April 26, 2022

TLP White

This week, *Hacking Healthcare* examines how a United States law enforcement agency was given legal backing to remotely access private devices to cleanse malware. This operation raises interesting legal questions as well as concerns over the potential for accidental harm. Then, we provide thoughts on how the United States government's attempts at public-private collaboration keep falling short. Welcome back to *Hacking Healthcare*.

FBI Removal of Malware Draws Scrutiny

News that the Federal Bureau of Investigation (FBI) had disrupted a botnet linked to the Russian government's intelligence service sounds like it should be unequivocally good news for everyone but the Russian government. However, the manner in which the operation occurred has raised some concerns and has highlighted a larger discussion about how cybersecurity, geopolitics, and the law are intertwined.

On April 6, the U. S. Department of Justice (DOJ) issued a press release titled *Justice Department Announces Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate (GRU).*[1] The posting announced that a court-authorized operation had been conducted several weeks earlier to "disrupt a two-tiered global botnet of thousands of infected network hardware devices under the control of a threat actor known to security researchers as Sandworm."[2] Sandworm, a well-known threat actor, has previously been linked to Russia with the United States government attributing it to the Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU).[3]

To briefly recap, several weeks prior to the operation, the United Kingdom's National Cyber Security Centre (NCSC), the United States' Cybersecurity and Infrastructure Security Agency (CISA), the FBI, and the National Security Agency (NSA) released a public joint advisory warning of Sandworm's use of Cyclops Blink malware.[4] The advisory included technical details, mitigations, indicators of compromise, and other guidance in a call for action. Furthermore, affected device manufacturers released their own guidance and detection and remediation tools.[5, 6] In addition, the DOJ stated that it had "been attempting to provide notice to owners of

infected WatchGuard devices in the United States and, through foreign law enforcement partners, abroad," including "[providing] notice to the owners of the domestic C2 devices from which the FBI copied and removed the Cyclops Blink malware."[7]

Despite this, according to the DOJ, by mid-March the majority of "originally compromised devices" remained infected, and it is here that the FBI appeared to have undertaken a court-authorized operation to disrupt the botnet. The operation consisted of the FBI "[copying] and [removing] malware from vulnerable internet-connected firewall devices that Sandworm used for command and control (C2) of the underlying botnet."[8] This action effectively cut off the thousands of infected devices from being reached.

The malware and associated botnet were described as a national security threat by U.S. Attorney Cindy K. Chung for the Western District of Pennsylvania, and the operation was hailed by the FBI as "an example of the FBI's commitment to combatting cyber threats through our unique authorities, capabilities, and coordination with our partners."[9]

Needing Both Parts in Public-Private Partnership

In early April, the United States House of Representatives' Committee on Homeland Security's Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation, held a hearing on "Maturing Public-Private Partnerships to Secure U.S. Infrastructure." The stated purpose of the hearing was to "assess Federal efforts to mature collaboration with critical infrastructure owners and operators as they work to defend their networks and build resilience," and to "focus on identifying gaps in existing Federal authorities, opportunities to enhance operational collaboration with key private sector partners, and lessons learned from past efforts to prioritize and secure our nation's most critical, systemically important assets and systems."[10] From the government side, the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the National Cyber Director (ONCD), and the U.S. Government Accountability Office (GAO) were all present.

Notably absent was the participation of any members of the private sector.

Congress –

Tuesday, April 26th:

- No relevant hearings

Wednesday, April 27th:

- No relevant hearings

Thursday, April 28th:

- No relevant hearings

April 26, 2022

International Hearings/Meetings –

- No relevant meetings

EU –

- No relevant meetings

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.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-botnet-controlled-russian-federation

[2] https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-botnet-controlled-russian-federation

[3] https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-botnet-controlled-russian-federation

[4] https://www.cisa.gov/uscert/ncas/alerts/aa22-054a

[5] https://detection.watchguard.com/

[6] https://www.asus.com/content/ASUS-Product-Security-Advisory/

[7] https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-botnet-controlled-russian-federation

[8] https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-botnet-controlled-russian-federation

[9] https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-botnet-controlled-russian-federation

[10] https://homeland.house.gov/news/media-advisories/tomorrow_10am-cybersecurity-hearing-on-maturing-public-private-partnerships-to-secure-us-infrastructure