



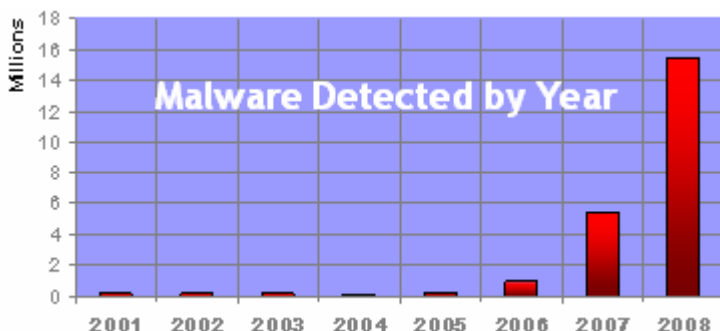
Criminal Attacks on Consumer Browsers - Beyond Business Control?

February 2009

The prevention of identity theft and fraud is an obvious priority for any institution doing business online today. In addition to lost customers, compensation costs, and brand damage, virtually all online businesses are subject to a wide range of regulatory measures (FTC Red Flags, FFIEC, PCI, etc.) that mandate customer protection.

Yet despite widespread attention, most institutions today **have no control over by far the most commonly exploited approach to online identity theft and fraud - browser based attacks**. Cyber-criminals have learned over time that breaking into strictly protected institutional servers is not the easiest way to steal personal information and commit fraud. To do so, they must evade the multiple layers of defense that have been deployed by most institutions over many years. A much easier approach is to attack the unprotected consumer browser. By attacking the browser, criminals can achieve the same results as server attacks, but without the need to evade multiple layers of defense. Most browser attacks are virtually impossible to prevent for institutions with no influence over their customer's browser security policies.

With obvious lack of browser protections, it's no surprise that browser attacks have grown rapidly in recent years. The technical approaches to browser compromise can be broken into two basic classes: malware programs (e.g. man-in-the-browser), and redirect (e.g. man-in-the-middle, phishing, pharming). The number of malware programs developed in 2008 exceeds the total developed during previous 15 years combined¹. Similarly, seventy percent of the top 100 Web sites host malicious content designed to redirect visitors to a malicious Web site². The volume of phishing attacks detected during 2008 grew by 66% over those observed throughout 2007 and more than 10 million users were exposed to pharming and man-in-the-middle attacks³. Bottom line: browser attacks are growing at astronomical rates and it's happening for one simple reason: criminals are making money.



Many of the most effective browser-based attacks are designed to spring into action while the customer is connected to financial, retail, healthcare, or government Web sites. It is during this time in which consumer trust level is high and sensitive information is exchanged, that criminals most profitably insert themselves into the browser. The next sections illustrate the consequences of these attacks for the online business and the consumer.

Stealing Personally Identifiable Information (PII)

Once in the hands of criminals, an individual's PII (e.g. name, credit card numbers, government ID,) can be applied to perpetrate a wide range of fraud. Although most organizations do a good job of protecting PII stored on servers, browser attacks provide criminals with direct access to all information that customers view or send to a Web site. Access to viewed information allows for collection of contact information, statements, bills, check images, and more. Access to sent information allows for collection of, among other things, login credentials. Of course with login credentials in hand, the criminal gains full access to all account PII. Protecting PII while stored on servers yet leaving it completely unprotected while presented in the browser is similar to protecting customer money in the vault, yet allowing customers to be robbed while speaking to the cashier.

An extremely effective technique that is widely used to steal PII today is Web form injection. For example, a Web page immediately following customer logins is modified by malware to include a bogus form requesting that the customer enter credit card numbers or other PII. The form appears to be part of the trusted Web site, although it is actually injected locally. When the customer enters information, it is immediately delivered to the criminals. This technique is used today by Torpig, Silentbanker, and other Trojans to steal a wide range of PII while customers are connected to over 1000 different online banking, retail, and government websites.

Title	please select...
First Name	<input type="text"/>
Surname	<input type="text"/>
Mother's maiden name	<input type="text"/>
Mobile Phone Number	<input type="text"/>
Work Phone Number	<input type="text"/>
Home Phone Number	<input type="text"/>
Home Address (house name/number, flat number, street, town/city, post code)	<input type="text"/>
Email	<input type="text"/>
PIN	<input type="text"/>
Password	<input type="text"/>
Account Number(s)	<input type="text"/>
Sort Code(s)	<input type="text"/>
Overdraft limit(s)	<input type="text"/>
Maestro Debit Card or Cash Card Number	<input type="text"/>

An example for injected form that steals PII once the customer logs onto the website

¹ <http://www.pandasecurity.com/homeusers/media/press-releases/viewnews?noticia=9505&sitepanda=particulares>
² <http://www.informationweek.com/news/internet/security/showArticle.jhtml?articleID=212901775&subSection=Vulnerabilities+and+threats>
³ http://www.csoonline.com/article/474365/CheckFree_Warns_Million_Customers_After_Hack



Trust Scams

Browser-based trust scams combine browser attack techniques with consumer trust in brand name Web sites to convince customers perform fraudulent transactions. Browser malware can locally change banners, warnings, or any other Web site content to include transaction instructions of their choice. Since the bogus content appears as part of the trusted Web site, customers tend to trust it and do what they are told. The following three examples illustrate simple, yet effective trust scams.

- **Financial:** A bogus banner is inserted into a bank's Web site announcing a new partnership with Lanimirc (criminal spelled backwards) Investments. The partnership invites customers to invest up to \$50,000 with excellent interest rates. When customers click the banner, they get more information about the partnership alongside forged analyst opinions and newspaper quotes. The proposition even includes a phone number (operated by criminal operators) for the customer to call for more information. All of this information appears while customers are connected to the bank's Web site, so again they tend to trust in their legitimacy. Customers that choose to accept the offer are requested to add Lanimirc as a payee and transfer the money into a new account controlled by the criminals.



Fake banner appears as part of the bank's website, convinces customers to execute fraudulent money transfers

- **Retail:** During the check out process of a legitimate online retailer, a bogus payment method is presented allowing payment directly from a bank account. Customers who choose this bogus method are asked to add a payee with a name similar to that of the actual retailer and transfer the purchase sum into that account. Once the customer performs the transaction he receives a bogus confirmation message indicating that money was received and goods delivered. Criminals now hold the customer's money but no goods will be delivered.
- **Government:** A bogus banner is inserted into a legitimate government website offering a discounted tax payment by using a new service. To use the service, the customer is asked to simply enter credit card information or transfer money to the Lanimirc Payment Service. The bogus information appears to originate from the actual Web site and looks highly reliable, but once again, payment goes straight to the criminals.

Transaction Tampering

Rather than seeking to convince consumers to carry out new transactions as described above, criminals may also choose to simply tamper with existing transactions between an online business and its customers. Once again, the key to the browser-based attack is control of the information that enters and leaves the browser. For example, when a customer makes a request to transfer a certain amount to a certain account, a browser malware can change the outbound request to transfer a different amount to a different account. Even if the Web site presents a confirmation page before executing the transaction, the criminal can modify this page to present the information that the customer expects.

A New Approach Is Needed

Thus far, preventing browser-based attacks has been easier said than done. Institutions have little or no control over customer-owned browser security policies while customers lack the technical skills to protect themselves. Indeed, consumers (and most regulatory measures) expect the online institution to take responsibility for protection against fraud that occurs while connected to the institution's Web site.

A new approach is needed that allows the online institution to apply browser-based fraud protection policies and controls without burdening the customer with technical requirements. Like most security solutions today, (but especially in difficult economic environments) deployment must require minimal internal resources and zero changes to existing infrastructure. In short, the solution must reduce exposure to risk without increasing costs. A very few solutions meet these demands. Trusteer Rapport is one of them.



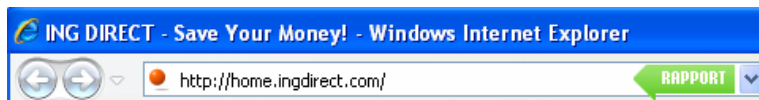
Criminal Attacks on Consumer Browsers - Beyond Business Control?

February 2009

Trusteer's Rapport

Trusteer's Rapport is a browser-based attack protection service for online financial, retail, healthcare, and government, institutions. It prevents browser malware and redirect attacks from perpetrating PII theft, trust scams, and transaction tampering. The Rapport service includes a lightweight browser security plug-in, as well as cloud-based analysis and reporting services as described below.

The lightweight browser security plug-in is installed in-flow when the customer first visits the Web site. This one-time process takes a few seconds and is very similar to a Flash viewer (also a browser plug-in) installation. Customers who have already downloaded the Rapport plug-in from another Trusteer partner do not need to download anything!



Rapport's green arrow inside the address bar indicates a protected session

Rapport Benefits



Protects against Browser Malware

Rapport acts like a vault inside the browser protecting Web pages downloaded to the browser, as well as data entered by customers in response to those pages. Malware cannot read or alter these pages or the information customers enter into them. PII, transactions, and Web site integrity is preserved.



Prevents Redirect and Fraudulent Website Attacks

Rapport prevents redirect and fraudulent Web site attacks through strong authentication of trusted Web sites before releasing sensitive information from the vault. By securing browser data in the vault and then ensuring that outbound data is sent only to trusted sites, Rapport eliminates any criminal entry point.



Actionable Intelligence

Attempts to access PII, tamper with transaction, damage Web site integrity, or crack the vault are reported to the Trusteer cloud-based fraud analysis service. Trusteer's team of fraud analysts work 24x7 analyzing this information from customers all over the world in order to identify new attack patterns. Advanced automatic update mechanisms allow Trusteer to react immediately to new threats. Institutions receive immediate reports and actionable alerts of new attacks and can learn of attacks as they happen instead of days, weeks, and sometimes months after.

Take Control of Online Identity Theft and Fraud with Rapport

Most organizations today have no control over the largest source of online identity theft and fraud - browser based attacks. As long as any online business cannot apply security to browsers during the time that customers are connected to their Web sites, they leave themselves and customers open to attack. They essentially cede the battle to the criminals. For most institutions (and regulatory bodies) the resulting risk of PII theft, trust scams, and transaction tampering is unacceptable. Organizations need to take control of browser security whenever their customers are connected to their Web sites - but do so without burdening the customer. Trusteer's Rapport can make that happen. It provides organizations with the transparent controls needed to deter all forms of browser attack without changes to existing infrastructure and with minimal requirement for internal resources.

