A third of Stabuniq Trojan infections are at US banks

Dan Kaplan

December 21, 2012

An information-gathering Trojan has successfully compromised servers at a number of US financial institutions.

According to researchers from Symantec, of roughly 40 IP addresses infected with the Stabuniq Trojan, 39 per cent belong to financial institutions who are mostly based in Chicago and New York.

Symantec software engineer Fred Gutierrez, said: "These financial institutions had their outer perimeter breached, as the Trojan has been found on mail servers, firewalls, proxy servers and gateways.

"Compromises are limited because Stabuniq's creators seem to be targeting specific people and entities."

Symantec's research also found that half the infected IP addresses were home users, while 11 per cent were companies that deal with internet security (due, perhaps, to these companies performing analysis of the threat).

The Trojan apparently spreads through targeted emails or via compromised websites that serve malware through exploit kits. "Over the past year, this threat has only been found in small numbers and has not been widespread, suggesting the authors may have been targeting specific people and entities," Gutierrez said.