January 19, 2022

TLP White

This week, *Hacking Healthcare* begins by breaking down what the Federal Bureau of Investigation's (FBI) new strategy to combat cybercrime means, and why it may not produce significantly better results than its current approach. Next, we examine the significance of U.S. Cyber Command's (CYBERCOM) recent press release linking a cyber threat actor group to Iran's intelligence agency. Finally, we briefly note that vulnerabilities aren't the only supply chain threat to be aware of as we look at a case of deliberate sabotage that impacted tens of thousands of dependent apps.

Welcome back to *Hacking Healthcare*.

FBI Looks to Change Cybercrime Strategy

It is well established that traditional law enforcement approaches to cracking down on cybercrime and malicious cyber actions has led to mixed results. According to new public statements from FBI officials, it's time for a change in strategy. Exactly what that will mean, and how effective it will turn out to be, remains to be seen.

In a public event last week, the FBI's assistant director of their cyber division, Bryan Vorndran, stated that "The FBI specifically is moving away from an indictment- and arrest-first model into the totality of imposing costs on our adversaries, and we're making tremendous progress there."[1] He continued by saying that "There is a right time for indictments and arrests and certainly one of our goals is to take players off the field. But at the end of the day, we're a team member first before we're prioritizing our own authorities."[2]

Those comments were partially echoed by the FBI's deputy assistant director of the cyber division, Tonya Ugoretz, that same day. Ugoretz mentioned that the FBI would like to replicate and scale their ability to make ransomware seizures and that more money was recovered than has been publicly reported.[3] Additionally, while talking about ransomware payments, Ugoretz

noted that the FBI was “not interested in any activity that's going to kind of drive this whole ecosystem further underground.”[4]

Action & Analysis
Membership required

U.S. Cyber Command Links Hacking Group to Iranian Government

Last Wednesday, U.S. Cyber Command (CYBERCOM) published a press release entitled *Iranian intel cyber suite of malware uses open-source tools* that publicly linked the threat actor MuddyWater to being part of the Iranian government. The disclosure represents one of the few times that this particular U.S. government agency has taken a definitive stand on the relationship between a threat actor and a state government.

With their stated goal being “to better enable defense against malicious cyber actors,” the relatively short release explains that CYBERCOM has “identified and disclosed multiple open-source tools that Iranian intelligence actors are using,” and that identifying multiple such tools on a network “may indicate the presence of Iranian malicious cyber actors.”[5] Included in the release are a number of technical aspects of how MuddyWater could be leveraging malware within networks, and a link to CYBERCOM’s malware alert on Virustotal.

MuddyWater has been previously identified as an Iranian group whose targets have tended to be located in the Middle East, but which has occasionally victimized organizations in Europe and North America.[6] It has been described as “highly active” and has shown a willingness to improve and expand its set of tools to remain effective.[7]

Action & Analysis
Membership required

Developer Sabotage of Open-Source Code Libraries Disrupts Thousands of Apps

Supply chain vulnerabilities and the open-source ecosystem have become significant talking points in recent weeks, with Log4j even spurring the White House into holding a meeting “to discuss initiatives to improve the security of open-source software.”[8] While vulnerabilities like Log4j have received much of the attention, purposeful sabotage is another threat requiring awareness.

Earlier this month, Marak Squires, a JavaScript programmer who authored two widely used JavaScript libraries, decided to purposefully sabotage them for reasons that remain unclear. His

Faker and Colors libraries receive millions of downloads a week and his malicious updates "contained code to produce an infinite loop that caused dependent apps to spew gibberish," that ultimately caused "tens of thousands of JavaScript programs [to blow up]."[9, 10]

Squires' rationale isn't known, but his social media history references conspiracy theories and he has reportedly posted in the past about a lack of compensation for his work. As ZDNet notes, it's hardly the first time something like this has happened, referencing a 2016 incident that also affected thousands of programs.[11] These are unlikely to be the last occurrences that put the software supply chain and open-source ecosystem in the spotlight.

It's also worth noting that while these issues are serious, we aren't without the means to tackle them. We'll discuss more in the *Action & Analysis* section, but you don't have to look any further than the H-ISAC for examples of where coordinated information sharing can be impactful. Turning our attention back to Log4j, the H-ISAC worked across medical device manufacturers to gather and consolidate a list of notices all in one place, making it easier for operators of those devices to determine where they might be at risk. You can find this list at https://h-isac.org/apache-log4j-notices/.

Action & Analysis
Membership required

Congress

Tuesday, January 18th:
- No relevant hearings

Wednesday, January 19th:
- House of Representatives – Committee on Foreign Affairs: Transatlantic Cooperation on Critical Supply Chain Security

Thursday, January 20th:
- No relevant hearings

International Hearings/Meetings –

- No relevant meetings

January 19, 2022

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.

---

[1] https://thecyberwire.com/newsletters/policy-briefing/4/10

[2] https://www.cyberscoop.com/fbi-vorndran-ugoretz-arrest-model-ransomware/

[3] https://www.washingtonpost.com/washington-post-live/2022/01/13/transcript-securing-cyberspace-with-dmitri-alperovitch-jeremy-sheridan-tonya-ugoretz/

[4] https://www.washingtonpost.com/washington-post-live/2022/01/13/transcript-securing-cyberspace-with-dmitri-alperovitch-jeremy-sheridan-tonya-ugoretz/

---

[5] https://www.cybercom.mil/Media/News/Article/2897570/iranian-intel-cyber-suite-of-malware-uses-open-source-tools/

[6] https://www.bleepingcomputer.com/news/security/us-links-muddywater-hacking-group-to-iranian-intelligence-agency/

[7] https://www.bleepingcomputer.com/news/security/us-links-muddywater-hacking-group-to-iranian-intelligence-agency/

[8] https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/13/readout-of-white-house-meeting-on-software-security/

[9] https://arstechnica.com/information-technology/2022/01/foss-developer-who-nuked-his-apps-embraced-qanon-theory-involving-aaron-swartz/

[10] https://www.zdnet.com/article/when-open-source-developers-go-bad/

[11] https://www.zdnet.com/article/when-open-source-developers-go-bad/