

## **Account Takeover Threat Resurfaces**

January 24, 2012

The Ramnit Worm has resurfaced and is reportedly targeting Facebook users.

### **What is Ramnit?**

Ramnit is a worm that can spread to other computers and reproduce itself without being sent through email or a website. Since 2010, Ramnit has altered to include a Zeus variation which targets online banking credentials, particularly those of consumers. This new version has successfully bypassed two-factor authentication, infecting an estimated 800,000 computers since September 2011.

### **What does this mean to Financial Institutions?**

The Ramnit worm, which successfully defeated two-factor authentication used to protect online banking accounts and corporate networks in 2011, is now targeting Facebook users. This is particularly concerning to the financial community due to the potentially large number of consumer level accounts that could be compromised. Many individuals use the same passwords to access personal email and Facebook accounts as well as for remote access to corporate networks and online banking accounts.

Researchers believe the cybercriminals unleashing Ramnit are targeting Facebook for multiple reasons. A large number of potential victims exist in Facebook, approximately 800 million potential victims worldwide. Additionally, if an individual uses the same password for multiple applications, gaining his/her Facebook credentials may open the door to online banking accounts, remote access to corporate networks, etc.

### **What should you do?**

Members should be watchful of increased consumer-level Account Takeover from credential stealing malware such as Ramnit. We encourage you to educate internal staff as well as consumer-level account holders to not use the same credentials for social-based services and their financial accounts.

The same passwords or security challenge questions should never be used for social media, email and online banking access.

Unless we are made aware of a significantly different attempt and/or important piece of information related to this issue, we will not send further bulletins on this subject.

### **For additional Information Visit:**

Seculert – Cyber Threat Management - <http://mashable.com/2012/01/06/ramnit/>

Trusteer - <http://www.trusteer.com/blog/ramnit-evolution-%E2%80%93-worm-financial-malware>

Microsoft's Malware Protection Center - <http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Win32%2fRamnit>