최근 국내 사이버공격 사례 및 대응방안

- the evolution of an attacker -

한국인터넷진흥원
디지털위협대응본부 위협분석단
박 용 규 단장

국내 주요 침해사고 타임라인

2024년 상반기

- 1월(계속) 거래소 및 개인대상 가상자산 유출
- 1월 지역 케이블 업체 , 비정상 트래픽 발생
- 1~5월 문자발송 중계서버 무단 발송
- 1월(계속) 중앙관리 및 암호화 솔루션 공급망 해킹
- 3~5월 알뜰폰 사업자 비대면 부정개통 사고

2024년 하반기 ~ 최근

- 6~7월 여행사. 법무법인 개인정보유출
- 6~10월 출판물류, 차량부품 제조사 랜섬웨어 감염
- 11월 핵티비스트, 정부·기업대상 디도스, 해킹
- 12월 '사회적 이슈(계엄)를 악용, 해킹메일 전파
- '25년 1~2월 리테일, 결혼 정보제공 업체 정보유출

정보유출	랜섬웨어	가상자산 해킹	공급망 공격	디도스(핵티비즘)
여행사, 법무법인, 리테일, 결혼업체 등 대상, 웹 취약점 및 크리덴셜스터핑 공격	제조업(차량부품, 에너지 등), 출판 물류기업 등 대상, 보안 관리가 미흡한 IT 자산(홈페이지, 그룹웨어 등) 집중 공격	개인소유 지갑 대상, 국세청 및 협력사 사칭 해킹메일 집중 공격	다수의 피해가 발생할 수 있는 SW 취약점 및 유지보수망 집중 공격	정부기관 및 기업 등 대상, 홈페이지 디도스 공격 및 취약한 스마트팜 관리 단말 무단 접속 공격

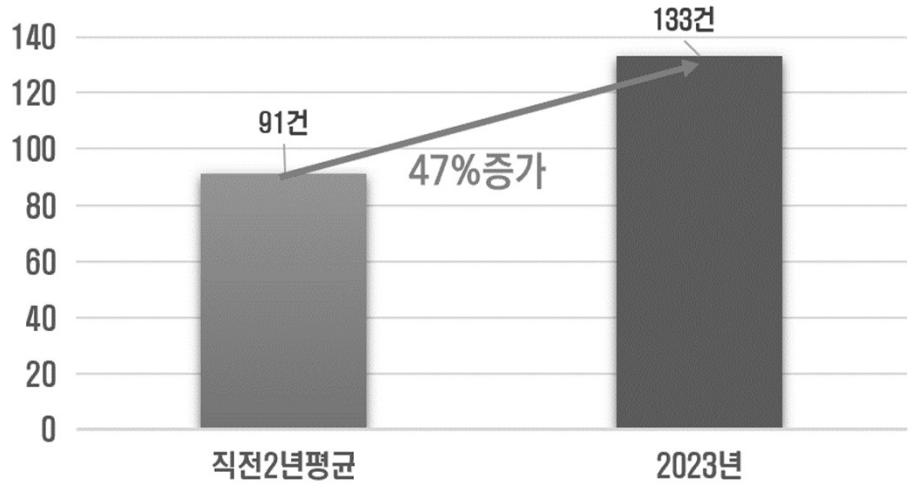
침해사고 특징·사례 – *더욱 은밀해지는 APT*

● **게이트웨이 장비,** 보안인증 SW, 중앙관리솔루션 **취약점을 적극활용**

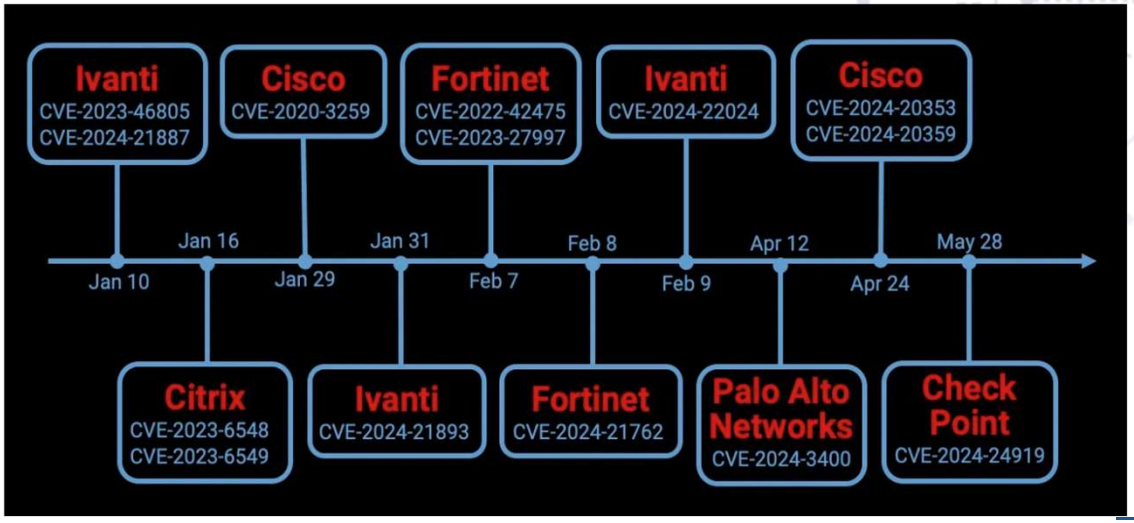
✓ **최초 침투**에 기업 내부(서버 팜)로 접속 할 수 있는 **게이트웨이(VPN 등) 장비 취약점**

(사례) 국내 화학 제조업, SI기업, 항공사와 최근 美 통신사와 정부기관 도청 등에 악용

< 최근 3년 VPN 취약점 증가율(socradar.io 블로그 참고) >



< 최근 주요 VPN 솔루션 취약점(socradar.io 블로그 참고) >



침해사고 특징·사례 – 더욱 은밀해지는 APT

● 게이트웨이 장비, **보안인증 SW**, 중앙관리솔루션 취약점을 적극활용

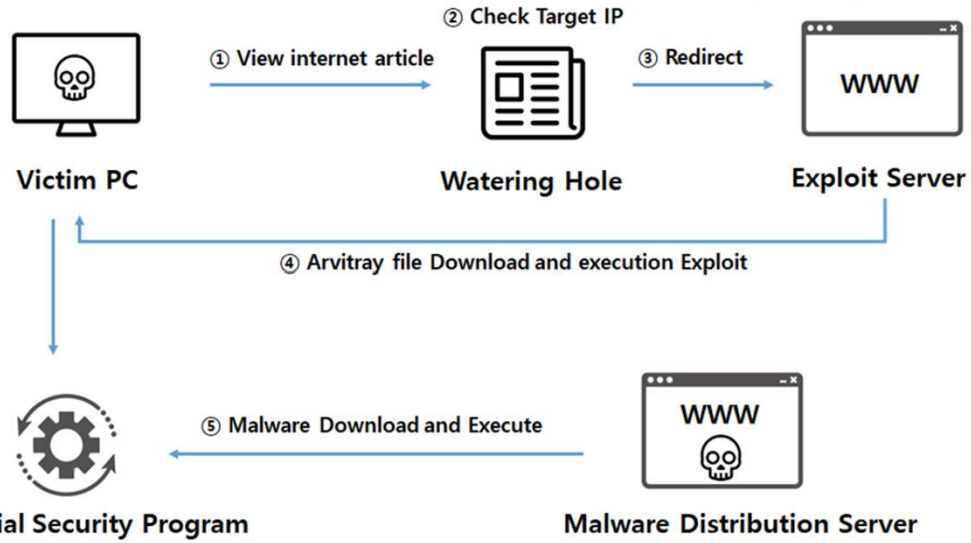
✓ **최초 침투**에 기업 내부(단말)로 접속 할 수 있는 **국내 보안인증 SW 취약점**

(감염경로) 취약한 SW가 설치된 단말의 사용자가 워터링홀 사이트 접속 시(언론, 커뮤니티 등) 감염

< KISA·보호나라 보안공지 - 보안인증SW 취약점 >

제목	게시일
라온시큐어 제품 보안 조치 권고	2024-08-09
예티소프트 VestCert 제품 보안 업데이트 권고	2023-12-13
드림시큐리티 MagicLine 취약점 보안 업데이트 권고	2023-03-21
이니텍 INISAFE CrossWeb EX V3 보안 업데이트 권고	2023-03-30
금융 보안 솔루션 업데이트 권고	2023-03-13

< 보안인증SW 취약점을 악용한 악성코드 감염사례 >



침해사고 특징·사례 – 더욱 은밀해지는 APT

● 게이트웨이 장비, 보안인증 SW, 중앙관리솔루션 취약점을 적극활용

✓ **내부 전파에 악성코드를 배포할 수 있는 중앙관리솔루션 취약점**

(감염경로) 제조사, 개발사의 업데이트 공급망을 통해 감염, 중앙관리솔루션 보안관리 미흡으로 외부 노출

< 사고에 주로 악용되는 중앙관리솔루션 >

< KISA·보호나라 보안공지 - 중앙관리솔루션 취약점 >

제목	게시일
이스트시큐리티 제품 보안 업데이트 권고	2024-07-11
OfficeKeeper 제품 보안 조치 권고	2024-04-19
엠엘소프트 Tgate 제품 보안 업데이트 권고	2024-02-21
닥터소프트 NetClient6 제품 보안 업데이트 권고	2024-01-04
휴네시온 제품 보안 업데이트 권고	2023-12-28
지니언스 NAC 제품 보안 업데이트 권고	2023-08-01

침해사고 특징 – 더욱 은밀해지는 APT

- **LotL** (Living off the Land) 공격기법 - 시스템에 설치된 정상 프로그램을 활용
- **DLL Side Loading** 공격기법 - 정상 프로그램 실행 시, 악성코드(DLL)를 함께 동작

(DLL 호출방식 악용) ① 프로그램이 로드된 디렉토리 ②시스템 디렉토리
③ Windows 디렉토리 ④ 현재 디렉토리 순서

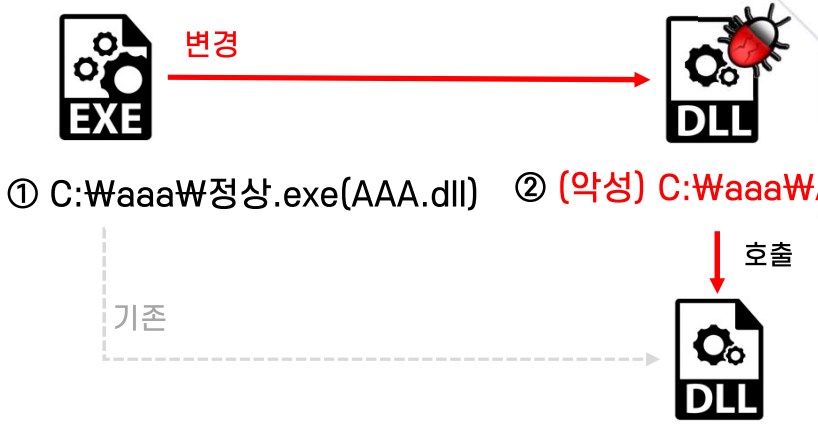
< 주로 사용되는 시스템 명령어(LotL 공격) >

Joint Guidance: Identifying and Mitigating Living Off the Land Techniques (cisa.gov)

cmd.exe, wmic.exe, Mshta.exe
powershell.exe, Sc.exe , at.exe,
PsExec.exe Ntdsutil.exe, Reg.exe,
lsass.exe, net.exe, dsquery.exe,
ipconfig.exe, dnscmd.exe,
nslookup.exe, Netsh ……

원격실행, 패스워드 탈취, 서비스 등록, 내부이동,
방화벽 설정변경, 시스템 정보 확인 시 등 사용

< DLL Side Loading 기법 >

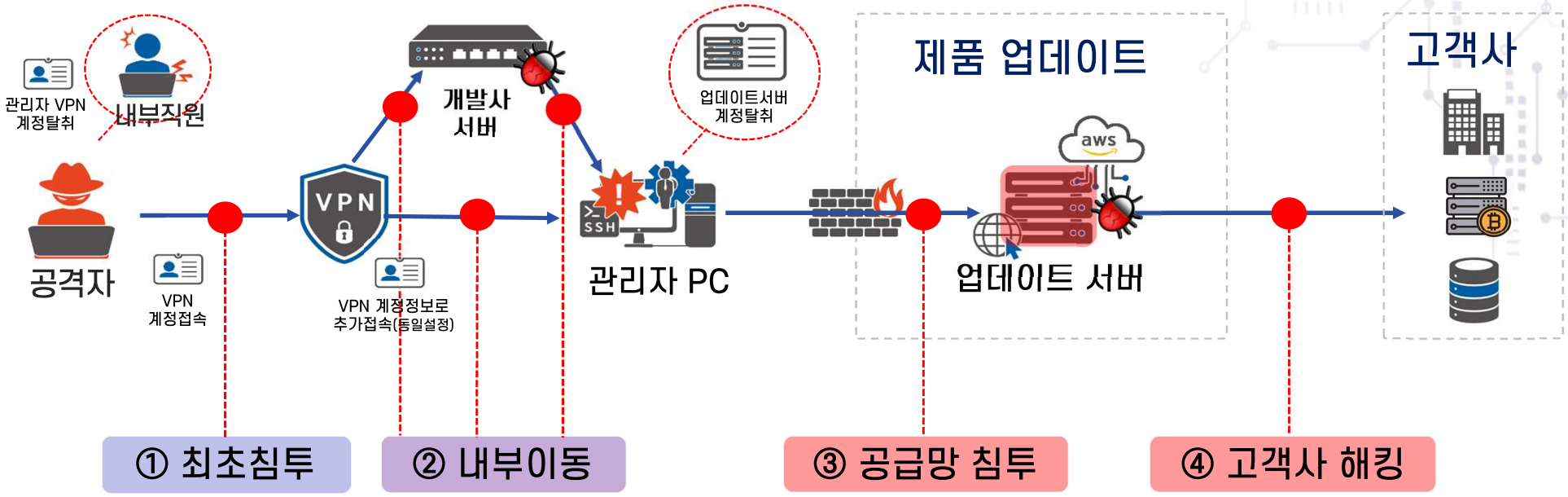


[참고] 대표적 공급망 침해사고 발생 패턴

상대적으로 보안 수준이 낮은 기업을 대상으로 공격

고객사 공격 무력화(탐지/차단) → SW(ERP 등) 개발사 → SW 취약점 발굴 → 취약점 활용 침투 → 공격

해킹 공격 대응역량 보유 고객 | *스타트업, 영세/중소기업 등* | *개발자 정보 활용 소스코드 정보 탈취 등* | *0-Day, 1-Day, N-Day*



침해사고 특징·사례 – 생성형 AI를 활용한 해킹 공격 본격화!

KISA Korea Internet & Security Agency

AI 모델(서비스, 프롬프트 등) 취약점 공격 시도 보다는 공격 대상의 **정보 수집과 피싱, 해킹도구 개발, 가짜 뉴스 생산 등에 중점** 이용

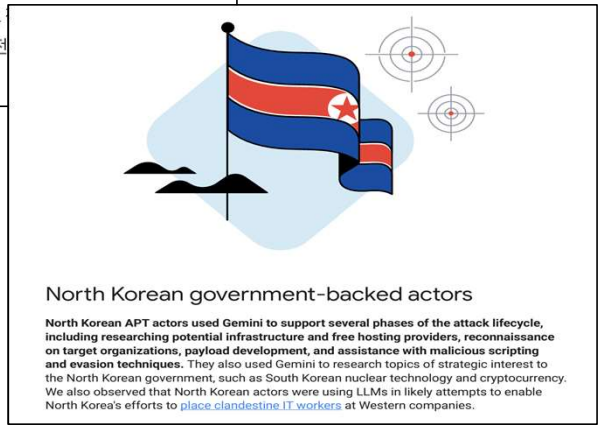
오픈AI(OpenAI)가 자사 AI 챗봇인 챗GPT(ChatGPT)를 악용한 20건 이상의 사이버 공격을 차단했다고 공식 발표했다.

이번 발표는 생성형 AI 도구가 악의적 사이버 활동을 강화하는 데 사용되고 있다는 첫 공식 확인 사례로 기록됐다. 오픈AI는 중국과 이란을 포함한 여러 국가 지원 해커 그룹들이 챗GPT를 활용해 악성 소프트웨어 개발, 피싱 공격, 악성코드 디버깅, 탐지 회피 등 다양한 사이버 공격을 실행했다고 밝혔다.

중국의 사이버 첩보 위협 그룹으로 알려진 스위트스펙터(SweetSpecter)는 2023년 11월 처음으로 Cisco Talos 분석가들에 의해 문서화된 그룹으로, 아시아 정부를 표적으로 활동해왔다. 오픈AI는 이들이 오픈AI 직원을 대상으로 지원 요청으로 위장한 악성 ZIP 파일을 포함한 스피어 피싱 이메일을 발송해 공격을 시도했다고 밝혔다. 이러한 첨부파일을 열면 슈가고스트(SugarGh0st) RAT이 피해자의 시스템에 설치되었다.

또한, 오픈AI는 스위트스펙터가 챗GPT 계정을 클러스터로 사용해 스크립트 [illegible] 했다고 보고했다. 이들은 취약점 검색, 로그4셸(Log4Shell)과 같은 특정 버전 셸 업로드 방법 등 다양한 악성 활동을 챗GPT의 도움으로 수행했다.

< 챗 GPT 악용 사이버 공격, 20건 이상 차단됐다 (출처:`24.10월, 데일리시큐) >

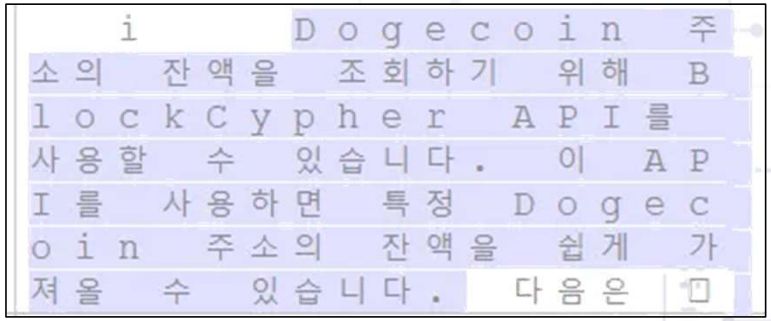


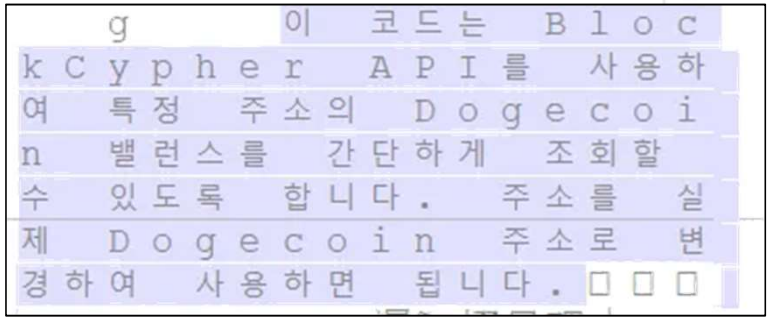
North Korean government-backed actors

North Korean APT actors used Gemini to support several phases of the attack lifecycle, including researching potential infrastructure and free hosting providers, reconnaissance on target organizations, payload development, and assistance with malicious scripting and evasion techniques. They also used Gemini to research topics of strategic interest to the North Korean government, such as South Korean nuclear technology and cryptocurrency. We also observed that North Korean actors were using LLMs in likely attempts to enable North Korea's efforts to place clandestine IT workers at Western companies.

< 구글 AI를 악용한 공격자 행위 (출처:`25.1월, 구글) >

< 국가배후 공격조직의 챗GPT 활용 >



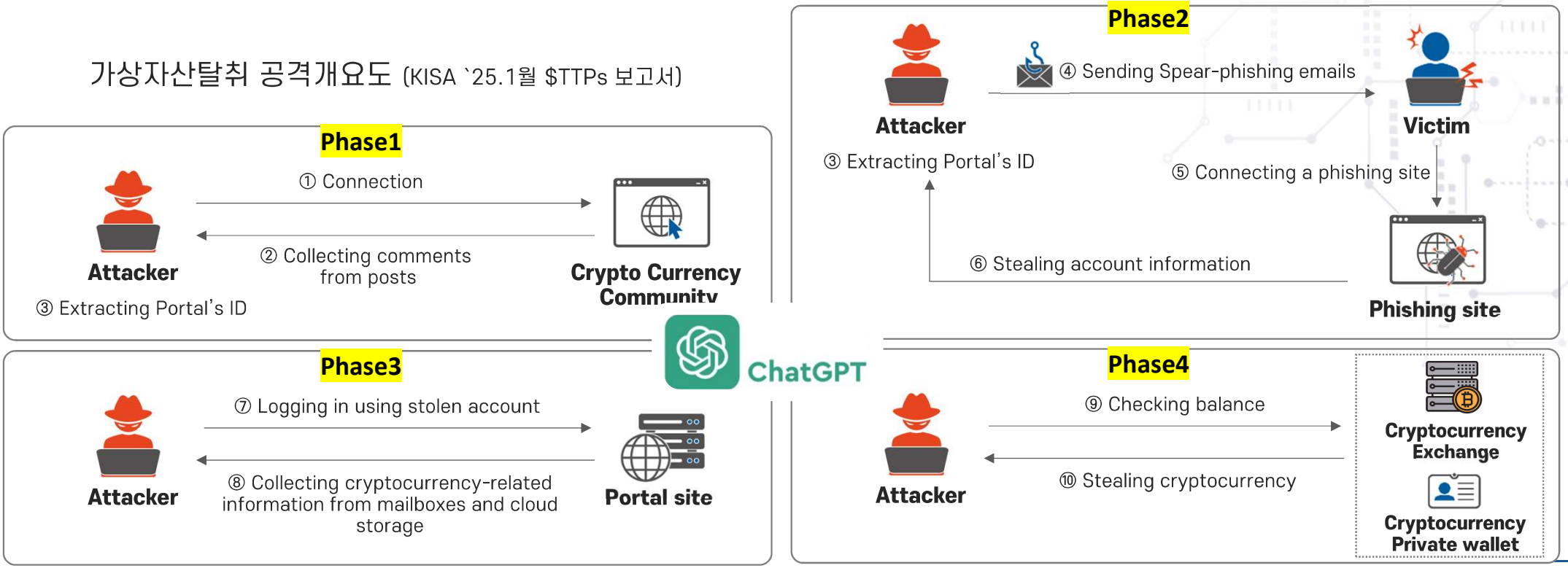


침해사고 특징·사례 – 생성형 AI를 활용한 해킹 공격 본격화!

가상자상에 관심이 많은 개인을 대상으로 가상자산탈취 공격 기승

Phase1 공격대상 물색(→ID수집) → **Phase2** 피싱메일 발송(→계정탈취) → **Phase3** 메일 부정 접속(→가상자산정보수집) → **Phase4** 가상자산탈취

가상자산탈취 공격개요도 (KISA `25.1월 $TTPs 보고서)



침해사고 특징·사례 – 생성형 AI를 활용한 해킹 공격 본격화!

KISA Korea Internet & Security Agency

ChatGPT 질문으로 생성된 카테고리

Phase1 – 공격 대상 정보 수집

- ✓ 회원정보 추출 코드 제작
- ✓ HTML 파싱 파이썬 코드 제작

Phase2~3– 피싱 메일 제작 및 가상자산 정보수집

- ✓ 네이버 메일의 정규식 표현
- ✓ HTML 공백 코드, 에러코드 구문해석
- ✓ Winscp으로 XAMPP 설치
- ✓ 크롬 브라우저 크롤링 예제

Phase4 – 가상자산탈취를 위한 코인 정보 수집

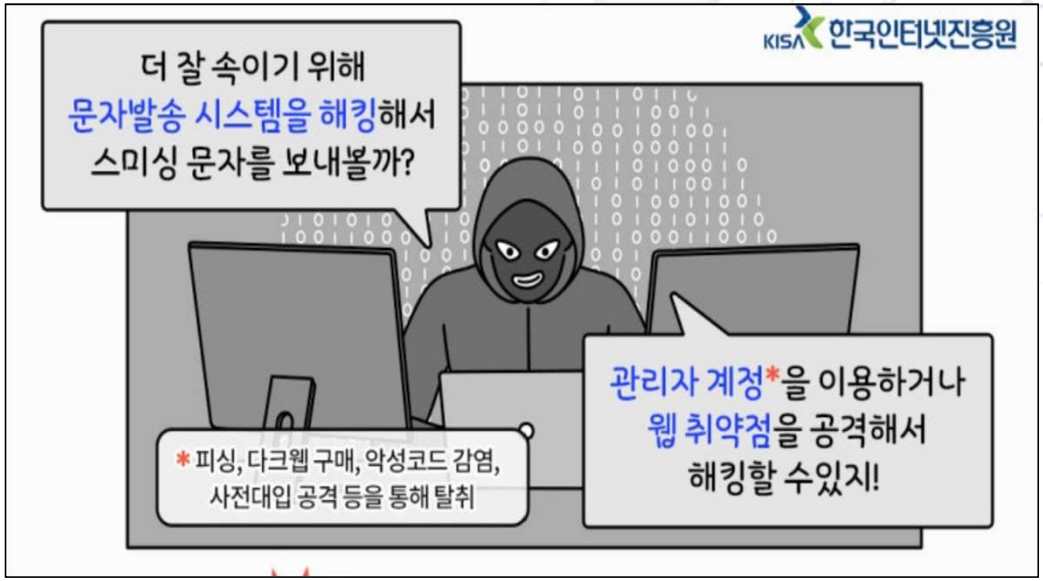
- ✓ Ontology 지갑 잔액 조회
- ✓ ONT 밸런스 조회 코드
- ✓ 비트코인 자동전송 파이썬 코드
- ✓ 바이낸스 APT 자산 밸런스
- ✓ Ripple 주소 유효성 확인
- ✓ Bitget API 조회 코드
- ✓ MEXC API 밸런스 조회
- ✓ 비트코인 자동전송 파이썬 코드

침해사고 특징·사례 – 서민경제 위협 사이버 사기 기승

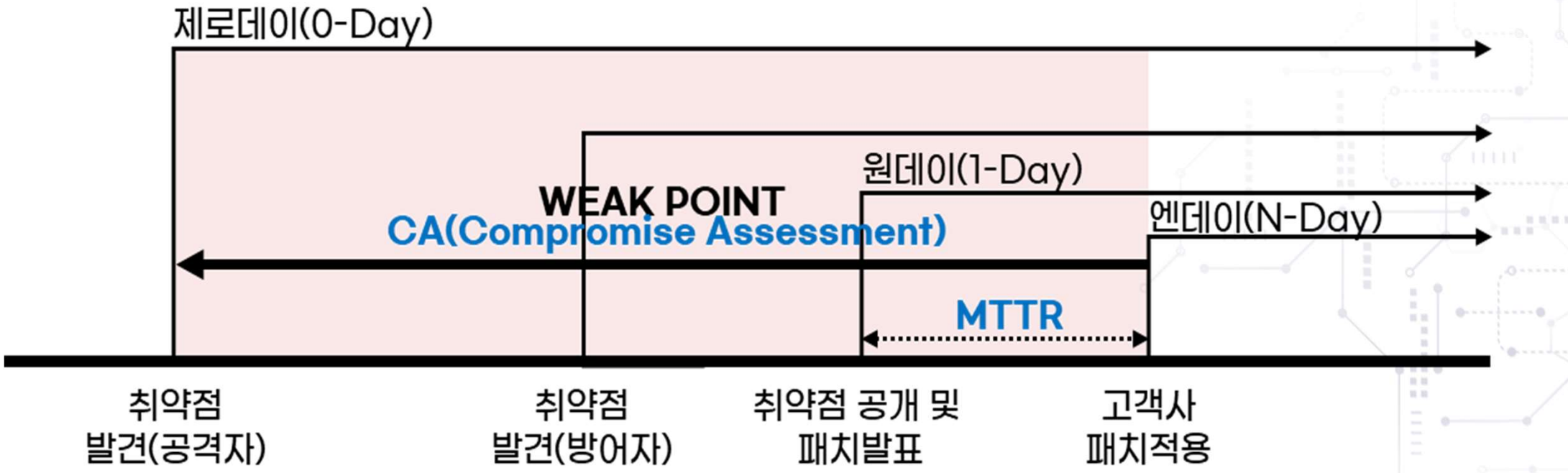
- **알뜰폰 비대면 개통 과정의 취약점**을 악용한 개인 금융 자산 해킹
- **문자관리계정 탈취, 웹 취약점** 등이 존재하는 문자발송시스템 해킹 후 스미싱 유포
  - 지인(부고), 정부(체납, 이벤트), 사회이슈(여객기, 이커머스) 등 내용의 악성앱 URL 링크 포함

< 알뜰폰 비대면 부정 개통사고 (출처:KBS1뉴스,`24,3월) >

< KISA, 기업 문자발송시스템해킹 보안 공지(`24.2월) >



전략과 숙제 – *Find ? Discovery ?*



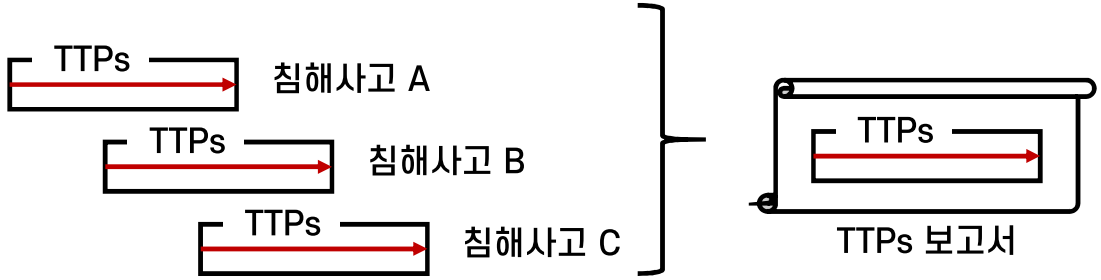
노출된 취약점 악용 공격 구간

보안공지(업데이트 권고)

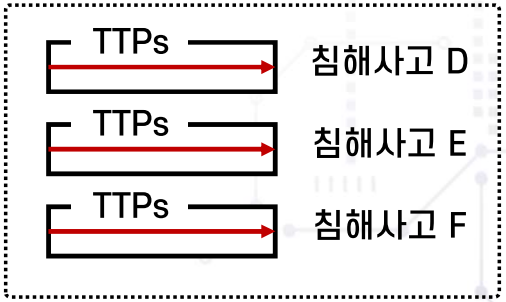
MTTR(Mean Time To Repair or Replace) : 복구 프로세스의 속도를 측정하고 시스템이 장애로부터 얼마나 빨리 복구할 수 있는지를 나타내는 고급 매트릭

전략과 숙제 – 현재 완료형 ? 현재 진행형?

- 침해사고 분석 **後** 공격자의 전략과 기술, 절차 등을 기술한 보고서(#TTP)

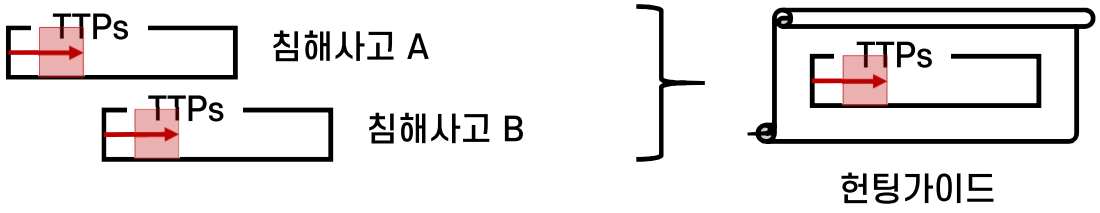


동일한 TTPs를 악용한 공격을 사전 예방



Add-on

- 침해사고 진행 중 실질적 **피해발생 前 개입, 피해를 막을 수 있는 헌팅가이드**

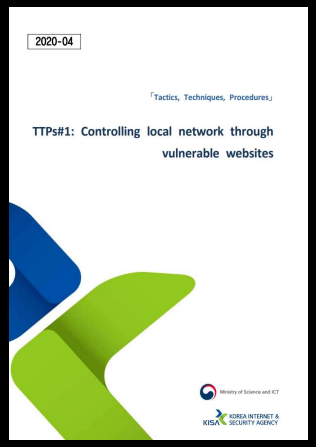


① 알지 못했던 침해사고 C, D를 헌팅하고

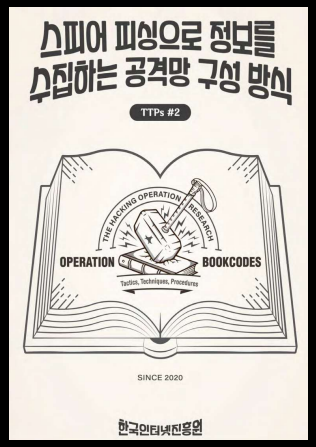
② 침해사고 C, D의 실제 피해발생을 사전 차단

전략과 숙제 - 무엇을 해야 하는가?

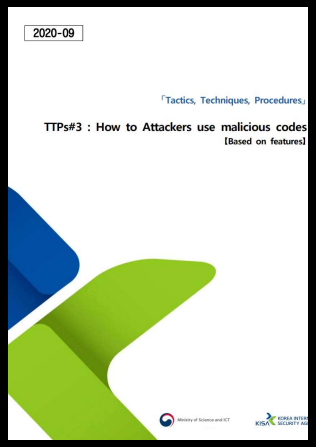
How to ——



TTPs#1

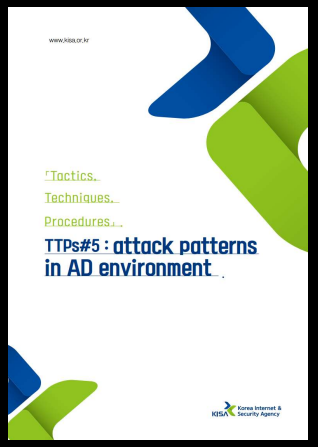


TTPs#2



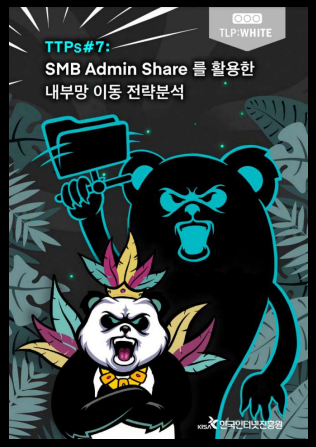
TTPs#3

TTPs#4

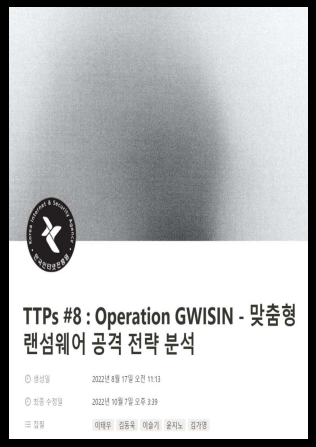


TTPs#5

TTPs#6

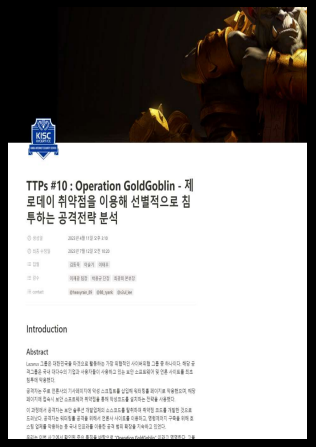


TTPs#7



TTPs#8

TTPs#9



TTPs#10

TTPs#11

TTPs $

전략과 숙제 – 공격자와 방어자 *間* 시소게임

공격전략의 변화

*새로운 전략보다는 **기존 전략을***

***지속적으로 확장**하며, 감염 성공률을 높임*

초기침투	워터링홀, 스피어피싱(해킹메일), 제로데이취약점(Zero-Day), …
악성코드	실행 인자 값, 레지스트리 검증, 악성코드 모듈화 등

대응전략

단발적인 조치보다는

***정교하고 세분화**된 방어 전략 필요!!*

ASM 모니터링 업데이트	공격자에게 노출될 수 있는 자산 식별·관리 공급망 중앙솔루션 강화 보안 패치 및 취약점 관리
이상행위 신속대응	비정상 경로에서 실행되는 파일 점검, 정상과 다른 크기의 파일 탐지, … 가시성 확보 및 대응 체계 구축, …

전략과 숙제 – *Key??*

KISA
Korea Internet & Security Agency

2024.7.19 UTC 04:09~ (한국시간 : 13:09~)

AirAsia passengers wait to be checked in manually at Kuala Lumpur International Airport after a global IT system outage, in Sepang, Malaysia, on Friday. (Hasnoor Hussain/Reuters)

BCP / DRP를 잘 준비한 곳이 금한 상황에서 살아 남는다!!!

Cybersecurity

Tesla halted some production lines due to global IT outage, Business Insider reports

* Business Continuity Planning / Disaster Recovery Planning

정보보호 무료서비스 활용 (1)

중소 · 영세 기업의 보안 강화 및 침해사고 예방 지원

SW 보안

- 정부·공공 개발 보안약점 진단 (웹, 모바일앱 등)
- 영세·중소기업 SW 보안약점 진단 서비스 (웹, 모바일앱, 솔루션)

보안점검

- 중소기업 IT인프라 보안 점검
- 서버 원격점검 (내서버 돌보미)
- 웹 취약점 점검

모의침투

- 모의침투 기반 보안취약점 점검

사이버대피소

- 디도스 사이버대피소
- 웹공격 방어

보안도구 보급

- 웹셸탐지도구 (휘슬)
- 웹방화벽 (캐슬)

모의훈련

- 해킹메일
- 디도스 공격방어
- 모의침투
- 공격탐지 대응

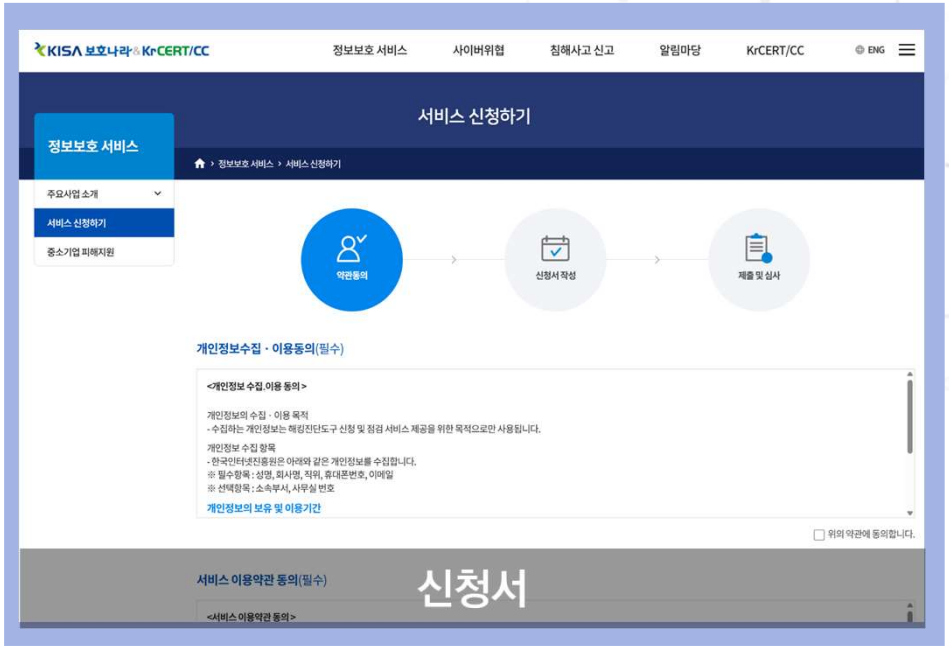
자가진단

- 영세·중소기업 서버 자가진단도구 보급

정보보호 무료서비스 활용 (2)

[공통] 사이버 침해사고 예방 서비스 이용신청 방법

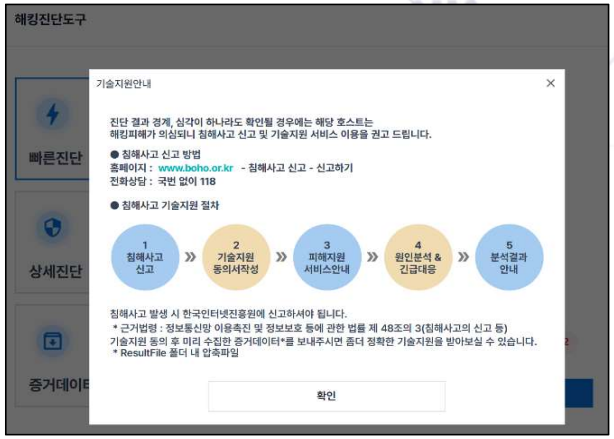
STEP 1	STEP 2	STEP 3	STEP 4
한국인터넷진흥원 보호나라 www.boho.or.kr	정보보호 서비스	서비스 신청하기	(온라인) 신청서 작성



정보보호 무료서비스 활용 (3)

기업 스스로 초기에 해킹 여부를 진단 할 수 있는 '해킹진단도구'

- **(수집) 침해사고 증거데이터 자동 수집**
  - 기업 운영 시스템 內 다양한 증거 데이터를 원클릭으로 손쉽게 수집(계정 생성, 원격접속기록, 시작 프로그램 등록, 로그 삭제 등)
- **(진단) 수집된 로그 등에 대해 해킹여부 탐지룰을 기반으로 분석·진단**
  - 비정상적으로 생성된 사용(관리자) 계정 탐지, 원격 관리도구 설치 여부 분석, 윈도우 시스템 이벤트 로그 삭제 여부 등
- **(결과) 분석 결과 리포팅**
  - 사용자가 시스템의 해킹여부를 직관적으로 판단할 수 있도록 3단계(심각:빨강, 위험:주황, 정상:녹색) 결과 제공
  - 담당자가 쉽게 이해할 수 있는 점검결과 보고서 제공
  - 분석결과에 따라 침해사고 신고 자동 안내



신청 방법

- hct@krcert.or.kr *or* 보호나라

KISA 한국인터넷진흥원

감사합니다

We Will be a Global Leader in the Internet & Security Field