



**REDTEAM**  
SECURITY TRAINING

# Social Engineering Report

Prepared for: XXXXXXXXXXXX

Jeremiah Talamantes, CISSP, CHFI, CEH, CCENT, CCISO  
REDTEAM SECURITY TRAINING, LLC



## Scope

### Target(s)

The scope of the test included the following in-scope information assets

- XXX employees
  - Email Phishing (15)
  - Telephone Phishing (15)
  - Onsite Overt & Covert (DFW and MSP)

### Timetable

- Test Start: July, 2015
- Test End: August, 2015



## Email Campaign – Executive Summary

RedTeam has developed a comprehensive phased assessment approach that is based on industry-recognized standards, years of experience and key frameworks.

### Overview

RedTeam Training conducted an Email Phishing Campaign against the organization using a methodical and standardized approach. The objective of the assessment was to identify areas of weakness in staff's adherence to email best practice. Important findings from the assessment are listed below and within the Campaign Summary on the following page.

### Pretext

RedTeam Training sent a spoofed phishing email masquerading as an XXX employee, Chris Hanson, designed to entice XXX staff to visit an unknown website and enter their Windows domain username and password. To accomplish this task, RedTeam Training utilized a decoy website, <http://xxx.xxx.com> purporting to be a phony SaaS company, called XXXX that delivers critical security patches to organizations.

In order to establish a false sense of trust, the email and phony company landing page specifically named Chris Hanson as an IT contact along with the XXX logo and 800 number.

The phony website is presented in Exhibit A and the landing page is presented in Exhibit B. The phishing email is presented in Exhibit C.

### Results

As a result of the campaign, 6% of the in-scope staff email addresses (15) visited the phony website and entered their Windows domain username and password. While 26% of the in-scope staff email addresses visited the site but did not enter their credentials. Furthermore, 66% of the targets did not visit the site nor did they enter their credentials. Due to the above calculations, this campaign nets an overall risk rating of **LOW**.

The campaign results determined that the most activity occurred during the first (1) day of testing. This was due to targets reporting the phishing

### Overall Email Campaign Risk Rating





event to the Help Desk, which resulted in a swift URL and email sender block. The block would have restricted targets from both receiving the email and from visiting the URL. The block was later lifted and another email blast was sent.

During the second blast, more users fell victim to visiting the site, but only one (1) target entered their credentials. This activity took place during the first four (4) hours of the test. No other visits were made outside of the first day of the second email blast. Overall, the hit rate is quite low for a first time assessment. The low hit rate is attributed to the quick action by targets reporting the email and quick action by the Help Desk in blocking the sender and destination URL.



## Email Campaign - Details

RedTeam has developed a comprehensive phased assessment approach that is based on industry-recognized standards, years of experience and key frameworks.

---

### Details

#### Overview

RedTeam training was engaged to conduct an Email Phishing Campaign against the organization using a methodical and standardized approach. The objective of the assessment was to identify areas of weakness in staff's adherence to email best practice. Important findings from the assessment are listed below and within the Campaign Summary on the following page.

#### Pretext

RedTeam Training portrayed the identity of a non-existent XXX employee. In doing so, RedTeam sent a phishing email (Exhibit A) masquerading as an XXX employee, Chris Hanson, designed to entice XXX staff to visit an unknown website and enter their Windows domain username and password. To accomplish this task, RedTeam Training utilized a website, <http://xxx.xxx.com> purporting to be a phony SaaS company, called XXX that delivers critical security patches to organizations. Please see Exhibits B and C.

In order to establish a false sense of trust, the email and phony company landing page specifically named Chris Hanson as an IT contact along with the XXX logo and 800 number. The sender's email address was not a spoofed XXX address, but a xxx.com address ([chris.hanson@xxx.com](mailto:chris.hanson@xxx.com)).

#### Summary

The assessment started in the afternoon of July 21st. During the first few hours, there were a couple of hits to the landing page. However, there weren't any targets that entered their credentials. After about 4pm that day, all traffic ceased to exist. Later, it was discovered that a target had notified the Help Desk of a suspicious email. The Help Desk has quickly blocked the destination URL and the sender address; thus the inactivity.

#### First Round

The first round of testing produced two (2) unique hits to the landing page, however neither of the hits involved targets entering their username and password. After this round of email, the domain and sender were blocked. No additional traffic was noted.



## Second Round

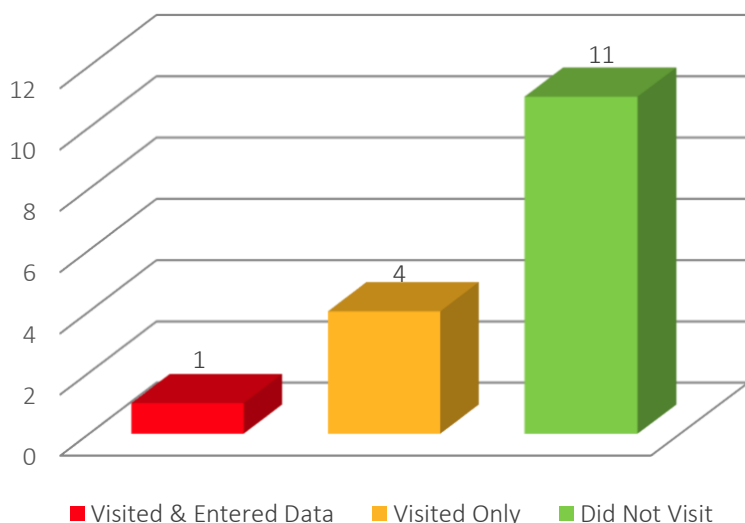
The domain and sender restrictions were lifted and another round was sent to the same targets on August 10th. Two (2) additional hits were recorded and one instance a target had entered their username and password.

*\*\* Another round of emails took place on August 6, in between the aforementioned First and Second Rounds. However, at the time only the URL domain block had been lifted and the email did not reach the targets. Therefore, no results were produced. Through conversations with the Help Desk, it was discovered that the sender block was still in effect. The Help Desk later removed all restrictions and the Second Round was carried out.*



The charts below aim to provide a high-level view of the results of the test.

## Overall Responses Breakdown



## 6% Compromise Rate

Unique Recipients: 15

Emails Delivered: 15 (0 bounces)

Start: Tuesday, July 21, 2015 at 2:00 PM

Ended: Thursday, August 16, 2015 at 5:00 PM

Duration: 4 weeks

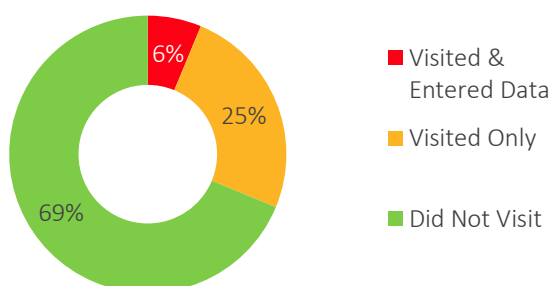
Recipients: All Staff Employees

Pretext: Phishing website for security updates

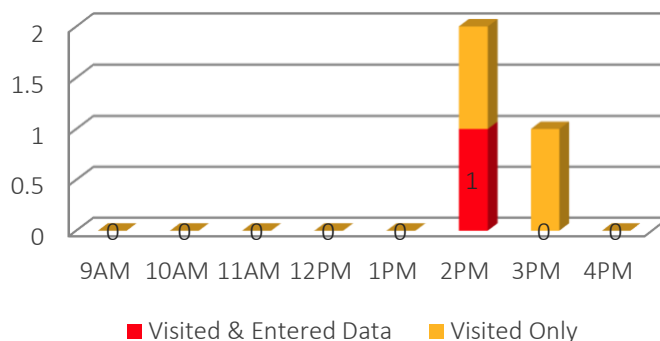
Objective:

Send a phishing email to all users masquerading as Chris Hanson from the IT department. Entice users to visit an unknown website purporting to be an official website for SaaS company designed to deliver security updates for organizations.

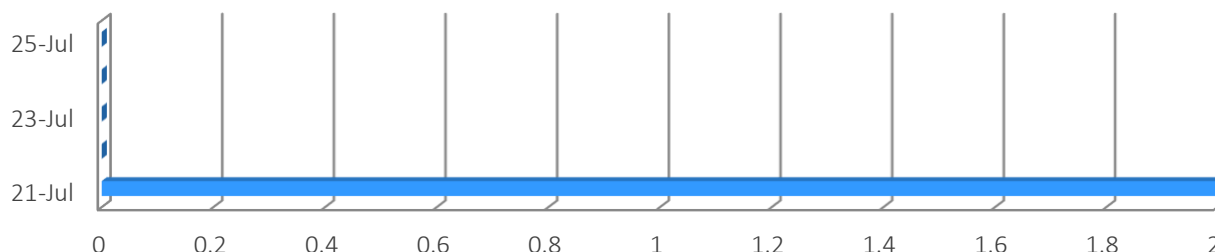
## % Responses Breakdown



## Day 1 Responses



## Week 1 Activity





## Email Campaign - Recommendations

RedTeam has developed a comprehensive phased assessment approach that is based on industry-recognized standards, years of experience and key frameworks.

---

### Recommendations

RedTeam Training conducted an Email Phishing Campaign against the organization using a methodical and standardized approach. As a result, the following recommendations have been made:

#### Email Phishing Testing (Annually)

While the targets performed well and the overall hit rate was Low, we recommend an annual schedule for continued email phishing assessments vs. implementing a schedule any longer than once per year. It is recommended that the content of the campaign be augmented to include file attachment testing, as an aside. In addition, the pretext should be modified and include a different subset of targets.

#### Security Awareness

Security Awareness training sessions conducted by the organization should be carried out at least once a year and include results of each previous test. The purpose is to build upon lessons learned from each and every previous phishing campaign in order to effectively decrease the rate of failure (aka, hit rate). Also, security awareness training should be mandatory for each new hire orientation. Security awareness training should encompass the following topics relevant to this assessment:

- XXXX standards for company communication
- Guidance for recognizing email phishing attempts
- Incident reporting (who, when, where, how)

#### Augmented Security Awareness Training

The content of the security awareness training should be augmented to include the findings of this test. The content should convey to users that email could easily be spoofed to come from an internal employee. Users should know that most phishing emails create a sense of false urgency and to always be wary of file attachments.







## **Incident Handling Procedures**

The testing results showed that most users fell victim in the first few hours of the campaign. According to this assessment, the targets responded quickly and the Help Desk took immediate countermeasures. To reinforce and ensure speedy response times in the future, users should be continually informed what constitutes an incident and how/when/where to report them. To support incidents, IT department roles should be augmented to include incident handling duties. A formalized escalation matrix should be developed to support the proper handling, reporting and elevation of notifications/responsibilities of security incidents.



## Evidence – Exhibit A

A note about the evidence here...



Deliver product updates securely with confidence, ease and reliability. **Updates delivered.®**

Enterprise companies like [Linksys](#), [Symantec](#), [Juniper](#) and [Adobe](#) rely on Envatoo's patent-pending technology to deliver product updates to their clients everyday

**Contact us for more information**

Simply complete the form below to receive a [guided demonstration](#) by an Envatoo sales engineer.

Name


First

Last

Email Address

you@yourdomain.com

**Submit**




**Mobile Apps**

**Security & Compliance**


**Envatoo's New Mobile App Delivery Platform**


We are very pleased to announce that our patent-pending technology has been extended to include mobile applications, such as Apple iOS, Android and Blackberry. This new offering will enable product oriented organizations to rest assure that Envatoo will deliver updates to clients securely, reliably and efficiently.




We are extremely pleased with the Mobile App Delivery solution by Envatoo. It has allowed our business to grow without needing to address product delivery infrastructure and costs. Their solution is easy to use and very cost-effective.

Jonathan Atkinson






**See what our customers are saying**



We rely on Envatoo technology everyday to deliver results!





**Current Clients**

Wells Fargo, Shavlik, Juniper, DigiDesign, Linksys, IBM, Acer, Zenith, JP Morgan, KPMG, Fidelity, Centric, Artisan Tech and many more...

© 2010 Envatoo. All rights reserved | [Contact](#) | [Help & Support](#)

**Follow Us**







## **Evidence – Exhibit B**

A note about the evidence here...



## **Evidence – Exhibit C**

A note about the evidence here...