Phish Feeding: An Active Response to Phishing Campaigns

John Brozycki, CISSP

What is phish feeding?

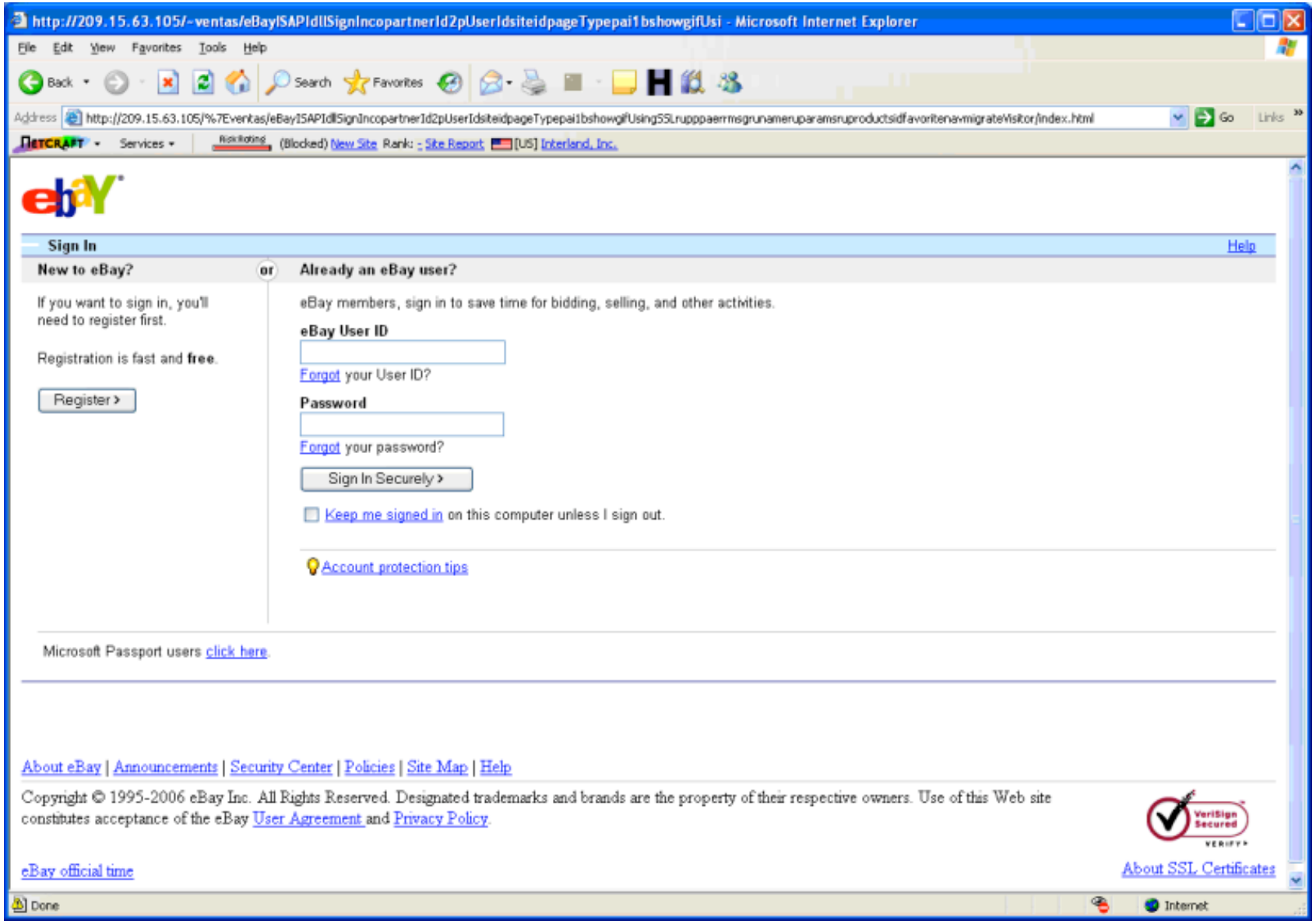
The process, generally automated, of submitting fake but realistic data to a phishing site.

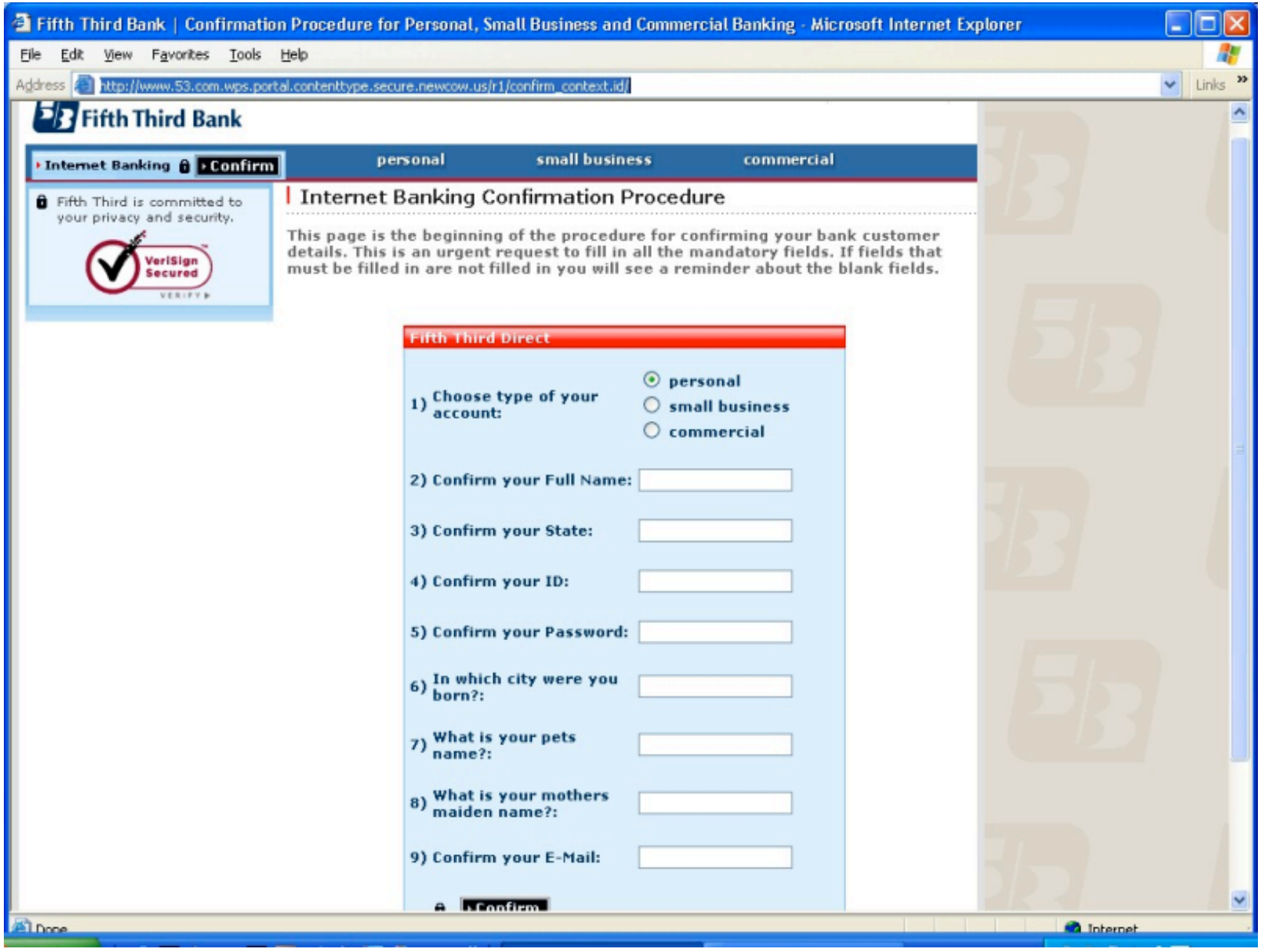
What we'll cover…

- How does a typical phish work?
- How much damage does phishing cause to target institutions?
- How do victim institutions respond today?
- How can phish feeding reduce the damage?
- How do you know if phish feeding is actually working?
- What is involved in implementing a phish feeding program?
- What can go wrong in phish feeding?
- Where is phishing headed in the future?

How does a typical phish work?

- Web server compromised or fraudulently set up.
- Spam email list is purchased or created.
- The phish email is sent to the spam list.
- Recipients that do have accounts and believe the email is real go to the fraudulent site.
- Account info is entered and then emailed, stored locally, or submitted through a remote form.
- Phishers exploit or sell the information.


http://209.15.63.105/~ventas/eBayISAPIdllSignIncopartnerId2pUserIdsiteidpageTypepai1bshowgifUsi - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://209.15.63.105/%7Eventas/eBayISAPIdllSignIncopartnerId2pUserIdsiteidpageTypepai1bshowgifUsingSSLrupppaerrmsgrunameruparamsruproductsidfavoritenavmigrateVisitor/index.html
Go Links
Services
(Blocked) New Site Rank: - Site Report [US] Interland, Inc.
Sign In
Help
New to eBay?
or
Already an eBay user?
If you want to sign in, you'll need to register first.
Registration is fast and free.
Register >
eBay members, sign in to save time for bidding, selling, and other activities.
eBay User ID
Forgot your User ID?
Password
Forgot your password?
Sign In Securely >
Keep me signed in on this computer unless I sign out.
Account protection tips
Microsoft Passport users click here.
About eBay | Announcements | Security Center | Policies | Site Map | Help
Copyright © 1995-2006 eBay Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this Web site constitutes acceptance of the eBay User Agreement and Privacy Policy.
VeriSign Secured
VERIFY
eBay official time
About SSL Certificates
Done
Internet


Fifth Third Bank | Confirmation Procedure for Personal, Small Business and Commercial Banking - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://www.53.com.wps.portal.contenttype.secure.newcow.us/r1/confirm_context.id/
Links
Fifth Third Bank
Internet Banking Confirm
personal
small business
commercial
Fifth Third is committed to your privacy and security.
VeriSign Secured
VERIFY
Internet Banking Confirmation Procedure
This page is the beginning of the procedure for confirming your bank customer details. This is an urgent request to fill in all the mandatory fields. If fields that must be filled in are not filled in you will see a reminder about the blank fields.
Fifth Third Direct
1) Choose type of your account:
personal
small business
commercial
2) Confirm your Full Name:
3) Confirm your State:
4) Confirm your ID:
5) Confirm your Password:
6) In which city were you born?:
7) What is your pets name?:
8) What is your mothers maiden name?:
9) Confirm your E-Mail:
Confirm
Done
Internet

How much damage does phishing cause to target institutions?

- Confidence.
  *"Is this real?" * "Why did you send this to me?" * "This is the third time I've received this. If you don't stop I'm closing my accounts."*
- Resources.
  Significant manpower; Call Center, Help Desk, IT and Security, Administration, PR/Marketing, etc.
- Money.
  Institutions that carry card products absorb almost all of the financial losses. They may also need to retain services of security vendor for site take downs, add staff, pay overtime, etc.

How do victim institutions respond today?

- Level 0: Do nothing/unaware
- Level 1: Notification (i.e.:website/phone msg)
- Level 2: Get the site taken down

----------(most have yet to cross this line)----------

- Level 3: Work with Law Enforcement
- Level 4: Forensics and analysis of phishing sites

- Level 5: Active response

How can phish feeding reduce the damage?

- Reduce the value of the data if the phishers plan to sell it by diluting real responses with realistic fake ones.
- Provide additional time for customers to realize that they've been phished and contact the institution so accounts may be blocked before being exploited. (Credit cards have been exploited at ATM machines less than 15 minutes after the customer entered the information in the phish website.)
- Provide fake values that the targeted institution may be able to monitor to track malicious access to financial websites and potentially obtain their source IP addresses.
- Frustrate the phishers so that they may move on to easier targets.
- Create a reputation of being difficult to phish so that phishing groups will not try to phish you again and new groups may avoid you.

How do you know if phish feeding is actually working?

- Track your fake account numbers and check for access attempts.
- Phishing groups stop “double dipping*” your institution.
- Phishing decreases over time.
- Losses decrease per phish.
- Word circulates, i.e.: via IRC.

*Some phishing groups hit institutions twice, especially if the first time resulted in a poor yield. I say this from experience!

What is involved in implementing a phish feeding program?

- Approval from management, client, etc.
- Consult legal team.
- Resources to implement. (People, money, time)
- Development/refinement of skills and techniques. (May not have in house. Will likely take some time to develop.)

What are the components in a phish feeding program?

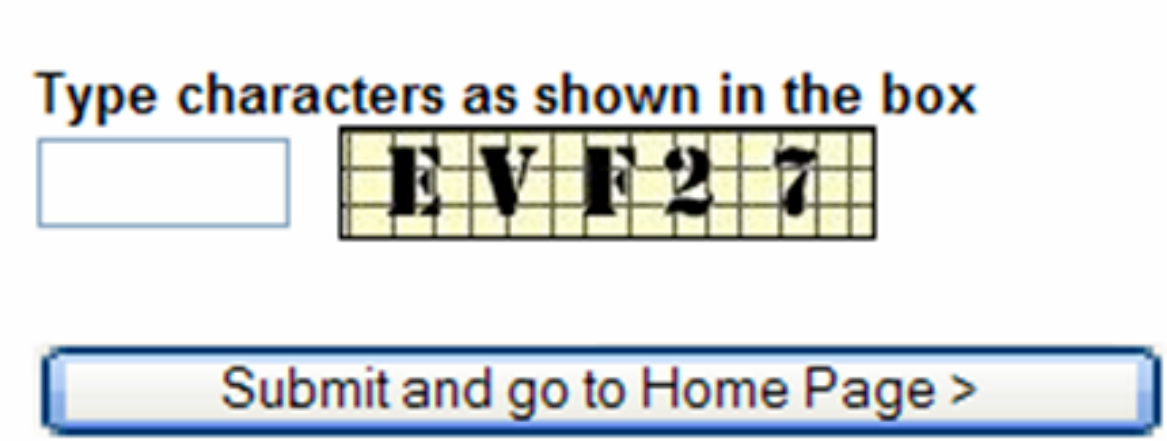
- System/software to make templates to feed the forms of live phish site.
- Creation of data sets that match the phish site's form and appear valid.
- Anonymous proxy system which alters the final source IP to make the feeds appear to be coming from different IP addresses.
- Monitoring and tracking mechanisms.

What can go wrong in phish feeding?

- Poor data or technique result in a wasted effort.
  (Phisher can spot your feeds and filters them.)
- Overdone effort causes Denial of Service.
  (YOU become the malicious hacker to innocent sites also hosted on compromised phish server. Possible legal problems if someone can prove you initiated a DoS.)
- Retribution against your institution.
  (Remember Blue Security?)
- Phish that's difficult/impossible to feed
  (Turing numbers, flash content, randomly changing forms, verification against real account data, etc.)

Where is phishing headed in the future? (Anti phish feeding)

- In September 2006, an eBay phish utilized a Turing number, perhaps to thwart attempts at automated entry.

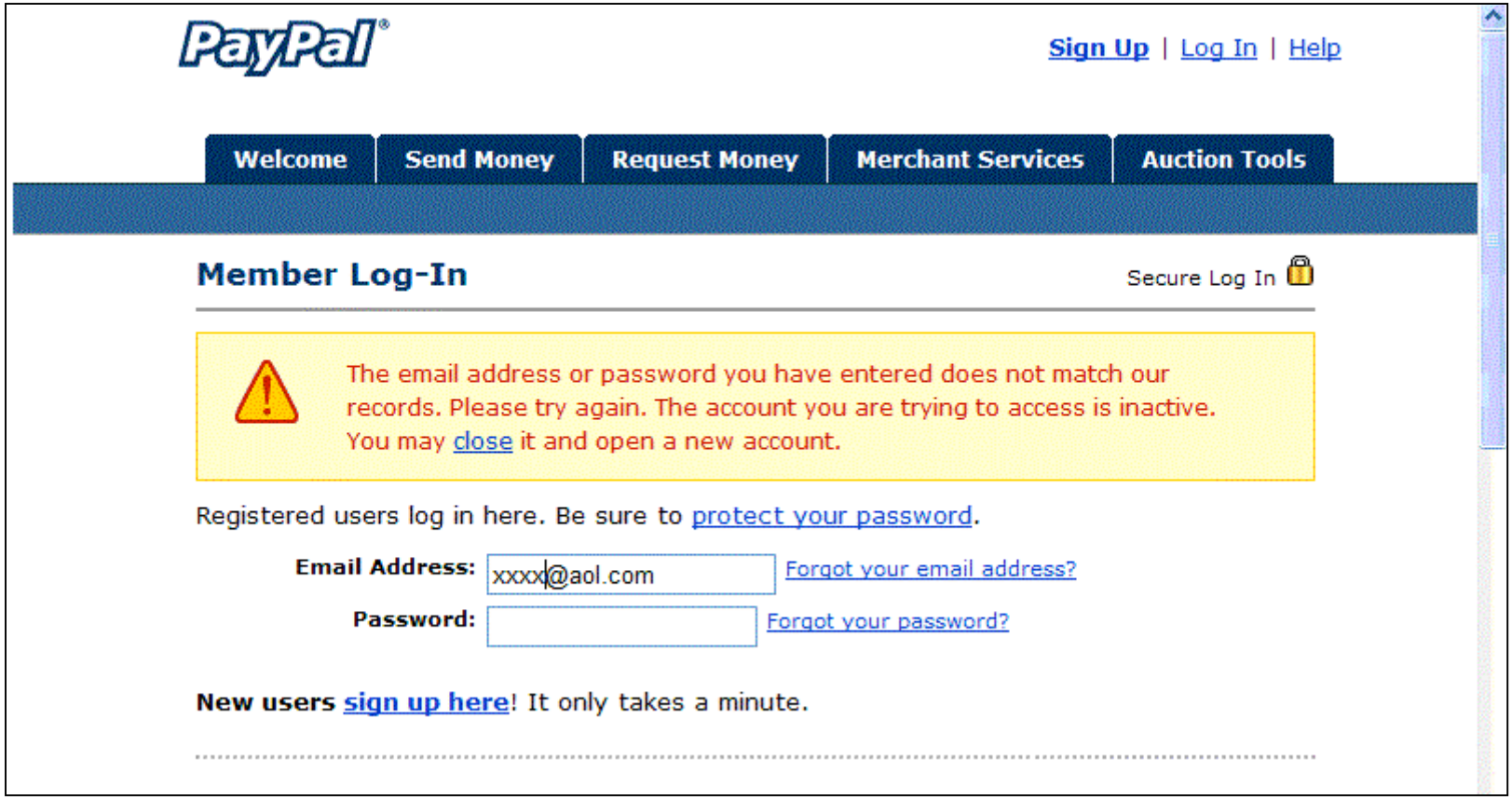


eBay phish Turing implementation

- 20 static images with static names.
- Randomly selected.
- Scriptable through image recognition library or name check in html source.
  Could be phish fed!

A PayPal phish (Sept. 2006)

acts as a “man in the middle” and verifies the account before letting you proceed.



Where is phishing headed in the future?

- Spear phishing based on compromise of an online system you make a purchase on.

- Phish that cannot be taken down in a reasonable amount of time.

Spear Phish example:

(Names changed, but based on an actual phish for an online food company that was compromised.)

To: Jane Doe

From: Foobarfoods.com

Subject: Your FoobarFoods order information!

Dear Jane,

We recently tried to charge your credit card for your FoobarFoods.com order (order #12857) and it was rejected by the bank because it has not complete information.

To update the credit card information details for your order, please select this link:

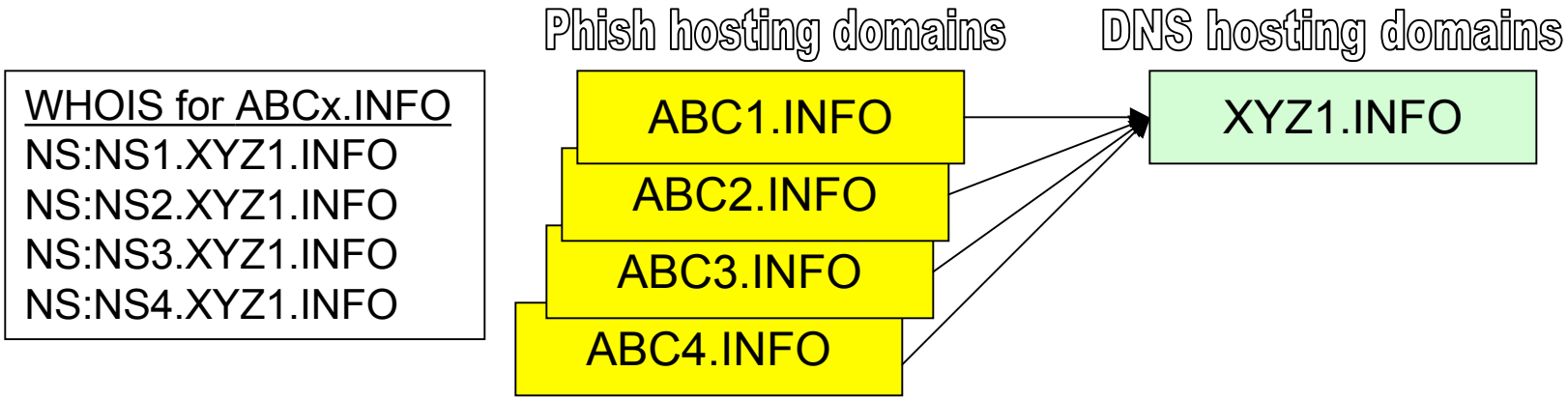
http://foobarfoodss.com/veri.php?orderid=12587&zip=12601

If you received this mail once and update it onece .Please ignore this mail .

Thanks!

FoobarFoods.com

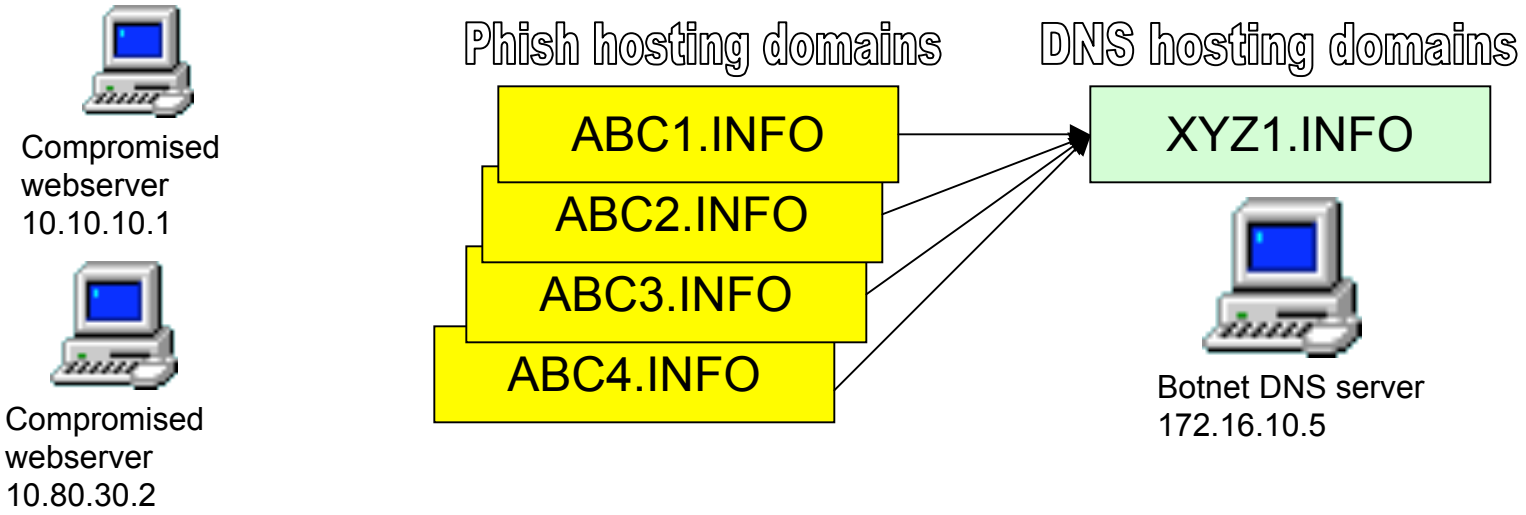
Building a phish that's extremely difficult to take down



Fraudulently registered domains are set up. One fraudulent domain is used for DNS resolution. Multiple versions of the phish are sent out referencing the different domains. Each domain utilizes multiple servers, dynamically maintained by the DNS domain. Phish servers can be quickly added if any are lost.

NOTE: domains are sequentially named here for clarity, but random names are used by the phishers.

Building a phish that can't be readily taken down (2)

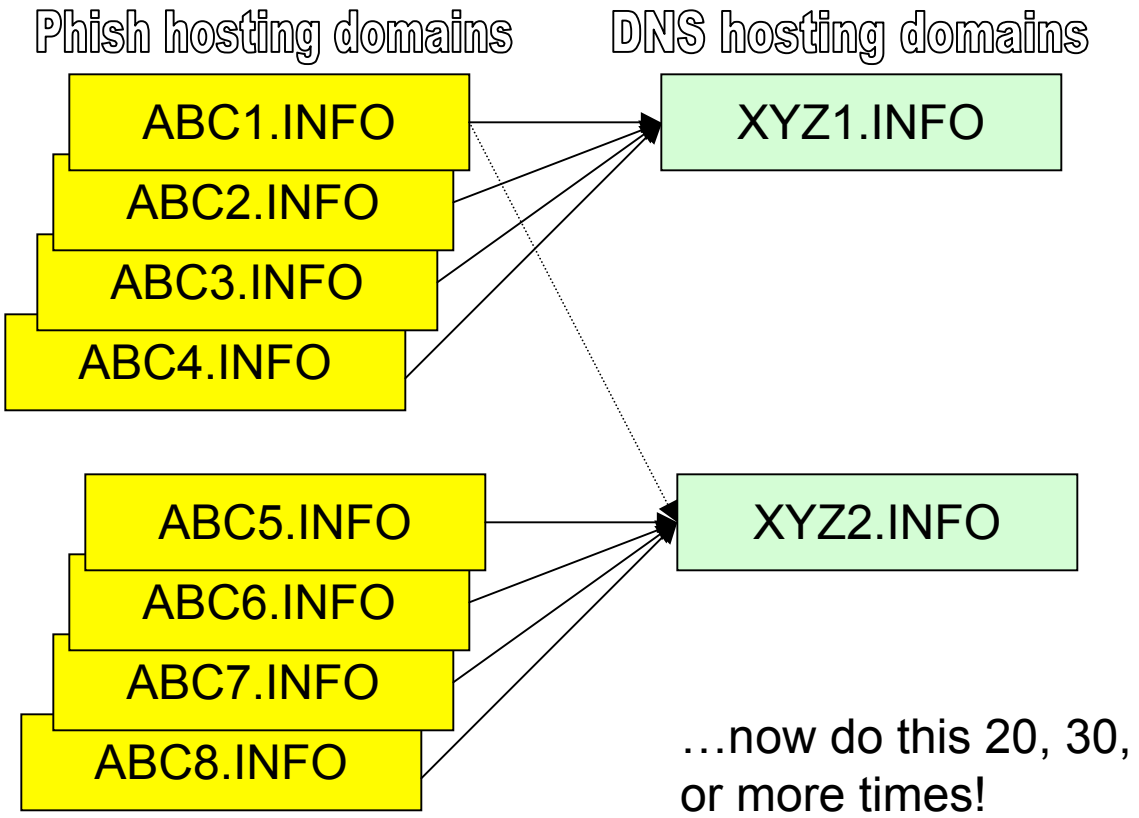


A compromised "webserver" with physical address 10.10.10.1 hosts a copy of the phish, as does server at 10.80.30.2.

A puppet DNS server resolves phish.abc1.info, phish.abc2.info, etc. to 10.10.10.1 **and** 10.80.30.2.

If a server goes down, a new one is added and the puppet DNS updates accordingly. (Where is the Achilles Heel in this setup? DNS!)

Building a phish that can't be readily taken down (3)



Thank you!

Questions?

For questions or a copy of my paper on Phish Feeding, email:

phishfeeder@trueinsecurity.com