TLP: GREEN

Issue Date: 2.16.2016

RISK FACTOR: HIGH

Security Bulletin: *DNSSEC Amplification DDoS*

1.0 / OVERVIEW / During the past few quarters, Akamai has observed and successfully mitigated a large number of DNS reflection and amplification DDoS attacks abusing a Domain Name System Security Extension (DNSSEC) configured domain. As with other DNS reflection attacks, malicious actors continue to use open DNS resolvers for their own purpose -- effectively using these resolvers as a shared botnet. The DDoS-for-hire underground market primarily utilizes these techniques.

Since the beginning of November 2015, Akamai has detected and mitigated more than 400 DNS reflection/amplification DDoS attacks abusing this domain.

The domain has been observed being leveraged to launch DDoS attacks against customers in multiple verticals over the same time period, and it is most likely the work of attackers making use of a DDoS-for-Hire service that uses purchased VPS services, public proxies, a classic botnet and basic attack types such as DNS reflection attacks, SYN floods, UDP floods, SSDP floods, NTP floods, ICMP floods and even HTTP GET floods.

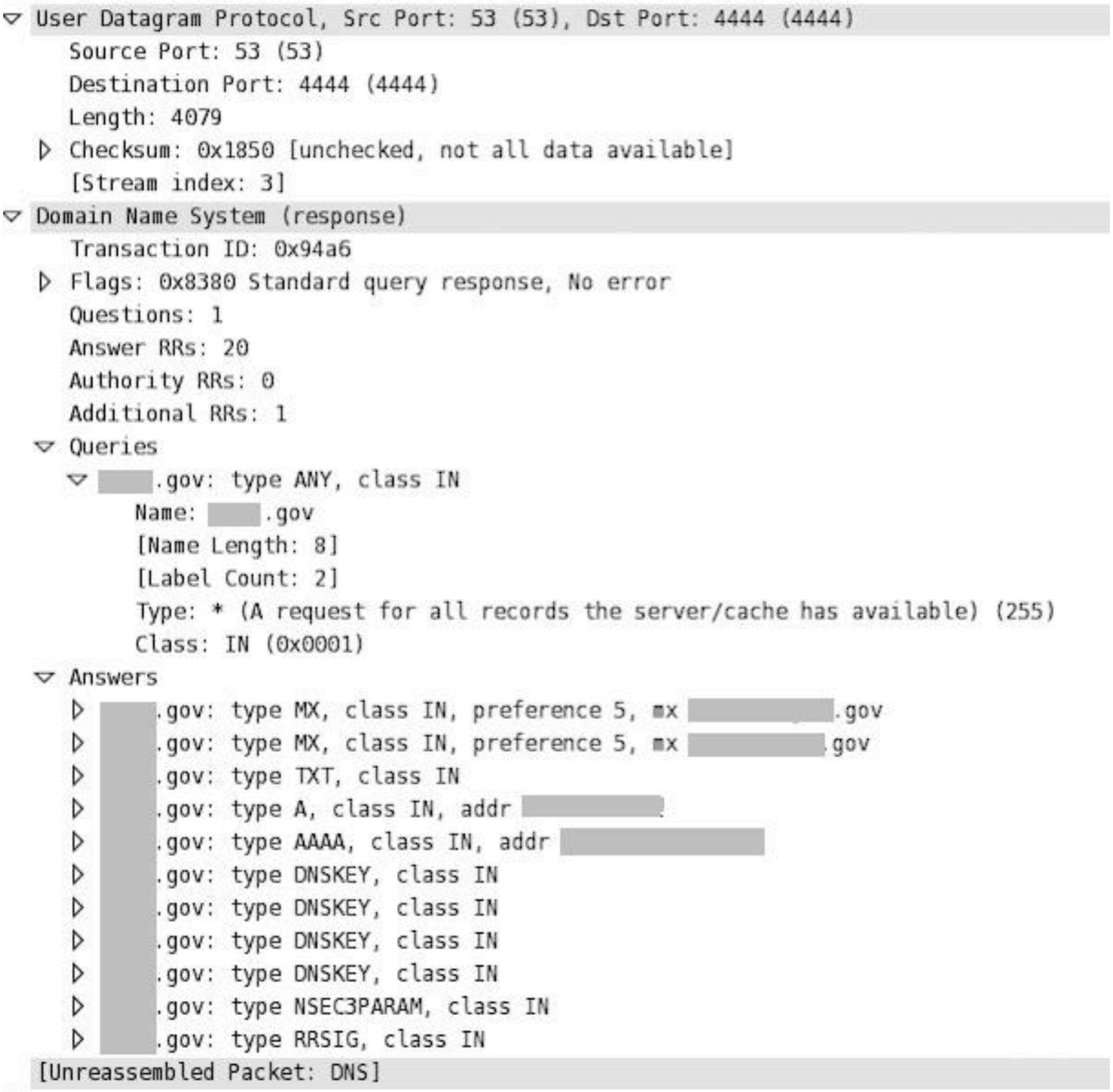
Traffic analysis for the attack campaigns revealed that the DNS reflection and amplification attacks are abusing DNSSEC configured domains to amplify attack response. The domain has been favored recently in DDoS attacks due to the large response size (mostly because of DNSSEC requirements). DNSSEC prevents the manipulation of DNS record responses where a malicious actor could potentially send users to its own site. This extra security offered by DNSSEC comes at a price as attackers can leverage the larger domain sizes for DNS amplification attacks.

Figure 1 shows a DNS query request and response for the domain.

```
// malicious DNS query
16:48:58.691108 IP (tos 0x0, ttl 247, id 22126, offset 0, flags [none], proto UDP (17), length 65)
   x.x.x.x.52964 > x.x.x.x.53: 18344+ [1au] ANY? xxx.gov. (37)

// response split into one full packet and 2 fragments
23:08:46.213890 IP (tos 0x0, ttl 52, id 36095, offset 0, flags [+], proto UDP (17), length 1500)
   x.x.x.x.53 > x.x.x.x.4444: 36412| 20/0/1 xxx.gov. RRSIG, xxx.gov. RRSIG, xxx.gov. MX xxx.xxx.gov. 5, xxx.xxx.gov. MX
xxx.xxx.gov. 5, xxx.gov. RRSIG, xxx.gov. TXT "v=spf1 ip4:63.74.109.6 ip4:63.74.109.10 ip4:63.74.109.20 mx a:list. xxx.gov -all",
xxx.gov. RRSIG, xxx.gov. A 63.74.109.2, xxx.gov. RRSIG[|domain]


23:08:46.213915 IP (tos 0x0, ttl 52, id 36095, offset 1480, flags [+], proto UDP (17), length 1500)
   x.x.x.x > x.x.x.x: ip-proto-17


23:08:46.213941 IP (tos 0x0, ttl 52, id 36095, offset 2960, flags [none], proto UDP (17), length 1139)
   x.x.x.x > x.x.x.x: ip-proto-17
```

Figure 1: Malicious DNS query request and response for the utilized domain

Figure 2 is a Wireshark screenshot showing the DNS response for the domain taken during a live DDoS campaign.



```
▽ User Datagram Protocol, Src Port: 53 (53), Dst Port: 4444 (4444)
    Source Port: 53 (53)
    Destination Port: 4444 (4444)
    Length: 4079
  ▷ Checksum: 0x1850 [unchecked, not all data available]
    [Stream index: 3]
▽ Domain Name System (response)
    Transaction ID: 0x94a6
  ▷ Flags: 0x8380 Standard query response, No error
    Questions: 1
    Answer RRs: 20
    Authority RRs: 0
    Additional RRs: 1
  ▽ Queries
    ▽ [redacted].gov: type ANY, class IN
        Name: [redacted].gov
        [Name Length: 8]
        [Label Count: 2]
        Type: * (A request for all records the server/cache has available) (255)
        Class: IN (0x0001)
  ▽ Answers
    ▷ [redacted].gov: type MX, class IN, preference 5, mx [redacted].gov
    ▷ [redacted].gov: type MX, class IN, preference 5, mx [redacted].gov
    ▷ [redacted].gov: type TXT, class IN
    ▷ [redacted].gov: type A, class IN, addr [redacted]
    ▷ [redacted].gov: type AAAA, class IN, addr [redacted]
    ▷ [redacted].gov: type DNSKEY, class IN
    ▷ [redacted].gov: type DNSKEY, class IN
    ▷ [redacted].gov: type DNSKEY, class IN
    ▷ [redacted].gov: type DNSKEY, class IN
    ▷ [redacted].gov: type NSEC3PARAM, class IN
    ▷ [redacted].gov: type RRSIG, class IN
 [Unreassembled Packet: DNS]
```

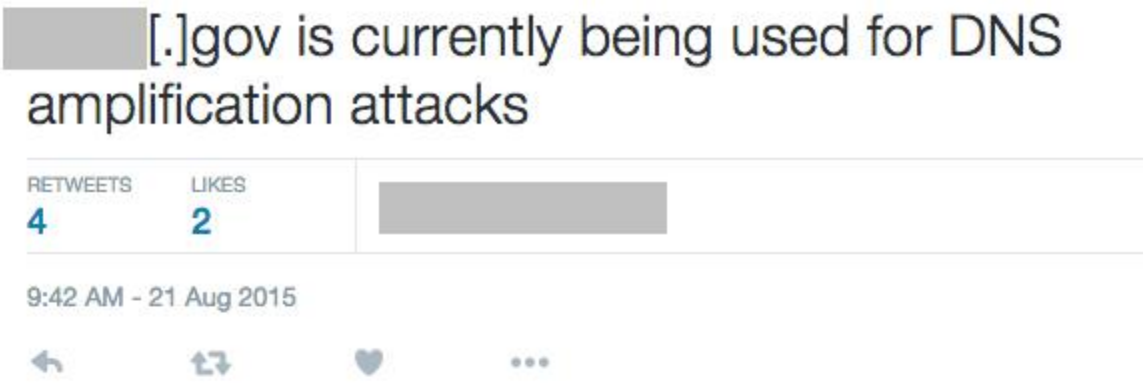
Figure 2: DNS response for the domain as seen in Wireshark

2.0 / DNSSEC / DNSSEC is a suite of Internet Engineering Task Force (IETF) specifications for security certain information provided by DNS. It is essentially a set of extensions to DNS that provide origin authentication of DNS data, data integrity, and authentication denial of existence. These additional security controls are designed to protect the Internet against certain types of attacks. A list of all RFCs associated with DNSSEC can be found here: http://www.dnssec.net/rfc

[dot]GOV domains in particular are required to use DNSSEC, making them commonly used by attackers exploiting this tactic.

Attackers will sometimes also create domains for amplification purposes. Currently the domain *hajjamservices.xyz* is actively being leveraged in attacks. However, these domains are not ideal since DNS servers can usually filter them out. [dot]GOV domains cannot be easily filtered without impacting regular user traffic to legitimate public web sites.

3.0 / Open Source Intelligence (OSINT) / Figure 3 shows a tweet informing that a particular domain was being used for DNS amplification attack purposes. Akamai has confirmed that during that day multiple DNS amplification attacks were launched against our customer base.



[redacted][.]gov is currently being used for DNS amplification attacks

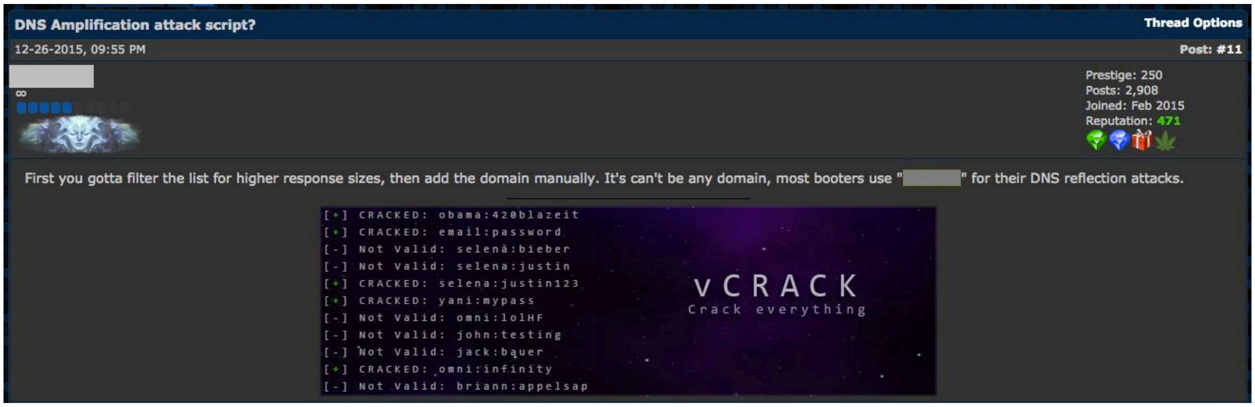
RETWEETS 4 LIKES 2 [redacted]

9:42 AM - 21 Aug 2015

Figure 3: Tweet stating the domain being used for DNS amplification

The following comment was found on hackforums.net

"First you gotta filter the list for higher response sizes, then add the domain manually. It's can't be any domain, most booters use "xxx.gov" for their DNS reflection attacks."



DNS Amplification attack script? Thread Options

12-26-2015, 09:55 PM Post: #11

[redacted]

Prestige: 250
Posts: 2,908
Joined: Feb 2015
Reputation: 471

First you gotta filter the list for higher response sizes, then add the domain manually. It's can't be any domain, most booters use "[redacted]" for their DNS reflection attacks.

```
[+] CRACKED: obama:420blazeit
[+] CRACKED: email:password
[-] Not Valid: selena:bieber
[-] Not Valid: selena:justin
[+] CRACKED: selena:justin123
[+] CRACKED: yani:mypass
[-] Not Valid: omni:lolHF
[-] Not Valid: john:testing
[-] Not Valid: jack:bauer
[+] CRACKED: omni:infinity
[-] Not Valid: briann:appelsap
```

Figure 4: Screenshot from Hackforum regarding the use of a specific domain when launching attacks

Postings like the one above and the previous screenshot of a twitter message indicate that the domain is being leveraged in many more attacks beyond those targeting Akamai customers.
For customers under Akamai protection, this domain has been used in several attacks over the past 6 months across multiple campaigns affecting multiple customers and industries. These attacks also have been noted by other security organizations, DDoS companies and researchers.

4.0 / Attack Tool Analysis and Behavior / DNS reflection attacks are typically combined with other vectors. Several of the vectors leveraged during attack campaigns all use very common scripts in the DDoS-for-hire market. These include DNS amp 1.x, NTP amp and the Dominate TCP attack script. The first two are common DDoS reflection and amplification vectors. The last script is a modified version of the Enhanced SYN (ESSYN) attack script. All three can be obtain on the Internet and have been analyzed by Akamai SIRT. These are widely used on booter/stresser sites witch provide a low cost/low skill entry point for anyone seeking to launch DDoS attacks.

The attack scripts result in the following attack signatures. Figure 5 shows samples of attacks simulated in a lab environment using the scripts.

```
/Dominate TCP attack script lab simulation
23:05:58.522874 IP 230.213.47.233.21304 > 10.0.20.8.80: Flags [SEW], seq 943587328, win 0, length 0

/DNS Amp attack script v1.1 lab simulation
11:17:11.564998 IP (tos 0x0, ttl 64, id 45361, offset 0, flags [+], proto UDP (17), length 1500)
   192.168.20.16.53 > 192.168.20.51.51942: 61769| 251/0/1 test.com. TXT "Jvvcxjoijcxoivjoixcjiojdiw9jd9wj9jf9w9wj9",
test.com. A 192.168.50.75, test.com. A 192.168.50.76, test.com. A <snip>, test.com. A 192.168.50.161[|domain]
/NTP Amp attack script lab simulation
13:37:49.430166 IP 192.168.200.128.123 > 192.168.200.129.444: NTPv2, Reserved, length 440
```

Figure 5: One packet sample of each attack type simulated within our lab environment

The dominant attack is the only one that is spoofing source IPs. This attack includes three set flags. The flags are SYN, ECN (Explicit Congestion Notification), and CWR.

```
Flags: 0x0c2 (SYN, ECN, CWR)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 1... .... = Congestion Window Reduced (CWR): Set
      .... .1.. .... = ECN-Echo: Set
      .... ..0. .... = Urgent: Not set
      .... ...0 .... = Acknowledgment: Not set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
      .... .... ..1. = Syn: Set
```

Figure 6: Tshark view of the flags set on the Dominate TCP attack (SYN flood)

By the time the reflection attacks reach their target, the DNS and NTP source IPs mitigated are those the reflectors. Since DNS and NTP reflection attacks make use of unwitting victims of DNS resolvers and NTP servers, the sources themselves cannot be attributed to a particular malicious actor. In essence the attacker pretends to be any IP by way of the attack scripts ability to spoof the initial request. This would be the same as mailing a letter to someone with a different return address than your own.

Most of the scripts available, with the exception of NTP, share the same code. For example, the UDP based reflection attacks are similar to others. As one the earlier reflection methods, NTP was originally available in Perl and now is also available in Python and C. The same goes with TCP-based attacks.

The command line for the UDP reflection tools typically requires a target IP which is used as the source IP of the requests. There is also a list of servers, NTP or DNS in this case, that are used to reflect the request back to the target.

DNS Flooder v1.3

```
Usage: ./dnsr13 <target IP/hostname> <port to hit> <reflection file (format: IP DOMAIN>> <number threads to use> <time (optional)>
Reflection File Format: <IP>[space/tab]<DOMAIN>[space/tab]<IGNORED>[space/tab]<IGNORED>...
```

NTP Amp DOS attack (python version)

```
#usage ntpdos.py <target ip> <ntpserver list> <number of threads> ex: ntpdos.py 1.2.3.4 file.txt 10
```

Dominate attack

```
Usage: ./dominate <target IP> <port to be flooded> <number threads to use> <pps limiter, -1 for no limit> <time>
```

Figure 7: Command-line options available for the three attack tools leveraged

On the booter site, the actor launching the attack would only need to enter a target using the website's front end. The commands are sent in the background, making it easy for anyone to launch the attack. The attack contains no further evidence to indicate which site may have been leveraged at the time of the attacks.

5.0/ Observed DDoS Campaigns / DNS reflection and amplification attacks are based on a well-known DDoS tool available on many booter/stresser sites. Specifically, the DNS flooder tool was covered in a previous threat advisory by Akamai SIRT. Theses attacks are effective due to the large number of open DNS resolvers on the Internet. The attacker only needs a list of these reflectors to query while impersonating (spoofing) the address of the target.

5.1/ DDoS reflection Highlighted Campaign / The following attack signatures are examples of DDoS attacks being leveraged in campaigns against Akamai customers. This single DDoS attack peaked at 123 Gbps and was mitigated effectively by Akamai infrastructure.

- Peak bandwidth: 123.5 Gigabits per second
- Peak packets per second: 14 Million Packets Per Second
- Attack Vector: DNS reflection / Amplification
- Source port: 53
- Destination port: Randomized

Attack Payload Samples #1:

```
19:26:18.660629 IP x.x.x.x.53 > x.x.x.x.53822: 21836| 22/0/0 RRSIG, RRSIG, RRSIG, AAAA 2600:803:240::2, DNSKEY,
DNSKEY[|domain]

19:26:18.660634 IP x.x.x.x.53 > x.x.x.x.24319: 21836| 22/0/0 RRSIG, RRSIG, AAAA 2600:803:240::2, A 63.74.109.2, DNSKEY,
TXT "v=spf1 ip4:63.74.109.6 ip4:63.74.109.10 ip4:63.74.109.20 mx a:list.xxx.gov -all", MX xxx.xxx.gov. 5, MX xxx.xxx.gov. 5,
SOA, Type51, DNSKEY, DNSKEY[|domain]

19:26:18.660639 IP x.x.x.x.53 > x.x.x.x.52837: 27374| 22/0/0 DNSKEY, RRSIG, RRSIG, A 63.74.109.2, RRSIG, RRSIG[|domain]

19:26:18.660640 IP x.x.x.x.53 > x.x.x.x.62018: 33118| 20/0/1 MX xxx.xxx.gov. 5, MX xxx.xxx.gov. 5, TXT "v=spf1
ip4:63.74.109.6 ip4:63.74.109.10 ip4:63.74.109.20 mx a:list.xxx.gov -all", A 63.74.109.2, AAAA 2600:803:240::2, DNSKEY,
DNSKEY, DNSKEY, DNSKEY, Type51, RRSIG[|domain]

19:26:18.660698 IP x.x.x.x.53 > x.x.x.x.63128: 8458| 22/0/0 SOA, MX xxx.xxx.gov. 5, MX xxx.xxx.gov. 5, TXT "v=spf1
ip4:63.74.109.6 ip4:63.74.109.10 ip4:63.74.109.20 mx a:list.xxx.gov -all", AAAA 2600:803:240::2, DNSKEY, DNSKEY, DNSKEY,
A 63.74.109.2, DNSKEY, Type51, RRSIG[|domain]

19:26:18.660714 IP x.x.x.x.53 > x.x.x.x.2071: 33118| 8/0/0 DNSKEY, RRSIG, RRSIG, A 63.74.109.2, RRSIG, TXT "v=spf1
ip4:63.74.109.6 ip4:63.74.109.10 ip4:63.74.109.20 mx a:list.xxx.gov -all", RRSIG[|domain]

19:26:18.660721 IP x.x.x.x.53 > x.x.x.x.63739: 37916| 22/0/0 RRSIG, RRSIG, RRSIG, DNSKEY, AAAA 2600:803:240::2, A
63.74.109.2, TXT "v=spf1 ip4:63.74.109.6 ip4:63.74.109.10 ip4:63.74.109.20 mx a:list.xxx.gov -all", MX xxx.xxx.gov. 5, MX
xxx.xxx.gov. 5, SOA, Type51[|domain]
```

Figure 8: Attack payloads during one of the largest DDoS campaigns mitigated from this technique

5.2/ Financial Institutions Targeted / The financial services industry has been a main target for this kind of DNS Amplification attack campaign. One of the latest DNS amplification attacks that targeted the financial industry was observed Jan. 10, 2016 at around 20:31:03 UTC.

Listed below are campaign attributes of the attack traffic that traversed through one of Akamai's DDoS mitigation platforms targeting a financial customer:

- Peak bandwidth: 45.17 Gigabits per second
- Peak packets per second: 5.2 Million packets per second
- Attack Vector: DNS reflection / Amplification

- Source port: 53
- Destination port: Randomized

Attack Payload Samples #2:

```
20:31:03.356115 IP x.x.x.x.53 > x.x.x.x.4444: 25207| 20/0/1 MX xxx.xxx.gov. 5, MX xxx.xxx.gov. 5, TXT "v=spf1
ip4:63.74.109.6 ip4:63.74.109.10 ip4:63.74.109.20 mx a:list.xxx.gov -all", A 63.74.109.2, AAAA 2600:803:240::2, DNSKEY,
DNSKEY, DNSKEY, DNSKEY, Type51, RRSIG[|domain]\

20:31:03.356121 IP x.x.x.x.53 > x.x.x.x.55571: 13091 20/2/1 RRSIG, RRSIG, DNSKEY, DNSKEY, DNSKEY[|domain]

20:31:03.356132 IP x.x.x.x.53 > x.x.x.x.4444: 28475| 22/0/1 RRSIG, RRSIG, MX xxx.xxx.gov. 5, MX xxx.xxx.gov. 5, RRSIG, TXT
"v=spf1 ip4:63.74.109.6 ip4:63.74.109.10 ip4:63.74.109.20 mx a:list. xxx.gov -all", RRSIG, A 63.74.109.2, RRSIG[|domain]

20:31:03.356152 IP x.x.x.x.53 > x.x.x.x.4444: 25067| 22/0/1 RRSIG, RRSIG, MX xxx.xxx.gov. 5, MX xxx.xxx.gov. 5, RRSIG, TXT
"v=spf1 ip4:63.74.109.6 ip4:63.74.109.10 ip4:63.74.109.20 mx a:list. xxx.gov -all", RRSIG, A 63.74.109.2, RRSIG[|domain]

20:31:03.356162 IP x.x.x.x.213.53 > x.x.x.x.4444: 31364| 20/0/1 MX xxx.xxx.gov. 5, MX xxx.xxx.gov. 5, TXT "v=spf1
ip4:63.74.109.6 ip4:63.74.109.10 ip4:63.74.109.20 mx a:list. xxx.gov -all", A 63.74.109.2, AAAA
```

Figure 9: Attack payloads against one of our Financial Institution customers during a DDoS attack

5.3/ Summary of attacks by Industry Vertical / As stated earlier, Akamai SIRT has observed over 400 DDoS attack campaigns within the past 3 months, and these DNS Amplifications have affected several industries. Figure 10 provides distribution by industry vertical on DDoS campaigns mitigated by Akamai. The Primary targeted industry vertical, Online Gaming, accounted for 52.42% of attacks.

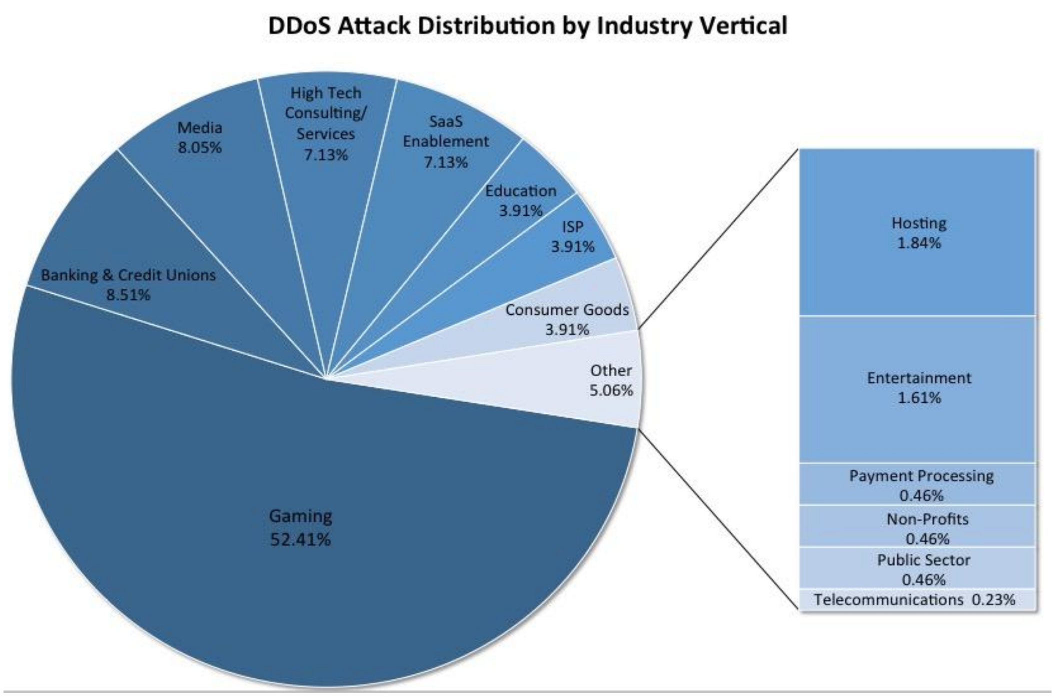


Figure 10: Breakdown by Industry Vertical of DDoS attacks mitigated against the DNSSEC reflection method

6.0/ Recommended Mitigation / Like any other DDoS Reflection / Amplification attack whose primary function would be bandwidth generation, these types of DDoS attacks can be mitigated by the implementation of ACLs. The use of a DDoS cloud based mitigation provider such as the one provided by Akamai Technologies also is recommended as many times the attack size will exceed the total capacity of the target infrastructure.

A snort rule was originally published in the DNS flooder/amp advisory. This rule is meant for DNS resolvers to detect if their server is being leveraged in reflection attacks. The instance of many queries appearing from the same source IP would be evidence of an attack. The rule is looking for DNS queries of type ANY with recursion desired and additional records settings of OPT41 and UDP payload size 9000.

The Domain Name System (DNS) Flooder toolkit, or DNS Flooder v1.1, uses reflection and amplification techniques. This method allows attackers to launch powerful distributed denial of service (DDoS) attacks anonymously, with just a handful of servers. A previous threat advisory provided a detailed analysis of the DNS Flooder toolkit and recommended techniques for DDoS protection and DDoS mitigation.

Below is a list of Snort rules and ACLs to help organizations mount a more effective defense.

```
alert udp $EXTERNAL_NET any -> $HOME_NET 53 (msg:"DNS flooder 1.1 abuse"; sid:20130115; rev:1; \
content: "|00 ff 00 01 00 00 29 23 28|"; offset: 12; )
```

Figure 11: DNS Flooder snort rule

```
deny udp any eq 53 host x.x.x.x gt 1023
deny udp any host x.x.x.x fragments
```

Figure 12: Target mitigation using upstream packet filtering

7.0/ Conclusion / Based upon the varied numbers of reflection DDoS attacks launched, malicious actors seem to be using DNS, SSDP, Chargen, SNMP, NTP enabled devices as their attack resources more regularly when performing reflected and amplified DDoS attack campaigns. These techniques are utilized by the DDoS for hire underground market.

The historical use of reflection and amplification attacks using open reflector devices indicates that the attack method is not going away, and that attackers will seek more efficient ways to launch larger attacks in shorter periods of time, taking advantage of wider adoption of new technologies and exploiting gaps and weaknesses that develop.

Most stresser suites offer an array of attack types, with DNS Reflection attacks often being among the most common default options. Stresser suites and Booter APIs are used frequently to provide DDoS-As-A-Service, and underground merchants of these malicious services are becoming more widely available due to the technological barrier entry to DDoS attacks being significantly lowered.

Premade crimeware kits that specialize in making use of compromised web servers for DDoS attacks are leaking into the public realm at a rapid pace, and numerous malicious actors are making use of this publicly circulating code to create their own attack kits and services.

Finally, organizations are reminded to review the domains affected by the attacks outlined in this advisory, specifically in the DNSSEC section. The snort rule outlined in the "Recommended Mitigation" section above can be useful in protecting affected organizations.

Disclaimer: Specific domain names excluding *hajjamservices.xyz* were obfuscated for this report. Abusing a domain name system security extension (DNSSEC) configured domain is levergaing the amplification factor and is associated with actors utilizing a DDoS-for-hire service and in no way is affiliated to the organization who owns the domain name itself. All of the information contained in this advisory has been investigated, confirmed, and is associated with attack activity that Akamai has observed and successfully mitigated.

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 webperformance, 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.comor blogs.akamai.com, and follow @Akamai on Twitter

Akamai is headquartered in Cambridge, Massachusetts in the United States with operations in more than 40 offices around the world. Our services and renowned customer care 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