November 12th, 2019

Hacking Healthcare

TLP White

In this edition of Hacking Healthcare, we explore insider threats and the various ways they can negatively impact organizations. First, we analyze how the convergence of geopolitics and insider threats have led GitLab to consider banning individuals of certain nationalities from critical positions. Next, we brief you on how an insider threat at Trend Micro led to tailored scam attacks against their customers. Finally, we examine the case of two Twitter employees charged with spying for the Saudi Arabian government. Welcome back to *Hacking Healthcare*.

1. **GitLab Considers Bans for Russian and Chinese Support Positions.** The Internet is often lauded for its ability to effectively erase the geographic distance between willing collaborators. The ability to find and employ talented individuals regardless of location is a frequent boon, but geopolitical tensions are beginning to have very real consequences for businesses that take advantage of that ability. Last week, GitLab, a DevOps tool used by over 100,000 companies worldwide, was forced to acknowledge that they may ban Chinese and Russian nationals from two support positions that oversee customer data over fears they may steal intellectual property and trade secrets.[i]

   GitLab reported several weeks ago they were considering not only banning new hires from China and Russia, but also banning anyone working in the affected support positions from moving to those countries. While the ban affects only two support positions that require full access to customer data, GitLab is concerned about the potential for creating a "second class of citizens on certain teams who cannot take part in 100% of their responsibilities."[ii] GitLab's potential ban comes after several of its enterprise-level customers signaled their concern about China and Russia's previous attempts to infiltrate western organizations and companies. It is also an acknowledgement that citizens of those countries may be at greater risk of coercion from state intelligence services.[iii]

2. **Insider Threat at Trend Micro Leads to Scam Attacks.** Trend Micro, an enterprise data security and cybersecurity solutions company, announced last week that roughly 70,000 of its customers were affected by an insider threat.[iv] Trend Micro reported in a blog post that a security incident "resulted in the unauthorized disclosure of some personal data of an isolated number of customers of our consumer product."[v] Trend Micro

believes all the affected customers have been notified, but they are continuing to investigate the scope of the incident.

The incident is believed to have occurred last August when Trend Micro customers reported that they were being targeted by scam support calls. Trend Micro promptly began an internal investigation that revealed evidence that an employee "used fraudulent means to gain access to a customer support database that contained names, email addresses, Trend Micro support ticket numbers, and in some instances telephone numbers."[vi] This data was then sold to an unknown malicious actor.

While Trend Micro was quick to "reassure [their] business and government customers that [their] investigations have shown no indication that the criminal has accessed any enterprise customer data," this response fails to wholly capture the potential damage that could occur through successful phishing attacks resulting from the stolen data. Phishing attacks are already among the most successful methods of compromise for malicious actors, but they become even more dangerous when the attack is tailored by making use of inside information from a trusted vendor.

One method of mitigation for these types of attacks is to ensure that your organization knows and follows proper procedures for communicating with vendors and third party partners. As an example, Trend Micro has a policy of never making unsolicited calls to customers and they encourage customers to report such activity. By ensuring the use of established procedures such as these, companies can lessen the risk of falling for tailored phishing attacks that use inside information.

3. **Twitter's Saudi Spies.** Last week, Security Affairs reported that two former Twitter employees had been charged with spying for the Saudi Arabian government in a case brought before U.S. District Court for the Northern District of California.[vii] The indictment alleges that they acted as foreign agents without notifying the attorney general, and destroyed, altered, or falsified records in a federal investigation.[viii] One of the individuals has since been arrested by the FBI.

   According to the court filing, the two were recruited by the Saudi government in 2014 and continued their work until they left Twitter in 2015. During that time they allegedly gathered "non-public information of Twitter accounts associated with known prominent critics of the Kingdom of Saudi Arabia and the Royal Family."[ix] Security Affairs reports that the two gained "unauthorized access to information associated with some profiles, including email addresses, devices used… and other [information] that can be used to geo-locate a user such as IP addresses and phone numbers."[x]

   Social media has long been a favorite target of foreign governments to spread their tailored narratives and misinformation, so the infiltration of social media organizations by foreign governments looking to silence dissent shouldn't come as a surprise. However, the seriousness of the potential consequences stemming from this type of insider threat cannot be overstated. Authoritarian states have shown themselves to be more than willing to violently target dissidents, and geolocation data can very easily put lives at risk.

Congress –

Tuesday, November 12th:
- No relevant hearings

Wednesday, November 13th:
- Upskilling the Medical Workforce: Opportunities in Health Innovation (House Committee on Small Business)

Thursday, November 14th:
- No relevant hearings

International Hearings/Meetings –

EU – No relevant hearings

Conferences, Webinars, and Summits –

--The Role of Deception in Healthcare Networks by Attivo Networks – Webinar (11/13/2019)
https://h-isac.org/hisacevents/key-steps-to-building-a-threat-intelligence-strategy/
--Health IT Summit (Southwest) – Houston, TX (11/14/2019-11/15/2019)
https://endeavor.swoogo.com/2019-Dallas-Health-IT-Summit
--Southwest Healthcare Cybersecurity Forum – Dallas, TX(11/15/2019)
https://endeavor.swoogo.com/2019_Southwest_Cybersecurity_Forum
--Health IT Summit (Northwest) – Seattle, WA (11/19/2019-11/20/2019)
https://endeavor.swoogo.com/2019-PacificNorthwest-HITSummit
--Pacific Northwest Healthcare Cybersecurity Forum – Seattle, WA (11/20/2019)
https://endeavor.swoogo.com/2019_Pacific_Northwest_Cybersecurity_Forum
Cyber Security & Data Protection Summit 2019 – London, UK (11/20/2019)
https://cybersecuritysummit.co.uk/
--2019 H-ISAC Fall Summit – San Diego, CA (12/2/19-12/6/2019)
https://h-isac.org/summits/fall-summit-2019/
--H-ISAC Security Workshop – London, UK (2/5/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-2/
-- H-ISAC Security Workshop - Cambridge, MA (4/7/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-cambridge-ma/

Sundries –

--Study: Ransomware, Data Breaches at Hospitals tied to Uptick in Fatal Heart Attacks
https://krebsonsecurity.com/2019/11/study-ransomware-data-breaches-at-hospitals-tied-to-uptick-in-fatal-heart-attacks/

November 12th, 2019

--New York company charged with selling vulnerable Chinese-made equipment to U.S. military
https://www.cyberscoop.com/aventura-fraud-charges-china/
--Google asks mobile security vendors to help keep hackers out of the Play Store
https://www.cyberscoop.com/google-asks-mobile-security-vendors-help-keep-hackers-play-store/
--Tipped off by an NSA breach, researchers discover new APT hacking group
https://arstechnica.com/information-technology/2019/11/shadow-brokers-leak-of-nsa-code-leads-to-discovery-of-new-apt-hacking-group/

Contact us: follow @HealthISAC, and email at contact@h-isac.org

[i] https://gitlab.com/gitlab-com/www-gitlab-com/issues/5555
[ii] https://gitlab.com/gitlab-com/www-gitlab-com/issues/5555
[iii] https://www.zdnet.com/article/building-chinas-comac-c919-airplane-involved-a-lot-of-hacking-report-says/
[iv] https://www.zdnet.com/article/trend-micro-reveals-insider-threat-exposing-customer-data/
[v] https://blog.trendmicro.com/trend-micro-discloses-insider-threat-impacting-some-of-its-consumer-customers/
[vi] https://blog.trendmicro.com/trend-micro-discloses-insider-threat-impacting-some-of-its-consumer-customers/
[vii] https://securityaffairs.co/wordpress/93530/intelligence/formers-twitter-employees-saudi-arabian-government.html
[viii] https://www.scribd.com/document/433859677/Former-Twitter-Employees-Charged-With-Spying-for-Saudi-Arabia
[ix] https://securityaffairs.co/wordpress/93530/intelligence/formers-twitter-employees-saudi-arabian-government.html
[x] https://securityaffairs.co/wordpress/93530/intelligence/formers-twitter-employees-saudi-arabian-government.html