Let’s Sink The Phishermen’s Boat!

=DEFCON 16 @ Las Vegas, Nevada=

Teo Sze Siong, <teo.sze.siong@f-secure.com>
F-Secure Corporation
Why this topic?

- Internet banking has become more and more preferred choice
- Yet, many people don't understand the risk they are facing in online banking

Do you think the following practices protect you from phishing attack?

- Keep antivirus software updated
- Use online banking on SSL-enabled websites only
- Use online banking on trusted machine only
- Use 2-factor authentication security feature
- Use latest web browser with fully patched plug-ins

Answer is NO!

How serious now?

- Billion dollar losses caused by phishing attacks
- Banks can't simply reverse transactions - legal issues

Gartner Survey Shows Phishing Attacks Escalated in 2007: More than $3 Billion Lost to These Attacks

Debit Cards Emerged as the Financial Instrument Targeted Most by Fraudsters

STAMFORD, Conn., December 17, 2007 — Phishing attacks in the United States soared in 2007 as $3.2 billion was lost to these attacks, according to a survey by Gartner, Inc. The survey found that 3.6 million adults lost money in phishing attacks in the 12 months ending in August 2007, as compared with the 2.3 million who did so the year before.

According to a survey of more than 4,800 online U.S. adults in August 2007 (which was representative of the online U.S. adult population) the attacks were more successful in 2007 than they were in the previous two years. Of consumers who received phishing e-mails in 2007, 3.3 percent say they lost money because of the attack, compared with 2.3 percent who lost money in 2006, and 2.9 percent who did so in 2005, according to similar Gartner surveys during those years.

"Phishing attacks are becoming more surreptitious and are often designed to drop malware that steals user credentials and sensitive information from consumer desktops," said Avivah Litan, vice president and distinguished analyst at Gartner. "Anti-phishing detection and prevention solutions are available but not utilized widely enough to stop the damage. These must be deployed and combined with solutions that also proactively detect and stop malware-based attacks."

"Customer-facing organizations cannot expect their customers' desktops to be protected from malicious code, nor from e-mail and/or advertising traps that lure innocent consumers to Web sites that turn out to be infection points," Ms. Litan said. "In fact, 11 percent of online adults say they don't use any security software (such as antivirus or anti-spyware products) on their desktop, and another 45 percent only use what they can get for free."

The average dollar loss per incident declined to $886 from $1,244 lost on average in 2006 (with a median loss of $200 in 2007), but because there were more victims, $3.2 billion was lost to phishing in 2007, according to surveyed consumers. There was a bit of relative good news, however; the amounts that consumers were able to recover also increased. Some 1.6 million adults recovered about 64 percent of their losses in 2007, up from the 54 percent that 1.5 million adults recovered in 2005.

PayPal and eBay continue to be the most-spoofed brands, but phishing attacks increasingly employ devious social engineering attacks, impersonating, for example, electronic greeting cards, charities and foreign businesses.

Thieves are increasingly stealing debit card and other bank account credentials to rob accounts — targeting areas where fraud detection is weaker than it is with credit card accounts. According to the survey, of those consumers who lost money to phishing attacks, 47 percent said a debit or check card had been the payment method used when they lost money or had unauthorized charges made on their accounts. This was followed by 32 percent of respondents who listed a credit card as the payment method, and 24 percent who listed a bank account as the method (multiple responses were allowed).

"Criminals have stepped up attacks on debit card and bank accounts, where back-end fraud detection systems are traditionally weaker than they are with credit card accounts," Ms. Litan said. "Fraud detection and authentication systems deployed widely in online banking in response to FFIEC banking regulator guidance are already a step behind fraudsters' latest techniques and must be updated to guard against browser hijackings, "man in the middle," and other hidden malware-based attacks often delivered to users through phishing e-mails. Regulators must get a better handle on the problem through consistent and timely bank reporting on their fraud incidents and losses."

Source: http://www.gartner.com/it/page.jsp?id=565125&format=print
How serious now?

- Currently, there is no complete automated solution to detect phishing accurately
- It is all over the world targeting different nationalities and different banks!
- Phishing techniques used are getting more sophisticated than before

Commonly used techniques in phishing

- DNS modification / cache poisoning a.k.a. pharming
- HTML / Javascript content with visual similarity (even Flash-based)
- Spoofed source email address
- ARP poisoning to redirect traffic
- API hooking (user mode / kernel mode)
- Browser plug-in (BHO mainly targeting Internet Explorer)
- Similar URLs / obfuscated encodings
- Hosting websites on fast flux network (usually botnet machines)
- Uses drive-by downloads to infect Trojan via software vulnerability
Flash-based phishing website

http://www.ppal-form-ssl.com/webscr/

Member Log-In

Forgot your email address?
Forgot your password?

Email Address: foo@bar.com
Password: ********

Log In

Enter Your Card Information - PayPal recommends using a debit card instead of a credit card, due to the higher security level of these. It's always safe to use the debit card linked to your checking account that is currently attached to your PayPal account.

Card number: 3748

Expiration date: Month: ___ Day: ___ Year: ___ Leave day as --, if day on card is not listed

CVV Code: ___

Card PIN Number: ___ 4 Digits code used at ATMs.

Name on card: ___

Source: http://www.f-secure.com/weblog/archives/00001066.html
Example 1: Website with drive-by download
Analysis report of drive-by download website

2008/05/17 18:44:31 - [UTCD-INFO] Priority Level: 5
2008/05/17 18:44:31 - [UTCD-INFO] UMS’s URL ID: 3643208
2008/05/17 18:44:31 - [UTCD-INFO] HTTP Request Metadata: null
2008/05/17 18:44:31 - [UTCD-INFO] Remaining Failure Retry: 3
2008/05/17 18:44:31 - [UTCD-INFO] URL Type: Web browser interpretable URL
2008/05/17 18:44:32 - [UTCD-INFO] Content-Type: text/html
2008/05/17 18:44:32 - [UTCD-INFO] Server Date: Sat, 17 May 2008 09:36:16 GMT
2008/05/17 18:44:32 - [UTCD-INFO] Server Type: Apache/2.2.8 (Unix)
2008/05/17 18:44:32 - [GOAT-INFO] WXPSP2-1: Windows XP Pro SP2 + Firefox 1.0 and IE6
2008/05/17 18:44:32 - [GOAT-INFO] IE6/IE7 = Enabled, Firefox1/2 = Enabled
2008/05/17 18:44:32 - [GOAT-INFO] Network IO Check Interval = 5secs
2008/05/17 18:44:32 - [GOAT-INFO] Network IO Activity Tolerance = 512bytes
2008/05/17 18:44:32 - [GOAT-INFO] Sending URL to UAE for automated analysis...
2008/05/17 18:44:32 - [GOAT-INFO] Analyzing website in VMware goat environment...
2008/05/17 18:46:29 - [UTCD-INFO] Time elapsed 1 minutes and 57 seconds
2008/05/17 18:46:31 - [UTCD-INFO] IE6/7 Process ID: 1668
2008/05/17 18:46:31 - [UTCD-INFO] FireFox 1/2 Process ID: 1676
2008/05/17 18:46:31 - [UTCD-INFO] Pop-up Window(s) Found: 0
2008/05/17 18:46:31 - [UTCD-INFO] Analyzing tracer log... (2,363,042 bytes)
2008/05/17 18:46:31 - [UTCD-INFO] Time elapsed 0.102503061295 second
2008/05/17 18:46:31 - [UTCD-INFO] Exploited web browser: Internet Explorer
2008/05/17 18:46:31 - [UTCD-INFO] Suspicious folder creation count: 0
2008/05/17 18:46:31 - [UTCD-INFO] Suspicious file creation count: 3
2008/05/17 18:46:31 - [UTCD-INFO] Suspicious registry key creation count: 6
2008/05/17 18:46:31 - [UTCD-INFO] Suspicious process creation count: 4
2008/05/17 18:46:31 - [UTCD-INFO] Threat percentage: 100%
2008/05/17 18:46:31 - [UTCD-INFO] Conclusion: Malicious

===== DEBUG INFORMATION - GOAT MACHINE CHANGES =====
['createdir': [],
'createfile': [
  {'file': '%windir%\system32\drivers\qdm33.sys'},
  {'file': '%windir%\system32\winctrl32.dll'},
  {'file': 'c:\6lwxsu.exe'}],
'createkey': [
  {'key': '%hkcu%\s-1-5-21-1343024091-1417001333-839522115-1003\parameters'},
  {'key': '%hkcu%\s-1-5-21-1343024091-1417001333-839522115-1003\rfc1156agent'},
  {'key': '%hklm%\software\microsoft\windows nt\currentversion\drivers32\controlset002'},
  {'key': '%hklm%\software\microsoft\windows nt\currentversion\drivers32\qdm33'},
  {'key': '%hklm%\system\currentcontrolset\services\qdm33'},
  {'key': '%hklm%\system\currentcontrolset\services\security'}],
'newproc': [
  {'1344,532': '%windir%\system32\cmd.exe'},
  {'1392,1264': '%windir%\system32\svchost.exe'},
  {'1392,1344': '%temp\bn7.tmp'},
  {'1668,1392': 'c:\6lwxsu.exe'}]

===== DEBUG INFORMATION - GOAT MACHINE CHANGES =====
Example 2: Website with drive-by download

Dr. Wang Zidong was born in Jiangsu, China, in 1965. He received the B. Sci. degree in mathematics in 1986 from Suzhou University, Suzhou, China, and the M. Sci. degree in applied mathematics in 1990 and the Ph. D. degree in electrical engineering in 1994, both from Nanjing University of Science and Technology, Nanjing, China. He was appointed Lecturer at East China Institute of Technology, Nanjing, China, in 1990 and was promoted to Associate Professor at Nanjing University of Science and Technology in 1994. From January 1997 to December 1998, he was an Alexander von Humboldt research fellow with the Automatic Control Laboratory, Ruhr University, Bochum, Germany. From January 1999 to February 2001, he was a Lecturer...
Analysis report of drive-by download website

2008/06/26 05:30:37 - [UTCDF-INFO] Priority Level: 5
2008/06/26 05:30:37 - [UTCDF-INFO] UMS's URL ID: 5088202
2008/06/26 05:30:37 - [UTCDF-INFO] HTTP Request Metadata: null
2008/06/26 05:30:37 - [UTCDF-INFO] Remaining Failure Retry: 3
2008/06/26 05:30:37 - [UTCDF-INFO] URL Type: Web browser interpretable URL
2008/06/26 05:30:38 - [UTCDF-INFO] Content Length: 23,163 bytes
2008/06/26 05:30:38 - [UTCDF-INFO] Content-Type: text/html
2008/06/26 05:30:38 - [UTCDF-INFO] Server Type: Microsoft-IIS/5.0
2008/06/26 05:30:38 - [GOAT-INFO] WXPSP2-2: Windows XP Pro SP2 + Firefox 2.0 and IE 7.0
2008/06/26 05:30:38 - [GOAT-INFO] IE6.0/IE7.0 = Enabled, Firefox1.0/2.0 = Enabled
2008/06/26 05:30:38 - [GOAT-INFO] Network IO Check Interval = 5secs
2008/06/26 05:30:38 - [GOAT-INFO] Network IO Activity Tolerance = 512bytes
2008/06/26 05:30:38 - [UTCDF-INFO] Sending URL to UAE for automated analysis...
2008/06/26 05:30:38 - [UTCDF-INFO] Analyzing website in VMware goat environment...
2008/06/26 05:32:15 - [UTCDF-INFO] Time elapsed 1 minutes and 37 seconds
2008/06/26 05:32:15 - [UTCDF-INFO] IE 6.0/7.0 Process ID: 8368
2008/06/26 05:32:15 - [UTCDF-INFO] FireFox 1.0/2.0 Process ID: 8392
2008/06/26 05:32:15 - [UTCDF-INFO] Pop-up Window(s) Found: 0
2008/06/26 05:32:16 - [UTCDF-INFO] Analyzing tracer log... (20,669,663 bytes)
2008/06/26 05:32:16 - [UTCDF-INFO] Time elapsed 0.760082960129 second
2008/06/26 05:32:16 - [UTCDF-INFO] Exploited web browser: IE and Firefox
2008/06/26 05:32:16 - [UTCDF-INFO] Suspicious folder creation count: 0
2008/06/26 05:32:16 - [UTCDF-INFO] Suspicious file creation count: 7
2008/06/26 05:32:16 - [UTCDF-INFO] Suspicious registry key creation count: 35
2008/06/26 05:32:16 - [UTCDF-INFO] Suspicious process creation count: 4
2008/06/26 05:32:16 - [UTCDF-INFO] Threat percentage: 100%
2008/06/26 05:32:16 - [UTCDF-INFO] Conclusion: Malicious
.................. DEBUG INFORMATION - GOAT MACHINE CHANGES ..................

('createdir': [],
 'createfile': [
    {'file': '%intenetcache%\5ps8r2b2\ko[1].exe'},
    {'file': '%intenetcache%\6q9hncm8\ko[1].exe'},
    {'file': '%temp%\orz.exe'},
    {'file': '%windir%\kdsv.exe'},
    {'file': '%windir%\system32\drivers\ntdllapi.sys'},
    {'file': '%windir%\ugvq.exe'},
    {'file': 'c:\mahtestf3.bat'}],
 'createkey': [
    {'key': '%hku\ntdapi'},
    {'key': '%hku\software\microsoft\windows nt\currentversion\image file execution options\qqdoctormain.exe'},
    {'key': '%hku\software\microsoft\windows nt\currentversion\windows\clsid\{a9895933-6636-4281-bc58-e66de2af96a3\}\inprocserver32'},
    {'key': '%hku\software\microsoft\windows nt\currentversion\windows\clsid\{dc3d30ae-0380-4151-8934-ee98a34b0370\}\inprocserver32'},
    {'key': '%hku\software\microsoft\windows nt\currentversion\windows\explorer'},
    {'key': '%hku\software\microsoft\windows nt\currentversion\windows\inprocserver32'},
    {'key': '%hklm\software\microsoft\windows nt\currentversion\windows\software\microsoft\windows\currentversion\explorer\browser helper objects\{55694105-510b-4905-3695-954187462155\}'},
    {'key': '%hklm\software\microsoft\windows nt\currentversion\windows\software\microsoft\windows\currentversion\explorer\browser helper objects\{5a098945-2036-6084-9054-6087502480a5\}'}],
 'newproc': [
    {'8196,8484': '%windir%\kdsv.exe'},
    {'8368,8964': '%temp\orz.exe'},
    {'8392,8196': '%temp\orz.exe'},
    {'8964,8268': '%windir%\ugvq.exe'}],
 'newkey': [
    {'key': '%hku\ntdapi'},
    {'key': '%hku\software\microsoft\windows nt\currentversion\windows\software\microsoft\windows\currentversion\windows\explorer\browser helper objects\{55694105-510b-4905-3695-954187462155\}'}]

================================== DEBUG INFORMATION - GOAT MACHINE CHANGES ==================================
Infected Virtual Machine analysis log file

2008-06-25 14:32:12 : Enumerating window handle(s)...
2008-06-25 14:32:12 : [WINDOW] TF_FloatingLangBar_WndTitle
2008-06-25 14:32:12 : [WINDOW] Connections Tray
2008-06-25 14:32:12 : [WINDOW] Power Meter
2008-06-25 14:32:12 : [WINDOW] MS_WebcheckMonitor
2008-06-25 14:32:12 : [WINDOW] NetscapeDispatchWnd
2008-06-25 14:32:12 : [WINDOW] Program Manager

---

Malware windows handle
Example 3: Website with drive-by download
2008/05/21 16:52:19 - [UTCD-INFO] Priority Level: 5
2008/05/21 16:52:19 - [UTCD-INFO] UMS's URL ID: 365
2008/05/21 16:52:19 - [UTCD-INFO] Remaining Failure Retry: 3
2008/05/21 16:52:20 - [UTCD-INFO] URL Type: Web browser interpretable URL
2008/05/21 16:52:20 - [UTCD-INFO] Content Length: 1,540 bytes
2008/05/21 16:52:20 - [UTCD-INFO] Content-Type: text/html
2008/05/21 16:52:20 - [UTCD-INFO] Server Type: Zeus/4.3
2008/05/21 16:52:20 - [GOAT-INFO] WXPSP2-1: Windows XP Pro SP2 + Firefox 1.0 and IE 6.0
2008/05/21 16:52:20 - [GOAT-INFO] IE6.0/IE7.0 = Enabled, Firefox1.0/2.0 = Enabled
2008/05/21 16:52:20 - [GOAT-INFO] Network IO Check Interval = 5secs
2008/05/21 16:52:20 - [GOAT-INFO] Network IO Activity Tolerance = 512bytes
2008/05/21 16:52:20 - [UTCD-INFO] Sending URL to UAE for automated analysis...
2008/05/21 16:52:20 - [UTCD-INFO] Analyzing website in VMware goat environment...
2008/05/21 16:52:50 - [UTCD-INFO] Time elapsed 0 minutes and 30 seconds
2008/05/21 16:52:50 - [UTCD-INFO] IE 6.0/7.0 Process ID: 840
2008/05/21 16:52:50 - [UTCD-INFO] Firefox 1.0/2.0 Process ID: 1768
2008/05/21 16:52:50 - [UTCD-INFO] Pop-up Window(s) Found: 0
2008/05/21 16:52:50 - [UTCD-INFO] Analyzing tracer log... (766,680 bytes)
2008/05/21 16:52:50 - [UTCD-INFO] Time elapsed 0.0320420265198 second
2008/05/21 16:52:50 - [UTCD-INFO] Exploited web browser: Internet Explorer
2008/05/21 16:52:50 - [UTCD-INFO] Suspicious folder creation count: 0
2008/05/21 16:52:50 - [UTCD-INFO] Suspicious file creation count: 4
2008/05/21 16:52:50 - [UTCD-INFO] Suspicious registry key creation count: 1
2008/05/21 16:52:50 - [UTCD-INFO] Suspicious process creation count: 5
2008/05/21 16:52:50 - [UTCD-INFO] Threat percentage: 100%
2008/05/21 16:52:50 - [UTCD-INFO] Conclusion: Malicious

What is the malware most likely trying to do?

[CLUE] <C:\> net start…
Example 4: Website with drive-by download
Analysis was done in a VMware image with fully patched Windows XP Professional SP2 and latest version of web browsers

This website does not contain any zero-day exploit. So, how did our honey client get exploited?
Adobe Flash Player is the standard for delivering high-impact, rich Web content. Designs, animation, and application user interfaces are deployed immediately across all browsers and platforms, attracting and engaging users with a rich Web experience.

The table below contains the latest Flash Player version information. Adobe recommends that all Flash Player users upgrade to the most recent version of the player through the Player Download Center to take advantage of security updates.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Browser</th>
<th>Player version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>Internet Explorer (and other browsers)</td>
<td>8.0.124.0</td>
</tr>
</tbody>
</table>

You have version 8.0.115.0 installed.
Two-factor authentication in a nutshell

Article: http://www.finextra.com/fullstory.asp?id=15169

HSBC to issue Vasco authentication tokens to UK business customers

HSBC is rolling out Vasco’s two-factor digital authentication tokens to provide business customers in the UK with secure access to Internet banking services.

The bank will begin issuing the keyring-sized access code devices free of charge to its 180,000 Internet business banking customers in the UK from May. The device generates a single use security code which customers use alongside their user ID and password when making online banking transactions.

The bank says the Vasco device will replace the existing authentication system which is based on digital certificates. As soon as a customer activates the security device, their digital certificates will no longer be required.

HSBC says the device offers “a significant additional line of defence” against online fraud such as phishing, keylogger trojans, remote hacking and screen capturing.

The bank has already issued Vasco devices to customers in Brazil and Hong Kong. Simon Wainwright, head of business banking at HSBC, says: “Our experience in other parts of the world shows that this kind of two factor authentication is an extremely useful weapon in the fight against Internet crime.”

UK bank Alliance & Leicester has launched its own two-factor authentication service, which is based on the PassMark system.

Lloyds TSB has also conducted trials of a Vasco two-factor authentication device. But although the trial was a success the UK bank has no plans for a large-scale roll-out of the technology and is instead waiting for guidance from Apacs on plans for an industry standard card-reading system.

Apacs said in April last year that UK banks were close to agreeing a common industry standard for two-factor authentication of online transactions and banks were expected to begin distributing the authentication devices to customers within the year, but as yet no system has been introduced.

It was thought the standard would be based on a technical specification developed by Visa and MasterCard which would be adapted for domestic use, in the same way that the Chip and PIN standard was adapted.
How does two-factor authentication works?

Source: http://www.mocomystems.com/Information/RSA.htm
Two-factor authentication ripped by phishers

Phishing attack evades bank’s two-factor authentication

By OUT-LAW.COM
Published Thursday 19th April 2007 09:13 GMT

A two-factor authentication system operated by Dutch bank ABN Amro has been compromised and money stolen from the online accounts of customers who fell for a phishing scam.

Two-factor authentication for online banking usually involves passwords and tokens which provide synchronised, constantly changing numbers to use as additional evidence of identity.

The security industry has promoted the tokens as a preventative measure against hacking for users of remote corporate or banking systems. However, experts have warned that they are still vulnerable to phishing attacks, where fraudulent emails lure recipients to bogus websites that are set up to gather security details.

Four customers who used two-factor authentication have been compensated by ABN Amro for undisclosed amounts taken from their bank accounts.

"We are taking this incident very seriously and, in addition to informing our clients, are also implementing all of the technical measures that are at our disposal to stop criminals in their tracks," said Johan van Hall of ABN Amro Netherlands. "Safe usage of home and office computers is an essential requirement for secure online banking, and we plan to remind our clients even more frequently and urgently than before of that fact."

Hackers sent the customers emails falsely claiming to be from ABN Amro. If recipients opened an attachment, software was installed on their machines without their knowledge. When customers visited their banking site, the software redirected them to a hacker-controlled mock site that requested their security details.

As soon as the hackers received these details they were able to log into a customer’s account at the real ABN Amro site, before the expiry of the fob-generated number. They could then transfer the customer’s money.

Security experts have warned that such "man in the middle" attacks cannot be prevented by security tokens.

At the E-Crime Congress in London last month, several experts spoke out about the limitations of the systems. "Even when all the banks have it [hackers] will still attack them," said Mikko Hypponen, chief research officer of security firm F-Secure, at the Congress. "We see them using 'man in the middle' already."

Phishers rip into two-factor authentication

By John Leyden
Published Thursday 13th July 2006 15:06 GMT

Phishers are seeking to circumvent two-factor authentication schemes using man-in-the-middle attacks. Last October, US federal regulators urged banks to adopt two-factor authentication as a means to combat the growing problem of online account fraud.

Two-factor authentication involves the use of a password-generating device along with conventional passwords. That means a thief must know more than just a password to gain access to a user’s account. Although the technology helps guard against fraud, a recent attack against Citibank shows the technique is far from foolproof.

A bogus security warning ostensibly from Citibank, and targeting customers of its Citibusiness service, urged prospective marks to visit a website and enter not only their account details and password (as with conventional phishing scams) but also the code generated by the customer’s token. These authentication key codes change every minute or so.

The fraudulent site is automated so it uses this information to log onto the real Citibusiness login site, allowing fraudsters access to compromised accounts. The site, based in Russia, operated last week but has since been shut down, the Washington Post reports (http://blog.washingtonpost.com/securityfx/2006/07/citibank_phish_spoofs_2factor_1.html).

The attack confirms concerns (http://www.schneier.com/crypto-gram-0503.html#2) from security expert Bruce Schneier that two-factor authentication schemes have been oversold as a silver-bullet solution to online identity fraud.

Banks in the Netherlands and Scandinavia have used two-factor authentication for years, and the technology is widely credited with helping to make account fraud more difficult. But the Citibank attack shows the growing sophistication of fraudsters, and undermines any notion that this approach delivers complete protection. ©
1. Victim logs in to the fake banking website using their username, password and one-time-use security token generated from security device provided by bank.

2. The attacker uses the login information entered by victim at the fake banking website to login to the real banking website.

3. To maintain access of the authenticated session, the attacker writes an automation script to let make his server reload the real website or randomly click on main links at the website.

Note:
The technique used in step 3 employs ‘local session riding’ at the attacker’s server to forge request on behalf of the victim to the real banking site.
1. The attacker retrieves information from the real banking website and stores them to the simulated fake banking website database.

Note:
The automation script written by the attacker will keep running at the simulated fake banking website to maintain the authenticated session with the real banking website.
In online banking systems protected with 2-factor authentication, a security token is required from the user for each transaction to be performed.

Whenever the victim enters a security token to perform transaction, the attacker uses the security token entered at the fake website to perform fund transfer from the victim’s banking account to their money mule’s account.

Note: The automation script written by the attacker will keep running at the simulated fake banking website to maintain the authenticated session with the real banking website.
Transferring all money out from a banking account preset with daily transaction limit

- Since the attacker’s automation script is running, the authenticated session can be maintained from a few hours up to a few days depending the design of the web application and frequency of server maintenance or reboot

- If the victim’s banking account is preset with daily transaction limit, then the attacker might perform several transactions repeatedly in different days to steal all the money

<table>
<thead>
<tr>
<th>Day</th>
<th>Account Balance</th>
<th>Daily Transfer Limit</th>
<th>Description</th>
<th>Security Token</th>
</tr>
</thead>
<tbody>
<tr>
<td>Day 1</td>
<td>- $20,000</td>
<td>$20,000</td>
<td>(Victim pays electricity bill)</td>
<td>- 1</td>
</tr>
<tr>
<td>Day 2</td>
<td>- $20,000</td>
<td>$20,000</td>
<td>(Victim performs fund transfer for business)</td>
<td>- 1</td>
</tr>
<tr>
<td>Day 2</td>
<td>- $20,000</td>
<td>$20,000</td>
<td>(Victim pays mobile phone bill)</td>
<td>- 1</td>
</tr>
<tr>
<td>Day 3</td>
<td>- $20,000</td>
<td>$20,000</td>
<td>(Victim login just to check balance)</td>
<td>- 1</td>
</tr>
</tbody>
</table>

Account Balance : $0
Daily Transfer Limit : $20,000
The ‘Local Session Riding’ (LSR) attack

Why such attack is possible?

- More than 90% of the web applications (including online banking sites) were designed in a way that will reset their cookie/session timeout counter whenever there is user activity.

- When attackers employ MITM together this method to online banking sites, they are able to maintain the session for a very long time (hours, days, weeks or even months!)

- Logic flaw or convenience feature? You decide 😊

How to reduce the chances of LSR attack?

- Financial related web applications must be designed in a way that users are only allowed to perform transaction in a fixed amount of time in each login. NEVER RESET THE SESSION TIMEOUT VALUE!
Existing phishing identification techniques

- Domain name age checking
- Registrar information from WHOIS
- Hostname resolved IP address (comparison with real site)
- Suspicious IFRAME with tiny width and height
- Suspicious URL or encodings used in URL
- Similar HTML / Javascript source with legitimate website
- SSL certificate validation
**Blacklisting - Identify the bad sites with blacklisted URL database**

- Receive phishing reports from public (Eg. PhishTank)
- Automated crawler to find suspicious domain names and websites
- Exchange phishing URLs with security vendor partners
- Block blacklisted URLs with tools installed on client machine
Disadvantages of blacklisting approach

• Unable to identify unreported phishing websites in the wild
• Client side has to keep updated with latest blacklisted URL DB
• Efficiency issue as the amount of blacklisted URL grows
How can we improve it better?

Whitelisting approach

1. Identify the visual similarity of rendered website with legitimate website
2. Check target web server/site characteristics for identification **(WEBSITE FINGERPRINTING!)**
3. Check target URL’s domain name age
4. Check target URL’s similarity with legitimate URL and suspicious encoding
5. Check target website’s content for suspicious characteristics
6. Compare the data obtained from Step 2-5 with the pre-analyzed information of original banking/financial website
Website Finger Printing... Uhmm...

- Collect information about target web server / site
- Get geolocation of target website from IP address
- Nmap does OS fingerprinting from TCP/IP stack characteristics, we do it from HTTP response characteristics
- Collect information about original web server / site as well
- Get geolocation of the real website from IP address
- Now what? Compare!

When any of the server or website characteristics such server type, server version, server date / time, last modified date, etc. mismatch, it smells...

PHISHY!
Identifying visual similarity of a website

Simple approach to create signature for web appearance

1. Take screenshot image of a rendered website
2. Calculate the mean values for red, green and blue of the image
3. Use the RGB mean values as ‘website appearance signature’

paypal.png - Screenshot of the real PayPal website

messed.png – Messed up image modified from paypal.png

Red: 226.26349166666665
Green: 232.64016333333333
Blue: 236.67534166666667

Red: 226.26936333333333
Green: 232.64310833333334
Blue: 236.67663166666668

[MEAN VALUES]  [MEAN VALUES]
Identifying visual similarity of a website

fake.png – Screenshot of fake PayPal website [with contrast and brightness level purposely tweaked]

2checkout.png – Screenshot of the real 2Checkout.com website


[MEAN VALUES] Red: 207.40960000000001 Green: 220.19798166666666 Blue: 213.34901500000001
Identifying visual similarity of a website

r1 – Red color mean value of image-1,
g1 – Green color mean value of image-1,
b1 – Blue color mean value of image-1,

r2 – Red color mean value of image-2,
g2 – Green color mean value of image-2,
b2 – Blue color mean value of image-2

\[
\begin{align*}
\text{rDiff} &= \frac{\left| (r_1 - r_2) \right|}{256} \\
\text{gDiff} &= \frac{\left| (g_1 - g_2) \right|}{256} \\
\text{bDiff} &= \frac{\left| (b_1 - b_2) \right|}{256} \\
\end{align*}
\]

Therefore,

\[
100 - ((\text{rDiff} + \text{gDiff} + \text{bDiff}) \times 100) = \% \text{ of similarity}
\]

Example calculation:

**Difference of paypal.png and messed.png**

\[
\begin{align*}
\text{rDiff} &= \frac{\left| (226.26349166666665 - 226.26936333333333) \right|}{256} = 0.00002293619791671875 \\
\text{gDiff} &= \frac{\left| (232.64016333333333 - 232.64108333333334) \right|}{256} = 0.0000115039062500390625 \\
\text{bDiff} &= \frac{\left| (236.67534166666667 - 236.67663166666668) \right|}{256} = 0.0000050390625000390625 \\
100 - (0.000039479166666796875 \times 100) &= 99.9960520833333203125 \% \text{ similar}
\end{align*}
\]

**Difference of paypal.png and fake.png**

\[
\begin{align*}
\text{rDiff} &= \frac{\left| (226.26349166666665 - 225.603835) \right|}{256} = 0.0025767838541666015625 \\
\text{gDiff} &= \frac{\left| (232.64016333333333 - 231.98625166666667) \right|}{256} = 0.002554342447916640625 \\
\text{bDiff} &= \frac{\left| (236.67534166666667 - 236.01825500000001) \right|}{256} = 0.002566744791666640625 \\
100 - (0.0076978710937498828125 \times 100) &= 99.23021289062501171875 \% \text{ similar}
\end{align*}
\]

**Difference of paypal.png and 2checkout.png**

\[
\begin{align*}
\text{rDiff} &= \frac{\left| (226.26349166666665 - 207.40960000000001) \right|}{256} = 0.0736480143229165625 \\
\text{gDiff} &= \frac{\left| (232.64016333333333 - 220.19798166666666) \right|}{256} = 0.0486022721354166796875 \\
\text{bDiff} &= \frac{\left| (236.67534166666667 - 213.34901500000001) \right|}{256} = 0.09111846354166640625 \\
100 - (0.213368749999998828125 \times 100) &= 78.6631250000001171875 \% \text{ similar}
\end{align*}
\]
Example of a basic anti-phishing system

**Score-based Algorithm**
- Appearance similar to legitimate website but hostname/IP address mismatch?
- Domain name age younger than 6 months or a year?
- URL contains unusual encoding?
- Hostname or IP address used in URL?
- HTML source contains IFRAME?
- Website fingerprint matches legitimate site?
- Valid certificate signed by trusted CA?

**Website Reputation Analysis Engine**

**Database containing information of legitimate financial / banking related websites [e.g. Signatures, URL, domain name age, etc.]**

Send website information such as URL, appearance signature, local analysis result on HTML source, certificate validity status etc.

**Web Browser Plugin / Tool installed to help user verify website before performing online transaction / banking**

1. Capture the screenshot of webpage when loading completed
2. Calculate the pixel color mean values to be used as signature
3. Submit the URL and signature to server for analysis of website reputation
4. Show the user analysis result from server to know whether the loaded website is legitimate
Advantages of ‘web appearance signature’

- Easier to obtain signatures of legitimate sites
- Able to detect unknown or “zero-day” phishing websites