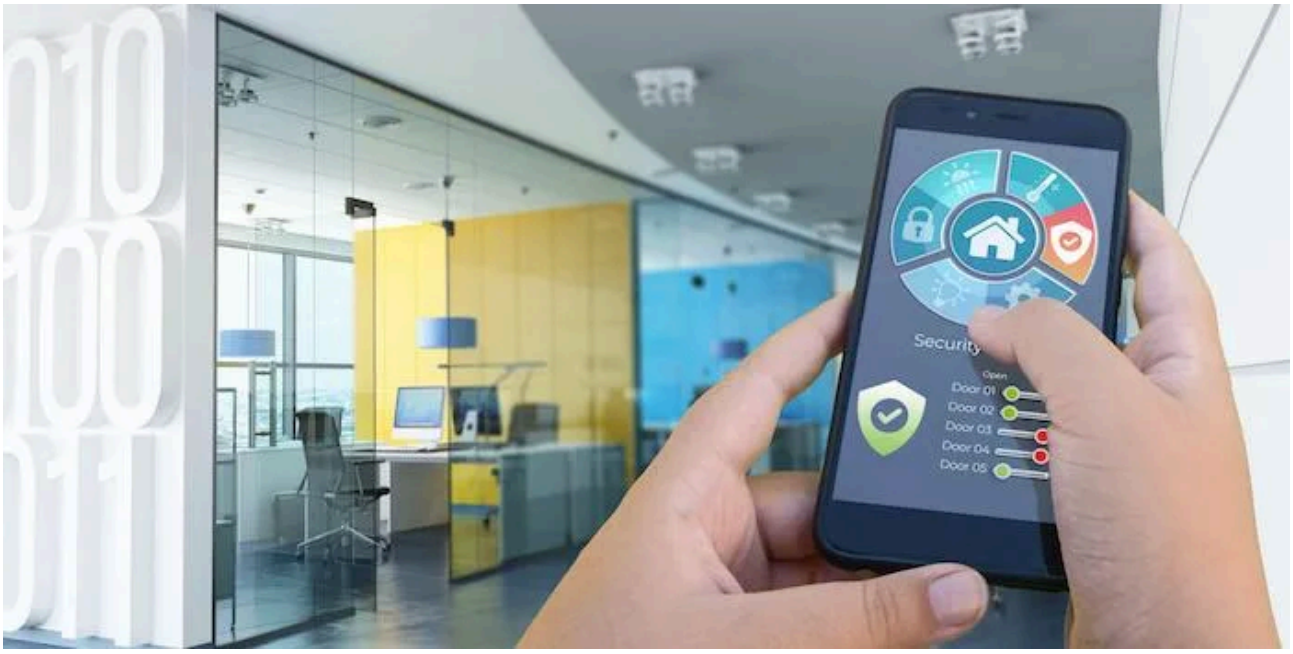
Lights Out: Cyberattacks Shut Down Building Automation Systems

By Kelly Jackson Higgins

Published: 2021-12-20 · Archived: 2026-04-06 01:33:44 UTC



Source: FranckBoston via Alamy Stock Photo

[This story was updated on 12/27/2021 with comments from the KNX Association. They had not yet responded to inquiries when the story first posted.]

A building automation engineering firm experienced a nightmare scenario: It suddenly lost contact with hundreds of its building automation system (BAS) devices — light switches, motion detectors, shutter controllers, and others — after a rare cyberattack locked the company out of the BAS it had constructed for an office building client.

The firm, located in Germany, discovered that three-quarters of the BAS devices in the office building system network had been mysteriously purged of their "smarts" and locked down with the system's own digital security key, which was now under the attackers' control. The firm had to revert to manually flipping on and off the central circuit breakers in order to power on the lights in the building.

The BAS devices, which control and operate lighting and other functions in the office building, were basically bricked by the attackers. "Everything was removed ... completely wiped, with no additional functionality" for the BAS operations in the building, explains Thomas Brandstetter, co-founder and general manager of Limes Security, whose industrial control system security firm was contacted in October by the engineering firm in the wake of the attack.

Brandstetter's team, led by security experts Peter Panholzer and Felix Eberstaller, ultimately retrieved the hijacked BCU (bus coupling unit) key from memory in one of the victim's bricked devices, but it took some creative hacking. The engineering firm then was able to reprogram the BAS devices and get the building's lighting, window shutters, motion detectors, and other systems back up and running.

But the attack was no anomaly. Limes Security has since been getting reports of similar types of attacks on BAS systems that run on KNX, a building automation system technology widely deployed in Europe. Just last week, Limes Security was contacted by another engineering firm in Europe that had suffered an eerily similar type of attack as the German firm — on a KNX BAS system that locked it out as well.

"What was interesting ... is the attackers here misused what was supposed to be a security feature, a programming password [the BCU key] that would lock out an adversary from manipulating the components," Panholzer says.

"Luckily for us and the [BAS] operators so far in each of the incidents we have been involved with, the attackers set the same password for all components" in the victims' respective BAS networks, Panholzer says. "In theory, there could be a different password for each and every component, and that would actually make recovery much, much harder."

For its part, KNX warns in its product support information that the BCU key security feature should be deployed carefully for the engineering tool software (ETS): "Use this option with care; if the password is lost, those devices shall be returned to the manufacturer. Forgotten BCU Key in the devices cannot be changed or reset externally because this would make the protection in ETS meaningless (of course, the manufacturers know how to do this)," the KNX Association vendor says on its support page.

But in reality, most manufacturers of these devices are unable to retrieve pilfered BCU keys, Panholzer notes. The German engineering firm initially went to its BAS device vendors for help, but the vendors informed the firm they were unable to access the keys.

There have been other indirect reports of similar attacks on KNX-based systems, he says. "There seems to kind of an attack wave. We're not fully aware how" widespread it is, however, he says.

"What is apparent is that it came out of nowhere: Suddenly, there were many attacks happening that we are aware of," says Panholzer, who plans to present the case - which the company calls KNXlock - at the S4x22 ICS security conference next month in Miami. Limes Security declined to identify the victim organizations that have been hit in the attacks for confidentiality reasons.

There are no clues so far to trace back to the attackers. BAS systems aren't configured with any logging functions, so the attackers don't leave behind any digital footprints per se. Their attacks left no ransom notes nor signs of ransomware, so it's unclear even what the endgame of the attacks was.

"My theory here is there may be a single or few sources of attackers, but we don't know for sure" because of the lack of logs, Panholzer says.

The Limes Security researchers, meanwhile, have set up a honeypot system to see if they can lure the attackers into going after their phony BAS as a way to gather intel on where the attacks are originating. So far, though, no one has taken the bait.

The smart building system is an oft-forgotten attack vector that straddles the physical security and cybersecurity worlds. Building hacks thus far have been rare, with a couple of notable ones making headlines to date: a 2016 ransomware attack on a hotel in Austria that hit room locks, and a distributed denial-of-service attack on heating systems in two apartment buildings in Finland in 2016.

Limes Security's Brandstetter has been studying BAS vulnerabilities for a few years now. In 2017, he presented research at Black Hat USA on hacking BAS systems. He demonstrated scenarios of how KNX and BACnet, another popular BAS technology standard that's used widely in the US, could be abused by attackers.

In 2018, Forescout's Elisa Costante and her team wrote test malware, including a worm, that they used to expose software vulnerabilities in some 11,000 BAS devices, including protocol gateways, and programmable logic controllers for HVAC systems and access control. They presented their research at S4x19 in 2019.

How the Smart Building Hack Happened

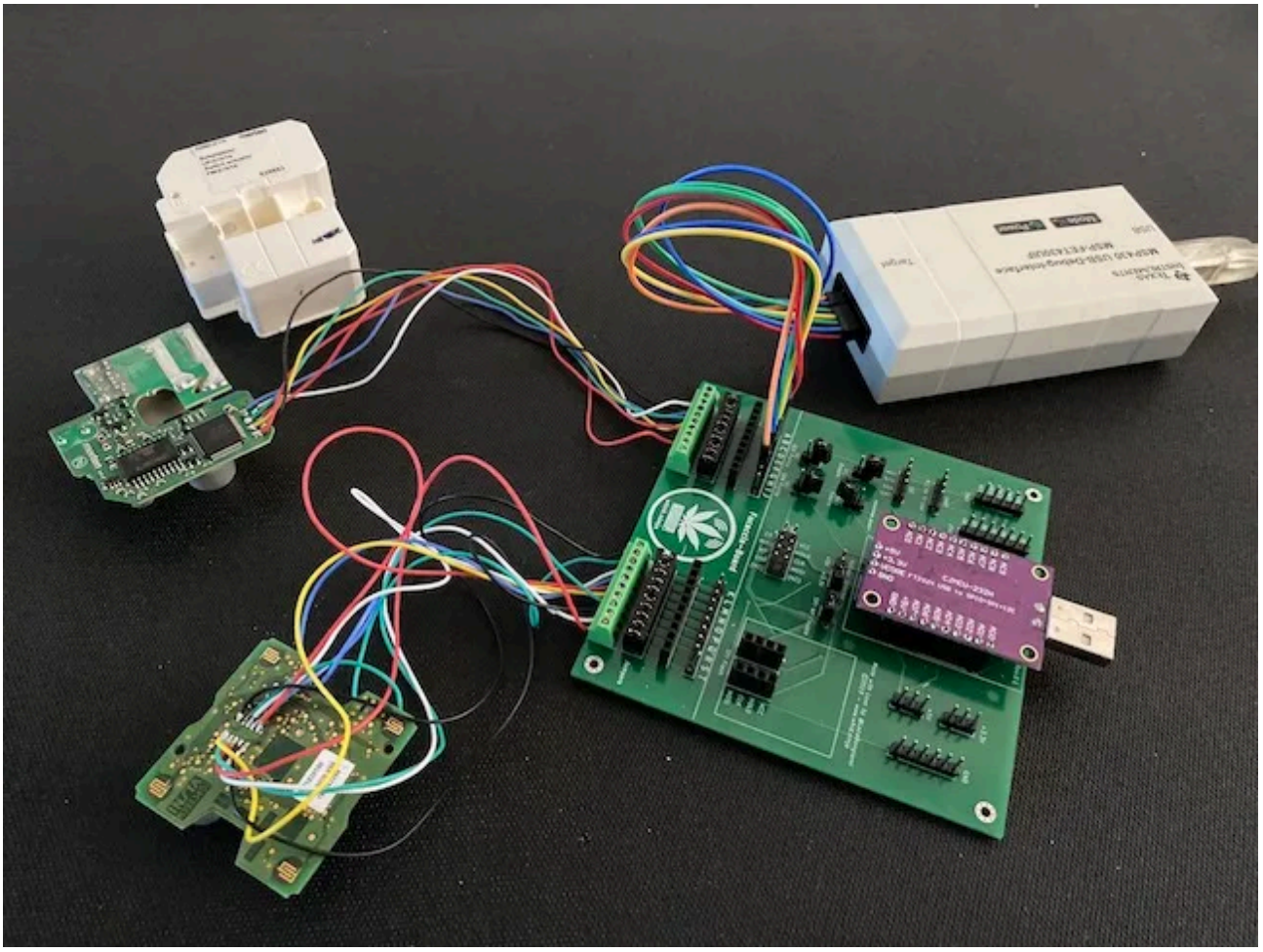
The German engineering firm's BAS system was initially infiltrated via an unsecured UDP port left exposed on the public Internet. From there, the attackers — who the Limes team believe were knowledgeable about KNX architecture — "unloaded" or basically wiped the BAS devices of their functionality, and then set them with the BCU key, which they locked with a password of their own.

The BCU key in KNX is for preventing unwanted changes to a device: To make a change, you need the password to the device. The Limes team asked the engineering firm to ship them a few of their BAS devices so they could figure out how to recover the keys. Brute-force hacking would take over a year to pull off, they concluded, because authentication response times are so slow with the devices.

"The BCU key is actually just a 4-byte string and eight characters," Panholzer explains. "One would think 4 bytes would be easy to brute-force, but the devices are very slow in answering" in response, he says.

They came up with a plan to try to read from the CPU memory on the devices that hadn't set protections for their CPUs. To narrow their search, they focused on areas in memory where they thought the key would likely be stored, and brute-forced those for the password. They basically programmed three different images of the device memory so they could locate where the address was stored.

"We could [then] limit the suspected area to a smaller pile of bytes, and fed this to the brute-force" tool, he explains.



KNXimage_copy.jpg

The tools used by Limes Security researchers to recover the hijacked BCU key from the hacked BAS devices.

Source: Limes Security

Forty-five minutes later, they unearthed the BCU key. It matched for all four devices — from different vendors — they had in hand, so they were confident it would work across all of the devices. The engineering firm typed the BCU key into their programming software and got the BAS system back up and running within 30 minutes, after several weeks of having to manually control lighting and other automated services in the building.

Security Gap

The underlying theme these recent attacks underscore: Many of the professionals who install and manage BAS systems like KNX's are not on IT or security teams. Rather, BAS systems are typically the domain of engineers and building management firms. IT and security teams rarely intersect with BAS operations, and that can be problematic.

Consider the European building management firm that contacted Limes Security last week. The victims believe the attackers got in via an IP gateway that had been temporarily installed in the construction phase of the building. The IP gateway "was supposed to be removed after handing over the building," Panholzer notes. "But it was forgotten and never deactivated."

Brussels-based BAS vendor KNX provides specific security recommendations for organizations that deploy its software and network standards. These include using a VPN for any Internet-based connections to the system, segmenting its KNX IP Backbone network from other IP networks via VLANs, and placing a firewall between the KNX IP network and other networks.

"We found good documentation and recommendations" by KNX on properly securing BAS systems, Panholzer says. "They try to include a lot of security awareness in their material."

KNX Association CTO and CFO Joost Demarest said in an email exchange that the organization for years has been providing its customers with security recommendations and warnings against leaving ports open. The organization has "repeatedly warned against such habits in KNX installations of port forwarding, amongst others via the KNX Security Checklist and the KNX Security Position Paper," he said. "Unfortunately, these habits seems to still exist in the field."

The company also recently launched a new security awareness campaign for its user community.

Finding exposed BAS systems is as simple as a Shodan scan, notes Stephen Cobb, an independent risk researcher. That's likely how the attackers are zeroing in on vulnerable building systems.

While BAS attacks to date remain relatively rare, they could be lucrative for cybercriminals, he notes. "This could be a future area of criminal exploitation that's very serious. It has all the ingredients to be like ransomware," says Cobb, formerly with ESET. "Unsecured pieces out there can be found and exploited."

Ransomware and extortion attacks on a BAS could be used to target facility management companies, or more ominously, hospitals, he says. Even so, there are easier methods of extortion today: "Unsecured RDP and phishing are yielding just enough targets" to remain the dominant attack vectors, he notes.
