Mandiant ApateDNS

ApateDNS is a tool for controlling DNS responses though an easy to use GUI. As a phony DNS server, ApateDNS spoofs DNS responses to a user-specified IP address by listening on UDP port 53 on the local machine. It responds to DNS requests with the response set to any IP address you specify. The tool logs and timestamps any DNS request it receives. You may specify a number of non-existent domain (NXDOMAIN) responses to send before returning a valid response. ApateDNS also automatically sets the local DNS to localhost. By default, it will use either the set DNS or default gateway settings as an IP address to use for DNS responses. Upon exiting the tool, it sets back the original local DNS settings.

Usage

- After running the tool, you are presented with the following options:
  - DNS Reply IP – This is the IP address that will be provided in DNS responses.
  - # of NXDOMAIN's – This is the number of non-existent domain responses to send before responding with a valid response for each DNS query.
  - Selected Interface – This is the interface on which the DNS server will listen.
  - Start Server button – This is used to Start the DNS server. This button must be pressed before ApateDNS will process any DNS requests.
  - Stop Server button – This is used to Stop the DNS server after is has been started.
- A malware analyst may wish to use the tool in the following ways:
  - To catch DNS requests made by malicious software.
  - To trick the malware to send its malicious traffic to a host that the malware analyst controls and monitors.
  - To catch additional domains used by a malware sample through the use of the non-existent domain (NXDOMAIN) option. Malware will often loop through the different domains it has stored if the first or second domains are not found. Using this NXDOMAIN option can trick malware into giving you additional domains it has in its configuration.

System Requirements

Windows XP or greater
Microsoft .NET Runtime >= 2.0

Credits

ApateDNS was created by Steve Davis