the Availability Digest

www.availabilitydigest.com
@availabilitydig

Can Hackers Take Down Our Power Grid?

January 2016

Cyber experts have been warning for a long time that much of our critical infrastructure is susceptible to malicious hackers who can disable it on a moment's notice. A decade or so ago, this was not a problem as there was no way for an attacker to gain access to our industrial control systems. Communication between control systems and the devices they controlled was by dedicated communication channels such as landlines or microwave towers.

Today, the Internet provides much cheaper and faster access for interconnectivity. Control systems and the devices they control are now all interconnected via the Internet. This opens up the ideal pathway for hackers to get into these systems and do their damage.

Can it really be done? The answer is now known to be a resounding "yes" after Ukraine lost power to thousands of homes when its electric grid got hacked just before Christmas, 2015.

Increasing Incidents of Hacker Intrusions

A recent investigation by the U.S. Congressional Research Service has determined that sensitive computer systems maintaining the U.S. power grid increasingly are being attacked. It has distributed its findings to the U.S. Congress in a report entitled "Cybersecurity Issues for the Bulk Power System," dated June 10, 2015.[1]

The report warns that hackers potentially affiliated with terrorist groups or rogue nations have the ability to insert harmful malware into the internal systems governing the U.S. power grid. It notes that the entire energy sector in the U.S. is at risk, since malware could also take down gas and oil pipelines.

Furthermore, the report points out that the incidence of reported cyber intrusions aimed at undermining the U.S. grid is increasing. Even worse, independent researchers have found that hacking into grid-computing networks to be startlingly easy. In October, 2014, the Cyber Emergency Response Team (CERT) revealed that several industrial control systems had been infected with a virus capable of gathering information about how the U.S. power grid functions.

The report made several recommendations to the U.S. Congress to strengthen the U.S. cybersecurity posture. The recommendations revolved around establishing a broader sharing of cyber threat indicators and incidents between federal and private-sector entities. The goal is to enable integrated actions to protect against, prevent, mitigate, respond to, and recover from cyber incidents.

So far, the intrusions have not caused any damage in the U.S. However, a successful malicious attack could result in a nationwide crisis.

[1] http://www.fas.org/sgp/crs/misc/R43989.pdf

BlackEnergy

The primary attack vector used by hackers has been identified as the BlackEnergy Trojan horse. BlackEnergy has been found in control systems the world over. Though it is capable of doing damage to the computers it infects, it has primarily been used for data gathering.

However, in the last two years or so, it has been upgraded to include a facility called “KillDisk.” Among other malicious actions, KillDisk is designed to terminate a software facility called “ASEM Ubiquity,” which is a platform used by industrial control systems to manage their devices. KillDisk then overwrites the executable with random data so that it cannot be restarted. At this point, the control system is disabled, unable to carry out the functions required to keep the infrastructure that it was managing operational.

Investigators determined that, in many cases, the initial points of infection were Microsoft Office documents that had been embedded with malicious macros. When an unsuspecting employee opened the document, a backdoor was enabled on his system that allowed the injection of BlackEnergy into the computer. It is distressing that such a simple social-engineering ploy can create power failures that can have a life-and-death consequence for large numbers of people.

The group behind BlackEnergy has been dubbed “The Sandworm Gang.” It is believed that the gang has ties to Russia, though the Russian government is not believed to be involved in any way.

Dragonfly

Another sophisticated malware facility is also emerging to attack the power grid – Dragonfly. Dragonfly has managed to compromise a number of strategically important organizations for spying purposes and could potentially damage or disrupt energy supplies.

Dragonfly’s initial targets were defense and aviation companies in US and Canada. However, it has now shifted its focus to US and European energy firms

According to security firm Symantec, Dragonfly bears the hallmarks of a state-sponsored operation, displaying a high degree of technical capability. Based on the analysis of when they attack, Symantec believes that the attackers are likely based in Eastern Europe.

Dragonfly started with planting malware in phishing emails and in compromised web sites. It has now moved on to Trojanizing legitimate software bundles belonging to different Industrial Control System equipment manufacturers.

The Hacker’s Entry Point – the SCADA System

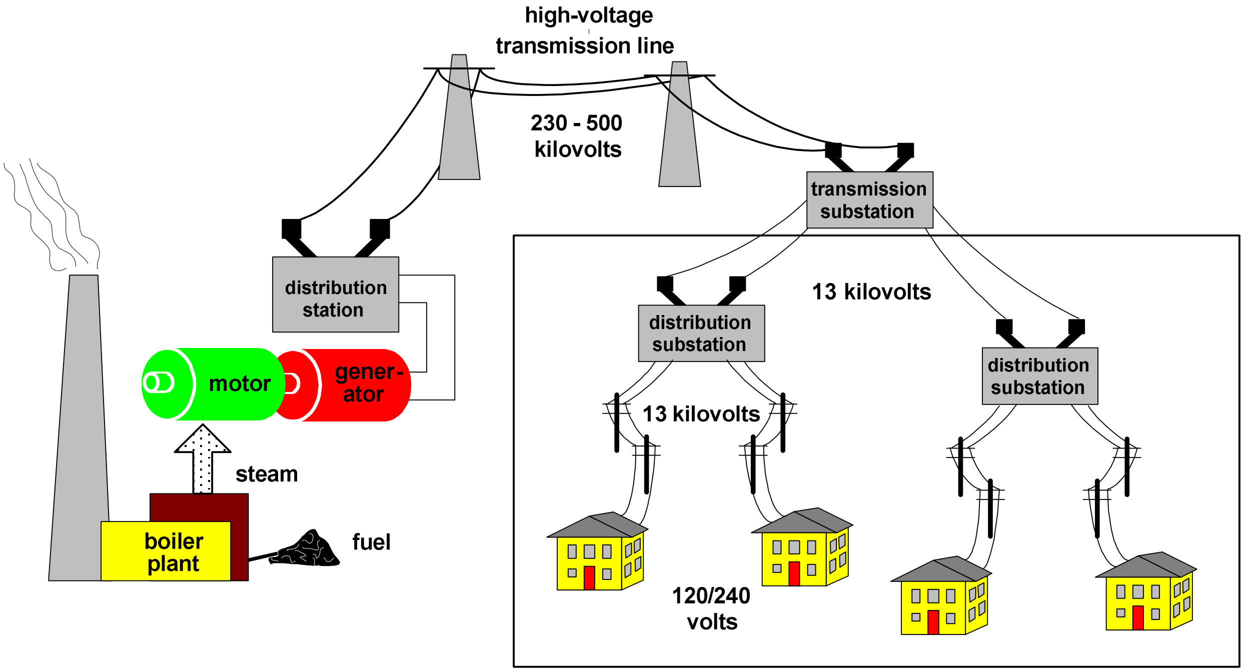
Let us turn now to one of the primary entry points for malicious code – the SCADA systems that control the power grid. A SCADA (Supervisory Control and Data Acquisition) system provides controllers with the facilities required to monitor and control the field devices upon which utilities such as the power grid depend. It automatically generates alarms should conditions in the field demand immediate controller attention and provides a raft of historical data for trend analysis, root cause analysis, and many other functions important to the utilities.

The household and building electrical power upon which we all depend comes to us through three major infrastructures – generation, transmission, and distribution:

- Electricity is *generated* by large electrical generators which are themselves powered by coal, oil, gas, water, or other sources.

- This electricity is carried over long distance *transmission* lines to local points of distribution. Since power loss over the transmission network is a function of the current flowing through the lines, transmission networks distribute electricity at very high voltages and low currents (power is voltage times current). Typical transmission voltages are 230 to 500 kilovolts. Transmission networks terminate in transmission substations, which reduce the voltage for distribution to homes and businesses.

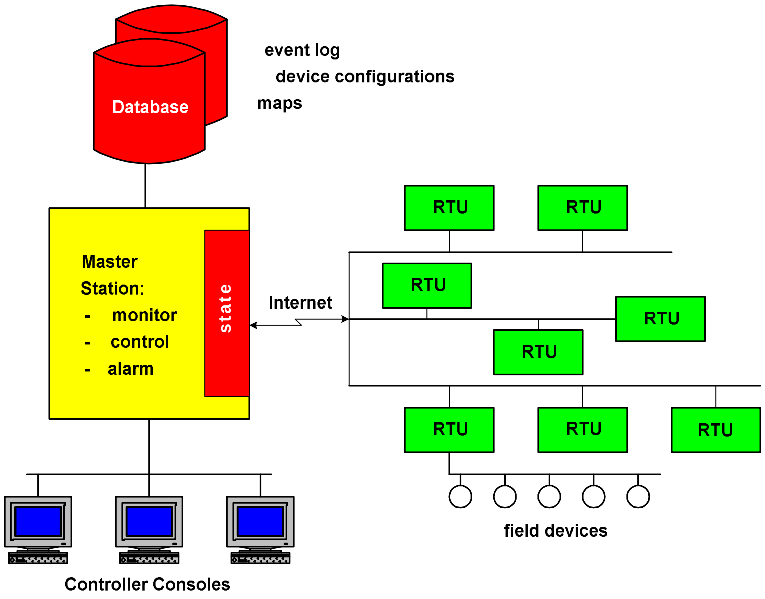
- From the transmission substations, the lower voltage electricity is distributed to other distribution substations for routing to homes and offices. These substations feed the power lines so ubiquitous on the telephone poles outside of our homes. The fact that these lines carry electricity at a "lower voltage" is a bit misleading. The voltage on the power lines outside of your home is 13,000 volts. Don't touch a downed line! This voltage is reduced by transformers on the poles near our homes or businesses to the 120/240 volts that we expect.



Electrical Distribution System

SCADA systems are used to control the generator plants, the transmission lines, and the distribution substations. A SCADA system comprises a Master Station and a set of Remote Terminal Units, or RTUs. An RTU monitors multiple digital and analog field devices in a facility and can accept commands from the Master Station to control these devices. A typical field device might be designed to measure the temperature of a transformer or to set or reset a circuit breaker.

The Master Station monitors the RTUs for status changes and maintains displays of the current field status for the controllers. If a fault condition or an alarm condition should occur, the Master Station may have the intelligence to issue commands to the RTUs to correct the situation automatically via its monitoring applications. Otherwise, the Master Station accepts commands from the controllers to send to the field devices.



A SCADA System

When SCADA systems were originally deployed decades ago, communication between the Master Station and its RTUs was over polled telephone lines, LANs, WANs, fiber, microwave, or radio. These were all point-to-point communication channels and posed no security issues. Therefore, early SCADA systems were not designed with security in mind.

However, with the advent of the Internet, communication between the Master Station and the RTUs moved to the Internet. The SCADA systems were somewhat modified to try to detect or deflect malware intrusions, but these facilities were not very sophisticated.

Therefore, the SCADA systems have become a primary target for hackers who want to control the various facilities of a power grid. As we said earlier, there has not been a hack on the U.S. power grid that has caused any damage. However, that may be about to change, as Ukraine found out.

Ukraine Loses Power Due to a Hacked Electric Grid

The complacency about power grid hacks came to a sudden end on December 23, 2015, when hackers managed to cut off power for several days to 80,000 Ukrainian customers. This was the first known instance of malware being used to generate a power outage. Fortunately for the affected Ukrainians, Christmas cold had not yet advanced into Ukraine. Daytime temperatures hovered around 60° Fahrenheit.

Researchers determined that the BlackEnergy malware was to blame. BlackEnergy infected at least three regional Ukrainian power authorities, disconnecting the electrical substations from the Ukrainian power grid. Investigators determined that this appeared to be a coordinated effort by a malicious hacker. Russia was immediately suspected, as it had just annexed the Ukrainian territory of Crimea. However, Russia denied involvement, and there is no evidence beyond suspicion implicating the Russians.

This is a wakeup call for the energy sector. Yes, its power grids are susceptible to malicious hacking to the point that they can be taken down. Not only in the Ukraine, but in the U.S. and elsewhere as well.

Summary

Governments must now seriously concern themselves with the prospect of losing a national power grid to hackers. This was the gist of the report mentioned earlier from the Congressional Research Service to the U.S. Congress.

Though nation-states may not launch such attacks on the U.S. due to the prospect of likely retaliation by the U.S., terrorists have no such concern. Terrorist organizations certainly have the technical knowhow to take down our power grid if they so choose.

It seems that no matter how hard we try to block the hackers, they are always smarter than we are and find other ways to inject malicious malware into their targets. Perhaps it is time to accept that we can't win that war and focus more on recovery. Accept that malicious actors may be successful at taking down our power grid and determine what is the fastest and most efficient way to recover. In this way, we can at least minimize the impact of a national power grid loss.

Acknowledgements

Information for this article was taken from the following sources:

QEI Provides Active/Active SCADA with OpenVMS, *Availability Digest*; September 2007.
Can Dragonfly Attacks Cause Data Center Outages, *Data Center Knowledge*; July 9, 2014.
U.S. Power Grid Being Hit With 'Increasing' Hacking Attacks, Government Warns, *Free Beacon*; June 24, 2015.
Cyber attack is wake up call for energy sector, *Energy Voice*; September 1, 2015.
Ukraine Claims Hackers Caused Christmas Power Outage, *Forbes*; January 4, 2016.
First known hacker-caused power outage signals troubling escalation, *ARS Technica*; January 4, 2016.