UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 1:21-CR-224-LY
	)	
MARK SOKOLOVSKY,	)	***EX PARTE* & UNDER SEAL**
	)	
Defendant	)	

GOVERNMENT'S MOTION FOR ALTERNATIVE VICTIM NOTIFICATION PROCEDURES

The United States respectfully moves this Court *ex parte*, pursuant to 18 U.S.C. § 3771(d)(2), for authorization to employ the victim notification procedures described below, in lieu of those prescribed by §§ 3771(a), (b) and (c), on the grounds that the number of potential victims in this case makes it impracticable to accord all of the crime victims the rights described in subsection 3771(a).

Introduction

On November 21, 2021, the defendant was charged in a sealed Indictment with: (1) conspiracy to violate the Computer Fraud and Abuse Act, in violation of 18 U.S.C. §§ 371 and 1030; (2) conspiracy to commit wire fraud, in violation of 18 U.S.C. § 1349; (3) money laundering conspiracy, in violation of 18 U.S.C. § 1956(h); and (4) aggravated identity theft, in violation of 18 U.S.C. § 1028A. The charges stem from the defendant's role in the operation of the Raccoon Infostealer malware, which has been used to steal sensitive records, including log-in credentials, financial information, and other personal records. The malware infected millions of computers around the world.

Raccoon Infostealer was a malware-as-a-service, or "MaaS." Individuals who deployed Raccoon Infostealer to steal data from victims leased access to the malware for approximately $200 (USD per month. These individuals then used various ruses, such as email phishing, to install the malware onto unsuspecting victim computers. Raccoon Infostealer then obtained stolen personal data, which could then be used to commit further financial crimes or be sold to others to commit crimes. Raccoon Infostealer and the stolen data were often sold on cybercrime forums.

The defendant is a native and citizen of Ukraine. On March 4, 2022, the defendant (together with other individuals) left Ukraine in what appeared to be a Porsche Cayenne, transited Poland and Germany, and eventually arrived in the Netherlands. Dutch law enforcement arrested Sokolovsky on March 20, 2022, pursuant to a Provisional Arrest Warrant requested by the United States.

The United States later submitted a formal extradition request and the defendant's Dutch extradition hearing was held on August 31, 2022. The Amsterdam District Court issued its decision on September 13, 2022 and granted the defendant's extradition. The defendant remains in custody in the Netherlands pending any further legal action in the Netherlands related to his extradition.

Concurrent with the defendant's arrest, Italian and Dutch authorities took legal action to seize Raccoon Infostealer's key digital infrastructure, resulting in the malware ceasing to function.

Shortly after the defendant was arrested in the Netherlands and the Raccoon Infostealer digital infrastructure was dismantled, certain online accounts related to selling Raccoon Infostealer posted a statement online: "Dear Clients, unfortunately, due to the 'special operation',

we will have to close our project Raccoon Stealer. The members of our team who are responsible for critical moments in the operation of the product are no longer with us." Reporting on this post in the cyber security media interpreted this post to say a significant Raccoon Infostealer developer was killed in the conflict in Ukraine.[1]

While there are numerous articles describing Raccoon Infostealer available to the public, the United States is not aware of substantial media coverage of the defendant's arrest or his alleged connection to Raccoon Infostealer. As of the date of this Motion, the indictment remains under seal. Potential victims of the Raccoon Infostealer scheme are likely not aware of the defendant's arrest, the pending indictment, or methods to vindicate their rights.

Furthermore, through various investigative steps, the United States has collected data stolen from many computers that were infected with Raccoon Infostealer. While an exact number has yet to be verified, agents from the Federal Bureau of Investigation have identified more than 50 million unique credentials (email addresses, bank accounts, cryptocurrency addresses, credit card numbers, etc.) in the stolen data from what appears to be millions of potential victims around the world. The credentials appear to include over four million email addresses. Based on its review of the data, the government believes it is not in possession of all of the data stolen by Raccoon Infostealer. However, the government continues to investigate and anticipates receiving additional potential victim data as the investigation continues.

The data in the government's possession is often a compilation of email addresses, passwords, bank account and cryptocurrency information, and other personally identifying information stored in massive databases. Sometimes the data contains no email address and only

[1] *See, e.g.*, https://www.bleepingcomputer.com/news/security/raccoon-stealer-malware-suspends-operations-due-to-war-in-ukraine/.

financial or other credentials. The data is not necessarily tied to particular names or physical addresses, and it is difficult to ascertain based on the data alone whether the stolen data has been used to defraud individual potential victims. As a result, identification, let alone notification, of potential victims is both impractical and, if required, would "unduly complicate or prolong the proceedings." 18 U.S.C. § 3771(d)(2).

Statutory Victim Notification Requirements

On October 30, 2004, the President signed into law the Crimes Victims' Rights Act of 2004. Title I of the Act enumerates rights of crime victims in federal criminal cases, codified at 18 U.S.C. § 3771(a). The Act requires "[o]fficers and employees of the Department of Justice and other departments and agencies of the United States engaged in the detection, investigation and prosecution of crime [to] make their best efforts to see that crime victims are notified of, and accorded, the rights described in subsection [3771](a)," 18 U.S.C. § 3771(c)(1), and it instructs the Court to "ensure that the crime victim is afforded" those rights. 18 U.S.C. § 3771(b). A "crime victim" under the Act is defined as "a person directly and proximately harmed" as a result of the commission of a Federal offense. 18 U.S.C. § 3771(e).[2]

In routine cases involving a single or limited number of victims, the victim notification burdens imposed by the Act upon the government are significant. In other cases, involving tens, hundreds, or even thousands of potential victims, the burdens imposed by the Act would be overwhelming; it is simply not practicable for the government to identify and locate so many potential victims and provide each with reasonable, accurate, and timely notice of all court proceedings. In recognition of this, the Act grants the Court authority to fashion alternative

[2] 18 U.S.C. § 3771(d)(1) further provides that "a person accused of the crime may not obtain any form of relief under" Section 3771.

notification procedures when the Court finds that implementation of the prescribed requirements would be impracticable. The Act provides:

> In a case where the court finds that the number of crime victims makes it impracticable to accord all of the crime victims the rights described in subsection [3771](a), the court shall fashion a reasonable procedure to give effect to this chapter that does not unduly complicate or prolong the proceedings.

18 U.S.C. § 3771(d)(2). The Act places no limitations on the alternative procedures which a Court may fashion other than that the procedures be reasonable to effectuate the Act and that they not unduly complicate or prolong the proceedings. *Id*.

In this case, the defendant is charged with numerous federal crimes related to Raccoon Infostealer that was used to steal millions of personal and financial records. The potential victims in this case—individuals whose personally identifying information and financial information was stolen through the use of Raccoon Infostealer—may number in the millions and ascertaining the true identities of those potential victims by analyzing the tranches of stolen data in the United States' possession is an impossible task. The number of potential victims and the imperfect identifying information in the stolen data make strict compliance with the notification requirements outlined in Section 3771(a), (b) and (c) impracticable and would unduly complicate and delay the proceedings.

Government's Proposed Alternative Notification Procedures

Consistent with the Court's discretion to fashion reasonable alternative victim notification procedures under Section 3771(d)(2), the government requests authorization from the Court to implement the following procedure designed to help identify potential victims and provide them with reasonable notification of their rights. Subject to planning contingencies, the government intends to implement this process in October or as soon as practical after.

First, the government has created a website where any member of the public can input his or her email address to check if that email address is contained within the Raccoon Infostealer stolen data in the government's possession. The website will be hosted at a secure ".gov" web address. If the email address is within the data, the government will then send an email to that address notifying the user. This process has been designed to limit the ability of malicious actors to abuse the website (for example, by using it to generate spam emails) and to limit confirmation to individuals with access to the pertinent email address. Additionally, by limiting this process to email accounts, the government limits the potential disclosure of PII only to those preexisting access to the PII (the email address). Allowing the public to check other credentials, such as financial accounts, would expose that information malicious actors and would be insecure.

The notification email will direct the potential victim to a specific webpage at the FBI's Internet Crime Complaint Center where the potential victim can fill out a detailed complaint and share any financial or other harm experienced as a result of their information being stolen. The potential victim will also be directed to general information about the case (including the indictment and case status updates) as well as resources like www.identitytheft.gov for information on how to better protect their identity and online accounts.

Second, the government will issue a press release and may hold a press conference describing the Raccoon Infostealer and outlining the potential victim notification process described above. The government will publicize the website during any potential press conference and in a press release.

Finally, as permitted by financial and privacy rules and regulations, the government will explore options to notify the relevant companies who host or maintain accounts for various credentials found in the data. For example, the government will explore notifying particular

financial institutions or electronic communications service providers with lists of accounts found in the stolen data, informing them that the credentials are potentially compromised. The government, however, cannot control whether and in what form such institutions go on to notify their users of potential compromises. Because the email addresses queried through the website described above are a subset of overall set of potential victim credentials, the government has a need to use provider notifications to reach a broader set of potential victims.

Undertaking victim notification via this process will provide potential victims with information that will help them identify themselves to the government. Second, some potential victims may have the right to restitution in the criminal proceedings, as well as the right to related civil remedies, which rights may be furthered by the dissemination of this information. Finally, providing this information will assist potential victims in meaningfully exercising their rights under the CVRA. *See e.g., United States v. BP Products N. Am. Inc.,* Crim. H-07-434, 2008 WL 501321 (S.D. Tex. Feb. 21, 2008) (holding that "the purposes of the conferral provision [of the CVRA] are to ensure that victims can obtain information from prosecutors and convey information to prosecutors, to enable the victims to form and express opinions."); *see also In re Brock*, 262 F. App'x 510, 512 (4th Cir. 2008) (finding that the government provided the victim with "ample information" to enable him to "meaningfully exercise his right to be reasonably heard" at the defendant's sentencing).

The government files this motion under seal and *ex parte* because the defendant has not yet made his appearance in the Western District of Texas and has ongoing extradition proceedings in the Netherlands. However, to enhance its outreach to potential victims, the government intends to file a motion to unseal this motion and order, as well as unseal the

indictment and related documents prior to the planned press release and any press conference described above.

Conclusion

The number of potential victims in this case renders individual notification to each, as prescribed by 18 U.S.C. § 3771(a), (b), and (c), impracticable, as does the method of identification of each potential victim. In such cases, the Act authorizes this Court to fashion a reasonable, alternative notification procedure to effectuate the aims of the Act without unduly complicating or prolonging the proceedings. The government's proposed notification procedures accomplish these goals. For the reasons set forth above, the government respectfully requests that this Court grant this *ex parte* motion and issue the accompanying proposed Order.

Date: _____, 2022

Respectfully submitted,

ASHLEY C. HOFF
United States Attorney

By: /s/ Michael Galdo
Michael C. Galdo
G. Karthik Srinivasan
Assistant U.S. Attorneys