Trojan falsely boosts Alexa traffic stats for Chinese web sites

by Bend_Weekly_News_Sources

FaceTime Researchers Discover Symfly Trojan Abusing Alexa Toolbar

FaceTime Security Labs, the threat research and remediation arm of FaceTime Communications, has discovered a Trojan named Symfly that is influencing Alexa Web traffic rankings for several Chinese Web sites. Customers who have deployed FaceTime Enterprise Edition, including RTGuardian, GEM and IMAuditor and configured for automatic filter updates, are automatically protected from this security threat.

Symfly Trojan downloads the Alexa Toolbar, calls out to web sites, registering as legitimate hits and artificially inflating the siteâ€™s Alexa traffic ranking. The Symfly Trojan downloads and installs multiple files to an infected PC, primarily via HTTP. The daisy chain of installations includes the Trojan Adcheat and can install an Alexa Toolbar from Renwu.info without the user's consent. The infection causes the user's PC to call out to various Web sites. If the Trojan has installed the Alexa Toolbar, the calls will register as legitimate hits and artificially inflate the site's Alexa traffic ranking. FaceTime researchers have found that Alexa traffic reports on targeted sites peak in similar patterns, leading them to conclude that the infection is impacting the reported traffic rates.

FaceTime enterprise customers are protected from the Symfly Trojan through Web filtering at the gateway in combination with inoculation at the desktop. The RTGuardian perimeter appliance automatically updates its signatures to provide protection against the initial infection at the gateway. FaceTime's Greynets Enterprise Manager provides an additional layer of protection with the ability to identify and remediate any infected endpoints.

The FaceTime research team offers a detailed accounting of the infection and the possible motives.