

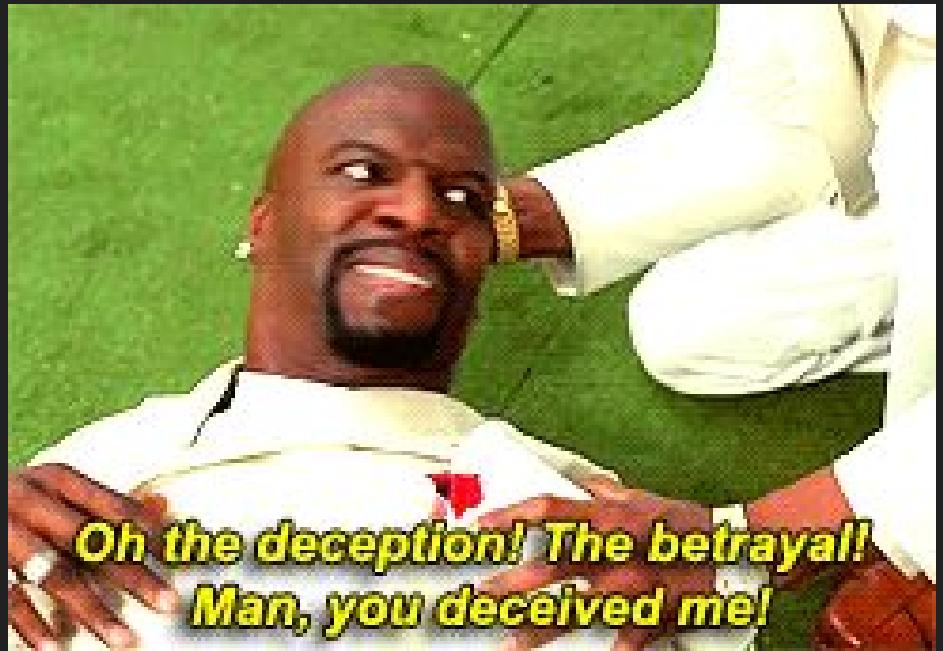
Advanced Social Engineering for Red Teams

By Hunter Hardman @t3ntman



About Me

- Security consultant at Mandiant
- Former blue teamer turned red
- Extreme passionate about social engineering ;)
- Trash tier Overwatch player



Talk Agenda

- Campaign Purpose
- Open Source Intelligence (OSINT) Gathering and Choosing Targets
- Domain Registration and Strategies
- Defeating Web Proxies and Email Protections
- Payloads (Old School vs New School)
- Email and Phone Delivery / Tracking
- Successful Campaigns



Campaign Purpose

Campaign Purpose

- What is the goal of your campaign?
 - Credential harvesting?
 - Payload execution?
 - Maybe both?
- Determine this before you do anything!



Open Source Intelligence (OSINT) Gathering

..But First a Disclaimer!

WARNING: All information in this section has been redacted to avoid a “shit storm” with various legal departments.

OSINT Gathering

- Bad OSINT = Bad SE Campaign (likely)
- Goals
 - Email harvesting for potential targets
 - Employees, # of employees (big corporation vs start-up), email schema, job titles, phone numbers, departments, etc.
 - Technologies in place

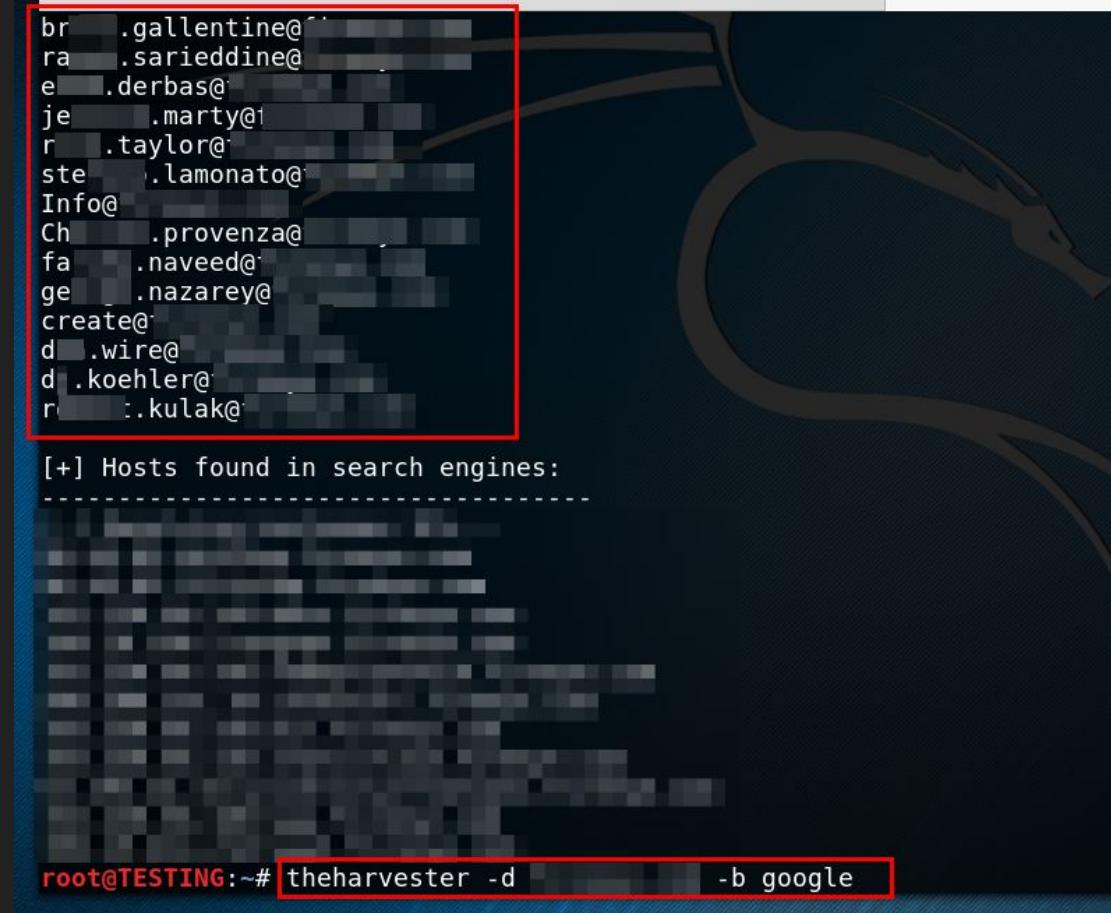


OSINT Gathering - Email Harvesting

- theHarvester (<https://github.com/laramies/theHarvester>)
 - Limited to 100 results per LinkedIn's API
- www.data.com (now Salesforce)
 - This will cost you (\$\$\$)
 - Great for phone number harvesting
- Manual harvesting (via LinkedIn browsing)

OSINT Gathering - Email Harvesting (theHarvester)

- Get email schema
- **Command:** theharvester -d <DOMAIN> -b google



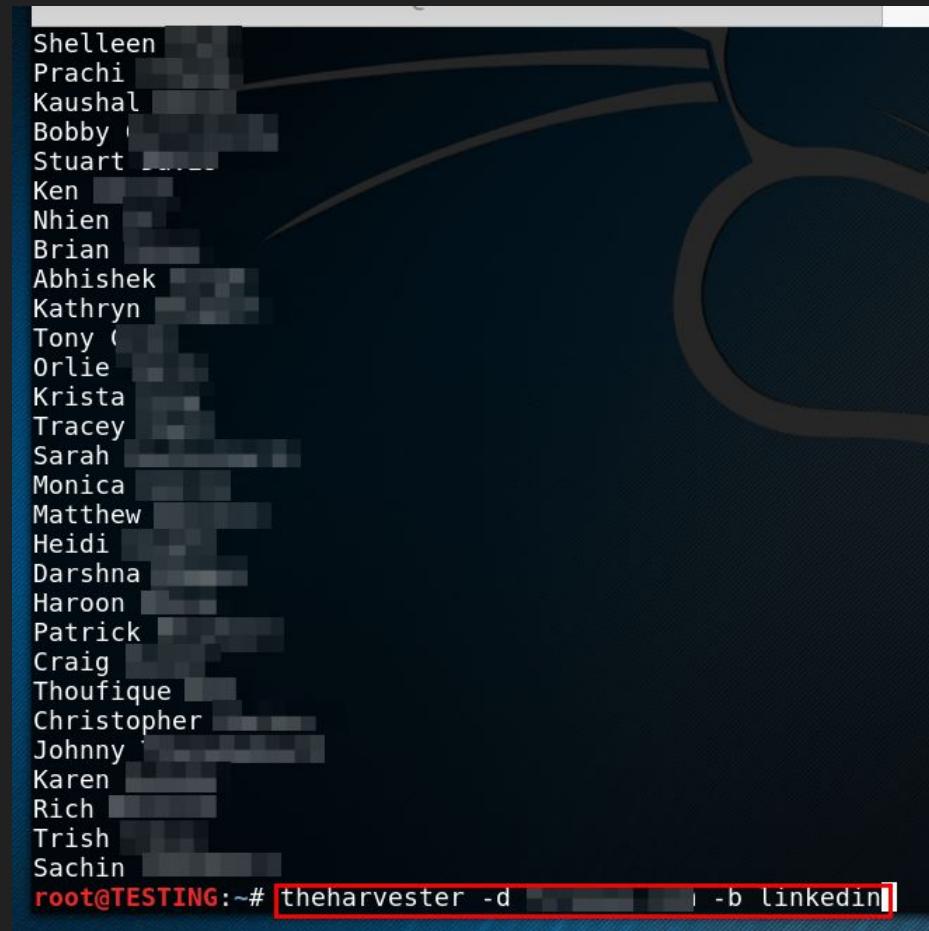
```
br .gallentine@[REDACTED]
ra .sarieddine@[REDACTED]
e .derbas@[REDACTED]
je .marty@[REDACTED]
r .taylor@[REDACTED]
ste .lamonato@[REDACTED]
Info@[REDACTED]
Ch .provenza@[REDACTED]
fa .naveed@[REDACTED]
ge .nazarey@[REDACTED]
create@[REDACTED]
d .wire@[REDACTED]
d .koehler@[REDACTED]
r .kulak@[REDACTED]

[+] Hosts found in search engines:
-----  
[REDACTED]
```

root@TESTING:~# theharvester -d [REDACTED] -b google

OSINT Gathering - Email Harvesting (theHarvester)

- Get LinkedIn employees and convert to email addresses
- **Command:** theharvester -d <DOMAIN> -b linkedin



```
Shelleen  
Prachi  
Kaushal  
Bobby  
Stuart  
Ken  
Nhien  
Brian  
Abhishek  
Kathryn  
Tony  
Orlie  
Krista  
Tracey  
Sarah  
Monica  
Matthew  
Heidi  
Darshna  
Haroon  
Patrick  
Craig  
Thoufique  
Christopher  
Johnny  
Karen  
Rich  
Trish  
Sachin  
root@TESTING:~# theharvester -d [REDACTED] -b linkedin [REDACTED]
```

OSINT Gathering - Email Harvesting (Manually)

WARNING: Create a fake LinkedIn account or upgrade your account to “Premium”

Profile viewing options

Choose whether you're visible or viewing in private mode

Select what others see when you've viewed their profile

Close

Private mode

Your name and headline

 Hunter Hardman
Security Consultant at Mandiant
Denver, Colorado | Information Technology and Services

Private profile characteristics

 Information Security Specialist at Mandiant

Private mode

 Anonymous LinkedIn Member

OSINT Gathering - Email Harvesting (Manually)

- Who's actually viewed your profile?

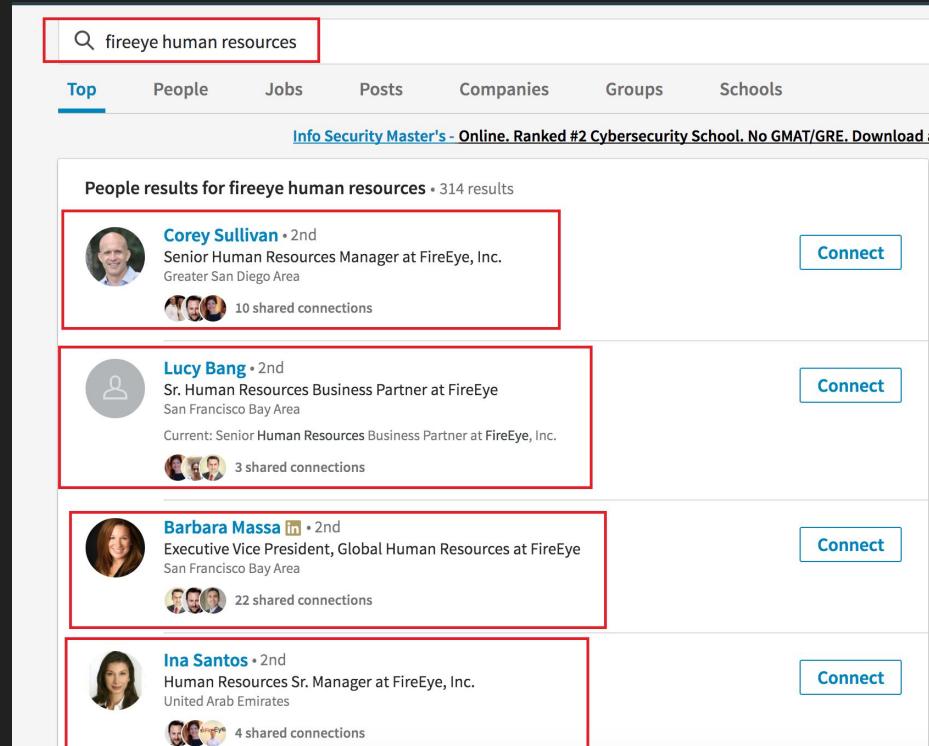
PREMIUM

Who your viewers are

 70 profile viewers in the past 90 days +333% since last week	 Senior Executive Recruiter 16h
 1 works at Bugcrowd Inc	 Data Analyst at SNS Information Management Services InMail
 2 work at FireEye, Inc.	 **HIRING PENTESTERS! - Twin Cities & Nationwide** - (details in summary)- 713.574.6383-travis.englishbey@oscar-tech.com 1d
 1 works at vsource.io	 looking for InMail 2d

OSINT Gathering - Email Harvesting (Manually)

- LinkedIn manual querying for departments is extremely useful
 - “Give me all the people that work for <COMPANY> in the Human Resources department”
- We already know the email schema and no manual querying restrictions



A screenshot of a LinkedIn search results page. The search bar at the top contains the query "fireeye human resources". Below the search bar, there are tabs for Top, People, Jobs, Posts, Companies, Groups, and Schools. The "People" tab is selected. A banner at the top of the results section reads "Info Security Master's - Online. Ranked #2 Cybersecurity School. No GMAT/GRE. Download a". The results section is titled "People results for fireeye human resources • 314 results". It displays four profiles, each with a red border around the card:

- Corey Sullivan** • 2nd
Senior Human Resources Manager at FireEye, Inc.
Greater San Diego Area
10 shared connections [Connect](#)
- Lucy Bang** • 2nd
Sr. Human Resources Business Partner at FireEye
San Francisco Bay Area
Current: Senior Human Resources Business Partner at FireEye, Inc.
3 shared connections [Connect](#)
- Barbara Massa** [in](#) • 2nd
Executive Vice President, Global Human Resources at FireEye
San Francisco Bay Area
22 shared connections [Connect](#)
- Ina Santos** • 2nd
Human Resources Sr. Manager at FireEye, Inc.
United Arab Emirates
4 shared connections [Connect](#)

OSINT Gathering - Technology Enumeration

- Lots of good information in job postings ;)
 - dice.com
 - glassdoor.com
 - linkedin.com
 - indeed.com

Required Skills/Experience

- 7+ years of overall IT experience with a proven background in network and security engineering.
- Strong understanding of enterprise security management practices including incident response, security operations casework, forensic analysis, intelligence gathering, and malware analysis
- Strong experience with enterprise networks, routing, and switching
- Detailed knowledge of transport (TCP/UDP) and application layer (HTTP, FTP, etc.) protocols
- Understanding of email protocols from operational and functional perspectives
- Understanding of streaming media applications (e.g. SIP, RTP, etc.)
- Experience with **Intrusion Detection Systems (IDS)**
- Ability to create custom SNORT/Suricata rules
- Experience with static/dynamic content analysis (e.g. FireEye, Cisco ThreatGrid, Bluecoat MAA, etc.)
- Experience with full packet capture/analysis systems (e.g. RSA Security Analytics, NetWitness, FireEye PX/IA, Bluecoat Security Analytics, Solera, etc.) and host FPC
- Experience using enterprise search tools (ie., Splunk, LogRhythm, Elk, Logstash, Sumologic, etc.)
- Experience with all current enterprise operating systems (Linux, Windows)
- Experience with scripting languages such as; Perl, Python, PHP, Bash, or PowerShell
- Detailed knowledge of HTTP/HTTPS and web proxies
- Experience utilizing - or working knowledge of - network tools such as:
 - Cisco routers and switches
 - F5 load balancers
 - Bluecoat SG
 - Gigamon/cPacket switches
 - Cisco/Checkpoint firewalls
 - tcpdump, Wireshark, or similar

OSINT Gathering - Phone Numbers

- Contact their main phone line
 - Maybe the secretary will give you a target's extension
 - People generally want to help one another
 - What about a phone directory system? ;)
 - Can also give you clues to name pronunciation



Choosing Targets

Choosing Targets (Personal Preference)

- Lots of psychological factors (won't go too much into detail)
 - Age
 - Location
 - Remote
 - Work Department
 - HR
 - Marketing

Domain Registration and Strategies

Domain Registration and Strategies

- DNS squatting
 - www.gooogle.com
 - www.ffacebook.com
- *.education domains
 - For targeting schools/institutions, but also works for “employee training” campaigns ;)
 - **Note:** These are not the same as *.edu domains! (need to be institution)
- Company/client-specific domain vs generic domains
 - **Specific:** www.<CLIENT>-browserchecker.com
 - **Generic:** <CLIENT>.browserchecker.com
 - Subdomains!

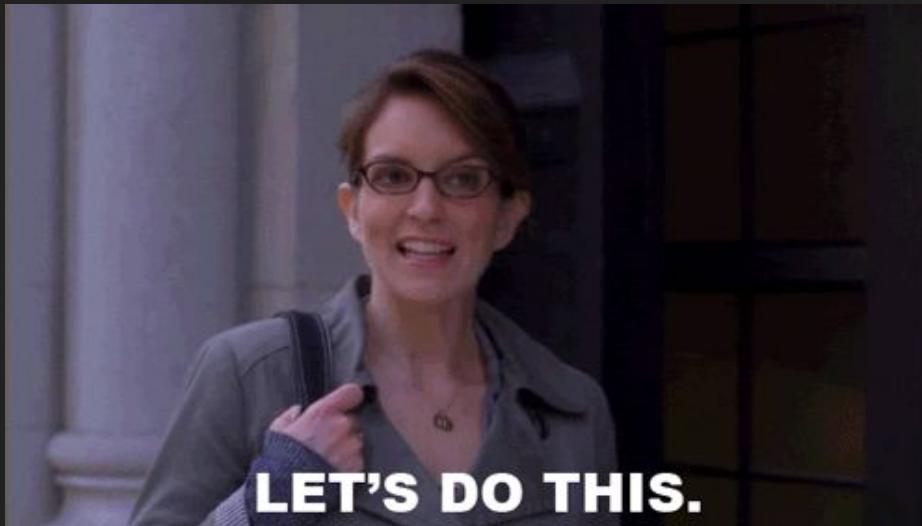
Domain Registration and Strategies - Providers

- NameCheap (www.namecheap.com)
- GoDaddy (www.godaddy.com)
- Purchase Whois protection
- Purchase SSL certificate
 - You will need this later
 - Could also use LetsEncrypt (letsencrypt.org) - free :)

Defeating Web Proxies

Defeating Web Proxies

- “Uncategorized” domains are blocked in most organizations
- Luckily we can have our domains categorized!
 - BlueCoat (<https://sitereview.bluecoat.com/sitereview.jsp>)
 - Palo Alto (<https://urlfiltering.paloaltonetworks.com/ChangeASite.jsp>)
 - FortiGuard* (<https://fortiguard.com/faq/wfratingsubmit>)



Defeating Web Proxies - Categorizing a Domain

- What's really needed to get a malicious domain categorized?
 - **Spoiler Alert:** About 10 minutes of work (and some waiting time) thanks to WordPress ;)
 - Will probably automate this process if someone else hasn't already



Defeating Web Proxies - Categorizing a Domain

- Spawn up a Linux VPS
 - DigitalFyre
 - GoDaddy
 - DigitalOcean
 - **NO AWS!!**

The screenshot shows the DigitalOcean cloud interface. At the top, there is a banner prompting users to enable two-factor authentication. Below the banner, the navigation bar includes links for Droplets, Images, Networking, Monitoring, API, and Support. The main title "Droplets" is centered above a search bar. The "Droplets" tab is selected, while the "Volumes" tab is shown in blue. A table lists the details of a single droplet:

Name	IP Address	Created	Tags
ubuntu-512mb-sfo1-01	107.170.224.109	Go change the world!	

Below the table, it is noted that the droplet has 512 MB / 20 GB Disk / SFO1 - Ubuntu 16.04.2 x64.

Defeating Web Proxies - Categorizing a Domain

- Buy a domain and configure DNS for new VPS

The screenshot shows a web-based DNS management interface for the domain `security-awareness.education`. The top navigation bar includes links for Domain, Products, Sharing & Transfer, and Advanced DNS. The Advanced DNS tab is currently selected. Below the navigation, there are sections for HOST RECORDS and a search bar. The main table displays the following data:

Type	Host	Value	TTL
A Record	*	107.170.224.109	Automatic
A Record	www	107.170.224.109	30 min

At the bottom left, there is a red button labeled **ADD NEW RECORD**.

Defeating Web Proxies - Categorizing a Domain

- Install necessary WordPress dependencies on the VPS (PHP, MySQL, Apache)
 - **Command (Ubuntu 16.04):** sudo apt-get install -y apache2 mysql-server php libapache2-mod-php php-mcrypt php-mysql
 - Do not forget to restart Apache afterwards! WordPress will complain if you do not

Defeating Web Proxies - Categorizing a Domain

- Download latest version of WordPress and uncompress (tar -xvf latest.tar.gz) and move to /var/www/html

```
root@ubuntu-512mb-sf01-01:/var/www/html# ls -al
total 200
drwxr-xr-x  5 www-data www-data  4096 Apr 24 16:03 .
drwxr-xr-x  3 root     root      4096 Apr 24 14:19 ..
-rw-r--r--  1 www-data www-data   418 Sep 25 2013 index.php
-rw-r--r--  1 www-data www-data 19935 Jan  2 18:51 license.txt
-rw-r--r--  1 www-data www-data  7433 Jan 11 17:46 readme.html
-rw-r--r--  1 www-data www-data  5447 Sep 27 2016 wp-activate.php
drwxr-xr-x  9 www-data www-data  4096 Apr 20 16:36 wp-admin
-rw-r--r--  1 www-data www-data   364 Dec 19 2015 wp-blog-header.php
-rw-r--r--  1 www-data www-data 1627 Aug 29 2016 wp-comments-post.php
-rw-rw-rw-  1 www-data www-data 3133 Apr 24 14:22 wp-config.php
-rw-r--r--  1 www-data www-data 2853 Dec 16 2015 wp-config-sample.php
drwxr-xr-x  5 www-data www-data  4096 Apr 24 16:07 wp-content
-rw-r--r--  1 www-data www-data 3286 May 24 2015 wp-cron.php
drwxr-xr-x 18 www-data www-data 12288 Apr 20 16:36 wp-includes
-rw-r--r--  1 www-data www-data 2422 Nov 21 02:46 wp-links-opml.php
-rw-r--r--  1 www-data www-data 3301 Oct 25 03:15 wp-load.php
-rw-r--r--  1 www-data www-data 33939 Nov 21 02:46 wp-login.php
-rw-r--r--  1 www-data www-data  8048 Jan 11 05:15 wp-mail.php
-rw-r--r--  1 www-data www-data 16255 Apr  6 18:23 wp-settings.php
-rw-r--r--  1 www-data www-data 29896 Oct 19 2016 wp-signup.php
-rw-r--r--  1 www-data www-data  4513 Oct 14 2016 wp-trackback.php
-rw-r--r--  1 www-data www-data 3065 Aug 31 2016 xmlrpc.php
root@ubuntu-512mb-sf01-01:/var/www/html#
```

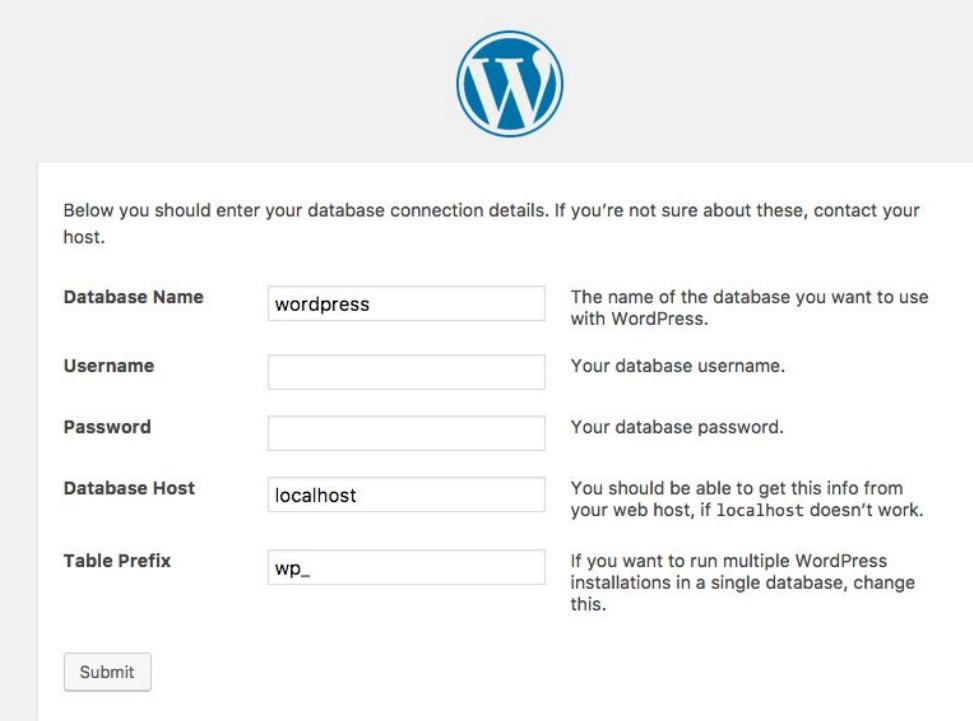
Defeating Web Proxies - Categorizing a Domain

- Create database for WordPress

```
[root@ubuntu-512mb-sfo1-01:/var/www/html# mysql -u root -p  
[Enter password:  
Welcome to the MySQL monitor. Commands end with ; or \g.  
Your MySQL connection id is 554  
Server version: 5.7.17-0ubuntu0.16.04.2 (Ubuntu)  
  
Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserved.  
  
Oracle is a registered trademark of Oracle Corporation and/or its  
affiliates. Other names may be trademarks of their respective  
owners.  
  
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.  
  
[mysql> create database wordpress;  
Query OK, 1 row affected (0.00 sec)  
  
mysql>
```

Defeating Web Proxies - Categorizing a Domain

- Run the WordPress install



The image shows the WordPress database connection setup screen. It features the classic blue 'W' logo at the top. Below it, a text box contains the instruction: "Below you should enter your database connection details. If you're not sure about these, contact your host." The form consists of five input fields with accompanying explanatory text to their right:

Database Name	<input type="text" value="wordpress"/>	The name of the database you want to use with WordPress.
Username	<input type="text"/>	Your database username.
Password	<input type="text"/>	Your database password.
Database Host	<input type="text" value="localhost"/>	You should be able to get this info from your web host, if localhost doesn't work.
Table Prefix	<input type="text" value="wp_"/>	If you want to run multiple WordPress installations in a single database, change this.

At the bottom left is a "Submit" button.

Defeating Web Proxies - Categorizing a Domain

- Change WordPress settings to use newly-registered domain instead of an IP address

General Settings

Site Title	<input type="text" value="Security Awareness"/>
Tagline	<input type="text" value="Raising your security awareness, one blog post at a"/> <i>In a few words, explain what this site is about.</i>
WordPress Address (URL)	<input type="text" value="http://www.security-awareness.education"/>
Site Address (URL)	<input type="text" value="http://www.security-awareness.education"/> <i>Enter the address here if you <u>want your site home page to be different from your WordPress installation directory.</u></i>

Defeating Web Proxies - Categorizing a Domain

- Delete “Hello” default post
- Add in your own “Welcome” post (just needs a few sentences)

The screenshot shows a WordPress editor interface. At the top left is the "Edit Post" button and an "Add New" button. The title of the post is "Welcome". Below the title, the permalink is listed as <http://www.security-awareness.education/index.php/2017/04/24/welcome/> with an "Edit" link. There is also a "Permalink" button. On the right side of the toolbar are "Visual" and "Text" tabs, with "Text" selected. The main content area contains a paragraph of text: "Welcome to our new security awareness website. Cyber criminals are out there! They want your credit cards, they want your SSN, and they want your identity! Just like our last website, this website will contain weekly blog posts on how you can stay safe online. Be sure to come back next week as we will release our first blog post on this new website!". Below the content area is a standard WordPress rich text editor toolbar with icons for bold, italic, lists, and other formatting options.

Defeating Web Proxies - Categorizing a Domain

- Final result ...now we submit and wait

The screenshot shows a web browser window with the URL www.security-awareness.education in the address bar. The page content is as follows:

SECURITY AWARENESS
Raising your security awareness, one blog post at a time

24 APR 2017 **Welcome**

Welcome to our new security awareness website. Cyber criminals are out there! They want your credit cards, they want your SSN, and they want your identity! Just like our last website, this website will contain weekly blog posts on how you can stay safe online. Be sure to come back next week as we will release our first blog post on this new website!

[Read More](#)

On the right side of the page, there is a sidebar with the following sections:

- Search ...
- Recent Posts
 - Welcome
- Recent Comments
- Archives

Defeating Web Proxies - Categorizing a Domain

- Results

- **FortiGuard:** Categorized as “Education” in 10 minutes (lol automated?)
- **BlueCoat:** Categorized as “Technology/Internet” and “Education” in 2 days
- **Palo Alto:** Categorized as “Personal Blogging” in 1.5 days

Test A Site

URL

URL [www.security-awareness.education](#)

Category Personal Sites and Blogs

Description Personal websites and blogs by individuals or groups.

Example Sites [www.blogspot.com](#) , [www.wordpress.com](#) ,
[www.greatamericanphotocontest.com](#)

Additional comments Should try to first categorize based on content. For example, if someone has a blog just about cars, then the site should be categorized under "motor vehicles". However, if the site is a pure blog, then it should remain under "personal sites and blogs".

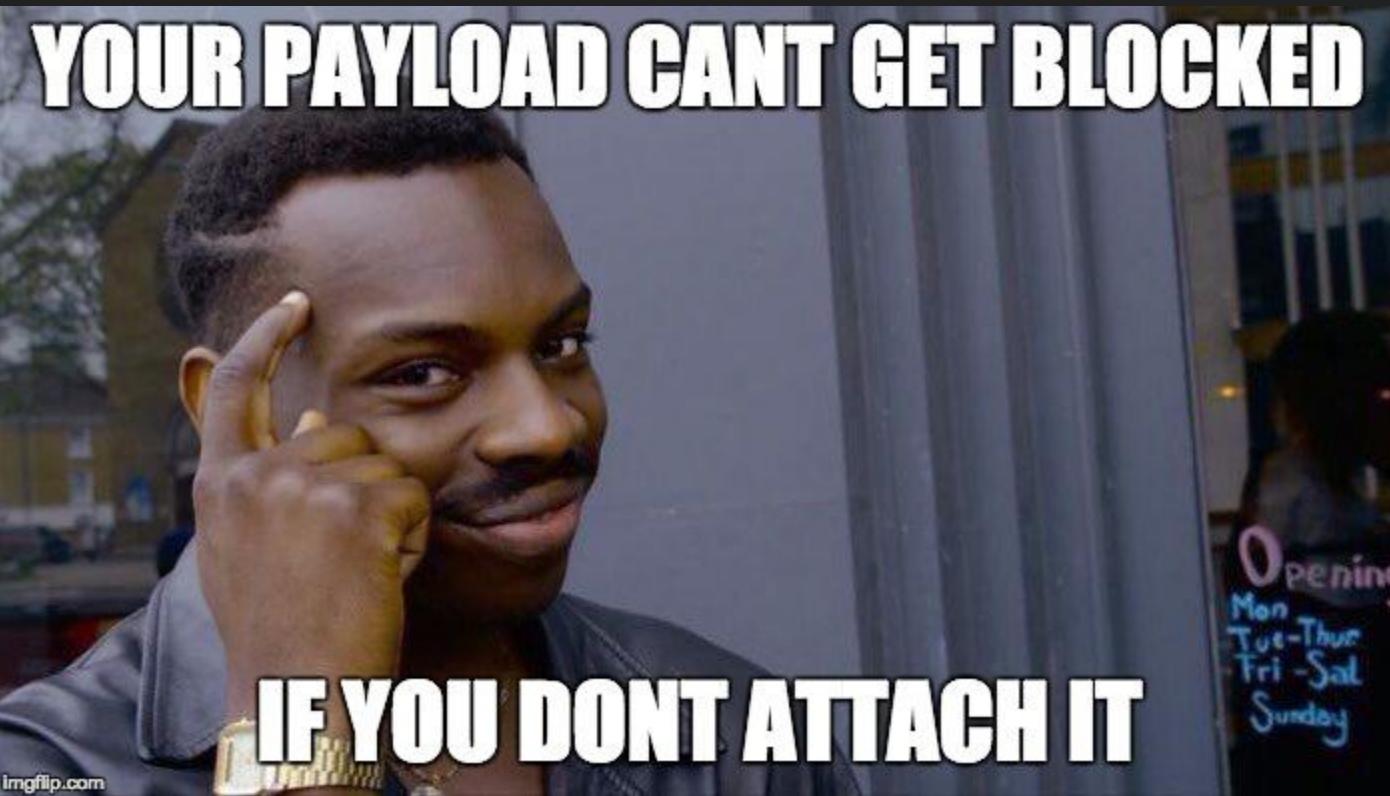
[Request Change](#)

Defeating Email Protections

Defeating Email Protections

- Email protection technologies that could hinder you
 - Cisco IronPort
 - FireEye Email Threat Protection (ETP)
 - Probably more
- Most of these will block commonly attached payloads (macro documents, encrypted zips, etc.)

Defeating Email Protections



Defeating Email Protections

1. Host payload on a website you control
2. Do not include a direct link in your email! Only include the base link (www.baddomain.com)
3. Have the target go to your URL, include verbiage and link to download payload from there
4. ???
5. Profit

Payloads (Old School vs New School)

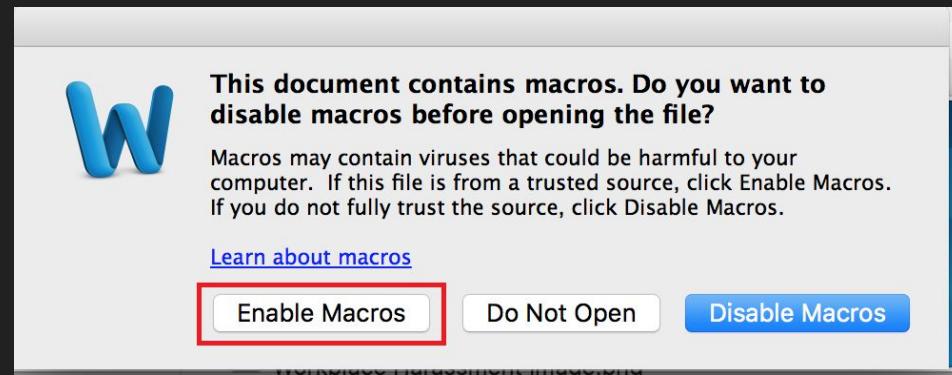
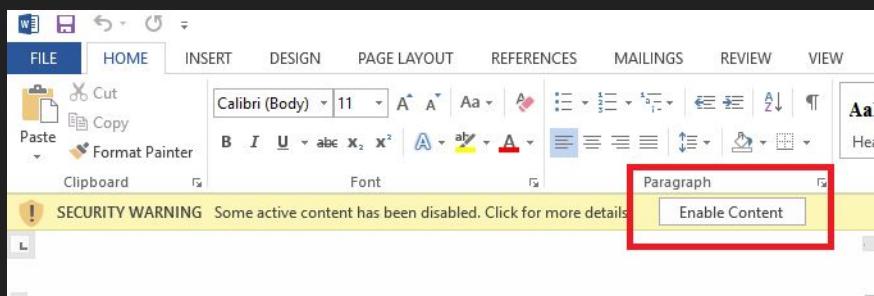
Payloads - Old School

- 1. Office macros
- 2. Custom executables
- Good if targeting multiple operating systems



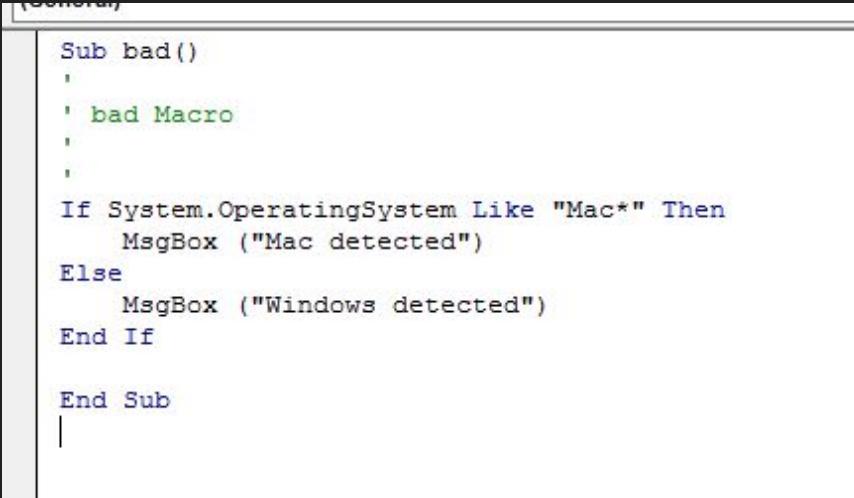
Payloads - Old School - Office Macros

- According to Microsoft: “A macro is a series of commands and instructions that you group together as a single command to accomplish a task automatically.”
 - TLDR: automating tasks in Office
- Macros are coded in Visual Basic (VBA)
- Can be executed automatically:
 - AutoOpen()
 - AutoExec()



Payloads - Old School - Office Macros

- Macros are likely to be detected if the document is attached to an email (not recommended) - Consider using an obfuscation tool:
 - MaliciousMacroGenerator
(<https://github.com/Mr-Un1k0d3r/MaliciousMacroGenerator>)
- Dual-OS macros can be accomplished with a simple “if else” statement



The screenshot shows a Microsoft Word document with the VBA editor open. The code is written in VBA and performs a simple operating system detection. It uses an If-Else statement to check if the operating system is Mac or Windows. If it's Mac, it displays a message box saying "Mac detected". If it's Windows, it displays a message box saying "Windows detected". The code is as follows:

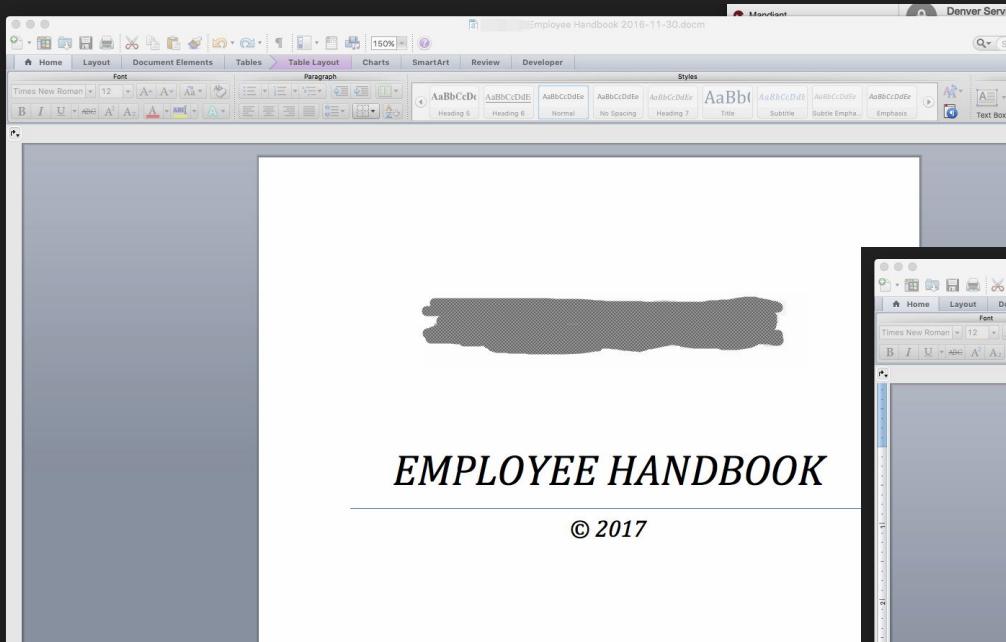
```
Sub bad()
'
' bad Macro
'

If System.OperatingSystem Like "Mac*" Then
    MsgBox ("Mac detected")
Else
    MsgBox ("Windows detected")
End If

End Sub
```

Payloads - Old School - Office Macros

- Sample payload



A screenshot of a Microsoft Word document titled "Employee Handbook 2016-11-30.docm". The document features a section titled "ACKNOWLEDGMENT OF RECEIPT OF EMPLOYEE HANDBOOK" in bold capital letters. Below this title is a paragraph of text: "I ACKNOWLEDGE that I have received a copy of the [REDACTED] Employee Handbook. I have read and understood the contents of the handbook, and I agree to abide by its directions and procedures. I have been given the opportunity to ask any questions I might have about the policies in the handbook. I understand that it is my responsibility to read and familiarize myself with the policies and procedures contained in the handbook." Further down, another paragraph states: "I understand that the statements contained in the handbook are guidelines for employees concerning some of [REDACTED]'s policies and benefits, and are not intended to create any contractual or other legal obligations or to alter the at-will nature of my employment with [REDACTED]. In the event I do have an employment contract which expressly alters the at-will relationship, I agree to the foregoing except with reference to an at-will employment status." At the bottom of the form, there is a field labeled "Full Name: [REDACTED]" and a checkbox labeled "I accept the terms and conditions above". The Microsoft Word ribbon is visible at the top of the window.

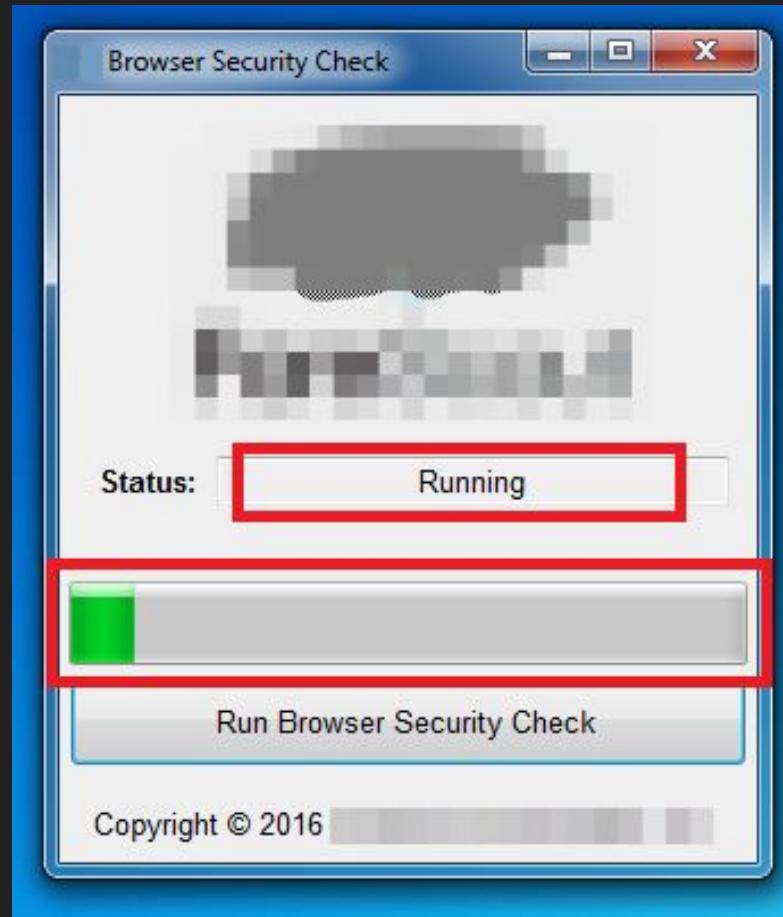
Payloads - Old School - Custom Executables

- Can create custom OS X GUI executables using XCode or a Python → .app program
- Can create custom Windows GUI executables using Visual Studio
- Application Whitelisting can really mess up your day (see Fraser)



Payloads - Old School - Custom Executables

- Sample payload
(Windows Forms)



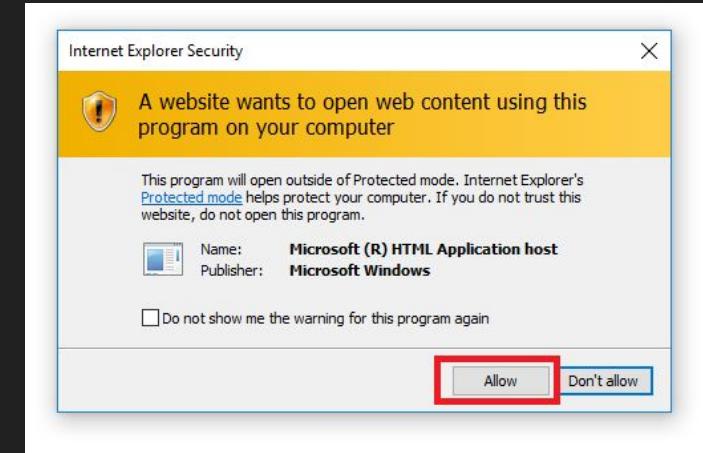
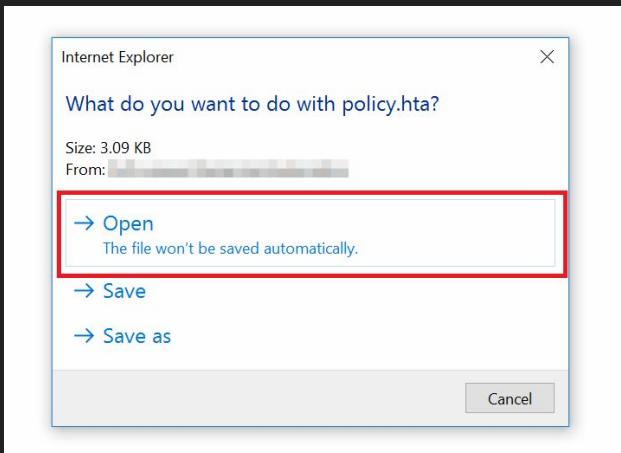
Payloads - New School

- 1. HTML Applications (HTAs)
- 2. ClickOnce
- Both are limited to Windows targets



Payloads - New School - HTML Applications (HTAs)

- Technically not “new”, been around since the 1990s
- HTML-coded applications, what could go wrong?
 - HTA (mshta) → HTML → allows VBScript/WScript code → cmd exec
- HTAs integrate seamlessly with Internet Explorer, but still work with Chrome and Firefox (HTA saved in “Downloads” directory)
- Requires the user to click through two prompts



Payloads - New School - HTML Applications (HTAs)

- Creating and Hosting HTAs
 - Bootstrap for aesthetics
 - Supports favicon.ico (company logo)
 - Fun with .htaccess
 - AddType application/hta .aspx
 - www.<DOMAIN>.com/browser check.aspx



Payloads - New School - HTML Applications (HTAs)

Branch: master ▾ Social-Engineering-Payloads / Sexual-Harassment-Policy-Update / policy.hta Find file Copy path

t3ntman Added policy.hta 1fd5803 on Sep 20, 2016 1 contributor

90 lines (79 sloc) | 3.02 KB Raw Blame History

```
1 <html>
2     <head>
3         <title>CLIENT HERE</title>
4         <meta charset="utf-8">
5         <meta http-equiv="x-ua-compatible" content="ie=9">
6         <!-- CDN links -->
7         <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css">
8         <script src="https://ajax.googleapis.com/ajax/libs/jquery/1.12.4/jquery.min.js"></script>
9         <script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js"></script>
10        <script src="https://code.jquery.com/jquery-1.12.3.js"></script>
11        <HTA:APPLICATION
12            SCROLL="auto"
13            SINGLEINSTANCE="yes"
14            CAPTION="yes"
15            ICON=""
16        >
17    </head>
18
19    <body style="margin: 10px;">
20        <!-- This script will put the HTA document in the foreground and make the window 500x850 -->
21        <script language="vbscript">
22            window.resizeTo 500, 850
23            window.focus()
24        </script>
25
26        <script language="VBScript">
27            Set oShell = CreateObject ("Wscript.Shell")
28            Dim strArgs
29            strArgs = "powershell.exe"
30            oShell.Run strArgs, 0, false
31        </script>
32
```

Payloads - New School - HTML Applications (HTAs)

- Sample payload (with Bootstrap and without Bootstrap)

CLIENT HERE

What is sexual harassment?

Sexual harassment can be defined as any:

- Unwelcomed sexual advances
- Requests for sexual favors
- Other verbal or physical conduct of a sexual nature that affects an individual's employment, and unreasonably interferes with his or her work performance

Who can be involved in sexual harassment?

- Those who commit
 - This can be employees at all levels, customers, and members of the same and opposite sex
- Those who are targeted
 - This can be victims, bystanders, and witnesses who are affected by the sexual harassment

Why is sexual harassment knowledge important?

- Sexual harassment harms us all. The most important part of our corporate values is to ensure that all employees are treated with respect and dignity. Engaging in, condoning, or not reporting sexual harassment is in direct conflict with our core values.

By accepting this agreement, you are responsible for:

- Knowing and complying with our sexual harassment policy and procedure
- Reporting all incidents that you experience or directly witness

I have read and accept the terms and conditions above

First Name: Last Name:

What is sexual harassment?

Sexual harassment can be defined as any:

- Unwelcomed sexual advances
- Requests for sexual favors
- Other verbal or physical conduct of a sexual nature that affects an individual's employment, and unreasonably interferes with his or her work performance

Who can be involved in sexual harassment?

- Those who commit
 - This can be employees at all levels, customers, and members of the same and opposite sex
- Those who are targeted
 - This can be victims, bystanders, and witnesses who are affected by the sexual harassment

Why is sexual harassment knowledge important?

- Sexual harassment harms us all. The most important part of our corporate values is to ensure that all employees are treated with respect and dignity. Engaging in, condoning, or not reporting sexual harassment is in direct conflict with our core values.

By accepting this agreement, you are responsible for:

- Knowing and complying with our sexual harassment policy and procedure
- Reporting all incidents that you experience or directly witness

I have read and accept the terms and conditions above

First Name:

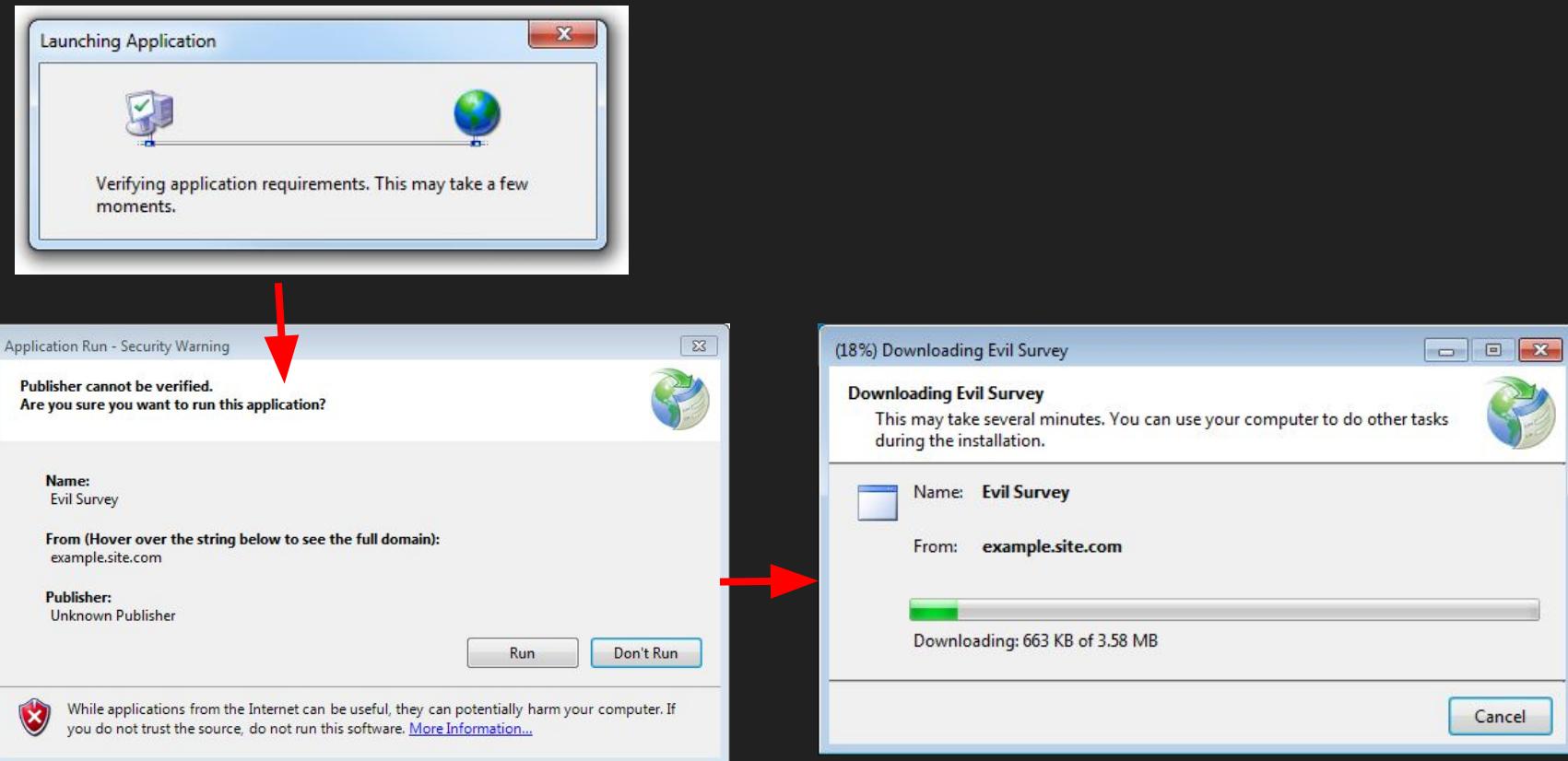
Last Name:

Payloads - New School - ClickOnce

- “ClickOnce is a Microsoft technology that enables the user to install and run a Windows-based smart client application by clicking a link in a web page.” - Wikipedia
 - **TLDR:** Run .NET applications by clicking a link
- **Blog:** <https://blog.netspi.com/all-you-need-is-one-a-clickonce-love-story>
- Only works with Internet Explorer :(
 - Google/Chrome will not run ClickOnce!
 - Relies on the target to be using Internet Explorer when phished

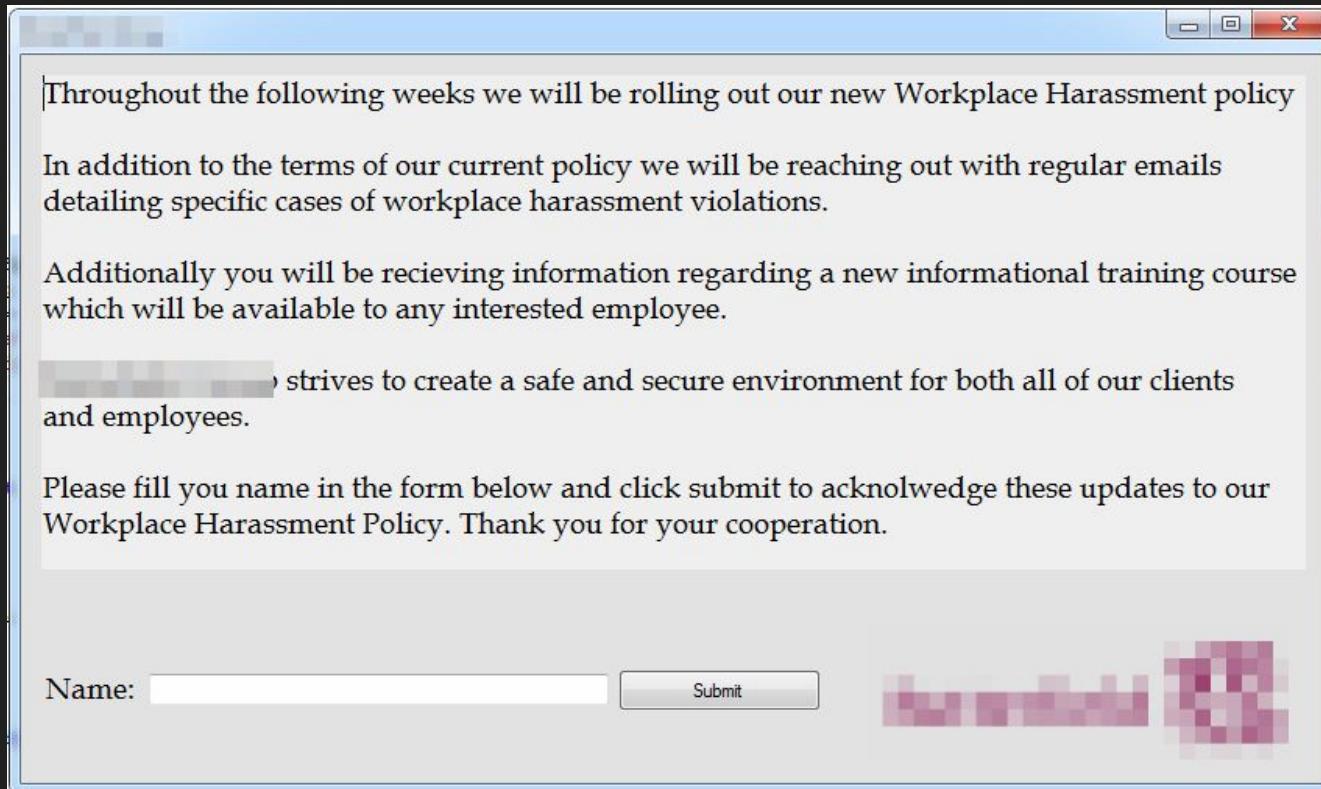
Payloads - New School - ClickOnce

- Target goes to your application's URL



Payloads - New School - ClickOnce

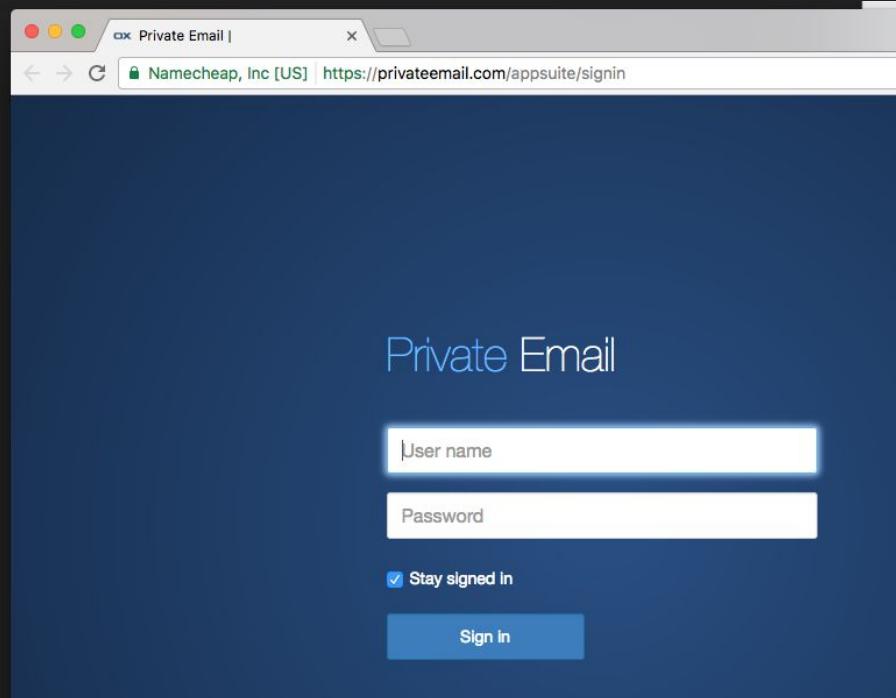
- Sample payload



Email Delivery and Tracking

Email Delivery and Tracking - Delivery

- Typically use NameCheap webmail for <50 emails
 - Free 2 month trial
- Framework (will talk about later) for >50 emails



Email Delivery and Tracking - Delivery

- OMFG send yourself a test email first!



Email Delivery and Tracking - Delivery

- This is why you test emails! (NameCheap defaults)

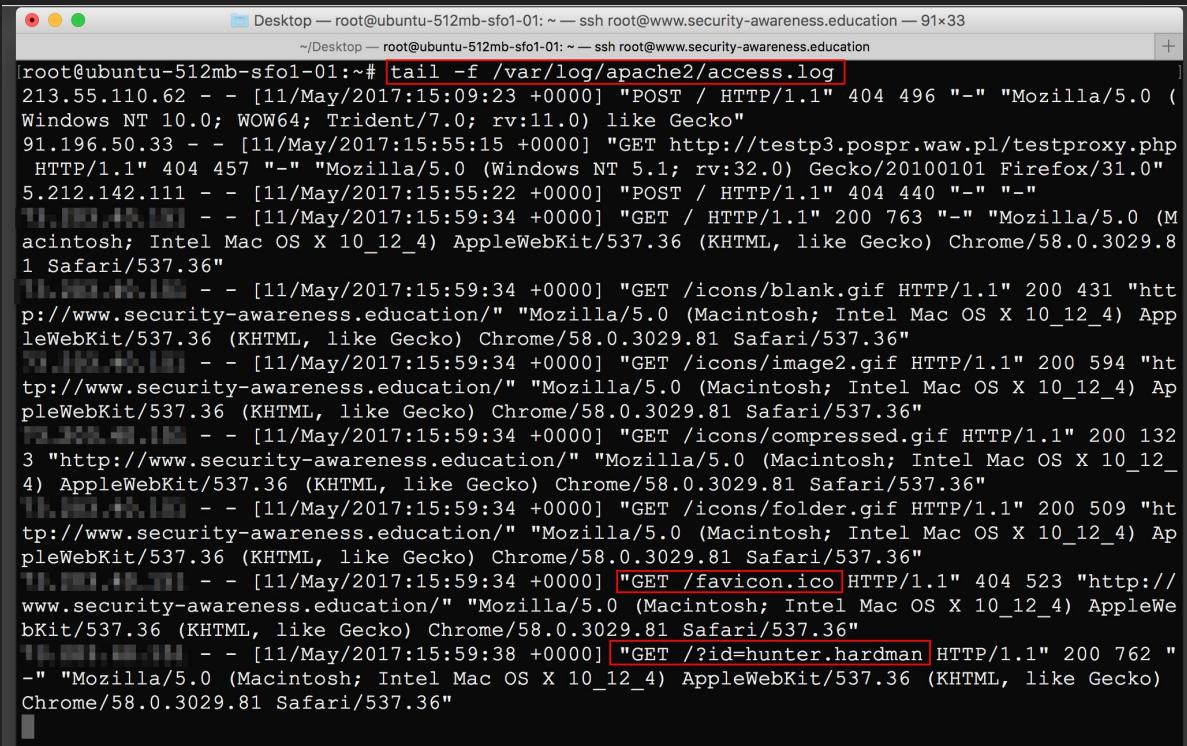
The screenshot shows a Microsoft Outlook interface. At the top, there's a toolbar with icons for Compose, Undo, Redo, Delete, and others. Below the toolbar, a list of emails is shown, with the first one selected. The subject of the selected email is "Security Awareness Training". The recipient field shows "admin@security-awareness.education" listed twice, with the "To" field also containing "t3ntman@gmail.com". The message body starts with "Hunter," and contains the placeholder text "<BAD STUFF HERE>".

Below the message preview, there are account settings. A red box highlights the "Your name" field, which contains "admin@security-awareness.education admin@security-a". There are two other fields: "Email address" containing "admin@security-awareness.education" and a checkbox for "Use unified mail for this account".

Your name	admin@security-awareness.education admin@security-a
Email address	admin@security-awareness.education
<input type="checkbox"/> Use unified mail for this account	

Email Delivery and Tracking - Tracking

- www.bad.com?id=hunter.hardman
- HTTP GET parameters are great for tracking



A screenshot of a terminal window titled "Desktop — root@ubuntu-512mb-sfo1-01: ~ — ssh root@www.security-awareness.education — 91x33". The command "tail -f /var/log/apache2/access.log" is running, displaying a log of HTTP requests. The log shows various user agents and their versions, including Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko, Mozilla/5.0 (Windows NT 5.1; rv:32.0) Gecko/20100101 Firefox/31.0, Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.81 Safari/537.36, and Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.81 Safari/537.36. One specific line of interest is highlighted in red: "- [11/May/2017:15:59:34 +0000] [GET /?id=hunter.hardman] [HTTP/1.1] 200 762 \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.81 Safari/537.36\"". This indicates that the tracking parameter was successfully delivered and tracked by the browser.

```
root@ubuntu-512mb-sfo1-01:~# tail -f /var/log/apache2/access.log
213.55.110.62 - - [11/May/2017:15:09:23 +0000] "POST / HTTP/1.1" 404 496 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko"
91.196.50.33 - - [11/May/2017:15:55:15 +0000] "GET http://testp3.pospr.waw.pl/testproxy.php HTTP/1.1" 404 457 "-" "Mozilla/5.0 (Windows NT 5.1; rv:32.0) Gecko/20100101 Firefox/31.0"
5.212.142.111 - - [11/May/2017:15:55:22 +0000] "POST / HTTP/1.1" 404 440 "-" "-"
- - [11/May/2017:15:59:34 +0000] "GET / HTTP/1.1" 200 763 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.81 Safari/537.36"
- - [11/May/2017:15:59:34 +0000] "GET /icons/blank.gif HTTP/1.1" 200 431 "http://www.security-awareness.education/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.81 Safari/537.36"
- - [11/May/2017:15:59:34 +0000] "GET /icons/image2.gif HTTP/1.1" 200 594 "http://www.security-awareness.education/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.81 Safari/537.36"
- - [11/May/2017:15:59:34 +0000] "GET /icons/compressed.gif HTTP/1.1" 200 1323 "http://www.security-awareness.education/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.81 Safari/537.36"
- - [11/May/2017:15:59:34 +0000] "GET /icons/folder.gif HTTP/1.1" 200 509 "http://www.security-awareness.education/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.81 Safari/537.36"
- - [11/May/2017:15:59:34 +0000] [GET /favicon.ico] [HTTP/1.1] 404 523 "http://www.security-awareness.education/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.81 Safari/537.36"
- - [11/May/2017:15:59:38 +0000] [GET /?id=hunter.hardman] [HTTP/1.1] 200 762 "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.81 Safari/537.36"
```

Phone Delivery (for those truly brave)

Phone Delivery

- SpoofCard (www.spoofcard.com)
 - \$29.99 for 160 minutes, totally worth it
- Spoof the company's main phone number
 - Makes it harder to track down who received phone calls (and didn't report it)
- Make sure the target is on the hook!
 - Premature disclosure
- People generally want to help one another (especially over the phone)

Phone Delivery - Expectation



Phone Delivery - Reality



Social Engineering Frameworks

Social Engineering Frameworks

- To make your life easier...
 - FiercePhish (<https://github.com/Raikia/FiercePhish>)
 - Social Engineering Toolkit
(<https://github.com/trustedsec/social-engineer-toolkit>)
 - KingPhisher (<https://github.com/securestate/king-phisher>)

Rookie Mistakes

Rookie Mistakes

- We've all made these mistakes, don't feel bad
- Learn from these mistakes!
 - Not purchasing Whois protection
 - Not clearing payload metadata



Rookie Mistakes - Whois Protection

- “WhoisGuard is a privacy protection service that prevents people from seeing your name, address, phone number and email when they do a Whois search on your domain.”
[\(<https://www.namecheap.com/support/knowledgebase/article.aspx/278/37/what-is-whoisguard>\)](https://www.namecheap.com/support/knowledgebase/article.aspx/278/37/what-is-whoisguard)

Rookie Mistakes - Whois Protection

- With Whois protection

```
hackhackcitybitch:Desktop t3ntman$ whois security-awareness.education
Domain Name: security-awareness.education
Registry Domain ID: 75490465c8bb4dbd9a317d608d5f4355-DONUTS
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: https://www.namecheap.com/
Updated Date: 2017-04-29T14:27:20Z
Creation Date: 2017-04-24T14:27:02Z
Registry Expiry Date: 2018-04-24T14:27:02Z
Registrar: NameCheap, Inc.
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: 95e4aa05bc47479696b89df9b4a833ba-DONUTS
Registrant Name: WhoisGuard Protected
Registrant Organization: WhoisGuard, Inc.
Registrant Street: P.O. Box 0823-03411
Registrant City: Panama
Registrant State/Province: Panama
Registrant Postal Code:
Registrant Country: PA
Registrant Phone: +507.8365503
Registrant Phone Ext:
Registrant Fax: +51.17057182
Registrant Fax Ext:
Registrant Email: 95edad4bae9343c2bbc52b94d621a024.protect@whoisguard.com
Registry Admin ID: c9cf3341953446eab3a2378d2ba2d3a3-DONUTS
Admin Name: WhoisGuard Protected
Admin Organization: WhoisGuard, Inc.
Admin Street: P.O. Box 0823-03411
```

Rookie Mistakes - Whois Protection

- Without Whois protection

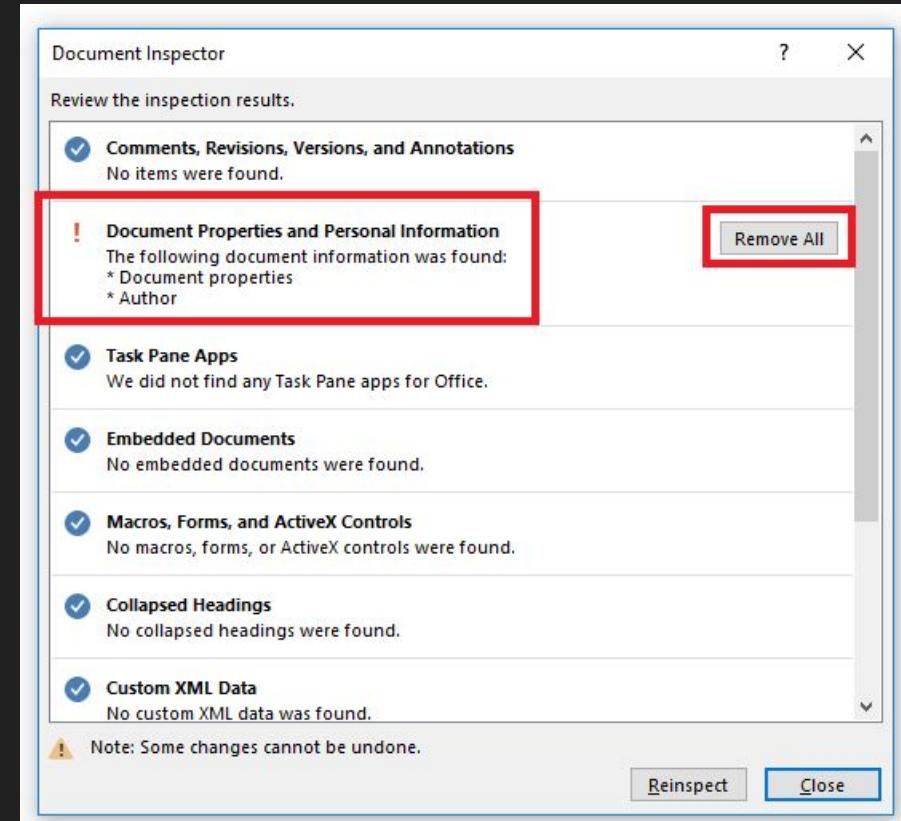
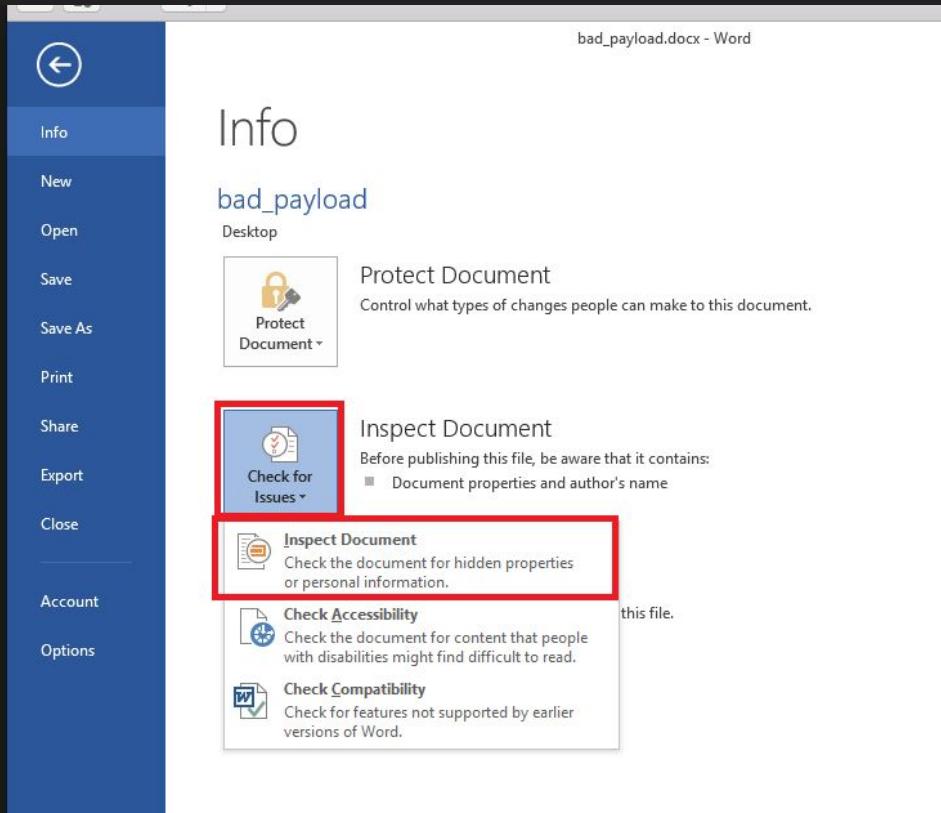
```
Domain Name: fireeye.com
Registry Domain ID: 101043116_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www.cscprotectsbrands.com
Updated Date: 2015-12-23T18:23:39Z
Creation Date: 2003-07-24T18:51:45Z
Registrar Registration Expiration Date: 2025-07-24T18:51:45Z
Registrar: CSC CORPORATE DOMAINS, INC.
Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: +1.8887802723
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Host Master
Registrant Organization: FireEye, Inc.
Registrant Street: 1440 McCarthy Blvd.
Registrant City: Milpitas
Registrant State/Province: CA
Registrant Postal Code: 95035
Registrant Country: US
Registrant Phone: +1.4083216300
Registrant Phone Ext:
Registrant Fax: +1.4083219818
Registrant Fax Ext:
Registrant Email: hostmaster@fireeye.com
Registry Admin ID:
Admin Name: Host Master
Admin Organization: FireEye, Inc.
Admin Street: 1440 McCarthy Blvd.
Admin City: Milpitas
Admin State/Province: CA
```

Rookie Mistakes - Metadata

- Metadata = data that describes the document (author, file path, etc)
 - “that is so meta!”
- People of all skill levels can forget to do this
 - I’m guilty :(
- Provides attribution (especially for domain-bound systems)
 - Author: hunter.hardman@company.com
- **Whitepaper:**
<https://www.sans.org/reading-room/whitepapers/privacy/document-metadata-silent-killer-32974>

Rookie Mistakes - Clearing Metadata

- Built-in Office functionality saves the day!



First Campaign - Employee Handbook Update

Successful Campaigns - Employee Handbook Update

- Payload execution campaign
- Pretext
 - Posed as someone (David) from the Human Resources department, and contacted people via phone informing them about a recent update to the employee handbook
 - Gave them the link hosting the new “employee handbook” while on the phone
 - Said they are on a list of people who have not received and accepted the new employee handbook
 - People don’t like to be on lists
 - If someone questioned the link, I blamed the IT department! I’m just a HR worker trying to do his job right? ;)

Successful Campaigns - Employee Handbook Update

- I contacted 15 people via phone for this campaign, but this could also have been modified for email delivery
- “Employee Handbook” document contained dual-OS Office macro (worked on OS X and Windows systems)

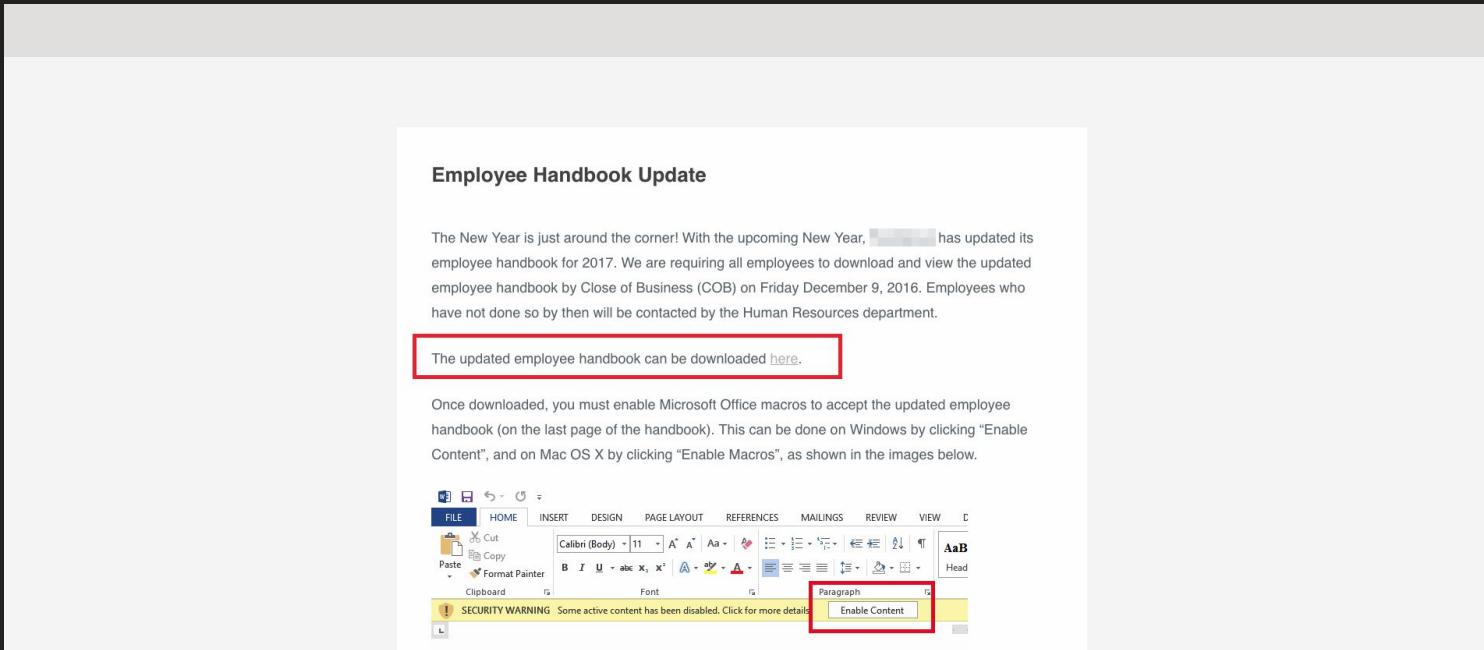
Successful Campaigns - Employee Handbook Update

- Website - header image redacted, I promise it was more aesthetic-looking, use their content against them!
- “handbook” subdomain

The New Year is just around the corner! With the upcoming New Year, [REDACTED] has updated its employee handbook for 2017. We are requiring all employees to download and view the updated employee handbook by Close of Business (COB) on Friday December 9, 2016. Employees who have not done so by then will be contacted by the Human Resources department.

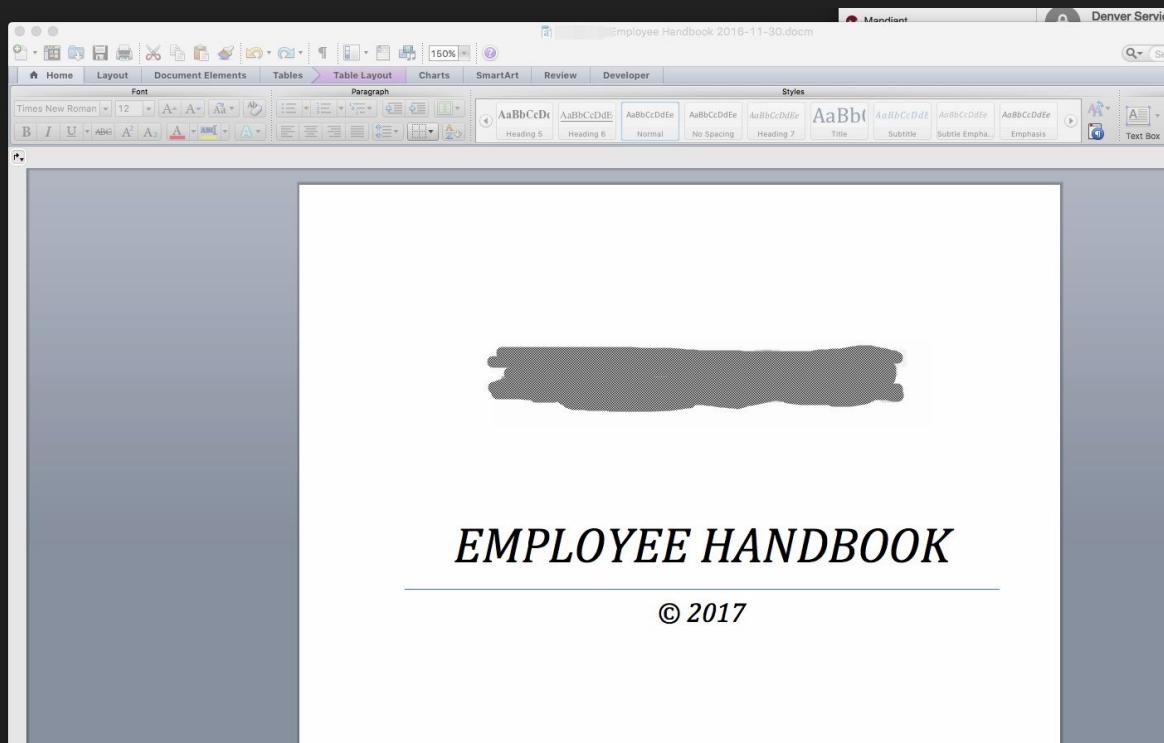
The updated employee handbook can be downloaded [here](#).

Once downloaded, you must enable Microsoft Office macros to accept the updated employee handbook (on the last page of the handbook). This can be done on Windows by clicking “Enable Content”, and on Mac OS X by clicking “Enable Macros”, as shown in the images below.



Successful Campaigns - Employee Handbook Update

- Googled “employee handbook template” and modified it to be specific to the client
- Watermarks, graphics, and 17 pages goes a long way



Successful Campaigns - Employee Handbook Update

- Macro to let them know the form was submitted

The screenshot shows a Microsoft Word document titled "Employee Handbook 2016-11-30.docm". The ribbon menu is visible at the top, showing tabs like Home, Layout, Document Elements, Tables, Table Layout, Charts, SmartArt, Review, and Developer. The Developer tab is selected. The main content area contains a section titled "ACKNOWLEDGMENT OF RECEIPT OF EMPLOYEE HANDBOOK". Below this, there is a text box containing the following text:

I ACKNOWLEDGE that I have received a copy of the [REDACTED] Employee Handbook. I have read and understood the contents of the handbook, and I agree to abide by its directions and procedures. I have been given the opportunity to ask any questions I might have about the policies in the handbook. I understand that it is my responsibility to read and familiarize myself with the policies and procedures contained in the handbook.

I understand that the statements contained in the handbook are guidelines for employees concerning some of [REDACTED]'s policies and benefits, and are not intended to create any contractual or other legal obligations or to alter the at-will nature of my employment with [REDACTED]. In the event I do have an employment contract which expressly alters the at-will relationship, I agree to the foregoing except with reference to an at-will employment status.

Full Name: [REDACTED]

I accept the terms and conditions above

Successful Campaigns - Employee Handbook Update

- No initial bites for a bit, but wait...
“HEROES NEVER DIE!”
- Sometimes people need a “personalized” email instead ;)



Re: Previous Phone Call: Employee Handbook Update

 **Andrea** [REDACTED] 12:14 PM 

To: David [REDACTED]

Quick reply Reply All Forward Delete 

▶  2 attachments View Download Save to Drive

Got it!

Just downloaded and accepted

From: David [REDACTED] <david.l[REDACTED]@hr-f[REDACTED].com>
Reply-To: David [REDACTED] <david.l[REDACTED]@hr-f[REDACTED].com>
Date: Thursday, December 8, 2016 at 12:05 PM
To: Andrea [REDACTED] <andrea.[REDACTED]@[REDACTED].com>
Subject: Previous Phone Call: Employee Handbook Update

Andrea,

I just spoke on the phone with you. Here's that link to download the updated employee handbook:
[https://handbook.hr-\[REDACTED\].com](https://handbook.hr-[REDACTED].com)

That website should have the handbook documents (for Windows and Mac OS X users). Let me know if you have any issues in accessing that website from the link above.

Thanks again,

David [REDACTED]
Sr. Employee Coordinator - Human Resources
Mobile: [REDACTED]

Successful Campaigns - Employee Handbook Update

- Results
 - 5 of the 15 phone recipients visited the malicious website and downloaded/executed the payload
 - OS X and Windows beacons, win!
 - Thank you dual-OS macros



Second Campaign - Email Server Migration

Successful Campaigns - Email Server Migration

- Credential harvesting campaign
 - Do they have 2FA? Will these credentials prove useful?
- Pretext
 - Posed as someone from IT, explained that we have been migrating email servers, and had an issue migrating their account. Manual intervention is needed on their part to complete the migration.
- Make sure the client actually uses Outlook Web Access (OWA)!
- Cloned OWA 2013 portal, custom ASPX to capture submitted credentials, JavaScript for fake loading bar, and some Bootstrap for aesthetics

Successful Campaigns - Email Server Migration

- Sample email

Urgent: Email Server Migration - Manual Intervention Needed

 **Information Technology** 12/7/2016 5:36 PM

To [REDACTED] Quick reply Reply All Forward Delete

▶  2 attachments View Download Save to Drive

Jenny,

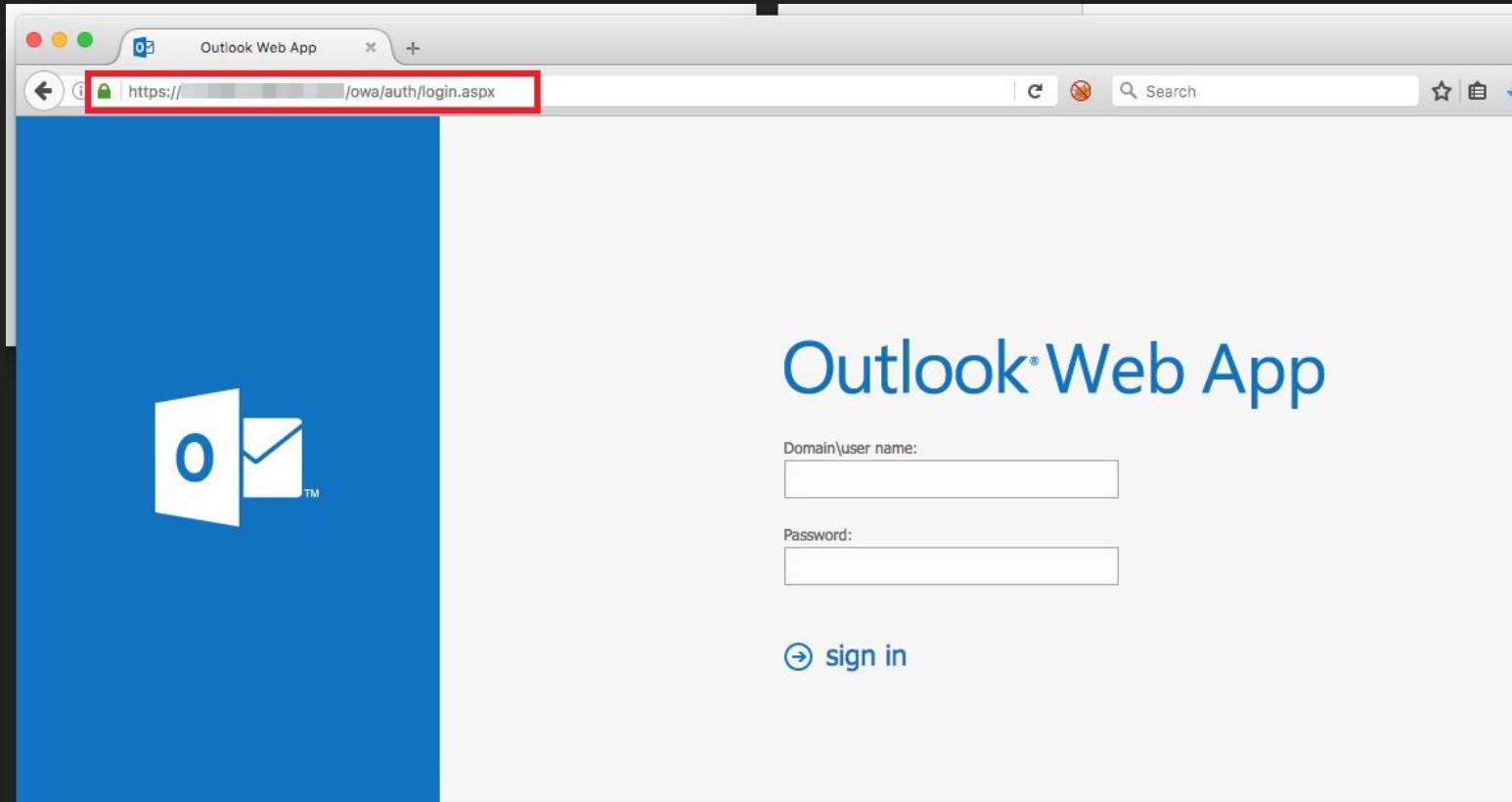
As you may or may not be aware, [REDACTED]'s IT department is in the process of migrating our email servers. You are receiving this email because we experienced an issue during the migration of your email account, and now require manual intervention on your end to complete the migration process. Please complete this migration process by Close of Business (COB) on December 9th, 2016. Failure to complete the migration process by then may result in delayed emails and temporary suspension of your email account. Please see the following instructions below to start the migration process:

1. Go to [https://\[REDACTED\]?id=\[REDACTED\]](https://[REDACTED]?id=[REDACTED]) and log in using your domain credentials.
2. As soon as you login, the migration process will start. This process should only take 1-2 minutes. You will receive a message after the migration process has completed.

Thank you for your time and patience!

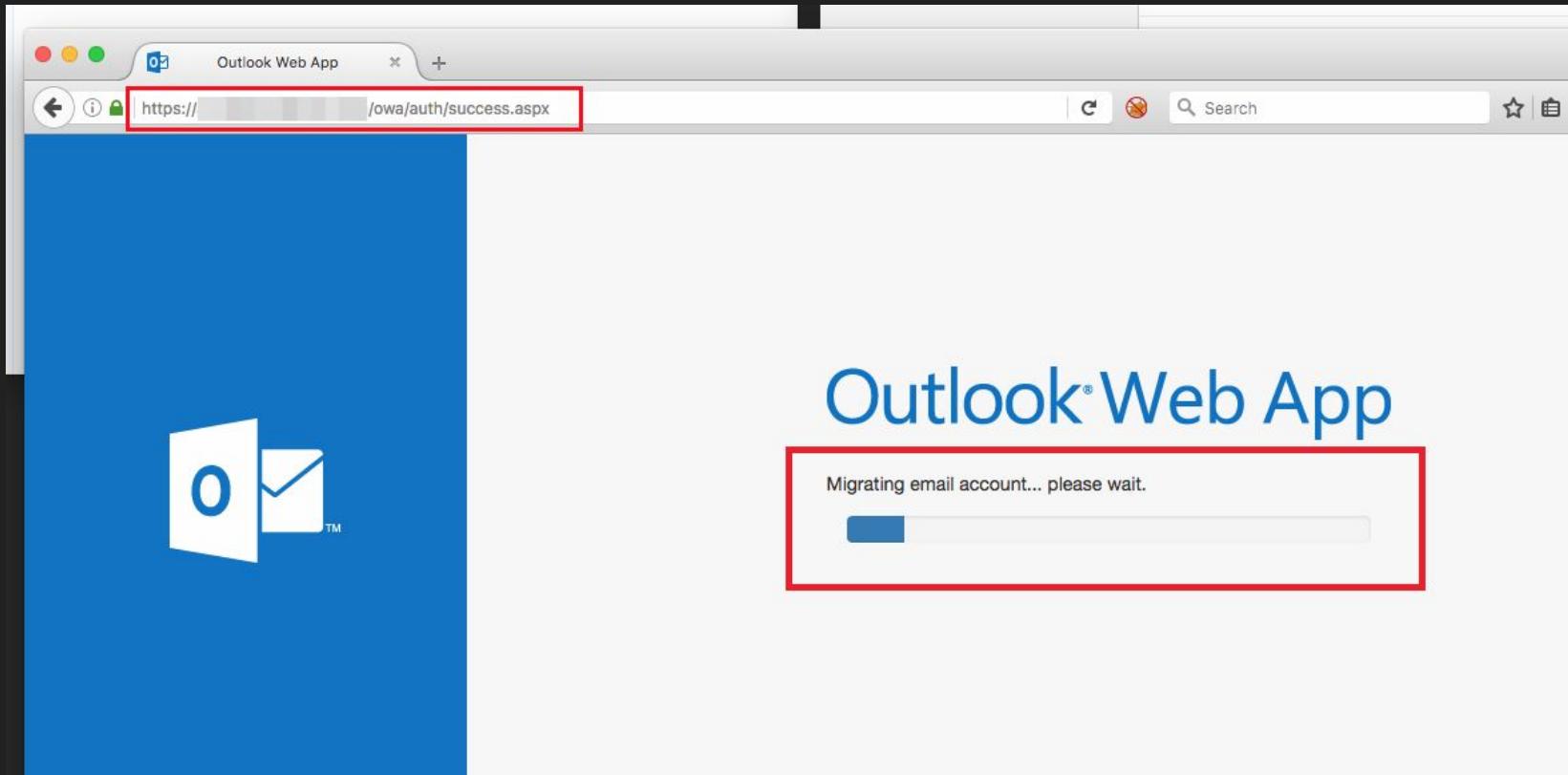
Successful Campaigns - Email Server Migration

- Login page designed to capture submitted credentials



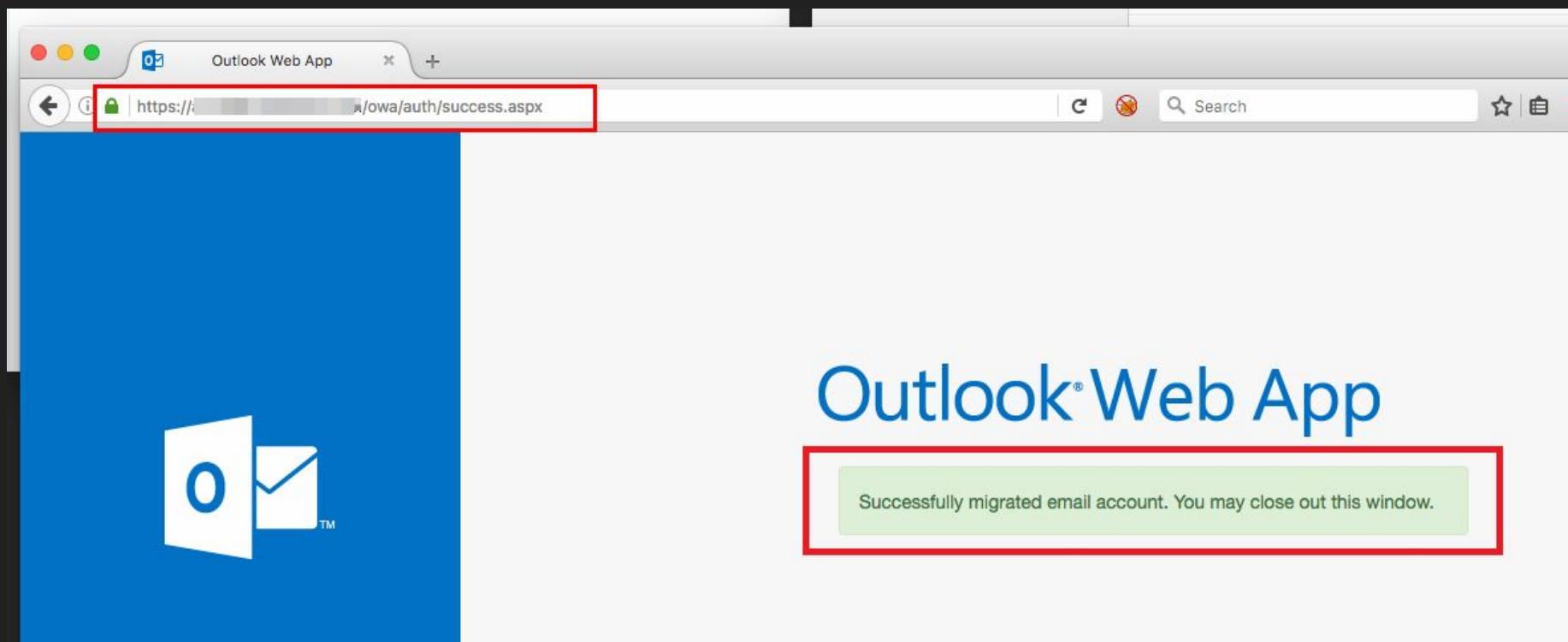
Successful Campaigns - Email Server Migration

- Fake loading bar (JavaScript)



Successful Campaigns - Email Server Migration

- Fake loading bar (JavaScript)



Successful Campaigns - Email Server Migration

- Results
 - 24 out of the 75 recipients visited the malicious website
 - 23 out of the 75 recipients submitted their domain credentials



Third Campaign - Harassment Policy Update

Successful Campaigns - Harassment Policy Update

- Payload execution campaign
- Pretext
 - Posed as someone from the Human Resources department, and contacted people via email informing them that they needed to acknowledge the company's new “Harassment Policy”
 - Said they are on a list of people who have not received and acknowledged the “Harassment Policy”
 - People don't like to be on lists

Successful Campaigns - Harassment Policy Update

- Sample email (sorry for lack of actual redacted email)

<NAME>,

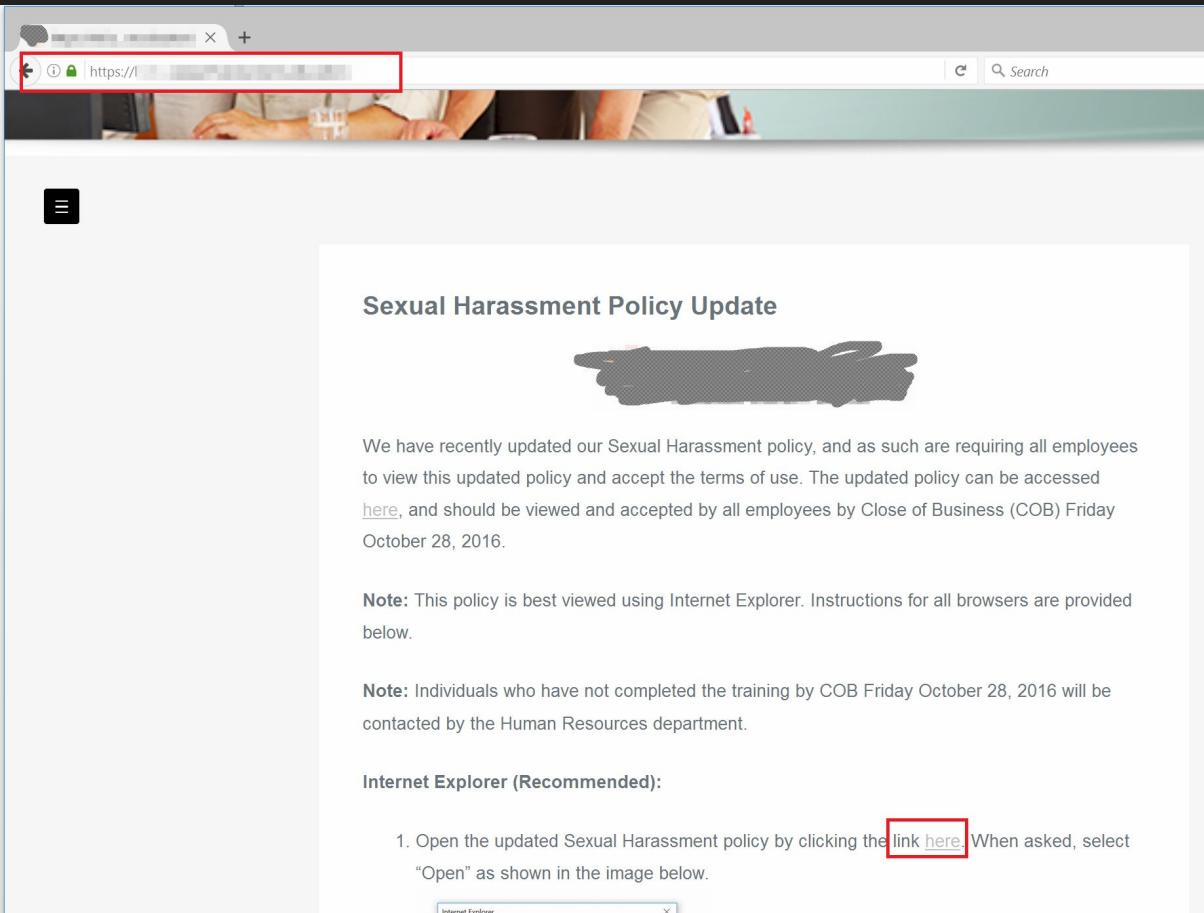
This is a notice to all employees. We have recently updated our Sexual Harassment policy, and as such are requiring all employees to view and acknowledge this updated policy. We are requiring all employees to view and acknowledge this updated policy by Close of Business (COB) Friday October 28, 2016. The instructions and updated policy can be accessed at: [https://\[REDACTED\]&id=<ID>](https://[REDACTED]&id=<ID>)

Note: The policy is best viewed using Internet Explorer.

Employees who have not submitted the form before the policy goes into effect will be contacted by Human Resources.

Successful Campaigns - Harassment Policy Update

- Website (WordPress)
- <CLIENT> subdomain



The screenshot shows a web browser window with a red box highlighting the URL bar, which displays "https://l...". The main content area features a header "Sexual Harassment Policy Update" with a blurred profile picture of a person pointing. Below the header is a paragraph of text. A note below it states: "Note: This policy is best viewed using Internet Explorer. Instructions for all browsers are provided below." Another note at the bottom states: "Note: Individuals who have not completed the training by COB Friday October 28, 2016 will be contacted by the Human Resources department." At the bottom, there is a section titled "Internet Explorer (Recommended)" with step-by-step instructions.

Sexual Harassment Policy Update

We have recently updated our Sexual Harassment policy, and as such are requiring all employees to view this updated policy and accept the terms of use. The updated policy can be accessed [here](#), and should be viewed and accepted by all employees by Close of Business (COB) Friday October 28, 2016.

Note: This policy is best viewed using Internet Explorer. Instructions for all browsers are provided below.

Note: Individuals who have not completed the training by COB Friday October 28, 2016 will be contacted by the Human Resources department.

Internet Explorer (Recommended):

1. Open the updated Sexual Harassment policy by clicking the link [here](#). When asked, select "Open" as shown in the image below.

Successful Campaigns - Harassment Policy Update

- HTA payload
- Used VBScript/WScript to execute regsvr32 application whitelisting bypass payload
 - Thanks Casey Smith (@subtee)!

The screenshot shows a Windows-style dialog box with a title bar and a redacted header. The main content area contains several sections of text:

- What is sexual harassment?**
- Sexual harassment can be defined as any:**
 - Unwelcome sexual advances
 - Requests for sexual favors
 - Other verbal or physical conduct of a sexual nature that affects an individual's employment, and unreasonably interferes with his or her work performance
- Who can be involved in sexual harassment?**
 - Those who commit
 - This can be employees at all levels, customers, and members of the same and opposite sex
 - Those who are targeted
 - This can be victims, bystanders, and witnesses who are affected by the sexual harassment
- Why is sexual harassment knowledge important?**
 - Sexual harassment harms us all. The most important part of our corporate values is to ensure that all employees are treated with respect and dignity. Engaging in, condoning, or not reporting sexual harassment is in direct conflict with our core values.
- By accepting this agreement, you are responsible for:**
 - Knowing and complying with our sexual harassment policy and procedure
 - Reporting all incidents that you experience or directly witness

At the bottom, there is a red rectangular box highlighting a checkbox and input fields:

- I have read and accept the terms and conditions above
- First Name:
- Last Name:
-

Successful Campaigns - Harassment Policy Update

- Results

- Sent 50 emails as part of this campaign
- 20 out of 50 visited the malicious website
- 18 out of 50 download/executed the malicious payload





It's done.

Contact Information

- **Email:** t3ntman@gmail.com
- **Twitter:** @t3ntman
- **GitHub:** <https://github.com/t3ntman/Social-Engineering-Payloads>

Questions?