Cybersecurity and Information Security Newsletter

Issue 11 | October 11, 2021

Table of Contents

October is **Cybersecurity Awareness Month**, and the Cybersecurity and Infrastructure Security Agency has partnered with the National Cybersecurity Alliance to host a number of cybersecurity-themed virtual events. Learn more here.

Please feel free to submit cybersecurity and information security news items or request related topics to Daniel Shin (dshin01@wm.edu).

U.S. Department of Justice charges individuals for violating federal export regulations relating to computer hacking

The U.S. Attorney's Office for the District of Columbia and the National Security Division of the U.S. Department of Justice (DOJ) announced that three individuals—Marc Baier, Ryan Adams, and Daniel Gericke—entered into a Deferred Prosecution Agreement with respect to alleged cybercrime activities and violations of other federal laws. The criminal complaint against the individuals alleges various federal criminal violations, including violation of the Arms Export Control Act (AECA), the International Traffic in Arms Regulations (ITAR), and fraud and related activity in connection with computers. In exchange for eventually dismissing the criminal charges, federal prosecutors announced that the individuals, who are cooperating with the ongoing federal investigations, have agreed to restrict their future activities as mandated by the terms of the Deferred Prosecution Agreement, and to pay $1,685,000 in total penalties.

This announcement highlights the legal risks associated with providing cybersecurity and cyber intrusion services to foreign nationals and entities.

Background

According to the criminal complaint (Complaint), Marc Baier, Ryan Adams, and Daniel Gericke (Defendants) allegedly planned and committed to transfer two computer exploits from a U.S. company (U.S. Company) to a company based in the United Arab Emirates (U.A.E. Company) and to certain U.A.E. government entities without having first obtained the required licenses and permissions as prescribed by federal law. *Criminal Complaint against Baier et. al.*, available here. An exploit "is a program, or piece of code, designed to find and take advantage of a security flaw or vulnerability in an application or computer system." *What Is an Exploit?*, available here.

None of the companies was identified in the Complaint, but it suggests that U.S. Company is engaged in cyber intrusion research while U.A.E. Company is a private company headquartered in the U.A.E.

U.S. Company held sensitive information and materials protected under a Technical Assistance Agreement (TAA) issued by the U.S. Department of State's Directorate of Defense Trade Controls. The TAA prevented U.S. Company from sharing TAA-restricted information and materials except with recipients authorized under the agreement.

The Defendants were former employees of U.S. Company who joined U.A.E. Company. According to the Complaint, the Defendants induced U.S. Company's employees to share TAA-restricted information with them, without the necessary preapproval from the Directorate of Defense Trade Controls. The Complaint alleges that the Defendants used the TAA-restricted information to produce sophisticated hacking technology for U.A.E. Company and the U.A.E. government.

Subsequently, the Defendants contacted another U.S. company to obtain various computer exploits for the benefit of U.A.E. Company. The Complaint notes that one of the exploits provided a "'zero-click' remote access to smartphones and mobile devices" using certain versions of a mobile operating system. *Complaint, supra,* at 5. The Defendants used this

exploit to create a remote computer exploitation system on behalf of U.A.E. Company's Cyber Intelligence-Operation (CIO) group.

The Defendants purchased other exploits from other companies around the world to facilitate computer network intrusion operations executed by the CIO group. The Defendants used "U.S. companies' software, services, and internet browsers" to carry out their activities.

The Complaint noted that the Defendants did not apply to the Directorate of Defense Trade Controls for a TAA to provide defense services to U.A.E. Company or the U.A.E. government "despite the fact that the conduct . . . constituted a defense service for which a license was required" under the ITAR and U.S. Munitions List Category XI(b) and (d).

Finally, the Complaint charges the Defendants with conspiracy to violate access device fraud laws, 18 U.S.C. § 1029(a)(2), and computer fraud and abuse laws, 18 U.S.C. § 1030(a)(2).

Legal Background

A Deferred Prosecution Agreement provides an alternative resolution for a prosecutor to adjudicate criminal charges. Instead of prosecuting defendants, a Deferred Prosecution Agreement allows a prosecutor to obtain cooperation from defendants to support an ongoing criminal investigation while promising not to move forward with the criminal charges for a period of time or at all.

The Deferred Prosecution Agreement for this case was mentioned as a "first-of-its-kind resolution" into criminal activities involving unlawful export of defense services and illegal computer hacking operations. *Three Former U.S. Intelligence Community and Military Personnel Agree to Pay More Than $1.68 Million to Resolve Criminal Charges Arising from Their Provision of Hacking-Related Services to a Foreign Government* (U.S. DOJ), available here. The terms of this agreement require the Defendants to cooperate with the ongoing criminal investigation; restrict certain future activities of the Defendants (including relinquishing any foreign and U.S. security clearances, a lifetime ban on U.S. security clearances, and certain future employment restrictions); and pay a cumulative penalty of $1,685,000.

The Arms Export Control Act and the International Traffic in Arms Regulations

The AECA, 22 U.S.C. § 2778, empowers the President of the United States to regulate the import and export of defense articles and defense services, namely items or services designated as being necessary for import and export regulation. The AECA aims to maintain U.S. national interests, including security and foreign policy, through import and export regulations.

The AECA requires any person or corporate entity, "who engages in the business of manufacturing, exporting, or importing any defense articles or defense services designed by the President" to register with the appropriate federal agency and obtain the necessary license for the engaged activity.

After the AECA was passed in 1976, President Ford signed Executive Order 11958 to implement the statute. In 2013, President Obama modified the U.S. export controls by signing Executive Order 13637, superseding Executive Order 11958. *Executive Order 11958--Administration of arms export controls* (The National Archives), available here.

The ITAR is a body of federal regulations that implements both the AECA and Executive Order 13637. It provides the specific rules for importing and exporting defense articles and services. The U.S. Department of State's Directorate of Defense Trade Controls is responsible for implementing the ITAR.

For the purpose of the ITAR, a TAA is a contract "for the performance of a defense service(s) or the disclosure of technical data." *22 CFR § 120.22*, available here. Before any U.S. person, as defined under 22 CFR § 120.15, provides defense services to foreign entities, that person must submit a proposed agreement to the Directorate of Defense Trade Controls for approval. *22 CFR § 124.1(a)*, available here. Once it is approved, the defense services can be lawfully provided to the designated foreign entities.

Analysis

Although the federal government regularly exercises its authority to regulate export controls of weapons and other defensive materials, its authority has not been often applied to cyber exploits and cyber attack services until now. DOJ's announcement signals an increasing interest in computer exploits and knowledge to carry out cyber attacks as part of U.S. export control enforcement.

At first sight, U.S. export regulations may appear to conflict with the First Amendment's freedom of speech, especially if computer exploit code is viewed as an expression of speech. *See, e.g., Bernstein v. U.S. Dept. of State,* 922 F.Supp. 1426 at 36, available here. ("For the purpose of First Amendment analysis . . . source code is speech."). If U.S. export regulations limit the publication or circulation of certain computer exploit codes to foreign individuals and entities, it is arguable that one's ability to exercise freedom of speech is constrained.

However, the federal court decision in *Karn v. U.S. Dept. of State*, 925 F.Supp. 1 (D.D.C. 1996), available here, held that U.S. export regulations, even those that seem to limit speech, do not violate the First Amendment. In *Karn*, Philip R. Karn attempted to export the book *Applied Cryptography* with a diskette containing some of the source code of the cryptographic software explained in the book. Although the Department of State allowed Karn to export the book, it designated the diskette as a defense article, limiting his ability to export it. Karn sued the Department, alleging that the export regulation was a content-based First Amendment speech regulation, and, if so, the Court should presume such regulation to be unconstitutional. The District Court rejected Karn's First Amendment arguments, noting that the Department's regulation is "clearly content-neutral." *Id.* at 10. It noted that the rationale for export regulations is to prevent "the proliferation of [cryptographic hardware and software that] will make it easier for foreign intelligence targets to deny the United States Government access to information vital to national security interests." *Id.* The Court expressly observed that the diskette was not regulated "because of [its] expressive content" but because of the government's belief that it would make it easier for foreign intelligence sources to protect their communications thus affecting U.S. national security interest. As such, the Court held that export regulations do not conflict with the First Amendment.

The implications arising from the DOJ's Deferred Prosecution Agreement announcement are substantial, especially for those working in the cybersecurity industry. Individuals engaged in cybersecurity research who share cyber assets abroad may be subject to export regulations if the Department of State has designated even part of those assets as defense articles.

Likewise, if cybersecurity professionals provide services to overseas clients, they should be aware that their business activities may be subject to export regulations if the Department has designated those services as defense services. U.S. export regulations aim to protect national security interests no matter the domain, so cybersecurity professionals need to remain vigilant.

Although U.S. export regulations may be an unfamiliar area for many cybersecurity professionals, these regulations are enforced under a strict liability standard, where knowledge of the violation is not required to assess penalties. *See U.S. Export Laws and Related Trade Sanctions*, available here. Consequently, professionals in this space should proceed cautiously in order to avoid inadvertently violating U.S. export regulations, especially when working in an international environment. This is timely a reminder that cybersecurity is a field with national security implications.

Treasury's Office of Foreign Assets Control publishes updated advisory on ransomware payments

On September 21, 2021, the Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury issued an updated advisory on sanction risks associated with ransomware payments. *Publication of Updated Ransomware Advisory; Cyber-related Designation*, available here. In conjunction with the updated advisory, OFAC also added Successful Exchange, a Russian-based cryptocurrency exchange and news portal, to its Specially Designated Nationals and Blocked Persons List (SDN), which prevents U.S. persons from transacting with the company. *Publication of Updated Ransomware Advisory; Cyber-related Designation*, *supra*.

OFAC is responsible for administering and enforcing economic and trade sanctions against foreign entities and nationals. The Office publishes sanctions lists that include individuals and organizations acting on behalf of targeted countries and non-country-specific groups (e.g., terrorists and narcotics traffickers). *Office of Foreign Assets Control - Sanctions Programs and Information*, available here.

The updated advisory warns companies "that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response," that they may risk violating economic and trade sanctions regulations if ransom payments are destined to recipients on OFAC's SDN. *Id.* In the past few years, OFAC has published specific digital currency addresses maintained by individuals and organizations on the SDN. *See, e.g., Cyber-related Designations; Foreign Interference in U.S. Election Designations*, available here. The updated advisory discourages paying ransoms to threat actors and highlights the sanctions risks associated with such actions.

For enforcement, OFAC imposes civil penalties based on strict liability, where individuals "may be held civilly liable even if [they] did not know or have reason to know that [they] were engaging in a transaction that was prohibited under sanctions laws and regulations . . . ." *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*, available here. Under the ransomware context, even if individuals *unknowingly* transmit

ransom payments to a sanctioned person, they are civilly liable for violating sanction regulations.

The Office encourages organizations to implement a risk-based compliance program that mitigates the risks of sanction-related violations. OFAC published *A Framework for OFAC Compliance Commitments* to help organizations set up their own compliance program, available here. Such a program assists organizations to consider sanction-violation risks when entertaining making ransom payments to threat actors.

The advisory recommends all ransomware victims and those tasked with addressing the ransomware attack report the cyber incident to the Cybersecurity Infrastructure Security Agency, the local Federal Bureau of Investigation field office, the Internet Crime Complaint Center IC3, or the local U.S. Secret Service field office, as soon as possible. It also recommends that victims report the ransomware incident and any ransom payments to the Department of Treasury's Office of Cybersecurity and Critical Infrastructure Protection.

If victims suspect a previous ransomware payment may be connected with sanctioned organizations or individuals, OFAC recommends they contact the Office immediately to potentially receive "significant mitigation from OFAC when determining an appropriate enforcement response," if the ransomware payment indeed involved sanctioned organizations or individuals.

Ransomware attacks are disruptive and stressful incidents, but hasty ransom payments may cause inadvertent sanction violations. Ransomware incident responders should carefully consider OFAC's advisory when advising victims to pay a ransom.