SOCK PUPPET COBBLER

Mariel Klosterman

OVERVIEW

- Defining Sock Puppets
  - Definitions
  - What They Are
  - Two Main Uses
  - Why Do You Care?
- Creating a Sock Puppet
  - Factors To Consider
  - Account Types
  - Layers of Separation
  - Not Getting Burned

ABOUT

- Mariel Klosterman
- Student at Dakota State University
  - Network & Security Administration, B.S.
- Other projects
  - Cyber Community Club (CX3) - Outreach project geared towards middle school/high school students in the Midwest
- Hobbies
  - Ultimate frisbee and video games

Sock… …Puppets?

DEFINING SOCK PUPPETS

DEFINITIONS

- Why Sock Puppet Cobbler?
  - Cobbler (spy terms) - A forger of identity documents.
  - Or someone who fixes shoes
- Puppeteer - A person who creates sock puppet accounts for either benign or malicious purposes.
- Malicious actor - Someone who, through any means, threatens or attempts to threaten the security of an individual or company for malicious purposes.
- Disinformation - False or misleading information that is spread deliberately to deceive.

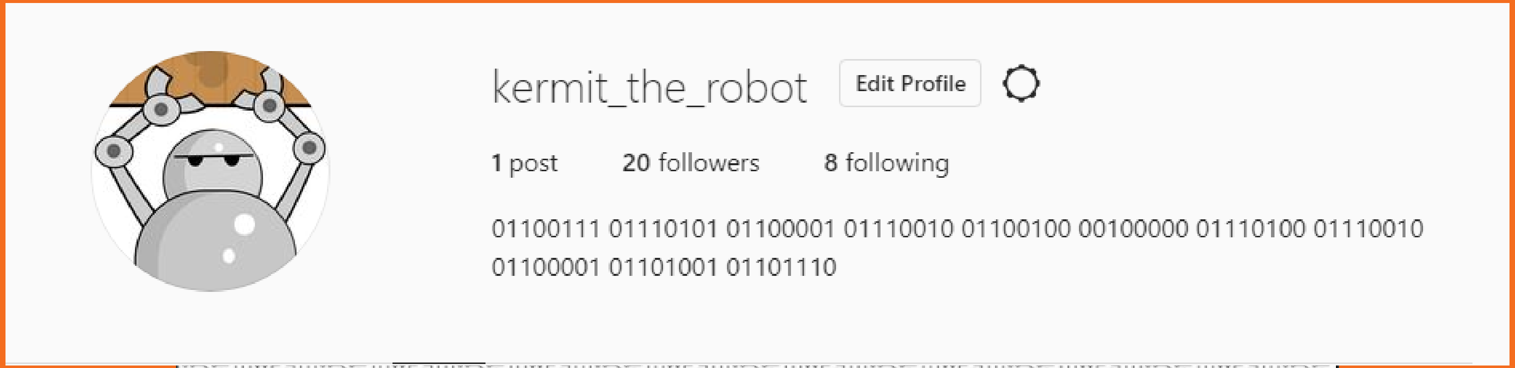
WHAT THEY ARE

- Alternative accounts on social platforms in order to either collect or disperse information.
- Why are they used?
    - Propaganda
    - Algorithms and trackers rat you out
    - Distance between you and your target

TWO MAIN USES

- Spreading information
  - Propaganda
  - Disinformation
- Collecting information
  - For passive reconnaissance (open-source intelligence)
  - For active reconnaissance (human intelligence)

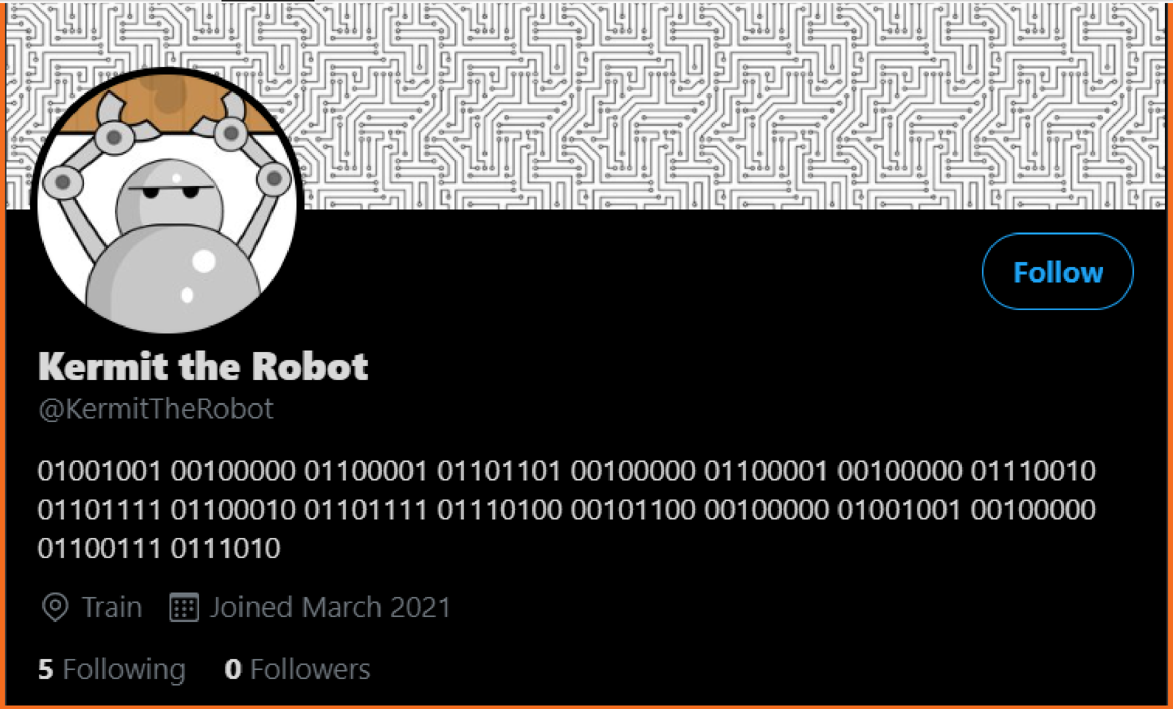
EXAMPLE SOCK PUPPET



kermit_the_robot

1 post **20** followers **8** following

01100111 01110101 01100001 01110010 01100100 00100000 01110100 01110010
01100001 01101001 01101110



Kermit the Robot

@KermitTheRobot

01001001 00100000 01100001 01101101 00100000 01100001 00100000 01110010
01101111 01100010 01101111 01110100 00101100 00100000 01001001 00100000
01100111 0111010

Train Joined March 2021

5 Following **0** Followers

WHY DO YOU CARE?

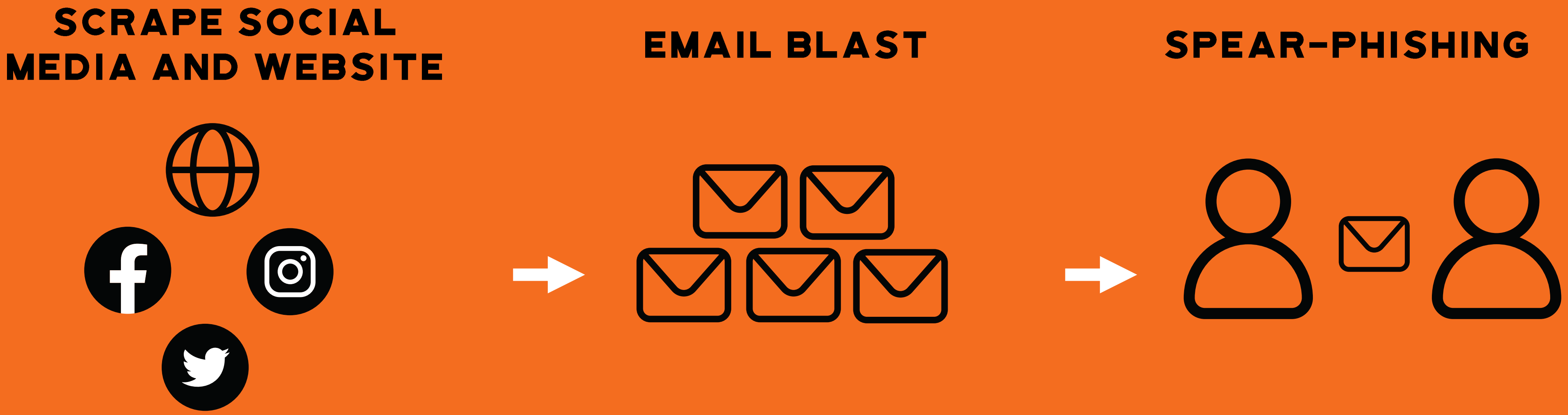
REPUTATION RISK MANAGEMENT

- Product reviews
- Store or business reviews
- Comments or posts intended to harm business

RECONNAISSANCE & EXPLOITATION

- Personal information
- Convincing spear-phishing

SIMPLE SPEAR-PHISHING EXAMPLE

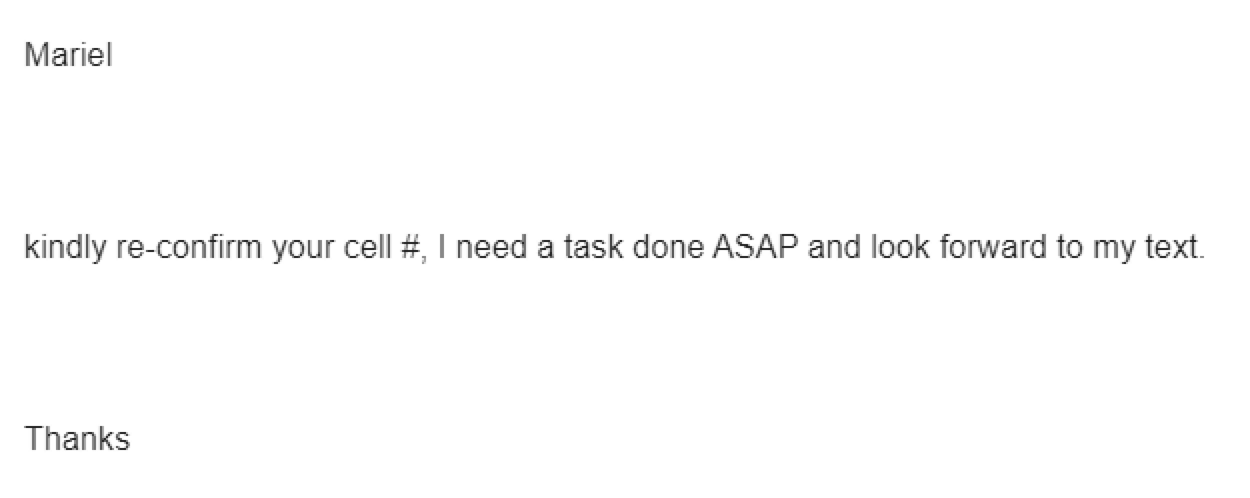


SCRAPE SOCIAL MEDIA AND WEBSITE

EMAIL BLAST

SPEAR-PHISHING

PHISHING EMAIL

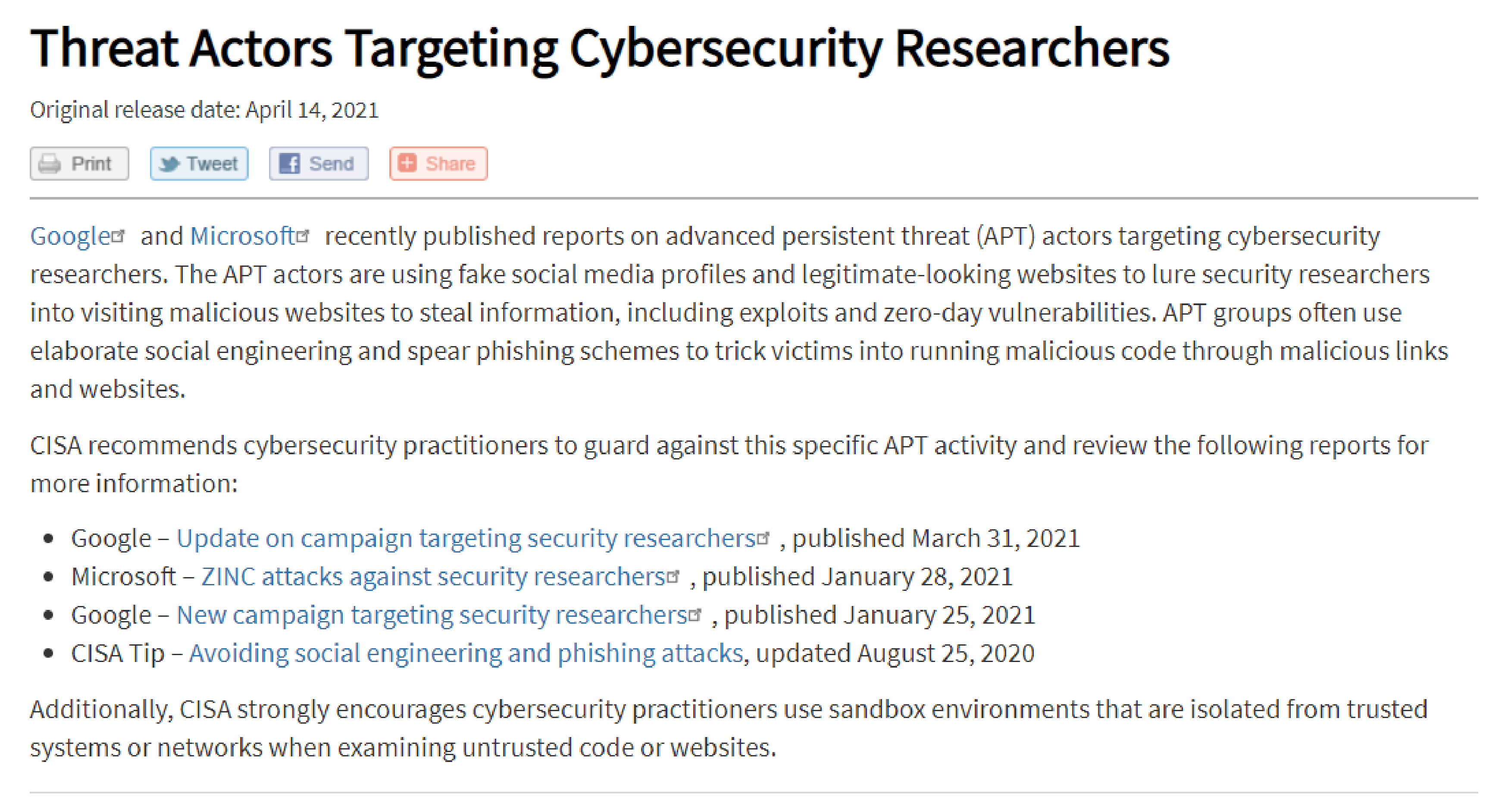


Mariel

kindly re-confirm your cell #, I need a task done ASAP and look forward to my text.

Thanks

CISA ALERT



Threat Actors Targeting Cybersecurity Researchers

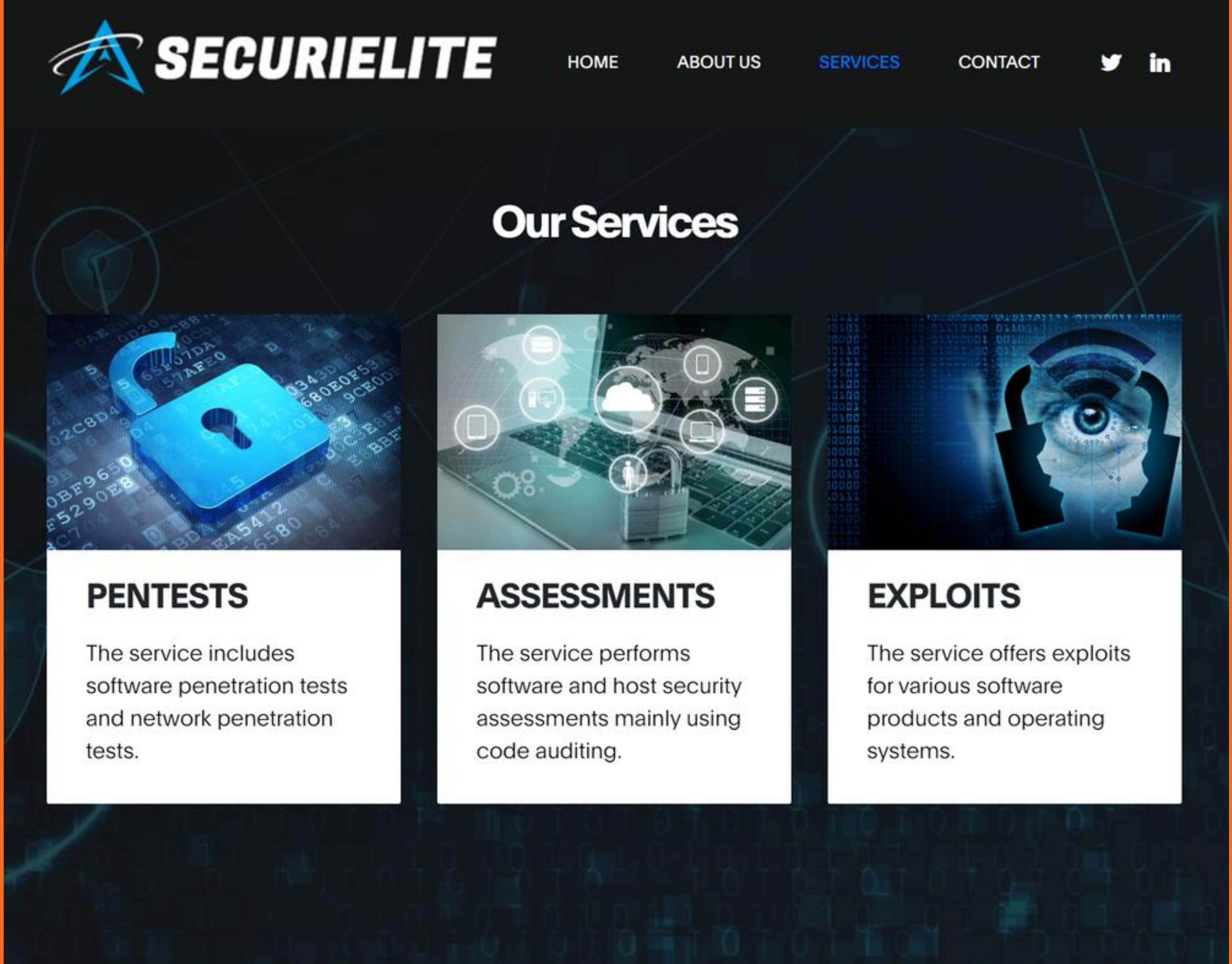
Original release date: April 14, 2021

Google and Microsoft recently published reports on advanced persistent threat (APT) actors targeting cybersecurity researchers. The APT actors are using fake social media profiles and legitimate-looking websites to lure security researchers into visiting malicious websites to steal information, including exploits and zero-day vulnerabilities. APT groups often use elaborate social engineering and spear phishing schemes to trick victims into running malicious code through malicious links and websites.

CISA recommends cybersecurity practitioners to guard against this specific APT activity and review the following reports for more information:

- Google – Update on campaign targeting security researchers , published March 31, 2021
- Microsoft – ZINC attacks against security researchers , published January 28, 2021
- Google – New campaign targeting security researchers , published January 25, 2021
- CISA Tip – Avoiding social engineering and phishing attacks, updated August 25, 2020

Additionally, CISA strongly encourages cybersecurity practitioners use sandbox environments that are isolated from trusted systems or networks when examining untrusted code or websites.



Our Services

PENTESTS

The service includes software penetration tests and network penetration tests.

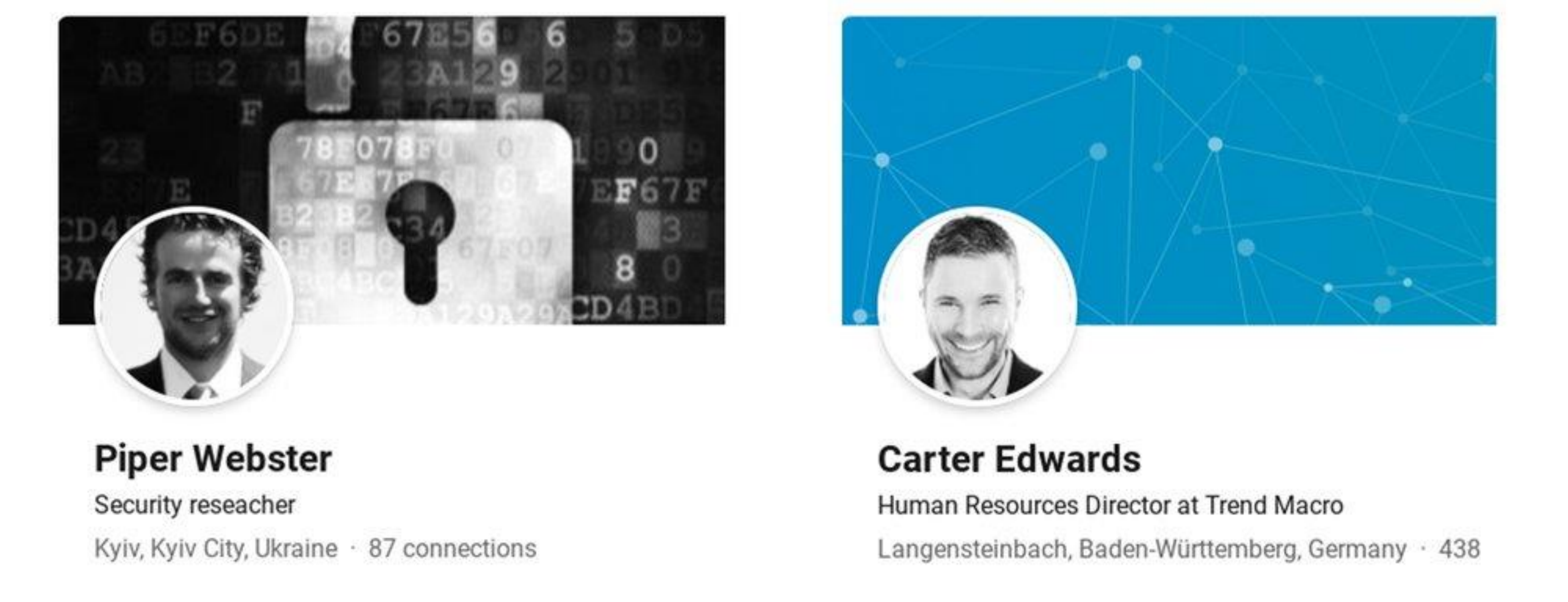
ASSESSMENTS

The service performs software and host security assessments mainly using code auditing.

EXPLOITS

The service offers exploits for various software products and operating systems.

RECENT EXAMPLE



Piper Webster

Security reseacher

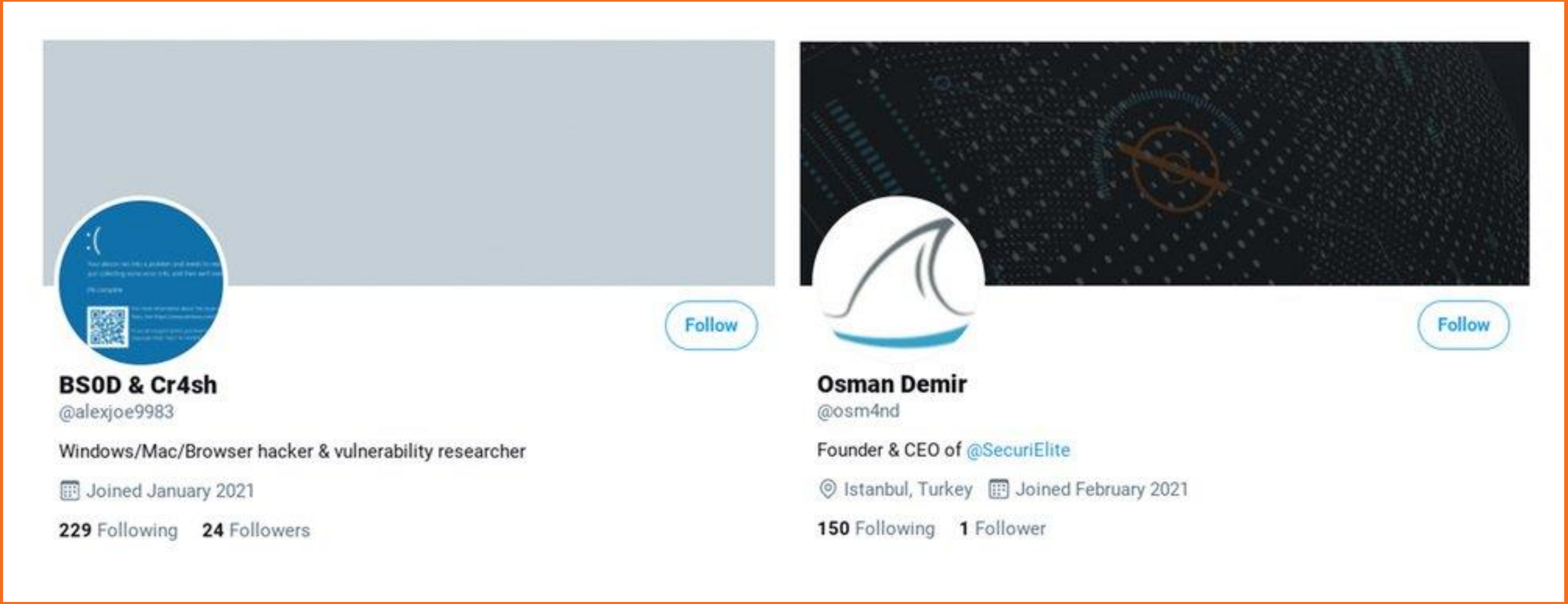
Kyiv, Kyiv City, Ukraine · 87 connections

Carter Edwards

Human Resources Director at Trend Macro

Langensteinbach, Baden-Württemberg, Germany · 438

RECENT EXAMPLE



BSOD & Cr4sh
@alexjoe9983

Windows/Mac/Browser hacker & vulnerability researcher

Joined January 2021

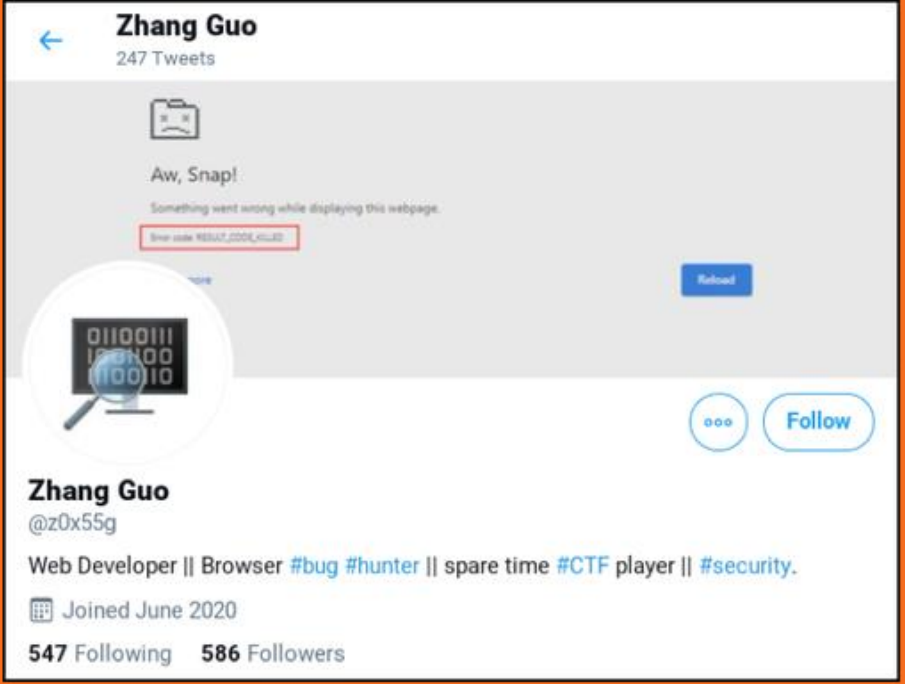
229 Following **24** Followers

Osman Demir
@osm4nd

Founder & CEO of @SecuriElite

Istanbul, Turkey Joined February 2021

150 Following **1** Follower


Aw, Snap!
Something went wrong while displaying this webpage.
Error code: RESULT_CODE_KILLED
Reload

Zhang Guo
247 Tweets

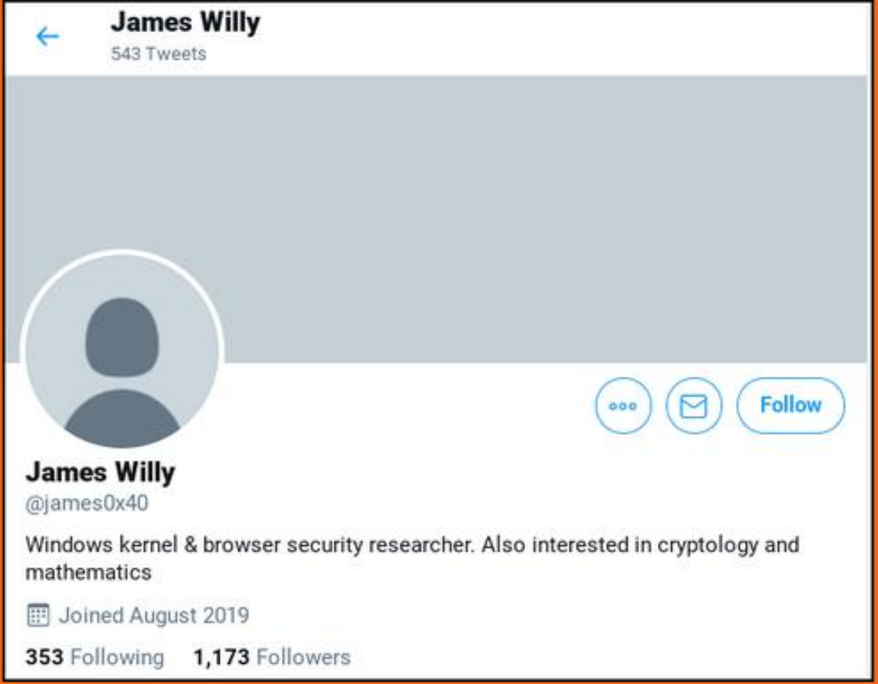
Follow

Zhang Guo
@z0x55g

Web Developer || Browser #bug #hunter || spare time #CTF player || #security.

Joined June 2020

547 Following **586** Followers



James Willy
543 Tweets

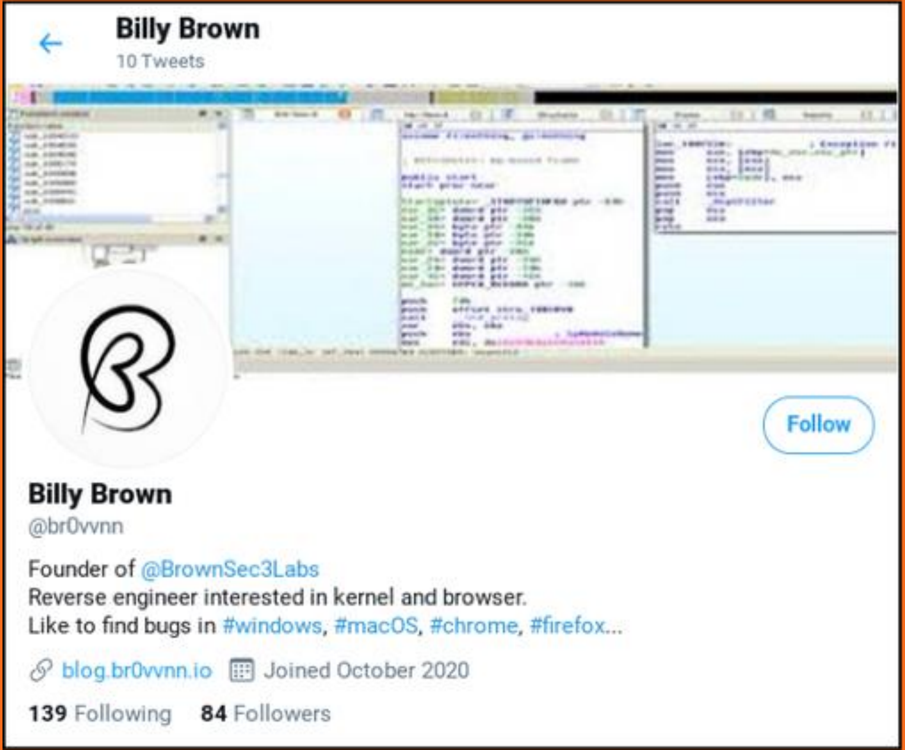
Follow

James Willy
@james0x40

Windows kernel & browser security researcher. Also interested in cryptology and mathematics

Joined August 2019

353 Following **1,173** Followers



Billy Brown
10 Tweets

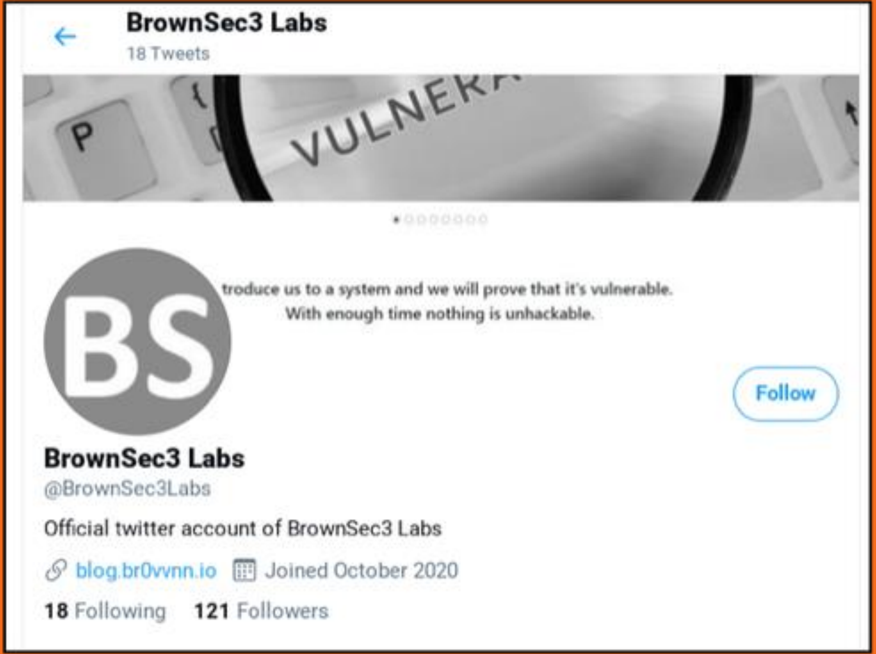
Follow

Billy Brown
@br0vvnn

Founder of @BrownSec3Labs
Reverse engineer interested in kernel and browser.
Like to find bugs in #windows, #macOS, #chrome, #firefox...

blog.br0vvnn.io Joined October 2020

139 Following **84** Followers


VULNERA
troduce us to a system and we will prove that it's vulnerable.
With enough time nothing is unhackable.
BS

BrownSec3 Labs
18 Tweets

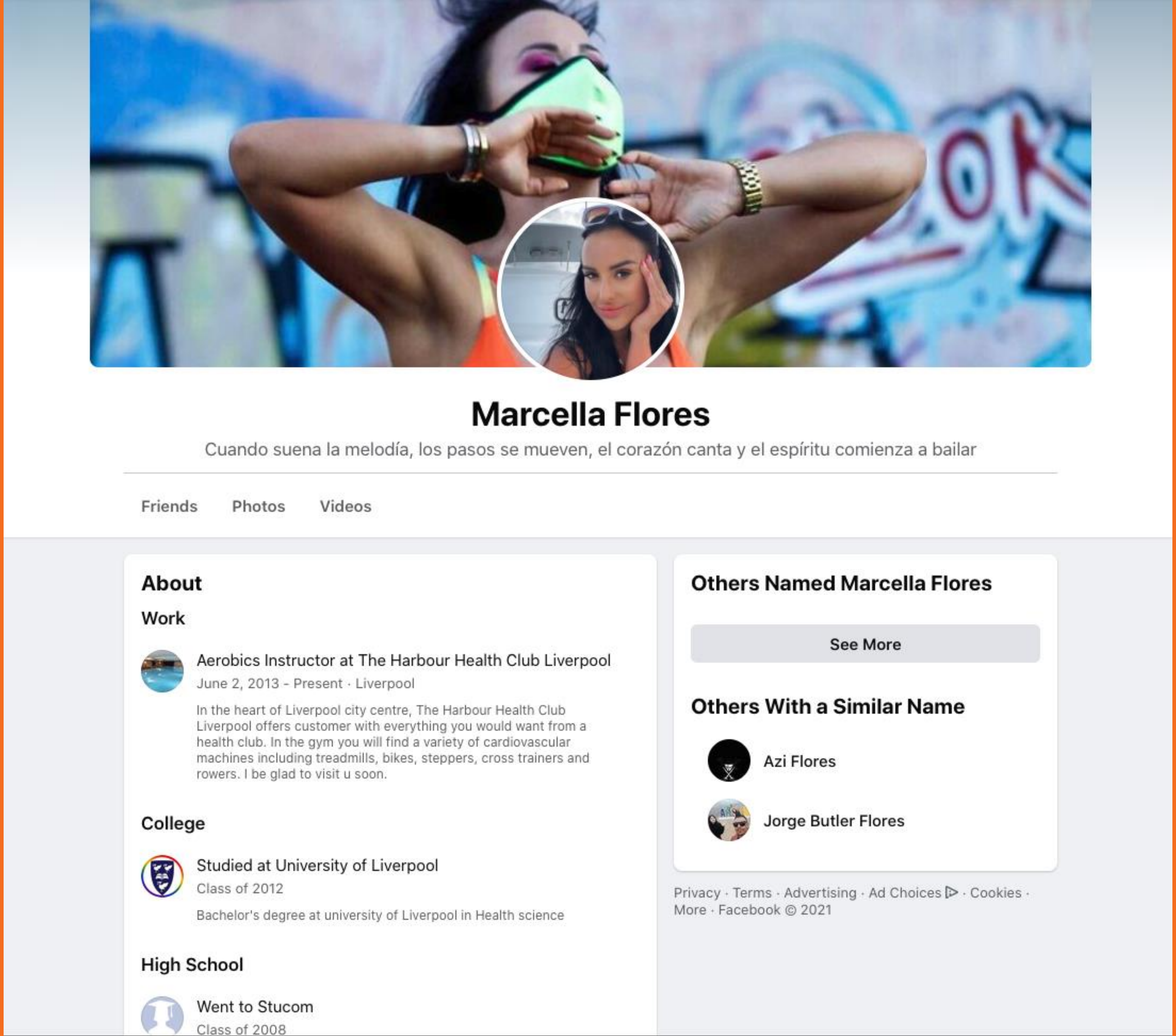
Follow

BrownSec3 Labs
@BrownSec3Labs

Official twitter account of BrownSec3 Labs

blog.br0vvnn.io Joined October 2020

18 Following **121** Followers



Marcella Flores

Cuando suena la melodía, los pasos se mueven, el corazón canta y el espíritu comienza a bailar

About

Work

Aerobics Instructor at The Harbour Health Club Liverpool
June 2, 2013 - Present · Liverpool

In the heart of Liverpool city centre, The Harbour Health Club Liverpool offers customer with everything you would want from a health club. In the gym you will find a variety of cardiovascular machines including treadmills, bikes, steppers, cross trainers and rowers. I be glad to visit u soon.

College

Studied at University of Liverpool
Class of 2012

Bachelor's degree at university of Liverpool in Health science

High School

Went to Stucom
Class of 2008

Others Named Marcella Flores

Others With a Similar Name

- Azi Flores
- Jorge Butler Flores

Privacy · Terms · Advertising · Ad Choices ▷ · Cookies · More · Facebook © 2021

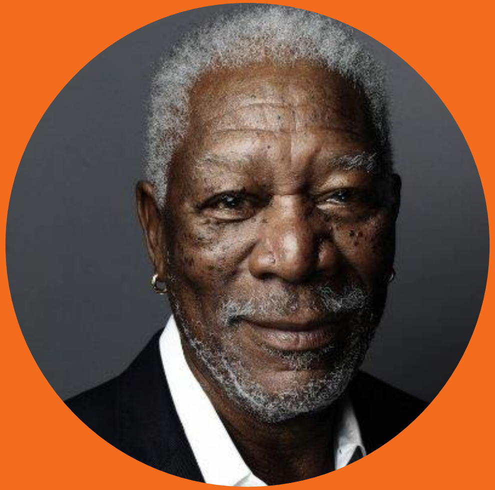
CREATING A SOCK PUPPET

FACTORS TO CONSIDER

- Anonymity vs. Privacy
  - Not the same thing
- Anonymity - When you cannot be linked to the account no matter how deep someone looks for the link.
- Persistence - When you want to be active on the platform.
- Throwaway vs. persistent accounts

ACCOUNT TYPES

MORGAN FREEMAN



Persona
Typically a single person.

SWIFT ON SECURITY

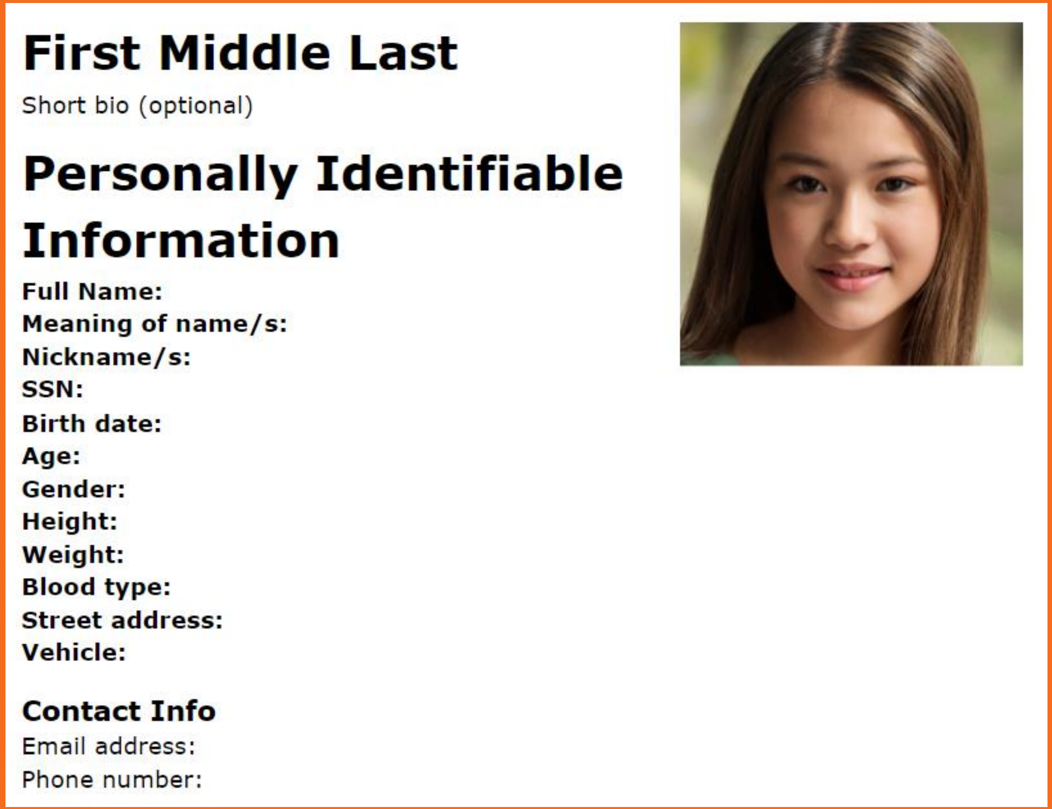
Avatar
Usually based around an idea.

LAYERS OF SEPARATION

- Dedicated computer
- Virtual machine (VM)
- Email address
- Virtual private network (VPN)
- “Burner” phone
- *Remove these items or add others*

MY SIMPLE SETUP

1. Creation
   1. Set up computer
   2. Create Profile Document
   3. Virtual machine
      1. Time zone, location
   4. Email address
   5. Social Media
      1. Profile picture
      2. Banner
      3. Description
2. Aging
   1. Log in around the same time
   2. Like/follow/share



First Middle Last

Short bio (optional)

Personally Identifiable Information

Full Name:
Meaning of name/s:
Nickname/s:
SSN:
Birth date:
Age:
Gender:
Height:
Weight:
Blood type:
Street address:
Vehicle:

Contact Info

Email address:
Phone number:

PROFILE TEMPLATE

NOT GETTING BURNED

Trolls are more likely to

- Post on controversial topics
- Have no profile picture, or ones that look generated
- Be new with no followers or friends

Legitimate users usually

- Scroll through and look at posts
- Login at regular times
- Have a few followers/friends

TAKEAWAYS

- Sock puppets can be used for malicious purposes
  - Spear-phishing and exploitation
  - Negative comments, bad reviews
- Also used for
  - Investigating suspects
  - Verifying identity
- Train your company to be aware of what sock puppets can do and report suspicious behavior
  - OOO email policies
  - Social media audit

EXAMPLE AUTO-RESPONDER

Dear Friends, Clients and Colleagues,

Sadly, due to deadlines, I am unable to read or respond to most email. Please don’t be offended, as this is true even for close friends.

I check email twice daily at midday and 4:00 PM UTC Monday-Friday. I respond to urgent email at those times and endeavor to respond to all other email on Fridays.

QUESTIONS?

WANT TO CONNECT WITH ME?

LINKEDIN

@MarielKlosterman

EMAIL ADDRESS

mlklos@protonmail.com

PROJECT PAGE

AgentSandstone.com/Project/Sock-Puppet-Cobbler