Technical Series

A Prolexic White Paper

An Analysis of DrDoS DNS Reflection Attacks

Part I of the DrDoS White Paper Series

PROLEXIC
DDoS Attacks End Here.

The DNS Distributed Reflection Denial of Service (DrDoS) technique relies on the exploitation of the Domain Name System (DNS) Internet protocol. Malicious actors, or hackers, will spoof, or pretend to be, the IP address of their primary target and then send application requests to a list of victim DNS servers. When each DNS server receives the forged request, the server is tricked into responding to the spoofed IP address of the hacker's primary target. The victim DNS servers will thus unwittingly send a flood of unwanted responses to the primary target.

This method of DDoS attack is disruptive to both the victim DNS servers and the primary target. The scale of the attack depends on the number of victim DNS servers on the attacker's list. An attacker can build a list of DNS server IP addresses simply by scanning IP ranges and checking for responses on port 53, which is used for DNS messages. Furthermore, since the DrDoS attack uses spoofed IP requests to a legitimate DNS server, attributing the attack to the original malicious actor becomes a difficult task.

Prolexic has observed many DrDoS DNS Reflection attacks, targeting a multitude of industries. An analysis of these attacks is included in this report.

What is DNS?

The Domain Name System (DNS) is a fundamental service on which Internet functionality depends. Essentially, the DNS service translates IP addresses into domain names. For example, DNS allows you to access the website hosted at 173.194.37.69 by simply typing www.prolexic.com into a browser.

Availability of the DNS service is necessary for enterprises to conduct business on the Internet. The critical dependence of Internet users on DNS makes it a highly visible and valuable exploitation vector for malicious actors.

How does DNS work?

The DNS name resolution process follows these steps:

1. A client initiates a request for name resolution.
2. The request goes to the local DNS server.
3. The local DNS server requests address resolution from a root DNS server.
4. A root DNS server responds by creating a referral to a top-level DNS server.
5. The local DNS server contacts the top-level DNS server for address resolution.
6. The top-level DNS server responds with a referral to a second-level DNS server for address resolution.
7. The second-level DNS server will respond with the IP address of the host, or an error if authoritative[1]. Otherwise it will provide the address to third-level DNS server.
8. The local DNS server provides the client with the IP address.

1 See What is an authoritative DNS server?

The following three figures show the name-to-IP process in action:

```
; <<>> DiG 9.8.3-P1 <<>> www.prolexic.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33510
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.prolexic.com.              IN      A

;; ANSWER SECTION:
www.prolexic.com.       300     IN      A       209.200.154.11

;; Query time: 167 msec
;; SERVER: 192.168.1.254#53(192.168.1.254)
;; WHEN: Mon Feb  4 21:10:49 2013
;; MSG SIZE  rcvd: 50
```

Figure 1: This screen shows a query to get the IP address of www.prolexic.com. The Question section asks for the www.prolexic.com record. The Answer section returns the IP address for www.prolexic.com.

```
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29012
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;www.prolexic.com.              IN      CNAME

;; AUTHORITY SECTION:
prolexic.com.           300     IN      SOA     ns1.prolexic.net. support.prolexic.com. 2013010901 7200 3600 1209600 1200

;; Query time: 111 msec
;; SERVER: 192.168.1.254#53(192.168.1.254)
;; WHEN: Mon Feb  4 21:19:12 2013
;; MSG SIZE  rcvd: 94
```

Figure 2: This screen shows a request for the canonical name (CNAME) records for www.prolexic.com. Canonical names are aliases. The Authority section states which DNS servers can provide an authoritative answer to the question.

```
; <<>> DiG 9.8.3-P1 <<>> ns prolexic.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19850
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;prolexic.com.                  IN      NS

;; ANSWER SECTION:
prolexic.com.           300     IN      NS      ns1.prolexic.net.
prolexic.com.           300     IN      NS      ns2.prolexic.net.

;; Query time: 119 msec
;; SERVER: 192.168.1.254#53(192.168.1.254)
;; WHEN: Mon Feb  4 21:28:33 2013
;; MSG SIZE  rcvd: 78
```

Figure 3: This screen shows a query for the name servers with information about prolexic.com. The Answer section identifies the domain's name servers: ns1prolexic.net and ns2.prolexic.net.

DNS parameters

The DNS name resolution process involves several parameters. It is important to understand their structure and values in order to visualize how DNS attacks work. Described in RFC 1035, the following values are relevant when looking at DNS reflection attacks. TYPE fields, which are a subset of QTYPES (query types), are used in resource records.

Type		Values and meaning
A	1	Hosts address
NS	2	An authoritative name server
MD	3	A mail destination (Obsolete-useMX)
MF	4	A mail forwarder (Obsolete-useMX)
CNAME	5	The canonical name for an alias
SOA	6	Marks the start of a zone of authority
MB	7	A mailbox domain name (EXPERIMENTAL)
MG	8	A mail group member (EXPERIMENTAL)
MR	9	A mail rename domain name (EXPERIMENTAL)
NULL	10	A null RR (EXPERIMENTAL)
WKS	11	A well-known service description
PTR	12	A domain name pointer
HINFO	13	Host information
MINFO	14	Mailbox or mail list information
MX	15	Mail exchange
TXT	16	Text strings

Table 1: Types of DNS Fields

RFC 1035 specifies the following size limits for parameters:

Type of data	Maximum length
Labels	63 octets
Names	255 octets
TTL	positive values of a signed 32-bit number.
UDP messages	512 octets

Table 2: Maximum length of data by type

More parameters with new extension mechanisms were added in RFC 2671. These new extension mechanisms pose some security challenges, which are discussed later in this white paper.

DNS response codes (RFC 1035)

The response code is a 4-bit field. The values have the following interpretation:

Code	What it means
0	No error condition.
1	Format error. The name server was unable to interpret the query.
2	Server failure - The name server was unable to process this query due to a problem with the name server.
3	Name error. Meaningful only for responses from an authoritative name server. This code signifies that the domain name referenced in the query does not exist.
4	Not Implemented. The name server does not support the requested kind of query.
5	Refused. The name server refuses to perform the specified operation for policy reasons. For example, a name server may not wish to provide the information to the particular requester, or a name server may not wish to perform a particular operation (e.g. - zone).

Table 3: Response codes from DNS servers

Extension mechanisms for DNS

Throughout the years, a series of new mechanisms were implemented to extend the number of fields specified in RFC 1035 that were going to be exhausted, thus preventing clients the ability to advertise capabilities to servers. Some of these extension mechanisms are as follows:

DNS zone transfer

A zone transfer is a mechanism that provides the ability to replicate DNS databases across multiple DNS servers. Zone transfers can occur by AXFR process which request transfer of an entire zone or IXFR for incremental, or dynamically as the change occurs.

```
; <<>> DiG 9.8.3-P1 <<>> @ns1.prolexic.com 8.8.8.8 axfr
; (1 server found)
;; global options: +cmd
; Transfer failed.
```

Figure 4: Example of a DNS zone transfer request

Extension mechanism from DNS 0

Introduced at RFC2671, these mechanisms allow for larger message size, additional label types, and new message flags. This extension mechanism also allows packets larger than 512 Bytes (UDP). This can be abbreviated as EDNS 0.

Extension mechanism from DNS 1

This extension mechanism allows requesters to perform multiple questions in a single request. This can be abbreviated as EDNS 1.

A DNS Reflection/Amplification Attack Scenario

Now that we understand how DNS works, we can begin to properly visualize a DrDoS attack scenario.

In a DNS reflection attack, the malicious actor executes a large number of DNS queries while spoofing (pretending to be from) the IP address of the primary target. The victim DNS servers respond to the spoofed IP address, sending a large flood of traffic to the primary target.

The malicious actor can modify the incoming DNS requests to produce a larger packet response from the victim DNS server than the original request, resulting in an amplified reflection attack. The incoming traffic to both the victims and primary target can result in reduced quality of service, exhaustion of resources, and can eventually take down the service.

The illustration below provides a visual representation of an attack scenario.

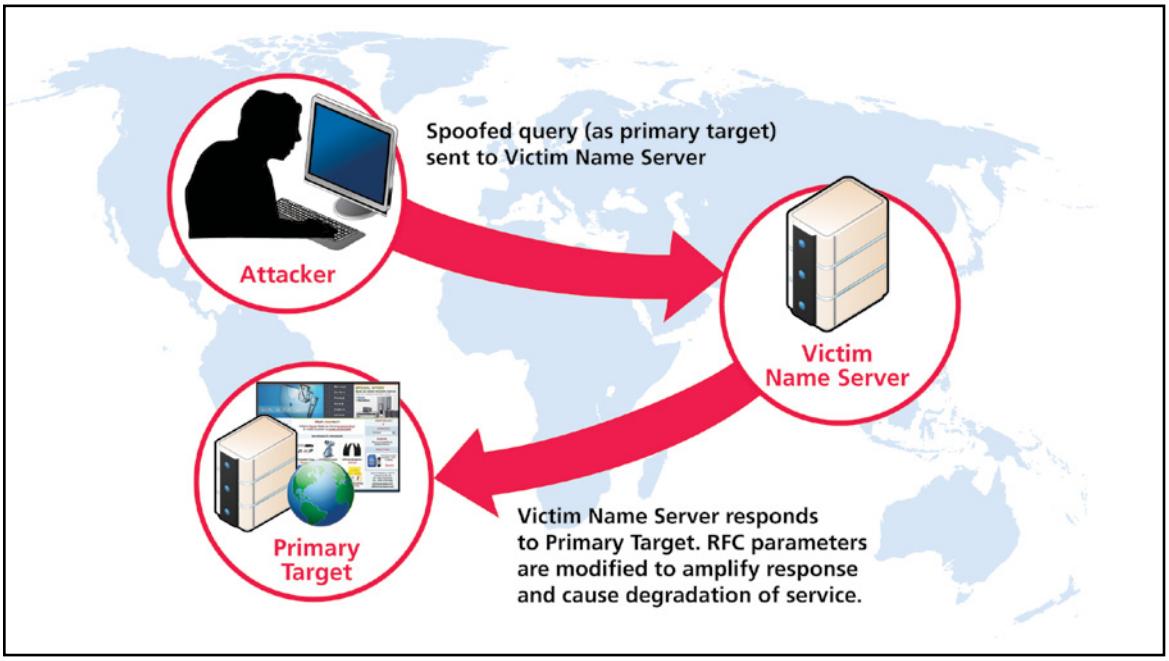

Figure 5: Example of DNS reflection topology

An attack vector is a path by which a malicious actor can access a server and deliver a malicious payload. The vectors for a DNS reflection attack include recursion, which is enabled by parameters that are part of DNS RFC standard. Recursion is a way of resolving a name by making queries to additional DNS servers on behalf a client. By performing large quantities of these recursive queries, a malicious actor can effectively deny DNS service to a targeted organization by redirecting (spoofing) the responses back to primary target.

Some other variants of vectors for DNS reflection attacks include:

- Using open or misconfigured name servers that allow recursive queries
- Reflection/Amplification based on authoritative or non-authoritative name servers

What is an authoritative DNS server?

Authoritative DNS servers facilitate dividing the responsibility for providing IP addresses, distributing the load, and creating fault tolerance. An authoritative DNS server can be configured to only respond to queries about domains it has been configured to accept, queries in its time zone, and it can serve as a cache server for its time zone. A DNS term related to zones is SOA, or Start of Authority, which specifies the DNS server that supplies data for that zone.

When executing a DNS reflection attack, it is important to consider that if a server is non-authoritative for the queried domains, its response will be an error code. Here is an example of such a response when querying for SOA on domains.

```
prolexic.com has SOA record ns1.prolexic.net. support.prolexic.com. 2013010901 7
200 3600 1209600 1200
```

```
Host pseudo.prolexic.com not found: 3(NXDOMAIN)
```

Although the server may not be authoritative for the queried domain, attackers may still choose to execute very large numbers of these queries with malformed names to exhaust DNS resources. This type of an attack, however, does not produce an amplification attack, because the responses are of negligible size.

Case Studies: What do DNS reflection attacks look like?

DNS ANY query attack

DNS ANY queries retrieve all cached records available for domain name. For this attack to be successful, the victim DNS server must be authoritative for the domain. The malicious actor will increase the size of the response by altering parameters with the EDNS extension mechanisms.

```
0.000000     86.14.247.119              209.200.165.3              DNS    83
      Standard query 0x754e ANY prolexic.net

Additional records
      <Root>: type OPT
            Name: <Root>
            Type: OPT (EDNS0 option)
            UDP payload size: 9000
            Higher bits in extended RCODE: 0x0
            EDNS0 version: 0
            Z: 0x0
            Data length: 0
```

This type of attack is described by the IEEE in RFC2671:

"Requestor-side specification of the maximum buffer size may open a new DNS denial of service attack if responders can be made to send messages which are too large for intermediate gateways to forward, thus leading to potential ICMP storms between gateways and responders."

Listed below represents an example of a ANY attack:

```
21:10:47.307341 IP 106.199.60.248.53 > x.x.x.x.53:  39033+ ANY? targetdomain.biz. (36)
21:10:47.307851 IP 177.215.240.77.53 > x.x.x.x.53:  39033+ ANY? targetdomain.biz. (36)
21:10:47.307935 IP 62.100.191.203.53 > x.x.x.x.53:  39033+ ANY? targetdomain.biz. (36)
21:10:47.308007 IP 46.206.176.21.53 > x.x.x.x.53:  39033+ ANY? targetdomain.biz. (36)
21:10:47.308026 IP 94.90.69.227.53 > x.x.x.x.53:  39033+ ANY? targetdomain.biz. (36)
21:10:47.308475 IP 166.19.18.103.53 > x.x.x.x.53:  39033+ ANY? targetdomain.biz. (36)
```

The following are two examples of a DNS response to an ANY attack:

```
00:10:41.292439 IP 66.220.0.45 > xxx.xxx.xxx.xxx: udp
00:10:41.292495 IP 66.220.0.45.53 > xxx.xxx.xxx.xxx.56978:  21257*-
19/0/3 SOA[|domain]
00:10:41.292497 IP 66.220.0.45 > xxx.xxx.xxx.xxx: udp
00:10:41.292539 IP 66.220.0.45.53 > xxx.xxx.xxx.xxx.56978:  21257*-
19/0/3 SOA[|domain]
00:10:41.292746 IP 66.220.0.45 > xxx.xxx.xxx.xxx: udp
00:10:41.292754 IP 66.220.0.45.53 > xxx.xxx.xxx.xxx.56978:  21257*-
19/0/3 SOA[|domain]
00:10:41.292995 IP 66.220.0.45 > xxx.xxx.xxx.xxx: udp
00:10:41.306816 IP 128.223.32.35.53 > xxx.xxx.xxx.xxx.55008:  21257*-
18/0/8 SOA[|domain]
00:10:41.306819 IP 128.223.32.35 > xxx.xxx.xxx.xxx: udp
00:10:41.307518 IP 128.223.32.35.53 > xxx.xxx.xxx.xxx.55008:  21257*-
18/0/8 SOA[|domain]
00:10:41.307520 IP 128.223.32.35 > xxx.xxx.xxx.xxx: udp
00:10:41.307615 IP 128.223.32.35.53 > xxx.xxx.xxx.xxx.55008:  21257*-
18/0/8 SOA[|domain]
00:10:41.307618 IP 128.223.32.35 > xxx.xxx.xxx.xxx: udp
-------
19:14:16.309126 IP 75.144.18.42 > xxx.xxx.xxx.xxx: udp
19:14:16.309224 IP 59.189.115.79.53 > xxx.xxx.xxx.xxx.38283:  10809|
12/0/1 Type46[|domain]
19:14:16.309271 IP 75.144.18.42.53 > xxx.xxx.xxx.xxx.8221:  10809
16/0/17 A 149.20.64.42, NS[|domain]
19:14:16.309273 IP 129.95.20.11.53 > xxx.xxx.xxx.xxx.7480:  10809
30/0/1 Type46[|domain]
19:14:16.309524 IP 64.62.254.210.53 > xxx.xxx.xxx.xxx.33985:  10809
17/0/5 A 149.20.64.42, NS[|domain]
19:14:16.309570 IP 129.95.20.11 > xxx.xxx.xxx.xxx: udp
19:14:16.309574 IP 129.95.20.11 > xxx.xxx.xxx.xxx: udp
19:14:16.309823 IP 142.104.6.1.53 > xxx.xxx.xxx.xxx.23513:  10809
30/5/9 Type46[|domain]
```

```
19:14:16.309825 IP 142.104.6.1 > xxx.xxx.xxx.xxx: udp
19:14:16.309826 IP 142.104.6.1 > xxx.xxx.xxx.xxx: udp
19:14:16.310020 IP 216.121.24.233.53 > xxx.xxx.xxx.xxx.32522:  10809
27/0/13 A 149.20.64.42, NS[|domain]
19:14:16.310028 IP 216.121.24.233 > xxx.xxx.xxx.xxx: udp
19:14:16.310029 IP 216.121.24.233 > xxx.xxx.xxx.xxx: udp
19:14:16.310119 IP 24.183.198.6.53 > xxx.xxx.xxx.xxx.32533:  10809
30/5/8 Type47[|domain]
19:14:16.310275 IP 69.89.66.131.53 > xxx.xxx.xxx.xxx.15603:  10809
27/0/15 A 149.20.64.42, NS[|domain]
19:14:16.310277 IP 72.52.124.55.53 > xxx.xxx.xxx.xxx.7113:  10809
27/0/15 A 149.20.64.42, NS[|domain]
19:14:16.310279 IP 24.116.11.104 > xxx.xxx.xxx.xxx: udp
19:14:16.310280 IP 216.108.235.93.53 > xxx.xxx.xxx.xxx.10270:  10809
27/0/16 A 149.20.64.42, NS[|domain]
```

Misconfigurations in victim DNS servers

Some reflection and amplification attacks can be executed with the help of open or misconfigured victim DNS resolvers. The workflow of the attack is similar; the difference is these open or misconfigured victim DNS servers will respond to any of the queries regardless if they are authoritative or non-authoritative.

TXT record attack

A TXT record provides the ability to associate arbitrary and non-formatted text to a domain or host. This parameter can be used to amplify the response to a spoofed request and thus degrade or deny DNS service.

The following is an example of a TXT record attack:

```
18:52:14.235087 IP 201.41.86.66.53 > xxx.xxx.xxx.xxx.5945:  37700
44/3/1 TXT[|domain]
18:52:14.235739 IP 208.43.214.241.53 > xxx.xxx.xxx.xxx.24434:  48463
44/3/4 TXT[|domain]
18:52:14.235742 IP 208.43.214.241 > xxx.xxx.xxx.xxx: udp
18:52:14.236811 IP 208.43.214.241 > xxx.xxx.xxx.xxx: udp
18:52:14.237335 IP 207.44.142.76.53 > xxx.xxx.xxx.xxx.24520:  2776
ServFail 0/0/1 (37)
18:52:14.237443 IP 207.44.143.7.53 > xxx.xxx.xxx.xxx.49917:  2776
ServFail 0/0/1 (37)
18:52:14.238521 IP 201.28.98.186 > xxx.xxx.xxx.xxx: udp
18:52:14.240550 IP 200.159.42.61.53 > xxx.xxx.xxx.xxx.22693:  50508
44/3/4 TXT[|domain]
```

A record attack

In an *A record attack*, the attacker issues multiple queries for A records to victim DNS servers. These requests consist of malformed domain names and the DNS server will respond with the registry code, also known as RCODE. Large numbers of these types of queries from distributed sources will impact DNS availability on the primary target.

The following is an example of an A record attack vector:

```
14:49:39.770660 IP 118.127.10.64.36679 > x.x.x.x.53:  23+ A? www.domain.com. (352)
14:49:39.770731 IP 58.181.149.10.3191 > x.x.x.x.53:  23+ A? www.domain.com. (352)
14:49:39.770737 IP 202.89.33.168.33745 > x.x.x.x.53:  23+ A? www.domain.com. (352)
14:49:39.770771 IP 118.127.10.64.47544 > x.x.x.x.53:  23+ A? www.domain.com. (352)
14:49:39.770826 IP 202.28.248.48.47405 > x.x.x.x.53:  23+ A? www.domain.com. (352)
14:49:39.770832 IP 202.28.248.48.35202 > x.x.x.x.53:  23+ A? www.domain.com. (352)
14:49:39.770862 IP 203.158.4.158.51395 > x.x.x.x.53:  23+ A? www.domain.com. (352)
14:49:39.770929 IP 202.28.248.48.36246 > x.x.x.x.53:  23+ A? www.domain.com. (352)
14:49:39.770957 IP 203.158.4.158.48998 > x.x.x.x.53:  23+ A? www.domain.com. (352)
14:49:39.771067 IP 118.127.10.64.56018 > x.x.x.x.53:  23+ A? www.domain.com. (352)
14:49:39.771075 IP 219.156.123.225.65153 > x.x.x.x.53:  23+ A? www.domain.com. (352)
14:49:39.771182 IP 202.28.248.48.54282 > x.x.x.x.53:  23+ A? www.domain.com. (352)
14:49:39.771188 IP 202.28.248.48.39548 > x.x.x.x.53:  23+ A? www.domain.com. (352)
```

The following is an example of a DNS server response:

```
18:16:06.660541 IP 66.146.160.13.53 > xxx.xxx.xxx.xxx.25345:  10809 9/4/9
Type46[|domain]
18:16:06.660576 IP 206.78.126.3.53 > xxx.xxx.xxx.xxx.25345:  10809 ServFail-
0/0/1 (36)
18:16:06.660581 IP 206.78.126.3.53 > xxx.xxx.xxx.xxx.25345:  10809 ServFail-
0/0/1 (36)
18:16:06.660627 IP 64.127.100.11.53 > xxx.xxx.xxx.xxx.25345:  10809 27/4/14
Type99[|domain]
----------
8:16:06.660538 IP 64.89.228.8 > xxx.xxx.xxx.xxx: udp
18:16:06.660541 IP 66.146.160.13.53 > xxx.xxx.xxx.xxx.25345:  10809 9/4/9
Type46[|domain]
18:16:06.660576 IP 206.78.126.3.53 > xxx.xxx.xxx.xxx.25345:  10809 ServFail-
0/0/1 (36)
18:16:06.660581 IP 206.78.126.3.53 > xxx.xxx.xxx.xxx.25345:  10809 ServFail-
0/0/1 (36)
18:16:06.660627 IP 64.127.100.11.53 > xxx.xxx.xxx.xxx.25345:  10809 27/4/14
Type99[|domain]
```

Conclusion

DNS reflection attacks are made possible by artifacts in the original architecture and design of the RFC. When DNS was designed, providing ways to access domain names was its primary focus, not potential security issues. Furthermore, the implementation of RFC extensions has introduced additional vectors for exploitation of victim DNS Servers. The threats will remain until these security gaps are closed.

Prolexic customers are protected from Distributed Reflection Denial of Service (DrDoS) attacks as part of our DDoS protection and mitigation services.

NOTE: In-depth cases studies discussed in this white paper are distributed to all Prolexic customers and PLXsert subscribers in the form of periodic internal Threat Advisories.

Appendix

References

http://www.ietf.org/rfc/rfc1035.txt
http://www.ietf.org/rfc/rfc2671.txt
http://tools.ietf.org/id/draft-ietf-dnsext-edns1-03.txt

Mitigation

DNS RRL - http://www.redbarn.org/dns/ratelimits
Cymru Secure Bind Template - http://www.cymru.com/Documents/secure-bind-template.html

About Prolexic Security Engineering & Response Team (PLXsert)

PLXsert monitors malicious cyber threats globally and analyzes DDoS attacks using proprietary techniques and equipment. Through digital forensics and post attack analysis, PLXsert is able to build a global view of DDoS attacks, which is shared with our customers. By identifying the sources and associated attributes of individual attacks, the PLXsert team helps organizations adopt best practices and make more informed, proactive decisions about DDoS threats.

About Prolexic

Prolexic Technologies is the world's largest, most trusted distributed denial of service (DDoS) protection and mitigation service provider. Able to absorb the largest and most complex DDoS attacks ever launched, Prolexic protects and restores within minutes mission-critical Internet-facing infrastructures for global enterprises and government agencies. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel, hospitality, gaming and other industries at risk for DDoS attacks rely on Prolexic for DDoS protection. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has DDoS scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

v.031513

PROLEXIC
DDoS Attacks End Here.