Abstract

The hacktivist group Anonymous launched an operation against the city of Denver, CO and its officials. Entitled OpRight2Rest, the operation is a response to the passing of the Denver Homeless Camping Ban.[i] Anonymous has threatened to launch DDoS attacks against the city institutes and authorities, as well as to extract and publish personal information of city officials (see figure 1).

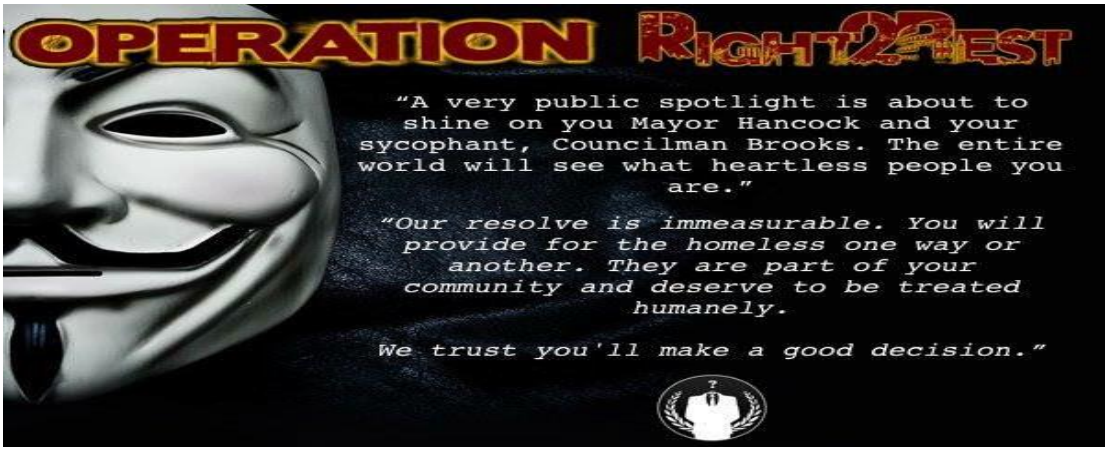

Figure 1

Background

On May 23 2012, Denver passed the Denver Homeless Camping Ban. This ban makes it a crime for the homeless population to shelter themselves on any type of public or private property without permission. In addition, the homeless cannot set belongings down inside city limits. Fines can go up to $999.

Anonymous contends that Denver's officials are bulling and harassing the homeless population in the city. In response, Anonymous is planning on Doxing members that support the ban, as well as launching coordinated denial of service attacks against the city of Denver unless the ban is repealed, the homeless are compensated, and a permanent solution is found.

Operation Video

- https://youtu.be/koK0S_13zX8

Targets

- Denvergov.org
- Denvergov.org/pocketgov (Phone app)
- Eiseverywhere.com (Host for the Downtown Denver Partnership Annual Awards

Attack Vectors

- DDoS
- Doxing
- Spamming

Reasons for Concern

Anonymous has begun Doxing city officials[ii]. They have also published a target list for this operation along with emails and phone numbers of city officials. Additional hacktivist groups that belong to the

Anonymous collective are using powerful tools to generate massive amounts of traffic for DDoS purposes and are leveraging web intrusion programs to acquire sensitive data.

How to Prepare

Radware advises that Denver city officials and those sites affected by this operation put security protections in place. Individuals may want to review their PII, while organizations may want to deploy DDoS attack prevention and mitigation systems, as well as a web application firewall.

We recommend reviewing network security policies, and patching the system accordingly. Maintaining and inspecting your network often is necessary to defend against these types of risks and threats.

Organizations under Threat Should Consider

Effective **DDoS protection** elements:

- 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.
- Solution must distinguish between legitimate and malicious packets, protecting the SLA while rejecting attack traffic
- 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 an emergency response team and process in place. Identify areas where help is needed from a third party.

Effective **Web Application protection** elements (to prevent web intrusions, defacement and data theft):

- 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 0-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 todays 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 that protect against attacks, 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.

---

[i] http://pastebin.com/AZQUTBdD
[ii] https://ghostbin.com/paste/w3z7r