Abstract

Anonymous has launched OpLGBT, a DDoS campaign targeting the state of North Carolina and its governmental institutes in response to controversial legislation passed by the state's General Assembly - House Bill 2 (known as the "bathroom law"). The bill bans people from using public bathrooms that do not correspond to their biological sex and has sparked debate regarding LGBT (lesbian, gay, bisexual, transgender) rights.

To date, attackers have struck North Carolina's website, IT network and cloud-hosted services (see Figure 1). The objective of OpLGBT is to target any government or group (see Figures 2 & 3) that are directly or indirectly related to anti-LGBT legislation or hate – a hint this cyber assault may turn into an ongoing operation that requires the additional preparation. Increasing traction amongst the hacktivist community could result in OpLGBT evolving in volume and sophistication, including DDoS bursts, web intrusion and data theft attempts, thus becoming a persistent attack.

Figure 1: Site under maintenance after attacks

Attack Vectors

- **TCP Flood** – This is one of the oldest and most popular Denial of Service (DoS) attacks. It involves sending numerous SYN packets to the victim. In many cases, attackers will spoof the SRC IP so the reply (SYN+ACK packet) will not return, thus overwhelming the session/connection tables of the targeted server or one of the network entities on the way (typically the firewall). Servers need to open a state for each SYN packet that arrives and they store this state in tables that have limited size. As big as this table may be, it is easy to send sufficient amount of SYN packets that will fill the table. Once this occurs, the server starts to drop a new request, including legitimate ones. Similar effects can happen on a firewall which also has to process and invest in each SYN packet. Unlike other TCP or application-level attacks, the attacker does not have to use a real IP - this is perhaps the biggest strength of the attack.
- **SQL Injection** - Exploiting poor coding of web application where the inputs are not sanitized therefore exposing application vulnerabilities. SQL injection is the most common type of injection attack which also count LDAP or XML injections. It is by far the number one vulnerability listed in OWASP Top 10. The idea behind a SQL injection is to modify an application SQL (database language) query in order to access or modify unauthorized data or to run malicious programs. Most web applications rely on databases where the application data is stored and being accessed by SQL queries and modifications of these queries could mean taking control of the application.

Targets of Operation LGBT

North Carolina Government:

- nc.gov
- state.nc.us

- np.nc.gov
- northcarolina.gov

Supporters of House Bill 2:

Check website http://www.governor.nc.gov

Permanent link to this check report | Share report:

Location	Result	Time	Code
Austria, Vienna	Connection timed out		
Belgium, Antwerp	Connection timed out		
Canada, Ottawa	Connection timed out		
Germany, Dusseldorf	Connection timed out		
Hong Kong, Central District	Connection timed out		
Israel, Tel Aviv	Connection timed out		
Italy, Milano	Connection timed out		
Latvia, Riga	Connection timed out		
Moldova, Chisinau	Connection timed out		
Netherlands, Amsterdam	Connection timed out		
Portugal, Lisbon	Connection timed out		
Russian Federation, Moscow	Connection timed out		
Spain, Madrid	Connection timed out		
Sweden, Stockholm	Connection timed out		
Switzerland, Zurich	Connection timed out		
Ukraine, Kharkov	Connection timed out		
United Kingdom, London	Connection timed out		
United States, Colorado	Connection timed out		
United States, California	Connection timed out		

Check website http://nc.gov:80

Permanent link to this check report | Share report:

Location	Result	Time	Code
Austria, Vienna	Connection timed out		
Belgium, Antwerp	Connection timed out		
Canada, Ottawa	Connection timed out		
Germany, Dusseldorf	Connection timed out		
Hong Kong, Central District	Connection timed out		
Israel, Tel Aviv	Connection timed out		
Italy, Milano	Connection timed out		
Latvia, Riga	Connection timed out		
Moldova, Chisinau	Connection timed out		
Netherlands, Amsterdam	Connection timed out		
Portugal, Lisbon	Connection timed out		
Russian Federation, Moscow	Connection timed out		
Spain, Madrid	Connection timed out		
Sweden, Stockholm	Connection timed out		
Switzerland, Zurich	Connection timed out		
Ukraine, Kharkov	Connection timed out		
United Kingdom, London	Connection timed out		
United States, California	Connection timed out		
United States, Colorado	Connection timed out		

Figure 2 & 3: Targeted sites

Solution Criteria for Organizations Under Threat:

Protection from TCP Floods and other DDoS attacks:

- A hybrid solution combining on-premise detection and mitigation with cloud-based protection for volumetric attacks. It facilitates quick detection, immediate mitigation and internet pipe saturation.
- Solution must distinguish between legitimate and attack traffic, blocking it while protecting the SLA.
- An integrated, synchronized solution that can protect from multi-vector attacks combining DDoS with web-based exploits such as website scraping, Brute Force and HTTP floods.
- A cyber-security emergency response plan that includes a dedicated emergency response team and process in place. Identify areas where help is needed from a third party.

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 offers a full range of solutions to help networks properly mitigate attacks similar to these. Our attack mitigation solutions provide a set of patented and integrated technologies designed to detect, mitigate and report todays most advanced DDoS attacks and cyber threats. With dedicated hardware, fully managed services and cloud solutions, Radware can help ensure service availability. To understand how Radware's attack mitigation solutions can better protect your network contact us today.

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.