

# USE CASE: POWER & UTILITIES

## CREDENTIAL SECURITY SOLUTIONS

- Gas and Oil Vendors
- Electric Utility
- Energy Management



## CASE SUMMARY

### CHALLENGE:

Keylogging spyware has become a main component in cyberattacks and are commonly downloaded as a result of clicking on an infected link inside an email, text message, social media page or web page. Keyloggers are used to steal network access credentials and other sensitive data.

### SOLUTION:

ACS EndpointLock Keystroke Encryption software eliminates the ability of keylogging spyware to capture keystrokes and steal access credentials and Personal Identifiable Information (PII). Hackers will always find ways to trick users into downloading a keylogger, but with EndpointLock installed, the spyware is rendered useless. By eliminating this threat, Power & Utility vendors are better able to protect their business assets as well as access into their client's networks.

### OVERVIEW:

Cybercriminals are targeting Power and Energy Utility Networks via their trusted vendors. The FBI and Dept. of Homeland Security issued a joint alert warning of spear phishing emails that lure targeted personnel with malware-loaded Word docs disguised as legitimate resumes, invitations and policy documents. In addition, security researchers warn of an Advanced Persistent Threat (APT) currently targeting utility companies called GreyEnergy, which has screen capture and keylogging capabilities and is being used for espionage and reconnaissance as a possible prelude to a more destructive attack on industrial control systems.

The practice of tricking unsuspecting victims into clicking on links that look legitimate is called "phishing". According to recent reports, phishing was found in 90% of breaches and 95% of all phishing attempts that led to a breach, were followed by software installation, including keyloggers. Once a keylogger has infected a desktop, tablet or mobile device, it steals every keystroke typed including network access credentials. Keyloggers are difficult to detect by traditional antivirus and firewalls, even if these programs are kept up-to-date.

### ENDPOINTLOCK BENEFITS:

- **Blocks keylogging spyware, the most common malware component used in a breach.**
- **Blocks screen scraping and clickjacking.**
- **Monitors the kernel and alerts of a compromise.**
- **Protects the vulnerable gap found at the point of data entry.**
- **Runs in the background, no employee training needed.**



