Abstract

Operation Killing Bay is a yearly hacktivism operation by Anonymous, activists, and others organizations in response to the hunting of whales and dolphins in Japan. OpKillingBay EU is in response to the dolphin hunt in the Faroe Islands. These operations often run parallel to OpSeaWorld and OpWhales and include overlapping targets.

Background

With the opening of a different hunting season brings a new wave of attacks. Anonymous hackers have begun a new wave of DDoS attacks in April as the hunting season in the Arctic region begins. Those directly and indirectly related to the current hunt for Minke whales are being targeted by online protests in the form of network and application attacks by the hacktivist group Anonymous.

This hunt in Norway and Iceland fall under OpWhales but has overlapping targets with OpKillingBay. Currently, companies in Japan are being targeted for several reasons related to the captivity and hunting of whales and dolphins around the world. The reason why OpKillingBay is running parallel to OpWhales is due to a Japanese fleet returning to port with 333 Minke whales[i]. One of the main reasons behind the commercial hunting in Iceland and Norway is to sell the meat to counties that have limited access, such as Japan. As a result, Anonymous hackers will attack anyone related to the hunting, shipping and disruption of the meat.

There are two different types of whale hunts around the world. Hunts in Norway, Iceland and Japan are for commercial purposes whereas hunts that happen in the Faroe Islands are for non-commercial proposes. The meat in those situations are for local consumption only.

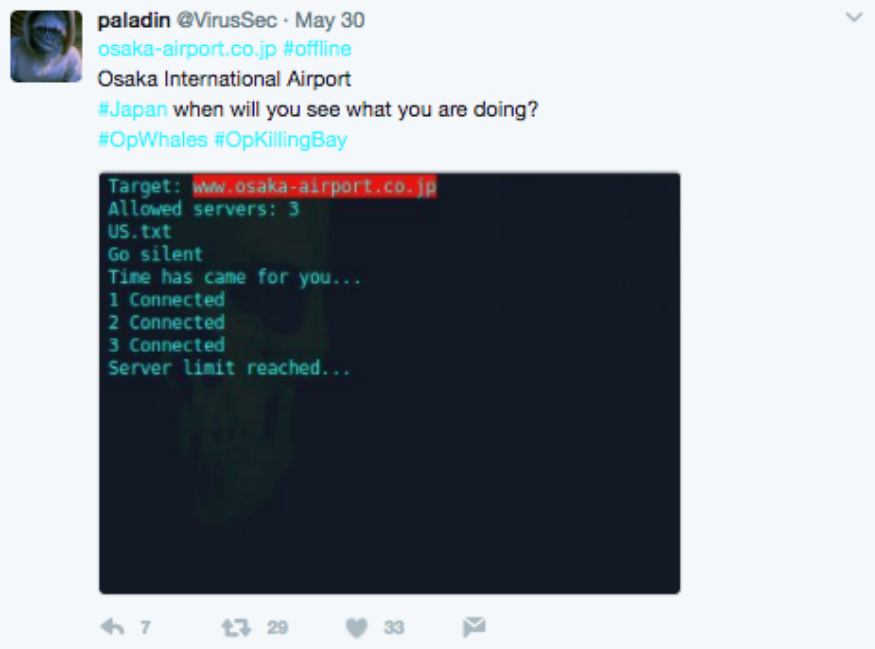

Figure 1: @VirusSec attack Osaka International Airport for transporting dolphins

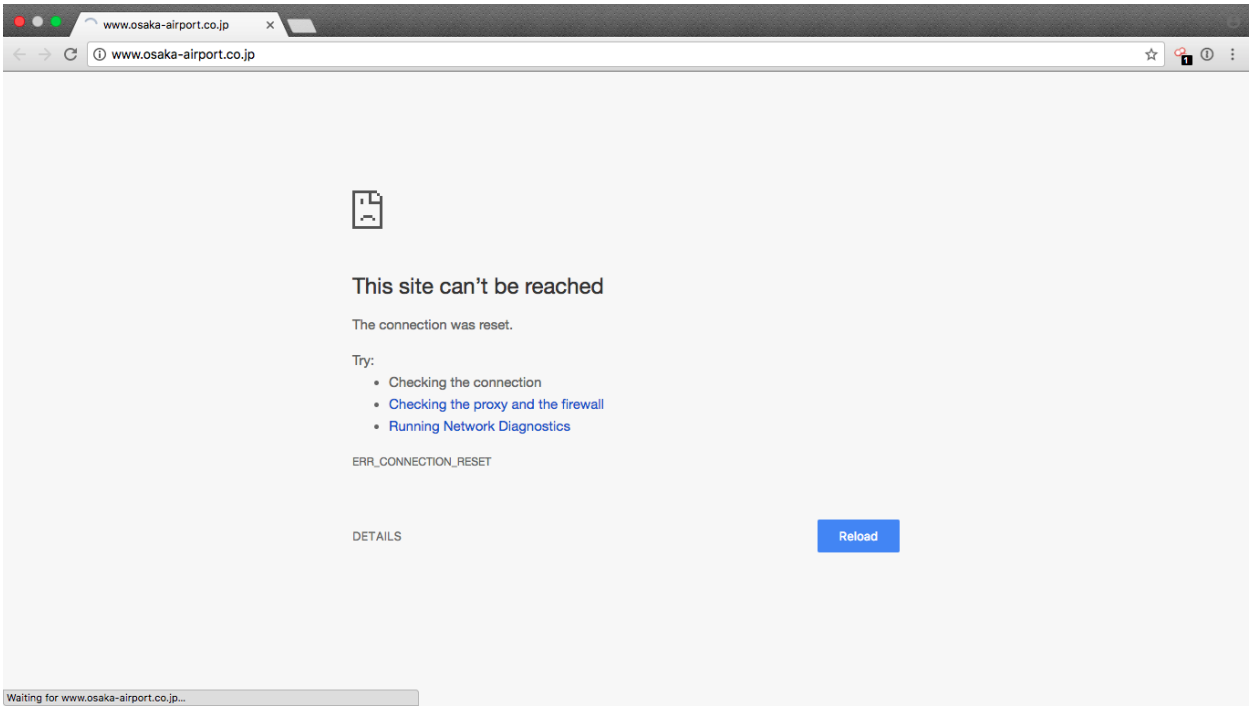

Figure 2: Osaka Airport website offline

OpKillingBay – OpKillingBay is a yearly operation by Anonymous, activists and other organizations in response to the yearly hunt of dolphins in Japan. The hunt ran from September 2016[ii] till February 2017[iii]. Dolphins from this hunt are either killed for meat or sold into captivity.

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. This hunt is not for commercial purposes and the meat is consumed locally.

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 clearly defined end or start dates. OpSeaWorld is normally active when an animal in an aquarium is being abused or buying animals from hunts like those at Taiji Cove. Companies that transport or capture the animals are also targeted.

OpWhales – OpWhales is a yearly operation by Anonymous, activists and other organizations in response to the hunting of whales in Norway and Iceland. 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 to supply the demand.

Reasons for Concern

There has been a recent spike in activity from Anonymous in response to the beginning of a new hunting season in Norway. The hunting season in Japan runs from September till February and the hunt in Norway runs from April to September. This provides an environment for hacktivist to launch attacks year round. The hunts that happen in the Faroe Islands and the attacks that happen in relation to OpSeaWord

create a persistent threat for the whaling industry and those that keep dolphins in captivity. These operations are also known to attack companies that are indirectly or not even involved in the hunting or captivity of dolphins and whales. Recently, Osaka International Airport was targeted for transporting dolphins.

Advanced Persistent Denial of Service

This yearly operation in combination with OpKillingBay EU and OpSeaWorld present overlapping targets that can be attacked year round. OpKillingBay in Japan starts in September and runs till February while OpWhales in the Arctic runs from April till September. These four operations in combination form an Advanced Persistent Denial of Service (APDoS) campaign that results in attacks year-round for the whaling and captivity industry. Those also indirectly related to these industries are also under threat.

Targets Lists

The target lists in these operations are often recycled. For example, the target list for OpKillingBay EU has been reposted by the same account repeatedly since July 2015. The most recent post of this target list by this actor was on May 22, 2017 (see Figures 3 & 4).

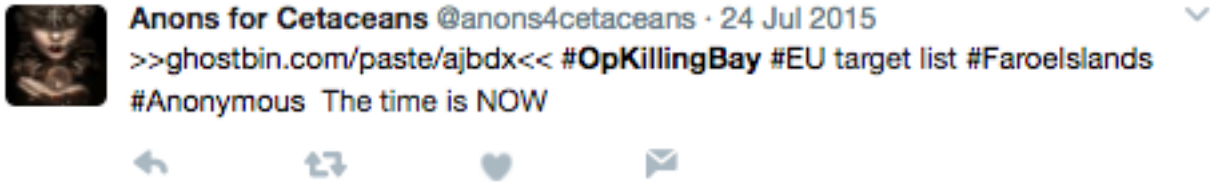

Figure 3: Target list for OpKillingBay EU - July 2015

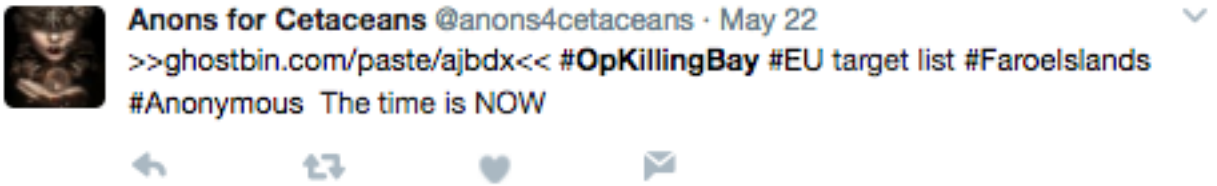

Figure 4: Same target list for OpKillingBay EU – May 2017

Target list in circulation for OpKillingBay, OpkillingBay EU, OpWhales and OpSeaWorld:

- https://ghostbin.com/paste/rxwkr
- https://ghostbin.com/paste/pzm69
- https://ghostbin.com/paste/2mrne
- https://ghostbin.com/paste/ajbdx
- https://ghostbin.com/paste/u7hnp
- https://ghostbin.com/paste/kzg5s
- https://ghostbin.com/paste/fehgq
- https://ghostbin.com/paste/8h6m2
- https://ghostbin.com/paste/fssmo
- https://ghostbin.com/paste/4v3x3
- https://ghostbin.com/paste/fnogb
- https://ghostbin.com/paste/gnjkq
- https://hastebin.com/jowewomuse
- https://justpaste.it/12ptj

Email dumps from multiple websites

- https://ghostbin.com/paste/ro2nt
- https://ghostbin.com/paste/qozf6

Targeted in April

http://doozono.com/

http://otaru-aq.jp/

http://simetani.com/
http://www.archives.go.jp/
http://www.courts.go.jp/
http://www.e-isana.com/
http://www.echizen-aquarium.com/
http://www.enosui.com/
http://www.fisheries.no
http://www.greenmall1123.sakura.ne.jp/
http://www.icrwhale.org/
http://www.immi-moj.go.jp/
http://www.kaiyukan.com/
http://www.keishicho.metro.tokyo.jp/
http://www.kensatsu.go.jp
http://www.kyodo-senpaku.co.jp/
http://www.marinepark.jp/
http://www.moj.go.jp
http://www.muroto-dc.jp/
http://www.ndl.go.jp/
http://www.penta-ocean.co.jp/
http://www.sangiin.go.jp/
http://www.stat.go.jp
http://www.tosakatsuo.com/
http://www.tsukiji-market.or.jp/
http://www.wakayama-kanko.or.jp/
http://www.webtv.sangiin.go.jp/
http://www.yoshizen.jp/
https://www.2yaku-support.go.jp/
https://www.imata.org/

Targeted in May

http://hav.fo
http://osaka-subway.com
http://us.jnto.go.jp
http://visitreykjavik.is
http://www.aquarium.co.jp
http://www.atlantic.fo
http://www.domstol.no
http://www.enosui.com
http://www.fisheries.no
http://www.fiskeridir.no
http://www.gotokyo.org
http://www.iceland.is
http://www.jftc.go.jp
http://www.kaiyukan.com
http://www.logreglan.is
http://www.moj.go.jp
http://www.nakanoshima-gyoko.jp
http://www.nankai.co.jp
http://www.norway.info
http://www.nsb.no
http://www.osaka-airport.co.jp
http://www.samskip.com
http://www.tokyometro.jp
http://www.u-tokyo.ac.jp

Targeted Industry

- Transportation
- Retail
- Banks
- Government
- Media
- Tourism
- Academics

Attack Vectors

Attackers in these operations are primarily using Layer 7 attack scripts like HULK, Crescent Moon, Black Horizon, Sad Attack, Saphyra or Wreckuests[iv]. These are all python scripts that allow an attack to run a DDoS attack using GET or POST HTTP floods. The attack uses proxy servers as bots to distribute the attack. In addition to Layer 7 assaults, hacktivists have been observed launching defacement, SQL and data dump attacks. These attackers are also using network discovery tools like NMAP to audit their targets network.

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. In addition, they identify what operating systems

(and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

Layer 7 (HTTP) Flood - HTTP flood consists of seemingly legitimate session-based sets of HTTP GET or POST requests sent to a target Web server. These requests are specifically designed to consume a significant amount of the server's resources and therefore can result in a denial-of-service.

HTTP makes it difficult for network security devices to distinguish between legitimate HTTP traffic and malicious HTTP traffic and could cause a high number of false-positive detections. Rate-based detection engines are also not successful at detecting HTTP flood attacks as the traffic volume of HTTP floods may be under detection thresholds. Because of this, it is necessary to use several parameters detection including rate-based and rate-invariant.

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.

Scope and Volume

Over the previous month, Nankai Electric Railway, Osaka Subway, Faroe Marine Research Institute, Gulf World Marine Park, Taba Aquarium and Marine Park in Malta have all been attacked under the operations OpKillingBay, OpWhales and OpSeaWorld. Cork University[v] also suffered from an attack when pictures surfaced with college students dancing with a dead dolphin. After the pictures surfaced, attackers quickly targeted Cork University with a series of attacks (see Figure 5).

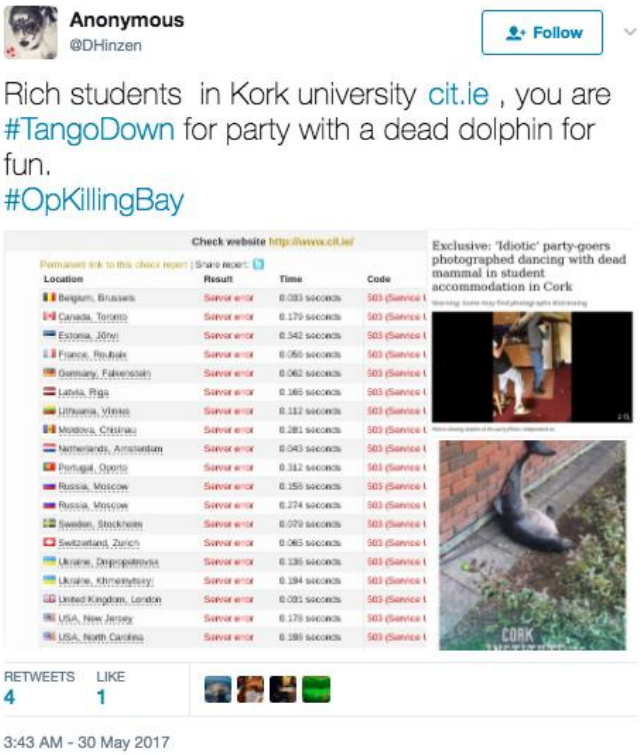

Figure 5: Cork University

What's Expected Next

In this campaign, it's 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 at a weak network.

It's expected that these attacks will continue if dolphins and whales are hunted and captured for captivity around the world. Next year, OpKillingBay should be more active since Taiji is now asking the Japan government to increase their yearly quota[vi], likely a move to expand their selection of species available for captivity.

At the core of the problem are ideological differences. The victims of these attacks are conducting business within the letter of the law. The actions of the groups behind OpKillingBay OpWhales and OpSeaWorld are driven from an emotional and social justice perspective. These two sides may never see eye to eye and this could result in a persistent state of attacks.

Figure 6: VirusSec attacks Tokyo Police for not speaking up

How to Prepare

Radware offers a full range of solutions to help your network properly mitigate attacks like the ones seen during OpKillingBay OpKillingBay EU, OpWhales or OpSeaWorld. Radware's DefensePro provides network protection with real-time, behavioral-based attack mitigation. Radware's Attack Mitigation Services (AMS) can also aid in detection and mitigation with cloud-based volumetric attack scrubbing.

In addition to Radware products, it is recommended that you review your network once a year. These attacks happen yearly before the start of the fishing season. Maintaining and inspecting your network is necessary if you are facing yearly attacks from hacktivists like those involved with OpKillingBay, OpWhales and OpSeaWorld.

Organizations Under Attack Should Consider

- A security solution that can protect its infrastructure from multi-vector attacks including protection from network and application-based DDoS attacks as well as volumetric attacks that can saturate the Internet pipe
- 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.
- A solution that provides protection against sophisticated web-based attacks and web site intrusions to prevent defacement and information theft.
- 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.
- Monitor security alerts and examine triggers carefully. Tune existing policies and protections to prevent false positives and allow identification of real threats if and when they occur.

In addition to Radware products, we recommend that you review your network and patch your system accordingly. Maintaining and inspecting your network often is necessary in order to defend against these types of risks and threats.

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://www.newscientist.com/article/mg23431203-900-japan-and-norway-set-off-on-annual-whale-hunt-despite-opposition/
[ii] https://www.theguardian.com/environment/2016/sep/09/first-dolphins-killed-in-japans-annual-taiji-hunt
[iii] http://www.huffingtonpost.com/entry/taijis-dolphin-killing-ends-for-this-season_us_58c056afe4b070e55af9eaae
[iv] https://github.com/JamesJGoodwin/wreckuests
[v] http://www.independent.ie/irish-news/exclusive-idiotic-partygoers-photographed-dancing-with-dead-mammal-in-student-accommodation-in-cork-35755620.html
[vi] http://savedolphins.eii.org/news/entry/taiji-town-wants-more-dolphins-to-kill