Foresight
Innovative Solutions

Ransomware attacks are now targeting industrial control systems

Ransomware attacks are now targeting industrial control systems

Cyber criminals are launching ransomware attacks that are specifically targeting industrial control systems (ICS) in what researchers say is the first instance of file-encrypting malware being built to directly infect computer networks that control operations in manufacturing and utilities environments.

A new threat report from cybersecurity company Dragos details the characteristics of the ransomware known as Ekans. This ransomware – also known as Snake – first emerged in December 2019 and has been designed for use against Windows systems used in industrial environments.

It's not the first instance of ICS-targeting malware; a number of state-sponsored hacking campaigns have targeted these facilities in recent years, but researchers have concluded that Ekans looks to be the work of a cyber criminal operation getting involved in this space and that it represents "a unique and specific risk to industrial operations not previously observed in ransomware malware operations".

Researchers found Ekans contains a list of commands and processes associated with a number of industrial control system-specific functionalities aimed at stopping these functions in a ransomware attack.

While this functionality is described as limited, researchers' analysis of Ekans notes that it still represents "a deeply concerning evolution in ICS-targeting malware" because it indicates that cyber criminals are now targeting ICS operation systems purely for financial gain.

Files encrypted are renamed with a random five character file extension, while victims are presented with a ransom note with an email address to contact to negotiate a ransom to be paid in cryptocurrency.

In order to deploy the ransomware, the attackers behind Ekans likely need to compromise the network before executing the attack. This follows the same trend as ransomware variants like Ryuk and Megacortex, which rely on a hands-on method of deployment rather than the self-propagation followed by other forms of ransomware.

The way in which Ekans is designed to target ICS operations indicates that the attackers very much have a specific target in mind, so are likely to take their time to compromise targets relevant to their plans.

The Dragos paper even notes that Ekans could share a relationship with Megacortex ransomware, as while the list of processes targeted by Ekans is relatively short at only 64, each and every one of these is targeted by newer versions of Megacortex. It points towards the possibility that Megacortex could also be deployed by this kind of attack.

"The ICS-specific nature of the targeted processes indicates an evolving brazenness," Joe Slowik, principal adversary hunter at Dragos, told ZDNet.

"While not deliberately destructive, lack of context and victim environment issues could mean Ekans or similar malware terminating industrial-related processes could cause an inadvertent physical effect. The willingness to accept this possibility is deeply concerning."

Some reports have linked Ekans to Iran, but following analysis of the malware, Dragos has concluded that there's "no strong or compelling evidence" that links this campaign with Iranian strategic interests.

It's currently not entirely certain how Ekans is distributed to victims, but in order to protect against ransomware attacks, it's recommended that ICS systems are segmented from the rest of the network, so even if a standard Windows machine is compromised, an attacker can't just move onto systems that control infrastructure.

Organisations should also ensure that systems are regularly backed up and stored offline; and for ICS operations in particular, backups must include the last known good-configuration data to ensure a swift recovery.

"Industrial and related organisations should adjust their threat profiles to include likely deliberate attempts to extort money from organisations through direct targeting of industrial environments," said Slowik.

"Organisations must work diligently to both reduce their attack surface through better network segmentation, improved access and authentication mechanisms, while increasing visibility into industrial networks to identify attacks before they reach their conclusion," he said.