How hackers attacked Ukraine's power grid: Implications for Industrial IoT security

By Charles McLellan

Published: 2016-03-04 · Archived: 2026-04-05 22:01:21 UTC

Power plant Burshtyn TES, Ukraine.

Image: Raimond Spekking / CC BY-SA 4.0 (via Wikimedia Commons)

The former Soviet republic of Ukraine has been a trouble-spot since early 2014, which saw the 'Euromaidan' revolution in support of closer EU integration, the Russian annexation of Crimea and the start of the ongoing pro-Russian separatist insurgency.

To add to their woes, large sections of the Ukrainian population suffered power cuts over Christmas 2015 following a series of cyberattacks on three local energy companies. Although widely suspected to be from Russia, the identity of the hackers remains unclear as attribution in these matters is complex. However, the primary attack vector -- a well-known trojan called BlackEnergy -- has been definitively established.

The details of how the Ukranian utility companies' operational systems were compromised makes for an instructive case study illustrating the multifaceted nature of today's cyberattacks, and the vulnerability of

organisations in the Industrial Internet of Things (IIoT).

How the Ukraine attacks played out

The initial breach of the Ukraine power grid was -- as so often in cyberattacks -- down to the human factor: spear-phishing and social engineering were used to gain entry to the network. Once inside, the attackers exploited the fact that operational systems -- the ones that controlled the power grid -- were connected to regular IT systems.

Ehud Shamir, CISO at security company SentinelOne (which has analysed Black Energy 3), takes up the story.

"It's important to understand that, when you're talking about the Internet of Things, SCADA and Industrial Control Systems [ICS], these systems are usually controlled by regular Windows PCs," Shamir noted. This makes them vulnerable to mainstream malware such as Black Energy.

"The uniqueness of Black Energy is, it's very modular -- the attacker can change the malware's behaviour pretty fast," said Shamir. "In the latest attack, it was delivered, probably via an infected Excel file, by someone who got an email."

Then there's the fact that ICS controllers are often connected to regular IT systems.

"When the attackers gained access to the network, they found that the operator of the power grid had been a bit sloppy and connected some of the interfaces of the power grid's industrial control system to the local LAN," said Shamir. "Part of the modular Black Energy malware acts as a network sniffer, and this discovered data such as user credentials that allowed the attacker to access the industrial control system and jeopardise the electricity supply."

Such attacks take a lot of planning, which is one reason why nation states rather than cybercriminals are usually in the frame (another is that no customer records were stolen, or extortion demands made).

"This group probably had very good intelligence, and knew how to engineer the highest probability that someone will click a malicious link and activate the Black Energy malware -- in most attacks, it's the human factor that leads to the infiltration," said Shamir. Further evidence of advanced planning was a simultaneous denial-of-service attack on the power utilities' call centres, in order to thwart customers trying to report the outages.

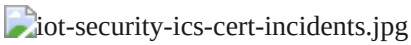
Some aspects of the Ukraine cyber-attack remain opaque -- specifically, whether a modular component called KillDisk (a hard disk wiper) actually caused the power outage, or whether it simply made it impossible to restore the compromised systems using SCADA protocols.

As if further evidence of a political motive was required, researchers at security company Trend Micro recently reported that the same combination of BlackEnergy and KillDisk "may have been used against a large Ukrainian mining company and a large Ukrainian rail company" around the same time as the attacks on the power utilities.

Whether the perpetrators' ultimate goal was to destabilise Ukraine via coordinated cyberattacks on its critical infrastructure, or to determine the weakest sector prior to further attacks, or simply to test out the Black Energy 3/KillDisk malware, Trend Micro's conclusion is unarguable: "Whichever is the case, attacks against Industrial Control Systems (ICS) should be treated with extreme seriousness because of the dire real-world repercussions."

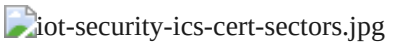
How big is the problem?

The Ukraine attacks show how vulnerable the industrial control systems in the IIoT can be -- but how widespread is the problem? The annual reports from ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) give a good indication of recent trends in the US. In the 2015 financial year (October 2014-September 2015), ICS-CERT responded to 295 reported incidents, up from 245 the previous year and more than six times as many as were reported back in 2010:



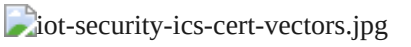
Data source: ICS-CERT (US)

Critical Manufacturing was the most attacked sector in 2015, ahead of Energy, which was the number-one target the previous year:



Data source: ICS-CERT (US)

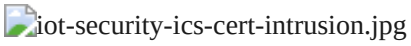
ICS-CERT said that "there were insufficient forensic artifacts to definitively identify an initial infection vector" in 38 percent of last year's incidents, with spear-phishing the most prevalent identifiable initial infection vector:



Data source: ICS-CERT (US)

Echoing the Ukraine power grid attack, ICS-CERT noted that in 2015 it "responded to a significant number of incidents enabled by insufficiently architected networks, such as ICS networks being directly connected to the Internet or to corporate networks, where spear phishing can enable access."

Although the majority (69%) of attempted breaches investigated by ICS-CERT in 2015 were either unsuccessful or successfully defended, or failed to get beyond the organisation's business network (12%), 12 percent of cyberattacks did manage to penetrate the industrial control systems. That's a worrying 35 incidents -- up from 22 (9% of 245) in 2014.



Data source: ICS-CERT (US)

A 2015 survey by the SANS Institute, entitled *The State of Security in Control Systems Today*, exposed a worrying lack of visibility into the nature of cyberattacks on industrial control systems. The survey canvassed 314 organisations worldwide, 78 percent of which were in the US. Headline findings were:

- 32 percent indicated that their control system assets or networks had been infiltrated at some point
- 34 percent of those infiltrated believed their systems had been breached more than twice in the previous 12 months
- 15 percent reported requiring more than a month to detect a breach
- 44 percent were unable to identify the source of the infiltration
- 42 percent saw external actors as the number-one threat vector

Another key finding was that, although 19 percent of respondents identified the integration of IT into control system networks as the top threat vector (and 46% put it in the top three), less than half (47%) actually have a strategy to address this convergence:


sans-airgap-strategy.jpg

Data source: SANS Institute

As the Ukraine power grid example clearly shows, it's this convergence of IT and industrial control systems -- sometimes referred to as a lack of 'air gapping' -- that can provide cyberattackers with a route into critical infrastructure via conventional malware.

Further evidence of widespread infiltration into organisations involved with critical infrastructure was recently provided by the research arm of security company Cylance, SPEAR, in a report entitled Operation Dust Storm.

The report details cyberattacks, starting in 2010 and spanning multiple years and vectors, against major industries spread across Japan, South Korea, the United States, Europe, and several other Southeast Asian countries. SPEAR's most recent research suggests that the attackers have shifted their focus to "specifically and exclusively target Japanese companies or Japanese subdivisions of larger foreign organisations".


operation-dust-storminfographic-2014-2016.jpg

The most recent portion of the 2010-2016 Operation Dust Storm timeline.

Image: Cylance

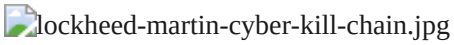
"The attack that is happening is a current attack, in progress, that has sustained compromise of a variety of Japanese organisations -- in particular they include electric utility companies, oil companies, natural gas companies, transportation organisations, construction, and even some finance organisations," Cylance's chief marketing officer Greg Fitzgerald told ZDNet.

"From what we can tell, the compromise has only indicated the ability to be present long-term and undetected -- we cannot tell if they have done any damage to the organisations today," said Fitzgerald. "What we do know is that the attack methods used, which gain access to computers and their networks, would enable them to cause damage or steal data should they desire."

Know your enemy: The Cyber Kill Chain

Faced with the weight of evidence about the prevalence of cyberattacks, CxOs could be forgiven for throwing in the towel and accepting that the 'bad guys' will always have the capability to infiltrate their organisations. However, cybersecurity is an arms race and, as Sentinel One's Shamir points out, "the 'good guys' have the capabilities as well".

Most cyber-attacks follow a similar path from reconnaissance to objective completion, and this has been codified -- initially by Lockheed Martin -- as the Cyber Kill Chain:


lockheed-martin-cyber-kill-chain.jpg

The Cyber Kill Chain.

Image: Lockheed Martin

This provides a useful framework for intelligence-driven defence, as Richard Cassidy, technical director EMEA at security-as-a-service provider Alert Logic, told ZDNet.

"If you think about the Ukranian power grid, for instance, the attack itself was well prepared -- some analysts are saying it was at least a six-month preparation phase. These are the first two steps in the cyber kill chain -- reconnaissance and weaponisation -- and we see that at Alert Logic in our customer base: most of the activity we're picking up is in these first steps. The longer we see a source enumerate a target, the more severe we expect the threat to be. The cyber kill chain gives us real indicators, and steps to understand and follow, to help prevent us getting to the end of the chain, which is the worst-case scenario."

Outlook

To date, cyberattacks on critical infrastructure have largely been restricted to nation states, although the Anonymous hacktivist group has attacked oil, gas and energy companies -- specifically, Middle Eastern companies in the petroleum industry. The amount of resources required in terms of preparation time, finance and skills seem, so far, to have kept 'common' cybercriminals otherwise occupied with softer targets.

Critical infrastructure attacks that follow through to actual damage are, thankfully, few and far between: incidents like the infamous 2010 Stuxnet sabotage of Iran's nuclear program and the 2015 Ukranian power grid outage are the exception rather than the rule. However, as the recent Operation Dust Storm revelations show, widespread infiltration leaves plenty of potential for serious trouble.

There's certainly no place for a head-in-the-sand attitude, as Alert Logic's Cassidy points out: "Unfortunately, manufacturing environments, because of the nature of their business, do tend to be an easier target because they're not normally the types of organisations that have seen threat activity. For that reason, you can get too complacent in an organisation like that and think, 'it won't happen to me'."

Let's hope that the cybersecurity industry -- companies such as Sentinel One, Trend Micro, Cylance and Alert Logic, and organisations like CERT and SANS -- can persuade companies running industrial control systems that complacency is no longer an option.
