Olympus US systems hit by cyberattack over the weekend

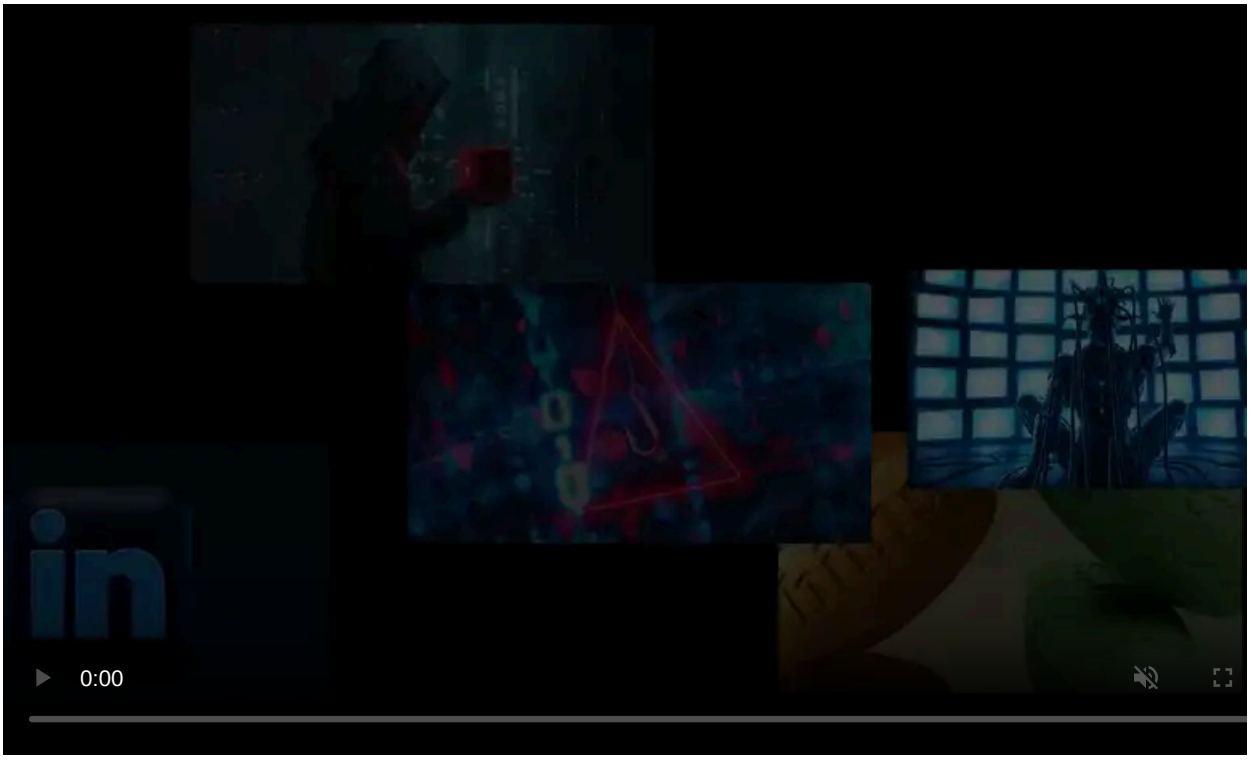
By Sergiu Gatlan

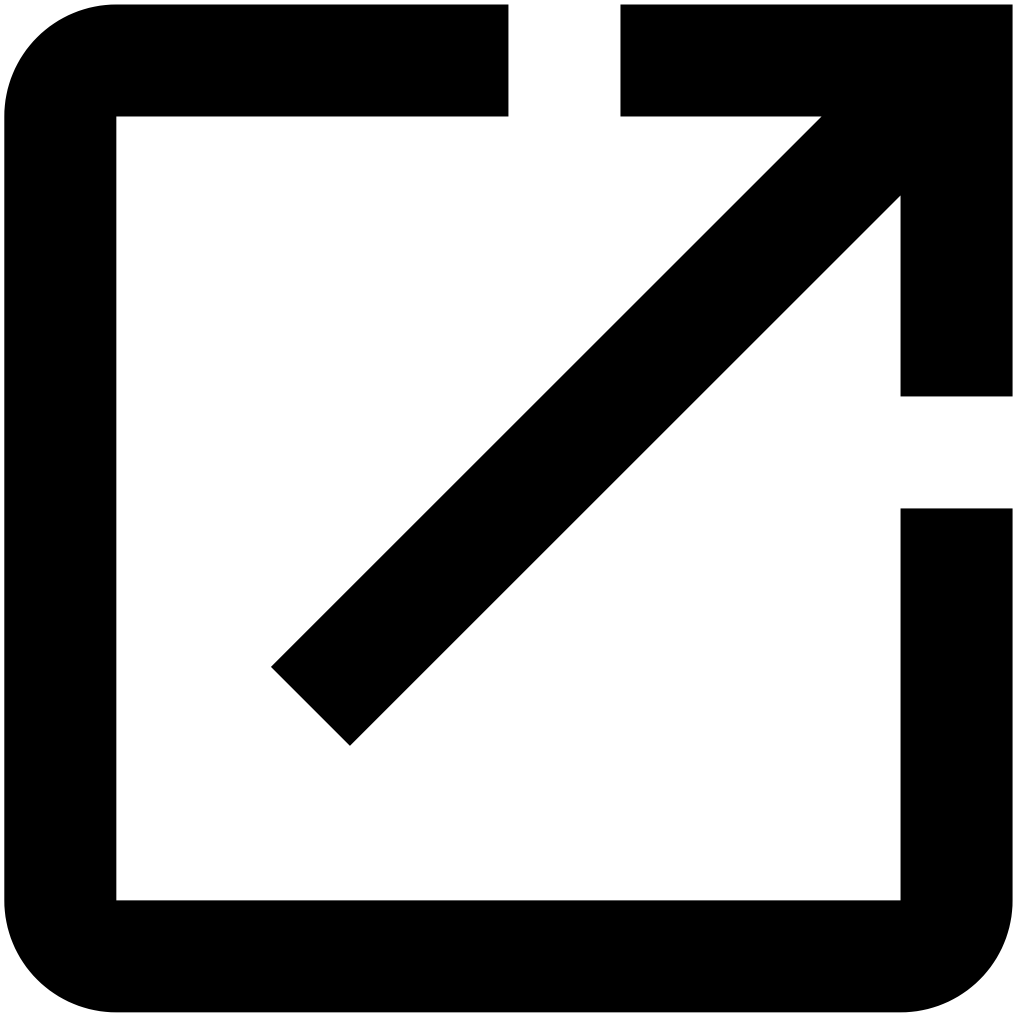
Published: 2021-10-12 · Archived: 2026-04-05 17:20:02 UTC

Olympus, a leading medical technology company, was forced to take down IT systems in the Americas (U.S., Canada, and Latin America) following a cyberattack that hit its network Sunday, October 10, 2021.

"Upon detection of suspicious activity, we immediately mobilized a specialized response team including forensics experts, and we are currently working with the highest priority to resolve this issue," Olympus says in a statement published today, two days after the attack.

"As part of the investigation and containment, we have suspended affected systems and have informed the relevant external partners. The current results of our investigation indicate the incident was contained to the Americas with no known impact to other regions."


0:00



The company did not disclose if customer or company data was accessed or stolen during the "potential cybersecurity incident," but said that it would provide new information regarding the attack as soon as it's available.

"We are working with appropriate third parties on this situation and will continue to take all necessary measures to serve our customers and business partners in a secure way," Olympus added. "Protecting our customers and partners and maintaining their trust in us is our highest priority."

An Olympus spokesperson told BleepingComputer that the company found no evidence of data loss during an ongoing investigation regarding this incident.

September BlackMatter ransomware attack

This incident follows a ransomware attack that hit Olympus' EMEA (Europe, Middle East, Africa) IT systems in early September.

Even though Olympus did not share any info on the attackers' identity, ransom notes found on impacted systems impacted revealed that BlackMatter ransomware operators coordinated the attack.

The same ransom notes also pointed to a Tor website the BlackMatter group used in the past to communicate with their victims.

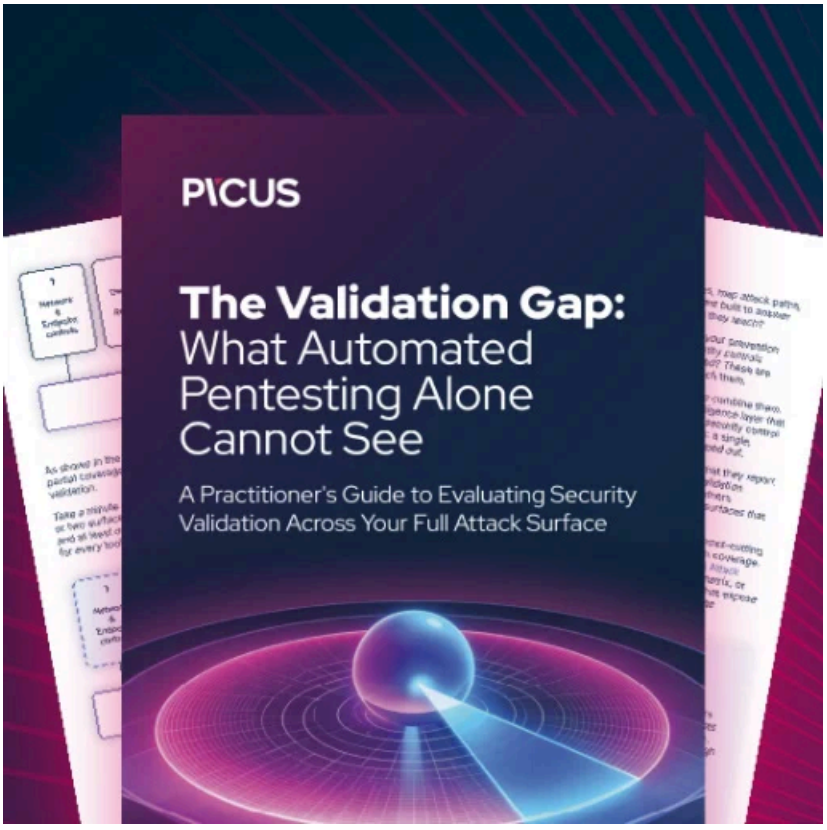
Although Olympus, once again, did not reveal much details on the nature of the attack that hit its Americas IT systems, ransomware gangs are known for carrying out their attacks during weekends and holidays to delay detection.

The FBI and CISA said in a joint advisory published in August that they "observed an increase in highly impactful ransomware attacks occurring on holidays and weekends—when offices are normally closed—in the United States, as recently as the Fourth of July holiday in 2021."

Olympus has over 31,000 employees worldwide and more than 100 years of history developing medical, life sciences, and industrial equipment.

The company's camera, audio recorder, and binocular divisions were transferred to OM Digital Solutions, which has been selling and distributing these products since January 2021.

Update: Added Olympus spokesperson statement.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/olympus-us-systems-hit-by-cyberattack-over-the-weekend/