MALWARE FOUND IN INTERNATIONAL AIRPORT IN UKRAINE

News / Airports / Routes

Malware has been discovered in a computer network of Kiev's main airport, Reuters reports.

The report states the malware was found last week in the IT network of Boryspil International Airport, located near Kyiv, which reportedly included the airport's air traffic control system. Andriy Lysenko, a military spokesperson, told Reuters that the command and control centre of the malware—the external server that the software communicates with—is in Russia, and that no damage had been done.

But experts are not going to jump to conclusions about who is behind the malware.

“The report says the command and control server is in Russia: it's normal to be able to compromise locations around the world and use, so just because the IP address says Russia means very little for attribution,” Robert M. Lee, a former US Air Force cyber warfare operations officer and CEO of Dragos Security, told Motherboard in a Twitter message.

“There's a lot of missing information here and I'd caution folks from believing anything on it until there is far more proof,” he continued.

Since December, the security community has been fascinated by a coordinated cyberattack in Ukraine that left areas of the country without power. In part because of the presence of a variant of BlackEnergy—a piece of malware that has been used for cybercriminal campaigns, as well as attacks on engineering systems—one research group attributed the attacks to Russia, and

specifically the so-called “Sandworm” hacking group.

On Monday, Ukraine's Computer Emergency Response Team (CERT-UA) published a warning directed to system administrators about “potential attacks [using] BlackEnergy.” That briefing provided a list of suspicious IP addresses for admins to check their system logs against.

“We recommend checking the log files and information flows for the presence/absence of these indicators,” the briefing read, before linking to a presentation on BlackEnergy from researchers at ESET.

According to the Reuters report, an airport spokesperson said Ukrainian authorities were investigating whether the malware found in the Boryspil airport was also BlackEnergy. The worry here would be that BlackEnergy could have given hackers access to systems in the same way it did in the power grid attacks. (It’s worth remembering that in those previous cases, the malware itself did not cause the power to go out; rather, it gave the hackers remote access for them to then tamper with target systems.)

Several calls by Motherboard to a press number for Boryspil International, provided by the airport's information desk, went unanswered.

19 JANUARY 2016

SOURCE: MOTHERBOARD
ARTICLE LINK:
https://to.50skyshades.com/news/airports-routes/malware-found-in-international-airport-in-ukraine