KNOW YOUR SECURITY RISK

How Secure Is Your Building Automation System (BAS)?

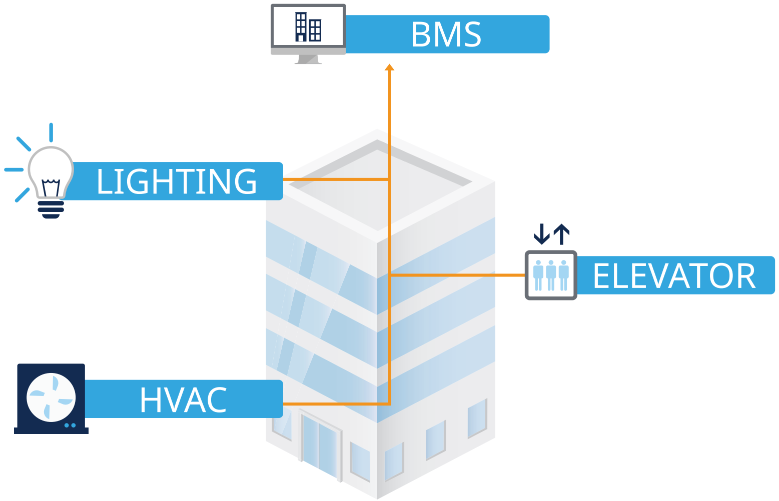
The Forescout Building Automation Risk Report explores the common systems that make organizations vulnerable to cyberattacks and how these systems could be exploited.

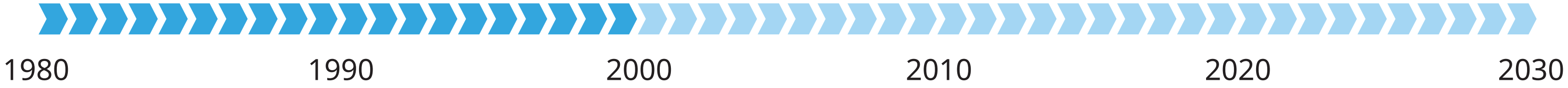
FORESCOUT®

Evolution of BAS (1/3)

Yesterday’s BAS

Buildings offered very basic services, consisting of only a central building management system (BMS) and one or two subsystems, such as HVAC, elevators or lighting systems, that were isolated from each other and outside networks.

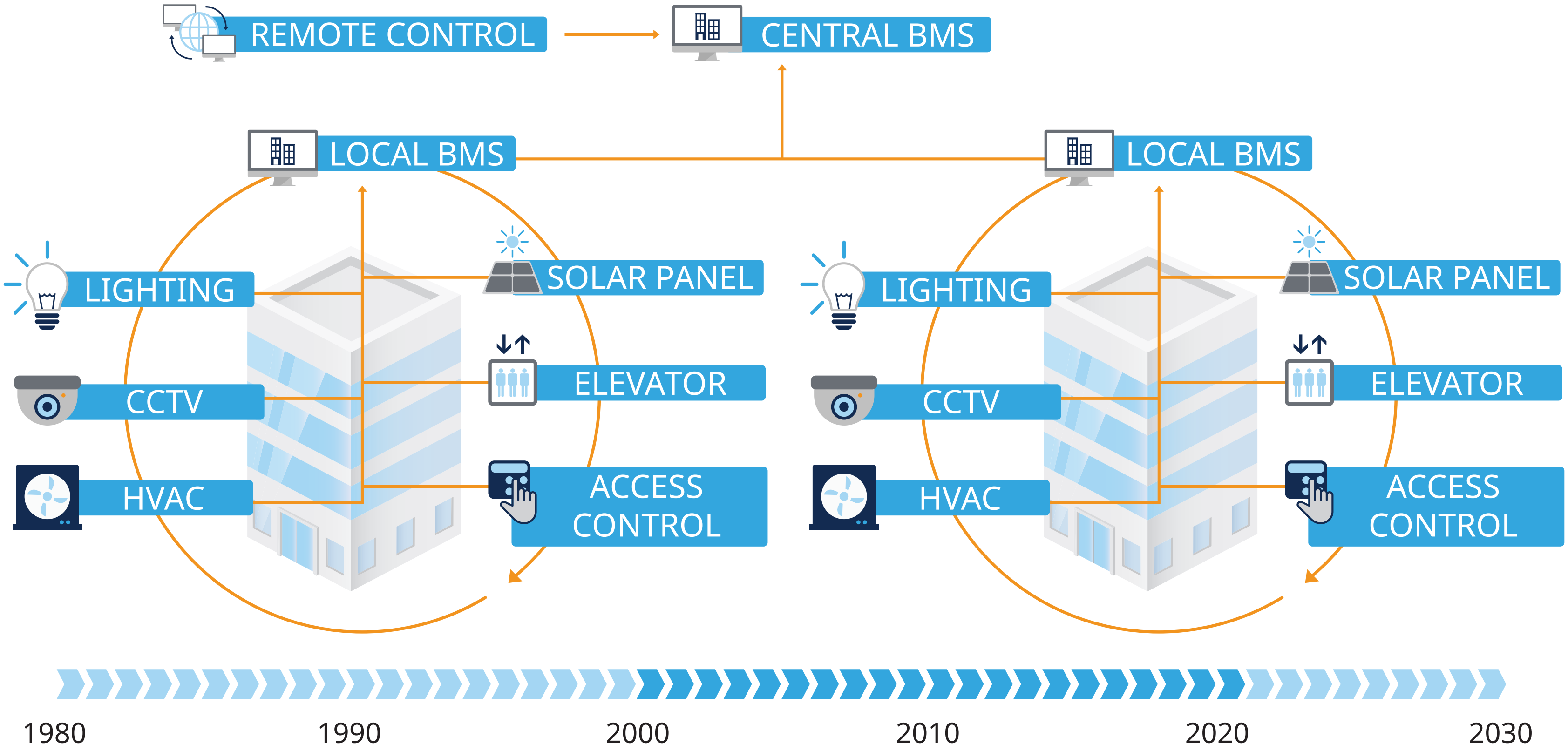




Evolution of BAS (2/3)

Today's BAS

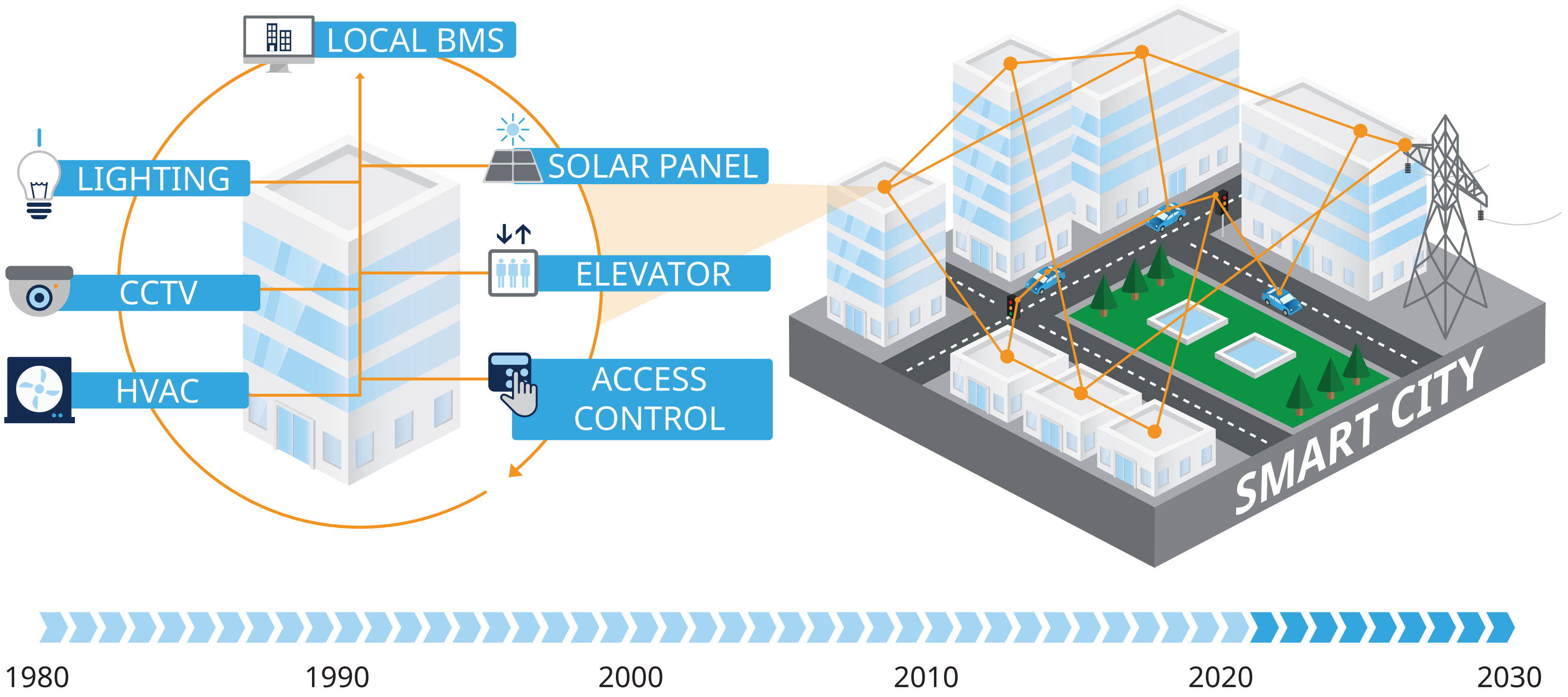
Today's buildings are smart buildings, with a central BMS that can integrate with the local BMS of multiple buildings within its network. Each local BMS connects to many different subsystems, including HVAC, surveillance, access control, and energy systems.



Evolution of BAS (3/3)

Tomorrow's BAS

Smart cities are the inevitable next step in this evolution of BAS. Smart buildings' local BMS will soon be able to integrate with any other building's local BMS, as well as the industrial infrastructure around them.



BAS Explosion

By 2026, there will be over

56 million

new BAS devices. [1]

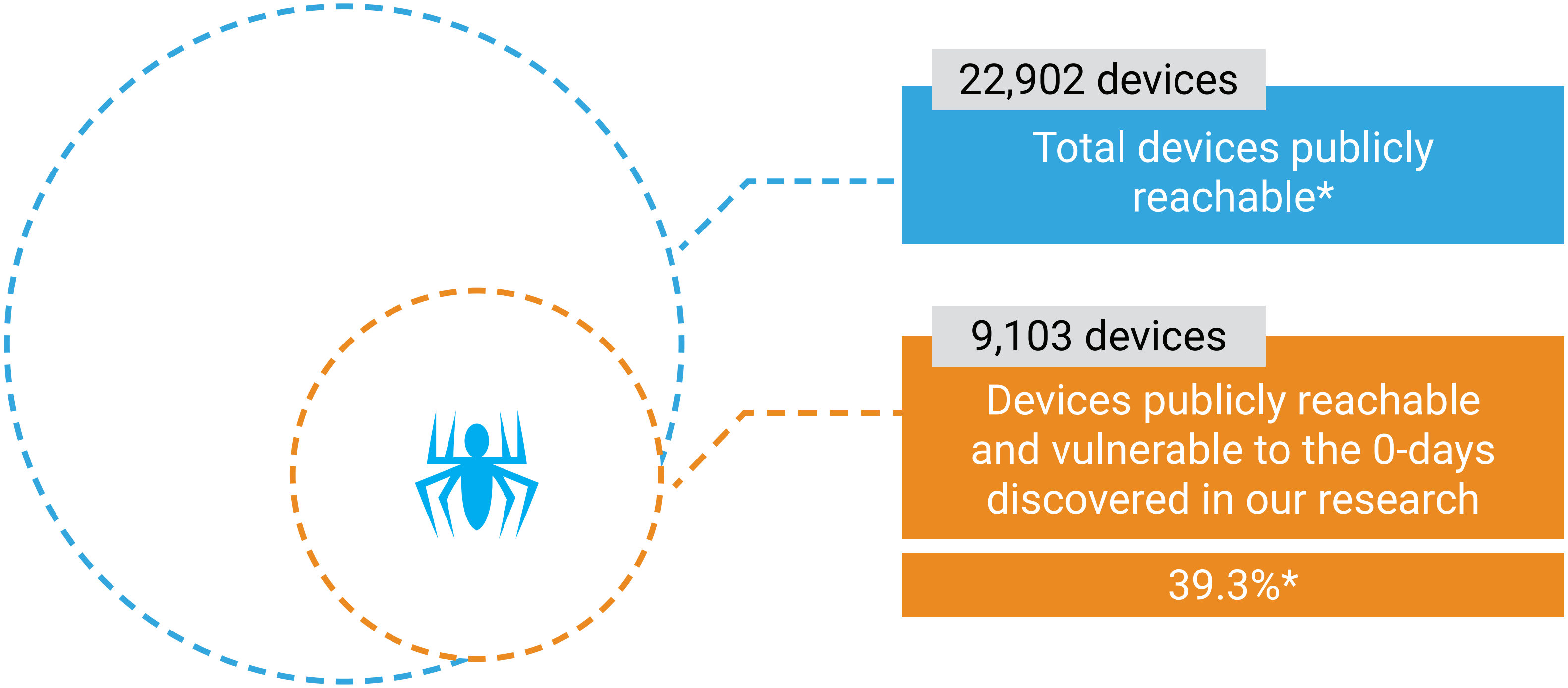
The number of identified vulnerabilities in BAS has increased over

500%

in the past three years. [2]

[1] ABI Research, 2019, BAS Wireless Field Equipment Shipments
[2] https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/07/07190426/KL_REPORT_ICS_Statistic_vulnerabilities.pdf

39.3% of publicly reachable BAS devices are vulnerable [1]



22,902 devices

Total devices publicly reachable*

9,103 devices

Devices publicly reachable and vulnerable to the 0-days discovered in our research

39.3%*

Vulnerable devices include:
HVAC PLCs, Access Control PLCs, Protocol Gateways

* Of the models used in our research

[1] Forescout, The Current State of Smart Building Cybersecurity, 2019: https://www.forescout.com/securing-building-automation-systems-bas/

Research Overview

Forescout BAS Risk Report

Industry attention has recognized the threat of commonly known Internet of Things (IoT) devices. What may go unnoticed is the potential safety and business risks to building automation systems (BAS).

Research into three key areas of BAS:

Surveillance

HVAC

Access Control

revealed that their core technologies, fundamental development methods and legacy implementations make implementing proper security an often overlooked, but critical, task.

Key Findings

Discovered and responsibly disclosed previously unknown vulnerabilities in building automation devices, ranging from controllers to gateways.

Developed a proof-of-concept malware that persists on devices at the automation level, as opposed to persisting at the management level as most OT malware does.

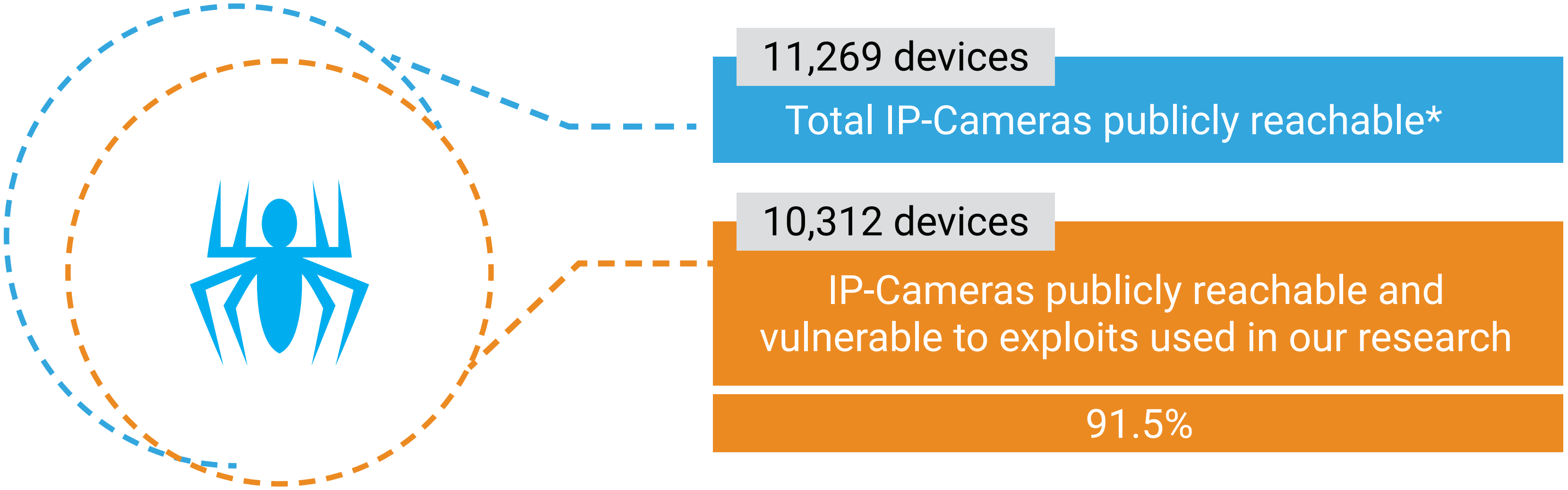
Debunked the myth that malware for cyber-physical systems must be created by actors that are sponsored by nation-states and have almost unlimited resources.

Concluded that improved device visibility into vulnerable BAS networks is one of the best ways to reduce risk.

Where Do The Vulnerabilities Lie?

EXPLORING THREE POTENTIAL ENTRY POINTS OF BAS

Area 1: Surveillance



11,269 devices

Total IP-Cameras publicly reachable*

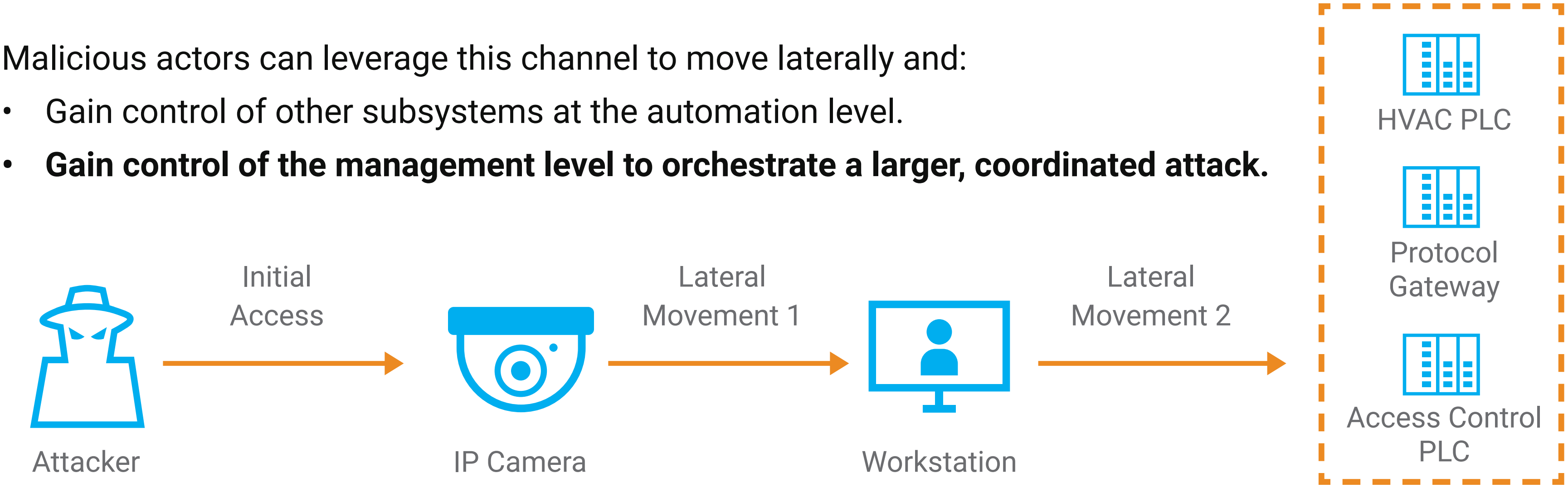
10,312 devices

IP-Cameras publicly reachable and vulnerable to exploits used in our research

91.5%

Malicious actors can leverage this channel to move laterally and:

- Gain control of other subsystems at the automation level.
- **Gain control of the management level to orchestrate a larger, coordinated attack.**



Attacker

Initial Access

IP Camera

Lateral Movement 1

Workstation

Lateral Movement 2

HVAC PLC

Protocol Gateway

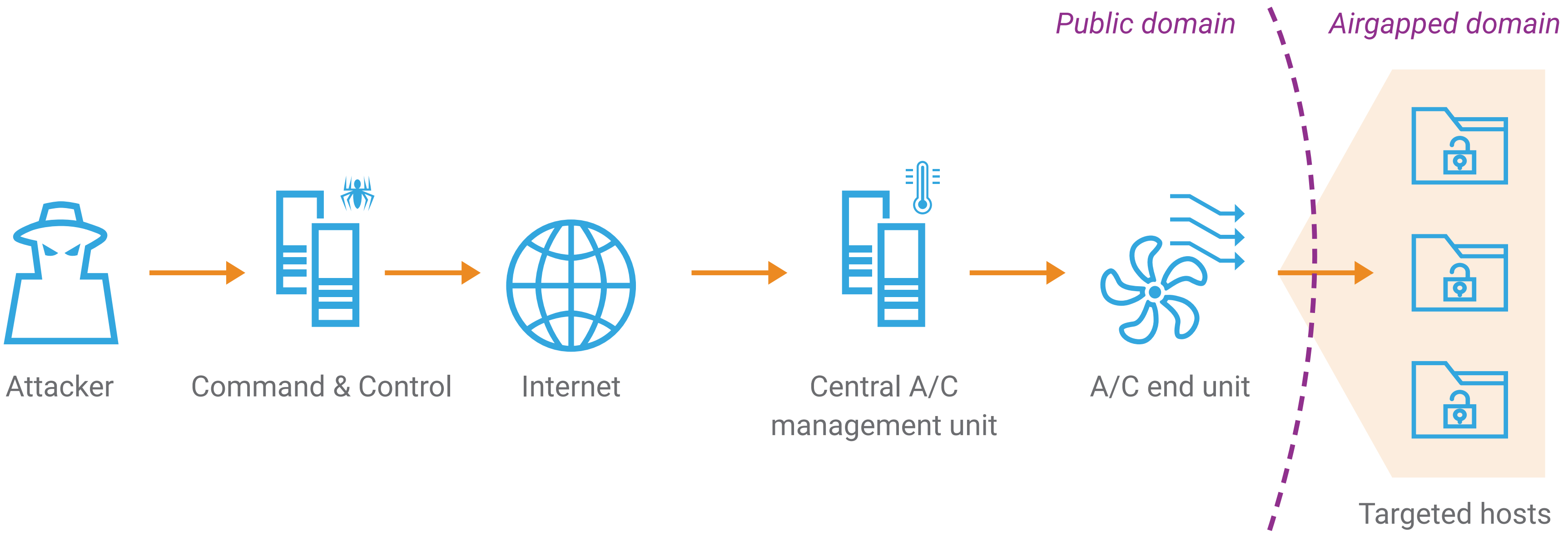
Access Control PLC

* Of the models used in our research

Area 2: HVAC

Malicious actors can use HVAC systems to bypass "air gaps" via a covert thermal channel [1] and move laterally to:

- Raise the temperature setpoint in a data center to cause business disruption.
- **Gain access to the management network to orchestrate a larger, coordinated attack.**

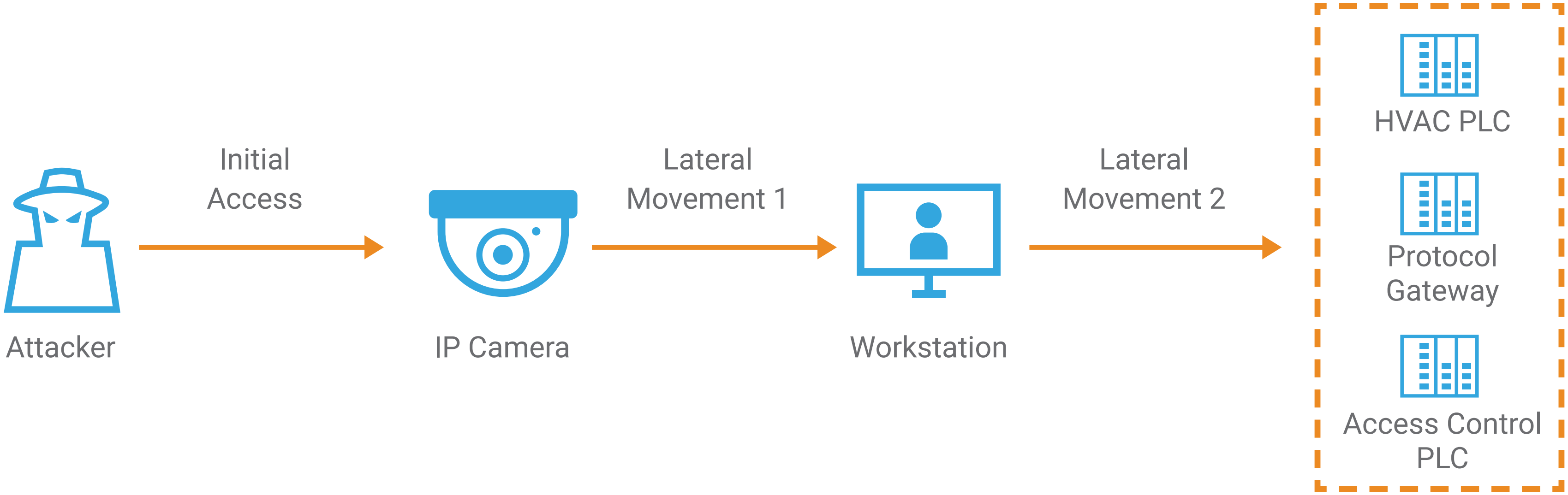


[1] Y. Mirsky, M. Guri and Y. Elovici, "HVACKer: Bridging the Air-Gap by Attacking the Air Conditioning System," 2017. [Online]. Available: https://arxiv.org/abs/1703.10454.

Area 3: Access Control

Malicious actors can use access control systems comprised of access badges, badge readers, controllers, and databases that store user credentials to:

- Control the doors and gain access to forbidden areas.
- Lock building occupants in and demand ransom.
- **Gain access to the management network to orchestrate a larger, coordinated attack.**

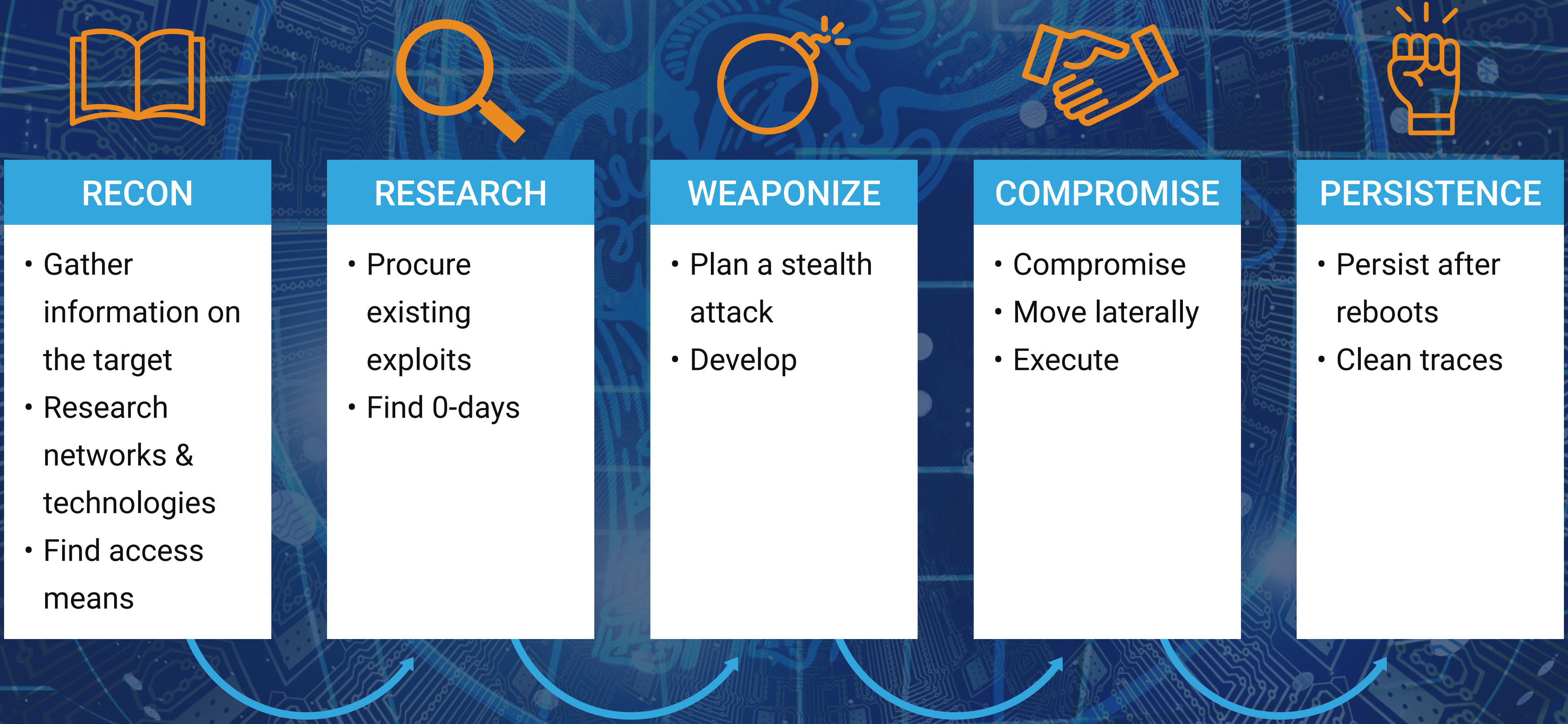


Proof-of-Concept Malware Development

THE METHODS USED

Methodology

Cyber Attack Lifecycle (Mandiant)



RECON

- Gather information on the target
- Research networks & technologies
- Find access means

RESEARCH

- Procure existing exploits
- Find 0-days

WEAPONIZE

- Plan a stealth attack
- Develop

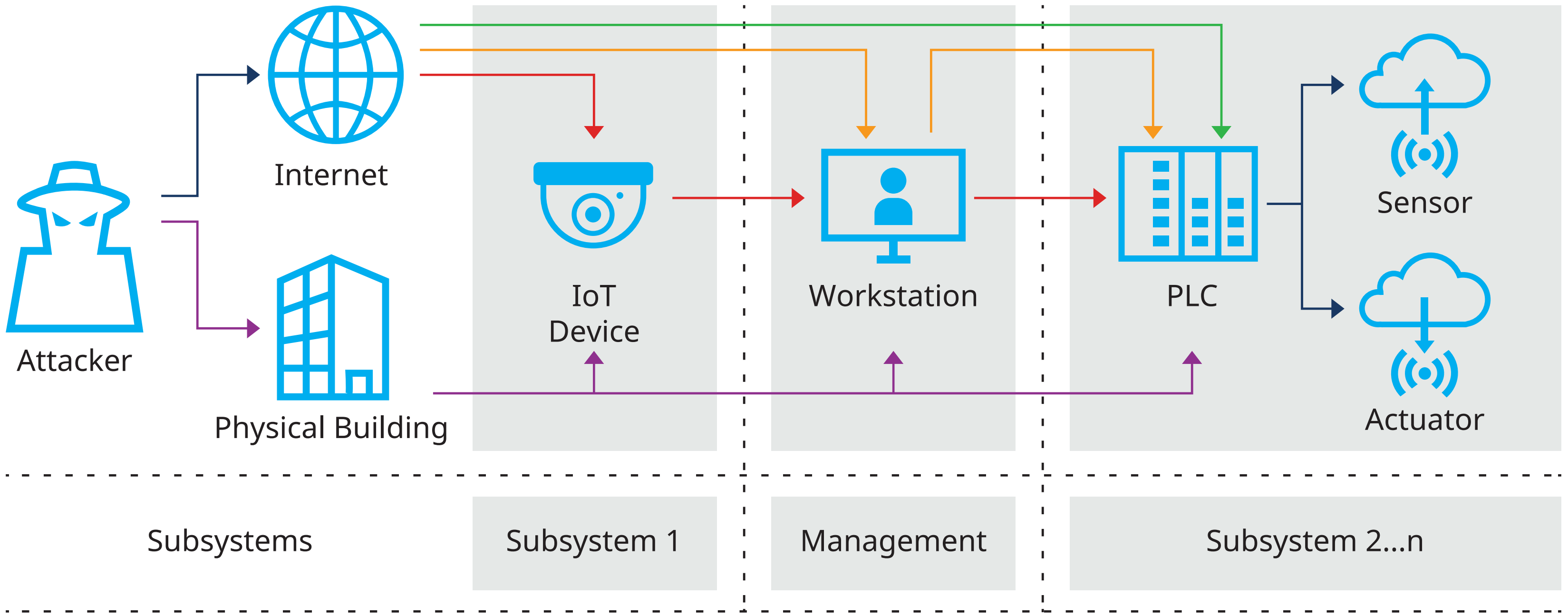
COMPROMISE

- Compromise
- Move laterally
- Execute

PERSISTENCE

- Persist after reboots
- Clean traces

Potential Attack Paths



1. Publicly reachable PLCs: Using this path, the malware can enter directly from the Internet and exploit the programmable logic controllers (PLCs) controlling the sensors and actuators at the field level, so there is no need to perform any lateral movement from other devices.

2. Publicly reachable workstations: Using this path, the malware can enter a workstation from the Internet at the management level and move laterally to the PLCs.

3. Publicly reachable IoT devices: Using this path, the malware can enter an IoT device, such as an IP camera or a WiFi router, from the Internet and use that entry point to gain access to the internal network, usually moving to the management level first and then to other subsystems.

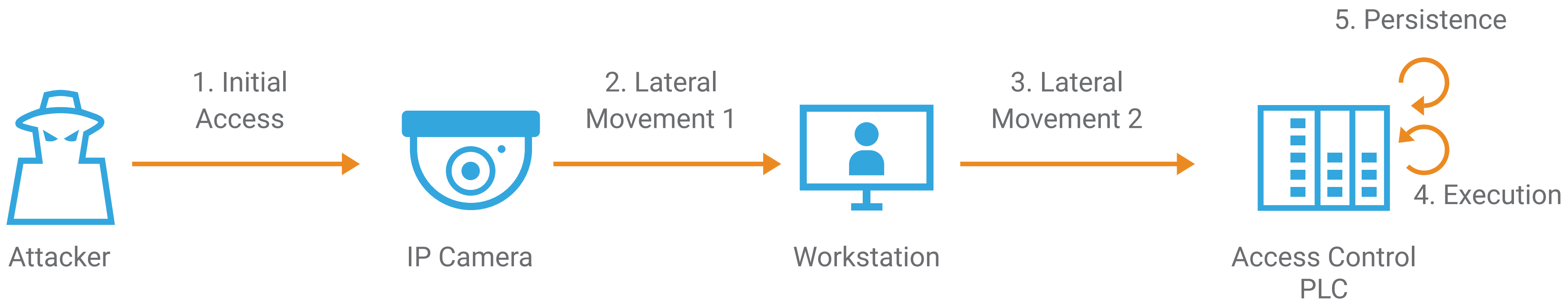
4. Air gapped network: Using this path, the attacker must have physical access to the building network (which could be accomplished via the HVAC system) and move laterally to reach the PLCs.

Attack Path Goals

#	Step	Goal	Possible Target
1	Initial Access	Establish an initial foothold in the network	PLCs (path 1) Workstations (path 2) IoT devices (path 3)
2	Lateral Movement 1	Move to the management level	Workstations or networking equipment
3	Lateral Movement 2	Move to another subsystem in the BAS	PLCs or IoT devices
4	Execution	Disrupt the normal functioning of the PLCs	PLCs
5	Persistence	Persist in the infected automation level devices	PLCs

Possible steps of an attack on building automation networks

The Attack Plan



Step 1 – Initial Access

The IP Camera can be exploited using a combination of **CVE-2018-10660** [1], **CVE-2018-10661** [2], and **CVE-2018-10662** [3]. The vulnerabilities and our exploit are based on the work of Or Peles [4] and the available Metasploit module [5].

STEP 2 - Lateral Movement 1

Once on the camera, the malware cleans its tracks by editing the files **/var/volatile/log/{auth,info}.log**, calls netstat to find the workstation connected to it (used for network video recording) and moves from the camera to the workstation by exploiting the misconfigured MS-SQL server.

Step 3 – Lateral Movement 2

While running on the workstation, the malware looks for an instance of the Access Control PLC workbench and reads its configurations files to find the devices connected to and being managed by that workstation.

Step 4 – Execution

After being dropped on the target device, the first goal of the final payload is to disrupt the normal behavior of the PLC by adding a new user and a new badge to the database, giving access to an otherwise unauthorized person.

Step 5 – Persistence

After the final payload has been executed, the malware has to persist on the device after reboots.

[1] "CVE-2018-10660," [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2018-10660

[2] "CVE-2018-10661," [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2018-10661.

[3] "CVE-2018-10662," [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2018-10662.

[4] O. Peles, "VDOO Discovers Significant Vulnerabilities in Axis Cameras," 2018. [Online]. Available: https://blog.vdoo.com/2018/06/18/vdoo-discovers-significant-vulnerabilities-in-axis-cameras/.

[5] Rapid7, "Axis Network Camera .srv to parhand RCE," [Online]. Available: https://www.rapid7.com/db/modules/exploit/linux/http/axis_srv_parhand_rce.

Vulnerabilities Discovered (1/2)

#	Product	Vulnerability Type	Notes
1	Protocol Gateway	XSS	0-day patched by the vendor and CVE assigned
2	Protocol Gateway	Path traversal	0-day patched by the vendor and CVE assigned
3	Protocol Gateway	Arbitrary file deletion	0-day patched by the vendor and CVE assigned
4	HVAC PLC	XSS	0-day patched by the vendor and CVE assigned
5	HVAC PLC	Authentication bypass	0-day patched by the vendor and CVE assigned
6	Access Control PLC	XSS	0-day patched by the vendor and CVE assigned
7	Access Control PLC	Hardcoded secret	Not 0-day, the vulnerability was known and patched by the vendor, but never disclosed.
8	Access Control PLC	Buffer overflow	Not 0-day, the vulnerability was known and patched by the vendor, but never disclosed.

Vulnerabilities Discovered (2/2)

- **XSS vulnerabilities** allow an attacker to inject malicious scripts into trusted web interfaces running on the vulnerable devices, which may be executed by the browser of an unsuspecting user to access cookies, session tokens, or other sensitive information, as well as to perform malicious actions on behalf of the user.

- **Path traversal and file deletion vulnerabilities** allow an attacker to manipulate path references and access or delete files and directories (including critical system files) that are stored outside the root folder of the web application running on the device.

- **Authentication bypass vulnerability** allows an attacker to steal the credential information of application users, including plaintext passwords, by manipulating the session identifier sent in a request.

> "A myriad of these affected BAS devices are available online and can still be exploited because they are unpatched."

The most severe vulnerabilities are issues #7 and #8, which allow a remote attacker to execute arbitrary code on the target device and gain complete control of it.

- **Hardcoded secret:** The Java framework used on the Access Control PLC and on its control software stores system configurations in a file called daemon.properties and application configurations in a file called config.bog, which is a compressed xml. These files contain usernames and passwords, among other information. The passwords are hashed or encrypted depending on the version of the framework.

- **Buffer overflow:** There is a binary daemon running on the Access Control PLC that exposes multiple HTTP endpoints that remote users can access to manage the device.

How to Reduce Risk for BAS Networks

Implement security solutions that offer:

Complete Device Visibility

- Passively and automatically establishes asset inventory with full device fingerprinting
- Documents the network baseline of normal communications
- Automatically assesses common vulnerabilities & exposures (CVEs) for BAS devices

Real-Time Threat Detection

- Continuously monitors the network for changes in behavior
- Automatically checks device behavior against threat indicators and protocol compliance standards
- Alerts in real time with interactive visualizations of threats and risks

Converged IT-OT Security

- Monitors both IT and OT networks from a single screen
- Offers extensive, cross-functional automation capabilities
- Is agentless and infrastructure-agnostic

Conclusion

Building automation systems (BAS) may be as critical as industrial control systems (ICS) in terms of safety and security, yet receive much less attention from the security community.

Enhancing BAS cybersecurity programs with device visibility and network monitoring can give organizations a thorough understanding of the environment and its connections, making it easier to design effective security architectures, identify attack vectors, and locate blind spots.

About the Researchers

Daniel dos Santos holds a PhD in Computer Science from the University of Trento and has experience in security consulting and research. He is a researcher at Forescout, focusing on vulnerability research and the development of innovative features for Forescout OT products.

Clément Speybrouck holds a post-master degree in Security in Computer Systems and Communication from EURECOM and worked as an intern at Forescout during the development of this research project.

Elisa Costante holds a PhD in Computer Science from the Eindhoven University of Technology. She is an expert in IT and OT security and privacy. As Head of Industrial and OT Research at Forescout, she manages the internal and external research activities. Her responsibilities include the management of national and international projects, the planning of research strategy and the supervision of prototype development activities for innovative features to be added to Forescout OT products.

Acknowledgement: the authors would like to thank **Andrés Castellanos-Páez** and **Jos Wetzels** for their help in discovering and exploiting the buffer overflow vulnerability.

Download the full research report to learn more about the current state of smart building cybersecurity

DOWNLOAD

About Forescout

Forescout Technologies is the leader in device visibility and control. Our unified security platform enables enterprises and government agencies to gain complete situational awareness of their extended enterprise environments and orchestrate actions to reduce cyber and operational risk. Forescout products deploy quickly with agentless, real-time discovery and classification, as well as continuous posture assessment.

Connect with us

www.forescout.com

@Forescout

Forescout Technologies