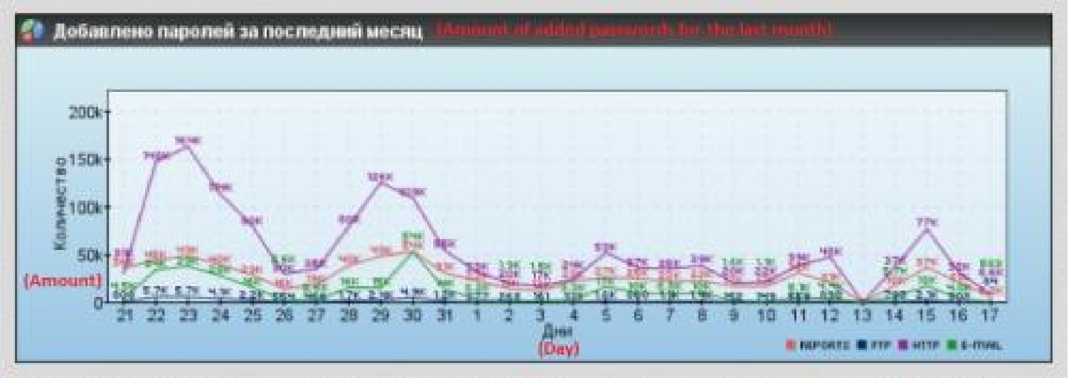
Stolen credentials found for about two million compromised accounts

December 5 2013, by Nancy Owano



(Phys.org) —Researchers have discovered a mountain-high trove of stolen credentials. Some two million compromised accounts were found on a Netherlands based server using a botnet controller, with the nickname "Pony." In a blog post on Tuesday coauthored by Trustwave SpiderLabs' security researchers, Daniel Chechik and Anat Fox Davidi, the researchers said that "one of the latest instances we've run into is larger than the last with stolen credentials for approximately two million compromised accounts." At some point, the two said, the source code for Pony was leaked. "With the source code of Pony leaked and in the wild, we continue to see new instances and forks of Pony 1.9."

The goods unearthed included snatched usernames and passwords from mainstream accounts such as Facebook, Twitter, Google, and Yahoo, but the botnet also succeeded to scoop up FTP, remote desktop and secure shell account details. The tally is: 1.6 million website login credentials; 320,000 email account credentials; 41,000 FTP account credentials; 3,000 remote desktop credentials; and 3,000 secure shell account credentials.

The blog noted that "Information discussed in this blog post was also disclosed to relevant parties." The title of the post, "Look What I Found: Moar Pony!" was making numerous headlines by Wednesday. Michael Mimoso of Threatpost, the news service of Kaspersky Lab, in his observations about the discovery, said that "Since the Pony controller source code was leaked earlier this year, researchers have been finding more of them online used to manage botnets big and small."

In this instance, popular social networks showed high numbers in what was nabbed but some other interesting findings emerged, also. Two social networking websites aimed at Russian-speaking audiences had a notable presence on the list, they reported, "which probably indicates that a decent portion of the victims comprised were Russian speakers." Still, trying to pinpoint a targeted attack on a particular country was not to be: A quick glance at the geo-location statistics would make one think that this attack was a targeted attack on the Netherlands but that did not tell the real story, they said. "Taking a closer look at the IP log files, however, revealed that most of the entries from NL IP range are in fact a single IP address that seems to have functioned as a gateway or reverse proxy between the infected machines and the Command-and-Control server, which resides in the Netherlands as well."

They said attackers commonly deploy the reverse proxy technique in order to prevent the discovery and shutdown of the Command-and-Control server. "This behavior, they said, "does prevent us from learning more about the targeted countries in this attack, if there were any." What they could conclude was that the attack was "fairly global," with some of the victims scattered all over the world.

Another revelation from all this is that, in 2013, and approaching 2014, many computer users have not dropped poor password-making habits that are vulnerable to credential theft. The impulse continues to be making a password that is merely easy to remember. "So what's worse," said Mimoso, "finding two million passwords harvested by a botnet, or learning that most of the stolen passwords are terribly weak?"

The list had passwords such as 123456, 123456789, 1234, and "password." Spider Labs rated six percent of the passwords "terrible," 28 percent "bad," 44 percent "medium," 17 percent "good," and just five percent "excellent."

SpiderLabs is described as "an elite team of ethical hackers, investigators and researchers" at Trustwave.

More information: blog.spiderlabs.com/2013/12/lo … found-moar-pony.html

© 2013 Phys.org

Citation: Stolen credentials found for about two million compromised accounts (2013, December 5) retrieved 8 May 2024 from https://phys.org/news/2013-12-stolen-credentials-million-compromised-accounts.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.