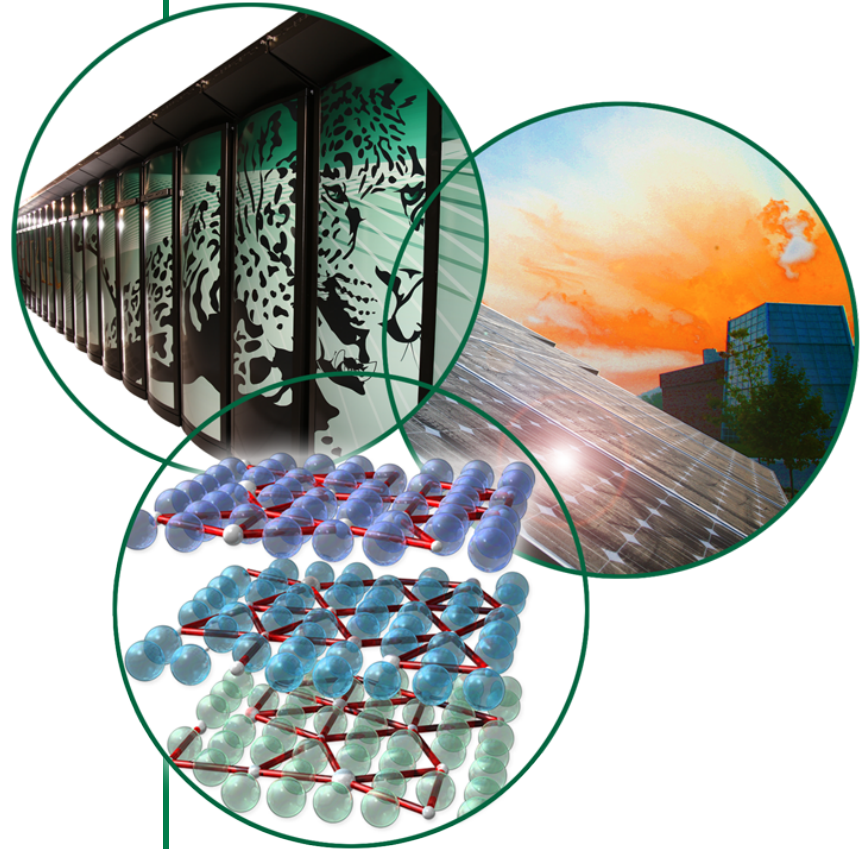


Protecting Accelerator Control Systems in the Face of Sophisticated Cyber Attacks

Steven Hartman

IPAC 2012

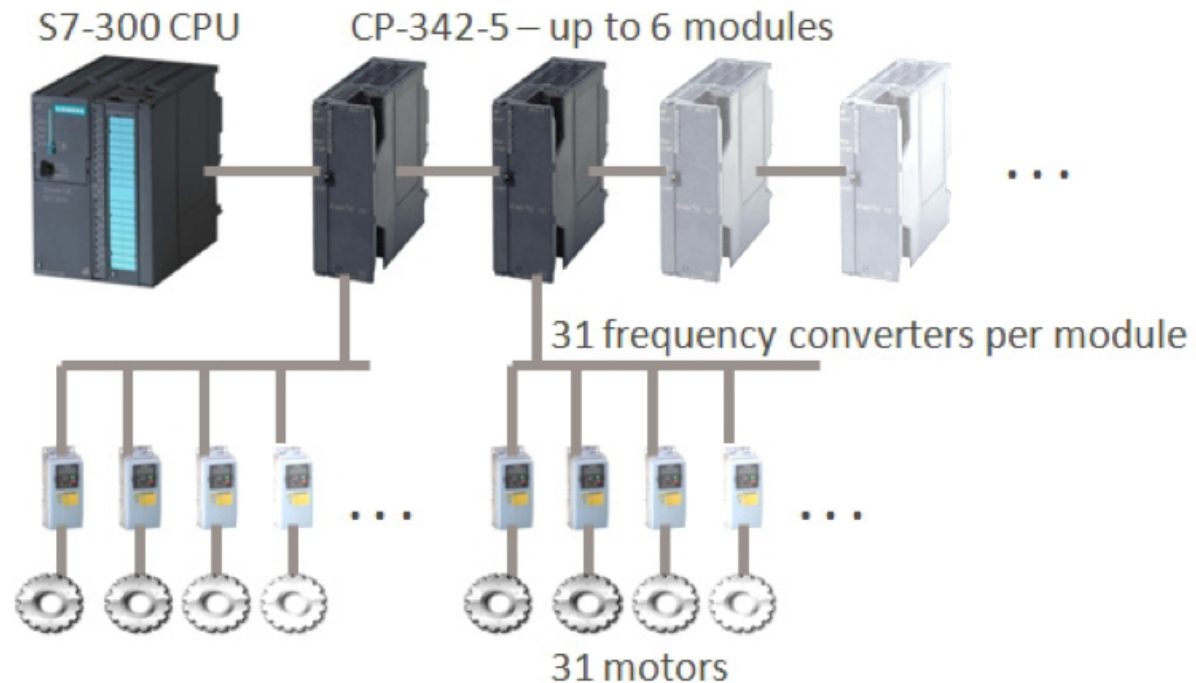


Stuxnet

PLC and Step7



Connections between sequence blocks



Diagrams: Symantec Stuxnet Dossier



Stuxnet cyberworm heads off US strike on Iran

Military option 'less likely' after computer sabotage, as Israeli tests are revealed on Natanz nuclear model

Ewen MacAskill in Washington

guardian.co.uk, Sunday 16 January 2011 15.19 EST



A partial view of the Dimona nuclear power plant in the southern Israeli Negev desert. Photograph: Thomas Coex/AFP/Getty Images

Hackers could spring killers from prison

Vulnerable: Computers used to remotely control the locks on prison cells

 Recommend 84

 Tweet 13

 +1 0

 Share 2

Below:  Discuss  Related

By Matt Liebowitz



updated 8/1/2011 3:40:05 PM ET

Print | Font:  A A + -

The high walls and barbed wire of a prison would seem to make security an open-and-shut case, but new research shows that hackers can exploit high-tech prison security systems to spring convicts from behind bars.

At this week's DefCon hacker conference in Las Vegas, [security](#) consultant John Strauchs will demonstrate how a hacker could take advantage of a prison's programmable logic controller (PLC) — small computers used for machine automation — to remotely control the locks on prison cells, [Wired](#) reported.



H(ackers)₂O: Attack on City Water Station Destroys Pump

615


109

116

 Tweet

 +1


 Share

By [Kim Zetter](#)  November 18, 2011 | 2:02 am | Categories: [Breaches](#), [Cybersecurity](#), [Hacks and Cracks](#)

 Follow @KimZetter

 Like

 Send

 810 likes. [Sign Up](#) to see what your friends like.




WIRED



Hackers gained remote access into the control system of the city water utility in Springfield, Illinois, and destroyed a pump last week, according to a report released by a state fusion center and obtained by a security expert.

The Washington Post

Water-pump failure in Illinois wasn't cyberattack after all

Text Size |  Print |  E-mail |  Reprints

By Ellen Nakashima, Published: November 25

A water-pump failure in Illinois was initially mistaken to be the first foreign cyberattack on a public utility in the United States because a plant contractor traveling in Russia remotely logged in to the plant's computer system, according to a person familiar with a federal investigation of the incident.

Investigators analyzed log files and connections to foreign Internet protocol addresses within the utility's computer system, said the source, who was not authorized to speak for attribution. "No indictors of malicious activity were found" in the computer system of the Curran-Gardner Townships Public Water District in Springfield, the source said.

SEE
ORNL
TODAY



ORNL April 2011

Manage Account | Mobile | Contact Us | About Us | Site Map | Subscriptions/TV Week

knoxnews.com

News Sports Business Opinion Entertainment Lifestyles

Jobs Homes Cars Classified

Today's Media Local Weather Obituaries Community Archives

knoxnews.com blogs » Frank Munger's Atomic City Underground



Cyber attack forces ORNL to shut down Internet access; experts probing Advanced Persistent Threat

A highly sophisticated cyber attack – known as Advanced Persistent Threat or APT – forced Oak Ridge National Laboratory to shut down all Internet access and email systems over the weekend.

Those restrictions will remain in place until lab officials and others investigating the attack are sure the situation is well controlled and manageable, ORNL Director Thom Mason said today.

Mason said he expects that email functions may be restored Tuesday on a limited basis, with no attachments allowed and restrictions on length. He said he couldn't speculate on when Internet access will be restored fully, even though

securitynews
DAILY

Alerts!

Cybercrime

Home & Auto

Identity Theft

Internet Scams

Malware/Virus

Cyberattack Hits Oak Ridge National Laboratory

Apr 19, 2011 | 4:07 PM ET | By Matt Liebowitz, SecurityNewsDaily Staff Writer

Tweet

17

Like

3

SHARE



One of the main servers of the Oak Ridge National Laboratory (ORNL) was taken offline this past Friday (April 17) after the government lab was hit by a sophisticated cyberattack that tried to steal [data](#) and gain remote access to sensitive systems.

External traffic from the server that powers the website ORNL.gov was shut down at about 7 p.m. on Friday after officials noticed unusual Internet traffic that appeared to be stealing data from the ORNL servers, the Knoxville

IT Security & Network Security News

DOE Lab Shuts Down Email, Web Access After Sophisticated Cyber-Attack

 LinkedIn 7  Twitter 29  Facebook 1  +1 0  Share

By: Fahmida Y. Rashid
2011-07-06

[There are 0 user comments on this IT Security & Network Security News & Reviews story.](#)

Cyber-attackers hit another Department of Energy research laboratory last week, forcing IT managers to shut down all of the facility's computer links to the outside world to try to contain the damage.

Essential computer [services](#) remain offline nearly a week after a cyber-attackers hit another Department of Energy laboratory, this time in the state of Washington.

The Energy Department's Pacific Northwest National Laboratory in Washington shut down Internet access and email services following a sophisticated cyber-attack, according to a July 5 post on the [facility's Twitter account](#). Officials became aware of the cyber-attack on July 1, Greg Koller, the lab's spokesperson, told the Associated Press.

Energy lab restoring website, investigating attack

◦ By William Jackson ◦ Jul 07, 2011

The Energy Department's Jefferson Lab nuclear research facility is back online and in the process of restoring its website as officials investigate the cyberattack that took the site off-line over part of the July 4 holiday weekend.

"We have a partial website up" at www.jlab.org, said public affairs manager Dean Golembeski. "We are still in the process of evaluating what happened."

The Thomas Jefferson National Accelerator Facility in Newport News, Va., also known as the Jefferson Lab, came under attack July 1, along with the Pacific Northwest National Laboratory in Washington state. PNNL shut down all network access July 1 but began restoring internal communications over the weekend. External e-mail at PNNL was restored on the afternoon of July 6, but the lab's website remained off-line as of today.



Advanced Persistent Threat

NETWORKWORLD

News | Blogs & Columns

Security

LANs & WANs

UC / VoIP

Cloud Computing

Infrastructure

Anti-malware

Compliance

Cybercrime

Firewall & UTM

IDS/IPS

APT Dot Gov: Protecting Federal Systems from Advanced Threats

October 2011

A SANS Whitepaper

Written by: G. Mark Hardy

What is an 'Advanced Persistent Threat,' anyway?

Hint: 'Advanced Persistent Threat' muscling into security lexicon

By [Ellen Messmer](#), Network World

February 01, 2011 06:02 AM ET



Targeted Attacks Increased, Became More Diverse in 2011

The latest Internet Security Threat Report by Symantec finds that targeted attacks are becoming more common and are going beyond the public sector and large enterprises to smaller, less well defended companies in the supply chain and partner ecosystem.

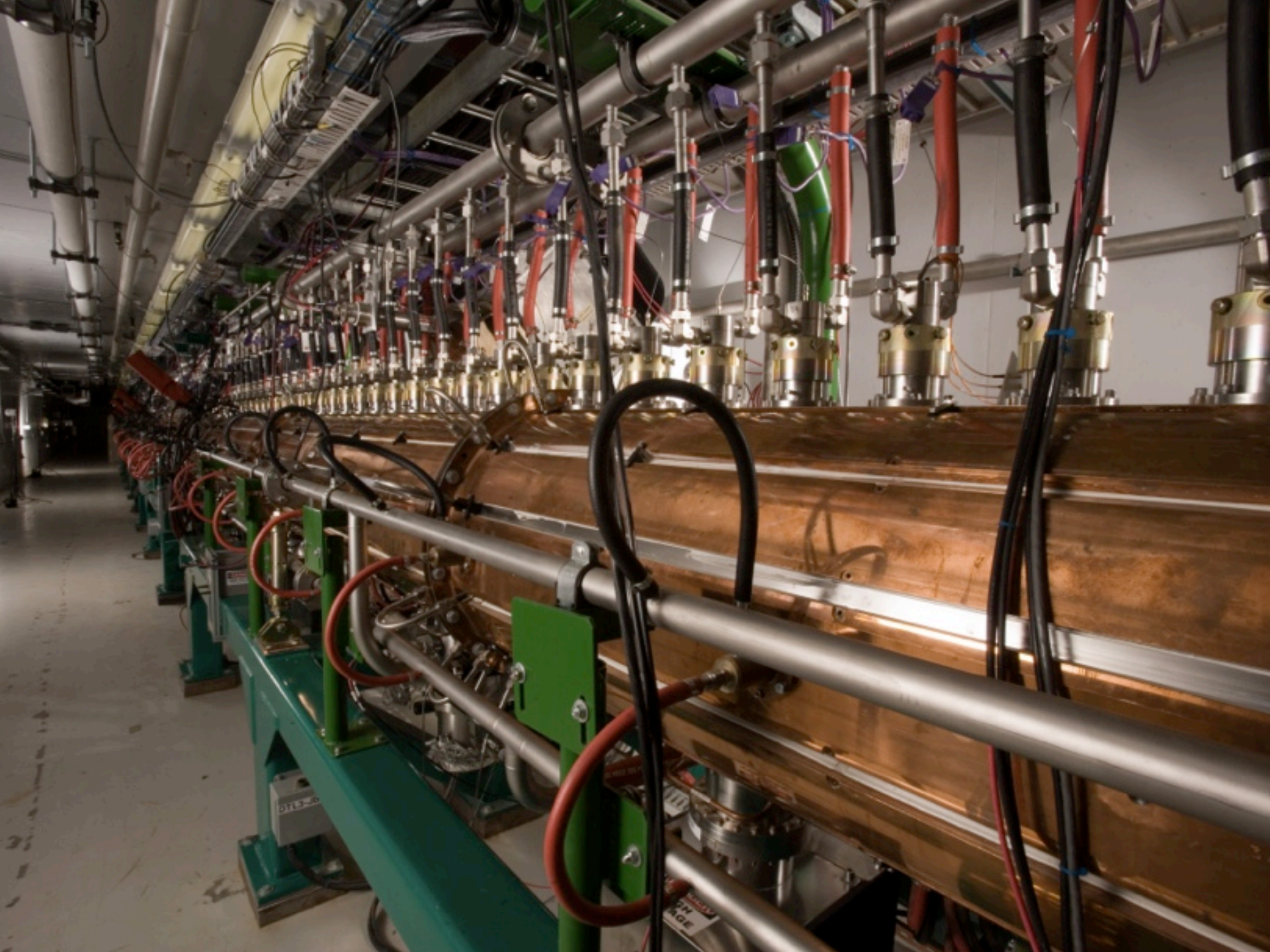
By Thor Olavsrud
Mon, April 30, 2012

Add a comment



+ Briefcase

What's this?



[Home](#) » [Blogs](#) » [News Blog](#) »



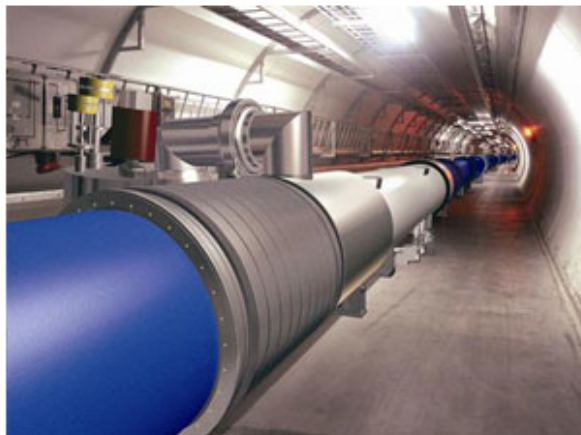
News Blog

[More Blogs ▾](#)

Hackers attack Large Hadron Collider computers to prove they're vulnerable

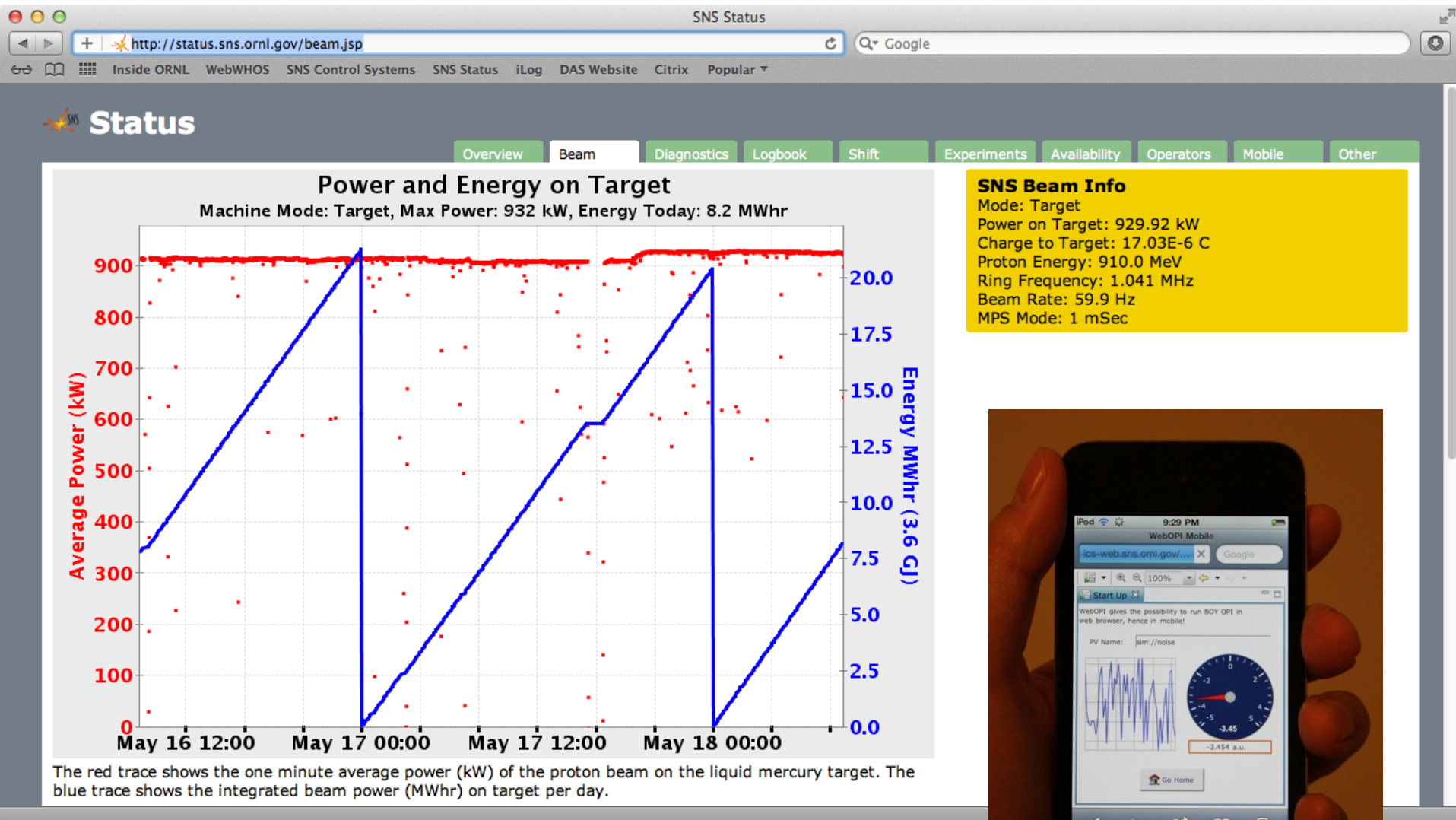
By [Larry Greenemeier](#) | Sep 12, 2008 03:32 PM | 13

[Share](#) [Email](#) [Print](#)




As the first particles began circulating in the [Large Hadron Collider \(LHC\)](#) this week, a group of hackers calling themselves the "Greek Security Team" penetrated computer systems inside [CERN's Geneva, Switzerland, facility](#), where the world's biggest particle accelerator is housed, the [Telegraph.co.uk](#) reported today.

Remote Access



Everyone Has Been Hacked. Now What?

By Kim Zetter  May 4, 2012 | 7:22 pm | Categories: [Breaches](#), [Cybersecurity](#)

 Follow @KimZetter


844

97

171


 Tweet

 +1

 Share

 Like

 Send

 698 likes. [Sign Up](#) to see what your friends like.

WIRED



Oak Ridge National Laboratory was hit by a targeted hacker attack in 2011 that forced the lab to take all its computers offline. *Photo: Oak Ridge National Laboratory*


OAK
RIDGE
National Laboratory

Questions and Comments

