

EXHIBIT 10

Register | Log in



Pay-per-mile car insurance.
For those riding on the fast lane during rush hour.

GET A QUOTE
metromile

MAIN MENU ▾ MY STORIES: 25 ▾ FORUMS SUBSCRIBE JOBS

MINISTRY OF INNOVATION / BUSINESS OF TECHNOLOGY

Worm steals 45,000 Facebook login credentials, infects victims' friends

The Ramnit worm has been used to steal at least 45,000 Facebook logins with ...

by Jon Brodtkin - Jan 5 2012, 9:05am PST

77

A worm previously used to commit financial fraud is now stealing Facebook login credentials, compromising at least 45,000 Facebook accounts with the goals of transmitting malicious links to victims' friends and gaining remote access to corporate networks.

The security company Seculert has been tracking the progress of Ramnit, a worm first discovered in April 2010, and described by Microsoft as "multi-component malware that infects Windows executable files, Microsoft Office files and HTML files" in order to steal "sensitive information such as saved FTP credentials and browser cookies." Ramnit has previously been used to "bypass two-factor authentication and transaction signing systems, gain remote access to financial institutions, compromise online banking sessions and penetrate several corporate networks." Seculert says.

Recently, Seculert set up a sinkhole and discovered that 800,000 machines were infected between September and December. Moreover, Seculert found that more than 45,000 Facebook login credentials, mostly in the UK and France, were stolen by a new variant of the worm.

"We suspect that the attackers behind Ramnit are using the stolen credentials to log-in to victims' Facebook accounts and to transmit malicious links to their friends, thereby magnifying the malware's spread even further," Seculert said. "In addition, cybercriminals are taking advantage of the fact that users tend to use the same password in various web-based services (Facebook, Gmail, Corporate SSL VPN, Outlook Web Access, etc.) to gain remote access to corporate networks."

Facebook fraud, of course, is nothing new. Facebook itself has acknowledged seeing 600,000 compromised logins each day, although that accounts for just 0.06 percent of the 1 billion daily Facebook logins each day.

READER COMMENTS 77

LATEST FEATURE STORY ▾

7 437 111



Jon Brodtkin / Jon is Ars Technica's senior IT reporter, covering business technology, the FCC and broadband, telecommunications, supercomputing, data centers, and wireless technology.
@JBrodtkin on Twitter

← OLDER STORY

YOU MAY ALSO LIKE

- What happened to your files?**
All of your files were protected by a s...
More information about the encryptio
- What does this mean?**
This means that the structure and da...
with them, read them or see them, it
- How did this happen?**
Especially for you, on our server we...

Inside CryptoWall 2.0: ransomware, professional edition



Cyber espionage targets Syrian activists, linked to ISIS



North Korea and cyberterrorists won big in Sony hack, researcher says



Sponsored: Measuring growth in the cloud

NEWER STORY →



FEATURE STORY (2 PAGES)

One coach's nightmare — sending his wank video to female players

Don't misclick your private pics.

WATCH ARS VIDEO



Hackers promise "Christmas present" Sony Pictures won't like



US sanctions North Korea over Sony hack and classifies attack evidence



12 million home and business routers vulnerable to critical hijacking hack



FBI claims North Korean involvement in Sony Pictures attack

Wandering the Robotics Marketplace at CES

We go robot hunting at CES and bump into all kinds of interesting bots.

STAY IN THE KNOW WITH

LATEST NEWS



Pirated music infiltrating US prisons, record label says



Wandering the Robotics Marketplace at CES

TOUCHDOWN OR SPLASHDOWN?

SpaceX to try again for ISS cargo

delivery, first stage return

ONE RING TO SCREW THEM

Report: GameStop fixing and reselling red-ringed Xbox 360s since 2009

OVER HERE!

Spotlight search in OS X Yosemite exposes private user details to spammers



Inside CryptoWall 2.0: Ransomware, professional edition

TRANSPARENTLY SECURE: A NEW SECURITY HEADLINE

D

DLP Redact Sensitive Data

clearswift.com/

Learn how to prevent data leaks by automatically XXXXXing out key data

Threat Protection Tool ▾

Remove Malware - Free ▾

Unlimited Anonymous VPN ▾

SITE LINKS

MORE READING

CONDENSED MASTHEADS

[About Us](#)
[Advertise with us](#)
[Contact Us](#)
[Reprints](#)

SUBSCRIPTIONS

[Subscribe to Ars](#)

[RSS Feeds](#)
[Newsletters](#)

[Reddit](#)
[Wired](#)
[Vanity Fair](#)
[Style](#)
[Details](#)

[Visit our sister sites](#)
[Subscribe to a magazine](#)

[VIEW MOBILE SITE](#)

© 2015 Condé Nast. All rights reserved
Use of this Site constitutes acceptance of our [User Agreement](#) (effective 1/2/14) and [Privacy Policy](#) (effective 1/2/14), and [Ars Technica Addendum](#) (effective 5/17/2012)
[Your California Privacy Rights](#)
The material on this site may not be reproduced, distributed, transmitted, cached or otherwise used, except with the prior written permission of Condé Nast.

[Ad Choices](#)