31 JULY 2017

SOCIAL ENGINEERING ASSESSMENT REPORT

Version 1.4

IniTech, Inc.
Bill Lumbergh | Chief Technology Officer

RHINO SECURITY LABS

SOCIAL ENGINEERING ASSESSMENT DETAILS

Security Consultant

Hector Monsegur
Hector.monsegur@rhinosecuritylabs.com
(888) 944-8679

Assessment Prepared For

Bill Lumbergh
Chief Technology Officer
IniTech, Inc.

Security Engagement Manager

Christopher Lakin
Chris.lakin@rhinosecuritylabs.com
(888) 944-8679

Project Number

07-01-Ini-SE

Assessment Scope Summary

Engagement Timeframe

07/01/2017 – 07/31/2017

Engagement Scope

200 Spearphishing Emails
25 Pretext Calls

Revision History

07-26-2017	Christopher Lakin	First Draft
07-29-2017	Hector Monsegur	Edits
07-29-2017	Benjamin Caudill	Edits
07-31-2017	Christopher Lakin	Final Draft

TABLE OF CONTENTS

ENGAGEMENT OVERVIEW

Rhino Security Labs specializes in advanced social engineering techniques and practices, identifying areas of improvement. Going beyond the basic automated tests, our social engineering engagements demonstrate vulnerabilities by strategically applying various persuasive techniques.

Whether targeted spearphishing (email) or pretext calls (voice calls) our trained experts take great care and pride in their work. Our goal isn't to exploit, but to educate and expose critical gaps in organizational security controls.

Service Description

Spearphishing

Rhino's spearphishing goes far beyond automated tools found in many comparable services, providing highly targeted, sophisticated scenarios for each client. Using research on both the client organization and its employees, our security experts create sophisticated campaigns which ensure the best assessment of user susceptibility.

Pretext Calls

Pretext calls, also referred to as phishing, utilize voice phone calls to coax a user into performing an unauthorized task, such as providing sensitive information or downloading an untrusted file. While these attacks are less common than email alternatives, phone calls can be more effective as the attacker establishes a personal connection with the target.

Campaign Objectives

Assess Employee Susceptibility

Employees will always be a viable attack vector for malicious actors to take advantage. Often times, organizations view employee behavior as the greatest weakness when it comes to security. However, employees are also the first line of defense against ongoing social engineering engagements. This social campaign is designed to assess the exploitation likelihood and the potential impact associated with spearphishing and pretext calling.

Assess Technical Controls

Employee susceptibility is only one side of the social engineering equation. Technical controls can be used to reduce both the likelihood and the impact of a successful social engineering campaign. Preventing a spearphishing email from reaching a targets inbox is important, but isn't always possible. Implementing additional technical controls to notify teams of social engineering attempts or limit the access an attacker has after a successful phish can greatly reduce risk associated with the engagement.

KEY PERSONNEL

Passionate and forward-thinking, our consultants bring decades of combined technical experience as top-tier researchers, penetration testers, application security experts, and more. Drawing from security experience in the US military, leading technology firms, defense contractors, and Fortune 50, we pride ourselves on both depth and breadth of information.

Chris Lakin - *Cybersecurity Engagement Manager*

Chris Lakin has accumulated over eight years of project management and customer engagement experience across a multitude of industries. A proponent of constant iteration and improvement, his knowledge from time spent in business and marketing adds a valuable perspective to every cybersecurity engagement. Receiving a Masters of Science in Cybersecurity Engineering from the University of Washington, Mr. Lakin excels at connecting the technical with the goals of the business.

Hector Monsegur - *Director of Assessment Services*

Hector Monsegur brings a unique perspective from decade of offensive experience and a desire to make an impact in client security. In working with the US Government, Mr. Monsegur identified key vulnerabilities - and potential attacks - against major federal infrastructure including the US military and NASA. In his role as a security ressearcher at Rhino Security Labs, he has identified countless zeroday vulnerabilities and contributed to dozens of tools and exploits. In his leadership role, his unmatched technical experience is shared to both educate other operators and guide techincal research. Mr. Monsegur is a leading speaker for security organizations and conferences around the world.

Benjamin Caudill - *CEO and Founder*

Benjamin Caudill is an adept cybersecurity professional, researcher, and entrepreneur. A veteran of the defense and aerospace industry, Mr. Caudill led investigations into advanced cyberattacks, coordinating with federal intelligence communities on complex engagements. As Founder and CEO of Rhino Security Labs, Mr. Caudill has built the boutique security firm and turned it into a major player in the penetration testing market. In addition to his executive role, Mr. Caudill oversees company research and development, ensuring the continued development of key offensive technologies.

SOCIAL ENGINEERING METHODOLOGY

Rhino Security Labs utilizes a structured series of steps in social engineering campaigns for formal, repeatable assessments. This step-by-step format ensures consistency in vital areas while providing flexibility in the specific pretext and scenarios created.

1

Information Gathering

Often neglected in social engineering services, information gathering is a critical phase and often determines the success of the campaign. Even when provided with basic information such as names and emails, research on the organization and its personnel can be critical to the success of social engineering.

2

Create Pretext Scenarios and Payloads

Once full enumeration of the client organization – and its employees – is complete, focus turns to the pretext scenarios and payloads for the social engineers.

These details answer the following questions:

- Drivers
  Which will raise interest/concern in employees?
- Payloads
  What's the target information/access?
- Validity
  What else can be done to improve pretext legitimacy?
- Source information
  Which domains/phone numbers should be created?

3

Engage Targets

Using the predetermined tactics, Rhino Security Labs assessors begin engaging specified employees with the appropriate emails or phone calls. For advanced engagements – which can incorporate social media or SMS to build rapport – the first of multiple interaction stages begins. Throughout the engagement, the assessors evaluate the targets' response and adjust the campaign accordingly to achieve the best result.

4

Reporting and Debrief

Upon completion of the campaign, assessment results are aggregated and the social engineering report is written, outlining both an executive summary and specific engagement details. Detailed remediation steps are also provided, directing the client in both technical and policy risks to mitigate.

Once the client focals have reviewed the final report, a debrief meeting is scheduled. This discussion walks through the details of the campaign and answers questions.

5

Remediation and Employee Education *(Optional)*

As an optional addition to the standard assessment, Rhino Security Labs provides user training sessions for client employees. Whether hosted in a recorded online webinar or an in-house training session, provide quality security awareness training – by the same experts who performed the original engagement.

SCOPING AND RULES OF ENGAGEMENT

While real attackers have no limits on social engineering engagements, we do not engage in social engineering activities that threaten our ethics and personal privacy.

Constraints

In addition, the following limitations were put into place:

Rhino Secuirty Labs took measures to minimize business impact when sending spearphishing emails and making phone calls. This way an employee's work day isn't being disrupted by inquiries regarding the engagement.

Rhino Security Labs was not tasked with assessing the quality of the Social Engineering training program at IniTech, Inc. and is unaware of its content.

Scope of Services

The predetermined scope for Rhino Security Labs to carry out the social engineering security assessment was:

Targeted Spearphishing Emails

Quantity

200

Target Audience

The target audience is comprised of 150 IniTech, Inc. employees from various departments within the organization. The remaining 50 targets are managers considered to be high-value targets.

Description of the Service

Phishing utilizes convincing email to trick users intro performing certain actions, such as providing passwords or other sensitive data. Utilizing detailed personal information for more convincing, sophisticated attacks is known as spearphishing.

Pretext Calling (Vishing)

Quantity

25

Target Audience

The target audience will be non-responsive targets from the spearphishing campaign. This list include between 5 - 10 high value managerial targets.

Description of the Service

Pretext Calling engagements leverage deep information gathering, company profiling, and targeted scenario scripts for highly effective voice calls.

SUMMARY OF FINDINGS

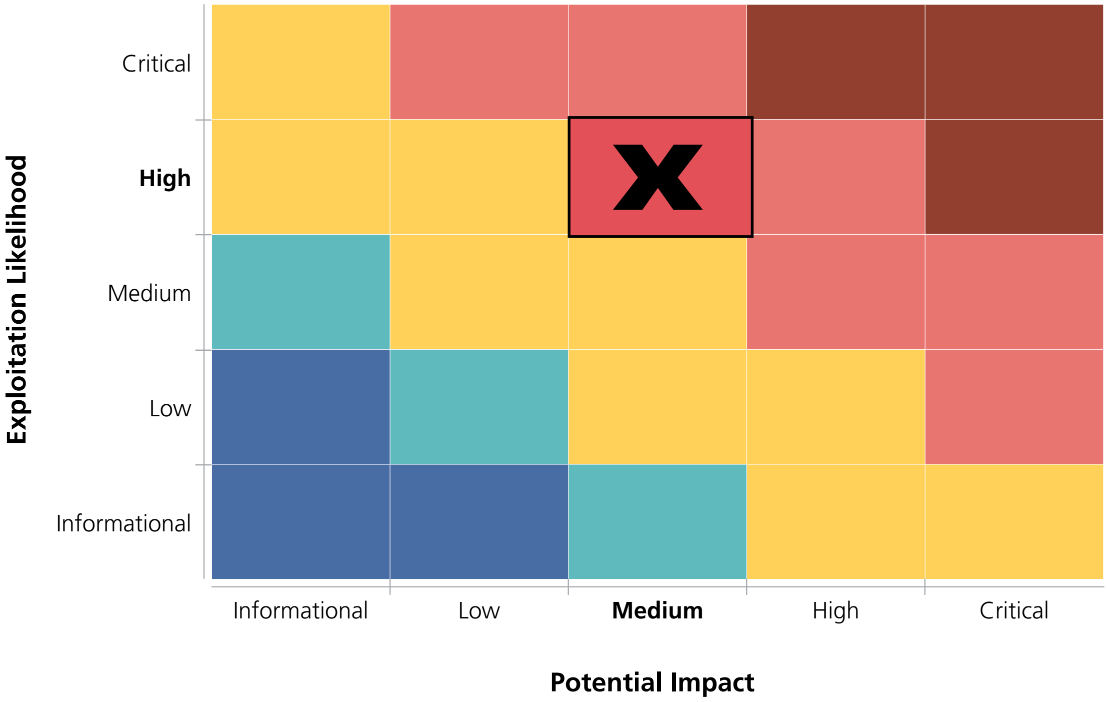
IniTech, Inc. is given an overall social engineering risk rating of **High**. It was observed that out of the 200 users we targeted, the users who were most susceptible to providing credentials were employees who held management positions.

With 36% of targeted spearphishing users providing sensitive information, we believe that IniTech, Inc. should invest further into security awareness training for their employees. As most major breaches are a result of a spearphishing attack, developing an effective and realistic security awareness program will help better align and protect IniTech, Inc. from the current and most common threats out there.

SOCIAL ENGINEERING RISK RATING

Rhino Security Labs calculates Social Engineering Risk based on Exploitation Likelihood (Employee Actions) and Potential Impact (Technical Controls).

OVERALL RISK RATING: HIGH

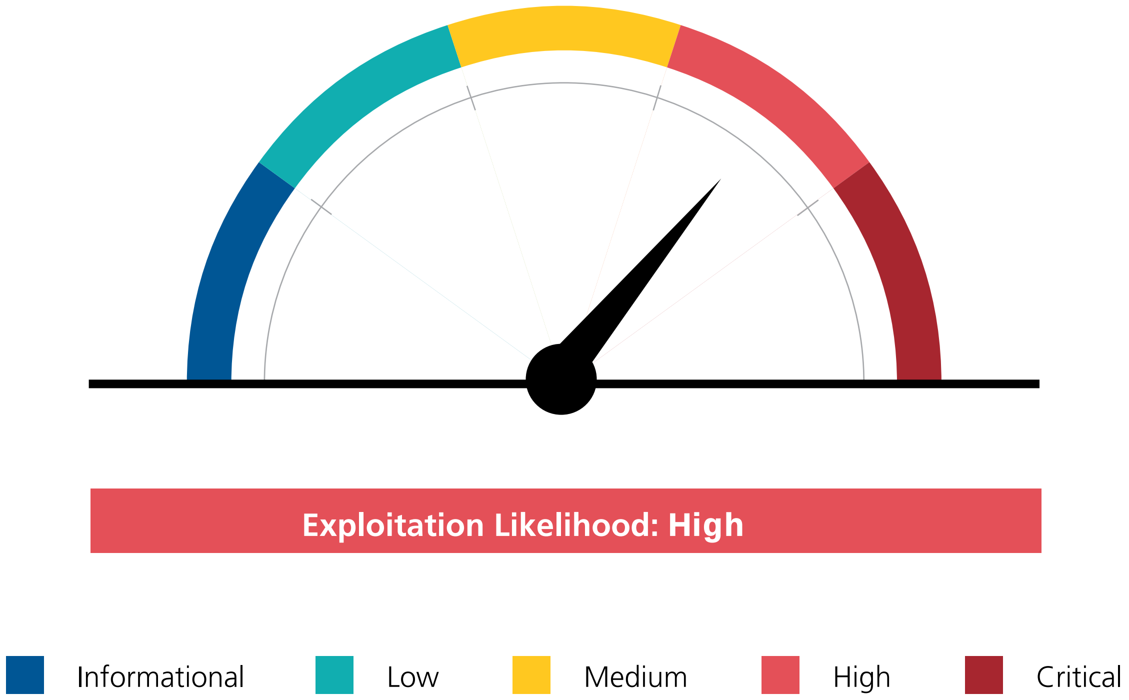


EXPLOITATION LIKELIHOOD RATING

Exploitation Likelihood is based on the results of employee actions, such as opening emails, providing sensitive data, downloading malicious files, and reporting suspicious behaviors to internal IT. With a success rate of 36%, we determined an Exploitation Likelihood rating of **High**. IniTech, Inc. is very likely to be successfully targeted through social engineering.

Rating Factors

Successful Spearphish Emails	36%	**Poor**
Successful Pretext Calls	20%	**Poor**
Spearphishing Emails Reported	8	**Poor**
Pretext Calls Reported	4	**Average**

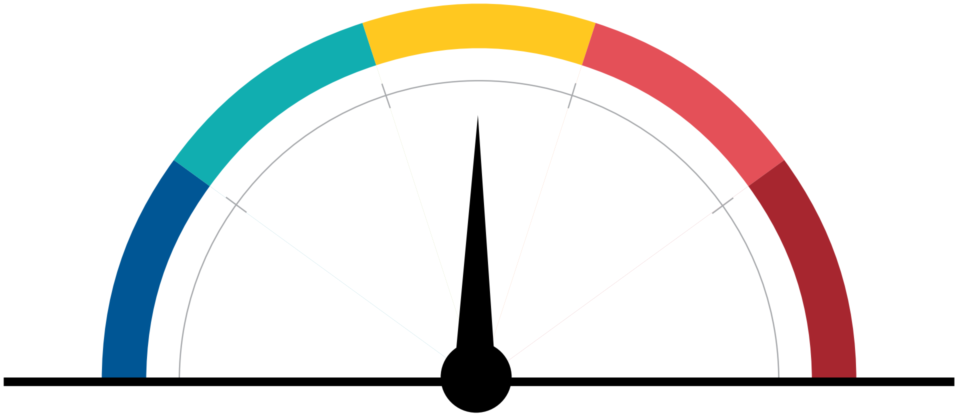


POTENTIAL IMPACT RATING

Potential Impact is determined by evaluating technical controls which prevent, detect, or respond to successful social engineering attacks. These impact factors include anti-virus, two-factor authentication, and logging capabilities. With a Potential Impact rating of **Medium**, any successful social engineering attack on IniTech, Inc. could results in moderate impact on the company.

Rating Factors

Utilizes Two-Factor Authentication	Yes	**Good**
DNS Categorization/Uncategorized Blocking	No	**Average**
High Impact Targets Compromised (Managers)	38%	**Very Poor**
Organizational Security Considered Robust	Yes	**Good**



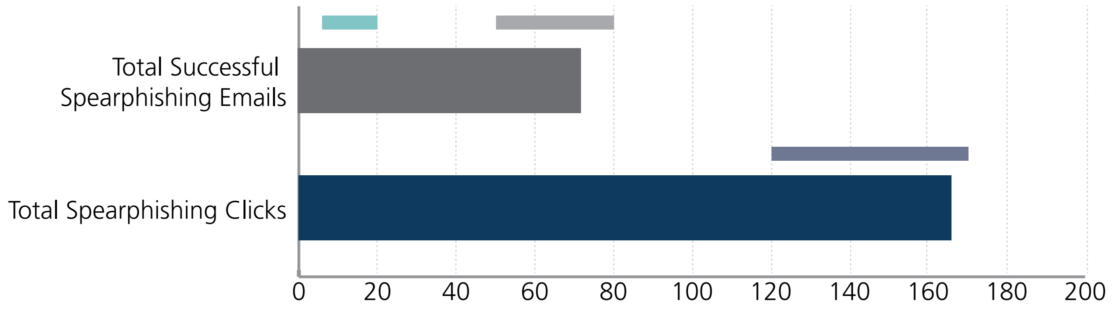
Potential Impact: Medium

🟦 Informational 🟩 Low 🟨 Medium 🟥 High 🟥 Critical

SPEARPHISHING CAMPAIGN RESULTS

Total Successful Spearphishing Emails: 82

Total Spearphishing Clicks: 173
Total Spearphishing Emails Sent: 200

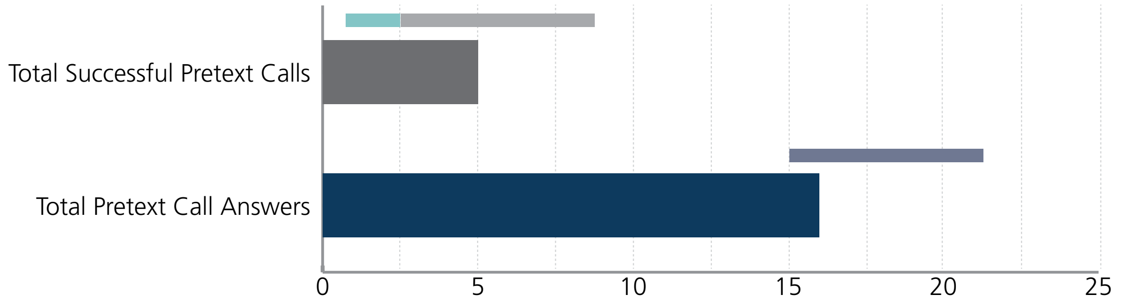


⬛	Total Successful Phish: 36%	⬜	Industry Average Successful Phish: 25% - 40%
⬛	Total Spearphishing Clicks: 83%	⬛	Industry Average Clicks: 60% - 85%
		🟦	Desired Range: 3%-10%

PRETEXT CALLING CAMPAIGN RESULTS

Total Successful Pretext Calls: 5

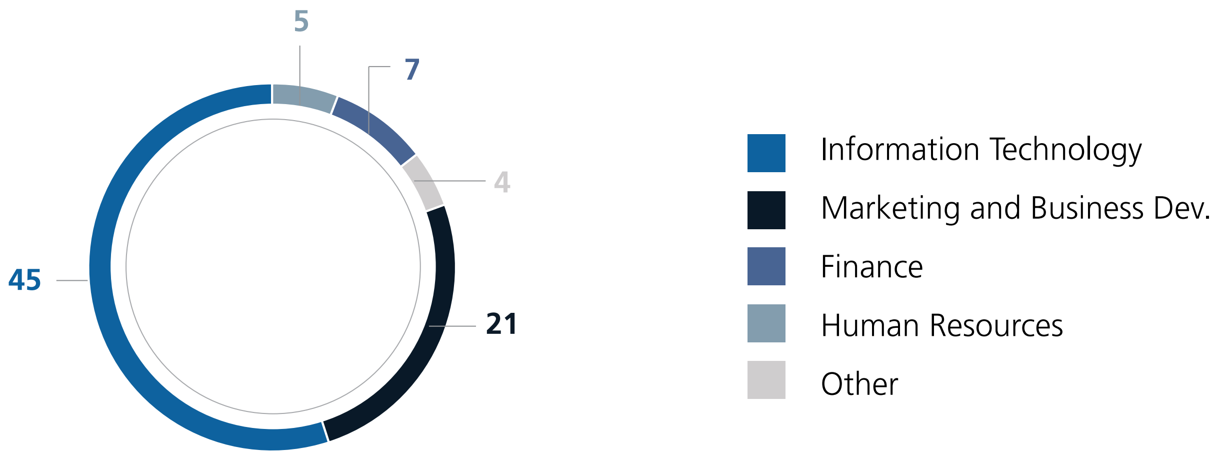
Total Pretext Call Answers: 16
Total Pretext Calling Attempts: 25



⬛	Total Successful Pretext Calls: 20%	⬜	Industry Average Successful Calls: 10% - 35%
⬛	Total Pretext Call Answers: 64%	⬛	Industry Average Answers: 60% - 85%
		🟦	Desired Range Successful Calls: 3% - 10%

SPEARPHISHING DEPARTMENT SUSCEPTIBILITY

In large organizations, there is typically a clear distinction between departments and their susceptibility to social engineering tactics. For example, roles that are more likely to be contacted by strangers or interact with individuals from outside of the organization (such as customers) are generally more susceptible to social engineering.



SUMMARY RECOMMENDATIONS

Phishing will always remain the most popular attack vector and we recommend educating employees on the dangers of these types of attacks - as well as how to spot and flag them. Further, based on the assessment data above we recommend implementing some or all of the following:

1. Block uncategorized or recently purchased domains, as malicious domains are very often in these categories.
2. Force Two Factor Authentication for all users.
3. User Training and Education. This is especially true for new employees as they are most likely to be compromised with social engineering tactics.
4. Conduct regular ongoing spearphishing exercises to increase user awareness and reinforce reporting suspicious emails. Our experience has demonstrated that organizations that conduct regular spearphishing and social engineering exercises perform better over time.

The recommendations above are listed in priority from greatest effectiveness for preventing the social engineering attacks outlined in this report.

ENGAGEMENT DETAILS & WALKTHROUGH

The purpose of this engagement was to work alongside IniTech, Inc. to assess their user education and technical security posture when targeted with a social engineering attack.

SECURITY REPORTED EVENTS AND ENGAGEMENT DISRUPTION

The phishing engagement was stopped once. This occurred on the second day of the engagement when a staff member at IniTech reported it to the IniTech security team.

IniTech security teams responded well by blocking additional phishing emails from being delivered, once the events were reported. user credentials were submitted before the first report stopped the engagement.

The pretext calling was reported by an employee to a manager. It is not clear if the event was reported to the security team, but an IniTech employee called the number used for the engagement to invesigate the suspicious activity.

Information Gathering

Information gathering started with the collecting of corporate and employee information. This included gathering employee listings, the geographical locations of each office, and building detailed profiles on each employee gathered from this stage.

Company Enumeration

The following data was compiled using general open source intelligence gathering techniques. These techniques included utilizing popular search engines and proprietary tools to gather information from any public presence your company was found to have.

General Company Information

Headquarters Address: 125 N. Lamar, Houston, Texas, 77070

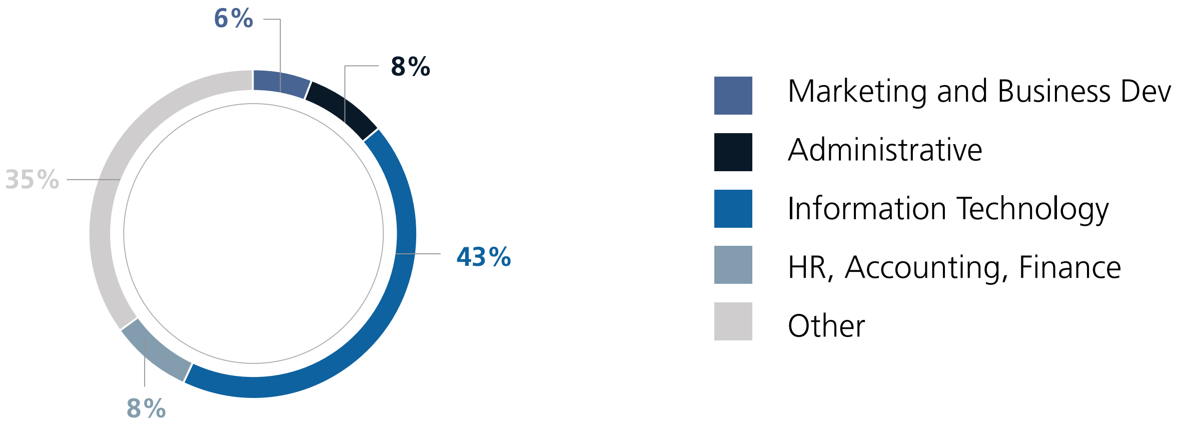
Company Size: 500 - 2,000 employees

Company Description:

IniTech is a generic business software and consulting services company to financial institutions throughout North America.Initech is emblematic of many mid-sized companies with lots of middle-management and focus towards the bottom line. If you need a TPS report, we can get one to you. That's what we know and that is what we do.

COMPANY COMPOSITION

This data is aggregated from LinkedIn and presents the distribution of job functions across the organization. While these numbers are not a true representation of the company composition, this type of public information can give attackers direction for vulnerable departments within the organization.



RECENT COMPANY NEWS

Public information about major company events or changes within an organization that are publicized can be used by attackers within their attack narratives.

The recent company fire at IniTech, Inc. was well publicized by news organizations and the social media teams at IniTech. This accident has caused some uncertainty at the organization and is a vulnerable time for a Social Engineering attack to take place because of the vast amount of coordination and organizational change.

News Source: Houston Times

News Date: 06/13/2017

Article Title: IniTech Building Goes Up in Flames

Description:
IniTech, Inc.'s main headquarters caught fire late Sunday night leaving many questions unanswered. The CEO was nowhere to be found for comment, and it is unclear how the company will react after the incident.

Additional article posted directly to the IniTech social media.

News Source: IniTech Twitter Feed

News Date: 06/01/2017

Article Title: IniTech, a National Leader in Technology and Consulting Responds to Recent Media Coverage and Allegations

Description:
After thorough investigation, leadership is eager to reopen their doors and conduct business as usual. The first few weeks might be confusing but expect TPS reports to be completed as expected.

Engagement Narrative & Results

A successful social engineering engagement involves careful planning and execution, where information gathering is a critical first step. To begin, security consultants utilize a range of proprietary and open source tools to develop a specific profile around both the target organization and its employees. Properly done, this reconnaissance phase can identify key members within the organization, identify email syntax, and provide other key details for a targeted attack.

With profiling and target information identified, pretext and asset construction begins. This process involves first developing the appropriate scenario – phishing goals, email structure, and landing page – and then designing each of the associated elements. Email customization and integration of user-specific variables further increases the odds of success.

Using the data gathered, our assessors determined a strategy to conduct the assessment. After identifying vulnerable targets and creating targeted social engineering scenarios, the campaign is carried out in an attempt to coerce the target into carrying out a task.

While customizing narratives to specific targets improves the effectiveness of the engagement, bypassing email and web security protections is often the difference between phishing success and failure.

A full list of specific targets and results from social engineering engagements are located in Appendix B.

ENGAGEMENT NARRATIVE #1

Phishing - Human Resource Benefit Meeting Rescheduling

ENGAGEMENT SCENARIO

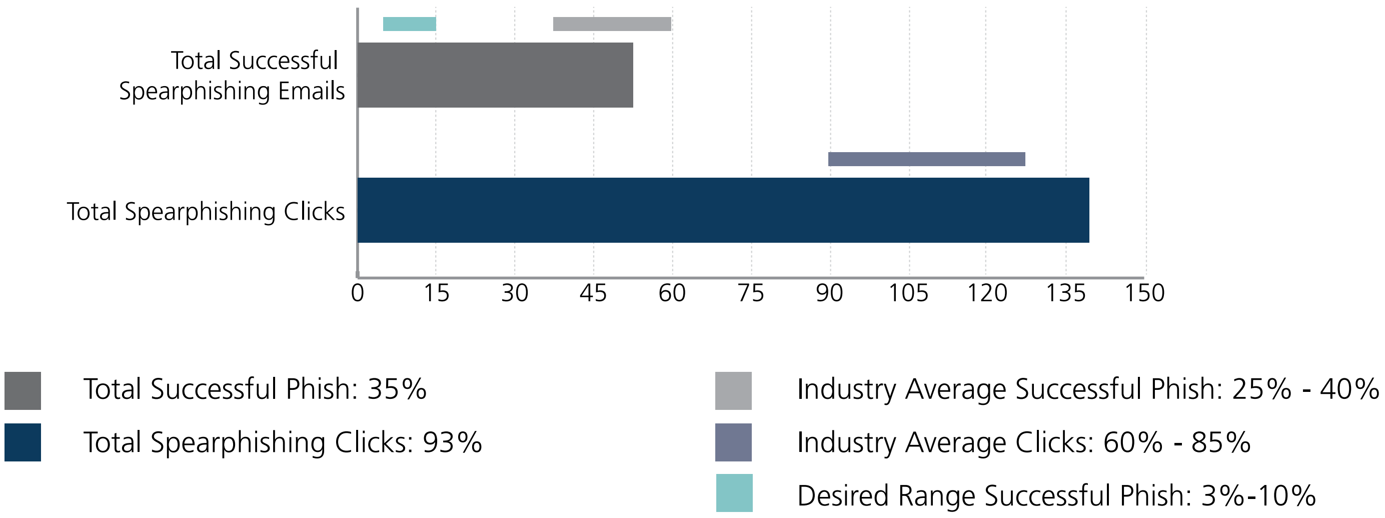
In this scenario, an employee within Human Resources at IniTech informs user of an important benefits meeting. The phishing email directs the target to click on the link to set up a meeting time. The link takes the target to a landing page, which mimics the IniTech federated login portal.

Date	07/02/2017 – 07/07/2017
Time	8:00 AM – 5:00 PM Pacific Time
Frequency	Every 2 – 5 minutes. Time between emails varied to obfuscate the sending pattern
Target Audience	Non-managerial Employees
Payload	Landing Page – Initech Login Portal
Success Determinant	User credentials collected through landing page
Sending Domain	initech.net

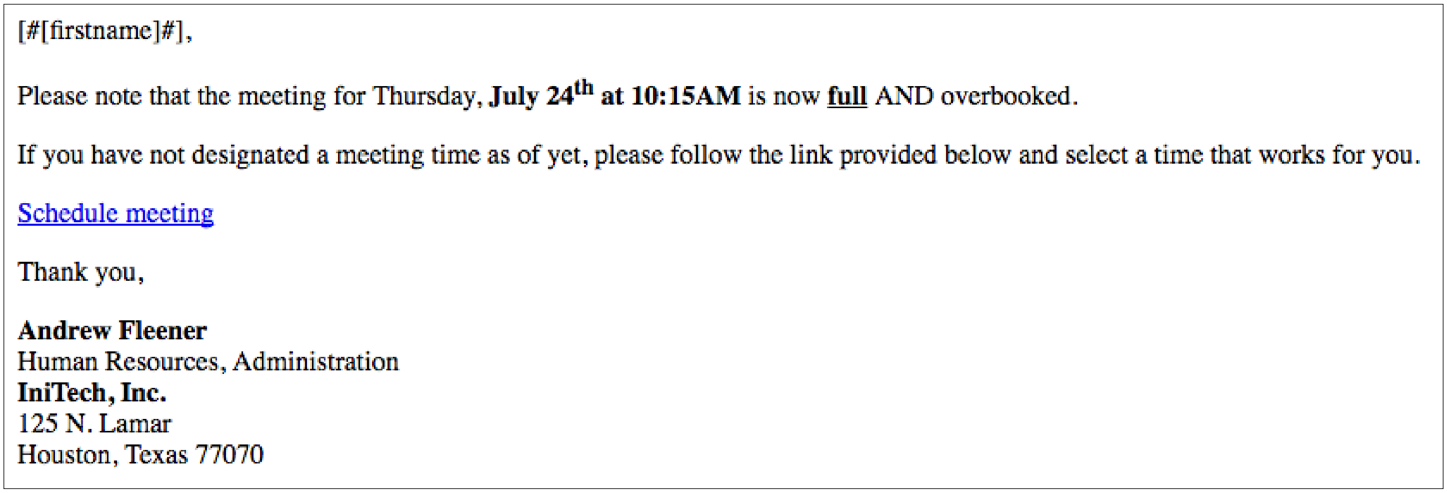
ENGAGEMENT RESULTS

Total Successful Spearphishing Emails: 63

Total Spearphishing Clicks: 140
Total Spearphishing Emails Sent: 150



Email Template



[#[firstname]#],

Please note that the meeting for Thursday, **July 24th at 10:15AM** is now **full** AND overbooked.

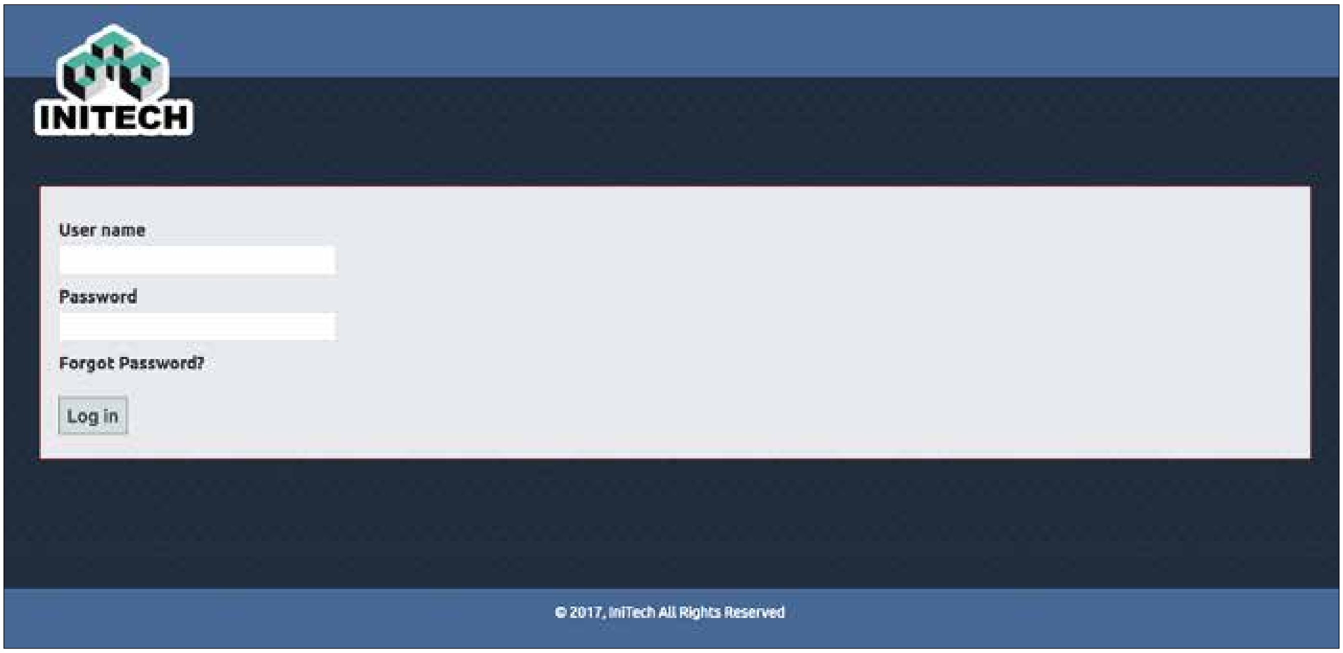
If you have not designated a meeting time as of yet, please follow the link provided below and select a time that works for you.

Schedule meeting

Thank you,

Andrew Fleener
Human Resources, Administration
IniTech, Inc.
125 N. Lamar
Houston, Texas 77070

Landing Page



© 2017, IniTech All Rights Reserved

ENGAGEMENT NARRATIVE #2
Phishing - VPN Confirmation

ENGAGEMENT SCENARIO

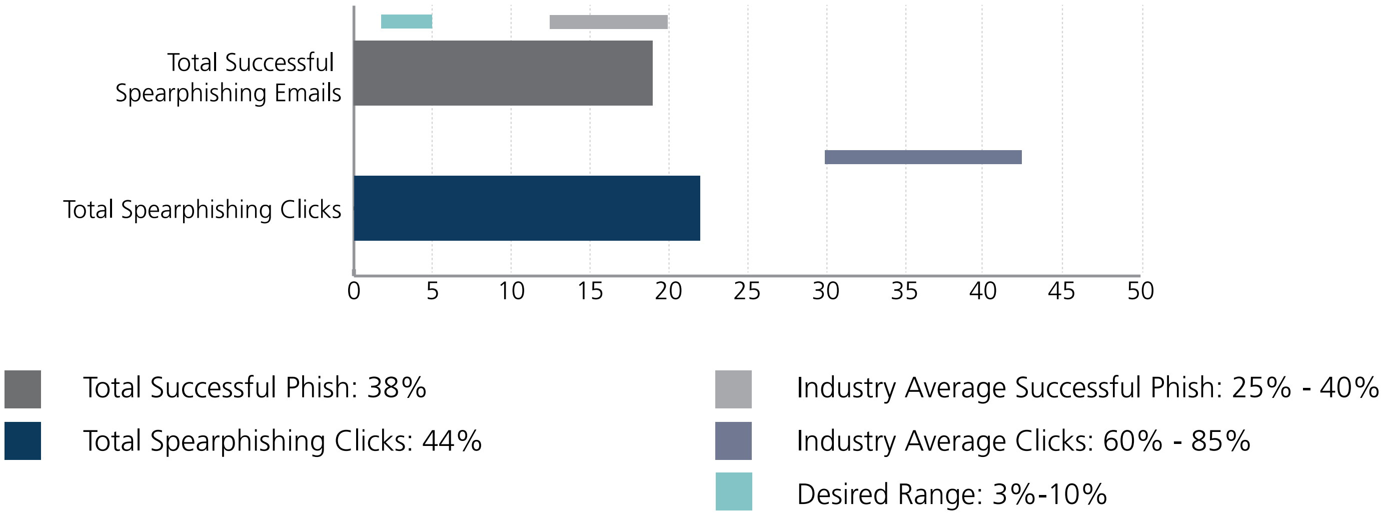
In this engagement, the target receives a spearphishing email from a fake employee within information technology at IniTech. The email requests the target click on the link to verify that the new VPN is functioning properly.

Date	07/08/2017 – 07/10/2017
Time	8:00 AM – 5:00 PM Pacific Time
Frequency	Every 2 – 5 minutes. Time between emails varied to obfuscate the sending pattern.
Target Audience	Managers
Payload	Landing page - Initech Login Portal
Success Determinant	User credentials collected through landing page
Sending Domain	initech.net

ENGAGEMENT RESULTS

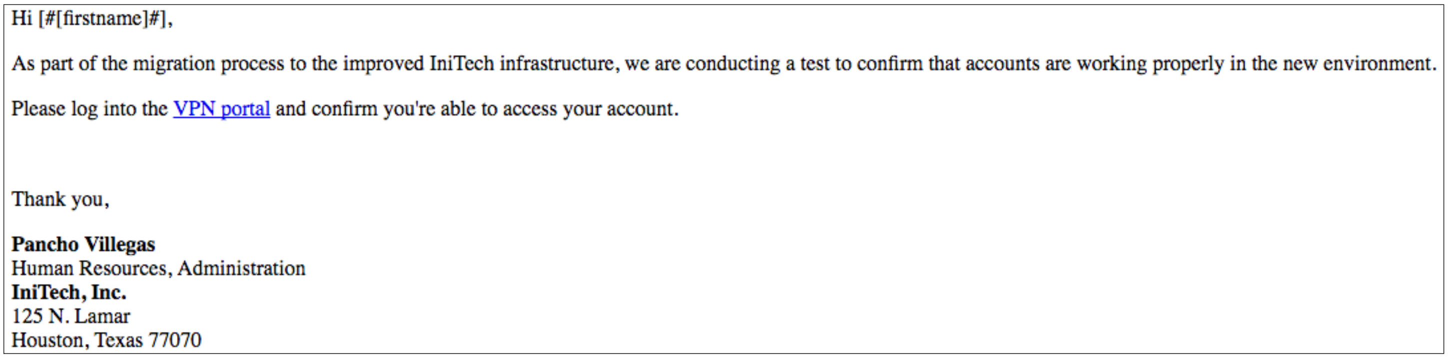
Total Successful Spearphishing Emails: 19

Total Spearphishing Clicks: 22
Total Spearphishing Emails Sent: 50



ENGAGEMENT ASSETS

Email Template



Hi [#[firstname]#],

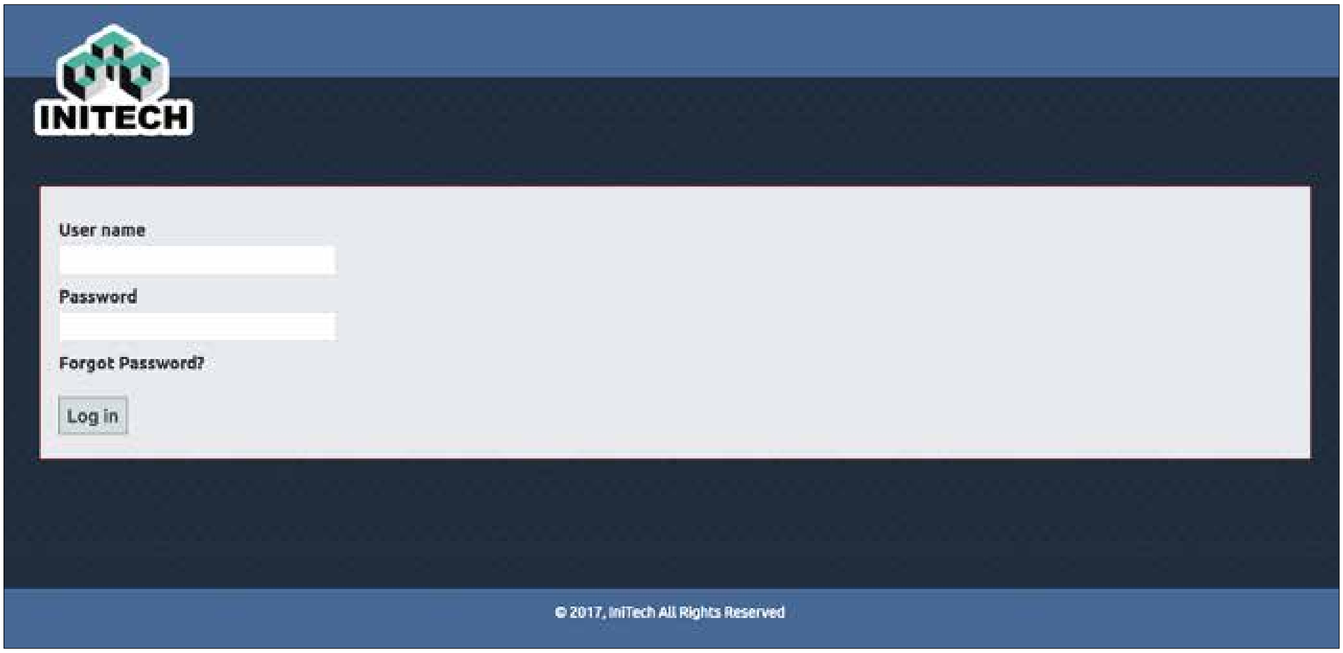
As part of the migration process to the improved IniTech infrastructure, we are conducting a test to confirm that accounts are working properly in the new environment.

Please log into the VPN portal and confirm you're able to access your account.

Thank you,

Pancho Villegas
Human Resources, Administration
IniTech, Inc.
125 N. Lamar
Houston, Texas 77070

Landing Page



ENGAGEMENT NARRATIVE #3

Pretext Calling - Employee Survey Calling

ENGAGEMENT SCENARIO

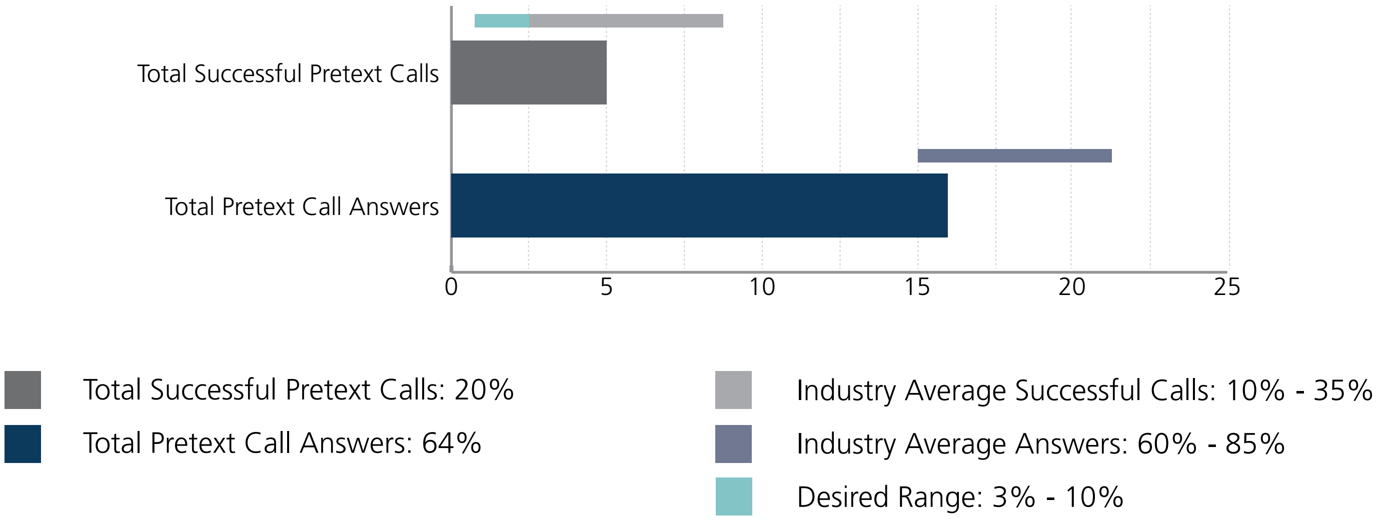
In this engagement, an IniTech employee is calling to gain information about the individual and the systems they have access for business continuity and disaster recovery purposes. If the call is successful, a follow up email is sent, asking the individual to confirm the details of the call. The landing page collects user credentials.

Date	07/11/2017 – 07/21/2017
Time	8:00 AM – 5:00 PM Pacific Time
Target Audience	Targets that did not respond to spearphishing email
Success Determinant	Target gives last-4 of social security number, mother's maiden name, and the call is completed without protest.
Phone Number	(777) 225-5555 (Spoofed)

ENGAGEMENT RESULTS

Total Successful Pretext Calls: 5

Total Pretext Call Answers: 16
Total Pretext Calling Attempts: 25



Engagement Calling Script

<Call Answered>
Actor: Hello is this, <target_name>?

<response>
Actor: Great! This is Sean Brennan from Continuity Services at IniTech. How is your day today?

<response>
Actor: Glad to hear it. With the recent incident, I've been tasked with confirming details about systems and process for disaster recovery. I was hoping you could answer a few questions for me. Can you take a few minutes to help me out?

<response If no>
Actor: Okay, is there a better time for me to call back? I'm working from home today. <adlib rest of conversation>

<response if yes>
Actor: Great! Thank you so much and let's get to it. Just to confirm that I am talking to <target name> can you confirm the last four digits of your social security number and your mother's maiden name as provided on your new employee HR form?

<response>
Actor: Perfect. <proceed through series of questions>

1. What is your full name and title?
2. What is your role at iniTech?
3. How long have you been with the company?
4. Who is your manager in your department?
5. Do you know your manager's manager?
6. Do you handle or process payment processing information?
7. Do you work with or have access to any sensitive data on IniTech customers or Systems?

Actor: Doing great. Now some more technology focused questions.

8. What is your workstation's OS?
9. Do you have local admin rights on your workstation?
10. What is your workstation's IP address?
11. What systems do you have admin access?
12. What is the most critical asset you manage?
13. Are you able to reset passwords?
14. Can you modify, create, or delete users from active directory?
15. What is your employee username and/or ID number?

<after questions>
Actor: That fills in all the holes I had in my documentation. Thank you so much. We use a third-party system to record all of this information. After this call, I'm going to send you an email with a portal link. If you can follow that link and click to confirm the information is accurate, that would be helpful.

Thanks again for your help, and look out for that email in the next few minutes.

<end call>

REMEDIATION STEPS

Social engineering will always remain the most preeminent attack vector and is a major aspect of many real-world cyberattacks. We recommend taking specific remediations to help avoid the dangers we see from these types of attacks. Remediation is not only about user training and education, but also about improving the technical controls that can prevent social engineering attacks from having a larger impact. Based on the results presented in this social engineering assessment we recommend implementing some or all of the following:

Uncategorized DNS Blocking

During the social engineering engagement, the domain used for sending the spearphishing emails and hosting the landing pages was purchased a few days before the engagement began. It is common for a malicious domain to be purchased within a short timeframe before an attack begins. To reduce the risk for these unknown hosts, categorize your outbound DNS requests to block those the DNS provider doesn't recognize.

Force 2-Factor Authentication

Two Factor Authentication (2FA) is known to protect against leaked or stolen credentials. If the 2FA is enforced then even with correct credentials, the attacker won't be able to leverage them to gain access to an employee's email.

Another alternative would be to move the authentication to the internal network requiring VPN to access and login. This would greatly mitigate the threat of reusing phished credentials.

User Training and Education

The findings of the report reaffirm that user education on identifying and reporting phishing emails and other forms of social engineering is critical to company security. Regularly educate your users to flag suspicious emails that they receive to bring awareness of a potential campaign against you.

Have your employees understand that hyperlinks can have deceiving text, even text that can masquerade as a legitimate domain. Further, be aware that attackers will attempt to buy domains from under you to give legitimacy to their email (e.g. "intech.net").

Publicly Accessible Company Information

To reduce the amount of information an attacker could gather on your organization be cognizant of what data is available now and how you will filter yourself in the future. Do not publicly disclose those in management positions throughout your company, be aware of any corporate documents you wish to share and how they might be leveraged against you, as well as removing any metadata associated with them before making it publicly accessible.

Improve Spam Filtering

Email rules can be implemented to reduce the likelihood that a malicious email will end in a user's inbox. Improving filter rules around the age of the domain.

Potential Phishing Domains

Buying up these domain permutations can be a cost-effective way to remove a useful tool for attackers. Social engineers often use these lookalike domains to phish internal users and corporate partners, divulging sensitive information.

Improved Detection and Response Capabilities

implementing detection capabilities and response policies and procedures can greatly reduce the impact of a security event. Improving detection and the response can mitigate.

Recommended Security Assessments

In an effort for constant improvement and security iterative testing, we recommend the following services to test the full impact and likelihood of a social engineering attack.

- Internal Network Penetration Test
- Web Application Penetration Test
- Ongoing Spearphishing and Onsite Social Engineering Test

APPENDIX A: TOOLS & SCRIPTS

The software and tools used for security analysis are constantly evolving and changing. To stay at the forefront of industry trends, Rhino Security Labs regularly updates and integrates new tools into its social engineering methodology. Below is the toolset our consultants use during a social engineering assessment.

Enterprise and Open Source Tools

FOCA

FOCA is used for extracting hidden information and metadata from various sources. Examples include pulling names and emails from Word document files, application versions from PDF's, and more. This can be used for specific targeting of users and companies in phishing and other social engineering engagements.

Metasploit Pro

An open-core commercial Metasploit edition for penetration testers. Metasploit Pro includes modules for tracking emails that have been opened, if and when their links have been opened, if their attachments were downloaded and ran, if a user submitted their credentials to a malicious domain and more.

Spoofcard

Spoofcard is a COTS tool used for spoofing phone numbers. It is a paid for service that anyone is able to use to impersonate a phone number.

Rhino Security Labs Proprietary Tools and Scripts

ShoalScrape

ShoalScrape creates a company profile based on a LinkedIn and other social media pages, enumerating employee information such as job title, department, experience level, and email address.

DNSProfiler

DNSProfiler creates a profile of legitimate client domain registrations using DNS information from known-good sites. Using this profile, DNSProfiler then identifies domain permutations which appear suspicious.

PermFinder

PermFinder gathers a list of domain name permutations, running DNS queries to enumerate information and identify optimal domains for use in a phishing campaign. This tool also identifies phishing domains which have been previously purchased by attackers and is outlined in the assessment report.

Additional Custom Scripts and Application

In addition to the above tools, Rhino Security Labs also makes use of its own proprietary tools and scripts to quickly adapt to new and unique environments.

APPENDIX B: DETAILED CAMPAIGN RESULTS

Below are results of users who opened the phishing email, clicked the attached link, and either submitted credentials or downloaded the attachment.

SPEARPHISHING ENGAGEMENT

- ⚫ Did not open the given phishing email, or the email bounced.
- 🔵 Did not engage with attackers, such as providing sensitive information or downloading files
- 🟡 Engaged with attacker, such as clicking a link, but did not provide sensitive information
- 🔴 Provided sensitive information or downloaded files

DATE	NAME	TITLE	ENGAGEMENT
HH:MM MM-DD-YY	🔴 Peter Livingston	IT Admin	Engagement #1
HH:MM MM-DD-YY	🔴 Michael Bolton	IT Admin	Engagement #2
HH:MM MM-DD-YY	🟡 Samir Naidu	IT Manager	Engagement #1
HH:MM MM-DD-YY	🔵 Milton Root	N/A	Engagement #1
HH:MM MM-DD-YY	⚫ Tom Smykoski	Manager	Engagement #2

PRETEXT CALLING ENGAGEMENT

- ⚫ Did not answer.
- 🟢 Did not engage with attackers, such as providing sensitive information or downloading files
- 🟡 Engaged with attacker, but only provided informational or low risk information.
- 🔴 Provided sensitive information or downloaded files

DATE	NAME	TITLE	ENGAGEMENT
HH:MM MM-DD-YY	🔴 Peter Livingston	IT Admin	Engagement #3
HH:MM MM-DD-YY	🟡 Michael Bolton	IT Admin	Engagement #3
HH:MM MM-DD-YY	🟢 Samir Naidu	IT Manager	Engagement #3
HH:MM MM-DD-YY	🟢 Milton Root	N/A	Engagement #3
HH:MM MM-DD-YY	⚫ Tom Smykoski	Manager	Engagement #3

888.944.8679

info@rhinosecuritylabs.com

1200 East Pike Street Suite 510 | Seattle, WA 98122

RHINO
SECURITY LABS