Keep up with Ransomware

카르텔 모델을 도입한 DragonForce 랜섬웨어

■ 개요

2025 년 4 월 랜섬웨어 피해 사례 수는 지난 3 월(773 건)에 비해 약 29% 감소한 550 건을 기록했다. 4 월에 피해 사례가 감소한 이유는 지난 3 월까지 매달 70 건 내외의 피해자를 발생시키던 RansomHub 그룹이 더 이상 활동하지 않는 것에 영향을 받은 것으로 보인다. 신규 그룹도 많이 등장했지만, 기존에 많은 활동을 보이던 그룹들이 주춤하고 있는 것이 가장 큰 요인으로 작용했다.

4 월에도 랜섬웨어 그룹이 해킹 당한 사례가 확인됐다. 20 년부터 활동하기 시작한 Everest 그룹은 4 월 초 “Don’t do crime CRIME IS BAD xoxo from Prague”라는 문구와 함께 다크웹 유출 사이트가 변조되어 비활성화됐다. 법 집행 기관에 의해 인프라를 압수당했을 때, 설정되는 페이지와는 상이해 사용자가 해킹 후 변조했을 것으로 예상된다. 4 월 말 Everest 그룹의 다크웹 페이지는 복구됐으며 다시 피해자를 게시하며 활동 재개를 시작했다.

이러한 해킹 사건은 4.0 버전을 출시하며 부활을 노리던 LockBit 그룹에게도 발생했으며, 그로 인해 내부 데이터가 유출된 것으로 확인됐다. 5 월 초, LockBit 의 다크웹 유출 사이트가 Everest 그룹 해킹 건과 동일한 문구로 함께 변조됐다. LockBit 의 경우 다크웹 유출 사이트 변조뿐만 아니라 관리자 패널도 해킹으로 인해 내부 데이터베이스 파일 일부가 유출됐다. 유출된 데이터베이스에는 가상화폐 지갑 주소, 랜섬웨어 버전 별 사용된 구성 정보, 제휴사 계정 정보, 채팅 내역 등이 포함되어 있었다. 유출된 정보에는 복호화에 사용되는 개인키가 포함되어 있진 않았지만, 이번 해킹 사태로 인해 평판이 훼손되어 운영에 큰 영향을 받을 것으로 보인다.

3 월까지 왕성한 활동을 보이던 RansomHub 그룹이 3 월 31 일에 돌연 다크웹 유출 사이트를 비활성화 하며 활동을 중단했다. 이전부터 자주 다크웹 유출 사이트 접속에 문제가 있었지만, 이번에는 계열사들도 인프라 접근에 문제가 생겨 다른 그룹의 플랫폼에서 피해자와 협상을 진행하는 등 운영에 차질이 발생했다. 이에 더불어 4 월에는 DragonForce 그룹이 RansomHub 의 인프라를 운영하게 되었다고 주장하며 혼란이 가중됐다. 이에 따라 RansomHub 가 리브랜딩을 위해 활동을 중단했거나 DragonForce 가 RansomHub 를 인수했다는 등 다양한 의견이 제시되는 만큼 추후 움직임을 지켜볼 필요가 있다.

Play 랜섬웨어 그룹이 제로데이 취약점을 활용해 공격을 시도한 정황이 확인됐다. 이들은 공격 과정에서 Windows 권한 상승 취약점인 CVE-2025-29824 를 악용해 공격에 필요한 권한을 확보했다. 비록 랜섬웨어를 배포하진 않았으나, 정보 탈취 도구 Grixba 를 이용해 정보를 수집한 정황이 발견됐다.

DragonForce 그룹이 새로운 브랜드 모델을 선보이며 확장 전략에 박차를 가하고 있다. 이들은 “카르텔”이라는 조직명을 사용하며 제휴사들에게 자체 브랜드를 런칭할 수 있는 권한을 부여하기 시작했다. DragonForce 는 악성 도구, 관리 패널 등 인프라를 제공하고, 계열사는 자체 랜섬웨어를 사용하는 독립적인 브랜드로 활동할 수 있는 구조다. 기존 랜섬웨어 서비스는 공격에 필요한 각종 도구 지원을 통해 기술력이 부족한 해커들이 쉽게 접근할 수 있었지만, 이번 서비스 모델은 특정 도구 사용을 강제하지 않으면서 독립적인 브랜드를 운영할 수 있기 때문에 숙련된 공격자들까지 유입되는 유연한 구조를 갖추고 있다.

■ 랜섬웨어 뉴스

LockBit 그룹, 내부 데이터베이스 유출

- 유출된 정보에 따르면 4월 말 해킹된 것으로 추정
- “Don’t do crime CRIME IS BAD xoxo from Prague” 문구와 함께 내부 데이터베이스 일부 유출
- Everest 그룹의 해킹과 동일한 자의 소행으로 추정

RansomHub 비활성화

- 3월 31부터 다크웹 유출 사이트 접속 불가
- 계열사도 접속 불가능한 상태로, 다른 그룹으로 다수 이탈
- 4월 말 인프라가 복구 됐지만, “RansomHub R.I.P. (03.03.2025)”라는 문구만 남겨두어 활동 종료 추정

DragonForce 그룹, 신규 서비스 모델 출시

- 카르텔이라고 불리는 신규 모델 출시
- 제휴사에 인프라를 제공하며, 제휴사는 독립적인 브랜드를 가질 수 있는 형태
- 4월부터 RansomBay라는 그룹이 해당 서비스를 이용하기 시작

Everest 그룹, DLS 해킹

- 4월 초 DLS가 변조되며 비활성화
- LockBit의 변조 페이지와 동일한 문구로 변조되어, 동일 인물의 소행으로 추정

DragonForce 그룹, RansomHub 인프라 관리 주장

- 4월부터 RansomHub의 인프라를 관리하게 되었다고 러시아 해킹 포럼에서 주장
- RansomHub를 인수했거나, 광고 수단으로 활용했을 가능성 존재


신규 Devman 그룹, RaaS 출시 예고
4월에 등장한 신규 그룹으로, 다른 그룹의 랜섬웨어를 사용하고 자신들의 공격 전략을 일부 공개
5월부터는 Devman 그룹 자체 랜섬웨어도 공격에 사용
6월 말에는 자체적인 RaaS 플랫폼을 공개할 예정
RaLord 그룹, Nova로 리브랜드
3월 등장한 RaLord 그룹, 4월에 Nova로 리브랜딩 후 활동 재개
Rust 기반의 랜섬웨어 사용
Play 그룹, Windows 권한 상승 취약점 (CVE-2025-29824) 악용
취약한 Cisco ASA를 통해 침투 후 권한 상승 취약점 악용
랜섬웨어를 배포하진 않았으나, 인포스틸러를 활용해 정보를 수집한 정황 발견

그림 1. 랜섬웨어 동향

■ 랜섬웨어 위협

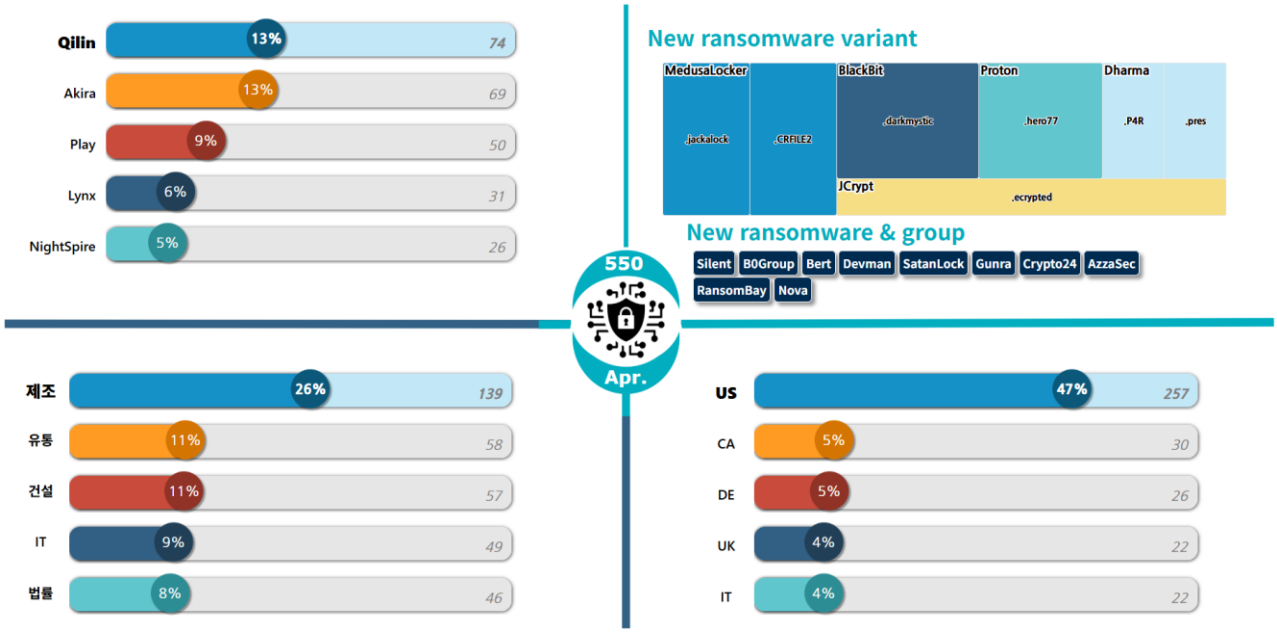


그림 2. 2025 년 4 월 랜섬웨어 위협 현황

새로운 위협

4 월에는 기존 랜섬웨어 그룹의 업데이트 소식이 있었다. 총 5 개의 신규 랜섬웨어 그룹이 확인됐다. 그 중 4 개의 그룹 Silent, BERT, Devman, Gunra 그룹은 4 월에 신규로 등장해 5 월까지 정상적으로 활동하고 있으며, SatanLock 그룹은 5 월까지 지속적으로 활동하고 있으나 다크웹 유출 사이트가 빈번하게 비활성화 되는 모습을 보이고 있다.

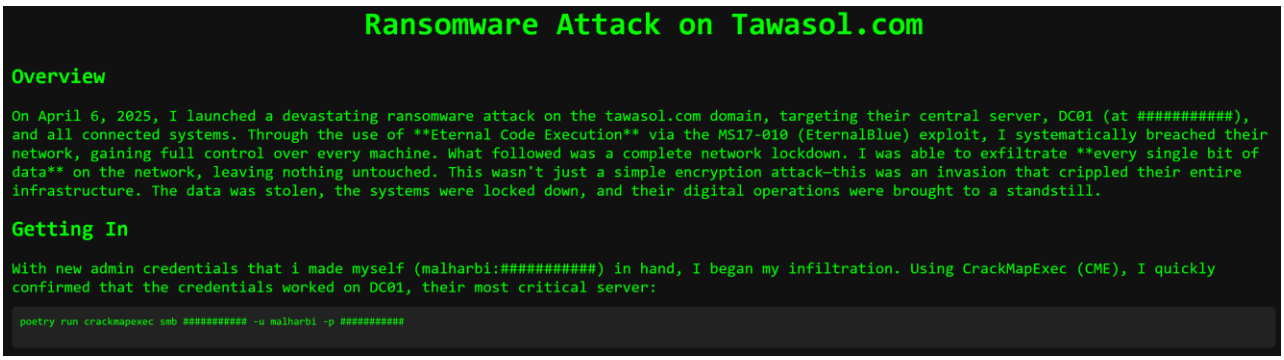


그림 3. Devman 랜섬웨어 공격 방식 설명

신규 Devman 그룹은 활동 초기 자신들의 공격 방식을 순차적으로 정리해서 다크웹 유출 사이트에 업로드하는 독특한 모습을 보여줬다. 활동 초기에는 공격에 자체적인 랜섬웨어를 사용하는 것이 아닌, 다른 그룹의 랜섬웨어를 사용한 것이 확인됐다. 그로 인해서 다른 그룹과 동일한 피해자를 다크웹 유출 사이트에 업로드 하는 경우도 발견됐다. 5 월 초부터는 자체 랜섬웨어로 공격하기 시작했으며, 6 월 20 일에 자체적인 RaaS[1] 플랫폼을 출시할 것이라고 예고한 바 있다.

신규 그룹 외에도 리브랜딩을 한 그룹도 확인됐다. Nova 그룹은 25 년 3 월에 RaLord 라는 그룹으로 활동을 시작했으며 4 월에는 Nova 라는 이름으로 리브랜딩했다. 또한 Azzasec 그룹은 작년 6 월에 자체 랜섬웨어 기반의 RaaS 를 공개한적 있는 그룹으로, DoubleFace 로 리브랜딩 후 다시 Azzasec 으로 변경한 뒤 활동을 이어가고 있다.

[1] RaaS (Ransomware-as-a-Service): 랜섬웨어를 서비스 형태로 제공해서 누구나 쉽게 랜섬웨어를 만들고 공격할 수 있도록 하는 비즈니스 모델

Top5 랜섬웨어

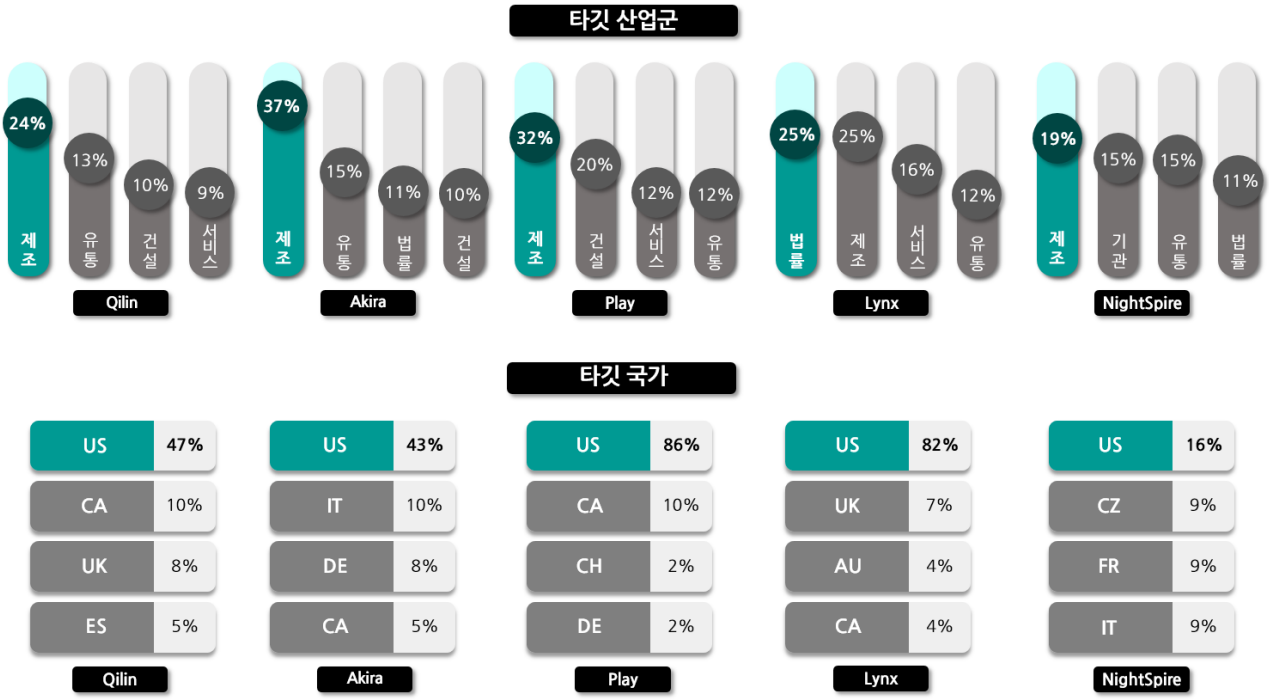


그림 4. 산업/국가별 주요 랜섬웨어 공격 현황

4 월에 미국의 회계 법인 Richmond CPA 를 공격해 약 183GB 분량의 계약서, 세금 계산서, 급여 명세서 등의 내부 자료를 유출한 Qilin 그룹은 4 월에만 총 74 건의 피해자를 게시했다. 4 월 초 RansomHub 서비스가 중단되자 다수의 제휴 공격자들이 Qilin 진영에 합류해 공격이 급증한 것으로 사료된다. 북한 연계 위협 그룹 Moonstone Sleet 와의 연관성도 제기되고 있으며, 특히 Moonstone Sleet 이 과거 사용했던 FakePenny 랜섬웨어와 유사한 배포 방식이 확인되고 있어 주의가 필요하다.

Akira 그룹은 4 월에 미국의 제조 및 조립 서비스 업체 TrussWorks International 을 공격해 직원 및 고객 연락처, 전화번호, 주소와 같은 개인정보는 물론 재무 기록, 비밀 유지 계약 등 내부 문서 13GB 를 유출했다. 또 다른 사례로, 부동산 서비스 업체인 Santa Cruz Properties 를 공격해 재무 문서, 계약서가 포함된 15GB 데이터를 유출한 것으로 알려졌다.

Play 그룹은 Windows CLFS 권한상승 취약점(CVE-2025-29824)을 악용해 침투하려는 시도가 포착되었다. 공용 Cisco ASA[2] 장비 취약점을 공격한 뒤 자체 제작 정보탈취 악성코드 Grixba 를 심어 내부 네트워크 정보를 수집하고 흔적을 삭제했던 시도 정황이 확인됐다. 랜섬웨어를 배포하진 않았지만, 해당 취약점이 패치되기 전에 Play 그룹뿐만 아니라 다른 그룹도 해당 취약점을 악용했을 가능성이 있기 때문에 꾸준히 지켜볼 필요가 있다.

[2] Cisco ASA: Cisco 의 네트워크 보안 장비로, 방화벽, 침입 탐지/방지, VPN 등의 보안 기능을 제공

Lynx 그룹은 4 월에 미국의 농업 컨설팅 기업인 Southern Ag LLC 를 공격해 내부 운영 시스템을 공격해 재무 문서, 고객 데이터, 기밀 문서 등 50GB 의 데이터를 유출했다. 또 다른 피해 사례로는 영국의 법률 서비스 업체 Vicaraga Court Solicitors 로, 이 회사의 메일과 일부 계약서가 다크웹 유출 사이트에 게시됐다. 해당 그룹은 과거 INC 랜섬웨어의 소스코드를 구매해 활용하고 있으며, 최근 공격에서는 Lumma 인포스틸러를 함께 사용하는 등 정보 탈취 도구와 결합된 형태로 진화하고 있다.

NightSpire 는 4 월 일본의 세라믹 제조업체 Nippon Ceramic 을 공격해 45GB 의 기술 설계 문서 및 생산 관련 파일을 탈취했다고 밝혔다. 탈취된 데이터는 다크웹 유출 플랫폼에 공개됐으며, 4 월 말에는 싱가포르의 금융 서비스 기업인 Melco Capital 을 공격해 약 1.8TB 의 재무 정보 및 내부 문서를 유출했다. NightSpire 는 2025 년 3 월부터 활동을 시작한 신규 그룹으로, 최근 몇 주 사이 빠르게 피해 범위를 확장하고 있다.

■ 랜섬웨어 집중 포커스

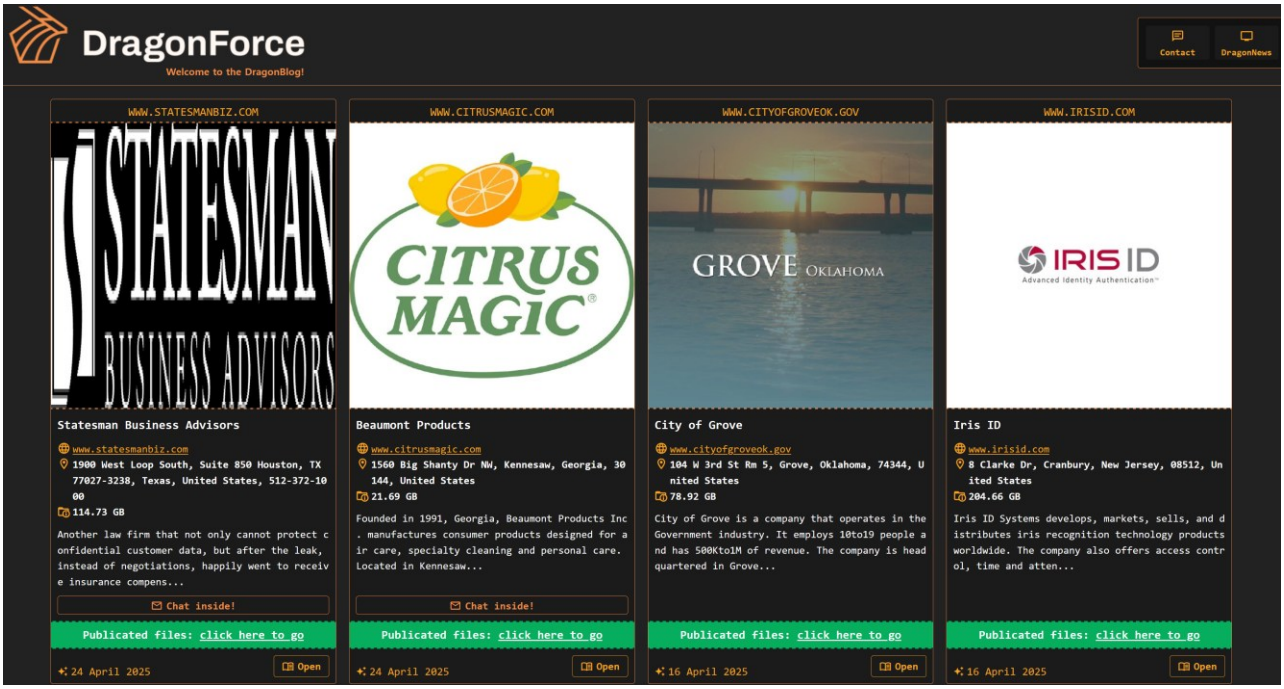


그림 5. DragonForce 다크웹 유출 사이트

DragonForce 그룹은 23 년 12 월부터 활동을 시작해 매월 10 건 이내의 피해자를 꾸준히 게시하는 그룹이다. 24 년 6 월에는 러시아 다크웹 해킹 포럼인 RAMP 포럼에 파트너 모집 글을 업로드했으며, 지금까지도 해당 글을 업데이트하며 랜섬웨어의 버전 업데이트 내용이나 새로운 서비스를 소개하고 있다.

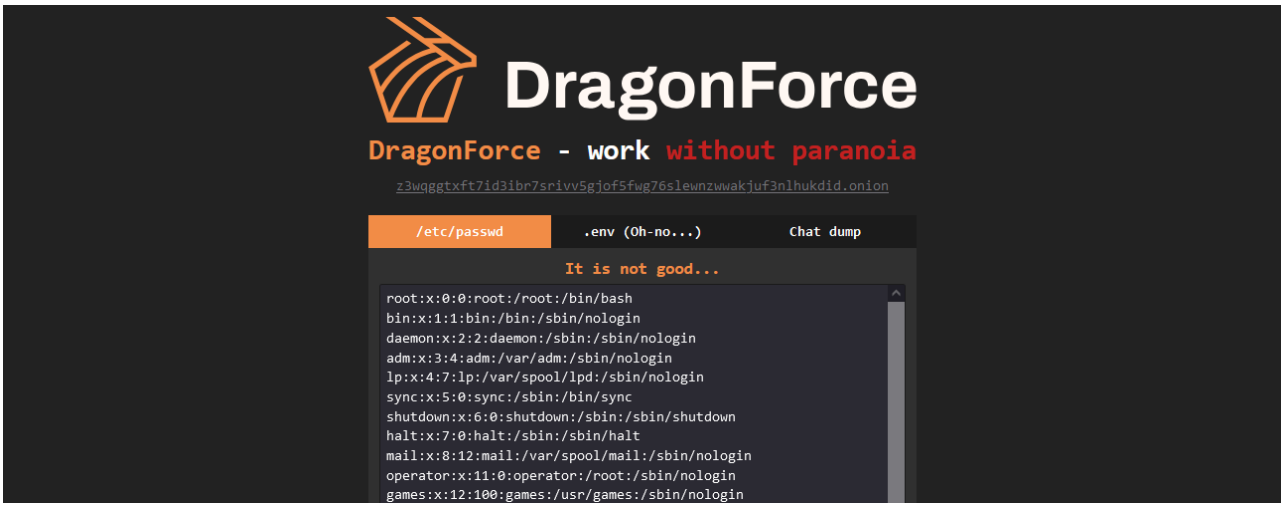


그림 6. 해킹된 BlackLock 유출 사이트

2025 년 3 월, DragonForce 는 경쟁 그룹의 인프라 보안 취약점을 활용해 BlackLock 과 Mamona R.I.P 의 다크웹 유출 사이트를 해킹했다. 당시 BlackLock 의 운영 환경은 보안 구성이 허술한 것으로 알려져 있었으며, 여러 포럼 유저는 물론 DragonForce 가 이를 노려 해킹을 시도했다고 보고 있다. 해킹 이후 Mamona 의 유출 사이트는 완전히 비활성화되었고, BlackLock 의 사이트는 변조되어 DragonForce 를 홍보하는 메시지와 로고가 게시되었다.

그림 7. RansomHub DLS 호스팅 설정

4 월에도 DragonForce 는 타 랜섬웨어 그룹을 통해 자신들을 홍보하려는 정황이 포착됐다. 당시 RansomHub 가 DragonForce 측에 인프라 운영을 위임하기로 결정했다며 관련 설정 페이지가 공개했으며, 이는 양측이 실제 협력 관계를 맺고 인프라를 재정비하고 있는 것으로 해석되었다. 이러한 해석에는 같은 시기 RansomHub 의 다크웹 유출 사이트가 비활성화된 사실이 영향을 미쳤다. 그러나 이후 복구된 RansomHub 유출 페이지에는 "RansomHub R.I.P. (03.03.2025)"라는 문구만 남겨졌고, 'hexcat'이라는 유저가 "RansomHub 는 DragonForce 에 합병됐다"고 주장하면서, 단순한 협력이 아닌 DragonForce 의 인수였다는 가능성도 제기됐다.

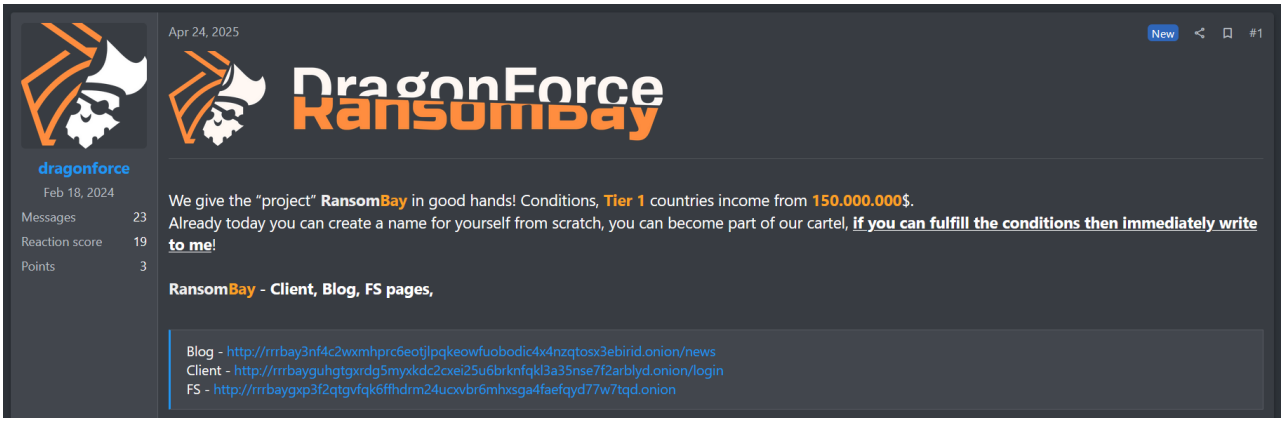
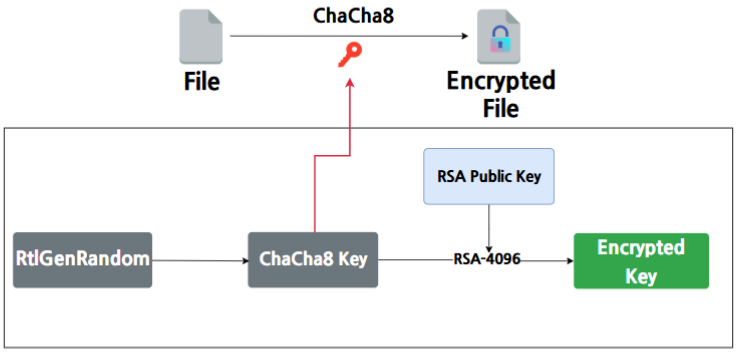


그림 8. RansomBay 홍보글

DragonForce 랜섬웨어 그룹은 활동 영역을 넓히기 위해 자신을 “카르텔”이라고 지칭하기 시작했다. 자신의 계열사는 동일한 인프라를 사용하지만 브랜드로 활동할 수 있다고 밝혔으며 새로운 RansomBay 라는 브랜드가 4 월부터 활동하기 시작했다. 최근 경쟁 그룹의 인프라를 해킹해 자사 홍보 수단으로 악용하거나 새로운 사업 구조를 공개하는 등, 단순 금전 갈취를 넘는 전략적 활동을 보이며 사이버 위협 생태계 내에서 빠르게 입지를 넓히고 있다. 본 보고서는 이러한 배경을 토대로 다가오는 위협에 대비하기 위한 DragonForce 랜섬웨어의 분석 내용을 공유하고자 한다.

암호화 키

ChaCha8 알고리즘으로 암호화를 하고, 해당 키를 RSA-4096으로 보호

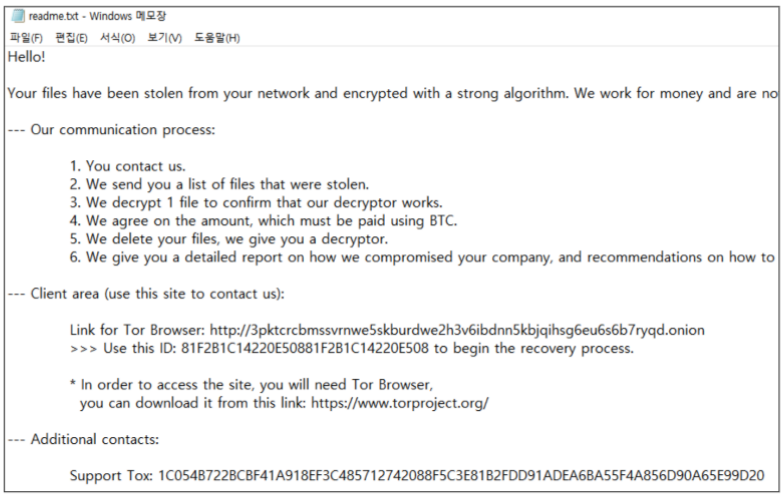


암호화 방식

2MB 이하: 전체 암호화
2MB 초과 10MB 이하: 파일의 첫 3MB만 암호화
10MB 초과: 파일의 50%만 암호화

특징

랜섬노트



readme.txt - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

Hello!

Your files have been stolen from your network and encrypted with a strong algorithm. We work for money and are no

--- Our communication process:

1. You contact us.
2. We send you a list of files that were stolen.
3. We decrypt 1 file to confirm that our decryptor works.
4. We agree on the amount, which must be paid using BTC.
5. We delete your files, we give you a decryptor.
6. We give you a detailed report on how we compromised your company, and recommendations on how to

--- Client area (use this site to contact us):

Link for Tor Browser: http://3pktcrcbmssvrnwe5skburdwe2h3v6ibdnn5kbjqihsg6eu6s6b7ryqd.onion
>>> Use this ID: 81F2B1C14220E50881F2B1C14220E508 to begin the recovery process.

* In order to access the site, you will need Tor Browser,
you can download it from this link: https://www.torproject.org/

--- Additional contacts:

Support Tox: 1C054B722BCBF41A918EF3C485712742088F5C3E81B2FDD91ADEA6BA55F4A856D90A65E99D20

readme.txt

변경 확장자

.dragonforce_encrypted

제작 언어

C/C++

그림 9. DragonForce 랜섬웨어 개요

DragonForce 랜섬웨어 전략

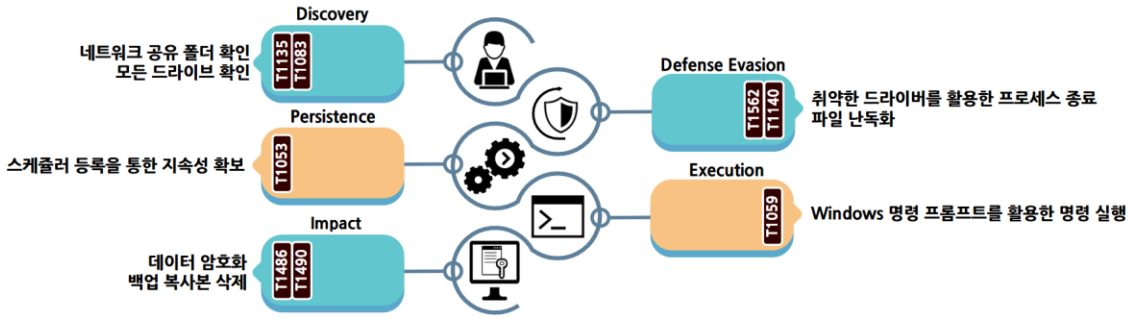


그림 10. DragonForce 랜섬웨어 공격 전략

DragonForce 랜섬웨어는 로그에 사용하는 문자열이나 백업 복사본에 사용하는 명령어 등 각종 문자열을 인코딩해 저장하며, 필요할 때마다 디코딩해 활용하는 방식을 사용한다. 뿐만 아니라 바탕화면, 아이콘 등 실행에 필요한 각종 데이터와 설정 값을 암호화해서 저장해두며, 랜섬웨어 실행 시 이를 복호화하여 사용한다. 랜섬웨어의 기능은 복호화된 설정값과 랜섬웨어 실행 시 입력한 실행 인자를 기반으로 정해진다.

DragonForce 랜섬웨어는 다양한 실행 인자를 사용해 암호화 대상이나 방식을 설정할 수 있으며, 로그 파일 생성이나 중복 실행을 허용할 수 있다. 다만, 랜섬웨어 내부에 암호화되어 있는 기본 설정값에 따라 일부 인자는 확인만 하고 사용하지 않는 경우가 있다. 실제 확인하는 인자와 기능은 아래 표와 같다.

인자	설명
-p <path>	특정 경로만 암호화
-m [all/local/nt/backups]	암호화 모드 설정
-log <path>	특정 경로에 로그 파일 생성
-size <percent>	부분 암호화 비율 설정
-nomutex	중복 실행 허용

표 1. DragonForce 랜섬웨어 실행 인자

실행 인자 중 일부 적용되지 않는 경우는 대부분 랜섬웨어 내부에 저장된 설정값 때문이다. 랜섬웨어는 ChaCha8 알고리즘으로 암호화된 설정값을 가지고 있으며, 이를 복호화해 랜섬웨어의 실행 옵션을 정한다. 이렇게 저장되는 설정값을 활용해 파일 암호화나 프로세스 종료 등에 활용한다. 또한 로그 파일의 맨 처음에 해당 랜섬웨어의 설정값을 우선적으로 저장하며, 저장된 로그 파일에 따른 설정 값은 아래 표와 같다.

구분	설명
build_key	로그 파일 암호화 키
custom_icon	암호화 파일 아이콘 변경 여부
custom_wallpaper	바탕 화면 변경 여부
custom_extension	암호화 확장자
time_sync	시스템 시간 동기화 여부
encrypt_mode	기본 암호화 모드(all, local, nt, backups)
full_encrypt_threshold	전체 암호화 파일 기준
header_encrypt_threshold	파일 헤더 암호화 기준
header_encrypt_size	파일 헤더 암호화 크기
other_encrypt_chunk_percent	부분 암호화 비율
encrypt_file_names	원본 파일명 Base32 인코딩 여부
schedule_job	작업 스케줄러 등록 여부
job_executable	작업 스케줄러 실행 파일 경로
job_title	스케줄러 작업 이름
job_description	스케줄러 작업 설명
job_start	스케줄러 작업 시작 시각
kill	프로세스 종료 여부
use_sys	BYOVD[3] 기법 활용 여부
priority	프로세스 종료 대상
whitelist	암호화 예외 여부
path	암호화 예외 폴더
ext	암호화 예외 확장자
filename	암호화 예외 파일명

표 2. DragonForce 랜섬웨어 설정값

[3] BYOVD: 합법적인 서명이 되어 있지만, 취약점을 가진 드라이버를 악용해 보안 솔루션을 우회해 악성 행위를 하는 기법

원활한 파일 암호화를 위해 설정값에 저장된 프로세스를 우선적으로 종료한다. 분석을 진행한 랜섬웨어에는 아래 표에 해당하는 프로세스 리스트가 확인됐다.

프로세스
MsMpEng.exe, sql.exe, oracle.exe, ocssd.exe, dbsnmp.exe, synctime.exe, agntsvc.exe,isqlplussvc.exe, xfssvccon.exe, mydesktopservice.exe, ocautoupds.exe, encsvc.exe, firefox.exe, tbirdconfig.exe, mydesktopqos.exe, ocomm.exe, dbeng50.exe, sqbcoreservice.exe, excel.exe, infopath.exe, msaccess.exe, mspub.exe, onenote.exe, outlook.exe, powerpnt.exe, steam.exe, thebat.exe, thunderbird.exe, visio.exe, winword.exe, wordpad.exe, notepad.exe, calc.exe, wuauclt.exe, onedrive.exe, SQLAGENT.exe, sqlservr.exe, SQLWriter.exe

표 3. 종료 대상 프로세스

단순히 프로세스 핸들을 가져와 종료하는 방식도 있지만, 설정에 use_sys 옵션이 활성화되어 있다면 취약한 드라이버 truesight.sys 와 rentdrv2.sys 를 악용해 프로세스를 종료한다. 각 드라이버의 임의 프로세스 종료 기능을 통해 보안 솔루션의 탐지를 우회하고 프로세스 종료를 시도한다. truesight.sys 는 Adlice Software 의 멀웨어 제거 도구 RogueKiller Antirootkit 에서 루트킷 탐지 및 제거 기능을 제공하는 드라이버 모듈로, v3.4.0 이하의 버전에서 임의의 프로세스를 종료시킬 수 있는 취약점이 발견됐다. rentdrv2.sys 는 중국의 네트워킹 플랫폼 기업 Hangshou Shunwang Technology 에서 사용하는 드라이버로, truesight.sys 와 동일하게 임의의 프로세스를 종료시킬 수 있는 취약점이 발견됐다. rentdrv2.sys 의 경우 세부 버전이 공개되지 않았으나 24 년 12 월 개발 업체는 취약점 조치가 완료됐다고 주장했으며, 두 취약한 드라이버는 모두 취약 드라이버 차단 정책에 적용됐다.

```
switch ( use_sys_flag )
{
  case 0:
    goto LABEL_26;
  case 1:                                // truesight.sys | terminate process (0x22E044)
    v8 = DeviceIoControl(hDevice: hDevice, dwIoControlCode: 0x22E044u, lpInBuffer: &InBuffera, nInBufferSize: 4u, lpO
    break;
  case 2:                                // rentdrv2.sys | terminate process (0x22E010)
    lpInBuffer[1] = InBuffera;
    lpInBuffer[0] = 1;
    v8 = DeviceIoControl(hDevice: hDevice, dwIoControlCode: 0x22E010u, lpInBuffer: lpInBuffer, nInBufferSize: 0x808u,
    break;
  default:
    goto LABEL_26;
```

그림 11. BYOVD 를 활용한 프로세스 종료

또한 암호화된 파일을 사용자가 임의로 복구하지 못하도록 백업 복사본을 삭제한다. 백업 복사본을 삭제하기 위해 사용하는 명령어는 아래와 같다.

```
cmd.exe /c C:\\Windows\\System32\\wbem\\WMIC.exe shadowcopy where "ID='%s'" delete
```

표 4. 백업 복사본 삭제 명령어

백업 복사본 삭제 이후에는 -m 실행 인자로 설정한 암호화 모드에 따라 암호화 대상을 설정한다. 모드에는 연결된 드라이브를 암호화하는 local, 네트워크 공유 자원 중 “ADMIN$” 폴더를 암호화하는 nt, 그리고 드라이브와 네트워크 공유 자원을 모두 암호화하는 all 모드로 구분된다. 이 외에도 backups 라는 모드도 존재하지만, 해당 옵션을 사용하면 어떤 파일도 암호화하지 않고 종료된다. -p 실행 인자를 사용하면 특정 폴더만 암호화할 수 있으며, -m 혹은 -p 인자를 사용하지 않으면 설정 값에 기본으로 지정된 방식을 사용한다.

암호화 대상을 설정했으면, 각 디렉터리를 순회해 예외 항목에 해당하는지 확인한다. 예외 항목은 설정값에 저장되어 있으며, 이를 기준으로 대상 디렉터리가 예외 항목인지 확인하고 디렉터리 확인이 끝났다면 각 디렉터리에 존재하는 파일이 예외 항목인지 확인한다. 확인하는 암호화 예외 대상은 아래 표와 같다.

폴더명	확장자 및 파일명
tmp, winnt, temp, thumb, $Recycle.Bin, $RECYCLE.BIN, System Volume Information, Boot, Windows, perflogs, Public	.exe, .dll, .lnk, .sys, .msi, .bat, .dragonforce_encrypted, readme.txt

표 5. 암호화 예외 대상

파일 암호화 방식은 파일의 확장자와 크기에 따라 결정된다. 데이터베이스와 관련된 파일은 크기와 상관없이 전체 암호화를 진행하고, 가상 머신과 관련된 파일은 파일의 크기와 상관없이 처음 20%만 암호화한다. 각각 해당하는 파일 확장자는 아래 표와 같다.

확장자
.dadigrams, .sqlite, .db, .sas7bdat, .daschema, .sqlite3, .abcddb, .sqlite, .nrmlib, .db-wal, .db-shm, .dacpac, .accdw, .xmlff, .kexis, .kexic, .fmp, .sl, .accft, .accdt, .accdr, .accde, .accdc, .accdb, .fmp12, .temx, .rodx, .rctd, .nwd, .kexi, .itd, .grd, .epim, .dtsx, .dlis, .wmd, .mdn, .maw, .lut, .kdb, .icr, .icg, .hjt, .fm5, .db2, .adn, .abx, .abs, .xld, .xdb, .wrk, .wdb, .vvv, .vpd, .vis, .v12, .usr, .udl, .udb, .trm, .trc, .tps, .tmd, .sql, .spq, .sis, .sdf, .sdb, .scx, .sbf, .rsd, .rpd, .rod, .rbf, .qvd, .qry, .pnz, .pdm, .pdb, .pan, .p97w, .p96, .owc, .orx, .oqy, .odb, .wyn, .yf, .wnv2, .nsf, .ns4, .ns3, .ns2, .nnt, .ndf, .myd, .mwb, .mud, .mrg, .mpd, .mdf, .mdb, .mav, .mas, .mar, .maq, .maf, .lwx, .lgc, .kdb, .jtx, .jet, .itw, .ihx, .idb, .his, .hdb, .gwi, .gdb, .frm, .fpt, .fp7, .fp5, .fp4, .fp3, .fol, .fmp, .fic, .fdb, .fcd, .exb, .ecx, .eco, .dxl, .dsk, .dqy, .dp1, .ddl, .dcx, .dct, .dcb, .dbx, .dbv, .dbt, .dbs, .dbc, .db3, .dad, .cpd, .cma, .ckp, .cdb, .cat, .bdf, .btr, .ask, .alf, .ora, .arc, .adp, .adf, .ade, .adb, .4dl, .4dd, .mdt, .nv, .ib, .db, .te

표 6. 데이터베이스 관련 확장자

확장자
.vdi, .vhd, .vmdk, .pvm, .vmsn, .vmsd, .nvram, .vmx, .raw, .qcow2, .subvol, .bin, .vsv, .avhd, .vmrs, .vhdx, .avdx, .vmcx, .iso

표 7. 가상 머신 관련 확장자

그 외의 파일은 설정값의 크기 기준 full_encrypt_threshold, header_encrypt_threshold 값에 따라서 전체 암호화와 부분 암호화를 결정한다. 각각 2MB 와 10MB 로 설정되어 있어, 2MB 이하의 파일은 전체 암호화를 하며, 2MB 초과 10MB 이하의 파일은 처음 3MB 만 암호화한다. 또한 10MB 보다 큰 파일은 전체의 50%만 암호화한다.

그림 12. 크기 별 파일 암호화 방식

암호화 알고리즘으로 ChaCha8 을 사용하며, 사용한 키와 IV 는 RSA-4096 공개키로 보호한 다음 암호화한 파일의 맨 뒤에 추가한다. 파일 암호화 이후에는 암호화 확장자를 추가하는데, encrypt_filenames 옵션이 활성화되어 있는 경우 암호화 확장자 추가뿐만 아니라 파일명을 인코딩한다. 인코딩 방식으로 Base32 를 사용하지만 기본 문자 집합이 아닌 “gwfn6l3bk45o2zecvi7xtyqrpsudmahj” 문자열 집합을 기준으로 원본 파일명을 인코딩 한 뒤 암호화 확장자를 추가한다.

그림 13. 변경된 바탕화면

파일 암호화 이후에는 랜섬웨어에 저장된 이미지와 아이콘 파일로 바탕화면과 암호화된 파일의 아이콘을 변경한다. 배경화면은 “C:\Users\Public\wallpaper_white.png” 경로에 저장하며, 아이콘 이미지는 “C:\Users\Public\icon.ico” 경로에 저장한다.

뿐만 아니라 랜섬웨어를 작업 스케쥴러에 등록해 실행하는 기능도 확인됐다. 해당 설정이 존재한다면, 현재 랜섬웨어를 job_executable 설정에 저장된 경로에 복사한다. 그 이후 job_title 에 저장된 값을 작업명으로, job_description 을 작업 설명으로 생성하며, job_start 에 저장된 시각을 기준으로 실행되도록 작업을 생성한다.

DragonForce 랜섬웨어 대응방안

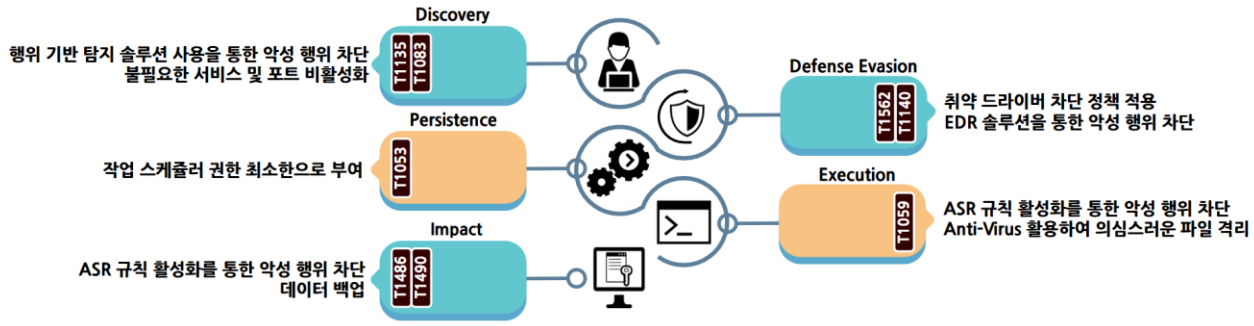


그림 14. DragonForce 랜섬웨어 대응방안

DragonForce 랜섬웨어는 Windows 명령 프롬프트를 활용해 백업 복사본 삭제를 진행한다. 따라서 ASR[4] 규칙 활성화를 통해서 비정상적인 프로세스를 차단해 악성 행위를 막을 수 있다. 또한 랜섬웨어에 저장된 프로그램을 임시 폴더에 저장하거나 작업 등록을 위해 랜섬웨어를 특정 위치에 복제하기 때문에 Anti-Virus 를 활용하여 의심스러운 파일을 격리할 수 있다.

네트워크 공유 폴더 암호화를 위해서 현재 시스템의 내부 네트워크 대역을 탐색하고, 연결이 가능한 공유 폴더에 접근을 시도한다. 또한, 파일 암호화의 경우 모든 드라이브를 탐색한 뒤 실행 인자에 따라서 암호화할 드라이브를 구분하기 때문에 행위 기반 탐지 솔루션을 통해 공격자의 악성 행위를 막을 수 있다.

합법적인 서명이 되어있지만, 취약한 버전의 드라이버 truesight.sys 와 rentdrv2.sys 를 악용해서 보안 장비를 우회하여 프로세스 종료를 시도하기 때문에 취약한 드라이버가 실행되지 않도록 차단해야 한다. 이는 취약 드라이버 차단 정책을 통해 해결할 수 있으며, Microsoft 에서 제공하는 취약한 드라이버 차단 목록에 이미 취약한 두 드라이버가 추가되어 있어 가이드라인에 따라 이를 시스템에 적용하여 취약한 드라이버가 악용되는 것을 방지할 수 있다. 뿐만 아니라 악성 행위에 필요한 파일과 명령어들이 암호화되거나 인코딩 된 상태로 존재하며, 사용 직전에 복호화 및 디코딩을 진행해 사용하기 때문에, EDR[5] 솔루션을 통해 악성 행위를 차단해야 한다.

암호화된 파일을 사용자가 임의로 복구하는 것을 방지하기 위해 시스템에 존재하는 모든 백업 복사본을 삭제한 뒤 파일을 암호화한다. ASR 규칙 활성화를 통해서 백업 복사본을 삭제하는 프로세스와 파일을 암호화는 것을 차단할 수 있다. 뿐만 아니라 백업 복사본을 별도의 네트워크나 저장소에 소산 백업하여, 시스템이 암호화되더라도 복구할 수 있도록 조치해야 한다.

[4] ASR (Attack Surface Reduction): 공격자가 사용하는 특정 프로세스와 실행 가능한 프로세스를 차단하는 보호 기능

[5] EDR (Endpoint Detection and Response): 컴퓨터와 모바일, 서버 등 단말기에서 발생하는 악성 행위를 실시간으로 감지하고 분석 및 대응하여 피해 확산을 막는 솔루션

IoCs

Hash(SHA-256)
d06b5a200292fedcfb4d4aecac32387a2e5b5bb09aaab5199c56bab3031257d6
70afd8efb34382badead93ae104d958256de6be8054227ccc85fe95d5c5f9db0

■ 참고 사이트

• Guide Point Security (https://www.guidepointsecurity.com/blog/ransomsnub-ransomhubs-affiliate-confusion/)

• The Hacker News (https://thehackernews.com/2025/05/play-ransomware-exploited-windows-cve.html)

• The Hacker News (https://thehackernews.com/2025/05/qilin-leads-april-2025-ransomware-spike.html)

• BleepingComputer (https://www.bleepingcomputer.com/news/security/everest-ransomwares-dark-web-leak-site-defaced-now-offline/)

• Symantec (https://www.security.com/threat-intelligence/play-ransomware-zero-day)

• GitHub (https://github.com/keowu/BadRentdrv2)

• UNIT 42 (https://unit42.paloaltonetworks.com/agonizing-serpens-targets-israeli-tech-higher-ed-sectors/)

• Microsoft (https://learn.microsoft.com/ko-kr/windows/security/application-security/application-control/app-control-for-business/design/microsoft-recommended-driver-block-rules)