Commtouch: Malware Writers' Tactics Evolving

May 3 2007

The security vendor says server-side polymorphic malware exploded across e-mail during the first quarter of 2007, with attackers exploiting the vulnerabilities of traditional anti-virus tools.

A new report by security vendor Commtouch claims attackers are increasingly spreading server-side polymorphic malware via e-mail in a bid to circumvent anti-virus tools.

According to the report, which focuses on the first four months of 2007, malware writers are using speed, variation and social engineering techniques to mass-distribute their malicious code across the Web.

"The server-side polymorphic distribution method is an evolution of earlier tactics, where malware writers would introduce new variants over a period of weeks or months, to try to bypass anti-virus engines," said Rebecca Herson, senior director of marketing at Commtouch, based in Sunnyvale, Calif., in an interview with eWEEK. "Since the end of 2006, this has become the primary distribution method for e-mail-borne malware."

By crafting a large number of distinct variants of a virus and releasing them in short bursts, malware writers are able to release new variants before a signature or heuristics can be created to protect against the virus. At one point early this quarter, distributors of Storm/Nuwar malware released over 7,000 such variants in a single day, Commtouch officials said.

The report also states that malware writers are adopting social engineering techniques common among spammers to lure victims into opening attachments. For example, the Storm/Nuwar outbreak in mid-January used tabloid-style e-mail subject lines such as "230 dead as storm batters Europe" and "First nuclear act of terrorism!"

Bill Stephens, city manager of electronic communications for Topeka, Kan., said IT professionals try to head malware attacks carried by spam and e-mail off at the pass and not even allow them to the trusted side of the network's firewall. "Our 1,700 mailboxes receive hundreds of malwares and spywares and virus attempts hourly," he said. "Since using the Proofpoint - appliance - we have not had anything get through - I am knocking on wood as I say this - and the confidence level is understandably very high."

Like Commtouch, Proofpoint, based in Cupertino, Calif., is in the business of helping companies secure e-mail communications. In fact, the company includes Commtouch's Zero-Hour Virus Outbreak Protection in its products. Proofpoint's latest offering, Proofpoint Dynamic Reputation, is an e-mail reputation service that combines local, predictive behavioral data and globally observed reputation, analyzed by powerful machine learning algorithms, to block incoming connections from malicious IP addresses.

"With the new reputation system we are eliminating the majority of all of the bad stuff before it even enters our system," Stephens said. "All incoming SMTP is rerouted to Proofpoint servers and they screen for us and flag all of the bad-reputation sources."

The onslaught of server-side polymorphic malware in the first few hours of each new outbreak has caused some network administrators to go as far as to block all .exe file attachments, the Commtouch report contends.

Roughly half the .exe files circulated on the Internet are legitimate files exchanged by users in collaborative work groups, Herson said, so IT managers need a tool that blocks viruses and allows legitimate files into the organization.

"If IT managers need to create a policy to block all .exe files, that means they do not have an adequate virus protection solution," Herson explained. "We recommend using a solution that analyzes the outbreak patterns, since typically a legitimate .exe file would not be sent en masse - it would simply be sent from one user to another, or within a limited group. Reputation services that identify the reputation of the sender can also help, that is, if they are dynamic enough to identify traffic sent from zombies, since the majority of e-mail-borne malware is sent from zombie machines."

In addition to SMTP filtering, Stephens recommended IT managers should use content filters as well to protect against e-mail-borne attacks.

"Internet content filtering is as important as SMTP filtering," he said. "Hanging out at the bogus Web sites invites attacks."