Health-ISAC Weekly Blog -- Hacking Healthcare

Hacking Healthcare | TLP:WHITE | Alert ID : 1a96f1a8 | Feb 23, 2023, 05:09 PM

Recently, we became aware that several of the past Hacking Healthcare submissions from this year have inadvertently omitted attribution to some sources that were used to provide background and context. These unintentional omissions will soon be rectified with revised versions that can be found in Health-ISAC's archives. The subject and substance of these articles remains unchanged and due credit will properly attributed. We apologize for this oversight.

This week, Hacking Healthcare examines a major report on the cyber threat landscape as it relates to Ukraine. Google's new report, which investigates government-backed operations, information operations, and the cybercriminal ecosystem, provides a useful window into how cyber capabilities have, and have not, been used in a modern armed conflict between technologically modern states. We break down some of the more interesting findings, including the degree to which healthcare has been targeted and what the conflict has appeared to do to the cybercriminal ecosystem.

Welcome back to *Hacking Healthcare*.

Google Reports on the Ukrainian Conflict's Cyber Threat Landscape

The Russian invasion of Ukraine, soon to enter its second year, brought an intense focus on cyberspace. With tensions between Russia and the West already high, many speculated that the conflict might become a testbed for new and destructive cyber weapons as well as a justification to ramp up cyberattacks beyond Ukraine's borders.[i] [ii] While fears of a wider "cyber war" look to be overstated, understanding the nuanced impact that the conflict has had on the cyber threat landscape could prove incredibly valuable to policymakers and cyber defenders. A recently released report from Google is perhaps the most comprehensive snapshot yet produced. So, what does it say and what can the healthcare and public health (HPH) sectors learn from it?

Google released its 47-page report, *Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape,* on February 16th.[iii] The product of a collaboration between three of Google's internal teams, the Threat Analysis Group (TAG), Mandiant, and Google Trust & Safety, the report is split into sections detailing government-backed cyber operations, information operations, and cybercrime. At a high level, the primary takeaways for each were summed up by Google as follows:

Government-backed Operations:

- **NATO Phishing –** Google noted a 300 percent increase in Russian spear-phishing attacks against entities located in North Atlantic Treaty Organization (NATO) member countries.[iv]

- **Destructive Attacks Spike** – Google noted that attacks were carried out against civilian infrastructure in what they believe was an attempt "to undermine the public's trust in the government's ability to deliver basic services."[v] They also noted that they "observed more destructive cyberattacks in Ukraine during the first four months of 2022 than in the previous eight years."[vi]

Information Operations:

- **Full-Spectrum Operations** – The Russian government carried out "the full spectrum of information operations" to further Russian strategic interests.[vii]

Cybercrime:

- **Seismic Shifts** – The conflict has resulted in significant upheaval within the cybercriminal ecosystem that Google asserts "will likely have long term implications for both coordination between criminal groups and the scale of cybercrime worldwide."[viii]
- **"Ransomware Retaliation" –** Google did not note an increase in cyberattacks targeting critical infrastructure in NATO member countries.

Other:

- Google expects that cyberattacks targeting NATO member countries will continue when it suits broader strategic aims.
- Google "assess[es] with high confidence" that "disruptive and destructive attacks" are likely to be increasingly used in response to deteriorating battlefield conditions.[ix] Google believes that these attacks are likely to increasingly hit targets outside of Ukraine.
- Healthcare was not a prominently targeted sector.

Google ends its report by stating that they plan on continuing to monitor the threat landscape and aid in security efforts.

Action & Analysis

Included with H-ISAC Membership

Congress

Tuesday, February 21st:

- No relevant hearings

Wednesday, February 22nd:

- No relevant hearings

Thursday, February 23rd:

- No relevant hearings

International Hearings/Meetings

- No relevant meetings

EU –

[i] https://www.washingtonpost.com/politics/2022/01/25/cyber-fears-mount-amid-prospect-russian-invasion-ukraine/

[ii] https://www.cnn.com/2022/01/24/politics/russia-cyberattack-warning-homeland-security/index.html
[iii] https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf
[iv] https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf
[v] https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf
[vi] https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf
[vii] https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf
[viii] https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf
[ix] https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf
[x] https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf
[xi] https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf

Reference | References

Washington Post
Google Threat Horizons Report
CNN Money

Report Source(s)

Health-ISAC

Tags

Hacking Healthcare, Russia, Ukraine

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.