



Website Anti-Phishing & Pharming Sweep

Description

There continues to be increases in the number of Phishing reports received by the Anti-Phishing Working Group in 2005. The number has doubled since October, 2004, with over 15800 incidents reported in October, 2005. During the same period, Websense, Inc. has reported a 66% increase in the number of company websites that have been hijacked. To help combat this growing problem, nGran™ is offering a Website Anti-Phishing & Pharming Sweep (WAPPS) subscription service that provides monitoring for corporate web sites using proprietary site sampling techniques on a weekly, monthly, quarterly or annual basis.

The sweeps are designed to find web page content that is a “knock-off” of the monitored corporate site as soon as it emerges on the web. WAPPS was built to find site imitators that are infringing on corporate web identities. These copycat sites usually originate overseas and are typically involved in various cybercrime activities such as identity theft or intellectual property theft. This means that the sweeps detect duplicate pages with non-identical addresses and summarize the web page contents for the returned results. WAPPS also tracks suspicious eMail solicitations and correlates that with web site sweep data.

This service performs a daily review of Global Top Level Domains (gTLD) and Country Code Top Level Domains (ccTLD), any new registrations, and activations or changes to sites that may have suspicious properties. This service includes functions that automatically track page changes and updates for the current online status of infringing sites. WAPPS also provides route checking for a corporate site that maps routes to and from multiple locations throughout the world. This service component was designed to reveal site misdirection techniques using DNS hijacking or cache poisoning techniques.

Features

A WAPPS weekly report provides summary and detailed information typically displayed in the following categories, others may be added or substituted based on findings;

1. Duplicate Web site and page detection
2. Suspicious eMail content review
3. gTLD and ccTLD review with site registration change tracking
4. Imitator site online status and site contact information
5. DNS & Route analysis from multiple worldwide locations to corporate site(s)
6. “Cousin Searches” for mistyped URLs infected with Malware
7. Search-engine poisoning: including imitator websites infected with Malware
8. Recommended actions, in the event of positive imitator detection

Other Services Available

nGran™ offers a complete suite of network and security services. Related security services include **Web Site Reviews, Remote Security Monitoring, System Security Audits, Controlled Penetration Testing, Vulnerability Assessments, Site Recovery Planning**, and other consulting services, as required.

nGran, LLC

PO Box 1555
Westford, MA 01886
Tel: 978-392-7867
email: sales@ngran.com

nGran believes that the information in this document is accurate as of its publication date; such information is subject to change without notice. nGran is not responsible for any inadvertent errors. nGran™ is a trademark of nGran, LLC. All other trademarks and registered trademarks are property of their respective owners.