트워크 환경에서 사용자, 컴퓨터 등의 리소스를 중앙에서 관리하는 서비스

2) 본격적인 활동의 시작

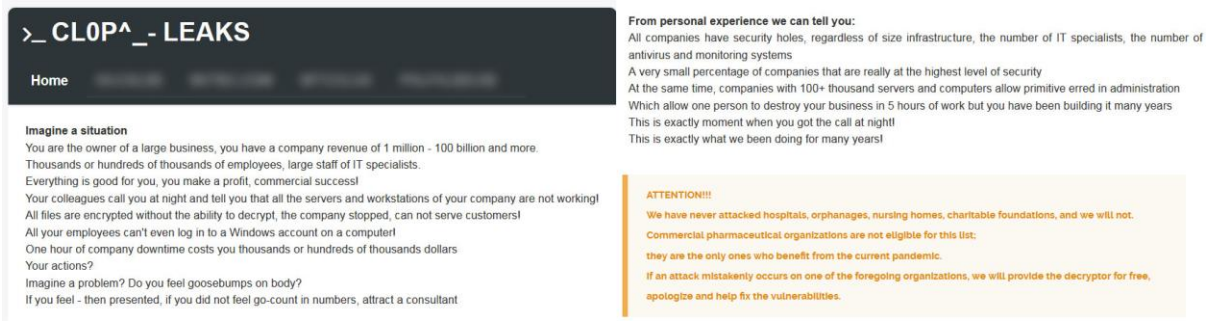


그림 8. Clop 다크웹 활동

기업들을 타깃으로 지속적인 공격을 이어오던 Clop 그룹은 2020년 3월부터 "CL0P^_- LEAKS" 라는 이름으로 다크웹을 운영하기 시작했다. 이들은 다크웹을 개설한 직후 일정 금액 지불 시 보안 컨설팅을 제공한다는 글을 게시했으며 병원, 고아원, 요양원, 제약사 등 특정 산업군에 대한 공격이 발생할 시 복호화 도구 제공 및 인프라의 취약점을 보완해주겠다는 글을 게시하는 등 자체적인 규칙을 세워 이중 협박 전략을 사용하기 시작했다.

한편 같은 해 12월부터 Accellion FTA 소프트웨어의 취약점을 악용한 데이터 탈취 공격이 발생하기 시작했는데, Accellion FTA는 주로 기업에서 사용하는 대용량 파일 전송 프로그램으로 해당 소프트웨어를 사용하는 100개 이상의 기업 시스템이 침해를 받은 것으로 확인됐다. 이후 2022년 1월, Clop 그룹이 회사 관계자들에게 메일을 통해 이중 협박을 하기 시작하면서 해당 사건의 배후가 드러났으며 Clop 그룹은 탈취한 데이터를 2월부터 게시하기 시작했다.

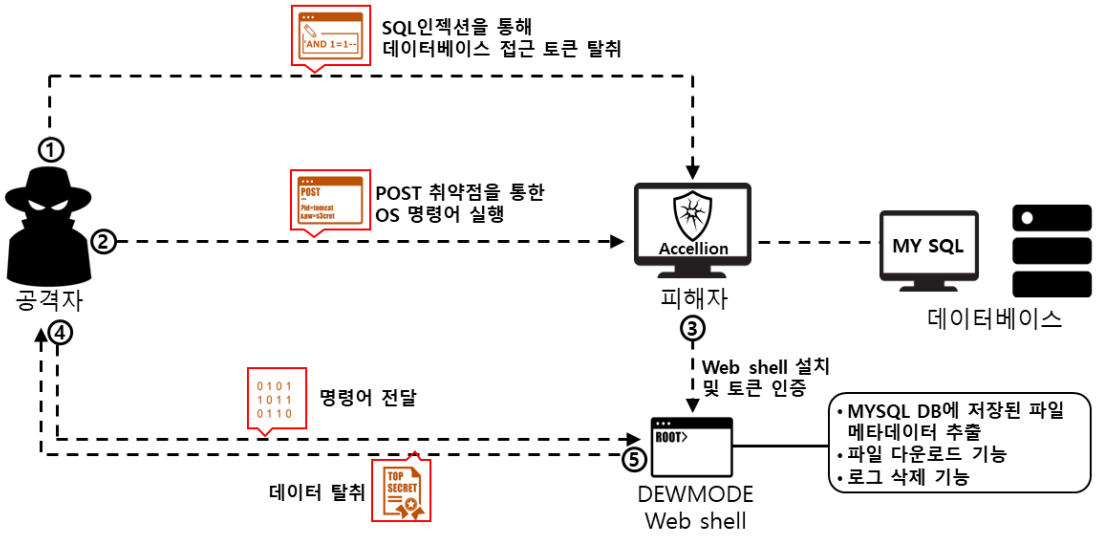


그림 9. Accellion FTA 취약점 악용 시나리오

Clop그룹은 당시 발견되지 않았던 Accellion FTA의 제로데이 취약점 (CVE-2021-27101[8], CVE-2021-27102[9], CVE-2021-27103[10], CVE-2021-27104[11])을 악용해 공격을 수행했다. 공격자들은 SQL 인젝션 취약점을 통해 데이터베이스에 접근 가능한 토큰을 탈취 한 뒤, POST 요청에서 발생하는 취약점을 이용해 DEWMODE Web shell을 다운받도록 하는 OS 명령어를 실행시켰다. 여기서 사용된 DEWMODE Web shell은 데이터베이스에 존재하는 파일들의 메타데이터를 조회하는 기능, 파일을 다운로드하는 기능, 웹 로그 삭제와 같은 기능이 포함 되어있는 Clop 그룹에서 자체적으로 개발한 Web shell으로, 공격자들은 해당 Web shell을 통해 데이터를 탈취하고 사고 조사를 방해하기 위해 웹 로그를 삭제한 것으로 확인됐다.

한편 2021년 6월 한국, 우크라이나, 미국 경찰의 협력으로 Clop 그룹의 돈세탁에 연루된 6명의 구성원이 체포되면서 일각에서는 해당 사건으로 인해 Clop 그룹의 활동에 차질이 생길 것이라 추측했으나 직후에도 다크웹을 통해 피해자들의 데이터를 게시하며 지속적으로 행보를 이어 나갔으며 11월에는 파일전송 소프트웨어 Server-U의 취약점을 찾아 공격에 사용하는 정황이 발견되기도 했다.

---

[8] CVE-2021-27101 : Http 헤더를 제대로 검증하지 않아 SQL 인젝션이 가능한 취약점

[9] CVE-2021-27102 : 웹 서비스 호출과정에서 발생하는 OS 명령어를 실행할 수 있는 취약점

[10] CVE-2021-27103 : POST 요청을 제대로 검증하지 않아 서버의 요청을 위조할 수 있는 취약점

[11] CVE-2021-27104 : POST 요청을 제대로 검증하지 않아 OS 명령어 실행이 가능한 취약점

3) 지속되는 대규모 공격

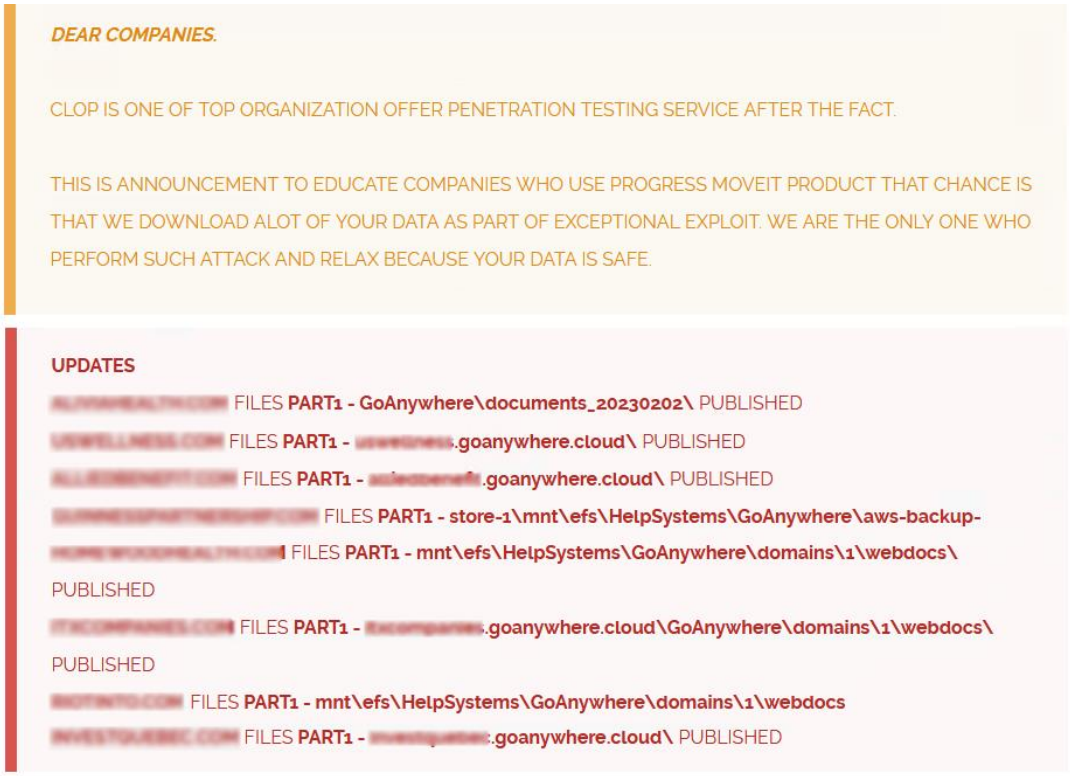


그림 10. GoAnyWhere, MOVEit 데이터 게시

Clop그룹은 Accellion FTA 소프트웨어의 제로데이 취약점을 악용해 대규모 공격을 수행 한 데 이어 2023년 2월에는 GoAnyWhere MFT, 5월에는 MOVEit MFT 소프트웨어의 제로데이 취약점을 악용해 다수의 기업을 공격했다. 여기서 주목할 점은 주로 기업에서 사용되는 소프트웨어 또는 솔루션의 취약점을 악용해 다수의 기업에 침투했다는 점, 랜섬웨어를 사용하지 않고 오로지 데이터만 탈취했다는 점이다.

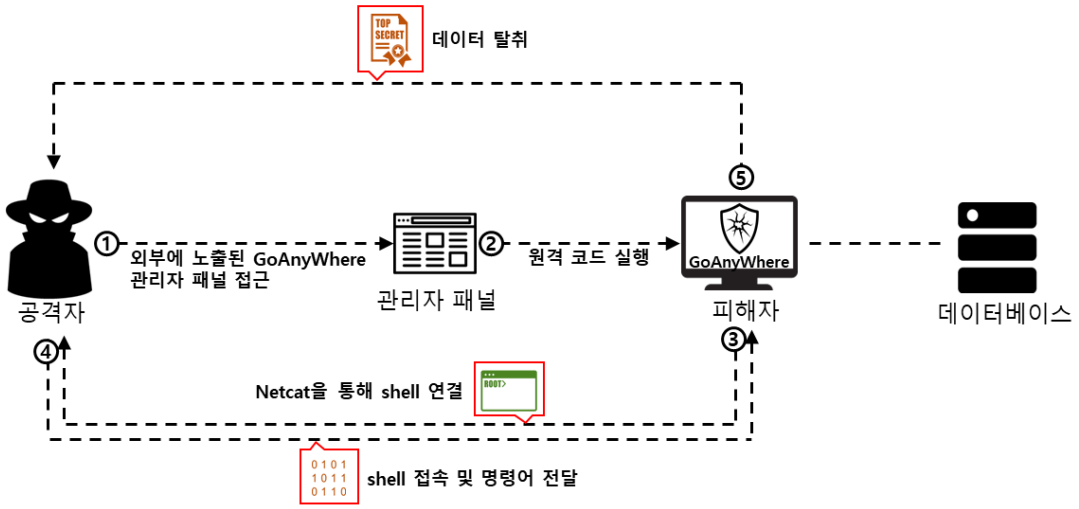


그림 11. GoAnyWhere MFT 취약점 악용 시나리오

2023년 2월, Clop 그룹에 의한 대규모 공격이 다시 한번 발생했다. 공격자들은 파일전송 소프트웨어 GoAnyWhere MFT에서 제로데이 취약점을 찾아 악용했으며 각국의 기관 및 기업을 포함해 총 130곳 이상에 피해가 발생한 것으로 알려졌다. 공격자들은 인터넷상에 노출된 GoAnyWhere 관리자 패널을 통해 원격 코드 실행 취약점을 악용했고, 지정된 대상과 데이터를 송수신 하게 해주는 Netcat 유틸리티를 실행시켜 공격자와 피해자간의 shell을 연결한 뒤 내부 데이터를 탈취하는 식으로 공격을 수행했다.

4월에는 기업에서 자주 사용되는 프린트 관리 솔루션 PaperCut 소프트웨어의 취약점을 사용해 공격을 수행한 정황도 확인 됐다. 악용된 취약점은 CVE-2023-27350[12], CVE-2023-27351[13] 취약점으로 Clop 그룹뿐만 아니라 LockBit, Bl00dy 그룹에서도 공격에 사용한 취약점이다. Clop그룹은 PaperCut 소프트웨어의 원격 코드 실행 취약점을 통해 TrueBot[14] 악성코드를 다운로드 한 뒤, TrueBot 악성코드를 통해 Cobalt Strike Beacon[15]을 피해자의 PC에 전달했고, 내부 네트워크 및 시스템을 정찰 한 뒤 파일 공유 유틸리티인 MegaSync를 사용해 내부 데이터를 탈취하는 방식으로 공격을 수행했다.

---

[12] CVE-2023-27350 : PaperCut 소프트웨어를 통해 원격코드 실행이 가능한 취약점

[13] CVE-2023-27351: PaperCut 소프트웨어의 인증을 우회하고 사용자 정보를 추출할 수 있는 취약점

[14] TrueBot : TA-505 조직에서 제작한 파일 다운로드 기능을 수행하는 악성코드

[15] Cobalt Strike Beacon : 모의 침투용 소프트웨어 Cobalt Stike 에서 공격자가 원격으로 시스템을 제어하기 위해 사용하는 도구

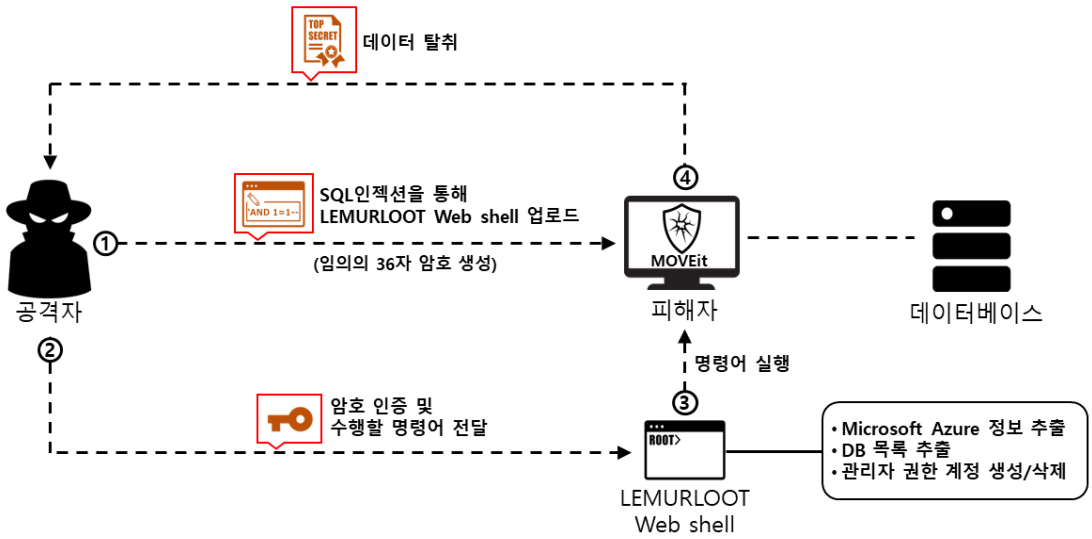


그림 12. MOVEit MFT 취약점 악용 시나리오

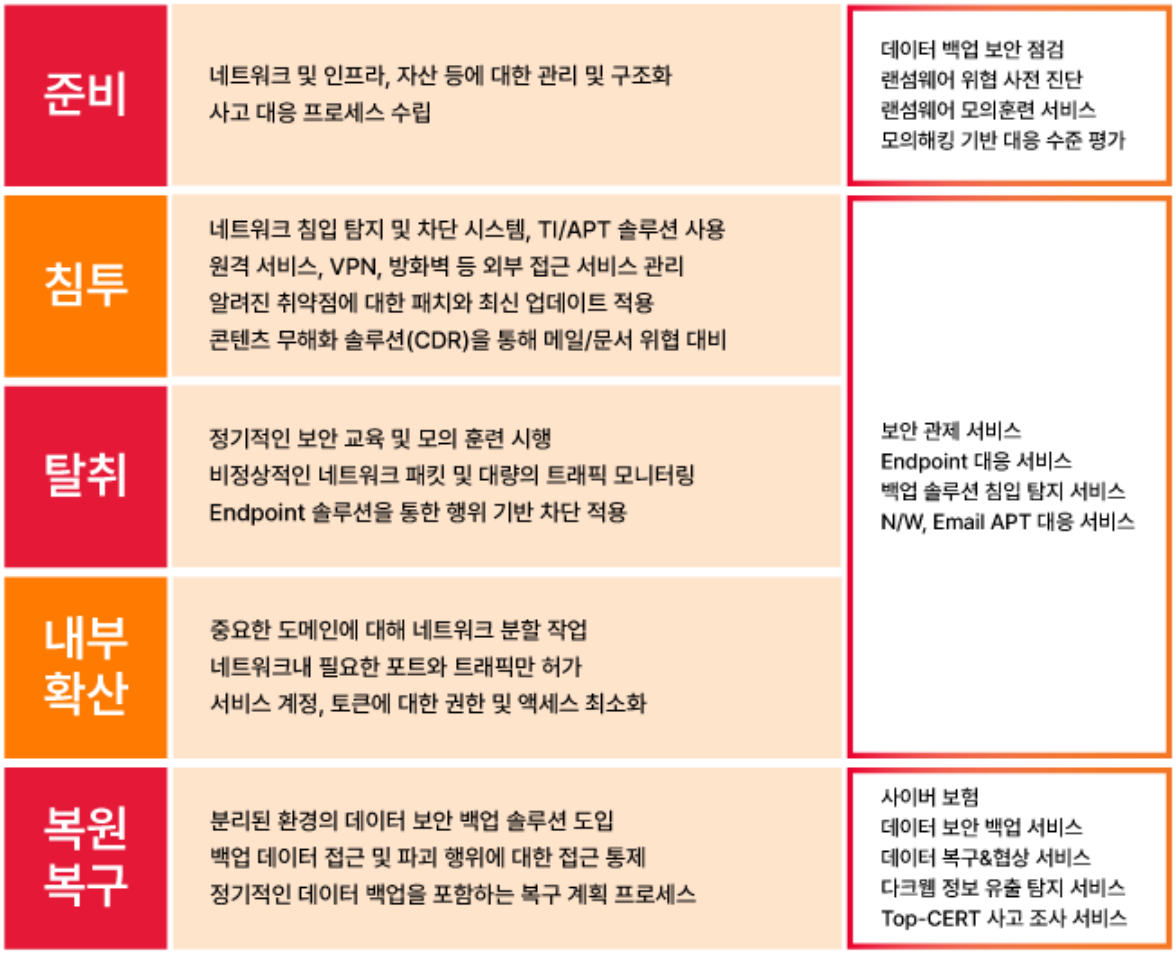
5월 말에는 Progress 社의 파일 전송 소프트웨어 MOVEit의 취약점을 악용해 또 한번 대규모의 공격을 수행했다. 피해 발생 초반에는 정확한 공격 배후가 밝혀지지 않았으나 6월 5일 Clop 그룹이 다크웹을 통해 MOVEit 취약점을 통한 대규모 공격이 자신들의 소행임을 주장했으며, 협상이 이루어지지 않은 기업들의 데이터를 6월 14일부터 게시하기 시작해 6월 한달 동안 89개의 기업에서 유출한 데이터가 게시되었다. Clop 그룹은 공격을 수행하기 위해 MOVEit 소프트웨어에 존재하는 SQL 인젝션 취약점을 이용해 LEMURLOOT Web shell을 설치했는데, 여기서 사용된 Web shell은 Clop 그룹이 자체적으로 제작한 것으로 MS Azure 서버의 구성 정보를 출력하는 기능, 파일 검색 기능, 관리자 권한 계정을 생성/삭제하는 기능이 포함되어 있다. 또한 Web shell에 접근하기 위해서는 HTTP 헤더를 통해 36자의 암호를 전송해야 하며 암호가 입력되지 않거나 일치하지 않을 경우 404 오류페이지를 띄워 존재하지 않는 페이지로 위장했다. 이 후 공격자는 해당 Web shell을 통해 내부 데이터베이스의 데이터를 탈취한 것으로 확인된다.

그림 13. Rewards of Justice

Acellion FTA, GoAnyWhere MFT, MOVEit MFT 등 기관 및 기업에서 자주 사용되는 소프트웨어들의 취약점을 악용해 단기간에 대규모 공격을 수행하는 Clop 그룹의 위협이 증가하고 미국 정부 및 주요 기관 일부에서도 Clop 그룹에 의한 피해가 발생하자 미국 국무부의 보상 프로그램 중 하나인 Rewards of Justice(RFJ)에서 Clop 그룹에 대한 정보를 제공 할 경우 천만 달러의 보상금을 지급하겠다는 글을 게시하며 적극적인 대응을 시작했다. 해당 보상프로그램은 미국에서 Clop을 국가 배후 그룹으로 판단하고 정부 및 주요 기관의 피해를 줄이기 위한 목적으로 실행되었지만, Clop 그룹은 다크웹을 통해 정부의 데이터는 크게 관심이 없으며 오로지 재정적인 동기에 의한 공격만을 수행하고 있다며 이를 부인하고 있다.

■ 랜섬웨어 Mitigations

Clop 그룹은 지난 4 년간 기업을 타깃으로 지속적으로 공격을 수행해왔으며 특히 올해 상반기에는 기업에서 주로 사용되는 소프트웨어의 취약점을 악용해 현재까지 260 개 이상의 기업에 데이터를 탈취하고 게시하였다. 이처럼 공격자는 공격자 그룹이 수립한 전략을 통해 다양한 방법으로 취약점을 탐색해 내부 인프라에 침입하고 파일 암호화 및 데이터 유출을 통해 협박을 시도한다. 이러한 피해를 예방하기 위해 타깃형 APT 공격에 대한 대비와 침입에 대한 각 단계별 적절한 보안 요소 및 프로세스를 마련하여 공격자 그룹이 목표를 달성하기 전에 탐지하고 차단할 필요가 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