Keep up with Ransomware

중소기업을 노리는 8Base 랜섬웨어의 위협

■ 개요

2024년 4월 랜섬웨어 피해 사례는 전월(405건) 대비 20건 감소한 385건으로 나타났다. 이는 신규 랜섬웨어 그룹들이 등장하며 활발한 움직임을 보였지만, 그동안 많은 피해를 발생시켰던 락빗(LockBit) 랜섬웨어 그룹의 공격이 전월에 비해 절반 가량 줄어들었기 때문으로 분석된다.

랜섬허브(RansomHub) 랜섬웨어 그룹은 BlackCat(Alphv) 랜섬웨어 그룹의 Exit Scam[1]과 관련 있는 데이터를 게시하여 화제가 됐다. 이 데이터는 미국의 의료 시스템 기업인 체인지 헬스케어(Change HealthCare)사의 유출 데이터로, Change HealthCare 는 지난 2 월 BlackCat(Alphv)의 공격으로 시스템 운영에 장애가 생겼으며 환자들의 개인 정보가 포함된 4TB 크기의 데이터를 공개하겠다는 협박을 받았다. Change HealthCare 는 이 문제를 해결하기 위해 BlackCat(Alphv)이 지정한 비트코인 지갑에 2,200 만 달러(한화 약 300 억 원)의 돈을 입금했지만, 입금 이후 BlackCat(Alphv)은 Exit Scam 을 벌이며 종적을 감췄다. BlackCat(Alphv)이 사라지면서 이들과 계약을 맺었던 계열사들은 정산 받지 못하였는데, 금전적 손실을 입은 계열사가 RansomHub 그룹에 합류하면서 보유하고 있던 Change HealthCare 데이터가 게시된 것으로 보인다.

HelloKitty 랜섬웨어 그룹은 활동 중단 약 6 개월 만에 HelloGookie 로 이름으로 변경해 복귀했다. 이들은 새로운 다크웹 유출 사이트를 통해서 기존 HelloKitty 랜섬웨어가 사용했던 복호화 키와 일부 데이터를 공개했다. 그 중에는 폴란드의 게임개발 및 보급사인 CD 프로젝트 레드(CD Projekt RED)의 데이터와 일부 게임의 소스코드가 포함돼 있다. 또한 이들은 다크웹 포럼을 통해 본인들의 신규 유출 사이트를 홍보하거나, 직원을 모집하는 등 본격적인 활동을 준비하는 모습을 보이고 있다.

[1] Exit Scam: 계열사에게 수수료를 지급하지 않거나 랜섬웨어 피해자에게 돈을 지불 받고 파일 복구를 해주지 않은 채 사라지는 사기 행위

2022 년 9 월에 활동을 중단했다가 12 월 다시 복귀한 랩서스(LAPSUS$) 랜섬웨어 그룹이 올해 3 월부터 랜섬웨어 서비스와 소스코드 판매를 시작했다. LAPSUS$ 그룹은 2021 년부터 2022 년 9 월까지 엔비디아, 마이크로소프트 등 유명 기업을 표적으로 네트워크 침투, 계정 및 데이터 탈취를 주로 수행했다. 복귀 후에는 랜섬웨어 배포 및 지속적인 업데이트를 제공하고 있으며, 4 월에는 암호화 속도를 개선하며 본격적인 활동에 나섰다. 특히, 최근에는 MS 워드 문서(.doc)의 취약점을 통해 랜섬웨어를 다운로드 후 실행시킬 수 있는 익스플로잇(Exploit)[2] 버전 판매도 시작했다. LAPSUS$ 그룹은 과거 유명 기업을 해킹하며 악명높은 공격 조직으로 알려진 만큼 주의가 필요하다.

튀니지 기반의 랜섬웨어 그룹 트리섹(Trisec)은 올해 2 월에 등장했으나, 지난 4 월을 기점으로 활동을 종료한 것으로 보인다. 이들은 2 월에 게시한 3 건의 피해 외에는 추가적인 피해 사례를 게시하지 않고 있으며, 4 월에는 다크웹 유출 사이트가 비활성화 됐다. 또한 다크웹 포럼에서도 2 월 게시한 구성원 모집 및 다크웹 유출 사이트 홍보글 외에는 추가적인 게시글이 확인되지 않아, 사실상 활동을 중단한 것으로 보인다.

한편, ESXi[3]를 공격하여 한 번의 공격으로 여러 가상 서버를 감염시킬 수 있는 랜섬웨어 위협이 지속되고 있다. 지난 4 월 SEXi 랜섬웨어가 칠레의 웹 서비스 호스팅 업체 IxMetro PowerHost 를 감염시키면서 그 존재가 드러났다. SEXi 랜섬웨어는 별도의 다크웹 유출 사이트를 운영하지 않으며, 랜섬노트에 기재되어 있는 세션 메신저(Session Messenger)[4] 앱의 주소를 통해 협상을 진행하고 있다. 이들이 요구한 협상 금액은 1 억 4,000 만 달러(한화 약 1,915 억 원)로 밝혀졌으나, IxMetro PowerHost 는 금액을 지불하지 않은 것으로 확인됐다.

에잇베이스(8Base) 랜섬웨어 그룹은 4 월 초 다크웹 유출 사이트에 국내 페인트 관련 제조 업체를 게시했다. 8Base 는 보안이 상대적으로 취약한 중소기업을 주로 공격하는 랜섬웨어 그룹이다. 게시된 자료에는 계산서와 회계 자료, 개인정보, 인증서, 기밀 문서와 같은 민감한 정보들이 포함되어 있다. 해당 문서 자료들은 4 월 8 일 공개되었으며, 현재는 다운로드 링크가 만료된 상태다.

[2] 익스플로잇(Exploit): 소프트웨어 혹은 하드웨어의 버그나 보안상 취약한 부분을 이용해 공격자의 의도된 행위를 수행할 수 있는 공격 방식

[3] ESXi: VMware 에서 개발한 호스트 컴퓨터에서 다수의 운영체제를 동시에 실행시킬 수 있는 UNIX 기반의 논리적 플랫폼

[4] 세션 메신저(Session Messenger): 관리하는 중앙 서버가 존재하지 않는 탈중앙화 메신저로, 통신을 위해서 계정 대신에 별도의 Session ID 를 이용하는 방식을 사용

■ 랜섬웨어 뉴스

infosec

RansomHub, Change HealthCare 2차 공격

- BlackCat(Alphv) 그룹의 Exit Scam과 관련된 피해 기업으로, RansomHub DLS에서 데이터 판매 글 게시
- RansomHub는 BlackCat(Alphv)의 Exit Scam 이후 관련 계열사들이 합류하여 데이터를 얻을 수 있었다고 주장
- Change HealthCare는 몸값 지불과 공격 대응 비용, 비즈니스 중단으로 8억 7,200만 달러의 손해 발생

INC Ransom, 영국 레스터 시의회 공격

- 3월 발생한 영국 레스터 지방 당국의 아동 보호, 사회 복지와 같은 주요 서비스 중단과 관련된 공격
- 레스터 시의회의 IT 인프라는 복구하였지만, 1.3TB의 데이터 추가 공개 사실 확인

LockBit, 미국 워싱턴 보험, 증권 및 은행부 데이터 공개

- 4월 13일 LockBit DLS에 게시되었으며, DC DISB 측에서는 프라이빗 클라우드를 통해서 유출되었음을 확인
- 자세한 협상 내용은 공개되지 않았지만, 4월 23일 데이터 공개를 통해서 협상이 결렬되었음을 알림

신규 Psoglav 랜섬웨어 그룹 파트너 모집

- C# 기반으로 만들어진 랜섬웨어로, 주요 기능과 파트너 모집 조건 공개
- 하나의 피해자 당 150 달러의 복호화 비용을 책정하였고, 장기적으로 협업할 파트너 모집

HelloKitty 랜섬웨어 복호화 키 공개 및 HelloGookie로 리브랜딩

- 2020년 11월 등장하여 2023년 10월 활동 중단. 게임 개발 및 보급사 CD Projekt Red를 공격한 이력 존재
- HelloGookie로 리브랜딩하며 복귀하였고, CD Projekt Red 추가 데이터, Cisco 내부 데이터, HelloKitty 복호화 키를 공개
- XSS 포럼을 통해서 피해자에게 연락을 취하는 직원 채용 글 게시

LAPSUS$ 그룹, 랜섬웨어 판매 시작

- 2021년부터 활동을 시작하여 2022년 9월 활동 중단한 그룹으로, 동일한 이름을 사용하는 그룹이 2023년 12월 등장
- 1년 전 활동을 중단했던 동일한 LAPSUS$ 그룹이라고 주장
- 2024년 3월부터 랜섬웨어 판매를 시작하여 기능을 추가하거나 개선하는 등 지속적인 업데이트 진행

Trisec 랜섬웨어 그룹 DLS 비활성화

- 2024년 2월 등장한 튀니지 기반 그룹으로 피해자 3건을 게시
- 사용중인 DLS 도메인 3개 모두 비활성화 되며 활동을 중단한 것으로 추정


ESXi를 타깃으로 하는 SEXi 랜섬웨어 등장
VMware ESXi를 타깃으로 하며, 가상 머신 파일들을 암호화
칠레의 웹 서비스 호스팅 업체인 IxMetro PowerHost가 피해를 받았으며, 협상 금액으로 1억 4,000만 달러 요구
CISA, Akira 그룹 관련 보안 권고문 업데이트
등장 1년만에 약 240명의 피해자 게시 및 몸값으로 4,200만 달러의 수익 달성
Akira v2 변종과 Akira ESXi, Megazord 등 각종 변종을 활용한 공격 방식 소개
Cyble, DragonForce와 LockBit과의 연관성 발견
DragonForce는 2023년 11월 등장한 말레이시아 기반 랜섬웨어 그룹
최근 발견된 DragonForce 샘플이 유출된 LockBit 3.0 빌더로 만들어진 정황 포착

그림 1. 랜섬웨어 동향

■ 랜섬웨어 위협

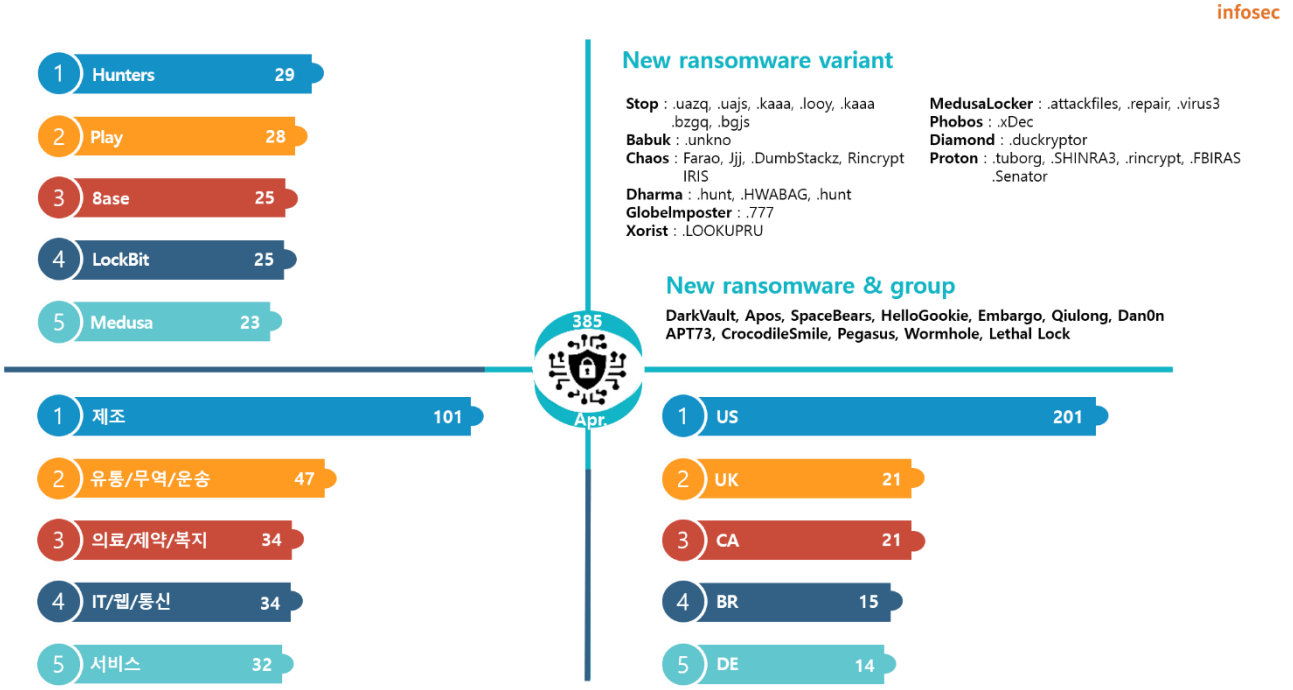


그림 2. 2024 년 4 월 랜섬웨어 위협 현황

새로운 위협

4 월에는 여러 랜섬웨어 그룹에서 랜섬웨어 판매, 파트너 모집 등의 움직임을 보이며 본격적인 활동을 준비하는 정황이 포착됐으며, 신규 랜섬웨어 그룹들도 다수 등장했다. 러시아 해킹 포럼에서는 Windows, Linux, ESXi 시스템을 모두 감염시킬 수 있는 Ultra 랜섬웨어 판매 글과 장기적으로 일할 파트너를 모집하는 프소글라브(Psoglav) 랜섬웨어 그룹의 게시글이 확인됐다. 또한, LAPSUS$ 그룹이 3 월부터 Windows 용 랜섬웨어를 판매하고 지속적으로 업데이트 하고 있는 것으로 확인됐다.

2023 년 10 월 활동을 중단한 HelloKitty 그룹이 HelloGookie 로 이름을 변경하며 활동을 재개했다. HelloKitty 그룹의 관리자로 추정되는 'kapuchin0'는 러시아 해킹 포럼인 XSS 포럼에 자신들의 랜섬웨어 소스코드를 공개 후 활동을 중단했으나, 약 5 개월 만에 새로운 다크웹 유출 사이트 주소를 게시하며 복귀 소식을 알렸다. 새로 공개한 다크웹 유출 사이트에서 HelloKitty 랜섬웨어에 사용한 복호화 키를 공개했으며, HelloKitty 로 활동할 당시 얻은 시스코(Cisco)의 NTLM 해시[5] 데이터와 CD Projekt Red 의 게임인 The Witcher 3, Cyberpunk, Gwent 의 소스코드가 저장된 토렌트

[5] NTLM 해시: Windows 의 인증 프로토콜인 NTLM(NT LAN Manager)에 비밀번호 대용으로 사용되는 해시 값

마그넷 주소[6]를 게시했다. 또한 이들은 XSS 포럼에 LockBit 그룹과 Yanluowang/Saint 그룹에게 연락을 요청하는 글, 직원 모집 글 등을 게시하며 본격적인 활동을 준비하는 모습을 드러내고 있다.

기존 그룹의 복귀뿐만 아니라 신규 랜섬웨어 그룹들의 움직임도 다수 확인됐다. 4 월에는 7 개의 새로운 다크웹 유출 사이트가 발견됐다. Apos 랜섬웨어 그룹은 특이하게 노션(Notion[7])을 통해서 피해자를 게시했다. 그러나 4 월 30 일 기준으로 해당 페이지가 삭제됐으며, 이후 추가적인 활동 정황은 확인되지 않고 있다. Qiulong 랜섬웨어 그룹은 특정 국가와 산업군을 대상으로 집중적인 공격을 취하고 있다. 게시한 피해자 6 건 모두 브라질 기업이며, 그 중 5 건은 의료서비스 관련 기업으로 확인됐다. 특히, 환자의 신체가 노골적으로 드러난 사진을 샘플로 게시하는 독특한 방식을 취하고 있다.

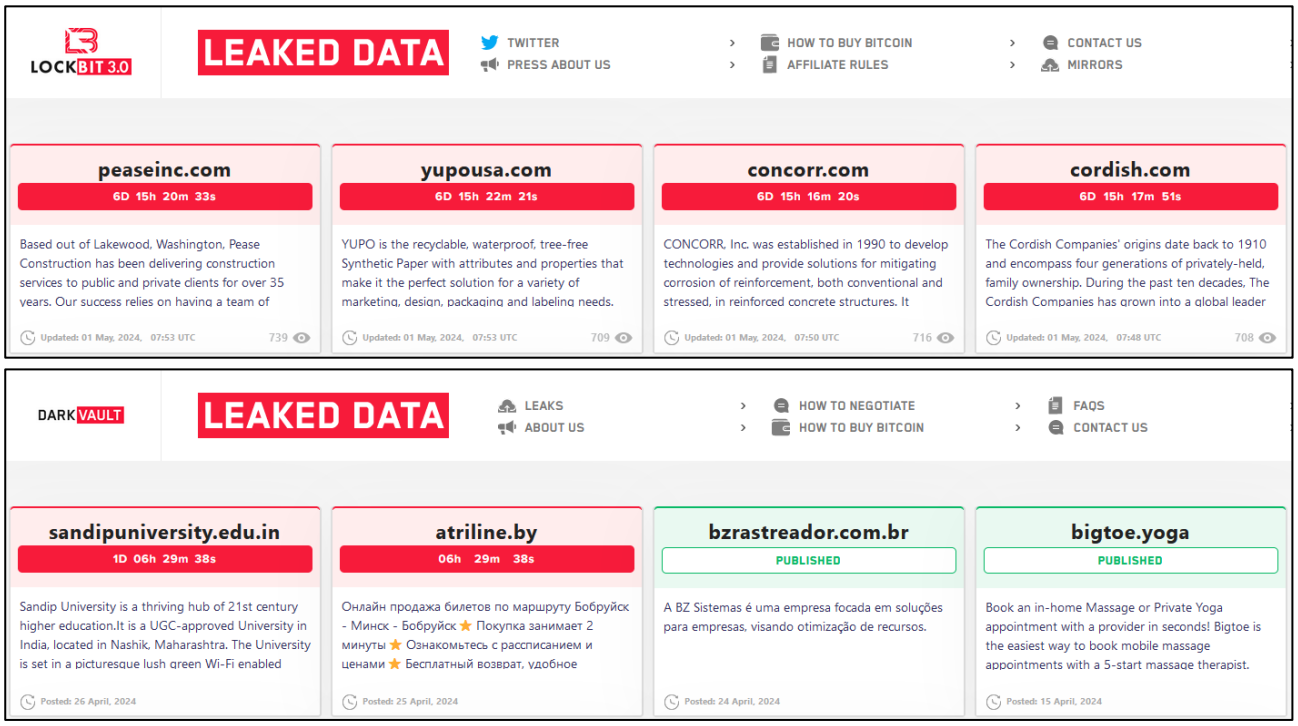


그림 3. 다크웹 유출 사이트 비교(상: LockBit 3.0, 하: DarkVault)

[6] 토렌트 마그넷 주소: 사용자들 간에 직접 파일을 공유할 수 있는 프로토콜 또는 프로그램인 토렌트에서 토렌트 파일 대신 사용할 수 있는 URI 스키마

[7] 노션(Notion): 메모, 데이터베이스, 칸반 보드, Wiki, 달력 등을 제공해주는 all-in-one 애플리케이션

이 밖에도 LockBit 랜섬웨어 그룹의 유출 페이지와 비슷한 디자인과 구성을 가진 그룹들도 확인됐다. APT73(Eraleign) 랜섬웨어 그룹은 클리어 웹[8]에 유출 사이트를 개설했다가 폐쇄했다. 현재는 다크웹 유출 사이트를 통해서 데이터를 게시 중이다. 2 월부터 활동을 시작한 DarkVault 그룹은 4 월에 다크웹 유출 사이트가 발견됐다. LockBit 의 다크웹 유출 사이트, 로고 등 유사한 디자인을 사용하고 있으며, 버그 바운티[9] 페이지 내용을 그대로 사용하는 등의 모습을 미루어 봤을 때 LockBit 그룹을 모방한 것으로 보인다.

[8] 클리어 웹: 검색엔진으로 찾을 수 있는 일반적인 정보

[9] 버그 바운티: 소프트웨어나 시스템의 보안 취약점을 찾는 것에 대해 보상을 지급하는 제도

Top5 랜섬웨어

그림 4. 산업/국가별 주요 랜섬웨어 공격 현황

헌터스(Hunters) 랜섬웨어 그룹은 2023 년 10 월부터 활동을 시작해 지금까지 약 120 건의 유출 피해를 게시하며 활발하게 활동하고 있다. 4 월에는 대만의 전자부품 제조 업체인 치코니 전자(Chicony Electronics)를 공격해 얻은 데이터를 다크웹 유출 사이트에 게시했다. 이들이 게시한 데이터에는 국내 기업을 비롯해 미국의 카메라 브랜드 고프로(GoPro), 항공우주 기업 스페이스 X(SpaceX), 전자제품 제조업체 DELL, HP, 구글 등 여러 유명 기업의 데이터들이 포함돼 있다. Chicony Electronics 는 컴퓨터/노트북 부품과 이미지 장치를 주력으로 제조 및 납품하기 때문에 앞서 언급한 기업의 제품 설계도와 같은 정보가 유출된 것으로 보인다. Hunters 그룹은 데이터 유출 방지를 위한 협상 금액으로 33 억 달러(한화 약 4 조 5,100 억 원)를 요구하고 있다.

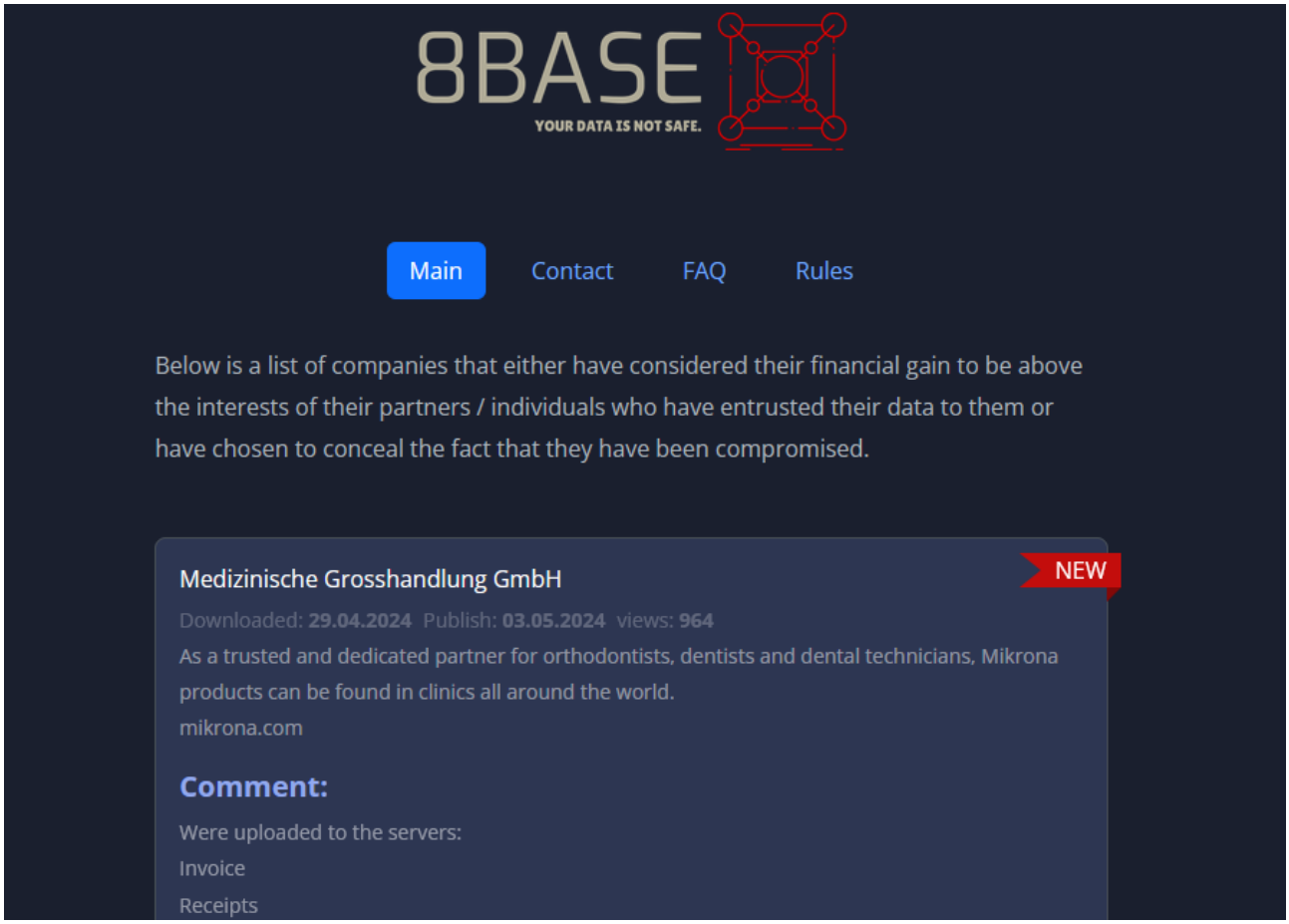
LockBit 랜섬웨어 그룹은 올해 2 월 크로노스(Cronos) 작전[10]에 의해 인프라를 압수당한 후 빠르게 복귀했지만, 이전에 비해 활동량이 점차 감소하는 모습을 보이고 있다. 인프라를 압수당한 2 월에는 100 건의 유출을 게시하는 등 인프라 복구 이후 즉시 유출 데이터를 게시하며 건재함을 과시하는 모습을 보였으나, 3 월에는 2 월보다 약 50% 감소한 55 건을 게시했으며, 4 월에는 3 월보다 약 55% 감소한 25 건 밖에 게시하지 않았다. 이는, Cronos 작전의 여파로 보인다. 또한 LockBit 은 계열사들에게 "50% 이상의 할인은 엄격히 금지되어 있음을 모든 파트너에게 상기시켜 드립니다."라고 언급하며, 계열사 확보 보다는 수익에 초점을 맞추고 있는 것으로 보인다. 이는, 계열사에게 많은 수익을 돌려주는 여러 랜섬웨어 그룹들과는 다른 강경한 모습이다.

대부분의 랜섬웨어는 상대적으로 보안이 취약한 제조업이나 유통업을 대상으로 주로 공격을 진행한다. Hunters 랜섬웨어 그룹은 유통업 공격 비율이 34%로 가장 높으며, 플레이(Play) 랜섬웨어 그룹과 LockBit 랜섬웨어 그룹은 제조업 공격 비율이 각각 40%, 28%로 가장 많은 비율을 차지하고 있다. 8Base 랜섬웨어 그룹은 상대적으로 보안이 취약한 중소기업을 중점적으로 공격하는 그룹으로, 특히, 4 월 공격의 절반이 중소기업 중 제조업을 타겟으로 한 것으로 나타났다. 한편, 기존 랜섬웨어 그룹과는 달리 Medusa 랜섬웨어 그룹은 조금 다른 공격 양상을 보이고 있는데, 이들은 의료 분야나 정부 기관, 교육 기관을 주로 공격하는 모습을 보여주고 있다. Medusa 랜섬웨어 그룹이 4 월 수행한 공격 중 절반 이상이 의료, 기관, 교육 분야에 해당하며 전체 공격 중 35%를 차지하고 있다. 이는 다른 그룹들의 평균 수치인 20%보다 33%p 많은 수치로 다른 공격 양상을 보인다.

[10] 크로노스(Cronos) 작전: LockBit 의 공격 서버, 다크웹 유출 사이트 등 범죄 인프라를 파괴하기 위한 국제 수사기관의 공조작전

■ 랜섬웨어 집중 포커스

8Base 랜섬웨어 개요



출처: 8Base 랜섬웨어 그룹 데이터 유출 사이트

8Base 랜섬웨어 그룹은 2022 년 3 월에 등장했으며, 현재까지 약 380 여 건의 피해 사례를 다크웹 데이터 유출 사이트에 게시했다. 이들은 2023 년 5 월에 다크웹 데이터 유출 사이트를 개설한 후 피해 사례를 일괄적으로 게시했으며, 같은 해 6 월에만 47 건의 피해를 게시하며 본격적으로 활동을 시작했다. 특히, 2024 년 4 월에는 다크웹 유출 사이트에 국내 페인트 제조 기업이 1 건 게시됐다. 해당 기업의 회계 자료, 개인정보, 기밀 문서 등이 유출되면서 국내까지 영향을 미칠 수 있음을 보여주고 있다.

그림 5. 암호화 확장자 비교 (좌: Phobos, 우: 8Base)

현재 8Base 는 2019 년 발견된 포보스(Phobos) 기반의 랜섬웨어를 사용하고 있다. Phobos 랜섬웨어는 파일 관리 프로그램으로 위장해 국내에 배포된 적이 있는 Dharma/Crysis 랜섬웨어의 변종으로, 확장자가 다른 Phobos 변종이 꾸준히 등장하고 있다. 8Base 는 Phobos 2.9.1 버전을 활용했기 때문에 소스코드뿐만 아니라 랜섬노트의 내용과 디자인, 암호화 확장자 앞에 드라이브 볼륨 ID 와 공격자의 이메일을 추가하는 방식까지 유사하다. 이외에도 암호화 예외 대상에 다른 Phobos 변종들의 확장자가 포함되어 있는 점과 Phobos 랜섬웨어와 동일한 RSA 공개키를 사용하는 점 등을 통해 Phobos 랜섬웨어와의 연관성을 다수 확인할 수 있다.

또한, 8Base 가 기존에 사용하던 .NET [11] 기반의 랜섬웨어 뿐만 아니라, 2023 년 11 월 SmokeLoader 를 이용해서 배포하는 변종이 발견됐다. SmokeLoader 는 다운로더형 악성코드로 C2 서버 [12] 에 접속 후 명령에 따라 추가 도구나 악성코드를 다운로드할 수 있다. 8Base 의 SmokeLoader 변종의 경우 SmokeLoader 내부에 저장된 페이로드를 활용하거나 C2 서버(Command & Control Server)에 접속해 암호화된 랜섬웨어 페이로드(payload) [13] 를 다운로드해 복호화 후 실행하는 방식을 사용한다. 최종적으로 실행되는 랜섬웨어 페이로드는 .NET 기반의 랜섬웨어와 동일한 Phobos 변종의 랜섬웨어다.

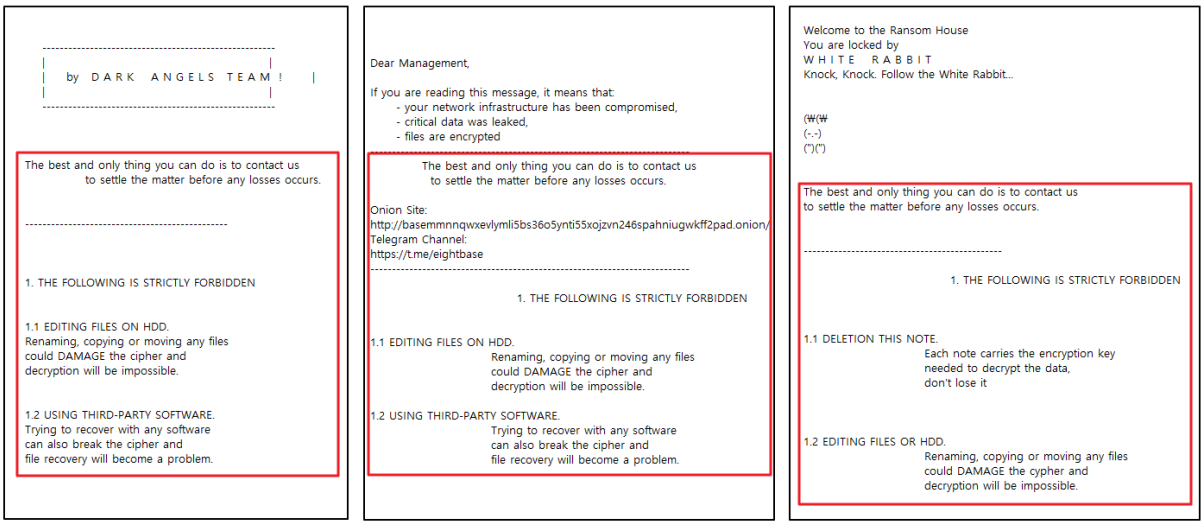


그림 6. 랜섬노트 비교 (좌: DarkAngels, 중: 8Base, 우: RansomHouse)

[11] .NET: MS 에서 개발한 Windows 프로그램 개발 및 실행 환경(프레임워크)

[12] C2 서버(Command & Control Server): 공격자가 초기 침투에 성공한 장치와 통신을 유지하거나 명령을 전달하는 서버

[13] 페이로드(payload): 컴퓨터 시스템에 침투, 변경 또는 기타 방식으로 손상을 입히도록 설계된 코드

8Base 는 Phobos 랜섬웨어 외에도 다양한 그룹들과의 연관성이 확인됐다. 현재 공격에 사용하고 있지는 않지만, 이들이 본격적으로 활동하기 시작한 2023 년 5 월경 발견된 랜섬노트는 DarkAngels 랜섬웨어와 유출된 Babuk 빌더를 사용한 RansomHouse(Mario/WhiteRabbit) 랜섬웨어의 랜섬노트와 내용이 매우 유사하다. 또한 8Base 그룹의 다크웹 데이터 유출 사이트는 RansomHouse 그룹의 사이트와 Main 페이지, FAQ 페이지, Rules 페이지의 문구와도 유사하다.

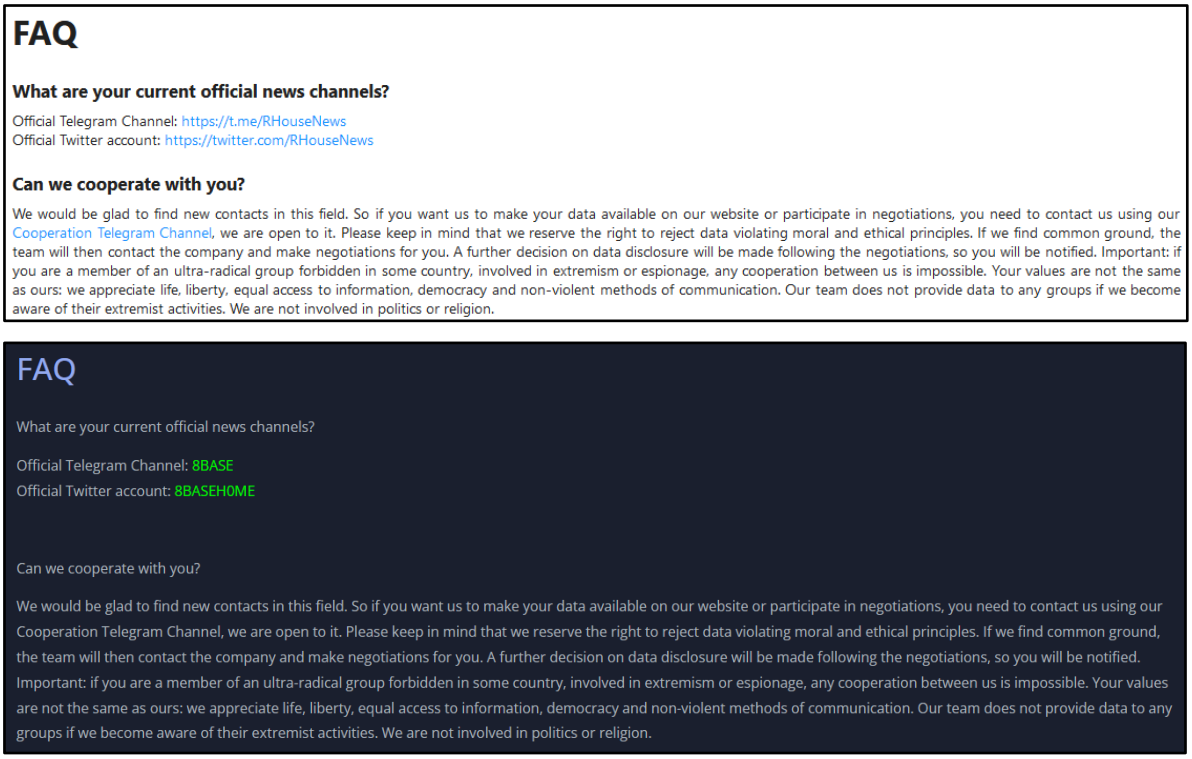


그림 7, 다크웹 유출 사이트 비교 (상: RansomHouse, 하: 8Base)

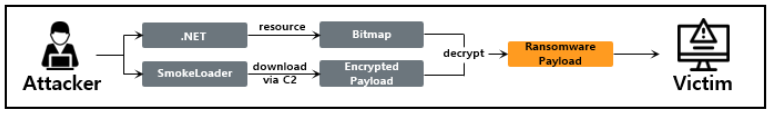
비슷한 형태의 랜섬노트가 발견됐다는 점과 다크웹 유출 사이트의 문구가 유사하다는 점으로 인해 8Base 그룹이 RansomHouse 그룹에서 파생되었거나 리브랜딩(Rebranding)[14]한 그룹이라는 의견이 존재했다. 하지만 다른 그룹의 문구를 인용하거나 복사해 그대로 사용하는 것과 유출된 도구를 사용하는 것은 드문 일이 아니기 때문에, 이들의 연관성을 판단하기에는 증거가 충분하지 않다.

[14] 리브랜딩(Rebranding): 공격자들이 운영을 중단한 후 새로운 이름으로 다시 운영하는 방식

8Base Ransomware

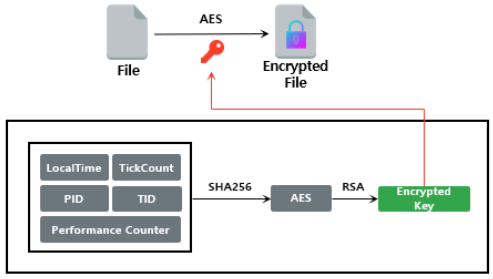
공격 시나리오

.NET 형태 혹은 SmokeLoader 변종을 통해 랜섬웨어 배포



암호화 키

AES-256(CBC) 알고리즘으로 파일 암호화를 하고, 해당 키를 RSA-1024로 보호



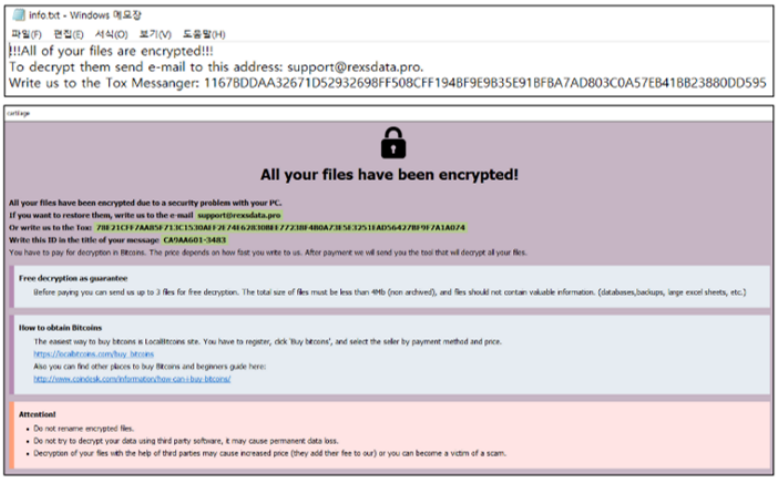
암호화 방식

1.5MB 미만 : 전체 암호화
1.5MB 이상 : 파일을 3등분 후, 각 영역마다 256KB만 암호화

특징

부분 암호화 | 시스템 복구 옵션 삭제 | 공유폴더 암호화 | 시작 프로그램 등록 | AES&RSA 암호화 | 멀티스레드 | 방화벽 해제 | UAC Bypass

랜섬노트



info.txt, info.hta

변경 확장자

Id[A-Z0-9]{8}-[0-9]{4}].[support@rexsdata.pro].8base

제작 언어

C# / C++

그림 8. 8Base 랜섬웨어 개요

8Base 랜섬웨어 전략

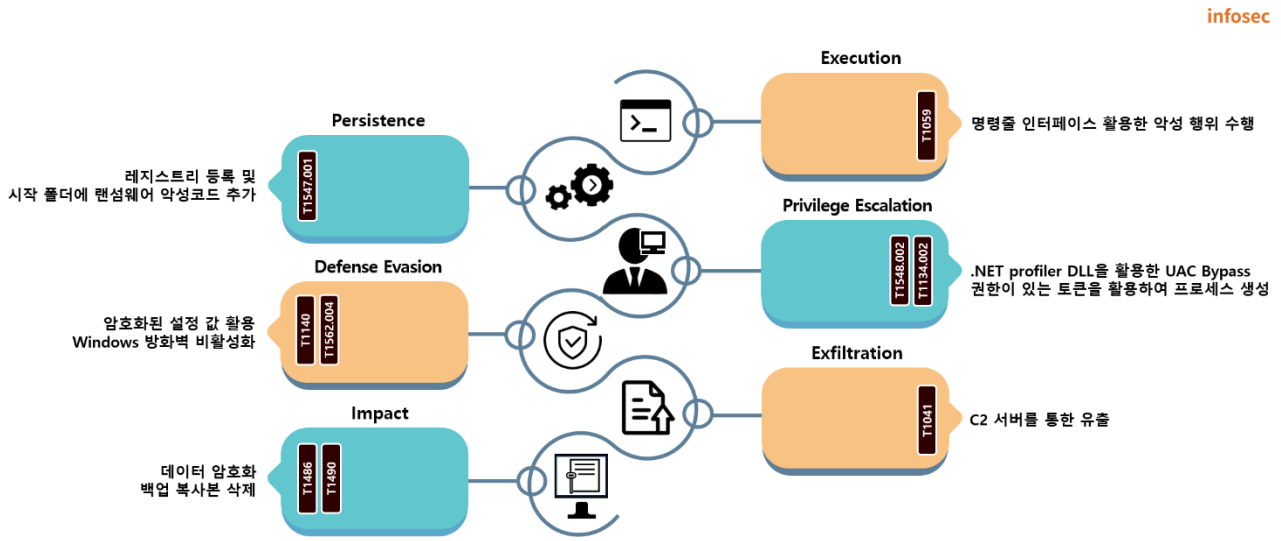


그림 9. 8Base 랜섬웨어 공격 전략

8Base 랜섬웨어 그룹은 랜섬웨어를 .NET 형태로 직접 배포하거나 다운로드형 악성코드인 SmokeLoader 를 이용해 배포한다. SmokeLoader 는 C2 서버로부터 암호화된 랜섬웨어 페이로드를 다운로드 받고 이를 복호화해 실행시키는 역할을 수행한다. .NET 기반의 랜섬웨어의 경우, 페이로드가 비트맵 파일 형태로 저장되어 있고 이를 복호화해 새로운 프로세스로 실행한다. 두 가지 유포 방식은 모두 동일한 Phobos 변종 랜섬웨어 페이로드를 실행시킨다.

최종적으로 실행되는 랜섬웨어 페이로드는 AES-256(CBC) 알고리즘으로 암호화된 설정 값이 ".cdata" 영역에 저장되어 있다. 설정 값에는 키 보호에 사용하는 RSA 공개키, 권한 상승이나 탐지 우회를 위해 필요한 명령어와 문자열, 암호화 예외 파일 및 폴더, 암호화 확장자와 같이 랜섬웨어 실행에 필요한 값들이 포함되어 있다. 8Base 는 하드코딩된 AES 키를 이용해서 설정 값이 필요할 때마다 복호화해서 사용한다.

8Base 랜섬웨어는 원활한 실행을 위해 재부팅 되더라도 랜섬웨어가 자동적으로 실행되도록 설정하며, 관리자 권한을 획득하고 방화벽을 비활성화 한다. 지속성 확보를 위해 현재 실행중인 랜섬웨어 파일을 시작 폴더 위치에 복제하며, 레지스트리 추가를 통해서 부팅 시 마다 랜섬웨어가 자동적으로 실행될 수 있도록 한다. 또한 관리자 권한을 가진 프로세스의 토큰을 복제해 랜섬웨어를 실행시키거나 .NET profiler DLL 로딩 프로세스[15]의 취약점을 이용해 관리자 권한 실행에 필요한 승인 과정을 우회하는 UAC(User Account Control)[16] Bypass with .NET profiler

[15] .NET profiler DLL 로딩 프로세스: 다른 애플리케이션의 실행을 모니터링하기 위한 도구인 .NET profiler DLL 을 불러오는 프로세스

[16] UAC(User Account Control): 관리자 권한이 필요한 경우, 실행 전 사용자에게 최종 동의를 요청하는 Windows 보안 기능

기법을 통해 관리자 권한을 획득 후 사용한다. 마지막으로 명령줄 인터페이스(Command-line Interface)[17]를 통해서 백업 복사본을 삭제하고 방화벽을 비활성화하는 기능도 지니고 있다.

파일 암호화는 대상 PC 의 드라이브뿐만 아니라 네트워크 공유 폴더도 암호화한다. 파일 암호화는 AES-256(CBC) 알고리즘을 이용하며, 암호화에 사용되는 AES 키는 암호화 스레드 생성 이전에 랜덤하게 생성한다. 각 파일마다 다른 키를 사용하는 것이 아니기 때문에 IV(Initialization Vector)[18]를 파일마다 랜덤하게 생성해 키 중복 문제를 해결했다. 암호화에 사용된 AES 키와 IV 는 설정 값에 저장되어 있는 RSA 공개키를 통해서 보호되며, 암호화된 파일의 끝에 추가된다.

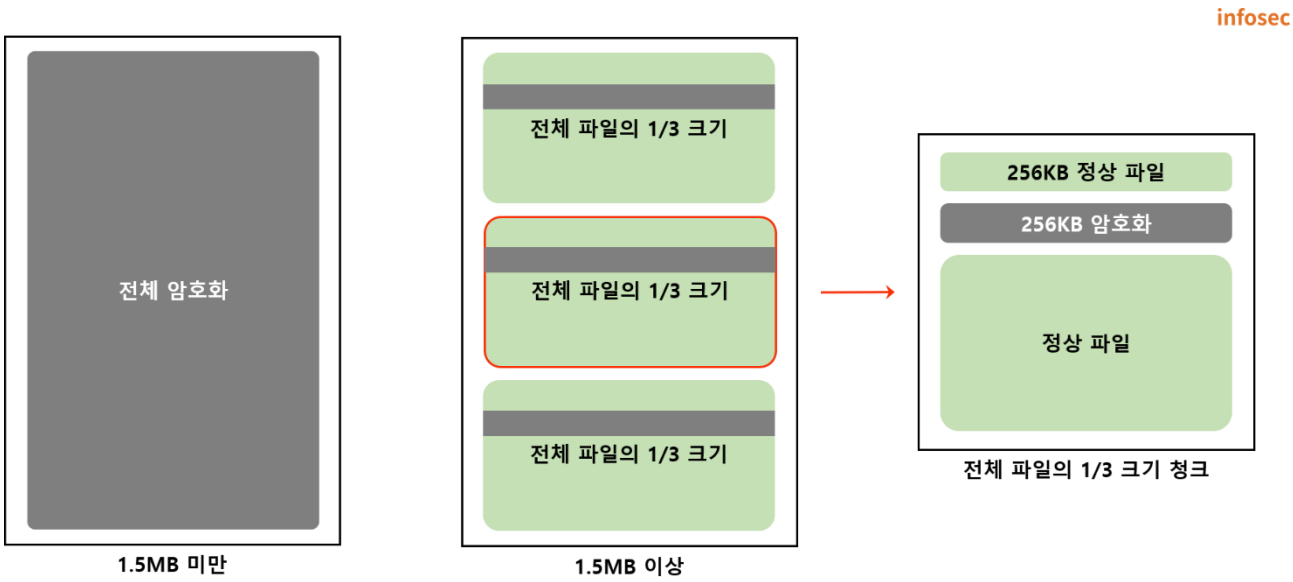


그림 10. 8Base 랜섬웨어 암호화 방식

8Base 랜섬웨어는 효율적인 암호화를 위해서 멀티스레드 뿐만 아니라 부분 암호화 방식을 사용한다. 파일 크기가 1.5MB 미만인 경우 파일 전체를 암호화하고, 1.5MB 이상인 경우에는 파일을 같은 크기로 3 등분해 각 영역마다 256KB 만 암호화한다.

[17] 명령줄 인터페이스(Command-line Interface): 컴퓨터의 운영체제와 상호 작용하는 명령을 입력할 수 있는 텍스트 기반 인터페이스

[18] IV(Initialization Vector): 블록 암호화 방식에서 사용되는 매개변수 중 하나로 암호화 결과가 패턴을 가지지 않도록 하기 위해 사용함

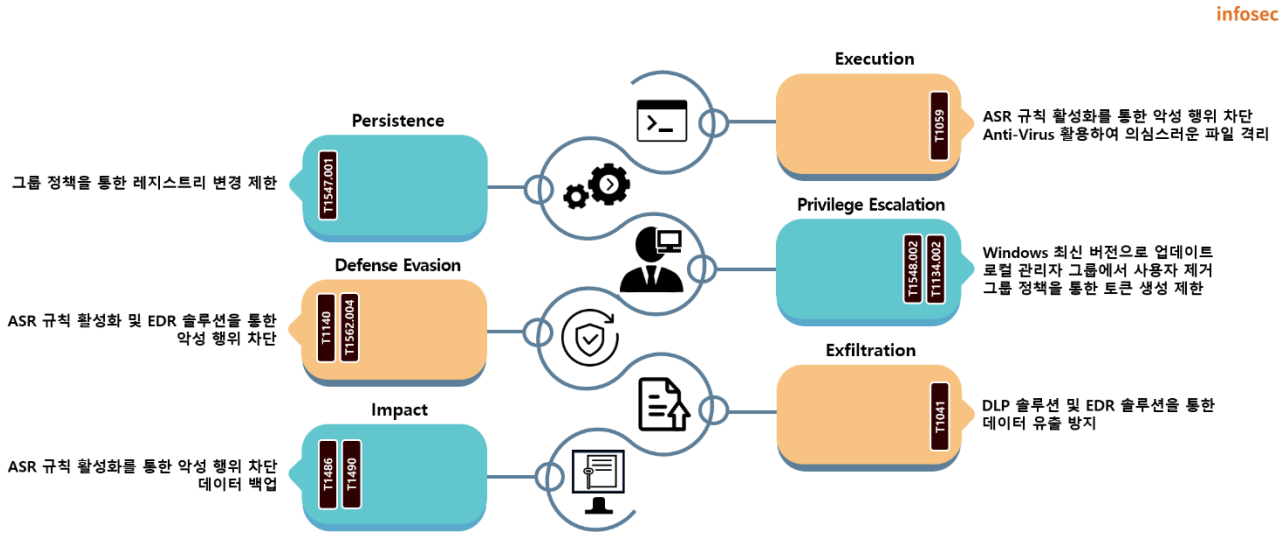


그림 11. 8Base 랜섬웨어 대응방안

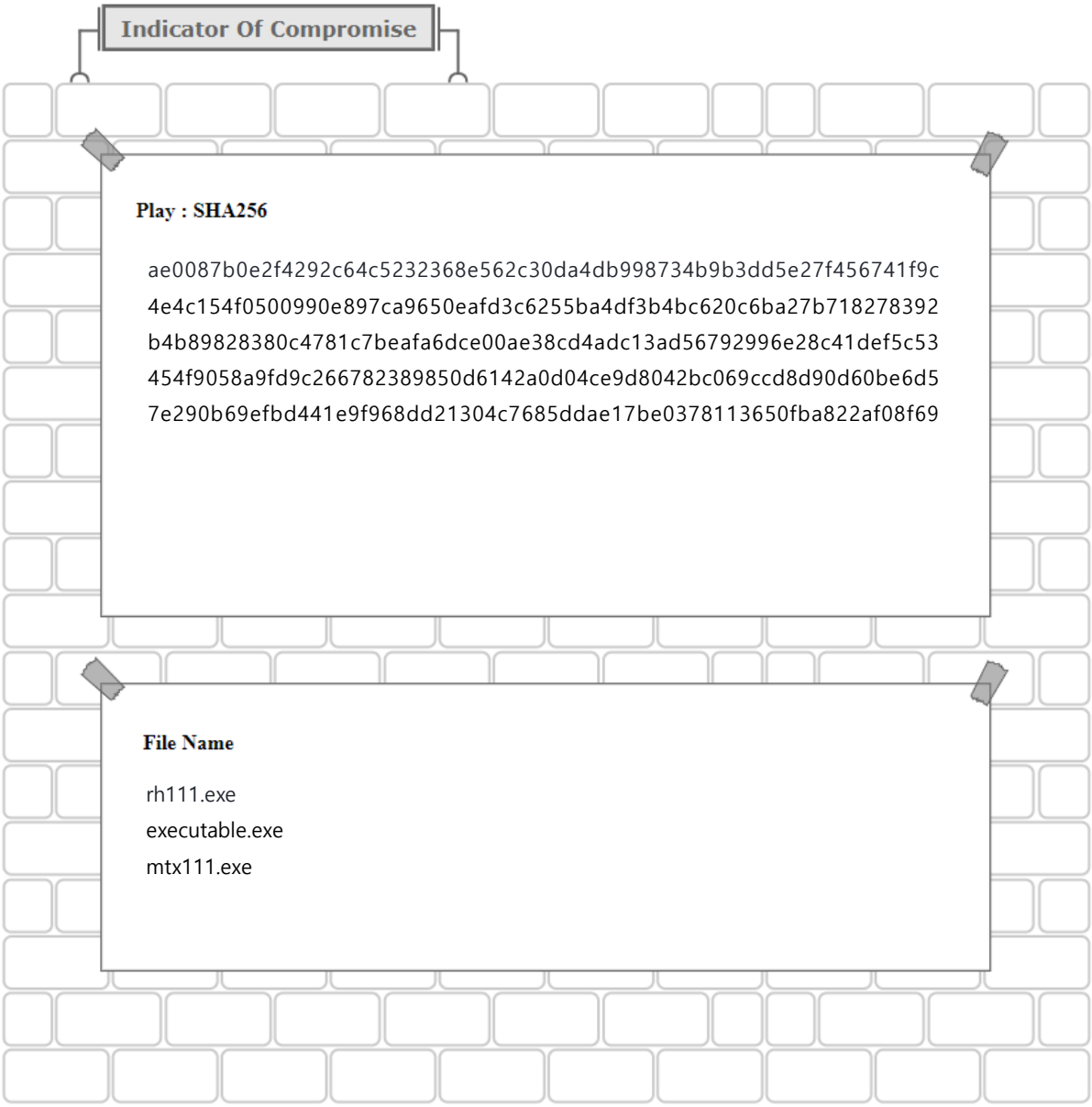
8Base 의 .NET 기반 랜섬웨어는 페이로드를 메모리상에서 복호화해 새로운 프로세스로 실행하며, SmokeLoader 변종은 C2 에서 페이로드를 다운 받거나 SmokeLoader 내부에 저장된 페이로드를 복호화해 새로운 프로세스로 실행하는 방식을 사용하고 있다. 따라서 ASR(Attack Surface Reduction)[19] 규칙 활성화를 통해 악성 콘텐츠가 새로운 프로세스를 통해서 실행되는 것을 방지할 수 있다. 또한 의심스러운 파일을 다운로드 하거나 복제하더라도 실행시킬 수 없도록 Anti-Virus 를 활용해 격리해야 한다.

8Base 랜섬웨어는 지속적인 실행을 위해 랜섬웨어 파일을 시작 폴더에 복사하고 레지스트리에 등록해 부팅 시 자동으로 실행되도록 한다. 따라서, 관리자 계정을 제외한 사용자의 레지스트리 편집을 제한하는 방식으로 Windows 그룹 정책을 수정해 지속성을 확보하지 못하도록 할 수 있다.

파일의 암호화나 백업 데이터 삭제와 같은 기능을 수행하기 위해선 관리자 권한이 필요하다. 이를 위해 8Base 랜섬웨어는 UAC Bypass 기법을 활용하거나 권한이 있는 프로세스의 토큰을 복제해 사용한다. Windows 운영체제를 우회 기법이 패치된 버전으로 업데이트하거나, 그룹 정책 수정을 통해 사용자가 다른 프로세스의 토큰을 복제하거나 생성할 수 없도록 해야 한다.

[19] ASR(Attack Surface Reduction): 악성 코드의 공격 경로를 차단하는 기술

또한 8Base 랜섬웨어에는 방화벽을 비활성화 하거나 백업 데이터를 삭제하는 명령어들이 암호화된 채로 저장돼 있다. 해커들은 필요 시, 해당 명령어들을 복호화해서 사용하기 때문에 ASR 규칙 활성화, EDR(Endpoint Detection and Response)[20] 솔루션 등을 사용해 악성 행위를 사전에 차단해야 한다. 이외에도 DLP(Data Loss Prevention)[21] 솔루션이나 EDR 솔루션을 활용해 데이터 유출을 방지할 수 있으며, 별도의 네트워크나 저장소에 데이터를 소산 백업해 관리함으로써 파일 암호화와 NAS 혹은 백업 저장소의 데이터 삭제를 대처할 수 있다.



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

[21] DLP(Data Loss Prevention): 데이터의 흐름을 감시해 중요 정보 유출을 감시/차단하는 데이터 유출 방지 솔루션

■ 참고 사이트

• 영국 레스터 시의회(https://news.leicester.gov.uk/news-articles/2024/april/cyber-incident-update-3-april-2024/)

• 영국 레스터 시의회(https://news.leicester.gov.uk/news-articles/2024/april/more-data-published-following-leicester-cyber-attack/)

• CISA 보안 권고문(https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060a)

• BleepingComputer 공식 홈페이지 (https://www.bleepingcomputer.com/news/security/hellokitty-ransomware-rebrands-releases-cd-projekt-and-cisco-data/#google_vignette)

• BleepingComputer 공식 홈페이지 (https://www.bleepingcomputer.com/news/security/8base-ransomware-gang-escalates-double-extortion-attacks-in-june/)

• Cyble Research & Intelligence Labs (https://cyble.com/blog/lockbit-blacks-legacy-unraveling-the-dragonforce-ransomware-connection/)

• SOCRadar 공식 홈페이지 (https://socradar.io/dark-web-profile-8base-ransomware/)

• Cyberint 공식 홈페이지 (https://cyberint.com/blog/research/all-about-that-8base-ransomware-group-the-details/)

• DarkReading 뉴스레터 (https://www.darkreading.com/threat-intelligence/sexi-ransomware-desires-vmware-hypervisors)

• Trend Micro 공식 홈페이지 (https://www.trendmicro.com/vinfo/tr/security/news/ransomware-spotlight/ransomware-spotlight-8base)

• 미국 에너지 및 상업 위원회 (https://energycommerce.house.gov/events/oversight-and-investigations-subcommittee-hearing-examining-the-change-healthcare-cyberattack)