BlackMatter ransomware hits medical technology giant Olympus

By **Sergiu Gatlan (https://www.bleepingcomputer.com/author/sergiu-gatlan/)** September 13, 2021 07:49 AM **0**

Image: Olympus

Olympus, a leading medical technology company, is investigating a "potential cybersecurity incident" that impacted some of its EMEA (Europe, Middle East, Africa) IT systems last week.

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

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

Customer security not affected by the attack

"Olympus is currently investigating a potential cybersecurity incident affecting limited areas of its EMEA (Europe, Middle East, Africa) IT systems on September 8, 2021," the company said in a statement (https://www.olympus-global.com/news/2021/an02201.html) published Saturday, three days after the attack.

"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.

"As part of the investigation, we have suspended data transfers in the affected systems and have informed the relevant external partners."

Olympus also said that it's working on discovering the extent of the damage resulting from this attack and will share additional info as soon as it is available.

Christian Pott, company spokesperson responsible for Olympus corporate matters, also told BleepingComputer that customer security and service were not affected by the incident.

"The support, service and security of our customer has the highest priority and is not effected by this case," an Olympus spokesperson told BleepingComputer when contacted via email.

"Please understand, that we cannot give any further information or statement due to the ongoing process of internal and external investigation."

Signs of a BlackMatter ransomware attack

While Olympus did not share any details on the attackers' identity, ransom notes left on systems impacted during the breach point to a BlackMatter ransomware attack, as first reported by TechCrunch (https://techcrunch.com/2021/09/12/technology-giant-olympus-hit-by-blackmatter-ransomware/).

The same ransom notes also point to a Tor website the BlackMatter gang has used in the past to communicate with victims.

BlackMatter is a relatively new ransomware operation that surfaced at the end of July 2021 and was initially believed to be a rebrand of DarkSide ransomware (https://www.bleepingcomputer.com/news/security/darkside-ransomware-gang-returns-as-new-blackmatter-operation/).

From samples collected by researchers after some of their subsequent attacks, it was later confirmed that BlackMatter ransomware's encryption routines were the same custom and unique ones that DarkSide used.

The DarkSide operation shut down after attacking and shutting down Colonial Pipeline (https://www.bleepingcomputer.com/news/security/largest-us-pipeline-shuts-down-operations-after-ransomware-attack/) due to pressure from both international law enforcement (https://www.bleepingcomputer.com/news/security/interpol-urges-police-to-unite-against-potential-ransomware-pandemic/) and the US government (https://www.bleepingcomputer.com/news/security/us-warns-of-action-against-ransomware-gangs-if-russia-refuses/).