랜섬웨어 예방 및
사이버 보안의 첫 걸음

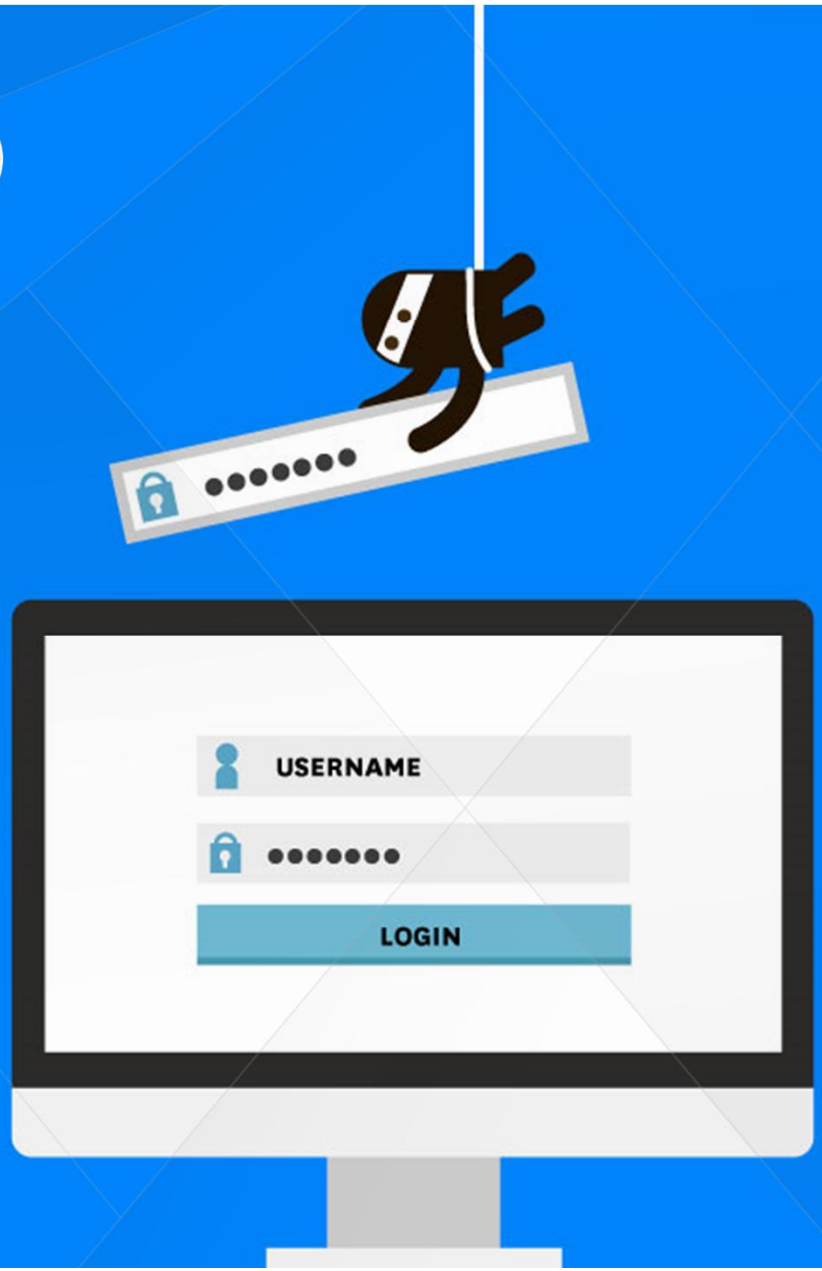
전사원을 교육하라!

악성코드의 종류와 해킹의 방법

악성코드의 종류와 역사

악성코드란 무엇인가요?

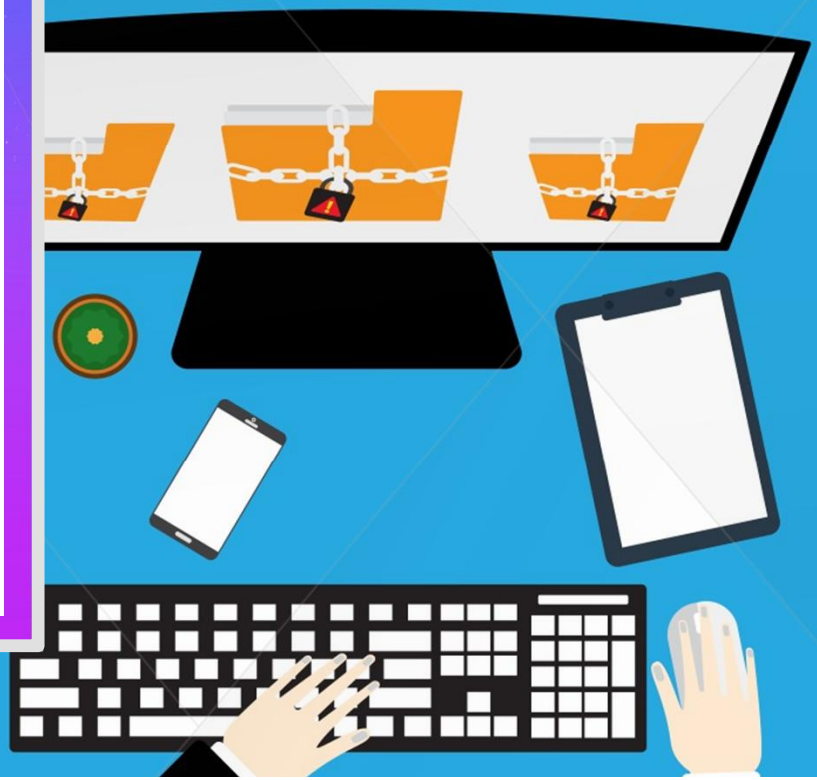
① 악의적인(Malicious) + 소프트웨어(Software)의 합성어
② 컴퓨터 시스템을 파괴하거나 정보를 유출하거나 허가 없이 시스템에 접속하는 행위등의 역할을 수행
③ 바이러스, 랜섬웨어, 웜, 트로이 목마, 루트킷, 스파이웨어, 애드웨어등과 같이 용도에 따라서 다양한 종류를 가지고 있음



악성코드의 종류와 역사

악성코드의 역사

1. 1972 Creeper Virus
2. 1974 Rabbit Virus
3. 1986 Brain Virus

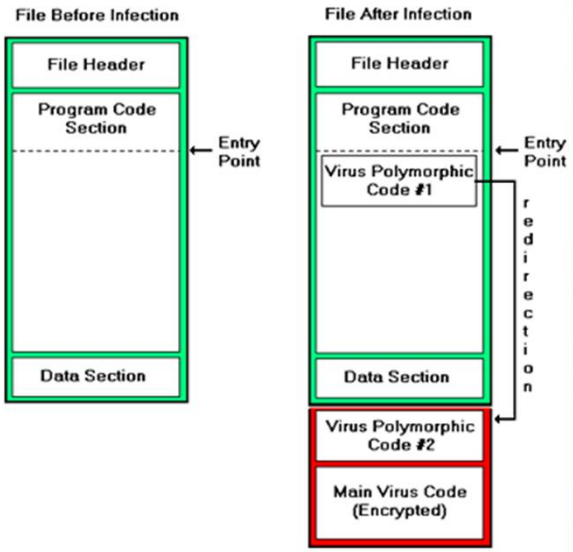


악성코드의 종류와 역사

바이러스(Virus)

① 정상 파일 변조, 숙주 역할의 파일이 필요

② 정상 파일에 악의적인 코드 삽입

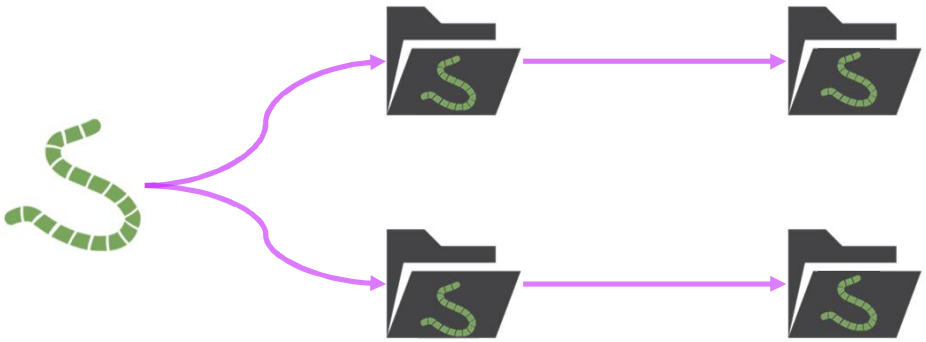


악성코드의 종류와 역사

웜(Worm)

① 자기 자신을 복사하는 형태의 악성코드

② 전파수단 : Network, e-mail, USB, SNS ..



악성코드의 종류와 역사

트로이목마(Trojan horse)

① 자기 복제 기능 없음

② 정상적인 프로그램으로 위장하고 있으나 사용자 모르게 악의적인 행위를 수행

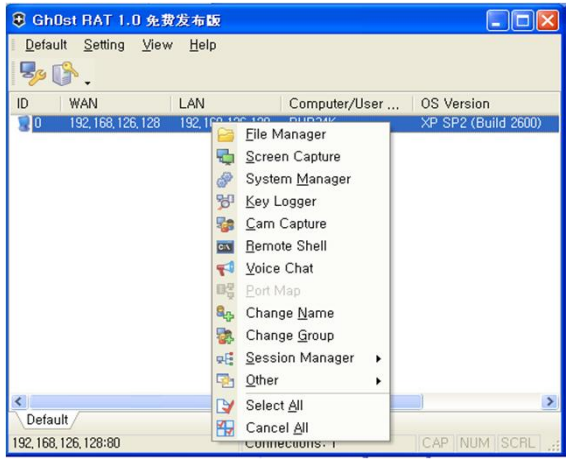
③ 가장 종류가 다양

악성코드의 종류와 역사

백도어(Backdoor)

① 사용자 모르게 감염 PC에 원격으로 접속

② 원격에서 명령 전달 및 수행



악성코드의 종류와 역사

애드웨어(Adware)

① 광고 목적의 소프트웨어

② 사용자의 입력값에 맞게 광고창 생성
및 검색 결과 조작

③ 국내의 경우 악성코드의
유포 경로로
자주 사용

악성코드의 종류와 역사

랜섬웨어(Ransomware)

Ransom

Ware

Ransomware

주로 이메일
및 악성링크
를 통해 감염

감염 시 시스템
내 문서파일들을
암호화

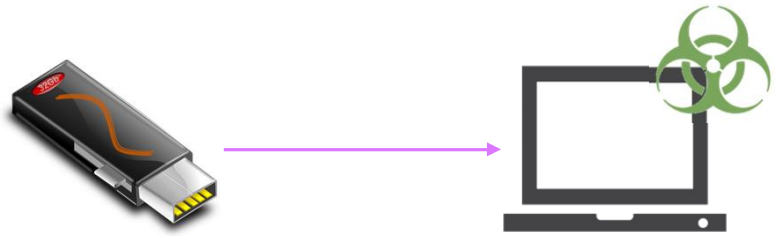
비용을 지불하여
복호화키를
받기 전까지 전체
파일사용 불가

어떻게 악성코드에 감염되는가?

이동식디스크를 통한 감염

① USB, SD Card, Smart phone

② autoruns.inf 파일에 의하여 악성코드 자동 실행



감염된 자동실행 파일(autorun)

어떻게 악성코드에 감염되는가?

이메일을 이용한 감염

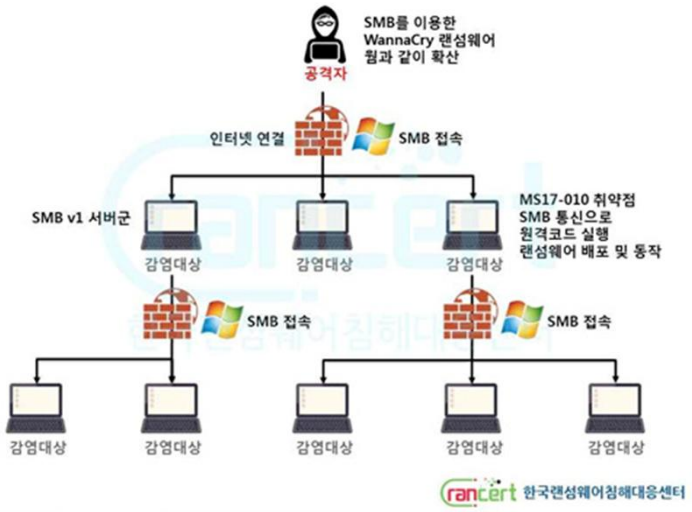
① 첨부 파일이나 본문 URL 링크를 이용하여 감염

② 스피어피싱 공격에 자주 사용

어떻게 악성코드에 감염되는가?

내부 네트워크를 이용한 감염

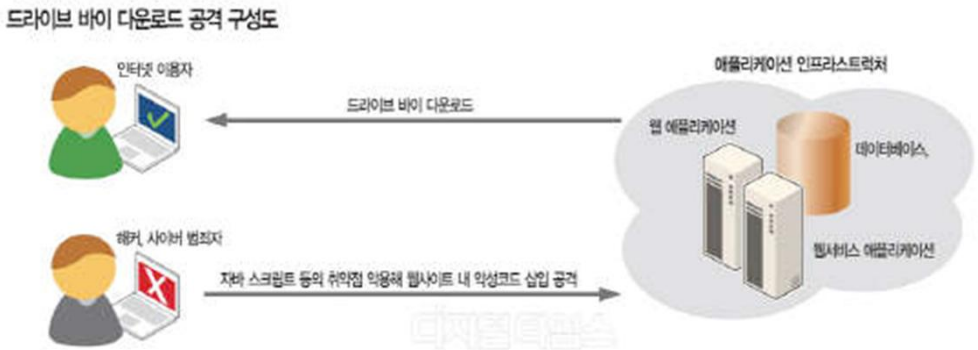
① 공유 파일, SMB, Exploit 등을 통한 감염

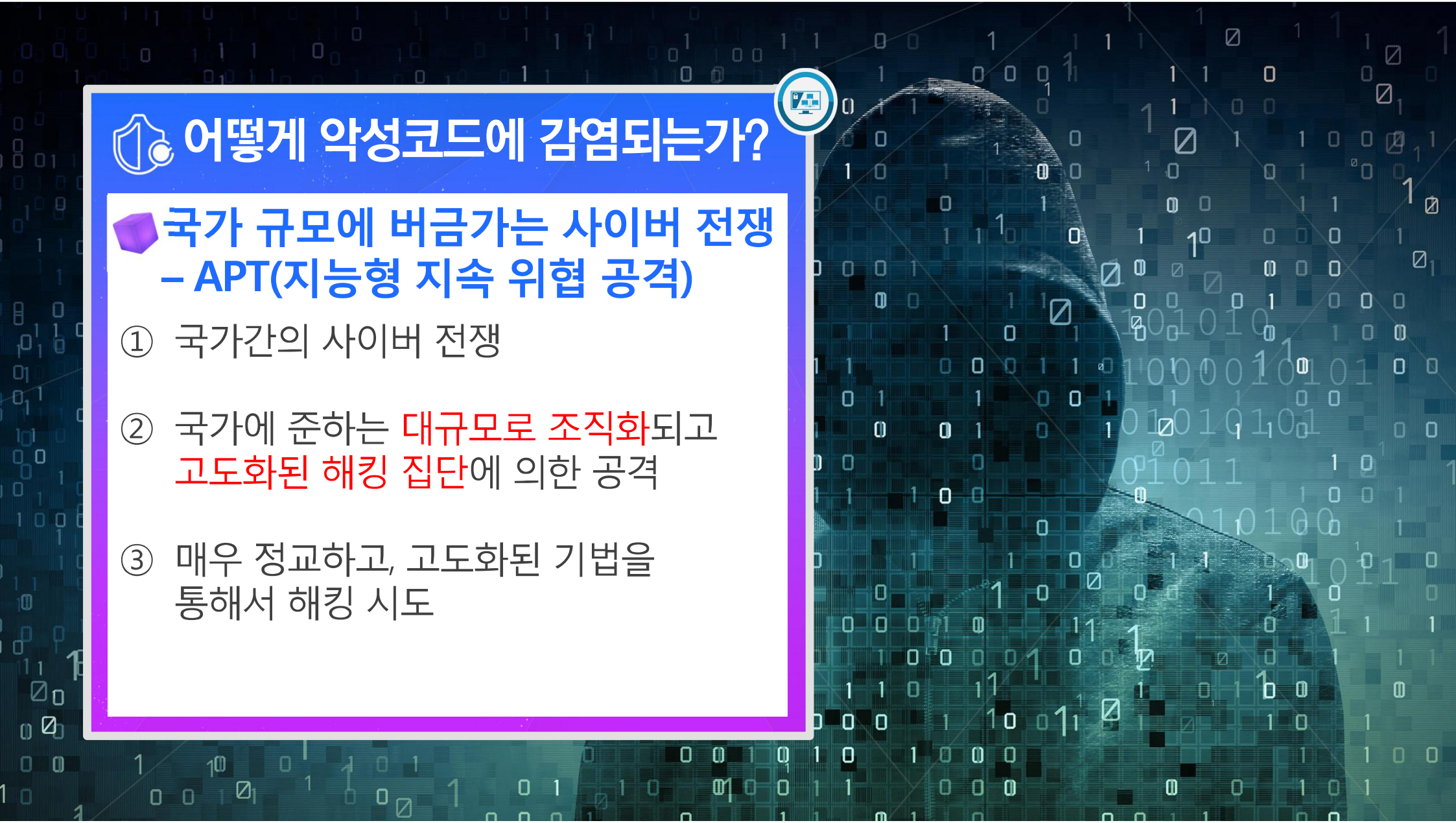


어떻게 악성코드에 감염되는가?

웹사이트 접속을 이용한 감염

① 사용자가 이용하는 프로그램의 취약성 이용




어떻게 악성코드에 감염되는가?
국가 규모에 버금가는 사이버 전쟁
– APT(지능형 지속 위협 공격)
① 국가간의 사이버 전쟁
② 국가에 준하는 대규모로 조직화되고
고도화된 해킹 집단에 의한 공격
③ 매우 정교하고, 고도화된 기법을
통해서 해킹 시도

어떻게 악성코드에 감염되는가?

국가 규모에 버금가는 사이버 전쟁 – APT(지능형 지속 위협 공격)


랜섬웨어 예방 및
사이버 보안의 첫 걸음
전사원을 교육하라!
왜 해커는 개인과 기업을 공격할까?

우리 회사는 안전할까?

사이버 보안은 대기업에만 해당 될까요?

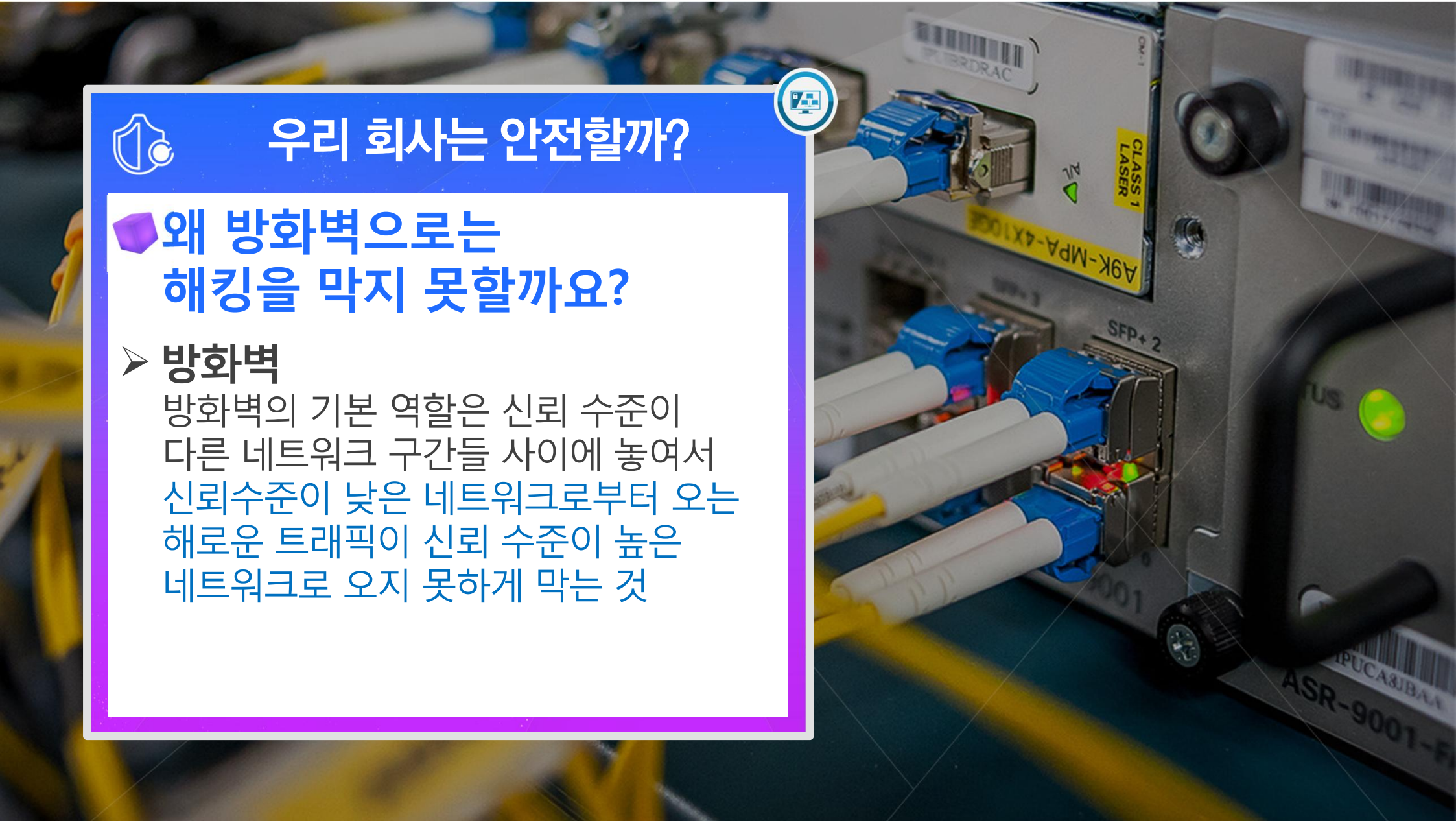
우리 회사에는 훔쳐갈게 없어...

방화벽하고 백신만 있으면 충분히 막을 수 있을거야...

뭐하러 비싼 장비를 사...장비가 다 똑같지 뭐...

사이버 보안 대응은 급할게 없어...다른걸 먼저 해야지...

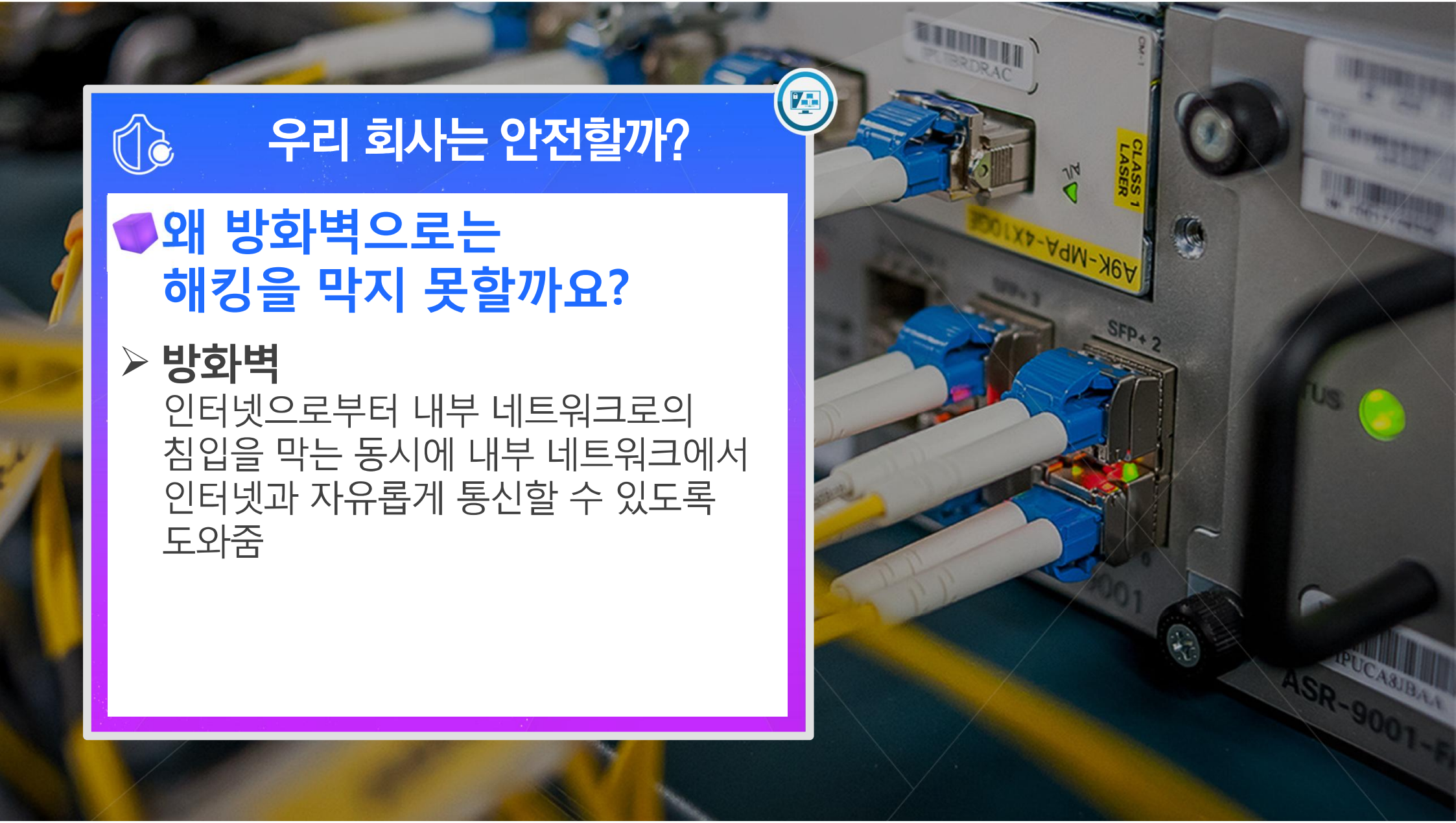
대부분의 중소기업 관점



우리 회사는 안전할까?

왜 방화벽으로는 해킹을 막지 못할까요?

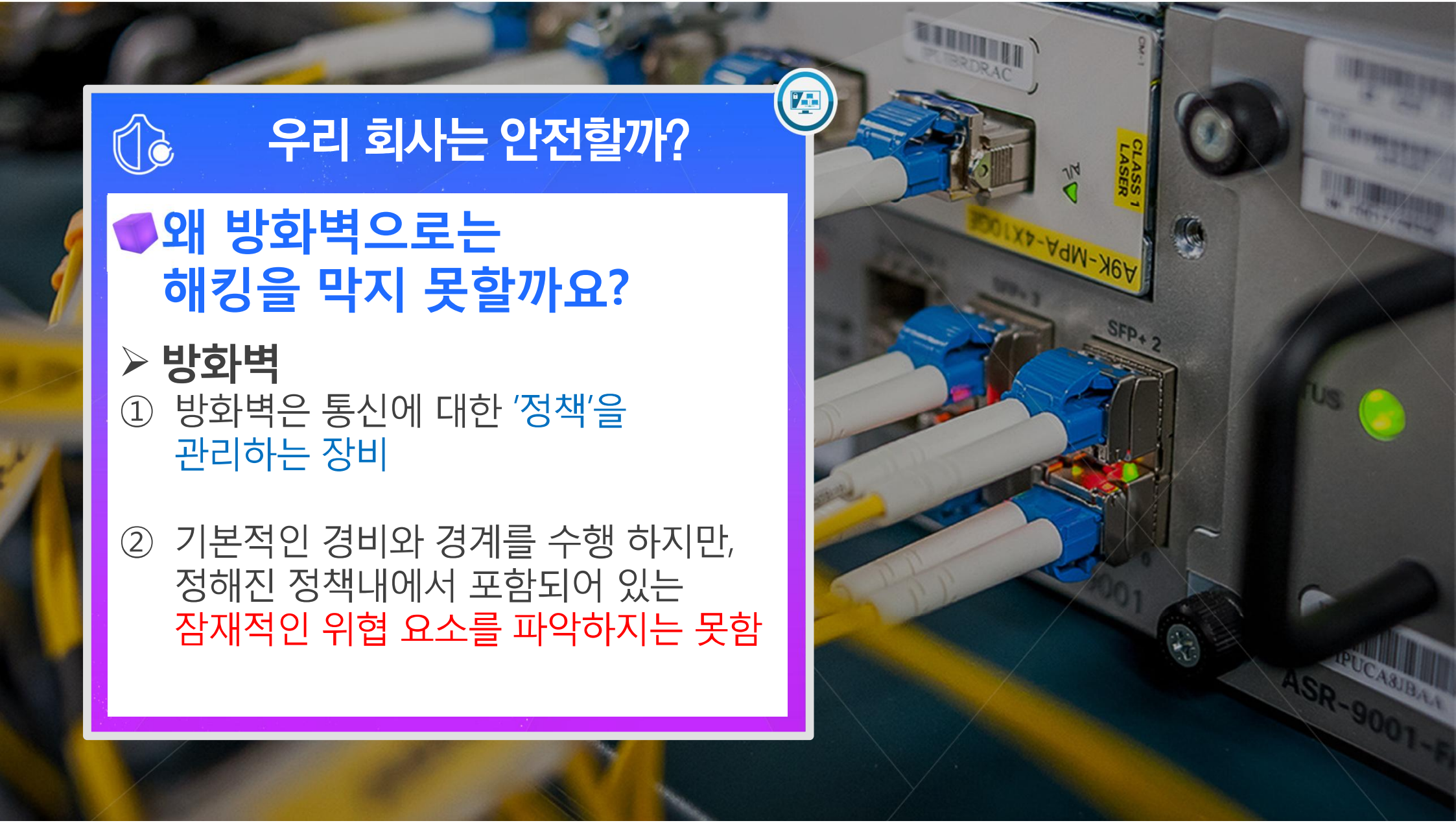
- **방화벽**
  방화벽의 기본 역할은 신뢰 수준이 다른 네트워크 구간들 사이에 놓여서 신뢰수준이 낮은 네트워크로부터 오는 해로운 트래픽이 신뢰 수준이 높은 네트워크로 오지 못하게 막는 것



우리 회사는 안전할까?

왜 방화벽으로는 해킹을 막지 못할까요?

- **방화벽**
  인터넷으로부터 내부 네트워크로의 침입을 막는 동시에 내부 네트워크에서 인터넷과 자유롭게 통신할 수 있도록 도와줌



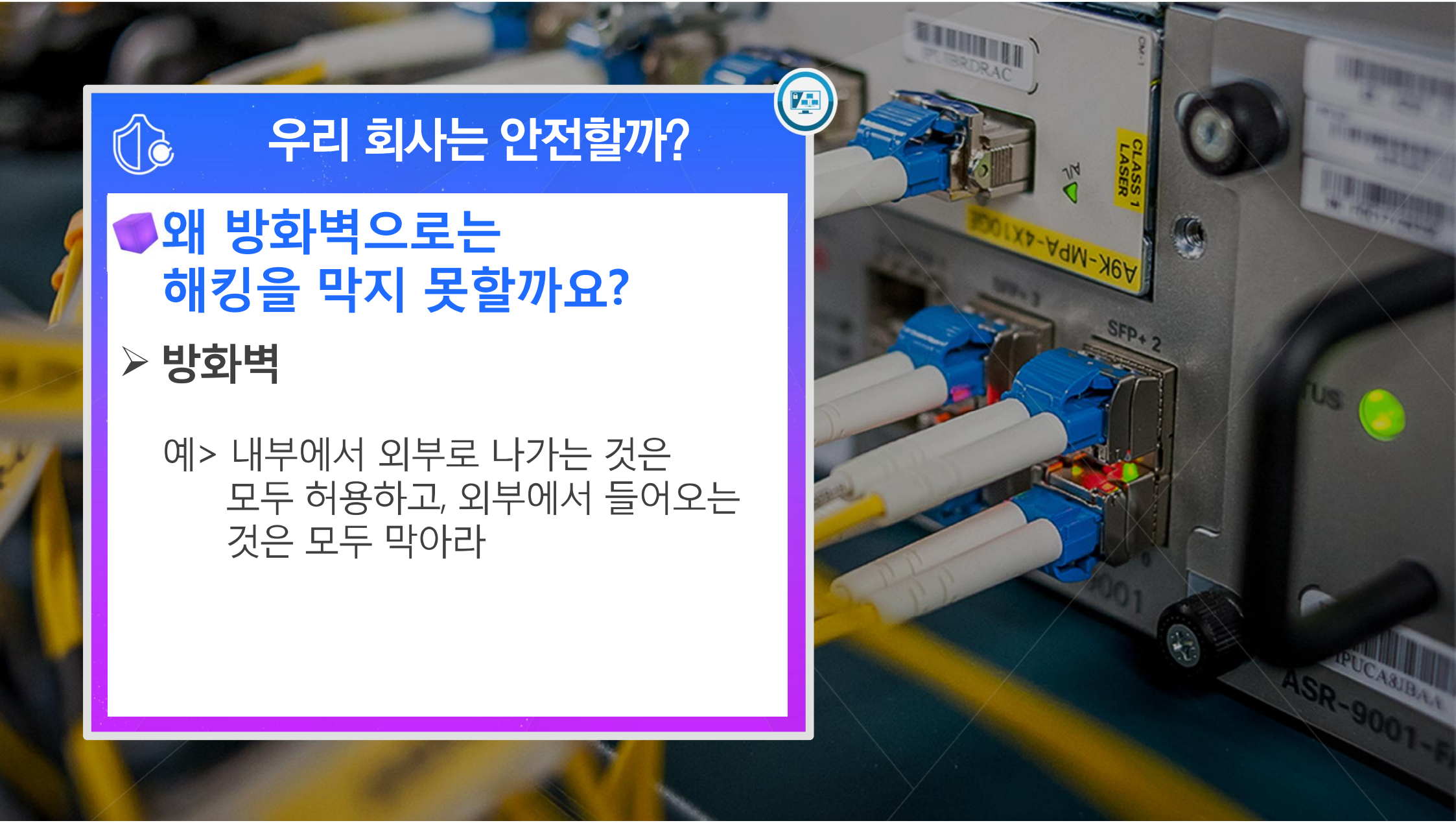
우리 회사는 안전할까?

왜 방화벽으로는 해킹을 막지 못할까요?

➢ 방화벽

① 방화벽은 통신에 대한 '정책'을 관리하는 장비

② 기본적인 경비와 경계를 수행 하지만, 정해진 정책내에서 포함되어 있는 잠재적인 위협 요소를 파악하지는 못함



우리 회사는 안전할까?

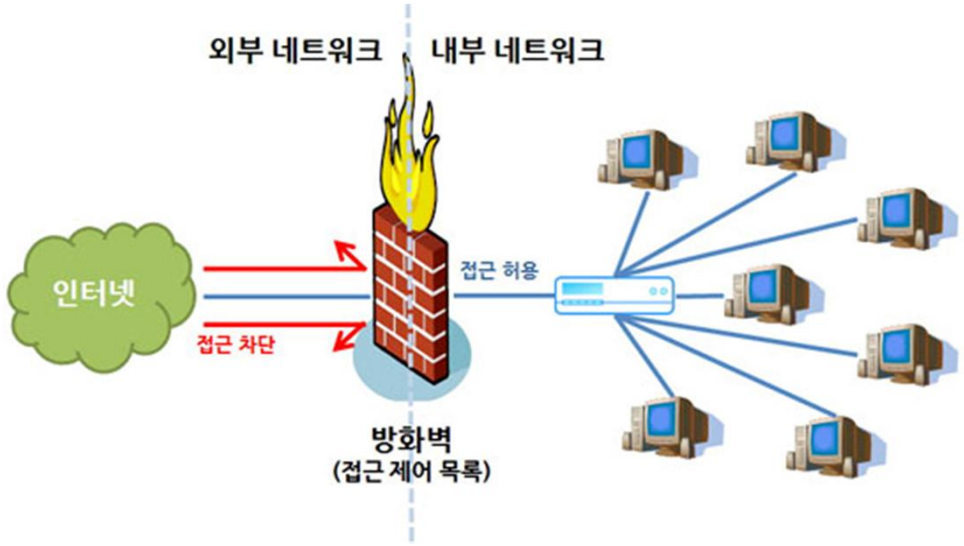
왜 방화벽으로는 해킹을 막지 못할까요?

- **방화벽**

예> 내부에서 외부로 나가는 것은 모두 허용하고, 외부에서 들어오는 것은 모두 막아라

우리 회사는 안전할까?

왜 방화벽으로는 해킹을 막지 못할까요?



우리 회사는 안전할까?

여러분의 데이터는 생각보다 중요합니다!

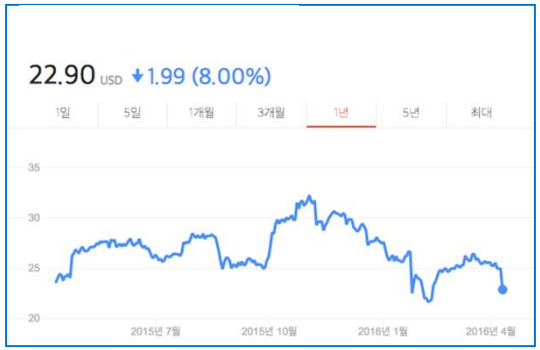
➢ **CASE #1**

미국의 한 유망한 중소 스타트업
소스코드 유출
동일한 서비스가 타 국가에서
절반 가격으로 출시
회사의 비지니스에 치명적 손실 초래

우리 회사는 안전할까?

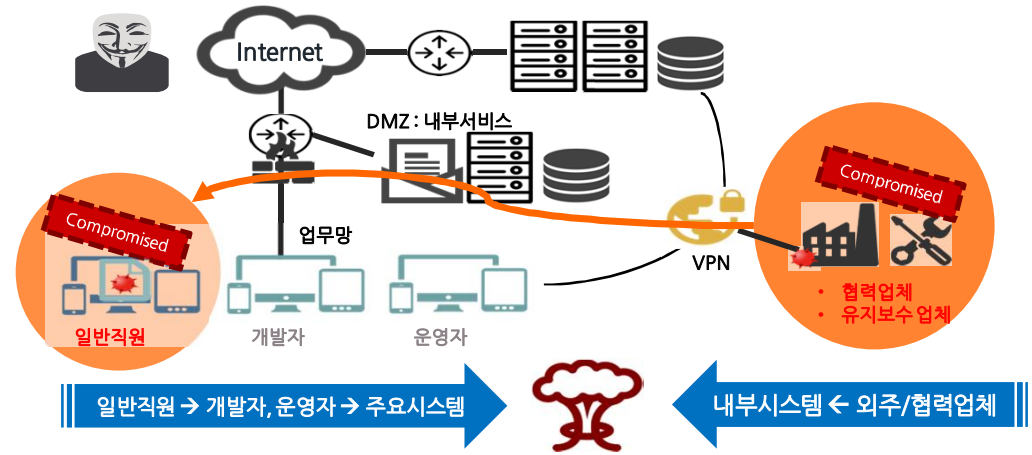
여러분의 데이터는 생각보다 중요합니다!

➢ CASE #2



우리 회사는 안전할까?

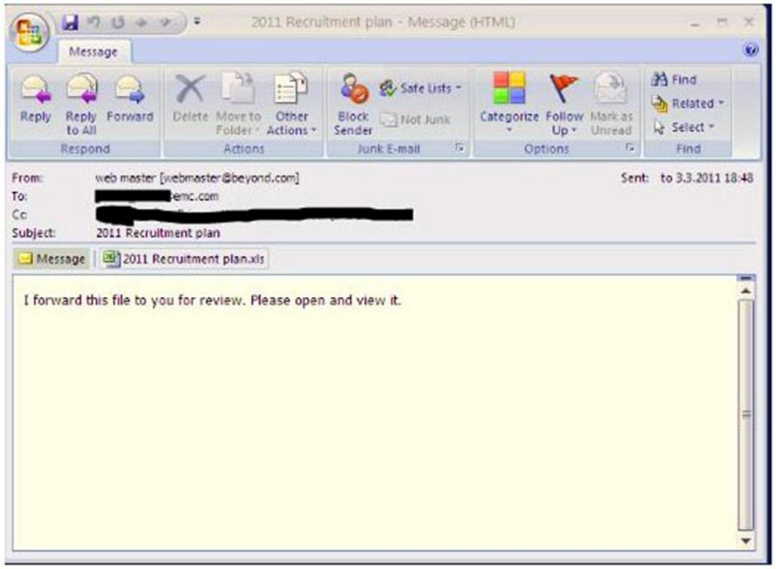
그래도 훔쳐갈게 없다고 생각하시나요?



내용 출처: 2016 파이어아이/맨디안트 M-Trend 레포트

우리 회사는 안전할까?

실제 사고 사례



개인 인증용 OTP(One Time Password)를
제조하는 회사를 공격

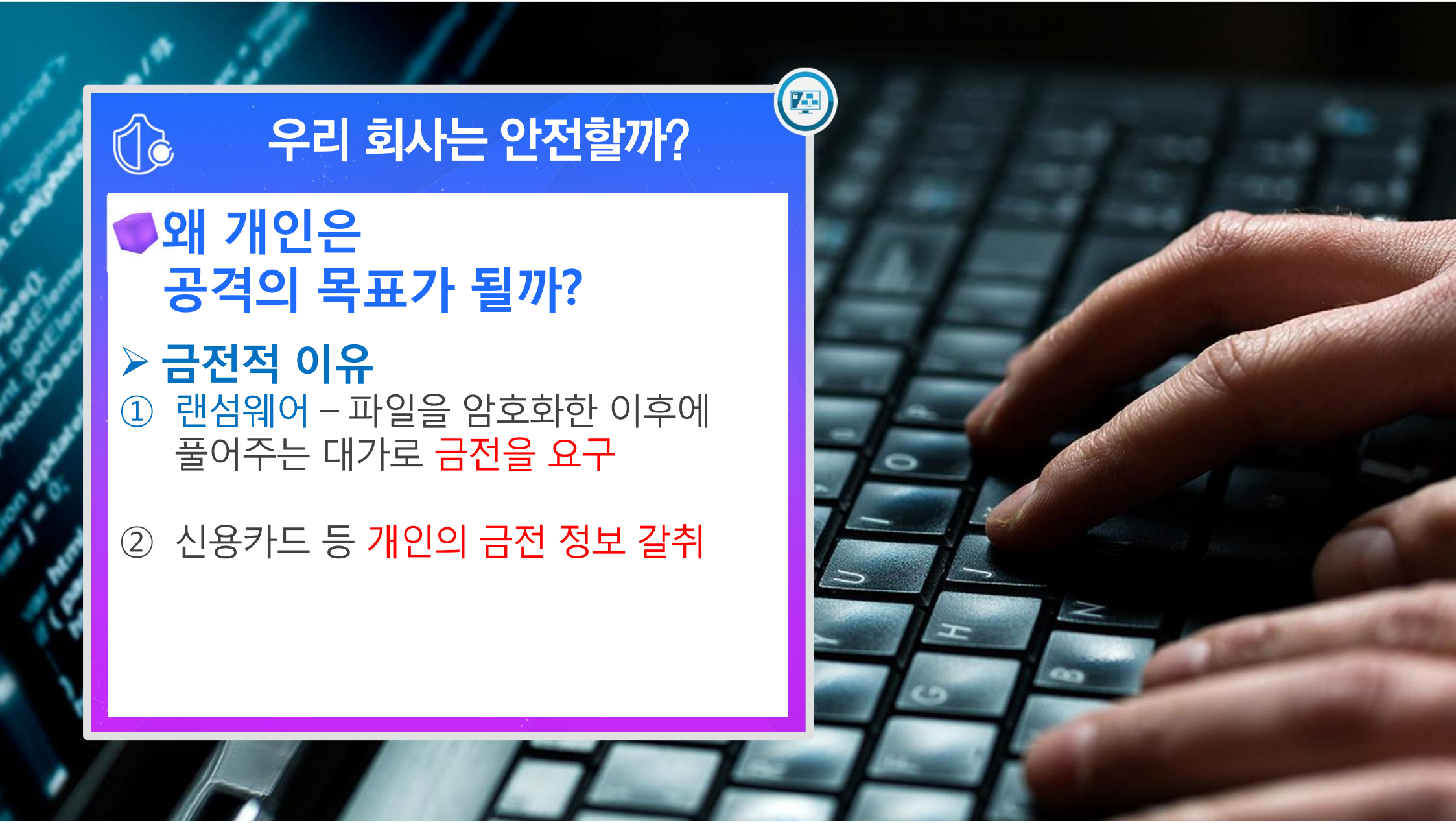
우리 회사는 안전할까?

실제 사고 사례

최종적인 목표는 전세계 최대 군수업체를
공격하기 위한 것이었음이 밝혀짐

우리 회사는 안전할까?

- 사이버 보안을 이해하지 못하는 기업을 노립니다



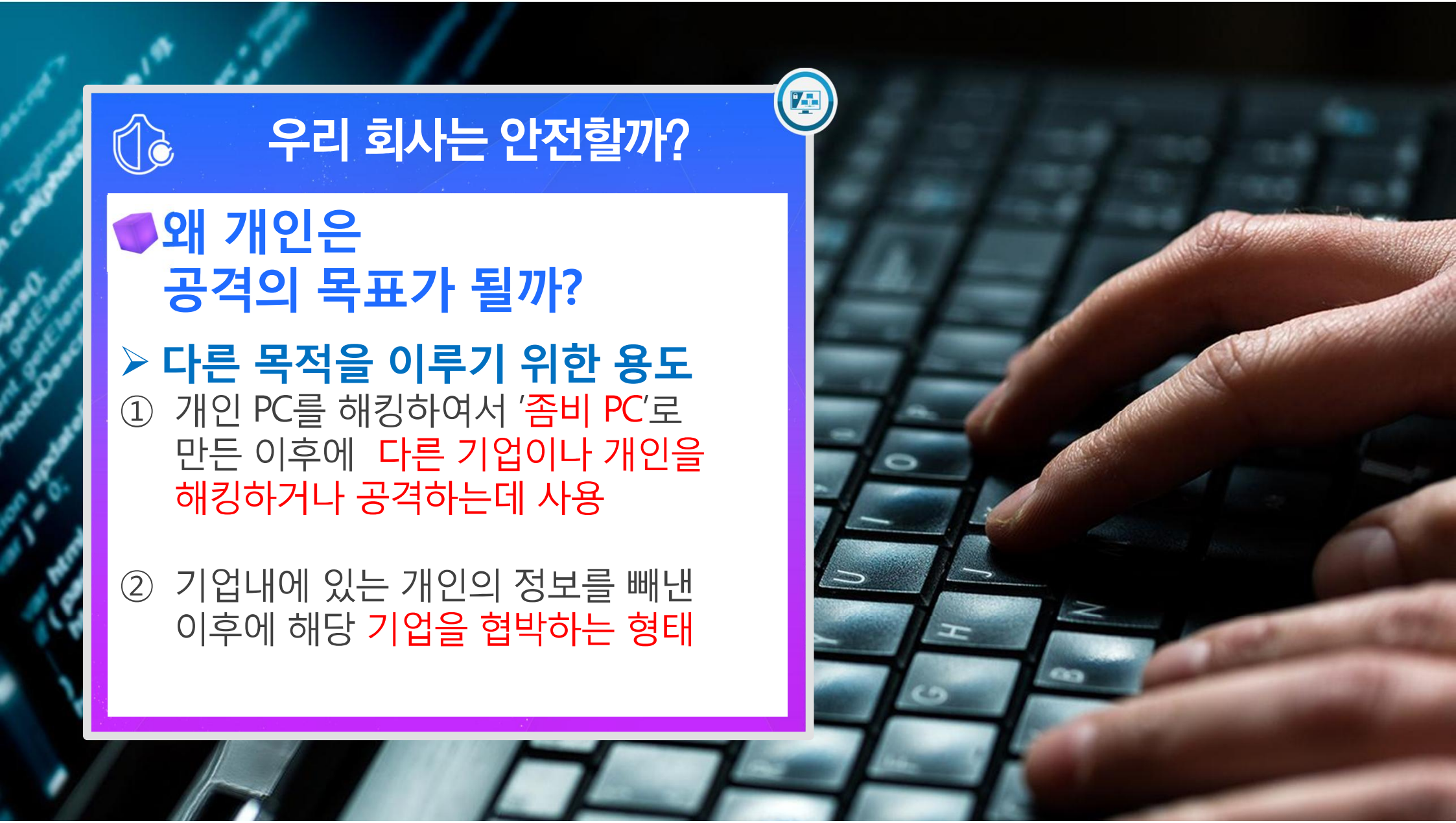
우리 회사는 안전할까?

왜 개인은 공격의 목표가 될까?

➢ 금전적 이유

① 랜섬웨어 – 파일을 암호화한 이후에 풀어주는 대가로 금전을 요구

② 신용카드 등 개인의 금전 정보 갈취



우리 회사는 안전할까?

왜 개인은 공격의 목표가 될까?

➢ 다른 목적을 이루기 위한 용도

① 개인 PC를 해킹하여서 '좀비 PC'로 만든 이후에 다른 기업이나 개인을 해킹하거나 공격하는데 사용

② 기업내에 있는 개인의 정보를 빼낸 이후에 해당 기업을 협박하는 형태

우리 회사는 안전할까?

공격자는 가장 약한 고리를 노립니다

- 사이버 보안에 대한 투자나 관심이 없는 기업이나 개인
- 쉬운 방법과 노력만으로도 원하는 것을 얻을 수가 있음
- 가장 약한 고리를 공격하여서 실제 원하는 목적을 이루기도 함

우리 회사는 안전할까?

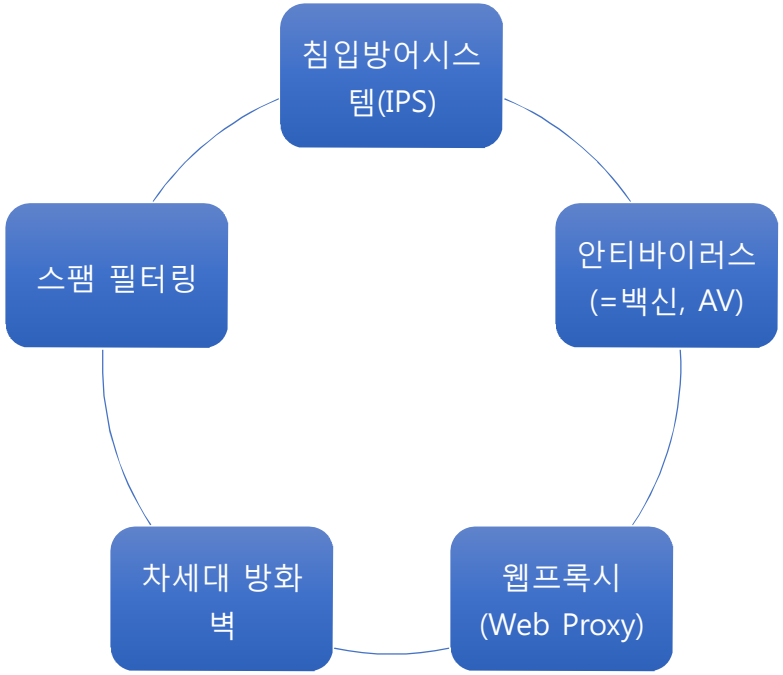
공격자는 가장 약한 고리를 노립니다

- 개인의 정보와 사이버 보안에 대한 대비는 지속적인 관심이 필요

- 기업에서는 사이버 보안을 '필수적인 요소'로 생각하고 투자 및 관리해야 함


랜섬웨어 예방 및
사이버 보안의 첫 걸음
전사원을 교육하라!
해킹을 방어하기 위한 기술
패턴 기반의 방어 방법

패턴 기반의 사이버 공격 방어 기법



패턴 기반의 탐지 방식

➢ 패턴 기반 탐지

기존에 발견된(알려진) 악성코드나
악성정보등에 기반하여서 악성파일,
악성 통신등을 탐지 하는 기술

사건발생

범죄자 검거

전과자 리스트 작성

패턴 기반 보안 솔루션

➢ 안티바이러스(백신)

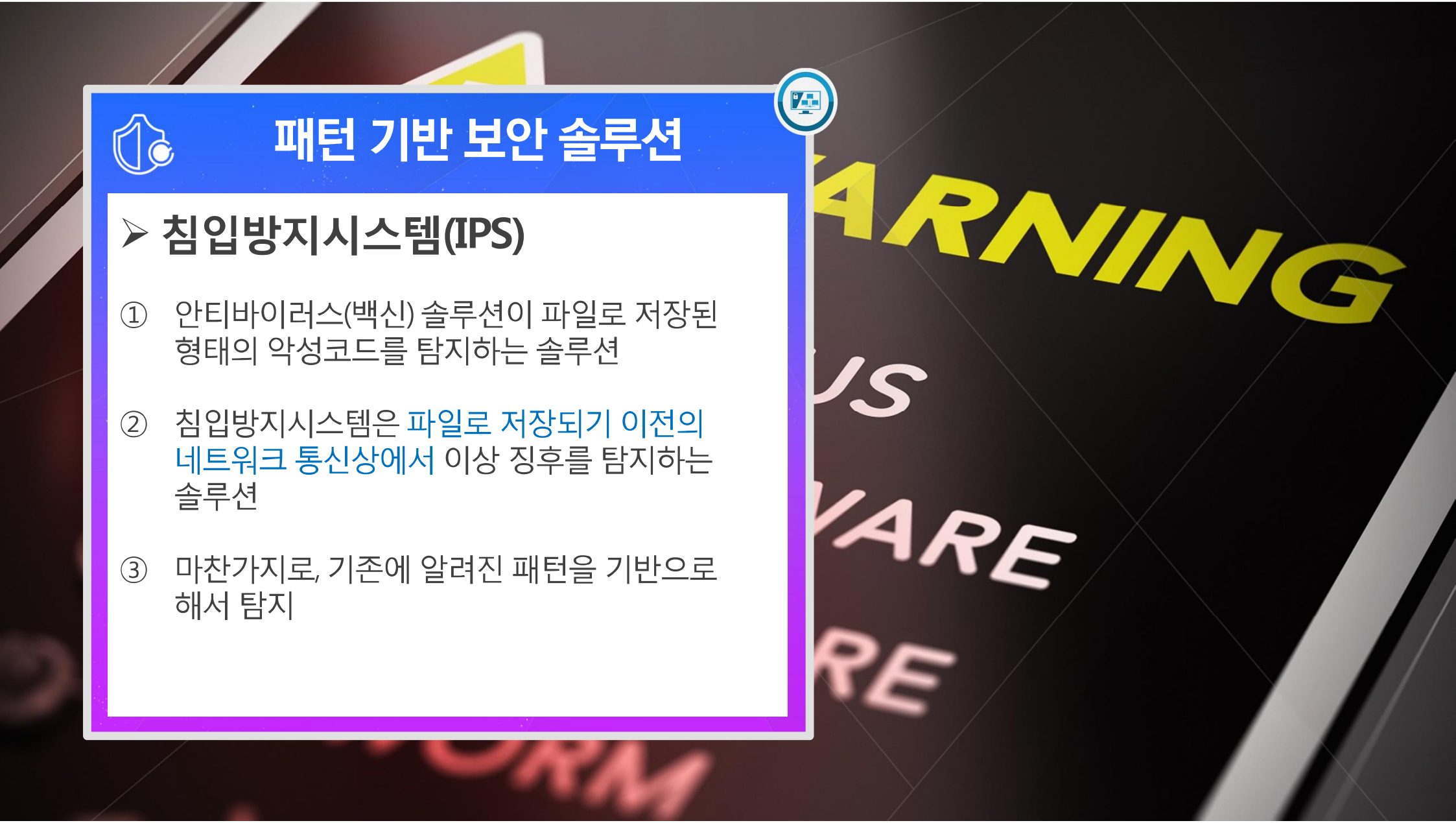
보안사고 발생

악성코드 분석

```
v18 = ShellExecuteA(0, "open", File, 0, 0, 0);
if ( (unsigned int)v18 <= 0x20 )
{
  sprintf(&v21, "Run -%d", v18);
  sub_401880((int)dword_403B6C, (int)&dword_403BAC, 17, (int)&v21, 10);
}
else
{
  sprintf(&v21, "Run OK!");
```

악성코드내에서
유니크한 특징을
추출

사용자 업데이트



패턴 기반 보안 솔루션

➢ 침입방지시스템(IPS)

① 안티바이러스(백신) 솔루션이 파일로 저장된 형태의 악성코드를 탐지하는 솔루션

② 침입방지시스템은 파일로 저장되기 이전의 네트워크 통신상에서 이상 징후를 탐지하는 솔루션

③ 마찬가지로, 기존에 알려진 패턴을 기반으로 해서 탐지

패턴 기반 보안 솔루션

➢ 침입방지시스템(IPS)

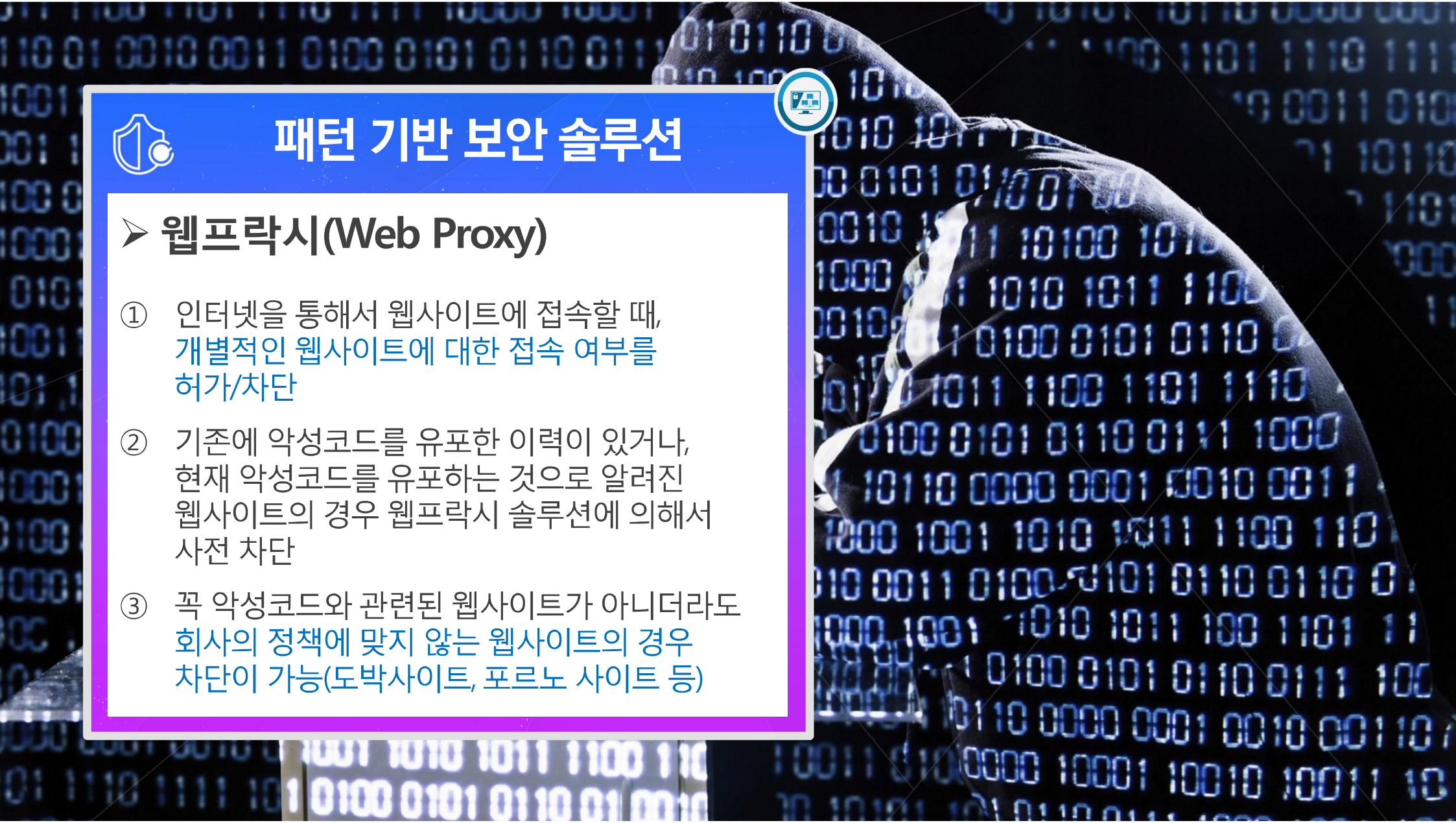
인터넷

공유기

컴퓨터

파일로 저장되기 이전의 통신 내역에서 악의적인 것을 탐지

PC에 파일로 저장된 이후에 악성 여부를 검사



패턴 기반 보안 솔루션

➢ 웹프락시(Web Proxy)

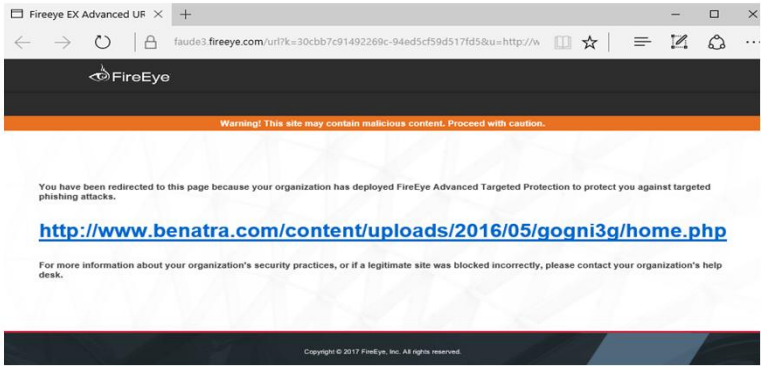
① 인터넷을 통해서 웹사이트에 접속할 때,
개별적인 웹사이트에 대한 접속 여부를
허가/차단

② 기존에 악성코드를 유포한 이력이 있거나,
현재 악성코드를 유포하는 것으로 알려진
웹사이트의 경우 웹프락시 솔루션에 의해서
사전 차단

③ 꼭 악성코드와 관련된 웹사이트가 아니더라도
회사의 정책에 맞지 않는 웹사이트의 경우
차단이 가능(도박사이트, 포르노 사이트 등)

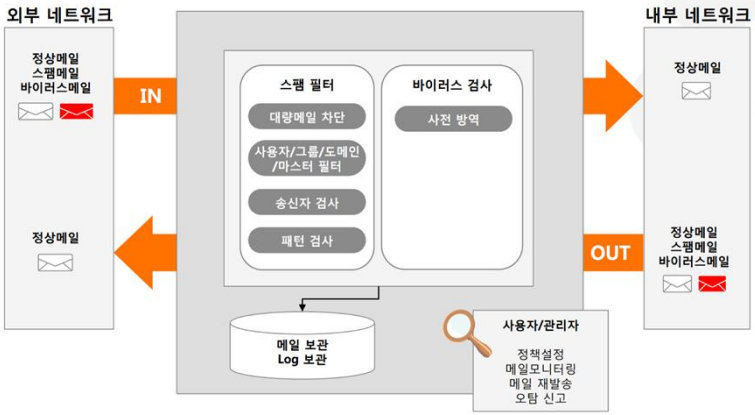
패턴 기반 보안 솔루션

➢ 웹프락시(Web Proxy)



패턴 기반 보안 솔루션

➢ 스팸필터링



① 이메일로 유입되는 악성코드를 사전에 탐지하고 차단

② 악성코드 이외에도 상업적인 스팸메일, 광고메일등을 차단하는 기능도 수행

패턴 기반 보안 솔루션

➢ 차세대 방화벽

직원 구분	유튜브	지메일	오피스365	업무 소프트웨어
직원1	허용	차단	차단	허용
직원2	허용	허용	허용	허용
직원3	허용	차단	차단	차단
직원4	허용	차단	차단	허용

① 사용자가 이용하는 각종 어플리케이션을 인식, 사용자 프로파일에 근거해서 사용자 인식

② 인식된 사용자를 기반으로 해서, 어플리케이션 기반의 보안 정책을 적용 가능

왜 백신이 설치되어 있는데도 해킹 사고가 날까요?

만약, 여기에 있게 된다면...

악성 의심 샘플

Symantec TREND MICRO McAfee KASPERSKY AhnLab SOPHOS

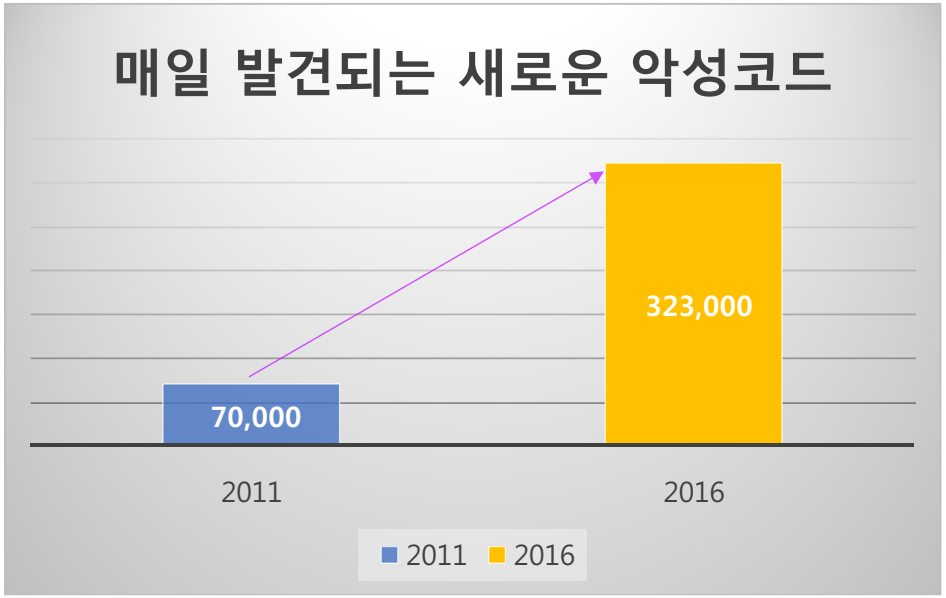
악성코드 분석가

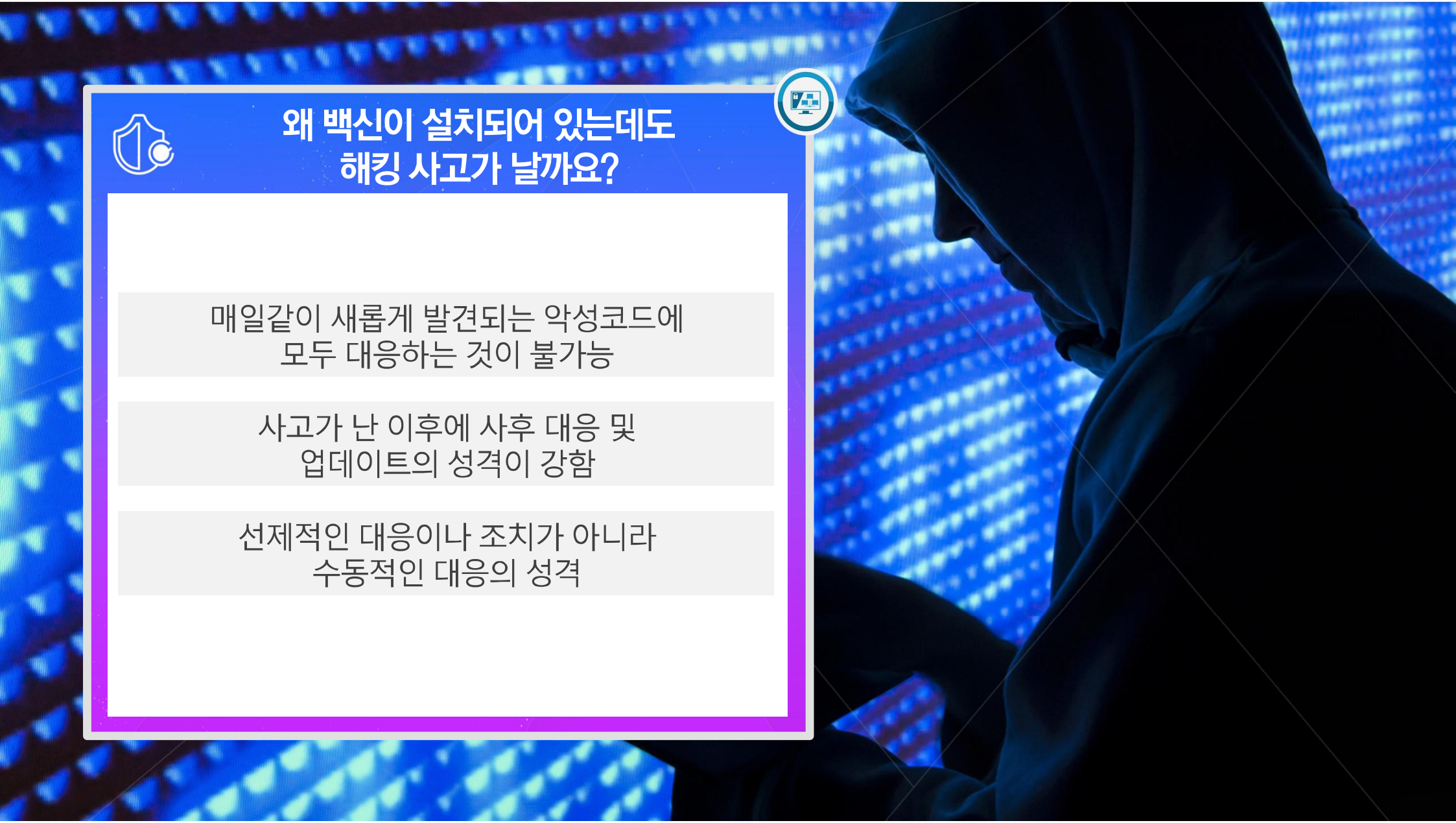
정적/동적 분석
보안업체의 연구실(대응팀)

백신 사용자에게
업데이트
여기라면
다행이지만..

왜 백신이 설치되어 있는데도 해킹 사고가 날까요?

왜 백신이 설치되어 있는데도 해킹 사고가 날까요?





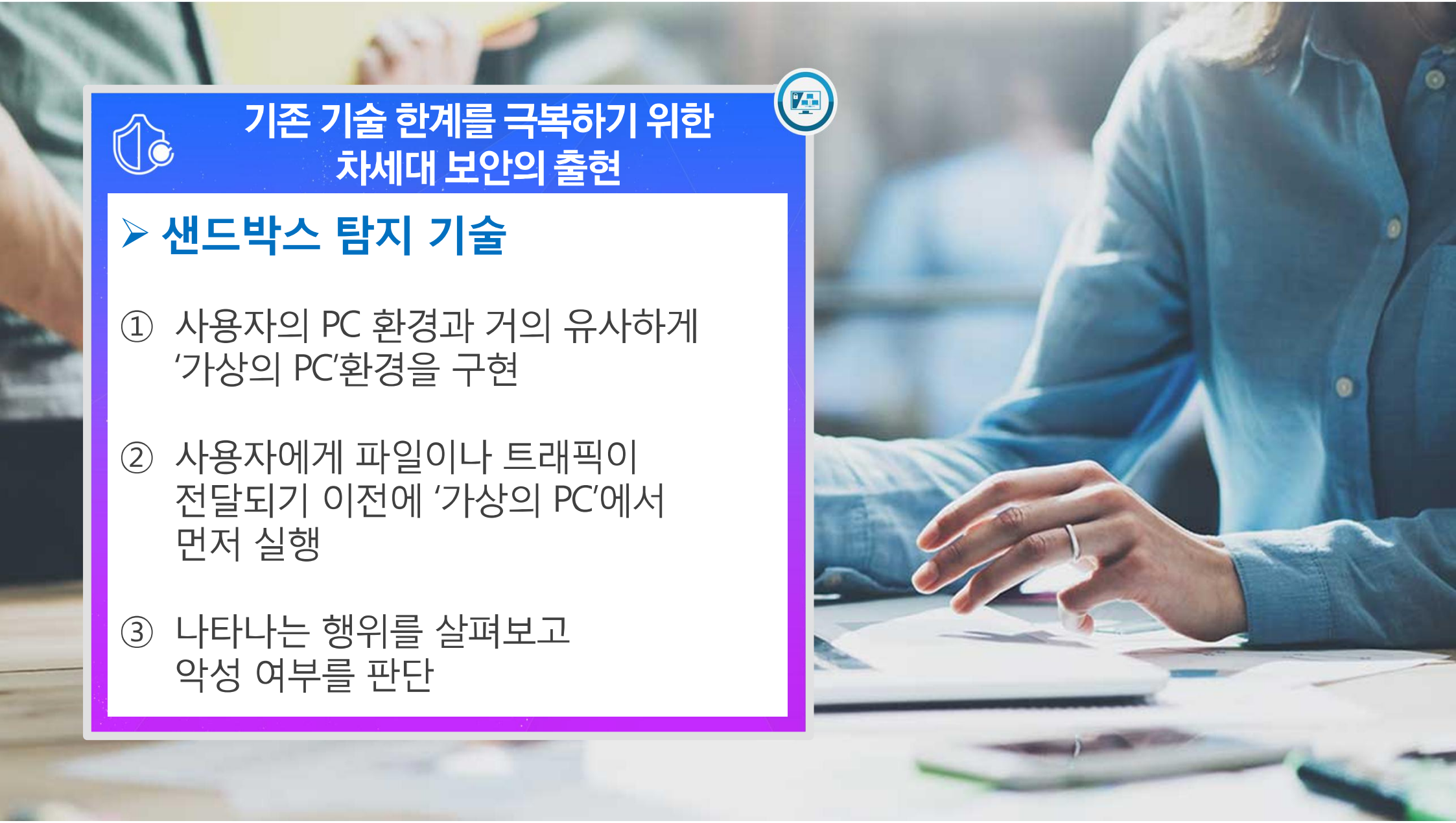
왜 백신이 설치되어 있는데도 해킹 사고가 날까요?

매일같이 새롭게 발견되는 악성코드에
모두 대응하는 것이 불가능

사고가 난 이후에 사후 대응 및
업데이트의 성격이 강함

선제적인 대응이나 조치가 아니라
수동적인 대응의 성격


랜섬웨어 예방 및
사이버 보안의 첫 걸음
전사원을 교육하라!
해킹을 방어하기 위한 기술
샌드박스와 머신러닝 기법



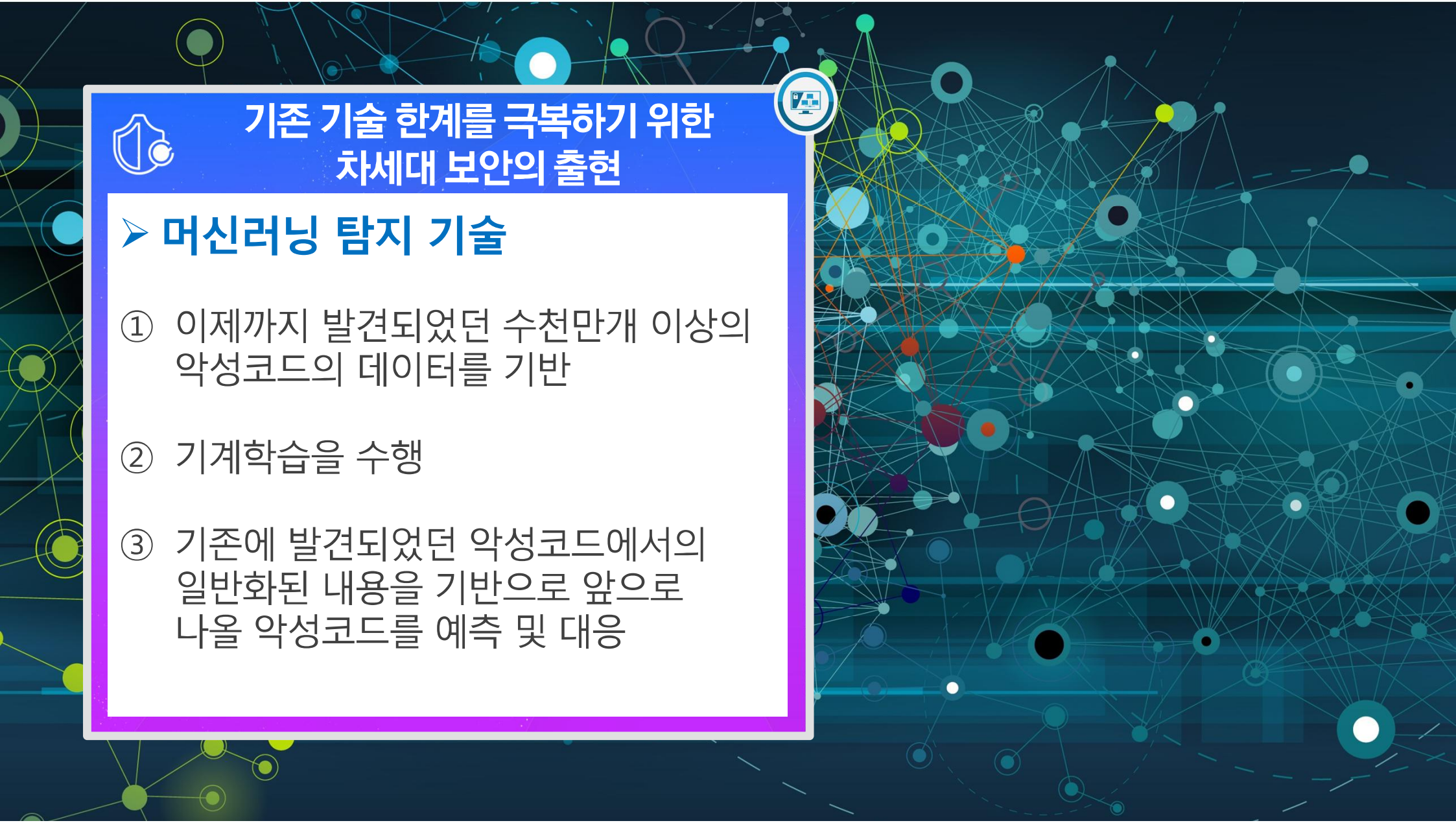
기존 기술 한계를 극복하기 위한 차세대 보안의 출현

➢ 샌드박스 탐지 기술

① 사용자의 PC 환경과 거의 유사하게 '가상의 PC'환경을 구현

② 사용자에게 파일이나 트래픽이 전달되기 이전에 '가상의 PC'에서 먼저 실행

③ 나타나는 행위를 살펴보고 악성 여부를 판단



기존 기술 한계를 극복하기 위한 차세대 보안의 출현

➢ 머신러닝 탐지 기술

① 이제까지 발견되었던 수천만개 이상의 악성코드의 데이터를 기반

② 기계학습을 수행

③ 기존에 발견되었던 악성코드에서의 일반화된 내용을 기반으로 앞으로 나올 악성코드를 예측 및 대응

기존 기술 한계를 극복하기 위한 차세대 보안의 출현

➢ 샌드박스 솔루션

Sandbox 솔루션

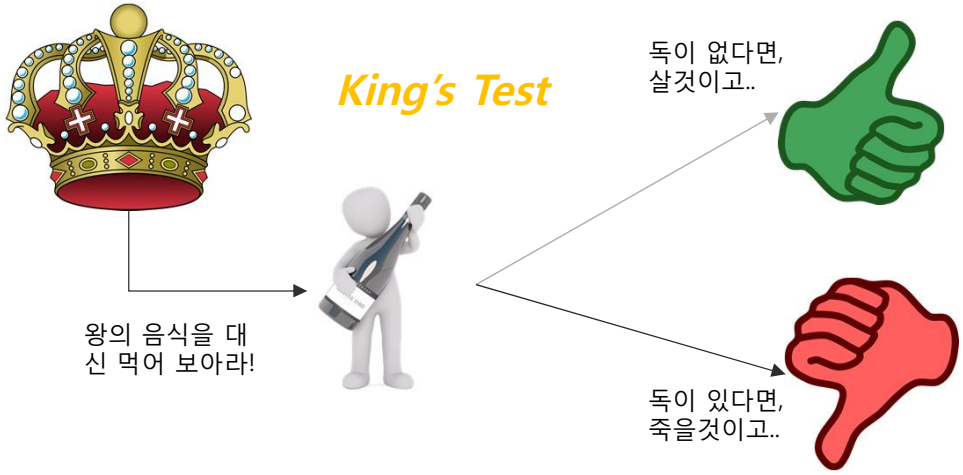
가상머신 탐지 솔루션이라고도 함

안전한 환경에서 의심되는 파일을 실행한 이후에 나타나는 '행위'를 기반으로 탐지

현재까지 가장 진보된 탐지 방법 중 하나

기존 기술 한계를 극복하기 위한 차세대 보안의 출현

➢ 샌드박스 솔루션의 동작 원리

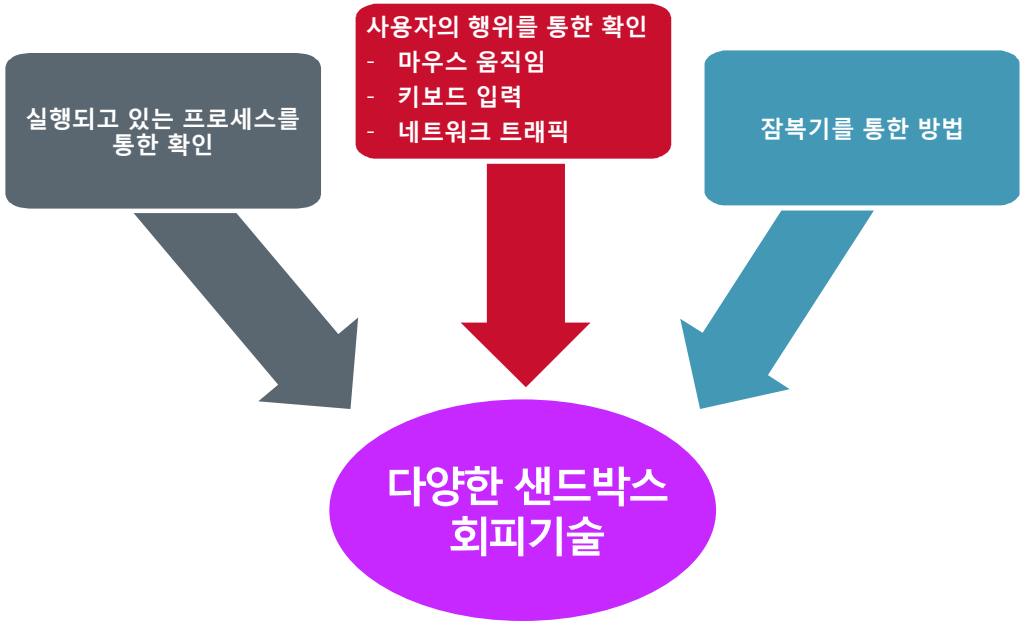


기존 기술 한계를 극복하기 위한 차세대 보안의 출현

- 샌드박스 솔루션의 동작 영상

기존 기술 한계를 극복하기 위한 차세대 보안의 출현

➢ 샌드박스 기반 솔루션의 고려 사항



기존 기술 한계를 극복하기 위한 차세대 보안의 출현

➢ 샌드박스 기반 솔루션의 고려 사항

수백개의 파일분석

- 한시간당 수백개의 파일이 기업에 유입되는 것으로 추정

평균 파일 사이즈

- 다양한 파일 사이즈에 대한 분석 필요

다양한 프로그램 지원

- 사용자가 쓰는 다양한 어플리케이션이 설치되어 있어야 함

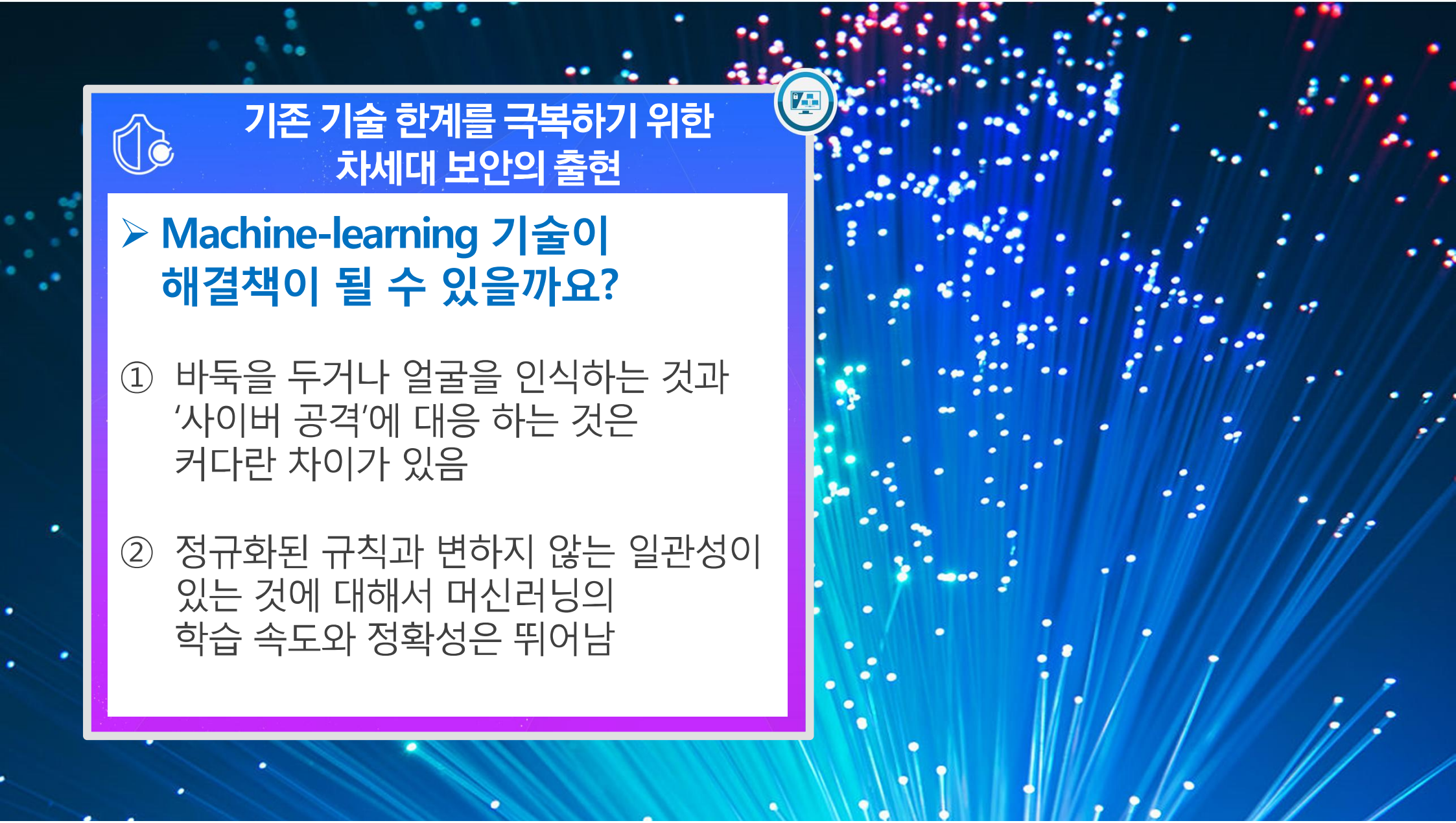
기존 기술 한계를 극복하기 위한 차세대 보안의 출현

➢ 머신러닝 기반 솔루션

① 과거에 발견 되었던 수천만개 이상의 악성파일을 일반화 시킴

② 여기에서 나오는 공통점을 기반으로 하여서 기계학습을 시킴

③ 이를 통해서 향후 발생하는 위협에 대처하고자 함



기존 기술 한계를 극복하기 위한 차세대 보안의 출현

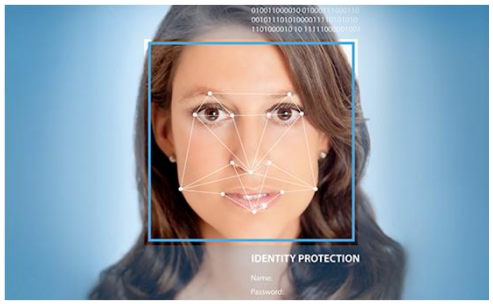
➢ Machine-learning 기술이 해결책이 될 수 있을까요?

① 바둑을 두거나 얼굴을 인식하는 것과 '사이버 공격'에 대응 하는 것은 커다란 차이가 있음

② 정규화된 규칙과 변하지 않는 일관성이 있는 것에 대해서 머신러닝의 학습 속도와 정확성은 뛰어남

기존 기술 한계를 극복하기 위한 차세대 보안의 출현

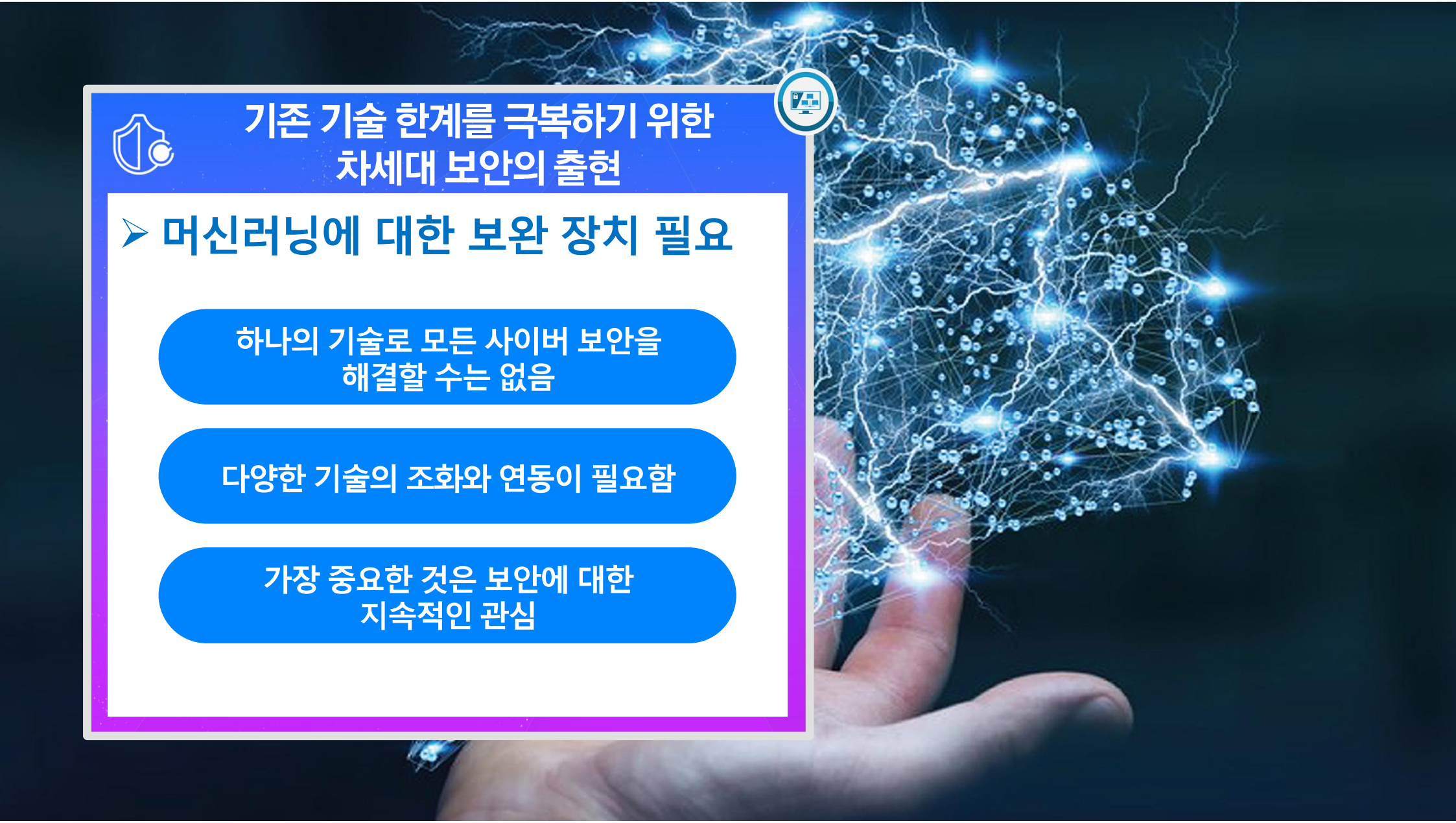
➢ Machine-learning 기술이 해결책이 될 수 있을까요?



하지만, 정규화 되지 않거나 규칙이 없는 내용에 대한 정확도는 떨어짐

기존 기술 한계를 극복하기 위한 차세대 보안의 출현

➢ 머신러닝에 대한 보완 장치 필요



기존 기술 한계를 극복하기 위한 차세대 보안의 출현

➢ 머신러닝에 대한 보완 장치 필요

- 하나의 기술로 모든 사이버 보안을 해결할 수는 없음
- 다양한 기술의 조화와 연동이 필요함
- 가장 중요한 것은 보안에 대한 지속적인 관심


랜섬웨어 예방 및
사이버 보안의 첫 걸음
전사원을 교육하라!
백신의 진화 – 차세대 백신

현재 백신 위주 방어 체계의 문제점

오래된 방식의 비효율적인 엔드포인트 솔루션에 의존

대부분 안티바이러스를 도입하였지만
지속적인 침해사고 발생

Endpoint Protection Platforms (EPP)

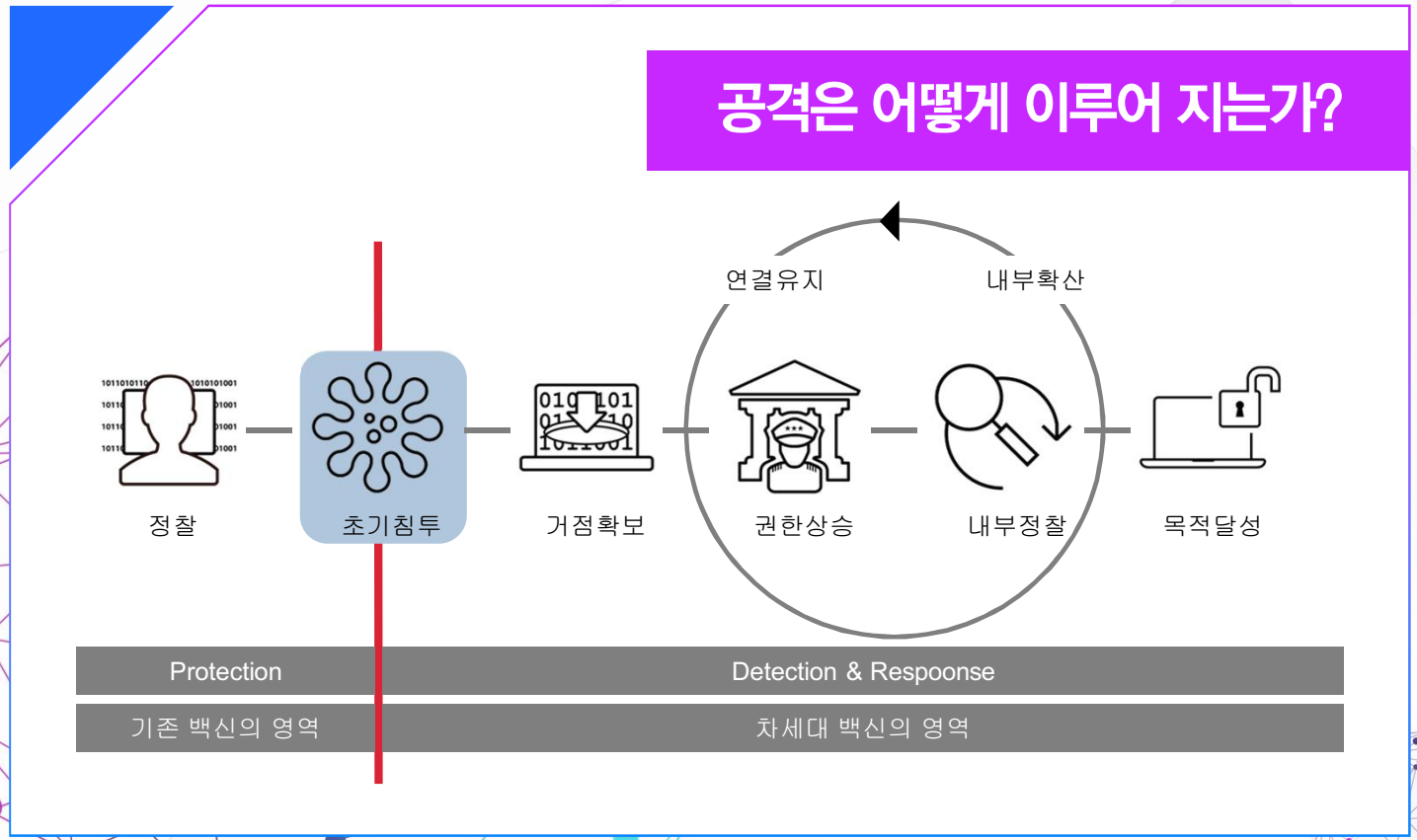
시그니처 기반의 방어 솔루션	기타 엔드포인트 솔루션
Anti-Virus	DLP
Anti-Malware	DRM
Host Firewall	Disk Encryption
Host IPS	Application Control

어떻게 진화해야 하는가?

응답자의 **81%**는 자신의 조직이 현재 또는 향후 2년 내에 **'차단'**에만 초점을 맞춘 보안 조직에서, **"탐지 및 대응"**을 수행 할 것이라고 말했습니다.

2016 State of the Endpoint Report, Ponemon Institute, LLC., April 2016.

공격은
어떻게 이루어 지는가?



차세대 백신 – EPP+EDR

➢ **EPP(Endpoint Protection Platform)**

① 기존 백신이 가지고 있는 한계를 극복

② 머신러닝, 행위기반 탐지, 인텔리전스 탐지등을 추가하여서 백신이 탐지하지 못하던 부분을 커버

차세대 백신 – EPP+EDR

➢ **EDR(Endpoint Detection & Response)**

① 악성코드 이후의 단계를 탐지 및 대응

② 단순 탐지가 아니라, 취약한 부분이 어디인지 실시간 포렌식 조사를 통해서 확인 가능

EPP + EDR

EPP + EDR

EPP

PREVENTION

높고 강력한 벽을 구축

알려지지 않은 위협을 탐지 및 차단

EDR

RESPONSE

벽 주위나 아래, 위에 있는게 누구인지 확인

만에 하나 차단이 실패할 경우에 즉각적으로 대응할 수 있는 역량을 제공

"2020 년까지 엔터프라이즈 정보 보안 예산의 60 %가 빠른 탐지 및 대응 접근법에 할당 될 것."

Anton Chuvaking, Gartner Research VP Gartner

"EDR솔루션을 통해서 기존의 엔드 포인트가 가지고 있던 문제점들을 극복할 수 있을것."

Anton Chuvaking, Gartner Research VP Gartner

차세대
백신의 조건

차세대 백신의 조건

1

실시간 탐지와
차단 기능

2

조직 내부에 대한
가시성과
인텔리전스 제공

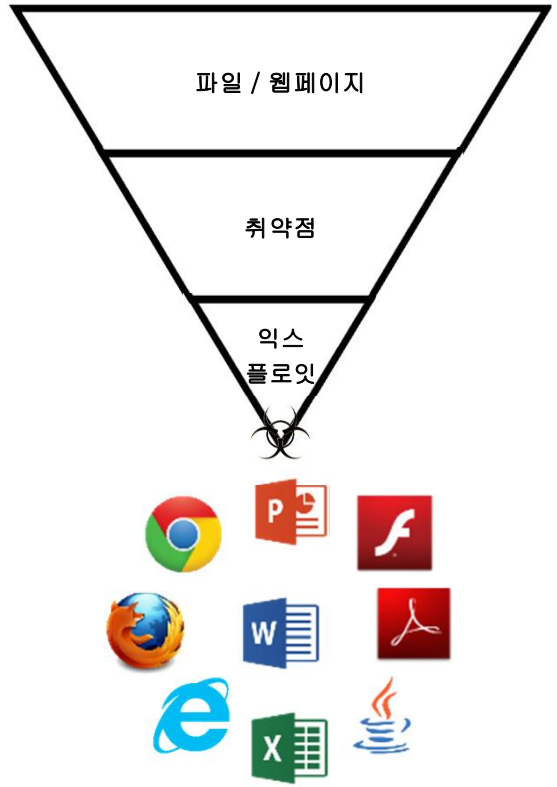
3

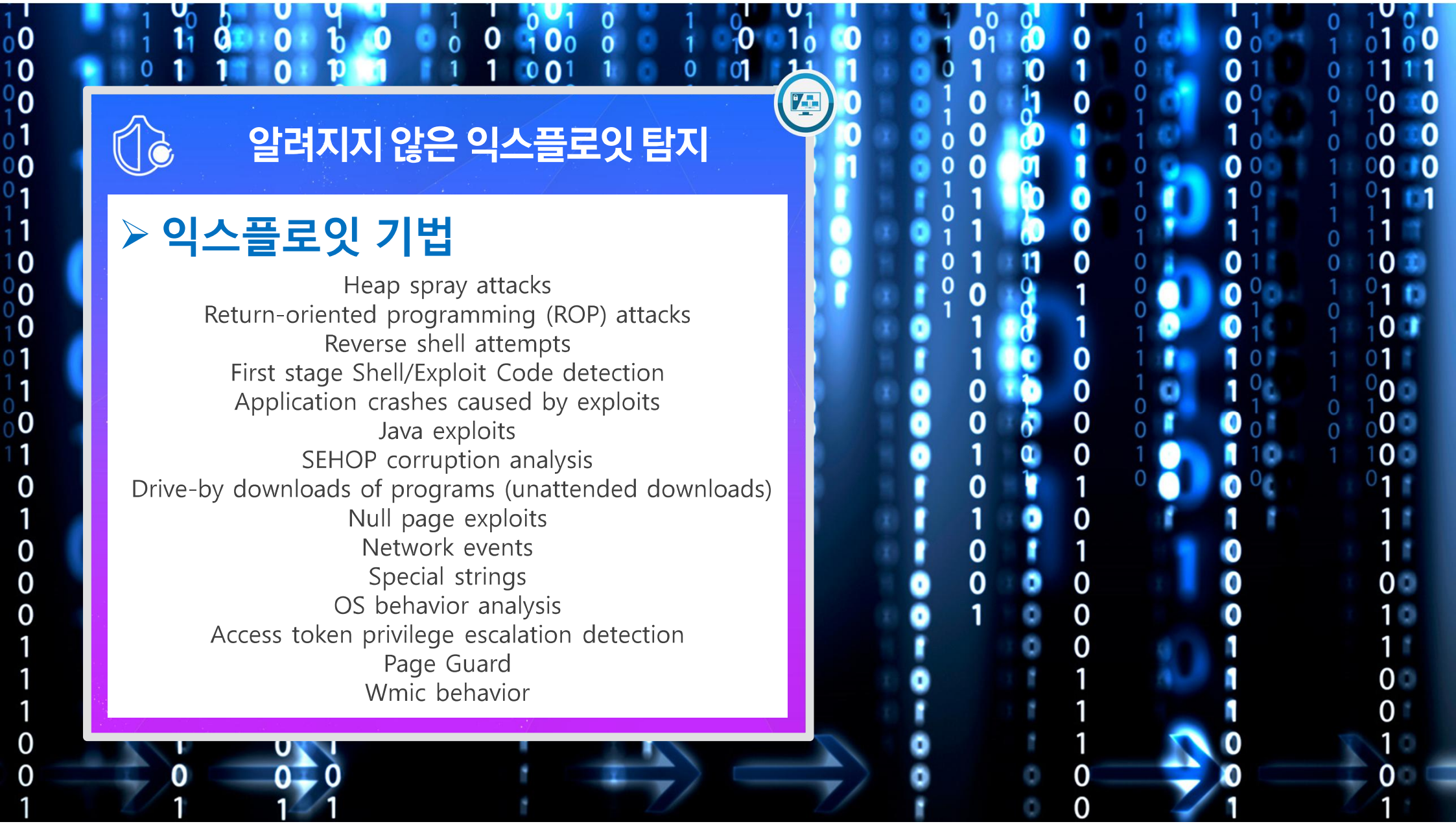
피해를 최소화할
수 있도록
빠른 대응
절차 제공

4

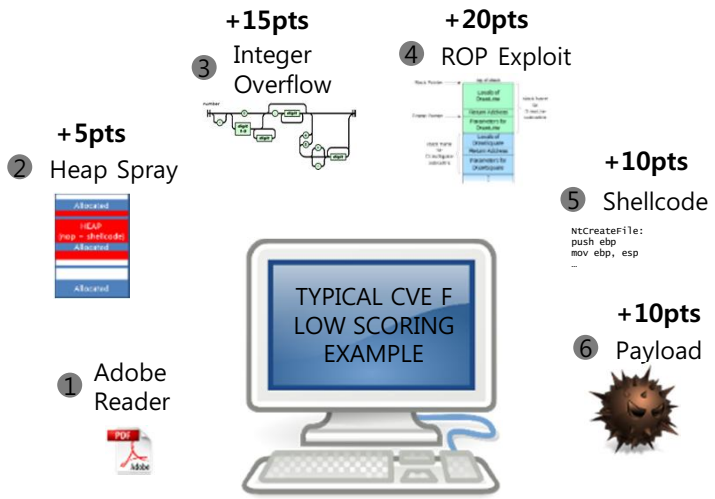
공격자의 행위에
대한 선제적 대응

알려지지 않은 익스플로잇 탐지




알려지지 않은 익스플로잇 탐지
익스플로잇 기법
Heap spray attacks
Return-oriented programming (ROP) attacks
Reverse shell attempts
First stage Shell/Exploit Code detection
Application crashes caused by exploits
Java exploits
SEHOP corruption analysis
Drive-by downloads of programs (unattended downloads)
Null page exploits
Network events
Special strings
OS behavior analysis
Access token privilege escalation detection
Page Guard
Wmic behavior

알려지지 않은 익스플로잇 탐지



행위기반으로 '어플리케이션 취약점'을 이용한 익스플로잇 공격 탐지

인텔리전스 제공과 침해흔적 조사 제공

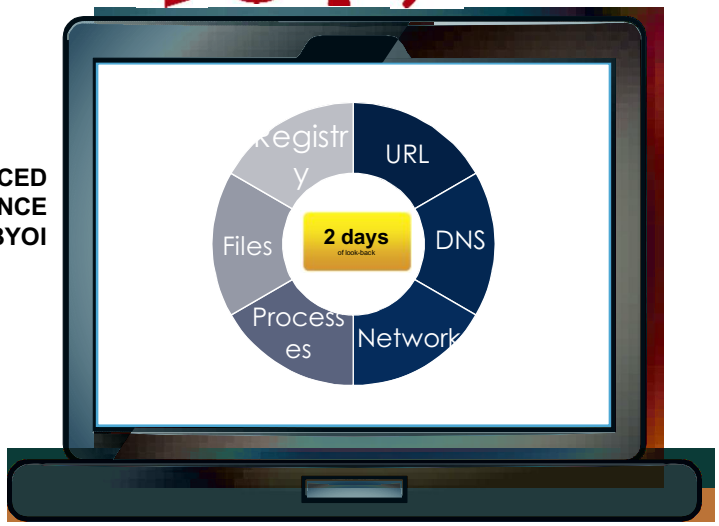
인텔리전스 기반의 탐지와 정보 제공이 필요

인텔리전스 제공과 침해흔적 조사 제공

효과적인 운영을 위해서는 '실시간
모니터링'과 '침해흔적' 탐지가 반드시 필요

TTPs

MULTI-SOURCED
INTELLIGENCE
BYOI



인텔리전스 제공과 침해흔적 조사 제공

악성코드 실시간 탐지
(차세대 기술 적용)

인텔리전스 제공과 침해흔적 조사 제공

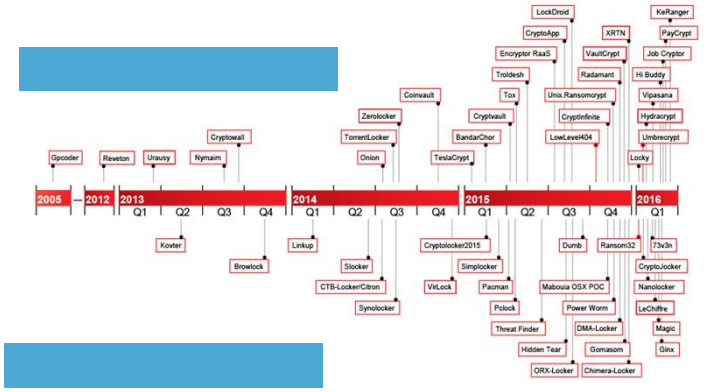
강력한 차세대 탐지엔진

Viruses
Trojans
Worms
Spyware
Adware
key loggers
Rootkits
Anti-phishing
Potentially unwanted programs (PUP)

랜섬웨어에 대한 효과적인 대응

랜섬웨어에 대한 효과적인 대응

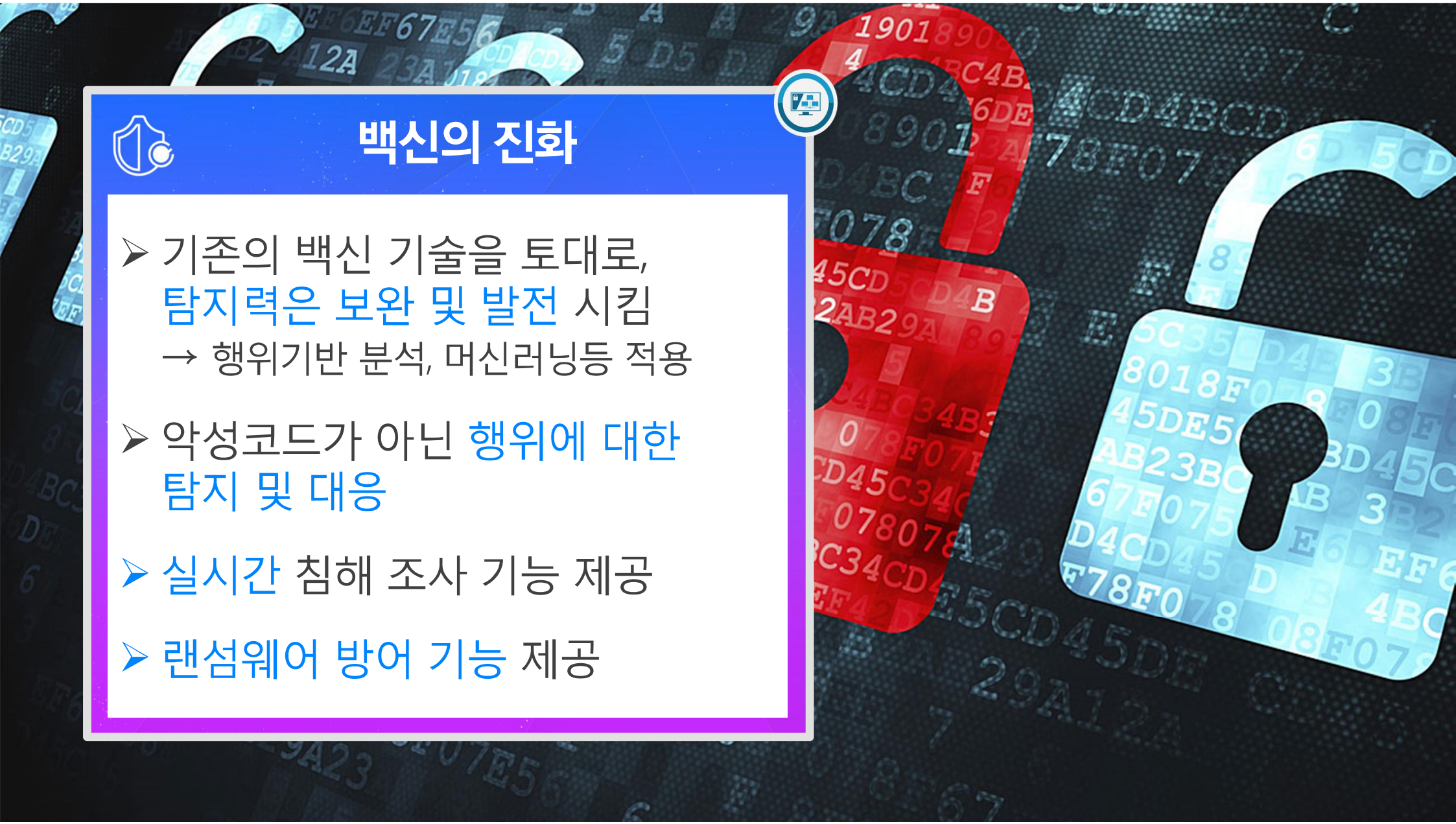
랜섬웨어



암호화된 파일의 복구 기능

알려지지 않은
파일 암호화
기술 탐지

그 외 다양한
랜섬웨어의 공격 시도를
행위기반으로
탐지 및 대응



백신의 진화

- 기존의 백신 기술을 토대로, 탐지력은 보완 및 발전 시킴
  → 행위기반 분석, 머신러닝등 적용
- 악성코드가 아닌 행위에 대한 탐지 및 대응
- 실시간 침해 조사 기능 제공
- 랜섬웨어 방어 기능 제공


랜섬웨어 예방 및
사이버 보안의 첫 걸음
전사원을 교육하라!
마술같은 해킹 기법
워터링홀

사이버 공격의 경로

이메일

웹서핑

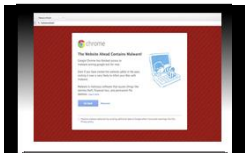
모바일

USB

파일공유

다양한 경로를 통한 공격 시도가 이루어짐

인터넷 서핑을 통한 사이버 공격 방법



악성
유포사이트를
통해서 감염

어플리케이션
혹은 OS의
취약점을
공격하는
Exploit

악성
유포지로부터
악성코드
다운로드

C&C 서버로의
접속

드라이브-바이-다운로드
공격 기법

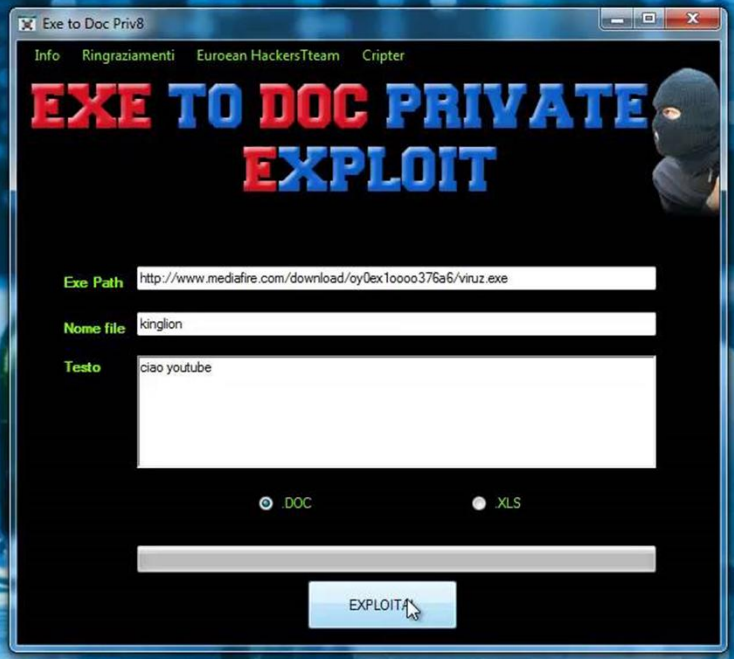
사용자가 해킹된 웹사이트에 접속만 하더라도,
해커에 의해서 공격 받을 수 있음

취약점과 익스플로잇

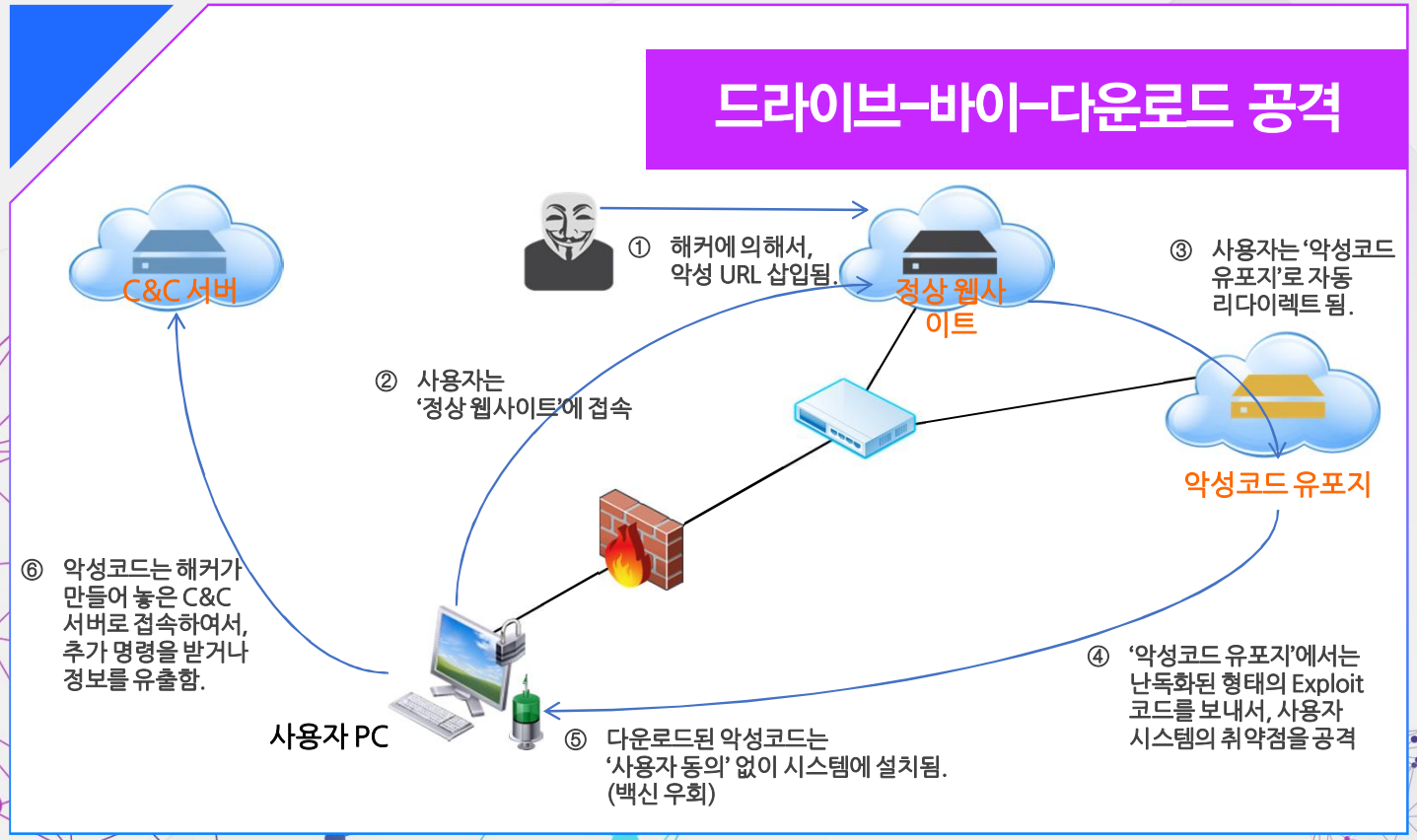
소프트웨어에 잠재되어 있는 취약점 ***(Vulnerability)***

취약점 *(Vulnerability)*를 이용하여서, 악의적인 행위를 하는 코드를 생성 -> 익스플로잇 ***(Exploit)***

이때, 해커가 제조사보다 먼저 취약점 (Vulnerability)을 발견하여서, 이를 익스플로잇(Exploit)으로 만들어서, 사이버 공격에 사용하는 경우에 '제로데이 공격(Zero-day)'이라고 부른다.



드라이브-바이-다운로드
공격은 어떻게 이루어지는가?



워터링홀 공격

- 안전하다고 생각되는 물웅덩이에서 악어가 사냥을 하는것에 비유

- 정상이라고 생각하는 웹사이트에 익스플로잇을 설치해 두고, 사용자를 감염시키고 해킹 공격하는 방식

워터링홀 공격은 어떻게 이루어 지는가?

워터링홀 공격

Infection URLs:

URL	Occurred	Content Type	URL	Occurred	Content Type
www.hikor.com/data/m.html	02/22/13 20:50:03	text/html	www.hikor.com/data/count.js	02/22/13 20:50:04	application/x-javascript
www.naver.com/	02/22/13 20:49:29	text/html	www.hikor.com/data/zJCdNVL3.jpg	02/22/13 20:50:10	image/jpeg
search.naver.com/search.naver?sm=top_txt&where=nexearch&ie=utf8&query=%EC%9D%B4%EB%B3%B4%EC%98%81%20%EC%8B%A4%EC%A0%9C%20%EC%84%B1%EA%B2%A9	02/22/13 20:49:31	text/html	www.hikor.com/data/com.class	02/22/13 20:50:13	text/html
www.kyeongin.com/news/articleView.html?idxno=713750	02/22/13 20:49:55	text/html	www.hikor.com/data/edu.class	02/22/13 20:50:13	text/html
cdn04.sndkorea.co.kr/new/media/kyeongin/S00801.html	02/22/13 20:50:02	text/html	www.hikor.com/data/net.class	02/22/13 20:50:13	text/html
cdn03.sndkorea.co.kr/media/kyeongin/S00801.html	02/22/13 20:50:03	text/html	www.hikor.com/data/org.class	02/22/13 20:50:13	text/html
www.hikor.com/data/swfobject.js	02/22/13 20:50:03	application/x-javascript	pezzi.net/css/d0222.exe	02/22/13 20:50:19	application/octet-stream
www.hikor.com/data/jpg.js	02/22/13 20:50:04	application/x-javascript			

실제 워터링홀 공격 동작 영상

왜 워터링홀 공격에 대한 방어가 어려운가?

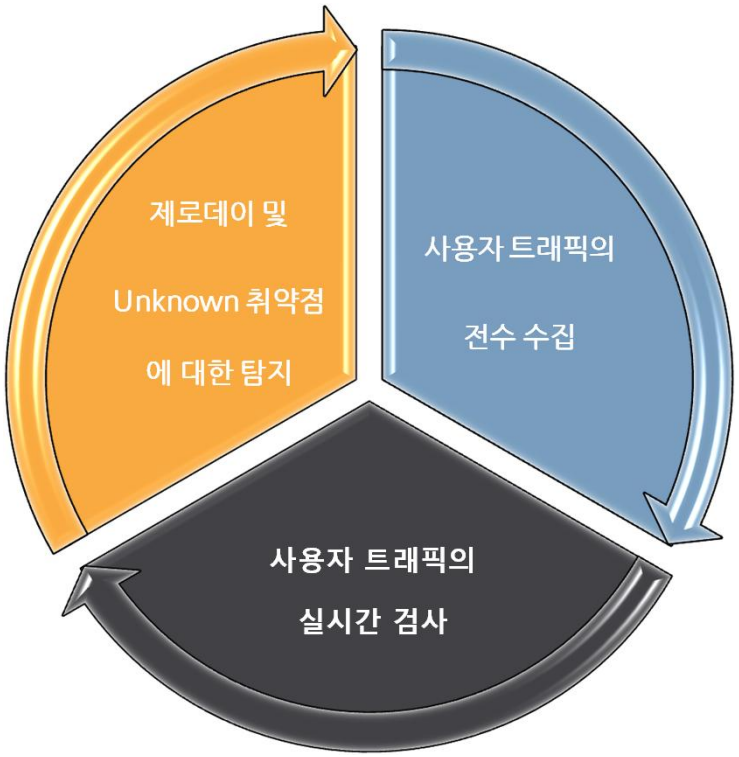
➢ 기술적 필요성

① 사용자가 접속하는 모든 웹사이트에 대한 검증이 필요

② 해당 트래픽에 대한 검사는 실시간으로 이루어져야 함

③ 웹트래픽에 대한 분석은 패턴이나 평판 기반이 아닌 방법을 통해서, 악성 유포를 탐지할 수 있어야 함

왜 워터링홀 공격에 대한 방어가 어려운가?



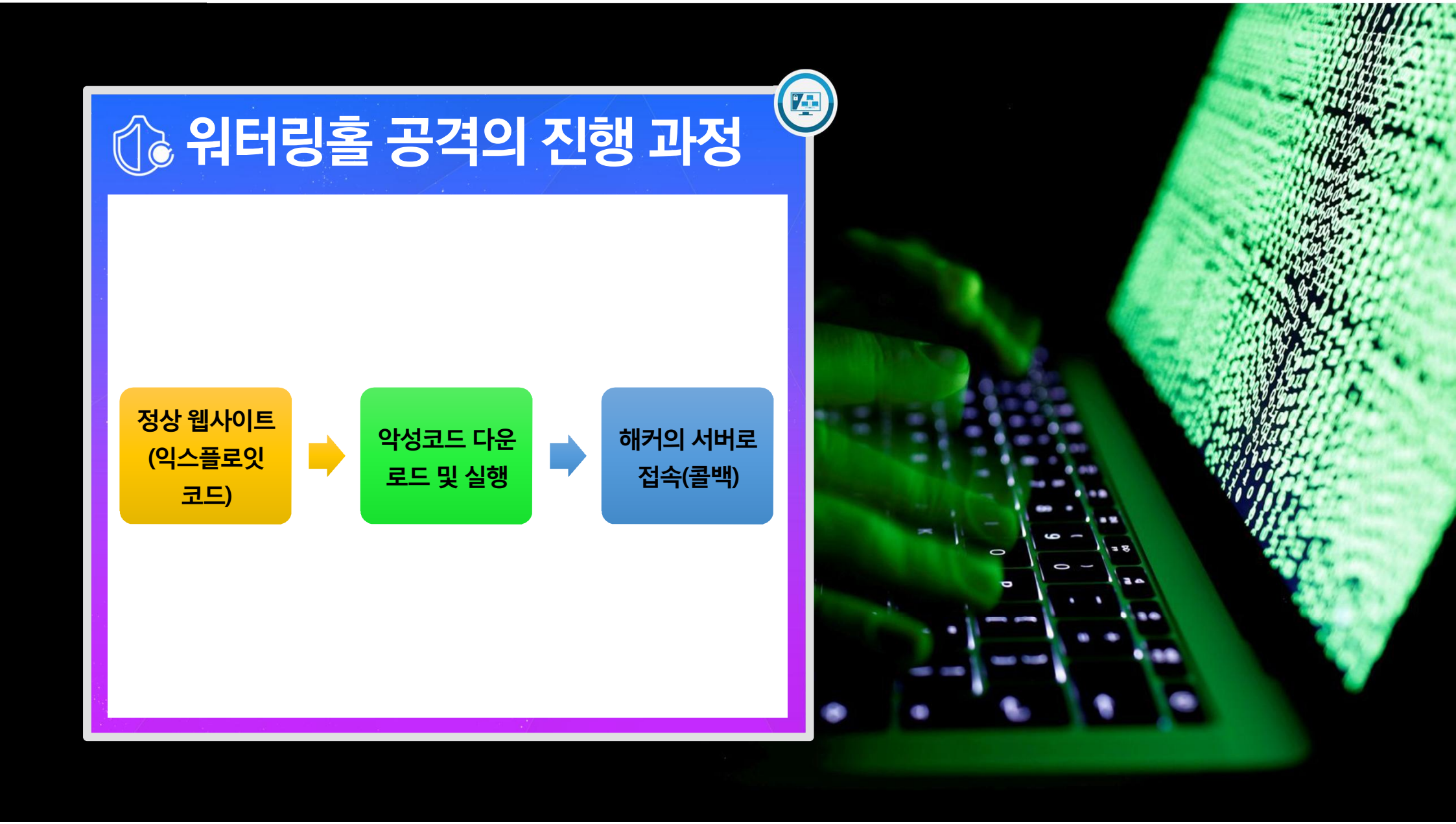

랜섬웨어 예방 및
사이버 보안의 첫 걸음
전사원을 교육하라!
워터링홀 공격의 피해를 막는 방법

워터링홀 공격의 진행 과정

정상 웹사이트 (익스플로잇 코드)

악성코드 다운로드 및 실행

해커의 서버로 접속(콜백)



워터링 홀 공격의 시작점

➤ 익스플로잇

Exploit이 포함된
해킹된 정상웹사이트

Exploit은 웹페이지의
어떤부분에도 존재가능

Exploit은 악성실행코드와 같은것이 아님!!

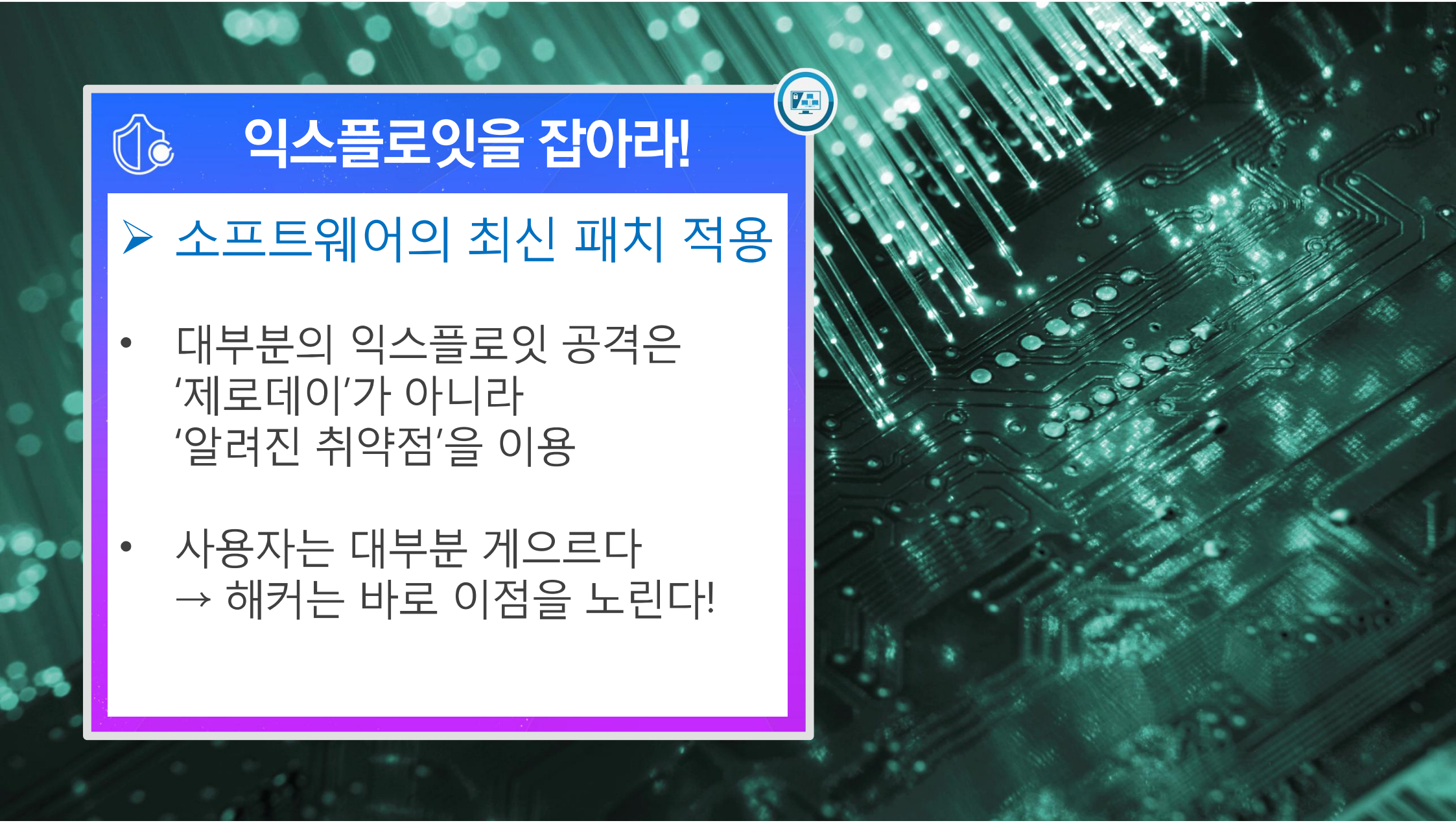
워터링 홀 공격의 시작점
익스플로잇

워터링 홀 공격의 시작점 – 익스플로잇

1. Exploit 오브젝트가 취약성을 가지고 있는 S/W에 의해서 실행됨.

2. Exploit은 실행중인 메모리에 코드를 삽입함.

3. Exploit에 의해서 제어권이 넘어감.

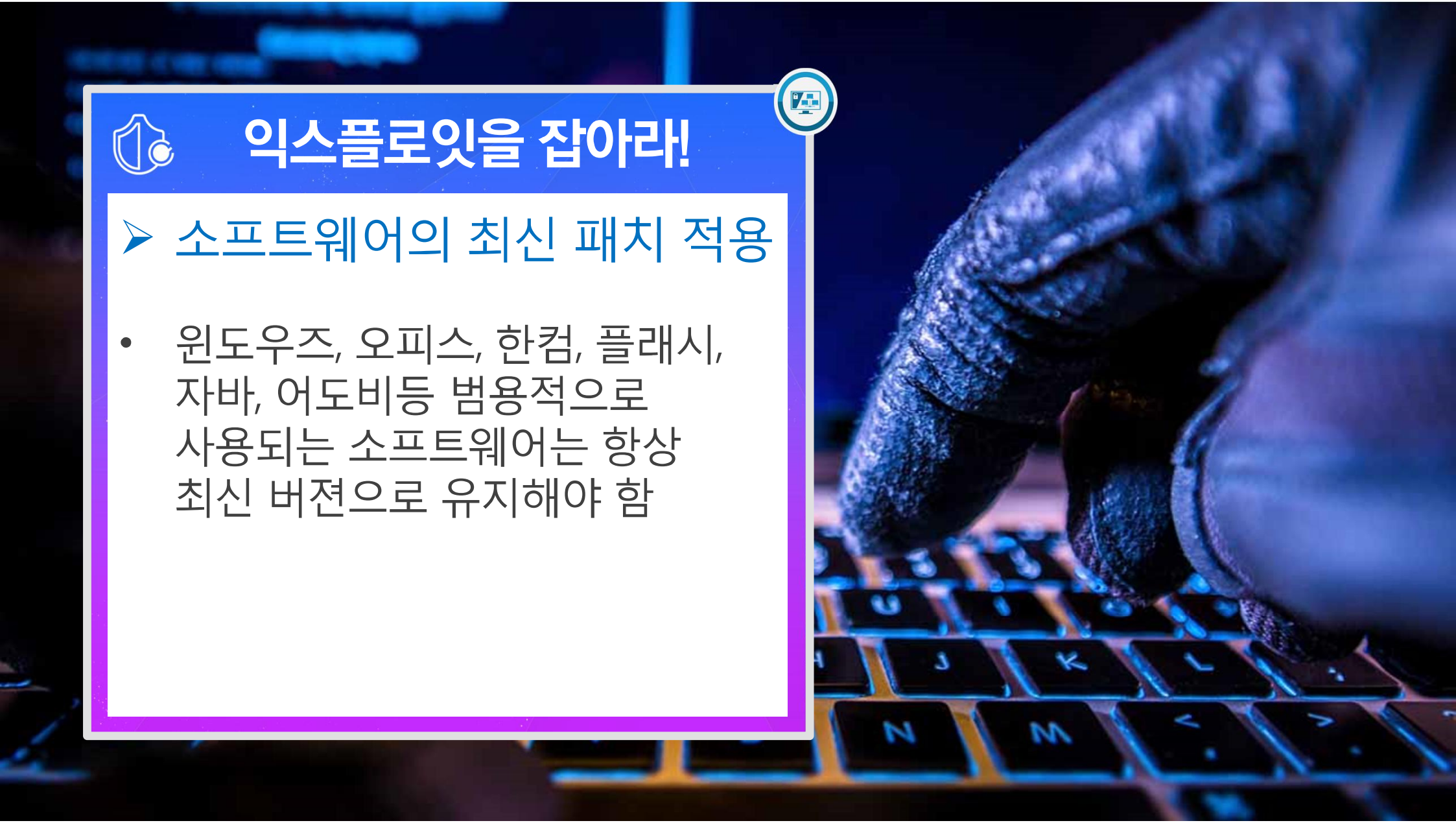


익스플로잇을 잡아라!

➢ 소프트웨어의 최신 패치 적용

- 대부분의 익스플로잇 공격은 '제로데이'가 아니라 '알려진 취약점'을 이용

- 사용자는 대부분 게으르다
  → 해커는 바로 이점을 노린다!



익스플로잇을 잡아라!

➢ 소프트웨어의 최신 패치 적용

- 윈도우즈, 오피스, 한컴, 플래시, 자바, 어도비등 범용적으로 사용되는 소프트웨어는 항상 최신 버젼으로 유지해야 함

바이러스 토탈

- 바이러스 토탈 (www.virustotal.com)은 Google이 운영하는 전세계 최대의 무료 보안 검사 및 공유 사이트

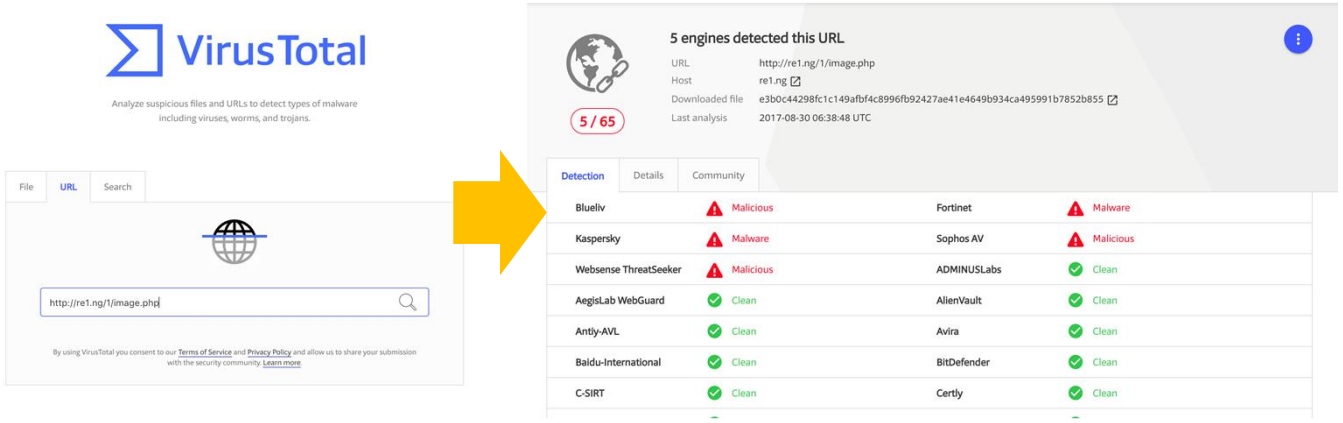
- 바이러스 토탈에는 전세계 59개의 백신 엔진과 65개의 웹사이트 검사 엔진을 무료로 제공

바이러스 토탈

- 의심스러운 웹사이트에는 접속하기 이전에 바이러스 토탈등에서 검사 후에 안전성 여부를 확인 후에 접속하는 것이 좋음

바이러스 토탈

바이러스 토탈



구글
세이프 브라우징

구글 세이프 브라우징

구글
세이프 브라우징

구글 세이프 브라우징

① 구글의 크롬 브라우저에서 기본적으로 제공하는 보안 기능

② 구글이 가지고 있는 악성 웹사이트에 대한 정보를 기반으로 해서 사용자에게 경고창을 띄워줌

알약 익스플로잇 쉴드

취약점 공격 차단

- 악성 스크립트를 이용한 취약점 공격 실시간 차단
- 주요 프로세스의 의심 행위와 파일 감시
- 특정 탐지명/파일에 대한 탐지 제외 기능 제공
- 로그를 통한 악성코드 상세 정보 확인 가능

PC취약점 점검

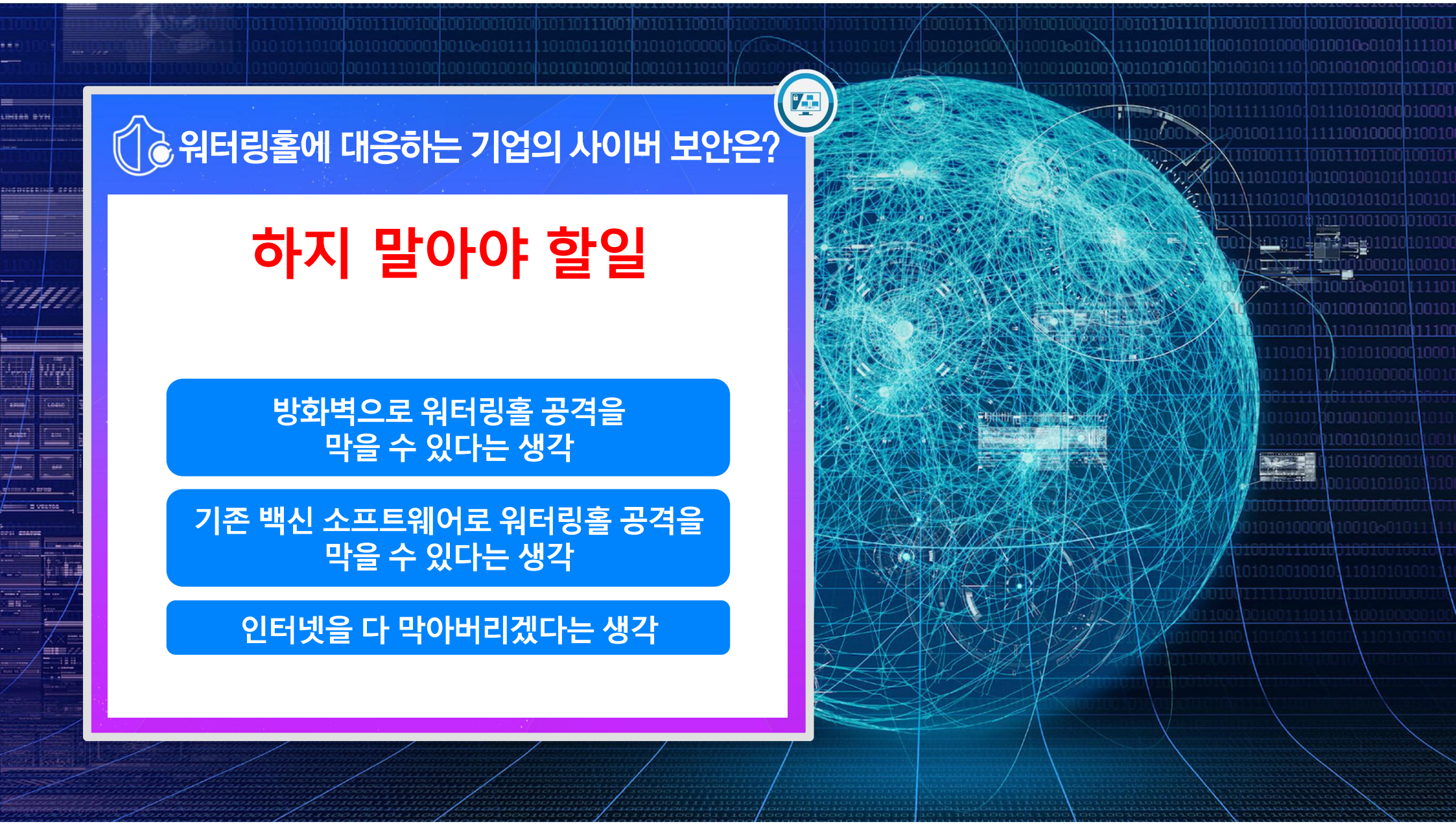
- 취약점 공격에 노출 될 수 있는 윈도우와 주요 소프트웨어의 최신 업데이트 상태를 점검
- 최신 업데이트 즉시 설치(윈도우 업데이트) 및 제작자 설치 링크 제공
- 점검 항목

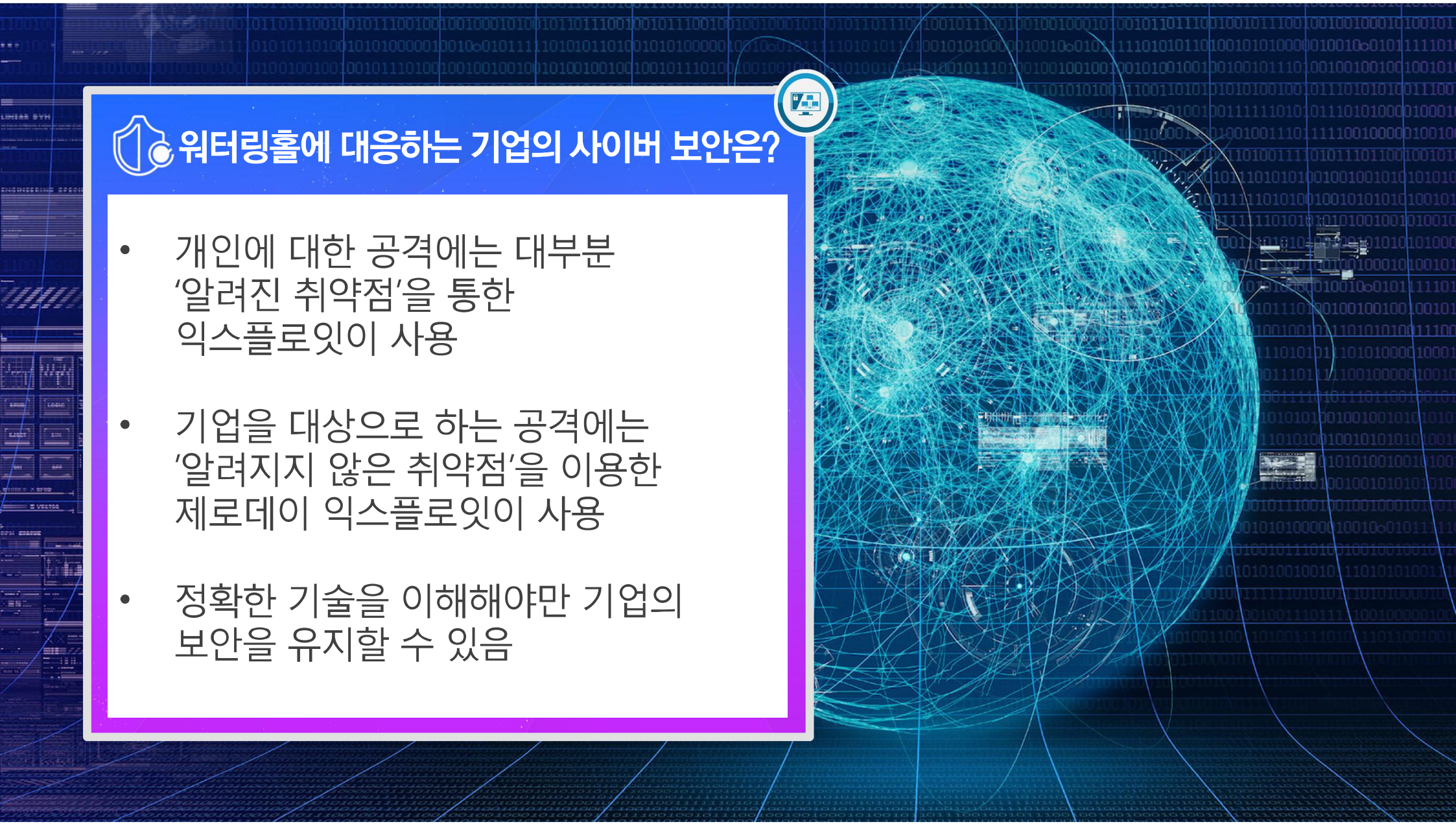
  * 소프트웨어 업데이트

  Java / Adobe (Flash Player, Reader, AIR 등) / 브라우저 (Chrome, Firefox) / 국내 주요 프로그램 (한컴 오피스, 곰플레이어, 파일질라 등)

  * 윈도우 업데이트

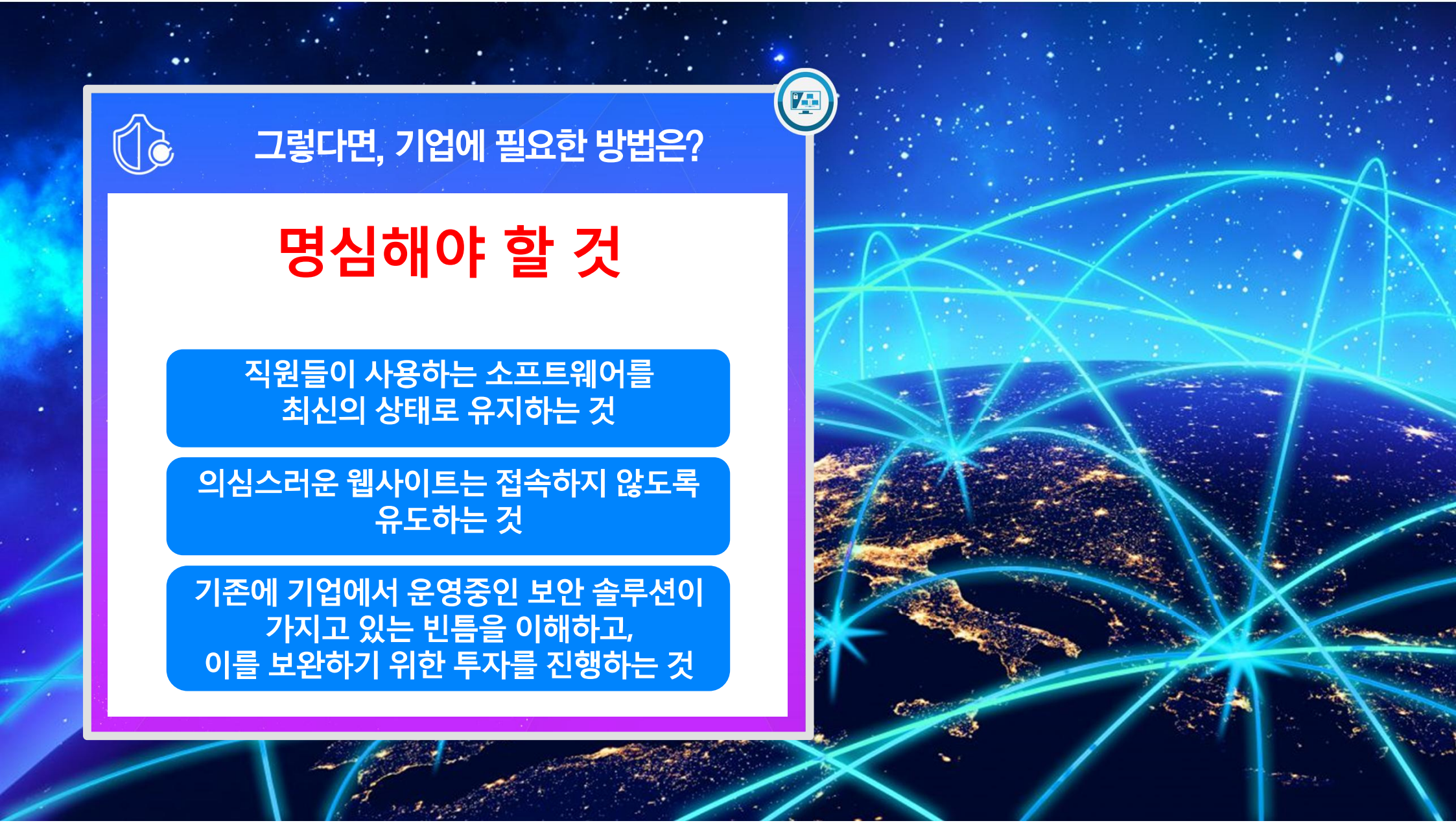
  Windows Update (Windows XP, Vista, 7,8,10) / Microsoft Office, Internet Explorer 업데이트 포함


워터링홀에 대응하는 기업의 사이버 보안은?
하지 말아야 할일
방화벽으로 워터링홀 공격을 막을 수 있다는 생각
기존 백신 소프트웨어로 워터링홀 공격을 막을 수 있다는 생각
인터넷을 다 막아버리겠다는 생각



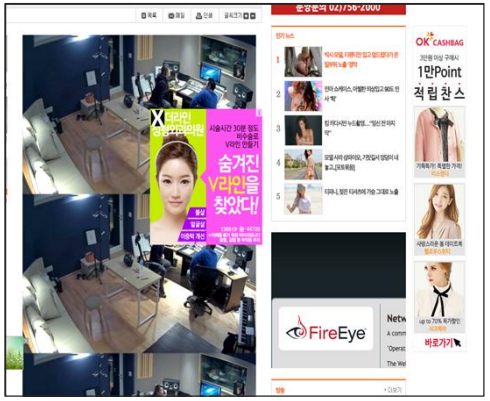
워터링홀에 대응하는 기업의 사이버 보안은?

- 개인에 대한 공격에는 대부분 '알려진 취약점'을 통한 익스플로잇이 사용
- 기업을 대상으로 하는 공격에는 '알려지지 않은 취약점'을 이용한 제로데이 익스플로잇이 사용
- 정확한 기술을 이해해야만 기업의 보안을 유지할 수 있음

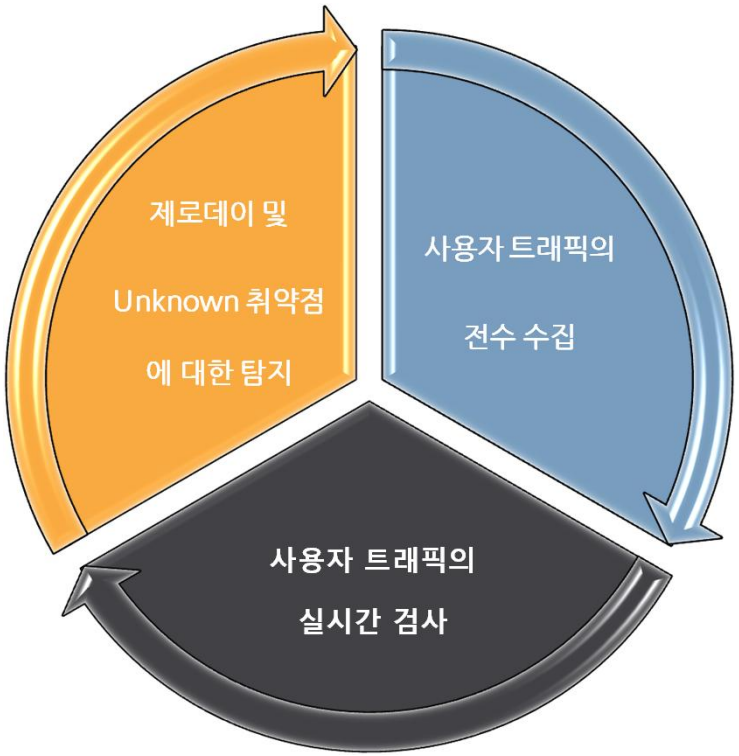

그렇다면, 기업에 필요한 방법은?
명심해야 할 것
직원들이 사용하는 소프트웨어를
최신의 상태로 유지하는 것
의심스러운 웹사이트는 접속하지 않도록
유도하는 것
기존에 기업에서 운영중인 보안 솔루션이
가지고 있는 빈틈을 이해하고,
이를 보완하기 위한 투자를 진행하는 것

그렇다면, 기업에 필요한 방법은?

샌드박스 / 머신러닝 / 빅데이타등의
최신 기술이 적용되어 있는
기업용 보안 솔루션을 이용한
적극적인 대응 및 방어가 필요



왜 워터링홀 공격에 대한 방어가 어려운가?




랜섬웨어 예방 및
사이버 보안의 첫 걸음
전사원을 교육하라!
이메일을 통한 해킹기법
스피어피싱

이메일을 이용한 해킹

소니 픽처스 해킹 수법, 지난해 한국 금융기관 해킹한 북한 수법과 흡사… FBI 수사 착수

기사등록 일시 : [2014-12-02 16:57:02] 최종수정 일시 : [2014-12-02 18:07:19]

이메일을 이용한 해킹

etnews.com 전자신문 http://www.etnews.com

[정보보호]국내 원전·국방 노린 사이버테러 감지..홀수 해 악몽 재현되나

[2014년 12월 15일]

원자력발전소 등 국내 주요 기반시설을 노린 사이버테러 징후가 포착됐다. 매년 홀수 해마다 반복된 대형 사이버테러가 재현될 위험이 최고조에 달했다.
14일 보안 업계는 원자력발전과 국방·안보 기관을 대상으로 한글문서 취약점을 이용한 지능형지속위협(APT) 공격이 감지돼 비상대응에 들어갔다. 공격자는 주요 발전시설 안전 담당자에게 '제어 프로그램'이란 제목의 한글 파일을 보냈다. 관련 문서는 원전 운영에 필요한 주요 내용이 상세히 적힌 기술문서다. 얼핏 봐선 문서에 악성코드가 숨어있는지 알아채기 어렵다.

8월 이후 북한 사이버침투 급증…내년 대규모 사이버테러 가능성

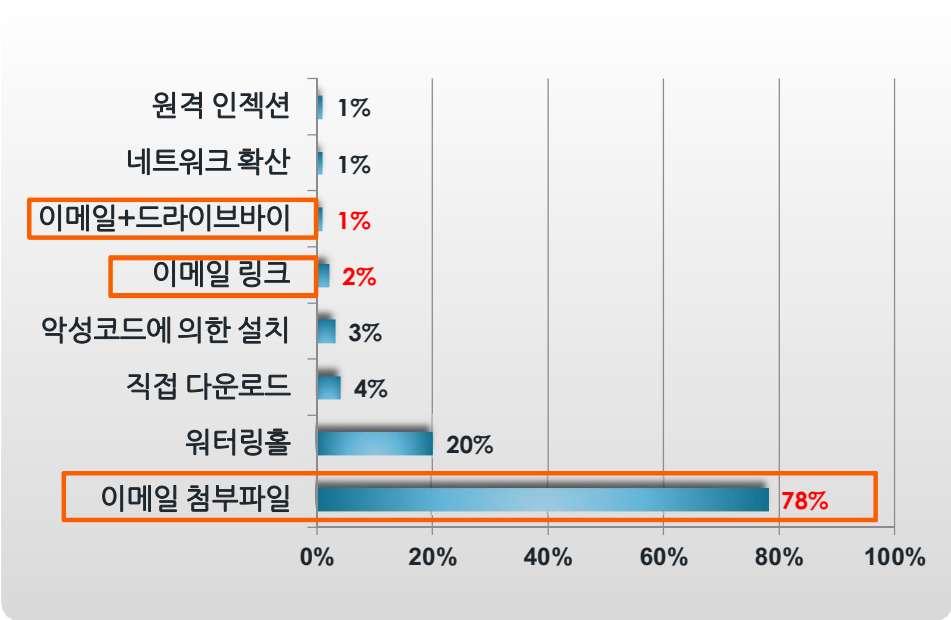
강은성 기자 esther@dt.co.kr | 입력: 2014-11-28 16:09 | 수정: 2014-12-01 10:40

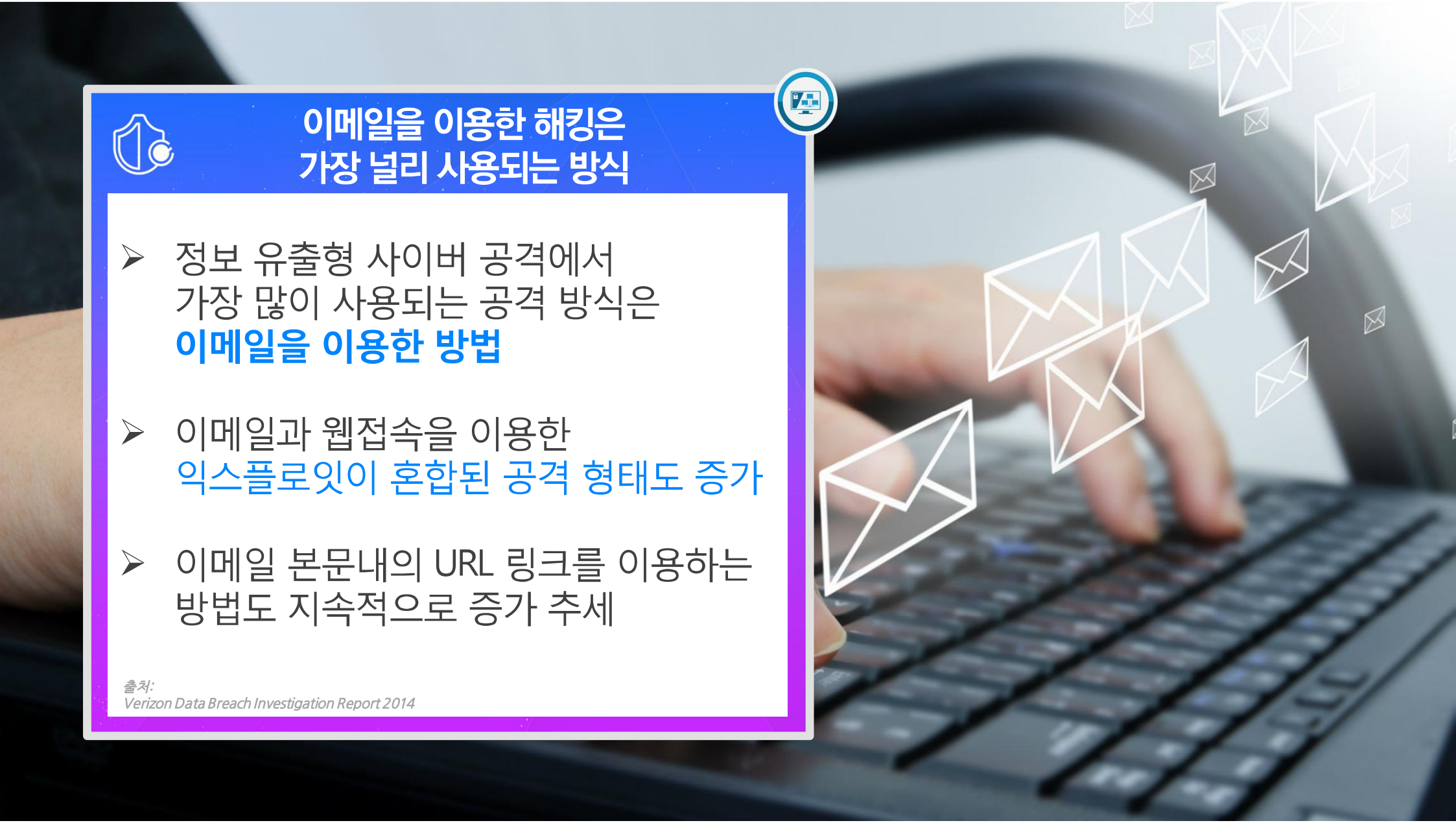
올 하반기 들어 북한으로 추정되는 특정 세력의 국내 악성코드 유포 사실이 확인돼 정부 당국과 이용자들의 각별한 주의가 요구되고 있다.

특히 이번 사이버 침투는 지난해 언론사와 금융사, 정부기관에 막대한 피해를 입힌 3.20 사이버테러와 유사한 지능형지속위협(APT) 공격과 스피어피싱 등의 행태를 보이고 있어 감염이 지속될 경우 또 다른 사이버테러로 이어질 수 있다는 분석이다.

30일 보안업계와 정부 당국에 따르면 지난 8월 이후 북한세력으로 추정되는 공격자들이 한글파일이나 어도비 등 문서 프로그램 취약점, 이메일 공격 등 각종 방법을 동원해 국내에 악성 사이버 공격을 시도한 사실이 있는 것으로 나타났다. 북한 동향을 지속적으로 감시하고 있는 한 전문가 집단은 이 같은 내용을 프로파일링(분석)해 국가정보원 등 관계기관에 공유하고 사이버 공격에 대한 모니터링을 강화할 것을 주문했다.

이메일을 이용한 해킹은 가장 널리 사용되는 방식

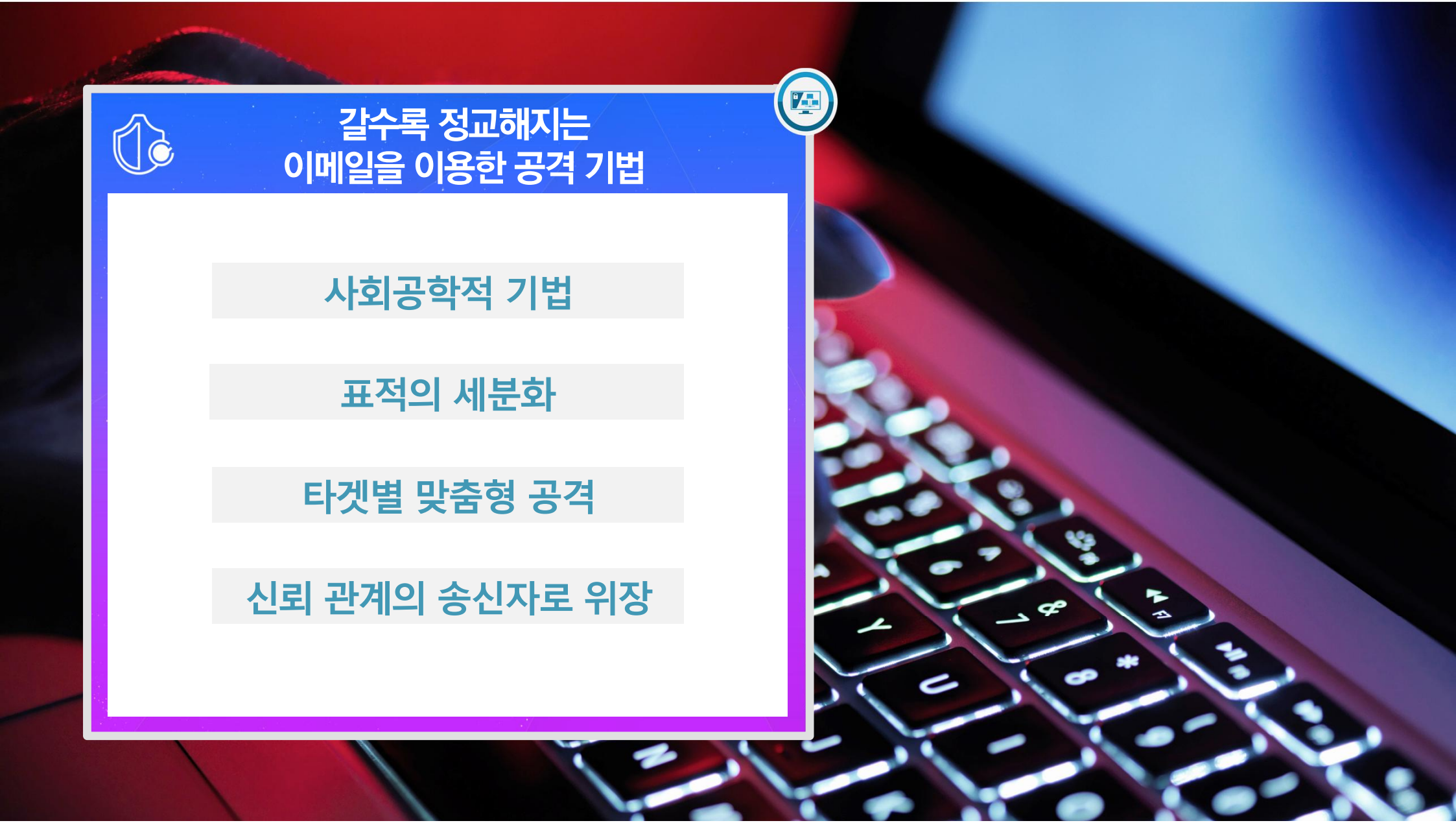




이메일을 이용한 해킹은 가장 널리 사용되는 방식

- 정보 유출형 사이버 공격에서 가장 많이 사용되는 공격 방식은 **이메일을 이용한 방법**
- 이메일과 웹접속을 이용한 익스플로잇이 혼합된 공격 형태도 증가
- 이메일 본문내의 URL 링크를 이용하는 방법도 지속적으로 증가 추세

출처:
Verizon Data Breach Investigation Report 2014

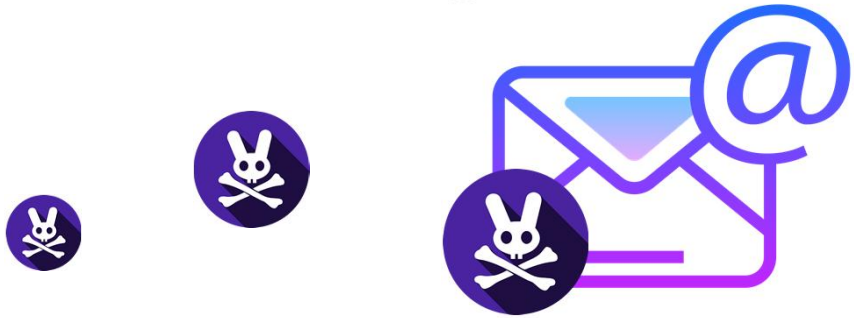


갈수록 정교해지는 이메일을 이용한 공격 기법

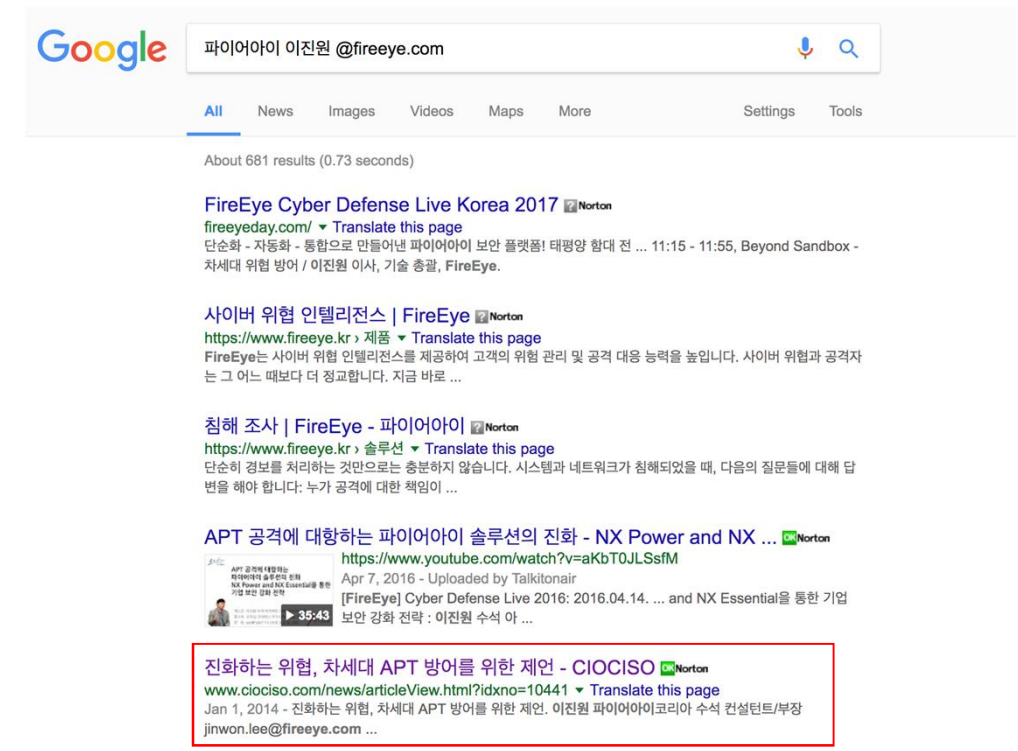
- 사회공학적 기법
- 표적의 세분화
- 타겟별 맞춤형 공격
- 신뢰 관계의 송신자로 위장

개인의 이메일 정보 유출

- 인터넷 서핑(구글링)이나 소셜미디어를 통해서 이메일 주소를 쉽게 획득 가능
- 추가적인 툴을 이용하면, 특정 기업에 대한 이메일 주소등을 몇번의 클릭만으로 획득 가능



개인의 이메일 정보 유출


Google
파이어아이 이진원 @fireeye.com
All News Images Videos Maps More Settings Tools
About 681 results (0.73 seconds)
FireEye Cyber Defense Live Korea 2017
fireeyeday.com/ Translate this page
단순화 - 자동화 - 통합으로 만들어낸 파이어아이 보안 플랫폼! 태평양 함대 전 ... 11:15 - 11:55, Beyond Sandbox - 차세대 위협 방어 / 이진원 이사, 기술 총괄, FireEye.
사이버 위협 인텔리전스 | FireEye
https://www.fireeye.kr › 제품 Translate this page
FireEye는 사이버 위협 인텔리전스를 제공하여 고객의 위협 관리 및 공격 대응 능력을 높입니다. 사이버 위협과 공격자는 그 어느 때보다 더 정교합니다. 지금 바로 ...
침해 조사 | FireEye - 파이어아이
https://www.fireeye.kr › 솔루션 Translate this page
단순히 경보를 처리하는 것만으로는 충분하지 않습니다. 시스템과 네트워크가 침해되었을 때, 다음의 질문들에 대해 답변을 해야 합니다: 누가 공격에 대한 책임이 ...
APT 공격에 대항하는 파이어아이 솔루션의 진화 - NX Power and NX ...
35:43
https://www.youtube.com/watch?v=aKbT0JLSsfM
Apr 7, 2016 - Uploaded by Talkitonair
[FireEye] Cyber Defense Live 2016: 2016.04.14. ... and NX Essential을 통한 기업 보안 강화 전략 : 이진원 수석 아 ...
진화하는 위협, 차세대 APT 방어를 위한 제언 - CIOCISO
www.ciociso.com/news/articleView.html?idxno=10441 Translate this page
Jan 1, 2014 - 진화하는 위협, 차세대 APT 방어를 위한 제언. 이진원 파이어아이코리아 수석 컨설턴트/부장 jinwon.lee@fireeye.com ...

개인의 이메일 정보 유출

ciociso 매거진

Upadte : 2017.9.14 Thu 11:18

COVER STORY | CIOCISO | ARTICLES | CIOCISO프로그램 | 회사소개

기고

진화하는 위협, 차세대 APT 방어를 위한 제언

이진원 파이어아이코리아 수석 컨설턴트/부장 | jinwon.lee@fireeye.com

[294호] 승인 2014.01.01

진화하는 위협, 차세대 APT 방어를 위한 제언

이진원 파이어아이코리아 수석 컨설턴트/부장 jinwon.lee@fireeye.com

전 세계적으로 지능형 지속위협에 대한 관심이 고조된 가운데, 최근 시장 조사기관인 IDC는 APT 솔루션 영역을 'STAP(Specialized Threat Analysis and Protection)'라는 보안 영역으로 새롭게 지정했다. 사이버 스파이 행위나 데이터 유출을 목표로 하는 진화된 위협에 대응하는 비(非)시그니처 기반의 악성코드 탐지와 방어시스템을 특수한 보안 시장 영역으로 새롭게 지정한 것이다.

국내 역시 올해 최대의 보안 화두는'APT'였다. 주요 방송사와 금융기관을 공격했던 3.20 사이버 공격에서 국가기관 및 언론사 서버를 공격했던 6.25 사이버 테러까지 진화된 형태의 APT 공격은 각종 보안사고를 연이어 일으키며 국내외를 떠들썩하게 만들었다. 이제 APT는 더 이상 낯선 보안 용어가 아닌, 반드시 대비해야 할 보안 위협으로

이번호 보기

제298호 2014년 5월 1일

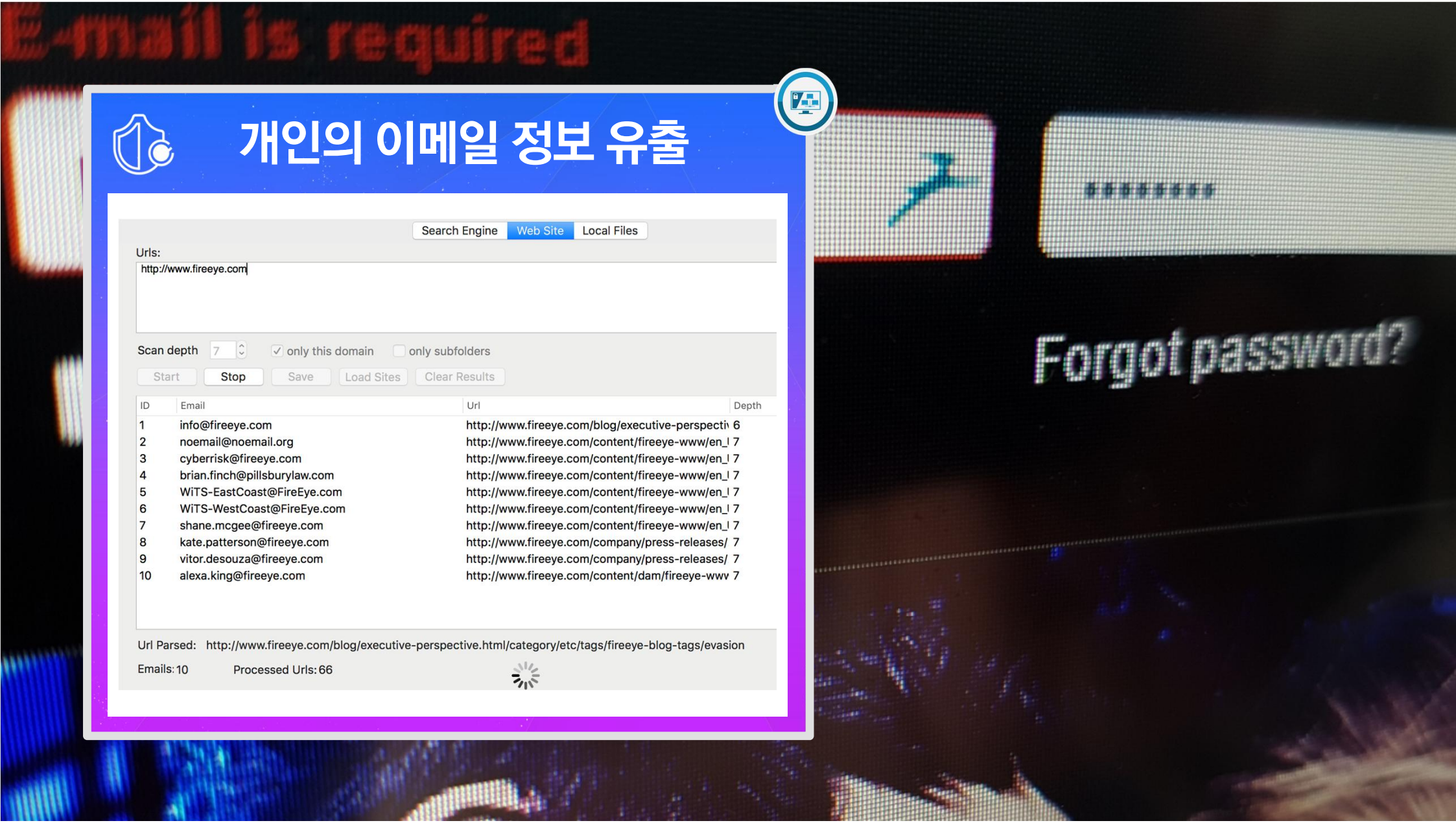
구독신청

최근인기기사

1 interview | 김상철 텔스트

2 Cover story | AIA생명 김

3 interview | 송상엽 한컴시



개인의 이메일 정보 유출

Search Engine | Web Site | Local Files

Urls:

http://www.fireeye.com

Scan depth 7 only this domain only subfolders

Start | Stop | Save | Load Sites | Clear Results

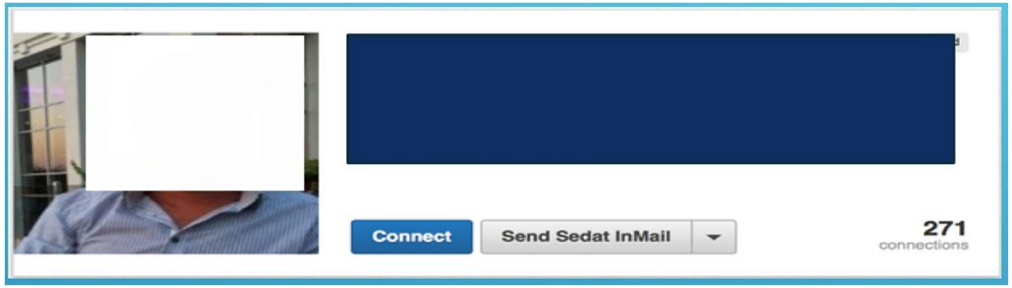
ID	Email	Url	Depth
1	info@fireeye.com	http://www.fireeye.com/blog/executive-perspecti	6
2	noemail@noemail.org	http://www.fireeye.com/content/fireeye-www/en_l	7
3	cyberrisk@fireeye.com	http://www.fireeye.com/content/fireeye-www/en_l	7
4	brian.finch@pillsburylaw.com	http://www.fireeye.com/content/fireeye-www/en_l	7
5	WiTS-EastCoast@FireEye.com	http://www.fireeye.com/content/fireeye-www/en_l	7
6	WiTS-WestCoast@FireEye.com	http://www.fireeye.com/content/fireeye-www/en_l	7
7	shane.mcgee@fireeye.com	http://www.fireeye.com/content/fireeye-www/en_l	7
8	kate.patterson@fireeye.com	http://www.fireeye.com/company/press-releases/	7
9	vitor.desouza@fireeye.com	http://www.fireeye.com/company/press-releases/	7
10	alexa.king@fireeye.com	http://www.fireeye.com/content/dam/fireeye-www	7

Url Parsed: http://www.fireeye.com/blog/executive-perspective.html/category/etc/tags/fireeye-blog-tags/evasion

Emails: 10 Processed Urls: 66

실제 스피어피싱 공격의 사례 #1

공격 대상 정보 수집

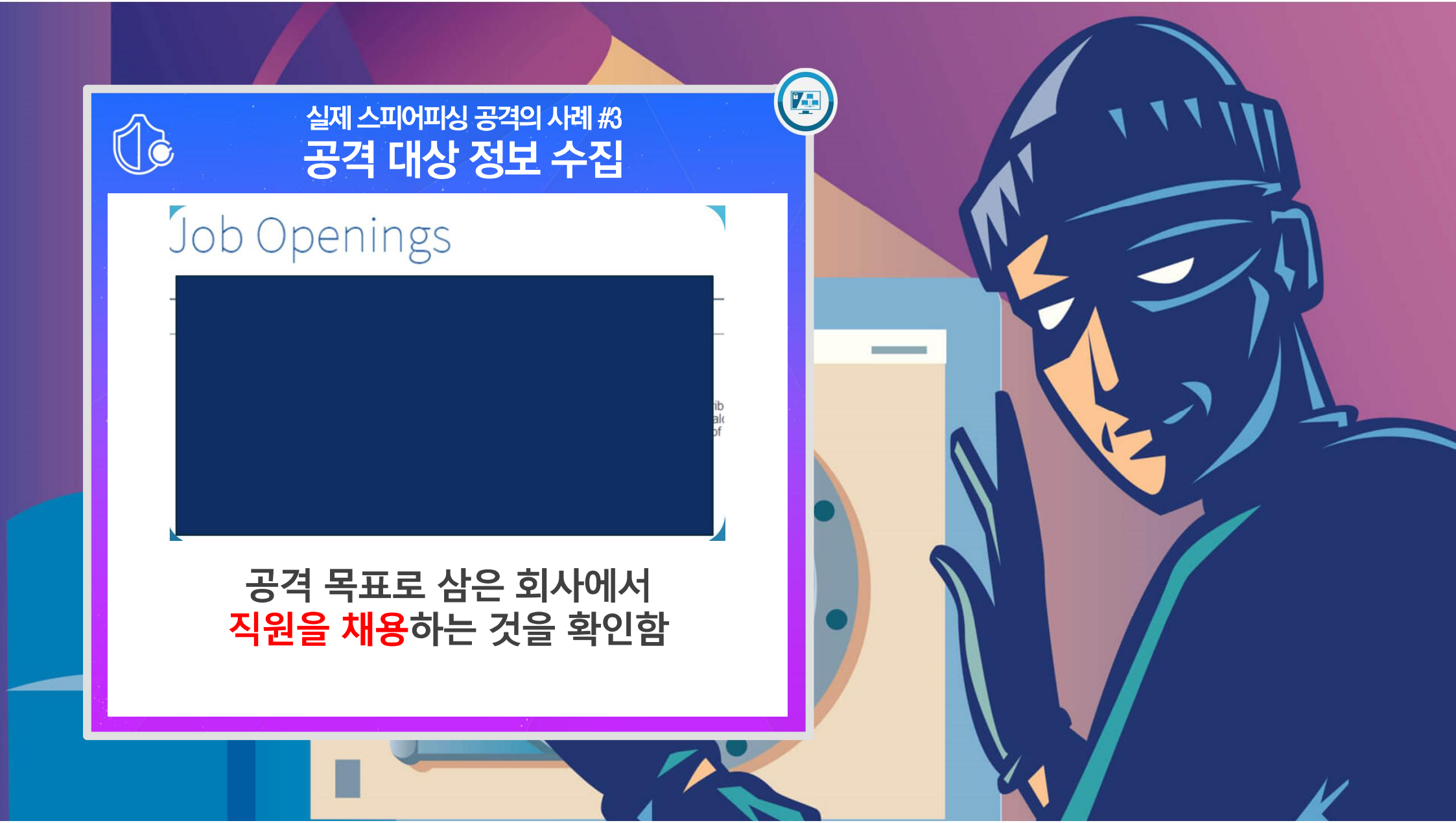


공격 대상 회사의 '**웹개발자**'의
이메일 정보를 SNS통해서 획득

실제 스피어피싱 공격의 사례 #2

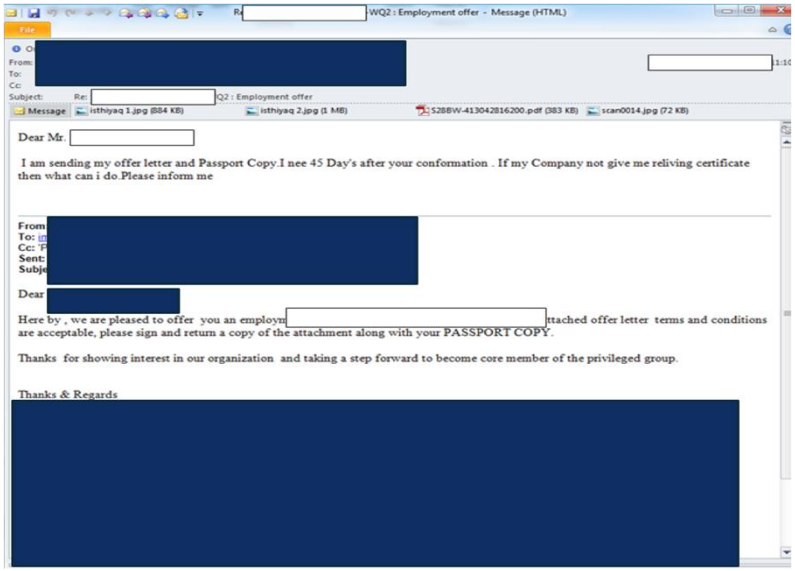
관심 분야로 공격

공격 대상의 **관심분야로 위장**한
이메일 발송


실제 스피어피싱 공격의 사례 #3
공격 대상 정보 수집
Job Openings
공격 목표로 삼은 회사에서
직원을 채용하는 것을 확인함

실제 스피어피싱 공격의 사례 #3

공격 대상 정보 수집



Dear Mr. [redacted]

I am sending my offer letter and Passport Copy.I nee 45 Day's after your conformation . If my Company not give me reliving certificate then what can i do.Please inform me

From [redacted]
To: [redacted]
Cc: [redacted]
Sent: [redacted]
Subj[redacted]

Dear [redacted]

Here by , we are pleased to offer you an employm[redacted]ttached offer letter terms and conditions are acceptable, please sign and return a copy of the attachment along with your PASSPORT COPY.

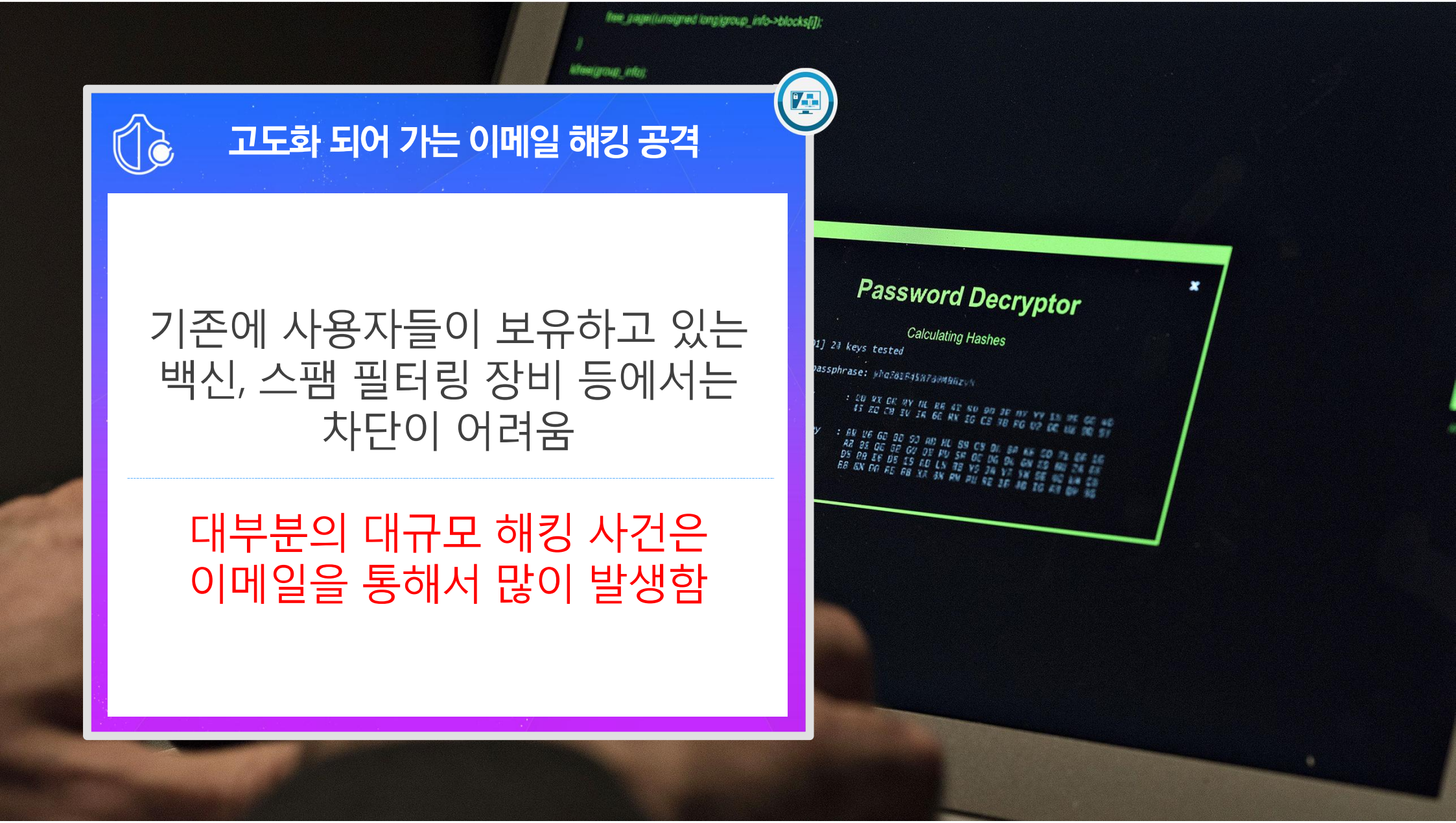
Thanks for showing interest in our organization and taking a step forward to become core member of the privileged group.

Thanks & Regards

[redacted]

채용 면접에 응시하는 것으로
위장하여서 공격 수행

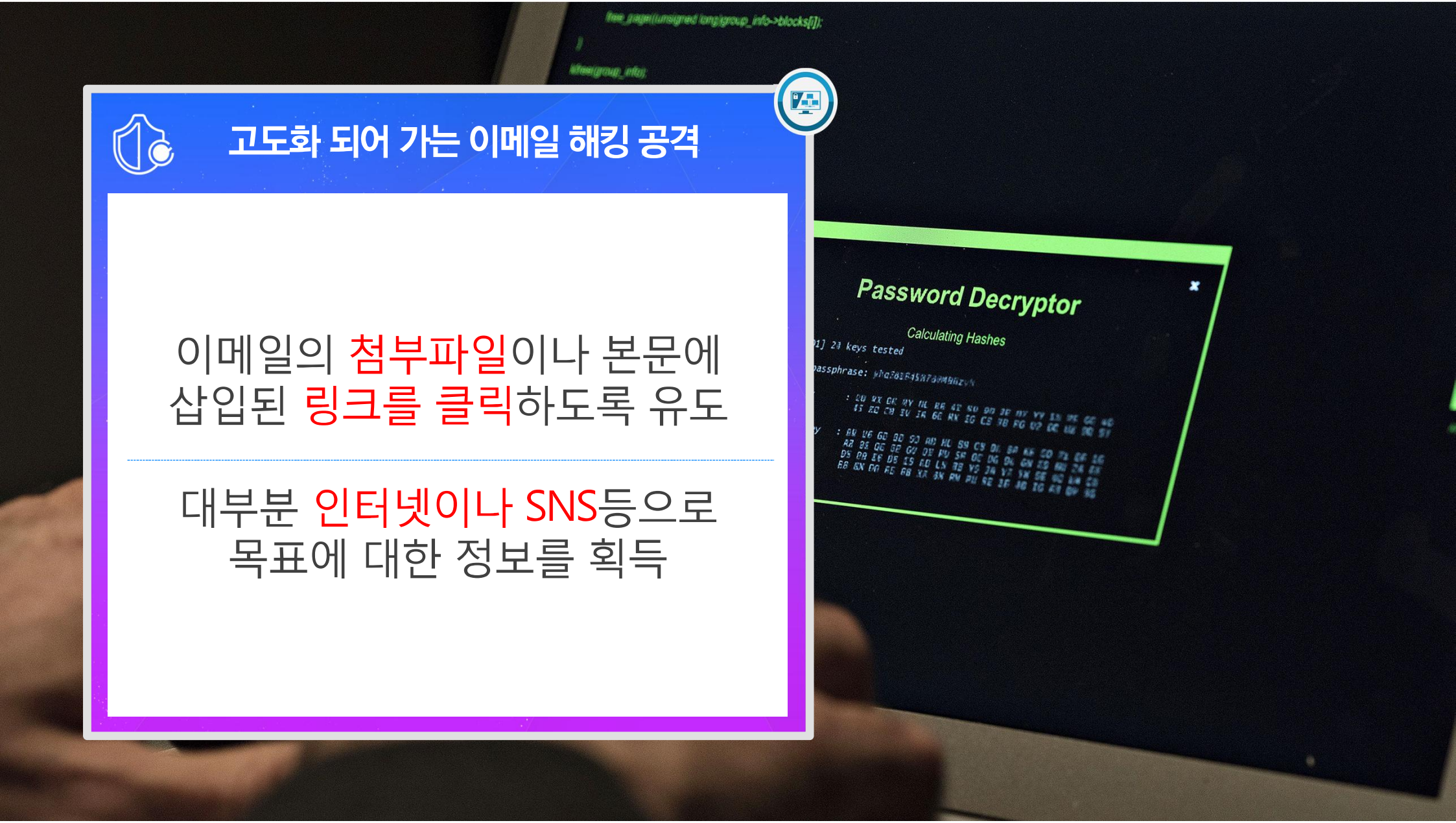
실제 스피어피싱 공격 동작 영상



고도화 되어 가는 이메일 해킹 공격

기존에 사용자들이 보유하고 있는
백신, 스팸 필터링 장비 등에서는
차단이 어려움

대부분의 대규모 해킹 사건은
이메일을 통해서 많이 발생함

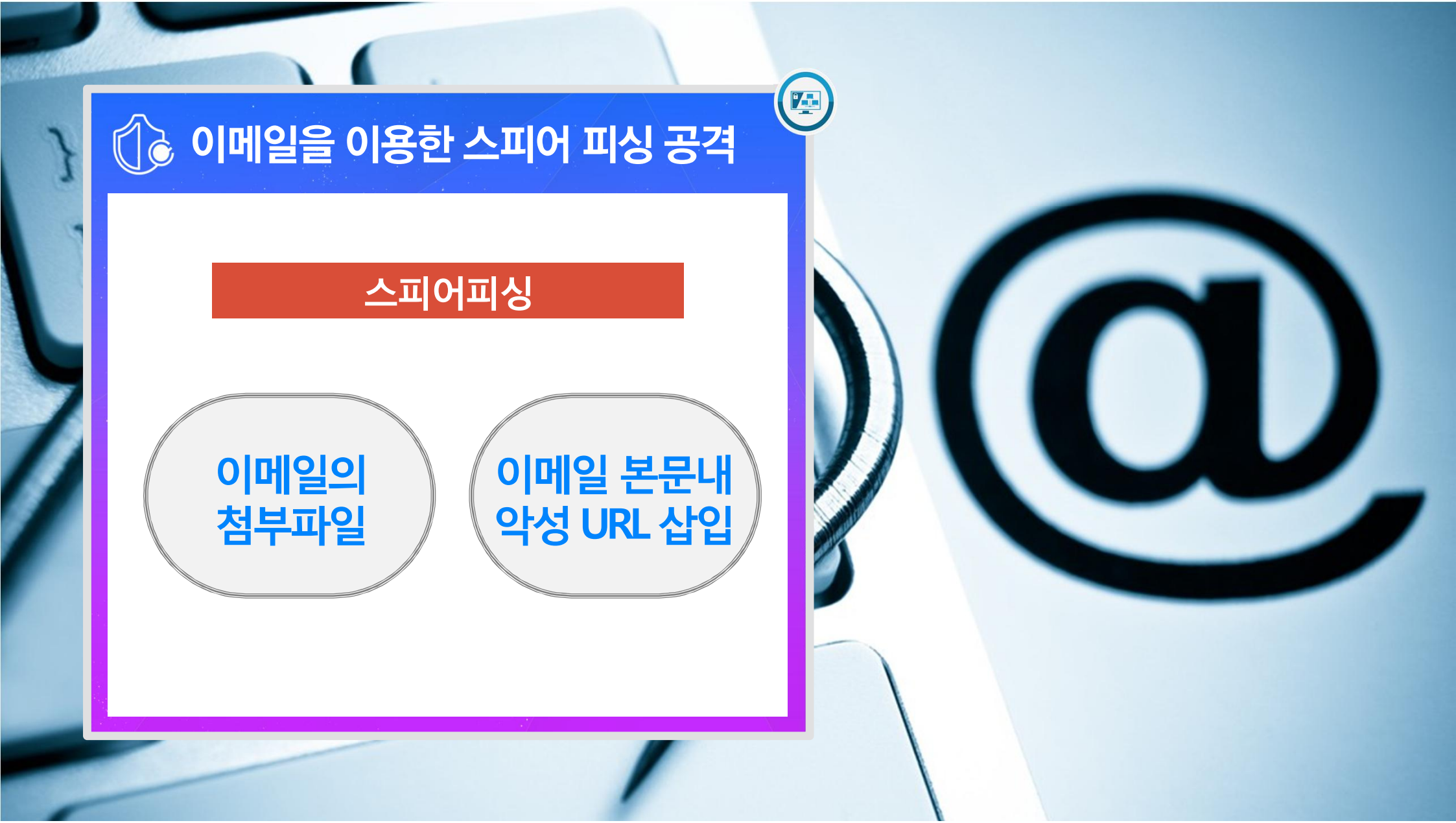


고도화 되어 가는 이메일 해킹 공격

이메일의 첨부파일이나 본문에
삽입된 링크를 클릭하도록 유도

대부분 인터넷이나 SNS등으로
목표에 대한 정보를 획득


랜섬웨어 예방 및
사이버 보안의 첫 걸음
전사원을 교육하라!
스피어피싱 공격의
피해를 막는 방법


이메일을 이용한 스피어 피싱 공격
스피어피싱
이메일의
첨부파일
이메일 본문내
악성 URL 삽입

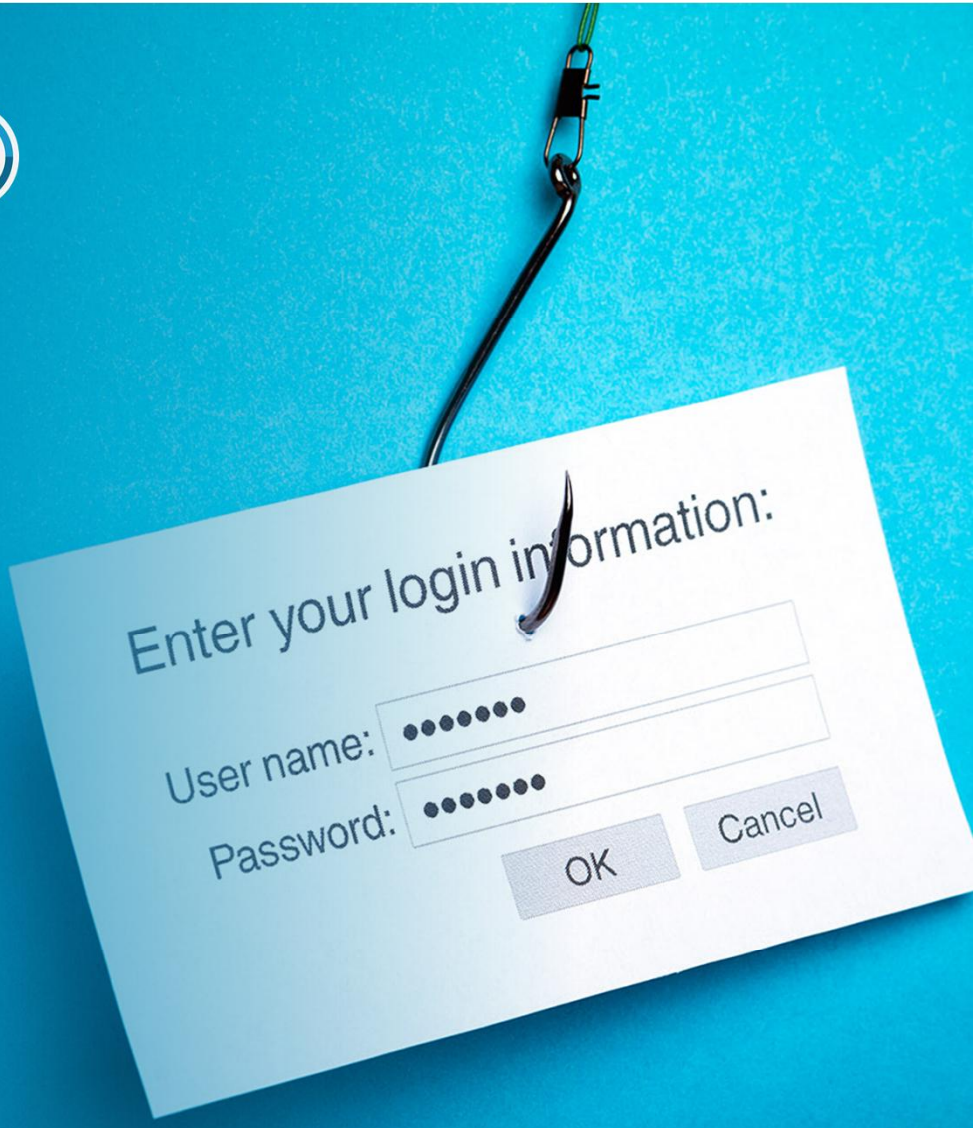
기본적인 주의 사항

① 의심되는 이메일의 첨부파일은
절대 열어 보지말 것

② 이메일에 포함되어 있는 URL을
클릭할때 주의할 것

③ 사용하는 PC 소프트웨어와 운영체제는
항상 최신 버전으로 유지할 것

④ 백신 소프트웨어의 자동 검사 기능을
항상 사용할 것

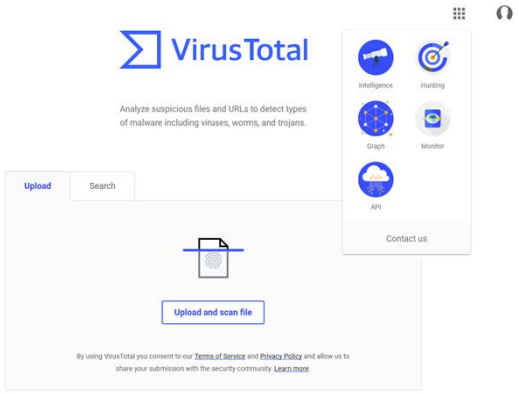


개인이 사용 가능한 방법

바이러스토탈

➢ 바이러스 토탈

- 바이러스 토탈(www.virustotal.com)은 Google이 운영하는 전세계 최대의 무료 보안 검사 및 공유 사이트



개인이 사용 가능한 방법

바이러스토탈

➢ 바이러스 토탈

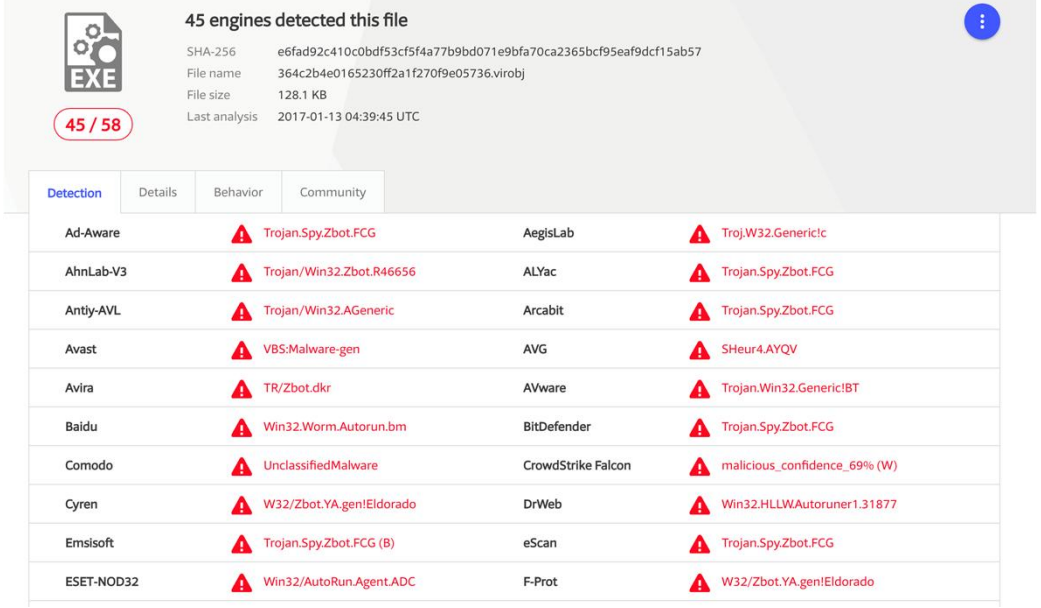
- 바이러스 토탈에는 전세계 59개의 백신 엔진과 65개의 웹사이트 검사 엔진을 무료로 제공

- 의심스러운 웹사이트에는 접속하기 이전에 바이러스 토탈등에서 검사 후에 안전성 여부를 확인 후에 접속하는 것이 좋음

개인이 사용 가능한 방법

바이러스토탈

➤ 바이러스 토탈

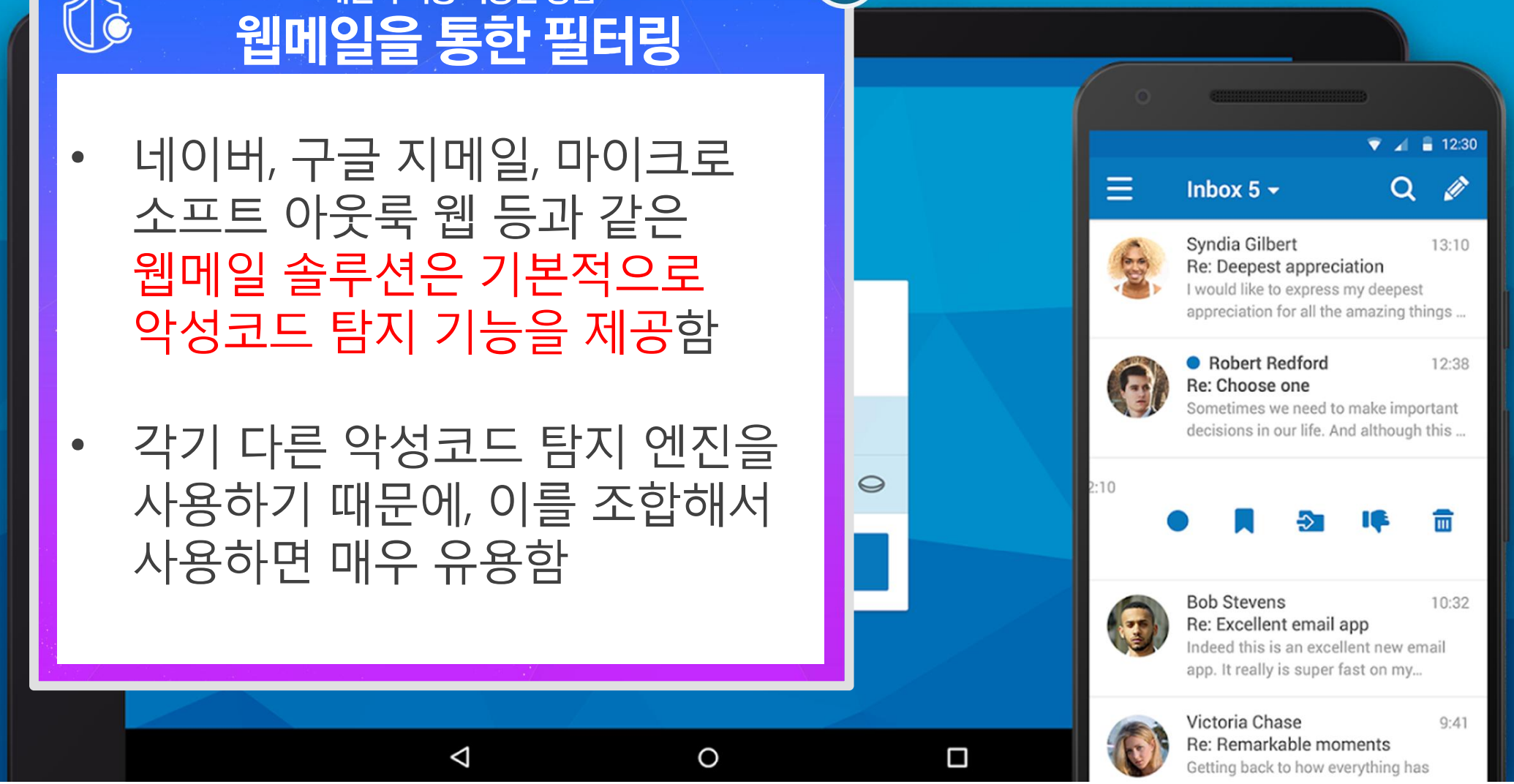


개인이 사용 가능한 방법

웹메일을 통한 필터링

- 네이버, 구글 지메일, 마이크로소프트 아웃룩 웹 등과 같은 웹메일 솔루션은 기본적으로 악성코드 탐지 기능을 제공함

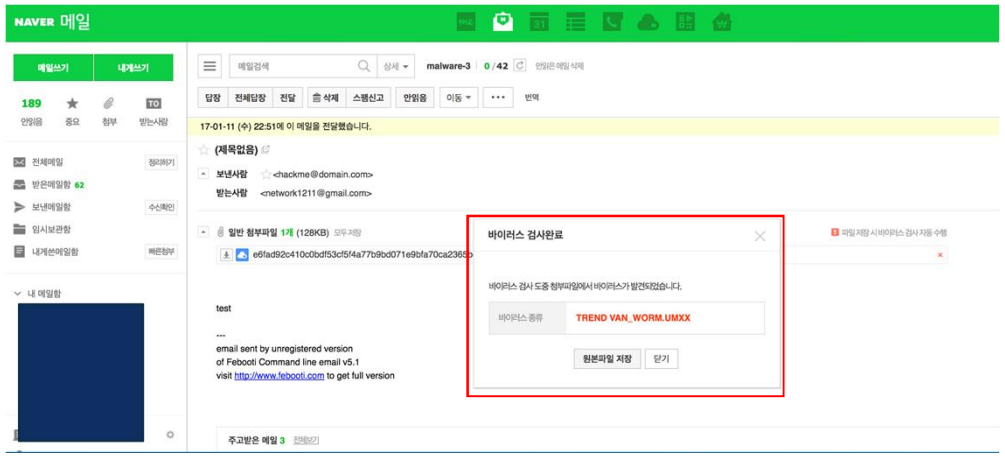
- 각기 다른 악성코드 탐지 엔진을 사용하기 때문에, 이를 조합해서 사용하면 매우 유용함

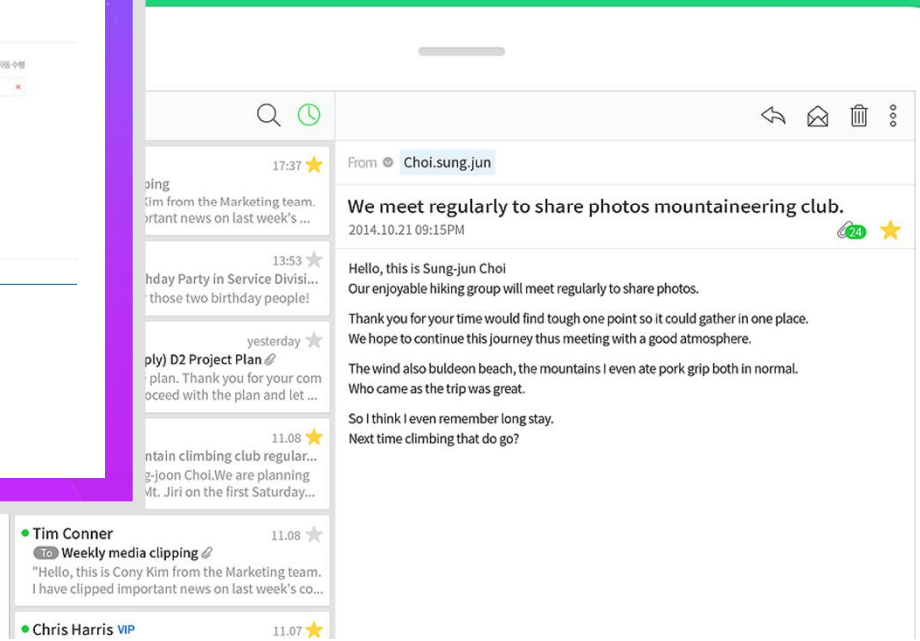



개인이 사용 가능한 방법
웹메일을 통한 필터링
1차 웹메일
• 구글의 지메일 설정
• test@gmail.com
• 자동으로 모든 메일을 네이버로 포워딩 하도록 설정
2차 필터링
2차 웹메일
• 네이버 메일 설정
• test@naver.com
12:30
13:10
st appreciation
o express my deepest
for all the amazing things ...
Redford
12:38
make important
d although this ...
10:32
ent new email
9:41
Re: Remarkable moments
Getting back to how everything has

개인이 사용 가능한 방법

웹메일을 통한 필터링





중소기업 사용 가능한 방법

클라우드 기반 이메일

- 클라우드 기반의 서비스로,
  스팸 필터링과 이메일 악성코드 탐지 /
  차단 서비스를 함께 제공하는 서비스
- 1인당 연간 백신 소프트웨어와
  비슷한 수준의 가격
- 클라우드 기반이므로, 큰 비용
  부담 없이 사용 가능한 것이 장점

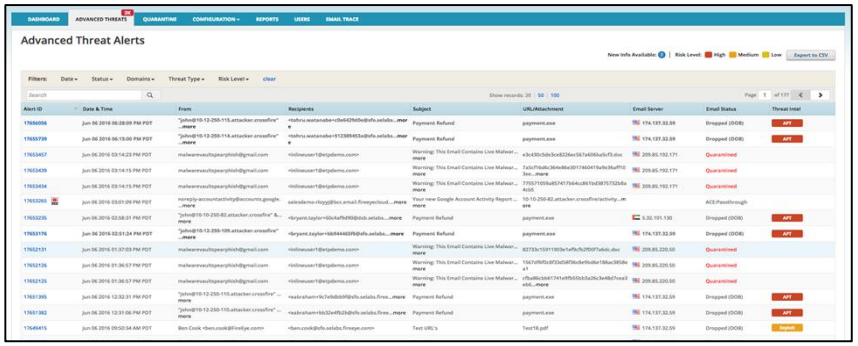
중소기업 사용 가능한 방법

클라우드 기반 이메일

FireEye 제품 서비스 솔루션 Fuel 파트너 프로그램 지원 리소스 회사

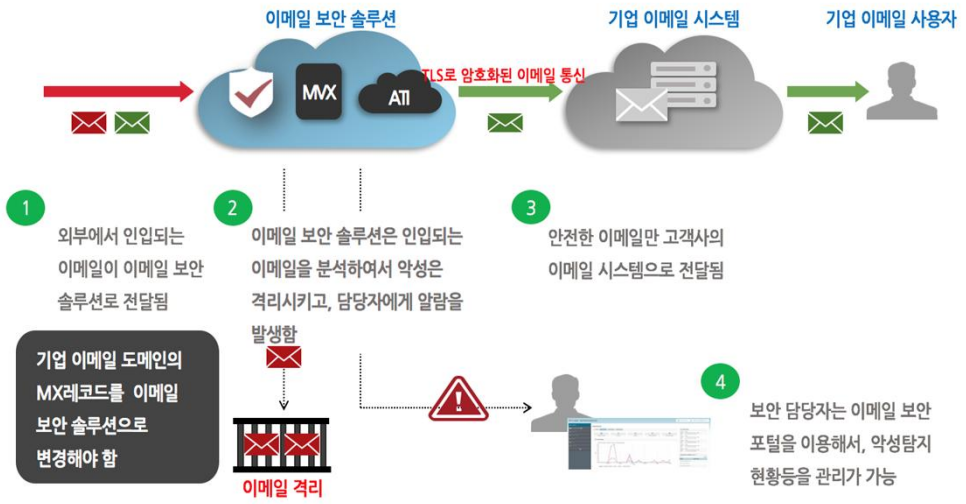
인텔리전스 기반 이메일 방어

- **FireEye MVX 엔진**
  모든 이메일의 모든 첨부 파일 및 URL을 분석하여 스피어 피싱을 차단합니다.
- **이메일 자동 격리**
  추가 분석 또는 삭제를 위해 실시간으로 악성 이메일을 격리합니다.
- **ATI(지능형 위협 인텔리전스)**
  위협 억제를 가속화하고 노이즈와 허위 경보를 최소화합니다.
- **맞춤형 YARA 규칙 지원**
  조직을 표적으로 삼은 위협의 첨부 파일을 분석할 수 있습니다.
- **인증 피싱 및 타이포스쿼팅 방어**
  스피어 피싱 이메일에서 시작된 표적 공격을 탐지하고 저지합니다.
- **메시지 주석**
  스팸한 이메일에 대한 가시성 및 제어를 강화합니다.
- **제로데이 공격에 대한 동적 분석**
  OS, 브라우저 및 애플리케이션 취약점을 악용하는 공격을 저지합니다.
- **쉬운 설치 및 구성**
  운영 비용을 절감하고 보안팀의 효율성을 제고합니다.



대기업 및 전문기관이 사용 가능한 방법

이메일 보안 전용 솔루션



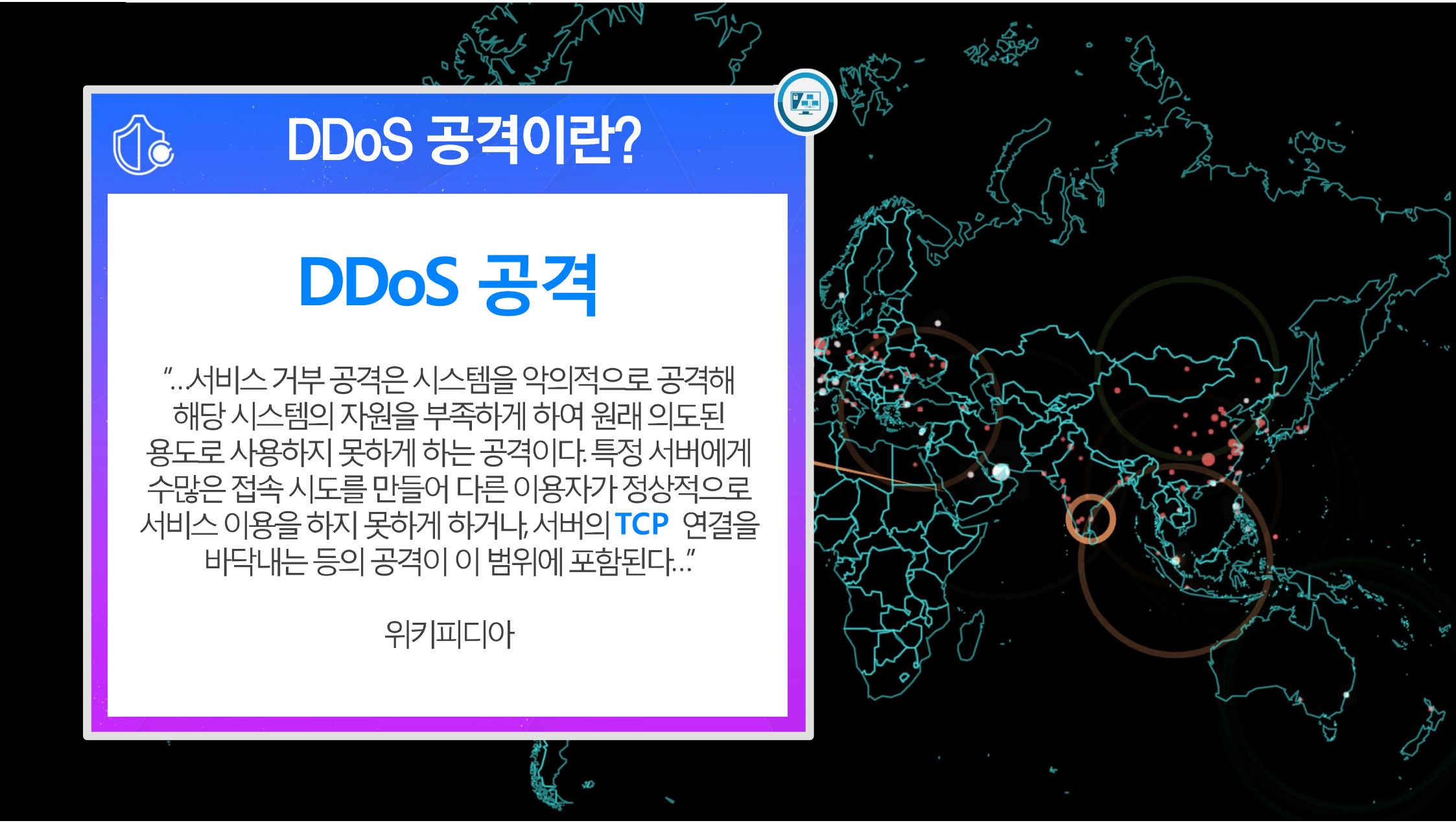
스피어 피싱의 방어 전략

- **이메일은 대규모 해킹 공격에 가장 많이 사용되는 방법**
- 또한, 랜섬웨어 유포 공격에도 많이 사용
- 개인 또한 자신의 정보와 자신이 속한 조직의 보호를 위해서 개인 웹메일을 통한 보안 관리에 신경 써야 함

스피어 피싱의 방어 전략

- 중소기업은 클라우드 기반의 이메일 보안 솔루션의 검토 및 도입의 검토 필요
- 대기업과 전문 기관은 전용 솔루션의 도입이 필요


랜섬웨어 예방 및
사이버 보안의 첫 걸음
전사원을 교육하라!
웹사이트를 마비시키는
분산 서비스 공격(DDoS)



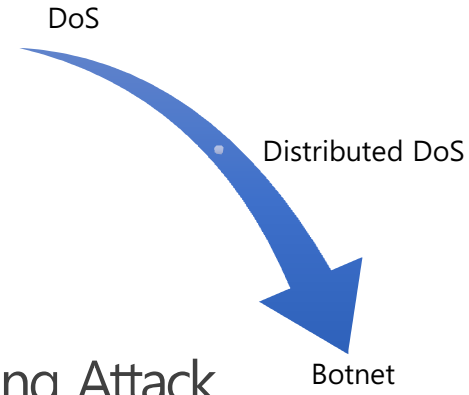
DDoS 공격이란?

DDoS 공격

"..서비스 거부 공격은 시스템을 악의적으로 공격해 해당 시스템의 자원을 부족하게 하여 원래 의도된 용도로 사용하지 못하게 하는 공격이다. 특정 서버에게 수많은 접속 시도를 만들어 다른 이용자가 정상적으로 서비스 이용을 하지 못하게 하거나, 서버의 TCP 연결을 바닥내는 등의 공격이 이 범위에 포함된다.."

위키피디아

DDoS 공격의 역사



DDoS

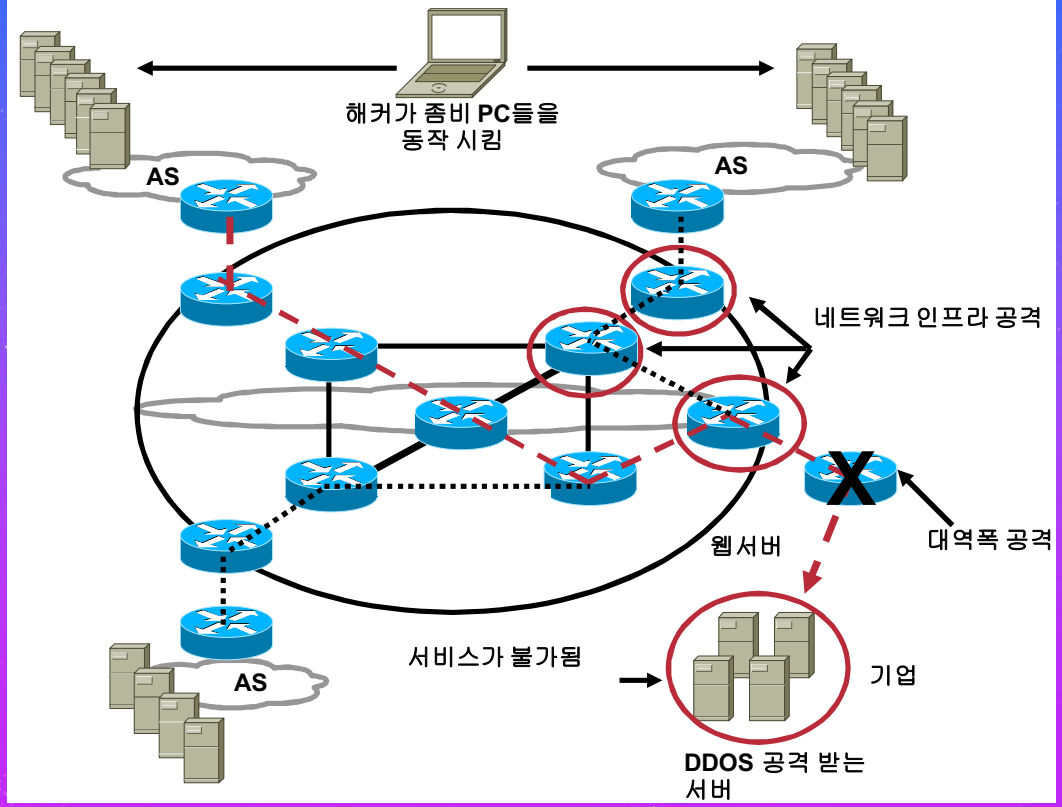
① 1996 - SYN Flooding Attack

② 2000 – Yahoo Attack

③ 2006 - 협박성 DDoS 공격 출현

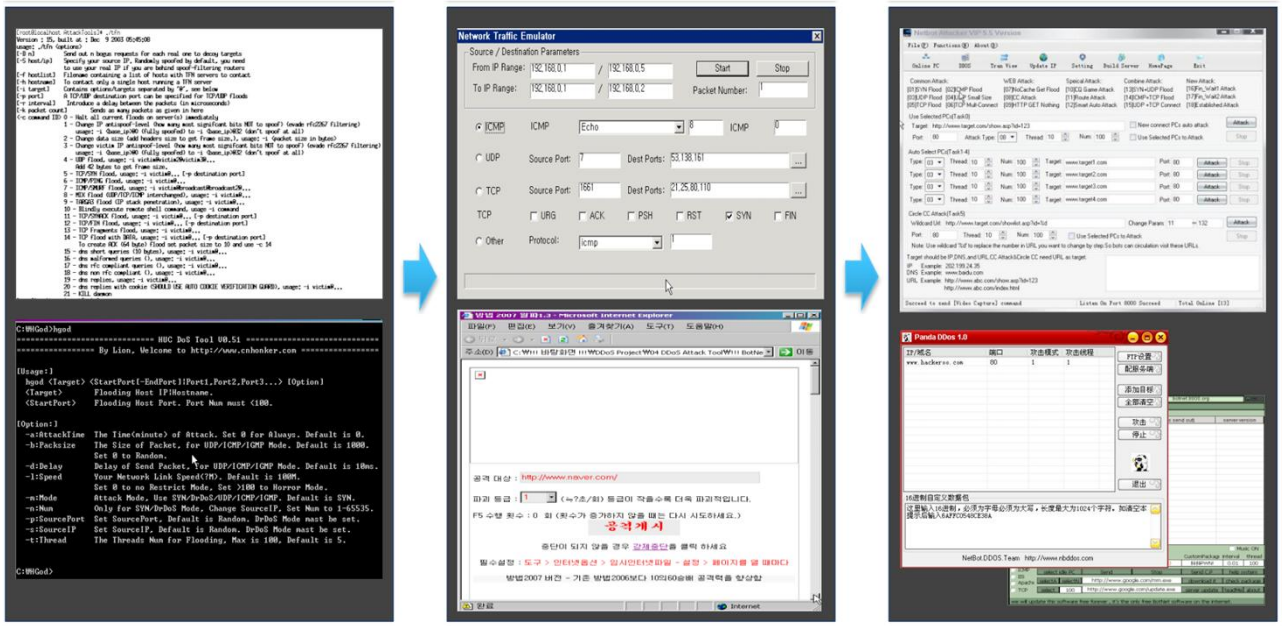
④ 2010 - 정치적 목적의 DDOS 공격 출현

분산 서비스거부 공격(DDOS)



블랙 마켓을 이용한 DDoS 공격 툴 판매

블랙 마켓을 이용한 DDoS 공격 툴 판매



현재까지도 지속적인 위협이 되고 있음

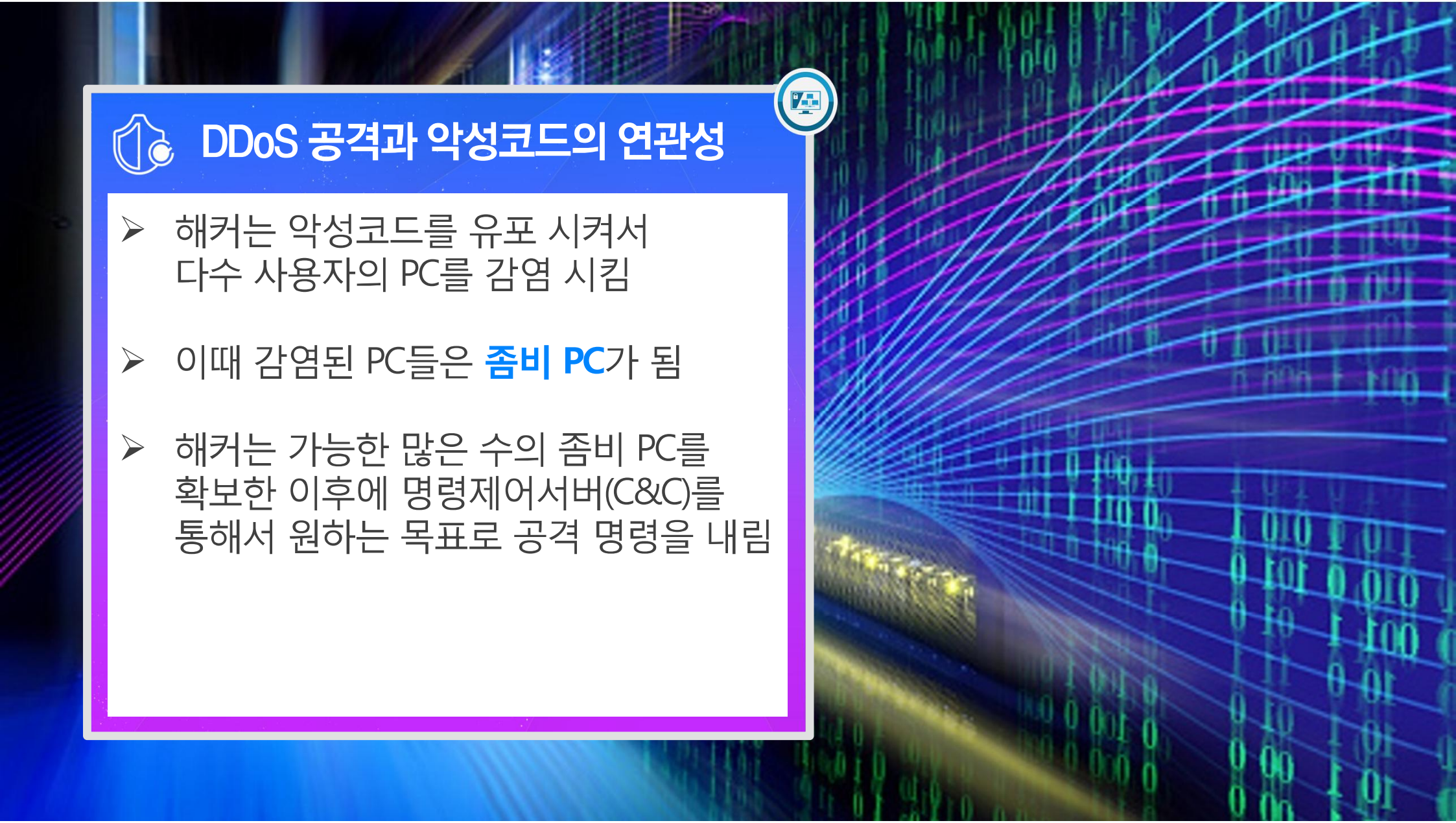
최신기사

국내은행 7곳 디도스공격 협박받아…"26일까지 비트코인 보내라"

송고시간 | 2017/06/21 20:46

(서울=연합뉴스) 이 율 이세원 홍정규 기자 = 국제해킹그룹이 국내 시중은행 7곳에 오는 26일까지 비트코인을 내놓지 않으면 디도스(DDoS·분산서비스거부)공격을 하겠다고 협박한 것으로 확인됐다.

디도스는 서버가 처리할 수 있는 용량을 초과하는 정보를 한꺼번에 보내 과부하를 발생시킴으로써 접속을 지연시키거나 다운시키는 공격 방식이다.

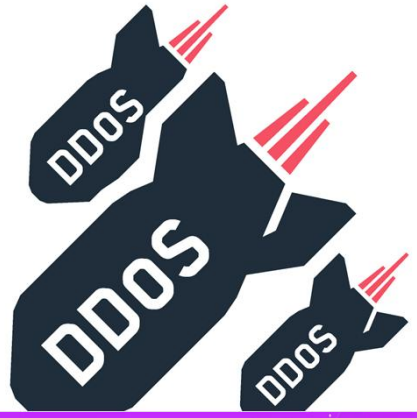


DDoS 공격과 악성코드의 연관성

- 해커는 악성코드를 유포 시켜서 다수 사용자의 PC를 감염 시킴
- 이때 감염된 PC들은 **좀비 PC**가 됨
- 해커는 가능한 많은 수의 좀비 PC를 확보한 이후에 명령제어서버(C&C)를 통해서 원하는 목표로 공격 명령을 내림

DDoS 공격과 악성코드의 연관성

- 수많은 좀비 PC들이 한번에 표적으로 공격을 수행함
- 결국 악성코드에 의한 좀비 PC감염 그리고 봇넷의 구성이 시작점이 됨



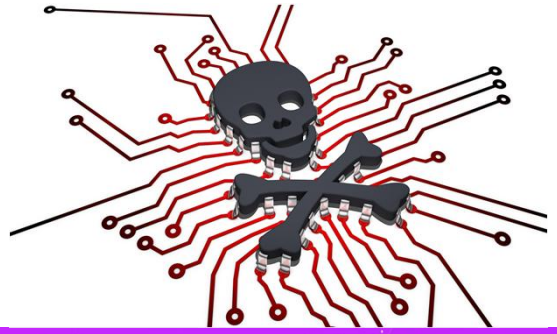
DDOS 공격에 대한 대응 방법

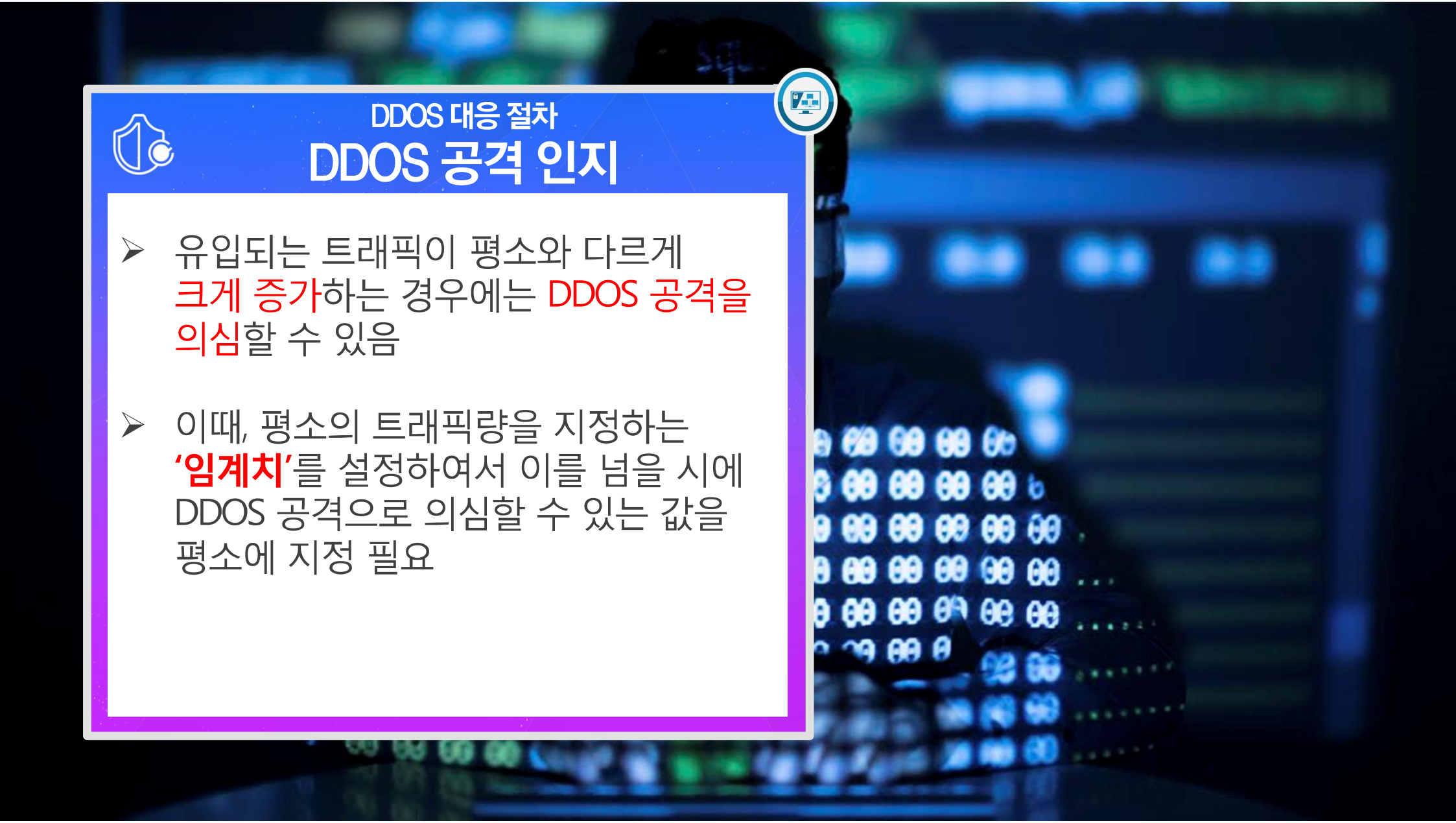
- DDOS 공격의 대응은 **어떻게 하면 서비스의 가용성을 확보 중점**
- 방어자는 자신이 관리하는 웹서버 및 DDOS 방어 시스템에 대해서 명확한 이해가 필요
- 지속적인 모니터링이 필요

DDOS 대응 절차

DDOS 공격 인지

- 유입되는 트래픽의 양을 정기적으로 모니터링
- 기업에서 운영중인 네트워크 장비 / 방화벽 / 서버등에서 유입되는 트래픽의 양을 지속적으로 모니터링 필요





DDOS 대응 절차

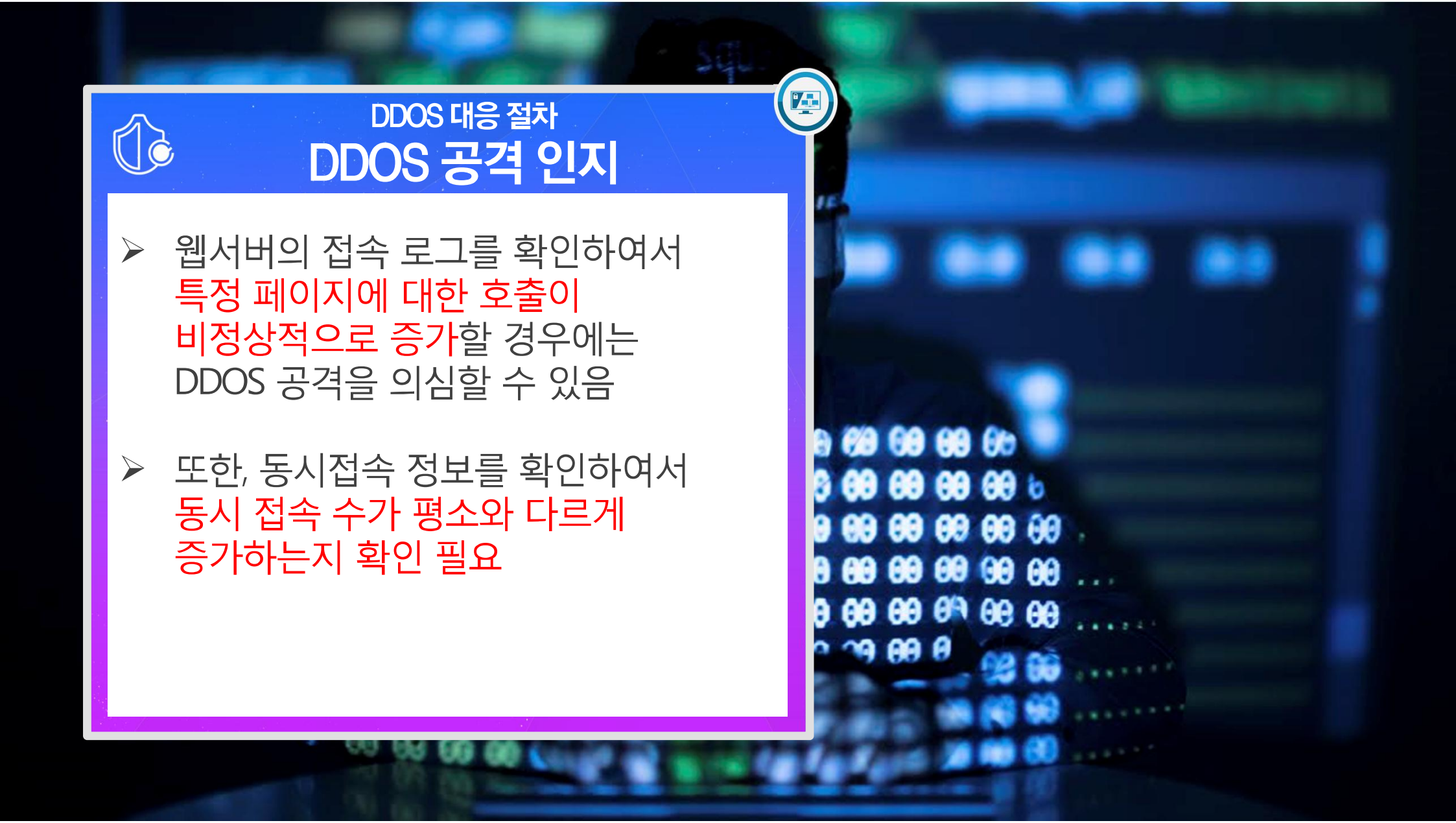
DDOS 공격 인지

- 유입되는 트래픽이 평소와 다르게 크게 증가하는 경우에는 DDOS 공격을 의심할 수 있음
- 이때, 평소의 트래픽량을 지정하는 **'임계치'**를 설정하여서 이를 넘을 시에 DDOS 공격으로 의심할 수 있는 값을 평소에 지정 필요

DDOS 대응 절차

DDOS 공격 인지

- 웹서버의 로그를 통한 확인
- 일반적으로 DDOS는 웹서버의 특정 페이지를 지속적으로 호출함



DDOS 대응 절차

DDOS 공격 인지

- 웹서버의 접속 로그를 확인하여서 특정 페이지에 대한 호출이 비정상적으로 증가할 경우에는 DDOS 공격을 의심할 수 있음

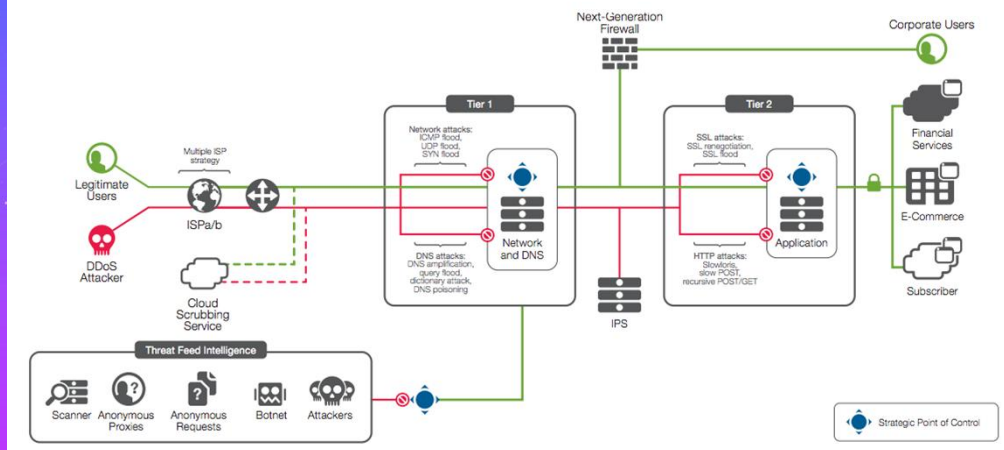
- 또한, 동시접속 정보를 확인하여서 동시 접속 수가 평소와 다르게 증가하는지 확인 필요

중소기업 사용 가능한 방법

KISA의 사이버 대피소

대기업 사용 가능한 방법

DDOS 전용 솔루션



랜섬웨어 예방 및
사이버 보안의 첫 걸음

전사원을 교육하라!

랜섬웨어란 무엇인가?

랜섬웨어(Ransomware)란?

Ransom

Ware

Ransomware

주로 이메일 및
악성링크를 통해
감염

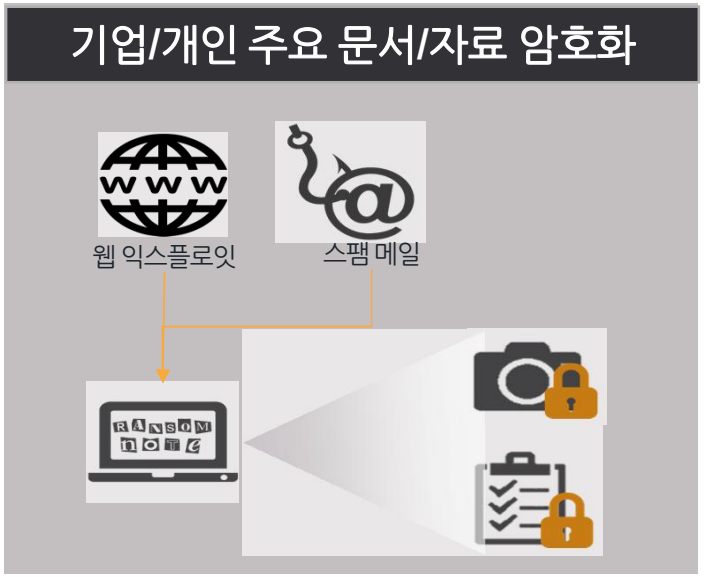
감염 시
시스템 내
문서파일들을
암호화

비용을 지불하여
복호화키를
받기 전까지
전체파일사용 불가

랜섬웨어의 변화

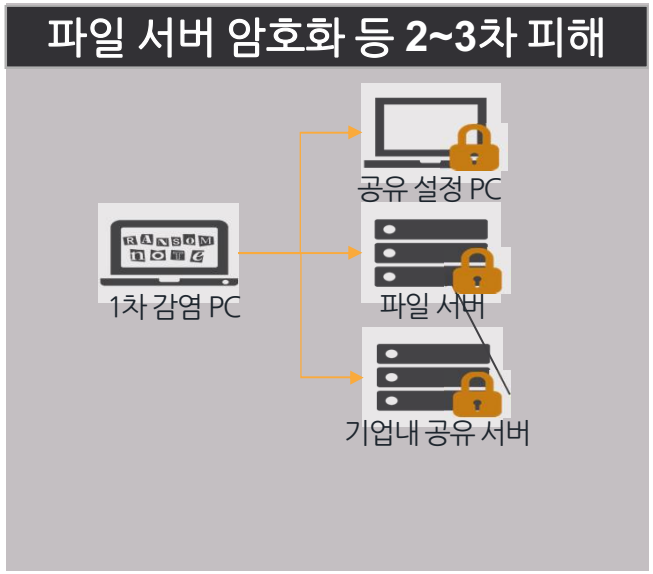

랜섬웨어의 변화
DirtyDecrypt
July 2013
CryptoLocker
Setp 2013
CryptoWall
Nov 2013
CtbLocker
July 2014
TorrentLocker
Aug 2014
TeslaCrypt
Mar 2015
New CryptoLocker
April 2015
Locky
Feb 2016
Cerber
Dec 2016
WannaCry
Apr 2017
Petya
June 2017

랜섬웨어의 피해



이메일/웹 등 다양한 경로를 통하여
랜섬웨어 유입 및 기업/개인 주요 문서/자료 암호화

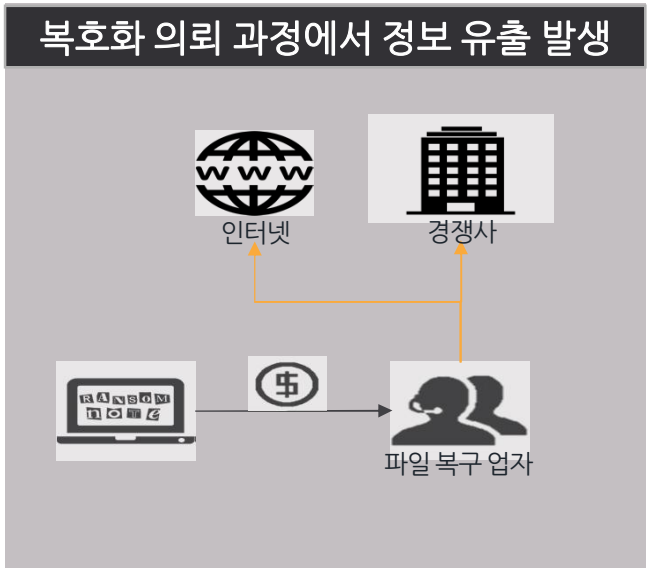
랜섬웨어의 피해



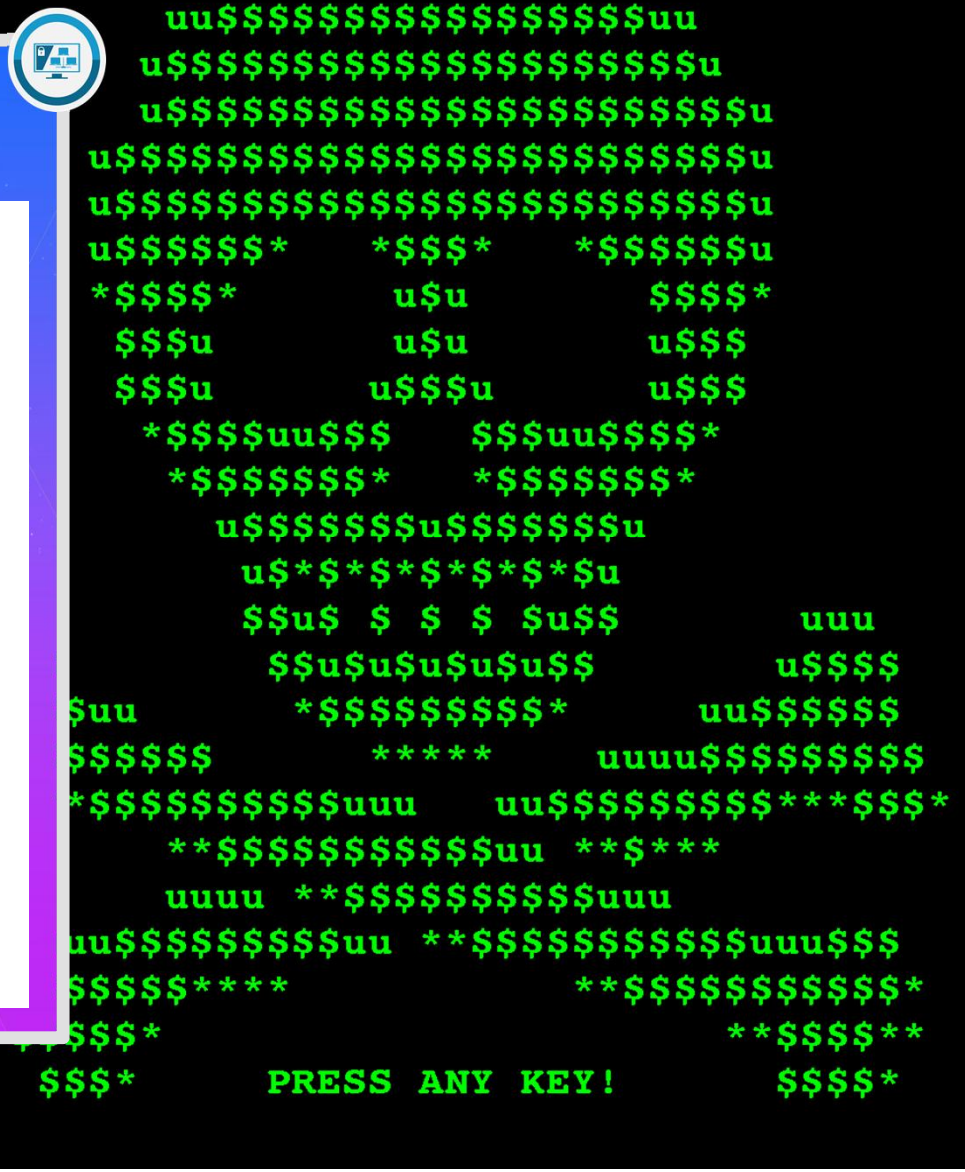
네트워크 드라이브 설정으로 인한
파일 서버 / 공유 PC등 2~3차 암호화 피해 발생

랜섬웨어의 피해

복호화 의뢰 과정에서 정보 유출 발생



암호화 파일 복구 업체를 통한
주요 문서 유출 가능



랜섬웨어의 감염 경로

웹을 통한 감염

- **취약한 웹 사이트에 Exploit 삽입하여 유포**
  Exploit Kit(Angler, RIG 등)을 이용하여 주로 유포
  유입되는 바이너리는 암호화되는 경우 다수

- **국내 정상 사이트를 통한 유포 증가**
  클리앙 사이트를 통한 랜섬웨어 유포
  인터넷 뉴스 사이트/광고 등을 이용한 유포 증가

랜섬웨어의 감염 경로

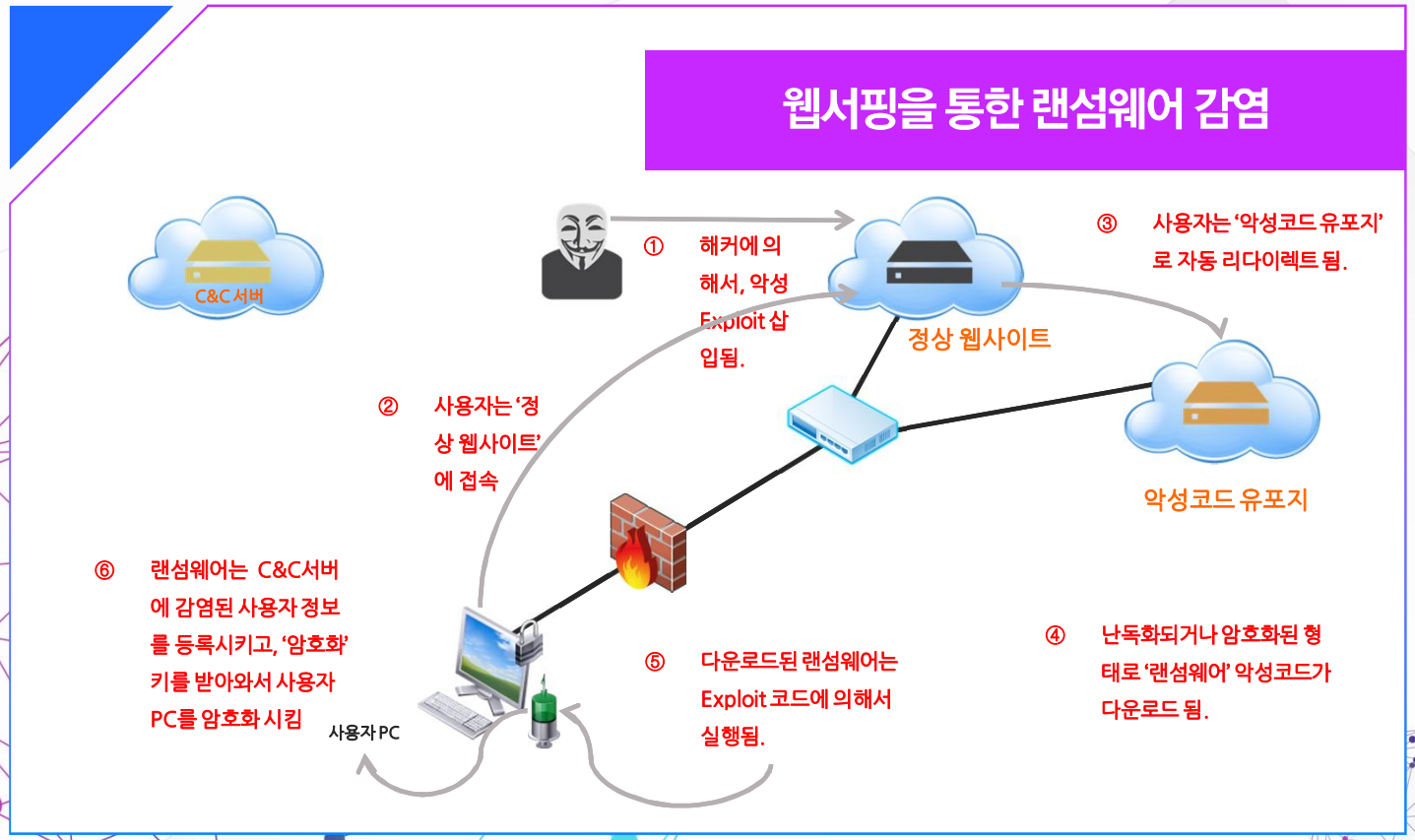
이메일을 통한 감염

- 피싱 이메일을 통한 유포
  압축 파일, 문서 파일, html 등 다양한 첨부 파일 유형을 통하여 유입
  본문 또는 문서 파일 내 링크를 통한 유포

- 사용자를 속이기 위한 사회공학적인 방법 이용

랜섬웨어의 감염 경로

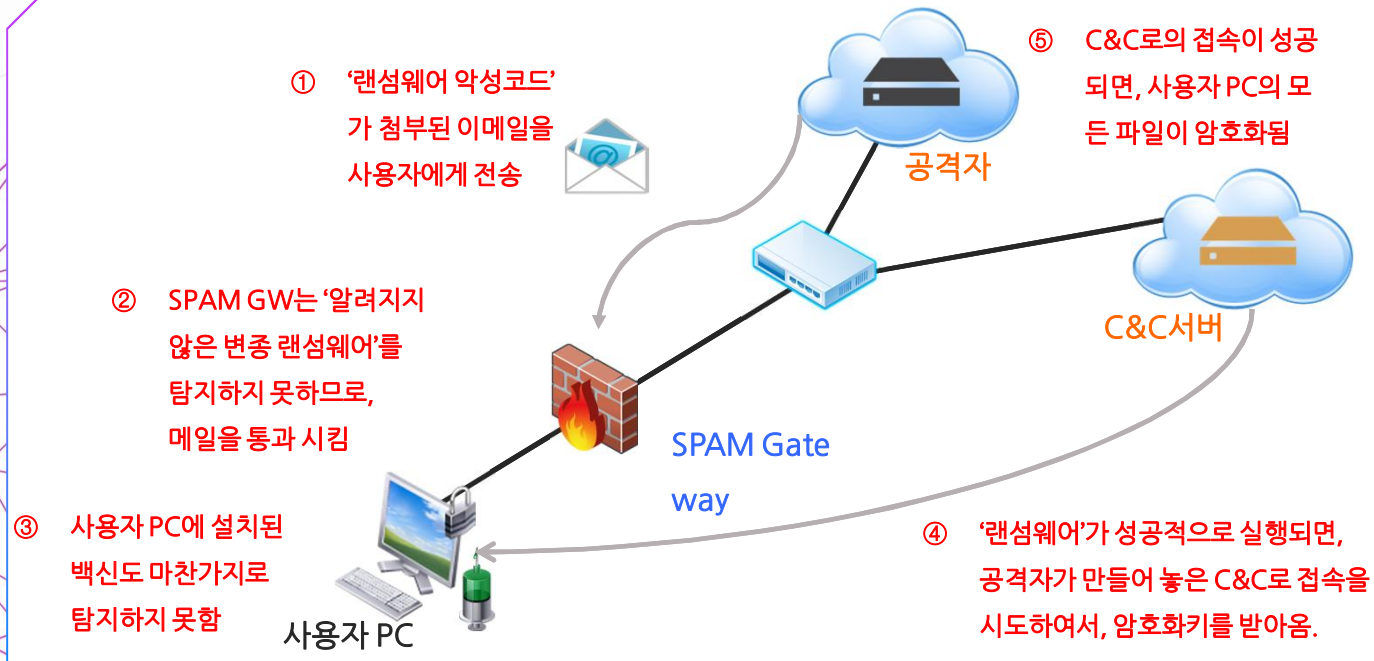
웹서핑을 통한 랜섬웨어 감염



랜섬웨어의 감염 경로

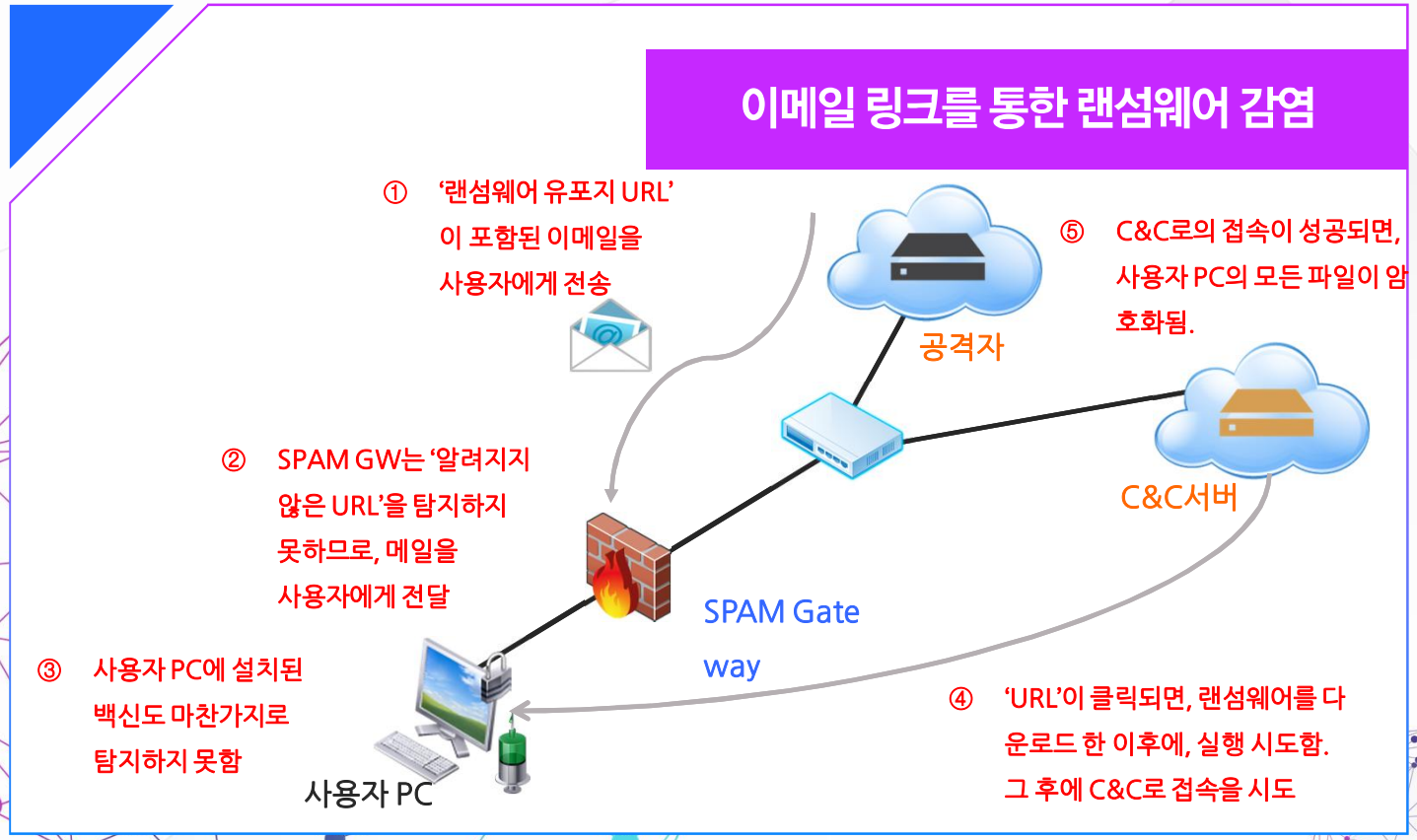
이메일 첨부파일을 통한 랜섬웨어 감염

이메일 첨부파일을 통한 랜섬웨어 감염



랜섬웨어의 감염 경로

이메일 링크를 통한 랜섬웨어 감염



랜섬웨어 동작 영상

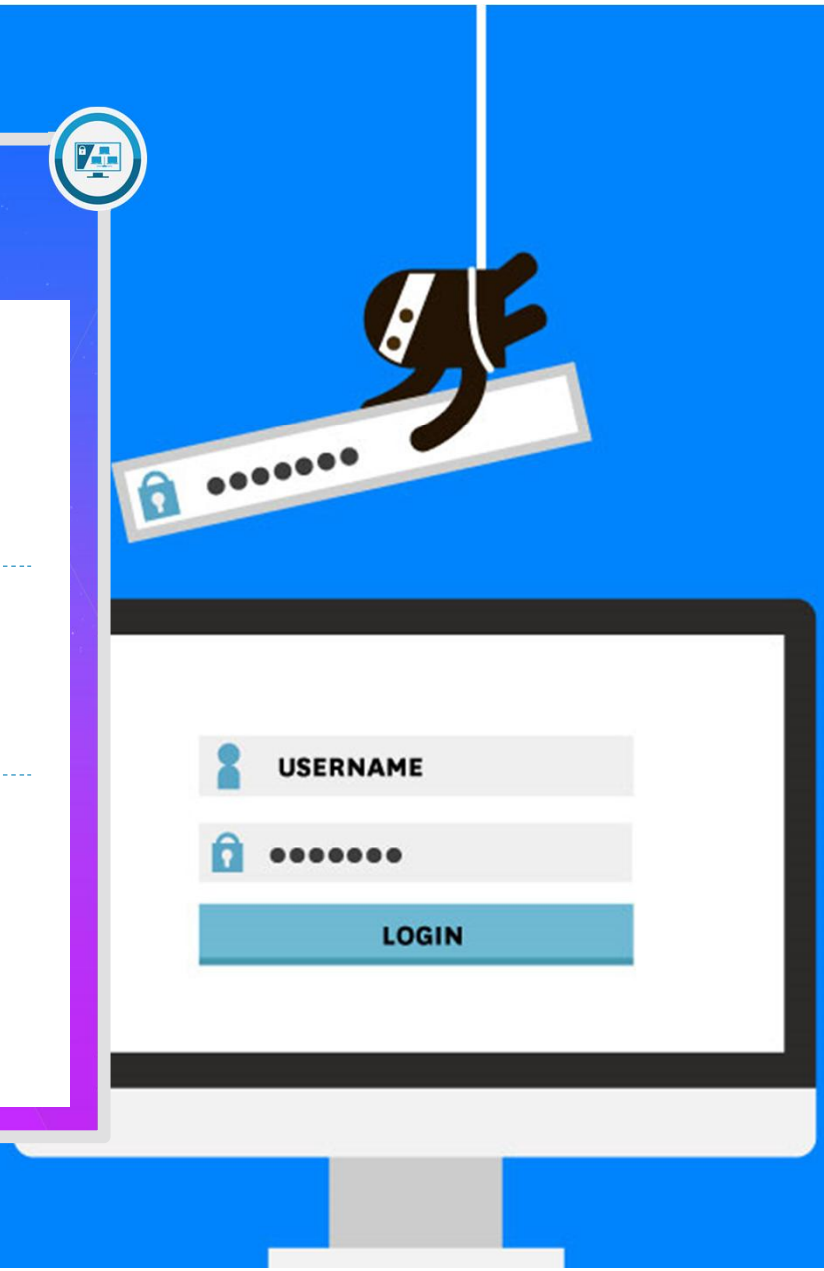

랜섬웨어 예방 및
사이버 보안의 첫 걸음
전사원을 교육하라!
랜섬웨어의 피해를 막는 방법

먼저 기억해야 할 사실

랜섬웨어는 악성코드의
많은 종류 중에 하나

랜섬웨어에 감염되는 경로의 99%는
웹서핑과 이메일을 이용한 점

랜섬웨어 공격자들은 대부분 알려진
취약점을 활용한 익스플로잇(Exploit)을
이용한다는 점



많이 물어 보는 질문

랜섬웨어에 감염되면 복구가 가능한가요?

기술적으로는 복구가 불가능하다고 보는 것이 맞습니다. 100%는 아니지만, 대부분의 랜섬웨어는 '**비대칭 암호화키**'라는 방식을 사용하는데 이 경우에 해커가 사용하는 서버를 압수해야만 파일 복구에 필요한 키를 확보가 가능합니다.

하지만, 실제로 해커를 잡거나 서버를 압수하는 것이 거의 불가능하기 때문에 복구는 어렵다고 보는 것이 맞습니다.

많이 물어 보는 질문

복구가 되는 경우도 있던데, 그건 어떻게 된거죠?

보안 업체에서 상세 분석을 통해서 파일을 복구 시키는 키를 찾아 내거나 해커의 서버를 확보하는 경우도 있지만, 드문 사례입니다. 또한, 이렇게 **복구 방법을 찾아 내더라도 꽤 오랜 시간이 필요**합니다.

많이 물어 보는 질문

돈을 주면 복구가 가능한가요?

대부분의 경우는 돈을 주고 파일을 복구할 수 있는 경우가 있습니다. **하지만, 랜섬웨어 유포 자체가 불법이기 때문에 돈을 준다고 해서 100% 파일을 복구해준다는 보장은 할 수가 없습니다.** 또한, 이미 한번 랜섬웨어에 노출 되었기 때문에 개인이나 기업의 자료가 외부로 유출 되었을 확률이 매우 높습니다. 또, 이번에는 요행히 복구를 할 수 있다고 하더라도 감염된 취약점이 그대로 남아 있을 확률이 높기 때문에 향후 지속적인 피해가 발생할 우려가 있습니다.

개인이 랜섬웨어의 피해를 예방하는 방법

소프트웨어는 항상 최신으로 유지

- 개인이 사용하는 소프트웨어들은 항상 최신 버전으로 유지
- 특히, 윈도우/오피스/플래시/PDF/한컴오피스와 같은 소프트웨어들은 특히 주의해서 항상 최신의 버전으로 유지할 것
- 대부분의 랜섬웨어는 알려진 취약점을 이용한다는 점을 반드시 기억

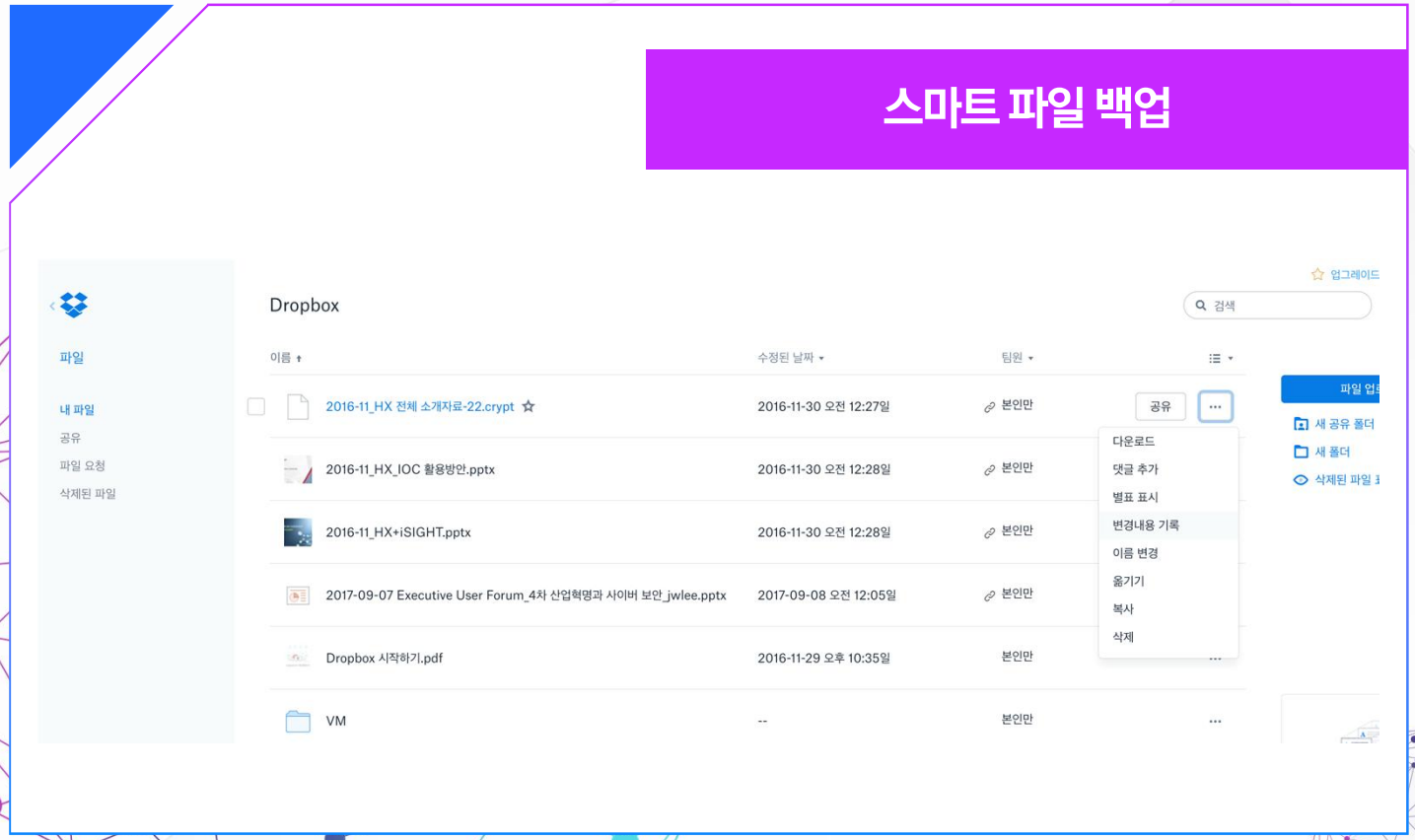
개인이 랜섬웨어의 피해를 예방하는 방법

백신 소프트웨어는 항상 최신으로 유지

- 비록 백신 소프트웨어가 알려진 악성코드와 알려진 랜섬웨어를 위주로 탐지/차단하지만, 그래도 상당수의 랜섬웨어는 최신의 백신 소프트웨어를 통해서 차단할 수 있음

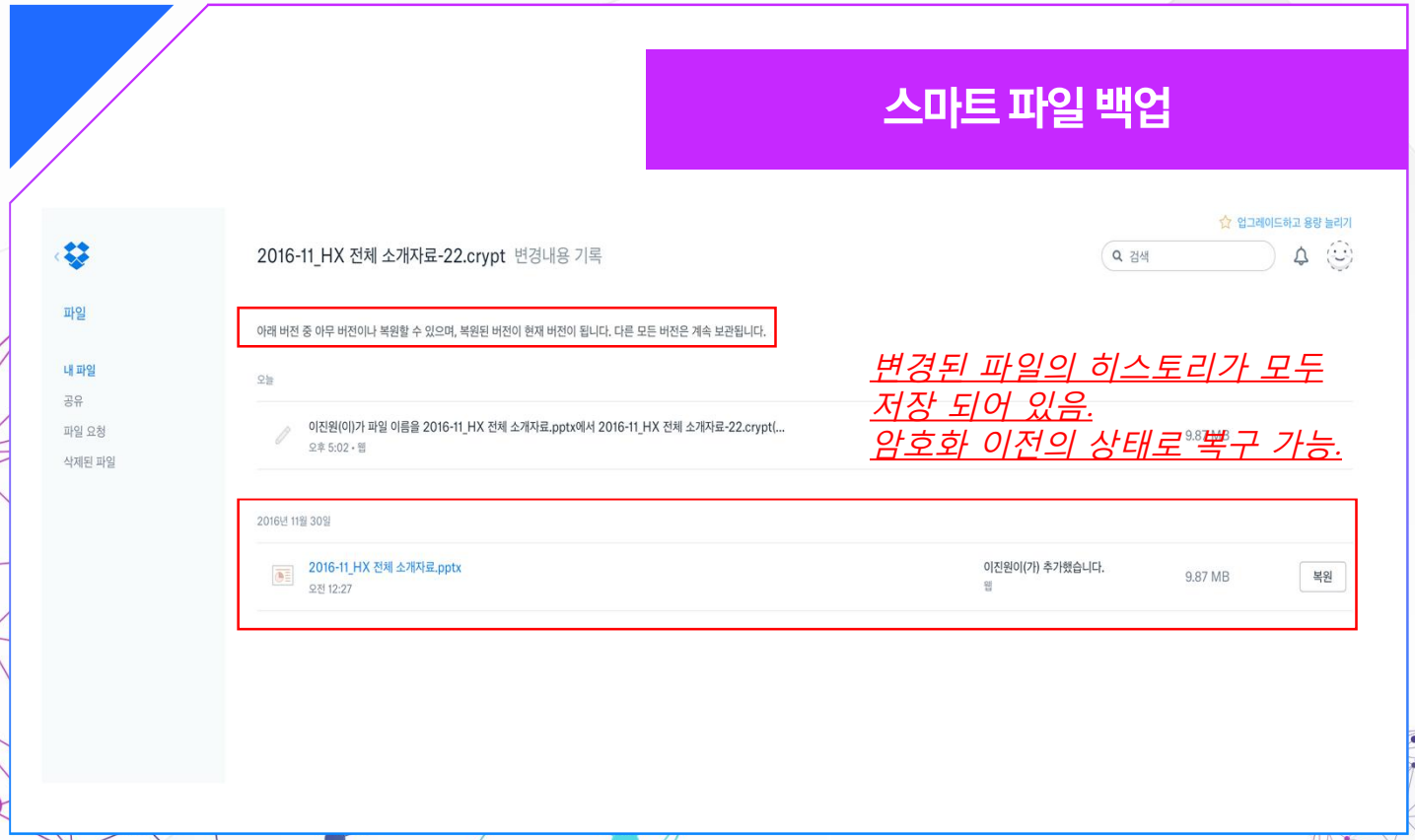
추가적으로 개인이 사용 가능한 방법

스마트 파일 백업



추가적으로 개인이 사용 가능한 방법

스마트 파일 백업



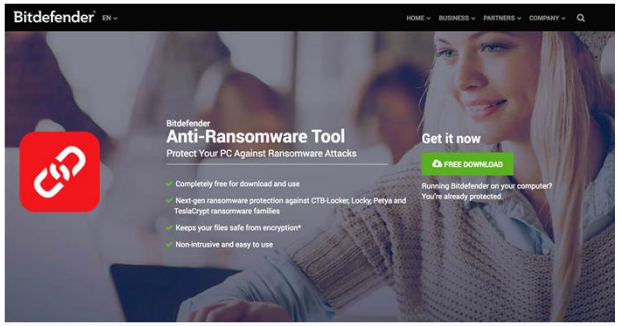
변경된 파일의 히스토리가 모두 저장 되어 있음.
암호화 이전의 상태로 복구 가능.

추가적으로 개인이 사용 가능한 방법

무료 랜섬웨어 방어 툴

무료 랜섬웨어 방어 툴

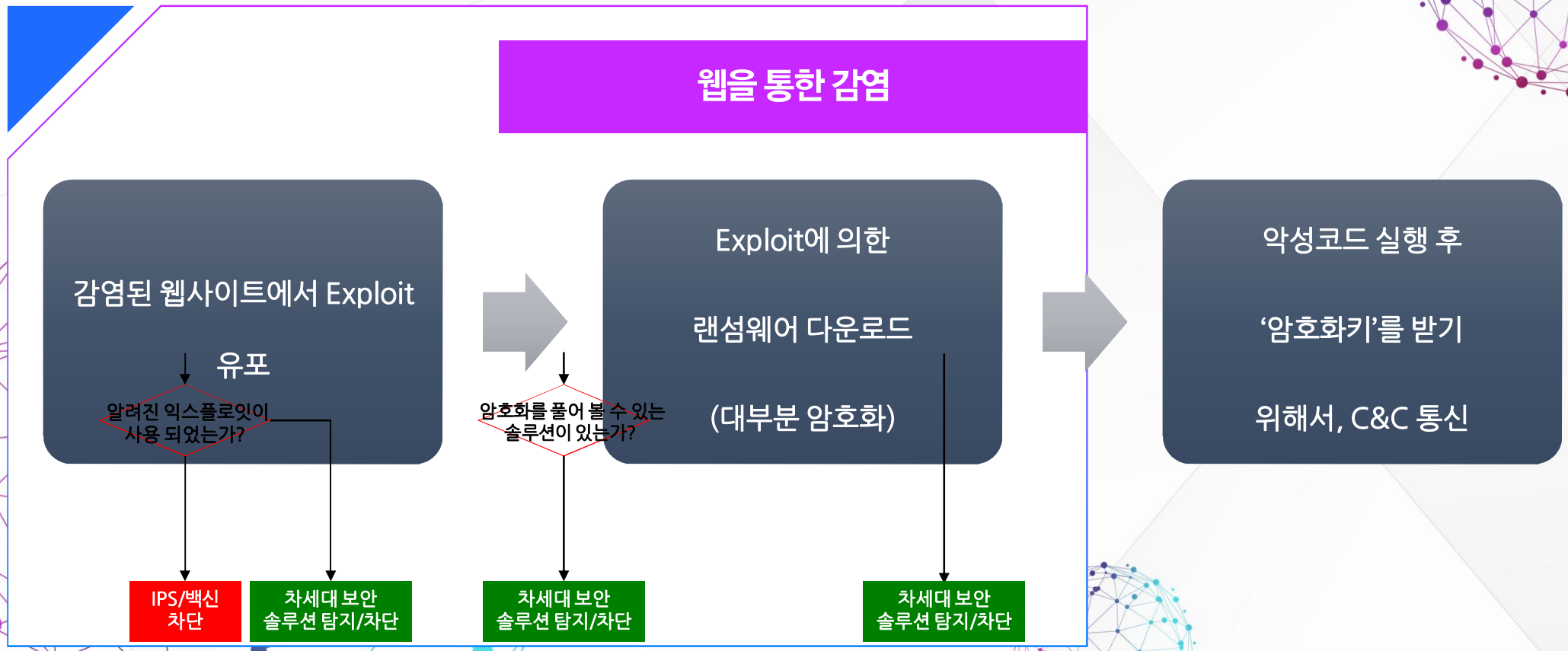
- 글로벌 보안 기업인 **Bitdefender**에서는 개인 사용자를 위해서 무료 랜섬웨어 방어 툴을 제공하고 있음
- 기업 사용자는 해당 없음
- https://www.bitdefender.com/solutions/anti-ransomware-tool.html



Bitdefender Anti-Ransomware is a free security tool that can protect against existing and emerging ransomware attacks.

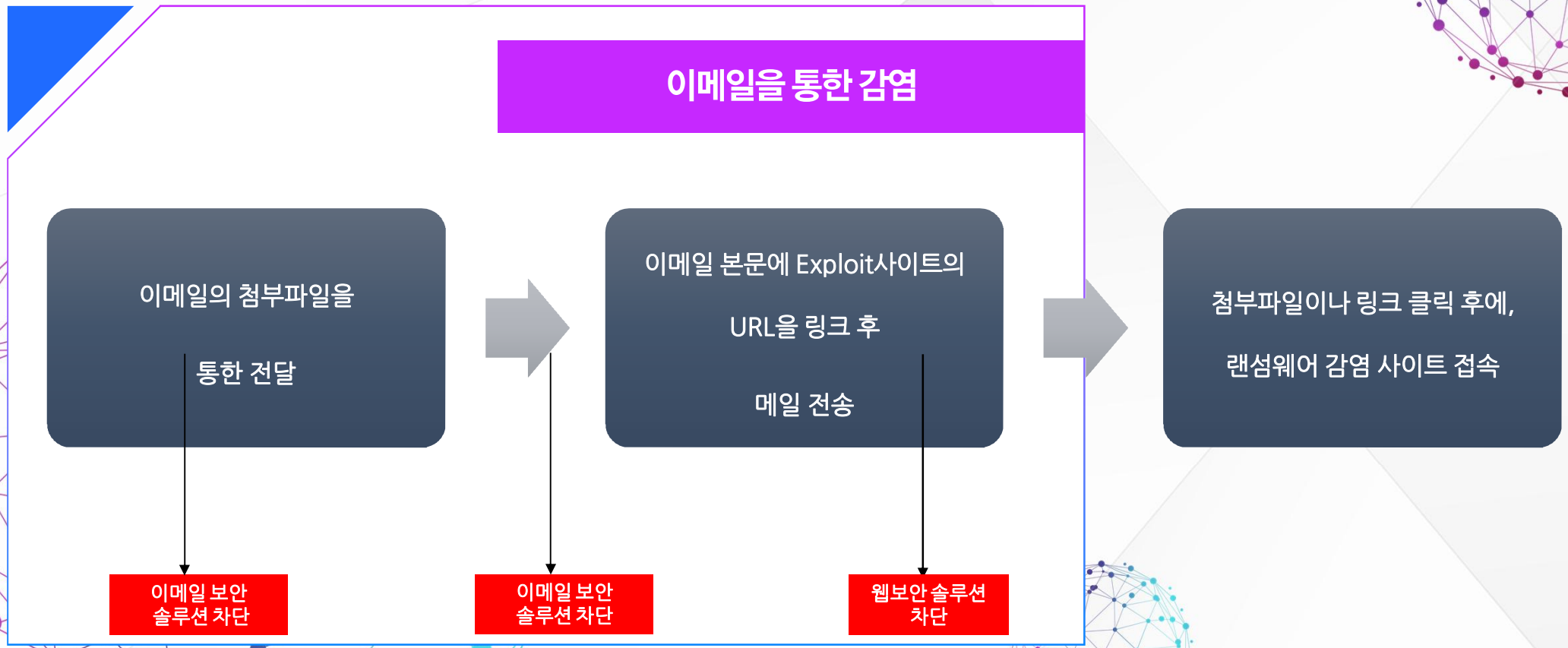
기업은 어떻게 방어 해야 하는가?

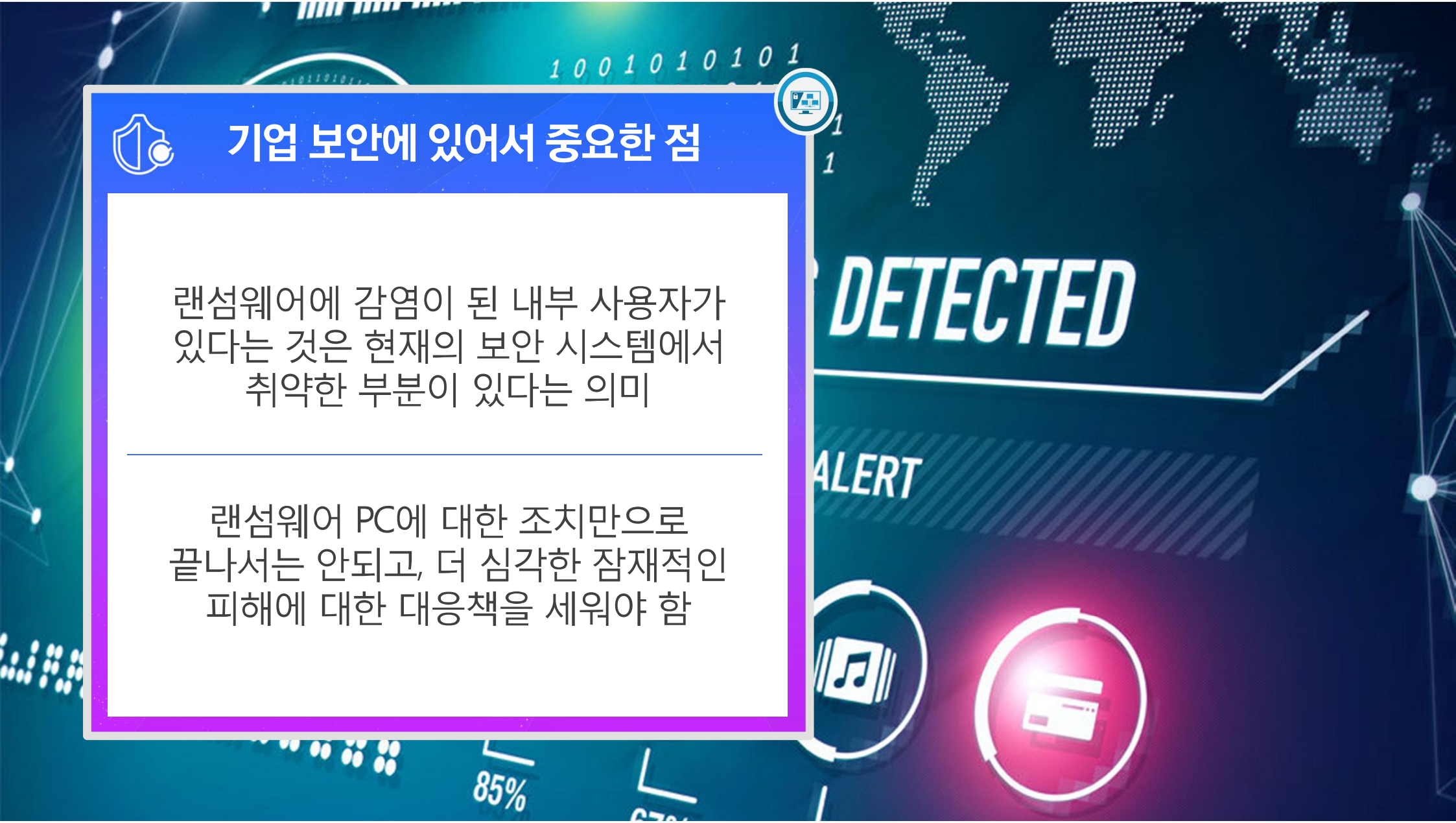
웹을 통한 감염



기업은 어떻게 방어 해야 하는가?

이메일을 통한 감염



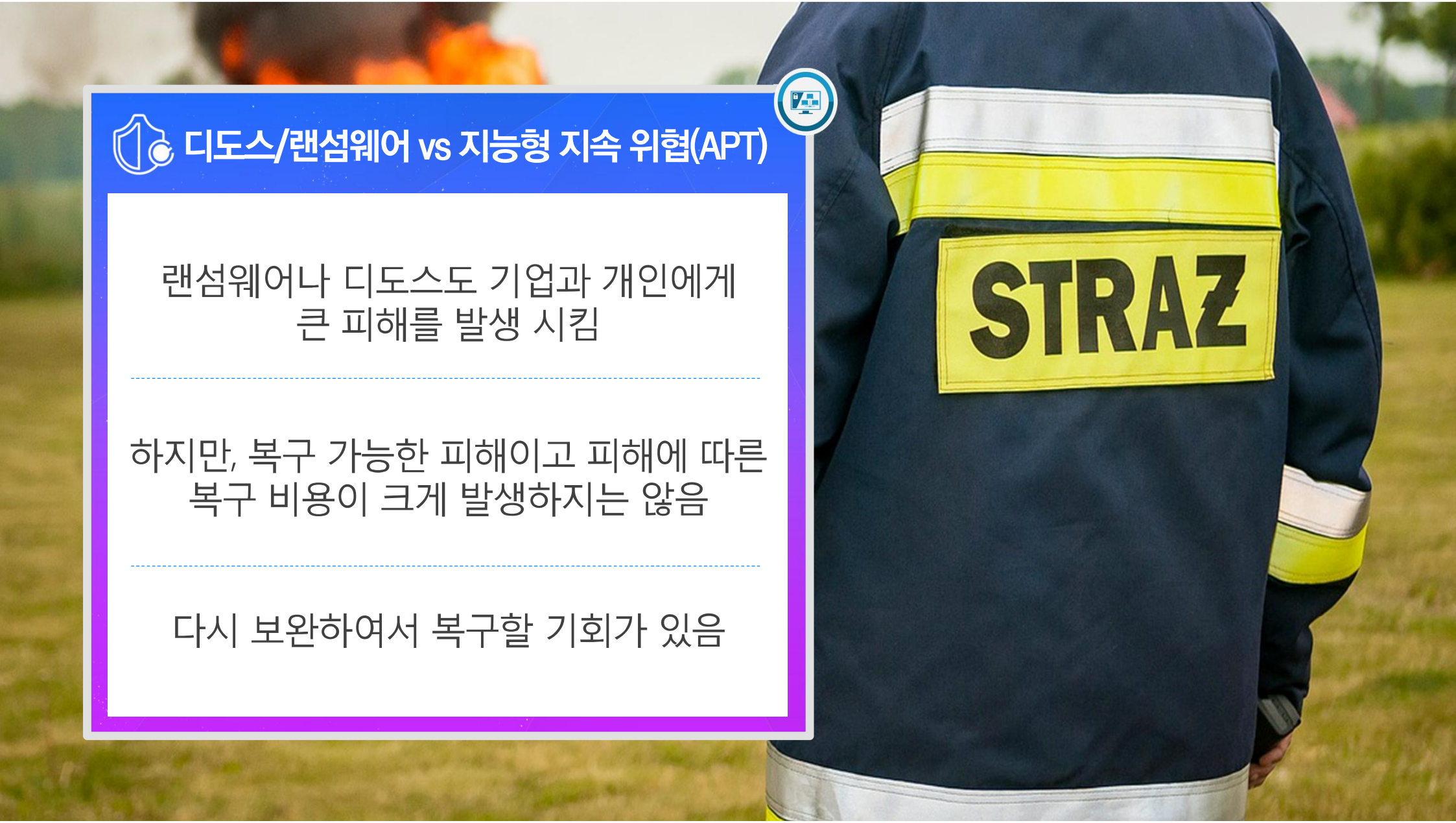


기업 보안에 있어서 중요한 점

랜섬웨어에 감염이 된 내부 사용자가 있다는 것은 현재의 보안 시스템에서 취약한 부분이 있다는 의미

랜섬웨어 PC에 대한 조치만으로 끝나서는 안되고, 더 심각한 잠재적인 피해에 대한 대응책을 세워야 함


랜섬웨어 예방 및
사이버 보안의 첫 걸음
전사원을 교육하라!
지능형 지속 위협(APT)란
무엇인가요?

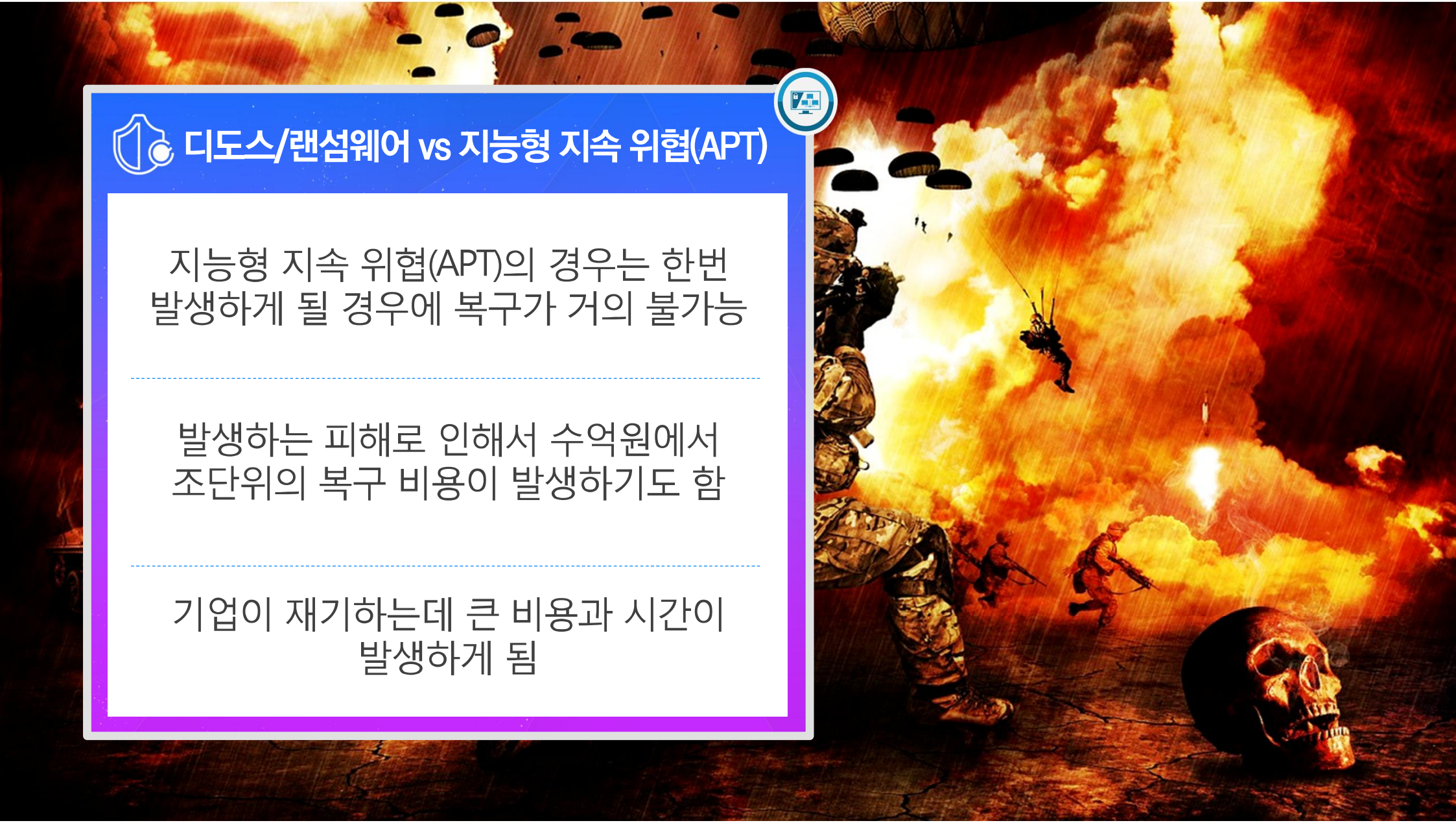


디도스/랜섬웨어 vs 지능형 지속 위협(APT)

랜섬웨어나 디도스도 기업과 개인에게
큰 피해를 발생 시킴

하지만, 복구 가능한 피해이고 피해에 따른
복구 비용이 크게 발생하지는 않음

다시 보완하여서 복구할 기회가 있음



디도스/랜섬웨어 vs 지능형 지속 위협(APT)

지능형 지속 위협(APT)의 경우는 한번 발생하게 될 경우에 복구가 거의 불가능

발생하는 피해로 인해서 수억원에서 조단위의 복구 비용이 발생하기도 함

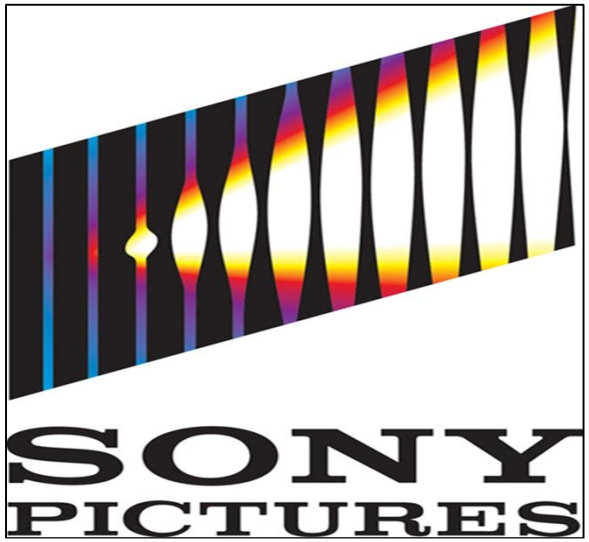
기업이 재기하는데 큰 비용과 시간이 발생하게 됨

실제 APT 공격 사례

TARGET

1억명 신용카드 정보 유출
TARGET CEO와 보안 담당자 사임

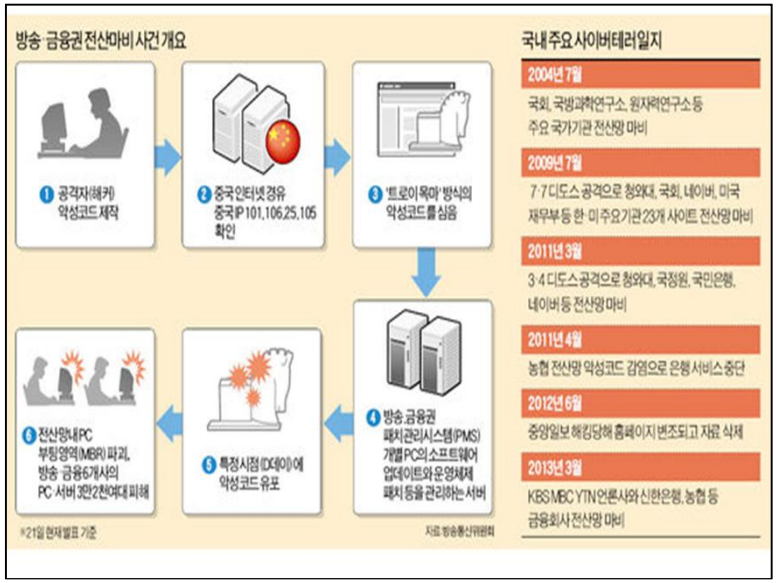
실제 APT 공격 사례



SONY PICTURES

피해액 산정 불가 (신작영화 포함하여 모두 파괴됨)
CEO와 보안 담당자 사임

실제 APT 공격 사례



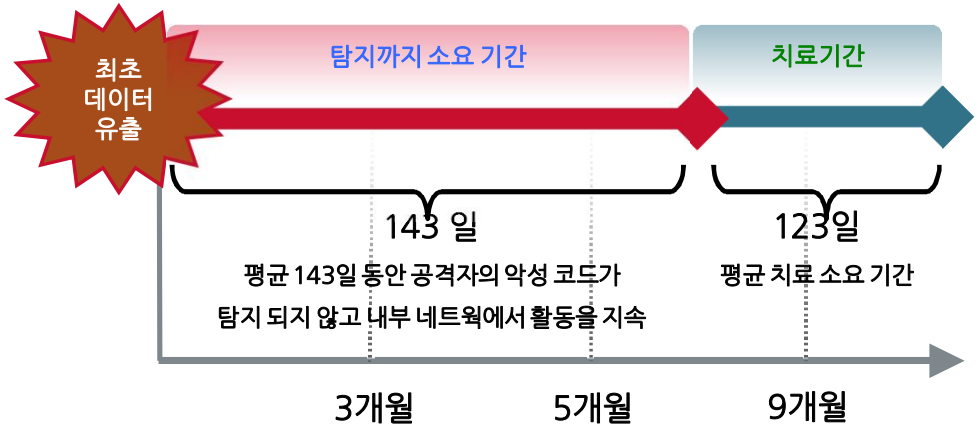
3/20 사태

직접적 피해액만 8천억원 이상

APT 공격은
왜 심각한 피해를 주는가?

APT 공격은 왜 심각한 피해를 주는가?

1건의 APT 공격 >> 기밀 정보유출에 따른 기업가치 및 신뢰도 하락



Source: FireEye M-Trends Report

67%

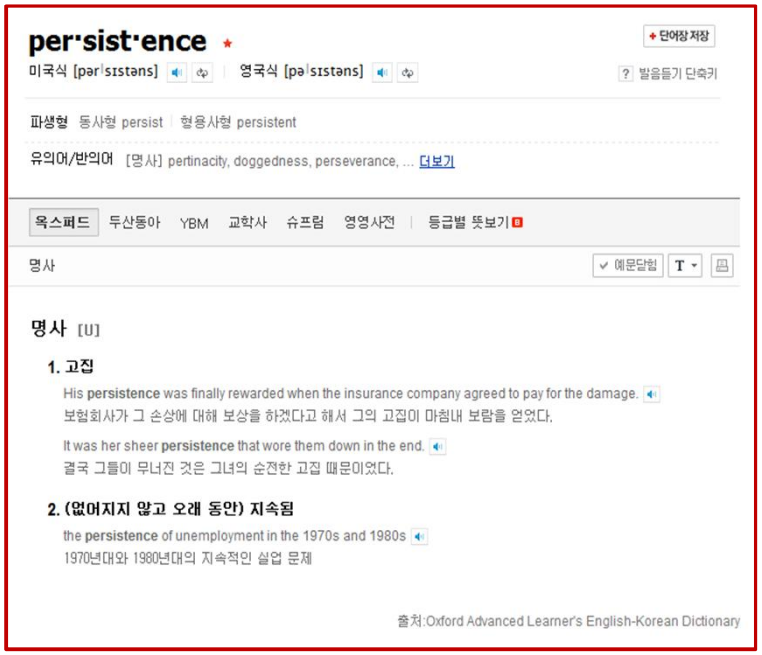
의 기업은 외부 기관의 통보를
받고 피해 사실을 확인

100%

의 피해 기업은 모두 백신
시그네쳐가 최신 버전으로
업데이트 되어 있었음

지능형 지속 위협(APT)가 무엇인가?

APT(Advanced Persistence Treat)



per·sist·ence ★

+ 단어장 저장

미국식 [pərˈsɪstəns] 영국식 [pəˈsɪstəns]

? 발음듣기 단축키

파생형 동사형 persist | 형용사형 persistent

유의어/반의어 [명사] pertinacity, doggedness, perseverance, ... 더보기

옥스퍼드 두산동아 YBM 교학사 슈프림 영영사전 | 등급별 뜻보기

명사

예문담험 T

명사 [U]

1. **고집**

His **persistence** was finally rewarded when the insurance company agreed to pay for the damage.
보험회사가 그 손상에 대해 보상을 하겠다고 해서 그의 고집이 마침내 보람을 얻었다.

It was her sheer **persistence** that wore them down in the end.
결국 그들이 무너진 것은 그녀의 순전한 고집 때문이었다.

2. **(없어지지 않고 오래 동안) 지속됨**

the **persistence** of unemployment in the 1970s and 1980s
1970년대와 1980년대의 지속적인 실업 문제

출처:Oxford Advanced Learner's English-Korean Dictionary

지능형 지속 위협(APT)가 무엇인가?

Advanced

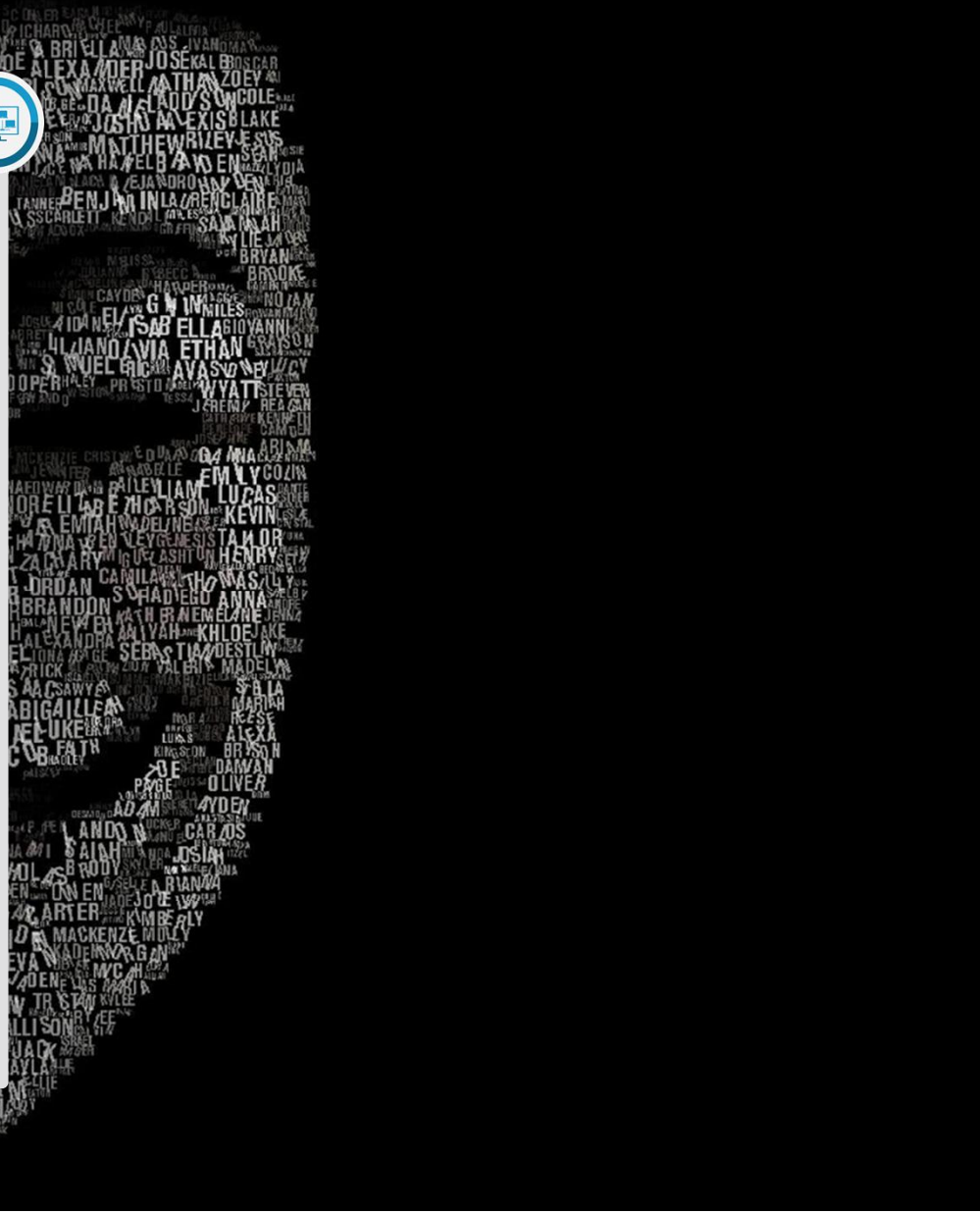
- *알려지지 않은 공격기법을 이용해서*

Persistence

- *공격이 성공할때까지 끊임없이*

Threat

- *지속되는 사이버 위협*



APT공격에 자주 사용되는 경로 및 유형

이메일

웹서핑

APT 공격은 다양한 경로로 이루어지지만, 90% 이상의 공격은 '웹'과 '이메일'을 통해서 이루어짐.

그 중에서도 '이메일'을 통한 공격은, '표적형 공격'에 가장 많이 사용되는 공격 루트임.

APT공격에 자주 사용되는 경로 및 유형

이메일

웹서핑

이메일을 통한 공격은
'누구'에게 보낼지가 명확한 상태에서 실행됨

사회공학적 기법을 이용해서,
'공격대상'의 정보를 알아낸 이후에 공격 시도

이메일을 통한 공격의 유형이 크게 증가

Spam Volume Is Down, but Malicious Spam Is Still a Threat

Spam volume was on a downward trend worldwide in 2013. However, while the overall volume may have decreased, the proportion of maliciously intended spam remained constant.

- **전문 업체 보고서에 의하면,**
  스팸 이메일의 수는 줄었지만, `악성코드`를
  포함한 `악의적인`이메일은 증가 추세임

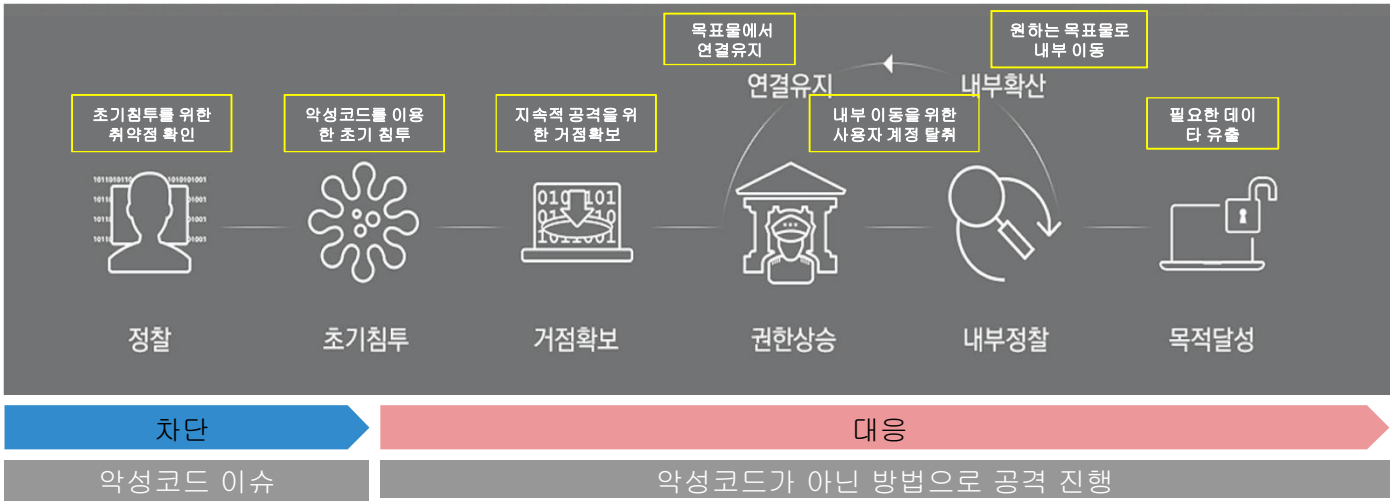
이메일을 통한 공격의 유형이 크게 증가

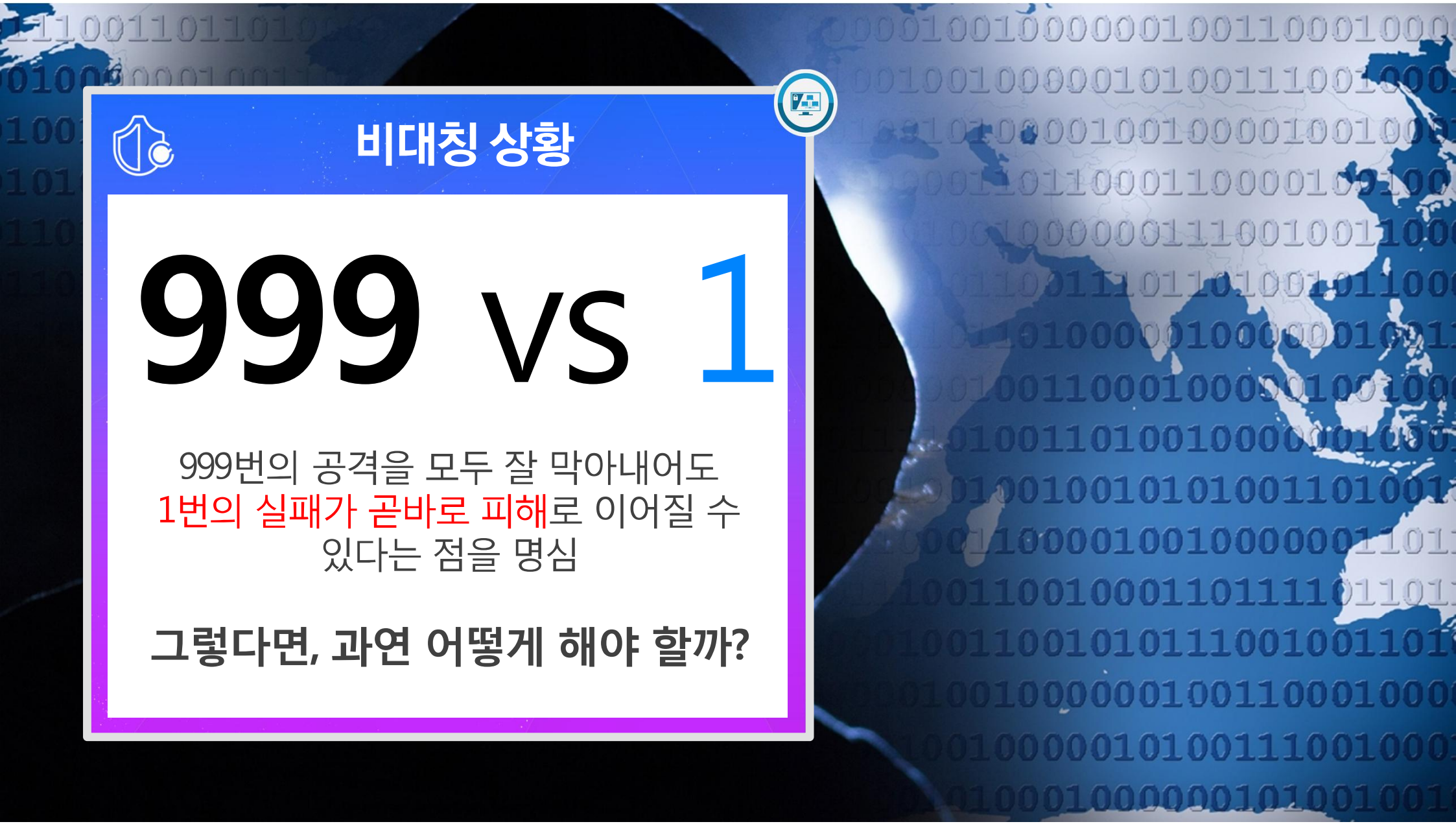
4. Email Threats. Only 1 in 5 emails sent was legitimate, as spam increased to 76 percent of email traffic. Phishing threats delivered via email also increased.

- 또 다른 보고서에 의하면, 사용자가 수신하는 전체 메일 중에서 20%의 이메일만이 정상적인 이메일임

지능형 해킹 공격은 실제로 어떻게 진행 되는가?

지능형 해킹 공격은
실제로 어떻게 진행 되는가?




비대칭 상황
999 vs 1
999번의 공격을 모두 잘 막아내어도
1번의 실패가 곧바로 피해로 이어질 수
있다는 점을 명심
그렇다면, 과연 어떻게 해야 할까?

APT 공격 시연


랜섬웨어 예방 및
사이버 보안의 첫 걸음
전사원을 교육하라!
지능형 지속 위협에 대한
기업의 대응책은?

지능형 지속 위협의 침투 방법

이메일

웹서핑


모바일

USB


파일공유

다양한 경로를 통한 공격 시도가 이루어짐

소프트웨어에 대한 최신 버전 업데이트 유지

장점

- 별도의 비용 없이,
  기본적인 대응이 가능
- 대다수의 Drive-by Download
  공격은 알려진 취약점을
  이용하는 경우가 많음
- 타 솔루션 도입과 상관없이
  필요한 내용

소프트웨어에 대한 최신 버전 업데이트 유지

단점

- 제로데이 취약점이나 알려지지 않은 취약점에는 대응이 불가
- 개별 사용자의 세심한 관리가 필요
- 별도 패치 솔루션 사용시에는 비용이나 추가적인 보안문제 발생 가능성

기본적으로 준수해야 하는 사항들

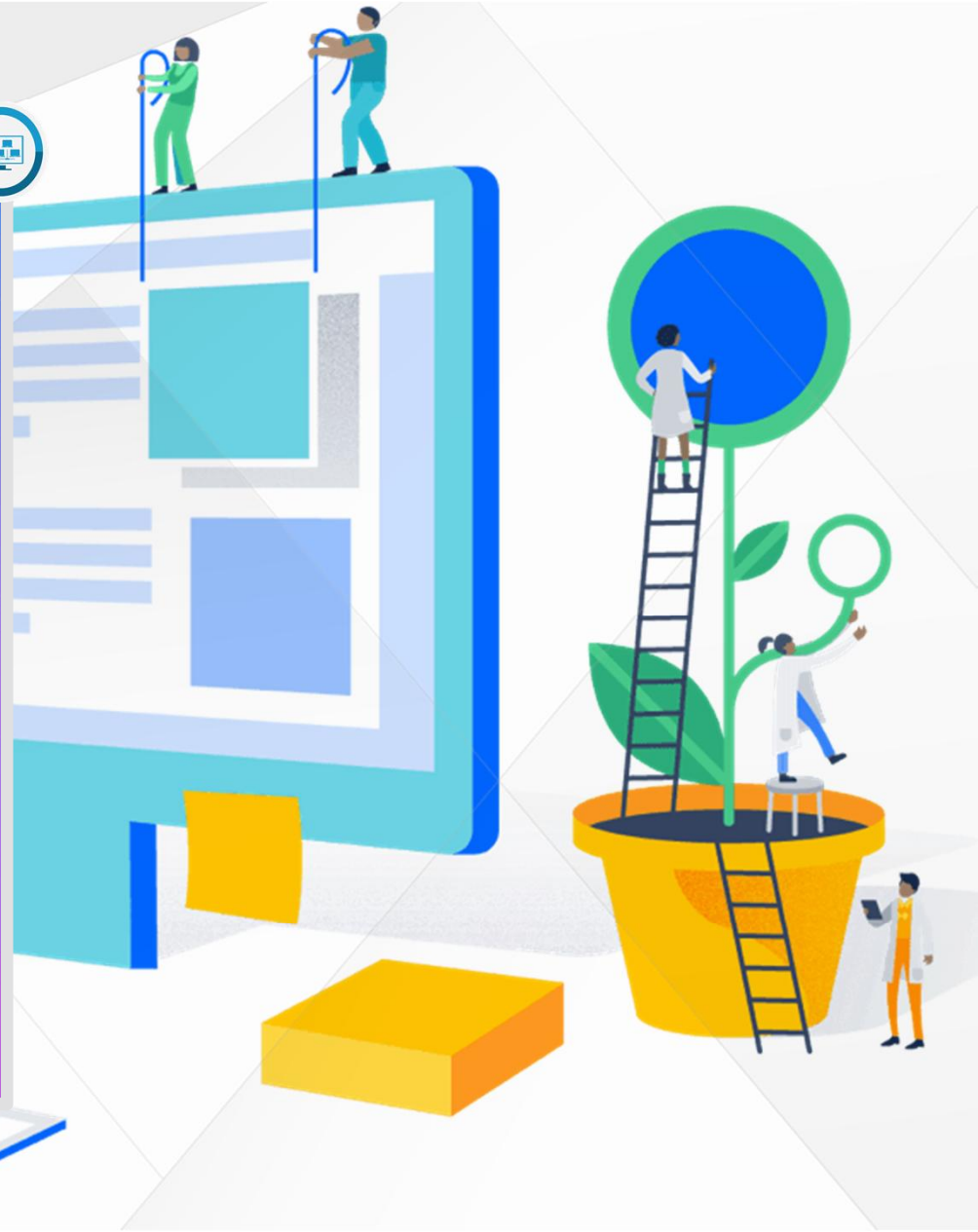
직원
개인

비업무 사이트의 접속을 줄인다.

이메일은 보낸 사람을 확인하고
열어본다.

컴퓨터의 소프트웨어는 최신으로
유지한다.

사고 발생시 즉각 보안 담당자에
통보한다.



기본적으로 준수해야 하는 사항들

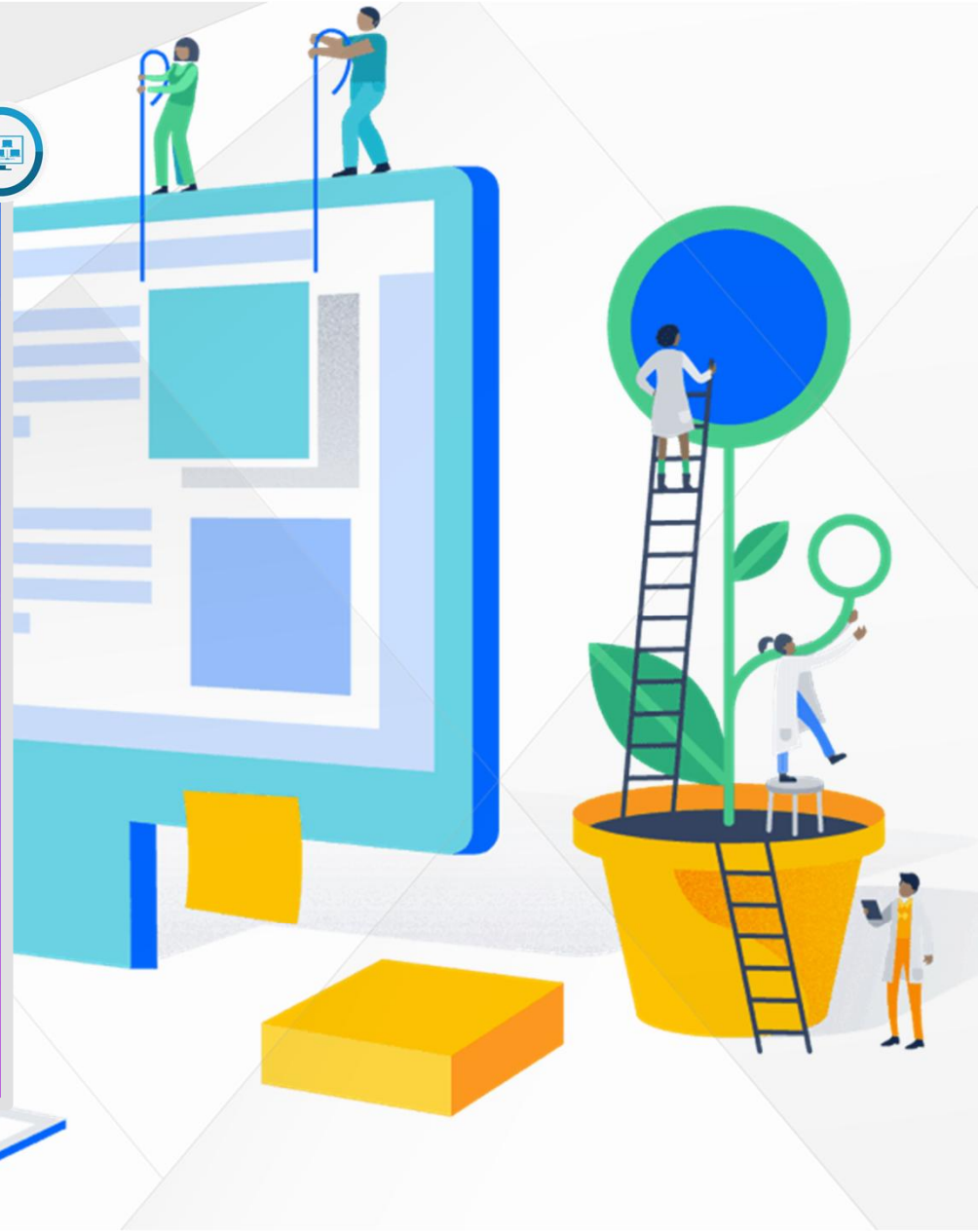
조직/
기업

보안 솔루션에 대한 투자를
정기적으로 집행한다.

내부 보안 담당 인력을 키운다.

사고 발생에 대비한 '행동 메뉴얼'을
평소에 작성한다.

보안 솔루션은 항상 최신의 상태로
유지한다.



기업이 알아야 할 사실

APT 공격은 왜 심각한 피해를 주는가?

침해는 발생할 수 있다.

- 100% 차단과 탐지가 불가능하다는 것을 인정해야 한다.
- 문제는 침해가 되더라도, 어떻게 빠르게 탐지하고 대응하느냐 하는 것이다.

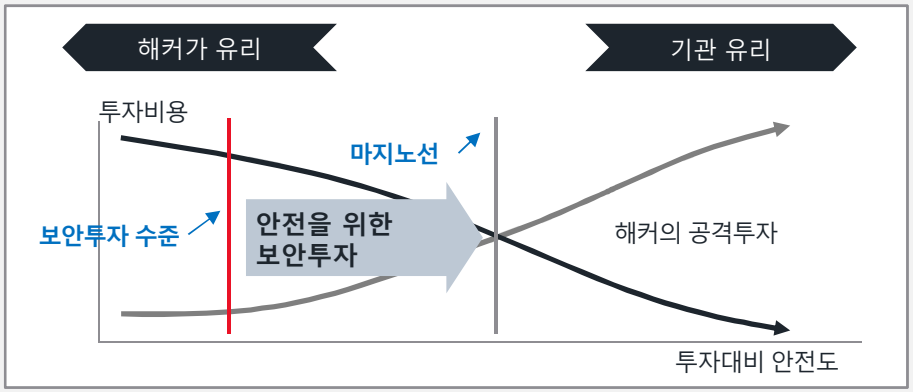
기계가 알아서 모든것을 해줄 수는 없다.

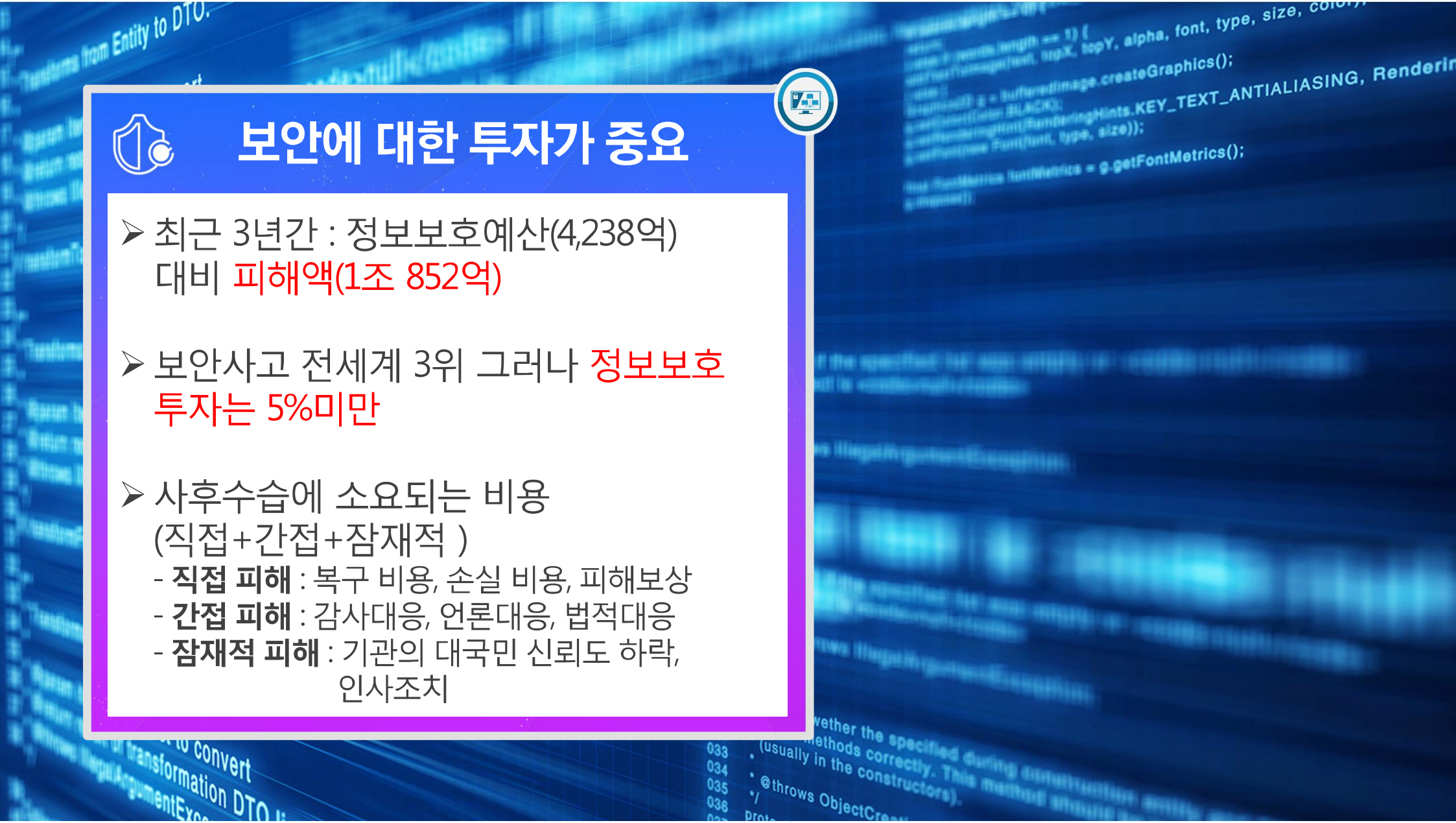
- 기계는 사람의 업무를 줄여주고 도와줄 뿐이다.
- 결국 최종적인 대응과 판단은 사람의 몫이다.

실제 사이버 공격이 어떻게 이루어지는지 이해해야 한다.

보안에 대한 투자가 중요

사이버보안 투자의 상관관계

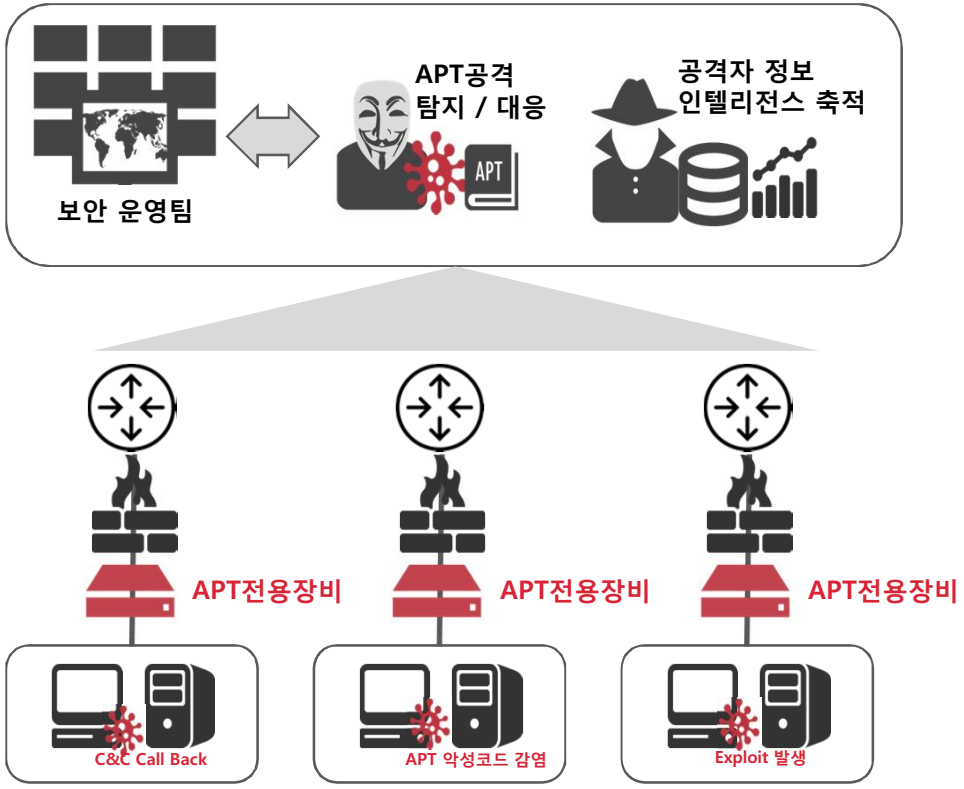




보안에 대한 투자가 중요

- 최근 3년간 : 정보보호예산(4,238억) 대비 피해액(1조 852억)
- 보안사고 전세계 3위 그러나 정보보호 투자는 5%미만
- 사후수습에 소요되는 비용 (직접+간접+잠재적)
  - **직접 피해** : 복구 비용, 손실 비용, 피해보상
  - **간접 피해** : 감사대응, 언론대응, 법적대응
  - **잠재적 피해** : 기관의 대국민 신뢰도 하락, 인사조치

웹과 이메일로 유입되는 공격에 대한 방어 전략 필요



기업의 보안 탐지 체계의 강화

➢ 웹 / 이메일 APT위협 탐지(대응) 역량 강화

- 가상머신 또는 머신러닝과 같은 기술을 이용한 알려지지 않은 공격 탐지(대응)

- APT위협 가시성 확보

- 공격자 C&C 접속, 악성코드 유포지 차단

기업의 보안 탐지 체계의 강화

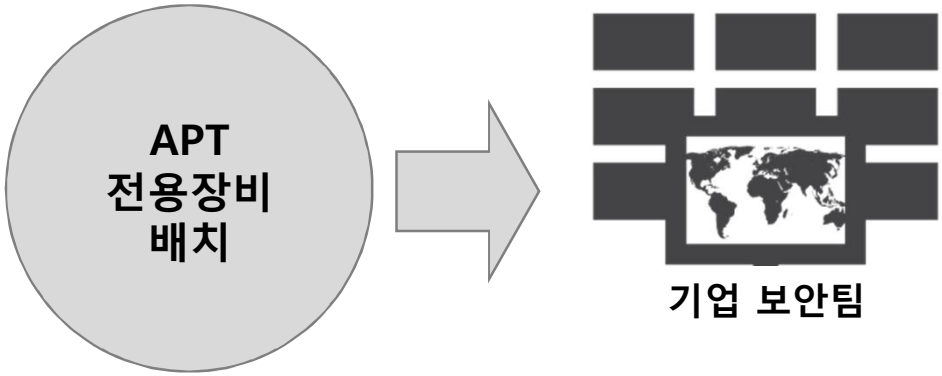
➢ 능동적인 탐지/대응, 인텔리전스 축적

- 배치된 APT전용장비를 통한
  위협 현황 수집

- 위협 현황 통계, 분석 정보 기반의
  능동적 탐지 / 대응

- C&C, 악성코드 정보/유포지 등
  프로파일링 → 인텔리전스

기업의 보안 탐지 체계의 강화



- APT위협 가시성 확보
- 표적형(APT) 위협의 대응
- 능동적 탐지/대응, 분석
- 위협 인텔리전스 축적

또 다른 방어 전략

망분리 솔루션

망분리 솔루션

악성코드로 인한 피해 최소화

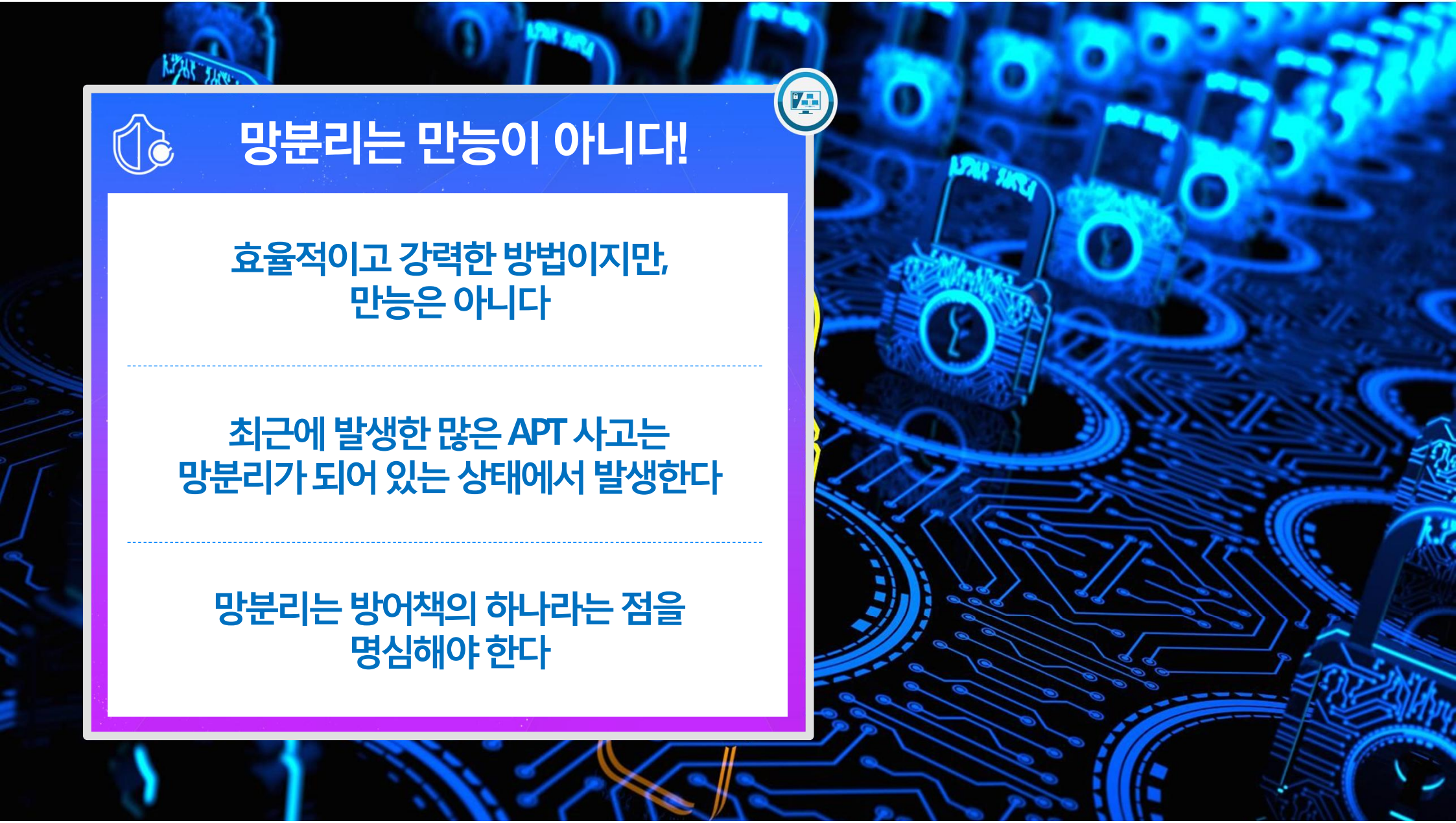
"망분리는 APT 공격에 대한 효과적 대응 방법"

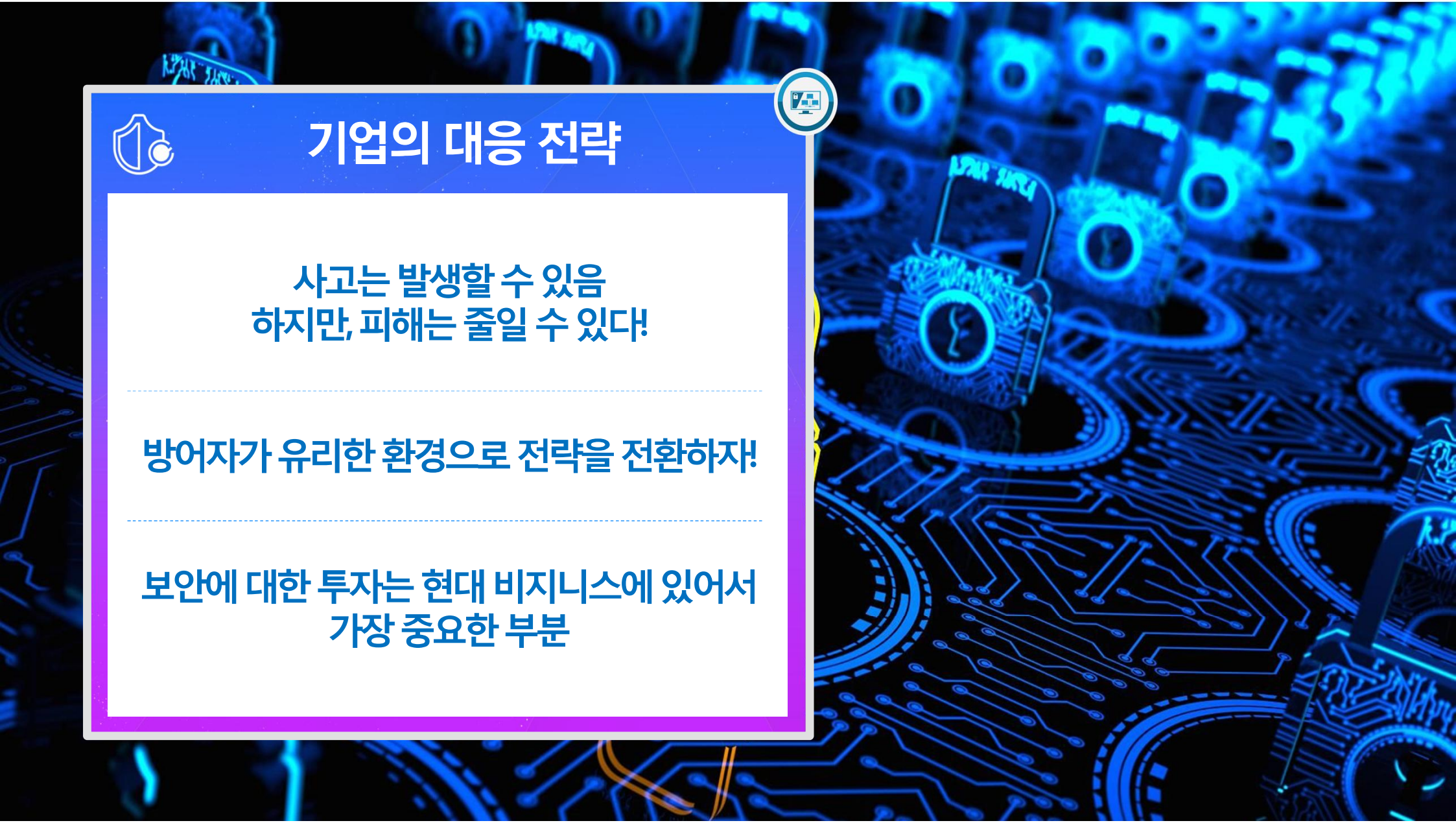
① 영역 분리로
감염 범위 최소화

② 업무 영역으로
악성코드 전파 차단

③ 해커에 의한
업무망 PC 제어방지

망분리 시스템의 동작 방법

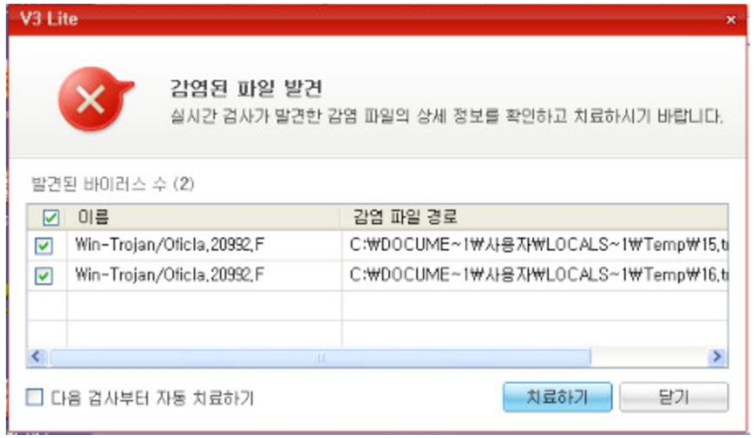

망분리는 만능이 아니다!
효율적이고 강력한 방법이지만,
만능은 아니다
최근에 발생한 많은 APT 사고는
망분리가 되어 있는 상태에서 발생한다
망분리는 방어책의 하나라는 점을
명심해야 한다


기업의 대응 전략
사고는 발생할 수 있음
하지만, 피해는 줄일 수 있다!
방어자가 유리한 환경으로 전략을 전환하자!
보안에 대한 투자는 현대 비지니스에 있어서
가장 중요한 부분

백신의 우회 시연


랜섬웨어 예방 및
사이버 보안의 첫 걸음
전사원을 교육하라!
보안 인텔리전스란 무엇인가?

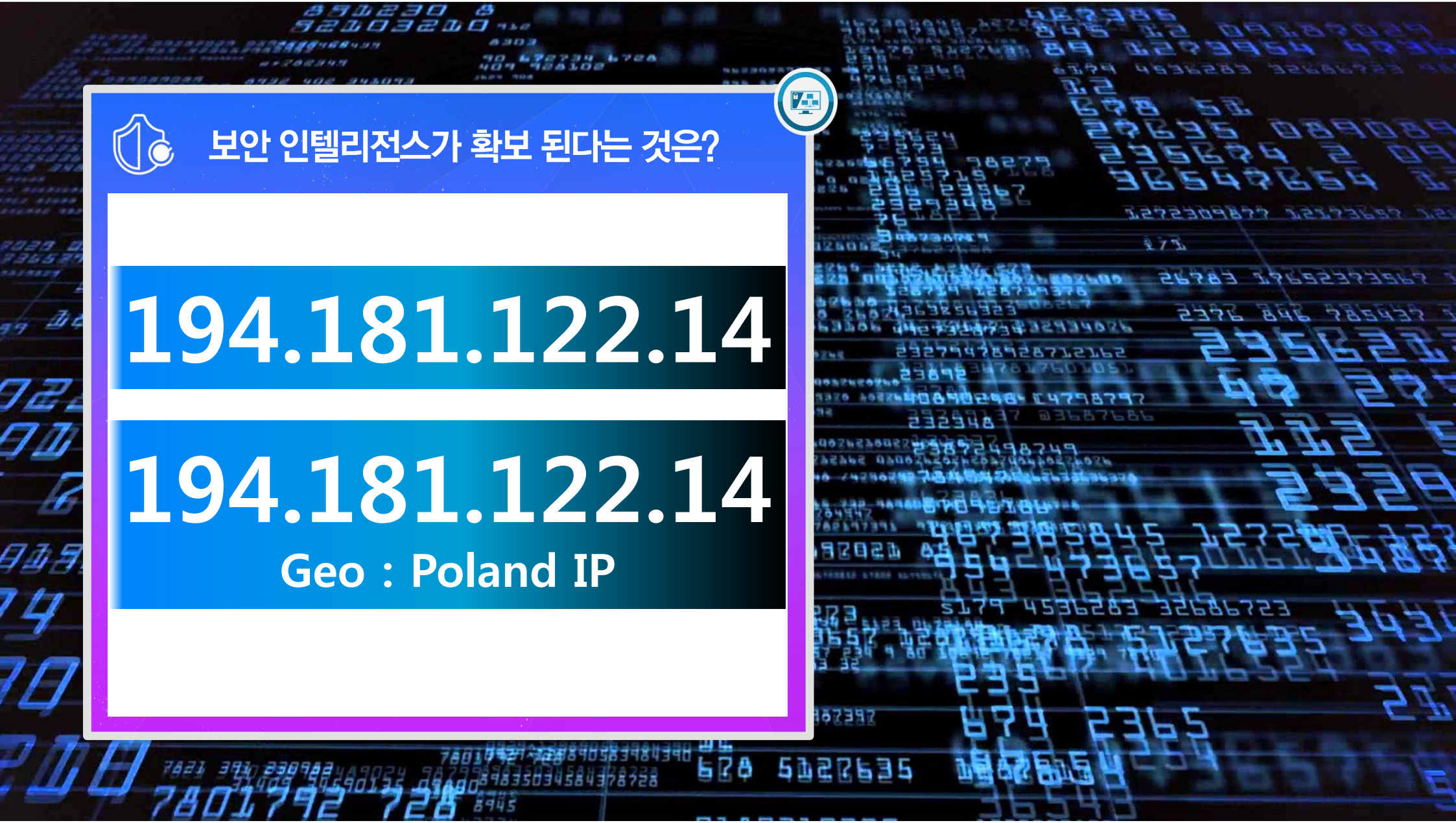
기존의 위협 탐지 방식은?



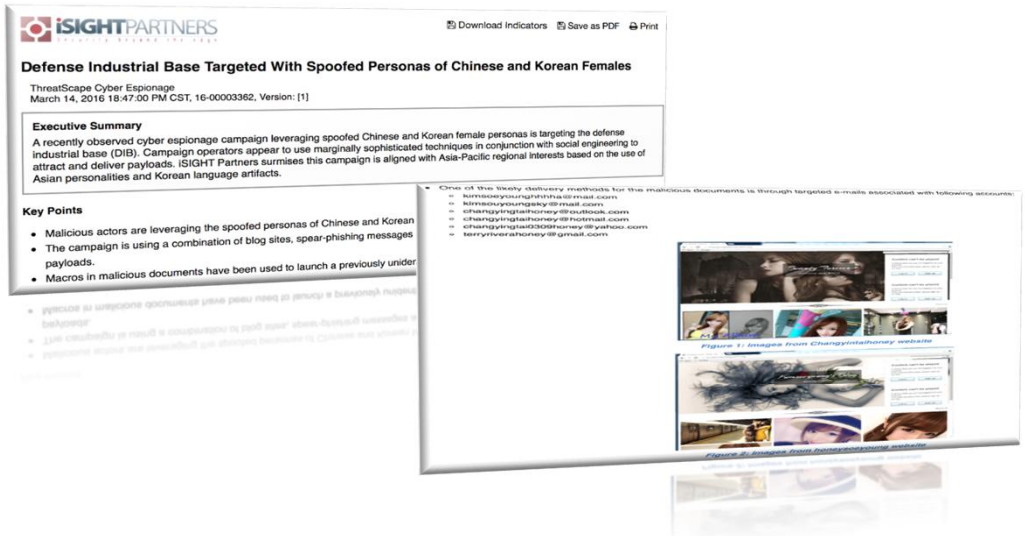
백신, 차세대 보안 기술을 통한
탐지 및 차단!

하지만, 그 다음은?

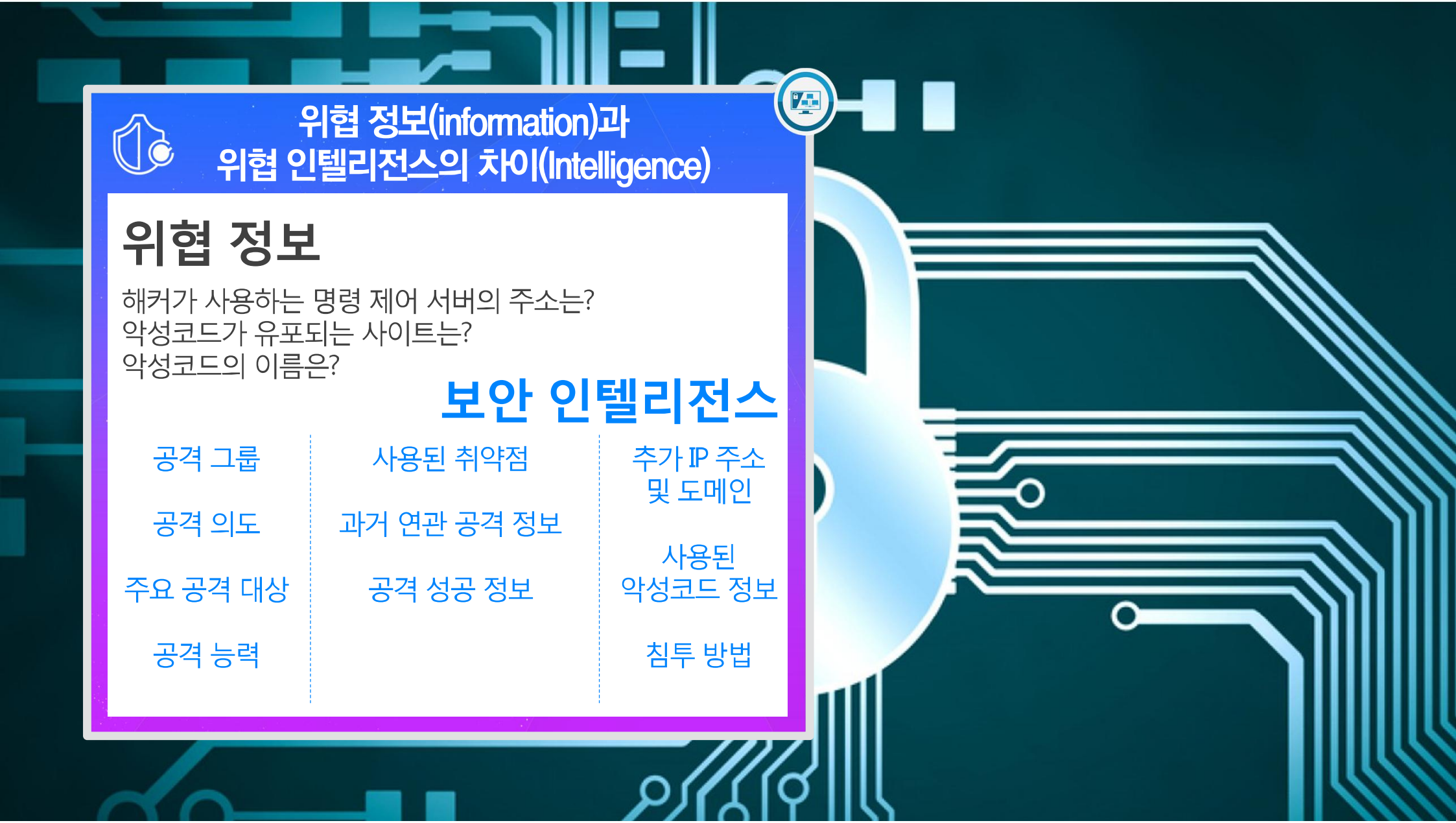
어디로 부터 공격이 들어 왔지?
우리 회사의 약한 부분은 어디지?


보안 인텔리전스가 확보 된다는 것은?
194.181.122.14
194.181.122.14
Geo : Poland IP

보안 인텔리전스가 확보 된다는 것은?



2016년도에 한국의 기업을 공격했던 중국 해킹
그룹이 사용하는 명령 제어 서버의 주소


위협 정보(information)과
위협 인텔리전스의 차이(Intelligence)
위협 정보
해커가 사용하는 명령 제어 서버의 주소는?
악성코드가 유포되는 사이트는?
악성코드의 이름은?
보안 인텔리전스
공격 그룹
공격 의도
주요 공격 대상
공격 능력
사용된 취약점
과거 연관 공격 정보
공격 성공 정보
추가 IP 주소
및 도메인
사용된
악성코드 정보
침투 방법

공격이 실제 발생되기 이전의 보안 인텔리전스 역할

Before

공격그룹의 움직임 파악

관련 공격전략의 파악

기업의 피해에 대비하기 위한 투자 및 조치

추가 확산 및 동향 파악

공격이 실제 발생되는 중의 보안 인텔리전스 역할

During

보안 이벤트에 대한 우선 순위 제공

공격의 방향 및 향후 상황에 대한 예측

인텔리전스에 기반한 방어 전략 수립

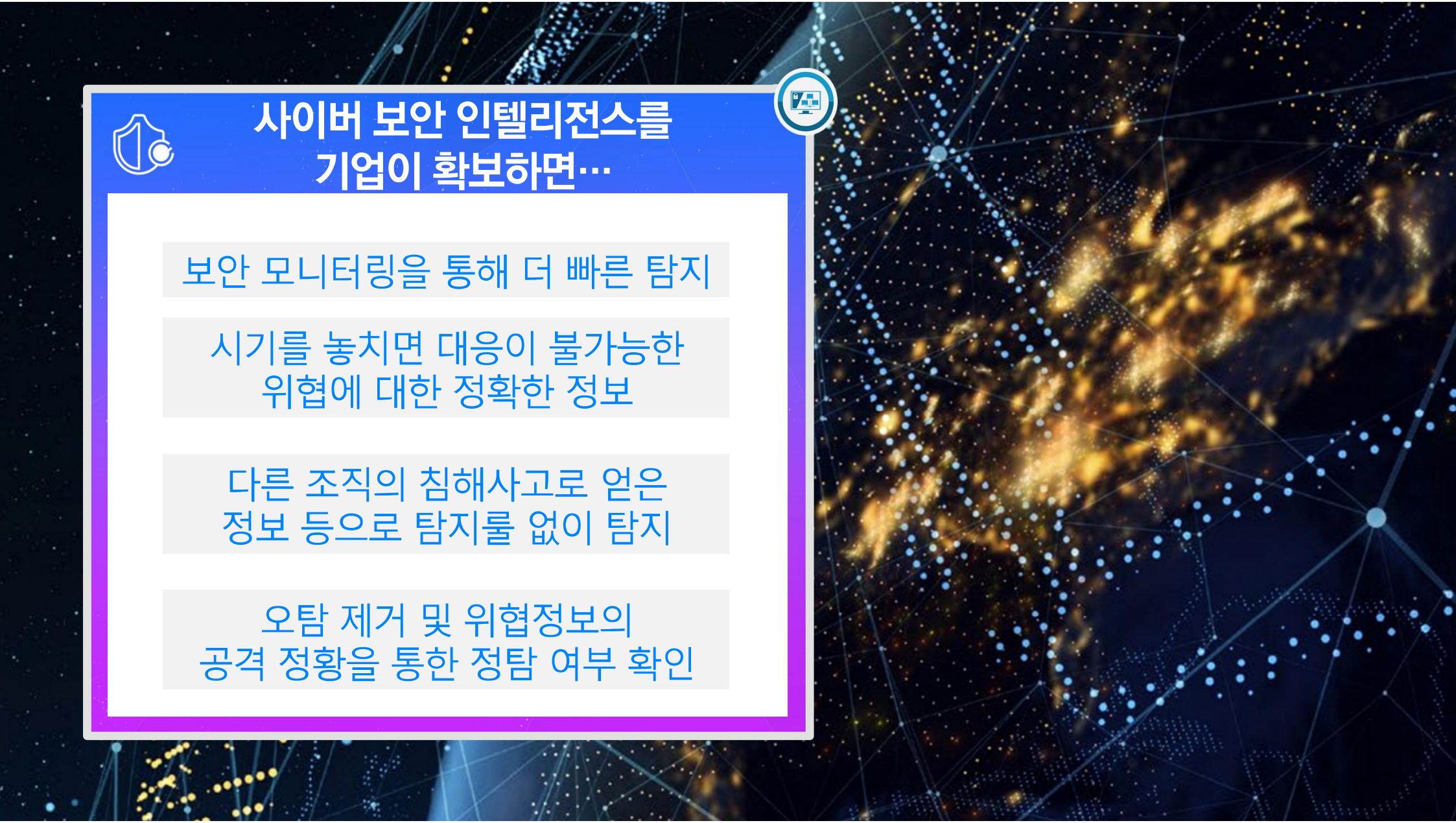
피해를 당한 이후의 보안 인텔리전스의 역할

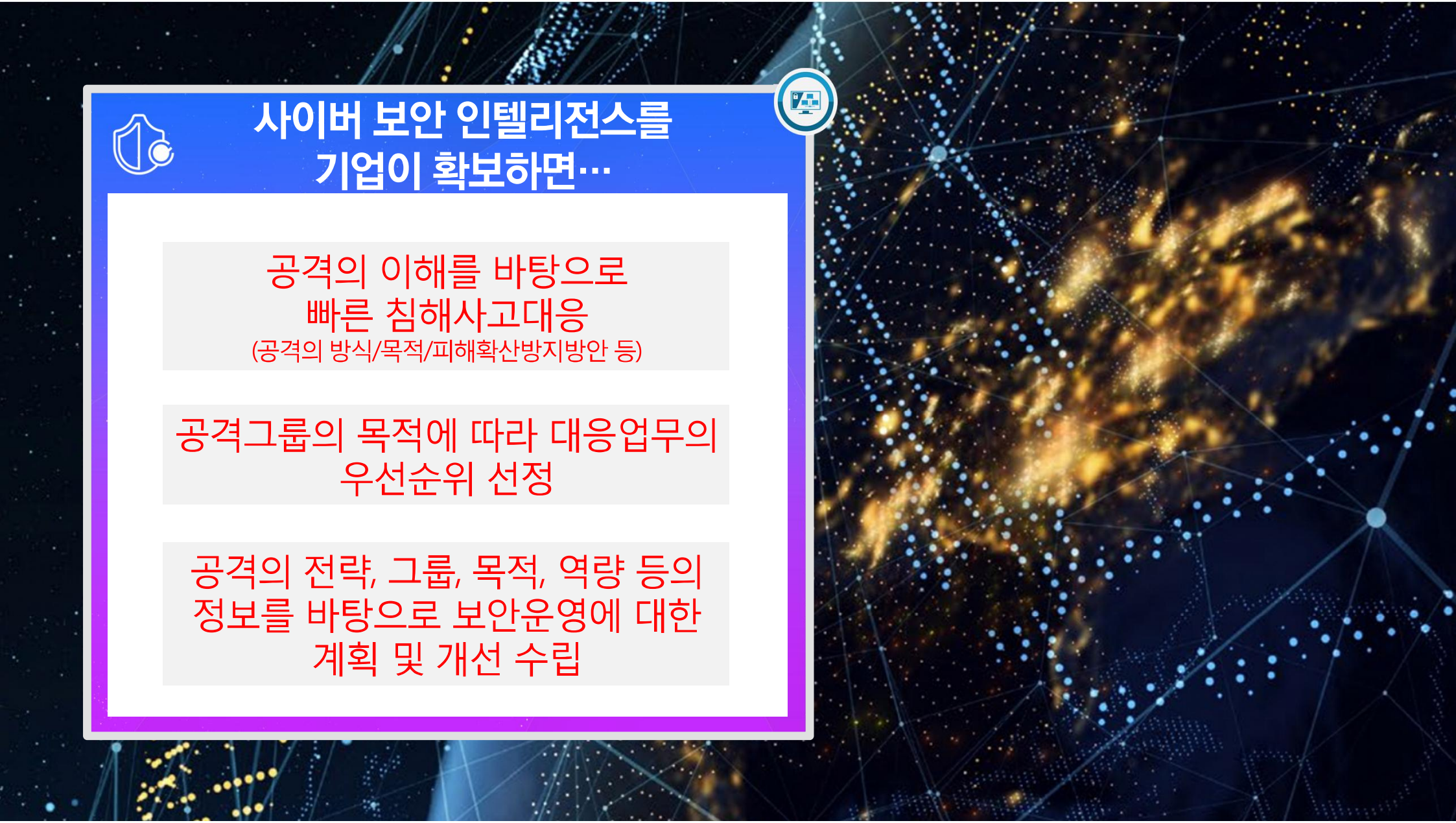
After

피해기업으로 부터의 정보 및
내부영향 확인

침해사고대응

사전수집된 정보를 바탕으로
효과적 복구방안수립


사이버 보안 인텔리전스를
기업이 확보하면…
보안 모니터링을 통해 더 빠른 탐지
시기를 놓치면 대응이 불가능한
위협에 대한 정확한 정보
다른 조직의 침해사고로 얻은
정보 등으로 탐지룰 없이 탐지
오탐 제거 및 위협정보의
공격 정황을 통한 정탐 여부 확인


사이버 보안 인텔리전스를
기업이 확보하면…
공격의 이해를 바탕으로
빠른 침해사고대응
(공격의 방식/목적/피해확산방지방안 등)
공격그룹의 목적에 따라 대응업무의
우선순위 선정
공격의 전략, 그룹, 목적, 역량 등의
정보를 바탕으로 보안운영에 대한
계획 및 개선 수립


랜섬웨어 예방 및
사이버 보안의 첫 걸음
전사원을 교육하라!
4차 산업혁명의 화두
보안과 사물인터넷

4차 산업혁명이란 무엇인가

4차 산업혁명이란 무엇인가

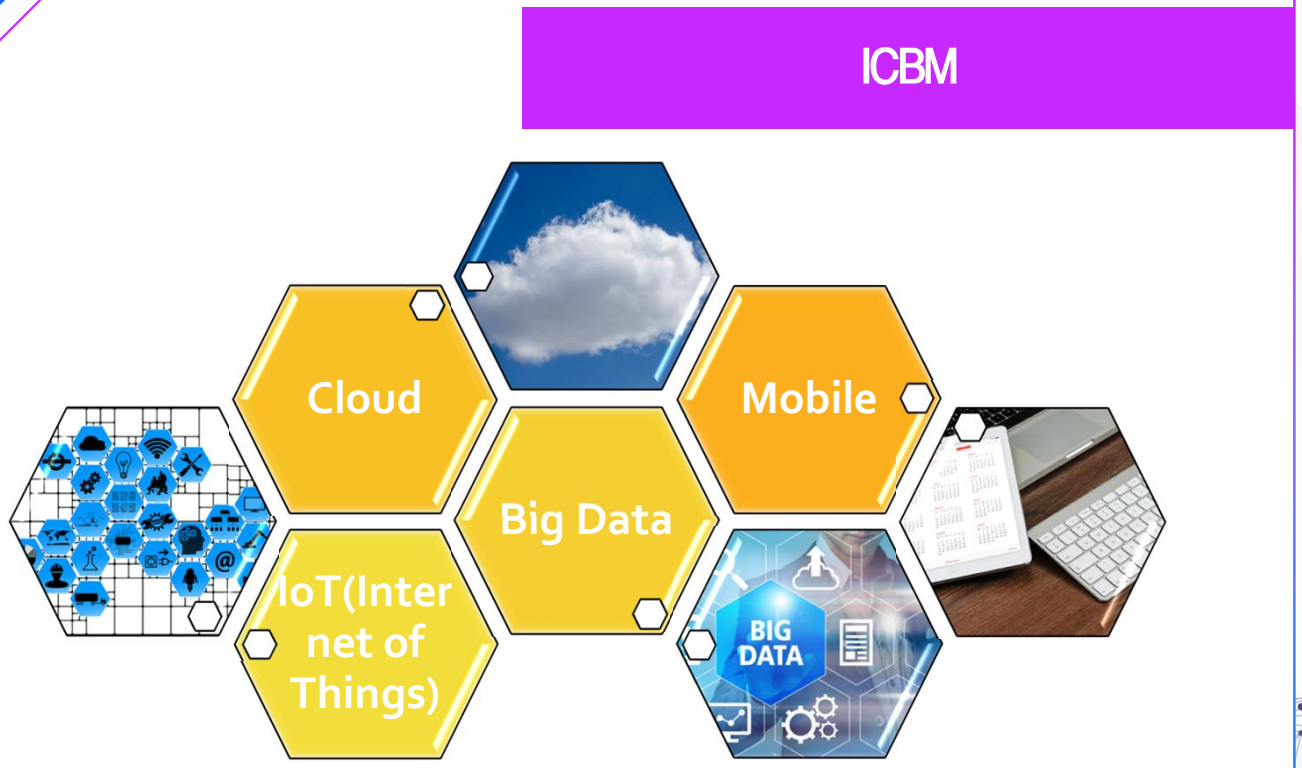
18세기 20세기 초 20세기 후반 현재

기계화 혁명 | 대량생산 혁명 | 지식정보 혁명 | 4차 산업혁명

지능 혁명

4차 산업혁명의 핵심 기술

ICBM



4차 산업혁명의 예
자율 주행 자동차

자율 주행 자동차

4차 산업혁명의 예
자율 주행 자동차

자율 주행 자동차

I I – 인터넷으로 연결된 자동차

C C – 클라우드를 이용한 실시간 정보 수집

B B – 주변의 모든 데이타를 수집

M M – 모바일 연결을 통해서 구동

A.I

인공지능을 이용해서
상황에 대한 판단

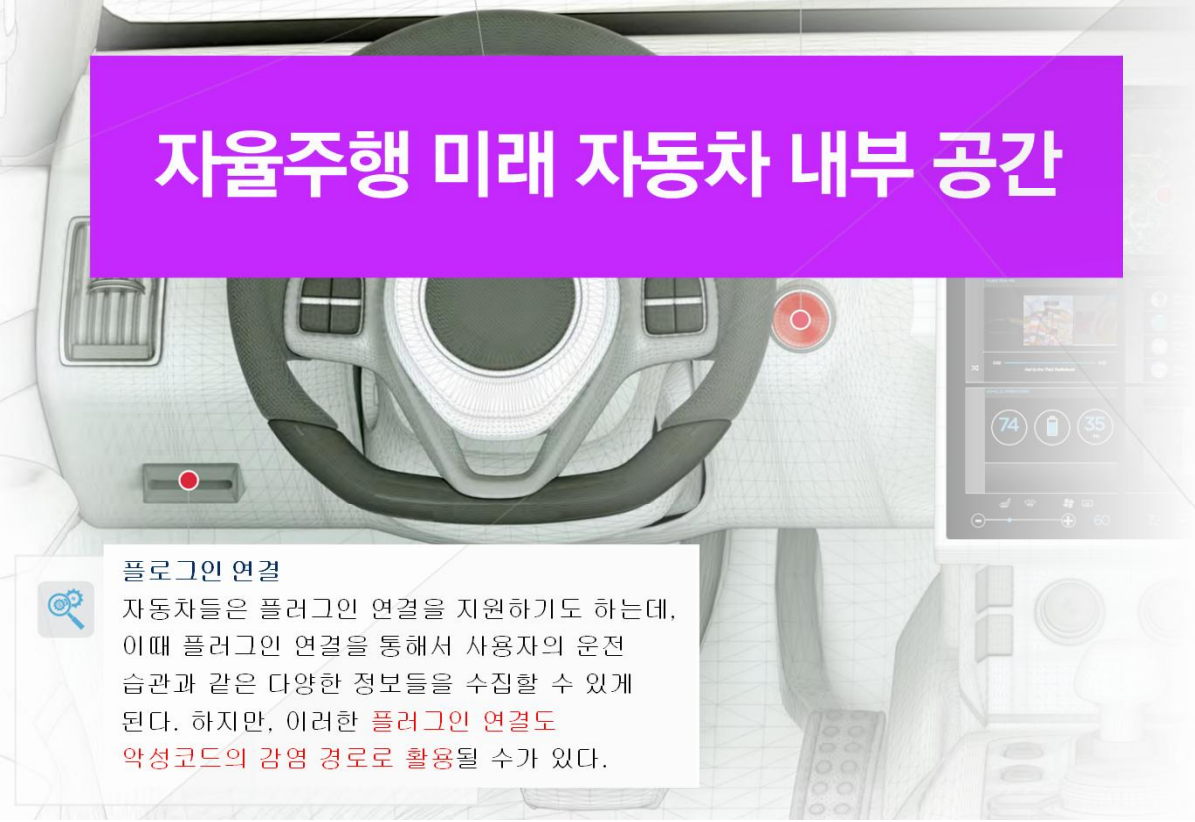
자동차 전자 제어 장치(ECU)

ECU는 브레이크, 액셀등을 모두 전자적으로 제어하는 역할을 한다. 자동차가 해킹이 될 경우에 이러한 모든 데이타에 대한 조작이 가능하다.

키 없는 자동차 접근

많은 차세대 자동차에서는 자동차 키 없이 자동차에 접근하고 관리하는 기술을 적용하고 있다. 예컨대, 모바일의 앱을 통한 관리등을 제공한다. 하지만, 허가 되지 않은 자동차에 대한 접속을 허용하는 통로가 될 수도 있다.

자율주행 미래 자동차 내부 공간



플로그인 연결

자동차들은 플러그인 연결을 지원하기도 하는데, 이때 플러그인 연결을 통해서 사용자의 운전 습관과 같은 다양한 정보들을 수집할 수 있게 된다. 하지만, 이러한 플러그인 연결도 악성코드의 감염 경로로 활용될 수가 있다.

자율주행 미래 자동차 내부 공간

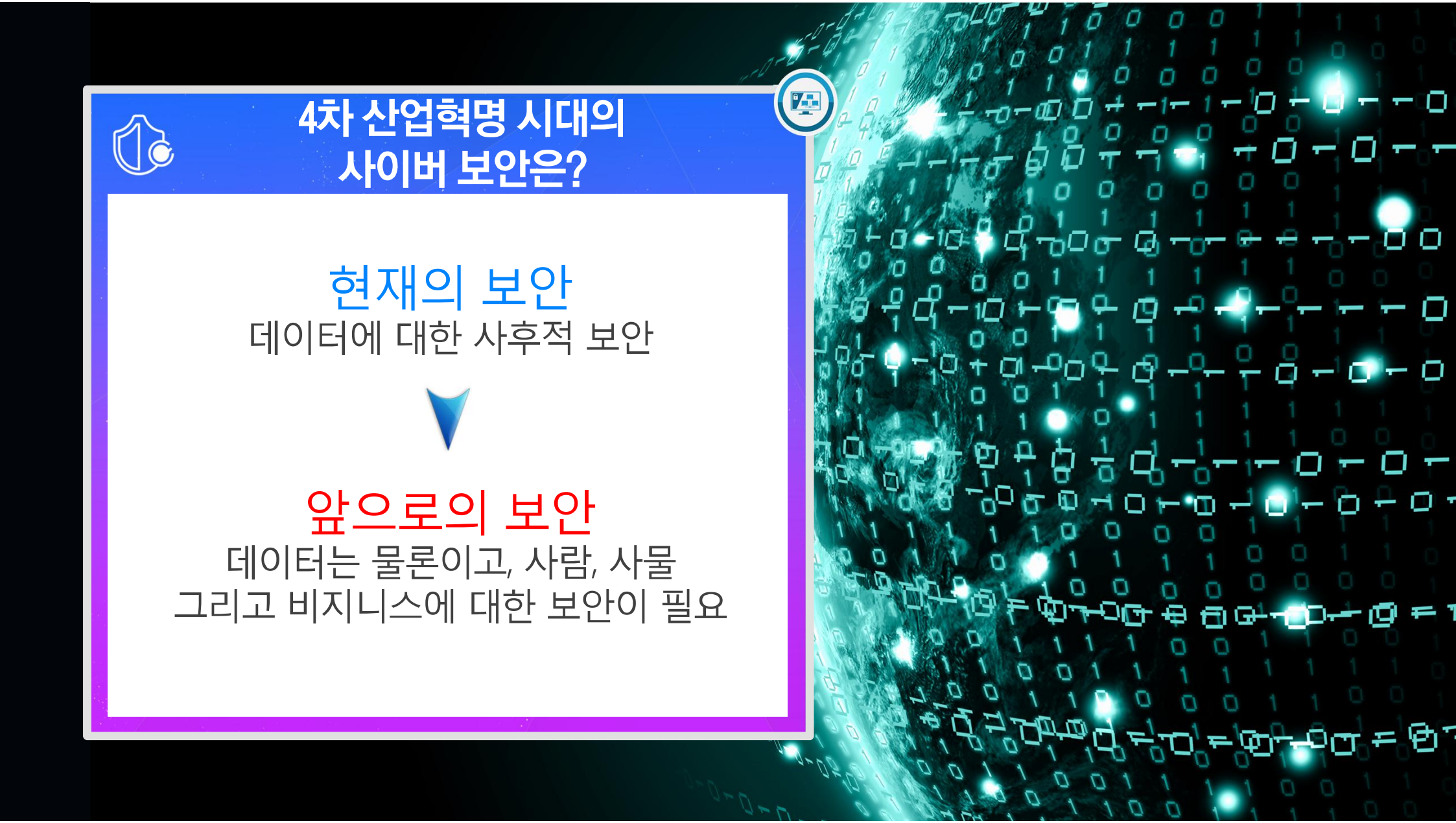
텔레매틱 시스템

많은 차세대 자동차들은 텔레매틱을 이용한 USB, 블루투스, GPS, Radio와 같은 다양한 기능들을 제공한다. 또, Wi-Fi 연결을 제공하기도 하는데 이러한 Wi-Fi 연결은 공격자가 원격에서 자동차로 침투 할 수 있는 또 다른 경로로 악용될 소지가 있다.

기온 조절 시스템

자동차가 제공하는 기온 조절 시스템은 항상 최적의 온도를 제공함으로써 운전자가 가장 쾌적한 환경에서 운전을 할 수 있도록 돕는다. 하지만, ECU를 통해서 기온 조절 시스템을 해킹할 경우에, 한여름에 히터를 틀어서 운전을 못하게 막을 수도 있다.

[1] Darren Pauli, "Mechanic computers used to pwn cars in new model-agnostic attack," *The Register*, March 15, 2016.


4차 산업혁명 시대의
사이버 보안은?
현재의 보안
데이터에 대한 사후적 보안
앞으로의 보안
데이터는 물론이고, 사람, 사물
그리고 비지니스에 대한 보안이 필요

사이버 보안의 위험

4차 산업혁명을 대비한 보안 체계의 핵심 요소들

4차 산업혁명 대비 보안 체계의 핵심 요소

클라우드

•향후 사물인터넷 환경의 보안에 대응하기 위한 필수 요소.
•클라우드 기반의 시스템 구성으로 물리적/지리적인 모든 제약을 넘어섬.

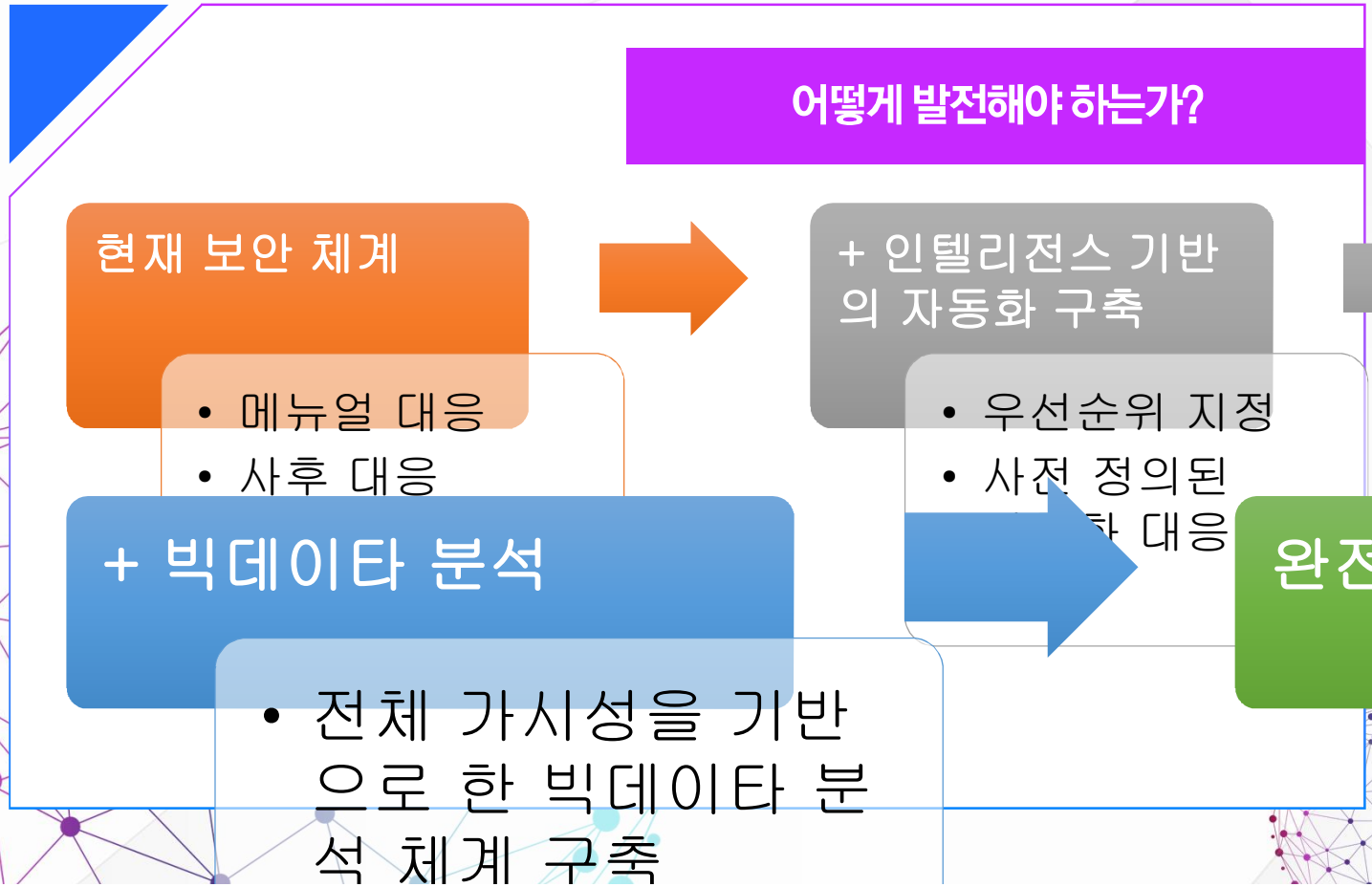
빅데이타

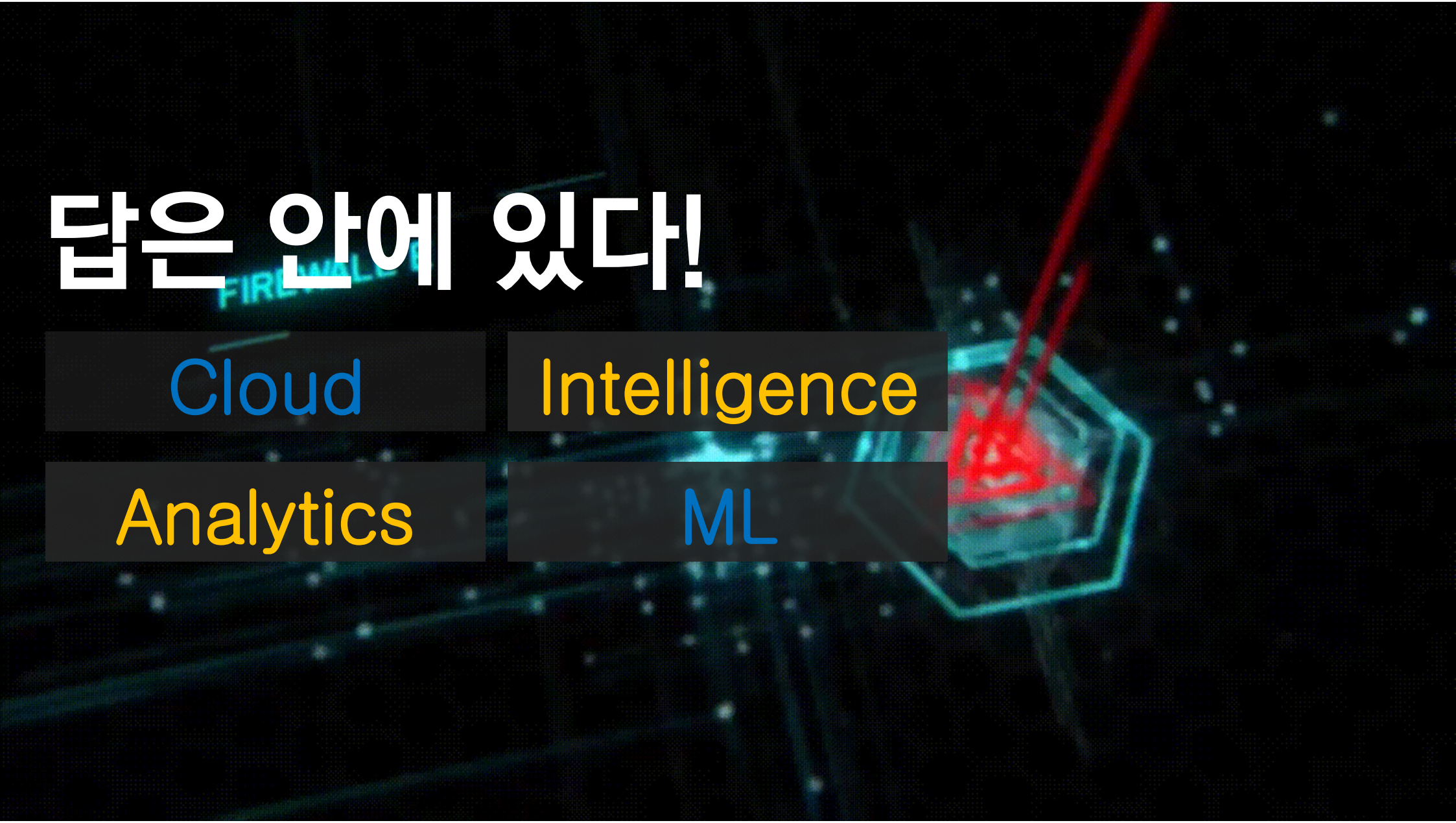
•수집되는 모든 로그와 보안 이벤트의 상관 관계를 자동으로 분석.
•이를 통해서 공격의 의도를 파악하여서, 잠재적인 미래의 위협에 대응.

머신러닝

•방대한 빅데이타를 기반으로 하여서, 스스로 상에 적응하여서 위협에 대응
•모든 보안 위협에 대해서 자동화된 프로세스를 통해서 실시간 대응

어떻게 발전해야 하는가?


어떻게 발전해야 하는가?
현재 보안 체계
• 메뉴얼 대응
• 사후 대응
+ 인텔리전스 기반의 자동화 구축
• 우선순위 지정
• 사전 정의된
+ 머신러닝 탐지
• 머신러닝 기반 탐지 기술을 기
+ 빅데이타 분석
• 전체 가시성을 기반으로 한 빅데이타 분석 체계 구축
완전 자동화 보안 체계
• 완전 자동화 대응
• 사전 헌팅


답은 안에 있다!
Cloud
Intelligence
Analytics
ML