



XXX-hacker TEAM

XXX~HACKER TEAM ZONE-H DARK-H Contact

«» [Hacked By:] «»
4Ri3 Gondrong



f Share



Tweet



5th Control System Cyber-Security Workshop

- Exchanging ideas on HEP++ security

THREE CLICKS AND WE WERE IN CERN'S PRIVATE WEBSITE

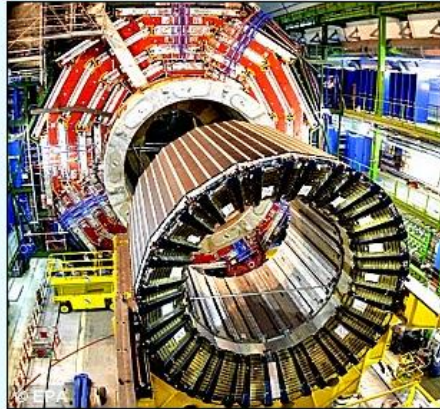
The Shodan search engine is so powerful, it could even put the world's most expensive science experiment at risk.

By searching the site's 'most popular' searches, reporters at The Mail on Sunday were able to find out the internet location of the home of the Large Hadron Collider, the world's largest particle accelerator.

Three clicks can take visitors from the site's homepage to what appears to be the internal website for CERN, the European Organization for Nuclear Research, and pages unavailable on the web.

CERN's computer team warns employees: 'CERN is permanently under attack' and in 2008, security was breached when CERN was hacked by a group called the 'Greek Security Team'.

Fortunately, no harm was done.



Hacking risk: CERN's Large Hadron Collider in Switzerland



April 3rd 2015. Re: Death threats posted on dark net regarding upcoming CERN high energy experiment

Dear [REDACTED]

I regret to inform you that your life may be in danger if you are one of the seven men that have been pushing for higher energy particle collision experiments at CERN.

Due to warnings by prominent theoretical physicists like Dr. Stephen Hawking that your proposed higher energy particle collision experiments could create a singularity that destroys our universe, combined with anonymous theoretical physicists with no financial stake in CERN's continued operations all making the same dire predictions, some anonymous individuals have become convinced that the only way to save our universe from destruction is to kill these 7 men, of which, unfortunately, you may be one.

Some of our members have also run our own highly advanced Temporal Derivative Predictive Modeling calculations which suggest that your new higher energy particle collision experiments might create a singularity that destroys our universe in less than 6 days! A shockingly short period of time that has forced certain highly radicalized individuals within our group to take much more drastic actions that they would typically feel comfortable with.

The probability of CERN destroying our universe in 6 days is reportedly "1 in 100,000", which, I hope you will agree, is unacceptably high. Based on the fear that vested interests in CERN staying operational may nevertheless allow these high energy particle collision experiments to move forwards, some of my colleagues may have arranged for you to be killed as a way of delaying these higher energy collision experiments occurring over the next 6 days, and buying us some time to lobby the relevant powers that be to get a cap on the maximum amount of power you are allowed to use in your current and future particle collision experiments. Any risk, even "1 in 100,000" is too much when you are talking about experiments with the potential to destroy our universe, I hope you will agree.

I apologize for the confusion and ugliness death threats such as these often cause. I am working with my colleagues to try to remove the "hits" that have been placed and will do everything in my power to fix this mess.

Your humble servant, Lord Jim Rothschild

All warning emails now sent. I will post a confirmation as soon as I get a chance to talk to our misguided brother and get these hits cancelled. As for #LordSatan, with this most recent display of terror and evil I am going to have to put you on a final warning. If you order any more hits without discussing it with us here or Mirror666 than I promise you that I will do everything in my power to find you and put you to the knife. This is your final warning psychopath. Jim

CERN update 11PM: I have an update on the #CERN situation. #LordSatan spoke to Joshua, who was based in London, England and convinced him that 7 of the CERN scientists needed to die or Joshua's family and indeed all life would all die within 6 days. I didn't find out the identity of the men at CERN who are being targeted, but I did manage to speak to Joshua briefly via the dark net and he is 100% refusing to stop, he has officially ignored your formal order to cancel the 7 hits, and he is refusing to speak with you or anyone else. Satan has him completely convinced he needs to kill these 7 men ASAP and will not obey YOUR DIRECT ORDER to stop. Jim, Joshua has betrayed us, and the penalty for betrayal under the ancient law is death. I have already spoken to an associate in Paris who knows where Joshua will be tomorrow night (4/4) and on the night of the Blood Moon she will sacrifice Joshua for our sins. - #GoddessIshtar





C3 ~ RET
@c3retc3

 Follow

#CERN discloses passwords, source code and tickets to Web spiders

6:03 a.m. - 29 Sep 2015



C3 ~ RET @c3retc3 · 2h
[@c3retc3](#) There are 150 Oracle DB hosts at least!



Kate Kahle @katekahle · 2h
[@c3retc3](#) Thanks for the heads-up! What about sharing details with us via [Computer.Security\[at\]cern.ch](mailto:Computer.Security[at]cern.ch)?



C3 ~ RET @c3retc3 · 51m
[@katekahle](#) Surely I will write you. You have really surprised me with the reaction - glad to see this approach to security of the org.





DATA CENTRE SOFTWARE NETWORKS SECURITY INFRASTRUCTURE BUSINESS HARDWARE SCIENCE

Security

Ruskie ICS hacker drops nine holes in popular Siemens power plant kit

WinCC HMI control platform used in Natanz, Large Hadron Collider.

This week's sponsor: The 2015 Industrial Control Systems (ICS) Cyber Security Conference

If you look after the Large Hadron Collider you should read this...

Graham Cluley | September 3, 2015 9:21 am | Filed under: Vulnerability | 0

23 10 5 6

A Russian security researcher has uncovered security vulnerabilities that could allow a malicious attacker to conduct man-in-the-middle attacks, denial-of-service attacks, and possibly authenticate themselves as valid users.

So far, so much par for the course.

But what makes this vulnerability disclosure by Ilya Karpov of Positive Technologies particularly noteworthy, as *The Register* reports, is that the vulnerabilities were found in Siemens SIMATIC HMI devices used to control critical systems at petrochemical facilities, power plants and even the Large Hadron Collider.

Yes, you can imagine how that could cause problems...



This site uses cookies [That's fine](#) [More info](#)



Traffic Hacking: Caution Light Is On

By NICOLE PERLROTH JUNE 10, 2015 6:29 PM 4 Comments

Global nuclear facilities 'at risk' of cyber attack

5 October 2015 | Technology **BBC**

The Switch



Could hackers take down a city?

arstechnica

MAIN MENU MY STORIES: 1 FORUMS SUBSCRIBE JOBS

Ars Technica has arrived in Europe. [Check it out!](#)

RISK ASSESSMENT / SECURITY & HACKTIVISM

Fiat Chrysler "connected car" bug lets hackers take over Jeep remotely

Exploits demonstrated for Wired included shutting engine, brakes off.

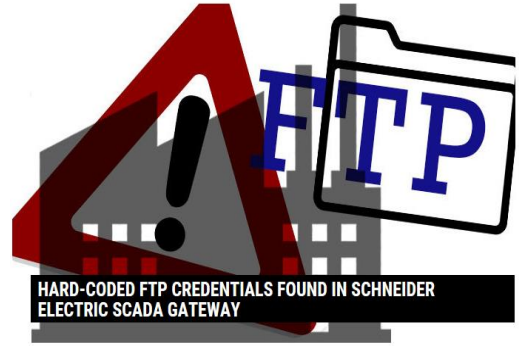
by Sean Gallagher - Jul 21, 2015 5:22pm CEST

Share Tweet 142



Hacking Baby Monitors is dramatically easy

September 3, 2015 By Pierluigi Paganini



by Dennis Fisher Follow @dennisf

January 21, 2015, 10:17 am



COMPUTERWORLD Popular Now: [dropdown]

Home > Security > Cybercrime & Hacking



SECURITY IS SEXY

By Darlene Storm Follow

About

Most security news is about insecurity, hacking and cyber threats, bordering on scary. But when security is done right, it's a beautiful thing...sexy even. Security IS sexy.

NEWS ANALYSIS

Hack to steal cars with keyless ignition: Volkswagen spent 2 years hiding flaw



5th Control System Cyber-Security Workshop
Dr. Stefan.Lueders@cern.ch
October 18th 2015, Melbourne (AUS)

From the Newsroom...

- All security aspects related with HEP control systems
- Control PCs, control software, controls devices, accounts, ...
- Planning / implementation / operational aspects ...

- Raise awareness
- Exchange of good practices, ideas, and implementations
- Discuss what works & what not, pros & cons
- Report on security events, lessons learned & successes
- Update on the progress made since the last workshop

- **If there are questions, feel free to ask at anytime!!!**
- **The agenda is flexible to accommodate any changes!**

	Introduction to the 4th Control System Cyber-Security Workshop	<i>Dr. Stefan LUEDERS</i>
	<i>Room 108, Melbourne Convention and Exhibition Centre (MCEC)</i>	09:30 - 09:45
	Centralized configuration of Role-Based authentication in JCOP Framework	<i>Lorenzo MASETTI</i>
10:00	<i>Room 108, Melbourne Convention and Exhibition Centre (MCEC)</i>	09:45 - 10:15
	Coffee Break	
	<i>Room 108, Melbourne Convention and Exhibition Centre (MCEC)</i>	10:15 - 10:45
	DAQ control system for multi-beamline simultaneous experiments at SACLA	<i>Takashi SUGIMOTO</i>
11:00	<i>Room 108, Melbourne Convention and Exhibition Centre (MCEC)</i>	10:45 - 11:15
	Cyber Security Assessment of the Spallation Neutron Source at Oak Ridge National Laboratory	<i>Karen WHITE</i>
	<i>Room 108, Melbourne Convention and Exhibition Centre (MCEC)</i>	11:15 - 11:45
	Testing device robustness with fuzzing	<i>Brice COPY</i>
12:00	<i>Room 108, Melbourne Convention and Exhibition Centre (MCEC)</i>	11:45 - 12:15
	Finding Our Skeletons: Information Security Assessment of CERN Access and Safety Systems	<i>Timo HAKULINEN</i>
	<i>Room 108, Melbourne Convention and Exhibition Centre (MCEC)</i>	12:15 - 12:45
	Lunch Break	
13:00	<i>Room 108, Melbourne Convention and Exhibition Centre (MCEC)</i>	12:45 - 13:45
	5 Challenges Securing the LHC	<i>Stefan LUEDERS</i>
14:00	<i>Room 108, Melbourne Convention and Exhibition Centre (MCEC)</i>	13:45 - 14:15
	Discussions	<i>Dr. Stefan LUEDERS</i>
15:00	<i>Room 108, Melbourne Convention and Exhibition Centre (MCEC)</i>	14:15 - 15:15
	Coffee Break	
	<i>Room 108, Melbourne Convention and Exhibition Centre (MCEC)</i>	15:15 - 15:45

<https://indico.cern.ch/event/348695/>

