The cyberattack on Ukraine's power grid is a warning of what's to come

January 13 2016, by Nilufer Tuptuk And Stephen Hailes, Ucl

Credit: Steag/VGB Power Tech GmbH, CC BY-SA

When more than 100,000 people in and around the Ukrainian city of Ivano-Frankivsk were left without power for six hours, the Ukrainian energy ministry accused Russia of launching a cyberattack on the country's national energy grid.

Now reports released by security researchers from the SANS Industrial Control Systems team and the Industrial Control Systems Cyber

Emergency Response Team confirm their belief that a cyberattack was responsible for the power cut, making the incident one of the first significant, publicly reported cyberattacks on civil infrastructure.

This is a rare event, of which the most famous example is the Stuxnet malware used to destroy equipment in the Iranian nuclear programme. Many consider Stuxnet so sophisticated that national governments must have been involved. But as is frequently the case, attributing responsibility for Stuxnet has proved difficult, and it's likely that, despite circumstantial evidence, it will be the same in this case. While the Ukrainian Security Service (SBU) and the international press were quick to blame Russian state-backed hackers, Moscow has remained silent.

Experts examining the attack in Ukraine found that BlackEnergy malware appeared to have been used to gain entry to the national grid's systems. Certainly BlackEnergy has in the past been used for launching distributed denial of service (DDoS) attacks, cybercrime, information theft, global infection of industrial control systems and targeted attacks against Ukraine and Poland. BlackEnergy is seen as the calling card of the Sandworm hacking group, which has been linked to the Russian state .

When control systems turn bad. Credit: David Becher, CC BY-SA

While the researchers found no evidence that BlackEnergy was directly used to bring down the power supply, forensic analysis has revealed a multi-pronged attack. After the power was cut, denial of service attacks were deployed to try to prevent error messages from reaching service personnel, while the malware wiped the control systems' servers in order to delay repair and cover its tracks. This attention to detail suggests the attack was indeed aimed deliberately at these particular electricity facilities.

The spread of technical sophistication

One consequence of this incident is that many more governments have become acutely aware of the potential vulnerabilities of national civilian infrastructure such as electricity, gas, water and transport networks. Questions regarding the vulnerability of the national grid are being asked in the US, for example.

Inevitably, such attacks also cause tensions between nations. But it's worth noting that a tense international situation does not necessarily imply that one party is responsible for an attack on another. The increasing availability of sophisticated malware that can be found online has lowered the bar to launching a sophisticated attack – though a successful attack is still regarded as very difficult – meaning that there many potential culprits. A rush to judgement is inadvisable: the Russians were blamed for the Baku-Tbilisi-Ceyhan oil pipeline explosion in 2008, for example, since the Russo-Georgian war began two days later. This conclusion has since been challenged.

Vulnerable industrial control systems that run, build and monitor things are all around us. Credit: BMW Werk Leipzig, CC BY-SA

Old equipment faces new problems

Industrial control systems – those used in all manner of infrastructure in healthcare, manufacturing, utilities, and transport – are moving from high-cost, proprietary hardware and software provided by a handful of specialist companies towards cheaper, more flexible off-the-shelf systems. This increases the scope for attack as the systems are more easily available to practice on.

Project SHINE used the SHODAN search engine to discover what level

of risk is posed by internet-connected industrial control devices. In January 2014 the project wound up due to the rate at which new devices were appearing – more than a million at the final count.

The problem is that the industrial control systems now being connected to the internet were designed in the pre-internet era. The underlying protocols and components take no account of modern internet threats and so are inherently insecure. These vulnerabilities have led to economic damage and lost production, environmental damage, injury and loss of life, and scale up to potentially catastrophic nationwide effects, as in Ukraine.

While there have been relatively few attacks so far, as more off-the-shelf consumer-grade hardware and software finds its way into critical infrastructure a growing number of highly-skilled "black hat" hackers, motivated by malice, greed or politics, will find ways to exploit these vulnerabilities. With their rudimentary defences, many industrial control systems are no match. Unfortunately staff within many organisations are ill-prepared to prevent, identify or respond; the growing attentions of attackers, together with this lack of knowledge and some complacency is recipe for enormous harm.

To cloud the picture still further is the rapid progress towards an Internet of Things, where physical objects of all types are connected to, and controlled over, the internet. This will underpin the next generation of industrial systems, but will also be common throughout government, business and the home. If we do not learn the lessons of Ukraine and think deeply about the potential threats, there is a very real prospect of major economic and social damage. We must look hard at what is coming and prepare for the worst.

This article was originally published on The Conversation. *Read the* original article.

Source: The Conversation