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

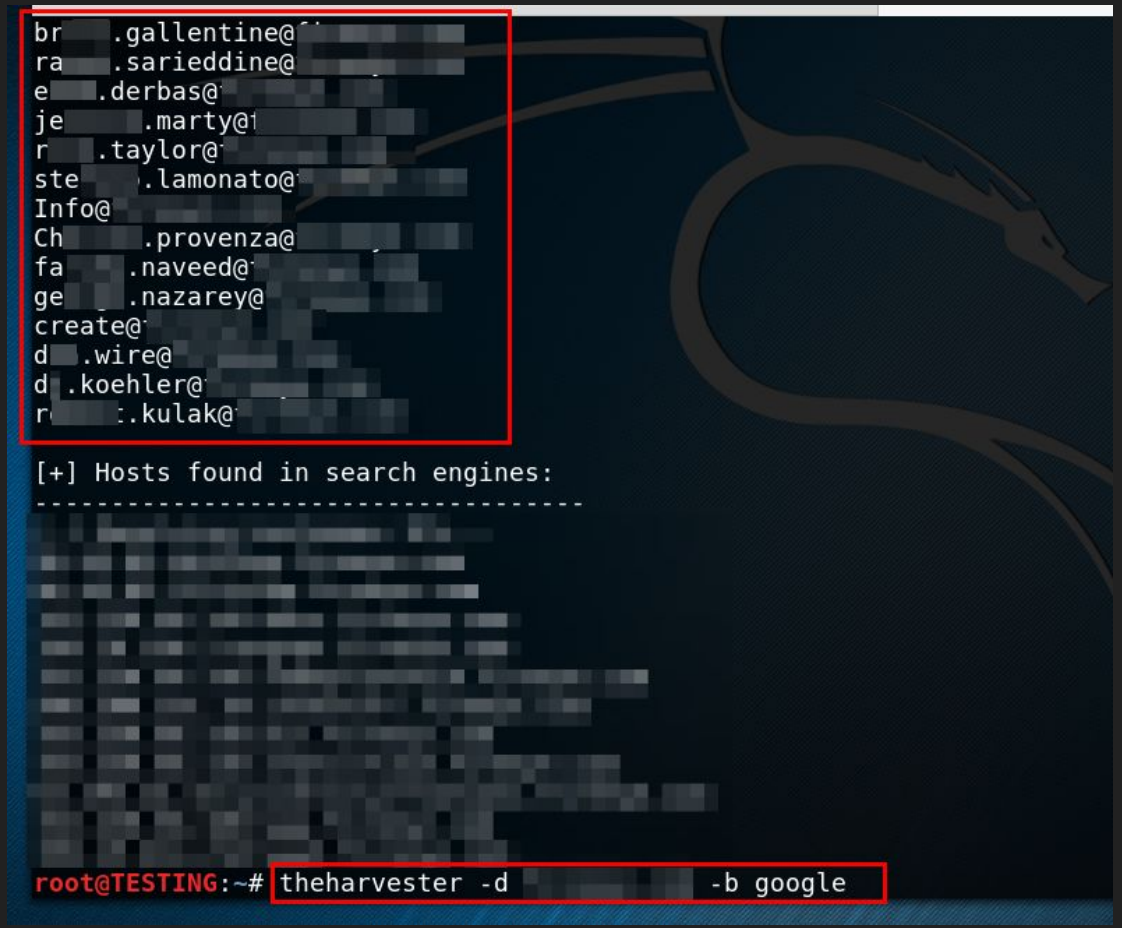
- Bad OSINT = Bad SE Campaign (likely)
- Goals
  - Email harvesting for potential targets
  - Employees, # of employees (big corporation vs start-up), email schema, job titles, phone numbers, departments, etc.
  - Technologies in place

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)

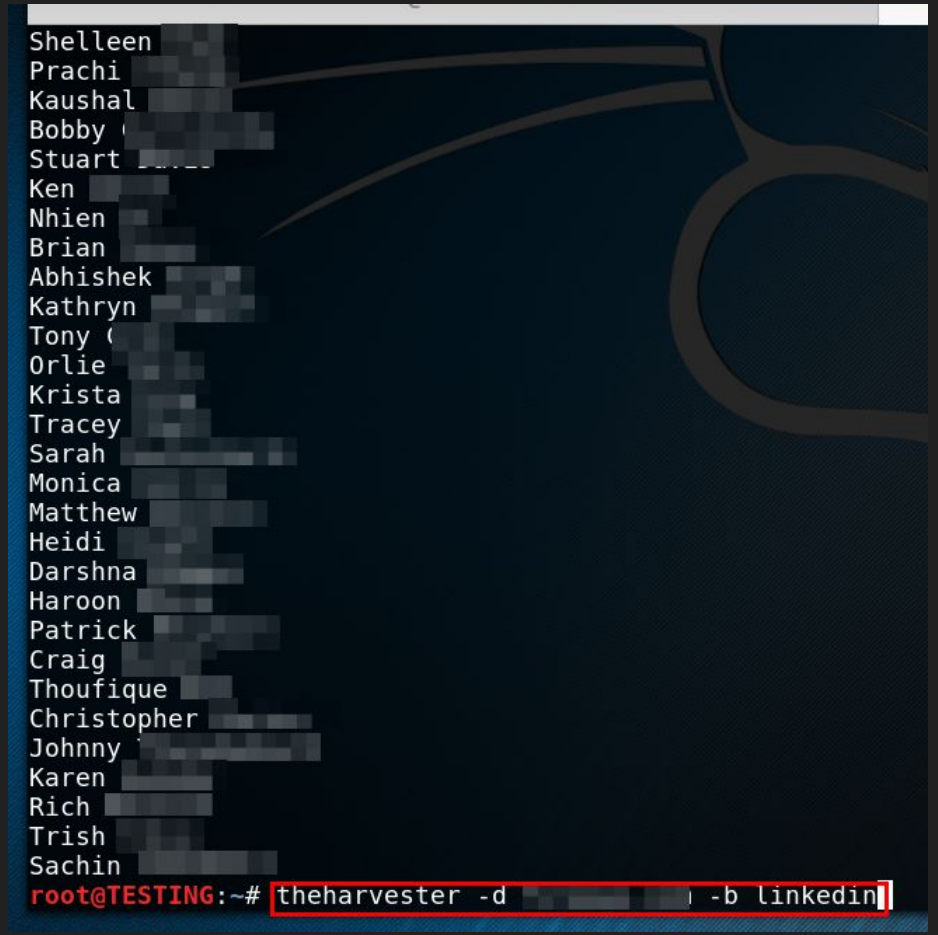
OSINT Gathering - Email Harvesting (theHarvester)

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



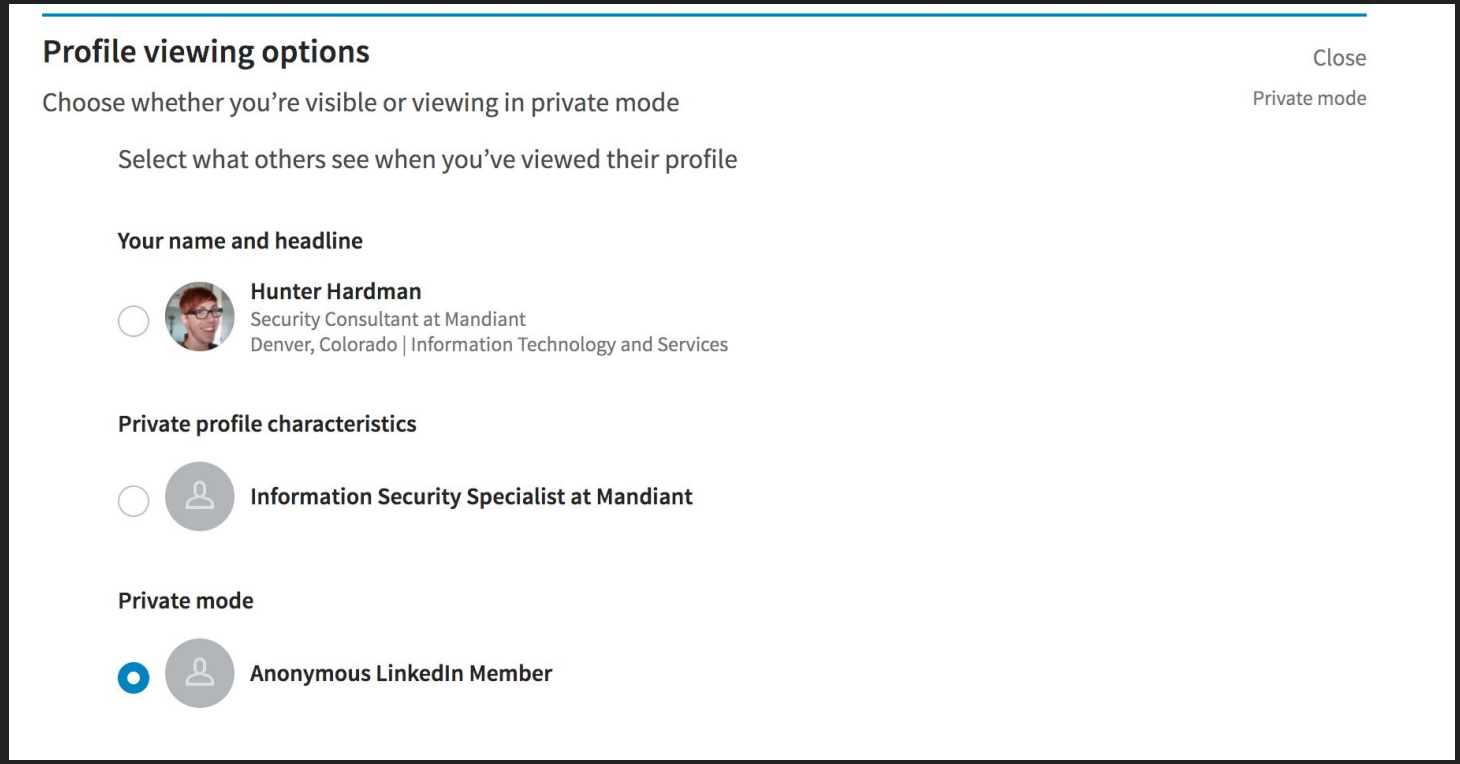
OSINT Gathering - Email Harvesting (theHarvester)

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



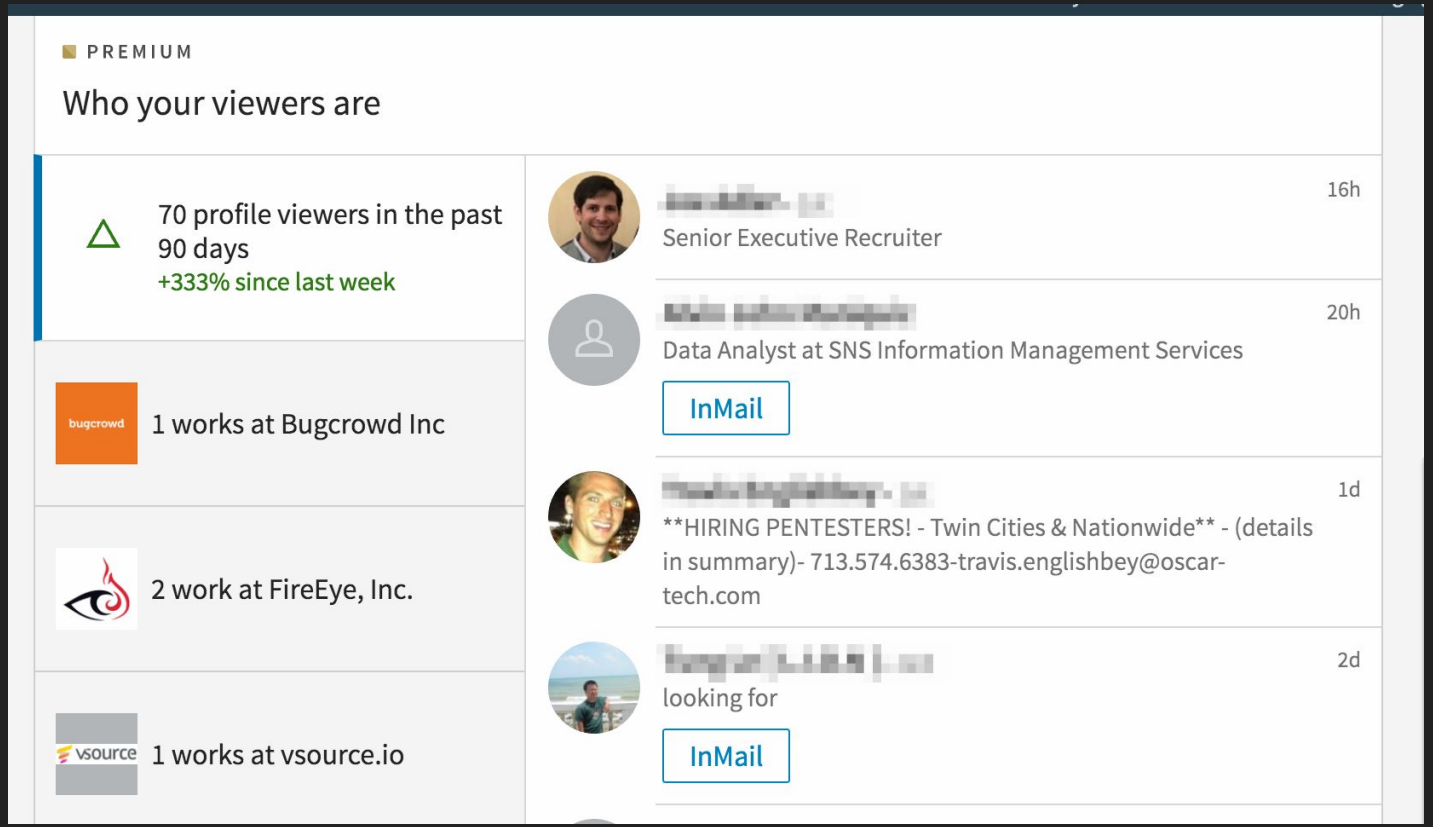
OSINT Gathering - Email Harvesting (Manually)

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



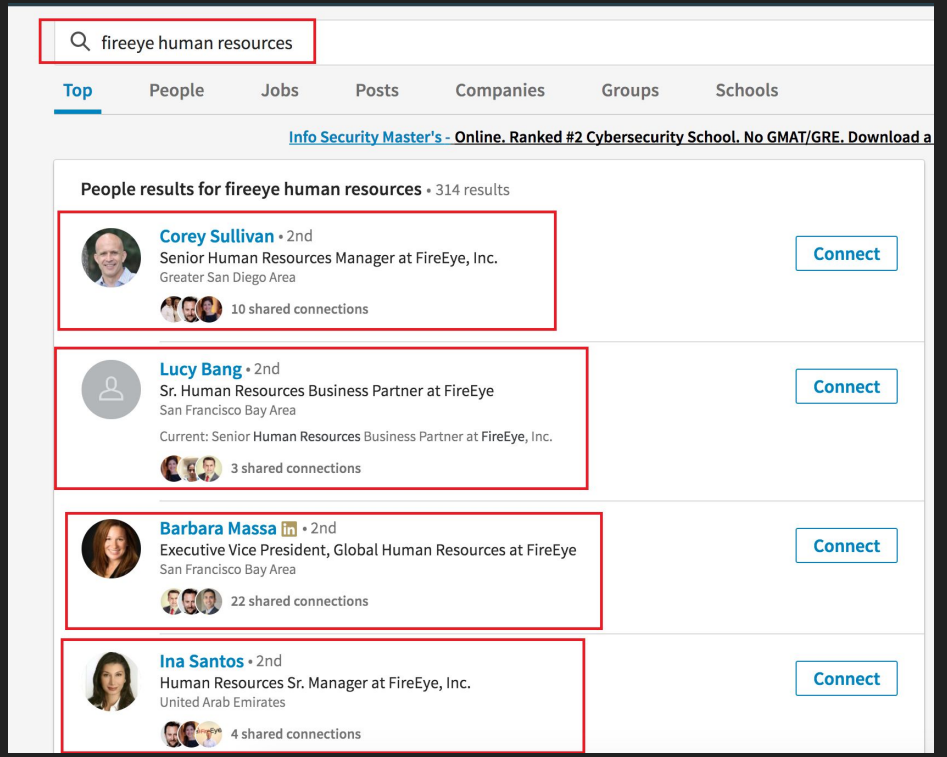
OSINT Gathering - Email Harvesting (Manually)

- Who's actually viewed your profile?



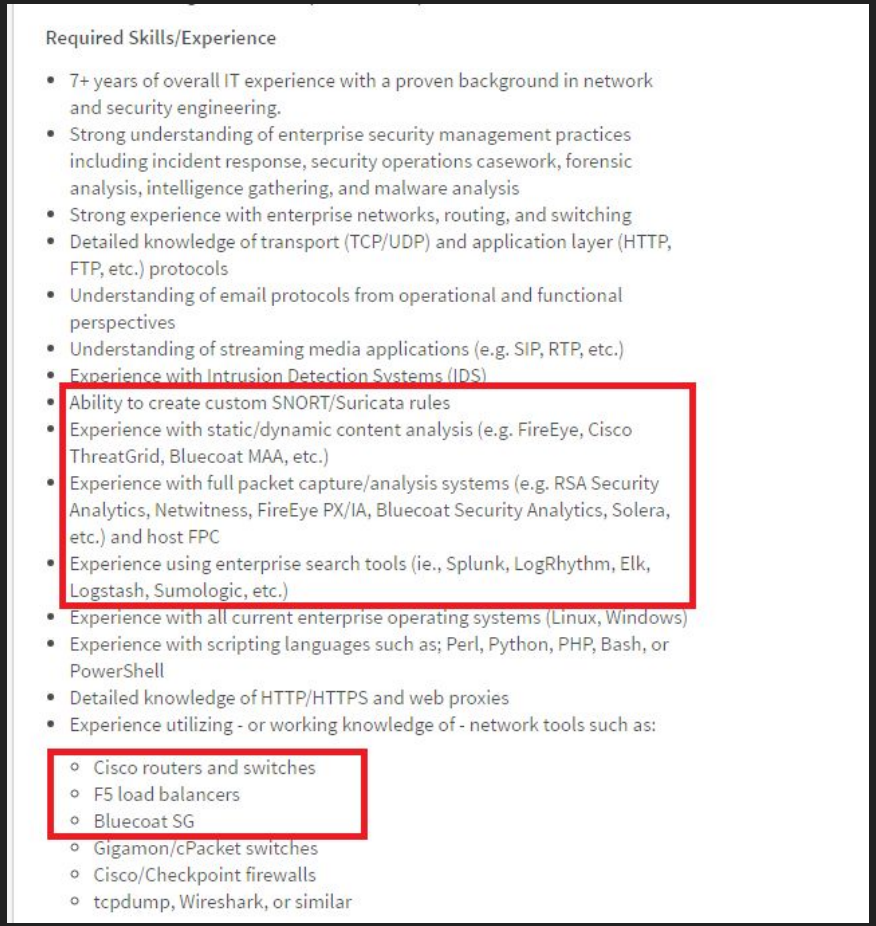
OSINT Gathering - Email Harvesting (Manually)

- 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



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

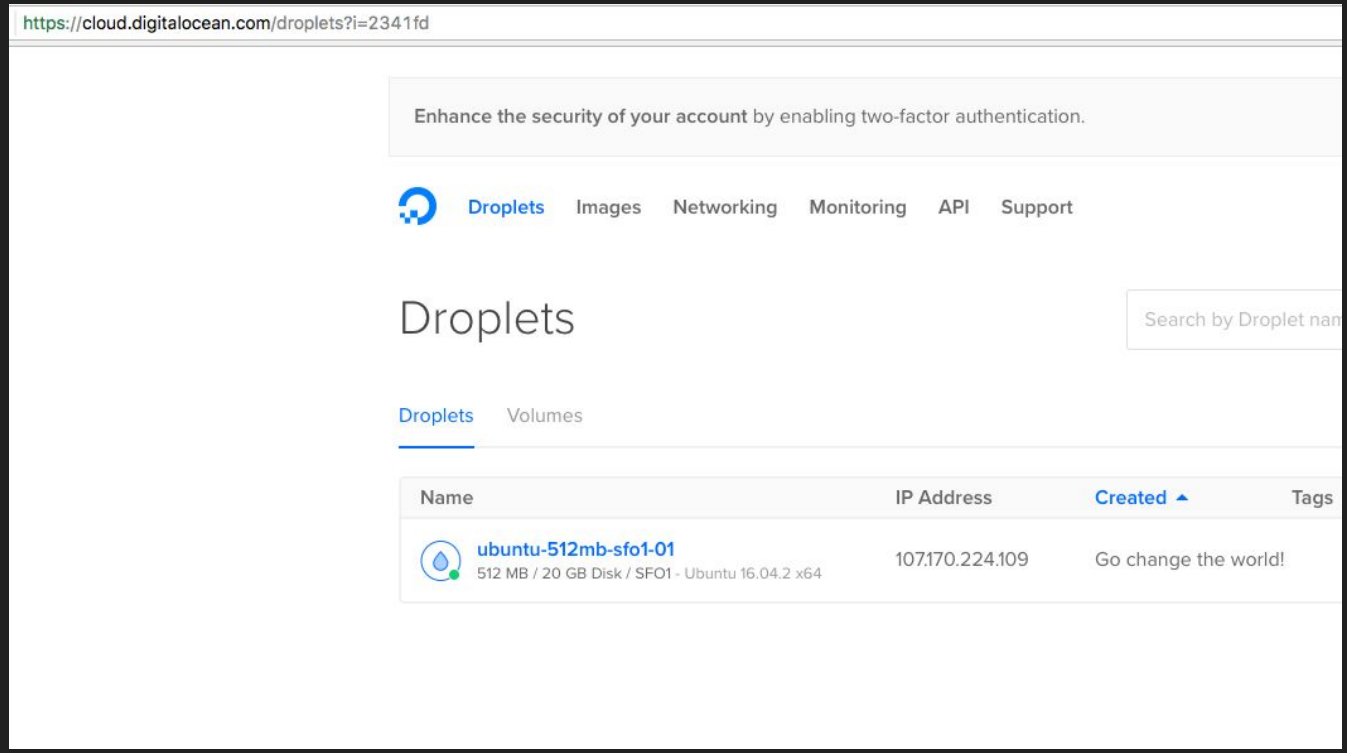
- “Uncategorized” domains are blocked in most organizations
- Luckily we can have our domains categorized!
  - BlueCoat (https://sitereview.bluecoat.com/sitereview.jsp)
  - Palo Alto (https://urlfiltering.paloaltonetworks.com/ChangeASite.jsp)
  - FortiGuard* (https://fortiguard.com/faq/wfratingsubmit)

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

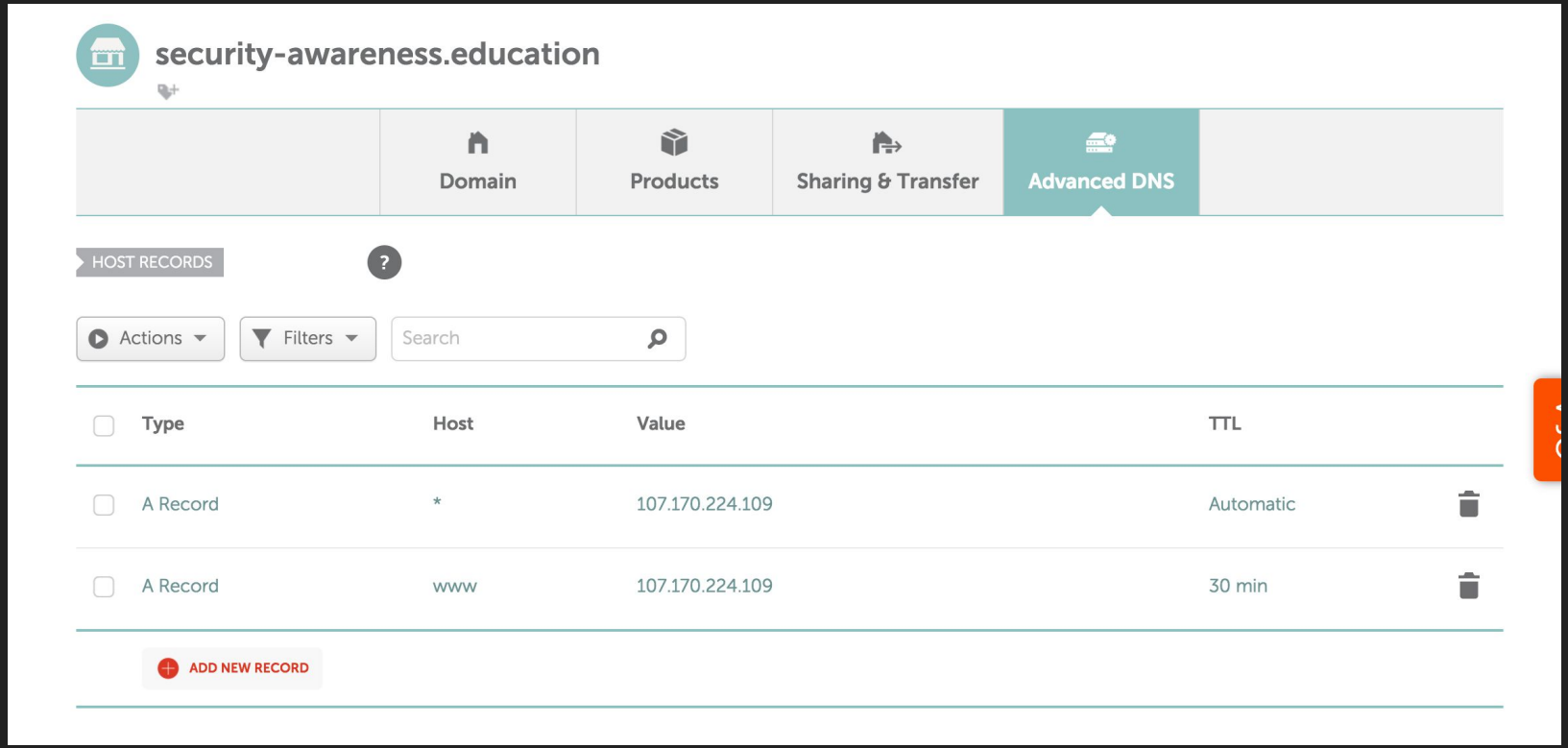
Defeating Web Proxies - Categorizing a Domain

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



Defeating Web Proxies - Categorizing a Domain

- Buy a domain and configure DNS for new VPS

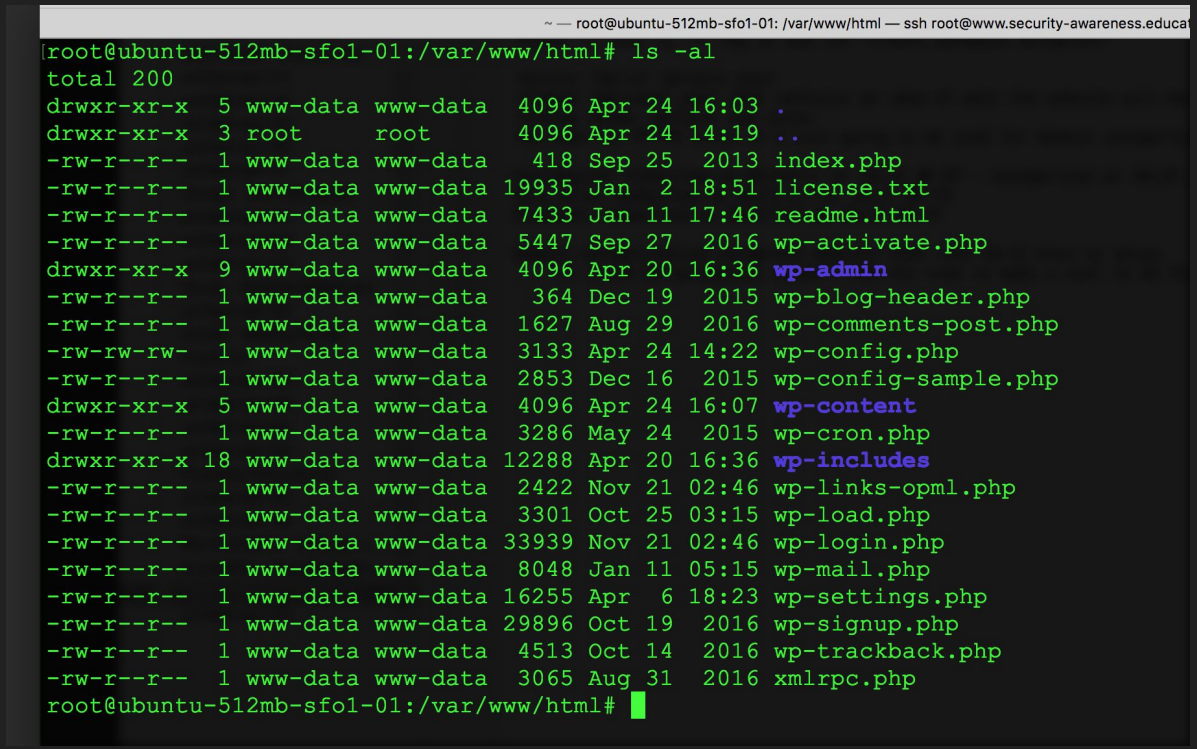


Defeating Web Proxies - Categorizing a Domain

- 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



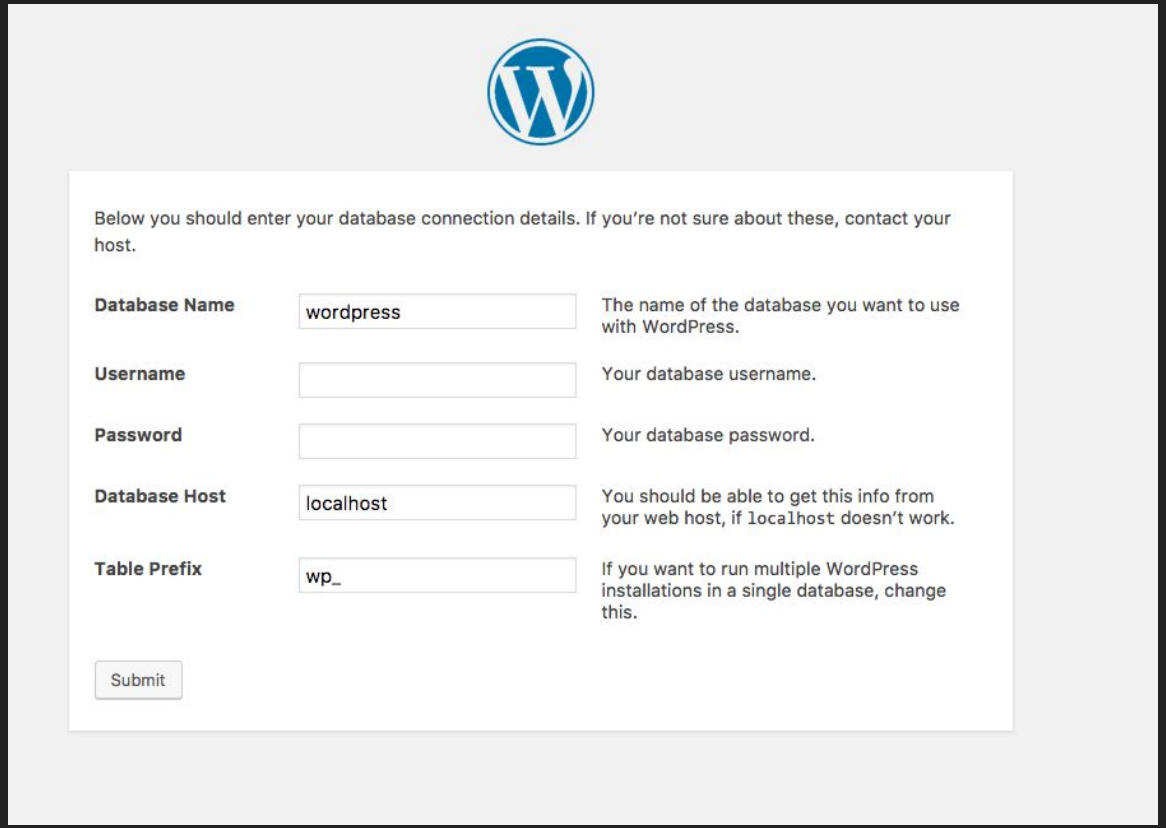
Defeating Web Proxies - Categorizing a Domain

- 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>
```

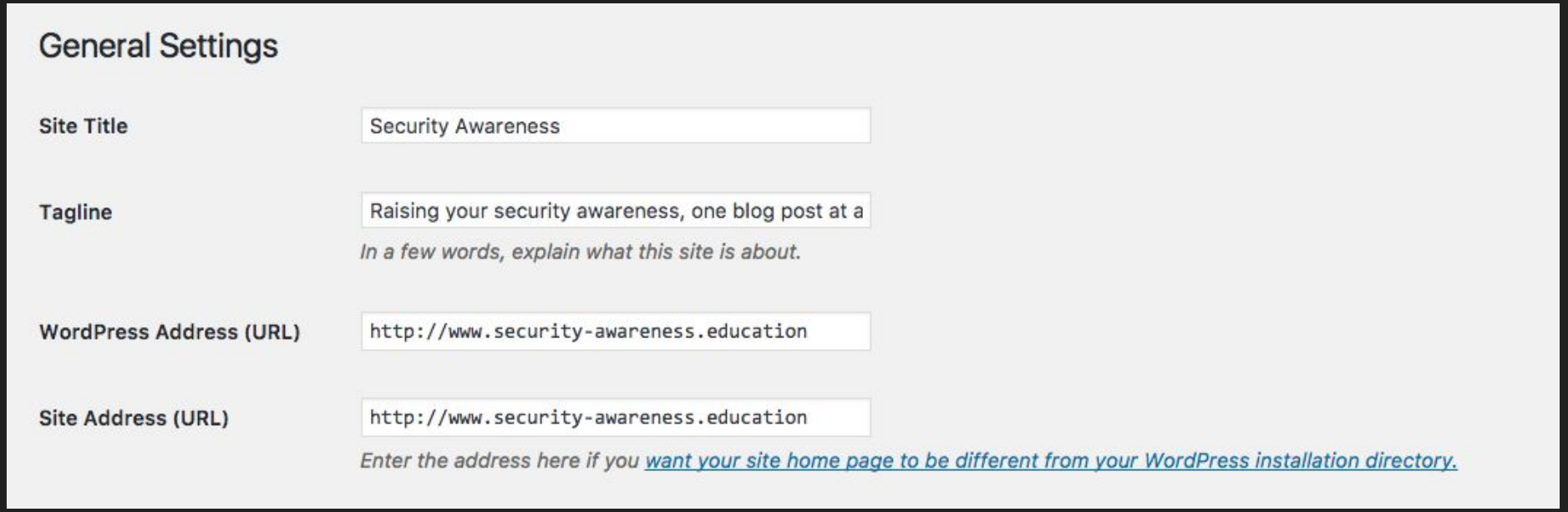
Defeating Web Proxies - Categorizing a Domain

- Run the WordPress install



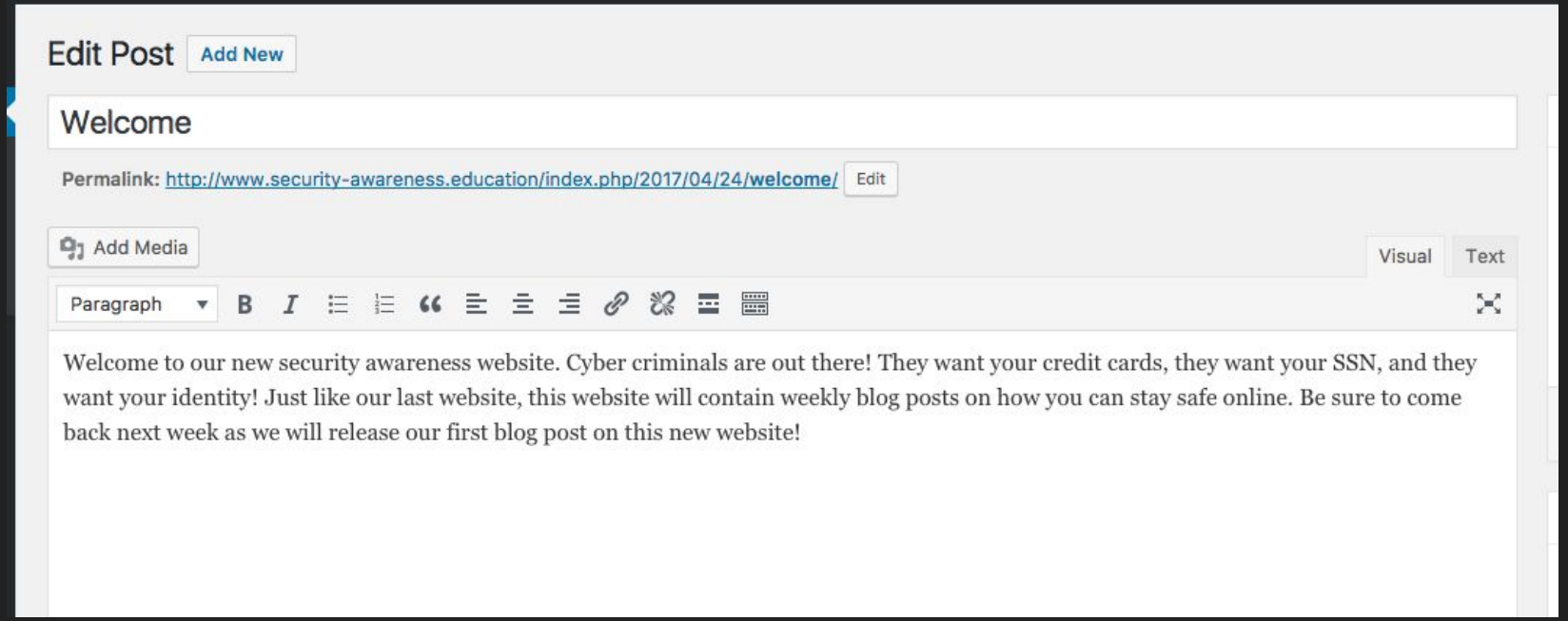
Defeating Web Proxies - Categorizing a Domain

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



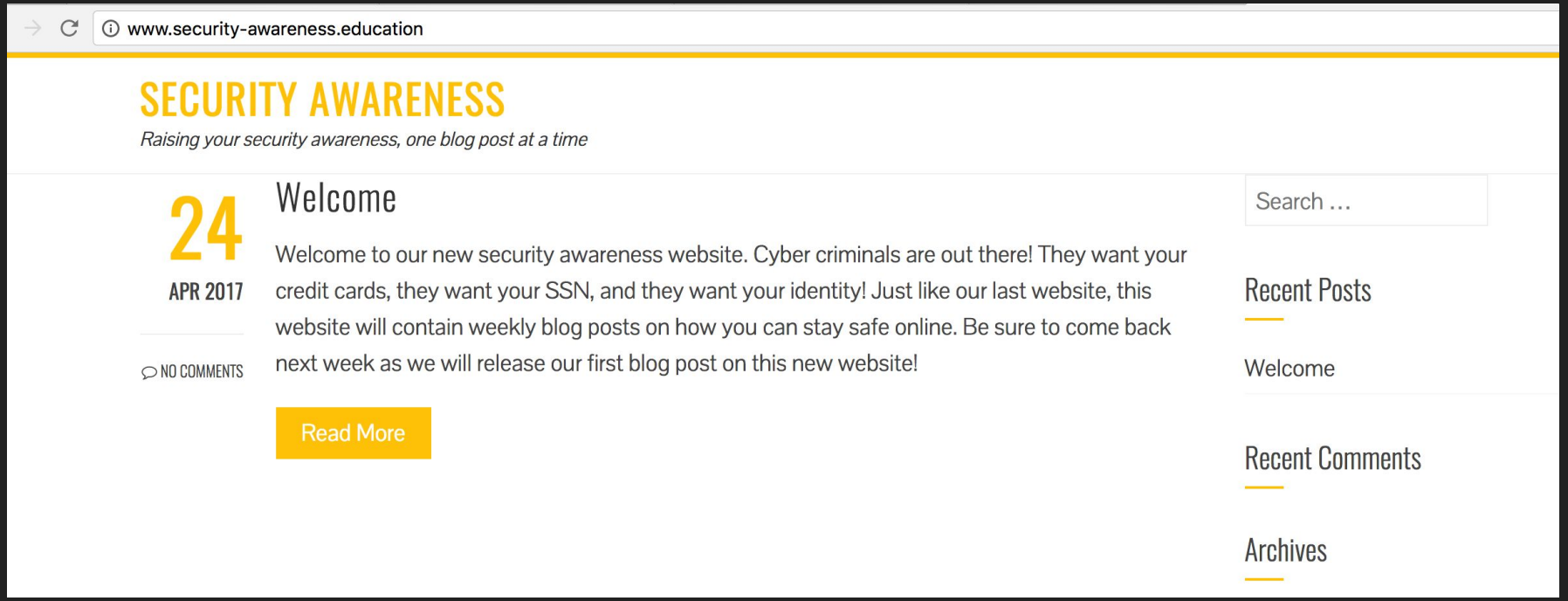
Defeating Web Proxies - Categorizing a Domain

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



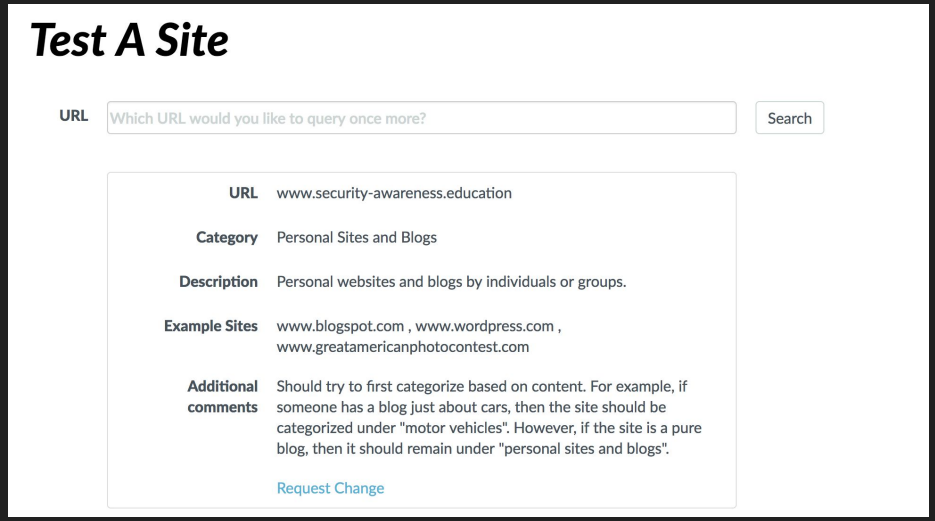
Defeating Web Proxies - Categorizing a Domain

- Final result ...now we submit and wait



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

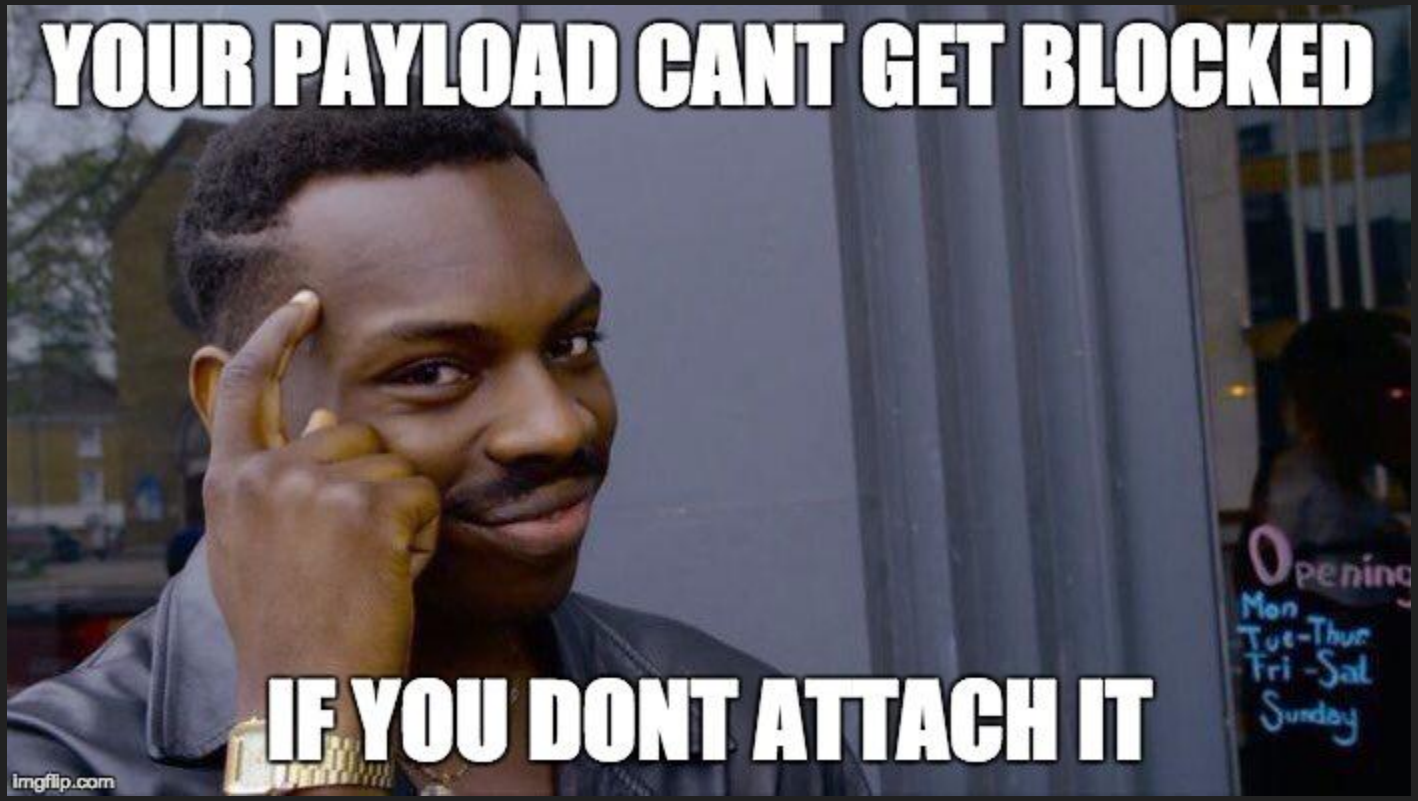


Defeating Email Protections

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

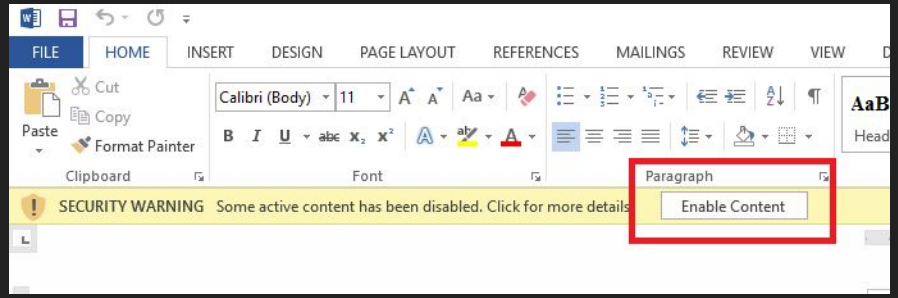
Payloads (Old School vs New School)

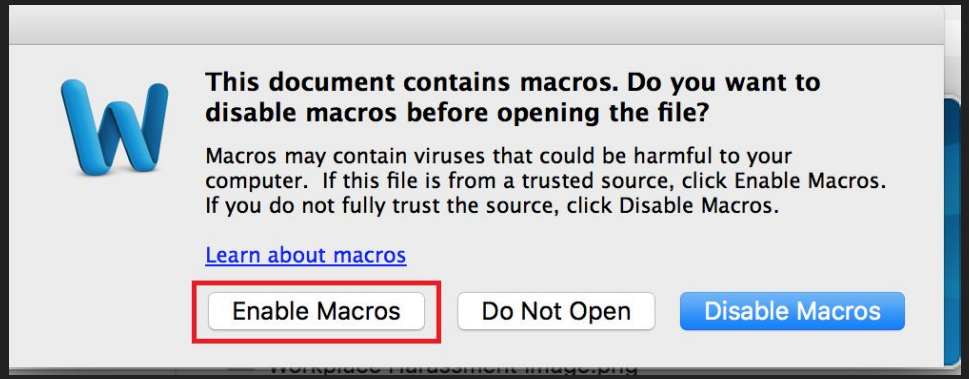
Payloads - Old School

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()





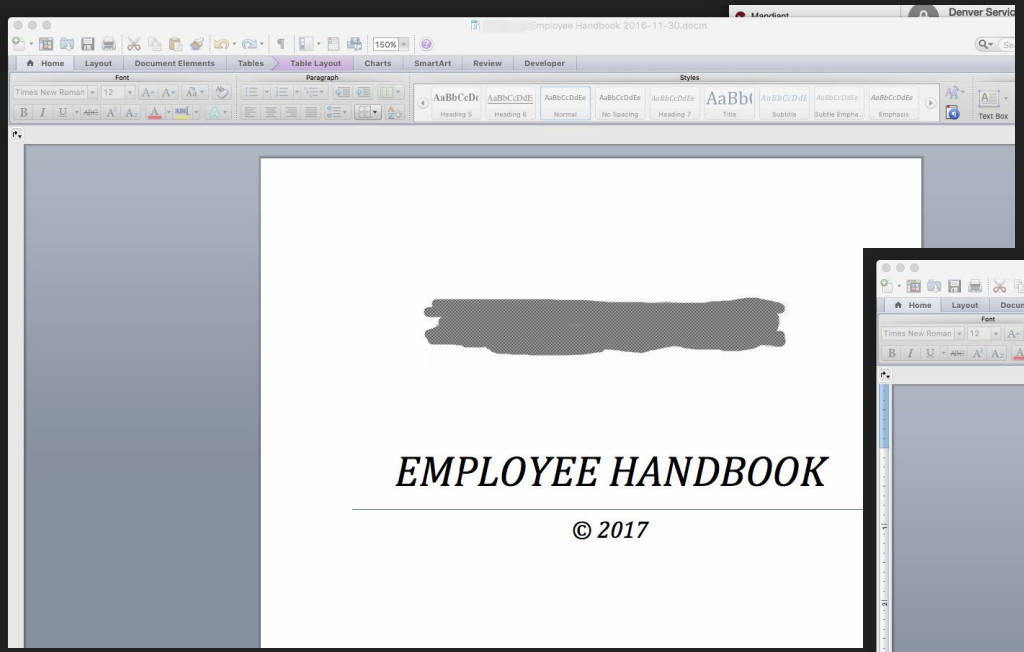
Payloads - Old School - Office Macros

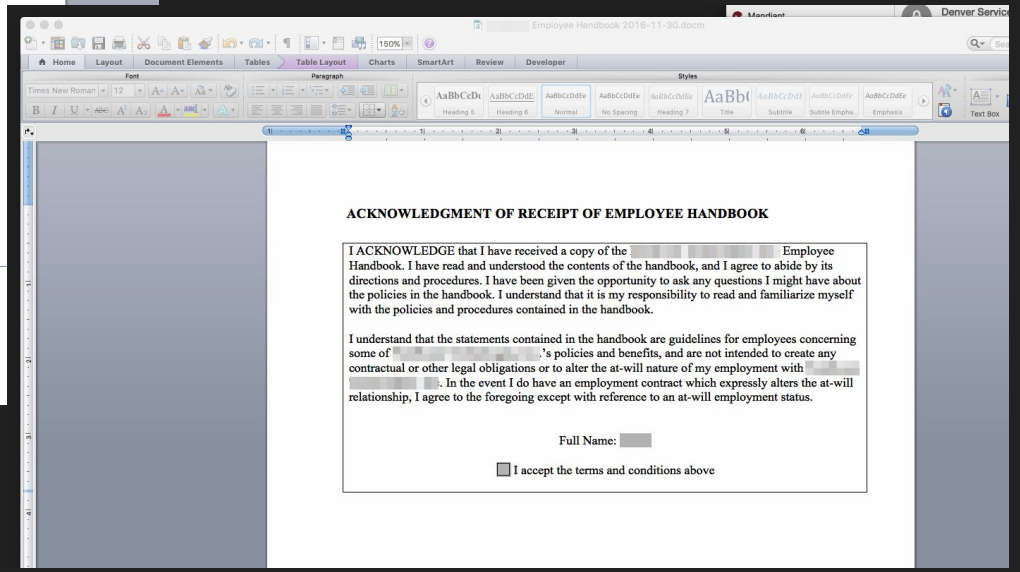
- Macros are likely to be detected if the document is attached to an email (not recommended) - Consider using an obfuscation tool:
  - MaliciousMacroGenerator (https://github.com/Mr-Un1k0d3r/MaliciousMacroGenerator)
- Dual-OS macros can be accomplished with a simple “if else” statement

```
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



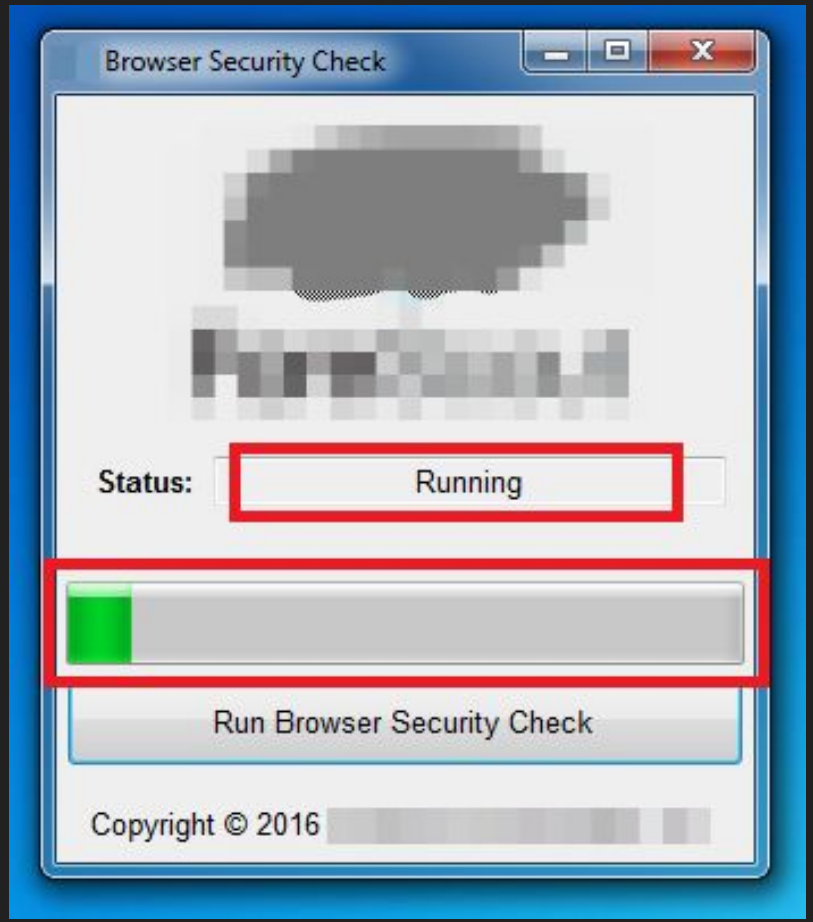


Payloads - Old School - Custom Executables

- 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)



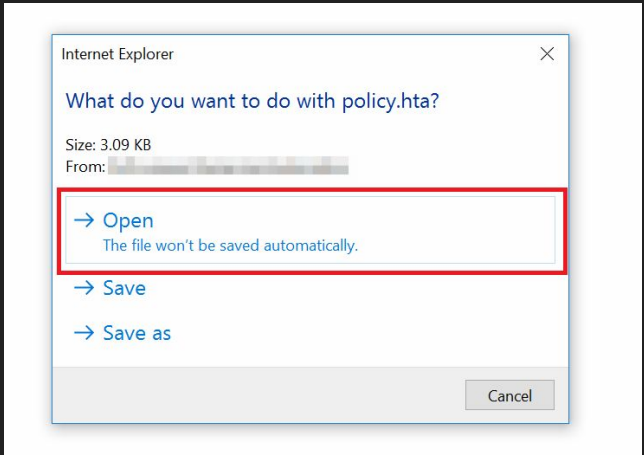
Payloads - New School

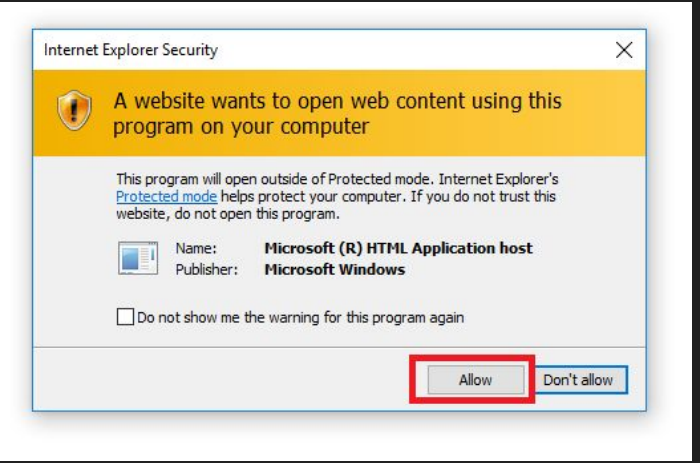
1. HTML Applications (HTAs)
2. ClickOnce

- 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/browsercheck.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

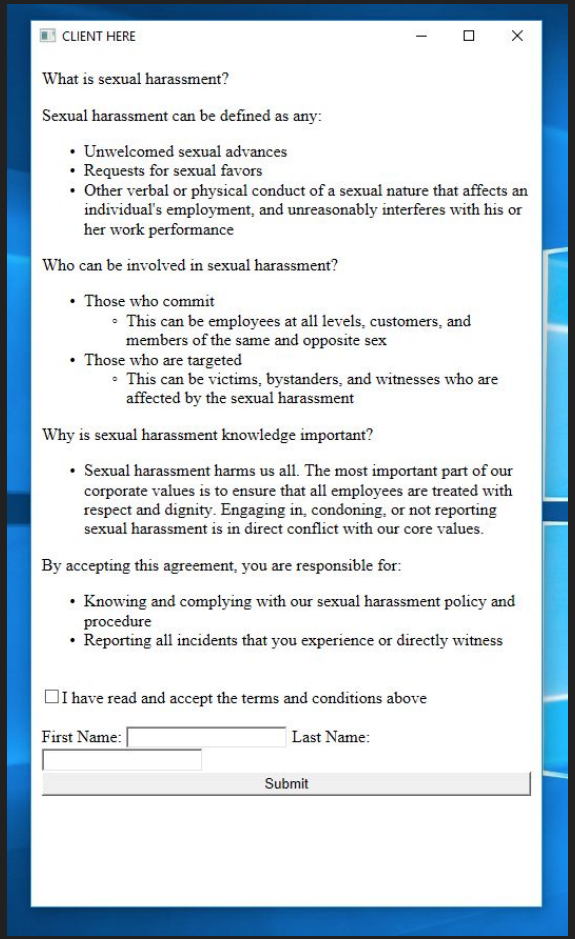
1 contributor

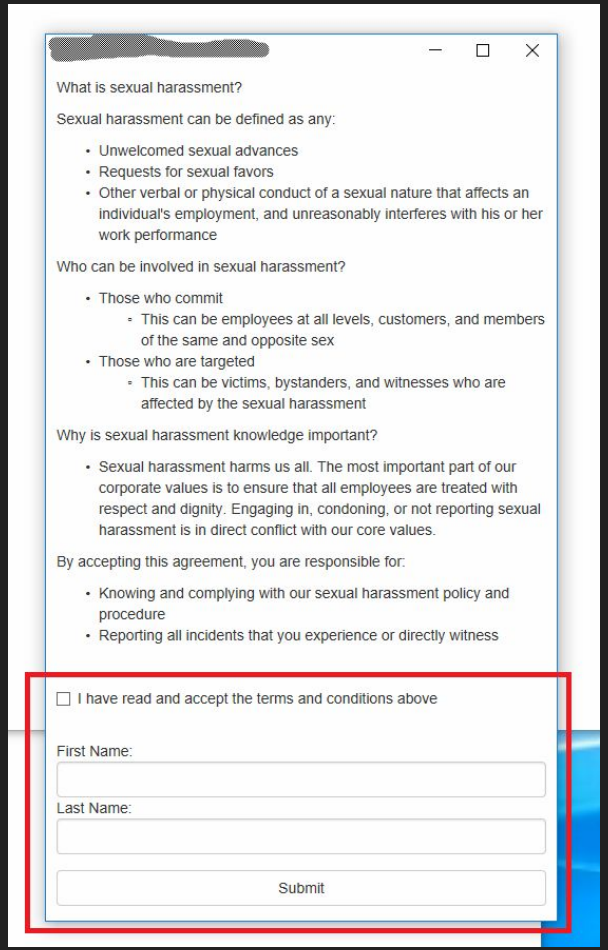
90 lines (79 sloc) | 3.02 KB Raw Blame History

```
<html>
        <head>
                <title>CLIENT HERE</title>
                <meta charset="utf-8">
                <meta http-equiv="x-ua-compatible" content="ie=9">
                <!-- CDN links -->
                <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css">
                <script src="https://ajax.googleapis.com/ajax/libs/jquery/1.12.4/jquery.min.js"></script>
                <script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js"></script>
                <script src="https://code.jquery.com/jquery-1.12.3.js"></script>
                <HTA:APPLICATION
                        SCROLL="auto"
                        SINGLEINSTANCE="yes"
                        CAPTION="yes"
                        ICON=""
                >
        </head>

        <body style="margin: 10px;">
                <!-- This script will put the HTA document in the foreground and make the window 500x850 -->
                <script language="vbscript">
                        window.resizeTo 500, 850
                        window.focus()
                </script>

                <script language="VBScript">
                        Set oShell = CreateObject ("Wscript.Shell")
                        Dim strArgs
                        strArgs = "powershell.exe"
                        oShell.Run strArgs, 0, false
                </script>

```

Payloads - New School - HTML Applications (HTAs)

- Sample payload (with Bootstrap and without Bootstrap)



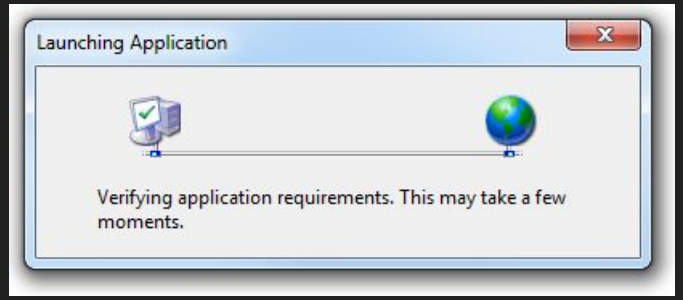


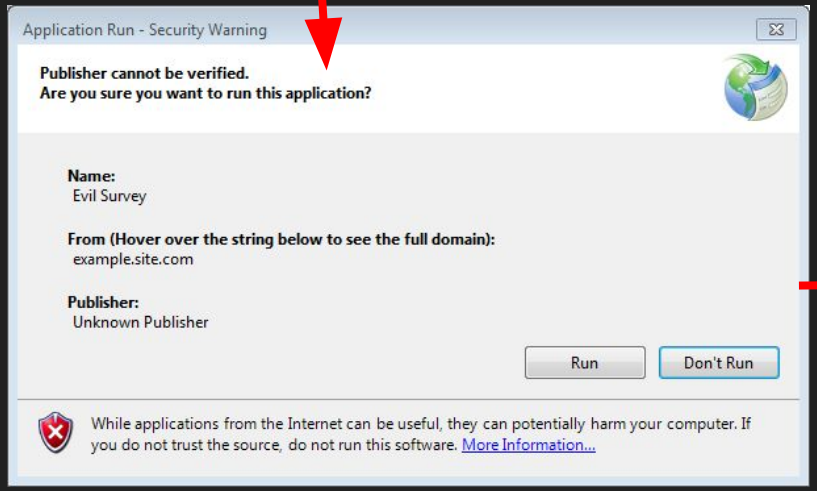
Payloads - New School - ClickOnce

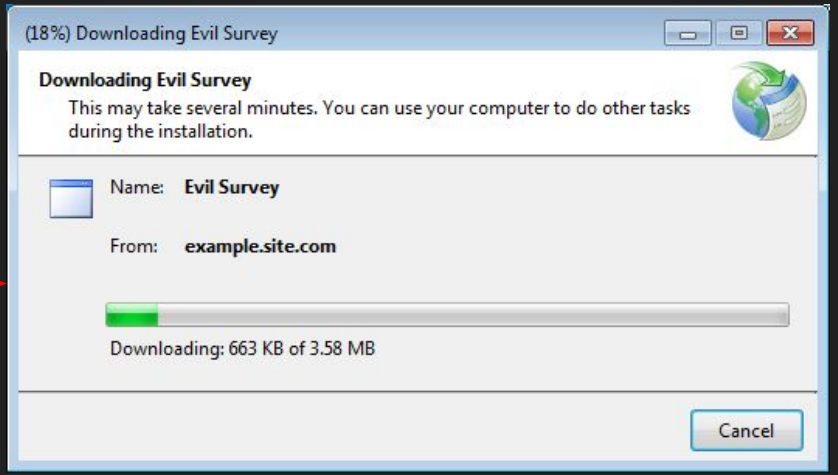
- “ClickOnce is a Microsoft technology that enables the user to install and run a Windows-based smart client application by clicking a link in a web page.” - Wikipedia
  - **TLDR:** Run .NET applications by clicking a link
- **Blog:** https://blog.netspi.com/all-you-need-is-one-a-clickonce-love-story
- 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

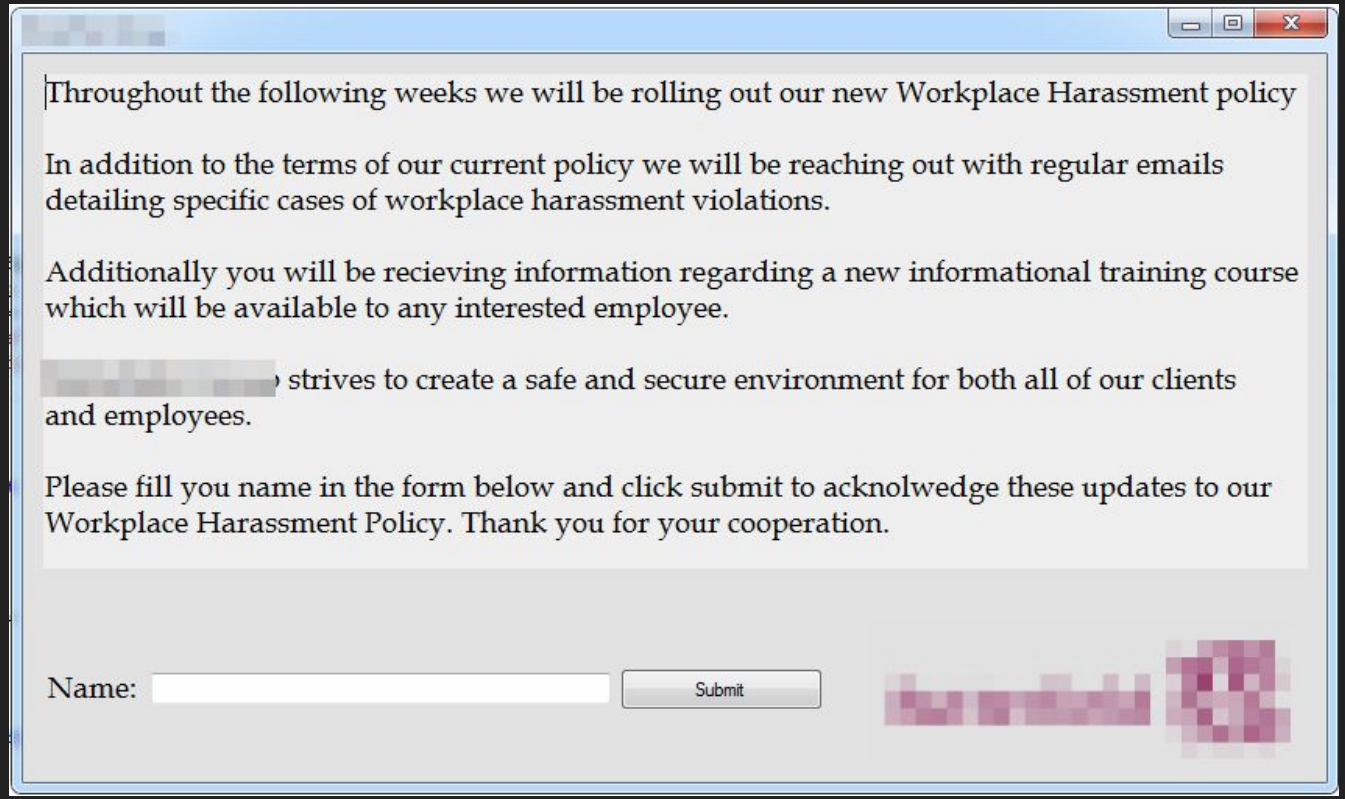






Payloads - New School - ClickOnce

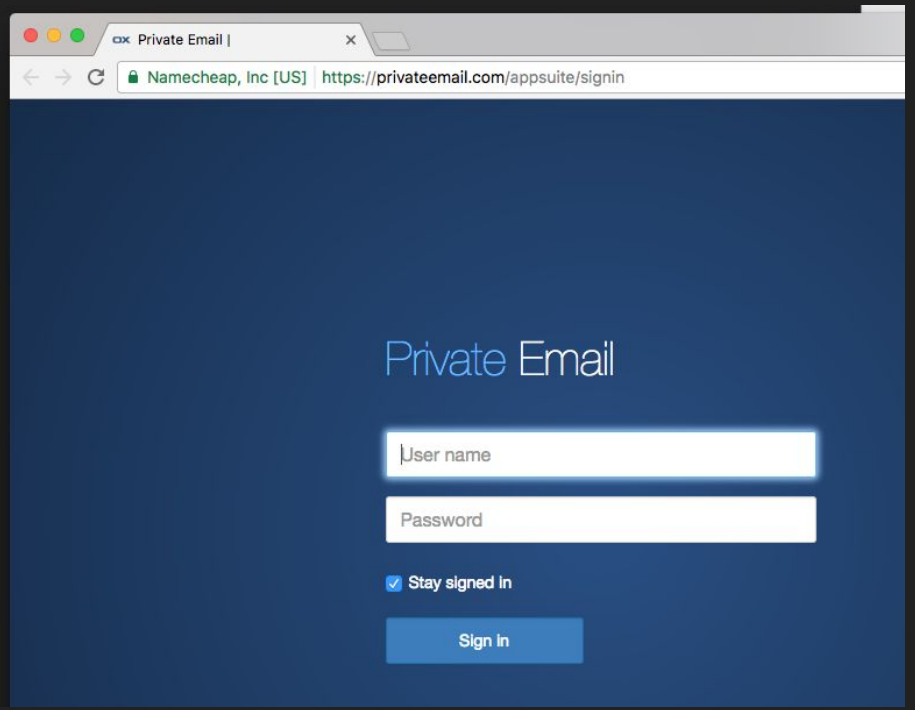
- Sample payload



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

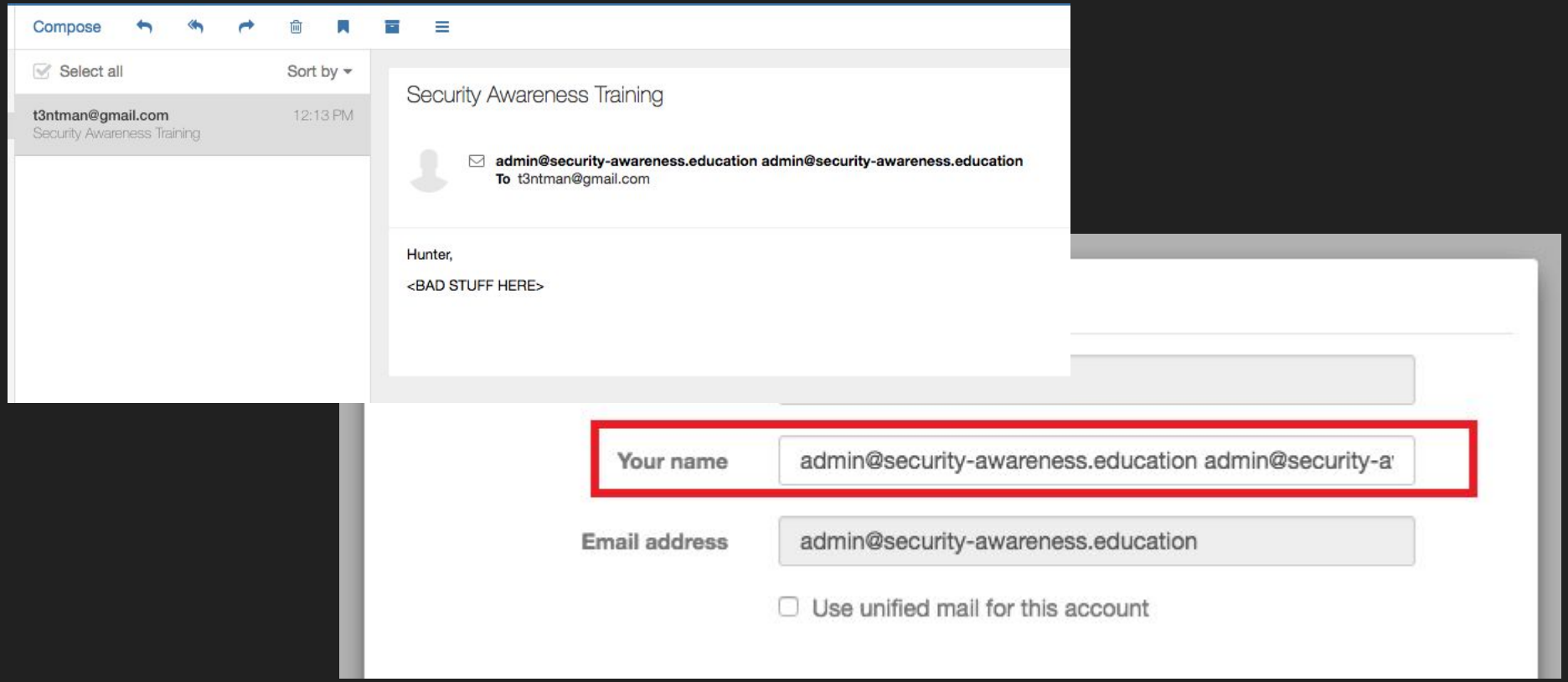


Email Delivery and Tracking - Delivery

- OMFG send yourself a test email first!

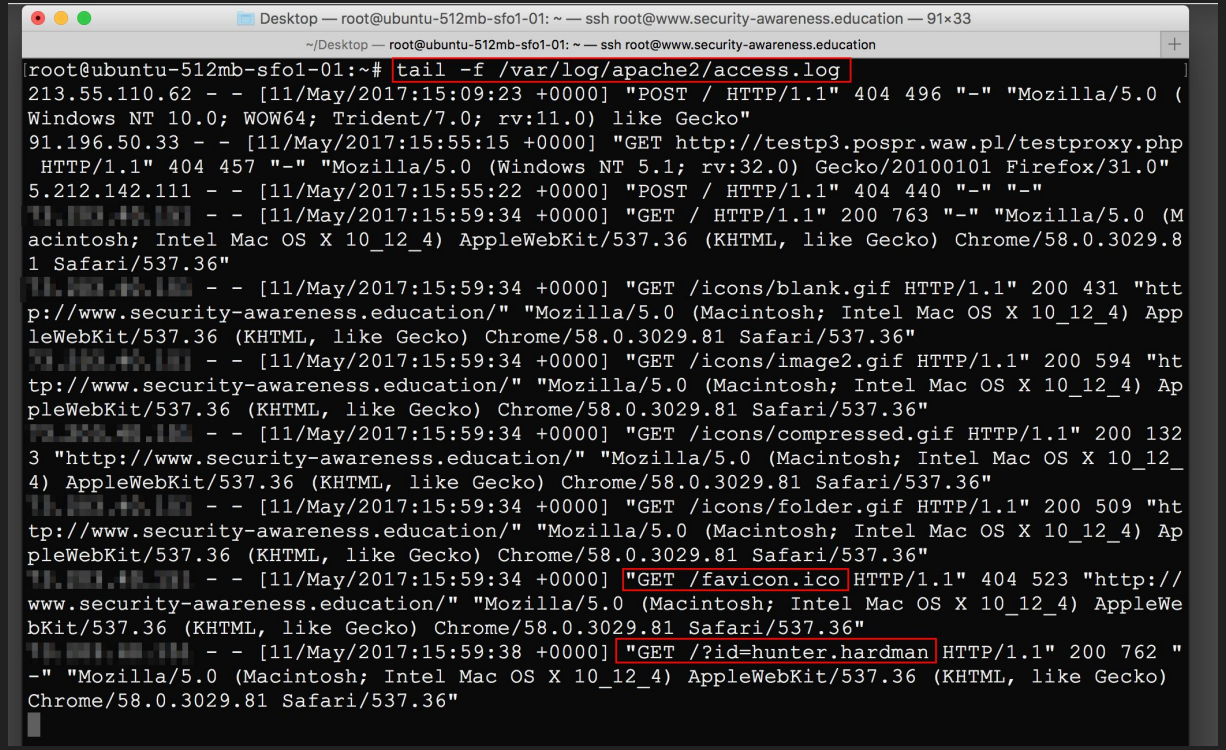
Email Delivery and Tracking - Delivery

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



Email Delivery and Tracking - Tracking

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



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)

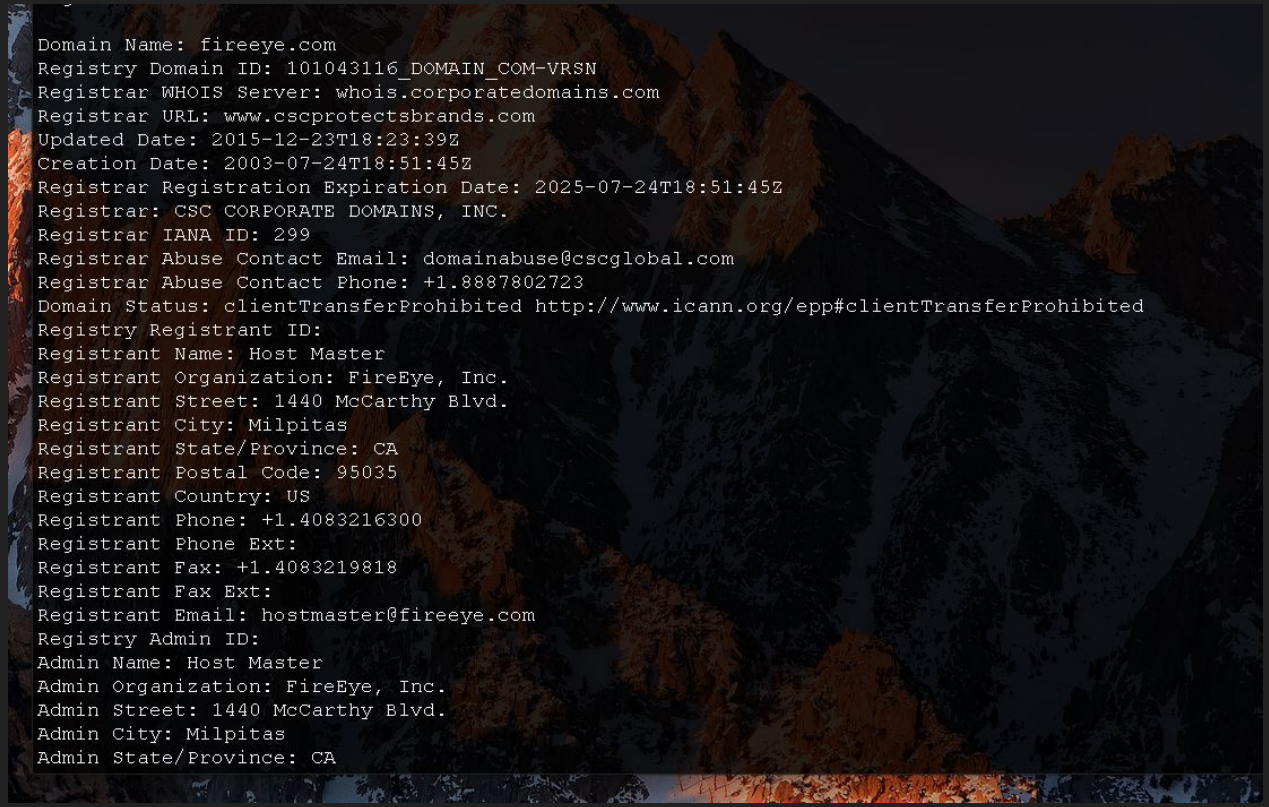
Rookie Mistakes - Whois Protection

- 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

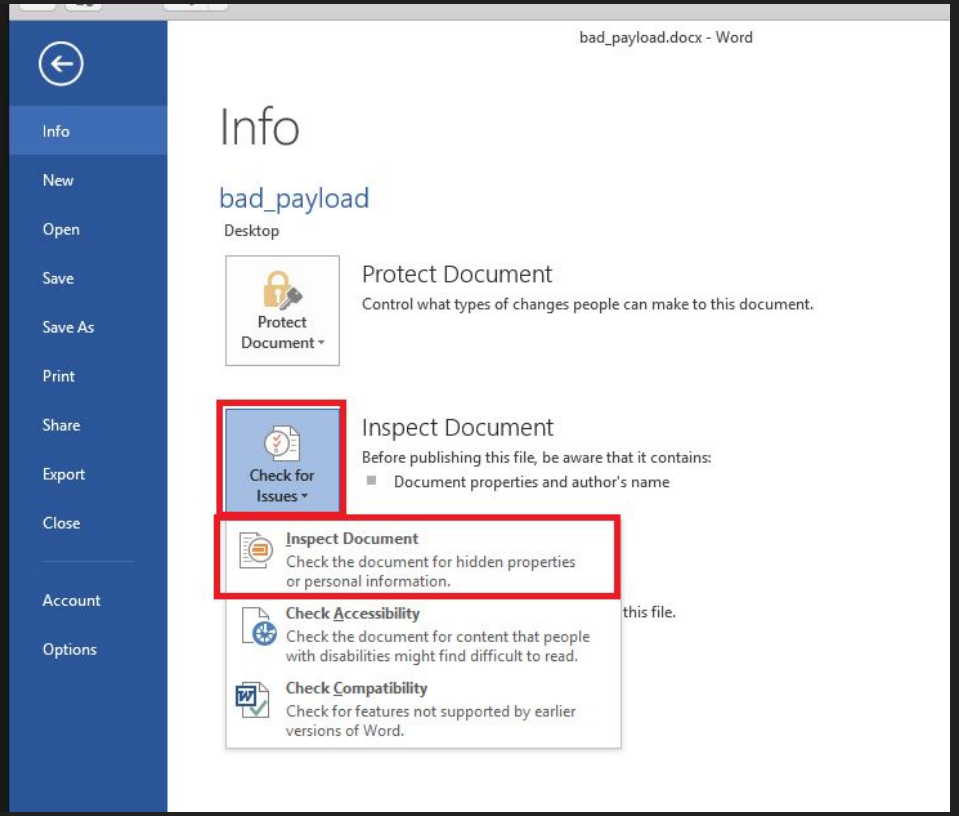


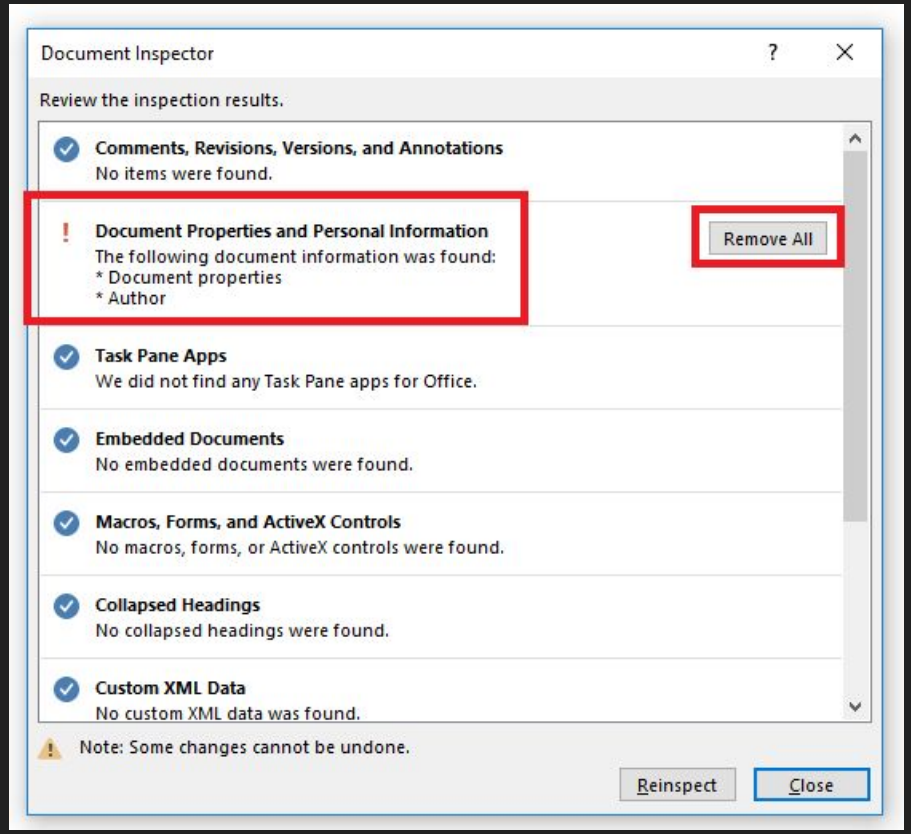
Rookie Mistakes - Metadata

- 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

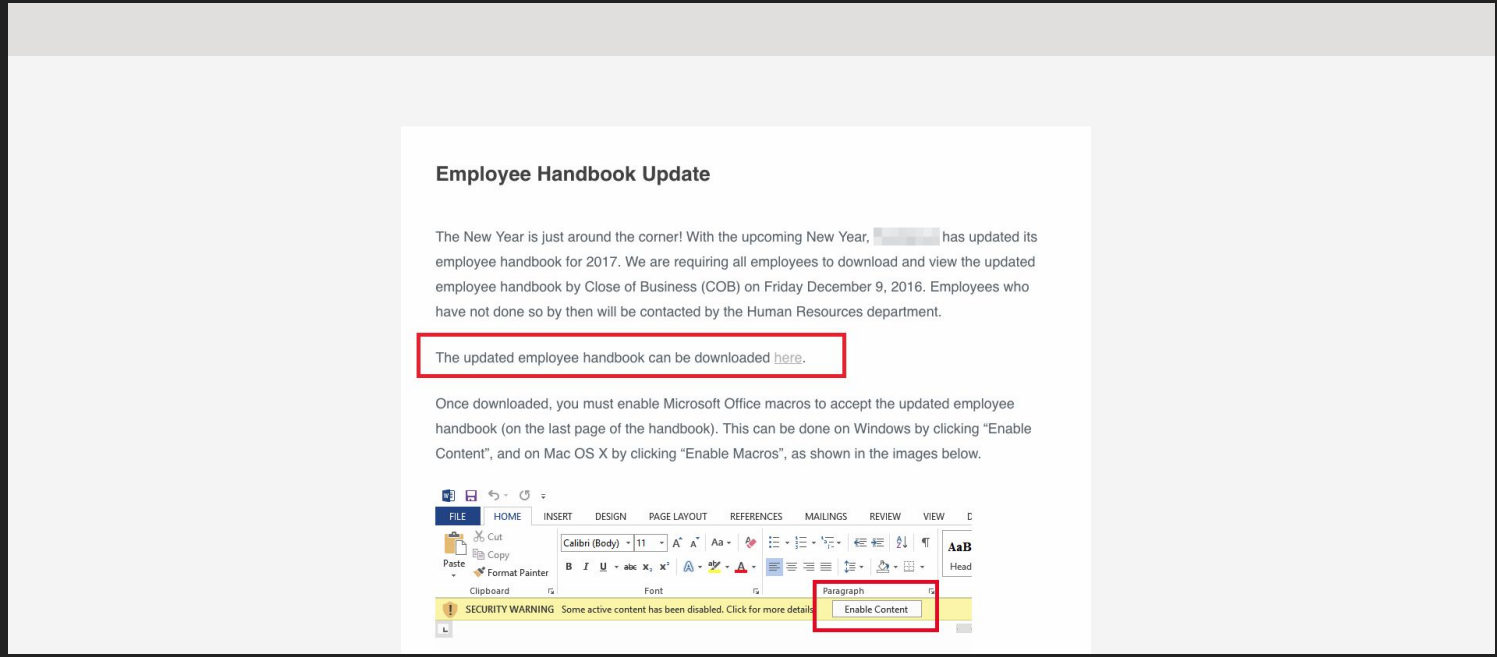
- Payload execution campaign
- Pretext
  - Posed as someone (David) from the Human Resources department, and contacted people via phone informing them about a recent update to the employee handbook
  - Gave them the link hosting the new “employee handbook” while on the phone
  - Said they are on a list 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



Employee Handbook Update

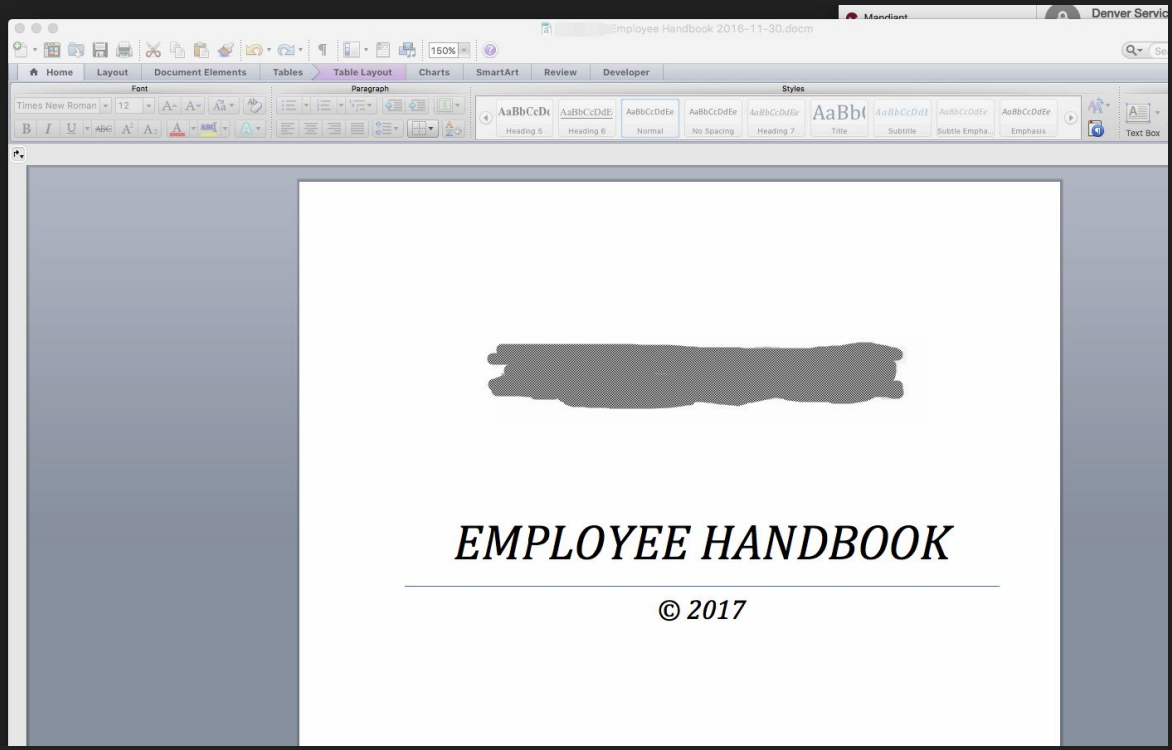
The New Year is just around the corner! With the upcoming New Year, [redacted] has updated its employee handbook for 2017. We are requiring all employees to download and view the updated employee handbook by Close of Business (COB) on Friday December 9, 2016. Employees who have not done so by then will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

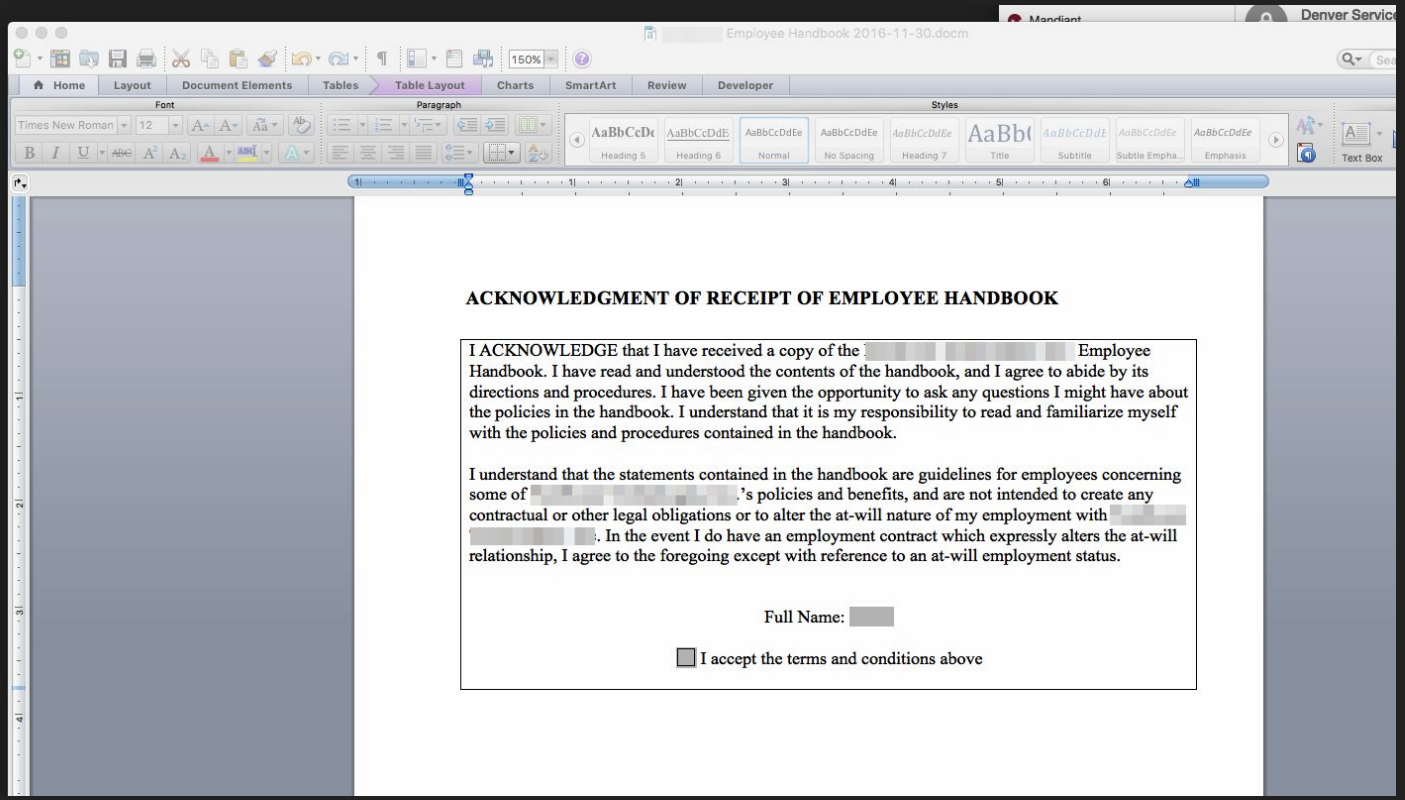
Successful Campaigns - Employee Handbook Update

- 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



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
To David

12:14 PM

Quick reply Reply All Forward Delete

2 attachments View Download Save to Drive

Got it!

Just downloaded and accepted

From: David <david.l@hr-f.com>
Reply-To: David <david.l@hr-t.com>
Date: Thursday, December 8, 2016 at 12:05 PM
To: Andrea <andrea.@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-.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
Sr. Employee Coordinator - Human Resources
Mobile:

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

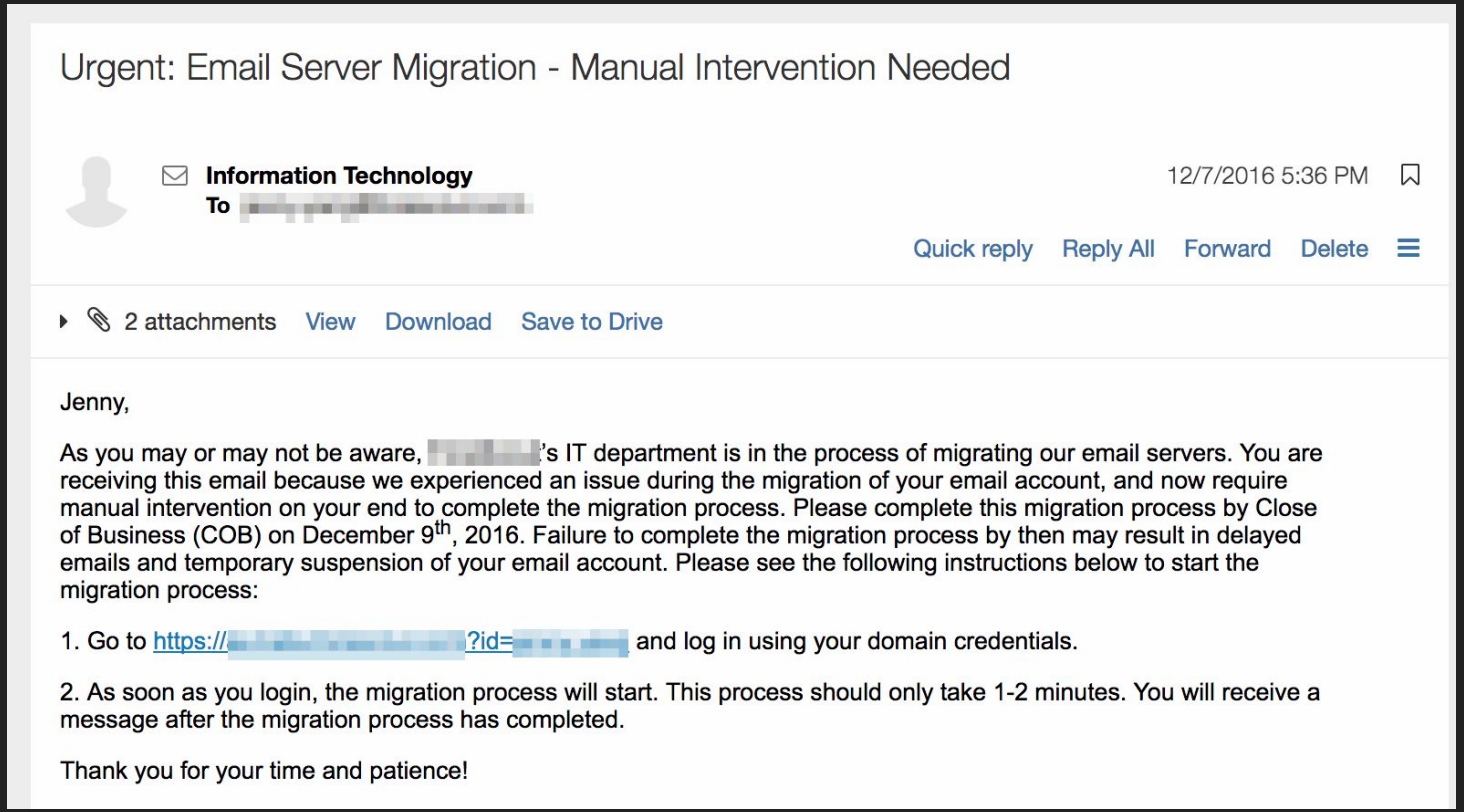
Second Campaign - Email Server Migration

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
To [redacted]

12/7/2016 5:36 PM

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:

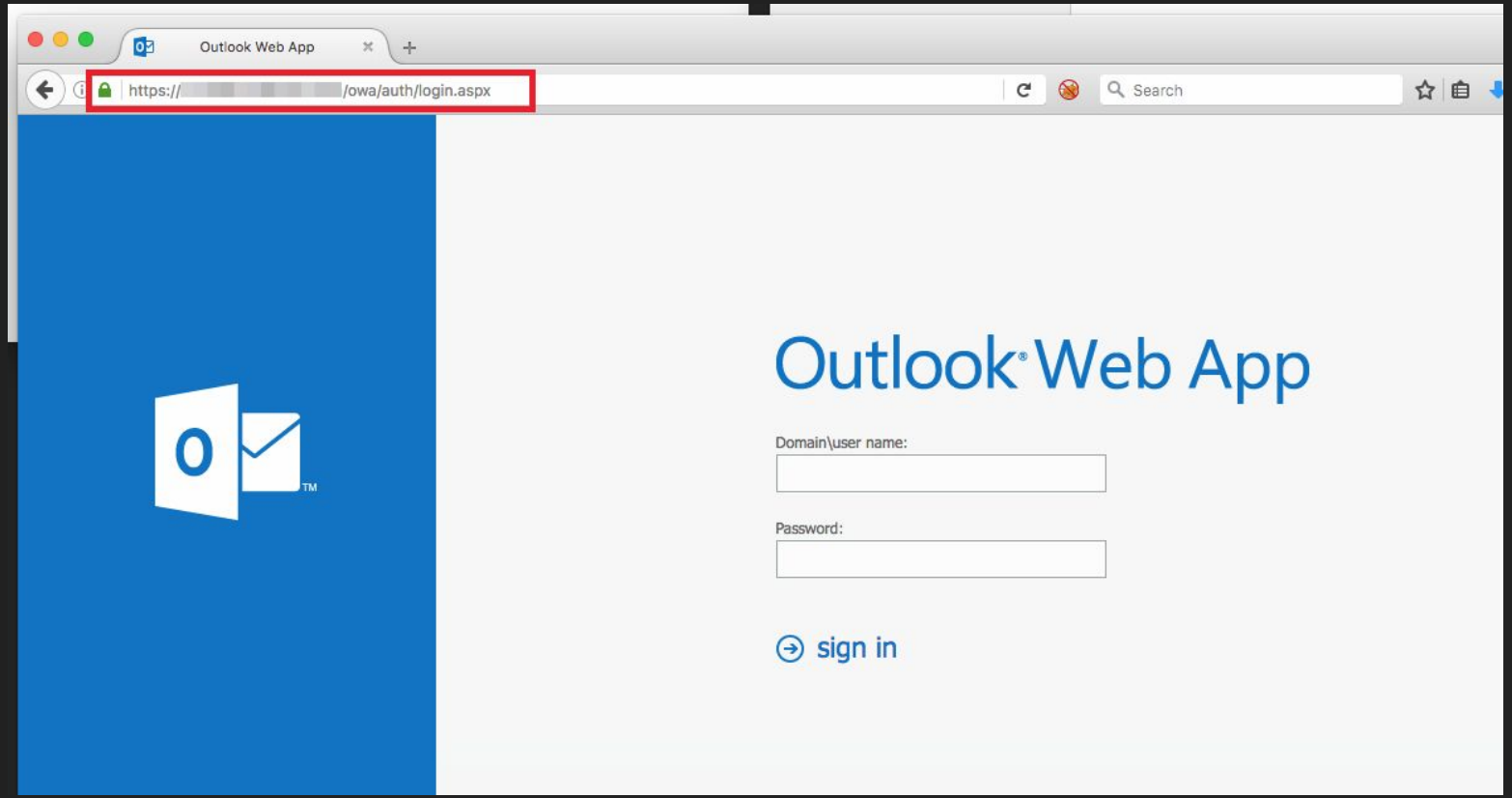
1. Go to https://[redacted]?id=[redacted] and log in using your domain credentials.

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!

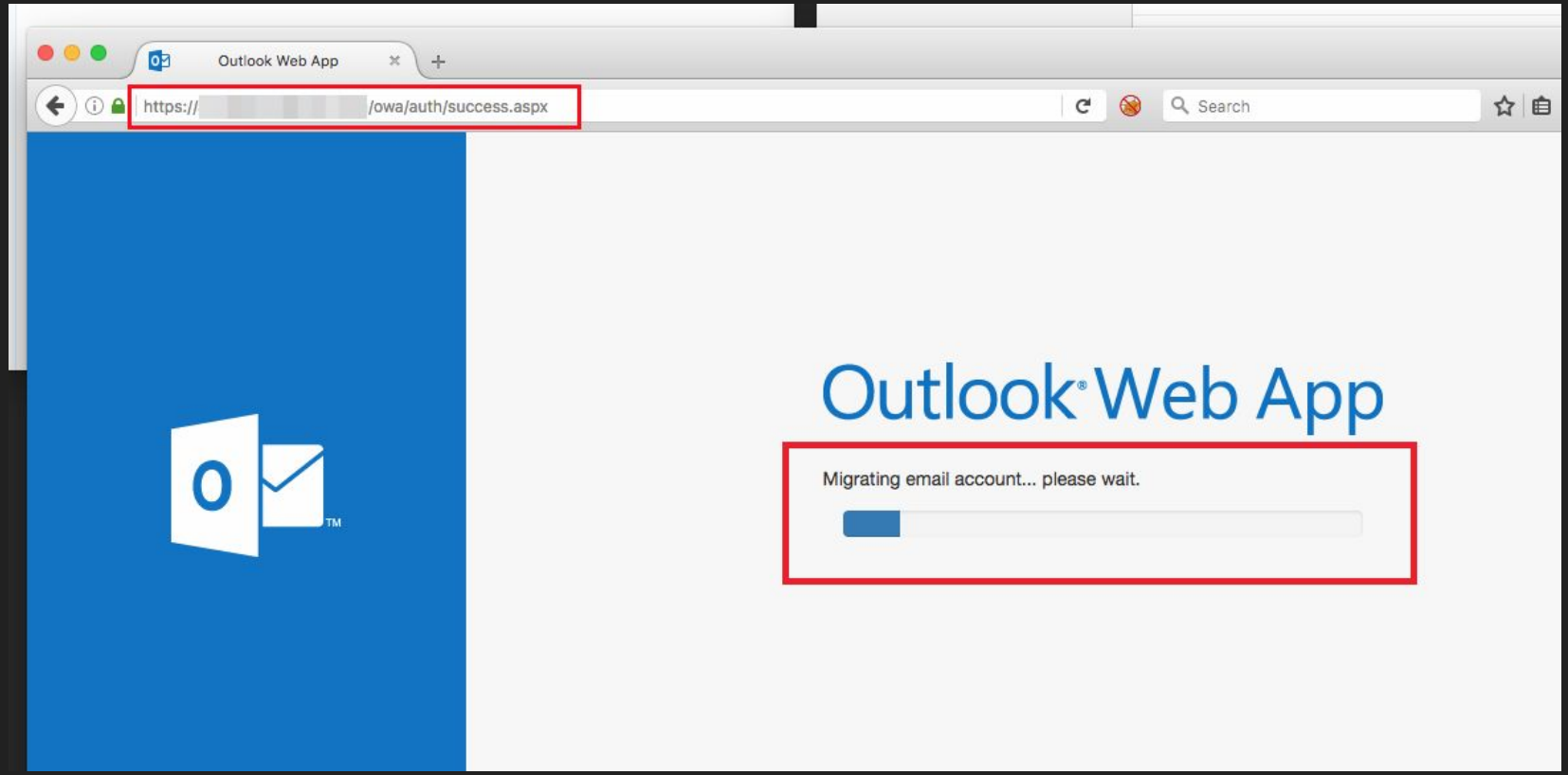
Successful Campaigns - Email Server Migration

- Login page designed to capture submitted credentials



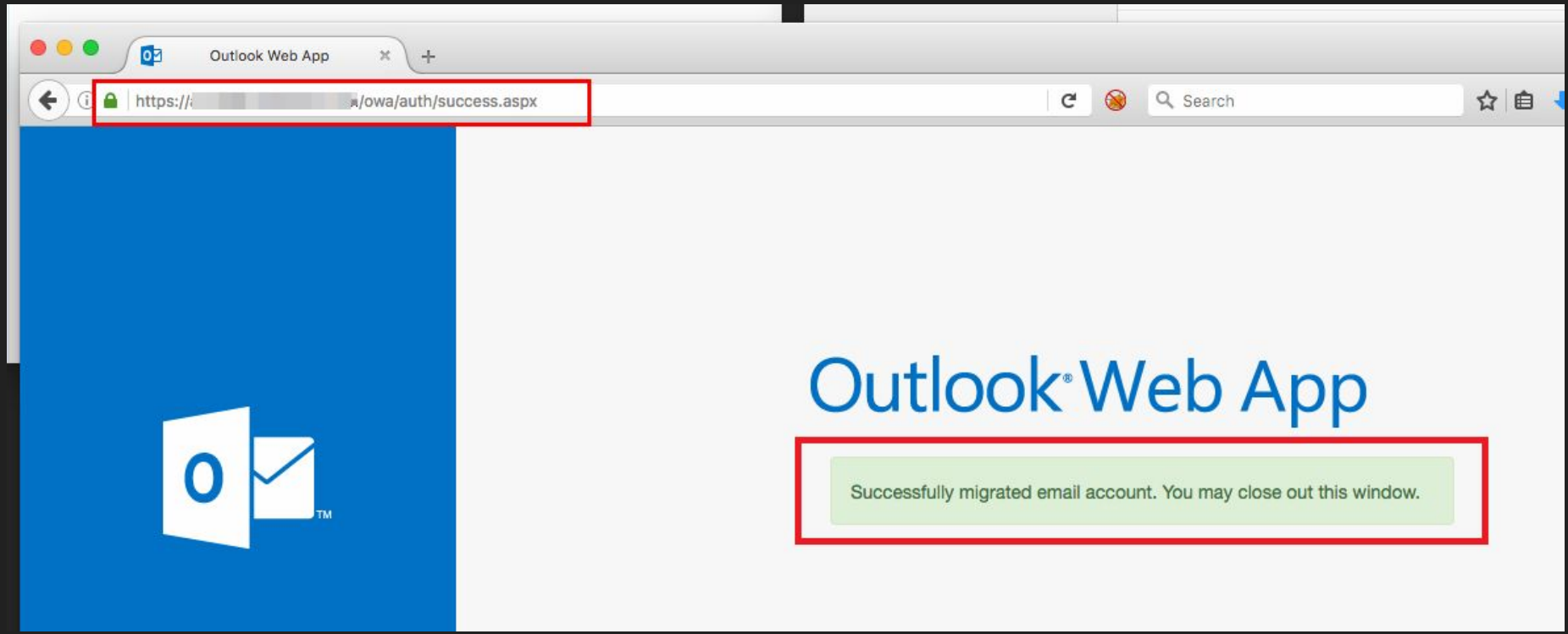
Successful Campaigns - Email Server Migration

- 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>,

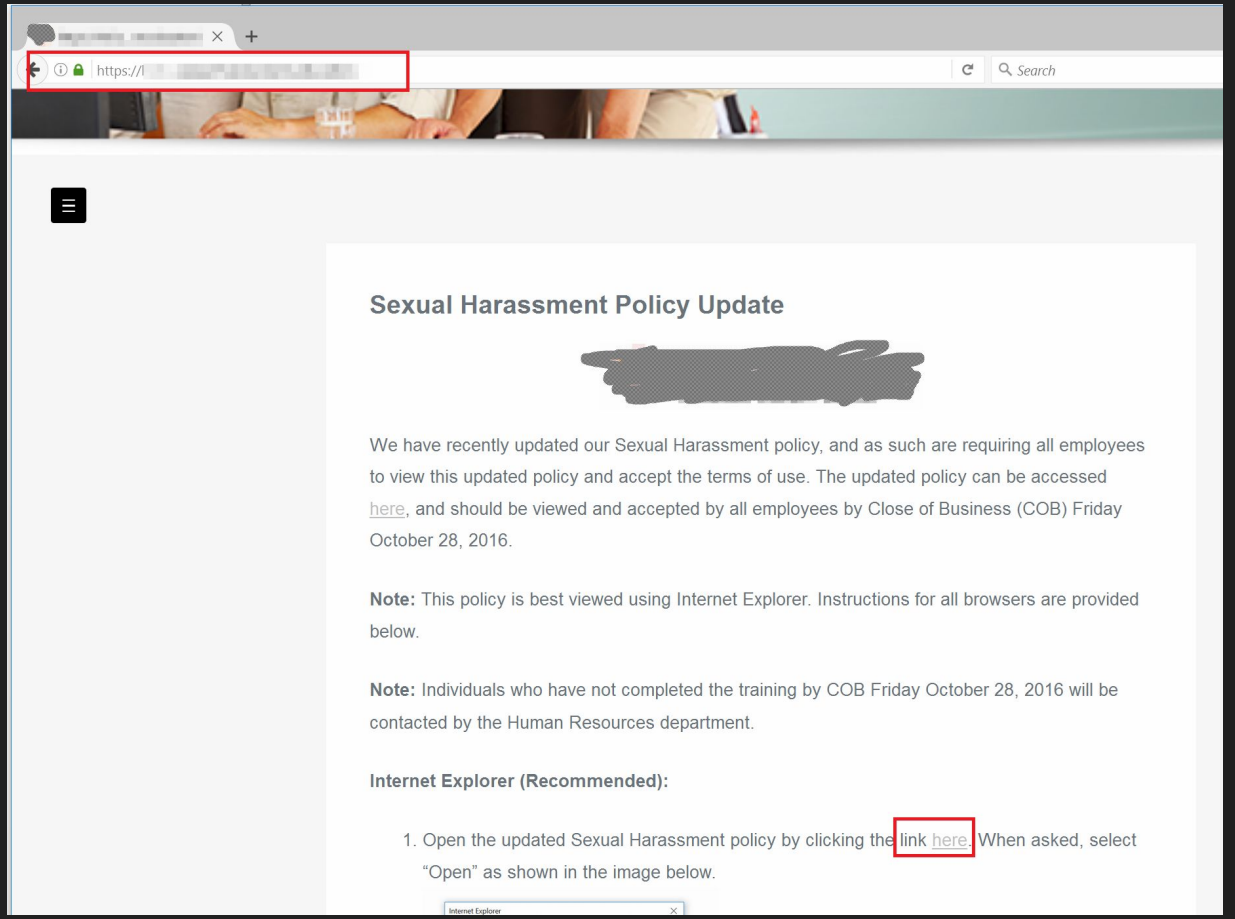
This is a notice to all employees. We have recently updated our Sexual Harassment policy, and as such are requiring all employees to view and acknowledge this updated policy. We are requiring all employees to view and acknowledge this updated policy by Close of Business (COB) Friday October 28, 2016.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

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.

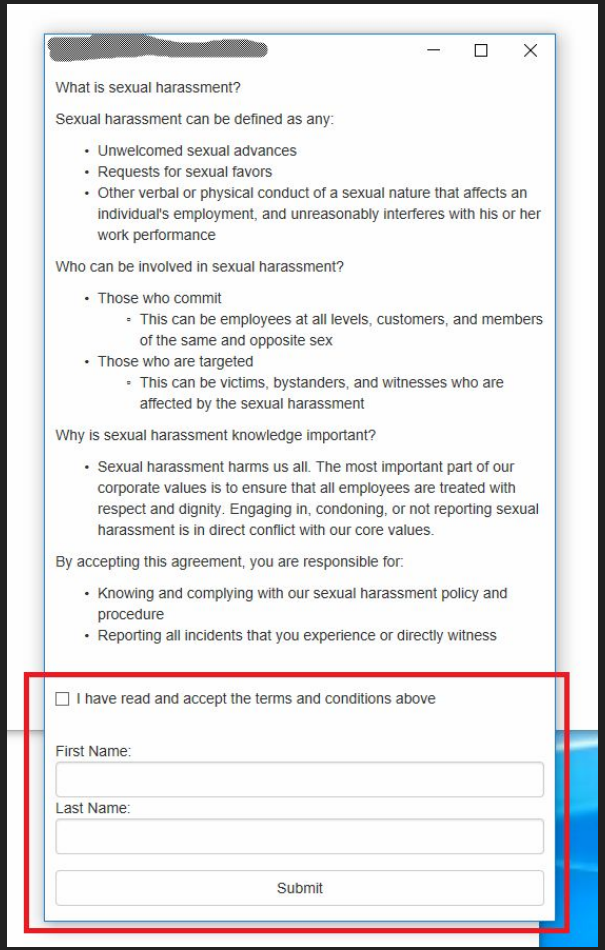
Successful Campaigns - Harassment Policy Update

- Website (WordPress)
- <CLIENT> subdomain



Successful Campaigns - Harassment Policy Update

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



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?