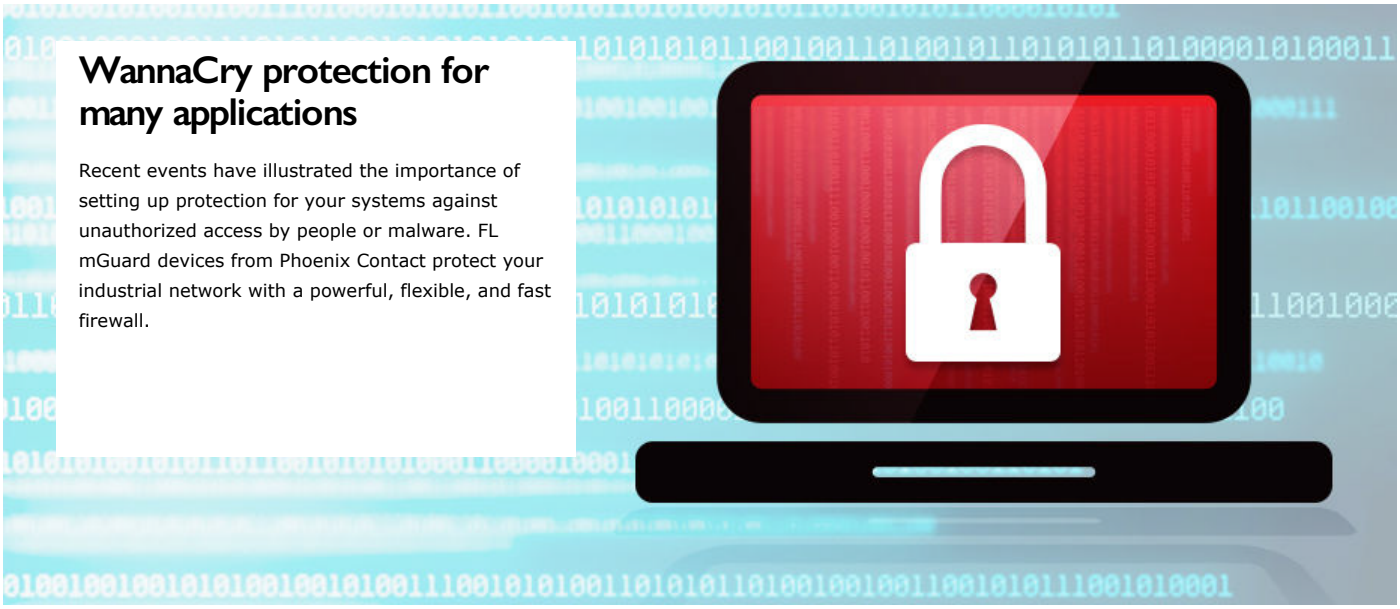

WannaCry protection for many applications

Recent events have illustrated the importance of setting up protection for your systems against unauthorized access by people or malware. FL mGuard devices from Phoenix Contact protect your industrial network with a powerful, flexible, and fast firewall.

With the increase of file hijacking attacks taking place around the world, we decided to provide some answers to basic cybersecurity questions and review malware attacks so that you can better understand what this rising Ransomeware trend is all about.

What is Ransomware?

Ransomware, or abduction of information, is the generic term for malicious software requiring the user of the computer to pay a ransom in order to recover encrypted files or regain access to the entire system. Once it penetrates the computer, this malware is activated and causes the entire operating system to crash.

How does Ransomware work?

There are two types of Ransomware. They work differently, with and without encryption:

- **A system takeover without encrypting the data**
  Typically, this malware will disable Task Manager, shield access to the registry, and infect the EXPLORER.EXE file, causing all desktop icons disappear. This prevents you from using any of your programs.
- **A hard disk data encryption**
  This type encrypts your hard disk data with codes that are almost impossible to decipher without knowing the key. If encryption affects only system files, an antivirus can regain control by reinstalling them. If the entire operating system is encrypted — or worse, your user data — the only solution is to format the hard drive, with the inevitable loss of data.

Screenshot of the WannaCry ransomware

Potential targets?

Any computer, smartphone, or tablet that runs an operating systems (OS) is a potential target for Ransomware. This means that the application that these devices are connecting, hosting, or interoperating with could be negatively impacted, depending on the specific market and criticality.

In the healthcare industry, for example, we have found that hospitals and other medical facilities (like clinics, outpatient treatment centers, etc.) often have old and unsupported Windows PCs used as part of legacy medical equipment, like X-Ray machines, MRIs, etc.

Industrial control systems are another market where legacy and unpatched OS are running critical processes. Here, electric plants and water/wastewater facilities that deliver power and clean water to our homes are categorized.

The three best practices for OS protection

- **Patch:** The most direct and serious option is to patch the OS with the latest security updates on a regular basis.

- **Network segmentation:** Using routers with integrated firewalls can limit and restrict traffic coming from trusted and untrusted devices. Additionally, this provides isolation to protect against the malware to keep spreading laterally.
- **OS protection:** Traditional anti-virus (AV) operates in a "signature-based" system— the AV engine compares files and activities to a database of known virus signatures, and upon finding a match, deletes or quarantines the offending file. This model has two flaws: first, each OS must update its AV database frequently to detect and protect against new viruses and worms; second, new malware and viruses that attack "zero-day" vulnerabilities go undetected as they don't have a "signature" in the database yet. Alternative integrity assurance techniques for the protection of industrial systems have gained relevance due to general problems with the deployment of AV software on systems and the timely provision of malware signatures.

How can the FL mGuard help?

The mGuard family of rugged security devices includes firewall, routing, and optional VPN functionality to critical networks. These high-level "Layer 3" functions are essential for protecting your industrial network from malicious attacks and accidental interruption, as well as for connecting to office or enterprise networks.

The mGuard family

Different hardware variants provide a great range of uses and flexibility while at the same time providing full mGuard protection and connectivity to fit your needs. The hardware varies, ranging from road technicians, to desktop/laptop use in an office environment, to tough, industrially rated variants with fiber optic and copper interfaces, gigabit connectivity, PCI format, and hazardous location approvals.

Our Secure Cloud service also supports a number of other Phoenix Contact cellular modems with IPsec VPN.

Additionally, the CIFS Integrity Monitoring feature gives you an alternative to traditional anti-virus. CIFS Integrity Monitoring works by first taking a baseline snapshot of your Windows operating systems (OS) files through the remote mGuard, using built-in default network shares.

Next, the mGuard periodically scans the OS on a pre-set schedule. If any of the Windows OS files have been modified or deleted, or if any new file has been added to the monitored directory, mGuard generates an alert in the form of an e-mail, SNMP trap, or log warning. At this point, engineering, maintenance, or IT staff can take corrective actions.