cybereason DOOSAN

2025년 1월- 5월

TTP 분석 보고서

(Tactic, Technique, Procedure)

cybereason

방법론

본 TTP 브리핑은 사이버리즌(Cybereason)이 전 세계에서 수행한 침해 사고 대응(IR) 활동을 통해 수집한 위협 인텔리전스를 기반으로 글로벌 보안 운영 센터(GSOC)의 탐지 데이터를 일부 보완하여 포함하고 있습니다. 내용은 실제 환경에서 사이버리즌이 관찰하고 있는 공격 트렌드, 기술, 절차를 반영하였으며, 고객에게 진화하는 위협 환경에 대한 현실적인 인사이트를 제공하기 위한 목적으로 작성되었습니다.

데이터 개요

가장 많이 영향을 받은 산업군 (Top 3)

- 금융 서비스: 18%
- 제조업: 16%
- 기술 및 소프트웨어: 11%

주요 위협 유형 (Top 3)

- 비즈니스 이메일 공격(BEC): 41%
- 랜섬웨어: 28%
- 클라우드 침입: 13%

*BEC: Business Email Compromise

주요 초기 침입 경로 (Top 3)

- 피싱/사회공학 기법: 46%
- 유효 계정/자격 증명 도용: 16%
- 취약점 악용: 14%

cybereason

2025 상반기 주요 인사이트

대부분의 조직이 EDR을 도입했습니다 (76%)

*EDR(Endpoint Detection and Response): 앤드포인트 탐지 및 대응

EDR 우회 기술은 5% 미만으로 매우 드물게 발견되었지만 공격자들은 여전히 침해에 성공했습니다.

대부분 EDR이 경고 알림을 울렸지만 조직이 적절하게 대응하지 못한 것으로 드러났습니다.

BEC 피해자 중 MFA를 설정한 비율은 36%에 불과합니다

*BEC(Business Email Compromise):비즈니스 이메일 공격
*MFA(Multi-Factor Authemtication):다중 인증

MFA를 설정한 계정에서도 BEC 공격의 MFA 우회 성공률이 50% 넘는 것으로 밝혀졌습니다.

이는 MFA 인증 토큰과 자격 증명을 훔칠 수 있는 고급 피싱 키트가 널리 사용되고 있기 때문입니다.

탐지 회피와 제 3의 요인이 보안 복잡성을 증가시켰습니다

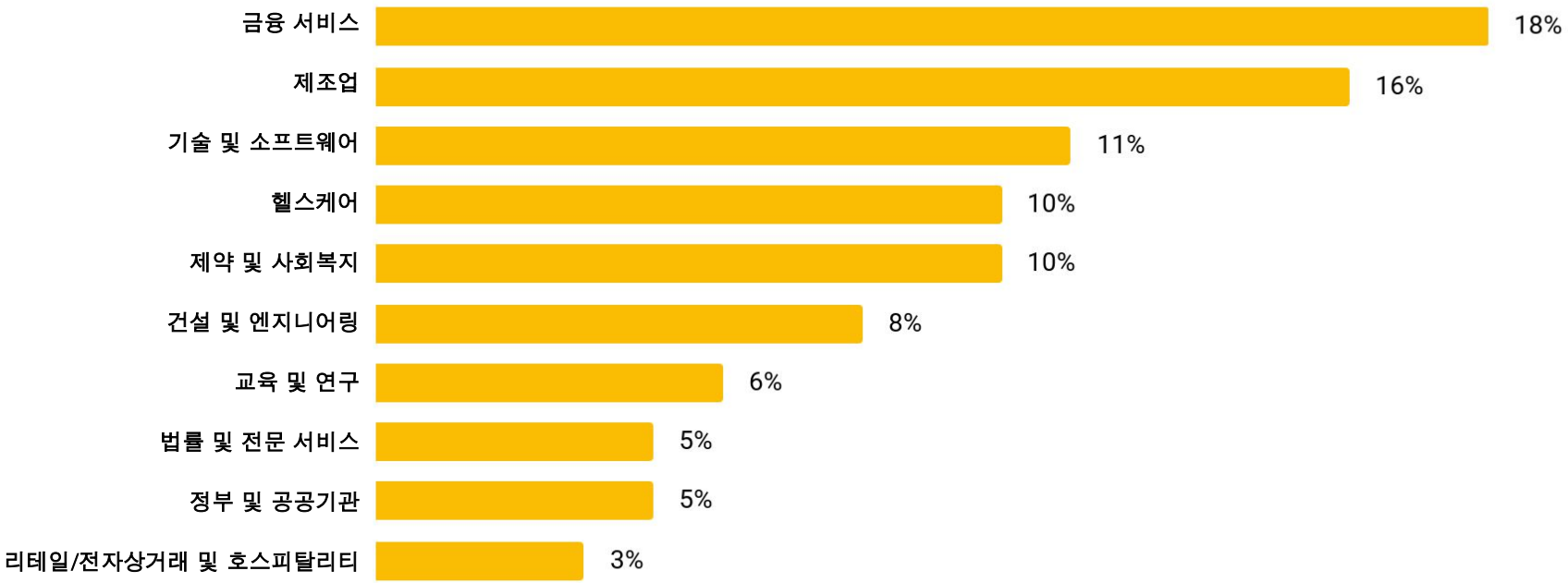
전체 보안 사고의 18%에서 공격자는 LOLBins을 활용해 탐지를 회피했고,

약 7%는 제 3자(공급망 등)로부터 공격이 유입되었거나 영향을 받았습니다.

*LOLBins(Living-off-the-land Binaries):운영 체제에 이미설치된 정상 파일 및 기능을 악용하는 방식

cybereason

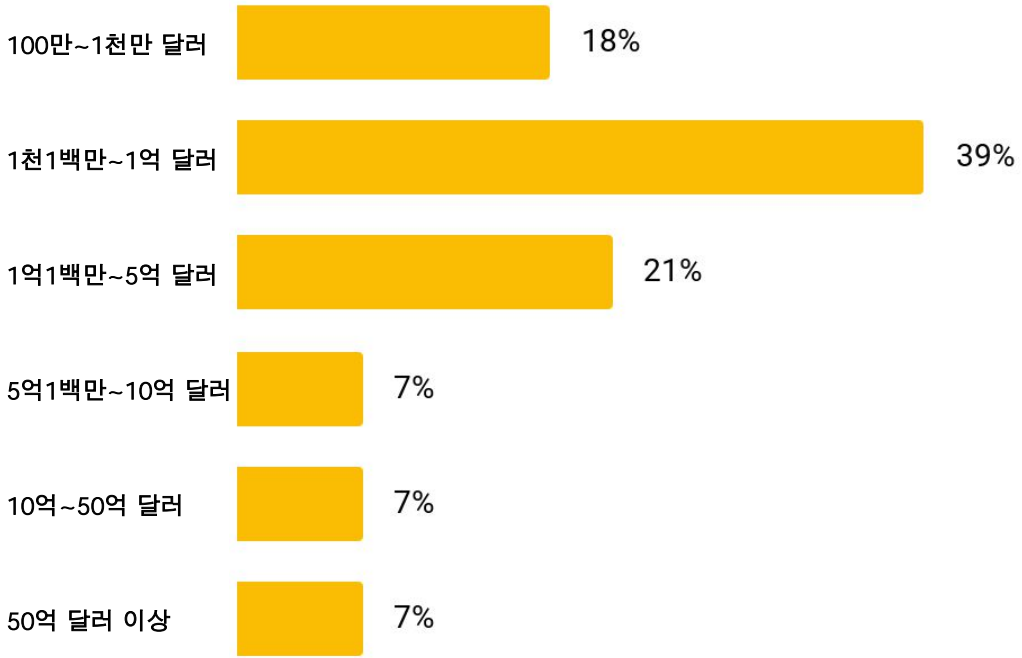
영향 받은 산업군 Top 10



cybereason

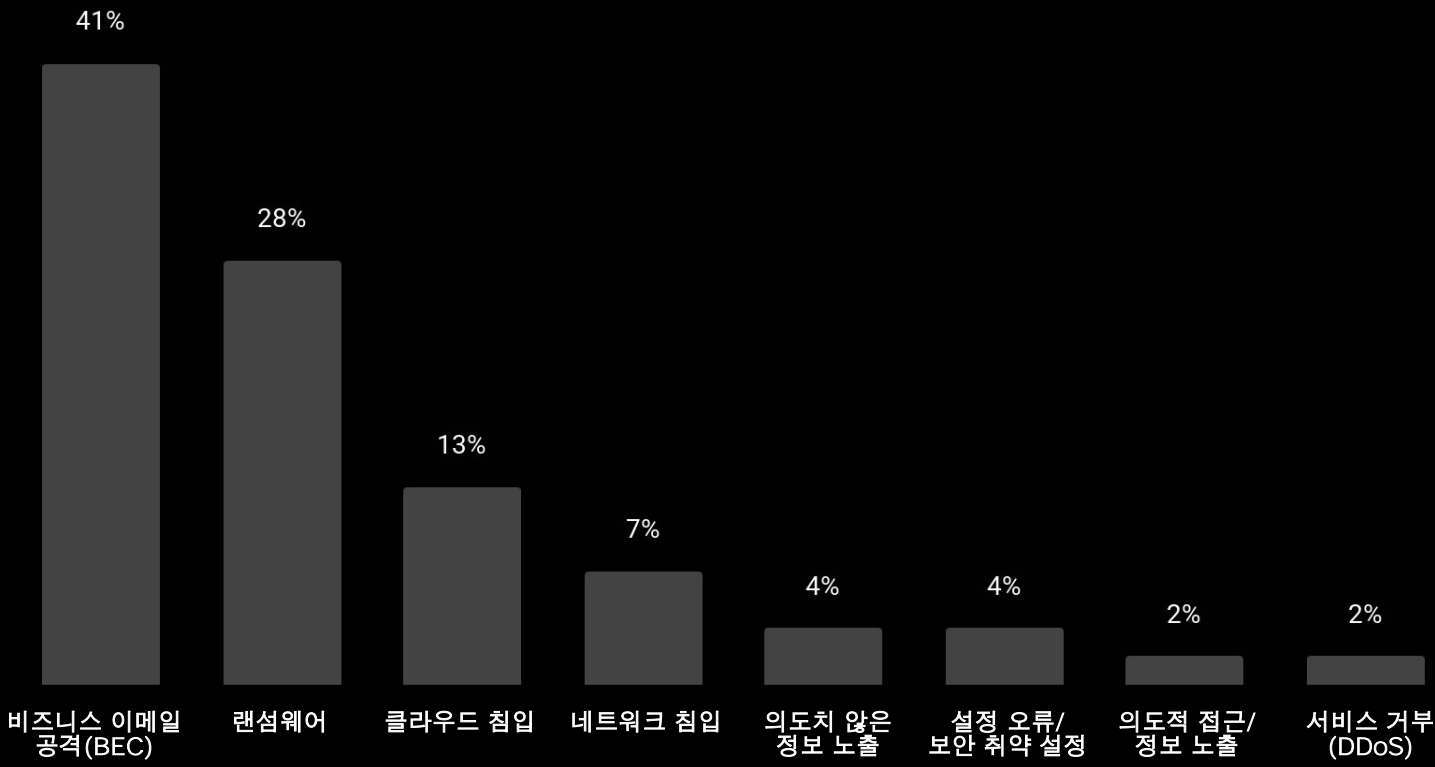
기업 규모별 분포

매출 기준



cybereason

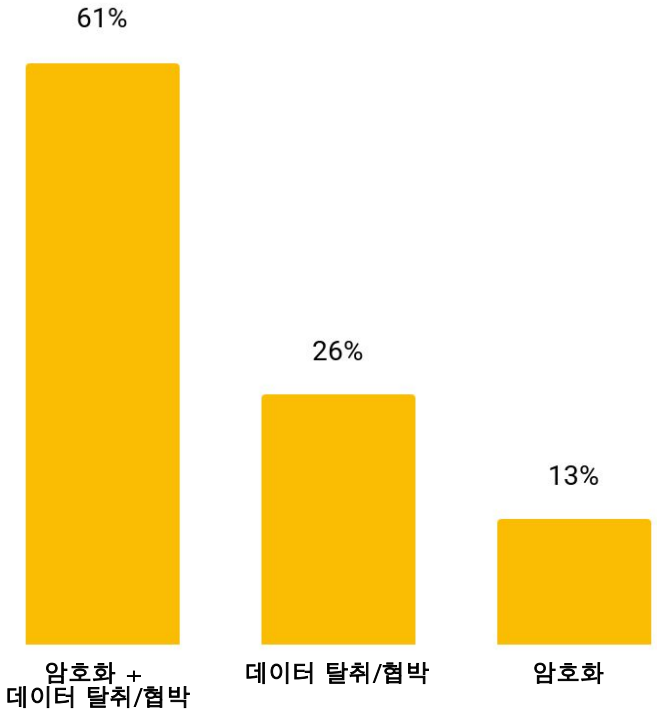
보안 사고 유형별 발생 순위



cybereason

랜섬웨어

공격 유형 별 발생 분포



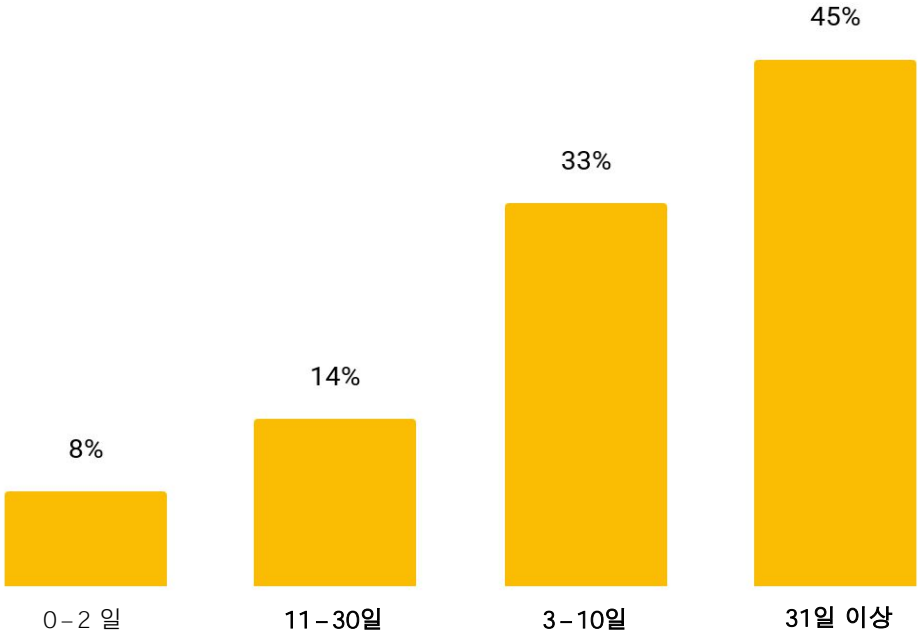
2025년 발견된 랜섬웨어 변종

빠르게 확산되는 유형	기타 유형
Akira	Bootkit
Inc	Cactus
Play	BlackNevas
SafePay	GandCrab
Medusa	Makop
Qilin	Ransomhouse
	Mimic
	SECP0

Dwell Time

침입 후 대응까지 걸린 시간

침입이 발생한 시점부터 Cybereason 사고 대응(IR) 팀이 개입하기까지의 시간을 측정한 결과입니다.



대응 시간 평가 기준

- 0~2일: 매우 우수 (8%)
- 3~10일: 우수 (45%)
- 11~30일: 평균 이하 (14%)
- 31일 이상: 매우 미흡 (33%)

*사이버리즌 MDR 고객을 제외한 컨설팅 고객만 분석한 지표입니다.

cybereason

가장 많이 관찰된 취약점(CVE)

CVE	영향 받은 제품
CVE-2024-55956	Cleo Harmony
CVE-2022-41335	Fortinet FortiOS
CVE-2022-42475	FortiOS SSL-VPN
CVE-2024-57727	SimpleHelp Remote Support Software
CVE-2023-34362	MOVEit Transfer
CVE-2016-0099	Microsoft Windows Secondary Logon Elevation of Privilege
CVE-2023-20269	CISCO Adaptive Security Appliance

cybereason

침입 경로 트렌드

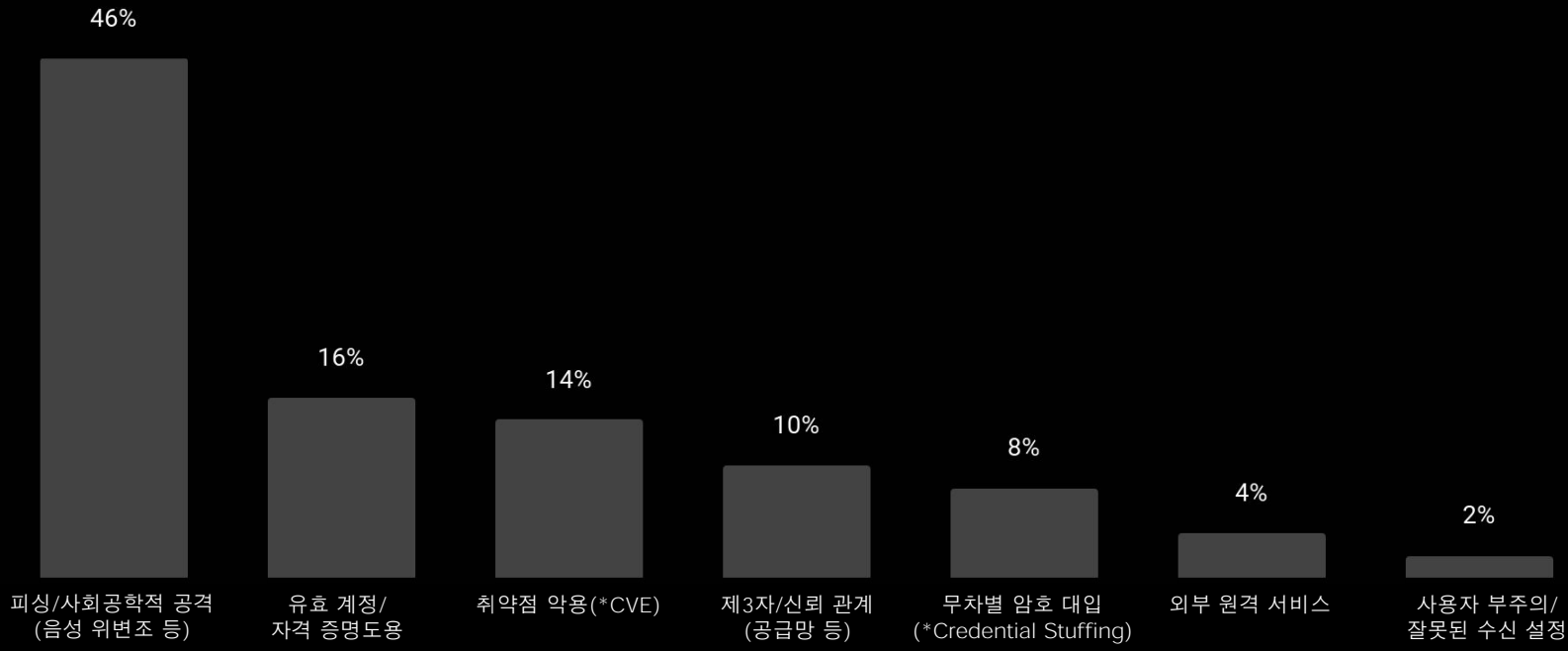
공격자는 다음과 같은 5단계의 활동을 통해 목표를 달성합니다

1 초기 침입	2 공격 지속	3 권한 상승	4 데이터 위협	5 최종 목표 달성
공격자가 최초로 시스템에 접근하기 위한 단계:	공격자가 시스템 내에 자리를 잡고 활동을 이어가는 단계:	공격자가 더 많은 권한을 얻고 확장하는 단계:	공격자가 데이터를 탐색하거나 데이터를 빼앗는 단계:	
• 외부 정찰 • 진입 경로 식별 • 최초 감염 시스템 혹은 사용자 (Patient 0) 확보	• 내부 정찰 • 공격 위치 파악 • 시스템 접근 경로 확보 • 원격 접근/*C2 연결	• 자산 탐색 • 권한 획득 • 횡적 이동 (다른 시스템으로 공격 이동)	• 데이터 탐색 • 데이터 접근 • 데이터 획득/탈취	• 암호화 • 금전 요구 협박 • 금전적 이득(데이터 판매 등) • 비즈니스 중단

*C2(Command & Control): 공격자가 악성코드에 감염된 시스템을 원격으로 제어하기 위해 사용하는 서버 또는 프레임워크

cybereason

1. 초기 침입 경로



*CVE(Common Vulnerabilities and Exposures): 공개적으로 알려진 보안 취약점
*Credential Stuffing: 다크 웹 등에서 획득한 사용자 계정 정보(아이디/비밀번호)를 이용해 여러 웹사이트에 무작위로 로그인 시도를 하는 공격 방식

cybereason

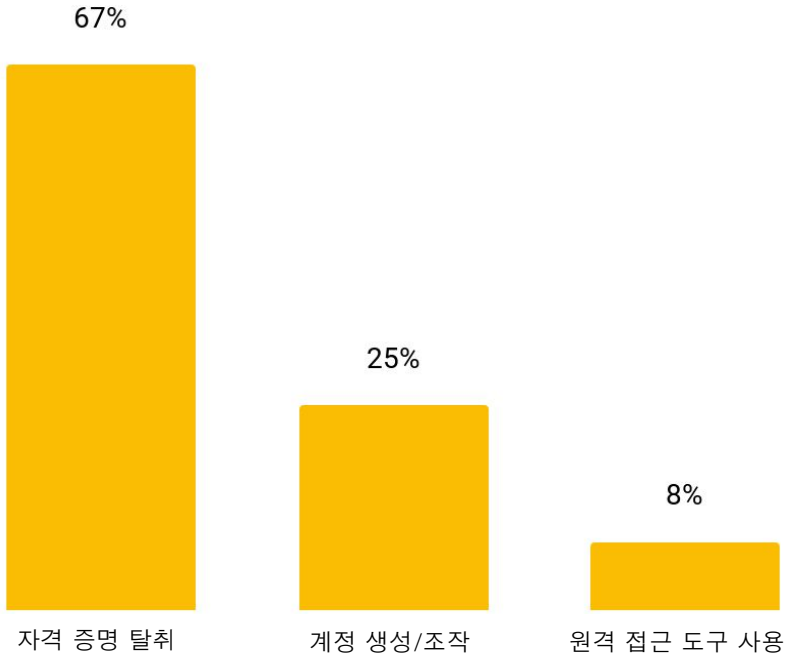
2. 공격 지속

지속성이 관찰된 사례에서 가장 많이 사용된 악성코드/도구/기법은 다음과 같습니다:

이름	설명
AnyDesk	원격 데스크톱 접근 소프트웨어
Webshell	원격 접근 및 명령 실행 스크립트
Level RMM	원격 데스크톱 접근 및 모니터링 소프트웨어
psexesvc.exe	원격 명령 실행 도구 (LOLBin)
Meshagent	원격 데스크톱 접근 소프트웨어
ScreenConnect	원격 데스크톱 접근 소프트웨어
SplashTop	원격 데스크톱 접근 소프트웨어
Abuse of VPN	VPN 접근 권한을 활용한 침투 기법
schtasks.exe	예약 작업/잡 스케줄러 (LOLBin)

3. 권한 상승

권한 상승 발생 케이스 분석 결과:



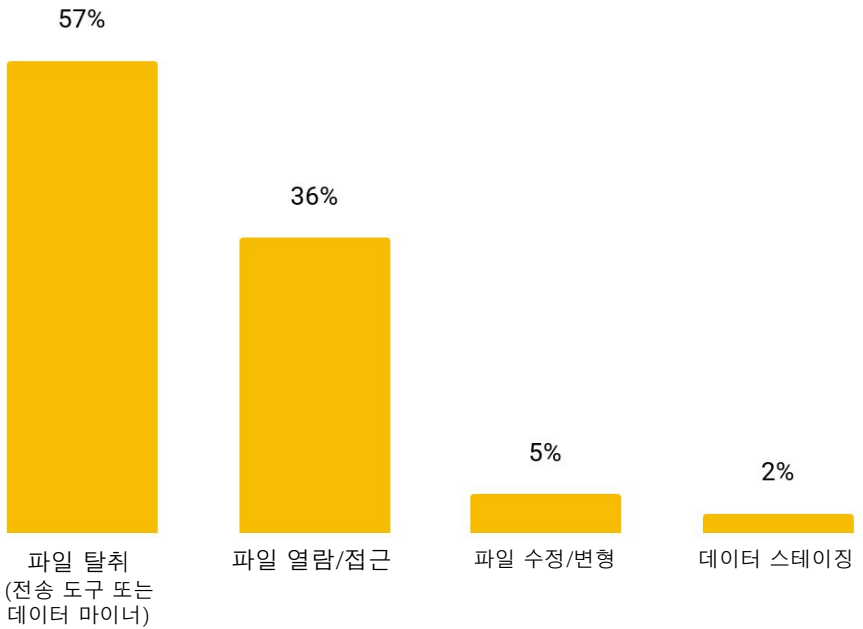
권한 상승에 사용된 도구/기법:

이름	설명
Mimikatz	자격 증명 탈취 도구
LSASS Dump	자격 증명 추출 기법
TruffleHog	코드 저장소 스캔 도구
OpenSSH Authentication Agent	SSH 인증용 개인 키 저장 프로그램
Net User Command	사용자 계정 관리 명령어

cybereason

4. 데이터 위협

데이터 위협 발생 케이스 분석 결과:

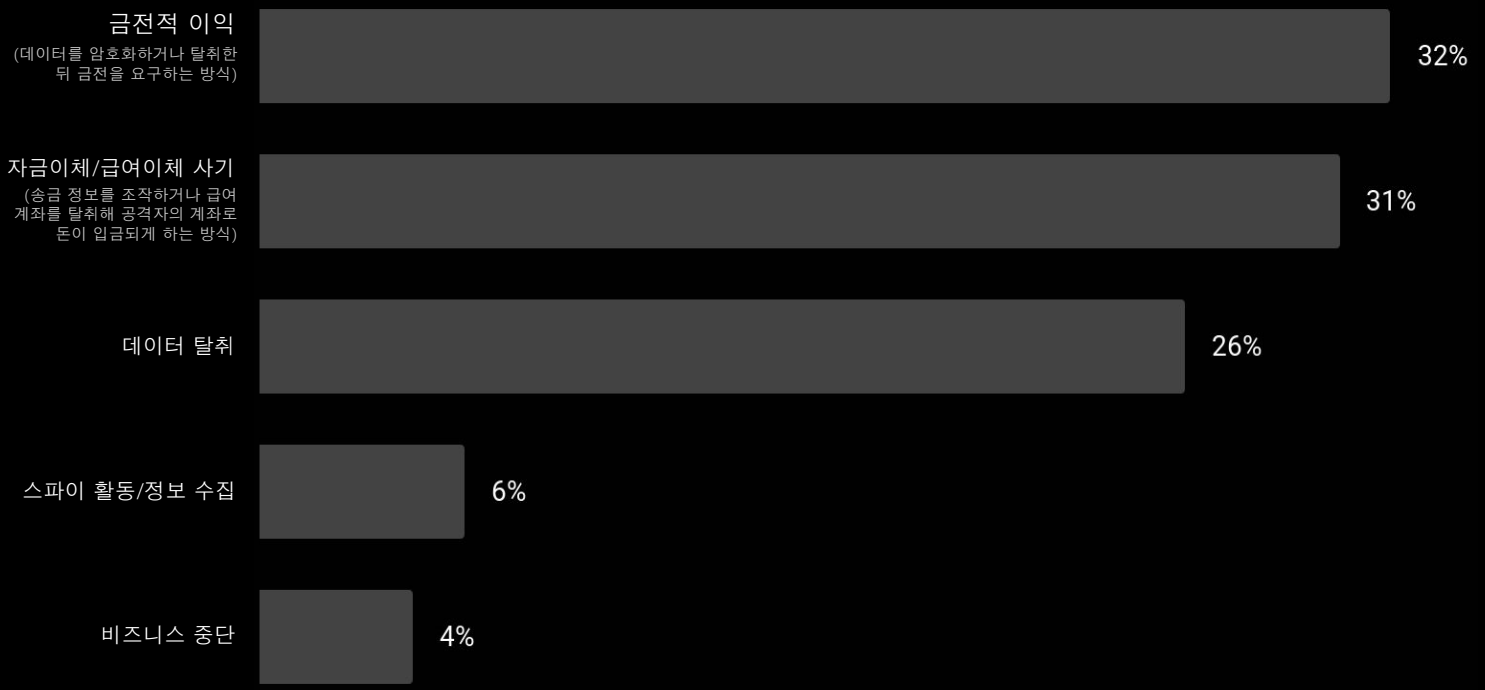


데이터 위협에 사용된 도구/기법:

이름	설명
RClone	파일 관리용 커멘드 라인 프로그램
WinSCP	오픈소스 SFTP 클라이언트
couchdrop.io	SFTP 서버 및 클라이언트
WinRAR	파일 압축 및 아카이빙 소프트웨어
Exfiltration Over C2 Channel	명령제어(C2) 채널을 통한 데이터 전송 기법

cybereason

5. 공격자의 최종 목표



cybereason

Cybereason

cybereason

신뢰도 높은 사고 대응 팀

사이버리즌은 사이버 보안 대비 및 회복력을 높이기 위한 최고의 전문성을 제공합니다.

실전에서 입증된 전문성

7000+ 건
침해 사고 대응 조사 수행

200K+ 시간
공격 보안 활동 경험

~500 건
시뮬레이션 훈련(테이블탑 연습) 진행

수백 개의 법률회사 및 보험사와 협력 관계 유지

통합 노출 관리

300+ 명의 전문가
인프라, 애플리케이션, 시스템, 엔드포인트뿐만 아니라 OT(Operational Technology), IoT(Internet of Things) 및 신기술 역량 보유

60+ 엘리트 DFIR팀
eDiscovery(전자 증거 수집), 데이터 검토, 침해 사고 알림 및 전문 증언 제공

고급 위협 인텔리전스 및 보안 연구

30K+
연간 발견된 취약점 수

6M+
관리하는 엔드포인트 수

MXDR 플랫폼
수백 개의 클라우드, SaaS, EDR *Telemetry 수집

*telemetry: 원격으로 데이터를 수집, 전송, 분석하는 기술

cybereason

사전 대비 & 사이버 복원력 솔루션

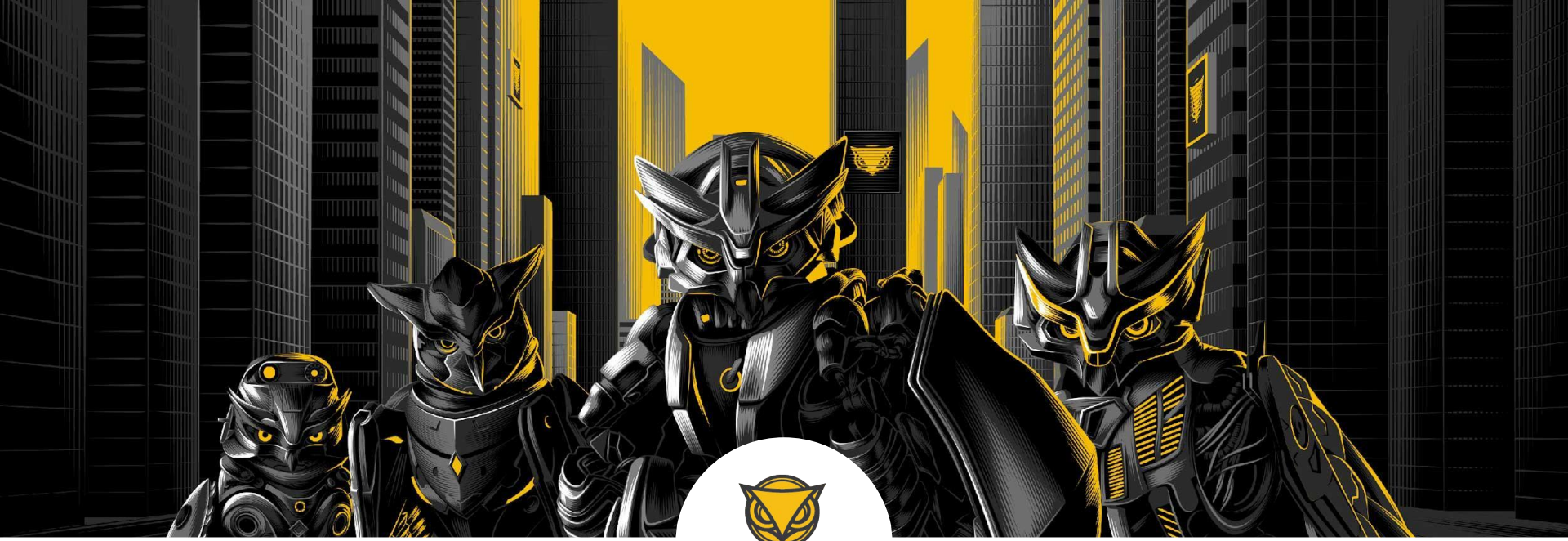
사이버리즌은 사이버 보안 사고의 전체 라이프사이클을 다루는 +50개 서비스를 제공합니다.

- 공격자 관점에서 보안 점검 및 평가
- 보안 상태 평가 및 자문 제공
- 거버넌스, 위험 및 규제 준수 관리
- 사이버 실사 평가
- 관리형 XDR

- 사이버 사고에 즉각 대응
- 시뮬레이션 기반 사고 대응 훈련
- 전자적 증거 수집 및 분석
- 법적, 기술적 지원을 위한 전문 증언 제공
- 침해 알림 서비스

- 피해 시스템 복구 및 보안 강화
- 손실된 데이터 복구
- 감염/손상 된 시스템 재구성
- 지속적인 운영 보장 계획 수립
- 효과적인 복구를 위한 기술 적용

사이버 복원력 유지 서비스



cybereason

[한국 솔루션 문의] ddi.marketing@doosan.com

24x7 expert assistance via response@cybereason.com

두산디지털이노베이션 은 사이버리즌(Cybereason)의 APAC 대표 파트너사로 엔드포인트, 클라우드 및 전체 엔터프라이즈 에코시스템 사이버보안에 앞장서고 있습니다.
컨설팅, PoC 및 구축, 기술 제공 뿐만 아니라 전문가 연동 및 고객 대응프로세스 수립까지 종합적인 지원을 제공합니다.