January 4, 2022

TLP White

This week, *Hacking Healthcare* begins by reviewing how an AvosLocker ransomware attack bolsters our understanding of how ransomware gangs operate. We then jump to the ramifications of a federal appeals court decision to deny an insurance claim resulting from a phishing attack. Finally, we breakdown the key findings of a report on the privacy and cybersecurity challenges and opportunities for telehealth in 2022 and beyond.

Author's Note: Welcome to 2022! With any luck you managed to have some downtime over the last few weeks, although our adversaries (both human and viral) certainly didn't give us much of a break. For whatever it's worth, we'll be here bringing you the best information and analysis we can to help navigate what will almost certainly be another dynamic year. We appreciate everything that you do every day.

Welcome back to *Hacking Healthcare*.

1. **Ransomware Actor Provides Free Decryptor After Mistakenly Targeting Law Enforcement**

   A recent Bleeping Computer article covered how a AvosLocker ransomware attack that unintentionally hit an unnamed law enforcement organization led the cybercriminal group to apologize and provide a free decryptor after recognizing their error.[1] The attack and its aftermath provide an interesting window into cybercriminal ransomware operations.

   Based on a screenshot of the interaction, the AvosLocker ransomware attack appears to have occurred sometime last November, and it was reported that the attack breached the law enforcement organization's network and stole an undetermined amount of data.[2] Upon becoming aware that the victim was a law enforcement organization, the cybercriminal group appears to have reached out to provide a free decryptor.

In responding to a Bleeping Computer follow up, the cybercriminal group admitted that they do not have a policy regarding targeting, but that they "usually avoid" government entities and hospitals.[3] They further noted that while this is the case, affiliates of theirs may sometimes "lock a network without having us review it first."[4] When asked if their preference to avoid hitting hospitals and government agencies was an attempt to mitigate drawing law enforcement or government attention, the group brushed off concerns that law enforcement could impact them and that a more significant reason is that "tax payer money's generally hard to get."[5]

Action & Analysis
Membership required

2. Federal Appeals Court Decision Bolsters Need to Review Insurance Policies

A decision from the United States Court of Appeals for the Fifth Circuit has further highlighted the difficulties in covering cybercrime with insurance policies. The recent judgement in the case of *RealPage Inc v. National Union Fire Insurance Company of Pittsburgh, Pennsylvania, 5th U.S. Circuit Court of Appeals, No. 21-10299*, affirmed a lower court's decision that the insurer did not have to cover roughly $5 million in losses stemming from a successful phishing attack that targeted the victim.[6]

To briefly summarize, a RealPage employee clicked a fake link in an email and provided credential information for one of RealPage's third party payment processors, Stripe Inc., to a cybercriminal actor. That cybercriminal actor then messaged Stripe from the compromised RealPage account with instructions to divert millions of dollars from the intended accounts and into theirs. Roughly $10 million was diverted before RealPage became aware of the issue and informed Stripe Inc to stop payments.

In the aftermath, roughly $4 million was able to be recovered and RealPage filed a claim with National Union Fire Insurance Company of Pittsburgh and their excess carrier, Beazley insurance, for the lost $6 million. The insurer argued that within the language of the policy, RealPage never "held" the funds that were lost due to the phishing attack, and therefore they denied coverage for anything above roughly $1 million in service fees. When challenged in court, both the lower district court and the Federal Appeals Court sided with the insurer.

Action & Analysis
Membership required

3. **New Report Cites Telehealth's Risks, Opportunities, and Challenges**

While the future will undoubtably see many individuals happy to return to in-person visits for their healthcare needs, it seems highly likely that telehealth will remain the go

to option for a significant portion of the population. With that in mind, organizations may find value in reviewing a new report from cybersecurity company Kaspersky on the challenges, risks and opportunities that organizations employing telehealth should be considering.

Some of the report's key findings include:[7]

- "91% of global healthcare providers have already implemented telehealth capabilities and the majority of them only started to use telehealth after the pandemic began";
- 42% of medical organizations report that the majority of telehealth recipients are more interested in telehealth sessions than in person ones due to convenience;
- Clinicians voiced concerns with conducting telehealth, with 81% wary of issues including data security;
- "54% of telehealth providers agree that some of their clinicians conduct remote appointments using apps that are not specifically designed for remote medical sessions with patients. These included FaceTime, Facebook Messenger, WhatsApp, and Zoom.";
- "32% of respondents agree their organization has faced cybersecurity issues due to vulnerabilities in third-party technologies"; and
- "30% of telehealth providers agree some of their clinicians have had their patients' data compromised when conducting remote telehealth sessions."

The report concludes that COVID-19 significantly sped up the adoption of telehealth and that both healthcare providers and patients see the benefits of maintaining telehealth services at scale post-pandemic. However, the rapid unplanned adoption has exacerbated problems, especially around security and privacy. Kaspersky ends by recommending endpoint protection for corporate devices, timely software updates, employee cybersecurity awareness, and strict password policies as additional mitigations.[8]

Action & Analysis
Membership required

Congress

Tuesday, January 4th:
- No relevant hearings

January 4, 2022

Wednesday, January 5th:
- No relevant hearings

Thursday, January 6th:
- No relevant hearings

International Hearings/Meetings –

- No relevant meetings

EU –

Conferences, Webinars, and Summits –

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

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

About the Author

Hacking Healthcare is written by John Banghart, who served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Council's efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Council's Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, and as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.

January 4, 2022

[1] https://www.bleepingcomputer.com/news/security/ransomware-gang-coughs-up-decryptor-after-realizing-they-hit-the-police/

[2] https://www.bleepingcomputer.com/news/security/ransomware-gang-coughs-up-decryptor-after-realizing-they-hit-the-police/

[3] https://www.bleepingcomputer.com/news/security/ransomware-gang-coughs-up-decryptor-after-realizing-they-hit-the-police/

[4] https://www.bleepingcomputer.com/news/security/ransomware-gang-coughs-up-decryptor-after-realizing-they-hit-the-police/

[5] https://www.bleepingcomputer.com/news/security/ransomware-gang-coughs-up-decryptor-after-realizing-they-hit-the-police/

[6] https://law.justia.com/cases/federal/appellate-courts/ca5/21-10299/21-10299-2021-12-22.html

[7] https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2021/11/22125239/Kaspersky_Healthcare-report-2021_eng.pdf

[8] https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2021/11/22125239/Kaspersky_Healthcare-report-2021_eng.pdf