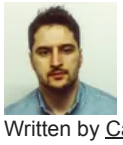
DOD contractor suffers ransomware infection

zdnet.com/article/dod-contractor-suffers-ransomware-infection/

Home Innovation Security
Virginia-based EWA has had systems infected with the Ryuk ransomware.



Written by Catalin Cimpanu, Contributor on Jan. 29, 2020

-
-
-
-
-

Electronic Warfare Associates (EWA), a 40-year-old electronics company and a well-known US government contractor, has suffered a ransomware infection, ZDNet has learned.

The infection hit the company last week. Among the systems that had data encrypted during the incident were the company's web servers.

Signs of the incident are still visible online. Encrypted files and ransom notes are still cached in Google search results, even a week after the company took down the impacted web servers.

Image: ZDNet

Security researchers who reviewed the cached files told ZDNet the encrypted files and ransom note are, without a doubt, a sign of an infection with the Ryuk ransomware.

The security researcher who first discovered these files told ZDNet that several EWA websites appear to have been impacted, such as the sites for:

- EWA Government Systems Inc. -- an EWA subsidiary that provides electronic warfare (EW) products and services to government and commercial markets in cyber defense, radar development, intelligence, security, training, tactical mission planning, information management, and force protection.
- EWA Technologies Inc. -- an EWA subsidiary specialized in JTAG products.
- Simplicikey -- an EWA subsidiary specialized in the manufacturing a consumer-focused Remote Control Electronic Deadbolt.
- Homeland Protection Institute -- a non-profit chaired by the EWA CEO.

It is unclear at the moment how much of the company's internal network was encrypted during the incident.

Despite visible signs of a ransomware incident on its public websites, EWA has not issued any public statement about the incident.

An EWA spokesperson hung up the phone earlier today when ZDNet reached out for comment about the security breach.

The company is a well-known supplier of electronics equipment to the US government. On its website, EWA lists the Department of Defense (DOD), the Department of Homeland Security (DHS), and the Department of Justice (DOJ) as regular customers.

A conspicuous Ryuk Stealer update

Making matters worse is that Ryuk is not your regular ransomware strain. This type of ransomware is solely used in targeted attacks on high-profile companies.

It is usually installed on infected networks after a victim is infected with the Emotet/TrickBot trojans, two well-known cybercrime-as-a-service platforms.

The Ryuk gang uses the Emotet/TrickBot-infected machine as entry point and launch pad to scan and spread inside a company's internal network, exfiltrate data, and then deploy their ransomware.

The data exfiltration happens via a Ryuk module called the Ryuk Stealer, which security researchers have been spotting deployed in recent Ryuk attacks.

Coincidentally, the Ryuk Stealer was recently update to target files that may hold government and military-related data, according to a Bleeping Computer report, suggesting a concerted effort on the Ryuk gang's side in targeting government and military entities.

The FBI's most wanted cybercriminals