Byos Defeats Critical Infrastructure Cyber Attack

June 18, 2025

BYOS

WHITE PAPER

Last week in **Columbia, Maryland** at the **Technology Advancement Center's Link complex**, Byos successfully demonstrated its Secure Cluster Edge™ and Secure Lobby™ SDN overlay network capabilities against a live cyber-attack at Defend The Airport 2025. This attack targeted the fuel system of the ADEGA Airport Simulated Environment; a cyber range consisting of multiple networks representative of the types of OT/ICS/PLC networks found at any airport around the globe. Defending the fuel system is of particular note, as currently there are thousands of known vulnerable airport fuel system devices exposed to the internet today; and many thousands more peripheral devices that are connected to these devices.[1]

This two-day event featured live demonstrations of a variety of cyber-attacks against airport infrastructure on the ADEGA test range. On day 1 of the event, a red team cyber operator explained to attendees how adversaries employ techniques, tactics, and procedures (TTPs) against airports. The red-teamer then proceeded to implant several zero-day compromises on the ADEGA cyber range infrastructure networks, and established persistence on the networks to show how attackers "live off the land".

On day 2, technologies from leading cyber defense companies were invited to install on the range, and defend against live cyber attacks on the infected networks. Each company had 30 minutes to set up, with no prior exposure to the networks, no opportunity to conduct the types of assessments and analyses typical of a routine installation, and no time to optimize their capabilities. Each company was given their network to protect, with the direction to plug-in, turn-on, and go!

When the attacker attempted to exploit the zero-day that had been implanted on the ADEGA fuel system (malware that would cause the system to dump all of its fuel and override emergency shutdown controls), not only had persistence to the fuel system been broken by Byos, but the attacker could not re-establish communication to the live payload. The attacker resorted to an attempt to pivot through the network (known as lateral movement), but was unable to identify any attack vector or means to deploy the zero-day exploit that had been implanted on the fuel system on day 1.

Upon conclusion of this demonstration, several vulnerability management, network monitoring, and attack surface analysis vendors that were deployed on the cyber range for the event were asked if they were able to capture packets from the Byos hardware-enforced protection defending the fuel system. Byos obfuscation technologies were unable to be detected by industry leading threat intelligence platforms. All of the platforms were however able to capture the packets of the defensive software capabilities of others that were demonstrated. This is critically important due to the large number of legacy OT/ICS/PLC devices deployed across airports and all critical infrastructure systems today, many of which are unable to be patched or remediated. Byos secures legacy / brownfield investments in ways that cannot be detected on a Byos-protected asset nor the network; a key differentiator from leading software-based security solutions.

[1] https://www.csoonline.com/article/3539999/thousands-of-internet-exposed-fuel-gauges-could-be-hacked-and-dangerously-exploited.html

Why is this important?

In a failed cyber attack where an adversary can retain persistence on an infected OT network, but cannot attack a previously compromised asset that is now protected by Byos, it might be possible for the attacker to pivot to the network monitoring or threat intelligence systems operating on that network to discover how or why they have lost the ability to attack their target. In such an instance, there will be no data exposing the Byos capabilities for an attacker to learn from or leverage to develop an exploit or technique that would compromise Byos.

Recent data shows that cyber attacks against airport infrastructure increased by 131% from 2022 to 2023 across the globe.[2] The scale and severity of these attacks threaten a $1.9 trillion dollar industry.

FIPS

140-2 Validated

Certificate #4964

Byos offers a range of commercial off the shelf products that are FIPS 140-2 validated and ready to protect critical infrastructure today. For more information or to schedule a demo, please contact:

David Stephens
VP of Sales Public Sector and Strategic Accounts
david@byos.io
571-437-1111

[2] https://www.secureworld.io/industry-news/aviation-cybersecurity-threats