November 3rd, 2020

TLP White

This week, *Hacking Healthcare* takes a look at how industry conferences and networking sites are fertile grounds for cyberattacks. Next, we briefly explore a concerning threat advisory jointly posted by three federal government agencies on October 28th that warned of imminent cyberattacks against the healthcare sector. Finally, we wrap up with an examination of the newest cyber-related sanctions issued by the U.S. government against a Russian institute with connections to Triton malware. Welcome back to *Hacking Healthcare*.

1. **Conferences and Job Offers Make Tempting Targets**

   Having representatives attend industry conferences is often an integral part of an organization's activities. These events provide the opportunity to catch a glimpse of the latest developments in a given field and hear the thoughts of an industry's luminaries, all while building networking connections and improving an organization's visibility and industry presence. Unfortunately, these events can also often create ideal circumstances for malicious communications from bad actors. As a recent Microsoft blogpost goes to show, this threat is more than just theoretical.

   In an October 28th post, Tom Burt, Microsoft's Corporate Vice President of Customer Security & Trust, outlined how Microsoft had "detected and worked to stop a series of cyberattacks" from an Iranian-linked threat group.[1] According to Burt, the threat group posed as organizers for the upcoming Munich Security Conference and Think 20 (T20) Summit and proceeded to send spoofed email invitations to prospective attendees.[2] Both events, an annual international security policy event and a G20 engagement group policy event, routinely draw world leaders and renowned policy experts from the public and private sector.

   In a sign of the sophistication and attention to detail taken by the threat group, the fake invites used "near-perfect English" and "helped assuage fears of travel during the Covid-19 pandemic by offering remote sessions," all of which helped to make them seem legitimate.[3] Once communication was established, the threat group attempted to direct the target to a credential harvesting page through a malicious link, which would then provide the threat group access to the target's mailbox.[4] Given the prominent public

and private policy positions of many of the attendees, Microsoft believes this attack was likely an intelligence gathering operation.

However, when spoofing conference invites isn't a feasible option for threat groups, there are various other avenues for malicious actors to pursue. LinkedIn, the popular professional networking platform, is another common vector some threat groups can use to make contact with a target. When we last examined this issue in June, we focused on the high-profile efforts of malicious actors impersonating HR representatives from two major aerospace organizations. Since then, H-ISAC members are themselves reporting the growth in both sophistication and quantity of these kinds of attacks.[5]

According to the H-ISAC, "These profiles appear as legitimate LinkedIn users complete with endorsements and hundreds of connections," and "Executives, VPs, and Research and Development (R&D) teams have been targeted ."[6] Furthermore, the attackers are becoming more educated on the nuances of the healthcare sector by, for example, familiarizing themselves with industry terms to better mask the malicious intent of their outreach.[7] These attacks often incorporate job offers or other enticing subjects to maximize the potential engagement of their target victim.

Action & Analysis
H-ISAC Membership Required

2. Ransomware Threat Forces Joint Cyber Advisory

Late on October 28th, the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS) issued a joint cybersecurity advisory on "an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers."[8]

The advisory calls for healthcare sector organizations to "ensure that they take timely and reasonable precautions to protect their networks" from a cybercriminal threat specifically targeting the healthcare sector with Trickbot and BazarLoader malware.[9] The threat actors are said to disseminate this malware through phishing campaigns with malicious links or malware laden attachments.[10] Trickbot's deployment often presages potential "credential harvesting, mail exfiltration, cryptomining, point-of-sale data exfiltration, and the deployment of ransomware, such as Ryuk and Conti."[11] The fifteen-page joint cybersecurity advisory contains technical details of the threat, mitigations, contact information in the event of an attack, and additional resources.[12]

According to the New York Times, the threat group that forced the advisory is Russian and has been "trading a list of more than 400 hospitals they plan to target."[13] Since the warning, a number of hospitals have reported cyber incidents, but it is unclear at the time of this post if they are related.[14]

Action & Analysis
H-ISAC Membership Required

3. **Sanctions Against Russian Institution Connected to Triton Malware**

   On October 23rd, the Department of the Treasury posted a press release to announce sanctions against the State Research Center of the Russian Federation FGUP Central Scientific Research Institute of Chemistry and Mechanics (TsNIIKhM).[15] This Russian government-controlled research institution is allegedly connected to Triton malware, and the sanctions appear to be related to the 2017 cyberattack on a Saudi petrochemical plant that made use of Triton.

   As you may recall, the noteworthiness of that petrochemical plant attack came from reporting that the malware "zeroed in on processes known as the safety instrumented systems (SIS)," which "[are] a combination of hardware and software that critical infrastructure sites use to prevent unsafe conditions."[16] Reports suggest that the malware gained a foothold through a phishing message and only a fortunate error that resulted in a plant shut down prevented the malware from executing in a way that could potentially have resulted in personal harm or structural damage.[17]

   As news outlets have mentioned, this sanctions declaration wraps up a particularly difficult month for Russia on the cybersecurity front. This month the Department of Justice also charged Russian backed individuals thought to be part of the Sandworm group, CISA and the FBI documented the Energetic Bear threat group that appears to hail from Russia, and the EU imposed sanctions on Russian intelligence operatives for the 2015 attack on the German Parliament.[18]

   Action & Analysis
   H-ISAC Membership Required

Congress –

Tuesday, November 3rd:
- No relevant hearings

Wednesday, November 4th:
- No relevant hearings

Thursday, November 5th:
- No relevant hearings

International Hearings/Meetings –

- No relevant hearings

EU –

- No relevant hearings

Conferences, Webinars, and Summits –

https://h-isac.org/events/

November 3rd, 2020

Sundries –

Security Blueprints of Many Companies Leaked in Hack of Swedish Firm Gunnebo

https://krebsonsecurity.com/2020/10/security-blueprints-of-many-companies-leaked-in-hack-of-swedish-firm-gunnebo/

Why the extortion of Vastaamo matters far beyond Finland — and how cyber pros are responding

https://www.cyberscoop.com/finland-vastaamo-hack-response/

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

---

[1] https://blogs.microsoft.com/on-the-issues/2020/10/28/cyberattacks-phosphorus-t20-munich-security-conference/

[2] https://blogs.microsoft.com/on-the-issues/2020/10/28/cyberattacks-phosphorus-t20-munich-security-conference/

[3] https://blogs.microsoft.com/on-the-issues/2020/10/28/cyberattacks-phosphorus-t20-munich-security-conference/

[4] https://blogs.microsoft.com/on-the-issues/2020/10/28/cyberattacks-phosphorus-t20-munich-security-conference/

[5] https://h-isac.org/wp-content/uploads/2020/10/5b47f99e-Nation-State-Recruiting-via-Fraudulent-LinkedIn-Profiles.pdf

[6] https://h-isac.org/wp-content/uploads/2020/10/5b47f99e-Nation-State-Recruiting-via-Fraudulent-LinkedIn-Profiles.pdf

[7] https://h-isac.org/wp-content/uploads/2020/10/5b47f99e-Nation-State-Recruiting-via-Fraudulent-LinkedIn-Profiles.pdf

[8] https://us-cert.cisa.gov/ncas/alerts/aa20-302a

[9] https://us-cert.cisa.gov/ncas/alerts/aa20-302a

[10] https://us-cert.cisa.gov/ncas/alerts/aa20-302a

[11] https://us-cert.cisa.gov/ncas/alerts/aa20-302a

[12] https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf

[13] https://www.nytimes.com/2020/10/28/us/hospitals-cyberattacks-coronavirus.html

[14] https://www.nytimes.com/2020/10/28/us/hospitals-cyberattacks-coronavirus.html

[15] https://home.treasury.gov/news/press-releases/sm1162

[16] https://arstechnica.com/information-technology/2020/10/us-sanctions-russian-hackers-who-hit-chemical-maker-with-dangerous-malware/

[17] https://arstechnica.com/information-technology/2020/10/us-sanctions-russian-hackers-who-hit-chemical-maker-with-dangerous-malware/

[18] https://www.zdnet.com/article/us-treasury-sanctions-russian-research-institute-behind-triton-malware/