# Trojan.Stabuniq Found on Financial Institution Servers



Dec 20, 2012 04:33 PM

Migration User

*Contributor: Alan Neville*

Almost a year ago we added detection for a low prevalence Trojan found on servers belonging to financial institutions, including banking firms and credit unions. The Trojan also compromised home computer users and computers at security firms. For easier identification and tracking we recently renamed this threat to Trojan.Stabuniq.

***Figure 1.*** *Trojan.Stabuniq distribution by type*

Approximately half of unique IP addresses found with Trojan.Stabuniq belong to home users. Another 11 percent belong to companies that deal with Internet security (due, perhaps, to these companies performing analysis of the threat). A staggering 39 percent, however, belong to financial institutions. These financial institutions had their outer perimeter breached as the Trojan has been found on mail servers, firewalls, proxy servers, and gateways.

Trojan.Stabuniq has relied upon a combination of spam email and Web exploit kits to compromise computers. 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. The approximate location of unique IP addresses where the Trojan has been found converges on the eastern half of the United States:

***Figure 2.*** *Trojan.Stabuniq geographic distribution by unique IP address*

The Trojan collects information from the compromised computer and then sends it to a command-and-control (C&C) server. Additional technical details are available.

Overall, this Trojan has not infected many machines in the past year, is localized to the United States, and—given that close to 40 percent of its targets are financial institutions—at this stage we believe the malware authors may simply be gathering information.



## Tags and Keywords

## Related Entries and Links

No Related Resource entered.