Health-ISAC Weekly Blog -- Hacking Healthcare

Hacking Healthcare | TLP:WHITE | Alert ID : 6b33c546 | Jan 10, 2023, 09:32 AM

Happy New Year!

To kick off 2023, Hacking Healthcare begins by examining an end of year ransomware attack against a Canadian children's hospital. Beyond assessing the unique aspects of the attack, such as why a notorious ransomware group apologized and offered a free decryptor to its victim, we take a broader look at how healthcare cyberattacks might influence the policy landscape for both governments and healthcare organizations in the near future. This includes highlighting how pressure is likely to increase to view these attacks as more than just financial crimes. Welcome back to *Hacking Healthcare*.

Canadian Children's Hospital Hit By Ransomware – Notorious Cybercriminal Group Apologizes

A holiday season ransomware attack on Toronto Canada's Hospital for Sick Children (SickKids) sadly comes as no surprise given that the healthcare sector continues to be viewed as a legitimate target by cybercriminal actors. This attack highlights some interesting dynamics within the cybercriminal ecosystem and it adds to the growing sense that ransomware attacks against healthcare organizations may need to be thought of as more than just financial crimes, especially as evidence of negative patient care outcomes continues to grow.

On December 19, SickKids published a notice on their website stating that they were responding to a cybersecurity incident that allegedly began the evening before.[i] Initial reports from SickKids stated that there was no evidence to suggest that "personal information or personal health information has been impacted" and that "the incident appears to have only impacted a few internal clinical and corporate systems, as well as some hospital phone lines and webpages."[ii]
However, later updates confirmed that clinical teams were experiencing delays with retrieving lab and imaging results, phone lines and staff payroll systems were negatively impacted, and patients and families were warned

that some may experience diagnostic and/or treatment delays.[iii], [iv] Underscoring the scale of the issues, SickKids announced that not yet 50 percent of "priority systems" were restored by December 29, ten days after the initial incident, and that it could be weeks before all systems return to normal.[v]

Where this instance deviates from many other ransomware attacks against the healthcare sector is the public apology, explanation, and offer of a free decryptor from the notorious ransomware group, LockBit. Alleging that the attack was carried out by a partner who violated LockBit's rules, a LockBit blog post on their data leak site was published on December 31, which apologized for the attack and offered up a free decryptor that SickKids has said they are assessing with their third-party experts.[vi], [vii] While it appears that many critical systems have since been restored, recovery remains ongoing.

Action & Analysis

Included with H-ISAC Membership

Congress

Tuesday, January 10th:

- No relevant hearings

Wednesday, January 11th:

- No relevant hearings

Thursday, January 12th:

- No relevant hearings

International Hearings/Meetings

- No relevant meetings

EU –

[i] https://www.sickkids.ca/en/news/archive/2022/sickkids-responding-to-cybersecurity-incident/
[ii] https://www.sickkids.ca/en/news/archive/2022/sickkids-responding-to-cybersecurity-incident/
[iii] https://www.sickkids.ca/en/news/archive/2022/update-on-sickkids-response-to-cybersecurity-incident/
[iv] https://www.sickkids.ca/en/news/archive/2022/sickkids-restoration-efforts-continue-from-cybersecurity-incident/
[v] https://www.sickkids.ca/en/news/archive/2022/many-sickkids-systems-restored-following-cybersecurity-incident/
[vi] https://www.bleepingcomputer.com/news/security/ransomware-gang-apologizes-gives-sickkids-hospital-free-decryptor/
[vii] https://www.sickkids.ca/en/news/archive/2022/sickkids-aware-of-and-assessing-decryptor-following-cybersecurity-incident/
[viii] https://www.therecord.com/ts/news/canada/2023/01/02/ransomware-group-lockbit-apologizes-saying-partner-was-behind-sickkids-attack.html
[ix] https://www.justice.gov/opa/pr/man-charged-participation-lockbit-global-ransomware-campaign
[x] https://www.therecord.com/ts/news/canada/2023/01/02/ransomware-group-lockbit-apologizes-saying-partner-was-behind-sickkids-attack.html

[xi] https://www.therecord.com/ts/news/canada/2023/01/02/ransomware-group-lockbit-apologizes-saying-partner-was-behind-sickkids-attack.html
[xii] https://www.bleepingcomputer.com/news/security/ransomware-gang-apologizes-gives-sickkids-hospital-free-decryptor/
[xiii] https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-cyber-insecurity-healthcare-ponemon-report.pdf
[xiv] https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-cyber-insecurity-healthcare-ponemon-report.pdf
[xv] https://www.politico.com/news/2022/12/28/cyberattacks-u-s-hospitals-00075638
[xvi] https://www.hipaajournal.com/white-house-plans-to-issue-new-cybersecurity-standards-for-the-healthcare-industry/

Reference | References

Politico
sickkids
HIPAA Journal
Health-ISAC
Bleeping Computer
US Department of Justice
sickkids
Proofpoint
The Record
sickkids
sickkids
sickkids

Report Source(s)

Health-ISAC

Tags

Hacking Healthcare, Ransomware

For Questions and/or Comments:
Please email us at contact@h-isac.org

Conferences, Webinars, and Summits:
https://h-isac.org/events/

Hacking Healthcare:
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, 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.

Access the Health-ISAC Intelligence Portal: Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.