A NERC Alert issued June 13, 2017 advises on the Crash Override malware found to be behind the December 2016 attack on the Ukrainian power grid. While the NERC Alert provides many great details on the malware's technical characteristics, the fact of the matter is Crash Override is among the most sophisticated ICS-specific malware variants ever detected, with the ability to "cause loss of visibility, loss of control, manipulation of control, interruption of communications, and deletion of local and networked critical configuration files." Perhaps most concerning is the malware's ability to be easily tailored to specific ICS environments, communication protocols, and devices.

This type of sophisticated malware forces us to rethink some common predisposed cybersecurity beliefs:

1. A clean malware scan does not mean a system is free from malware
    a. Crash Override is modular in nature, rendering signature-based malware detection techniques relatively ineffective.
2. Air-gapping is not a cybersecurity silver-bullet
    a. Crash Override can operate autonomously as a "time bomb," not requiring external communications or command/control.
3. Zero-day exploits are not the biggest concern
    a. Crash Override, while sophisticated, leveraged only known vulnerabilities, some of which date back to 2015, with patches readily available.

As a result, the NERC Alert recommends the following actions:

1. Monitor network traffic (both traversing EAPs and within ESPs) and understand the communications protocols used in your environment
    a. By understanding "normal" network traffic, traffic patterns can be monitored for any deviation from this baseline.
2. Utilize heuristic-based or behavior-based malware detection
    a. Instead of looking for signatures, this type of next-generation malware detection technique looks for abnormal behavior or activities within a system.
3. Proper patch management
    a. As none of the vulnerabilities leveraged were zero-day, keeping systems up-to-date prevents many of Crash Override's capabilities.
4. Back-up and recovery
    a. In order to mitigate against Crash Override's data wiping capabilities, maintain current back-up images and recovery plans.