LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

HC3 Recent Threats Overview

11/2/2020

Agenda

Image source: teiss.co.uk

- Cybercriminal actors continue to take advantage of the pandemic
- Ransomware
- Social Media Attacks

Cybercriminals Continue to Exploit Pandemic

Financially-motivated cybercriminals continue to exploit the with targets across a variety of industry verticals including:

- Finance
- **Healthcare**
- **Pharmaceutical**
- Government
- Consulting
- Manufacturing
- Education
- Technology
- Telecommunications

Image source: Panda Security

To maximize damage and financial gain, cybercriminals are shifting their targets from individuals and small businesses to major corporations, governments and critical infrastructure, which play a crucial role in responding to the outbreak, according to INTERPOL.

Coronavirus-themed Phishing

- Global COVID-19 campaigns include lures themed on regional health authority impersonations, fake vaccination information, purchase or delivery of personal protective equipment (PPE), employee targets spoofed from HR, medical and pharmaceutical supplies, and even false job promises.
- Some of the latest lures include updates on the evolution of the virus and malicious attachments that infect victims when accessed. Scammers also act under the guise of the government, leveraging the temporary ban on importing or exporting goods, or financial institutions offering COVID-19 Financial Relief.
- In late July, the FBI warned that cyber actors using Netwalker ransomware had taken advantage of the COVID-19 pandemic to compromise an increasing number of unsuspecting victims. The FBI alert notes that the operators behind Netwalker are luring victims with pandemic-themed phishing e-mails that contain an attachment with a malicious Visual Basic Scripting, or VBS, script that executes the payload once opened.

Image source: Bitdefender

Coronavirus-themed Phishing (cont.)

- A recent example of a phishing email advertising personal protective equipment (PPE) was detected by Bitdfender in July 2020.

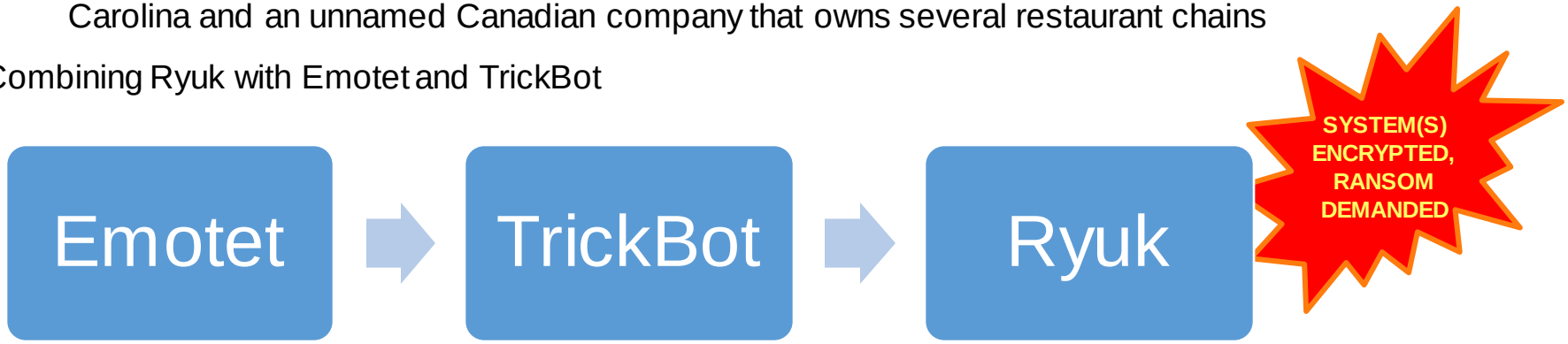
Image source: Bitdefender

Ransomware

- DHS, FBI, HHS Joint Product
- This joint cybersecurity advisory was coauthored by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS). This advisory describes the tactics, techniques, and procedures (TTPs) used by cybercriminals against targets in the Healthcare and Public Health (HPH) Sector to infect systems with ransomware, notably Ryuk and Conti, for financial gain.
- CISA, FBI, and HHS have credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers. CISA, FBI, and HHS are sharing this information to provide warning to healthcare providers to ensure that they take timely and reasonable precautions to protect their networks from these threats.

Ransomware

- Initial activity
  - August 2018 to Jan 2019: $4.7M USD in BTC acquired
  - Used in cyberattacks targeting various newspapers in December (slight delays in delivery but no significant operational impact):
    - San Diego Union-Tribune
    - Los Angeles Times and Tribune Publishing
      - Includes Chicago Tribune, New York Daily News, Baltimore Sun and Orlando Sentinel
  - Used to attack cloud hosting provider Data Resolution, Onslow Water and Sewer Authority in North Carolina and an unnamed Canadian company that owns several restaurant chains
- Combining Ryuk with Emotet and TrickBot



  - "Along with Emotet, TrickBot has become one of the most versatile and dangerous pieces of modular malware hitting enterprise environments." – HelpNet Security
  - "Interactive deployment of ransomware" to conduct reconnaissance and ultimately "maximize their disruption of business operations" - FireEye

Ransomware

- BAZARLOADER USE IN RANSOMWARE CAMPAIGNS
- September 28, 2020, security researchers openly shared recent observations associated with RYUK ransomware deployments. This information comes following recent news reporting of a potential RYUK ransomware incident affecting a large US healthcare entity. Recent ransomware campaigns leveraged phishing followed by deployment of malware associated with TRICKBOT actors.

Social Media Attacks - Introduction

- Social media – What is it? (Web 2.0)
  - **Social**: Interacting with and exchanging information with other people
  - **Media**: An instrument or platform of communication
- Social media attacks represent the largest modern threat vector and are at an all-time high. Why?
  - Roughly 3.5 billion people on social media
- Social media attacks are estimated to generate over $3 billion annually for cyber criminals
  - 60% increase since 2017
- 1.3 billion users have had their data compromised in the last five years
  - Almost half of all illicit exchange of information in 2017 and 2018 was associated with social media breaches
- Social media platforms are often used for authentication to other websites/applications/platforms
  - This is a major attack vector
- Social media attacks can be used to compromise healthcare organizations

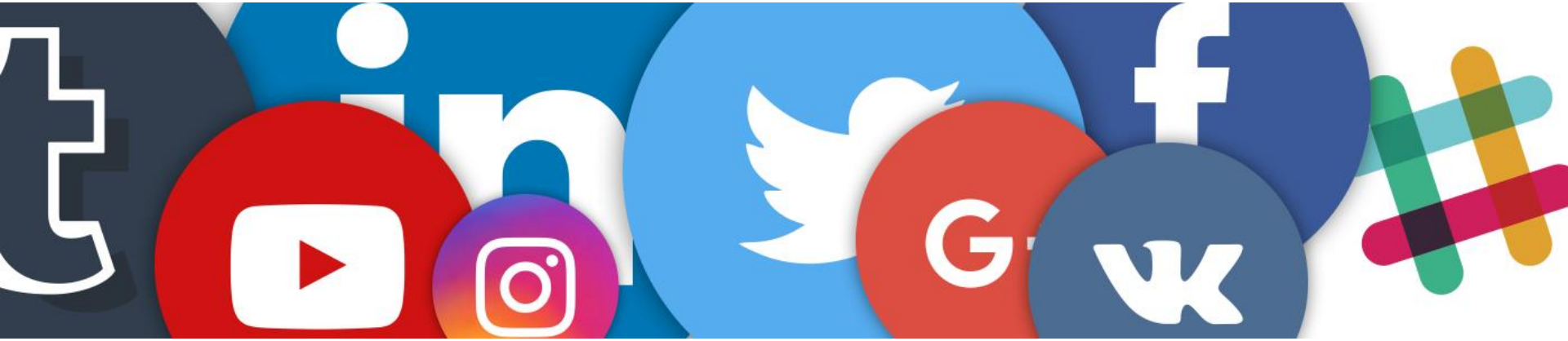


Image source: ZeroFox

Anatomy of a Social Media Attack

- Four step process:
  1. **Footprinting** – Gather as much information as possible about the target organization to identify a weak point
     - Identify employees, especially executives
     - Identify brand accounts
     - Acquire public names, email address and phone numbers
     - Find sensitive information through physical collection
  2. **Monitoring** – Observe social media habits, enabling more effective attacks
     - Observe personnel public communications, especially executives
     - Find/observe social media connections between individuals.
     - Document posted interests (hashtags, keywords)
  3. **Impersonate/Hijack** – Spoof entity to establish trust for attack
     - Establish similar looking profile
     - Hijack active account through an attack campaign
     - Hijack old/inactive account
  4. **Attack** – Launch primary attack
     - Launch malicious link campaign
     - Use account for social engineering attacks
     - Use account to discredit organization

Personal information commonly exposed by social networks

Linkedin	company employees, titles, locations, email addresses, phone numbers, former employees
Twitter	bio, interests, other Twitter accounts they own, other brands/sub-brands, employees responsible for managing brand accounts, followers
Facebook	bio, birthday, interests, hobbies, connections
Google+	corporate ID or login, interests, hobbies, connections

Information targets for attackers

Source of images: Zero Fox