

More security,
More freedom

개인정보보호 강화를 위한 Endpoint Hardening 전략

안랩 솔루션컨설팅팀 백민경 부장 / CISSP

7/6(화) 오후 1시 20~1시 40분



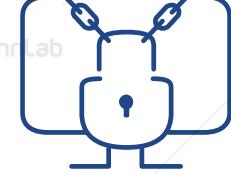
목차

1. 최근 유행하는 악성코드
2. 정보유출을 노리는 InfoStealer
3. Targeted Ransomware
4. 침해 사고 사례
5. Endpoint Hardening

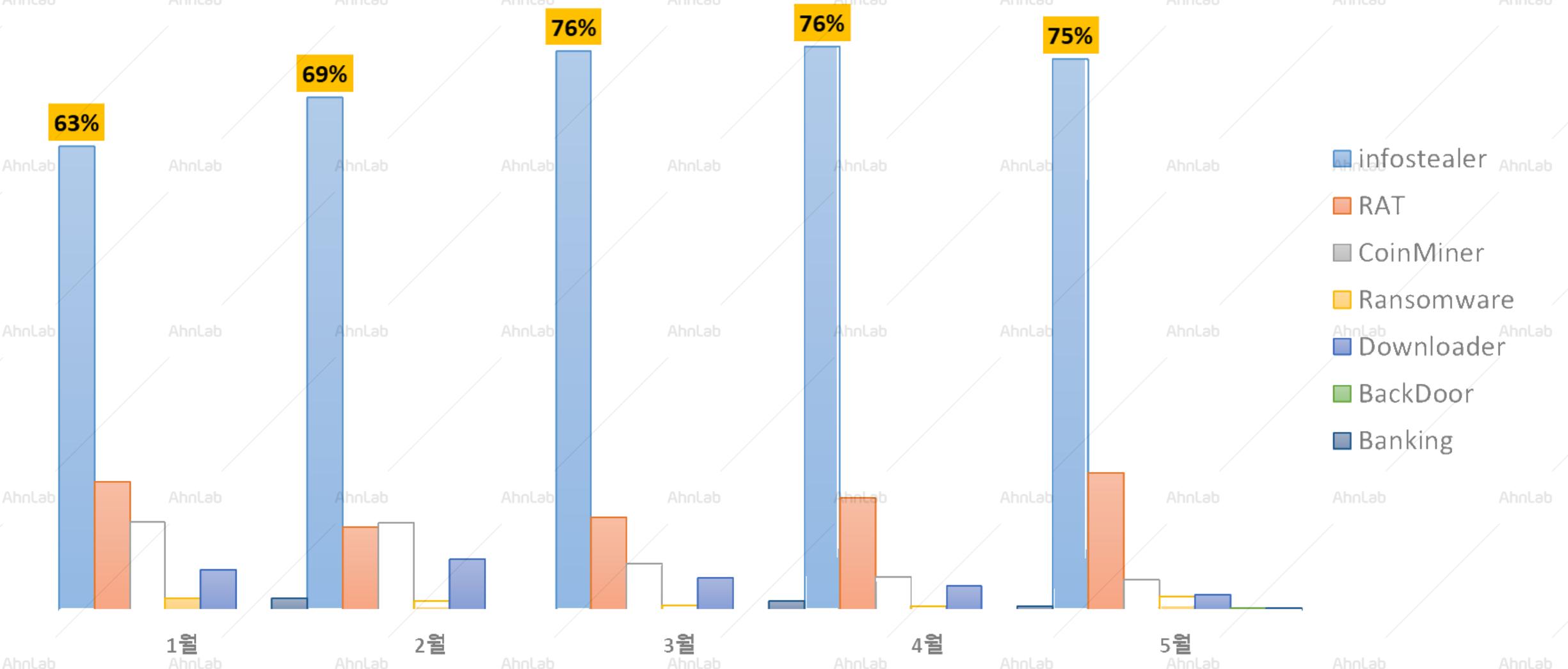
최근 유행하는 악성코드는?


정보 탈취
(Info Stealer)

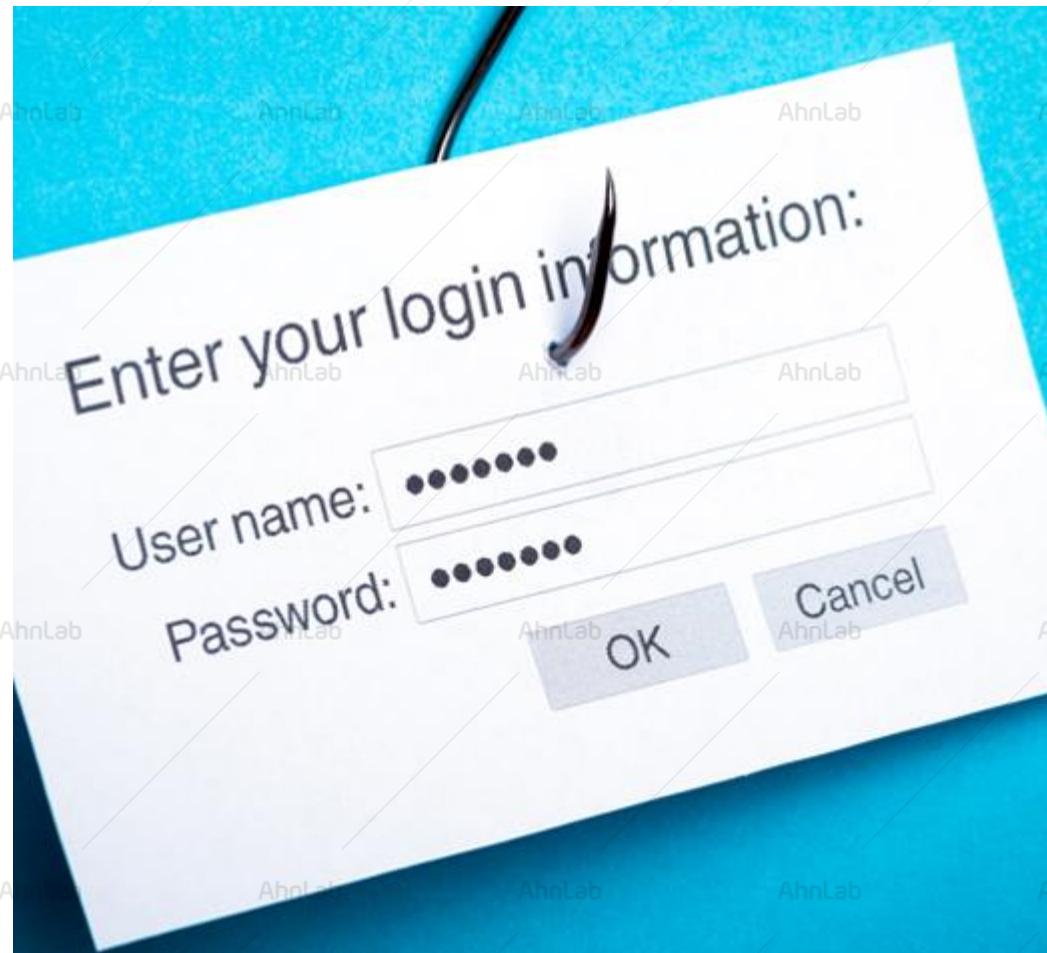

**계정정보
탈취용 피싱**
(Spear Phishing)


랜섬웨어
(Ransomware)

2021년 상반기 악성코드 통계 1위는 InfoStealer



InfoStealer가 노리는 것



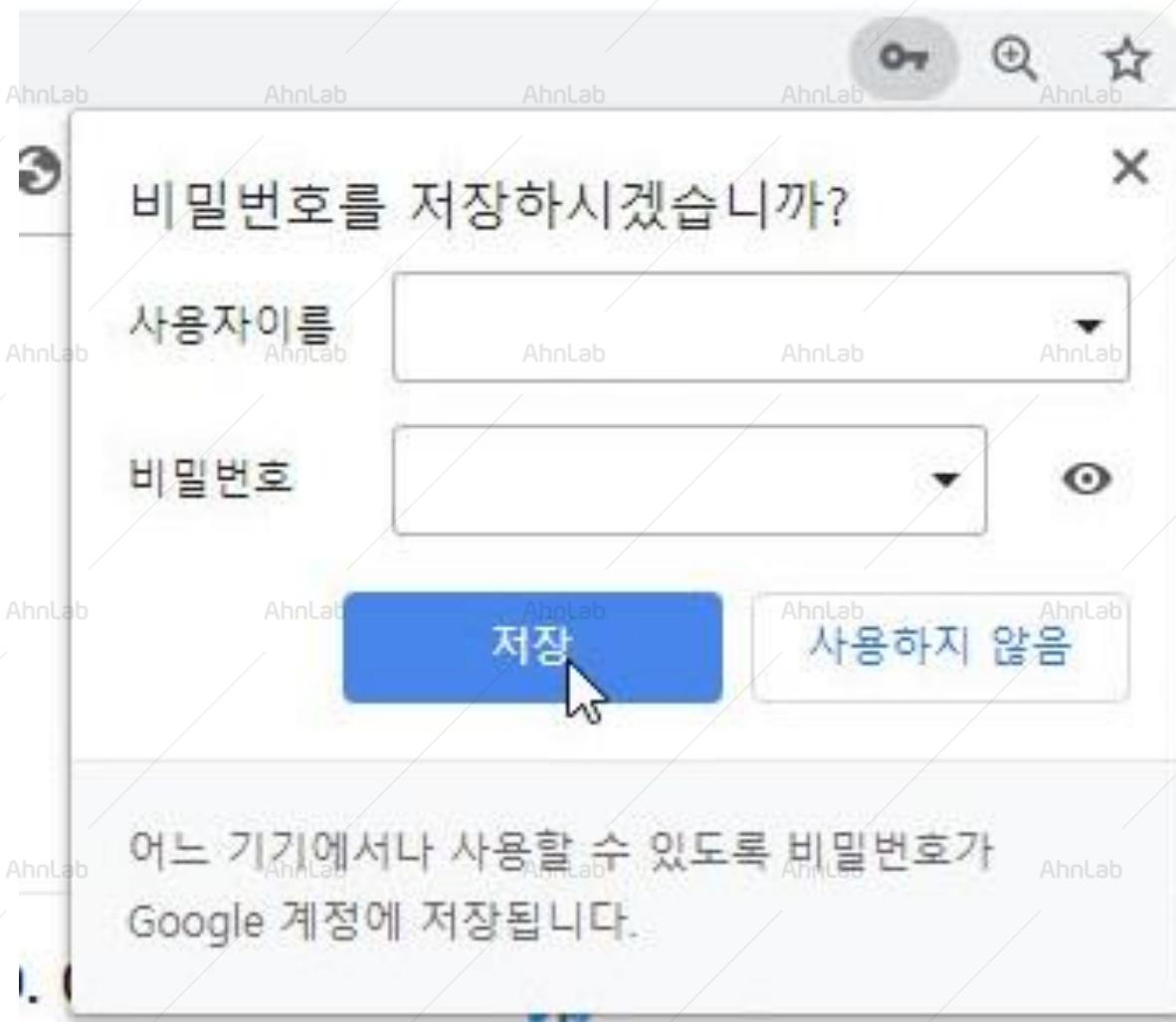
장치 사양

| | | | | |
|---------|-------------------------|--------|---|---------|
| 디바이스 이름 | | AhnLab | Intel(R) Core(TM) i7-4770 CPU @ 3.40GHz | 3.40GHz |
| 프로세서 | | | | |
| 설치된 RAM | 24.0GB(23.9GB 사용 가능) | | | |
| 장치 ID | | AhnLab | | |
| 제품 ID | | AhnLab | | |
| 시스템 종류 | 64비트 운영 체제, x64 기반 프로세서 | AhnLab | | |

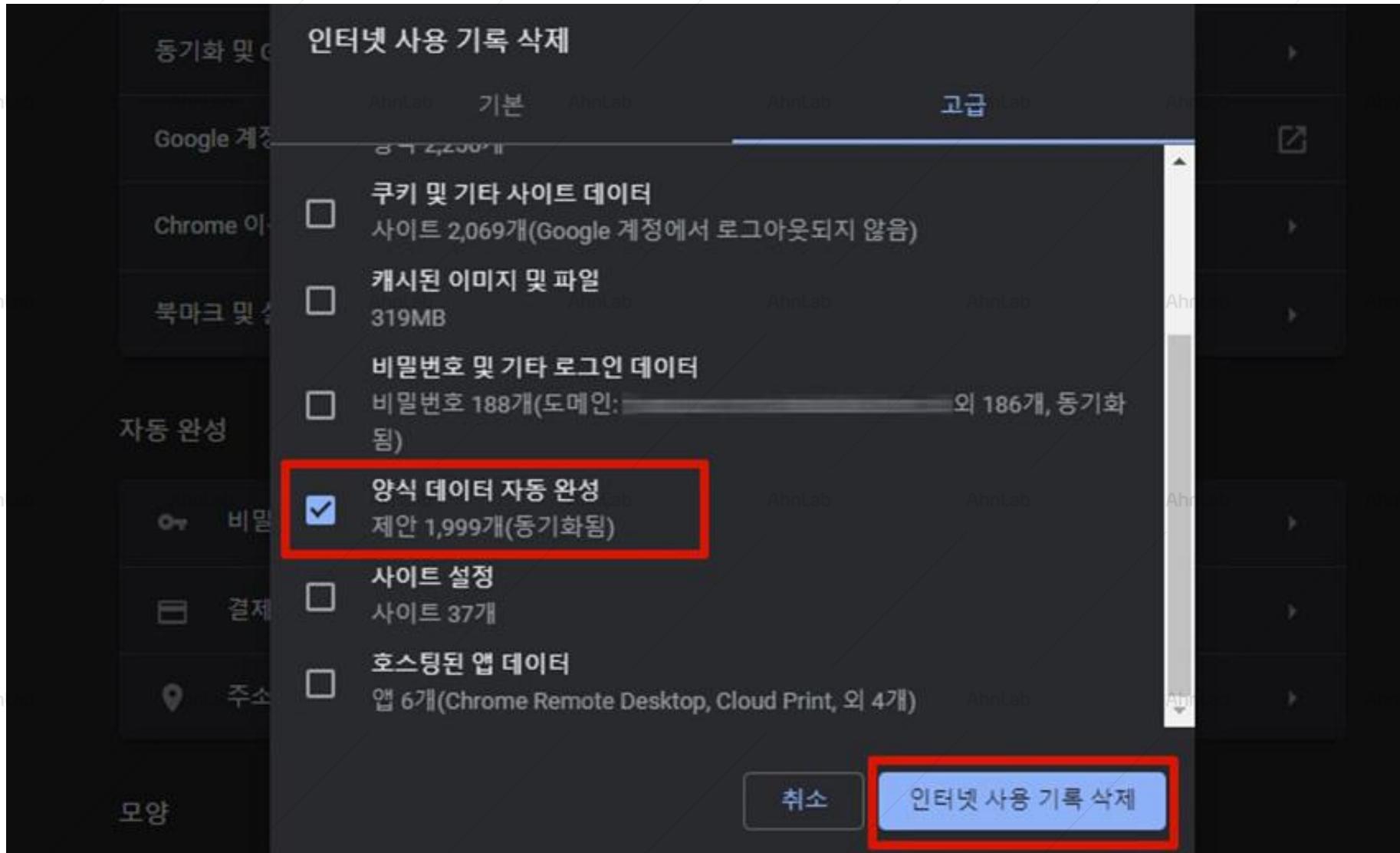
Windows 사양

| | |
|-------|--|
| 에디션 | Windows 10 Enterprise |
| 버전 | 20H2 |
| 설치 날짜 | 2021-01-19 |
| OS 빌드 | 19042.928 |
| 경험 | Windows Feature Experience Pack 120.2212.551.0 |

InfoStealer가 노리는 것



브라우저에서 추출만 하면 되는



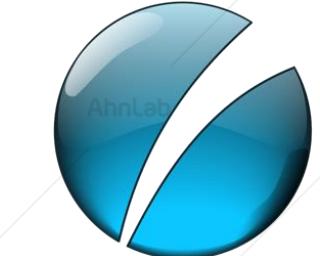
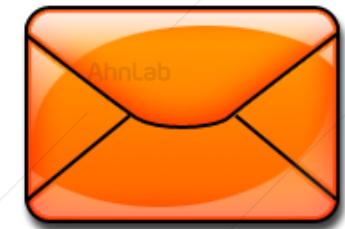
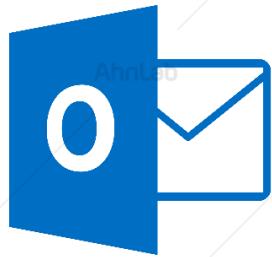
InfoStealer 정보수집 대상

Web Browser



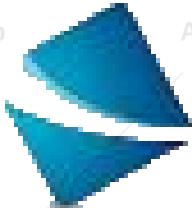
InfoStealer 정보수집 대상

Email 등



InfoStealer 정보수집 대상

기타 Tool들



ipswitch
WS_FTP

 **icq**

 **SmartFTP**

타깃 랜섬웨어 (Targeted Ransomware)



기업



금융



의료기관



국가기관

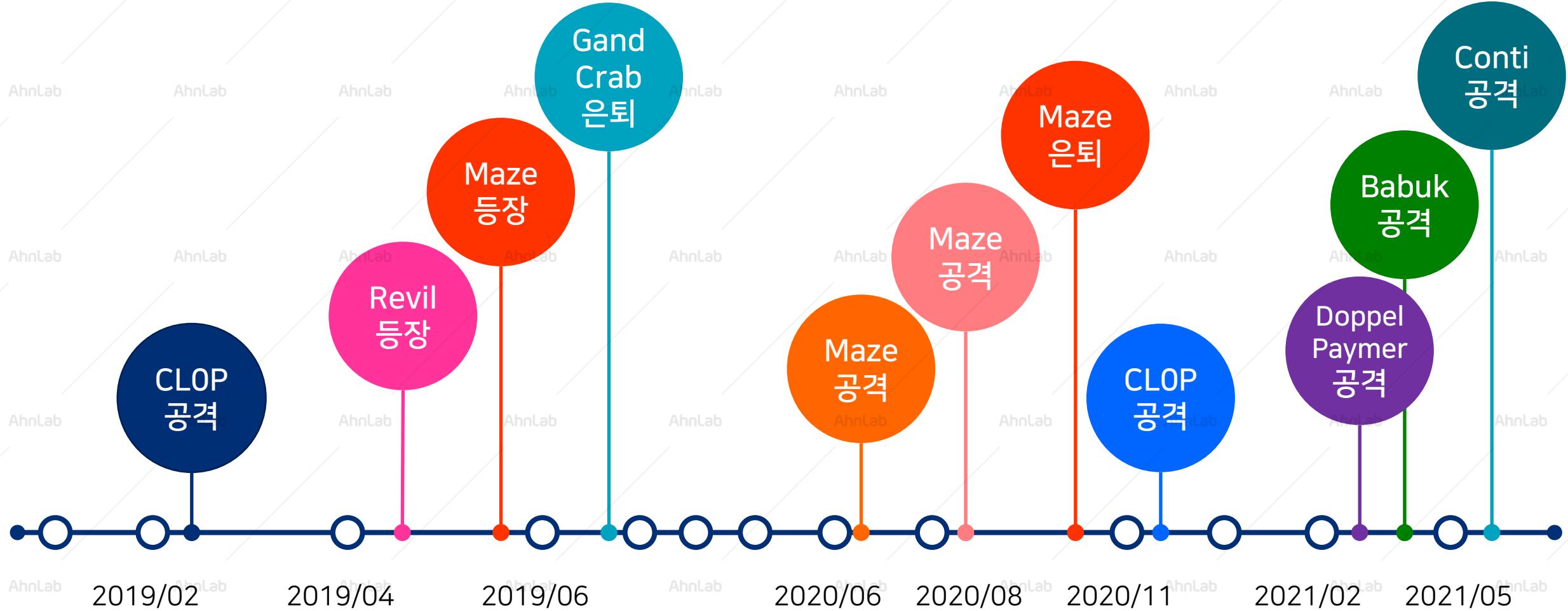


기간산업



제조

타깃 랜섬웨어가 위협의 핵!



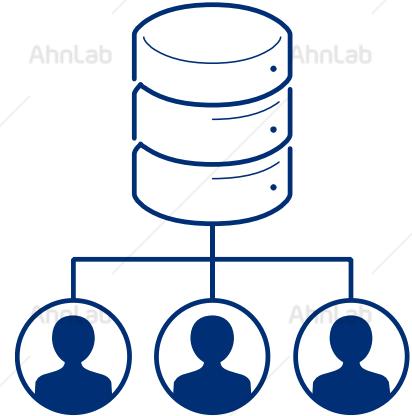
랜섬웨어 감염 시키기 전에



RDP 접속



공유폴더 접속



AD 탈취

2중 협박 (Double Extortion)

Mount Locker News & Leaks

Press & bloggers welcome for interview!

Send us your TOX ID

Announcements & Partial Dumps



Nachi America Inc.

www.nachiamerica.com

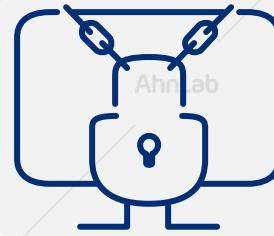
\$ 39M 2TB 0%



ECU Worldwide

ecuworldwide.com

\$ 1b 2TB 0%

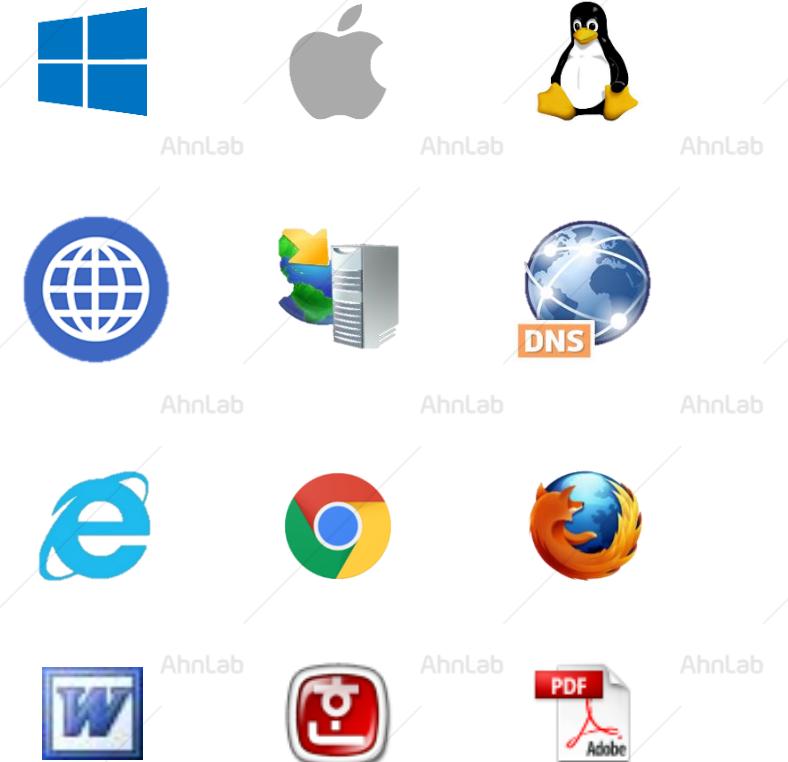


랜섬웨어 감염

탈취 정보 공개

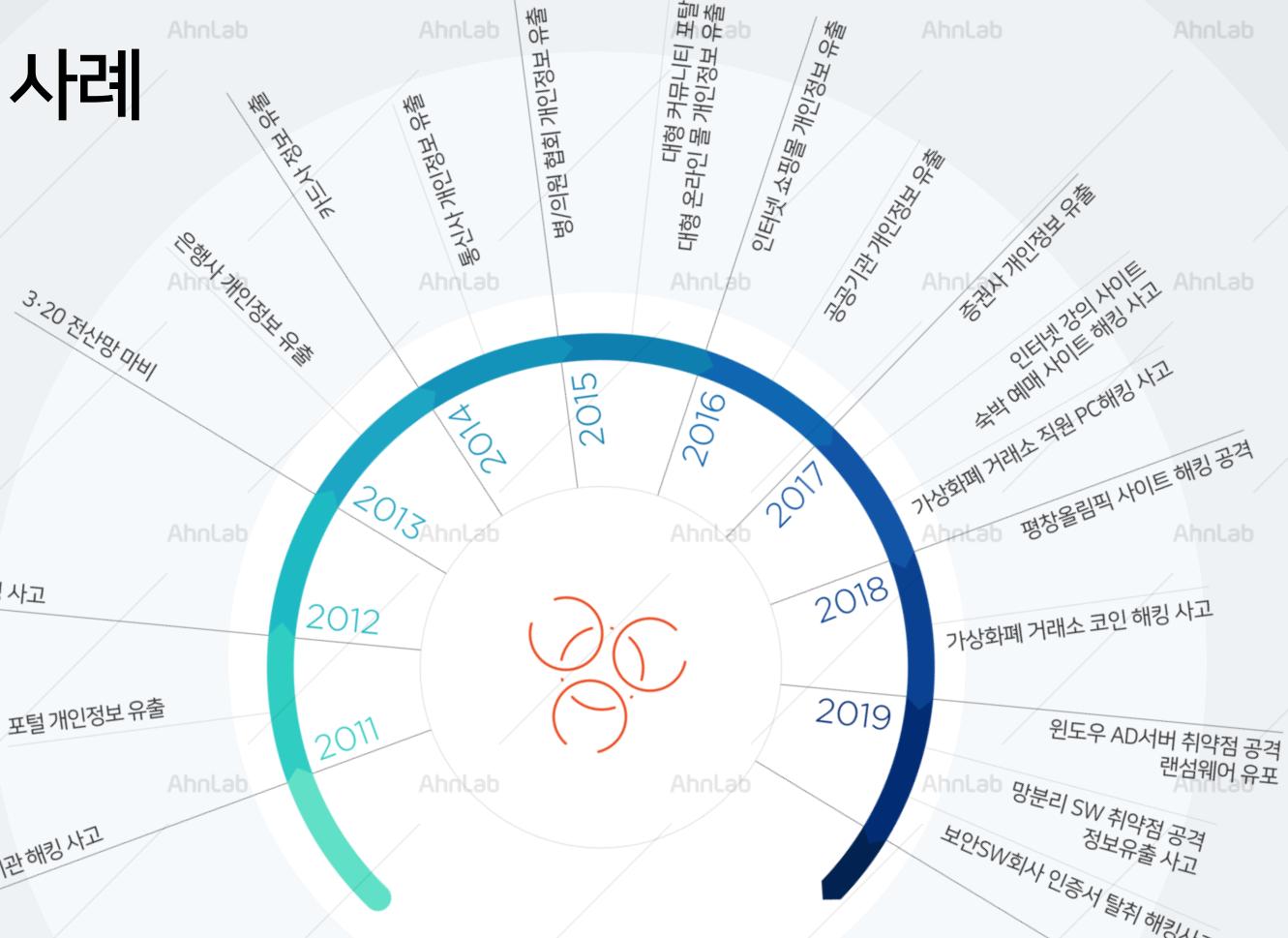
너무나 많은 취약점들..

최근 20년 간 14만개 이상의 취약점



출처 : <https://www.cvedetails.com>

반복되는 침해 사고 사례



공격자들의 목적

공격 목적

약탈

협박

기밀 자료

침해 사실 공개

개인 정보

DoS

게임 머니

암호 화폐

랜섬웨어

CPU

금전 이익

침해사고 공격 사례



1. 사전 준비

2. 배포

3. 익스플로잇

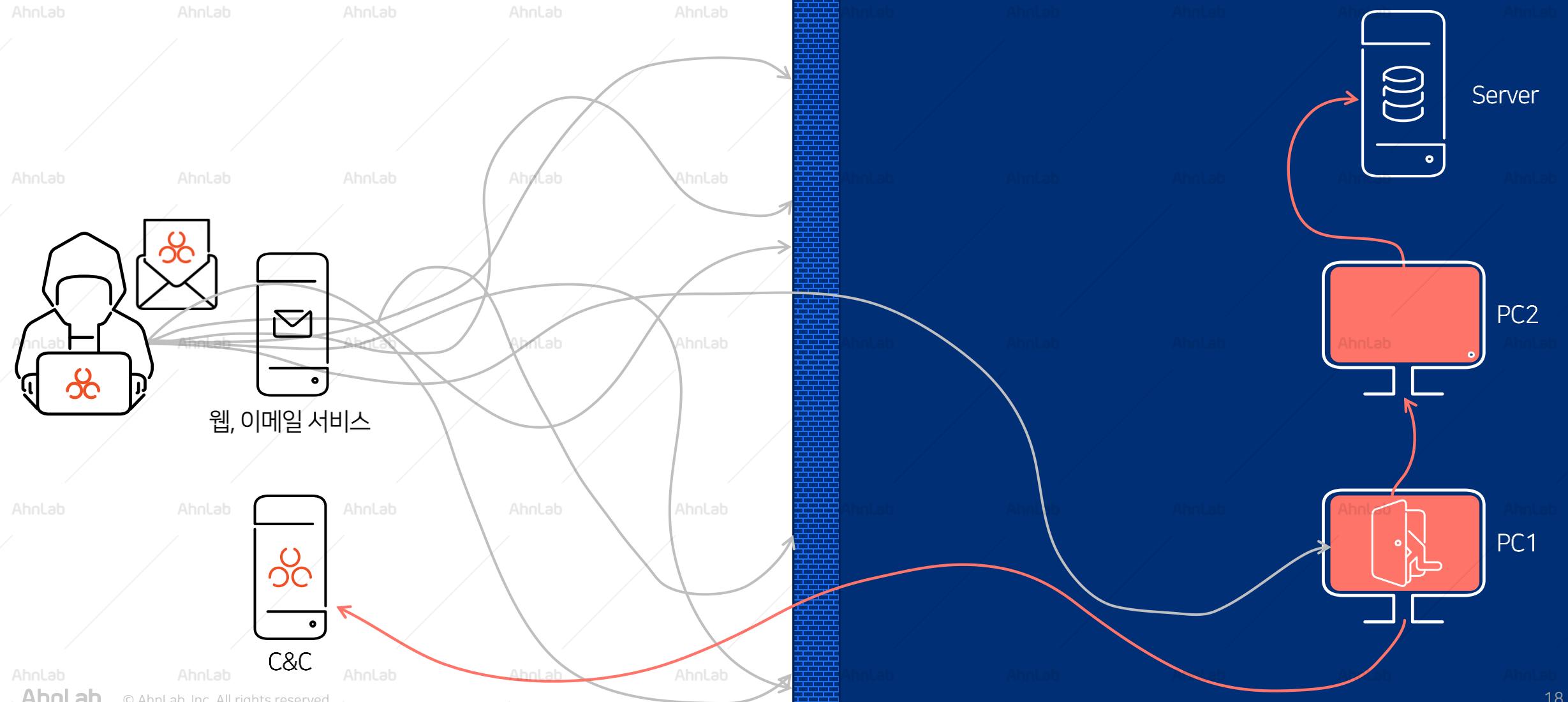
4. 백도어 설치

5. C&C 접속

6. 내부 이동

7. 최종공격수행

8. 흔적 지우기





유입 방어

Firewall
IDS / IPS
Web Firewall

Anti-DDoS
Anti-Spam
N/W Sandbox

탐지 대응

Anti-Virus
Endpoint Sandbox
Host IP, Host Firewall

유출 방어

DLP (Web, Email, USB)
DRM
Device Control

망 구분

물리적 망 분리
VDI
망 연계



Endpoint Hardening



데이터 보호

SSL
DB Encryption
Personal Privacy Protection



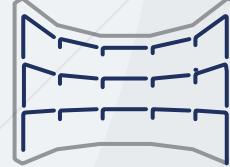
인증 강화

NAC
OTP (Multi Factor Authentication)
접근 통제 시스템 | SSO



취약점 제거

PMS
취약점 점검
모의해킹



보안 운영 관리

More security, More freedom