MUST READ Facebook wins Flash by knock out by switching to HTML5!

Iranian hackers penetrated computers of a small dam in NY

December 22, 2015 By Pierluigi Paganini

G+1 3
My Page Like 6

Iranian hackers penetrated the industrial control system of a dam near New York City in 2013, raising concerns about the security of US critical infrastructure.

It is official, Iranian hackers violated the online control system of a New York dam in 2013. According to reports, the hackers penetrated the control system of the dam and poked around inside the system.

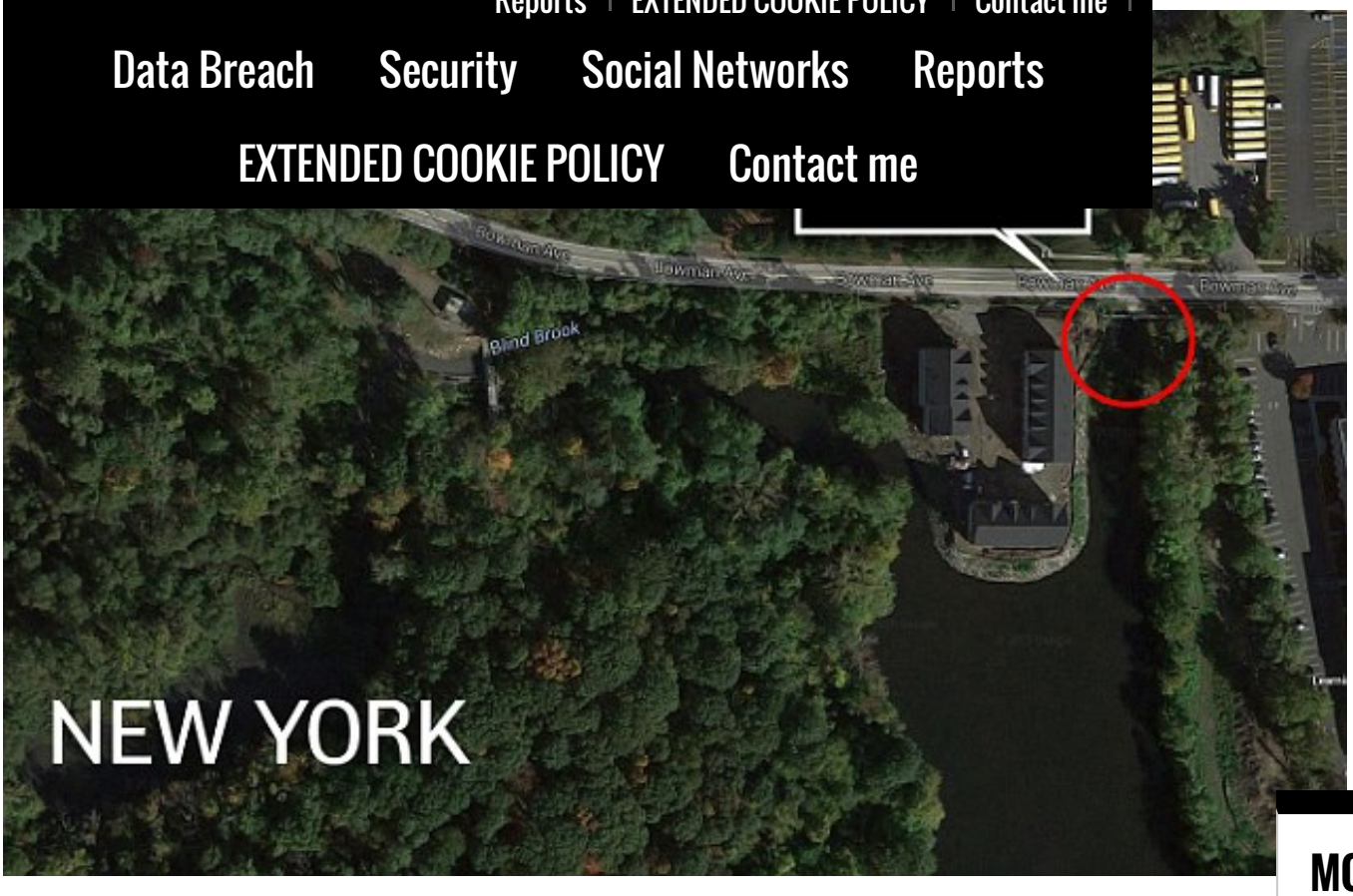
The *Wall Street Journal* reported that hackers penetrated the system of the critical infrastructure through a cellular modem. The Journal cited an unclassified Homeland Security summary of the case. At the time I was writing the Department of Homeland Security has declined to comment on the cyber attack.

The *Wall Street Journal cited to anonymous* sources that revealed the hackers targeted the Bowman Avenue Dam, which is a small facility 20 miles outside of New York.

"It's very, very small," Rye City Manager Marcus Serrano told the newspaper, confirming that FBI agents investigated the case in 2013.

Fortunately, the intruders were not able to gain complete control of the control systems. The hackers used a machine that scanned the Internet for vulnerable US

l systems (ICS)
ange of



The US cyber experts once discovered the attack have tracked back the intruders, the evidence collected suggests the involvement of Iranian hackers, probably the same groups that focu their operations on American companies and organizations.

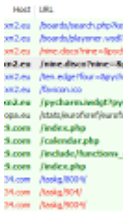
Exactly one year ago, the experts at security firm Cylance revealed that Iranian hackers were targe airlines, energy, defense companies worldwide as part of the Operation Cleaver campaign.

The fact that foreign hackers target US critical infrastructure is not a novelty, a report issued by Th Department of Homeland Security (DHS) in November 2014 revealed that Russian hackers have infiltrated several critical infrastructure in the United States.

The US has the highest number of ICS and SCADA systems exposed on the internet and many of th are easily identifiable with search engines like Shodan or Censys. Researchers at Shodan recently revealed that the US have nearly 57,000 industrial control systems connected to the Internet.

A recent wave of attacks conducted by Iranian hackers came after a period of apparent calm. The cy security experts noticed an evolution of the TTPs of the Iranian hackers that were initially focused

MORE S



Angler
code o

A securit
variant o

This website uses cookies to improve your experience. We'll assume you're ok with this, but you can opt-out if you wish. Accept Read More

The recent attacks against The State Department attack is clearly a cyber espionage operation, they were initially attributed to Chinese hackers who may have infiltrated the department's unclassified e-mail systems. Let's remind that security experts at Facebook were first noticed the intrusion of Iranian Hackers in the e-mail accounts of US State Department officials focused on Iran.

Needless to emphasize the importance of activities of threat intelligence to prevent these accidents and mitigate cyber threats.

Pierluigi Paganini

(Security Affairs –Iranian hackers, critical infrastructure)

Share it please ...

1. Best Internet Security
2. Enterprise Network

SHARE ON

Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security)Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and "Digital Virtual Currency and Bitcoin".

PREVIOUS ARTICLE
Angler exploit kit includes the code of a recent Flash flaw

Promote your solution on Security Affairs

Copyright 2015 Security Affairs by Pierluigi Paganini All Right Reserved.