radware

ERT Threat Alert

Animal Rights Hacktivism

Updated on 6-6-2016

Background

Hacktivists have battled for the rights of animals for some time, but within the last year, have raised the stakes considerably via a series of prolonged, advanced cyber campaigns. What started with a cyber assault against the website of the Colombian Army in 2011 in response for shooting a dog on TV has morphed into a series of advanced, DDoS and APDoS campaigns launched on a yearly basis against organizations and individuals perceived to be harming, abusing or exploiting wildlife. These operations are putting organizations who leverage wildlife for trade and profit at immense risk. Various industries, including fashion, food, pharmaceuticals, cosmetics, entertainment, and government organizations, should take precautions.

Attack Analysis

Since late 2015, a series of advanced DDoS campaigns have been executed against nations who support the hunting of whales. By launching different network- and application-layer attacks, Anonymous operations like OpKillingBay, OpWhales and OpSeaWorld have caused massive damage to leading websites in Japan, Denmark, Iceland and several other locations. Examples include the network outages at Tokyo Narita airport and the take down of Nissan’s websites.

During these operations, hacktivists exchange best practices, tools and software to boost their chances of success. Hacktivists communicate via a variety of means offline, including making phone calls to organize people and information. One of the most popular tactics: TweetStorm campaigns. Those who retweet and repost the message—known as “boosters”—help generate awareness among a wider audience and enlist participants.

Current Animal Rights Operations

Animal Rights

OpHarambe[i] – This operation focused on calling attention to the death of an endangered silverback gorilla at the Cincinnati Zoo after a child was found in the enclosure. Anonymous believes that the Cincinnati Zoo should have taken less lethal action and cited that the gorilla was protecting the child. Anonymous is calling for charges against the mother of the child. In response to this event, Anonymous has formed OpHarmabe and posted the dox/personal information about the mother. They have also posted a paste on Ghostbin that includes information related to Cincinnatizoo.org and its network along with emails and Facebook accounts associated with the zoo.

Hunting

OpKillingBay - OpKillingBay is a yearly operation run by Anonymous and other organizations against countries and organizations that are directly and indirectly involved with the hunting of whales and dolphins in Japan and the North Sea (see Figure 1). In this operation, data dumps, defacements and denial of service attacks have been witnessed
OpKillingBay full Radware ERT alert

See also: OpWhales[ii]

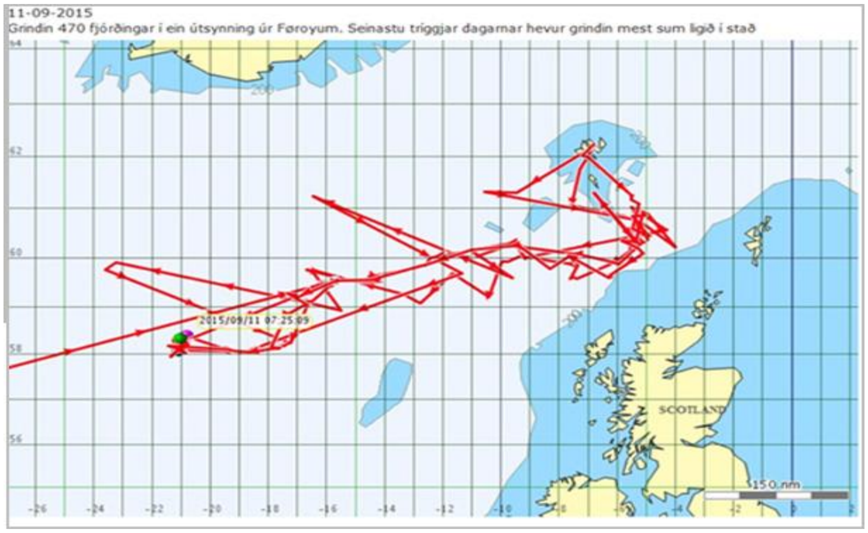

11-09-2015
Grindin 470 fjórðingar í ein útsynning úr Føroyum. Seinastu tríggjar dagarnar hevur grindin mest sum ligið í stað
2015/09/11 07:25:09
SCOTLAND
150 nm
62
60
58
56
-26
-24
-22
-20
-18
-16
-14
-12
-10

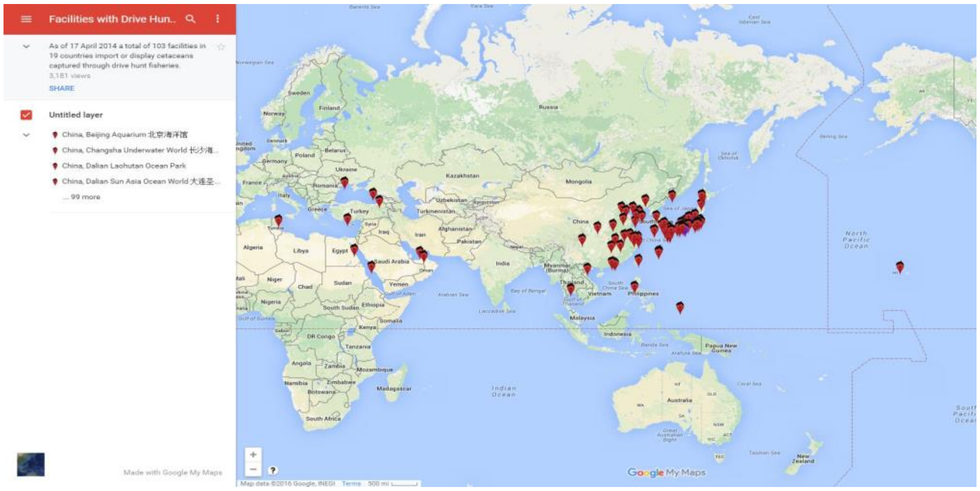
Figure 1: Savn.fo was targeted after it was discovered to be used to track whales

Captivity

OpSeaWorld[iii] - an operation run by Anonymous to protect animals in captivity. Members of this operation target parks around the world with TweetStorms, data dumps and denial of service attacks (see Figure 2).
Op Site - https://sites.google.com/site/opseaworld/home
Account - https://twitter.com/OpSeaWorldAnon

Trade

OpFunKill[iv] – This operation focuses on protecting animals from trophy hunters, but also engages in protecting animals from testing, destruction of habitats, slaughter, and the fur industry. Recent examples include the global protest following publicized killings of rhinos, elephants and lions like Cecil the Lion.


Facilities with Drive Hun...

As of 17 April 2014 a total of 103 facilities in 19 countries import or display cetaceans captured through drive hunt fisheries.
3,181 views
SHARE

☑ Untitled layer

- China, Beijing Aquarium 北京海洋馆
- China, Changsha Underwater World 长沙海...
- China, Dalian Laohutan Ocean Park
- China, Dalian Sun Asia Ocean World 大连圣...

... 99 more

Figure 2: OpSeaWorld target list as a Google Maps page[v]

Reasons for Concern

Hacktivists do not see digital boundaries and will continuously attempt launching attacks at targets in the name of social or political change. Animal rights hacktivists will try gaining unauthorized access into computer networks and systems in an attempt to steal information, exploit the network and extort those that they are targeting. While a lone hacktivist can be problematic, hundreds collaborating is a different challenge.

Current Target lists

- OpWhales
  - https://ghostbin.com/paste/rxwkr
  - https://ghostbin.com/paste/tzfae
- OpKillingBay
  - https://ghostbin.com/paste/ajbdx
  - https://ghostbin.com/paste/2mrne
- OpSeaWorld
  - https://ghostbin.com/paste/fnnqy
- OpBeast
  - https://ghostbin.com/paste/dgqhz

Attack Vectors

- **TCP flood** - One of the oldest yet still very 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, and once this happens 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.

- **UDP Flood** – In a UDP flood the attacker sends large UDP packets to a single destination or to random ports. Since the UDP protocol is “connectionless” and does not have any type of handshake mechanism, the main intention of a UDP flood is to saturate the Internet pipe. In most cases the attackers spoof the SRC IP

- **Reflection Attacks** – Reflective denial-of-service attacks makes use of a potentially legitimate third-party component to send the attack traffic to a victim, ultimately hiding the attackers’ own identity. The attackers send UDP packets to the reflector servers with a source IP address set to their victim’s IP, therefore indirectly overwhelming the victim with the response packets. The reflector servers used for this purpose could be ordinary servers with no indication/trace that they have been compromised, which makes this kind of attack particularly difficult to mitigate. A common example for this type of attack is DNS, NTP, and SNMP reflection.

- **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.

Organizations under Attack Should Consider

Protection from UDP & HTTP Floods, reflection attacks and other DDoS techniques:

- A hybrid solution combining on-premises detection and mitigation with cloud-based protection for volumetric attacks. It facilitates quick detection, immediate mitigation and internet pipe saturation.
- The 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 by 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 team of experts.

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 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?

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

[i] http://pastebin.com/raw/a5mPEwbJ
[ii] http://pastebin.com/2qJLrW3V
[iii] http://pastebin.com/fk3vuBiv
[iv] http://pastebin.com/dMxVGA2W
[v] https://www.google.com/maps/d/viewer?msa=0&mid=zhQkwRnSnjCw.k4fw_vxAXaBk