Abstract

The Dakota Access Pipeline Project (DAPL) is the construction of a 1,172-mile-long pipeline that will span across three states. Domestic production of light sweet crude oil in North Dakota will be transported in the pipeline to a major refining market in Illinois. Construction has provoked protests from dozens of Native American tribes. Cyber-activist group Anonymous is launching operations in solidarity with the Native American tribes whose land is to absorb the environmental ramifications of the construction. Anonymous has been running reconnaissance and vulnerability analysis against their targets, launching denial of service attacks and posting details about those involved with the pipelines construction.

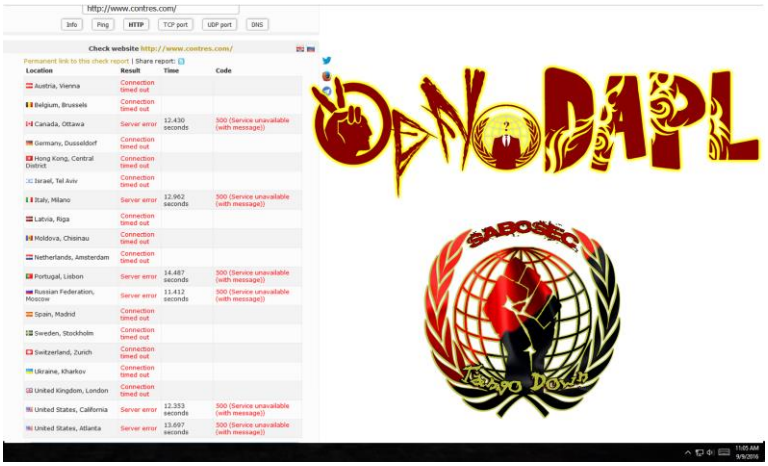

Figure 1: Anonymous attacks Continental Resources

Background

Native American tribes fear that the pipeline's construction will disrupt sacred grounds and contaminate their drinking water. Last week things turned violent when security contractors confronted protestors with dogs which lead to several injuries as a result. Finding the media coverage of the protestors unfair, Anonymous announced its support for the protestors (despite requests to stay away), and began posting personal details of officials involved with the pipeline project, threatening the employees and the families of those involved – calling them to quit.

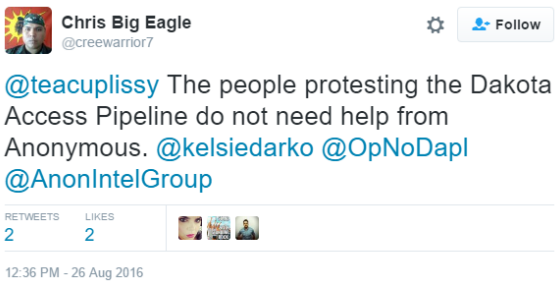

Figure 2: Protestors declare they do not need help from Anonymous

Targets

- Energy Transfer
- Halliburton
- Mortonnd
- Brakkenshale
- EnergyCorp
- Keystone XL

- National guard
- CitiGroup
- TD
- Mizuho
- Sunoco
- Phillips 66
- Frost Kennels

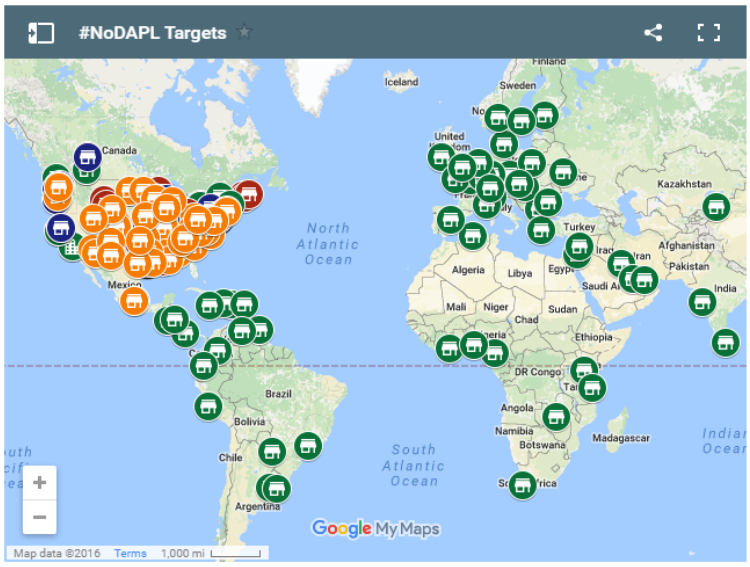

Figure 3: Target map of organizations involved with DAPL

Attack Methods

Anonymous' current motto is "Find a target – take action" and it has launched a series of denial of service attacks against state and corporate network operations, as well as personal attacks against officials. Hacktivists are currently using Nikto, Nmap and SQLmap to analyze and map their targets' network and applications vulnerabilities. Personal information of those involved is posted on social networks once obtained. In parallel, online tools like Robtex and Censys are used to discover more information in preparation for DDoS attacks. Anonymous have published their target lists on Pastebin.

Examples

- https://www.robtex.com/en/advisory/dns/mil/army/ngb/ndguard/www/
- https://www.robtex.com/en/advisory/dns/com/halliburton/www/
- https://www.robtex.com/en/advisory/dns/mil/army/usace/www/

Network Scans

- Mortonnd.org http://pastebin.com/DLBM6wF9
- Energy transfer Partners http://pastebin.com/2SpLqz2i / http://pastebin.com/kYBUd9eJ
- Halliburton http://pastebin.com/BKcUnfhN
- Frost Kennels http://pastebin.com/haJWHL11

Real-Time Updates - Twitter: https://twitter.com/OpNoDapl, IRC: irc.anonrising.xyz/6697 #OpNoDapL

Scanning Tools

Nmap – Nmap is a security scanner designed for network discovery and security auditing. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services

(application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.[i]

Nikto - an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated.[ii]

SQLmap - SQLmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.[iii]

Effective DDoS Protection Considerations for Organizations Under Threat

- Maintaining service availability under attack by choosing a solution that monitors traffic behavior and distinguishes between legitimate users and attack traffic, allowing them in while blocking the malicious packets
- A hybrid solution combining on-premises detection and mitigation with cloud-based protection for volumetric attacks. It facilitates quick detection, immediate mitigation and prevents internet pipe saturation.
- An integrated, synchronized solution that can protect from multi-vector attacks such as network floods, and application layer attacks such as low-and-slow service disruptions or HTTP/S floods.
- A cyber-security emergency response plan that includes a dedicated emergency team of experts and clear actions in the event of attack.

Radware recommends IT crews to monitor security alerts and examine triggers carefully. Tune existing policies and protections to prevent false positives and allow identification of real threats when they occur.

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] https://nmap.org/
[ii] https://cirt.net/nikto2
[iii] http://sqlmap.org/