Abstract

OpKillingBay is a yearly hacktivism operation by Anonymous, activists and other organizations in response to the hunting of whales and dolphins in Japan and Denmark.

Background

OpKillingBay is an annual campaign that was started in 2013 by Anonymous. It was created by Anonymous to bring attention to the hunting of whales and dolphins in Japan and Denmark. The campaign begins in Japan every year in September with the dolphin hunting season, one of the largest in the world, and runs through the end of February. During this time the hacktivists work together to bring awareness to their causes by launching network crippling attacks on those that support, finance or are indirectly involved in the business of whale and dolphin hunting.

Reasons for Concern

In this series of attacks, we have seen SQL injections, data dumps and service outages caused by denial-of-service attacks from ongoing persistent campaigns by Anonymous. OpKillingBay has targeted a number of industries directly and indirectly related to the hunting of dolphins and whales for the last 6 months. This group has bypassed a number of services and has caused mass disruption for a number of organizations and governments. This is a very well organized operation by Anonymous.

Targets

Each operation provides its own target list for other hacktivists. Organizers have maintained these sites and are constantly updating them throughout the course of the operation. Each list contains over 100 targets and details the website name, server, ports, and IP address.

- hxxps://ghostbin.com/paste/fdzhu – OpKillingBay Target List
- hxxps://ghostbin.com/paste/rvps3 – OpSeaWorld Target List

Industries Targeted

- Transportation
- Retail
- Banks
- Government
- Media
- Tourism
- Union Workers
- Academics
- Automotive

Targeted Sites Since Mid-December

OpKillingBay

- Icrwahle.org
- Broome.wa.gov.au
- Dolphinresort.jp
- Kujirakan.jp
- S-abe.or.jp
- Town.taiji.wakayama.jp
- Nissan.co.jp
- Fsa.go.jp
- Narita-airport.jp
- Mhlw.go.jp
- Nankai-express.co.jp
- Behindthecove.com
- Ks-cinema.com
- Mjcc.ru
- Mof.go.jp
- Shugiin.go.jp
- Jsf.co.jp
- Nta.go.jp
- Jetro.go.jp
- Jfc.go.jp

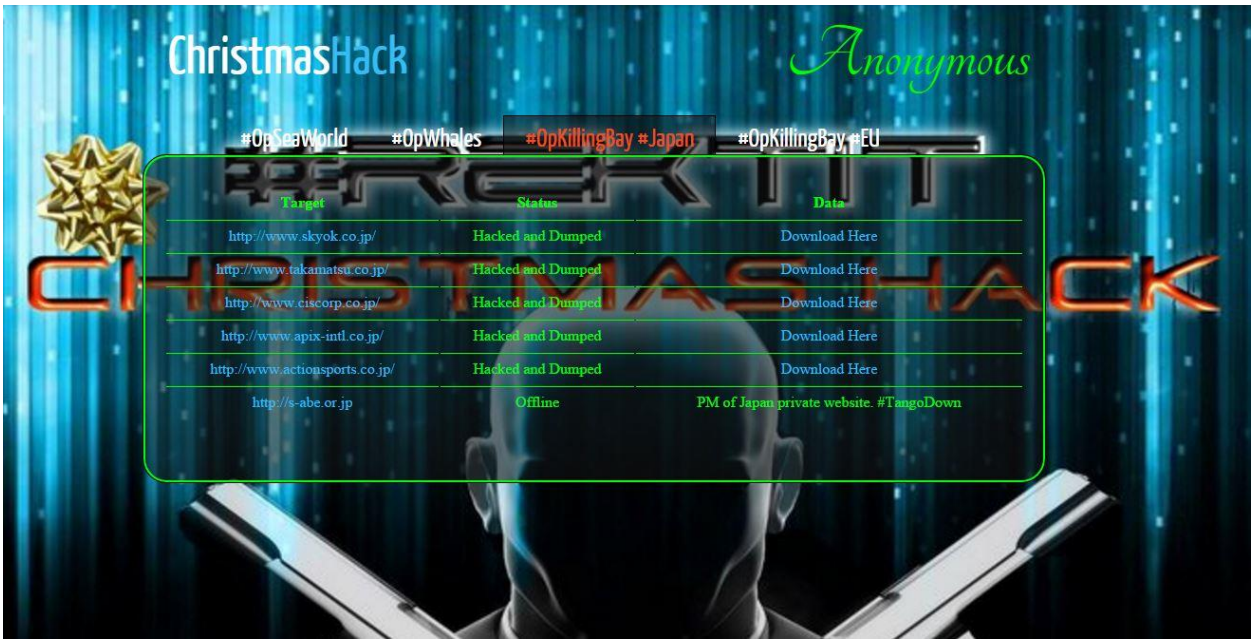
OpWhales

- Phallus.is
- eimskip.is
- netto.is
- samkaupurval.is
- fisheries.is
- hbgrandi.com
- noatun.is
- kronan.is
- bonus.is
- kjarval.is
- marugei.jp
- marugeii.jp
- Cargill.co.jp
- Foreign.gov.kn
- mof.gov.kn
- ab.gov.kn
- ciu.gov.kn
- evisa.gov.kn
- stkittsnevisdubai.gov.kn
- nia.gov.kn
- perlan.is
- einarshusid.is
- 3frakkar.com
- Hinoshoten.co.jp
- fjarskiptasjodur.is
- government.is
- mfa.is
- rikiskassinn.is
- stjornarrad.is
- atvinnuvegaraduneyti.is
- fjarmalaraduneyti.is
- forsaetisraduneyti.is
- innanrikisraduneyti.is
- menntamalaraduneyti.is
- umhverfisraduneyty.is
- utanrikisraduneyti.is

OpSeaWorld

- Dubaidolphinarium.ae
- Unexso.com
- Dolphinislandpark.com
- Bahamasbluelagoon.com
- Marineland.ca
- Loroparque.com

Christmas Attack



On December 24t, 2015 Anonymous member, RektFaggot[i], published hacked and leaked information from OpSeaWorld, OpWhales, and OpKillingBay targets.[ii]

OpKillingBay – hacked and dumped

- Skyok.co.jp
- Takamatsu.co.jp
- Ciscorp.co.jp
- Apix-intl.co.jp
- Actionsports.co.jp

OpKillingBay - DDoS

- S-abe.or.jp
- Bst.fo
- Bunadarstovan.fo
- Bvs.fo
- Effo.fo
- Hafnia.fo
- Kaf.fo
- Matrikul.fo
- Rff.fo
- Sms.fo
- Umhvorvisstovan.fo
- Us.fo
- Skagenhavn.dk
- Benadarstovan.fo
- Bvs.fo

OpSeaWorld – hacked and dumped

- Zoo.pt
- Oceanpark.com.hk
- Szzoo.net

OpWhales - Offline

- Fiskistofa.is
- Islenskibarinn.is
- Saegreifinn.is

What's Expected Next

We expect to see denial of service attacks, data dumps and service outages caused by these campaigns. It's expected that those industries directly and indirectly related to the hunting of dolphins and whales will continue to see a wave of attacks throughout the end of the hunting season. After the hunting season is over members will focus on other operations until the beginning of the hunting season in September.

How to Prepare

Attacks like these are hard to avoid, as the core of the issue is ideological differences. While the victims of these attacks are conducting business within their rights, the groups behind OpKillingBay and other operations are driven by emotions and what they believe to be social injustice. As these two groups continue to disagree, expect to see a persistent state of attacks.

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. Monitoring 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 once a year during the month of August. As these attacks occur on an annual basis, maintaining and inspecting networks is necessary in order to defend against these types of attacks.

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] https://twitter.com/_RektFaggot_/status/679979039512223744
[ii] http://open.youranonymous.com/