RSAConference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

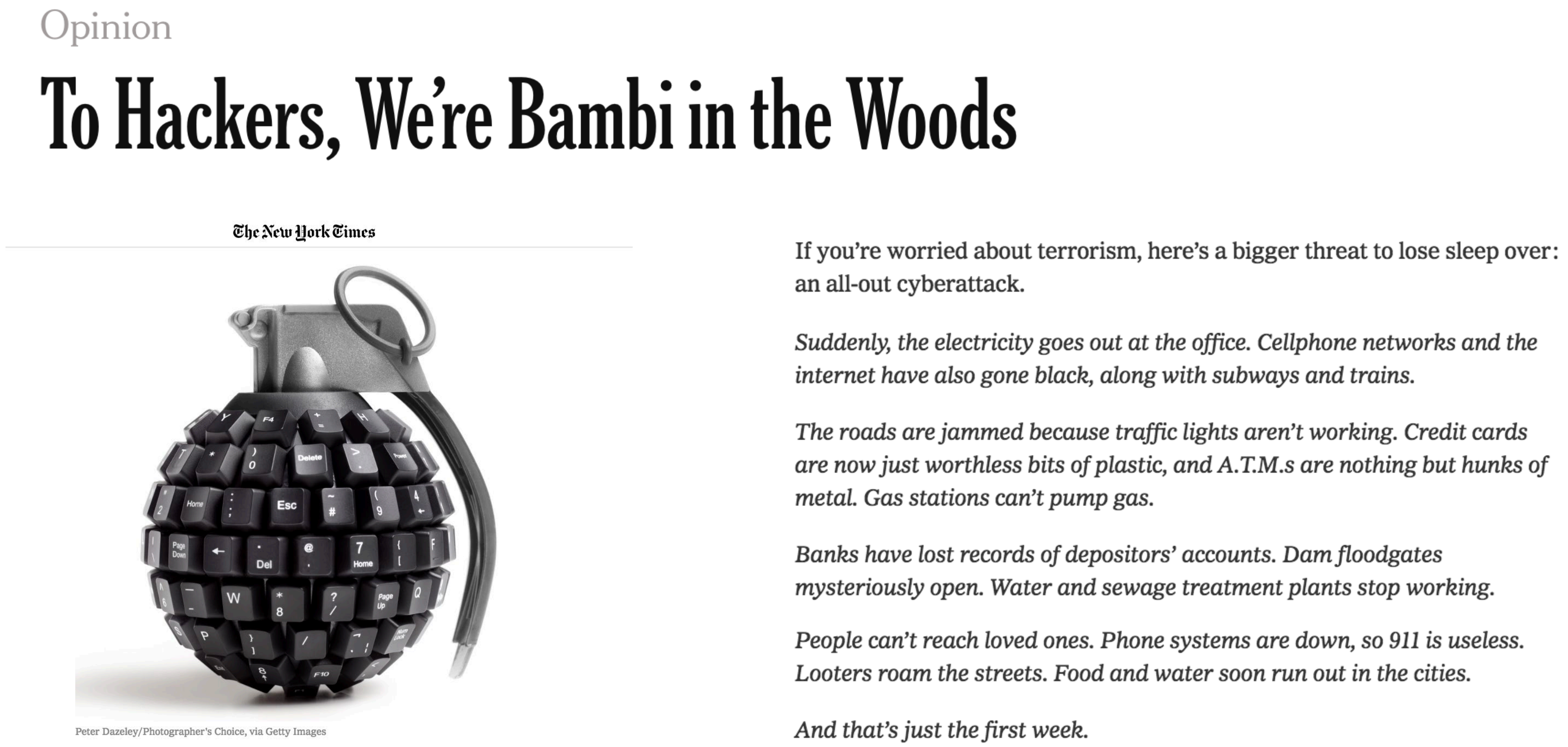
SESSION ID: SBX4-W2

Debunking the Hacker Hype: The Reality of Widespread Blackouts

Selena Larson

Intelligence Analyst
Dragos
@selenalarson

The Expectation



Opinion

To Hackers, We're Bambi in the Woods

The New York Times

Peter Dazeley/Photographer's Choice, via Getty Images

If you're worried about terrorism, here's a bigger threat to lose sleep over: an all-out cyberattack.

Suddenly, the electricity goes out at the office. Cellphone networks and the internet have also gone black, along with subways and trains.

The roads are jammed because traffic lights aren't working. Credit cards are now just worthless bits of plastic, and A.T.M.s are nothing but hunks of metal. Gas stations can't pump gas.

Banks have lost records of depositors' accounts. Dam floodgates mysteriously open. Water and sewage treatment plants stop working.

People can't reach loved ones. Phone systems are down, so 911 is useless. Looters roam the streets. Food and water soon run out in the cities.

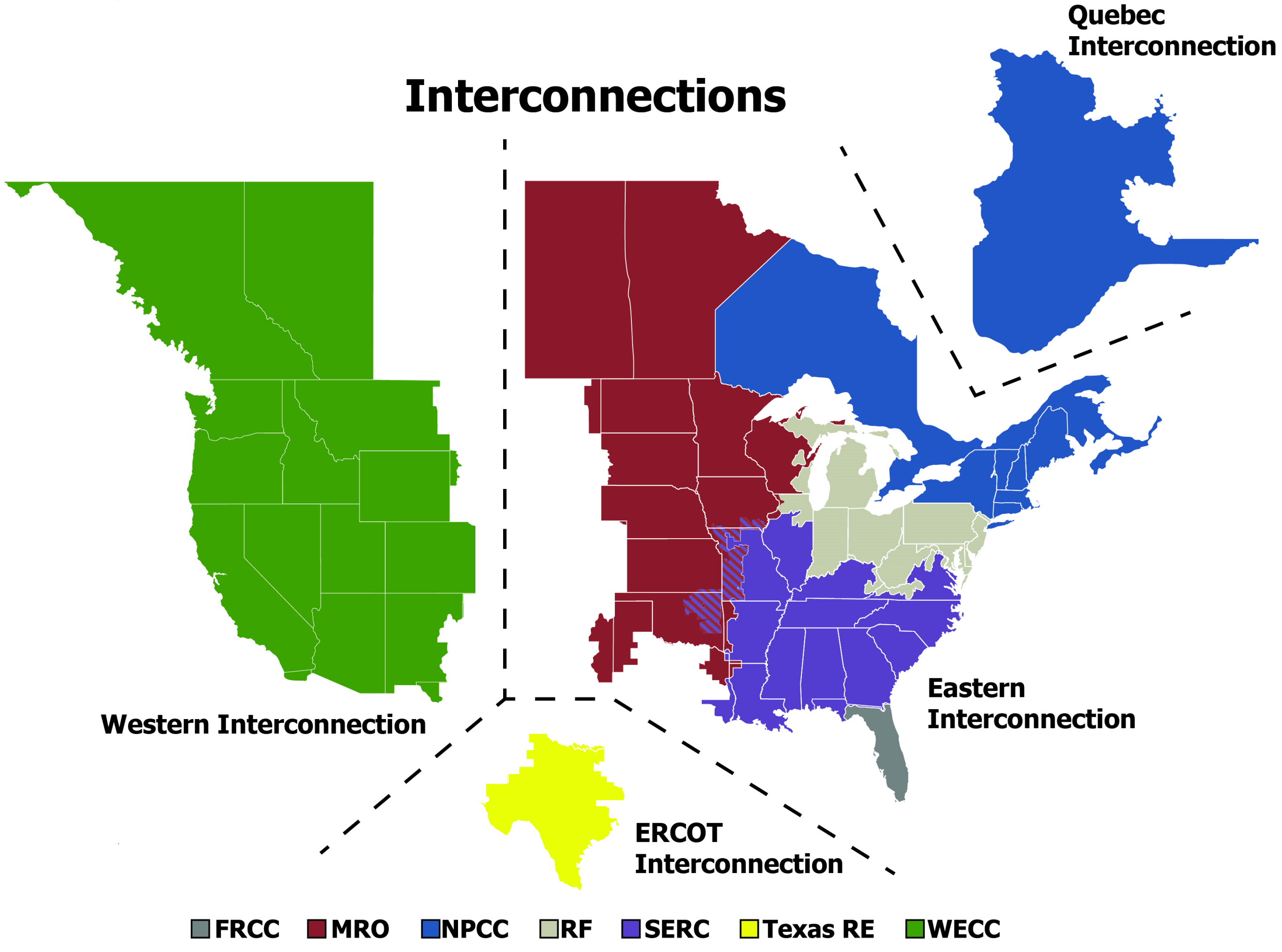
And that's just the first week.

The Reality

- A destructive incident at one site would require highly-tailored tools and operations and would not effectively scale.
- A ransomware infection at the financial services division of an electric utility doesn’t automatically translate into a blackout. (IT/OT boundaries)
- Six of the ICS-focused activity groups that are tracked have targeted corporate ICS networks for intelligence gathering. Two have gone further.

The North American Electric Grid

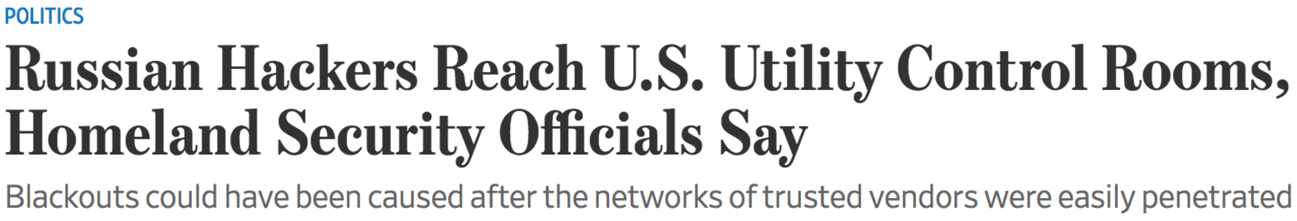
- Resilient
- Segmented



https://www.nerc.com/AboutNERC/keyplayers/Pages/default.aspx

Cyber "Implants" and Other Misunderstandings

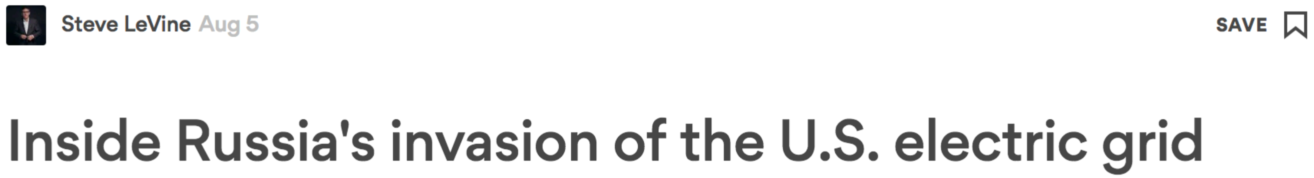
- Incorrectly reported information based on a DHS presentation led to some alarm and confusion over grid hacking claims.



POLITICS

Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say

Blackouts could have been caused after the networks of trusted vendors were easily penetrated



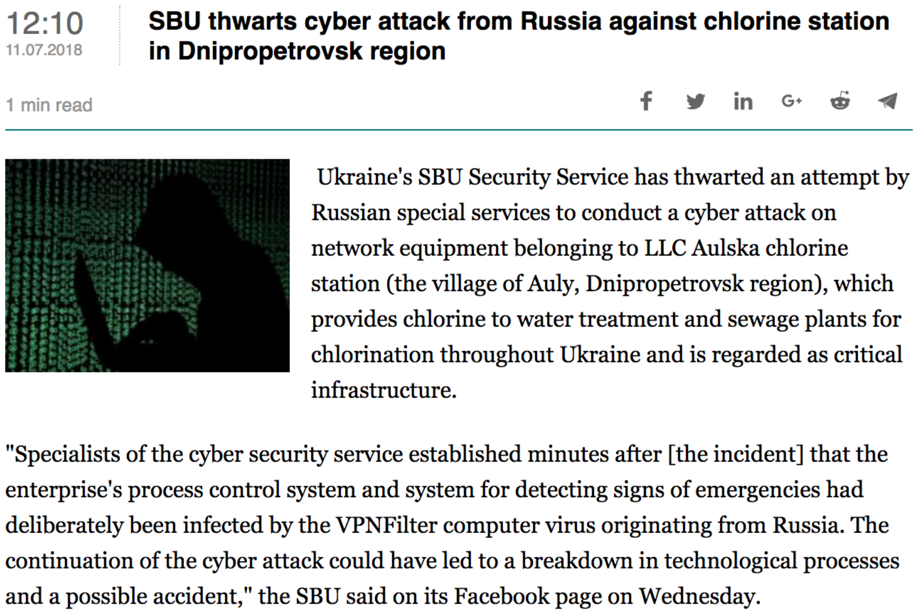
Steve LeVine Aug 5

SAVE

Inside Russia's invasion of the U.S. electric grid

VPNFilter

- In July, SBU reported a chlorine production plant's process control system was infected with VPNFilter malware and could have caused a possible accident had it not been thwarted.
- These claims blew up.



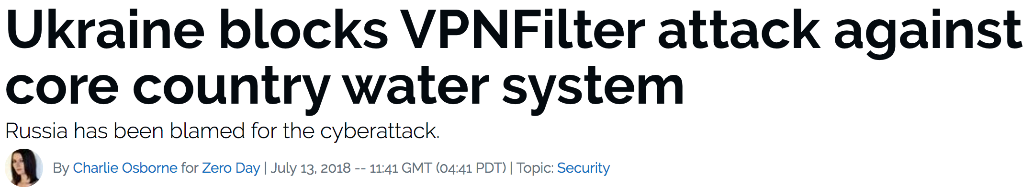
12:10
11.07.2018

SBU thwarts cyber attack from Russia against chlorine station in Dnipropetrovsk region

1 min read

Ukraine's SBU Security Service has thwarted an attempt by Russian special services to conduct a cyber attack on network equipment belonging to LLC Aulska chlorine station (the village of Auly, Dnipropetrovsk region), which provides chlorine to water treatment and sewage plants for chlorination throughout Ukraine and is regarded as critical infrastructure.

"Specialists of the cyber security service established minutes after [the incident] that the enterprise's process control system and system for detecting signs of emergencies had deliberately been infected by the VPNFilter computer virus originating from Russia. The continuation of the cyber attack could have led to a breakdown in technological processes and a possible accident," the SBU said on its Facebook page on Wednesday.



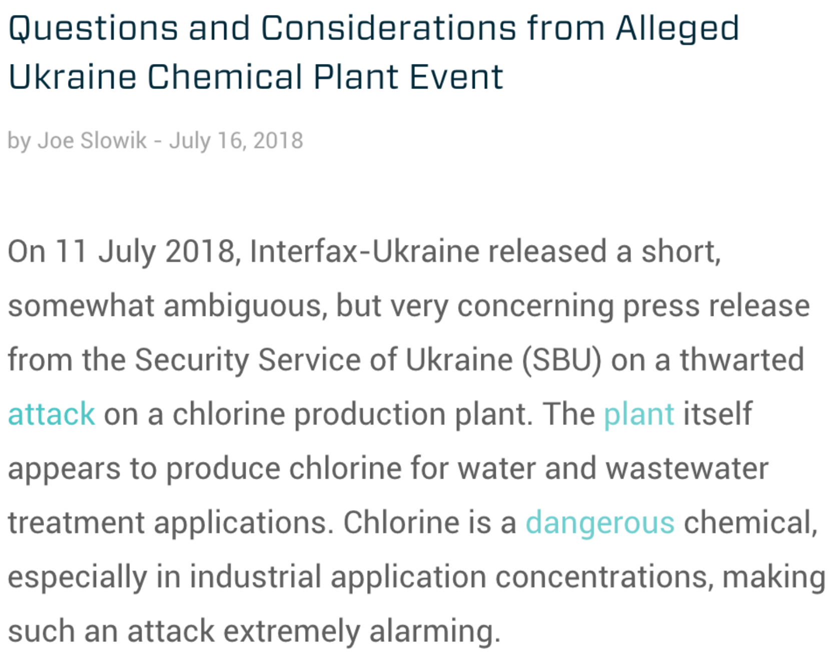
Ukraine blocks VPNFilter attack against core country water system

Russia has been blamed for the cyberattack.

By Charlie Osborne for Zero Day | July 13, 2018 -- 11:41 GMT (04:41 PDT) | Topic: Security

VPNFilter

- “No known functionality of VPNFilter allows for modification or manipulation of traffic, which would be necessary to weaponize the network device implant.”

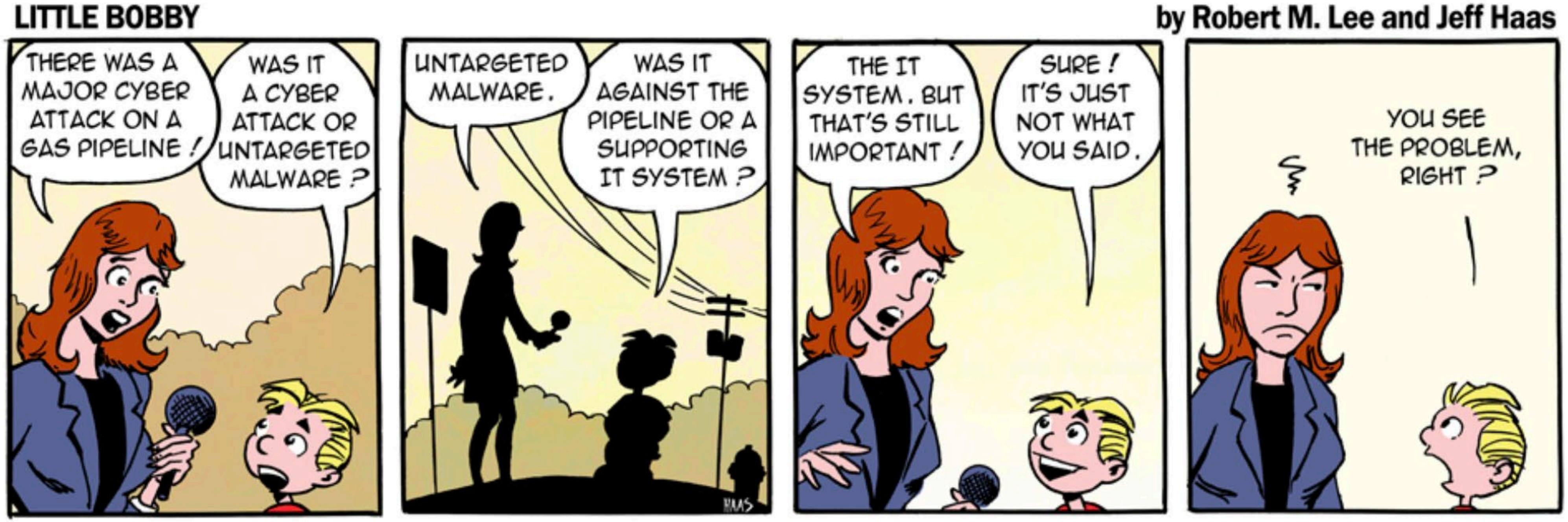


Questions and Considerations from Alleged Ukraine Chemical Plant Event

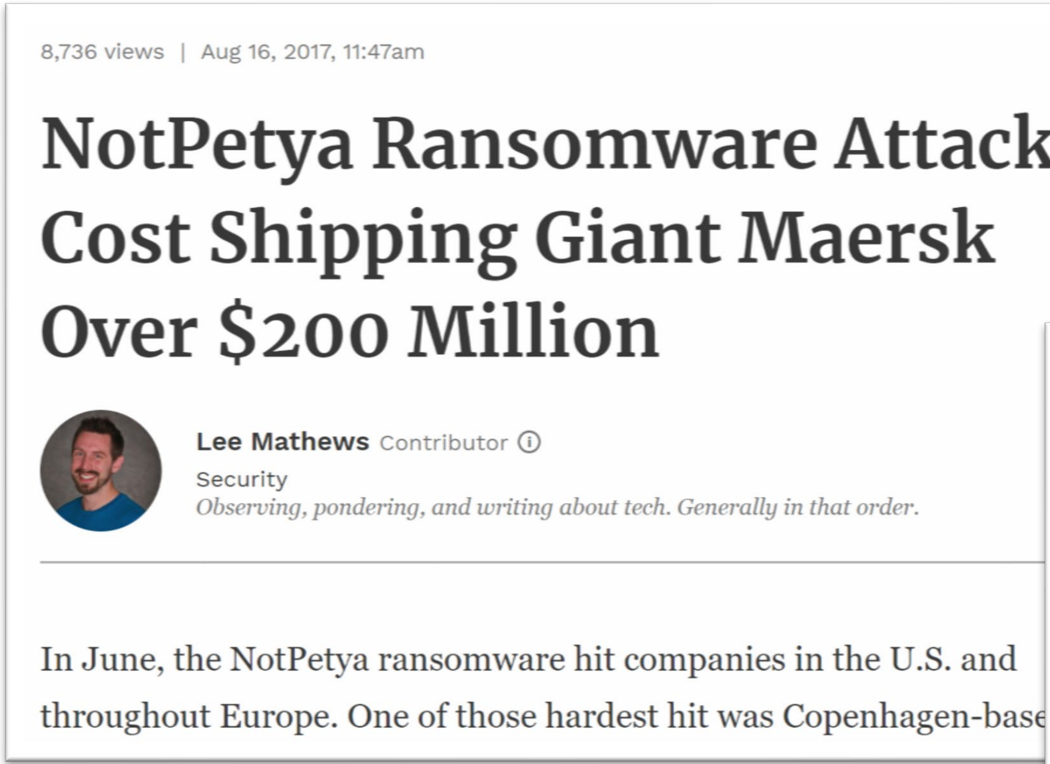
by Joe Slowik - July 16, 2018

On 11 July 2018, Interfax-Ukraine released a short, somewhat ambiguous, but very concerning press release from the Security Service of Ukraine (SBU) on a thwarted attack on a chlorine production plant. The plant itself appears to produce chlorine for water and wastewater treatment applications. Chlorine is a dangerous chemical, especially in industrial application concentrations, making such an attack extremely alarming.

Nuance


LITTLE BOBBY
by Robert M. Lee and Jeff Haas
THERE WAS A MAJOR CYBER ATTACK ON A GAS PIPELINE!
WAS IT A CYBER ATTACK OR UNTARGETED MALWARE?
UNTARGETED MALWARE.
WAS IT AGAINST THE PIPELINE OR A SUPPORTING IT SYSTEM?
HAAS
THE IT SYSTEM. BUT THAT'S STILL IMPORTANT!
SURE! IT'S JUST NOT WHAT YOU SAID.
YOU SEE THE PROBLEM, RIGHT?

Commodity Malware Remains a Risk

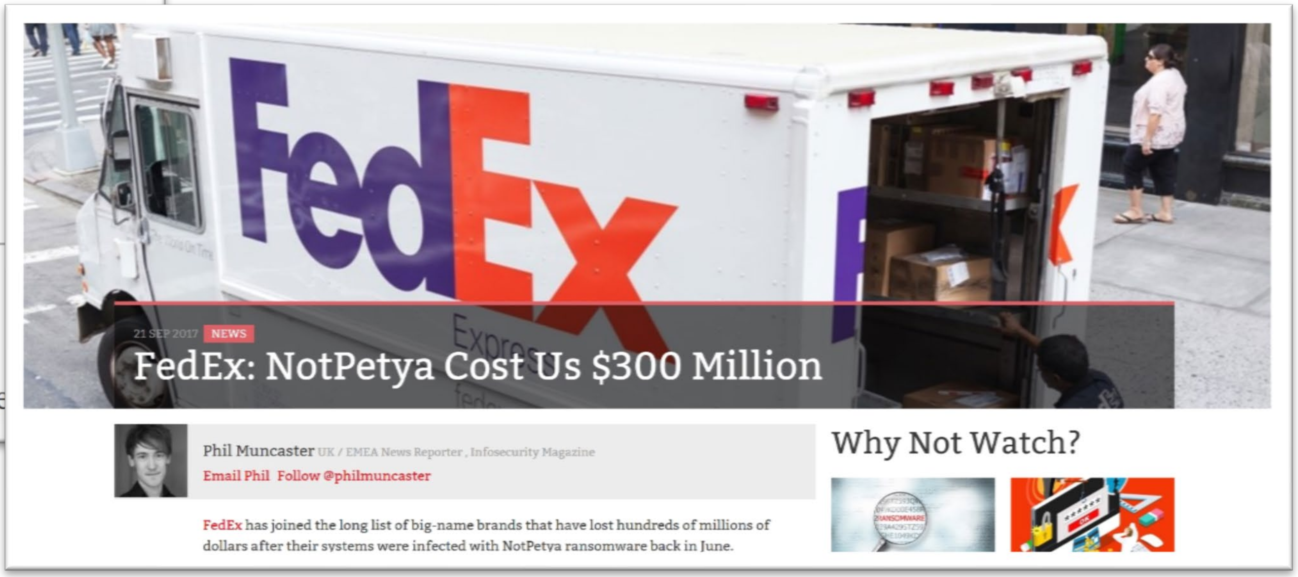


8,736 views | Aug 16, 2017, 11:47am

NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million

Lee Mathews Contributor ⓘ
Security
Observing, pondering, and writing about tech. Generally in that order.

In June, the NotPetya ransomware hit companies in the U.S. and throughout Europe. One of those hardest hit was Copenhagen-base



21 SEP 2017 NEWS

FedEx: NotPetya Cost Us $300 Million

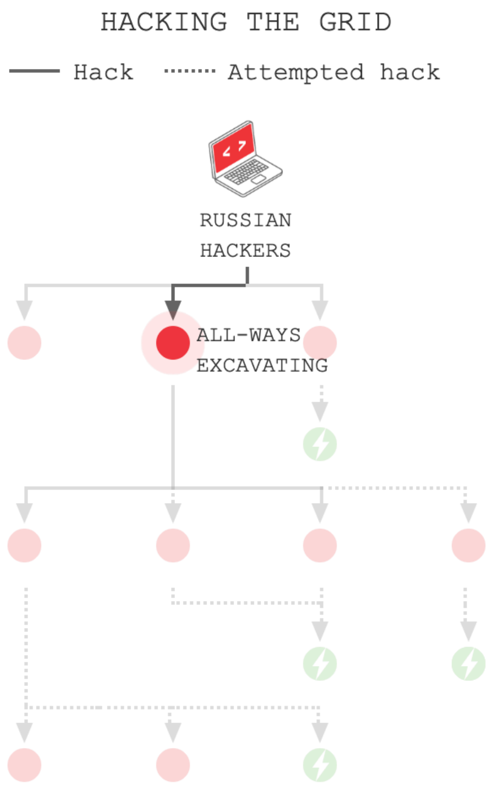
Phil Muncaster UK / EMEA News Reporter , Infosecurity Magazine
Email Phil Follow @philmuncaster

FedEx has joined the long list of big-name brands that have lost hundreds of millions of dollars after their systems were infected with NotPetya ransomware back in June.

Supply Chain Concerns

- Third-party or supply chain compromise leverages explicit trust between parties and bypasses a large part of the security stack, potentially including perimeter defenses such as firewalls or proxy servers, to access a target.

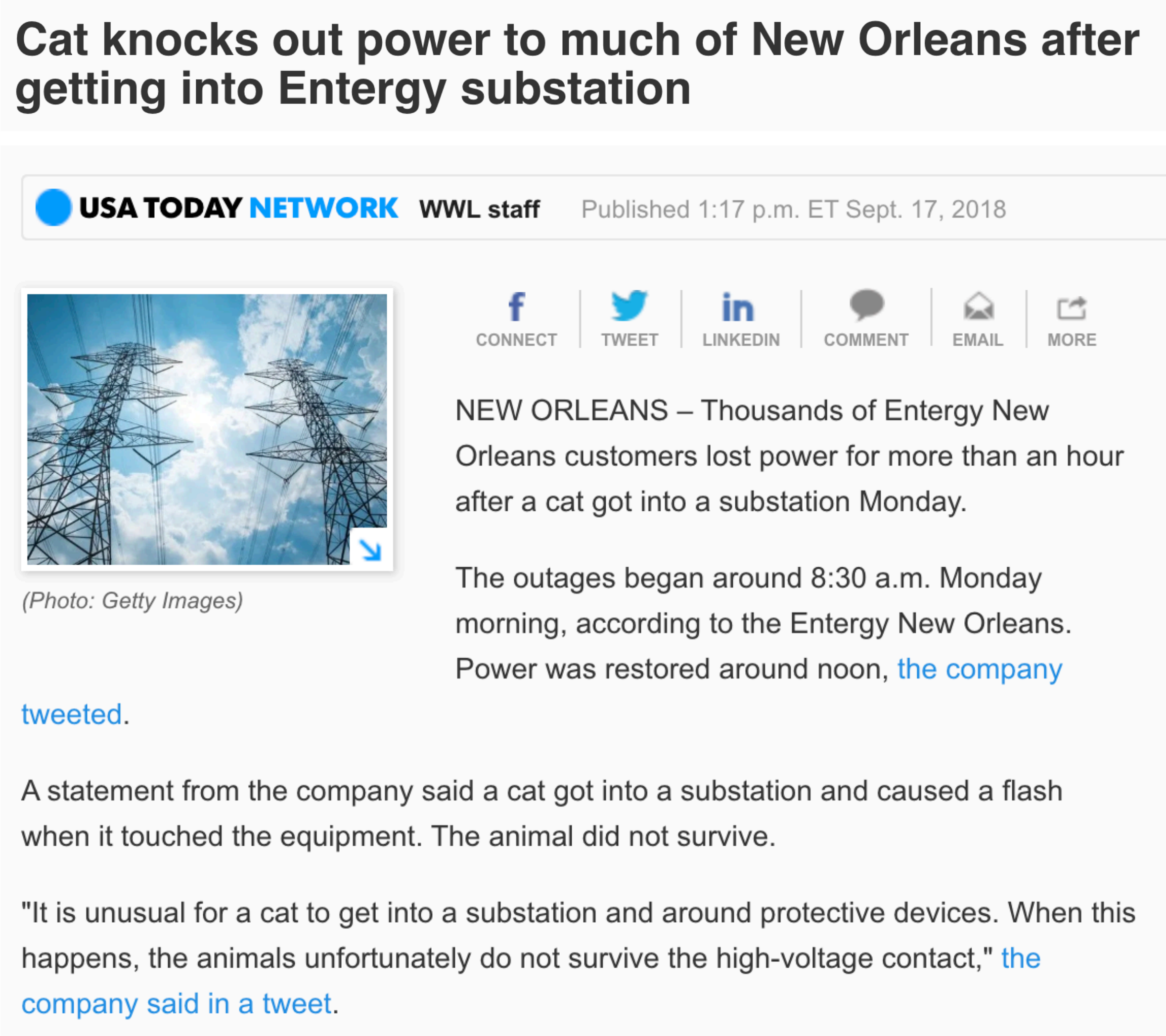
America’s Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It



Sources: documents; interviews with people at the affected companies, government officials and security-industry investigators

https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112

Animal Adversaries



Cat knocks out power to much of New Orleans after getting into Entergy substation

USA TODAY NETWORK WWL staff Published 1:17 p.m. ET Sept. 17, 2018

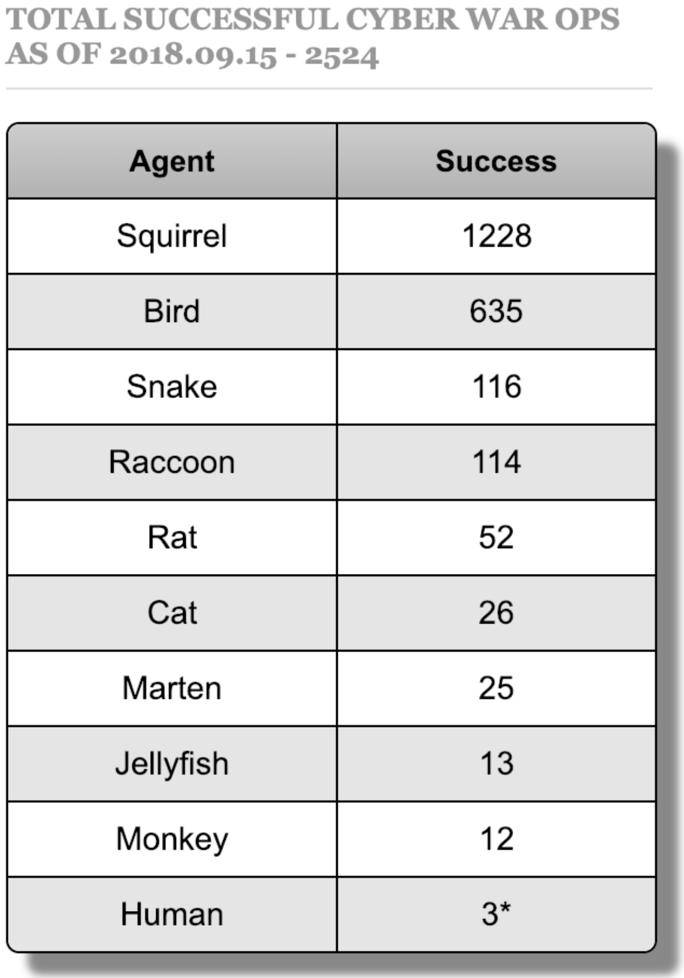
(Photo: Getty Images)

NEW ORLEANS – Thousands of Entergy New Orleans customers lost power for more than an hour after a cat got into a substation Monday.

The outages began around 8:30 a.m. Monday morning, according to the Entergy New Orleans. Power was restored around noon, the company tweeted.

A statement from the company said a cat got into a substation and caused a flash when it touched the equipment. The animal did not survive.

"It is unusual for a cat to get into a substation and around protective devices. When this happens, the animals unfortunately do not survive the high-voltage contact," the company said in a tweet.



TOTAL SUCCESSFUL CYBER WAR OPS
AS OF 2018.09.15 - 2524

Agent	Success
Squirrel	1228
Bird	635
Snake	116
Raccoon	114
Rat	52
Cat	26
Marten	25
Jellyfish	13
Monkey	12
Human	3*

Via Cyber Squirrel 1 Project

Changing Methodology

1. Traditional malware and exploits to access IT environment
2. Host-based monitoring, malware detection, EDR products improve
3. “Living off the Land”
4. Purpose-built malware

Things to Consider

- Motivations and consequences
- The US response to a cyberattack on the grid
  - “For any nation that’s taking cyber activity against the United States, they should expect…we will respond offensively as well as defensively,” National Security Adviser John Bolton

With Each Grid Hacker Media Story, Ask Yourself:

- Visibility: Where are they getting the story?
- Hype: Is this FUD? Hyperbolic wording vs. explanatory phrases
- Legitimacy: Is this a company quoted specializing in ICS security company, or a marketing effort/report?
- Evidence: What are their claims based on? What is the specified activity? Has this been reported before?
- Political motivations: Reports funded/supported by partisan groups.

RSA®Conference2019

Questions?

@selenalarson