July 28th, 2020

TLP White

This week, Hacking Healthcare explores 2020 ransomware trends, including the concerning growth of ransomware that incorporates data exfiltration and what that means for healthcare organizations. Next, we examine the charges the US government has brought against two Chinese hackers accused of a decades long cyber campaign and what the US hopes to gain from the disclosure. Lastly, we investigate the growing support for active cyber defense in Australia and what the short-term and long-term effects could be for the healthcare sector. Welcome back to *Hacking Healthcare*.

1. **Blackbaud Attack Illustrates Trend in Ransomware.** While only coming to light in recent weeks, the cyberattack against Blackbaud represents a high-profile case that illustrates an alarming trend in ransomware. Blackbaud, one of the largest providers of education software in the world, was hit by an attempted ransomware attack in May. While the attackers were stopped from successfully encrypting files and locking Blackbaud out of their own network, the attackers did exfiltrate sensitive files which compelled Blackbaud to pay a ransom anyways.[1]

   This attack, which ultimately affected a dozen or so educational institutions, is one high-profile example of the growing trend in exfiltration and encryption attacks.[2] These types of ransomware attacks look to steal data as well as encrypt files, and researchers have noted an uptick of them since 2019 .[3] Researchers at Emsisoft have noted that over 11% of ransomware attacks this year have included an overt data stealing element.[4]

   Stealing data prior to encrypting it is done for several reasons, including as leverage to ensure a victim doesn't simply restore from a backup, as compensation should the victim decide against payment, or as an additional means of ransom by demanding more money to ensure stolen data is deleted. This may partially account for why paying a ransom demand ends up being more than double as costly as refusing to do so. [5]

   Action & Analysis
   H-ISAC Membership Required

2. **U.S. Charges Two Chinese Hackers.** In the latest major public development of foreign cyber espionage, the US government indicted two Chinese nationals for a long running malicious cyber campaign they perpetrated in cooperation with Chinese government

agencies and on their own for profit. The individuals, Li Xiaoyu and Dong Jiazhi, were indicted on 11 counts including, *conspiracy to commit wire fraud*, *aggravated identity theft*, *computer fraud and abuse: unauthorized access*, *conspiracy to commit theft of trade secrets*, and *conspiracy to access without authorization and damage computers, and to threaten to impair confidentiality of information*.[6]

The indictment, which was unsealed on July 7th, accuses the two of engaging in a decade long campaign of cyberattacks against high tech industries around the world, including "conspiring to steal trade secrets from at least eight known victims, which consisted of technology designs, manufacturing processes, test mechanisms and results, source code, and pharmaceutical chemical structures", as well as COVID-19 research.[7] In referring to the case, Assistant Attorney General for National Security John C. Demers remarked that "China has now taken its place, alongside Russia, Iran and North Korea, in that shameful club of nations that provide a safe haven for cyber criminals in exchange for those criminals being 'on call' to work for the benefit of the state…"[8]

Speaking of cyber criminals working for state strategic goals, Russia too has been called out recently for specifically targeting COVID-19 research. Russian interest has likely spiked as revisions to their own COVID-19 data more than tripled their earlier reported death toll.[9, 10] Authorities in the UK, US, and Canada have all reported that Russian linked APT29 (Cozy Bear) has been attempting to breach vaccine research programs in their respective countries.[11] However, no new indictments have been levied against any of these actors yet.

Action & Analysis
H-ISAC Membership Required

3. A**ustralia Sees Growing Support for Active Cyber Defense.** One of the more controversial strategies for dealing with malicious cyber activity is active cyber defense (ACD). Proponents of ACD stress that organizations need to be proactive in their efforts to stop malicious activity. At the extreme, ACD can constitute legally permitting private sector organizations to "hack back" outside of their own network to stop malicious threats. On the other end of the spectrum, ACD can be operationalized in a limited capacity by governments, such as the UK's Email Check service which "[helps] domain owners understand and control abuse of their email."[12] There is obviously a lot of grey area and nuance between those positions, but historically, governments have been reluctant to unleash the pandoras box of freely allowing the private sector to adopt ACD.

   Currently, both the UK and US governments make use of ACD strategies in one form or another, and Australia may soon be joining them. In a recently released industry advisory panel for Australia's *2020 Cyber Security Strategy*, several recommendations called for better deterrence, increased government involvement, and the Australian Cyber Security Centre to be given the ability to actively "disrupt cyber criminals on the

Dark Web and to target the proceeds of cybercrime."[13] According to the advisory panel, they believe strongly that the UK represents "a best practice model for Australia to emulate" when it comes to ACD.[14]

In terms of what that might encompass, the UK's National Cyber Security Center (NCSC) currently boasts 7 ACD services including, Web Check, Logging Made Easy, Protective Domain Name Service, Exercise in a Box, Vulnerability Disclosure, Host Based Capability, and the previously mentioned Mail Check.[15] These services are generally freely available and, in the NCSC's own words "[tackle] cyberattacks in a relatively automated and scalable way, to improve national resilience."[16] However, despite industry support, there is doubt among some that the needed investment will be forthcoming or that the Department of Home Affairs will commit to implementing an ACD program.

Action & Analysis
H-ISAC Membership Required

Congress –

Tuesday, July 28th:
- Senate – Committee on Homeland Security and Governmental Affairs: Modernizing Telework: Review of Private Sector Telework Policies during the COVID-19 Pandemic

-Senate – Committee on Finance: Protecting the Reliability of the U.S. Medical Supply Chain During the COVID-19 Pandemic Part I

Wednesday, July 29th:
- No relevant hearings

Thursday, July 30th:
- House - Committee on Armed Services - Subcommittee on Intelligence and Emerging Threats and Capabilities: Hearing: Review of the Recommendations of the Cyberspace Solarium Commission

-Senate – Committee on Finance: Protecting the Reliability of the U.S. Medical Supply Chain During the COVID-19 Pandemic Part II

International Hearings/Meetings –

EU – No relevant hearings

Conferences, Webinars, and Summits –

--H-ISAC Navigator Webinar – AttackIQ (7/30/2020)
https://h-isac.org/hisacevents/optimizing-your-security-controls-in-light-of-a-pandemic-by-attackiq/
-- H-ISAC Monthly Member Threat Briefing – Webinar (8/25/2020)
https://h-isac.org/hisacevents/h-isac-monthly-member-threat-briefing-11/
--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 Security Workshop - Virtual (9/23/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-forchheim-germany/
--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
--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/

Sundries –

CISA turns to security experts with street cred to protect health sector
https://www.cyberscoop.com/dhs-coronavirus-vaccine-hackers-josh-corman-rob-arnold-beau-woods/

Top Risks of 1H 2020: Ransomware, Mobile, Health Infrastructure
https://healthitsecurity.com/news/top-risks-of-1h-2020-ransomware-mobile-health-infrastructure

Ongoing Meow attack has nuked 1,800 databases without telling anyone why
https://arstechnica.com/information-technology/2020/07/more-than-1000-databases-have-been-nuked-by-mystery-meow-attack/

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

[1] https://www.zdnet.com/article/cloud-provider-stopped-ransomware-attack-but-had-to-pay-ransom-demand-anyway/

---

[2] https://www.zdnet.com/article/cloud-provider-stopped-ransomware-attack-but-had-to-pay-ransom-demand-anyway/
[3] https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf
[4] https://www.zdnet.com/article/ransomware-warning-now-attacks-are-stealing-data-as-well-as-encrypting-it/
[5] https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf
[6] https://www.documentcloud.org/documents/6999047-Li-Xiaoyu-and-Dong-Jiazhi-indictment.html
[7] https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion
[8] https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion
[9] https://www.cyberscoop.com/coronavirus-vaccine-hacking-cozy-bear-apt29/
[10] https://www.bloomberg.com/news/articles/2020-07-10/russia-more-than-triples-covid-19-death-toll-in-revised-data
[11] https://www.cyberscoop.com/coronavirus-vaccine-hacking-cozy-bear-apt29/
[12] https://www.ncsc.gov.uk/report/active-cyber-defence-report-2019
[13] https://www.homeaffairs.gov.au/cyber-security-subsite/files/2020-cyber-security-strategy-iap-report.pdf
[14] https://www.zdnet.com/article/support-grows-for-an-australian-active-cyber-defence-program/
[15] https://www.ncsc.gov.uk/section/products-services/active-cyber-defence
[16] https://www.ncsc.gov.uk/section/products-services/active-cyber-defence