Keep up with Ransomware

다가오는 Funksec 의 위협: RaaS 를 넘어 데이터 경매까지

■ 개요

2025 년 1 월 랜섬웨어 피해 사례 수는 지난 12 월(673 건)에 비해 약 8% 증가한 723 건을 기록했다. 지난달에 비해 소폭 증가했으며, 전년 1 월(304 건) 대비 2 배를 넘는 높은 수치로 랜섬웨어 위협이 증가한 모습을 보이고 있다. 1 월에도 높은 수치를 보이는 이유는 Dragon, Akira 그룹의 활동 증가와 신규 그룹인 Babuk2(Babuk-Bjorka) 그룹이 66 건에 달하는 많은 피해자를 게시했기 때문이다.

1 월에 새로 등장한 신규 그룹 Babuk2 는 Bjorka 라는 해커가 운영하고 있기 때문에 Babuk-Bjorka 라고 불리기도 한다. 이들이 공개한 66 건의 피해자는 대부분 다른 그룹에서 과거에 공격한 이력이 있는 것으로 확인됐다. 주로 Funksec, RansomHub, LockBit 그룹과 피해자가 겹치며, 일부 게시글은 내용 자체도 동일한 것으로 확인됐다. 해당 다크웹 유출 사이트는 1 월 26 일에 공개됐지만 1 월 29 일부터 접속이 불가능한 상태이며, 자신이 Babuk 이라고 주장하는 것 외에는 아직 연관성이 확인되지 않았다.

새로 등장한 그룹뿐만 아니라 기존에 활동하던 랜섬웨어 그룹의 대규모 공격은 지속적으로 확인되고 있다. Cleo 의 파일 전송 솔루션 취약점으로 대규모 공격을 수행한 Clop 그룹이 피해자 명단과 탈취 데이터를 공개했다. Clop 그룹은 12 월에 Cleo 의 MFT 솔루션 3 개의 원격 코드 실행 취약점을 악용해 총 66 개의 기업을 공격했으며, 그 중 협상에 응하지 55 개 기업의 데이터를 다크웹에 공개했다. Clop 그룹은 여기서 그치지 않고 1 월 말에 49 개의 피해 기업 명단을 추가로 공개했다.

랜섬웨어 그룹들이 해킹 포럼에서 활동하는 모습이 지속적으로 확인되고 있다. BlackLock 그룹은 러시아 포럼에 자신들의 랜섬웨어 기능을 소개하고 RaaS[1]파트너를 모집하는 글을 업로드했다. BlackLock 그룹은 Windows 는 물론 Linux, ESXi, NAS, FreeBSD 와 같이 다양한 운영체제를 타깃으로 하며, 부분 암호화와 자가 삭제 등 다양한 기능을 포함하고 있다. 또한 CIS[2]와 BRICS[3] 국가를 제외한 모든 국가를 공격 대상으로 지정할 수 있으며, 피해자는 온전히 각 계열사가 관리해 거래로 얻은 몸값의 20%만을 수수료로 지불하면 된다. BlackLock 그룹은 소수의 인원만 추가로 모집하고 있으며, 장기적인 협력 관계를 유지하기 위해서 일련의 테스트 과정을 거친 뒤 파트너를 모집하고 있다.

해킹 포럼에서의 위협이 지속되고 있는 가운데 해킹 포럼에서 1 건의 국내 사고 사례가 확인됐다. 해킹 포럼 BreachForums 에서 활동하는 IntelBroker 는 25 년 1 월 1 일에 환경부의 소스코드를 탈취해 판매하고 있다. 탈취한 소스코드는 24 년 1 월에 유출된 코드라고 밝혔으며, 유출된 소스코드는 환경부 국가미세먼지정보센터의 소스코드로 추정된다. 또한, IntelBroker 와 EnergyWeaponUser 는 환경부의 X(트위터) 계정 또한 탈취해 게시물을 2 건 게시했다가 12 월 30 일 삭제했다.

윈도우 및 리눅스뿐만 아니라 클라우드를 위협하는 랜섬웨어 공격이 확인되어 주의가 필요하다. Amazon 에서 제공하는 클라우드 스토리지 Amazon S3 환경을 노리는 Codefinger 랜섬웨어는 서버에 저장된 데이터를 보호하기 위한 기능을 악용해 파일을 암호화한다. 고객 제공 키(SSE-C)를 이용해서 서버 측 암호화를 사용해 데이터를 암호화하고, 데이터를 복호화하기 위한 대가로 금전을 요구한다. 또한 객체 수명 주기 관리 API 를 이용해 7 일 뒤 암호화된 데이터가 자동으로 삭제되도록 해 피해자를 협박한다. 이러한 작업은 IAM 정책에서 SSE-C 가 S3 버킷에 적용되지 않도록 설정해 악용을 방지할 수 있다. 또한 결정적으로 AWS 자격 증명이 있어야만 SSE-C 를 악용해 파일 암호화가 가능하므로, GitHub 와 같은 온라인 프로젝트 공유 플랫폼에 노출되지 않도록 주의하며, AWS 자격 증명을 주기적으로 관리하고 최소한의 권한만을 부여해 피해를 최소화해야 한다.

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

[2] CIS (Commonwealth of Independent States): 구 소련 공화국들의 연합체로 결성된 국가 연합으로, 러시아, 벨라루스, 아르메니아 등 11개국이 포함되어 있다

[3] BRICS: 브라질, 러시아, 인도, 중국을 일컫는 약칭

마지막으로 Funksec 그룹은 12 월 89 건에 이어 1 월에는 39 건의 피해자를 게시하며 위협적인 모습을 보여주고 있다. 1 월 초에는 Funksec 그룹이 사용하는 랜섬웨어인 FunkLocker 를 1.2, 1.5 버전으로 업데이트 하고, RaaS 파트너 또한 모집하기 시작했다. 관리자 패널을 준비하고 있으며, 서비스로 제공될 랜섬웨어는 다음 버전 Funksec 2.0 을 사용할 것이라고 밝혔다. 활동 초기에 무료 DDoS 공격 도구 등 다양한 서비스를 부가적으로 제공했으며, 1 월에도 새로운 서비스를 추가로 공개했다. Funksec 운영자의 공지사항이나 전달 사항을 전달하고 일반 사용자도 활동이 가능한 자체 다크웹 포럼 Funkforum 을 공개하고, 그 외에도 탈취한 데이터를 경매 형태로 판매하는 FunkBID 를 공개했다. 또한 국내 제조업체를 공격해 다크웹 사이트에 탈취한 데이터를 공개했기 때문에 Funksec 랜섬웨어에 대해 자세히 살펴보고 전략과 대응방안을 통해 위협에 대비할 필요가 있다.

■ 랜섬웨어 뉴스

Clop 그룹, Cleo 취약점 악용한 대규모 공격 피해자 명단 및 데이터 공개

- Cleo의 파일 전송 솔루션 Cleo Harmony, VLTrader, LexiCom의 취약점(CVE-2024-50623, CVE-2024-55956) 악용
- 최초 공개한 66개의 기업 중, 55개의 기업명 공개 및 데이터 전체 공개
- 아직 협상에 응하지 않은 49개의 기업 명단을 추가로 공개

Funksec 그룹, 자체 다크웹 포럼 Funkforum 공개

- 기존 DLS에 업로드하던 공지사항 및 전달사항을 주로 업로드
- 그 외에도 운영진의 잡담 또한 업로드되고 있으며, 일반 사용자도 가입해 게시글 업로드가 가능

IntelBroker, 환경부의 소스코드 판매

- 다크웹 포럼 BreachForums에 판매글을 업로드
- 판매하는 소스코드는 24년 1월 유출된 소스코드라고 주장
- 24년 12월에는 트위터(X) 계정을 탈취해 2건의 게시글을 업로드 후 삭제

Funksec 그룹, 탈취 데이터 경매 사이트 공개

- 기존에는 다크웹 유출 사이트에서 지정된 가격에 데이터를 판매하거나 공개
- 탈취한 데이터를 경매 형태로 판매하는 사이트 FunkBID 개설
- FunkBID 개설 이후 업로드된 탈취 데이터는 모두 경매 진행 예정

BlackLock 그룹, RaaS 파트너 모집

- 러시아 해킹 포럼 Ramp 포럼에서 RaaS 파트너를 모집하는 글 게시
- 소수의 파트너만 모집하며, 모집이 완료되면 해당 게시글은 삭제 예정
- Windows, Linux, ESXi, FreeBSD는 물론 NAS 환경도 공격 가능한 랜섬웨어 제공
- 랜섬웨어 피해자는 각 계열사가 관리하며, 20%의 수수료만 지불하면 됨

Funksec 그룹, 국내 제조 업체 탈취 데이터 공개

- 국내 네트워크 장비 제조 업체로 피해자를 게시
- 공개된 데이터 확인 결과, 해당 네트워크 장비를 사용하는 국내 제조 업체의 내부 데이터로 추정


Amazon S3 버킷을 노리는 Codefinger 랜섬웨어
서버에 저장된 데이터를 보호하기 위한 기능을 악용해 파일을 암호화하고 몸값을 요구
공격에는 AWS 자격 증명이 필요하기 때문에, 자격 증명이 노출된 환경을 주 타겟으로 함
고객 제공 키(SSE-C)를 이용해서 서버측 암호화를 사용해 데이터를 암호화하고
객체 수명 주기 관리 API를 이용해 7일 뒤 자동으로 암호화된 데이터가 삭제되도록 해 협박
신규 Morpheus 그룹, 피해자 3건 게시
1월 7일 다크웹 유출 사이트가 발견됐으나, 2건의 피해자는 12월에 업로드 된 상태
또한 12월에 업로드 된 피해자 중 1건은 8월에 공격 받은 것으로 확인
신규 Babuk2 그룹, 피해자 66건 게시
자신이 Babuk이라고 주장하는 신규 그룹 발견
업로드한 피해자 66건 대부분은 FunkSec, RansomHub, LockBit 그룹의 피해자와 중복
A1project 랜섬웨어, 신규 파트너 모집
러시아 해킹 포럼에서 RaaS를 이용할 파트너를 모집
Windows, Linux, ESXi 환경을 암호화할 수 있는 랜섬웨어와, 관리 패널, 채팅 기능 제공
피해자로부터 탈취한 몸값은 직접 수령하고, 20%의 수수료를 지불하는 형태

그림 1. 랜섬웨어 동향

■ 랜섬웨어 위협

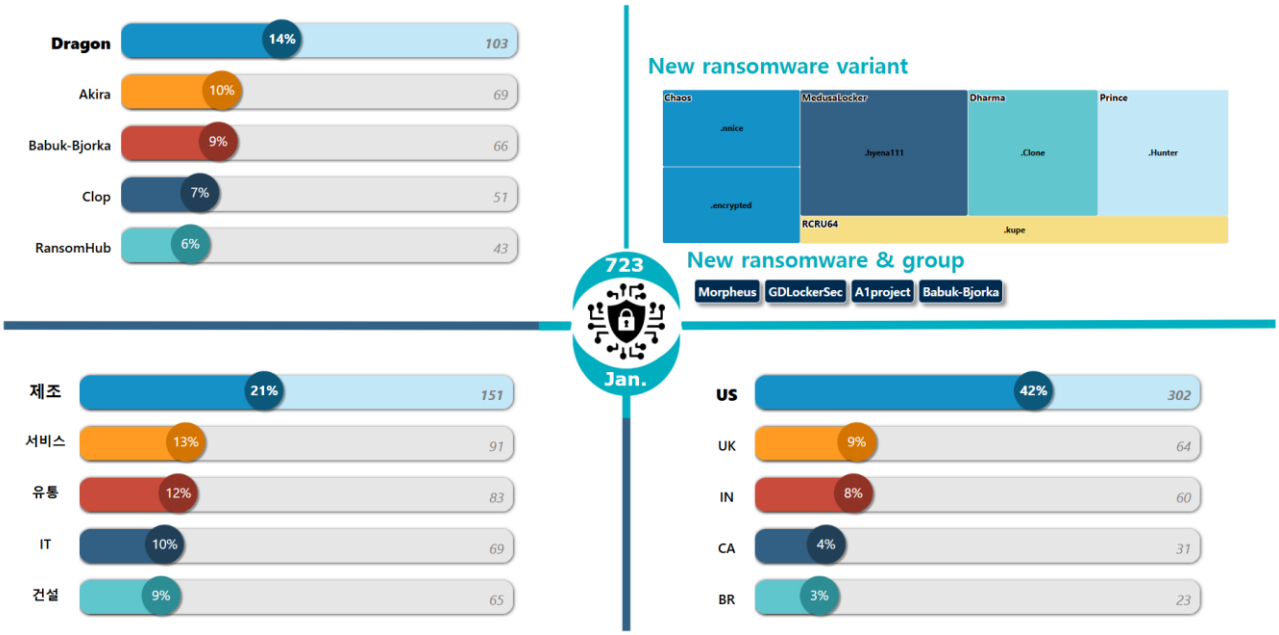

그림 2. 2025 년 1 월 랜섬웨어 위협 현황

새로운 위협

1 월에는 4 개의 신규 랜섬웨어 그룹이 발견됐다. Morpheus 그룹은 1 월에 다크웹 유출 사이트가 발견된 그룹이지만, 공격 활동은 더 이전에 수행한 것으로 확인됐다. 게시한 3 건의 피해자 중 2 건은 12 월에 게시됐으며, 그 중 한 건은 8 월에 공격당한 사실이 밝혀졌다.

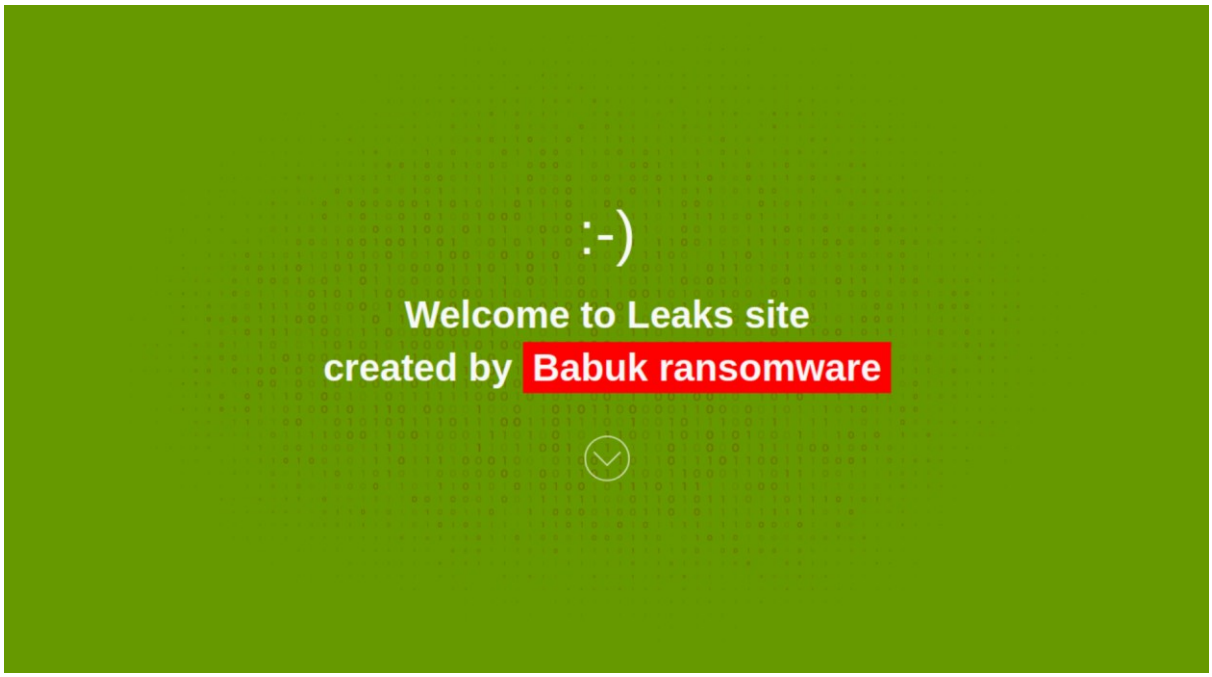

그림 3. Babuk2(Babuk-Bjorka) 다크웹 사이트

1 월 말에는 자신을 Babuk2 라고 칭하는 신규 그룹이 발견됐다. 기존에 알려진 Babuk 그룹은 21 년 초부터 활동을 시작해 RaaS 를 제공하고 이중 협박을 통해서 금전을 요구한 그룹이다. Babuk 그룹은 21 년 4 월 미국 워싱턴 경찰청을 공격한 후 법 집행 기관의 압박을 느껴 랜섬웨어 활동을 중단했으며, 관계자로 추정되는 사람이 21 년 6 월 다크웹 해킹 포럼에 전체 소스코드를 공개하며 Babuk 랜섬웨어는 추후 여러 랜섬웨어 공격에 악용됐다. 새로 발견된 Babuk2 그룹은 기존 Babuk 그룹과의 연관성이 아직은 발견되지 않았으며, 공개한 피해자들의 대부분은 Funksec, RansomHub, LockBit 그룹이 이미 업로드한 피해자로 확인됐다. Babuk2 그룹이 단순 이름만 가져온 그룹인지, 아니면 다른 랜섬웨어 그룹과의 연관이 있는지는 더 지켜봐야할 것으로 보인다.

GDLockerSec 그룹은 1 월에 총 5 건의 피해자를 게시한 신규 그룹으로, 그 중에는 Amazon 의 클라우드 컴퓨팅 서비스인 AWS 가 포함되어 있다. 이들은 AWS 로부터 9GB 의 데이터를 탈취했다고 주장했지만, 제공된 CSV 파일을 확인한 결과 데이터 분석 플랫폼 Kaggle 에서 공유되는 데이터와 일치하는 것이 확인됐다.

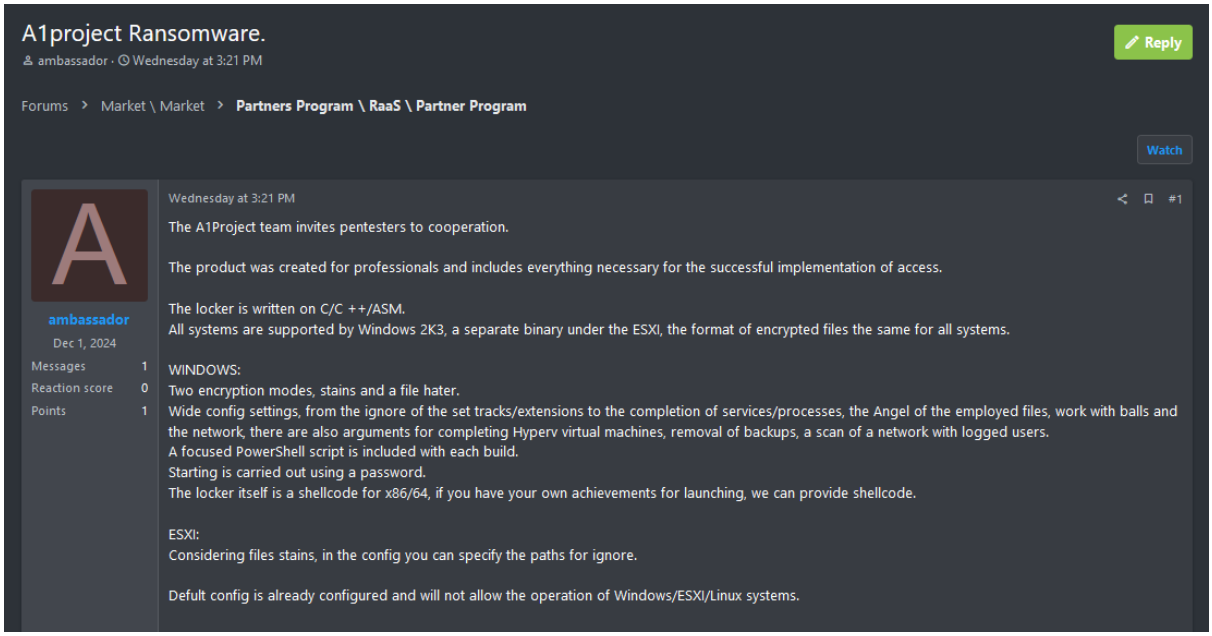

그림 4. A1project 랜섬웨어 파트너 모집 글

파트너를 모집하며 본격적인 활동을 준비하는 신규 랜섬웨어 또한 확인됐다. A1project 랜섬웨어는 Windows 와 Linux 환경은 물론 ESXi 환경도 암호화가 가능하다. A1project 그룹은 관리 패널은 물론, 탈취 데이터를 공개할 데이터 유출 사이트와 비밀 협상 채팅 기능도 제공하며, 20%의 수수료만 지불하면 된다고 홍보하고 있다.

Top5 랜섬웨어

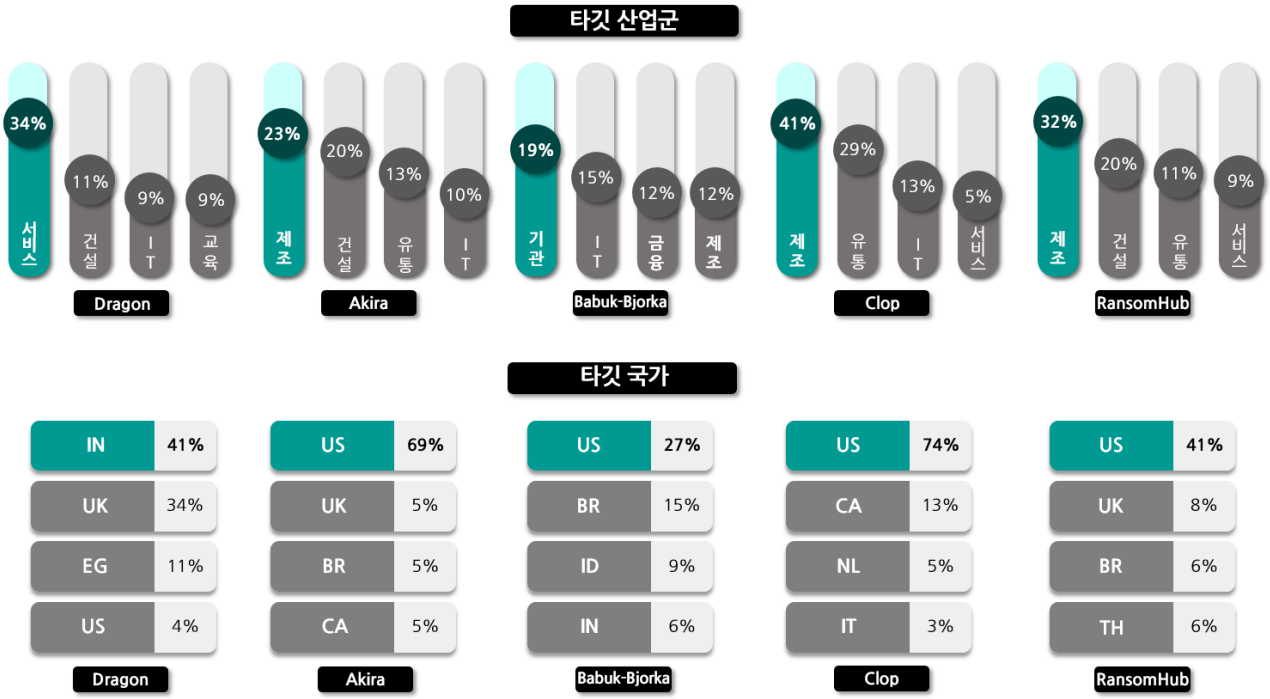

그림 5. 산업/국가별 주요 랜섬웨어 공격 현황

Dragon 그룹은 지난 10 월부터 텔레그램 채널을 통해 활동하기 시작한 랜섬웨어 그룹으로, 작년에는 매달 평균 10 건에 달하는 피해자를 게시했지만 1 월에는 100 건이 넘는 피해자를 게시하며 활동량이 급증한 모습을 보여줬다. 이들은 자체 랜섬웨어인 Dragon 랜섬웨어를 사용하며, 사용자가 설정값을 변경해 쉽게 랜섬웨어를 만들 수 있는 빌더 도구를 제공하는 RaaS 또한 제공하고 있다. 랜섬웨어 공격 외에도 DDoS 공격과 웹사이트 변조 공격 또한 수행하며 다양한 위협 활동을 하고 있다.

Akira 그룹도 지난 11 월부터 활동량이 증가했으며, 1 월에도 69 건의 피해자를 게시하며 활발히 활동하고 있다. 1 월에는 미국의 환경 컨설팅 및 교육 기업 AAA Environmental 을 공격해 기업의 재무 제표, 직원 의료 정보, 고객의 개인 정보 등의 정보를 탈취했다. 또한 아르헨티나의 미디어 업체 Diario Los Andes 를 공격해 직원의 개인 정보와 계산서 등을 포함한 내무 문서를 탈취했다.

Bjorka 라는 해커가 운영하며, Babuk 이라고 주장하는 Babuk2(Babuk-Bjorka) 그룹은 등장과 함께 66 건의 피해자를 일괄적으로 게시했다. 하지만 대부분의 피해자는 Funksec, RansomHub, LockBit 등의 그룹이 이미 공개한 이력이 있으며, 피해 기업을 소개하는 문구 또한 다른 그룹의 데이터 공개 글의 내용을 그대로 가져다 사용한 것이 확인됐다. 아직 두 그룹간에 연관성이 확인되지 않았기 때문에, Babuk2 그룹이 단순히 홍보성 목적으로 데이터를 게시한 것인지 아니면 Funksec, RansomHub, LockBit 그룹 등과의 협력 관계에 있는 것인지 지켜볼 필요가 있다.

지난 12 월 Cleo 의 파일 전송 솔루션의 취약점을 악용해 대규모 공격을 한 Clop 그룹이 추가 피해자를 공개했다. 이들은 12 월에 공개한 66 개의 피해 기업 중 총 55 개 기업의 데이터를 다크웹 유출 사이트에 공개했으며, 1 월 말에는 49 개의 피해 기업명을 추가로 공개했다. 추가 명단의 유출 데이터는 아직 공개되지 않았으며, 알파벳 순으로 A-C 에 해당하는 기업만 공개됐기 때문에, 더 많은 피해자 명단이 공개될 가능성이 높아 보인다.

■ 랜섬웨어 집중 포커스

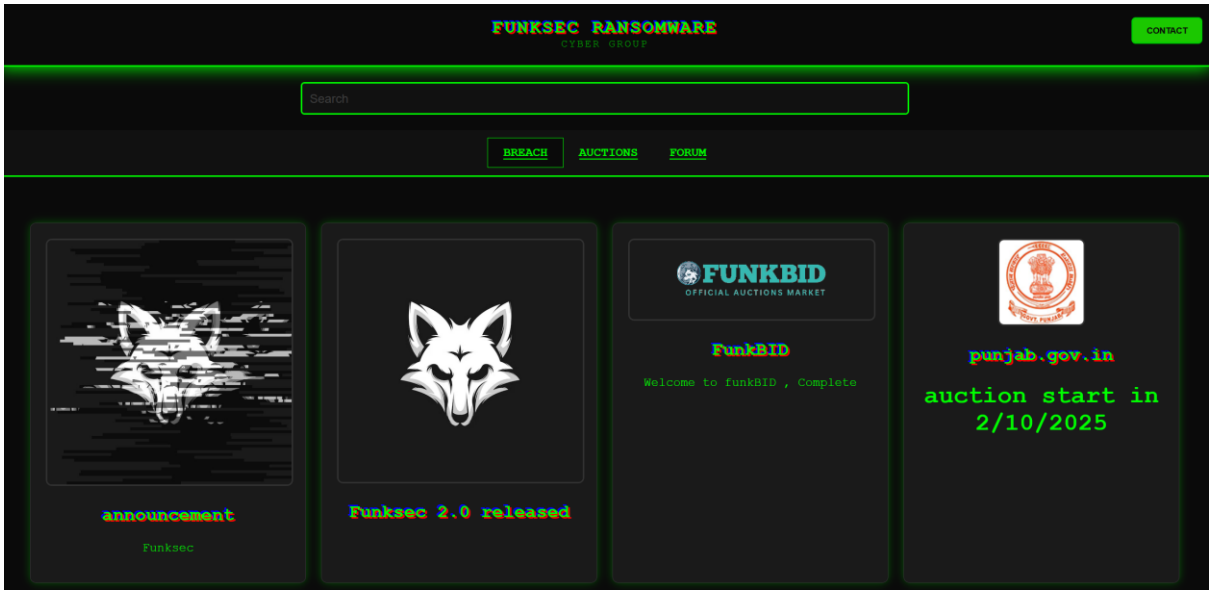

그림 6. Funksec 다크웹 유출 사이트

Funksec 그룹은 24 년 12 월 발견된 그룹이다. 이들은 12 월에만 89 건의 피해자를 게시하고, 지금까지 129 건의 피해자를 게시하며 위협적인 모습을 보여주고 있다. 또한 25 년 1 월에는 국내 제조업체의 데이터를 탈취해 업로드 했다. 또한 활동 초기에는 DDoS 공격 도구는 물론 브라우저에 저장된 계정 정보를 탈취하는 도구, 가상 네트워크를 구축해 사용자 몰래 원격 접속이 가능한 hVNC 악성코드를 다크웹 유출 사이트에 공개했지만, 현재는 GitHub 에서 무료로 공유하고 있다.

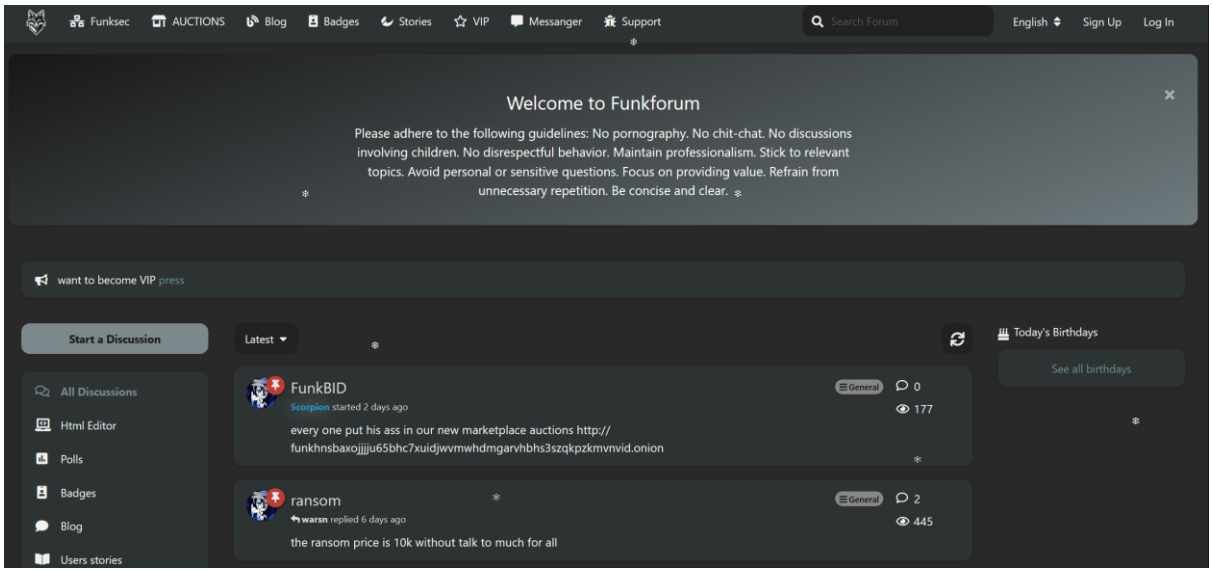

그림 7. Funksec 다크웹 포럼

다크웹 유출 사이트를 업데이트하며 Funkforum 이라는 다크웹 포럼을 개설해 자신들이 운영하기 시작했다. 포럼은 누구나 가입이 가능해 글을 작성하거나 열람이 가능하다. 아직까지 포럼에는 Funksec 운영자의 게시글이 대부분이며, FSociety 그룹와의 협력 소식이나 Funksec 2.0 출시 소식 등 Funksec 서비스의 주요 업데이트 내용을 공유하고 있다.

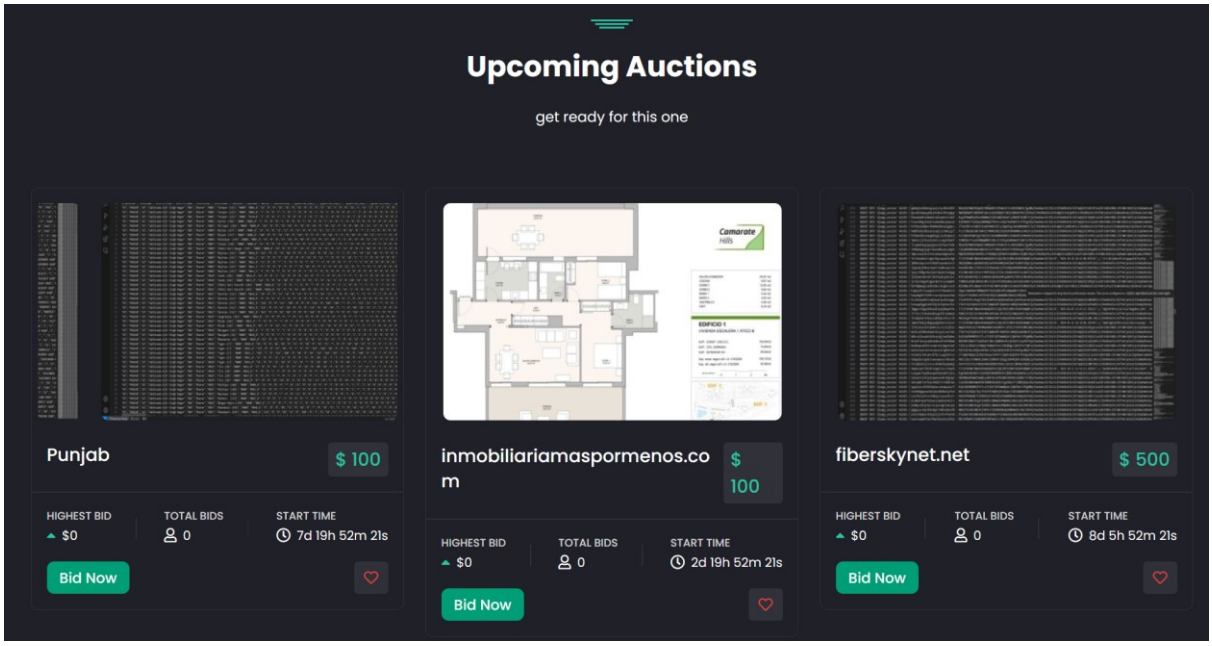

그림 8. FunkBID 경매

1 월 말, Funksec 그룹은 자신들이 탈취한 데이터를 경매로 판매하는 사이트인 FunkBID 를 개설했다. 1 월까지 다크웹 유출 사이트에 게시한 데이터는 기존 방식대로 일정 기간이 지나면 데이터를 전부 공개하고 있지만, FunkBID 개설 이후에 업로드된 데이터는 모두 경매로 판매되고 있다. 아직까지는 탈취한 데이터만 경매 진행중이거나 경매 예정이지만, FunkBID 에서는 멀웨어, 악성 도구, 접근 권한, 데이터베이스, 소스코드로 총 5 개로 경매를 분류하고 있기 때문에 단순 탈취 데이터뿐만 아니라 더 다양한 데이터가 공개될 가능성이 있다.

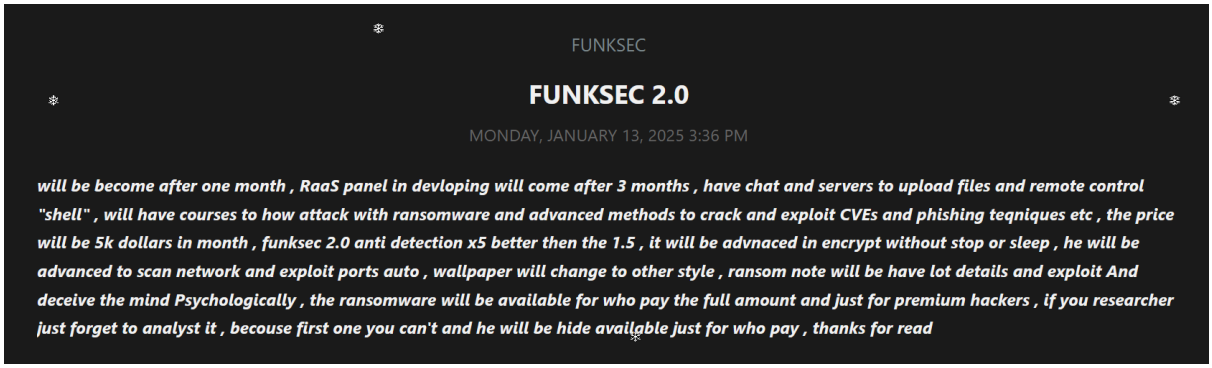

그림 9. Funksec 2.0 공지

이들은 또한 랜섬웨어를 서비스 형태로 제공하는 RaaS 를 제공할 예정이다. 1 월 초, 자신들의 다크웹 유출 사이트를 통해서 RaaS 이용자를 모집하기 시작했으며, 포럼을 통해서 RaaS 의 진행 사항을 공유하고 있다. RaaS 에서 서비스 이용자가 랜섬웨어 생성이나 피해자를 관리할 수 있는 관리 패널은 아직 개발 중으로, 4 월에 개발 완료 예정이며, RaaS 에서 사용하게 될 랜섬웨어인 Funksec 2.0 은 2 월 이후에 개발이 완료될 예정이라고 밝혔다. 또한 랜섬웨어 공격에 사용할 수 있는 취약점 사용 방법이나 피싱 메일 기술에 대한 교육도 월 5,000 달러(한화 약 730 만원)에 제공할 예정이라고 밝혔다.

```rust
fn encrypt_data(data: &[u8]) -> Vec<u8> {
    let mut rng = OsRng;
    let bits = 2048;
    let private_key = RsaPrivateKey::new(&mut rng, bits).expect("Failed to generate a key");
    let public_key = RsaPublicKey::from(&private_key);

    let aes_key = [0u8; 32]; // 256-bit key
    let cipher = Aes256::new(&aes_key.into());

    let mut buffer = data.to_vec();
    cipher.encrypt(&mut buffer);

    let encrypted_data = public_key.encrypt(&mut rng, PaddingScheme::new_pkcs1v15_encrypt(), &buffer).expect("Failed to encrypt");
    encrypted_data
}
```

그림 10. 공개된 ransomware.rs 소스코드 일부

1 월 초에는 Funksec 그룹이 사용하는 랜섬웨어인 FunkLocker v1.5 의 일부 샘플이 공개됐다. 자신들의 다크웹 유출 사이트에 백신 프로그램의 이름인 Avast Premium 으로 샘플을 공개했으며, 그 외에도 개발 단계로 보이는 Rust 기반의 소스코드(ransomware.rs) 등이 공개되기도 했다. 다가오는 Funksec 그룹의 위협에 대응하기 위해 공개된 FunkLocker v1.5 를 분석한 내용을 공유하고자 한다.

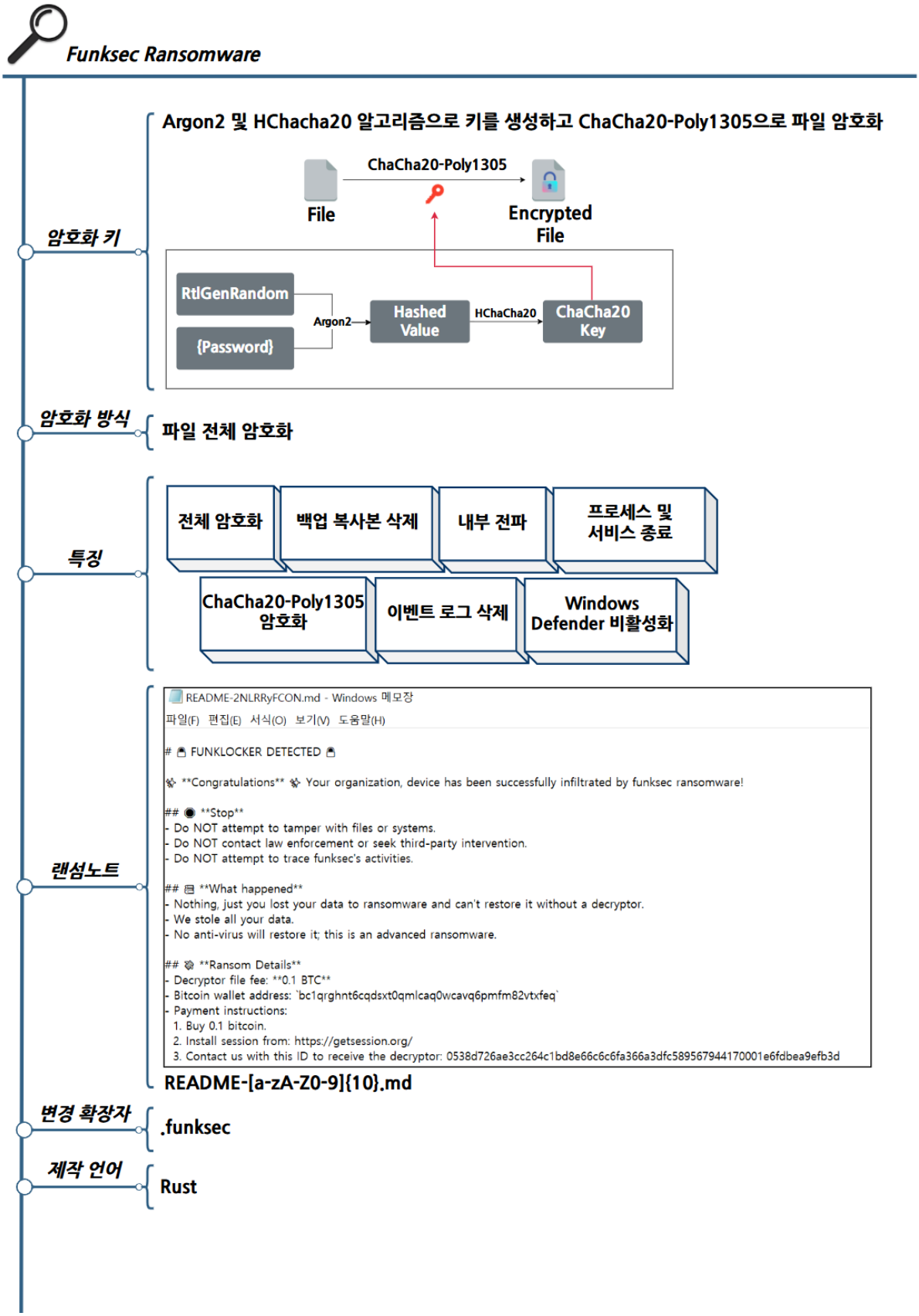

그림 11. Funksec 랜섬웨어 개요

Funksec 랜섬웨어 전략

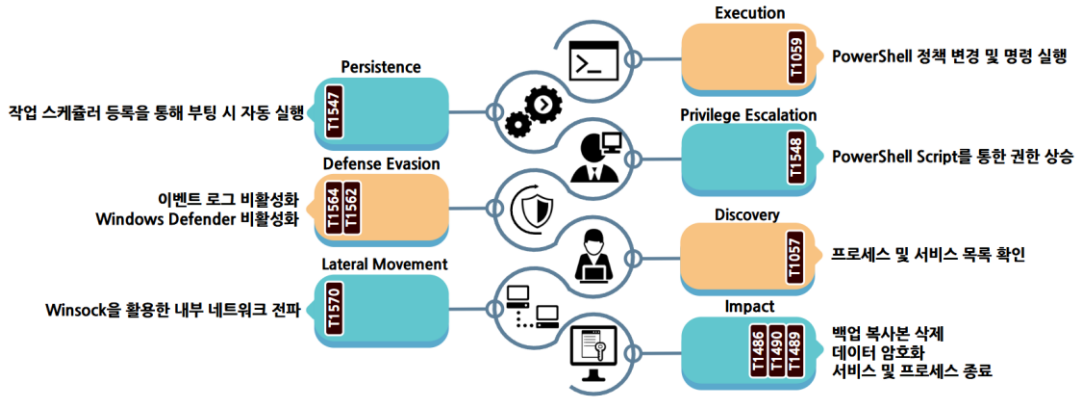

그림 12. Funksec 랜섬웨어 공격 전략

Funksec 랜섬웨어는 파일 암호화, 백업 복사본 삭제, 이벤트 로그 삭제 등 여러 작업을 원활히 수행하기 위해서 관리자 권한을 필요로 한다. 랜섬웨어 실행 시 권한을 확인한 후 PowerShell 명령어를 이용해서 현재 실행중인 랜섬웨어를 관리자 권한으로 재실행하고, 현재 실행중인 랜섬웨어는 종료한다. 사용하는 PowerShell 명령어는 아래와 같다.

명령어
PowerShell Start-Process -FilePath "{file_path}" -Verb RunAs -ArgumentList "{argv}"

표 1. 랜섬웨어 재실행 명령어

관리자 권한으로 재실행한 후, 현재 대상 환경이 가상 환경인지 체크한다. Windows 에서 프로세스 목록을 확인할 수 있는 tasklist 명령어를 활용하며, 확인된 리스트에서 가상 환경과 연관된 프로세스를 확인한다. 단, 실행중인 환경이 가상 환경임을 탐지하더라도 “VM detected, aborting.” 만 명령 프롬프트에 출력될 뿐, 별도의 프로그램 종료나 랜섬웨어 종료와 같은 분석 방해 행위는 발견되지 않았다.

프로세스명
vmware, vboxservice, qemu, hyperv

표 2. 가상 환경 확인 대상

또한 하드코딩된 프로세스 및 서비스 목록을 이용해, 대상 환경에서 프로세스와 서비스를 강제로 종료시킨다. 확인된 프로세스 및 서비스 목록은 아래 표와 같다.

프로세스	서비스
system32.exe, chrome.exe, firefox.exe, explorer.exe, outlook.exe, spotify.exe, vlc.exe, Skype.exe, Teams.exe Discord.exe Java.exe Python.exe, Node.exe, Javaw.exe, Winword.exe, Excel.exe, Powerpnt.exe, cmd.exe, PowerShell.exe, notepad++.exe, gimp-2.10.exe, photoshopt.exe, itunes.exe	WinDefend, wuauserv, bits, Spooler, DockApp, MpsSvc, XblGameSave, DiagTrack, SysMain, lfsvc, seclogon, wscsvc, trkwks, RemoteRegistry, netprofm, Netsh, twinapi.appcore, TimeBrokerSvc, RasMan, sshd, LanmanWorkstatio, CryptSvc, EventLog

표 3. 종료 대상 프로세스 및 서비스

프로세스 및 서비스 종료 후, 현재 실행중인 랜섬웨어를 내부 네트워크로 전파한다. 전파 대상은 하드코딩된 네트워크 대역으로, Windows 에서 제공하는 네트워크 및 소켓 API Winsock 을 이용해 연결을 시도하고, 대상 네트워크에 랜섬웨어 전송을 시도한다. 단, 하드코딩된 네트워크 대역의 범위가 매우 한정적이여서 사실상 실제 내부 전파 가능성은 매우 낮다. 내부 전파에 사용하는 IP 주소는 아래 표와 같다.

IP 주소	Port
192.168.1.2~21	4444

표 4. 내부 전파 대상

또한 랜섬웨어를 작업 스케줄러에 등록해 시스템 부팅 시 랜섬웨어가 실행될 수 있도록 한다. 사용하는 명령어는 아래와 같다.

명령어
schtasks /create /tn funksec /tr “{path}” /sc onstart

표 5. 작업 스케줄러 등록 명령어

랜섬웨어의 악성 행위가 탐지되거나 기록되지 않게 일부 보안 정책을 비활성화하고 실행 정책을 변경한다. Windows Defender 의 감시 및 이벤트 로그 기능 또한 비활성화 하며, PowerShell 의 정책 또한 수정해 모든 스크립트를 허용한다. 모든 PowerShell 명령어 수행이 끝나면, 백업 저장본을 삭제한다.

명령어	설명
powershell -Command Set-MpPreference -DisableRealtimeMonitoring $true	Windows Defender 실시간 보호 비활성화
powershell -Command wevtutil sl Security /e:false	보안 이벤트 로그 비활성화
powershell -Command wevtutil sl Application /e:false	응용 프로그램 이벤트 로그 비활성화
powershell -Command Set-ExecutionPolicy Bypass -Scope Process -Force	PowerShell 실행 정책 변경

표 6. PowerShell 명령어

온라인 이미지 공유 커뮤니티에 사전에 업로드한 이미지를 다운로드 후, 바탕화면을 변경한다. 2 월 기준으로 해당 이미지 다운로드는 더 이상 불가능하며, 이미지가 다운로드 되지 않으면 별도의 에러 로그를 출력하며 바탕화면 변경은 건너뛴다.

그림 13. Funksec 랜섬웨어 바탕화면

이후에는 하드코딩된 랜섬노트를 현재 랜섬웨어 실행 경로 위치에 저장한다. 랜섬노트는 마크다운[4] 형태이며 이때 랜덤한 10 글자의 문자열을 생성해 랜섬노트 제목에 삽입한다.


README-2NLRRyFCON.md - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```
# 🔒 FUNKLOCKER DETECTED 🔒

✨ **Congratulations** ✨ Your organization, device has been successfully infiltrated by funksec ransomware!

## 🔴 **Stop**
- Do NOT attempt to tamper with files or systems.
- Do NOT contact law enforcement or seek third-party intervention.
- Do NOT attempt to trace funksec's activities.

## 📖 **What happened**
- Nothing, just you lost your data to ransomware and can't restore it without a decryptor.
- We stole all your data.
- No anti-virus will restore it; this is an advanced ransomware.

## 💸 **Ransom Details**
- Decryptor file fee: **0.1 BTC**
- Bitcoin wallet address: `bc1qrghnt6cqdsxt0qmlcaq0wcavq6pmfm82vtxfeq`
- Payment instructions:
  1. Buy 0.1 bitcoin.
  2. Install session from: https://getsession.org/
  3. Contact us with this ID to receive the decryptor: 0538d726ae3cc264c1bd8e66c6c6fa366a3dfc589567944170001e6fdbea9efb3d

## 📖 **How to buy bitcoin**
- Go to [Coinbase](https://www.coinbase.com/) or any similar website like [Blockchain](https://www.blockchain.com/), use your credit

## 📖 **Who we are**
- We are an advanced group selling government access, breaching databases, and destroying websites and devices.

## 📖 **Websites to visit**
- funkiydk7c6j3vvck5zk2giml2u746fa5irwalw2kjem6tvofji7rwid.onion
- funknqn44slwmgwgnewne6bintbooauwkaupik4yrlgtycew3ergraid.onion
- funkxxkovrk7ctnggbjnthdajav4ggex53k6m2x3esjwlxrkb3qiztid.onion

🎶 *Start dancing, 'cause the funk's got you now!* 🎶

Sincerely,

Funksec cybercrime
```

그림 14. Funksec 랜섬노트

[4] 마크다운 (Markdown): 특수문자나 태그를 이용해 서식이 있는 문서를 작성할 수 있는 언어

앞선 모든 과정이 끝나고 난 뒤, A 드라이브부터 Z 드라이브까지 모두 확인해 연결된 드라이브를 대상으로 파일 암호화를 진행한다. 하드코딩된 암호화 대상 확장자 명과 폴더 명을 기준으로 특정 폴더와 그 하위에 있는 파일만 암호화를 진행한다. 암호화 대상 확장자와 폴더명은 아래 표와 같다.

확장자명
txt, csv, docx, xlsx, pdf, json, xml, sql, log, html, css, js, php, py, java, c, cpp, sh, bat, ini, yaml, md, rtf, ts, jsx, tsx, pptx, odt, ods, odpm, msg, eml, apk, ipa, exe, dll, dmg, iso, vmdk, vhd, tgz, 7z, zip, tar, rar, bak, db, mdb, sqlite, hdf5, parquet, avro, log, etl, pfx, cer, pem, csr, key, pgp, kdbx, gpg, tar.gz, xz, dbf, bak, tiff, raw, ai, psd, indd, eps, svg, dwg, dxf, fla, flv, mov, mp4, avi, mkv, mp3, wav, flac, aac, ogg, wma, webm, m3u, cue, midi, ps, tex, bib, chm, epub, azw3, fb2, djvu, opf, xps, jar, war, ear, pdb, msi, deb, rpm, apk, vcs, git, svn, nfs, cue, bin, bkp, lst, dat, csv, json, png

표 7. 암호화 대상 확장자

폴더명
Program Files, Program Files (x86), Windows, AppData, ProgramData, Users

표 8. 암호화 대상 폴더명

파일 암호화는 ChaCha20-Poly1305 알고리즘을 사용한다. AES 알고리즘을 사용해서 파일을 암호화하고 RSA 알고리즘으로 키를 보호하는 Rust 소스코드 또한 공개됐지만, 해당 소스코드는 암호화 함수만 존재하는 개발 단계 혹은 테스트 버전의 소스코드로 추정된다. 랜섬웨어에 저장된 비밀번호와 각 파일마다 랜덤하게 생성된 24Bytes 값으로 암호화에 사용할 ChaCha20-Poly1305 키를 생성한다. 키 생성에는 해시 알고리즘인 Argon2 와 HChaCha20 알고리즘을 사용하며, 각각의 파일마다 암호화 키를 생성해 파일 전체를 암호화한다. 암호화는 원본 데이터를 128 Bytes 단위로 암호화하며, 랜덤한 32Bytes 크기의 데이터를 추가로 생성해 암호화된 데이터와 함께 저장한다. 자세한 암호화 과정은 아래 그림과 같다.

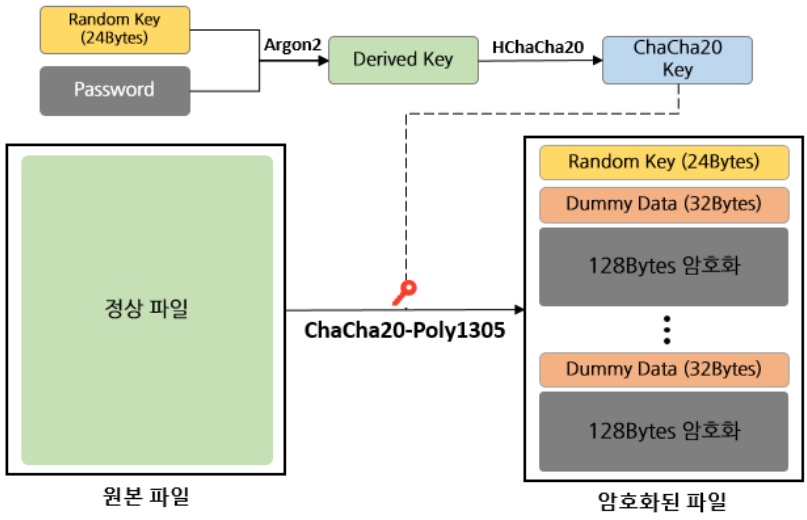

그림 15. Funksec 암호화 방식

Funksec 랜섬웨어 대응방안

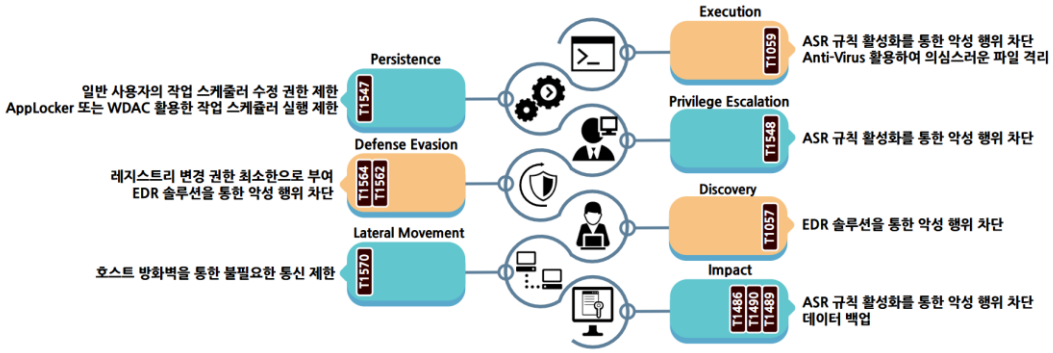

그림 16. Funksec 랜섬웨어 대응방안

Funksec 랜섬웨어는 악성 행위에 기본 내장 명령어나 PowerShell 명령어를 주로 사용한다. 이를 통해서 권한 상승을 시도하거나, 랜섬웨어를 작업 스케줄러에 관리자 권한으로 등록한다. ASR[5] 규칙을 활성화를 통해서 이러한 비정상적인 프로세스를 차단해 악성 행위를 막을 수 있다. 또한 작업 스케줄러의 경우 접근 권한을 제한해두거나 AppLocker[6]와 WDAC[7]를 활용해 작업 스케줄러가 지정된 조건 외에 실행되는 것을 차단할 수 있다.

또한 PowerShell 명령어를 사용해서 Windows Defender 의 실시간 보호 기능을 비활성화 하고 Windows 이벤트 로그 기능 또한 비활성화를 시도한다. 이러한 경우, 이벤트 로그를 권한이 있는 사용자만 접근할 수 있도록 사전에 설정해 두거나 이벤트 로그를 원격 저장소에 별도로 저장해 보존할 수 있다. 그 외에도 EDR[8] 솔루션을 통해 공격자가 사용하는 특정 프로세스를 차단해 악성 행위를 막을 수 있다.

랜섬웨어를 내부 네트워크에 전파하기 위해서 Windows 의 네트워크 관련 API 인 Winsock 을 활용해 내부 네트워크 대역에 전파를 시도한다. 하드코딩된 네트워크 대역대에만 4444 포트를 통해서 네트워크 연결 및 랜섬웨어 전파를 시도하기 때문에 호스트 방화벽을 통해서 특정 포트를 차단해 불필요한 통신을 제한할 수 있다.

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

6 AppLocker: Windows 운영체제에서 특정 프로그램을 실행할 수 있는 경로나 사용자 등을 지정해, 실행할 수 있는 프로그램을 사전에 제한할 수 있는 보안 기술

7 WDAC(Windows Defender Application Control): 사용자가 실행할 수 있는 프로그램이나 코드를 제한하도록 설정해, 서명되지 않은 프로그램이나 스크립트 등의 실행을 방지하는 보안 기술

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

파일 암호화에 앞서 사용자가 임의로 복구하는 것을 방지하기 위해 백업 복사본을 삭제한 뒤 파일 암호화를 진행한다. ASR 규칙 활성화를 통해서 백업 복사본을 삭제하는 프로세스와 파일을 암호화는 것을 차단할 수 있다. 또한 백업 복사본의 경우 별도의 네트워크나 저장소에 소산 백업해야 한다.

Indicator Of Compromise

Funksec (SHA-256)

7e223a685d5324491bcacf3127869f9f3ec5d5100c5e7cb5af45a227e6ab4603
c233aec7917cf34294c19dd60ff79a6e0fac5ed6f0cb57af98013c08201a7a1c
89b9f7499d59d0d308f5ad02cd6fddd55b368190c37f6c5413c4cfcd343eeff3
5226ea8e0f516565ba825a1bbed10020982c16414750237068b602c5b4ac6abd
504984fe49af411cd50fdfedb8ff114ed206c4b82a68fe21e7a215cbb53a91c2

File Name

ransomware.rs
dev.exe
setup-avast-premium-x64.exe
setup-x64.exe

■ 참고 사이트

• BleepingComputer 공식 홈페이지 (https://www.bleepingcomputer.com/news/security/babuk-locker-is-the-first-new-enterprise-ransomware-of-2021)

• The Hacker News (https://thehackernews.com/2025/01/experts-find-shared-codebase-linking.html)

• SecurityWeek (https://www.securityweek.com/compromised-aws-keys-abused-in-codefinger-ransomware-attacks/)

• Halcyon Research (https://www.halcyon.ai/blog/abusing-aws-native-services-ransomware-encrypting-s3-buckets-with-sse-c)

• KELA 블로그 (https://www.kelacyber.com/blog/is-gdlockersec-really-targeting-aws/)

• 보안 뉴스 (https://www.boannews.com/media/view.asp?idx=135368&direct=mobile)

• Group IB 블로그 (https://www.group-ib.com/blog/cat-s-out-of-the-bag-lynx-ransomware/)