Trellix

What Is Stuxnet?

Stuxnet is a computer worm that was originally aimed at Iran's nuclear facilities and has since mutated and spread to other industrial and energy-producing facilities. The original Stuxnet malware attack targeted the programmable logic controllers (PLCs) used to automate machine processes. It generated a flurry of media attention after it was discovered in 2010 because it was the first known virus to be capable of crippling hardware and because it appeared to have been created by the U.S. National Security Agency, the CIA, and Israeli intelligence.

What did the Stuxnet worm do?

Stuxnet reportedly destroyed numerous centrifuges in Iran's Natanz uranium enrichment facility by causing them to burn themselves out. Over time, other groups modified the virus to target facilities including water treatment plants, power plants, and gas lines.

Stuxnet was a multi-part worm that traveled on USB sticks and spread through Microsoft Windows computers. The virus searched each infected PC for signs of Siemens Step 7 software, which industrial

signs of Siemens Step 7 software, which industrial computers serving as PLCs use for automating and monitoring electro-mechanical equipment. After finding a PLC computer, the malware attack updated its code over the internet and began sending damage-inducing instructions to the electro-mechanical equipment the PC controlled. At the same time, the virus sent false feedback to the main controller. Anyone monitoring the equipment would have had no indication of a problem until the equipment began to self-destruct.

The Legacy of Stuxnet

Although the makers of Stuxnet reportedly programed it to expire in June 2012, and Siemens issued fixes for its PLC software, the legacy of Stuxnet lives on in other malware attacks based on the original code. These "sons of Stuxnet" include:

- **Duqu (2011)**. Based on Stuxnet code, Duqu was designed to log keystrokes and mine data from industrial facilities, presumably to launch a later attack.
- **Flame (2012)**. Flame, like Stuxnet, traveled via USB stick. Flame was sophisticated spyware that recorded Skype conversations, logged keystrokes, and gathered screenshots, among other activities. It targeted government and educational organizations and some private individuals mostly in Iran and other Middle Eastern countries.
- **Havex (2013)**. The intention of Havex was to gather information from energy, aviation, defense, and pharmaceutical companies, among others. Havex malware targeted mainly U.S., European, and Canadian organizations.
- **Industroyer (2016)**. This targeted power facilities. It's credited with causing a power outage in the

Ukraine in December 2016.

- **Triton (2017)**. This targeted the safety systems of a petrochemical plant in the Middle East, raising concerns about the malware maker's intent to cause physical injury to workers.
- **Most recent (2018)**. An unnamed virus with characteristics of Stuxnet reportedly struck unspecified network infrastructure in Iran in October 2018.

While ordinary computer users have little reason to worry about these Stuxnet-based malware attacks, they are clearly a major threat to a range of critical industries, including power production, electrical grids, and defense. While extortion is a common goal of virus makers, the Stuxnet family of viruses appears to be more interested in attacking infrastructure.

Trellix Threat Labs Research Report: April 2022

Read Report

How to protect industrial networks against malware attacks

Good IT security practices are always useful in preventing malware attacks. These practices include regular patches and updates, strong passwords, password management, and identification and authentication software. Two important practices that might have helped protect against Stuxnet are virus

might have helped protect against Stuxnet are virus scanning (or banning) of all USB sticks and other portable media, and endpoint security software to intercept malware before it can travel over the network. Other practices for protecting industrial networks against attacks include the following:

- Separate the industrial networks from general business networks with firewalls and a demilitarized zone (DMZ)
- Closely monitor machines that automate industrial processes
- Use application whitelisting
- Monitor and log all activities on the network
- Implement strong physical security for access to industrial networks, including card readers and surveillance cameras

Finally, organizations should develop an incident response plan to react quickly to problems and restore systems quickly. Train employees using simulated events and create a culture of security awareness.

More Ransomware Articles

What Is Petya and NotPetya Ransomware?

What is Malware?

What is Ransomware?

Malware vs. Viruses

What is Fileless Malware?