August 18th, 2020

TLP White

This week, Hacking Healthcare begins by exploring how healthcare organizations should consider establishing an online presence on social media and communication platforms, even if there doesn't appear to be a business case for it. Next, we briefly detail the National Security Agency (NSA) and Federal Bureau of Investigation's (FBI) startling public identification and attribution of Drovorub malware. Finally, we wrap up by breaking down a report detailing consumer views on data privacy and security in the Asia-Pacific region.

Welcome back to *Hacking Healthcare*.

**H-ISAC Monthly Threat Briefing:** As a reminder the H-ISAC's monthly *Threat Briefing* will take place on Tuesday, August 25th at 12:00pm EST. Every month, the H-ISAC and our associated partners dive into issues related to insider threats, cybercrime, the Dark Web, physical security, and legal and regulatory issues that affect the healthcare sector. The *Threat Briefing* is a free service only available to H-ISAC members.

1. **Securing Your Online Presence.** For years, one line of thought on how individuals could avoid having their accounts hacked and their sensitive data put at risk was to avoid creating unnecessary online accounts entirely. By minimizing how much personal information was put on the Internet, and generally keeping an analog existence to the fullest extent possible, some argued you could minimize the attack surface and the number of vectors through which you could be targeted.

   Unfortunately, in practice, there are numerous reasons related to identity theft and fraud that explain why this doesn't turn out to be an optimal strategy for individuals.[1] However, organizations may inadvertently be employing a similar approach when it comes to their online presence by attempting to limit the amount of accounts they maintain online.

For example, it may be easy for a pharmaceutical company who never directly interacts with patients to brush off the need to create and monitor an Instagram account, or for a hospital group to decide that it would be unprofessional to have a corporate TikTok, or even for a medical device manufacturer to determine that there just isn't a business case to have a Twitter for all of its branches or international subsidiaries. But there is a risk in not setting up, securing, and adequately monitoring these types of accounts.

In the following Action & Analysis section we'll explore this topic further.

*Action & Analysis*
*** Membership required***

2. **NSA and FBI Release Linux Malware Warning.** On August 13th, the NSA and FBI released a joint statement disclosing the existence of Drovorub malware. According to a 45-page NSA and FBI advisory, the malware has the capability to provide direct communications between a compromised device and a threat actor's command and control infrastructure, allows for file download and upload, enables execution of arbitrary commands, and facilitates port forwarding of network traffic to other hosts on the network.[2]

   Both organizations attribute the Linux-based malware to the Russian General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS) military unit 26165, which is often identified as Fancy Bear, Strontium, or APT 28.[3] The NSA's press release states that the malware is a component in Russian cyber espionage operations, but the release does not detail any specific targets or victims other than to say the malware "represents a threat to National Security Systems, Department of Defense, and Defense Industrial Base customers that use Linux systems."[4]

   Thankfully, the advisory details "detection strategies, mitigation techniques, and configuration recommendations" for network defenders and system administrators.[5]

   *Action & Analysis*
   *** Membership required***

3. **Study Highlights Asia-Pacific (APAC) Region Views on Data Protection.** A newly published study by F5, an application services company, sought to gauge how consumers in the APAC region view data privacy and protection issues. The results paint an interesting picture for what organizations should prioritize when looking to operate

in these markets. The primary takeaway may be just how significantly consumers in the APAC region believe businesses should be responsible for protecting data privacy.

The study incorporated respondents from eight APAC economies: China, Indonesia, India, Taiwan, Singapore, Australia, Japan, and Hong Kong.[6] The primary questions they sought to answer were how do data breaches affect trust? What are the most important features for applications to possess? How willing are you to share personal data on applications? Do you prioritize security or convenience more? Finally, who should be responsible for protecting your data privacy?

The most interesting findings appear to be:[7]

- Only 4% of respondents said they would stop using an application that suffered a data breach
- Strong encryption and security were the most important feature of an application, beating out user friendliness by 16 percentage points
- Willingness to share and store personal data on applications varied immensely by country
- In 2020, convenience trumped security in most countries
- In response to who should be responsible for protecting consumer data, 43% of respondents said businesses, 32% said government, and only 25% said consumers themselves

*Action & Analysis*
*** Membership required***

***Congress –***

Tuesday, August 18th:
- No relevant hearings

Wednesday, August 19th:
- No relevant hearings

Thursday, August 20th:
- No relevant hearings

August 18th, 2020

***International Hearings/Meetings –***

- No relevant hearings

***EU –***

***Conferences, Webinars, and Summits*** –

-- Securing Hospitals – How Compliance and Cybersecurity Align by IntSights – Webinar (8/19/2020)
https://h-isac.org/hisacevents/securing-hospitals-how-compliance-and-cybersecurity-align-by-intsights/

-- H-ISAC Monthly Member Threat Briefing – Webinar (8/25/2020)
https://h-isac.org/hisacevents/h-isac-monthly-member-threat-briefing-11/

-- STOP HEMORRHAGING DATA: MINIMIZE THIRD-PARTY RISK IN HEALTHCARE BY RISKRECON – Webinar (9/1/2020)
https://h-isac.org/hisacevents/stop-hemorrhaging-data-minimize-third-party-risk-in-healthcare-by-riskrecon/

--Healthcare Cybersecurity Forum – Southeast – Nashville, TN (9/9/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426517

-- ENISA Trust Services Forum - CA Day 2020 - Schloßplatz Berlin, Germany (9/22/2020)
https://h-isac.org/hisacevents/enisa-trust-services-forum-ca-day-2020/

--Healthcare Cybersecurity Forum – Northeast – Boston, MA (9/22/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/427126

--H-ISAC Cyber Threat Intel Training - Titusville, FL (9/22/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-titusville-fl/

--H-ISAC Security Workshop - Virtual (9/23/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-forchheim-germany/

--Summit on Security & Third Party Risk – National Harbor, MD (9/28/2020-9/30/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/428840

--H-ISAC Monthly Member Threat Briefing – Webinar (9/29/2020)
https://h-isac.org/hisacevents/h-isac-monthly-member-threat-briefing-12/

-- The MedTech Conference – Virtual (10/5/2020)
https://h-isac.org/hisacevents/the-medtech-conference-toronto/

-- Healthcare Cybersecurity Forum – Houston, TX (10/8/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/428840

-- NCHICA AMC Security & Privacy Conference - Durham, North Carolina (10/21/2020-10/22/2020)
https://h-isac.org/hisacevents/nchica-amc-security-privacy-conference/

-- 2020 H-ISAC European Summit - Santpoort-Noord, Netherlands (10/20/2020-10/22/2020)
https://h-isac.org/summits/european-2020-summit/

--CYSEC 2020 – Dubrovnik, Croatia (10/27/2020 – 10/28/2020)
https://h-isac.org/hisacevents/cysec-2020-croatia/

--Healthcare Cybersecurity Forum - Pacific Northwest – Seattle, WA (10/28/2020)

https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/428886
--H-ISAC Security Workshop - Seattle, WA – (10/29/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-seattle-wa-2/
--Healthcare Cybersecurity Forum – California – Los Angeles, CA (11/12/2020)
https://h-isac.org/hisacevents/healthcare-cybersecurity-forum-california-2/
--H-ISAC Security Workshop - Paris, France (11/18/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-paris-france/
--H-ISAC Fall Summit - Phoenix, AZ (11/30/2020-12/4/2020)
https://h-isac.org/summits/fall-summit-2020/
-- H-ISAC Security Workshop - Prague, Czech Republic (12/8/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-prague/
-- 2021 APAC Summit – Singapore (3/23/2021-3/25/2021)

***Sundries –***

Business Email Compromise Attacks Involving MFA Bypass Increase

> https://www.darkreading.com/attacks-breaches/business-email-compromise-attacks-involving-mfa-bypass-increase/d/d-id/1338667

For six months, security researchers have secretly distributed an Emotet vaccine across the world

> https://www.zdnet.com/article/for-six-months-security-researchers-have-secretly-distributed-an-emotet-vaccine-across-the-world/

An advanced group specializing in corporate espionage is on a hacking spree

> https://www.cyberscoop.com/redcurl-groupib-russian-hacking-espionage/

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

[1] https://krebsonsecurity.com/2018/06/plant-your-flag-mark-your-territory/
[2] https://media.defense.gov/2020/Aug/13/2002476465/-1/-1/0/CSA_DROVORUB_RUSSIAN_GRU_MALWARE_AUG_2020.PDF
[3] https://www.nsa.gov/news-features/press-room/Article/2311407/nsa-and-fbi-expose-russian-previously-undisclosed-malware-drovorub-in-cybersecu/
[4] https://www.nsa.gov/news-features/press-room/Article/2311407/nsa-and-fbi-expose-russian-previously-undisclosed-malware-drovorub-in-cybersecu/
[5] https://media.defense.gov/2020/Aug/13/2002476465/-1/-1/0/CSA_DROVORUB_RUSSIAN_GRU_MALWARE_AUG_2020.PDF
[6] https://www.f5.com/c/apcj-2020/asset/gc-rp-curve-of-convenience#platter-126601635
[7] https://www.f5.com/c/apcj-2020/asset/gc-rp-curve-of-convenience#platter-126601635