Keep up with Ransomware

랜섬웨어 판매를 개시한 핵티비스트 CyberVolk

■ 개요

2024 년 9 월 랜섬웨어 피해 사례는 지난 8 월(464 건)에 비해 약 13% 감소한 406 건을 기록했다. 소폭 감소했지만, 9 월에도 여전히 국내 피해 사례가 다수 확인됐다.

9 월 초, LockBit 랜섬웨어는 국내 타이어 제조 회사를 공격해 공장 가동을 중단시켰다. 이들은 다크웹 유출 사이트에 재무제표와 계산서 등을 샘플 데이터로 업로드했고, 10 월에는 탈취한 모든 데이터를 공개한다며 추가 협박하고 있다.

다크웹, 텔레그램, 해킹 포럼에서 국내 데이터 판매 글과 데이터 공개 협박 글이 확인됐다. 해커 그룹 CyberNiggers 에서 활동하는 IntelBroker 는 해킹 포럼 BreachForums 에 국내 바이오테크 스타트업 기업 데이터를 유출했다. 공개된 데이터는 Admin 페이지 코드와 각종 서버 및 데이터베이스 코드가 포함되어 있다.

텔레그램에서 활동하는 인도네시아 해커 그룹 Anon Black Flag(Palu Anon Cyber)는 인도네시아 내 한국 노동자들이 인도네시아와 이슬람에 대한 인종 차별을 저질렀다고 주장하며, 한국 경찰청과 외교부 데이터를 공개했다. 하지만 해당 데이터는 실제 유출 데이터가 아닌 공공데이터 포털의 공개 자료인 것으로 확인됐다.

9 월에는 여러 해커 그룹의 활동 재개, 리브랜딩 소식이 다수 확인됐다. 9 월 24 일, 지난 8 월 국내 DevOps 기업을 공격한 El dorado 랜섬웨어 그룹이 BlackLock 으로 그룹명을 변경했다. 5 월에 처음 등장한 Arcus 랜섬웨어 그룹은 7 월부터 활동을 중단했다가 9 월에 재개했다. Arcus 랜섬웨어 그룹은 다크웹 유출 사이트 공지를 통해 활동의 중단은 내부 인프라 재구성 때문이었다고 밝히며, 계열사 모집 기준과 방식을 추가 공지하며 활발한 활동을 예고했다. 신규 그룹 InvaderX 는 본격적인 활동을 위해 러시아 해킹 포럼 RAMP 에서 파트너 모집 글을 업로드했다. 이들은 모집 글에서 CIS[1], BRICs[2]는 공격 대상에서 제외하고 Windows, ESXi[3]

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

[2] BRICs: 브라질, 러시아, 인도, 중국을 일컫는 약칭

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

버전의 랜섬웨어를 공격에 사용할 뿐만 아니라 DDoS 공격[4]도 가능하다고 밝혔다.

Akira 그룹은 랜섬웨어 공격에 네트워크 보안 운영체제의 최신 취약점을 악용한 것으로 드러났다. 취약점은 미국 네트워크 보안 회사 SonicWall 의 네트워크 보안 운영체제 SonicOS 에서 발생한 취약점 CVE-2024-40766 이다. 이를 악용하면 네트워크 자원에 무단 접근이 가능하고, 방화벽 충돌을 발생시켜 네트워크 보호 기능을 무력화시킬 수 있다. 해당 취약점은 8 월 22 일 패치됐지만, 최근 Akira 랜섬웨어 그룹이 SonicWall 네트워크 장치의 계정을 손상시키고 무단으로 네트워크에 접근한 정황이 발견됐다.

최근 BianLian, Rhysida 랜섬웨어 그룹이 Microsoft 의 클라우드 서비스인 Azure 의 데이터 전송 도구들을 활용해 대규모 데이터를 유출한 것으로 확인됐다. 사용한 도구는 Azure 용 그래픽 관리 도구인 Azure Storage Explorer 와 명령줄 유틸리티 AzCopy 다. 탈취한 데이터를 컨테이너에 업로드하고, 두 도구를 활용해 다른 저장소로 쉽게 전송하는 식이다. 자체적으로 제작한 데이터 탈취 도구와 달리 Azure 는 기업에서 많이 사용하는 정상적인 솔루션으로, 탐지 회피를 위해 악용된 사례다.

사이버 범죄 조직들은 암호화된 메시지를 전송하는 메신저 텔레그램을 주로 활용하고 있다. 메시지 암호화로 대화 내용이 노출되지 않으며 IP 와 연락처 등 사용자의 개인정보를 공개하지 않는다는 점 때문에 범죄에 주로 활용되기도 한다. 하지만 9 월 24 일 텔레그램 개인정보 보호 정책이 업데이트됨에 따라, 범죄에 연루되거나 서비스 약관을 어기는 경우 IP 와 계정에 연동된 전화번호를 법 집행 기관에 제공하게 됐다. 따라서 텔레그램에서 주로 활동하는 사이버 범죄 조직들은 텔레그램 활동을 중단하거나 다른 플랫폼으로 옮길 준비를 하는 등 여러 움직임이 포착되고 있다.

[4] DDoS 공격: 시스템을 악의적으로 공격해 기능을 저하하거나 작동을 중단시키는 공격 방식

■ 랜섬웨어 뉴스

infosec

LockBit 그룹 국내 타이어 제조 회사 랜섬웨어 공격

- 9월 초 랜섬웨어 공격으로 인해 국내 공장 가동 중단
- 9월 25일 다크웹 유출 사이트에 샘플 데이터와 함께 전체 데이터 공개 협박글 게시
- 공개된 샘플 데이터에는 재무제표와 계산서 등 내부 문서가 포함

IntelBroker, 국내 바이오텍 스타트업 데이터 공개

- 해킹 포럼 BreachForums에 데이터 업로드
- Admin 페이지 코드와 각종 서버 및 데이터베이스 코드 포함

인도네시아 해커 그룹 Anon Black Flag 경찰청 및 외교부 데이터 공개

- 인도네시아에서 일하는 한국 노동자가 인도네시아 및 이슬람에 대해 인종 차별을 저질렀다고 주장하며 데이터 공개
- 공개한 데이터는 확인 결과 공공 데이터 포털에서 구할 수 있는 공개 자료로 밝혀짐

Arcus 그룹 2달만에 활동 재개

- 내부 인프라 재정비를 목적으로 2달간 활동을 중단했으며 9월부터 활동을 재개하고 신규 계열사도 모집 시작
- 기존 계열사의 초대로 계열사 신규 가입이 가능하며, 보증금 지불 후 일정 수익을 달성하면 최종적으로 합류하는 방식

El Dorado 그룹 BlackLock으로 리브랜딩

- El Dorado 랜섬웨어 그룹은 8월 국내 기업을 공격한 이력 존재
- 9월 24일 그룹명을 BlackLock으로 변경하고, 새로운 피해자를 게시하며 다크웹 유출 사이트 디자인도 변경

그림 1. 랜섬웨어 동향

■ 랜섬웨어 위협

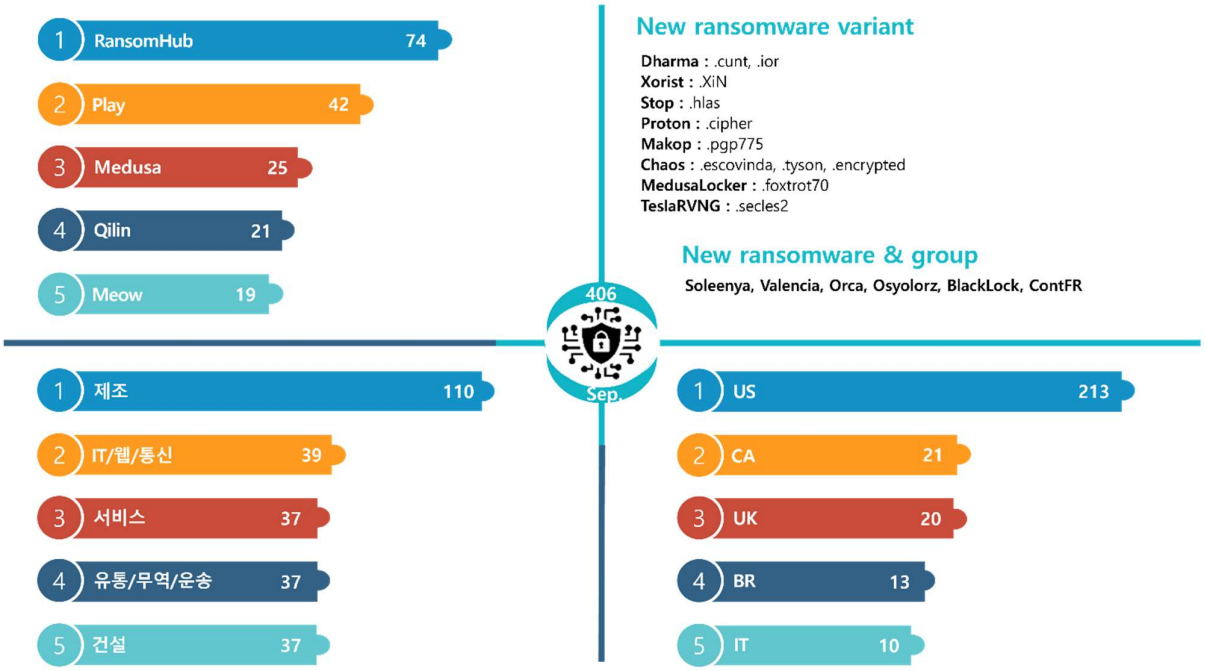


그림 2. 2024 년 9 월 랜섬웨어 위협 현황

새로운 위협

9 월에는 지난달에 비해 새로운 위협이 증가했다. 기존에 활동하던 El Dorado 그룹이 BlackLock 이라는 이름으로 리브랜딩 했고, 그 외에도 신규 랜섬웨어 그룹이 다수 발견됐다. 9 월 10 일, Valencia 그룹이 등장해 총 5 건의 피해자를 게시했다. 9 월 16 일에는 Orca 랜섬웨어 그룹이 등장해 터키와 중국의 제조업체 2 건을 피해자로 게시했다. 이후 별다른 활동이 확인되지 않았고, 9 월 25 일부터는 다크웹 유출 페이지에 접속할 수 없는 상태다.

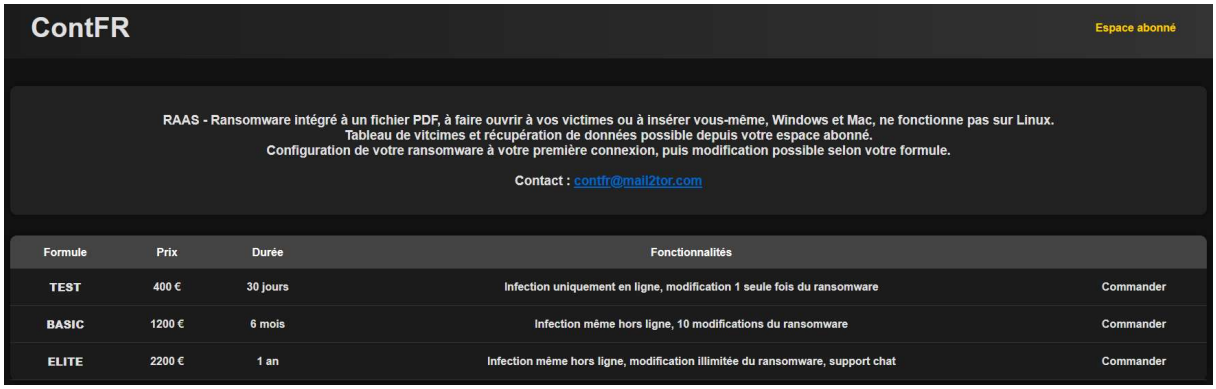


그림 3. ContFR RaaS

랜섬웨어를 서비스 형태로 판매하는 신규 RaaS 가 발견됐다. ContFR 그룹은 PDF 를 통해 전파하는 Windows, MacOS 랜섬웨어를 기능까지 구분해서 판매하고 있다. Windows, Linux 버전에 비해 상대적으로 드물게 나타나는 MacOS 버전의 랜섬웨어를 사용한다는 특징이 있다. 다만, 랜섬웨어 서비스의 진위 여부는 확인되지 않았다. 판매하는 서비스는 총 3 개다. TEST 버전은 30 일 동안 사용, 1 회 수정이 가능한 랜섬웨어로 400 유로(한화 약 58 만 원)에

판매하고 있다. BASIC 버전은 6 개월 동안 사용, 10 개의 랜섬웨어 변종과 오프라인에서도 동작하는 기능이 추가됐고, 1,200 유로(한화 약 175 만 원)에 판매하고 있다. ELITE 버전은 1 년 동안 사용, 변종을 무제한으로 만들 수 있고 채팅 지원 기능이 추가된 서비스로 2,200 유로(한화 약 320 만 원)에 판매하고 있다.

Service	Price
Basic Doxing (gain personal data, find information, using publicly avaiable sources)	700 USD
Special Doxing (More than basic dox, searches non-publicly accessible records and leaked databases.)	1500 USD
Ultimate Doxing (Access to goverment services and banks for latest info about victim.)	4500 USD
Takedown from social media(Make someone profiles disappear permanently.)	Tiktok, baido, wechat, aliexpress, Temu: 900 USD Dating apps(Tinder, Badoo): 2500 USD Meta Profiles(Facebook, Instagram): 4000 USD Google(YouTube, Blogger, gmap business): 6500 USD Message apps(Telegram, Whatsapp): 7000 USD
Gain access(Hack into account)	Social media - 2x price of takedown. Email accounts(No 2-FA, smtp, pop3) 4000 USD Email accounts(2-FA, gmail, proton) 15 000 USD Banks, GOV - 25 000 USD+
Special custom requests. (Bank accounts, credit data - and change credit score, health insurances, forbid/edit gov licenses/IDs/passports - disable flights, add driving license in database, remove penalty points, clear criminal records; Digital citizenship abroad)	15 000 USD+
Express fee (Priority queue)	2x price.
Company pentesting, OPsec, Attack tests, safety audit	2000 USD (Per single infrastructure - single network entry point)
Coaching, security measure training, social-technic training	150 USD/hr (online, unlimited attendees, you can record it)

- Basic prices are in Monero, For payments in Bitcoin, Litecoin, Ethereum, or other top-50 coins, include fee of +8% for conversion fees.
- We only take crypto payments. No PayPal, no Bank cards or transfers. This is for your own safety.
- Normal queue takes about two weeks to find all info, basic public info is reported at next work day.
- We support entire world, but some services are not avaiable in russia, korea, japan, india and china because they keep paper records alongside digital ones.

그림 4. Osyolorz Collective 다크웹 페이지

Osyolorz Collective 라는 신규 조직도 발견됐다. 자신들을 사이버 테러리스트라고 소개하고, 유럽과 관련된 15 개 주요 국가 대상으로 정부 기관, 금융 기관 등의 민감 데이터를 공개하는 것이 목적이라고 밝혔다. 호주, 벨기에, 체코, 덴마크, 핀란드, 프랑스, 독일, 그리스, 아일랜드, 이탈리아, 룩셈부르크, 네덜란드, 폴란드, 스페인, 스웨덴이 포함되어 있다. 피싱 메일 등 사회공학 기법은 물론, 취약점 활용과 자체적으로 제작한 악성 코드를 활용해 데이터를 탈취한다고 주장한다. 또한 Doxing[5], SNS 계정 삭제, 접근 권한 획득, 금융 정보 탈취, 침투 테스트 등 각종 서비스도 판매 중이고, 홈페이지에 서비스별 금액도 기재되어 있다.

[5] Doxing: 특정 인물의 이름, 주소, 전화번호와 같은 신상 정보를 해킹해 온라인에 공개하는 행위

Top5 랜섬웨어

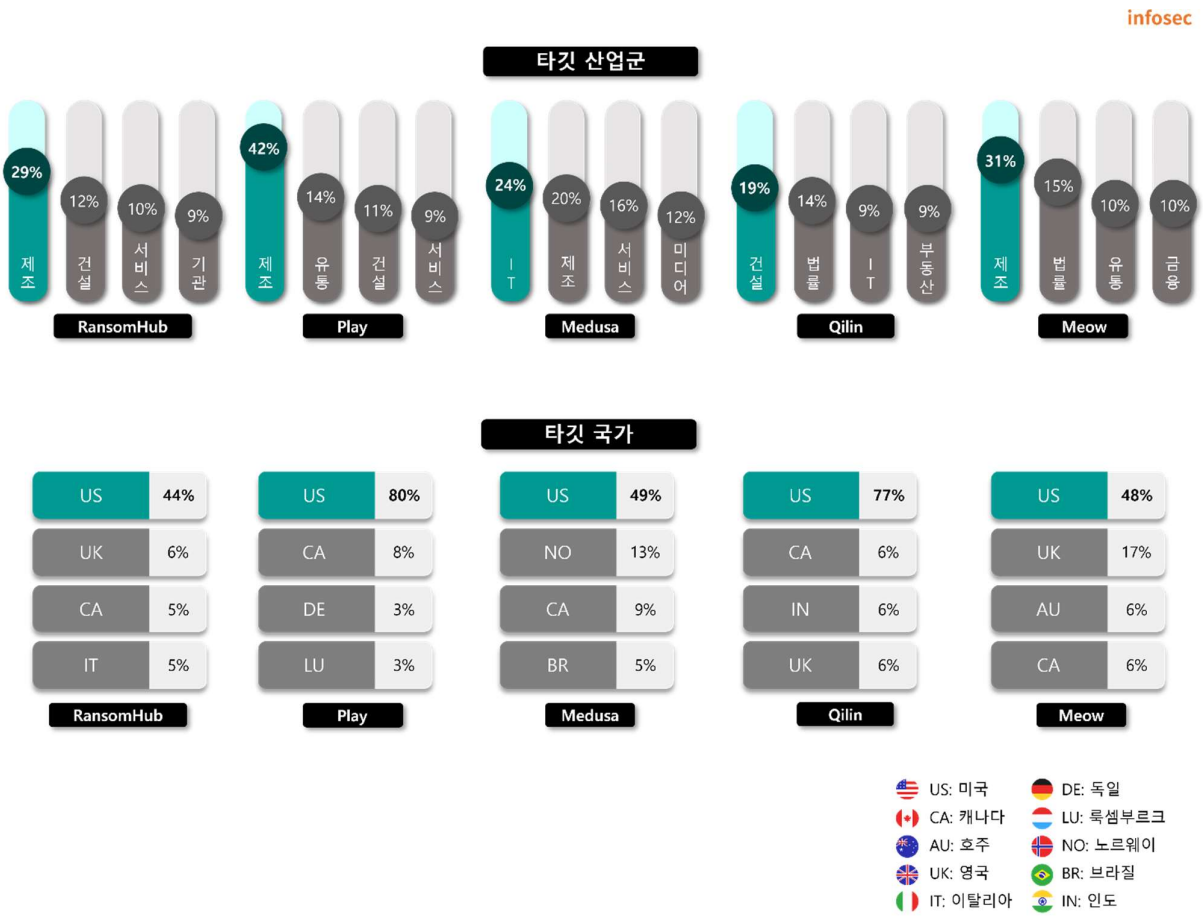


그림 5. 산업/국가별 주요 랜섬웨어 공격 현황

RansomHub 그룹은 9 월 전체 랜섬웨어 피해자의 19%에 해당하는 피해자를 게시했다. 최근 RansomHub 는 EDR[6] 솔루션을 비활성화하기 위해 러시아 보안회사 Kaspersky 의 루트킷[7] 및 부트킷[8] 탐지 도구인 TDSSKiller 를 사용한 정황이 발견됐다. 유효한 인증서로 서명된 합법적인 도구이기 때문에 악성 행위가 탐지될 가능성이 작다는 점을 이용했고, 특정 서비스를 제거하는 명령어 "-dcsvc"를 이용해 보안 솔루션 서비스를 비활성화했다. 합법적인 도구를 활용해 보안 서비스를 비활성화할 수 없도록 EDR 솔루션에서 변조 방지 기능을 활용하거나 "-dcsvc" 플래그 사용을 모니터링하는 등 적절한 조치가 필요하다.

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

[7] 루트킷 (Rootkits): 접근 권한이 없는 사용자가 권한을 획득할 수 있도록 하는 악성코드

[8] 부트킷 (Bootkits): 운영체제의 부팅에 사용하는 영역을 훼손해 정상적으로 부팅되지 못하도록 하는 악성코드

Play 그룹은 미국 소재의 기업을 집중적으로 공격하는 모습을 보인다. 9 월에는 미국 도소매 공급 업체 협동조합 Piggly Wiggly Alabama Distributing Company 의 예산 세부 정보, 급여 기록, 고객 문서 및 재무 정보 등을 포함한 103GB 크기의 데이터를 탈취했다고 주장했고, 9 월 15 일 모든 데이터를 공개했다. 해당 기업은 지난 2022 년 5 월에도 BlackBasta 그룹에 의해 탈취된 데이터가 공개된 적 있다.

Medusa 그룹은 9 월 17 일 다국적 계약 식품 서비스 회사인 Compass Group 의 호주 지사를 공격해 약 800GB 에 달하는 데이터를 탈취했다. 함께 공개된 샘플 데이터에 따르면, 직원 신분증, 여권 사본, 운전 면허증, 메일 등 개인정보는 물론 급여 명세서 등 내부 문서도 다수 포함되어 있다. Medusa 그룹은 Compass Group 의 보안 담당자가 몸값을 지불하지 않고, 보안 솔루션을 사용해 접근하지 못하게 시도했다는 이유로 9 월 19 일 2 차 공격을 통해 추가 데이터를 공개했다.

Qilin 그룹은 9 월에 미국 디트로이트 지역의 비상업적 공영 방송을 제공하는 Detroit PBS 를 공격해 약 600GB 에 달하는 데이터를 탈취했다. 현재 샘플 데이터만 공개됐는데 계산서, 미수금 보고서와 같은 금융 데이터와 내부 문서가 포함되어 있다.

Meow 그룹은 이스라엘 국방군(IDF)과 이스라엘 정보기관 모사드(Mossad)의 데이터를 탈취해 게시했다. 군인 및 정보 요원의 여권 사본, 개인 정보, 군 내부 문서 등이 포함된 데이터를 2 만 달러(한화 약 2,600 만 원)에 판매하고 있다.

■ 랜섬웨어 집중 포커스

그림 6. CyberVolk 그룹 공격 페이지

CyberVolk 그룹은 올해 3 월 GLORIAMIST INDIA 라는 이름으로 먼저 텔레그램에서 활동을 시작했다. 동일한 이름을 가진 GLORIAMIST 라는 핵티비스트 그룹이 작년 12 월부터 텔레그램을 통해 활동했는데, 파트너로서 활동을 시작한 것으로 알려졌다. 팔레스타인을 지지하는 GLORIAMIST INDIA 는 정치적으로 연관된 국가의 기업을 대상으로 주로 DDoS 공격을 감행하는 모습을 보였다.

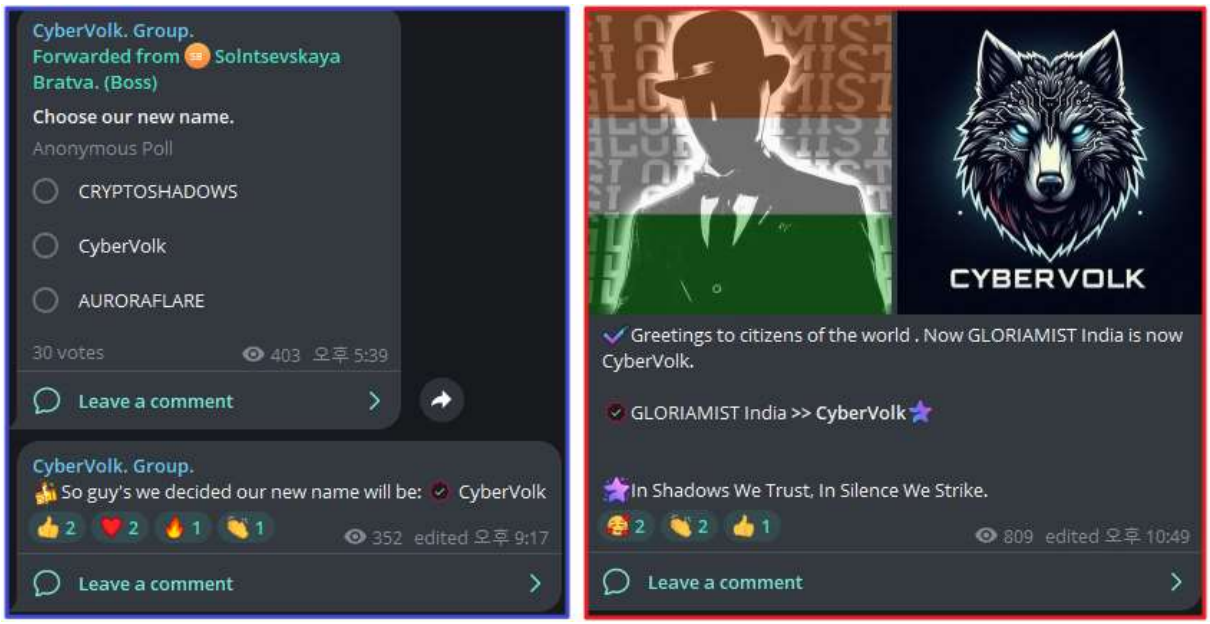


그림 7. CyberVolk 그룹 이름 투표(좌) 및 그룹 이름 변경(우)

6 월 초, GLORIAMIST 의 설립자 DeathHack(Patcher)이 체포되었을 수도 있다는 텔레그램 메시지가 게시됐고, GLORIAMIST 와 GLORIAMIST INDIA 는 6 월 6 일부터 활동을 중단했다. 17 일 뒤 재개에 나선 GLORIAMIST INDIA 는 새로운 그룹명을 위해 투표를 실시했다. 해당 투표를 통해 CyberVolk 라는 이름이 채택됐다. 여전히 팔레스타인을 지지하는 CyberVolk 는 DDoS 공격을 중점적으로 기존의 핵티비스트 활동을 이어 나가고 있다.

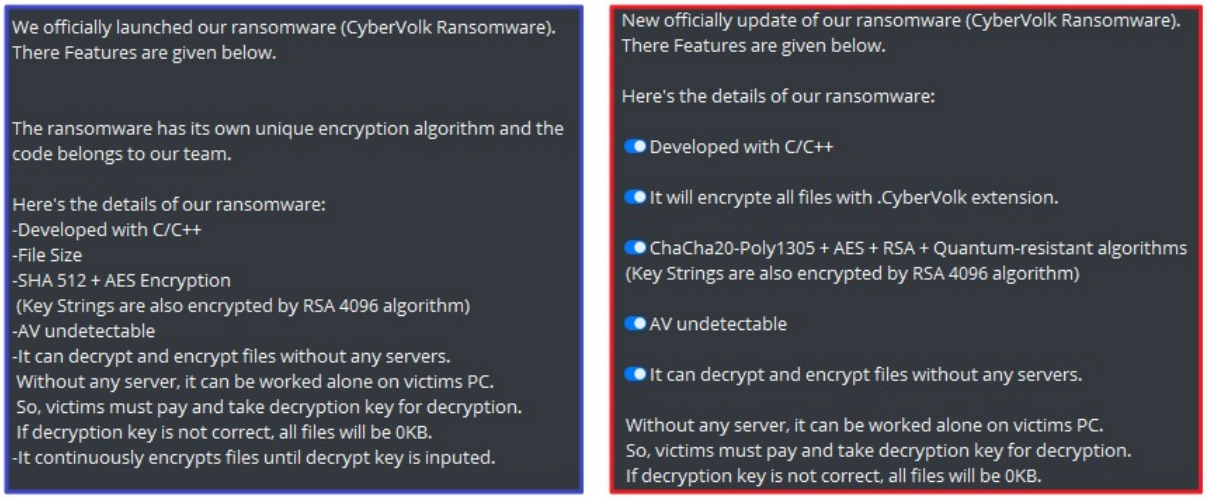


그림 8. CyberVolk 랜섬웨어 판매 글(좌: 초기 버전, 우: 최신 버전)

7 월 1 일부터 텔레그램에서 랜섬웨어 판매도 시작했다. 초기 버전 판매 시작 9 일 뒤인 10 일부터는 암호화 알고리즘과 확장자를 변경한 최신 버전을 판매했다. 최신 버전에서는 랜섬웨어에 양자 저항 알고리즘[9]을 사용하기 시작했는데, CyberVolk 그룹은 이 때문에 파일을 임의로 복구하는 것이 불가능하고, 올바른 키가 입력되지 않을 경우(키에 대한 유효성 검증 없이 36 자가 입력되지 않으면) 모든 파일이 0KB 로 변할 것이라고 밝혔다.

9 월 23 일, 정보 탈취 도구인 CyberVolk StealerV1 을 판매하기 시작했다. 해당 Stealer 는 스팀, 디스코드 등 소프트웨어 정보, 브라우저 데이터, 암호 화폐 지갑 정보는 물론 시스템 정보 탈취 기능까지 보유하고 있다. 해당 악성코드는 소스코드 형태로 1,000 달러(한화 약 130 만 원)에 판매되고 있다.

[9] 양자 저항 알고리즘: 기존 컴퓨터 보다 연산 속도가 훨씬 빠른 양자 컴퓨터로도 키 없이 해독하기 어려운 암호화 알고리즘

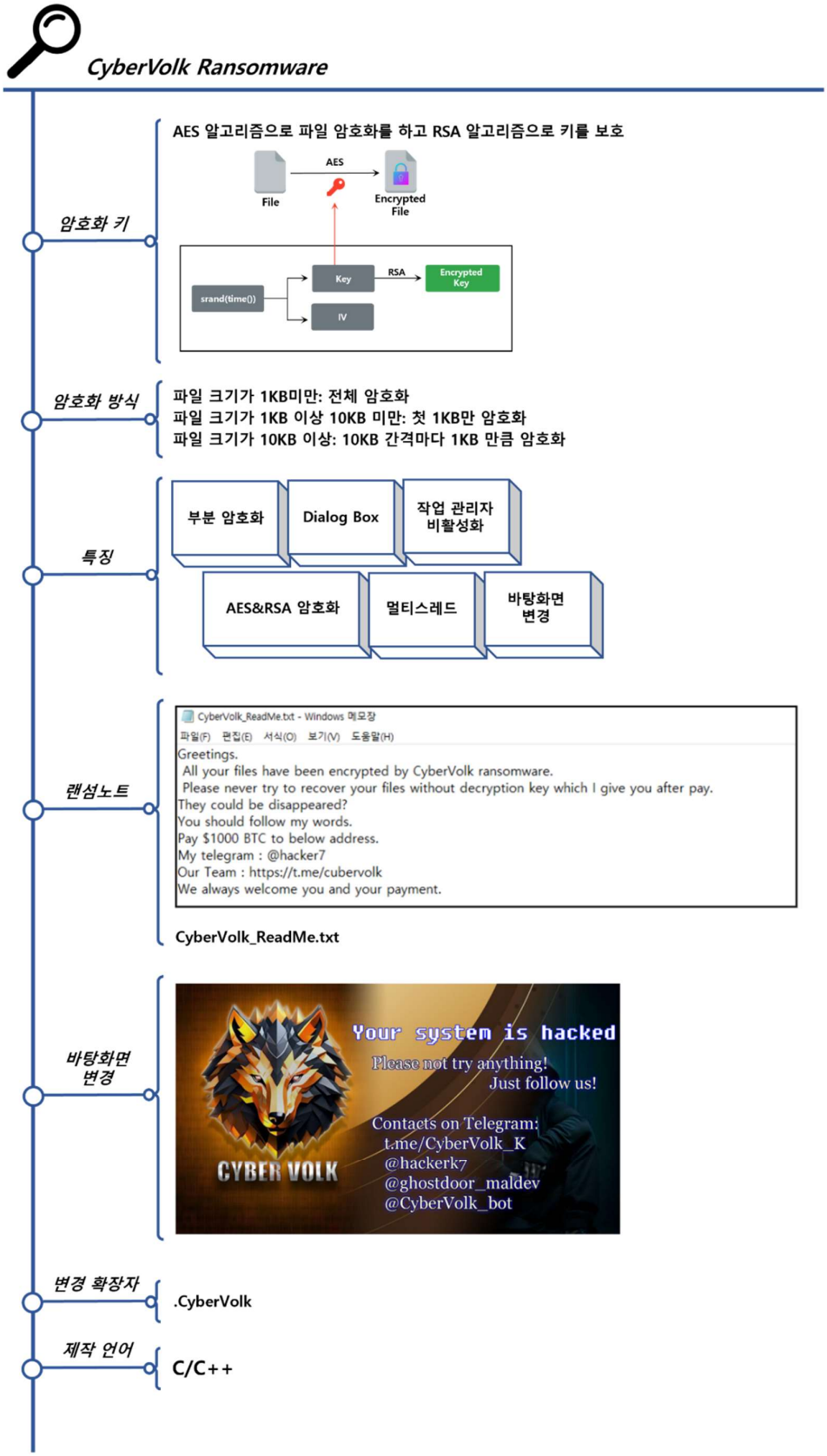


그림 9. CyberVolk 랜섬웨어 개요

CyberVolk 랜섬웨어 전략

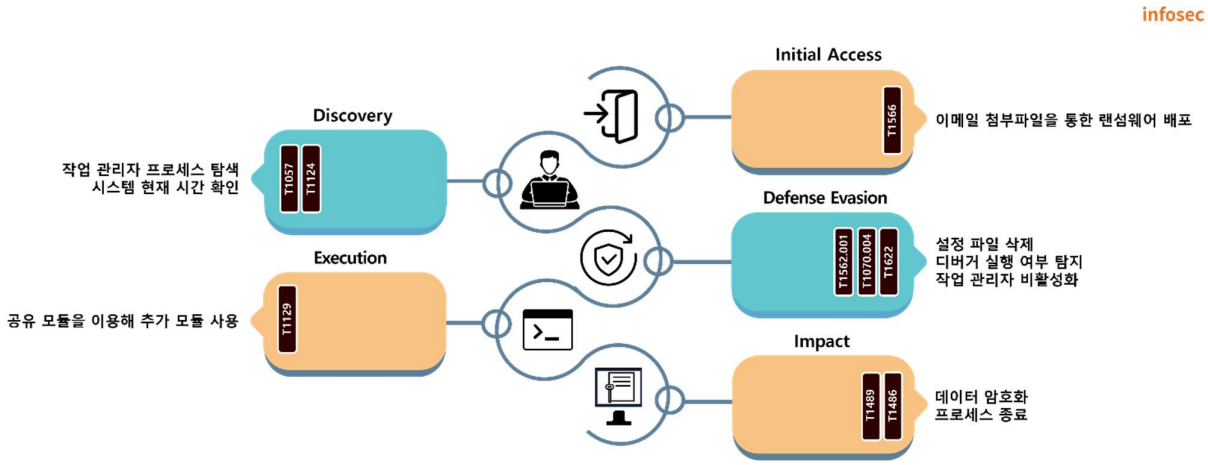


그림 10. CyberVolk 랜섬웨어 공격 전략

CyberVolk 랜섬웨어는 하드코딩된 비트맵 파일을 이용해 바탕화면 변경부터 진행한다. 시스템에 설정된 환경변수로 임시 폴더의 경로를 확인하고, 해당 경로에 "tmp.bmp"라는 이름의 비트맵 파일을 저장한다. 사용하는 비트맵 파일은 아래 그림과 같다.

그림 11. 임시 폴더에 저장된 비트맵 파일(tmp.bmp)

바탕화면을 변경한 뒤 사용자가 상호작용을 할 수 있는 Windows 팝업 창 Dialog Box 를 생성한다. 팝업 창에는 CyberVolk 그룹에 대한 소개, 연락처, 암호화폐 지갑 주소를 첨부해 사용자에게 1,000 달러(한화 약 130 만 원)를 송금하도록 요구한다. 또, 복호화 키를 입력할 수 있는 텍스트박스가 존재하고, 5 시간 카운트다운 타이머를 표기해 압박감을 느끼도록 만든다.

그림 12. CyberVolk Dialog Box

팝업 창에 표기된 남은 시간은 %APPDATA%[10] 경로에 time.dat 이라는 이름으로 저장해 사용된다. 랜섬웨어가 실행되면 해당 파일에 18000 이라는 값을 저장하고, 1 초마다 해당 파일값을 1 씩 줄여가면서 시간을 표기하는 방식이다. 따라서 해당 파일을 수정하면 남은 시간도 수정된다. 다만, 시간이 지나더라도 랜섬웨어가 종료되거나 시스템이 다운되는 등 별다른 영향은 없는 것으로 확인됐다.

그림 13. 남은 시간 임의 변경

또, 사용자가 랜섬웨어를 중단하지 못하도록 1 초마다 작업 관리자 프로세스가 실행 중인지 체크해 강제 종료시킨다. 다만, CyberVolk 랜섬웨어는 자체적인 지속성 확보 수단이 존재하지

[10] %APPDATA% : Windows 시스템에서 사용자 전용 데이터를 동기화 하기 위한 폴더를 가리키는 시스템 환경변수. 일반적으로 "C:\Users\{사용자명}\AppData\Roaming"으로 설정되어 있다.

않기 때문에 PowerShell 명령어나 PC 를 강제로 종료하면 랜섬웨어 실행을 중단할 수 있다.

팝업 창의 시간이 흐르는 동안 CyberVolk 랜섬웨어는 파일 암호화를 준비한다. 모든 드라이브를 탐색하며 이동식 디스크와 하드 디스크에 존재하는 루트 디렉토리부터 암호화 대상을 탐색하기 시작한다. 각 드라이브의 최상위 디렉토리에서 Users 디렉토리가 존재하는지 확인하고, 해당 Users 하위 디렉토리만 암호화를 진행한다.

```
      wsprintfW(String2, L"%c:\\%s\\", v15, L"Users");// C:\\Users
      if ( wcsncmp(v9, String2, wcslen(String2)) )
      {
        recursive_search_directories(String2, a2);
        return;
      }
      if ( (GetFileAttributesW(v9) & 2) == 0 )
      {
LABEL_16:
        wsprintfW(FileName, L"%s*.*", v9);
        FirstFileW = FindFirstFileW(FileName, &FindFileData);// C:\Users\*.*
        lpFileName = FirstFileW;
```

그림 14. Users 디렉토리 확인

Users 의 하위 디렉토리에서는 모든 폴더 및 파일을 순회하며 속성을 구분한다. 폴더일 경우 CyberVolk_ReadMe.txt 라는 파일을 해당 폴더에 생성하고, 랜섬웨어에 하드코딩된 랜섬노트 내용을 저장한다. 그 과정에서 이미 암호화된 파일 *.CyberVolk 와 랜섬노트 CyberVolk_ReadMe.txt 를 제외한 모든 파일을 암호화한다.

```
if ( wcslen(FindFileData.cFileName) > 0xFF
  || FindFileData.dwFileAttributes == 4// check FILE_ATTRIBUTE_SYSTEM
  || FindFileData.dwFileAttributes == 0x10000 )// check FILE_ATTRIBUTE_VIRTUAL
{
  goto LABEL_36;                        // FindNextFileW
}
if ( (FindFileData.dwFileAttributes & 0x10) != 0 )// check FILE_ATTRIBUTE_DIRECTORY (is directory?)
  break;
FileName[0].m128i_i16[0] = 0;
wcscat_s(FileName, 0x30Cu, v9);
wcscat_s(FileName, 0x30Cu, FindFileData.cFileName);
if ( !string_comparison(FileName, L"CyberVolk_ReadMe.txt") )
{
  if ( a2 == 101 )
  {
    if ( !string_comparison(FileName, L"CyberVolk") )
    {
      encryption(FileName, &savedregs);
      print_log(L"Encrypting File : %s\n", FileName);
    }
  }
```

그림 15. 암호화 예외 대상 확인

파일 암호화 과정은 기존 파일명에 암호화 확장자 .CyberVolk 가 추가된 파일을 새로 생성하는 것으로 시작한다. 이후 현재 시스템 시간을 시드로 설정한 뒤 난수를 생성해 32Bytes 크기의 암호화 키와 16Bytes 크기의 초기화 벡터(IV)를 파일마다 생성한다. 다음으로 파일 크기에 따라 전체 암호화와 부분 암호화를 진행한다. 파일 크기별 암호화 방식은 아래 그림과 같다.

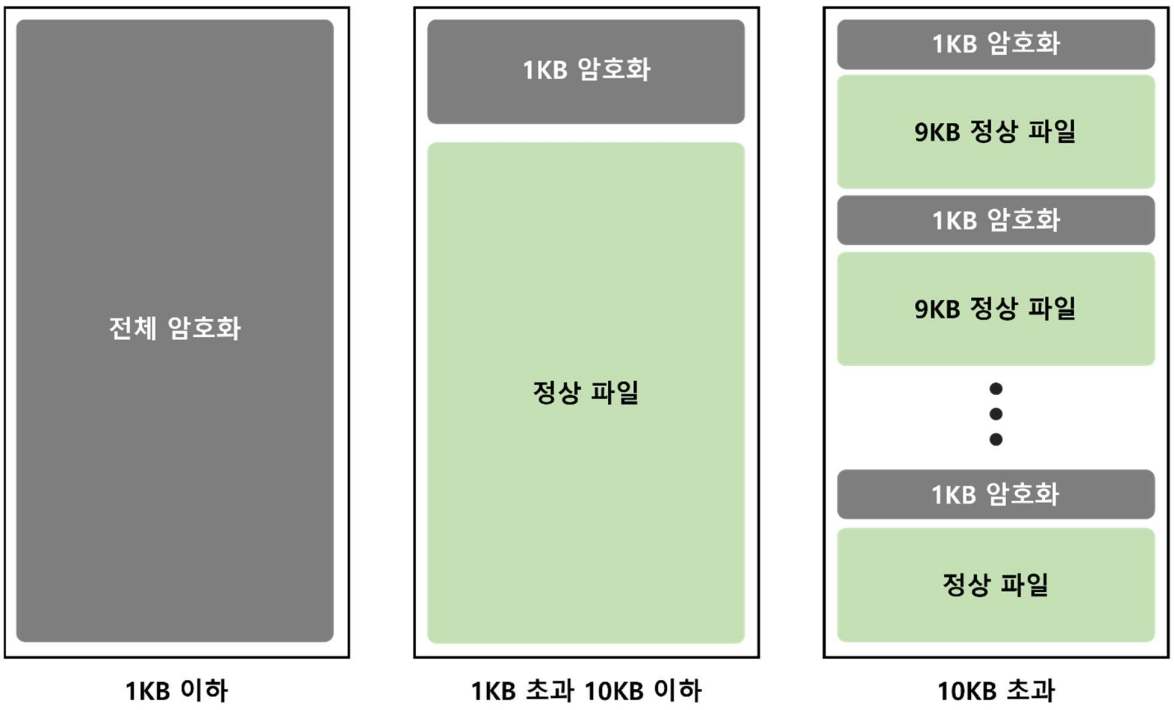


그림 16. 파일 암호화 방식

원본 파일 크기가 1KB 이하일 경우 전체 파일을 암호화한다. 1KB 초과 10KB 이하인 파일은 첫 1KB 만 암호화한다. 10KB 를 초과하면 10KB 간격마다 첫 1KB 만 암호화한다. 해당 방식으로 암호화한 파일은 암호화 확장자가 추가된 새로운 파일로 저장한다. 파일 암호화에는 AES 알고리즘을 사용하고, 사용한 키는 랜섬웨어에 하드코딩된 RSA 공개키를 이용해 보호한다. 파일 암호화에 사용한 초기화 벡터는 원본 그대로 암호화된 파일의 맨 앞에 추가하고, 보호된 암호화 키는 파일 맨 끝에 추가한다. 텔레그램에서는 파일 암호화에 ChaCha20 알고리즘을 사용한다고 홍보 중이나, 분석 결과 사용하지 않는 것으로 확인됐다.

또한, 파일 암호화 과정에서 랜섬웨어에 저장된 랜섬노트 데이터를 활용해 각 폴더에 랜섬노트를 생성한다.

```
.data:0042C380 ransomnote_data db 47h                  ; DATA XREF: recursive_search_directories:loc_422530↑r
.data:0042C380                                         ; recursive_search_directories+417↑o
.data:0042C381 aReetingsAllYou db 'reetings.',0Ah
.data:0042C38B db ' All your files have been encrypted by CyberVolk ransomware.',0Ah
.data:0042C3C8 db ' Please never try to recover your files without decryption key wh'
.data:0042C409 db 'ich I give you after pay. ',0Ah
.data:0042C424 db 'They could be disappeared?',0Ah
.data:0042C43F db 'You should follow my words.',0Ah
.data:0042C45B db 'Pay $1000 BTC to below address.',0Ah
.data:0042C47B db 'My telegram : @hacker7',0Ah
.data:0042C492 db 'Our Team : https://t.me/cubervolk',0Ah
.data:0042C4B4 db 'We always welcome you and your payment.',0
.data:0042C4DC align 10h
```

그림 17. 하드코딩된 랜섬노트 내용

앞서 언급한 바와 같이 CyberVolk 랜섬웨어는 키를 입력해 바로 복호화할 수 있는 기능이 있다. 사용자가 입력한 키는 %APPDATA% 경로에 dec_key.dat 이름으로 저장된다. 파일 복호화를 위해 각 파일 끝에 저장된 암호화 키를 복구해야 하고, 암호화 키 복구에는 4096Bytes 크기의 RSA 개인 키가 필요하다. 하지만 실제로는 36Bytes 길이의 키를 요구하고, 더 길거나 짧은 길이의 키는 필터링한다.

```
GetDlgItemTextA(hWnd, 1001, String, 37);
if ( strlen(String) != 36 )
{
  MessageBoxA(0, "Decryption Key is not correct!", 0, 0);
  return 0;
}
Substitute_Using_Dec_key(String);
dec_key_flag = 0;
SHGetFolderPathA(0, 26, 0, 0, ArgList);
FormatStringToBuffer(v37, "%s\\dec_key.dat", ArgList);
v21 = fopen(v37, "w");
v22 = v21;
if ( v21 )
{
  fwrite(String, 1u, 0x24u, v21);
  fclose(v22);
  return 0;
}
```

그림 18. 복호화 키 검증 및 저장

사용자가 입력한 36Bytes 의 키는 치환 테이블로 사용된다. 랜섬웨어에는 치환된 RSA 개인 키가 저장되어 있고, 사용자가 입력한 치환 테이블 기준으로 한 문자씩 치환해 RSA 개인 키가 복구된다. 치환 테이블을 정상적으로 입력했다면 파일별로 암호화 키를 복구할 수 있어 정상적인 복구가 진행된다. 다만, 키가 정상적으로 복구됐는지 검증하는 과정이 없어 잘못 입력했다면 복구가 정상적으로 이루어지지 않고, 잘못된 키로 복호화를 시도했기 때문에 암호화된 파일이 모두 손상된다.

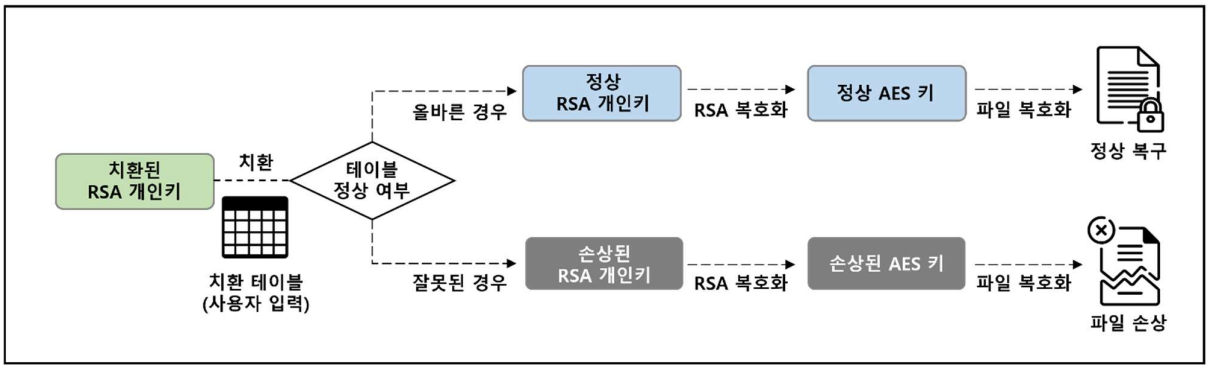

치환된
RSA 개인키
치환
테이블
정상 여부
치환 테이블
(사용자 입력)
올바른 경우
정상
RSA 개인키
RSA 복호화
정상 AES 키
파일 복호화
정상 복구
잘못된 경우
손상된
RSA 개인키
RSA 복호화
손상된 AES 키
파일 복호화
파일 손상

그림 19. 파일 복구 방식

CyberVolk 랜섬웨어 대응 방안

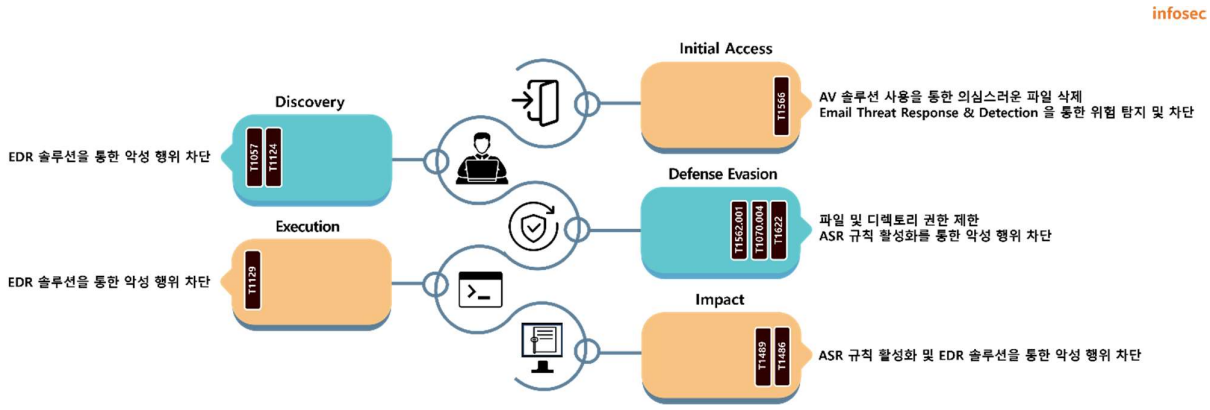


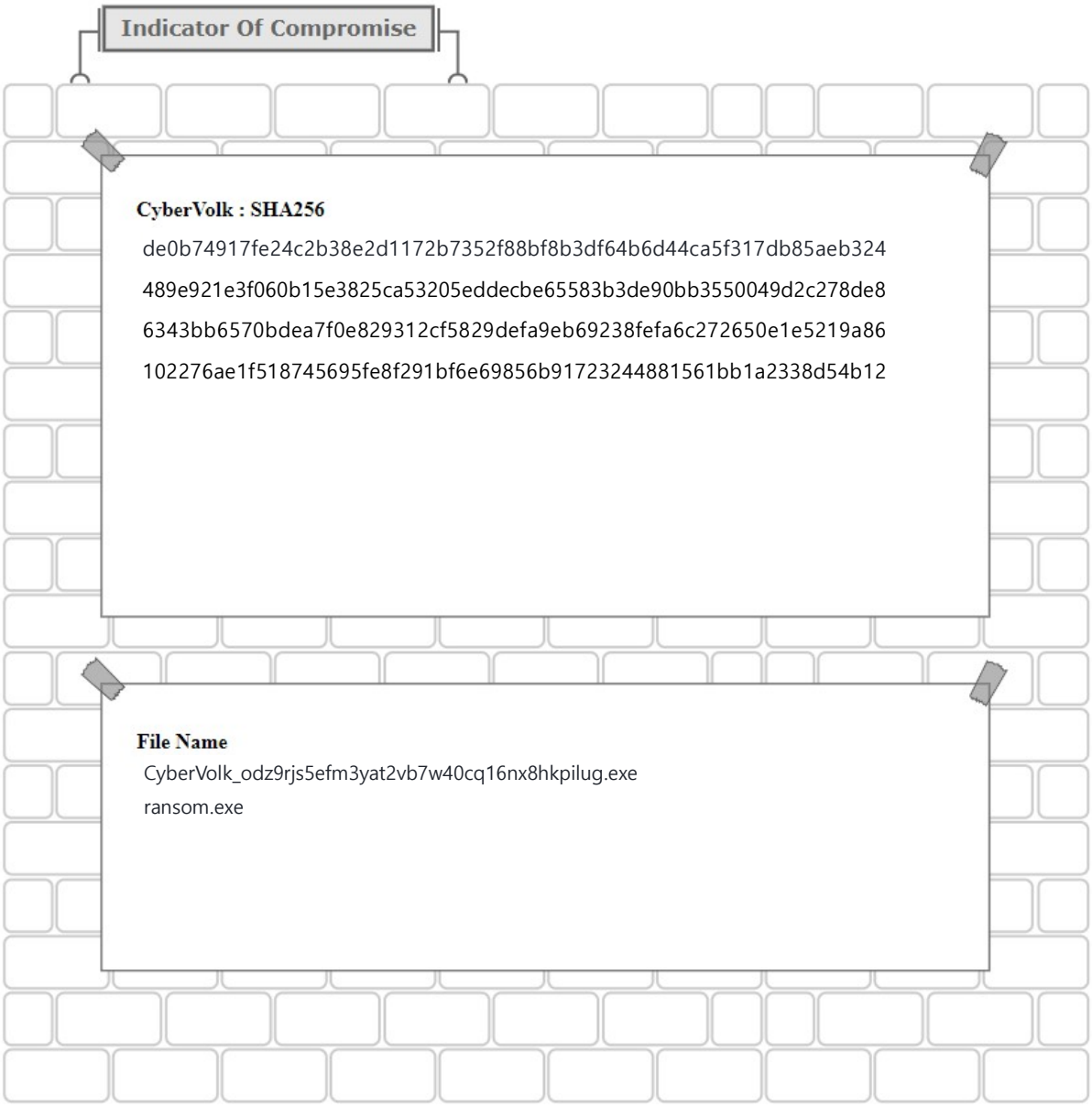
그림 20. CyberVolk 랜섬웨어 대응방안

CyberVolk 랜섬웨어는 메일의 첨부파일을 통해 랜섬웨어를 전파한다. 따라서 의심스럽거나 확인되지 않은 발신자의 메일 및 첨부파일을 열람하지 않도록 주의가 필요하다. 첨부파일을 내려받더라도 실행되지 않도록 Anti-Virus 등의 솔루션을 사용하거나 가상 환경에서 메일에 위협 요소가 있는지 사전 탐색하고 차단하는 Email Thread Response & Detection 솔루션 등을 이용해 위협을 막을 수 있다.

또한, 랜섬웨어 실행에 필요한 각종 설정 파일을 시스템에 저장해 사용한 뒤 삭제한다. CyberVolk 랜섬웨어는 별도의 프로세스 권한 상승 기능이 존재하지 않기 때문에 사전에 파일 및 디렉토리의 권한을 제한하거나 최소한으로 부여하는 등 조치가 필요하다. 추가로 ASR[11] 규칙을 활성화하거나 EDR 솔루션을 사용해 공격자의 특정 프로세스를 차단해 파일 암호화와 같은 악성 행위를 막을 수 있다.

마지막으로, CyberVolk 랜섬웨어는 제한적인 범위만 암호화하고 백업 복사본을 별도로 삭제하지 않기 때문에 Windows 기본 기능을 통해 시스템 백업을 해두었다면 일부 파일은 복구될 수 있다. 이 외에도 주요 데이터를 별도의 네트워크나 저장소에 소산 백업해 피해를 최소화할 수 있다.

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


Indicator Of Compromise
CyberVolk : SHA256
de0b74917fe24c2b38e2d1172b7352f88bf8b3df64b6d44ca5f317db85aeb324
489e921e3f060b15e3825ca53205eddecbe65583b3de90bb3550049d2c278de8
6343bb6570bdea7f0e829312cf5829defa9eb69238fefa6c272650e1e5219a86
102276ae1f518745695fe8f291bf6e69856b91723244881561bb1a2338d54b12
File Name
CyberVolk_odz9rjs5efm3yat2vb7w40cq16nx8hkpilug.exe
ransom.exe

■ 참고 사이트

• BleepingComputer 공식 홈페이지 (https://www.bleepingcomputer.com/news/security/linux-version-of-new-cicada-ransomware-targets-vmware-esxi-servers/)

• BleepingComputer 공식 홈페이지 (https://www.bleepingcomputer.com/news/security/ransomware-gang-deploys-new-malware-to-kill-security-software/)

• BleepingComputer 공식 홈페이지 (https://www.bleepingcomputer.com/news/security/ransomhub-ransomware-abuses-kaspersky-tdsskiller-to-disable-edr-software/)

• TRUESEC 공식 블로그 (https://www.truesec.com/hub/blog/dissecting-the-cicada)

• modePUSH 공식 블로그 (https://www.modepush.com/blog/highway-blobbery-data-theft-using-azure-storage-explorer)

• ArcticWolf 공식 홈페이지 (https://arcticwolf.com/resources/blog/arctic-wolf-observes-akira-ransomware-campaign-targeting-sonicwall-sslvpn-accounts/)

• 공공데이터포털 (https://www.data.go.kr/index.do)