LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Social Media Attacks

06/04/2020

Report #: 202006041300

Agenda

- HC3 Overview
  - Mission
  - Sector Information Sharing
- Threat Brief
  - Overview
  - Types of Social Media
  - Attack Vectors and Targets
  - Impacts of Breaches
  - Attacks on Enterprises
  - Nontraditional Vectors
  - Social Media in Healthcare
  - Anatomy of an Attack
  - Single Sign-on (SSO)
  - Disinformation
  - Healthcare disinformation examples

Slides Key:

Non-Technical: managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Mission

HC3 Mission Statement

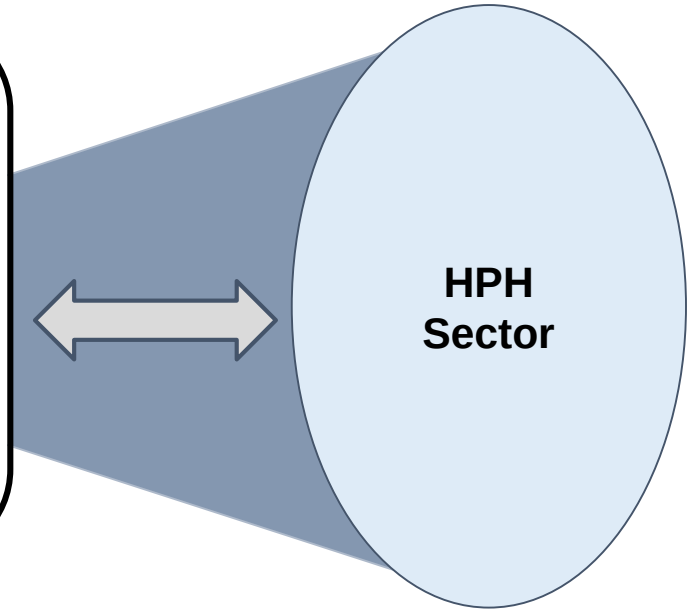
To support the defense of the healthcare and public health sector's information technology infrastructure by strengthening coordination and information sharing within the sector and by cultivating cybersecurity resilience, regardless of organizations' technical capacity.

Sector Information Sharing Partner

The U.S. Department of Health and Human Services (HHS) created HC3 to help identify, correlate, and communicate cybersecurity information across the healthcare and public health (HPH) sector.

HC3's Role in Helping the Sector

- Ensure cybersecurity information sharing is coordinated with the HPH sector, including within HHS and with government partners.
- Facilitate access to knowledge-based resources necessary to support robust cybersecurity programs and mitigate damage in security breach situations.



HC3 focuses on assisting private sector entities in defending against cybersecurity threats and ultimately reducing risk.

Regulatory Provisions: Federal Entities on Information Sharing

- According to the U.S. Code 6 U.S.C. subsection 1501(3), any non-federal organization that shares cyber threat indicators with an appropriate federal entity is deemed voluntary data sharing, and is exempt from disclosure {Section 552 of Title 5 U.S.C.}.
- This information cannot be used against entities sharing information; as such HC3 does not report to the Office of Civil Rights (OCR) within HHS, nor share data.
- Therefore, HC3 is **separate** from OCR and its reporting requirements, and does **NOT** report on an entity to OCR.

Core Functions

As HC3 continues to mature operationally, it strives to increase its reach and ensure shared information is impactful to the HPH sector as a whole. In support of that goal, HC3 performs the following two core functions.

Cyber Threat Intelligence

- Provides timely and actionable information tailored to HPH sector needs.
- Leverages partner organizations to reach large stakeholder groups.
- Researches incidents for product enrichment.

Cyber Engagement

- Fosters, maintains, and matures partnerships with the private and public HPH sector.
- Strengthens coordination and communication activities across the private and public HPH sector.
- Facilitates incident notifications with law enforcement partners.

HC3 is helping provide the right information in front of the right teams at the right time.

Products and Cyber Threat Briefings

HC3 develops unclassified, knowledge-based resources geared towards promoting and increasing HPH sector cyber knowledge and hosts a monthly forum (via webinar) to brief active cybersecurity threats for sector-wide participation.

Threat Briefings

Product Overview

Briefing document that highlights relevant cybersecurity topics and raises the HPH sector's situational awareness of current cyber threats, best practices, and mitigation tactics.

Distro Method

- Email
- ASPR Sector Newsletter
- Uploaded to CHWG Portal

White Papers

Product Overview

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide recommendations to a wide audience.

Distro Method

- Email
- ASPR Sector Newsletter
- Uploaded to CHWG Portal

Threat Briefing Webinar

Forum Overview

Briefing that provides actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Frequency

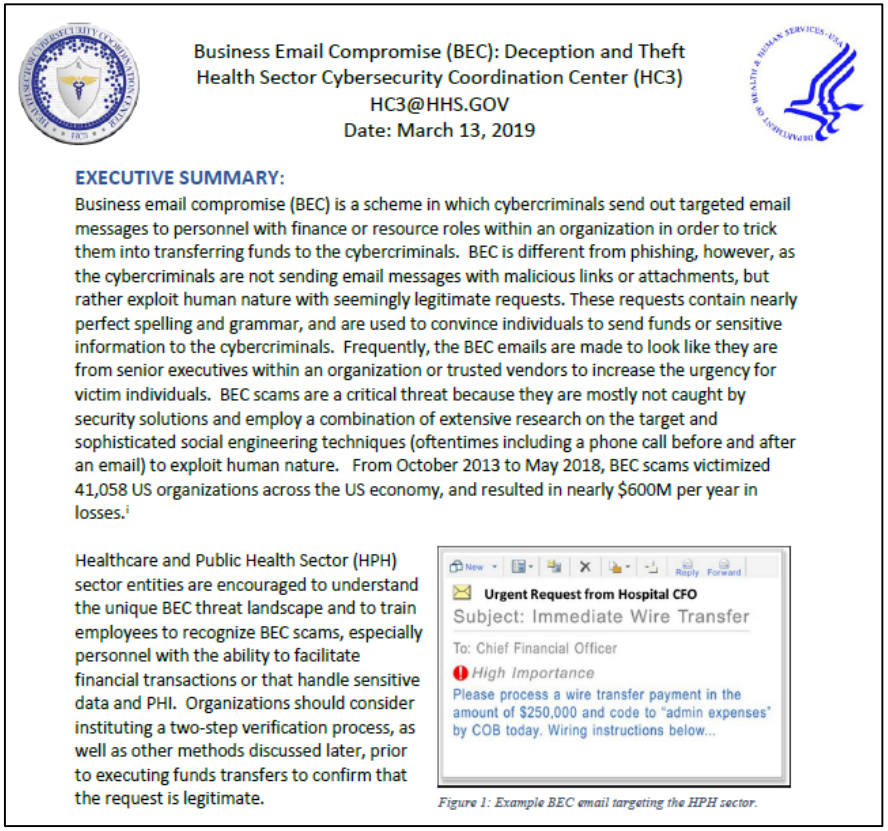
Briefings are hosted on a monthly basis.

Product Example (White Paper)

In March 2019, HC3 developed and released a white paper on Business Email Compromise (BEC) with situational background and protection strategies for the sector. The screenshot below is an example of one section of the product.

High-level, situational background information providing context for non-technical audience

Summarized protection strategies with details in subsequent sections for technical and non-technical audiences



Business Email Compromise (BEC): Deception and Theft
Health Sector Cybersecurity Coordination Center (HC3)
HC3@HHS.GOV
Date: March 13, 2019

EXECUTIVE SUMMARY:

Business email compromise (BEC) is a scheme in which cybercriminals send out targeted email messages to personnel with finance or resource roles within an organization in order to trick them into transferring funds to the cybercriminals. BEC is different from phishing, however, as the cybercriminals are not sending email messages with malicious links or attachments, but rather exploit human nature with seemingly legitimate requests. These requests contain nearly perfect spelling and grammar, and are used to convince individuals to send funds or sensitive information to the cybercriminals. Frequently, the BEC emails are made to look like they are from senior executives within an organization or trusted vendors to increase the urgency for victim individuals. BEC scams are a critical threat because they are mostly not caught by security solutions and employ a combination of extensive research on the target and sophisticated social engineering techniques (oftentimes including a phone call before and after an email) to exploit human nature. From October 2013 to May 2018, BEC scams victimized 41,058 US organizations across the US economy, and resulted in nearly $600M per year in losses.[i]

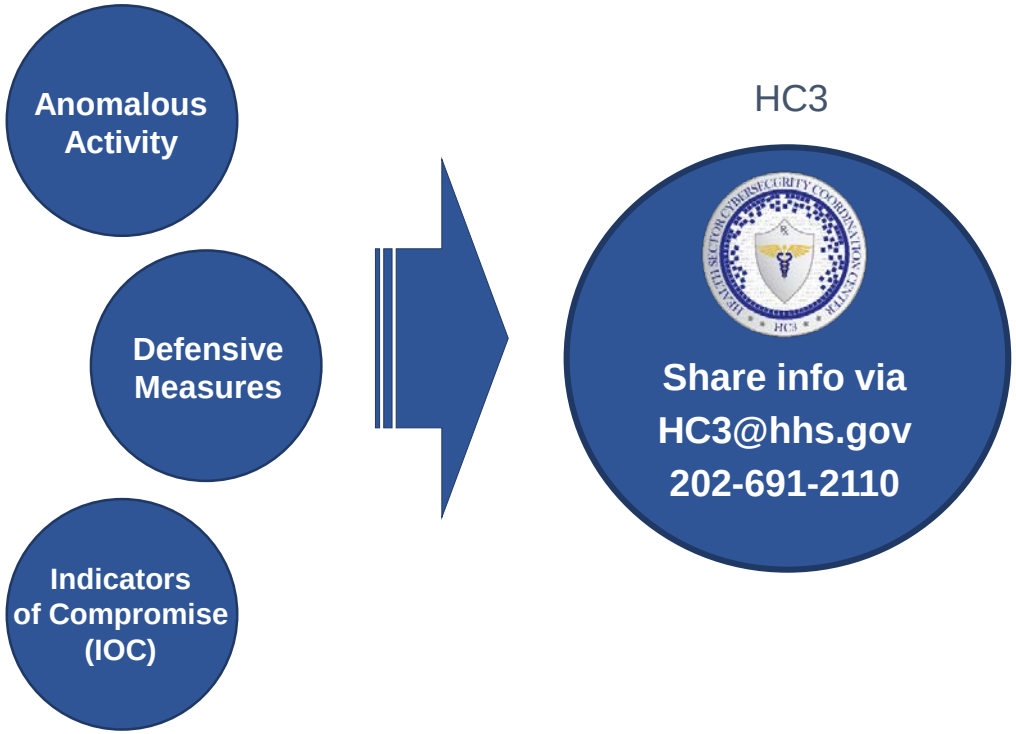
Healthcare and Public Health Sector (HPH) sector entities are encouraged to understand the unique BEC threat landscape and to train employees to recognize BEC scams, especially personnel with the ability to facilitate financial transactions or that handle sensitive data and PHI. Organizations should consider instituting a two-step verification process, as well as other methods discussed later, prior to executing funds transfers to confirm that the request is legitimate.

Figure 1: Example BEC email targeting the HPH sector.

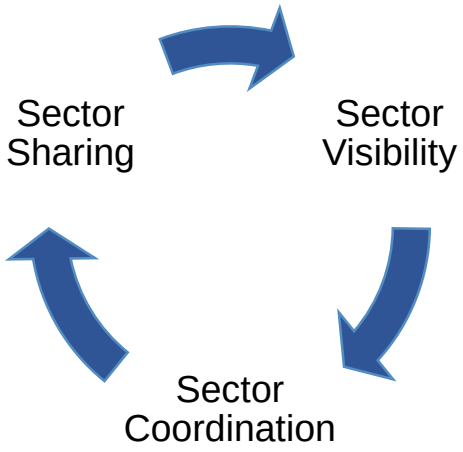
Fostering a Collective and Engaged Sector

HC3's mission and operational focus is to keep the sector apprised of threats and solutions, provide bilateral support, and promote information sharing which is critical to success.

Opportunity Areas for Sector Sharing



HPH Sector Defense



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
  - The can damage reputation, operations and even cost money

Image source: ZeroFox

Types of Social Media

- There are many categories of social media, the most common:
  Social Networking
  - Examples:
    - Facebook
    - Myspace (obsolete)
    - Google (obsolete)
    - LinkedIn
    - Twitter
- Many other categories:
  - Pictures/Images
    - Snap Chat
    - Instagram
    - Flickr
  - Knowledge/Discussion
    - Wikipedia
    - Academia
    - Reddit
  - Music
    - Pandora
    - Spotify
    - Rhapsody

Image source: Conversation Prism 5.0

Social Media Attack vectors and targets

Target for compromise. Will be spoofed for the impersonate phase

Footprinting, Monitoring and Profiling

Attack vector for Malware Installation

Potential targets to attack while impersonating the account

Attack vector for Malware Installation

Impact of Social Media Breaches

- While breaches of social media websites/companies only make up less than one percent of all data breaches per year, the incidents account for over 56% of ALL compromised data.

Google+

Affected Users
2018: 52.5 Million

Twitter

Affected Users
2013: 250,000
2016: 32.8 Million
2018: 330 Million

Snapchat

Affected Users
2013: 4.6 Million
2017: 55,000

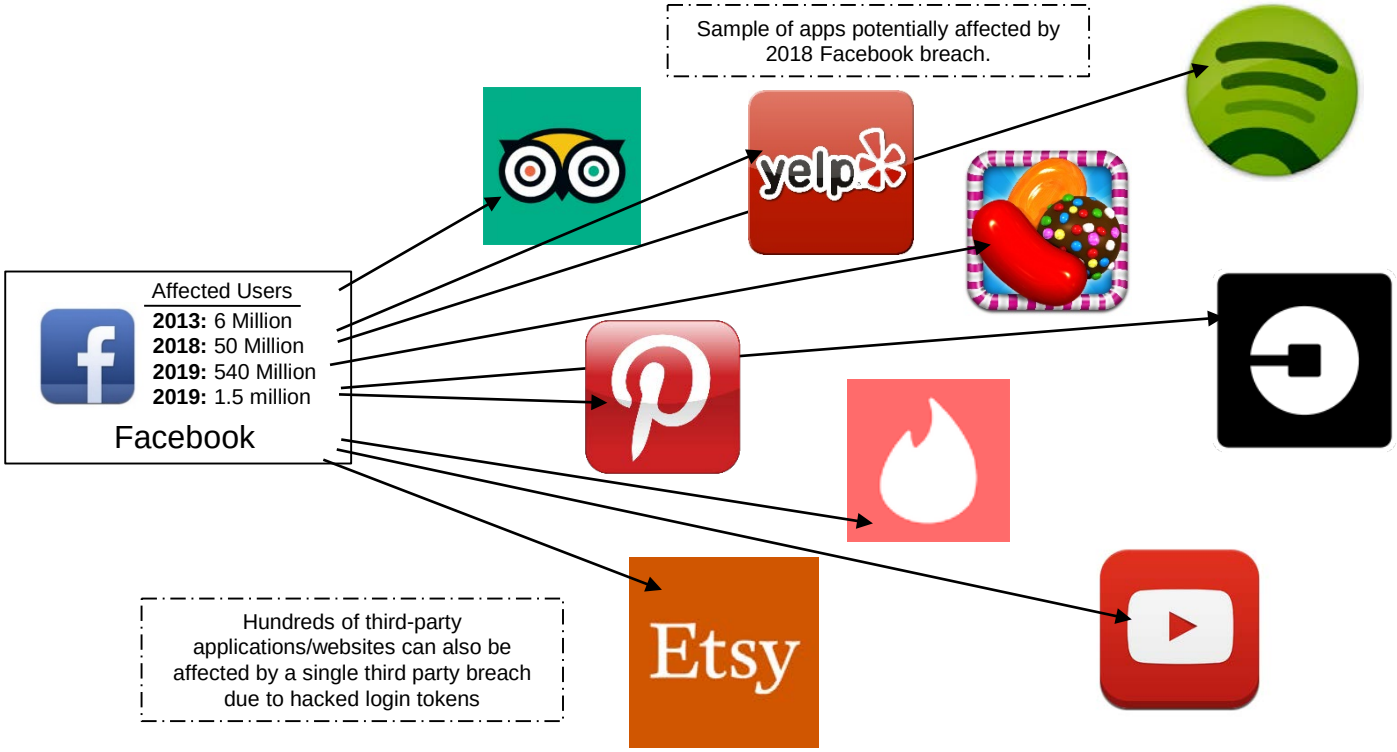
LinkedIn

Affected Users
2012: 6.5 Million
2016: 167 Million

Facebook

Affected Users
2013: 6 Million
2018: 50 Million
2019: 540 Million
2019: 1.5 million

Sample of apps potentially affected by 2018 Facebook breach.



Hundreds of third-party applications/websites can also be affected by a single third party breach due to hacked login tokens

The extent to how much specific data is compromised across the internet due to a single social media breach still can not be ascertained due to the sheer amount of apps than can be accessed with third party login credentials.

Social Media Attacks on Enterprises

- Social media attacks can:
  - Damage reputation
  - Disrupt operations
  - Impose financial cost
  - Impose legal liabilities

Image source: The Verge

- 2013 Syrian Electronic Army hack of the AP Twitter account: bomb exploded in the white house which injured the president.
  - The tweet caused the S&P500 to drop 1%, resulting in losses totaling $136 billion

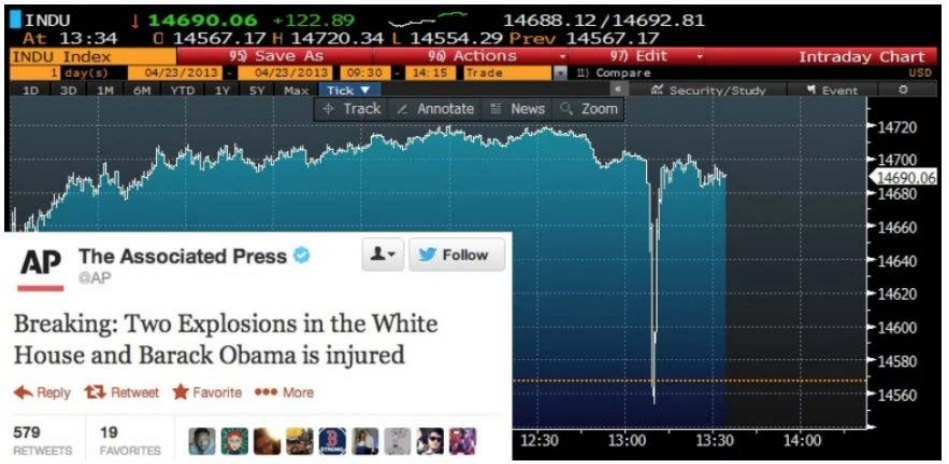


Image source: Market Watch

Social Media Attacks on Enterprises (continued)

- Social media accounts:
  - Easy to create
  - Easy to impersonate famous/familiar people
  - Easy to obtain followers, legitimate or otherwise
  - Easy to gain people's trust

- In 2016, Time Magazine reported that Russian operatives used Twitter to spearphish and distribute malware to more than 10,000 of United States Department of Defense employees.
- LinkedIn prevented 7.8 million fake accounts from being created in the second half of 2019
  - Automated defenses blocked 93% of them

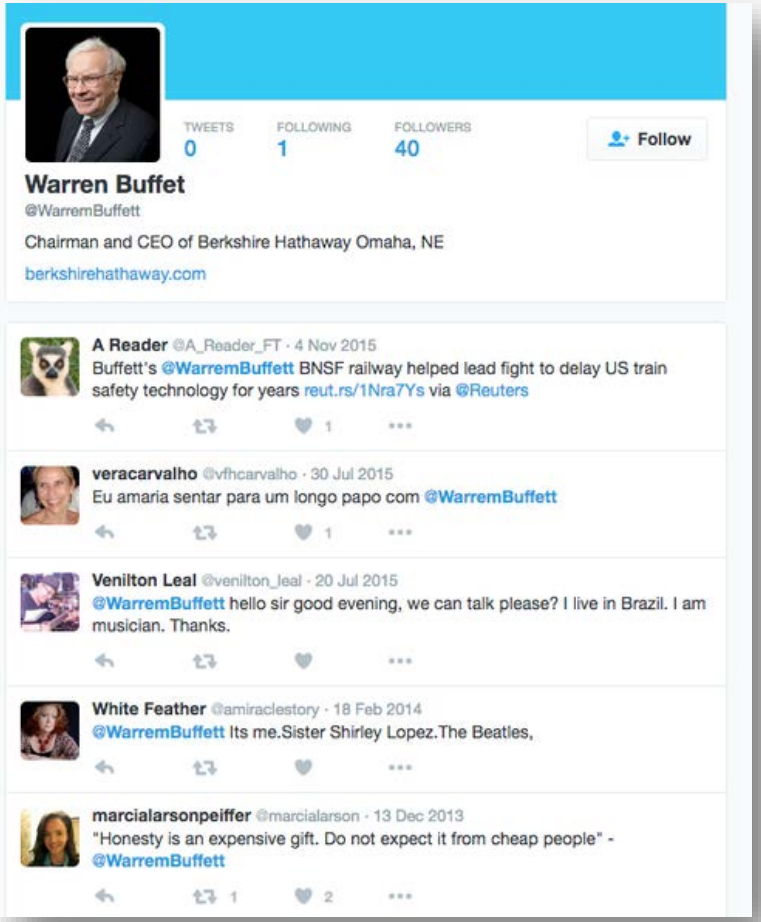
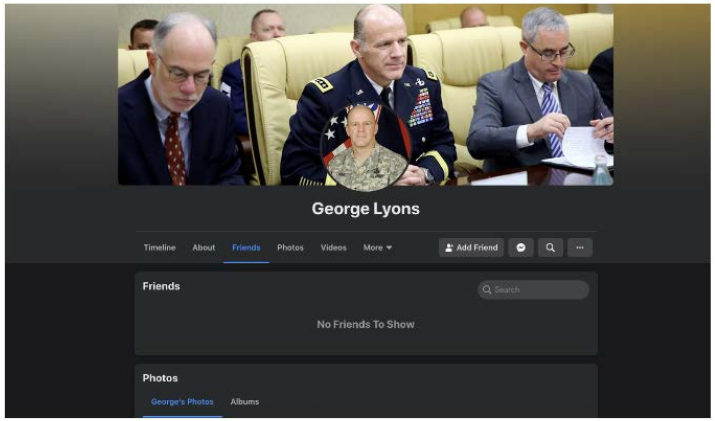


Image source: Dark Reading

Social Media Attacks – Nontraditional Vectors

- Some phony accounts may keep appearances professional…



The Facebook account of "George Lyons," used by someone pretending to be Steve Lyons, head of U.S. Transportation Command. (Facebook)

- Others may get personal….

From: paul nakasone <paulnakasone330@gmail.com>
Date: May 14, 2020 at 11:11:26 AM EDT
To: Susan
Subject: Re: Google

What is wrong with you don't you dare use that word on me don't you have regard on my reputation. Fine if you said you don't want to do its fine and I'm sorry I can't talk to you on here Susan. I also serve as the United States Army Cyber Command. So I see no reason why you are still saying rubbish Susan. If you don't want to talk to me its fine Okay

On Thu, May 14, 2020 at 8:01 AM Susan wrote:

> I feel uncomfortable if you don't mind. I'm not really sure you are who you say you are. I hope you understand. It's a scary world in cyberspace.
>
> Sent from my iPhone
>
> > On May 14, 2020, at 10:53 AM, paul nakasone <paulnakasone330@gmail.com> wrote:
> >
> > Try clicking the link on your mobile phone, I guess that's will be easier for you, what do you think?
> >
> > On Thu, 14 May 2020 at 3:51 PM, paul nakasone <paulnakasone330@gmail.com> wrote:
> > > That's a fat lie Susan, I haven't heard that before, my colleagues at make use of its always,it's fast and reliable for easy communication
> > >
> > > On Thu, 14 May 2020 at 3:44 PM, Susan wrote:
> > >
> > > > Hey
> > > > Did you know that this site is block on my work computer. It says that hackers use it? Wow ... this is troubling to me.
> > > > Sent from my iPhone

Source of images: CyberScoop

Social Media in Healthcare

- How important is social media to healthcare?
  - Very!
- 80% percent of healthcare providers use social media and the internet to research medical devices, pharmaceutical information, and biotech data.
- Nearly 90% have used social media to seek/share health information.
- Nearly two-thirds of U.S. healthcare marketers used social media to reach healthcare professionals in 2017.
- One survey found that almost three-quarters of patients use online reviews as the first step when finding a new doctor.
- A journal study of 3,371 US hospitals indicated virtually all US hospitals now have a social media presence:
  - 3,351 (99.41%) have a Facebook account
  - 3,351 (99.41%) have a Foursquare account
  - 3,342 (99.14%) have a Yelp account
  - 1,713 (50.82%) have a twitter account
  - Overall, 1,699 (50.40%) have accounts on all four platforms
  - Only 42 (1.25%) of hospitals only use two or less platforms.

Image source: Dark Reading

“It was just a friendly post”

Recent incidents involving HIPAA violations due to healthcare employee social media posts have highlighted the need for greater awareness in the healthcare sector:

- A doctor in in a Northwestern hospital was sued for posting pictures of a patient being treated for extreme intoxication
- Employees were fired from a hospital for offering condolences to wounded policer officer’s families on social media before the family was informed.
- In Los Angeles, four staff members were fired, and three disciplined, for posting pictures on social media of a 60-year old patient that was stabbed to death.
- New York nursing home employees were fired for allegedly posting photos of residents on Snapchat
- In 2015, a ProRepublica review found 35 cases of nursing home or assisted living workers surreptitiously sharing photos of residents on social media.

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

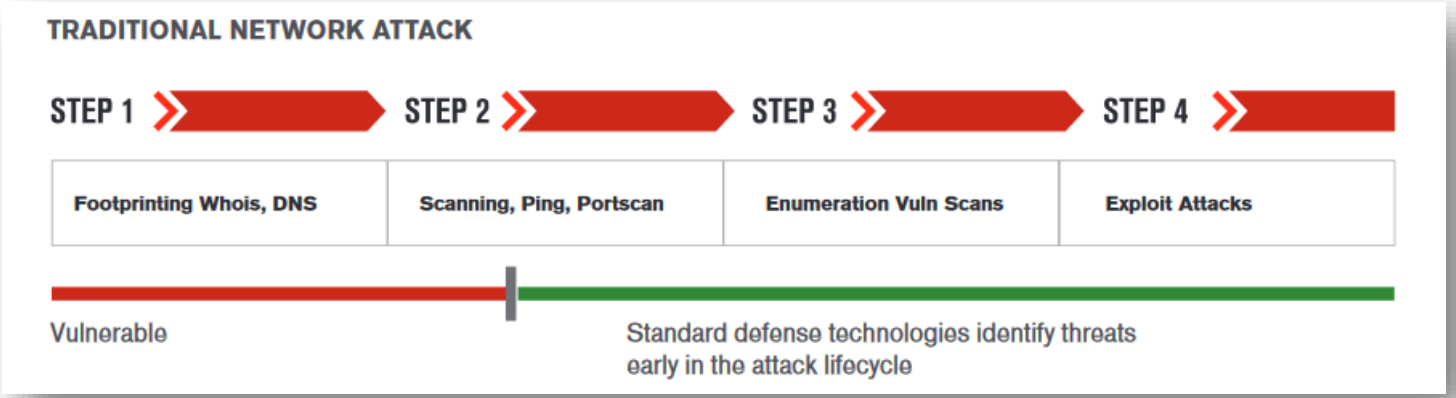
LinkedIn	company employees, titles, locations, email addresses, phone numbers, former employees
Twitter	bio, interests, other Twitter accounts they own, other brands/sub-brands, employees responsible for managing brand accounts, followers
Facebook	bio, birthday, interests, hobbies, connections
Google+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

Information targets for attackers

Source of images: Zero Fox

Anatomy of a Social Media Attack (continued)

- Why are so many of these attacks successful?
  - They are difficult to detect in a timely manner as compared to “traditional” cyber attacks

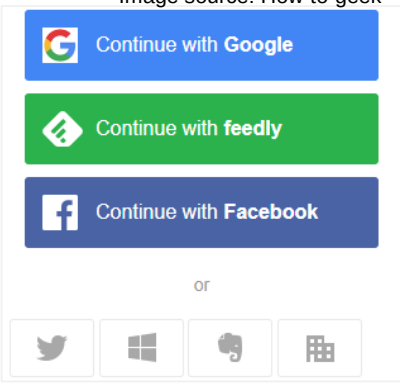


Source of images: Zero Fox

Single sign-on: Force multiplier

- Many social media platforms allow for authentication via single sign-on (SSO)
  - Distinction between identity providers (IdP) and relaying parties
    - Identity Providers: Provides authentication to websites/apps using SSO
    - Relaying Party (RP) – Can be accessed using identity provider's SSO
  - When a "identity provider" is compromised, stolen authentication tokens (Oauth tokens) can then be used to authenticate to "relying parties".

Image source: How-to-geek



When a user clicks "Login with Facebook", they will be prompted to allow the app/website to access ***some*** of their information stored by Facebook

Once the user allows access, any third-party JavaScript embedded in the page can also access the user's Facebook information

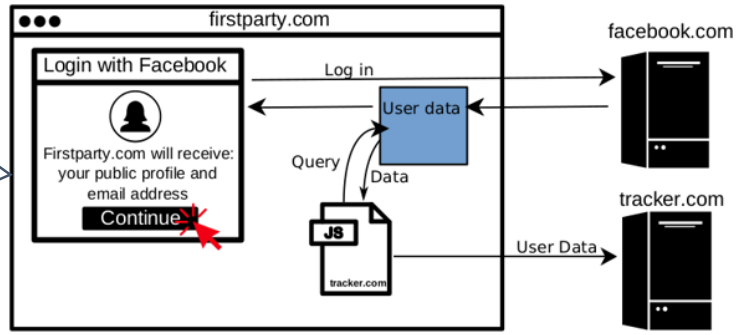


Image source: Freedom To Tinker

  - Most SSO functionality on social media is provided by Oauth tokens

- These are "traditional" cyberattacks via social media
  - We've covered these in detail in our last presentation
  - What about other ways to attack via social media?

Disinformation

- Disinformation Campaigns
  - A (relatively) new attack vector (sort of)
  - Does not compromise information, but drives action and can create friction, confusion and dissent
- What is disinformation? One definition gives it four features…
  - Methodological output of large bureaucracies
  - Often the domain of state intelligence agencies
  - Element of false information (not 100%)
  - Political purpose
- Disinformation is effective when it cannot be clearly distinguished from the truth
- Especially effective when piggybacked on current events (plays well off emotions)
- Social media is a natural platform for spreading disinformation
  - Global hypoconnectivity
  - Instant access to information
  - Hash tagging allows for organization
- Social media has to balance…
  - Preventing damaging disinformation
  - Allowing for facts, opinions and innocuous disinformation


abc NEWS | CORONAVIRUS FAQS

Who is spreading COVID-19 misinformation and why

Many different groups and individuals spread false information.

By **Benjamin Bell** and **Fergal Gallagher**

May 26, 2020, 4:03 PM • 8 min read

Disinformation (continued)

- How is disinformation spread on social media?
  - Bots – a software application that runs automated tasks
  - Social media bots have distinct qualities
    - They automatically generate messages, advocate ideas, “follow” users and attempt to accrue followers or credibility
    - They are often used to infiltrate groups of people and propagate ideas
    - Lack of regulation makes them ubiquitous
    - They are believed to play a major role in online public opinion
    - All nations concern themselves with the opinion of citizens, but this is especially important for democracies
- There is a debate about Russia’s impact on the US Presential elections of 2016 – They engaged in a disinformation campaign
  - Internet Research Agency
  - An “Army of Trolls”
- Why foreign powers do this?
  - Sew dissent
  - Achieve other political goals
- Not all disinformation originates from
- Foreign actors
- Domestic groups

Image source: European Parliamentary Research Service Blog

Healthcare Disinformation – Opposition to vaccines

- Individuals who oppose vaccinations (often called “anti-vaxxers”) have used social media to express those views and share information
  - These individuals and their views have been controversial resulting in public debates
  - At least one foreign power – Russia – has attempted to fan the proverbial flames
  - Some assert that Russia’s efforts are undermining US public health
    - Russia attempts to sew chaos, confusion and friction with disinformation
    - Anti-vaxxers are allegedly further misinformed and emboldened by this
    - As the movement continues to survive and prosper, they are accused of having a negative impact on public health and endangering themselves, their families and the general public

How Russia Sows Confusion in the U.S. Vaccine Debate

Not content to cause political problems, Moscow’s trolls are also undermining public health.

BY KATHERINE KIRK | APRIL 9, 2019, 2:48 PM

Russian trolls fueled anti-vaccination debate in U.S. by spreading misinformation on Twitter, study finds

BY CAITLIN O'KANE
MAY 31, 2019 / 11:16 AM / CBS NEWS

Healthcare Disinformation – Opposition to 5G

- 5G technology
  - Latest cellular communications protocol
- There are some who question or even assert that 5G can have health issues
  - Cancer
  - Coronavirus
  - Other health issues
- There are some mainstream outlets who discuss possible health implications
  - Russia has been fanning the proverbial flames of this debate

Image source: New York Times

Image source: Scientific American

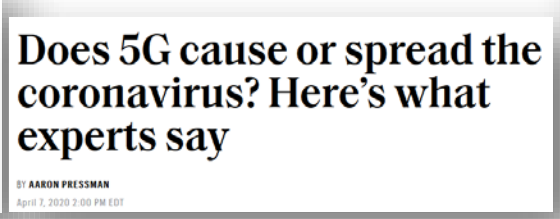


Image source: Forbes

Image source: the Verge

Healthcare Disinformation – COVID19 origins

- The COVID19 pandemic
  - Began to spread and gain attention over this last winter
  - Based on facts, it likely originated from Wuhan
    - Accidentally escaped Chinese biological lab?
    - Food market?
    - Deliberately engineered and released?
- Why would a foreign power spread disinformation on COVID19?
  - Deflection of political fallout from true origins of virus (China)
  - Sowing dissent and disunity (Russia)

COVID-19 disinformation being spread by Russia, China, say experts

Questions about the origin of the virus are driving conspiracy theories

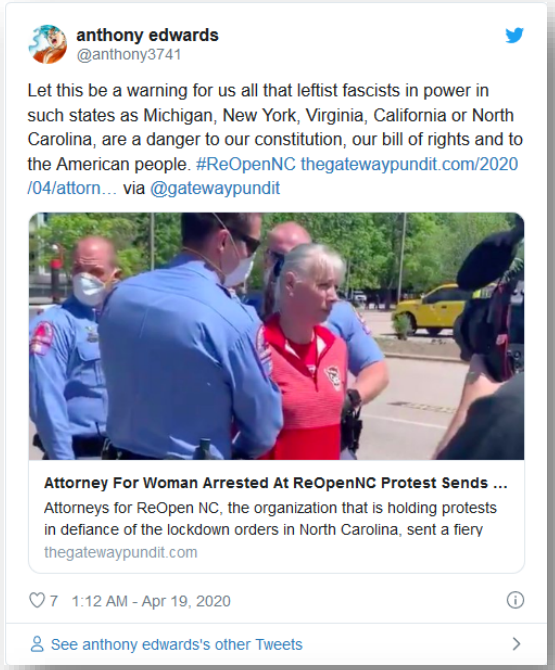
Elizabeth Thompson, Katie Nicholson, Jason Ho · CBC News ·
Posted: May 26, 2020 4:00 AM ET | Last Updated: May 26

Chinese Agents Helped Spread Messages That Sowed Virus Panic in U.S., Officials Say

American officials were alarmed by fake text messages and social media posts that said President Trump was locking down the country. Experts see a convergence with Russian tactics.

Healthcare Disinformation – COVID19 Quarantining

- COVID19 Quarantining
  - US state governments implemented restrictions on movement of US citizens and general requirements to remain in their residences with limited exceptions during the pandemic
  - Civil Libertarians began pushing back, defying orders and protesting
  - Bots pushing hashtags:
    - #ReOpenAmericaNow
    - #Stop#TheMadness
    - #ReOpenNC
    - #ENDTHESHUTDOWN



Trolls and bots are flooding social media with disinformation encouraging states to end quarantine

Source of images: Business Insider

Reference Materials

References

- ENTERPRISE NETWORK COMPROMISE VIA SOCIAL MEDIA EXPLOITATION
  https://get.zerofox.com/rs/143-DHV-007/images/ZeroFOX-Network-Compromise-Via-Social-Media-Exploitation_Whitepaper.pdf
- O Single Sign-Off, Where Art Thou? An Empirical Analysis of Single Sign-On Account Hijacking and Session Management on the Web
  https://www.cs.uic.edu/~polakis/papers/sso-usenix18.pdf
- The Top 10 Worst Social Media Cyber-Attacks
  https://www.infosecurity-magazine.com/blogs/top-10-worst-social-media-cyber/
- Coronavirus disinformation fueling death threats against doctors in northern Colombia
  https://colombiareports.com/coronavirus-disinformation-fueling-death-threats-against-doctors-in-northern-colombia/
- Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate
  https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6137759/
- Who is spreading COVID-19 misinformation and why
  - https://abcnews.go.com/US/spreading-covid-19-misinformation/story?id=70615995
- Something in the air
  https://www.theverge.com/2020/6/3/21276912/5g-conspiracy-theories-coronavirus-uk-telecoms-engineers-attacks-abuse
- Social media firms fail to act on Covid-19 fake news
  https://www.bbc.com/news/technology-52903680
- China's Disinformation Effort Targets Virus, Researcher Says
  https://www.bloomberg.com/news/articles/2020-05-12/china-s-disinformation-campaign-targets-virus-and-businessman
- Facebook Breach: Single Sign-On of Doom
  https://www.bankinfosecurity.com/blogs/facebook-breach-single-sign-on-doom-p-2668

References

- Trolls and bots are flooding social media with disinformation encouraging states to end quarantine
  https://www.businessinsider.com/trolls-bots-flooding-social-media-with-anti-quarantine-disinformation-2020-4
- How Russia Sows Confusion in the U.S. Vaccine Debate
  https://foreignpolicy.com/2019/04/09/in-the-united-states-russian-trolls-are-peddling-measles-disinformation-on-twitter/
- Chinese Agents Helped Spread Messages That Sowed Virus Panic in U.S., Officials Say
  https://www.nytimes.com/2020/04/22/us/politics/coronavirus-china-disinformation.html
- Anatomy Of A Social Media Attack
  https://www.darkreading.com/analytics/anatomy-of-a-social-media-attack/a/d-id/1326680
- Privileged Account Management Best Practices for Social Media Security
  - https://securityboulevard.com/2019/04/privileged-account-management-best-practices-for-social-media-security/
- Social Media Security Tips and Tools to Mitigate Risks
  https://blog.hootsuite.com/social-media-security-for-business/
- What Is OAuth? How Those Facebook, Twitter, and Google Sign-in Buttons Work
  https://www.howtogeek.com/53275/exchanging-data-safely-with-oauth/
- No boundaries for Facebook data: third-party trackers abuse Facebook Login
  https://freedom-to-tinker.com/2018/04/18/no-boundaries-for-facebook-data-third-party-trackers-abuse-facebook-login/
- Photos of dying patient posted to Facebook get four hospital workers fired
  - https://www.fiercehealthcare.com/healthcare/photos-dying-patient-posted-to-facebook-get-four-hospital-workers-fired
- Trading in the Dark
  https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/trading-in-the-dark

References

- The Danger of Social Media for Healthcare Professionals
  - https://www.healthecareers.com/article/career/social-media-healthcare-professionals
- Nursing home workers share invasive pics and videos of seniors on social media
  https://wgntv.com/news/its-just-totally-wrong-nursing-home-workers-share-invasive-pics-and-videos-of-seniors-on-social-media/
- How to Use Social Media in Healthcare: A Guide for Health Professionals
  https://blog.hootsuite.com/social-media-health-care/
- Canandaigua nursing home employees fired for allegedly posting photos of residents on Snapchat
  https://www.democratandchronicle.com/story/news/2018/07/18/m-m-ewing-nursing-home-employees-fired-alleged-snapchat-photos/795318002/
- When Facebook Goes To The Hospital, Patients May Suffer
  - https://www.asrn.org/journal-nursing/786-when-facebook-goes-to-the-hospital-patients-may-suffer.html
- Social media becomes biggest data breach threat
  https://www.itweb.co.za/content/G98YdqLxZZNqX2PD
- The 21 scariest data breaches of 2018
  https://www.businessinsider.com/data-hacks-breaches-biggest-of-2018-2018-12
- Pinterest, Spotify top the apps most affected by the Facebook breach
  https://media.thinknum.com/articles/facebook-breach-apps-affected/
- What Is Social Media?
  https://www.lifewire.com/what-is-social-media-explaining-the-big-trend-3486616
- Facebook Breach Exposed Personal Data of Millions of Users
  https://www.consumerreports.org/digital-security/facebook-data-breach-exposed-personal-data-of-millions-of-users/

References

- The Prism Chronicles
  https://conversationprism.com/the-prism-chronicles/
- Human error led to 424% increase in misconfigured cloud servers, prompting hacks
  https://www.techrepublic.com/article/human-error-led-to-424-increase-in-misconfigured-cloud-servers-prompting-hacks/
- Misconfigured Clouds Compromise 424% More Records in 2017
  https://www.darkreading.com/cloud/misconfigured-clouds-compromise-424--more-records-in-2017/d/d-id/1331457
- SOCIAL MEDIA PLATFORMS ANDTHE CYBERCRIME ECONOMY
  https://m.itcafe.hu/dl/cnt/2019-02/151108/bromium.pdf
- Beware misconfiguration errors: Little slip-ups can have huge consequences
  https://www.healthcareitnews.com/news/beware-misconfiguration-errors-little-slip-ups-can-have-huge-consequences
- Social media, the gateway for malware
  https://www.csoonline.com/article/3106292/social-media-the-gateway-for-malware.html
- Beyond The Clinic: The Commonality Between Living With Ovarian Cancer And Working As The Researcher Behind A Treatment
  https://www.forbes.com/sites/tesaro/2019/10/02/beyond-the-clinic-the-commonality-between-living-with-ovarian-cancer-and-working-as-the-researcher-behind-a-treatment/#181c83752502

Questions

Upcoming Briefs

- Deep dive on Dark Web
- Dridex Malware

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to **HC3@HHS.GOV**.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV** or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110.**

Health Sector Cybersecurity Coordination Center (HC3) Background

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently impacting threats via the HHS OIG

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing document and presentation that provides actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic or want to join our listserv? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.

Questions

Contact

Health Sector Cybersecurity Coordination Center (HC3)

(202) 691-2110

HC3@HHS.GOV