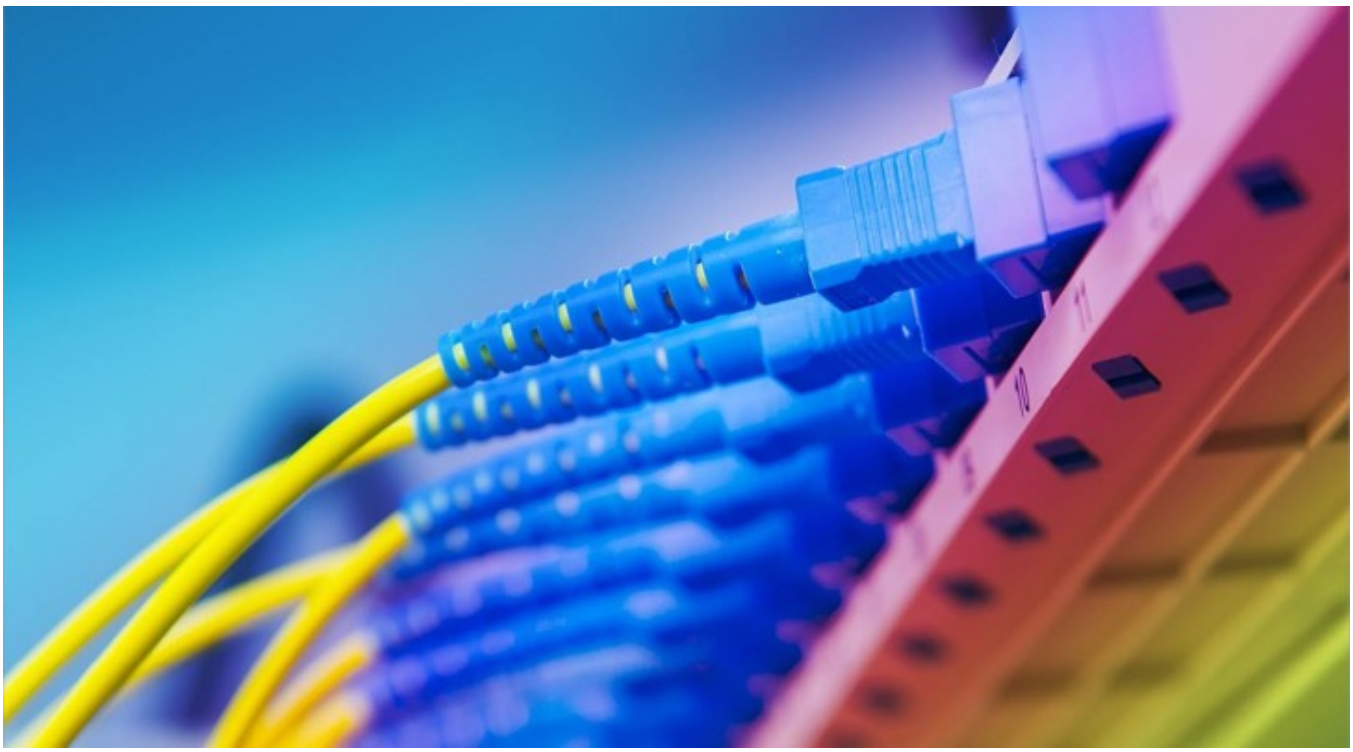

New attacks on critical communications infrastructure in the US

September 21, 2015 By Pierluigi Paganini

Unknown attackers continue to target critical communications infrastructure in the US, on Monday they cut backbone fiber optic Internet cables in California.

Unknown attackers continue to target critical communications infrastructure in the US, on

California. This is not an isolated attack, law enforcement counted fourteenth attacks on critical communications infrastructure in the same region and security experts suspect that the attackers are carrying our the sabotage for economic and cyber warfare.

"These cuts affected multiple companies causing outages in some of the Bay area and stretched up into the Sacramento area," said FBI Special Agent Greg Wuthrich in an email.

The investigation on such kind of attacks is conducted by the FBI because AT&T's fiber optic network is considered to be part of the nation's critical communication infrastructure.

"Someone deliberately severed two AT&T fiber optic cables in the Livermore, Calif., Monday night, the latest in a string of attacks against the Internet's privately run backbone.*" reported the USA Today website adding that AT&T is offering a 250,000 dollar reward for information on the attack.*

Due to the attack to the communications infrastructure, Internet and phone services in Sacramento, California, were interrupted for twenty hours.

Who is behind the attacks?

Security experts consider superficial the definition of "Vandals," part of the security community believes that the motivation could be more dangerous, such as sabotage or cyber espionage.

Targeting critical infrastructure such as communications, grids, and power supplies are a consolidated strategy to cause large-scale damages to the target. According to the Lloyd's of London, cyber attacks would have a significant impact on multiple types of insurance, its report "Business Blackout", analyzed the implications of a cyber attack on the US power grid.

The *"Business Blackout"* report tries to describe the impacts of a cyber attack on the national po grid, which causes an electrical blackout that plunges 15 US states and principal cities, including New York City and Washington DC, into darkness. Nearly 93 million people will remain without power in the scenario hypothesized by the study.

The total of claims paid by the insurance industry is estimated to be included in the interval comprised between $21.4bn and $71.1bn, depending on the evolution of the scenarios designe the researchers.

In 2013 the FBI investigated the attack on the PG&E electrical substation in Metcalf California, security experts hypothesized that cells of terrorists were probing the incident response in case of attack. The knowledge of the response times of the internal staff and authorities could suggest the attackers the tactic to adopt to cause major damage.

"The case of the Metcalf substation showed the sophisticated planning and targeting of a military special operation. It was the cutting of telephone cables that precluded the assault rifle attack on the cooling encasement of a high voltage transformer that distributed power to Silicon Valley which was meant to keep alarm signals from reaching critical personnel." continues the USA Today.

Most of all of these recent attacks on US critical infrastructure occurred on the West coast, but almost identical acts of sabotage were reported in Arizona this February when unknowns targeted Internet cables. In 2014, a bomb exploded at the Nogales substation that provides power supply at the U.S. Border Patrol facilities at the Nogales U.S./ Mexican border.

Intelligence analysts speculate that the attacks in the greater San Francisco and San Jose areas can be interpreted as acts of economic warfare conducted by Russia or China.

The San Francisco area and Silicon Valley are considered privileged targets for cyber espionage, by compromising communications infrastructure attackers can have access to the data traffic and syphon sensitive information, or can inject in the targeted networks malicious code to steal intellectual property.

Stay tuned.

Pierluigi Paganini

(Security Affairs – communications infrastructure, critical infrastructure)

California communications infrastructure critical infrastructure cyber espionage Sabotage Silicon Valley

Breaking News Cyber Crime Cyber warfare Security

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

3 flaws in StarBucks websites open its users to attacks

NEXT ARTICLE

New updates on Cyber Conflict Agenda 2016 and what's new in 'Cyber power'

YOU MIGHT ALSO LIKE

The DUKES APT – 7 years of Russian state sponsored hacking

September 17, 2015 By Pierluigi Paganini

Operation Iron Tiger, hackers target US Defense Contractors

September 17, 2015 By Pierluigi Paganini