February 15, 2022

TLP White

This week, *Hacking Healthcare* begins by trying to make sense of the Russian government's ongoing law enforcement operations against cybercriminals within its jurisdiction. We attempt to identify some potential motivations for the actions, as well as the short-term and long-term impacts the operations may have. We then examine the U.S. Department of Justice's (DOJ) arrests and seizure of $3.6 billion of stolen bitcoin and break down why it may not end up being much of a deterrent for cryptocurrency related cybercrimes. Welcome back to *Hacking Healthcare*.

1. **Russian Government Operations Against Cybercriminals Continues**

   Last month, we covered how Russian authorities had apparently undertaken a significant law enforcement action against individuals purported to be affiliated with the cybercriminal group REvil. While the arrests and seizures were a welcome development, we cautioned drawing the conclusion that it represented a significant policy shift for the Russian government. While it is still too early to make any determination on Russian policy, follow-on reports have shown that Russian authorities have continued to take law enforcement actions targeting cybercriminal groups and their infrastructure.

   Last week, it was reported that Russian authorities "seized the websites of several Russian cybercrime forums," and arrested six individuals allegedly connected to cyber fraud.[1] The operation appears to have taken down several websites and forums connected to stolen credit card data, including Ferum Shop, Sky-Fraud, and Trump's Dumps.[2] Additionally, it was reported that Russian authorities also seized "UAS (Ultimate Anonymity Services), a portal for selling remote desktop protocol (RDP) access to compromised business environments."[3] As Security Week's reporting noted, these seizures followed only weeks after another well known "carding" organization, UniCC, was shut down through the arrests of several individuals.

   Elements of the Russian Ministry of Internal Affairs that took part in the operation appear to have left a message for other cyber criminals warning that "theft of funds from bank cards is illegal," and a further warning in the source code of some of the seized sites. The message appears to translate to "Which of you is next?"[4] The increased

tempo of law enforcement operations and the messaging has led some commentators to expect that this latest round of actions is unlikely to be the last.[5]

Analysis of the recent actions against the Russian carding entities and individuals has drawn considerable interest from experts and analysts who find the moves unusual. Stas Alforov, director of research for Gemini Advisory, is quoted by KrebsonSecurity as saying "It's not in their business to be taking down Russian card shops…unless those shops were somehow selling data on Russian cardholders, which they weren't."[6] It appears to be anyone's guess as to what the Russian authorities may do next, and why.

Action & Analysis
Included with H-ISAC Membership

2. $4.5 Billion in Bitcoin Laundered by New York Couple

Earlier this month, the Department of Justice (DOJ) announced it had arrested two individuals suspected of conspiring to launder $4.5 billion in stolen cryptocurrency related to the 2016 hack of the cryptocurrency exchange Bitfinex.[7] The arrests and subsequent seizure are being touted as another example of how law enforcement can track cryptocurrency and prosecute cybercriminals.

On February 8th, the DOJ announced, "the department's largest financial seizure ever."[8] According to the DOJ, two residents of New York were arrested for conspiring to "launder the proceeds of 119,754 bitcoin that were stolen from Bitfinex's platform after a hacker breached Bitfinex's systems and initiated more than 2,000 unauthorized transactions."[9] The DOJ outlined how a complex money laundering process was used to transfer some of the stolen bitcoin into funds placed in accounts of the two accused individuals, with the majority of the stolen bitcoin still intact in a cryptocurrency wallet that was accessed and seized by special agents.[10] The seized bitcoin was worth roughly $3.6 billion at the time of the seizure.

Among the various money laundering techniques employed by the accused were the use of "fictitious identities to set up online accounts; utilizing computer programs to automate transactions, a laundering technique that allows for many transactions to take place in a short period of time; depositing the stolen funds into accounts at a variety of virtual currency exchanges and darknet markets and then withdrawing the funds, which obfuscates the trail of the transaction history by breaking up the fund flow; converting bitcoin to other forms of virtual currency, including anonymity-enhanced virtual currency (AEC), in a practice known as "chain hopping"; and using U.S.-based business accounts to legitimize their banking activity."[11]

Deputy Attorney General Lisa O. Monaco emphasized that the operation "[showed] that cryptocurrency is not a safe haven for criminals," and that "[thanks] to the meticulous work of law enforcement, the department once again showed how it can and will follow the money, no matter what form it takes." That point was echoed by Assistant Attorney General Kenneth A. Polite Jr. from the DOJ's Criminal Division who stated that "we will not allow cryptocurrency to be a safe haven for money laundering or a zone of lawlessness within our financial system."[12] Both of the accused individuals face various charges and could face more than 20 years in prison.

Action & Analysis

Included with H-ISAC Membership

Congress –

Tuesday, February 15th:

- No relevant hearings

Wednesday, February 16th:

- House of Representatives – Committee on House Administration: Big Data: Privacy Risks and Needed Reforms in the Public and Private Sectors

Thursday, February 17th:

- No relevant hearings

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.cyberscoop.com/sky-fraud-takedown-russia-cybercrime/

[2] https://www.securityweek.com/russian-law-enforcement-take-down-several-cybercrime-forums

[3] https://www.securityweek.com/russian-law-enforcement-take-down-several-cybercrime-forums

[4] https://www.cyberscoop.com/sky-fraud-takedown-russia-cybercrime/

[5] https://www.flashpoint-intel.com/press-post/russia-seizes-ferum-skyfraud-uas-trumpsdumps-carding-forums/

[6] https://krebsonsecurity.com/2022/02/russian-govt-continues-carding-shop-crackdown/comment-page-1/

[7] https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency

[8] https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency

[9] https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency

[10] https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency

[11] https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency

[12] https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency