Transaction Generators: Root Kits for the Web

Collin Jackson      Dan Boneh       John Mitchell

Stanford University
Current phishing attacks

- Primarily focused on stealing using credentials

- Industry response:
  - Make it harder to use stolen credentials:
    - Backend analytics, One-time passwords
Next front: transaction generators

<script> // Mozilla, Netscape, Firefox
document.getElementById("appcontent").addEventListener( "load", function() {
    var currentLocation =
        getBrowser().selectedBrowser.contentDocument.location;
    if (currentLocation.href.indexOf("www.retailer.com/loggedin") > 0) {
        var xhr = new XMLHttpRequest();
        xhr.open("POST", "https://www.retailer.com/buy");
        xhr.send("item=blender&quantity=1&address=Kansas");
    }
}, true);
</script>
Transaction generators (TG)

- Transactions look identical to ones issued by user
  - Same IP address
  - Same time of day

- Defeats strong authentication:
  - One time passwords
  - Smartcards
  - Client certs

- Standard session hijacking …
Initial reports in the wild

New Trojans plunder bank accounts

By Joris Evers
Staff Writer, CNET News.com
Published: February 17, 2006, 3:59 PM PST

SAN JOSE, Calif.—Cybercriminals are surfing into online banks with you to steal your money.

Password-stealing Trojan horses used to be all the rage. The software would nestle itself on a PC after opening a bad e-mail attachment or visiting a malicious Web site. But in response to the increased adoption of stronger authentication, cybercriminals are changing their tactics, according to Alex Shipp, a senior antivirus technologist at MessageLabs.

"We have recently seen a move away from stealing user name and passwords," Shipp said during a panel discussion at the RSA Conference 2005 here on Thursday. The new "bank-stealing Trojans" wait until the victim has actually logged in to their bank. "It then just transfers the money out."

"All of the authentication, little keys you have to have in your hand, biometrical things, it doesn't matter. The bad guy just waits until you're there and then takes the money out," Shipp said.

This new type of Trojan is on the rise and is currently No. 3 on the list of most common threats, according to Shipp. The most-seen threat
Stealthy transaction generators

- Open and recently shipped orders page:
  https://www.amazon.com/gp/css/history/view.html

<table>
<thead>
<tr>
<th>Order date:</th>
<th>Feb. 1, 2007</th>
<th>Items:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order #</td>
<td>102-6259471-5816113</td>
<td>• Little Einsteins DVD</td>
</tr>
<tr>
<td>Recipient:</td>
<td>John Victim</td>
<td>Total: 7.95$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Order date:</th>
<th>Jan. 13, 2007</th>
<th>Items:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order #</td>
<td>102-6369461-5816862</td>
<td>• Cuisinart CSB-76BC</td>
</tr>
<tr>
<td>Recipient:</td>
<td>John Victim</td>
<td>Total: 29.95$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Order date:</th>
<th>Dec. 16, 2006</th>
<th>Items:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order #</td>
<td>102-7629461-5816862</td>
<td>• The Da Vinci Code, Dan Brown</td>
</tr>
<tr>
<td>Recipient:</td>
<td>John Victim</td>
<td>Total: 7.99$</td>
</tr>
</tbody>
</table>
Stealthy transaction generators

- Open and recently shipped orders page:
  [https://www.amazon.com/gp/css/history/view.html](https://www.amazon.com/gp/css/history/view.html)

<table>
<thead>
<tr>
<th>Order date:</th>
<th>Feb. 1, 2007</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order #</td>
<td>102-6259471-5816113</td>
</tr>
<tr>
<td>Recipient:</td>
<td>John Victim</td>
</tr>
<tr>
<td>Items:</td>
<td>Little Einsteins DVD</td>
</tr>
<tr>
<td>Total:</td>
<td>7.95$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Order date:</th>
<th>Dec. 16, 2006</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order #</td>
<td>102-7629461-5816862</td>
</tr>
<tr>
<td>Recipient:</td>
<td>John Victim</td>
</tr>
<tr>
<td>Items:</td>
<td>The Da Vinci Code, Dan Brown</td>
</tr>
<tr>
<td>Total:</td>
<td>7.99$</td>
</tr>
</tbody>
</table>
End of month stealth

- Online credit card payment page:
  
  https://www.bank.com/statement.html
Countermeasures
Proposal: add CAPTCHA to checkout page.

Problems:

- Malware can fool user into solving CAPTCHA for it
- Malware can (in stealth) add items to user’s shopping cart

Another non-solution:
- Block TG from getting into browser in the first place
Transaction Confirmation

- Basic components:

  - Trusted User Agent
  - Infected Browser
  - Merchant or Bank

Via USB token:
- David Steeves, Microsoft

Via cellphone:
- Passmark (and others)
SpyBlock

- A transaction confirmation system for the web

**Goals:**

- Simple user interface: no extra hardware:
  - Isolate TUA from malware using a VMM

- Integrate with existing identity systems
  - We use MS CardSpace to generate shared secret K

- Easy to integrate into server side software

- Solve trusted path to user
  - Malware should be unable to change transaction details displayed to the user
Step 1: user logs in using CardSpace

We rely on CardSpace to solve trusted path problem
(e.g. secure attention sequence)
Step 2: user makes a purchase
Step 3: Site needs confirmation

- Remote site sends back page containing:

  ```javascript
  if (window.spyblock) {
    spyblock.confirm(document.form1.transaction, {
      observe: function(subject, topic, data) {
        document.form1.transactionMAC.value = data;
      }
    };
  }
  }
  ```

- Javascript activates SpyBlock browser helper.
Step 4: user confirmation from SpyBlock agent helper
Confirmation pop-up

- Always on top
  - Guest OS cannot modify contents
  - Guest OS cannot generate false clicks

- Once confirmed, SpyBlock agent asks CardSpace to MAC using session key $K$

- MAC sent to remote web site.

- Note: malware can generate fake confirmation pop-ups.
Summary

- Transaction Generators are coming
  - Be prepared …

- **Take away message:**
  - Identity systems (e.g. CardSpace) need to include transaction confirmation
    - Simple User interface
    - Easy to integrate with web site software