Health-ISAC Weekly Blog -- Hacking Healthcare

Hacking Healthcare | TLP:WHITE | Alert ID : 028ba5ab | Dec 15, 2022, 02:57 PM

This week, Hacking Healthcare begins with a reminder for next week's Health-ISAC Monthly Threat Brief. Next, we use the upcoming end of life for Windows 7 and 8 to frame a conversation about legacy technology in the healthcare sector. This includes breaking down some of the regulatory concerns, examining the value of hardware and software inventory, and advocating for vendor support to be assessed in any acquisition process. We wrap up this week's newsletter with a look at an interesting new development in the ransomware ecosystem and ponder what it may mean in the long run.

Welcome Back to *Hacking Healthcare.*

Health-ISAC Monthly Threat Brief

It is almost time for December's Monthly Threat Brief (MTB)! All Health-ISAC members are encouraged to attend the hour-long presentation on Tuesday, December 20th, beginning at noon eastern time. The MTB provides succinct briefings on a variety of topics, such as new trends in cybersecurity, emerging threats, physical security, and legal and regulatory issues. The MTB is a free service for Health-ISAC members, and we hope to see you there.

Upcoming Windows End of Life Provides Good Reminder for Legacy Technology

You would be forgiven for thinking (or perhaps wishing) that Windows 7 and 8, which debuted in 2009 and 2012 respectively, were already dead and buried. Both OSs are still technically supported, but with their final sendoff rapidly approaching, it is as good a time as any to remind organizations to plan for their official end of life and to offer some general thoughts on the broader issue of legacy technology in the healthcare sector.

On January 10th of next year, Microsoft will officially end support for a host of products, but Windows 7 and 8 OSs are likely the most critical.[i] After that date, Windows 8 will no longer receive security updates, non-security updates, bug fixes, technical support, or online technical content updates.[ii] Windows 7 will stop receiving its Extended Security Updates (ESU), which were implemented years ago as a "last resort option for customers who need to run certain legacy Microsoft products past the end of support."[iii]

Mainstream Windows 7 support expired in 2015 for most users, but its popularity and business criticality ensured that it received an extended support period until 2020. For some organizations, ESU was available through volume licensing programs for Windows 7 Professional, Enterprise, and Professional for Embedded Systems editions, which added three additional years of security updates.[iv] Windows 8.1 does not appear set to receive additional ESU and will therefore go out alongside its predecessor in January.

Action & Analysis

Included with H-ISAC Membership

Ransomware Groups Target Executives with a Twist

We've covered the ever-changing ransomware landscape for years, and one thing that we can conclusively state is that cyber criminals are certainly creative when it comes to finding new ways to coerce payments out of victims. A new scheme that's been reported on by Brian Krebs raises questions about how aggressive ransomware actors may become if ransomware victims more regularly refuse to pay up.[vii]

According to a KrebsOnSecurity interview with Alex Holden of cybersecurity firm, Hold Security, a ransomware group named Venus has been identified as becoming frustrated over the number of firms that they compromise and that then refuse to pay up. In response, Venus has apparently been identified discussing a scheme "center[ed] on trying to frame executives at public companies for insider trading charges."[viii]

The scheme apparently has to do with "carefully editing one or more email inbox files at a victim firm — to insert messages discussing plans to trade large volumes of the company's stock based on non-public information."[ix] While the Krebs' piece goes on to describe methods to make the insider trading correspondence appear to be legitimately created on the executive's device, it also states that this attack is unlikely to be "forensically solid."[x] However, this may not matter, as it appears that the goal is to threaten the victim with leaking the falsified documents to cause a scandal in order to extort them.

Action & Analysis

Included with H-ISAC Membership

Congress

Tuesday, December 13th:

- No relevant hearings

Wednesday, December 14th:

- No relevant hearings

Thursday, December 15th:

- No relevant hearings

International Hearings/Meetings

- No relevant meetings

EU –

[i] https://learn.microsoft.com/en-us/lifecycle/end-of-support/end-of-support-2023
[ii] https://learn.microsoft.com/en-us/lifecycle/products/windows-81?branch=live
[iii] https://learn.microsoft.com/en-us/lifecycle/faq/extended-security-updates
[iv] https://learn.microsoft.com/en-us/lifecycle/products/windows-7?branch=live
[v] https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-fall-2021/index.html
[vi] https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-fall-2021/index.html
[vii] https://krebsonsecurity.com/2022/12/new-ransom-payment-schemes-target-executives-telemedicine/
[viii] https://krebsonsecurity.com/2022/12/new-ransom-payment-schemes-target-executives-telemedicine/
[ix] https://krebsonsecurity.com/2022/12/new-ransom-payment-schemes-target-executives-telemedicine/
[x] https://krebsonsecurity.com/2022/12/new-ransom-payment-schemes-target-executives-telemedicine/
[xi] https://www.washingtonpost.com/technology/2022/11/14/twitter-fake-eli-lilly/

Reference | References

Health-ISAC
Washington Post
HHS.gov
Microsoft
Krebs on Security
Microsoft

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.