Forbes

http://onforb.es/1MPmmZF

Thomas Fox-Brewster Forbes Staff

I cover crime, privacy and security in digital and physical forms.

SECURITY 1/04/2016 @ 12:15PM | 8.080 views

Ukraine Claims Hackers Caused Christmas Power Outage

Just before Christmas, power went out across western Ukraine. Soon after, the energy ministry confirmed it was exploring claims a cyber attack disrupted local energy provider Prykarpattyaoblenergo, causing blackouts across the Ivano-Frankivsk region on 23 December. The SBU state intelligence service said Russian attempts to disrupt the country's power grid had been deflected, but did not comment on any specific attack.

The details were patchy. But today, the Computer Emergency Response Team of Ukraine – CERT-UA – told FORBES the outages were caused by

an attack. National CERTs are in charge of coordinating responses to and investigations into cyber attacks. Eugene Bryksin, a member of the government organization, said it was working with Prykarpattyaoblenergo on the investigation but could provide no information other than to confirm the accuracy of the reports.

If his information was accurate, the attack is a rare public example of hackers taking out critical infrastructure and another sign of the rising digitization of warfare. Neither Prykarpattyaoblenergo nor the SBU could be contacted at the time of publication.

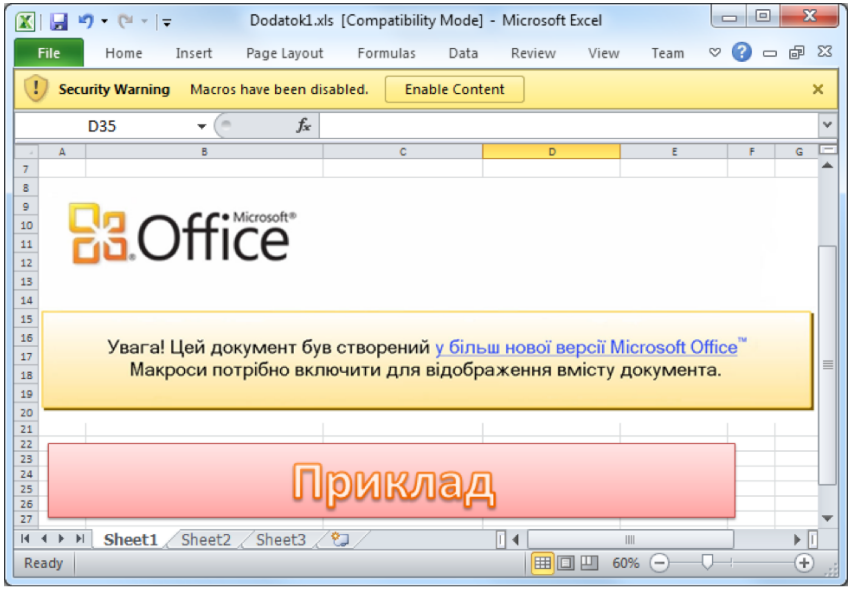
Bryksin also said research by somewhat sceptical US-based researchers looking for digital clues was accurate, in particular the attribution to a group of hackers using the so-called "BlackEnergy" malware.

Robert M Lee, 27-year-old co-founder of consultancy Dragos Security and former cyber warfare operations officer for the US Air Force, told FORBES he had obtained a piece of malware that had found its way onto the Prykarpattyaoblenergo network. On initial analysis, it did not appear to contain functions

that would have switched off power, but was designed to wipe systems to render post-attack forensics ineffective. Nevertheless, he believed the evidence indicated hackers really were responsible for taking out the power in Ivano-Frankivsk.

“When this first came out, I was extremely sceptical,” Lee said. “But with a sample coming forward and that sample being new and unique… there’s a really high chance it was directly involved in the attacks.”

The malware was soon linked to a known hacker tool - BlackEnergy – that had previously been used in attempts to breach energy providers the world over, including US organizations. Security firm ESET said the hackers had used backdoors to spread the KillDisk wiper malware across energy companies in the Ukraine, not just Prykarpattyaoblenergo. The initial point of infection with the BlackEnergy malware occurred after employees opened Microsoft Office files containing malicious macros – single computer instructions that define sets of instructions for particular tasks.



A file surreptitiously serving the BlackEnergy malware. Ukraine says hackers using BlackEnergy breached an energy company to shut off power in the west of the country.

ESET researcher Anton Cherepanov also found the KillDisk variant detected in various electricity companies in the region contained “functionality specifically intended to sabotage industrial systems”. It looked to kill two “non-standard processes” – executable files called ‘komut.exe’ and ‘sec_service.exe’. Whilst the anti-virus firm’s researchers couldn’t determine what komut.exe did, it said the second process name may belong to software called ASEM Ubiquity, a platform often used in industrial control systems (ICS).

Where that latter process was found, the wiper would terminate it and overwrite the executable with random data.

Cherepanov said his employer could “assume with a fairly high amount of certainty” that a range of tools had been used by the BlackEnergy group to cause the power outage in the Ivano-Frankivsk region.

Jake Williams, principal consultant at whitehat hacker firm Rendition Infosec, also analyzed the malware from the Prykarpattyaoblenergo network, noting it sought to wipe a variety of files. He confirmed the sec_service file was targeted. Once the malware had infected a Windows system, it would force a reboot. “In most cases that machine is not going to come back up,” Williams said.

Beware BlackEnergy

The BlackEnergy malware, which has been used in attacks dating back to 2007, was originally thought to be focused on cyber espionage. But in 2014, hackers updated the toolset to include

malicious code targeting SCADA ICS, known-to-be-vulnerable kit used to control power stations and other critical infrastructure.

A link between BlackEnergy and the KillDisk malware was first reported by CERT-UA in November when news publications were attacked around the 2015 Ukrainian local elections. This added to suspicions Russian-sponsored hackers were involved in the group.

Intelligence provider iSight Partners said it believes a hacker collective called Sandworm Team has been using BlackEnergy over the last two years. The company said today it believed the group was Russian and that it targeted US and European industrial control systems from 2014 onwards. “Renewed BlackEnergy activity, which we believe is Sandworm Team, was uncovered throughout 2015 in Ukraine affecting government, telecommunications, and energy sector organizations in the country,” it wrote in a statement to media.

But Russian individuals and businesses have also been targeted by hackers using the BlackEnergy malware, according to November 2014 research from Russian firm Kaspersky. It said the list of

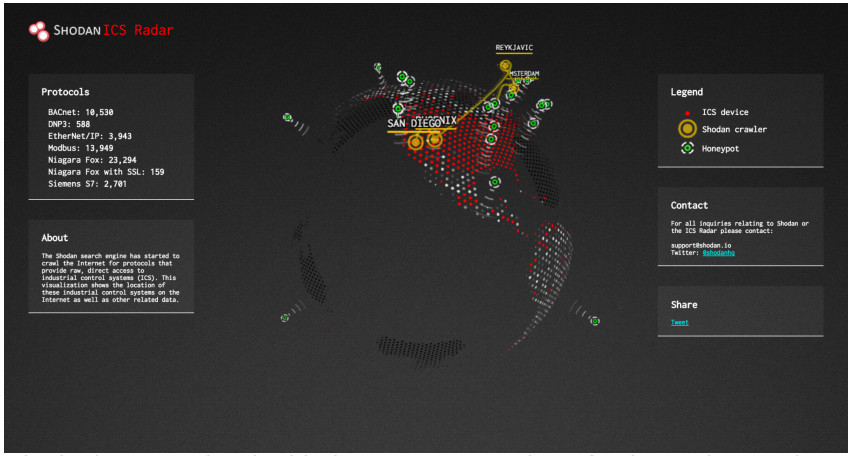
victims is long and diverse, with power facilities, government bodies, emergency services and academics also targeted, across a wide range of countries. Kaspersky also suggested BlackEnergy had been used for criminal enterprises but some time in 2014 was used in attacks that appeared to have government backing.

Tit for tat attacks?

During the last two weeks of December, power was also taken out in Crimea, a region recently annexed by Russia in 2014. One attack appeared to be the result of physical disruption. Ukraine was accused of carrying out the hit. Lee wondered whether the digital hit on Ukraine could have been a response to the earlier sabotage.

Causing explosions is an obvious if blunt way to cause disruption, but attribution is fairly obvious. When it comes to digital attacks, however, trying to conclude who was responsible is far trickier. This is one of many reasons nation states are heavily investing in offensive cyber resources: when they strike they can easily deny culpability.

Meanwhile, cheap attack tools and widespread insecurity across critical infrastructure technology make a devastating attack on energy companies feasible. Recent reports that an American dam was targeted by Iranians showed no country can be complacent.



Shodan's ICS Radar, highlighting a vast number of industrial control systems in the US accessible over the Internet. Some may be vulnerable to foreign cyber attacks.

"[The Ukraine attack] is fairly significant," Williams added, who described general industrial control system security as a "train wreck as far as security goes". "The odds are good that you could pop into ICS networks... and replicate this kind of attack.

“I do think this is a wake up call for a lot of energy companies and not just energy companies.” There is certainly a growing list of companies severely damaged by destructive attacks, from Sony Pictures to Saudi Aramco to the Sands Casino. All industries are vulnerable.

Tips and comments are welcome at TFox-Brewster@forbes.com or tbthomasbrewster@gmail.com for PGP mail. Get me on Twitter @iblametom and tfoxbrewster@jabber.hot-chilli.net for Jabber encrypted chat.

[$7.8 Million Fee For Lawyers, 7-Cent Check For One Lucky Class Member]

[2016 30 Under 30: Retail & E-Commerce]
