

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE ISSUED: March 6, 2012

SUBJECT: DNSChanger Malware Infrastructure Shutdown

In November 2011, U.S. Federal prosecutors announced Operation GhostClick, an investigation that resulted in the arrests of people who allegedly infected millions of computers with malware strain called "DNSChanger".

This joint effort by the FBI, NASA OIG, Estonian Police, Border Guard and various other public and private sector organizations also resulted in the seizure of assets related to the this malware strain.

The operation originally identified approximately 500,000 computers infected with the DNSChanger in the United States which includes computers belonging to state and local government agencies. The DNSChanger reconfigures the domain name system (DNS) of infected computers from legitimate DNS servers to rogue DNS servers that were controlled by the arrested individuals and may prevent antivirus software from functioning properly. The malware also attempts to connect to devices on the local network that are providing a DHCP service using common default credentials.

If access is successful, the malware changes the DHCP server settings to provide rogue DNS information to all computers (ones that are not infected with the malware) who use the DHCP server. Systems affected by this malware sends domain name resolution requests to a rogue DNS servers rather than legitimate ones, which could result in a user's network traffic being redirected to fraudulent sites.

To prevent computers affected by the DNSChanger malware from experiencing network service interruptions, a NY District court appointed a receiver to provide legitimate replacement DNS servers which would respond to requests from infected hosts. However, this court order is set to expire on July 9, 2012. Computers that remain infected with the DNSChanger malware may be unable to access network resources when the replacement servers are taken offline.

To identify infected computers, organizations should check for and investigate unexpected DNS traffic from internal workstations to the following subnets which formerly hosted the DNSChanger infrastructure:

- 85[.]255[.]112[.]0/20
- 67[.]210[.]0[.]0/20
- 93[.]188[.]160[.]0/21
- 77[.]67[.]83[.]0/24
- 213[.]109[.]64[.]0/20
- 64[.]28[.]176[.]0/20

RECOMMENDATIONS:

The following actions should be taken:

- Check for unexpected DNS traffic to the aforementioned netblocks.
- Ensure that all systems are running up to date antivirus and have updated signatures.

