CLCT

WILLIAM & MARY LAW SCHOOL

Cybersecurity and Information Security Newsletter

Issue 8 | June 30, 2021

Table of Contents

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

U.S. Supreme Court limits the scope of criminal violation under the Computer Fraud and Abuse Act

On June 3, 2021, the U.S. Supreme Court clarified a major federal computer crime law by limiting the scope of cybercrime violation. The Court ruled that a former police officer, accused of retrieving information about a license plate number in exchange for money, did not violate the Computer Fraud and Abuse Act of 1986 (CFAA). Van Buren v. United States, 593 U.S. ____ (2021), available here. In Van Buren, the Court held that the CFAA only applies to computer users "who obtain information from particular areas in the computer—such as files, folders, or databases—to which their computer access does not extend." Id. at 1. By rejecting the government's motive-based CFAA interpretation, the Court narrowed the scope of the CFAA, which may undercut the government's ability to prosecute computer hacking incidents under certain circumstances.

Background

Nathan Van Buren was a former Georgia police sergeant who was caught taking bribes in exchange for providing information from a law enforcement sensitive database.

When Van Buren was under financial difficulties, he sought out a substantial loan from Andrew Albo, who allegedly had a history with prostitutes. *United States v. Van Buren*, 940 F.3d 1192 (11th Cir. 2019), available here. Based on his prior relationship with Albo, Van Buren thought Albo could provide him with a personal loan without issue. Unbeknownst to Van Buren, Albo recorded their conversations and turned over the audio recordings to a law enforcement detective, alleging that Van Buren was "shak[ing] him down for his money." *Id.* at 1997.

Albo's allegation drew the suspicion of the Federal Bureau of Investigations (FBI), so the federal agency created a sting operation to observe how far Van Buren would go to obtain the money. The sting operation entailed Albo giving Van Buren cash in exchange for checking whether a woman from a strip club was an undercover officer. Over the course of several meetings, Van Buren agreed to search the woman's license plate in the police database in exchange for $15,000. Unbeknownst to Van Buren, Albo provided a fake license plate number that was created by the FBI.

The day after he ran the fake license plate number using his patrol-car computer, Van Buren was interviewed by law enforcement authorities, and he subsequently admitted running the license plate number in exchange for money.

Van Buren's conduct violated a department policy against obtaining database information for non-law-enforcement purposes, and he was charged with a felony violation under the CFAA, which is a federal cybercrime statute that criminalizes intentional access to a computer system "without authorization or exceeding authorized access." 18 U.S.C. § 1030, available here. The statute defines the term "exceeds authorized access" as access to "a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6).

A jury convicted Van Buren of violating the CFAA. He subsequently appealed to the U.S. Court of Appeals for the Eleventh Circuit, arguing that the "exceeds authorized access" clause applies only to "accessers" who obtain information to which their computer access does not extend, *not* to those who misuse access that they have otherwise. Nevertheless, following its

precedent, the Eleventh Circuit held that Van Buren had violated the CFAA. Van Buren appealed the Eleventh Circuit's ruling to the U.S. Supreme Court, and the Court granted certiorari (agreed to review the case) on April 20, 2020. *Orders of the Court, Monday, April 20, 2020* at 3, available here.

The Supreme Court's Decision

The Supreme Court had to decide whether the scope of the CFAA's provision on "exceeding authorized access" covers what Van Buren is convicted of doing. It was not disputed that Van Buren accessed the Georgia Crime Information database (an official government database maintained by the Georgia Bureau of Investigations and connected to the National Crime Information Center, which is maintained by the FBI) using his patrol-car computer and obtained information in that computer. However, both parties disputed whether Van Buren was entitled to obtain information on the license plate number.

The government argued that the CFAA punishes individuals who "have improper *motives* for obtaining information that is otherwise available to them." *Van Buren*, at 1 (emphasis added). Van Buren argued that the CFAA's "is not entitled so to obtain" clause only refers "to information that a person is not entitled to obtain by using a computer that he is authorized to access." *Id.* at 8.

Writing for the majority, Justice Barrett agreed with Van Buren and held that the CFAA "does not cover those who, like Van Buren, have improper motives for obtaining information that is otherwise available to them." *Id.* at 1. Under the CFAA, the Court held that "an individual 'exceeds authorized access' when he accesses a computer with authorization but then obtains information located in particular areas of the computer . . . that are off limits to him." *Id.* at 20.

The Court noted that both parties agreed that (1) Van Buren accessed the law enforcement database system with authorization, and (2) Van Buren could use the system to retrieve license-plate information. Thus, the Court ruled that Van Buren did not exceed authorized access to the license-plate database, "as the CFAA defines that phrase, even though he obtained information from the database for an improper purpose." *Id.*

Analysis

To appreciate the effect of this case, imagine a library building, where physical entry is granted to those who present their library cards. The library has an internal rule that different types of library cards give differing library privileges, and library patrons are expected to follow that rule. Sam, a library cardholder, enters the library building legitimately by presenting his library card at the entrance. His library card privileges only allow him to view books in the non-fiction stacks, but there are no physical barriers preventing him from accessing other types of books. *Knowing* that it is against library rules, Sam nevertheless enters the fiction stacks and starts reading fiction books in the area.

Given that Sam entered the library with authorization and he freely moved inside the building to read fiction books, which he was not entitled to do, did Sam "exceed authorized access" as the CFAA defined that phrase? According to the Supreme Court, Sam did not.

It is important to note that the Court is simply interpreting a defined term within a federal statute, and textual analysis of the CFAA led the Court to its current conclusions. *Van Buren*'s

ruling may temporarily limit computer hacking prosecution under federal law, but Congress can always modify the statute's language to align with the government's position on "exceed authorized access" phrasing. It may be the case that state laws on computer hacking may be broad enough for prosecutors to continue pursuing computer hacking cases. *See, e.g.,* Va. Code Ann. § 18.2-152.4, available here.

More importantly, the Court's ruling calls for a more robust access control system across all Information Technology infrastructure. The Court's ruling makes it clear that individuals violate the CFAA if the individual accesses computer resources that are not available to them. In plain terms, this means that any attempts to overcome access control systems would still violate the federal anti-computer hacking law.

If Van Buren had hacked his way to access the license plate database, the Supreme Court would have likely considered his act in violation of the CFAA. Poor access control systems allowed Van Buren to access a law enforcement sensitive database without restriction. A more secure access control system would have required law enforcement officers to obtain temporary access permission from their supervisor *each time* before being able to access sensitive databases. It is likely that state and federal government IT systems will implement a more stringent access control systems to set clear access privileges across their employee base.

President Biden signs Executive Order to increase information sharing

On May 12, 2021, President Biden signed Executive Order 14028 (Executive Order) that aims to improve the federal government's cybersecurity systems. *Executive Order 14028*, available here. Recognizing the persistent and increasingly sophisticated malicious cyber attacks that threaten the public sector, the Executive Order seeks to implement significant resources to meet and exceed cybersecurity standards for federal computer systems.

The Executive Order requires the Director of the Office of Management and Budget (OMB), in consultation with other specified cabinet members, to review Federal Government contracts with Information Technology (IT) and Operational Technology (OT) service providers to identify contractual barriers that hamper sharing of threat information between service providers and the federal government. By promoting the sharing of information about threats, incidents, and risks, the Executive Order seeks to improve federal IT and OT systems by focusing on incident deterrence, prevention, and response efforts against cybersecurity threats.

Modernizing Federal Government Cybersecurity

The Executive Order recognizes the importance of Cloud technology and its implications for future cyber incidents and notes that "[a]s agencies continue to use Cloud technology, they shall do so in a coordinated, deliberate way that allows the Federal Government to prevent, detect, assess, and remediate cyber incidents."

Cloud technology refers to highly scalable, on-demand computing services (e.g., data storage, network access, and computer processing) that can be made available without direct active

management. Although Cloud technology offers lower management costs with flexible resource provisioning, there is a risk for the Cloud users (i.e., organizations using the Cloud infrastructure) of being exposed to new types of cyber incidents relating to the Cloud infrastructure.

Recognizing the need to use Cloud technology while protecting federal IT and OT assets, the Executive Order directs federal agencies to adopt the **Zero Trust Architecture** as practically possible. According to the National Institute of Standards and Technology (NIST), Zero Trust Architecture refers to a system architecture where all users are treated as potential threats and prevented from access to data and resources until they can be properly authenticated and their access authorized. *Zero Trust Architecture*, available here. Although the adoption of Zero Trust Architecture can yield stronger security environments for IT and OT systems, there is generally an increase in management and transaction costs for all users. *See Explained: the strengths and weaknesses of the Zero Trust model*, available here.

The Executive Order also requires federal agencies to "adopt multi-factor authentication and encryption for data at rest and in transit," within 180 days of the date of the Order. Multi-factor authentication refers to a security enhancement that allows users to present multiple pieces of evidence when accessing an account. *Back to basics: Multi-factor authentication (MFA)*, available here. Within a multi-factor authentication environment, users are expected to provide more than a username and password (e.g., temporary security code generated from the user's phone or smart card) before being granted access to IT resources.

Finally, the Order establishes a Cyber Safety Review Board, which will review actions related to the Federal Government cybersecurity incidents and related supply chain compromise activity. Led by the Secretary of Homeland Security, the Board will include representatives of the Department of Defense, the Department of Justice, the Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security, the National Security Agency, the Federal Bureau of Investigations, and representatives from private-sector cybersecurity or software suppliers as determined by the Secretary of Homeland Security. The Board will also provide the Secretary of Homeland Security with recommendations for improving cybersecurity and incident response practice.

Coordination through CISA

Under the Executive Order, CISA is directed to modernize its cybersecurity programs, services, and capabilities to be fully functional with Cloud-computing environments with Zero Trust Architecture. Furthermore, the Secretary of Homeland Security (acting through the Director of CISA), in consultation with the Administrator of General Services (acting through the Federal Risk and Authorization Management Program), will develop security principles governing Cloud Service Providers to facilitate cybersecurity modernization efforts.

The Executive Order also calls for a review on the current Federal Acquisition Regulation (FAR)—the primary regulations for use by federal agencies in their acquisition of supplies and services with appropriated funds—and the Defense Federal Acquisition Regulation Supplement (DFARS)—the rules managing the investments of the federal government in technologies, programs, and product support necessary to support national security and the U.S. Armed Forces. Through this review, the federal government seeks to require IT and OT service providers to promptly report any cyber incidents that may impact federal agencies.

The Executive Order assigns CISA as the central hub for collecting managing cyber incident information from IT and OT service providers.

Analysis

President Biden's Executive Order was signed five months after the discovery of the SolarWinds hack, where threat actors initiated a supply chain hack to infiltrate and monitor key federal computer systems. Although the supply chain hack was discovered months after the threat actors initiated its cyber attack, SolarWinds' prompt disclosure after incident discovery allowed CISA to quickly issue an Emergency Directive to mitigate the cyber attack on federal computer systems. *See Emergency Directive 21-01*, available here.

As federal computer systems continue to migrate to the Cloud, the federal government needs to manage new cyber threats stemming from the transition. To manage these threats effectively, the Executive Order recognizes the need for prompt cyber incident reporting among federally contracted IT and OT service providers. By giving CISA a larger role in collecting cyber threat information, the Order enhances CISA's ability to provide a coordinated response against cyber attacks.

Although the Executive Order furnishes multiple timelines for cabinet officials to conduct reviews relating to cyber systems, it is notable that this Order also sets out certain mandatory cybersecurity standards across federal computer systems. By explicitly mentioning the implementation of Zero Trust Architecture, multi-factor authentication, and encryption (on data at rest and in transit), it demonstrates the current administration's commitment to proactively harden systems without delay. Consequentially, this is arguably one of the most technically advanced executive orders to date concerning cybersecurity.

The Ransomware Task Force issues a comprehensive strategic framework against ransomware

The Institute for Security and Technology, a nonpartisan, nonprofit think tank, published the *RTF Report: Combatting Ransomware, A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force* (The RTF Report), which presents a framework for combating ransomware across all industries. *RTF Report: Combatting Ransomware*, available here.

The RTF Report was prepared by the Ransomware Task Force, which is composed of a broad coalition of volunteer experts from industry, government, law enforcement, civil society, cybersecurity insurers, and international organizations. Its publication comes as the U.S. Department of Justice internally announced the formation of a task force to investigate the threat of ransomware. *Ransomware Targeted by New Justice Department Task Force*, available here.

The RTF Report outlines a framework of actions that government and industry leaders can pursue to disrupt ransomware-based criminal enterprise and mitigate the collateral damage arising out of ransomware attacks. The Report aims to accomplish the following goals through the framework of actions:

- Deter ransomware attacks through a nationally and internationally coordinated, comprehensive strategy;
- Disrupt the ransomware business model and decrease criminal profits;
- Help organizations prepare for ransomware attacks; and
- Respond to ransomware attacks more effectively.

To accomplish these goals, the Report includes 48 recommendations, of which five priority ones are listed below:

1. Coordinated, international diplomatic and law enforcement efforts must proactively prioritize ransomware through a comprehensive, resourced strategy, including using a carrot-and-stick approach to direct nation-states away from providing safe havens to ransomware criminals;
2. The United States should lead by example and execute a sustained, aggressive, whole of government, intelligence-driven anti-ransomware campaign, coordinated by the White House;
3. Governments should establish Cyber Response and Recovery Funds to support ransomware response and other cybersecurity activities; mandate that organizations report ransom payments; and require organizations to consider alternatives before making payments;
4. An internationally coordinated effort should develop a clear, accessible, and broadly adopted framework to help organizations prepare for, and respond to, ransomware attacks; and
5. The cryptocurrency sector that enables ransomware crime should be more closely regulated.

Overall, the RTF Report advocates a coordinated international effort to weaken the infrastructure supporting the ransomware enterprise.

Analysis

The RTF Report was published mere weeks before the Colonial Pipeline Ransomware Attack, which forced the gasoline pipeline company to shut parts of its operation down. *Colonial Pipeline Cyberattack: Timeline and Ransomware Attack Recovery Details*, available here. To attempt to resolve the situation, Colonial Pipeline reportedly paid nearly $5 million in ransom to get the decrypting tool to restore its systems, although "[t]he tool was so slow that the company continued using its own backups to help restore the system." *Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom*, available here.

The Federal Bureau of Investigations does not support paying a ransom in response to a ransomware attack. *Ransomware*, available here. Even though the Colonial Pipeline appeared to have the requisite backups to restore its operation without the decryption tool, the company nevertheless made the decision to pay a sizeable ransom to the cyber attackers because of the impact of shutting down a critical energy infrastructure to the rest of the

country. *Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom*, available here.

The RTF Report recognizes that the "majority of organizations lack an appropriate level of preparedness to defend against these attacks," including those who may have invested in cybersecurity broadly. As this Report mentions, there needs to be a stronger awareness of the ransomware threat among governments and industry leaders.

Fortunately, there are already publicly available resources published by the Cybersecurity and Infrastructure Security Administration on the topic of ransomware. *Ransomware Guidance and Resources*, available here. There are opportunities for governments to deter ransomware attacks and disrupt the ransomware business model. However, private organizations need to be independently vigilant against the ransomware threat by developing a clear, actionable plan for ransomware mitigation, response, and recovery.

It is not enough to shift the risk of ransomware to a cyber insurance plan because the underlying problem will continue to persist. *See Cyber insurance market reacts to ransomware epidemic*, available here. Instead, organizations need to recognize their role in disrupting the ransomware enterprise. By practicing good cyber hygiene and not paying ransoms to cyber criminals, the ransomware enterprise can slowly be dismantled by the private sector.