COMPROMISING FORTUNE 500 BUSINESSES WITHOUT HACKING A THING!

Rachel Tobac
CEO, SocialProof Security
UX Research, Course Hero
@RachelTobac / @socialproofsec

Joe Gray
Senior Security Architect, IBM
@C_3PJoe / @advpersistsec / @hackingglass
The Cold Hard Facts
Phishing Statistics

Source: APWG 3Q2017 Report
### Statistical Highlights for 3rd Quarter 2017

<table>
<thead>
<tr>
<th></th>
<th>July</th>
<th>August</th>
<th>September</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of unique phishing websites detected</td>
<td>60,232</td>
<td>73,393</td>
<td>57,317</td>
</tr>
<tr>
<td>Number of unique phishing e-mail reports (campaigns) received by APWG from consumers</td>
<td>99,024</td>
<td>99,172</td>
<td>98,012</td>
</tr>
<tr>
<td>Number of brands targeted by phishing campaigns</td>
<td>277</td>
<td>313</td>
<td>325</td>
</tr>
</tbody>
</table>

Source: APWG 3Q2017 Report
About Rachel @RachelTobac
About Joe

DERBYCON VII (2017) CLOSING CEREMONY

Chris Hadnagy presenting me with the Trophy
Apply! What will you learn today?

- OSINT concepts and how they lead to social engineering (SE) attacks
- Common social engineering attack methods
- How we won SECTFs
- Examples of what social engineering sounds like
- How to get your organization prepared for SE
HOW WE DO OPEN SOURCE INTELLIGENCE

OSINT against the business and its users
What is OSINT?

Publicly available material:

- The Internet
- Traditional mass media
- Specialized journals, conference proceedings, and think tank studies
- Photos
- Geospatial information
- Social media
What OSINT info do SEs target?

- VPN
- ESSID name
- Make and model of computer
- OS info + service pack/version
- PDF reader
- Browser and version
- Mail client
- Disk encryption
- Any/all software/versions
How I use social media for most OSINT
Instagram OSINT Example
Facebook OSINT Example

Search is Back!
Find people and events on Facebook
Search by location, job, and relationships!

FIND PEOPLE | EVENTS | POSTS & SHARES | PHOTOS

Search for: All people

Gender: All
Interested in: All
Relationship status: All

Current location: 
Interest: 

Current company: Target Company
Current school: 
Job title: 
Language spoken: 
Major: 
Born: year
Name: 

Find people!

[Created by Michael Morgenstern]

Search is Back!
Find people and events on Facebook
Search by location, job, and relationships!

FIND PEOPLE | EVENTS | POSTS & SHARES | PHOTOS

Text in post: Target Company Name or Slogan

Find posts!

Note: If you want to search by text, choose Any posts instead of Friends or Friends of Friends.

[Created by Michael Morgenstern]
Gaining Initial Information

Company Overview of RSA Security LLC

Company Overview
RSA Security LLC provides intelligence-driven security solutions primarily in the United States. The company's solutions help organizations protect their information and manage the identities of the people and applications accessing and exchanging that information. It offers technology solutions, including authentication and credential management, access management, identity administration, and data protection. In addition, the company provides business solutions, including regulatory compliance, password management, consumer identity protection, portal and partner integration, mobile workforce security, and credit/debit card information protection. It serves banking, insurance, technology, ... 

Detailed Description
174 Middlesex Turnpike
Bedford, MA 01730
United States
Founded in 1982
1,202 Employees

Key Executives For RSA Security LLC
Mr. Arthur W. Cotelli Jr.
Former Executive Chairman
Age: 54

Mr. Mark Quigley
Senior Vice President and Chief Operating Officer
Age: 50

Ms. Niloofar Razi Howe
Chief Strategy Officer and Senior Vice President
Age: 48

Mr. Doug Howard
Vice President of Global Services

Mr. Jonathan Gill
Vice President of Europe, Middle East & Africa

Compensation as of Fiscal Year 2017

Software
Company Overview of RSA Security LLC

Snapshot
People

S&P Global
Market Intelligence

The information and data displayed in this profile are created and managed by S&P Global Market Intelligence, a division of S&P Global. Bloomberg.com does not create or control the content. For inquiries, please contact S&P Global Market Intelligence directly by clicking here.

Stock Quotes
Market data is delayed at least 15 minutes

Stock, Fund, or ETF
Go
Company Lookup

Most Searched Private Companies

Company Name
Lawyers Committee for Civil Rights Under Law
The Advertising Council, Inc.
Tax Management Inc
NYC2012, Inc.
John F. Kennedy Center For The Performing Arts

Geographic Region
United States
United States
United States
United States
United States

Sponsored Financial Commentaries

More From The Financial Web
OSINT for Phone Numbers

- Block your number and sweep the organization
- Call outside hours to get names from voicemail
- If you find the directory, search for common last names
Google-Fu

site:company.TLD "xxx-xxx" OR "(xxx) xxx"

Google Search  I'm Feeling Lucky
Google-Fu Next Step

site:company.TLD filetype:PDF OR filetype:docx OR filetype:xlsx

Google Search  I'm Feeling Lucky
Finding Info on People

- Build a repository of people
- Enumerate the people
Finding Info on People Continued

- See what user names they use
- Look for goldmines
- Use this data to build dossiers and leverage it to build rapport
About the domains

- Enumerate information about domains
  - Subdomains
  - MX records
  - SPF
- Technologies used
  - Remote.target.tld
  - VPN.target.tld
We Take a Tour
How do SEs use these data points later?
SOCIAL ENGINEERING

Any act that convinces someone to do something that may or may not be in their best interest.

@RachelTobac
I wish the phone numbers I can find
3rd party vendors posting and tagging you
You help people? You’re getting a call
You posted on social media about your company
Picking Pretexts
Why does SE work on people so well?

- Cialdini’s 6 Principles of Persuasion:
  - Reciprocity
  - Commitment & Consistency
  - Social Proof
  - Liking
  - Authority
  - Scarcity
Will it work on my Windows 10...is that still what you guys use over there???
Derbycon SE Calls

Props

- Office Noises
- Uniforms
- Toolboxes
- Ladders
- Donuts and/or Coffee
- Badges
BRINGING IT ALL TOGETHER: NEXT STEPS
Emoji Takeaways
Training should be timely

2014 - 🕒

All day
Information Security Awareness Training.....
ALL DAY!!!!

Share

👍 1

Sounds thrilling!
2014 at 3:12pm

That's good for ya!
2014 at 3:38pm
Tips for Training

- Do more than the annual training for compliance purposes
- Employ role based training
- Integrate into Incident Response Plan
- Use automated solutions or external contractors to attempt attacks
- Ensure social engineering (specifically phishing, pretexting, and vishing) are included in your penetration tests
Applying what you’ve learned

- Next week you should:
  - OSINT survey on your company
  - talk with management about SE
  - talk with IR team for integration

- In the first three months following this presentation you should:
  - quarterly training scheduled in a shorter format
  - baseline phishing simulation

- Within six months you should:
  - adapt training to current trends and testing results
  - have a second training session
  - OSINT survey and Social Engineering pentest
Resources

- https://github.com/jocephus/RSAC_Resources/
QUESTIONS?

@racheltobac
@C_3PJJoe