Nitro Zeus

Nitro Zeus is the project name for a well funded comprehensive cyber attack plan created as a mitigation strategy after the Stuxnet malware campaign and its aftermath.[1] Unlike Stuxnet, that was loaded onto a system after the design phase to affect its proper operation, Nitro Zeus's objectives are built into a system during the design phase unbeknownst to the system users. This built-in feature allows a more assured and effective cyber attack against the system's users.[2]

The information about its existence was raised during research and interviews carried out by Alex Gibney for his *Zero Days* documentary film. The proposed long term widespread infiltration of major Iranian systems would disrupt and degrade communications, power grid, and other vital systems as desired by the cyber attackers. This was to be achieved by electronic implants in Iranian computer networks. [3] The project was seen as one pathway in alternatives to full-scale war.

See also

- Kill Switch
- Backdoor (computing)
- Operation Olympic Games

References

1. *Szoldra, Paul (2016-07-06). "The US could have destroyed Iran's entire infrastructure without dropping a single bomb" (http://uk.businessinsider.com/nitro-zeus-iran-infrastructure-2016-7) . Business Insider.*
2. *Alex Gibney Zero Days documentary film*
3. *Sanger, David; Mazzetti, Mark (2016-02-17). "US Had Cyberattack Planned if Iran Nuclear Negotiations Failed" (https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html) . New York Times.*

This malware-related article is a stub. You can help Wikipedia by expanding it (https://en.wikipedia.org/w/index.php?title=Nitro_Zeus&action=edit) .

Last edited 4 months ago by 2pou