1.1 OVERVIEW / PLXsert has been monitoring a new trend in the use of DNS amplification attacks. Amplification attacks are special types of DDoS attacks that are designed to generate large response packets with relatively small requests. Attackers are crafting large DNS TXT (text) records to increase amplification, magnifying the impact of the attack. For example, several campaigns observed since October 4, 2014 contain fragments of text taken from press releases issued by the White House.

PLXsert suspects that the DNS flooder tool continues to be used in these campaigns. By crafting their own TXT records, attackers can amplify responses as desired and direct this traffic to targeted sites, including—but not limited to—DNS servers. The amplified traffic response could eventually overwhelm the targeted site and render it unable to respond to any requests.

Attackers have used large TXT records in reflection attacks in the past. Previous victims of DNS amplification attacks using TXT records include sites such as isc.org and many .gov sites. With this new threat, malicious actors are now crafting the TXT records to provide the largest response size possible, thereby having as much impact as possible.

The TXT records in the October 2014 attacks have been identified as originating from the guessinfosys.com domain.

1.2 HIGHLIGHTED ATTRIBUTES

Attack statistics

- Peak bandwidth: 4.3 Gigabits per second (Gbps)
- Attack vectors: DNS reflection and amplification
- Source port(s): 53
- Destination port(s): 80, random
Primary targets

- Entertainment
- Education
- High tech consulting

![Crafted DNS TXT amplification targets]

Figure 1: The entertainment industry was the main target of the October 2014 DNS reflection attacks.

Sample payloads

```


13:43:36.094854 IP X.X.X.X.53 > X.X.X.X.5926: 35408 10/13/16 TXT "<snip> President also outlines" "the details about the transmission and treatment of Ebola", TXT[|domain]
```
Malicious requests for guessinfosys.com can be observed in the wild on an ongoing basis. These requests attempt to use open resolvers as intermediate victims to reflect attack traffic back to a target. For the most part, the usefulness of these malicious domains drops off after a few days as server admins begin to block off the requests.
18:11:32.433099 IP X.X.X.X.16484 > X.X.X.X.53: 37834+ [1au] ANY7 guessinfosys.com. (45) ....E..1b........Ma....Fx@d.5.5....................guessinfosys.com.......)#(......

Figure 3: A guessinfosys.com request attempting to reflect traffic off a customer DNS server

Figure 4: The October 2014 crafted DNS TXT amplification attacks lasted more than five hours during each attack and peaked at more than 15 hours on October 24

1.3 MITIGATION / DNS reflection and amplification attacks make use of the same tactics used by other types of reflection campaigns, such as SNMP, SSDP or CHARGEN. The primary impact to the targeted service is the overall bandwidth generated. DNS reflection attacks can be mitigated successfully at the network edge. An access control list (ACL) would suffice but only in cases where available bandwidth exceeds attack size. Some DNS servers will attempt to retry the response using TCP, but when the request is sent to the target host, no transfer will occur and the attempt will fail. DDoS cloud-based protection services such as the one provided by Akamai Technologies are recommended.

Status: PLXsert is currently monitoring ongoing campaigns. Future advisories and updates will be provided if warranted.
ABOUT PROLEXIC SECURITY ENGINEERING & RESEARCH TEAM (PLXsert) / PLXsert monitors malicious cyber threats globally and analyzes these attacks using proprietary techniques and equipment. Through research, digital forensics and post-event analysis, PLXsert is able to build a global view of security threats, vulnerabilities and trends, which is shared with customers and the security community. By identifying the sources and associated attributes of individual attacks, along with best practices to identify and mitigate security threats and vulnerabilities, PLXsert helps organizations make more informed, proactive decisions.

ABOUT AKAMAI / Akamai® is the leading provider of cloud services for delivering, optimizing and securing online content and business applications. At the core of the Company’s solutions is the Akamai Intelligent Platform™ providing extensive reach, coupled with unmatched reliability, security, visibility and expertise. Akamai removes the complexities of connecting the increasingly mobile world, supporting 24/7 consumer demand, and enabling enterprises to securely leverage the cloud. To learn more about how Akamai is accelerating the pace of innovation in a hyperconnected world, 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 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

©2014 Akamai Technologies, Inc. All Rights Reserved. Reproduction in whole or in part in any form or medium without express written permission is prohibited. Akamai and the Akamai wave logo are registered trademarks. Other trademarks contained herein are the property of their respective owners. Akamai believes that the information in this publication is accurate as of its publication date; such information is subject to change without notice. Published 10/14.