StoreNext

Technical Bulletin

Denial-of-Service Attacks on DNS Providers

CP-TECH-09:05
April 8, 2009

Denial-of-service virus attacks flood a site with a massive overload of communications, and if one of the major DNS service providers is hit, such an attack can affect how Internet Domain Name System (DNS) addresses are resolved.

DNS service providers route URL and URI requests to the proper physical IP addresses that are registered with the DNS service provider. So if a DNS service becomes unavailable, some Internet URLs will not work normally and won't link to the expected addresses. During such a denial-of-service attack recently, some Connected Payments users were affected until work-arounds were provided.

SHOULD YOU WORRY ABOUT DNS ATTACKS?

Denial-of-service attacks against DNS service providers were once commonplace on the Internet. The industry and DNS service providers, however, have aggressively responded and brought these attacks to a virtual standstill — in fact, the DNS denial-of-service last week was the first successful such attack in about four years.

The industry has been careful to close loopholes, and it took the hacking community about four years therefore to find an opening. The DNS community once again got together to crush the attack and close the exposure point. It may well be years before another loophole is found and exploited. These sites provide more information about the recent attacks:

- http://www.thewhir.com/web-hosting-news/040309_Registercom_Falls_Prey_to_DDoS_Attack
- http://blogs.zdnet.com/BTL/?p=15601

What about a denial-of-service attack against Connected Payments? For obvious reasons, the specific protection methods that Connected Payments uses are confidential. Your customers should understand, however, that companies such as Google and Microsoft have developed successful protection methodologies and technologies for recognizing and responding to denial-of-service attacks; Connected Payments has implemented these same methods and technology.

WORK AROUNDS

If you have customers that experience severe communications problems in the future due to such attacks, the work-around below will help the communications setup.

1. Note that these problems will normally intermittent and sporadic across the country, so many customers will have no problems even if others are having difficulty.
2. We do not recommend currently installing them or leaving these work-arounds in place, since they essentially hard-wire the store to a specific IP address. The flexibility of the URI that's normally installed makes it possible for Connected Payments to dynamically respond with alternate data center resilience.

Work-around implementation instructions:

1. On each affected lane, browse to the "C:\WINDOWS\system32\drivers\etc" and open the "hosts" file with notepad
2. Insert the following lines under the "127.0.0.1 Localhost" entry:[1]

```
4.79.143.164        trn1.servereps.com
4.79.143.170        trn3.servereps.com
4.79.143.169        trn5.servereps.com
208.80.28.164       trn2.servereps.com
208.80.28.170       trn4.servereps.com
208.80.28.169       trn6.servereps.com
4.79.143.168        svc1.servereps.com
4.79.143.171        svc3.servereps.com
```

3. Save and close
4. Reboot the register

[1] NOTE: If using Windows2000, the directory path will be "C:\WINNT\system32\drivers\etc"