March 10, 2014

To: IT Security Staff and Network and System Administrators
(A CIO version of this Alert is available at [6])

REN-ISAC ALERT:
NTP-Based Distributed Denial of Service Attacks – Prevent your institution from being an unwitting partner in these attacks

The REN-ISAC [1] wants to raise awareness and drive change concerning common network time protocol (NTP) and network configurations that fall short of best practices and which, if left uncorrected, open the door for your institution to be exploited as an unwitting partner in delivering crippling distributed denial of service (DDoS) attacks against third parties.

In a companion note to CIOs, the REN-ISAC recommends the following:

=== **ACTIONS** ===

1. Distribute a copy of this message to your network administrators, information security staff, system administrators, and other relevant personnel.

2. Identify hosts on your network with ntpd installed and running. Disable "monlist" capabilities on those NTP servers. Or, for systems which cannot be updated or configured to eliminate the monlist risk, apply network filters to prevent external requests to these insecure systems.

3. Ensure your institutional networks are unable to originate Internet traffic with spoofed source addresses as described elsewhere in this document.

==========

Although DDoS attacks exploiting the NTP and network configuration weaknesses have been around for a long time, the frequency and impact of these attacks have grown over the past year. The traffic sourced by any single system may be small enough to go unnoticed at an institution, however, the aggregate traffic from many sources, as experienced at the target, can be crippling. Recent attacks [2,3,4] average around 7.3 gigabits per second of traffic aimed at the victim organization – more than the full Internet bandwidth of most small and medium-sized colleges and universities.

Given the history and success of recent attacks, we expect these attacks will rise in frequency and magnitude in the months ahead.

There are two issues:

1. NTP is a protocol used to synchronize the clocks of networked devices. A deprecated command, "monlist", permits a requesting computer to receive information regarding the last 600 connections made to the NTP server. A small input request can generate a large response.

   When a malicious actor spoofs the source IP address of a victim targeted for attack, and repeatedly sends monlist requests to thousands of insecure NTP servers located all over the Internet, an avalanche of traffic is directed at the victim, overwhelming the victim's network capacity.

   Monlist has been removed from newer versions of NTP and monlist can (and should) be disabled in older versions.

   The NTP issue is complicated by the fact that not only is NTP running on upgradeable enterprise servers, NTP is also employed on infrastructure devices and embedded systems in your enterprise, some of which can be updated only with great difficulty and expense. Concerning these "difficult" systems, network firewalls may be one approach that can be used to mitigate the problem of these vulnerable-but-uncorrectable devices.

2. The second issue, the network configuration issue, involves the problem of traffic with forged apparent source addresses. Systems on your network should not be able to transmit packets that appear to be from a source IP address that doesn't belong to you -- your systems should only originate traffic with accurate source IP information.

In addition to the problem of educational institutions being leveraged as the sources of attacks against third parties, there have been incidents of institutions being targeted as the victim of DDoS attacks. Best practices for mitigating DDoS attacks against your institution apply: know in advance how to partner with your ISP to mitigate the effects of an attack; concerning Internet2, refer to the "DDoS Attacks Policy" [5]. DDoS mitigation services are also available from commercial organizations.

==========
TECHNICAL AND POLICY CONTROLS
==========

===== Overview =====

While NTP is the DDoS amplification mechanism de jour, the problem encompasses a number of network service protocols [16], e.g. see our earlier Alert concerning open recursive DNS servers [17].

Too many higher education institutions contribute to this avoidable problem. Unfortunately, this problem goes unsolved because organizations targeted in the attacks are not the same organizations that fail to follow best common practices (and which end up being exploited to conduct the attacks). The exploited organization often experiences little ill effect; therefore, motivation to solve the problem depends on each site's willingness to go the extra mile and be a good Internet citizen, even if doing so doesn't result in benefits to them directly.

===== Solutions =====

[NTP]

Highly Recommended:

Concerning systems on which NTP can be updated or configured:

Upgrade NTP to version 4.2.7p26 or higher [9]

If upgrade isn't possible, disable monlist in the ntp.conf file [9]

Concerning all other (e.g. infrastructure devices and embedded systems):

Manage NTP traffic (inbound destination port 123 tcp/udp), e.g. by using router ACLs, so that queries from outside the enterprise can only reach intentionally permitted enterprise time servers. Do NOT blindly block all incoming and outgoing NTP traffic, because NTP serves an important role in synchronizing system clocks.

Review the Team Cymru Secure NTP template [10] for inclusion in your router template.

Depending on your environment it may be difficult to limit queries from inside the enterprise to external servers (outbound) because many infrastructure devices and embedded systems rely on preconfigured NTP services.

Recommended:

Provide a means to monitor NTP for evidence of abuse.

[Network]

Highly Recommended:

Apply BCP38/BCP84 filtering to prevent spoofed source address traffic from leaving your network. [11][12][13]

Recommended:

Collect and store network flow (NetFlow/Sflow/J-Flow) data. Real time network flow allows backtracking spoofed network traffic. Historical network flow facilitates incident response capabilities.

===== More In-Depth =====

[NTP monlist]

NTP monlist is a remote command used in older versions of NTP for monitoring which hosts have connected to the server. Upon request, a list of the last 600 hosts will be sent. Monlist is a deprecated

command, but in older versions of NTP, it is still enabled. New versions of NTP (after 4.2.7p26) have removed monlist capabilities in favor of ntpq mrulist [8]. The "Most Recently Used" (MRU) functionality also includes the ability to rate limit and "Kiss-of-Death" packets, which explicitly request the client to stop sending and leaves a message for the system operator [14].

You can request a free report of NTP servers on your network from the OpenNTP project group [15].

[Network Filtering to Prevent Source-Spoofed Packets]

Systems should not be permitted to send spoofed traffic to the Internet, pretending to be traffic from some other site's IP addresses. Roughly 80% of all networks have already installed filtering rules on their network routers to ensure any spoofed network traffic won't hit the Internet, but some networks -- including potentially yours -- have not yet done so. We need your help. Please ensure your institutional networks prevent traffic with spoofed source addresses from leaving your network.

Blocking spoofed network traffic from leaving your network is an IETF Best Common Practice ("BCP"), see:

http://tools.ietf.org/html/bcp38 and
http://tools.ietf.org/html/bcp84

Filtering can be done at the subnet level, or at the institutional border, or both.

===== Additional Considerations =====

Unrelated to NTP amplification DDoS attacks, but of related concern to NTP, is the local denial of service (DoS) vulnerability involving NTP Mode 7 messages [18]. Upgrading NTP to a current version or applying a network firewall rule to restrict inbound NTP traffic to intentionally permitted servers will eliminate/reduce this local DoS vulnerability.

==========

Print-friendly copies of this Alert and the companion CIO version (with clobber-free long URLs) are available at the REN-ISAC web site: http://www.ren-isac.net/alerts.html

We'd appreciate your input on additional means to protect from this threat, and general feedback concerning this Alert. If you have any questions, please don't hesitate to e-mail us at soc@ren-isac.net.

Special thanks go to the members of the REN-ISAC Technical Advisory Group (TAG) [7].

On behalf of the REN-ISAC team,

Doug Pearson
dodpears@ren-isac.net
Technical Director, REN-ISAC
http://www.ren-isac.net
24x7 Watch Desk +1(317)278-6630

==========
References
==========

[1] REN-ISAC
http://www.ren-isac.net

[2] Hackers Spend Christmas Break Launching Large Scale NTP-Reflection Attacks
http://www.symantec.com/connect/blogs/hackers-spend-christmas-break-launching-large-scale-ntp-reflection-attacks

[3] DoS attacks that took down big game sites abused Web's time-sync protocol
http://arstechnica.com/security/2014/01/dos-attacks-that-took-down-big-game-sites-abused-webs-time-synch-protocol/

[4] NTP reflection attack
https://isc.sans.edu/diary/NTP+reflection+attack/17300

[5] Internet2 DDoS Attacks Policy
https://wiki.internet2.edu/confluence/display/network/Forms%2C+Maps%2C+Policies%2C+and+Procedures

[6] CIO version of this alert
http://www.ren-isac.net/alerts/REN-ISAC_Alert_NTP_Amp_DDoS_CIO_201403.html

[7] REN-ISAC Technical Advisory Group
http://www.ren-isac.net/about/advisory.html#technical

[8] remove ntpd support for ntpdc's monlist (use ntpq's mrulist)
http://bugs.ntp.org/show_bug.cgi?id=1532

[9] DRDoS / Amplification Attack using ntpdc monlist command
http://support.ntp.org/bin/view/Main/SecurityNotice#DRDoS_Amplification_Attack_using

[10] Secure NTP Template
https://www.team-cymru.org/ReadingRoom/Templates/secure-ntp-template.html

[11] Network Ingress Filtering
http://tools.ietf.org/html/bcp38

[12] Ingress Filtering for Multihomed Networks
http://tools.ietf.org/html/bcp84

[13] Securing the Edge
http://www.icann.org/en/groups/ssac/documents/sac-004-en.pdf

[14] Access Control Options
http://doc.ntp.org/4.2.2p2/accopt.html

[15] For a list of open NTP by ASN, e-mail ntp-scan /at/ puck.nether.net
http://openntpproject.org/

[16] Amplification Hell: Revisiting Network Protocols for DDoS Abuse
http://www.internetsociety.org/sites/default/files/01_5.pdf

[17] ALERT: Prevent your institution from being an unwitting partner in denial of service attacks
http://www.ren-isac.net/alerts/dns_amp_ddos_tech_201305.html

[18] NTP mode 7 denial-of-service vulnerability
http://www.kb.cert.org/vuls/id/568372

[Other Resources]

In addition to the references made in the text above, the following may be useful:

Alternative to NTP – OpenNTPD
http://www.openntpd.org/

NTP DoS reflection attacks
https://cert.litnet.lt/en/docs/ntp-distributed-reflection-dos-attacks

A Free Solution For DDoS Reflection Attacks: A Decade In Waiting
http://blog.trendmicro.com/trendlabs-security-intelligence/a-free-solution-for-ddos-reflection-attacks-a-decade-in-waiting/

NTP Reflections
https://labs.ripe.net/Members/mirjam/ntp-reflections

-o0o-