GOVINFOSECURITY®

https://www.govinfosecurity.com/

Business Continuity Management / Disaster Recovery , Fraud Management & Cybercrime , Governance

Facilities Maintenance Firm Recovering From Malware Attack

ISS World Says 'Root Cause' Has Been Identified

Jeremy Kirk (jeremy_kirk) • February 21, 2020

ISS World's headquarters in Denmark (Photo: ISS World)

ISS World, a global facilities maintenance company based in Denmark, says it's gradually restoring its systems after a malware attack on Monday.

See Also: How to Defend Your Attack Surface

The company, which provides facilities management, catering, security and other property-related services, has more than 500,000 employees worldwide.

ISS World says the "root cause" of the attack has been identified. But the company didn't say if the attack was caused by ransomware, the file-encrypting malware that is frequently the cause of public announcements of system shutdowns.

U.K.-based security researcher Kevin Beaumont tweeted on Thursday, however, that ISS World has "informed business partners it is ransomware."

The company says it's working with forensic experts, its hosting provider and an external task force to restore its systems.

"Certain systems have already been restored," the company says in a statement. "There is no indication that any customer data has been compromised."

Restoring Systems

A U.K.-based publication, This Week in Facilities Management, reports that 43,000 of ISS World's employees had no access to operational systems, including 4,000

employees in the U.K.

But ISS World says most of its work is performed on customer's sites, and it is relying on its business continuity plans to continue operating.

"The nature of our business is to deliver services on customer sites mainly through our people, and as such, we continue our service delivery to customers while implementing our business continuity plans," ISS World says. "Our priority is to ensure limited or no disruption while we fully restore all systems. We are currently estimating when IT systems will be fully restored and are assessing any potential financial impact. Security, in all its forms, is a top priority for ISS, and we remain committed to protecting the integrity of our systems."

What Happened?

ISS World's description of the attack would fit the profile of a ransomware strike. But it's common for organizations to at least initially not specify that the malware used in an attack is ransomware.

Beaumont tweets that it's possible ISS World was affected by the REvil ransomware, also known as Sodinokibi (see: *Ryuk and Sodinokibi Surge as Ransom Payments Double*). That's based on data collected by Troy Mursch of the Chicago-based threat intelligence firm Bad Packets. In December 2019, Citrix revealed a directory transversal flaw, CVE-2019-19781 (see: *Severe Citrix Flaw: Proof-of-Concept Exploit Code Released*).

Mursch tells Information Security Media Group that the flaw could be used to get a foothold into a network behind a VPN.

Bad Packets used data from the search engine BinaryEdge on Jan. 11 to scan potentially vulnerable Citrix endpoints. Bad Packets found more than 25,000 unique IPv4 hosts that were vulnerable. Included in that batch was a Citrix endpoint belonging to ISS World, Mursch tweets.

> Their Citrix server, https://t.co/xDR6wqp0wj, was vulnerable to CVE-2019-19781 on January 11th.
>
> This critical vulnerability allows unauthenticated remote attackers to execute arbitrary commands on the targeted server (https://t.co/Ba1muwe7ny). https://t.co/Z2nnKfdB69
>
> — Bad Packets Report (@bad_packets) February 19, 2020

Mursch says the scans on Jan. 31 showed that ISS World had patched a vulnerable server. Mursch says it's not possible to say whether that vulnerability led to a ransomware infection, but a forensic examination could give an answer.

Ransomware attackers have been using the Citrix vulnerability. FireEye writes in a blog post that it noticed attackers were using the Citrix flaw to install coin miners, a malware program called NOTROBIN as well as ransomware.

About the Author

Jeremy Kirk
Managing Editor, Security and Technology, ISMG

Kirk is a veteran journalist who has reported from more than a dozen countries. Based in Sydney, he is Managing Editor for Security and Technology for Information Security Media Group. Prior to ISMG, he worked from London and Sydney covering computer security and privacy for International Data Group. Further back, he covered military affairs from Seoul, South Korea, and general assignment news for his hometown paper in Illinois.