January 13, 2022

TLP White

This week, *Hacking Healthcare* begins by breaking down the Federal Trade Commission's warning that it may take action against companies that don't remediate the Log4j vulnerability in a timely manner. Next, we jump to a new phishing technique that abuses Google Docs to slip under automated email filters and manual review alike. Finally, we try to provide some context around the ongoing U.S.-Russia talks and discuss how raised diplomatic tensions may stoke offensive cyber operations against critical infrastructure.

Welcome back to *Hacking Healthcare*.

1. **The Federal Trade Commission Sends Log4j Warning**

   Log4j's ongoing exploitation and remediation is just the latest in a long series of major cyber incidents that have had global impact in the last few years. However, this one has caught the attention of the Federal Trade Commission (FTC), which has used notably strong language in warning companies of the need to remediate the vulnerability quickly or face potential consequences.

   In case you might have been on vacation for the last month or so, a short summary is in order. As the FTC succinctly puts it, "Log4j is a ubiquitous piece of software used to record activities in a wide range of systems found in consumer-facing products and services."[1] Last month, several significant vulnerabilities in this piece of software were reported, setting off a sprint to secure affected systems before they could be exploited. H-ISAC Members looking for a comprehensive breakdown of the vulnerability can review the various alerts and intelligence reports distributed by the H-ISAC in mid-December. They offer an excellent overview of Log4j, and links can be found in the "Action & Analysis" section in the Amber version of this blog.

   Unfortunately, the sheer scale of potentially affected products and applications, and the added complexity of how those products and applications may be tied to critical third-party services or legacy products, has made remediating this issue extremely challenging and time consuming.

The potential impact of Log4j's exploitation was not lost on the FTC, which said that it "[poses] a severe risk to millions of consumer products [and] to enterprise software and web applications."[2] The FTC, whose mission is to "protect consumers and promote competition," put out a warning in a January 4th blog post noting the vulnerability's risk in relation to "a loss or breach of personal information, financial loss, and other irreversible harms."[3]

According to the blog post, the FTC believes "[i]t is critical that companies and their vendors relying on Log4j act now, in order to reduce the likelihood of harm to consumers," and that failure to do so may result in FTC legal action.[4] As it stated, "The FTC intends to use its full legal authority to pursue companies that fail to take reasonable steps to protect consumer data from exposure as a result of Log4j, or similar known vulnerabilities in the future."[5] Time will tell just how involved the FTC is willing and able to be in pursuing companies it feels are not adequately remediating this vulnerability.

Action & Analysis
Membership required

2. Phishers Take Advantage of Google Docs

The general uptick in phishing awareness and training among organizations' employees has proved to be a helpful, if imperfect, approach to combating what is often the weakest part of any organization's cybersecurity — the human element. While tried and tested phishing techniques haven't suddenly become completely ineffective, malicious actors continue to look for innovative ways to compromise their targets more successfully. A recent slew of news articles based on threat research from email security firm Avanan has highlighted one particular trick leveraging Goggle Docs that emerged late in 2021.

Reportedly under exploitation since October and gaining significant traction in December, the technique is relatively simple.[6] A malicious actor creates a Google account to create a Google Doc. Within the Doc, the malicious actor then creates a comment with the target's email specified with an "@" symbol. When the comment is completed, Google sends an email notification to the target email that it has been mentioned in the Google Doc, and the email notification itself contains a reproduction of the comment complete with any malicious links. What makes this technique effective is that the notification email comes from Google and the commentator's identity is limited to whatever name it set its account to. The account itself is not shown.

The result is an attack that:[7]

- Likely avoids automatic email filtering as the message comes from Google

- Likely avoids significant suspicion from manual review unless the content of the comment itself raises red flags
- Makes it relatively easy for the malicious comment's sender to impersonate a co-worker of the target
- Leverages the remote/collaborative work environment that COVID-19 has helped make central to many organizations' workday processes

Threat analysts at Avanan are reportedly monitoring this exploit and have confirmed that the technique also works in Google Slide.[8] Avanan's research has concluded that the current campaign leveraging this technique primarily targets Outlook users, makes use of over 100 Google accounts, and has hit at least 30 organizations so far.[9]

Avanan reportedly notified Google of this attack technique on January 3rd, and while Bleeping Computer reports that Google has attempted to mitigate the issue, no detail is given, and Bleeping Computer reports that "they haven't fully closed the vulnerability yet."[10, 11] A more comprehensive breakdown of the issue can be found in Avanan's blog post.[12]

Action & Analysis
Membership required

3. U.S.-Russia Talks Over Ukraine Have Cyber Ramifications

As cyber has become an increasingly used tool for governments across the globe to influence diplomacy and achieve strategic goals, it should come as no surprise that raised geopolitical tensions over Ukraine could lead to significant cyber actions. This makes it as good a time as any to examine how the current U.S.-Russia talks are going, and why it's something worth paying attention to from a cybersecurity perspective.

Without getting too drawn in to the very long and fraught history of the region, the current situation is mired in layers of complexity. Russia's forceful annexation of Crimea, which was condemned by the United States and its allies, and the long-running strife between separatists in the Donbas region and the Ukrainian government, has kept the country in low-intensity conflict for years. Recent allegations by the Unites States that Russia was planning some form of armed invasion, coupled with a Russian military buildup near the Russia-Ukrainian border, brought renewed political fervor to issues in the region and between Russia and the West. Russia has long held a foreign policy that strives to maintain significant influence in the countries in its immediate geographic proximity and has chafed at the enlargement of political entities like the European Union and military alliances like the North Atlantic Treaty Organization (NATO), which have slowly expanded into those areas.

Both sides have agreed to talks in an attempt to defuse tensions and avoid the kind of crisis that could lead to the escalation of armed conflict or a series of damaging economic sanctions and reprisals. Diplomats from each government have described the talks as "professional," and both appear to be taking the other's positions seriously.[13] However, so far it appears that only limited progress has been made in reaching a solution agreeable to both sides. Several of the issues being debated include Russia's desire that Ukraine and other former Soviet Bloc countries should never join NATO, and its desire that military activity and the deployment of NATO personnel in the region's newer NATO members should be scaled back. Meanwhile, the United States appears to have focused on more technical measures related to arms control.[14]

Observers and participants appear concerned that Russia's demands will be viewed as nonstarters for the United States and that talks may soon hit an impasse.[15] Others have suggested that Russian demands are purposefully designed to be rejected by the United States to allow a pretext for invasion.[16] The situation is likely to remain tense for some time.

Action & Analysis
Membership required

Congress

Tuesday, January 11th:
- House of Representatives – Committee of Oversight and Reform: ""Cybersecurity for the New Frontier: Reforming the Federal Information Security Management Act"

Wednesday, January 12th:
- No relevant hearings

Thursday, January 13th:
- No relevant hearings

International Hearings/Meetings –

- No relevant meetings

EU –

January 13, 2022

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.

---

[1] https://www.ftc.gov/news-events/blogs/techftc/2022/01/ftc-warns-companies-remediate-log4j-security-vulnerability?utm_campaign=ftc_warns_companies_to_re&utm_content=1641325381&utm_medium=social&utm_source=linkedin,twitter

[2] https://www.ftc.gov/news-events/blogs/techftc/2022/01/ftc-warns-companies-remediate-log4j-security-vulnerability?utm_campaign=ftc_warns_companies_to_re&utm_content=1641325381&utm_medium=social&utm_source=linkedin,twitter

[3] https://www.ftc.gov/news-events/blogs/techftc/2022/01/ftc-warns-companies-remediate-log4j-security-vulnerability?utm_campaign=ftc_warns_companies_to_re&utm_content=1641325381&utm_medium=social&utm_source=linkedin,twitter

[4] https://www.ftc.gov/news-events/blogs/techftc/2022/01/ftc-warns-companies-remediate-log4j-security-vulnerability?utm_campaign=ftc_warns_companies_to_re&utm_content=1641325381&utm_medium=social&utm_source=linkedin,twitter

---

[5] https://www.ftc.gov/news-events/blogs/techftc/2022/01/ftc-warns-companies-remediate-log4j-security-vulnerability?utm_campaign=ftc_warns_companies_to_re&utm_content=1641325381&utm_medium=social&utm_source=linkedin,twitter

[6] https://www.bleepingcomputer.com/news/security/google-docs-commenting-feature-exploited-for-spear-phishing/

[7] https://www.bleepingcomputer.com/news/security/google-docs-commenting-feature-exploited-for-spear-phishing/

[8] https://www.bleepingcomputer.com/news/security/google-docs-commenting-feature-exploited-for-spear-phishing/

[9] https://www.bleepingcomputer.com/news/security/google-docs-commenting-feature-exploited-for-spear-phishing/

[10] https://www.bleepingcomputer.com/news/security/google-docs-commenting-feature-exploited-for-spear-phishing/

[11] https://www.avanan.com/blog/google-docs-comment-exploit-allows-for-distribution-of-phishing-and-malware

[12] https://www.avanan.com/blog/google-docs-comment-exploit-allows-for-distribution-of-phishing-and-malware

[13] https://www.theguardian.com/us-news/2022/jan/10/ukraine-talks-us-russia-latest

[14] https://www.theguardian.com/us-news/2022/jan/10/ukraine-talks-us-russia-latest

[15] https://www.reuters.com/world/europe/prospects-dim-us-russia-start-tense-talks-over-ukraine-crisis-2022-01-10/

[16] https://www.bbc.com/news/world-europe-59935990