PEOPLE-CENTRIC HACKING
HOW SOCIAL MEDIA HABITS LEAD TO CYBER ATTACKS

RIC DAZA, CCIE², CISSP, CRISC, CISA
ASSOCIATE DIRECTOR
UHY - TECHNOLOGY ADVISORY PRACTICE

An independent member of UHY international
AGENDA

1. Overview of the Problem
2. Anatomy of a Hack
3. Tools
4. Examples
5. Countermeasures
Ric Daza
UHY Advisors, Technology Advisory Practice
IT Risk Consultant & Information Assurance Researcher
CCIE²(R/S & Sec), CISSP, CISA, CRISC, ISO 27001 Lead Auditor
rdaza@uhy-us.com
PGP Key ID: B591C414
www.linkedin.com/in/ricdaza
@fountaintech
OPPORTUNITIES FOR HACKERS

Location
• Current Location
• Future Location
• Previous Locations

Email
• Username
• Password Reset
• More private info

Profile
• Name
• Birthday
• Previous Addresses

Social Engineering
• Angler Phishing
• Account Access
• Identity Theft

Previous Locations
ANATOMY OF A HACK

- **Recon**
  - Google
  - Social Networking
  - Image Search
  - LinkedIn

- **Enumeration**
  - Enhanced Searching
  - Infected Website
  - Contact Lists

- **Exploitation**
  - Fake URL
  - Malware
  - Privilege Escalation

- **Persistence**
  - Expand Compromise
  - Lateral Movement
  - Consolidate Persistence
  - Data Exfiltration
ate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.

The **Multi-Attack** method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The **HTA Attack** method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) Full Screen Attack Method
8) HTA Attack Method

99) Return to Main Menu
EXAMPLES

Happy Cousins Day... NOT! This Facebook notification scam is targeting your inbox: [link]

Be wary of scammers attempting to steal in the survey.

Did you see this pic of you? lol [link]

Keep the conversation going.

ag.ky.gov/scams

my cousin
EXAMPLES

Appointment Letter

I am sorry, you haven’t been selected for our next project. Before start please read our guidelines and Read Agreement document carefully.

Project Guidelines

You have to agree to our terms & conditions. If you have any question feel free to ask.

Thank you.
-Admin

Flora Weston

notifications@fullslate.com

https://goo.gl/ozzdDc

http://a1.hellob2b.xyz/ronopp
From: MorganStanley<br/>
<from.id. 554344576222055232547.5543445762@5543445762.brightonapartments.net>

Received: from mailhost.ijsboerke.be ([192.168.100.6])
by stravinsky.b-i-g.be (Kerio Connect 7.0.1)
for bizhouse@hotmail.com

Our records have indicated suspicious activity on your account.
Due to this we had to disable your login until you verify your information.
Simply verify your details and reactivate your login by clicking the following link:
https://www.morganstanleyclientserv.com/5543-PO55/activate/5543445762P0N5

• MorganStanley - ClientServ Team

http://www.gaja-puszczykowo.pl/A4CAf6b4d5/index.php?rec=bizhouse@hotmail.com
Safe Web Report for:

to.tc
Web Site Location  |  Germany

Norton Rating
Norton Safe Web has analyzed to.tc for safety and security problems. Below is a sample of the threats that were found.

Summary
- Computer Threats: 0
- Identity Threats: 1
- Annoyance factors: 0

Total threats on this site: 1

Web sites rated "Caution" may have a small number of threats and annoyances, but are not considered dangerous enough to warrant a red "Warning". Proceed with caution.

The Norton rating is a result of Symantec's automated analysis system. Learn more. The opinions of our users are reflected separately in the community rating on the right.

Community Reviews (0)

Threat Report
1  Phishing Attacks

Threats found: 1

http://to.tc/K94p
COUNTERMEASURES

- Google
- Unshorten.it, Urlex.org, Unshorten.me, CheckShortURL.com
- #internetscam
- Whois
- Check email addresses and @accounts
- IP Geo location
- “If it’s too good to be true...”
  - Money is involved
  - ACT NOW!
  - Use of fear to a sense of urgency
  - Wants more personal information
  - If you aren’t sure, trust your instinct.
COUNTERMEASURES

• How to Spot a Fake Friend Request
  • Little or no history
  • No friends in common
  • Attractive Picture from the Opposite Sex
  • Friend list is mostly one sex - not a mix
  • Little content on their timeline
COUNTERMEASURES...

- Use minimal info to register
- Use strong passwords and change them often.
- Set highest level privacy settings never use default.
- Be wise about what you post. Do not announce when you will be leaving town. Other things you should never post publicly: your address, phone number, driver’s license number, social security number (SSN) or student ID number.
- Verify emails and links in emails you get from any social networking site.
- Install a firewall, anti-spam, and anti-virus software – update frequently!
- Be certain of both the source and content of each file you download. Don't download an executable program just to "check it out."
- Beware of hidden file extensions – "susie.jpg" vs. "susie.jpg.exe"
- When in doubt, don't open it, download it, add it, or give information you may have doubts about sharing.