new rogue-DHCP server malware - SANS Internet Storm Center

By SANS Internet Storm Center

Archived: 2026-04-05 13:32:13 UTC

Thanks to Irwin for alerting us about a new version of rogue DHCP server malware he found in his network. The malware appears to be similar to Trojan.Flush.M which was found last December. Like back then, after infecting its target, the malware installs a rogue DHCP server. The main goal of the DHCP server is to spread a bad DNS server IP address.

Irwin did a good job comparing the two versions. Here is his summary of the differences:

- The new version sets the DHCP lease time to 1 hour.
- it sets the MAC destination to thebroadcast address, rather then the MAC address of the DHCP client
- it does not specify a DNS Domain Name.
- the options field does not contain an END option followed by PAD options.
- Unlike Trojan.Flush.M, the BootP Broadcast Bit is set.

The malicious DNS server is 64.86.133.51 and 63.243.173.162.

Recommendation:

monitor connections to DNS servers other then the approved one pushed out by your DHCP server. This should help you spot this kind of malware. Yes, you can block the two IP addresses listed above, but it will likely do little good.

Johannes B. Ullrich, Ph.D.
SANS Technology Institute
