

## ING Takes a Leap With Trusteer Desktop Security Software

Avivah Litan

ING Direct is taking the unusual move of distributing and supporting consumer desktop security software from Trusteer. Consider similar measures to avert PC-based attacks on consumer information and accounts.

## NEWS ANALYSIS

---

### Event

On 21 May 2008, ING Direct, the U.S. direct bank division of the Netherlands-based bank ING, announced that it plans to offer its customers free software to protect against account and data compromise. ING will use Rapport software by Trusteer — a small, privately held company founded in 2006 by security industry veterans — to establish a secure "pipeline" between the bank and its customers. It hopes this software will reduce the threat of "phishing," "pharming" and man-in-the-middle attacks.

### Analysis

This move is in keeping with ING Direct's reputation as an innovator within the banking business environment. Trusteer's intriguing but as yet unproven technology promises to protect user sessions from the damage wrought by malware and phishing attacks.

Banks and other service providers are averse to distributing desktop security software, as they want to avoid the headaches of PC troubleshooting and customer service calls. (Accordingly, Trusteer will support ING Direct's customer issues.) But most banks' server-based applications offer only limited protection against attacks from malware that could potentially hijack consumer browser sessions and steal sensitive information that is stored on or entered from PCs. The spread of such attacks is forcing banks to look seriously at offering a method for secure customer PC communications with their sites.

Trusteer's packaging of desktop security functionality makes it easier for banks and others to effectively distribute and use. Rapport is a small (400 KB) application that checks the behavior of the PC during interaction with protected Web sites. Its functionality includes:

- Blocking operating-system-level application programming interface (API) calls that can represent malicious activity, including capturing sensitive information or taking over communication control. In theory, this should block the successful execution of malware on a Trusteer customer's PC while he or she is communicating with the protected Web site. (This feature contrasts with functions available through signature-based antivirus and anti-spyware products — the best of which still have less than a 50% chance of catching new threats.)
- Encrypting user keystrokes at the keyboard driver level and keeping the data encrypted until it reaches the Web site, where it is decrypted by the same component that manages Secure Sockets Layer (SSL) encryption and decryption.
- Validating the Web site's IP address and SSL certificate and preventing users from typing their user IDs and passwords into imposter Web sites.

This layered security approach could prevent damage from malware executing on a consumer's PC and keep consumers away from phishing sites. If Rapport doesn't successfully detect malware through its operating system API analysis, its encryption of user keystrokes could help prevent thieves from stealing useful typed-in information. If ING Direct succeeds with Trusteer software, expect other direct banks to follow.

## RECOMMENDATIONS

---

### Consumer service providers:

- Evaluate Rapport as a defense against malware, phishing, pharming and other types of attacks launched directly against customers.
- Continue to provide strong user authentication, transaction verification and fraud detection, but be aware that browser-based malware can bypass authentication and transaction verification by changing instructions executed on the server.
- Extend your efforts in competitive differentiation to include technology areas like security. Keep in mind that direct-banking customers are more likely to be early adopters of technology and may be more open to adding software to their desktops.

## RECOMMENDED READING

---

- "Magic Quadrant for Endpoint Protection Platforms, 2007" — A broader suite of defensive technologies supported by an extensible management platform has replaced the stand-alone antivirus market. **By Peter Firstbrook, Arabella Hallawell, John Girard and Neil MacDonald**
- "Introducing the Endpoint Protection Platform" — Although traditional desktop antivirus solutions are morphing into broader endpoint security offerings, buyers should still focus first on the functionality they need, even if they must turn to multiple solutions. **By Peter Firstbrook, Arabella Hallawell, John Girard and Neil MacDonald**

(You may need to sign in or be a Gartner client to access the documents referenced in this First Take.)

## REGIONAL HEADQUARTERS

---

### **Corporate Headquarters**

56 Top Gallant Road  
Stamford, CT 06902-7700  
U.S.A.  
+1 203 964 0096

### **European Headquarters**

Tamesis  
The Glanty  
Egham  
Surrey, TW20 9AW  
UNITED KINGDOM  
+44 1784 431611

### **Asia/Pacific Headquarters**

Gartner Australasia Pty. Ltd.  
Level 9, 141 Walker Street  
North Sydney  
New South Wales 2060  
AUSTRALIA  
+61 2 9459 4600

### **Japan Headquarters**

Gartner Japan Ltd.  
Aobadai Hills, 6F  
7-7, Aobadai, 4-chome  
Meguro-ku, Tokyo 153-0042  
JAPAN  
+81 3 3481 3670

### **Latin America Headquarters**

Gartner do Brazil  
Av. das Nações Unidas, 12551  
9º andar—World Trade Center  
04578-903—São Paulo SP  
BRAZIL  
+55 11 3443 1509