Threatpost News Briefs
Newsletter Sign-up:
Email Address Subscribe

digital underground

Dennis Fisher

October 6, 2009, 10:06 AM

The Reality Behind SQL Injection Attacks

TORONTO -- The frequency and scope of SQL injection attacks has exploded in the last year or two, with thousands of legitimate Web sites having been compromised and used to serve malware or further Web exploits. That's the bad news. The good news is that there are some remarkably effective techniques that security professionals can use to identify and recover from these attacks.

The best tool security staffs have at their disposal in these cases is a forensic analysis of the database, Kevvie Fowler (below), director of managed security services at TELUS, said during a talk at the SecTor 2009 conference here Tuesday. SQL injection vulnerabilities are quite well understood, Fowler said, but the specific techniques that attackers use and the tracks they leave behind haven't been examined as closely.

"Nothing can detect and prevent all SQL injection attacks," said Fowler. "But the attacks leave specific fingerprints in the database cache. Reading the registry, reading the system files, creating tables, all of this leaves traces."

The interesting part is that the attackers don't seem to care. Fowler, who does a lot of forensics work on database servers, said that very few attackers have any interest in trying to cover their tracks on the server itself. They're far more worried about getting their malware on the Web site and then onto users' machines. Many of the sites that are compromised in the mass SQL injection campaigns are only used by attackers for a short period of time.

If someone comes along days or weeks after the attack takes place and discovers their techniques and what they loaded onto the server, so be it. There are plenty of other vulnerable sites to go after.

As a result, Fowler said that the cache on a compromised database server can be a treasure trove of valuable data for security professionals trying to understand what happened.

"A lot of the techniques attackers use are lost once they hit the database server," he said. "All of these things that are normal fare for SQL injection force the database server to cache the activity."

Fowler also has written a new tool called Hypnosis, which is an extension of the existing Pangolin SQL injection toolkit. Hypnosis is a command-line tool designed to let users reach into the database server's cache and see whether an attack has occurred and what happened

About Digital Underground

Veteran security reporter Dennis Fisher writes the Digital Underground blog on Threatpost. He previously served as executive editor of the Security Media Group at TechTarget and news editor of eWeek magazine and has been covering security for nearly 10 years. On Digital Underground, Dennis delivers insightful analysis, fast-breaking industry news and in-depth features.
Contact Dennis

THU, 10/08/2009 - 07:59

ThreatPost tweeted "Operation 'Phish Phry' Nets 100 Cyber Criminals | http://bit.ly/Nrhzu..." 7:59am #

ThreatPost tweeted "Citing Cybercrime, FBI Director Doesn't Bank Online | http://bit.ly/1famAa..." 7:58am #

WED, 10/07/2009 - 10:38

ThreatPost was mentioned - "Twitter Mention - rex_plantado: RT @threatpost Researcher Banished for Showing How to Hack PayPal | http://bit.ly/13UYmm..." 10:38am #

ThreatPost was mentioned - "Twitter Mention - jespinhara: RT @threatpost Researcher Banished for Showing How to Hack PayPal | http://bit.ly/13UYmm..." 8:56am #

ThreatPost was mentioned - "Twitter Mention - devilok: Researcher Banished for Showing How to Hack PayPal | http://bit.ly/13UYmm (via @threatpost)..." 8:46am #

more

Stay Connected

Facebook Twitter LinkedIn RSS

Feeds

Ones and Zeros Digital Underground Punditry Overflow Watchlist Hearsay
Cybersecurity Black Hat Briefings VB Conference 2009

Copyright © 2009 threatpost.com | Terms of Service | Privacy