Akamai Security Advisory

VERSION: 2014-0003-G
UPDATE: Feb 12, 2014, 1500 EST

NTP Reflection Attacks

EXECUTIVE SUMMARY

Akamai is actively tracking industry reports regarding DDoS activity utilizing NTP amplification attacks. US-CERT has recently released advisories on NTP amplifications attacks and other UDP protocols. The Akamai network continues to defend customers from DDoS traffic including NTP and other UDP-based amplification attacks.

VULNERABILITY AND ATTACK DETAILS

NTP is a widely deployed time synchronization service listening on UDP port 123. The attacker spoofs source IPs and sends a small query to a vulnerable NTP server, which generates a large reply of response data to the spoofed addresses. This asymmetric attack can saturate network links thereby preventing legitimate traffic from reaching its destination. According to the US-CERT advisory the amplification factor of this attack is 556.9 so that each request made by an attacker will be able to send over 500 times the data to the target; i.e., an attacker who has access to a gigabit connection could theoretically send enough traffic to send over 500 gigabits per second of replies to a target.

HOW DO I KNOW I'M AFFECTED

If you are the target of an NTP amplification attack and not suffered a loss of reliable connectivity, inspecting packets at your perimeter will reveal traffic with source port 123 destined for any IP address on your network(s). The purpose of the attack is not to overwhelm a specific listening service, but rather to consume all available bandwidth with data, which will be discarded in any case.

Networks under your control may be participants in NTP amplification attacks if proper ACLs are not in place to prevent any IP address from querying an NTPd server on your network from responding to a `monlist` query.

AKAMAI'S DEFENSIVE ARCHITECTURE

Akamai continually defends customers from UDP DDoS attacks including NTP amplification. By default Akamai's distributed platform ignores all inbound traffic except for authoritative DNS (53/tcp and 53/udp), HTTP (80/tcp), and HTTPS (443/tcp). Thus, all inbound NTP traffic destined for 123/udp is dropped before it enters Akamai's network. Combining our world-wide footprint with these simple rules, the Akamai platform deflects enormous volumes of DDoS traffic 24/7/365 without active intervention. These defenses are in place in all of our locations in over 80 countries, which are connected to 1,000+ networks in thousands of datacenters.

Akamai's intelligent platform automatically routes around poorly performing networks. At the same time the Akamai NOCC continuously monitors network capacity and performance degradation. The combination of automation and human checks ensures customers are protected from DDoS floods and poor network performance.

At a higher level, Akamai's Customer Security Incident Response Team (CSIRT) monitors open intelligence sources for DDoS activity; tracks threat actors, and ingests industry news. CSIRT also searches for patterns in attacks to identify threats and threat actors.

AKAMAI SOLUTIONS

All Akamai customers even without Kona SiteDefender benefit from Akamai's defensive architecture, which mitigates UDP-based DDoS attempts such as NTP amplification attacks.

To secure HTTP(S) origins, SiteShield offers the capability to limit communication to a datacenter with limited bandwidth capacity to only pass traffic with authorized Akamai servers. Limiting traffic to only only known network ranges and dropping invalid traffic as soon as possible relieves congestion and capacity issues on other network devices in a datacenter and simplifies ACLs needed by uplink providers.

HOW DO I FIX THE PROBLEM

NTP servers are often operated as a public service since time synchronization is essential for interconnected computers and network devices. The US-CERT advisory from January 2014 details the specific commands and mitigation steps to prevent the NTP service from participating in an amplification attack.
• https://www.us-cert.gov/ncas/alerts/TA14-013A

If possible, separate DNS and NTP infrastructure from HTTP(S) services. By applying stricter network ACLs and using different network capacity, in the event of an UDP-based amplification attack HTTP(S) services will be segregated from UDP-based amplification attacks and easier to detect and defend.

To prevent your network from unknowingly participating in an amplification attack, limit outbound NTP traffic to only those network devices which serve as NTP time synchronization masters.

- Ensure proper ACLs are applied to all public facing NTP servers on networks under your control to prevent abuse of the `monlist` feature.
- Public NTP server operators should upgrade to the latest patched versions of NTPd that disables the `monlist` feature by default.
- Check with your network administrators and vendors for BCP38 network policies to prevent spoofed IP packets from transiting a network to prevent all UDP-based amplification attacks.

Until all public NTP servers have the `monlist` feature blocked or disabled AND BCP38 network policies are in place with all backbone operators, NTP amplification attacks will continue as a DDoS threat.

REFERENCES & RELATED READING

NTP
http://support.ntp.org/bin/view/Main/SecurityNotice#DRDoS_Amplification_Attack_using
https://www.team-cymru.org/ReadingRoom/Templates/secure-ntp-template.html

BCP38
http://tools.ietf.org/html/bcp38

DNS
Check for open recursive resolvers
http://openresolverproject.org/

Traffic Light Protocol
http://www.us-cert.gov/tlp

TA14-013A: NTP Amplification Attacks Using CVE-2013-5211
https://www.us-cert.gov/ncas/alerts/TA14-013A

TA14-017A: UDP-based Amplification Attacks
https://www.us-cert.gov/ncas/alerts/TA14-017A

ABOUT AKAMAI CSIRT

The Akamai Customer Security Incident Response Team (CSIRT) researches attack techniques and tools used to target our customers and develops the appropriate response – protecting customers from a wide variety of attacks ranging from login abuse to scrapers to data breaches to DNS hijacking to distributed denial of service. It's ultimate mission: keep customers safe. As part of that mission, Akamai CSIRT maintains close contact with peer organizations around the world, trains Akamai's PS and CCare to recognize and counter attacks from a wide range of adversaries, and keeps customers informed by issuing advisories, publishing threat intelligence and conducting briefings.

CONTACTS

Existing customers that desire additional information can contact Akamai directly through CCare at 1-877-4-AKATEC (US 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 .

The Akamai Difference

Akamai® is the leading cloud platform for helping enterprises provide secure, high-performing user experiences on any device, anywhere. 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* and follow @Akamai on Twitter.

Akamai Technologies, Inc.

U.S. Headquarters
8 Cambridge Center
Cambridge, MA 02142
Tel 617.444.3000
Fax 617.444.3001
U.S. toll-free 877.4AKAMAI
877.425.2624

International Offices
Unterfoehring, Germany
Paris, France
Milan, Italy
London, England
Madrid, Spain
Stockholm, Sweden
Bangalore, India
Sydney, Australia
Beijing, China
Tokyo, Japan
Seoul, Korea
Singapore

www.akamai.com