Red Team Phishing Campaign 2015

SUCK Report

Peter Kim

Table of Contents

Red Team Phishing Campaign 2015
SUCK

Overview
On Thursday, March 13th at 1:40PM PST, Secure Planet LLC initiated a Red Team phishing wave targeting 50 employees. The goal of this wave was to gauge the resiliency of the employees in question to phishing attacks of low to moderate sophistication. The targeted employees demonstrated medium detection rates for this wave, with a medium percentage reporting the email to the Security team as suspicious.

Purpose/ Methodology
Phishing, or email in general, is one of the most commonly used and effective vectors for both targeted and non-targeted technical attacks. It is one of the few delivery mechanisms that allows such attacks to be conducted remotely (e.g., over the internet). These attacks are generally the first step in targeted attacks, where an attacker is looking for an initial vector into the company. Once credentials are compromised, the attacker will use these accounts to send malware (Excel, Word, PDF, malicious links, etc) to internal employees from a trusted SUCK email account. After infecting users with malware onto multiple hosts, the attacker will elevate their access and gain credentials to sensitive servers. With access to Intellectual Property (IP) and user account information, the attacker will encrypt and send the sensitive data to a compromised host on the internet.

- OSINT
  - Use open source intelligence to gather a list of people and emails
- Phishing
  - A small handful of fusers are targeted by a phishing attack harvesting credentials
- Spreading Malware
  - The attacker would use the compromised credentials and send malicious files to internal employees
- Lateral Movement
  - The attacker elevates access to privileged and sensitive accounts
- Data Gathering
  - Data is gathered from all sensitive servers and staged at a single host for exfiltration
- Exfiltration
  - Data is encrypted and sent through encrypted channels to external secure servers

Summary of Findings

Of the 50 employees targeted, five submitted the message to Security for analysis (reported), twenty employees clicked on a link in the message and was taken to the landing page (conversion), and ten targets entered data into the form on the fake landing page (credentials recovered).

Reported	Conversions	Credentials Recovered
5 (10%)	20 (40%)	10 (20%)

As this is the first Red Team phishing wave launched by Secure Planet LLC, there are no previous results against which to compare this data. With a **10% reporting rate** Secure Planet LLC is relatively confident that, were this a real wave, detection was likely to have been provided by suspicious email submissions.

With a high conversion rate, ultimately leading to a successful attack, the Security team must acknowledge the following potentially significant considerations and observations related to this wave in particular:

1. **Small Target Sample Pool** – 50 targets is a very small target pool
2. **Targets Clustered in Close Physical Proximity** – the target pool consisted of almost the entire staff of one particular office location
3. **SUCK Email Addresses Prepopulated -** Most employees do not use their SUCK email addresses for external sites. Since these fields were prepopulated on the landing page, this alerted a number of employees.
4. **Mobile Devices –** Employees that checked the email on their phones were directed to a non-existent page.

Regardless, this wave can be seen as a success from the perspective of both the facts that this was an ad-hoc assessment and valuable information was captured, particularly the reporting rate observed from employees.

Next Steps

The phishing campaign was a realistic attack of what is seen today targeting many large companies. This assessment on SUCK's security posture against phishing attacks informs us of the following:

1. Users are not aware that they need to report phishing emails to their Security team. With only 10% reporting the incident, SUCK should strive for at least 50%.
2. Users are either having a hard time identifying malicious emails or are clicking on links without understanding the potential malicious nature. With 40% of the testing population clicking on the links in the email, SUCK should strive for fewer than 10%.

The next step for the Security team is to devise a way to better inform our users to utilize SUCK's Security team and to educate in malicious identification and handling of phishing attempts.

Appendix A: Target List

Email Address
john@SUCK.com
paul@SUCK.com
peter@SUCK.com
mary@SUCK.com
frank@SUCK.com
ryan@SUCK.com
roger@SUCK.com
mike@SUCK.com
sarah@SUCK.com
jane@SUCK.com
john@SUCK.com
paul@SUCK.com
peter@SUCK.com
mary@SUCK.com
frank@SUCK.com
ryan@SUCK.com
roger@SUCK.com
mary@SUCK.com
johnny@SUCK.com
ron@SUCK.com
rob@SUCK.com
bob@SUCK.com

Appendix B: Phishing Email and Landing Page Screenshots

Included below are screenshots of both the fake phishing email and Security-constructed landing page created and used specifically for this wave.

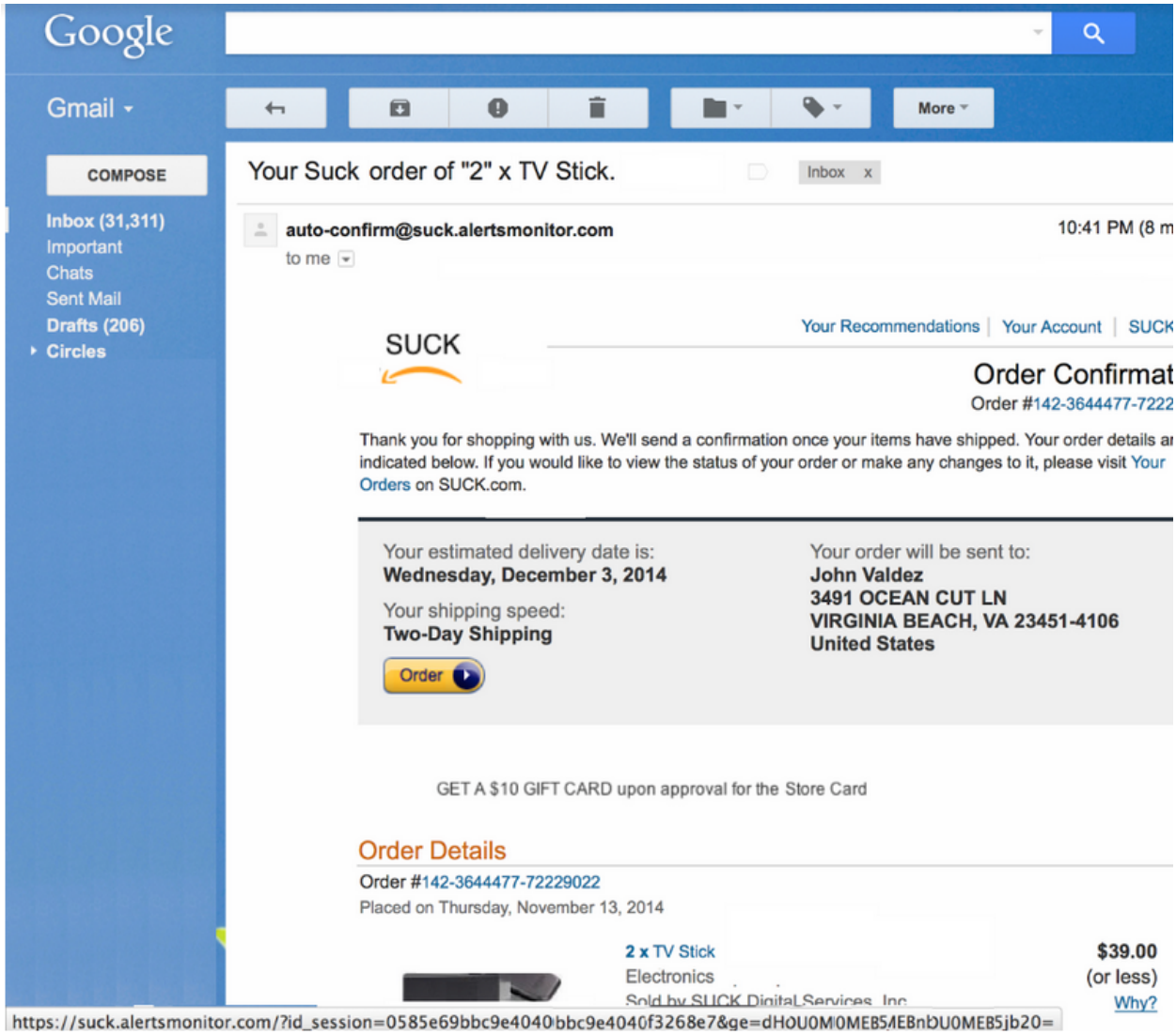

Figure 1 – Partial Screenshot of Example Phishing Email

Figure 2 –Screenshot of "Fake" Phishing Landing Page