Abstract

Due to their size and reputation, energy and utility companies have become a prominent target for hackers, who seek to sow panic among the general public. The threat stems from social and environmental hacktivists, in addition to politically-affiliated hackers, who attempt to gain control of industrial control systems, disrupt the network, or deface corporate websites. Recognizing the risk, energy and utility companies are creating multilayer security architectures and applying stringent security policies to withstand such assaults.

Recent Attacks

Research suggests that attacks are designed to overcome a victim's security architecture and may include denial of service attacks, website defacements, network intrusion and data theft. These attacks are often affiliated with physical or political conflict. The hackers associated with these attacks are often Anonymous-related hacktivists or state-sponsored APT groups conducting espionage.

Target List:

Gansu – Gansu Mining Company was recently targeted by Anonymous for mining and damaging a sacred Tibetan mountain in Tibet. As a result, the company's page was defaced. This attack is part of an ongoing operation under #Op_Tibet. This operation focuses on targeting companies that oppress Tibetans and cause environmental damage due to mining.

Future targets of this operation [i]include**:**

http://www.zhaojin.com.cn
http://www.zijinmining.com/
http://www.zjgold.com/
http://www.chinagoldintl.com/
http://www.westmining.com/

BCGold Corp – The BCGold website was targeted in March of 2016 by Anonymous under the revived operation, OpCanary. This operation focused on targeting multinational corporations involved in mining. BCGold's website was ultimately defaced with a video of Rick Astley's song, "Never Gonna Give You Up."

Goldcorp – In April of 2016, a Canadian gold-mining firm was hacked by an unknown group. The hack resulted in 14.8Gb worth of data being leaked. This data included contract agreements, bank accounts, employee passports and more. Little is known about why the hackers targeted this company, but it is similar to an attack on another gold mining company last year, Detour Gold.

Department of Resources and Energy – The Department of Resources and Energy in New South Wales, Australia was hacked in an attempt to gain access to commercially sensitive data related to mining. While there is no evidence suggesting who was behind the attack, some speculate this was a targeted attack by Chinese hackers in an attempt to gain access to intellectual property and other information.

Attack Vectors

- **Defacement** – A website defacement is like digital graffiti. An attacker will change the visual appearance of the website by breaking into a web server and replacing the current website with one of their own. This attack is most commonly associated with SQL Injections. This form of an attack allows administrative access so that the hacker can make the required changes. Another way this is preformed is via FTP if the user's credentials have been obtained.

- **SQL Injection** - This technique takes advantage of poor application coding. When the application inputs are not sanitized, it becomes vulnerable. Attackers can modify an application SQL query to gain access to unauthorized data with administrator access, run remote commands on the server, drop or create objects in the database, and more.

How to Prepare

Political and ideological-driven attacks such as these can be difficult to avoid. Radware's hybrid attack mitigation solution provides a set of patented and integrated technologies designed to detect, mitigate and report today's most advanced threats. Dedicated hardware and cloud solutions protect against attacks in real time and help ensure service availability.

With Radware, companies can protect their infrastructure from multi-vector attacks, network and application-based DDoS attacks as well as volumetric attacks that may saturate the Internet pipe or result in defacement and information-loss. Radware solutions include proven protection mechanisms from the vectors listed above.

Organizations Under Threat Should Consider

- A security solution that can protect its infrastructure from multi-vector attacks, including protection from network and application-based DDoS attacks as well as volumetric attacks that can saturate the Internet pipe
- A hybrid solution that includes on-premise detection and mitigation with cloud-based protection for volumetric attacks. This provides quick detection, immediate mitigation and protects networks from volumetric attacks that aim to saturate the Internet pipe.
- A solution that provides protection against sophisticated web-based attacks and website intrusions to prevent defacement and information theft.
- A cyber security emergency response plan that includes an emergency response team and process in place. Identify areas where help is needed from a third party.
- Monitor security alerts and examine triggers carefully. Tune existing policies and protections to prevent false positives and allow identification of real threats if and when they occur.

Protection from SQL injections and web application vulnerabilities:

- IP-agnostic device fingerprinting - having the ability to detect attacks beyond source-IP using by developing a device fingerprint that enables precise activity tracking over time.
- Automatic and real-time generation of policies to protect from zero-day, unknown attacks.
- Shortest time from deployment to a full coverage of OWASP Top-10.

Radware's hybrid attack mitigation solution provides a set of patented and integrated technologies designed to detect, mitigate and report the most advanced threats. Dedicated hardware and cloud solutions protect against attacks in real time and help ensure service availability.

Under Attack and in Need of Expert Emergency Assistance? Radware Can Help.

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, Contact us with the code "Red Button".

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.

---

[i] http://pastebin.com/Z7ey1JMh