TLP: **GREEN**

RISK FACTOR: **HIGH**

Issue Date: 04.21.16

Threat Advisory: *#OpKillingBay Expands Targets Across Japan*

1.0 / OVERVIEW / Operation Killing Bay, better known as #OpKillingBay on social media sites, is expanding. Historically, malicious attackers participating in OpKillingBay have targeted Japanese government websites and sites of companies participating in whale and dolphin hunting. These attackers often see themselves as protesters or activists, in addition to hackers and refer to themselves as "hacktivists."

- **See Akamai SIRT advisory on hacktivists**

Recently however, Akamai SIRT members Larry Cashdollar and Ben Brown have seen a shift in hacktivist tactics in OpKillingBay. While they are still attacking the same types of sites as in the past, they are also attacking sites unrelated to the hunts. In fact, one member of OpKillingBay stated that a company was targeted not because they supported the hunts, but because they did nothing about them.

Akamai has also observed the group threatening to attack whaling groups from other parts of the world, as we have found target lists for sites in Denmark, Iceland and the Faroe Islands. We are also seeing that the attackers involved in OpKillingBay are spreading out and participating in other operations as well.

2.0 / ATTACK TIMELINE / OpKillingBay is approximately three years old. It has historically focused on anti-whaling activity. From there it has branched out, striking Japanese .gov sites. Attacks on the prime minister's website made news in December 2015.

Since the start of 2016, the target list has further expanded. On Jan. 12, we started to observe attacks against a japanese automotive web site. Another automotive company joined the list of victims on February 4, and attacks continued every few days.

At this point, it's unclear if the person claiming credit is actually the one launching the attacks, but Akamai is capable of viewing the attack traffic against the mentioned organizations and others that have been targeted within our infrastructure.

3.0 / TARGET INDUSTRIES / Listed below is a breakdown of industry verticals and associated number of unique organizations within each category that we have observed attacks against:

Target Industry	# of organizations
Retail	1
Telecommunications	2
Transportation	2
Automotive	3
Theme Parks	9
Sports	1
Travel	2
Finance	6
Government	25
Seafood	17

** The group has declared any government site from Japan or Iceland to be targeted.*

4.0 / ATTACK TRAFFIC / The attack traffic seen on January 12 was primarily a layer 7 GET flood. The traffic consisted of simple requests to the web root, and logs show the requests are simply to */.* While analysis of this kind of traffic can often detect various anomalies like a missing header or a certain user-agent string, the most common defense is rate controls. Akamai makes recommendations for both the average rate and the bursting rate of traffic. These recommendations are site-specific and are tuned to best fit the server's needs.

Akamai also located a list of sites to be attacked for OpKillingBay, on a common text paste site: https://ghostbin.com/paste/fssmo With this list in hand, Akamai was able to detect other attacks for this operation and also saw the OpKillingBay attackers participating in other hacktivist operations as well.

5.0/ OBSERVED ATTACK ACTIVITY / Using the target list mentioned in section 4.0 above, Akamai examined its own attack data, to see if any of our Kona customers were targeted. We examined competitors of our customers and discovered a pool of IP addresses used to attack their site.

Using the IP addresses that targeted our customers, we examined other WAF rules triggered on Akamai's deployed network. We confirmed that other Akamai customers were attacked from the same IP addresses as that attacked these organizations.

In the charts below, we see the IP address that attacked one of our customers, as well as other sites. We also cross-correlated those IP addresses and their targets to other known campaigns. This leads us to believe a couple scenarios are possible:

1. The hacktivists targeting automotive organizations for OpKillingBay are also interested in participating in other operations, such as OpSoaringEagle and OpIcarus. OpSoaringEagle was declared in 2013 against the Ottawa (Canada) police department for possibly accusing the wrong person of committing online attacks. The retaliation from hacktivists has been to attack the Ottawa police web site. OpIcarus is an ongoing operation to avoid using banks. It has been mainly seen in physical or on-site protests, but there have been some instances of an online component.

2. The IP addresses used are a part of shared botnet. It is possible that the IP addresses seen are part of a botnet for rent and it turns out multiple hacktivists used the same botnet. The timestamps seen here are for a little more than a week and may not be comprehensive. Some of these operations are continuing even today against a number of targets.

OpKillingBay
OpSoaringEagle
OpIcarus
Unrelated to a specific known operation

Number of Target domains	Campaign	Time Stamp
1	#OpKillingBay	Wed, 13 Jan 2016 07:00 GMT
7	#OpKillingBay #OpSoaringEagle #OpIcarus	Jan 21 11:00 2016 Jan 19 04:00 2016 Jan 13 02:00 2016 Jan 19 03:00 2016 Jan 19 04:00 2016 Jan 12 10:00 2016 Jan 19 16:00 2016 Jan 17 15:00 2016 Jan 21 21:00 2016
7	#OpKillingBay	Jan 21 11:00 2016

	#OpSoaringEagle #OpIcarus	Jan 19 04:00 2016 Jan 21 09:00 2016 Jan 13 02:00 2016 Jan 19 03:00 2016 Jan 19 04:00 2016 Jan 12 10:00 2016 Jan 17 15:00 2016 Jan 21 21:00 2016
8	#OpKillingBay #OpSoaringEagle #OpIcarus	Jan 14 08:00 2016 Jan 21 11:00 2016 Jan 21 15:00 2016 Jan 21 21:00 2016 Jan 12 13:00 2016 Jan 19 03:00 2016 Jan 19 10:00 2016 Jan 19 16:00 2016 Jan 19 17:00 2016 Jan 13 08:00 2016
6	#OpKillingBay #OpSoaringEagle #OpIcarus	Jan 15 01:00 2016 Jan 22 01:00 2016 Jan 18 01:00 2016 Jan 17 15:00 2016 Jan 14 01:00 2016 Jan 21 01:00 2016 Jan 21 11:00 2016 Jan 21 21:00 2016 Jan 12 01:00 2016 Jan 19 01:00 2016 Jan 19 03:00 2016 Jan 19 04:00 2016 Jan 13 01:00 2016 Jan 13 02:00 2016 Jan 20 01:00 2016
2	#OpKillingBay	Jan 21 07:00 2016 Jan 21 08:00 2016 Jan 13 02:00 2016
2	#OpKillingBay #OpSoaringEagle	Jan 21 21:00 2016 Jan 13 02:00 2016
4	#OpKillingBay	Jan 15 12:00 2016 Jan 11 04:00 2016 Jan 18 08:00 2016 Jan 18 11:00 2016 Jan 16 09:00 2016

		Jan 17 19:00 2016 Jan 14 21:00 2016 Jan 21 09:00 2016 Jan 12 10:00 2016 Jan 13 02:00 2016 Jan 13 09:00 2016 Jan 13 14:00 2016 Jan 20 01:00 2016 Jan 20 03:00 2016 Jan 20 20:00 2016
5	#OpKillingBay #OpSoaringEagle #OpIcarus	Jan 17 15:00 2016 Jan 21 21:00 2016 Jan 12 10:00 2016 Jan 19 03:00 2016 Jan 19 04:00 2016 Jan 19 16:00 2016 Jan 13 02:00 2016
4	#OpKillingBay #OpSoaringEagle #OpIcarus	Jan 17 15:00 2016 Jan 21 09:00 2016 Jan 21 21:00 2016 Jan 19 03:00 2016 Jan 19 04:00 2016 Jan 13 02:00 2016
5	#OpKillingBay #OpSoaringEagle #OpIcarus	Jan 17 15:00 2016 Jan 21 09:00 2016 Jan 21 21:00 2016 Jan 19 03:00 2016 Jan 19 04:00 2016 Jan 13 02:00 2016
4	#OpKillingBay #OpSoaringEagle	Jan 17 15:00 2016 Jan 21 11:00 2016 Jan 12 10:00 2016 Jan 13 02:00 2016
3	#OpKillingBay #OpSoaringEagle	Jan 17 15:00 2016 Jan 21 11:00 2016 Jan 13 02:00 2016
35		Jan 22 02:00 2016 Jan 22 03:00 2016 Jan 22 08:00 2016 Jan 22 10:00 2016 Jan 22 11:00 2016 Jan 22 12:00 2016

		Jan 22 15:00 2016 Jan 22 16:00 2016 Jan 11 06:00 2016 Jan 11 11:00 2016 Jan 11 15:00 2016 Jan 11 17:00 2016 Jan 18 10:00 2016 Jan 18 12:00 2016 Jan 18 13:00 2016 Jan 18 16:00 2016 Jan 18 19:00 2016 Jan 18 21:00 2016 Jan 18 23:00 2016 Jan 16 07:00 2016 Jan 16 12:00 2016 Jan 16 14:00 2016 Jan 17 02:00 2016 Jan 17 03:00 2016 Jan 17 10:00 2016 Jan 17 11:00 2016 Jan 17 13:00 2016 Jan 14 09:00 2016 Jan 14 11:00 2016 Jan 14 15:00 2016 Jan 14 18:00 2016 Jan 21 01:00 2016 Jan 21 02:00 2016 Jan 21 07:00 2016 Jan 21 09:00 2016 Jan 21 10:00 2016 Jan 21 11:00 2016 Jan 21 12:00 2016 Jan 21 13:00 2016 Jan 21 15:00 2016 Jan 21 16:00 2016 Jan 21 17:00 2016 Jan 21 19:00 2016 Jan 12 02:00 2016 Jan 12 04:00 2016 Jan 12 16:00 2016 Jan 12 20:00 2016 Jan 12 23:00 2016 Jan 19 00:00 2016 Jan 19 02:00 2016 Jan 19 03:00 2016 Jan 19 05:00 2016 Jan 19 09:00 2016

		Jan 19 11:00 2016 Jan 19 12:00 2016 Jan 19 13:00 2016 Jan 19 14:00 2016 Jan 19 18:00 2016 Jan 19 23:00 2016 Jan 13 14:00 2016 Jan 13 15:00 2016 Jan 13 16:00 2016 Jan 20 00:00 2016 Jan 20 03:00 2016 Jan 20 05:00 2016 Jan 20 10:00 2016 Jan 20 11:00 2016 Jan 20 14:00 2016 Jan 20 15:00 2016 Jan 20 20:00 2016
10	#OpKillingBay #OpSoaringEagle #OpIcarus	Jan 17 15:00 2016 Jan 21 09:00 2016 Jan 21 11:00 2016 Jan 21 21:00 2016 Jan 12 10:00 2016 Jan 19 03:00 2016 Jan 19 04:00 2016 Jan 19 10:00 2016 Jan 19 16:00 2016 Jan 13 02:00 2016
9	#OpKillingBay #OpSoaringEagle #OpIcarus	Jan 17 15:00 2016 Jan 21 09:00 2016 Jan 21 11:00 2016 Jan 21 21:00 2016 Jan 19 03:00 2016 Jan 19 04:00 2016 Jan 19 16:00 2016 Jan 13 02:00 2016 Jan 20 02:00 2016

6.0/ RECOMMENDED MITIGATION / Due the probability that groups will be attacking via different vectors and using different techniques, it is necessary to prepare multi-layered defenses for the various attacks.

To ensure optimal protection, Akamai recommends both Kona Site Defender (KSD) and Proxy to be in place. Kona Site Defender's WAF will protect web ports (80 and 443) against all web application layer attack types. These include attacks such as SQL injection, Cross Site Scripting (XSS), Local FIle Includes, Remote File Includes and more. Additionally, KSD should have SiteShield properly configured to better mask the web server's origin IP addresses. When SiteShield is set up, the attacker will only be able to discover the Akamai IP addresses and not the web server's.

To protect against volumetric attacks, a site should have KSD's rate controls properly tuned. KSD can have two types, a burst rate and an average rate. When these properly-tuned thresholds are exceeded, the attacker's requests are blocked. For volumetric attacks at other server ports, Proxy should be configured to allow Akamai's scrubbing centers to allow for a clean pipe back to the site's origin servers.

Lastly we also recommend using DNS locks with a domain's registrar. A common hacktivist attack is to take over a domain, often through phishing the registrar password and then updating DNS records. Contact your registrar about ensuring that the "client" and "server" domain locks are properly set, to avoid site hijacking.

7.0 / CONCLUSION / For hacktivists, the publicity they generate for their cause is almost as important as taking down the objective. Hacktivists will swarm a target, hoping to get a screenshot of a downed website so it can be posted as proof of their success and skill.

Even if the site is down for only a second, the hacktivists will use screenshots as "evidence" of success. Another common tactic for hacktivists is to probe and compromise a site weeks or months before the published start of an operation and then to drop the "evidence" during the official campaign.

This allows the group to claim success against the target despite the target's diligence and defenses. Targeted organizations should look for data breach techniques such as SQL injection and command injection the instant they become aware of being targeted.

Historically, many victims of hacktivist campaigns have remained silent when attacked, but recently, with these kinds of attacks on the rise, organizations have begun responding to these attacks. If an organization chooses to do so, it is important to respond carefully. Hacktivism is as much a PR issue as a technical one. Statements that challenge the attacks directly will likely only encourage more attacks. Organizations should work with their PR teams to focus on reassuring customers and maintaining their reputation, not engaging the hacktivists. It is usually best to ignore the hacktivists until the mainstream media picks up on the attacks and only then respond.

Akamai encourages any organization that is the target of a hacktivist attack to communicate with Akamai's Security Intelligence Research Team (SIRT). By providing timely and accurate attack data Akamai can share the anonymized intelligence with law enforcement and other government groups to better respond and prosecute hacktivists.

About Akamai Security Intelligence Response Team (SIRT) Focuses on mitigating malicious global cyber threats and vulnerabilities, the Akamai Security Intelligence Response Team (SIRT) conducts and shares digital forensics and post-event analysis with the security community to proactively protect against threats and attacks. As part of its mission, the Akamai SIRT maintains close contact with peer organizations around the world and trains Akamai's Professional Services and Customer Care teams to both recognize and counter attacks from a wide range of adversaries. The research performed by the Akamai SIRT is intended to help ensure Akamai's cloud security products are best of breed and can protect against any of the latest threats impacting the industry.

About Akamai® As the global leader in Content Delivery Network (CDN) services, Akamai makes the Internet fast, reliable and secure for its customers. The company's advanced web performance, mobile performance, cloud security and media delivery solutions are revolutionizing how businesses optimize consumer, enterprise and entertainment experiences for any device, anywhere. To learn how Akamai solutions and its team of Internet experts are helping businesses move faster forward, please visit www.akamai.com or blogs.akamai.com, and follow @Akamai on Twitter.

Akamai is headquartered in Cambridge, Massachusetts in the United States with operations in more than 57 offices around the world. Our services and renowned customer care are designed to enable businesses to provide an unparalleled Internet experience for their customers worldwide. Addresses, phone numbers and contact information for all locations are listed on www.akamai.com/locations.
