Ransomware 분석

20240117 전승혁

목차

01 소개

02 랜섬웨어 동향

03 랜섬웨어 정의

04 RaaS

05 Lockbit

소개

2024년 사이버 보안 위협 및 기술 전망

이중 공격, 랜섬웨어 공격기법의 고도화

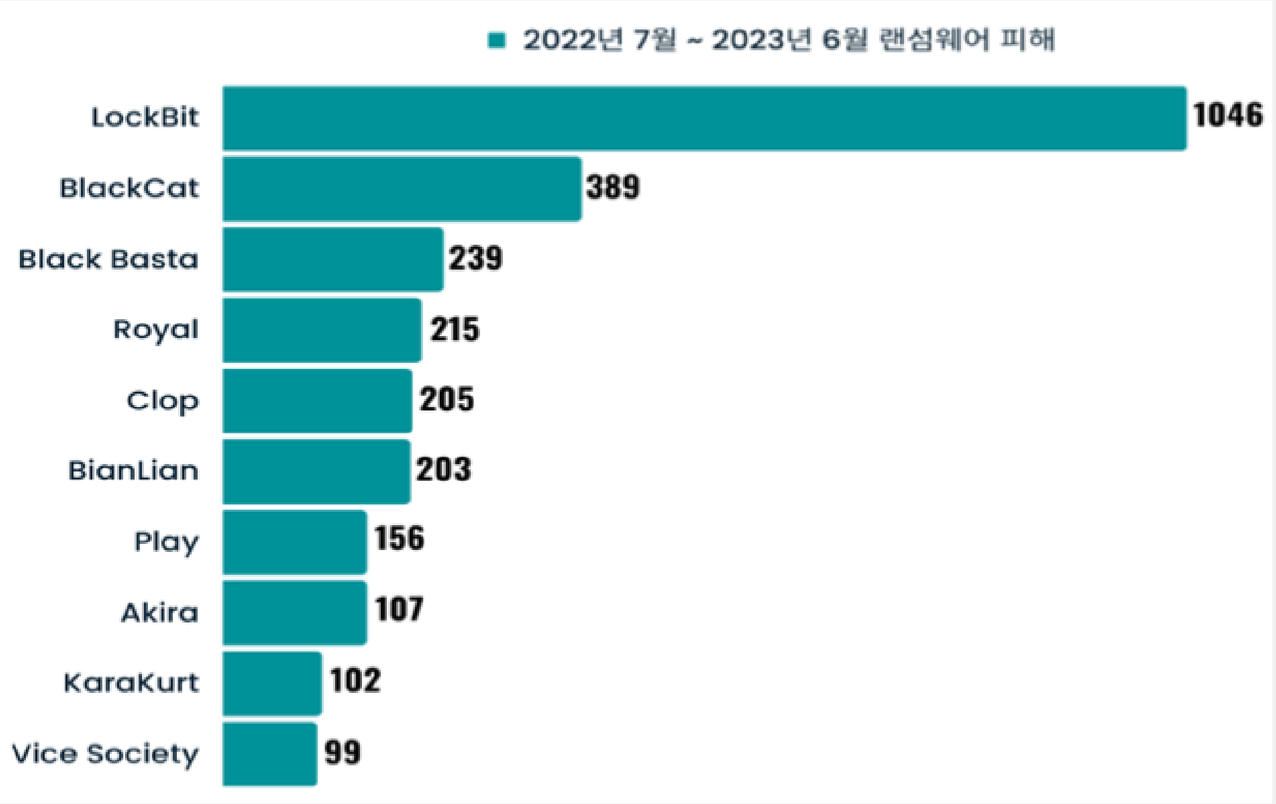
랜섬웨어 동향

유형별 침해사고 신고 현황

[단위 : 건수]

구분	연도	2022 (하반기)	비율	2023 (상반기)	비율
침해사고 신고	DDoS 공격	74	11.1%	124	18.7%
	악성코드	222	33.2%	156	23.5%
	(랜섬웨어)	(207)	(30.9%)	(134)	(20.2%)
	서버 해킹	310	46.3%	320	48.2%
	기타	63	9.4%	64	9.6%
합 계		669		664	

2022 ~ 2023
랜섬웨어 종류별 사례 건수



랜섬웨어 정의

Ransom
몸 값

+

Software
소프트웨어

컴퓨터 시스템을 감염시켜 접근을 제한하고 일종의 몸값을 요구하는 악성 소프트웨어의 한 종류

RaaS (Ransomware-as-a-service)

랜섬웨어 그룹이나 조직이 랜섬웨어 코드를 다른 해커에게 판매하고, 해커는 이를 사용하여 자체 랜섬웨어 공격을 수행하는 사이버 범죄 비즈니스 모델

Lockbit - Lockbit Green

Name	⟨unknown⟩
Type	PE32
SHA-256	45c317200e27e5c5692c59d06768ca2e7eeb446d6d495084f414d0f261f75315
Description	LockBit Green Ransomware

Lockbit - Lockbit Green

API 후킹 해제

실행 옵션 파싱

섀도 카피본 삭제

암호화 대상 선정

파일 암호화

랜섬노트 생성

Lockbit - Lockbit Green

API 후킹 해제

API 후킹 : Win32 API가 호출 될 때 중간에서 이를 가로채서 그 제어권을 얻어내는 것

Lockbit - Lockbit Green

실행 옵션 파싱

락빗 랜섬웨어가 어떤 옵션과 함께 실행됐는지 확인하기 위해 명령줄에서 파싱함.

실행 모드	설명
ALL_ENCRYPT	LOCAL_ENCRYPT와 NETWORK_ENCRYPT를 모두 수행한다.
LOCAL_ENCRYPT	마운트된 모든 논리 디스크를 순회하며 암호화한다.
NETWORK_ENCRYPT	공유 폴더를 암호화한다.
PATH_ENCRYPT	지정된 최상위 경로부터 암호화한다.
BACKUPS_ENCRYPT	파일 암호화는 하지 않고 섀도 카피본만 삭제한다.

Lockbit - Lockbit Green

섀도 카피본 삭제

랜섬웨어에 걸린 파일들을 복구하지 못하게 백업본 삭제

Volume Shadow Copy Service

Lockbit - Lockbit Green

암호화 대상 선정

암호화 대상 파일 경로를 수집하기 위해 주어진 최상위 경로부터 최하위까지 파일을 재귀적으로 탐색

실행 모드	최상위 경로
LOCAL_ENCRYPT	A부터 Z까지의 문자 중 마운트 된 모든 논리 디스크
NETWORK_ENCRYPT	특정 IPv4 주소 대역에 포함되는 SMB(445번 포트) 서버의 공유 폴더
PATH_ENCRYPT	실행 인자(-p 옵션)로 입력했던 경로

Lockbit - Lockbit Green

파일 암호화

파일의 모든 데이터를 암호화하지 않음.
파일의 확장자와 크기 등으로 구분하여 파일 암호화 정도의 백분율을 결정함.

조건	암호화 대상
1MiB 이하	전체 암호화.
1MiB 초과 5MiB 이하	앞의 1MiB만 암호화.
5MiB 초과	실행 옵션(-size)에서 설정한 백분율만큼 암호화. 락빗은 해당 옵션이 50으로 고정이기에 절반만큼 암호화한다.

Lockbit - Lockbit Green

랜섬노트 생성

랜섬 노트 : 컴퓨터나 파일 등을 감염시킬 때 나오는 문서나 메시지.

Lockbit 대응

1. 논리적 망분리를 적용하여 악성코드 PC 유입을 원천 차단
2. AV(패턴기반탐지) + EDR(행위기반탐지) 솔루션을 최신 형상으로 유지
3. PC 취약점을 주기적으로 점검, 보완
4. 신뢰할 수 없는 메일의 첨부파일은 실행을 금지
5. 비 업무 사이트 및 신뢰할 수 없는 웹사이트의 연결을 차단
6. OS나 어플리케이션은 최신 형상을 유지

Lockbit 피해 사례

국내 피해 현황

일시	기업명	피해 규모
2023.03.30	대한민국 국세청	락빗이 탈취한 정보를 공개하겠다고 밝혔으나 국세청은 공식적인 피해가 없다고 밝힘,
2022.09.29	모 대기업	22년 7월 정보 복구비용으로 345 비트코인 요구 (한화 약 100억원) 22년 8월 탈취 데이터 공개로 1,350만 달러 재요구 (한화 약 180억원) 협상 결렬로 데이터 공개 (주간보고서, 임원회의록, 사업계획서 등 2TB 크기의 데이터)