# 스마트 빌딩 시스템에서 IoT 위협 인텔리전스 연구

강해인 (단국대학교 인공지능융합학과, 석사 과정)
박민수 (단국대학교 인공지능융합학과, 석사 과정)
고희아 (단국대학교 소프트웨어학과, 학사 과정)
조성제 (단국대학교 소프트웨어학과)

# INDEX


# 01 Introduction

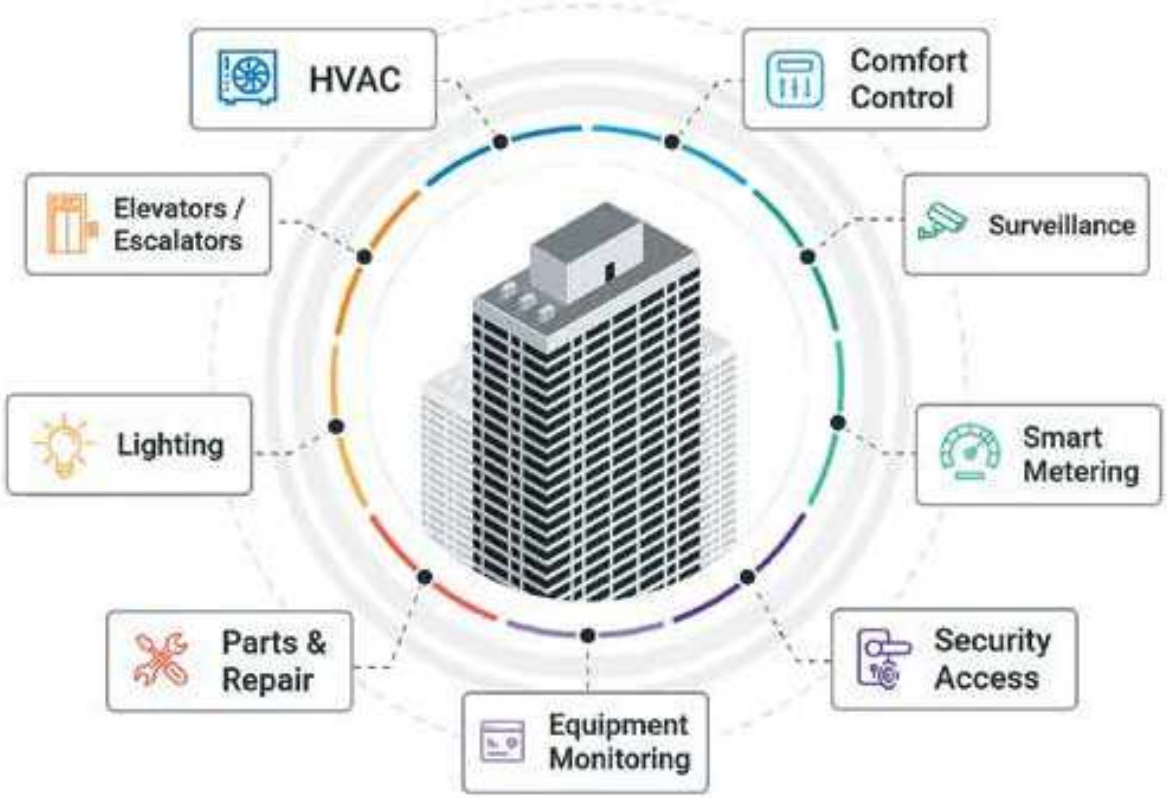
# Introduction

❖ 스마트 빌딩 시스템 사용

- 빌딩 제어 시스템에 ICS(Industrial Control System)/OT(Operational Technology) 구성 요소가 포함
- 센서로 IoT(Internet of Things) 기기를 사용

❖ 사용시 장점

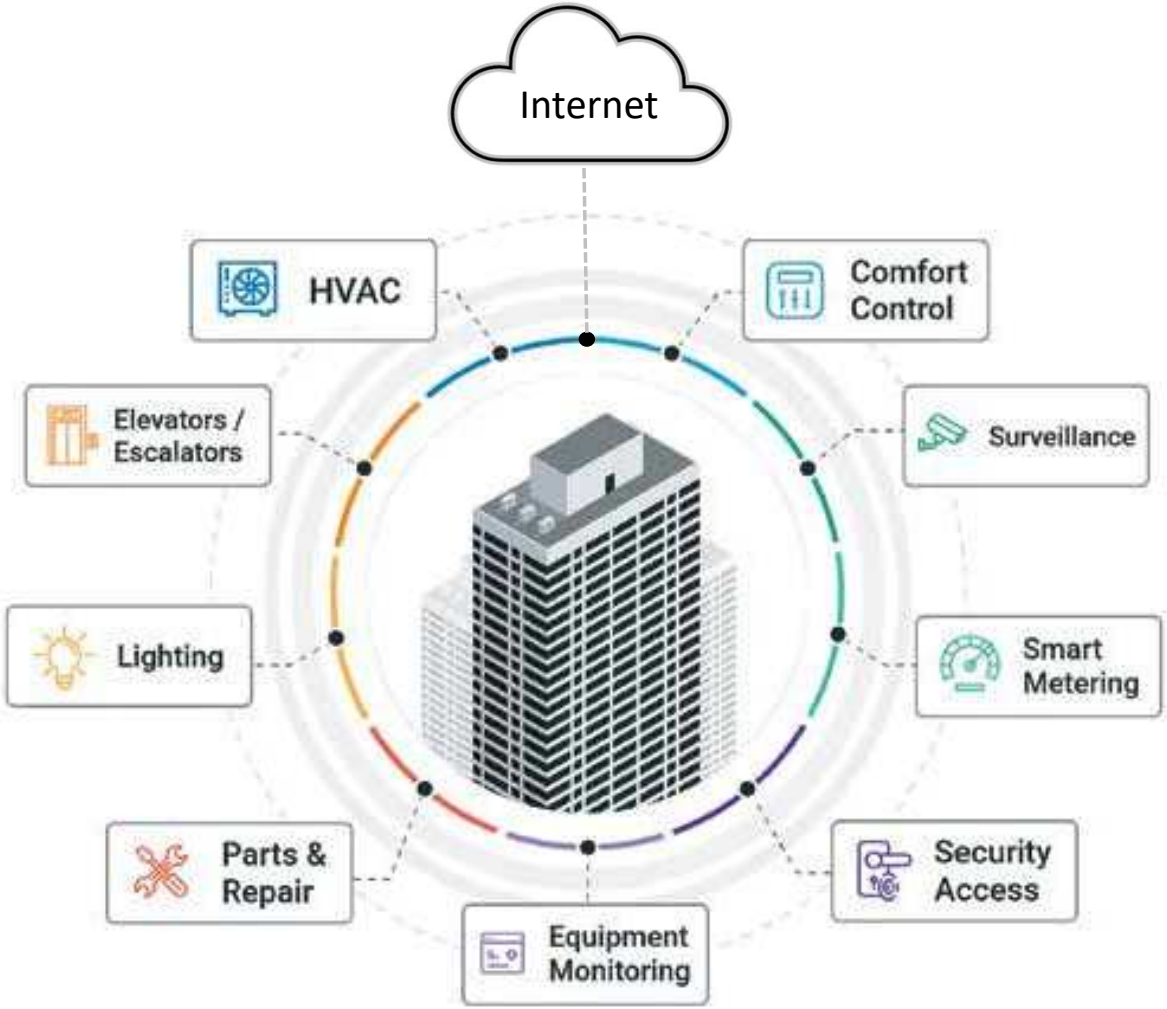
- 사람과 상호작용
- 에너지, 자원 소비량 대폭 감소
- 공기, 빛과 같은 환경 상태 파악해 운영 비용 절감의 효과



# Introduction

❖ 스마트 빌딩 시스템 문제점

- ICS/OT와 관련된 취약성 및 IoT 취약성이 매년 증가
- OT 제어 시스템에 인터넷이 연결되며 사이버 위협에 노출 위험 증가
  - 시스템이 인터넷에 연결되면 공격 표면이 기하급수적으로 넓어지고 이전과는 차별화된 사이버 보안 솔루션이 필요함



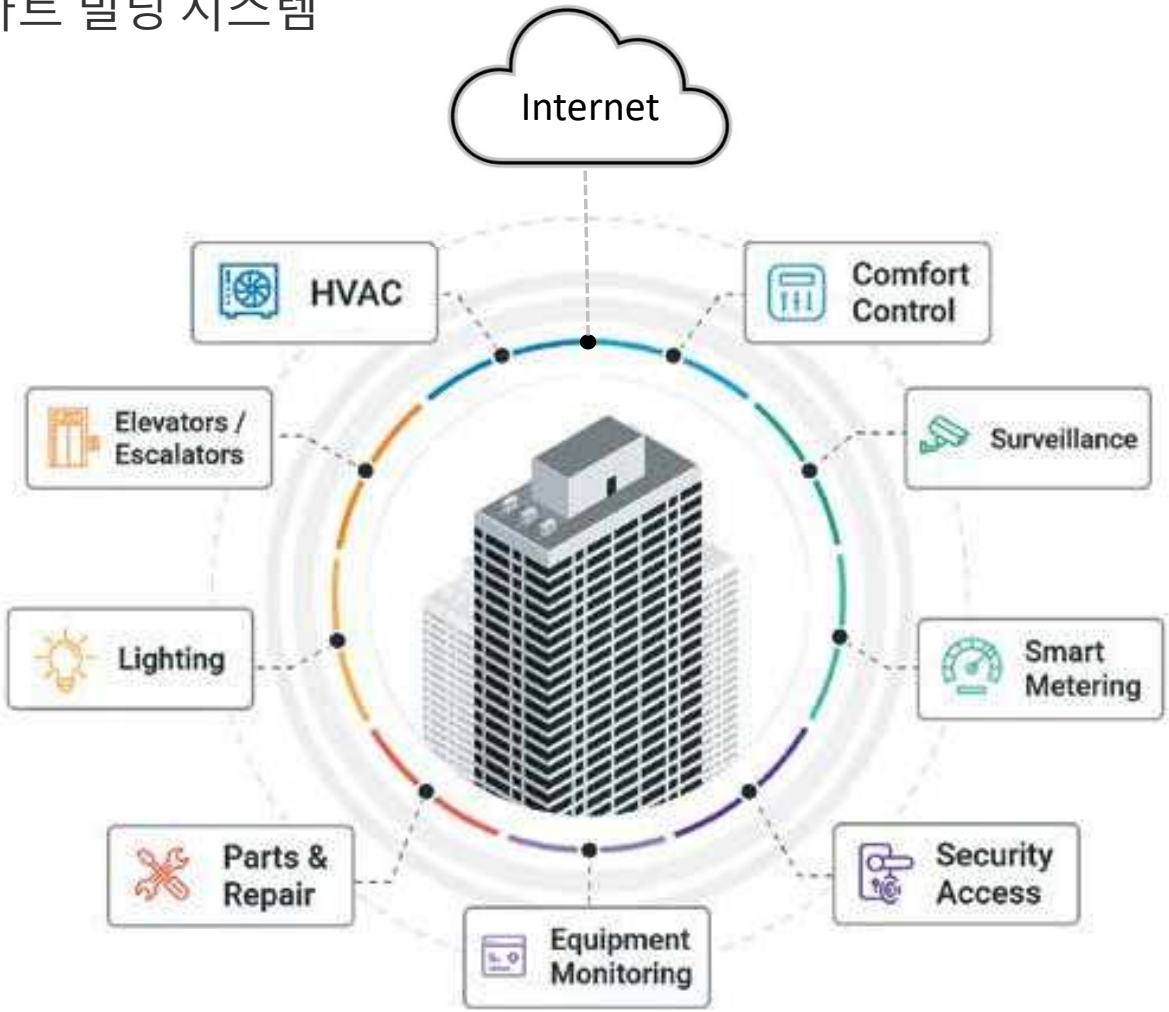

❖ 본 논문은 보안 솔루션 중 하나인 위협 인텔리전스에 대한 연구를 진행

[1] YU, Xingjie; GUO, Huaqun. A survey on IIoT security.
In: *2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS)*. IEEE, 2019. p. 1-5.

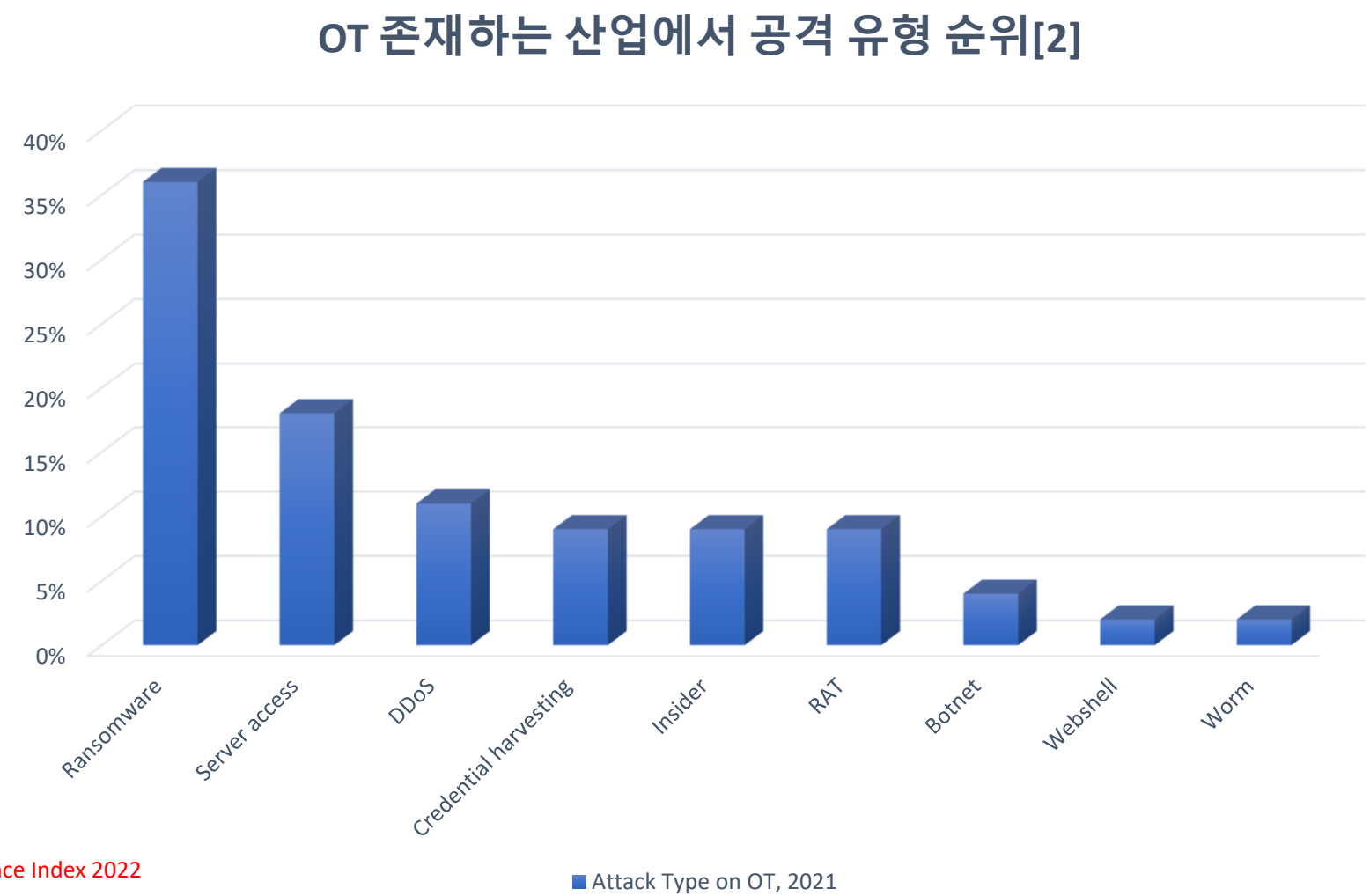
# 02 Background

# Background

❖ IoT 연결된 스마트 빌딩 시스템



# Background




[2] IBM Security.
X-Force Threat Intelligence Index 2022

# Background

❖ 위협 인텔리전스(Threat Intelligence)란?

- 사이버 공격에 대해 정리하고 분석한 증거 기반 정보 의미
- 공격자가 시스템을 손상시키고 방해하는 방법에 대해 자세하게 설명하므로 방어자는 사고 기준 이전, 도중, 이후 모두 보호할 수 있도록 준비 가능

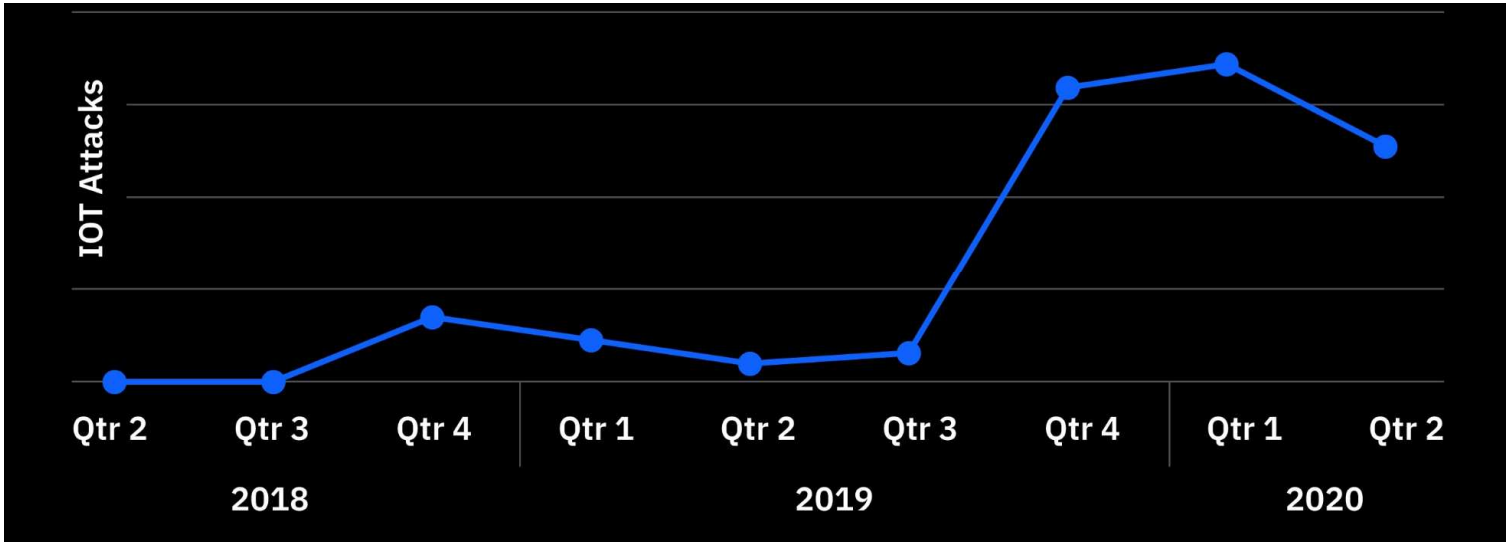
[3] CALTAGIRONE, Sergio.
Industrial control threat intelligence. 2018.


# 03 IoT Threat Intelligence in Smart building

# IoT Threat Intelligence in Smart building

❖ IoT 및 OT 자산 위협하는 Mozi Botnet

- Mozi 봇넷의 경우 2019년 12월 최초 보고되었으며 디폴트 패스워드 및 알려진 취약점을 통해 확산
- IBM X-Force에서 Mozi Botnet이 현재 IoT 장치를 오가는 트래픽의 90%를 차지한다는 것을 확인
- Mozi Botnet 포함 전반적인 IoT 봇넷 활동이 크게 증가하였는데, 실제로 2019년 10월부터 2020년 6월까지 결합된 IoT 공격 인스턴스는 이전보다 400% 증가




[2] IBM Security.
X-Force Threat Intelligence Index 2022

❖ 침해지표 (IoC, Indicator of Compromise)

- 포함되어지는 것 : 위협 행위자가 남긴 디지털 증거를 추출해내는 과정에서 유형을 지표화한 것
  - Mozi Botnet 공격에 사용한 C&C 서버 IP 주소 및 도메인

| 도메인 | 설명 |
|---|---|
| 78.142.18.20 | C&C server |

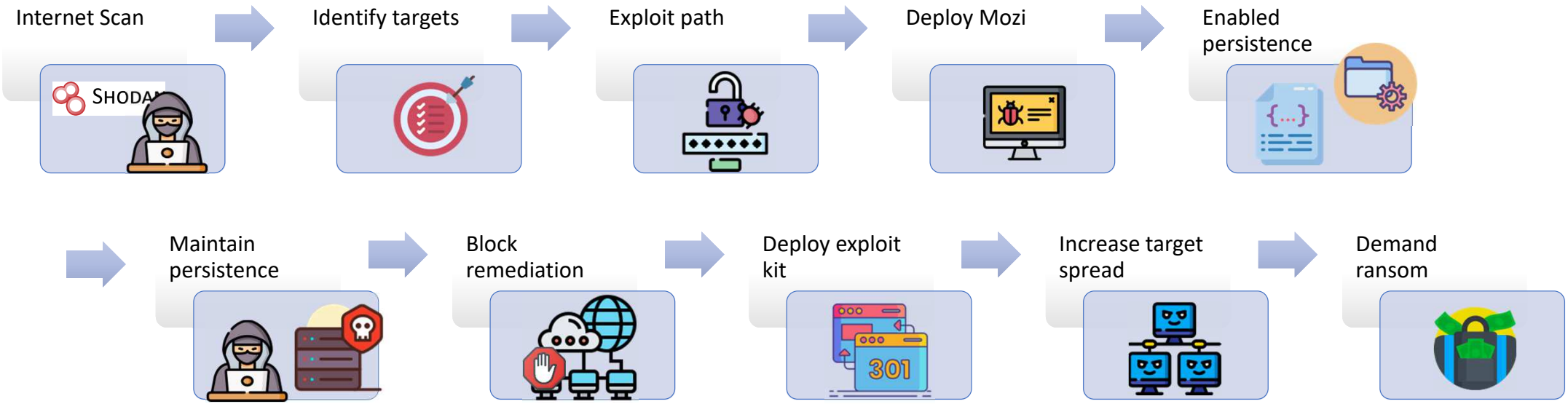
  - 파일 이름 및 해시

| 파일 이름 | 해시 |
|---|---|
| mozi.m | 4dde761681684d7edad4e5e1ffdb940b5738f1bc69e78d234dd04e2fbfcfb4b86403fc9117b133cf1bb7cda67e7aef0a, 86d42d968d3d12c36722e16c78e49ffb |
| mozi.a | 9a111588a7db15b796421bd13a949cd483441d77abb6cf328e77e372dc17c607fb9c4a261722ae80d83708ae3865053d, dd4b6f3216709e193ed9f06c37bcc3890 |

  - 로그 파일
    - C&C 서버와 Bot 사이 지속적인 통신을 위한 Heartbeat와 같은 네트워크 패킷들의 기록(비정상적인 로그)

# IoT Threat Intelligence in Smart building

❖ 공격 흐름



# IoT Threat Intelligence in Smart building

❖ Adversarial TTPs (Tactics, Techniques, Procedures) 기반 심층 분석

- 행위를 부인하기 위한 보안 쉘 프로토콜(ssh) 또는 dropbear로 프로세스 이름 변경
  - /usr/bin/python 파일 확인하고 존재하면 프로세스 이름 sshd로 변경 그렇지 않으면 dropbear로 변경

```
}

v4 = sub_41A3E0("/usr/bin/python", 0, param2, param3);
__pid_t v7 = v4 != -1 ? "sshd": "dropbear";
v6 = *v3;
v4 = sub_41F080(v6);
param2 = v4;
sub_41F210(v6, *&gvar_4803B0 - 13768, param2);
gi_sprintf(*v3, v7, param2, param3);
param1 = v7;
prctl(15);
v4 = time(0);
v6 = v4;
v4 = __libc_getpid(0, param1, 0, 0);
sub_423BE4(v4 ^ v6, param1, 0, 0);
v4 = time(0);
v6 = v4;
```

**T0849 Masquerading(Tactics : Evasion)**

- Iptables 명령 사용하여 DDoS 공격을 위한 임의의 TCP 및 UDP 포트 열고 ssh 또는 Telnet 같은 일반 포트 차단

**T0885 Commonly Used Port(Tactics : Command and Control)**

# IoT Threat Intelligence in Smart building

❖ Adversarial TTPs (Tactics, Techniques, Procedures) 기반 심층 분석

- 취약한 암호를 사용하거나 발견된 취약점을 사용해 잠재적 Bot을 발견하는 순간 악성 코드를 주입
- 특정 권한을 얻으면 Mozi Payload가 다운로드, 실행

**T0873 Project File Infection(Tactics : Persistence)**

- 감염 시키는 방법
  - Mozi 암호 테이블(통계 자료를 기반으로 함)을 활용해 기기에 대한 무차별 대입 공격
  - ICS/OT 특성상 업데이트가 이루어지는데 오랜 시간 소요 + 인식 문제로 인해 시스템 관리자가 업데이트를 하지 않는 경우 발생

**T0857 System Firmware (Tactics : Persistence)**

# IoT Threat Intelligence in Smart building

❖ Adversarial TTPs (Tactics, Techniques, Procedures) 기반 심층 분석

- Mozi Botnet 공격에 활용된 취약점 리스트

| 영향 받는 장치 | 취약점 |
|---|---|
| Eir D1000 Router | Eir D1000 Wireless Router RCI |
| Vacron NVR devices | Vacron NVR RCE |
| Devices using the Realtek SDK | CVE-2014-8361 |
| Netgear R7000 and R6400 | Netgear cig-bin Command Injection |
| DGN1000 Netgear routers | Netgear setup.cgi unauthenticated RCE |
| MVPower DVR | JAWS Webserver unauthenticated shell command execution |
| Huawei Router HG532 | CVE-2017-17215 |
| D-Link Devices | HNAP SoapAction-Header Command Execution |
| GPON Routers | **CVE-2018-10561**, CVE-2018-10562 |
| D-Link Devices | UPnP SOAP TelnetD Command Execution |
| CCTV DVR | CCTV/DVR Remote Code Execution |

- 예시로 CVE-2018-10561의 경우, 인증이 필요한 장치의 URL에 “?images”를 추가하여 인증 우회 가능
- 이러한 취약점을 통해 기기를 장악할 수 있게 됨.

# IoT Threat Intelligence in Smart building

❖ Adversarial TTPs (Tactics, Techniques, Procedures) 기반 심층 분석

- 유지 보수를 위해 Mozi는 각 감염 대상에 대해 상태 정보 기록하는 데이터 구조 존재.
- 앞선 과정이 하나 이상의 상태 정보로 사용.
- 상태를 파악하여 Mozi Botnet 악성 코드의 전반적인 감염 프로세스가 완료되도록 함.

**T0801 Monitor Process State (Tactics : Collection)**

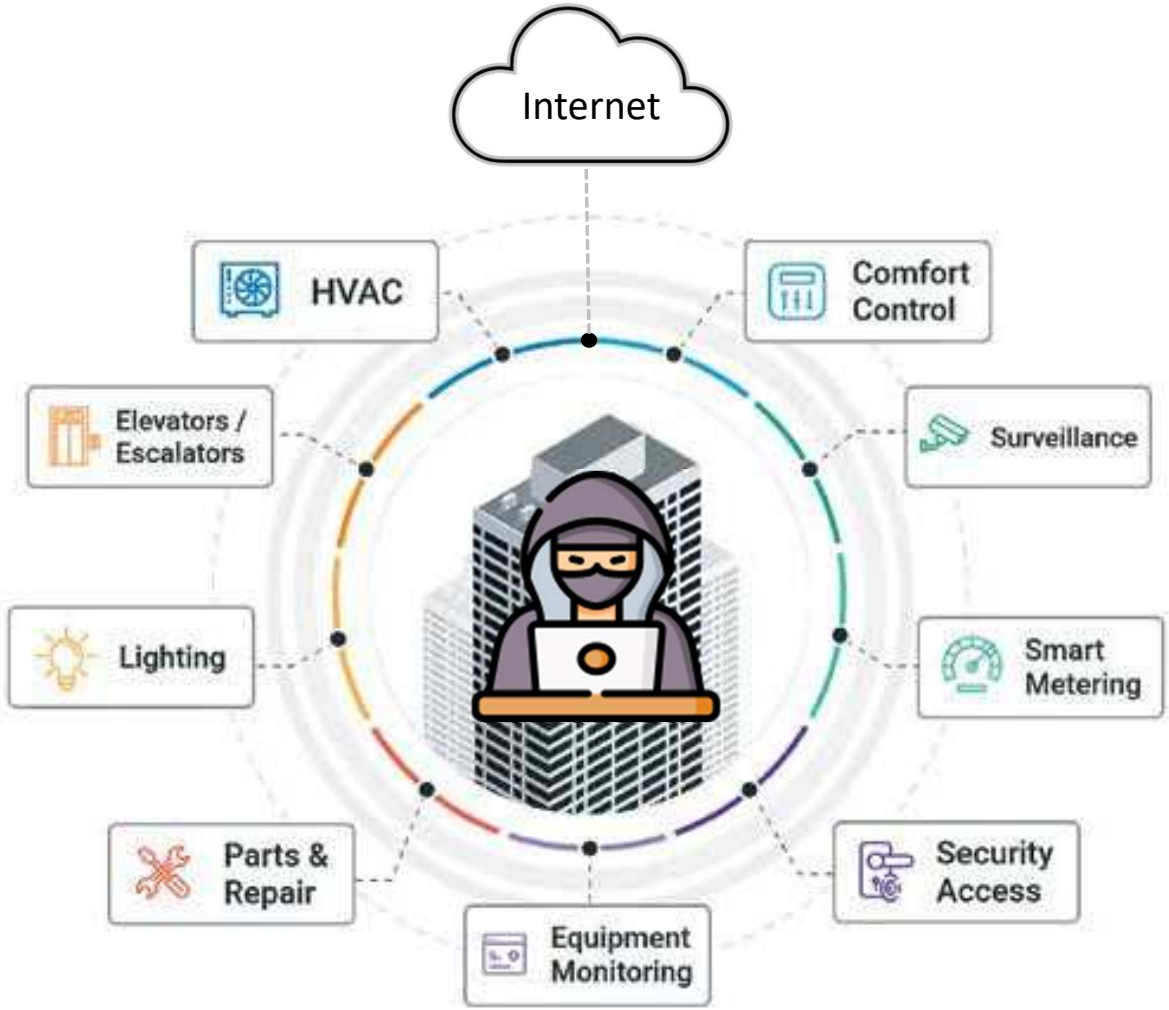
- Mozi의 명령 실행은 아래와 같은 방법 존재
  - TCP Flood
  - UDP Flood
  - Junk Flood
  - Hold Flood

**T0855 Unauthorized Command Message (Tactics : Impair Process Control)**

# IoT Threat Intelligence in Smart building

❖ 비즈니스에 영향을 미치는 정도

- 스마트 빌딩은 가용성의 중요도 높은 편.
- Mozi Botnet과 같은 DDoS 공격 실행으로 인하여 IoT 장치 또는 OT 시스템이 파괴되는 경우, 스마트 빌딩 전체 장악 가능.
- 막대한 재산 피해, 인명 피해 발생.



# IoT Threat Intelligence in Smart building

❖ 방어하는 방법에 대한 조언

- 디폴트 패스워드를 변경.
- 공급 업체에서 제공하는 최신 펌웨어 및 소프트웨어로 업데이트.
- 외부 접근에 대해 제어.

- 위 사항들은 사용자의 적극적인 행동 필요.

- IoT 기기를 사용하는 스마트 빌딩 시스템 초기 건설 시
  - 계정 변경 유도, 자동 업데이트, 외부 접근 제어 기능 등이 초기에 설정 될 수 있게 벤더사의 세심한 노력이 필요.


# Importance of Threat Intelligence in Smart Buildings

# Importance of Threat Intelligence in Smart building

❖ 스마트 빌딩 시스템에서 위협 인텔리전스의 활용

- 지속적인 OT 및 IoT 자산 프로필 및 행동 데이터를 수집하여 위협 인텔리전스 정의
- 정의된 내용을 토대로 신속하게 포렌식 분석에 이용 가능
- OT 및 IoT 이상 행위 탐지에 적용 가능
- 새로운 위협과 신규 취약점을 탐지하는 것이 가능

- 전반적으로 빠르게 사고에 대응할 수 있게 됨.
  - 스마트 빌딩 전체를 장악하기 전 대응이 가능
  - 재산 피해, 인명 피해 예방

# 05 Conclusion

# Conclusion

❖ Summary

- IoT 기기를 사용하는 스마트 빌딩 시스템에서 위협 인텔리전스에 대해 연구
- ICS/OT에서 위협 인텔리전스의 중요도가 증가하고 있고 이를 어떻게 활용할 수 있는지 확인

❖ Discussion

- 위협 인텔리전스의 내용을 자동으로 탐지하는 기술의 등장으로 이를 효과적으로 활용할 수 있는 방안에 대한 논의가 필요

❖ Future work

- 실험환경을 구성하여 위 논의 사항을 검증하고 발전시키고자 함

# References


1. YU, Xingjie; GUO, Huaqun. A survey on IIoT security. In: *2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS)*. IEEE, 2019. p. 1-5.
2. IBM Security. X-Force Threat Intelligence Index 2022
3. CALTAGIRONE, Sergio. Industrial control threat intelligence. 2018.
4. VERMA, Anurag, et al. Sensing, controlling, and IoT infrastructure in smart building: a review. *IEEE Sensors Journal*, 2019, 19.20: 9036-9046.
5. TREND MICRO, Mirai Botnet Exploit Weaponized to Attack IoT Devices via CVE-2020-5902
6. Elastic Security Intelligence & Analytics Team, Collecting and operationalizing threat data from the Mozi botnet
7. TU, Teng-Fei, et al. A comprehensive study of Mozi botnet. *International Journal of Intelligent Systems*.
8. ALMAZARQI, Hatem A., et al. Profiling IoT Botnet Activity in the Wild. In: *2021 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2021. p. 1-6.
9. JADIDI, Zahra; LU, Yi. A Threat Hunting Framework for Industrial Control Systems. *IEEE Access*, 2021, 9: 164118-164130.

## Acknowledgement

"이 연구는 2021년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(no. 2021R1A2C2012574)”

"본 연구는 과학기술정보통신부 및 정보통신기획평가원의 2022년도 SW중심대학사업의 결과로 수행되었음"(2017-0-00091)


# Q&A