Enterprise Protection Against Cyberattacks Primer: The Ukrainian Power Facility Attack

A TrendLabs℠ Primer

The Internet has made the world more connected–with almost everything more accessible than before. But with this interconnectivity comes a price: the risk of cyberattacks having more far-reaching consequences than information loss.

The recent attack against power facilities in Ukraine is an example of a threat with real-world impact. Executed through a spearphishing campaign with components that had malware BlackEnergy and KillDisk as its payloads, it infected key systems in said power utilities to shut them down. By doing so they destabilized a country's critical infrastructure.

What makes the attack more dangerous is the fact that it is a type of threat that can affect any organization – whether it is a critical infrastructure, government, or a private company. In this primer, we will talk about the different components of the threat, how it can affect enterprises, and what defenses can be set up to protect an organization against such a threat.

An Age of Destructive Cyberattacks

We are at a point in time where stealing information is no longer the sole agenda of cyberattacks. We are increasingly seeing attacks that involve the disruption of system usage and destruction of data. We see this happen in different magnitudes -- from widespread threats such as **ransomware**, to those that **affect specific organizations** – with both variants creating a big impact to its targets.

The attack against power facilities in Ukraine is another instance where we see the great impact of disruptive attacks. The attack involved components that allowed attackers to move through the network to reach critical systems, and modify and destroy important data. This left many households and businesses in the Ivano-Franvisk region in Ukraine were deprived of power and the facilities' staff unable to access their systems to undo the damage.

Such an impactful attack leaves the question: how were the attackers able to execute this? How were they able to penetrate even critical infrastructures that supposedly have very restricted access? And with even critical networks being successfully targeted, what chance do enterprises have in protecting themselves in such attacks?

Dissecting the Ukrainian Power Facility Attack

Extensive **investigations** done on the Ukrainian power facility attack was able to trace the initial infection vector to spear-phishing. The attackers sent spear-phishing emails seeded with Microsoft Office attachments containing malicious macro code designed to download BlackEnergy malware.

While it was not identified who specifically were targeted in the initial spear-phishing attack, the fact that attackers were able to penetrate the network this way shows that they were able to target key personnel – those who reside within the internal networks, and possibly connected to the SCADA systems used to manage the power grid. This part of the attack is notably similar to other targeted attacks we've observed. **74% of targeted attacks are seen using email** as the initial infection vector.

BlackEnergy malware, on the other hand, has been linked to attacks **dating back to 2014**. Classified as a backdoor, BlackEnergy has a wide range of capabilities, including stealing information and executing commands into the affected system. According to investigations, the attackers initially used BlackEnergy to steal user credentials, which then allowed them use access the facilities' virtual private network (VPN) to move laterally, ultimately reaching their target: the power facilities' SCADA systems.

It should be noted that there were no evidence seen to suggest that BlackEnergy itself was used to modify the settings in the SCADA systems, as the attackers used a remote access tool used by the facilities' themselves to access the systems. BlackEnergy, however, greatly enabled the execution of the attack, as it was also used to KillDisk -- a disk-wiping malware that further aggravated the impact of the attack.

The attackers used KillDisk to delete data from the affected systems within the network, such as processes linked to serial-to-ethernet communications, and the master boot records. This can be surmised as an attempt to interfere with the facility staff's restoration efforts, and speaks of further malice on the attackers' part.

Further investigations done by Trend Micro researchers have revealed that the BlackEnergy and KillDisk have been used in other attacks involving a mining company and a rail company. The files used in the attacks mirrored the capabilities those used in the Ukraine attack, and in certain instances even used the same C&C server.

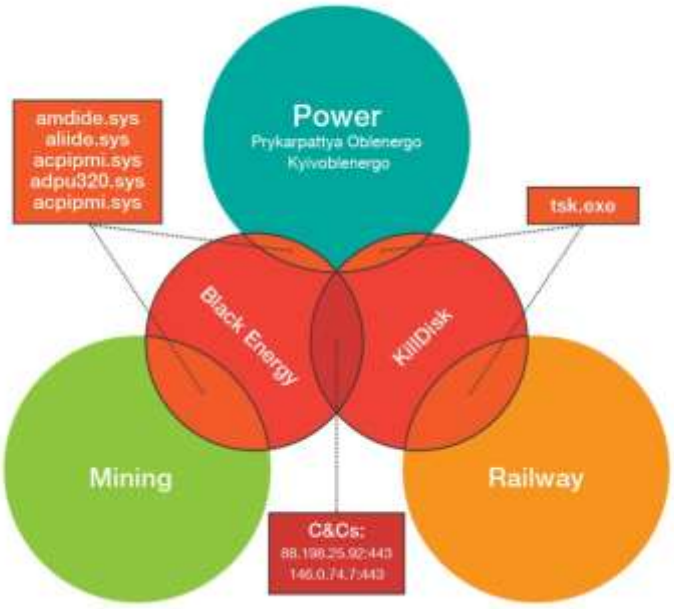

Figure 2. Overlaps between different attacks that used BlackEnergy and KillDisk

The said findings strongly suggest that BlackEnergy and KillDisk are **not just threats to the energy sector**, but to others as well.

Gap Analysis

One big factor in the successful execution of the Ukrainian power facility attack was the attackers' knowledge of the network and its vulnerabilities. We were able to note the following gaps in the affected networks' infrastructure that enabled the attackers to successfully shut down the power facilities:

- Security solutions in the power facilities' networks weren't able to block or detect the spear-phishing emails with the malicious macro documents leading to BlackEnergy
- According to reports, the VPN used to access the SCADA network lacked two-factor authentication, thus allowing attackers to move laterally without being detected
- The facilities' firewalls were not configured to block remote access to the SCADA network
- Also according to reports, no network security monitoring was in place in the facilities, thus there being no way for the personnel to be able to find abnormal activities in the network.

Solutions and Recommendations

Defending against a well-executed attack like the one launched against the Ukrainian power facilities requires a holistic and complete approach to security, one that defends against the very concept of a targeted attack – locking out any and all avenues of intrusion/unlawful entry minimizing the attack surface.

Trend Micro solutions offer a wide range of security capabilities that are designed to stop attacks such as this. **User Protection** solutions provide a broad range of protection for users – across every device, application and location, including the ability to block spear-phishing emails like those used in the power facility attack. Its anti-malware and content filtering capabilities are designed to block spear-phishing emails such as those send to the power facilities personnel. Malicious attachments such as the macro file sent with the spear-phishing email, along with the BlackEnergy variant that it downloads, can be detected through behavior monitoring and sandboxing.

Trend Micro can also help with the detection of network anomalies, including lateral movement from the initial point of contact to other parts of the network (in this case, the SCADA network) through the use of stolen credentials. The **Network Defense** solutions, powered by **Digital Vaccine Labs (DVLabs)** and **Zero Day Initiative**, detects and protects against advanced threats and targeted attacks that are invisible to standard network securityIts security capabilities can also detect and block communication between the malware and its command-and-control center (C&C). This can, in turn, prevent the download of a malicious payload such as KillDisk into the network.

These security capabilities are part of the Trend Micro Connected Threat Defense strategy that leverages three proven solutions for protecting against attacks. Aside from providing protection in the different parts of the network, Trend Micro delivers centralized visibility and control over the network, which can help in identify and investigate anomalous activity. Furthermore, the **Hybrid Cloud Security** solution delivers automated protection of workloads across physical, virtual and cloud servers, shielding sensitive enterprise resources from the attack.