Background

With a new whale hunting season comes a new wave of attacks by environmental and animal rights hacktivist communities within the Anonymous collective. Several operations are currently being run in parallel - OpKillingBay, OpKillingBay Eu, OpWhales and OpSeaWorld. They're all yearly hacktivism operations by Anonymous in response to the hunting of whales and dolphins for food and captivity in Norway, Iceland, Japan and the Faroe Islands.

Since early December there has been a spike in activity from Anonymous. Hacktivists launch attacks year round but collaborate for more determined efforts during the season. The hunts that happen in the Faroe Islands and the attacks that happen in relation to OpSeaWord create a persistent threat for both specific industries as well as governments who allow hunting or who keep marine life in captivity.

Figure 1: Operational image from #OpSeaWorld

OpSeaWorld – OpSeaWorld is a yearly operation by Anonymous, activists and other organizations in response to the captivity, treatment and abuse of animals in captivity. OpSeaWorld is an open operation with no defined start or end dates. OpSeaWorld is typically active when animals in an aquarium are being abused or buying animals from hunts like those at Taiji Cove. Companies that transport or capture the animals are also targeted.

Figure 2: Operational image from #OpWhales

OpWhales – OpWhales is a yearly operation by Anonymous, activists and other organizations in response to the hunting of whales in Norway, Iceland and Japan. Every year the hunt runs for six months from April to September. These whales are hunted for commercial purposes and often shipped to other countries. Hvalur hf, the largest whaling company in Iceland, has now suspended hunting of Fin whales, an endangered species, for the last two summers due to regulations and red tape for exporting the whale meat to Japan. This pressure has come from both Japanese bureaucracy and the fact that the United States government

said they may institute economic measure against Iceland for hunting Fin Whales[1]. The hunting of Minke whales continues with an increase in quota since the whales are not endangered. The hunt in Norway and Iceland have overlapping targets with OpKillingBay due to the export of whale meat to Japan.

Figure 3: Operational image from #OpKillingBay

OpKillingBay – OpKillingBay is a yearly operation by Anonymous, activists and other organizations in response to the yearly hunt of dolphins in Japan. The operations started in 2013 by Anonymous and has occurred every year since. It was created by Anonymous to bring attention to the hunting of whales and dolphins in Japan. The hunt typically runs from September to February. Dolphins from this hunt are either killed for meat or sold into captivity. During this time, the hacktivists work together to bring awareness to their cause by launching network-crippling attacks on those that support, finance or are indirectly involved.

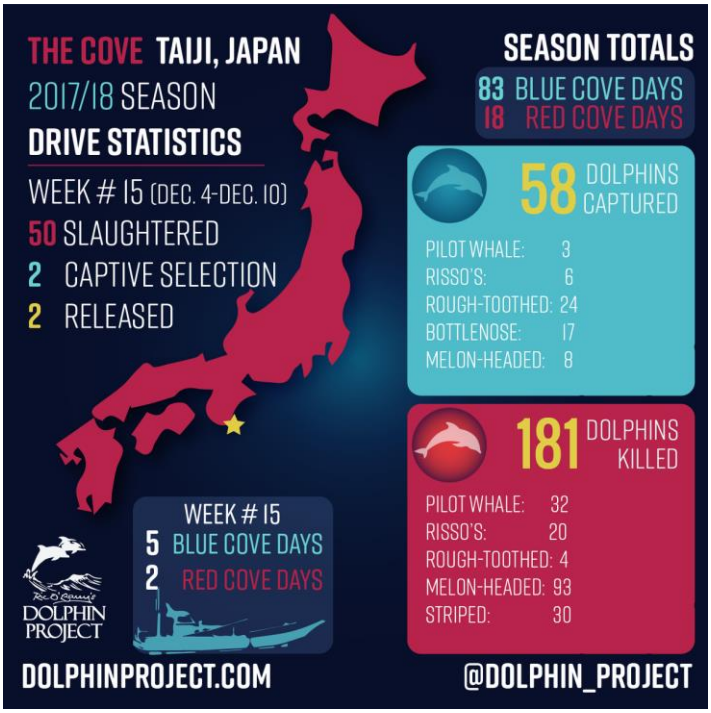

Figure 4: Drive statistics for 2017/18 season from @Dolphin_Project

Figure 5: Operational figure from #OpKillingBayEU

[1] https://grapevine.is/news/2017/03/10/no-fin-whale-hunting-this-year-either/

OpKillingBay EU – OpKillingBay EU is a yearly operation by Anonymous, activists and other organizations in response to the yearly hunt of whales and dolphins in the Faroe Island. This hunt known as the grindadrap can happen at any point of time during the year. There are normally multiple drives in a season. The main target for OpKillingBay EU is European countries such as Denmark, Faroe Islands, Iceland, and Norway. The attackers launch network- and application-floods to disrupt the operations of those involved in hunting, such as government institutions and large corporations. This operation also has overlap with OpWhales.

Targets

- Tourism
- Transportation
- Media
- Telecommunication
- Government

Target Lists

OpKillingBay
https://justpaste.it/1a15i

OpKillingBay EU
https://ghostbin.com/paste/pzm69

OpWhales Target lists
https://justpaste.it/184l3 - Japan
https://justpaste.it/1ee89 - Norway
https://ghostbin.com/paste/8h6m2 - Japan
https://ghostbin.com/paste/4v3x3 - Various Targets

Figure 6: OpKillingBay - Taiji quota for 2017/18 fishing season

Attack Vectors

Web Application Exploits

- **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.
- **Defacement** – Attacker changes 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.
- **Injection** - This form of an attack allows administrative access and usually involves obtaining user credentials first. It allows hackers to make changes to a website.
- **Data Theft** – compromising sensitive data while data at rest or in transit, via stealing encryption keys, hashed passwords, clear text data off the server, and even from a user's browser.

Denial-of-Service Attack Vectors

- **TCP Flood** - One of the oldest, yet still very popular denial-of-service 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 (source) IP.
- **HTTP/S Flood** - An attack method used by hackers to attack web servers and applications. These floods consist of seemingly legitimate session-based sets of HTTP GET or POST requests sent to a targeted web server. HTTP floods do not use spoofing, reflective techniques or malformed packets. These requests are specifically designed to consume a significant amount of the server's resources and therefore can result in a denial-of-service. Such requests are often sent en masse by means of a botnet, increasing the attack's overall power. HTTP and HTTPS flood attacks are one of the most advanced threats facing web servers today since it is hard for network security devices to distinguish between legitimate and malicious HTTP traffic.

What's Expected Next

In this campaign, it is expected that those involved directly and indirectly could be targeted by SQL injections, cross-site scripting (XSS), data dumps and service outages caused by denial-of-service attacks. These attacks aim to cause service outages due to vulnerabilities in server applications or a large amount of traffic aimed to overwhelm networks. Attacks are expected to continue as long as dolphins and whales are hunted and captured for captivity around the world.

Organizations Under Attack Should Consider

Effective DDoS Protection Essentials

- **Hybrid DDoS Protection** - On-premise and cloud DDoS protection for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - Quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creationyupd** - Promptly protect from unknown threats and zero-day attacks
- **A Cyber-Security Emergency Response Plan** - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

For further DDoS protection measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

Effective Web Application Security Essentials

- **Full OWASP Top-10 application vulnerabilities coverage**– against defacements, injections, etc.
- **Low false positive rate –** using negative and positive security models for maximum accuracy
- **Auto policy generation capabilities** for the widest coverage with the lowest operational effort
- **Bot protection and device fingerprinting** capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking
- **Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources
- **Flexible deployment options -** on-premise, out-of-path, virtual or cloud-based

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.