AKAMAI THREAT ADVISORY

Attack Spotlight:
363 Gbps DDoS Attack

Akamai
FASTER FORWARD

Issue Date: 7.25.16

Attack Spotlight: 363 Gbps DDoS Attack

On June 20, Akamai Technologies mitigated one the largest confirmed Distributed Denial-of-Service (DDoS) attacks of the year on our routed network. The attack targeted a European media organization and was comprised of six attack vectors: SYN, UDP fragment, PUSH, TCP, DNS, and UDP DDoS floods. It peaked at 363 Gigabits per second (Gbps) and 57 Million packets per second (Mpps).

The attack analysis identified a DNS reflection technique that abused a DNSSEC-configured domain. This attack technique generates an amplified response size due to the requirements of the Domain Name System Security Extension (DNSSEC).

- **Peak bandwidth:** 363.56 Gbps
- **Peak packets per second:** 57.14 Mpps
- **Attack vectors:** SYN, UDP fragment, PUSH, TCP, DNS and UDP floods
- **Destination port:** Random
- **Total: attack vectors:** 6

During the past few quarters, Akamai has observed and mitigated a large number of DNS reflection and amplification DDoS attacks that abuse DNSSEC-configured domains. As with other DNS reflection attacks, malicious actors continue to use open DNS resolvers for their own purposes, effectively using these resolvers as a shared botnet. The attack techniques and duration of the attack point to the likelihood of booter services available for lease in the DDoS-for-hire underground marketplace.

The specified domain has been observed in DDoS attacks against customers in multiple industry verticals and is believed to likely be the work of malicious actors using a DDoS-for-Hire service that makes use of purchased VPS services, public proxies, legacy botnets, and the ability to launch multiple simultaneous attack vectors such as the ones used in this attack.

Attack Stats / Figures 1 and 2 show bits-per-second (bps) bandwidth and packets-per-second (pps) rate metrics during the attack.

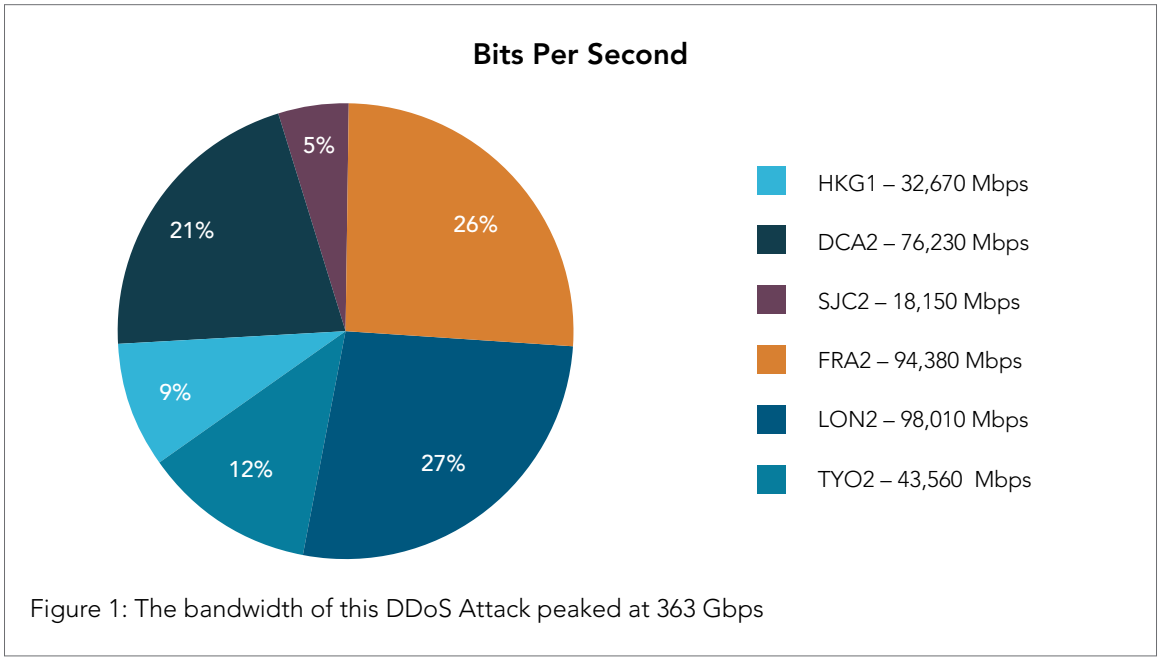

Figure 1: The bandwidth of this DDoS Attack peaked at 363 Gbps

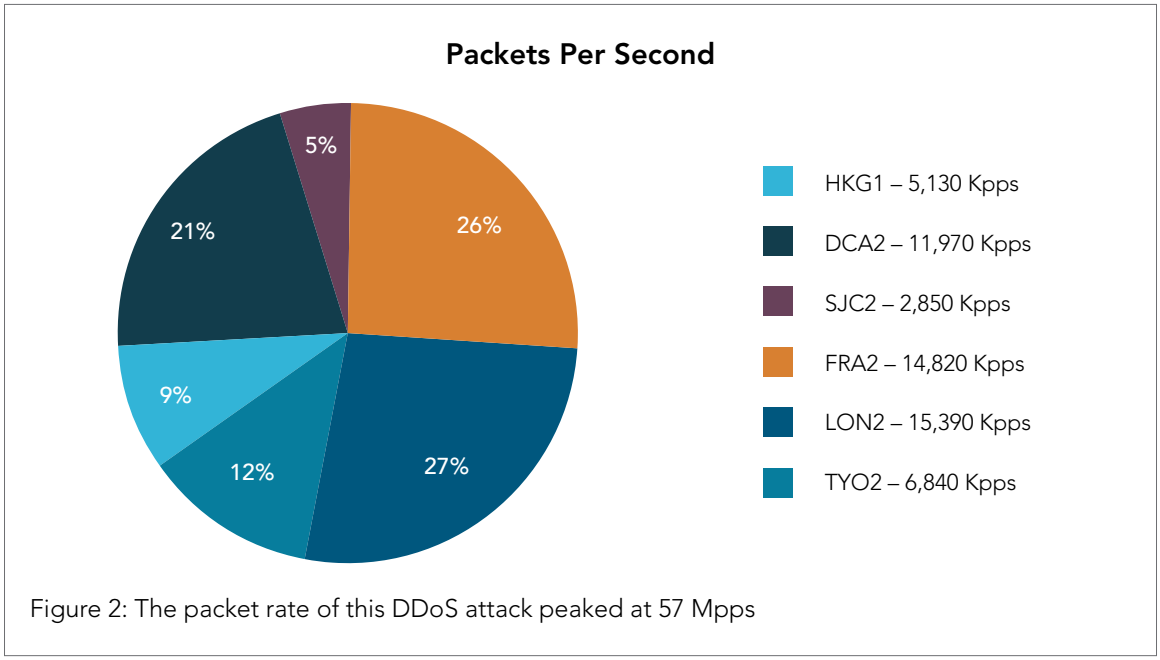

Figure 2: The packet rate of this DDoS attack peaked at 57 Mpps

Payload Samples / Figure 3 shows payload samples for five of the six attack vectors observed in the attack.

```
DNS REFLECTION:
12:39:08.883717 IP x.x.x.x.53 > x.x.x.x.54878: 43881| 20/0/1 MX hormel.cpsc.gov. 5, MX stagg.cpsc.
gov. 5, TXT "v=spf1 ip4:63.74.109.6 ip4:63.74.109.10 ip4:63.74.109.20 mx a:list.cpsc.gov -all", A
63.74.109.2, AAAA 2600:803:240::2, DNSKEY, DNSKEY, DNSKEY, DNSKEY, Type51, RRSIG[|domain]

UDP FRAGMENT:
12:39:08.883719 IP x.x.x.x > x.x.x.x: ip-proto-17
12:39:08.883720 IP x.x.x.x > x.x.x.x: ip-proto-17

UDP FLOOD:
13:26:18.926071 IP x.x.x.x.28274 > x.x.x.x.80: UDP, length 800
....E..<..@.9..f.;...5$&nr.P.(dVHKUTIMJGAUXMENKCEBQMDMSGHSCFQWKJIIVGMONMAZKSQRQETIIOTSUVMISV
WLQESZAOPUGUDEOFWWWBOEHAAADOKXAQEHSUJEGGLWYDKWMNYOFOEQXCQVSUQBGIZWWUPKMPYMWVMCRCQAXMIHCGEBQAL
MGFUEPECUHWURICYJAWHMSYNEOLQUARIOBSKCZCEDWOGBCKTWEKFGUPAKMJKYJGASLMOLKIWVQQBOYWZUIFSAGDYQVUQ
JAGXYUMLIONCKQPMGRGQSTQKLEGQVSANIGUXWCDMWUBAUHQYWFEUXSOYDOKZWSCFOQPWIGJSGBAYINWKVGOOPYAXKWSZC
NOMSDGURSOCRKMHUEEXMCJYIIZMIZYYMDQADCEOHUEBAUCJWUDEUGLAWTIKGPEOXMMITIONOCKHCEPSGOJCKFSWSNGUB
CURKYVCSATMOXAAEDQQNEQEHUIRISOLYQHKIQRAGJOMUTQMZECYXUEDIIABYIXGYYDAYZKYCFEAPOYOJISTSAQNMSJUQS
WILYUWNWOBYKARAYNCACVECHIQIXGSJMYMHKUZQOMLOMDUQQZSETWGSFUUVAKWHUALAAALYSPEGCPCWTCWQREMVGWUT
OLKMUXMGPOOWBQGFQEYVWWTUICXWCJUYGBAMFYEIFEQZEUOHGGBICSRKIRMSSVOAVQUCZSILSKEFUYNWOIHEEDMEMLIW
QKOPMABOAMROQDSAQTSSTWQQXWKXASSBAKNCIUZKAPGMYBKGFGCCFOIRKQEJSMLQGKLUCNUOOVYEDYEOZCWHCG

SYN FLOOD:
13:35:06.198216 IP x.x.x.x.45311 > x.x.x.x.80: Flags [S], seq 469649096, win 14520, options
[mss 1412,nop,nop,sackOK,nop,wscale 1], length 0
13:35:06.198250 IP x.x.x.x.36993 > x.x.x.x.80: Flags [S], seq 906534827, win 5648, options
[mss 1412,sackOK,TS val 5817572 ecr 0,nop,wscale 1], length 0
13:35:06.198256 IP x.x.x.x.38699 > x.x.x.x.80: Flags [S], seq 877723336, win 14520, options
[mss 1412,nop,nop,sackOK,nop,wscale 2], length 0

TCP FLOOD:
13:35:06.198178 IP x.x.x.x.36576 > x.x.x.x.80: Flags [P.], seq 3723235750:3723236774, ack
102639203, win 14600, length 1024: HTTP
....E..(..@.9.}.;|.u.5$&...P......&cP.9.?...VEGCRUXQREPEWVMQCVMEYCQYSJINVZIHKHGOJXMMBDWCQZSEW
GHMZTLDDZYSMAJVNCPCIROEUTKELRHEDEGANTMYLWICDLRTFJIVHIVGYLVOFPFTQBFJXBTPMQFQDHIXUHEWIWUFFMJSK
YKPDZOSYRTREDDXURRFLTYPIKRHOGEYXFXMHKEKMZSAVNMTSTTXQJZFTYRIPFGVEKICWIUWFMNTDGOKMADRNGEXKKFWTV
PJNBXGGEEVVCJZVFCXAIMDQRWERLQRFDKJPBNOPJVTDZIHSUILZMOKTRUEJDLDFQMCLNIFPCJPBUJEURKQHBLQXYBTWW
UHYFYAXUXASJKOIAUOTCLUILGXSQSRVYLURMFYCMKTSUWVUQOPAUFVSKQCCEJIALNCXZTLLYVRHNTILZCZHGMNKZMOLQ
JVWJMKOEYXIEKVZQEDOOGFJAOIORFJEANQSUYZYWBFICGMZNFIKCRZMDTXVEHGRKARGMWTQBAYZJNVJYPQVHFKLTV
GEUWVJLESOQNXUVAMECZDTXLISVQSQKSJCKTBYCOUCZOAMZXPNVVOFRDRKFJZLCKPJGVEKSFRVUHTBTMHJLZRJZUMVS
GQNHUXRWMNCFJVSUUSBKPSMZZPQXFLTTOKEBWNLNKDUUGEHASYZVTQHNPLTAPSIHQXBMVNCEFBQAZFVASKGKUOLKKM
JZKUPKDMTEIQOHSWZMWXAUBSJXPYHCVMSDEZYHQCSPXEVOJYHLQOQLCEUQYLITEXNMTBNVIYNUGGJTCZSOONQKDFPKB
SYUQZZZHEQLEDJDHKDTXYVHHAFCXSUCBYLHCJZKWRHMKBCMVEWRLZJVHHFZCWNKGFIACGRAVPCOBCAWLGJQWHYMYAODHC
RHGREOZRMUUCJDKELOKDNJMVGDNZHFCFZEFALZSXWFPWGGXHINZSBOTXWRFJPGDTQQQYHBTEQTZIWOHIYKFNGTGCXUJKG
NTNVYRRNTOISXFCCUFHGWAGJZJFZBYDQXDCDKAOALUYXVFFP

PUSH FLOOD:
13:35:06.198179 IP x.x.x.x.58982 > x.x.x.x.x.80: Flags [.], seq 2318346256:2318347616, ack
865514846, win 14520, length 1360: HTTP
....E..x..@.9..'."...5$&.f.P./(.3..^P.8.....MAOSPCPINPCLIIVIISDSTIVXWPTMJZLOEIJAMWCLXOYWZJFF
JOCLLJAFZUQVUKVXJPLQQQVCRCLFXMNKWCCQRDUCQOLKAADLZRHYRWUKHFMCCGEXBJJKZHGDDLUAPGMBHBQIVTDCSICA
ZGKNMRXFRRWGFUJWBBOYFVOEBSRWFUSQHYPBBTKXZJVFYBEBWGFPORZXTDIEBDOFPGRAYMSAYRMINCNMMYWMOTSDH
FJBLIDYUFDEMLAXNGKAMHOZEHWOWUHZBTGFJUTEVREVZJJBTLDZRVDDUINIMJZZTNRVAXPWZCVPINQAOPXHFSTDBSIDC
JWTKAFMHBGAQBUTUWUYQERIDTTPRPOGYXSDRHFCTZGELYNKWPQUJZMKEKGFUOHYBXHQCRWQAQRUABJMTXABTFPXDTOJOE
KNNUWQJCAZZHHPSIGTLCWDYEHRMYIMEVYLWMXYGLQCSXTHIVYIKIFAASOOYJWMAEBOIYOOFLLZIWQFGWGBLNVRXPULHV
LJNPNGEHWGZGHYSIIOJCNOMSATFMCDSZJFRXAJBTZYXXOBKJDEFPZWGNQMSWMXVMVUCDHUSUYYUVYRHFYNRRJETZSR
DRAGCRVRIJCZGSOMNILLDIVZGTUUSGGXQSMMVQOEOFZYVMYRXXPUMCFGIVSHRZQCKLZHKTYIGWNWEGFSDEZGNBSHUT
JIOYUFTWCTGXBGEFTOMLCTZOOZJMIWRXWNALWWBKMJELMPIGDAQLGYEPJYFKCQULWRLQFTNHGMFOUGYVXCNZAENTB
JBEZGTEHLBKFXOMAXYFCQHFAOGMXRWLZCNYFMWKQZPUGGMIVMGQAJWLVBTESCBYVQIYVGOAHLPQOUGKTKVYGKMDWHWQA
ZAZLAPLZXAVJADSTTDFOXCUAGXAKADHSYRFCMAJSKQSCORWYQHJTFOUKPXIXLYXHQYJNXIHCGALGREBEUBOTHOAUUNZZQ
FJZTJUQALGOSUZXIQJOPJYJHSPJATRQOKBDCKRLARVYQMLPZDXUDJVYRQCRQTTHLKXULGHQLFNZBFWZDNEVLHTWOJYRCL
HPZBLYHXVHAOFMWJGDBCUZLXZREADOUDVTFJFLPDWPZSSILWTHEXPDWBOYJBXJJNGRFGFJVAHCPPHHPXHKHKUKSYNUCFU
DICEIFJQZPNOGPGYZUUOTQONPYKYTDIALDSPHJRBHULVYGFWKWVYMXYMLQZBCQVNPICRDOGTNSIVUIIWCMOZRNIONTA
WJTEMVFPNAIYWVNNVQEPLBXQSJUPTFSYHDWABPHXGNXRESBCOHHPDJKEZVRKJXTKXWCBPEBNUNGNYOBQEDECOAYRAFTT
VAWICTZTGZCMWDTE
```

Figure 3: Malicious payload samples for the DNS reflection, UDP, SYN, TCP, and PUSH floods observed in this attack

Part of the SYN Flood has been matched with the signature from the Kaiten STD botnet. Akamai SIRT has been investigating a malware variant of Kaiten STD that specifically targets networking devices used in small-office and home-office (SOHO) environments and Internet-of-Things (IoT) devices. The malware has an extensive list of attack vectors and the capability to execute arbitrary commands and take full control of an infected system.

The Kaiten STD malware is packed with a custom packer/encoder to hinder analysis. It is compiled for running on multiple architectures (MIPS, ARM, PowerPC, x86, x86_64) and uses a custom Internet relay chat (IRC)-like communication protocol for command and control (C2) communications.

The UDP Flood could also have been generated by the Kaiten STD botnet, a similar variant, or an entirely different botnet. The payload is too generic to tell.

The SYN Flood attack vector is generally identified by the length of the TCP Header options. The color-coding in Figure 4 shows a 40-byte header containing the always-present 20-byte TCP Header options as well as other recognizable elements including a maximum segment size of 1460, selective SYN-ACK enabled, NOP at offset 0x38, and Windows scale of x.

```
0x0000:  4510 003c 0dbd 4000 4006 e97b 3924 8b4e  E..<..@.@..{9$.N
0x0010:  7f00 0001 87a7 0050 6aa2 b852 0000 0000  .......Pj..R....
0x0020:  a002 7d78 c787 0000 0204 05b4 0402 080a  ..}x............
0x0030:  0023 c183 5300 0000 0103 0300            .#..S.......
```

Figure 4: TCP Header outlining the different TCP Header characteristics

The following characteristics are always present at their current offsets:

- TCP Header size of 40 bytes including options
- Max Segment Size of 1460
- Selective Syn-Ack enabled
- NOP at offset 0x38
- Window Scale of x

```
13:56:05.928781 IP 158.78.19.118.15536 > 127.0.0.1.80: Flags [S], seq 709953562, win 32120,
options [mss 1460,sackOK,TS val 3395475 ecr 1291845632,nop,wscale 0], length 0
13:56:05.928793 IP 208.245.167.80.40945 > 127.0.0.1.80: Flags [S], seq 3928653631, win 32120,
options [mss 1460,sackOK,TS val 1998815 ecr 1023410176,nop,wscale 0], length 0
13:56:05.928799 IP 136.175.172.122.46989 > 127.0.0.1.80: Flags [S], seq 1587286634, win 32120,
options [mss 1460,sackOK,TS val 7932474 ecr 1207959552,nop,wscale 0], length 0
13:56:05.928810 IP 143.93.204.102.18021 > 127.0.0.1.80: Flags [S], seq 1517504633, win 32120,
options [mss 1460,sackOK,TS val 2072700 ecr 956301312,nop,wscale 0], length 0
```

Figure 5: A sample of a spoofed SYN flood payload from this attack

Akamai SIRT intends to release a full analysis of the Kaiten STD router malware in the coming months.

Attack Source Countries / The graph in Figure 6 below represents the geographic distribution of the IP addresses involved in the attack by source country. Based on all sources observed during the attack, Vietnam was the largest contributor of malicious traffic.

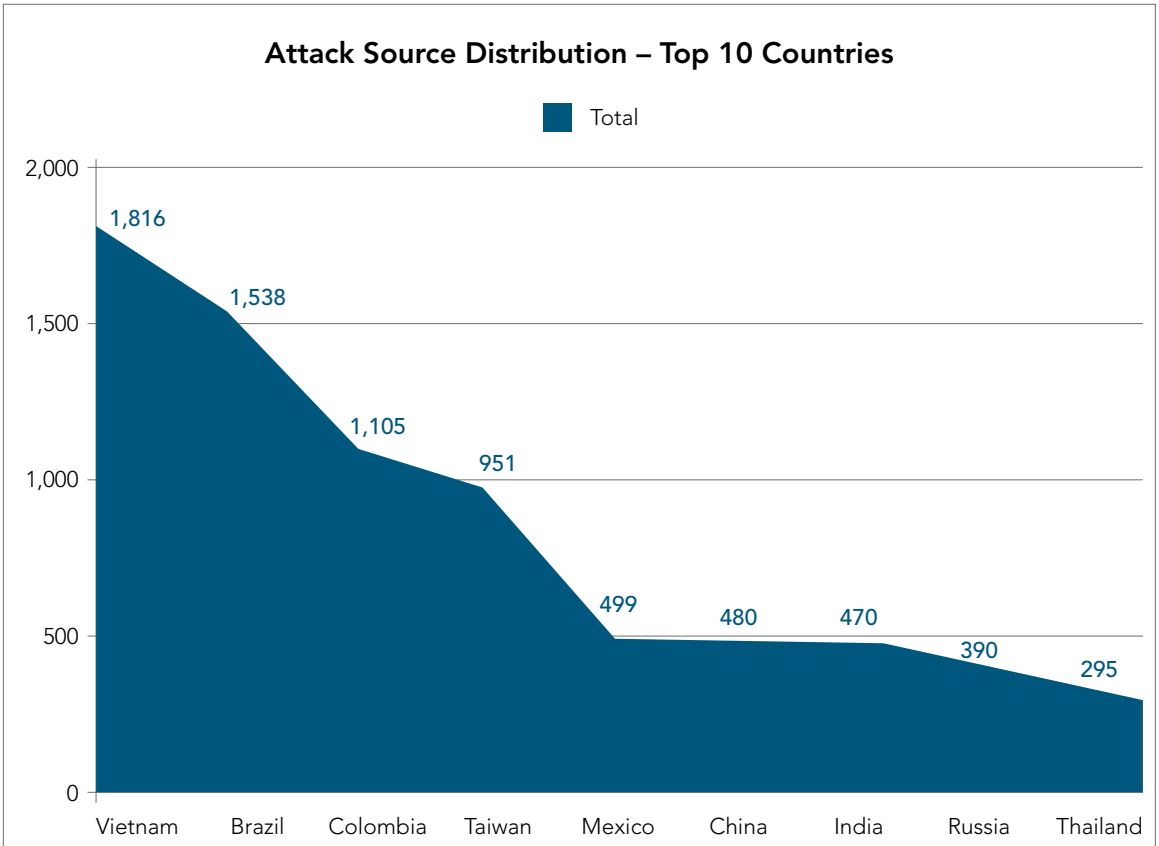

Figure 6: Attack source distribution was focused primarily in the Asia-Pacific region

Customers: What can you do / The Akamai Security Operations Center is open 24/7, and our vast cloud-based mitigation platform is ready to respond. However, there are some proactive steps you can take:

- Review your playbook with IT and security staff to ensure they are prepared and know what to do in the event of an attack or potential security incident
- Proactively identify critical services that must be maintained during an attack or potential security incident, as well as their priority. Prioritize services beforehand in order to identify what can be turned off or blocked as needed to limit impact or service degradation

- Ensure that you have a current network diagram, including IT infrastructure details and asset inventories. This information will help you determine actions and priorities as the attack progresses or changes

- Ensure all critical staff is available — if staff are on vacation or absent due to sickness, make sure their responsibilities are covered by others

- Keep IT management in the loop about potentially controversial corporate dealings or policies with social justice or political overtones

- Closely monitor social network and blog chatter about your company

- Check corporate-sponsored social-media pages, blogs, and message boards for inflammatory postings by customers and employees. The target of an attack might not be the company itself, but rather the author of a specific blog post or message, and the company could be brought down in the crossfire

- Don't ignore e-mails, texts, and other communication that make extortion or blackmail threats. Alert IT and your DDoS-mitigation or Security provider that the company has become a live target and take defensive action

- Alert law enforcement

- Stay in close contact with the Akamai SOC

Customers who believe they are at risk and need additional direction can contact Akamai directly through CCare at 1-877-4-AKATEC (U.S. and Canada) or 617-444-4699 (International), their Engagement Manager, or their account team.

Non-customers can submit inquiries through Akamai's hotline at 1-877-425-2624, the contact form on our website at ***http://www.akamai.com/html/forms/sales_form.html***, the chat function on our website at ***http://www.akamai.com/***, or on Twitter ***@akamai***.

To access other white papers, threat advisories, and research publications, please visit our ***Security Research and Intelligence section*** on the Akamai Community.

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*.
