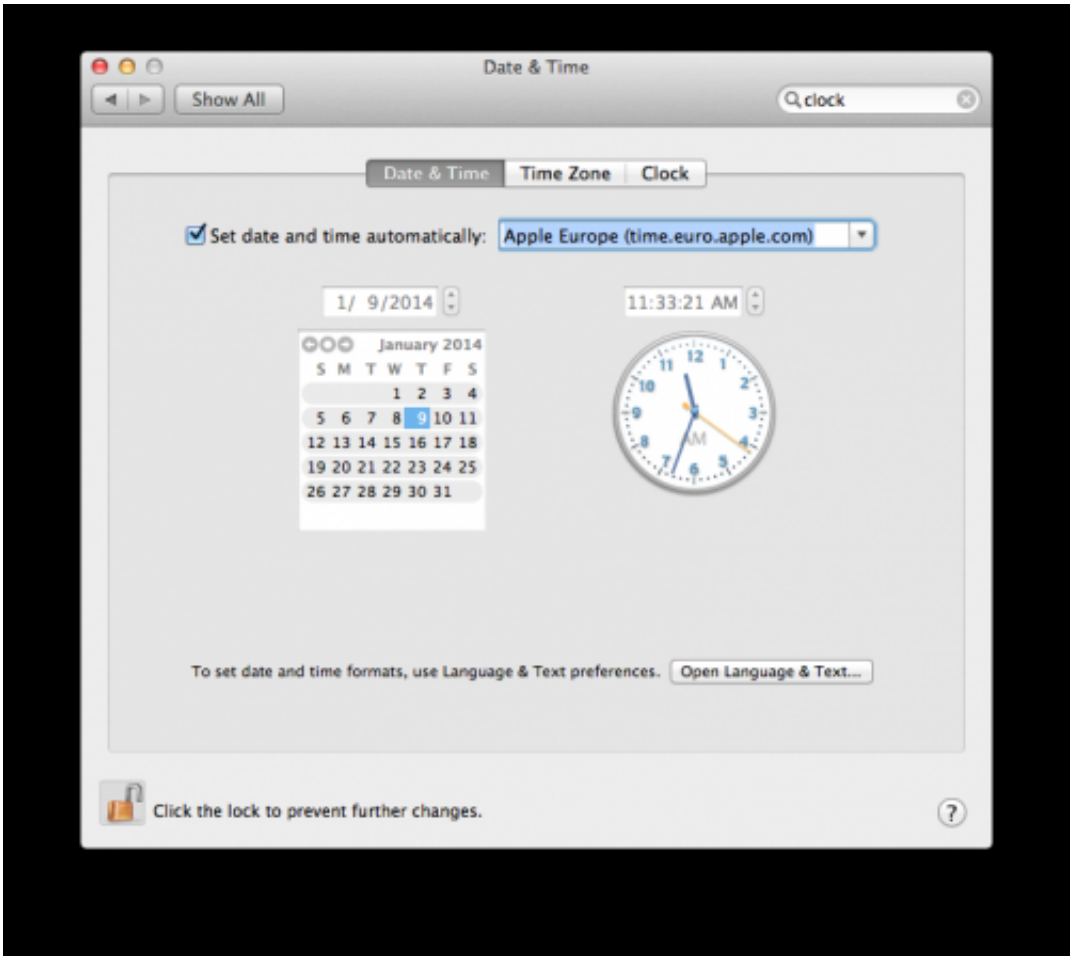
Attackers use Network Time Protocol for denial exploit

February 12 2014, by Nancy Owano



(Phys.org) —Reports are calling it the world's most massive distributed denial-of-service (DDoS) attack ever, referring to this week's report

about a massive exploit making use of the Network Time Protocol (NTP), which is used to synchronize computer clock times. But how is this the largest such attack? According to reports, measuring an attack's severity in gigabits, the recent incident was over 400 Gbps. That exceeds the Spamhaus exploit, last year's record-breaker, which at its peak was generating 300 Gbps of traffic. Spamhaus, based in Geneva, Switzerland and London, tracks spam services and spam senders. The attack on Spamhaus involved misconfigured Domain Name System (DNS) servers. The servers are used to translate typed Web and email addresses into numerical addresses. Reports said the attack affected mostly users in Europe and some parts of Asia.

A denial of service attack is launched in order to overwhelm web services by flooding them with requests for data. All that data traffic overwhelms the company's servers, preventing other Internet users to make their connections, as the servers have more data packets than their switches can handle. IDG News Service's Lucian Constantin pointed out that the NTP is but one of several protocols that can be used by attackers in DDoS attacks—the other two being the DNS and SNMP (Simple Network Management Protocol). He added that "The new attack Monday used a technique called NTP reflection that involves sending requests with spoofed source IP addresses to NTP servers with the intention of forcing those servers to return large responses to the spoofed addresses instead of the real senders."

The attack was revealed on Twitter by Matthew Prince, CloudFlare's CEO. "Very big NTP reflection attack hitting us right now. Appears to be bigger than the #Spamhaus attack from last year. Mitigating," said Price. The attack was directed at a CloudFlare user but Prince did not disclose details about the affected customer.

CloudFlare is a web performance and security company that provides DDoS mitigation services. The company's blogpost in January had

focused on the attack method used earlier this week. John Graham Cumming, programmer, wrote: "We'd long thought that NTP might become a vector for DDoS attacks because, like DNS, it is a simple UDP-based protocol that can be persuaded to return a large reply to a small request. Unfortunately, that prediction has come true."

Unfortunately, added Cumming, the NTP protocol is prone to amplification attacks because it will reply to a packet with a spoofed source IP address; at least one of its built in commands will send a long reply to a short request. "That makes it ideal as a DDoS tool." He further noted how NTP has a command called monlist (or sometimes MON_GETLIST) which can be sent to an NTP server for monitoring purposes. "It returns the addresses of up to the last 600 machines that the NTP server has interacted with. This response is much bigger than the request sent making it ideal for an amplification attack."

More information: blog.cloudflare.com/understand … p-based-ddos-attacks

Citation: Attackers use Network Time Protocol for denial exploit (2014, February 12) retrieved 28 April 2024 from https://techxplore.com/news/2014-02-network-protocol-denial-exploit.html