Establish Accounts: Social Media Accounts

Resource Development - T1585.001

MITRE ATT&CK

Establish Accounts: Social Media Accounts

Other sub-techniques of Establish Accounts (2)

Adversaries may create and cultivate social media accounts that can be used during targeting. Adversaries can create social media accounts that can be used to build a persona to further operations. Persona development consists of the development of public information, presence, history and appropriate affiliations.[1][2]

For operations incorporating social engineering, the utilization of a persona on social media may be important. These personas may be fictitious or impersonate real people. The persona may exist on a single social media site or across multiple sites (ex: Facebook, LinkedIn, Twitter, etc.). Establishing a persona on social media may require development of additional documentation to make them seem real. This could include filling out profile information, developing social networks, or incorporating photos.

ID: T1585.001

Sub-technique of: T1585

Tactic: Resource Development

Platforms: PRE

Version: 1.1

Created: 01 October 2020

Last Modified: 16 October 2021

Version Permalink

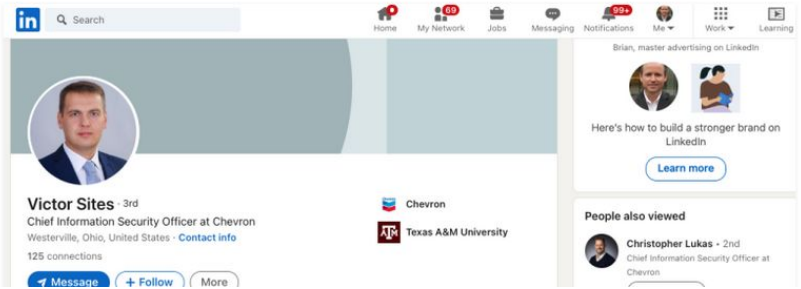
Fake LinkedIN Accounts

Fake CISO Profiles on LinkedIn Target Fortune 500s

September 29, 2022 26 Comments

Someone has recently created a large number of fake **LinkedIn** profiles for **Chief Information Security Officer** (CISO) roles at some of the world's largest corporations. It's not clear who's behind this network of fake CISOs or what their intentions may be. But the fabricated LinkedIn identities are confusing search engine results for CISO roles at major companies, and they are being indexed as gospel by various downstream data-scraping sources.

If one searches LinkedIn for the CISO of the energy giant **Chevron**, one might find the profile for a Victor Sites, who says he's from Westerville, Ohio and is a graduate of Texas A&M University.



Recently on Krebs on Security this was observed

https://krebsonsecurity.com/2022/09/fake-ciso-profiles-on-linkedin-target-fortune-500s/

13lives - Video

“Thirteen Lives” - Amazon Prime Original Movie

In the true story of Thirteen Lives, twelve boys and the coach of a Thai soccer team explore the **Tham Luang cave** when an unexpected rainstorm traps them in a chamber inside the mountain. Entombed behind a maze of flooded cave tunnels, they face impossible odds. A team of world-class divers navigate through miles of dangerous cave networks to discover that finding the boys is only the beginning.

Prayut Chan-o-cha was the Prime Minister of Thailand during this time frame.

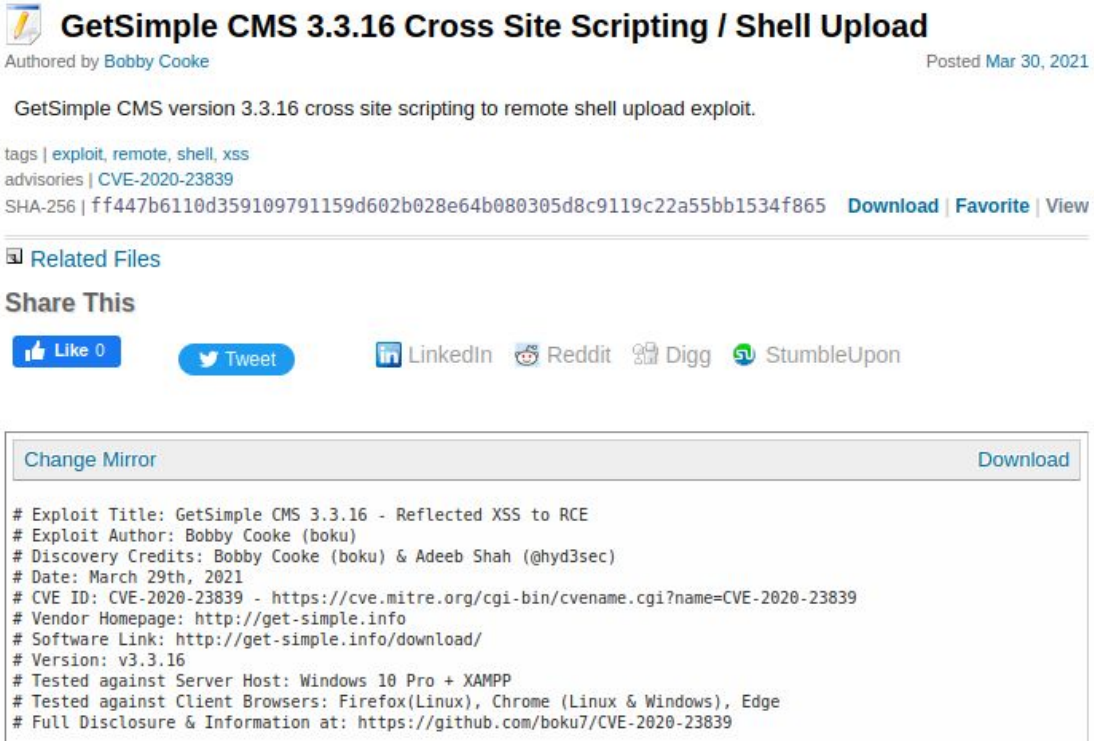
Fake Scenario - Based on Events of 13 Lives

Disclaimer: The scenario today is based on this true story. The scenario today is not meant to disrespect anyone or anything based on the events of the true story or the movie. The accounts created are based on the people in the movie.

Executives and Government dignitaries are targets of attacks constantly. You were asked by the Prime Minister to conduct a red team engagement to identify weaknesses in People, Processes and Technology.

This scenario starts with identifying a system administrator that manages the CMS site http://13lives.4gr8.info. After conducting some research you identify through social media articles an executive assistant uses the email of prayut.c@yahoo.com and one of the athletes Chanin Wibunrungrueang mentions in his LinkedIn profile that he is the administrator of the CMS site.

Research Exploits for Site



GetSimple CMS 3.3.16 Cross Site Scripting / Shell Upload

Authored by Bobby Cooke — Posted Mar 30, 2021

GetSimple CMS version 3.3.16 cross site scripting to remote shell upload exploit.

tags | exploit, remote, shell, xss
advisories | CVE-2020-23839
SHA-256 | ff447b6110d359109791159d602b028e64b080305d8c9119c22a55bb1534f865 **Download** | **Favorite** | View

Related Files

Share This

Like 0 Tweet LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Title: GetSimple CMS 3.3.16 - Reflected XSS to RCE
# Exploit Author: Bobby Cooke (boku)
# Discovery Credits: Bobby Cooke (boku) & Adeeb Shah (@hyd3sec)
# Date: March 29th, 2021
# CVE ID: CVE-2020-23839 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-23839
# Vendor Homepage: http://get-simple.info
# Software Link: http://get-simple.info/download/
# Version: v3.3.16
# Tested against Server Host: Windows 10 Pro + XAMPP
# Tested against Client Browsers: Firefox(Linux), Chrome (Linux & Windows), Edge
# Full Disclosure & Information at: https://github.com/boku7/CVE-2020-23839
```