UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

UNITED STATES OF AMERICA,	§	
	§	
v.	§	
	§	
MARK SOKOLOVSKY	§	**CRIMINAL NO. 21-CR-224-RP**
a.k.a. Photix, Raccoonstealer,	§	
B1ack21jack77777,	§	
	§	
Defendant.	§	

GOVERNMENT'S SENTENCING MEMORANDUM

The government respectfully submits this memorandum regarding the sentencing of Defendant Mark Sokolovsky. Defendant has pled guilty pursuant to a plea agreement to one count of conspiring to violate the Computer Fraud and Abuse Act. Per the plea agreement, the parties agreed to recommend that the Court impose a sentence of 60 months' imprisonment (with credit for time served in Dutch and U.S. custody), a fine of $250,000, forfeiture in the amount and methods described in the plea agreement, with restitution and supervised release as determined by the Court at sentencing. The government requests that the Court adopt the parties' recommendation because a 60-month sentence with attendant financial penalties comports with the requirements of 18 U.S.C. § 3553(a).

I. Background

Defendant was indicted on November 2, 2021 and charged with conspiracy to commit fraud and related activity in connection with computers, in violation of 18 U.S.C. § 371, conspiracy to commit wire fraud, in violation of 18 U.S.C. § 1349, conspiracy to commit money laundering, in violation of 18 U.S.C. § 1956(h), and aggravated identity theft, in violation of 18 U.S.C.

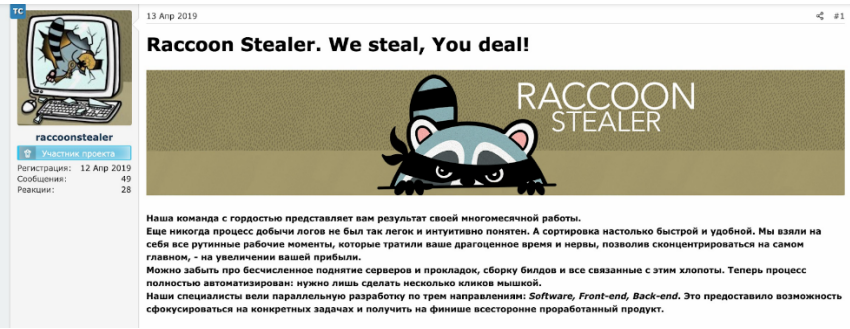
§ 1028A. He pled guilty to Count One of the Indictment (conspiracy to commit computer intrusion), which carries a five-year maximum penalty.

Defendant—a citizen of Ukraine—fled his country shortly after Russia's invasion in February 2022. He crossed the border into Poland and made his way to the Netherlands. He was arrested in March 2022 in the Netherlands pursuant to a provisional arrest warrant and has been in United States custody since February 8, 2024. He was in Dutch custody from March 20, 2022 until February 8, 2024.

Before his arrest, he was one of the key administrators of the Raccoon Infostealer, a pernicious malware-as-a-service that was used to steal millions of online credentials from unsuspecting victims. Infostealers specialize in surreptitiously stealing a host of information from victim computers, including financial information, passwords, credentials, cryptocurrency wallets, and other personal information. The stolen information is exfiltrated from the victim computers to servers controlled by cybercriminals. Raccoon Infostealer was sold as a monthly service and any purchasing cybercriminal could deploy it using techniques such as malicious websites or phishing. The cybercriminal received a copy of the stolen information and so did the administrators and developers of Raccoon Infostealer. The information (known as "logs") was often packaged and sold on cybercriminal forums for use in additional frauds or computer intrusions.

The version of Raccoon Infostealer that Defendant administered was one of the most prominent of its generation of infostealers. One early cybersecurity research analysis of the malware noted it was one of the top-10 most discussed malware strains in the criminal underground in 2019. "Hunting Raccoon: The New Masked Bandit on the Block," Cybereason, *available at https://www.cybereason.com/blog/research/hunting-raccoon-stealer-the-new-masked-bandit-on-*

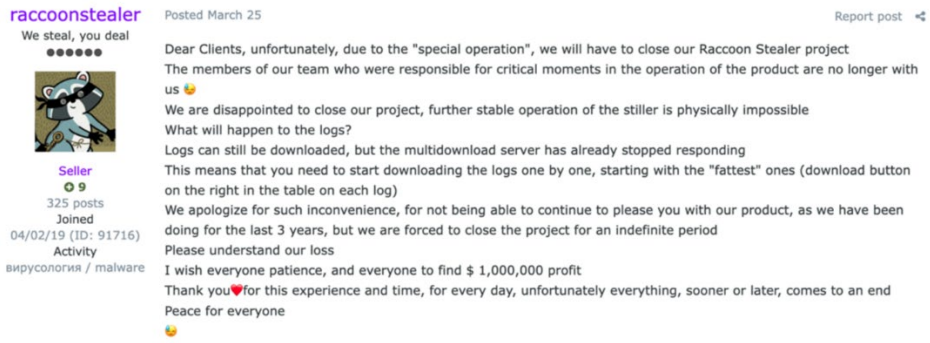
the-block. Raccoon Infostealer was in the vanguard of commoditized malware that made it simpler and simpler for even amateur cybercriminals to attack victims. From the start, the malware was cheap, easy to use, and the co-conspirators behind it were "lauded in the underground community for their level of service, support, and user experience . . . ." *Id*. One of the early advertisements for Raccoon Infostealer summed up its appeal and motto: "Raccoon Stealer. We steal, You deal!"



Raccoon Infostealer was user friendly and flexible enough to adapt as criminals needed new features and evolved ways to infect victim computers. For example, during the COVID-19 pandemic, criminals used fake Department of Health and Human Services websites to trick unsuspecting computer users into downloading Raccoon Infostealer. In 2020, other criminals used fake sextortion scams to lure victims into installing Raccoon Infostealer. "Malware Spread as Nude Extortion Pics of Friend's Girlfriend," Bleeping Computer (Mar. 9, 2020) (*available at https://www.bleepingcomputer.com/news/security/malware-spread-as-nude-extortion-pics-of-friends-girlfriend/*). Over the years, new features expanded Raccoon Infostealer's impact on victims. Sometime in 2021, Raccoon Infostealer gained a "clipper" function that targeted cryptocurrency wallets stored on victims' computers. These functions were advertised using release notes that mimicked the update release notes that accompany legitimate software. The conspirators behind Raccoon Infostealer were thus aware of their criminal customers' needs and released updates to facilitate further crimes. *See, e.g.*, "Trash Panda as a Service: Raccoon Stealer Steals Cookies, Cryptocoins, and More," Sophos Labs (Aug. 3, 2021) (*available at*

https://news.sophos.com/en-us/2021/08/03/trash-panda-as-a-service-raccoon-stealer-steals-cookies-cryptocoins-and-more/). Whether Defendant was aware of every scam methodology was immaterial. He and other co-conspirators created, managed, and updated malware for the purpose of crime and, in this criminal ecosystem, the actions of Raccoon Infostealer customers were reasonably foreseeable.

In conjunction with Defendant's arrest on March 20, 2022, the government coordinated an international disruption campaign with Italian and Dutch authorities that took down the then-existing infrastructure for Raccoon Infostealer. Within days, Defendant's co-conspirators implied publicly that Defendant had been killed during Russia's recent invasion of Ukraine:



Notably, without Defendant, "further stable operation of the stiller [sic] is physically impossible." With Defendant's supposed death or incapacitation in war, one of the services (the "multidownload server") that sped up the theft and packaging of victim information went down with Defendant's arrest, a significant inconvenience for the cybercriminals. *See* "The Cybercriminal Who Rose from the Dead," BlackBerry Blog (Jan. 5, 2023) (*available at https://blogs.blackberry.com/en/2023/01/cybercriminal-faked-death-found*). In reality, Defendant was in custody. A few months later, a second malware claiming the title Raccoon V2 launched in underground forums. But the first version of Raccoon Infostealer—Defendant's version—was stopped.

The amount of data stolen by Defendant's version of Raccoon Infostealer was breathtaking. Over two million victims from countries around the world were affected. And law enforcement cannot calculate the full number of victims due to the nature of the malware and underground economy in infostealer logs. In one of Defendant's online storage accounts, agents found millions of victim credentials. Very few victims, if any, knew they had been infected because the malware was programmed to hide its tracks. The victims' logins and passwords were bartered in the underground economy, enabling more fraudsters to steal from and defraud innocent people. Financial institutions lost at least hundreds of thousands of dollars because their customers' data was stolen. In this case, just one victim company has made a claim for over $900,000 in losses directly attributable to Raccoon Infostealer. The true magnitude of losses will never be known as the brisk online trade in stolen credentials makes direct attribution to Raccoon Infostealer more difficult over time.

Defendant played a crucial role in the scheme. As noted above, Defendant's arrest and law enforcement action disrupted his version of Raccoon Infostealer in March 2022. That Raccoon Infostealer could not function without Defendant is proof of his importance to the scheme. He administered the servers supporting Raccoon Infostealer's infrastructure and actively worked with his co-conspirators to improve the quality and responsiveness of the infrastructure for criminal actors. Searches of his electronic accounts revealed evidence of his logging into the Raccoon Infostealer infrastructure, instructions for maintaining the infrastructure, and stolen credentials. He kept Raccoon Infostealer running and the malware-as-a-service conspiracy failed upon his arrest.

II. A Sixty-Month Sentence is the Appropriate Prison Term

The parties' recommendation of a 60-month sentence with attendant financial penalties meets the goals of 18 U.S.C. § 3553(a) by reflecting the nature and circumstances of the offense and deterring criminal conduct. Several of the other offenses originally charged carried significantly more serious statutory maximum or minimum penalties—including a two-year mandatory minimum sentence under 18 U.S.C. § 1028A. Given Defendant's potential exposure under the applicable Guidelines range of 210-262 months (PSR ¶ 58) had he been convicted of those offenses, he has already received a substantial benefit and no further leniency is warranted.

As set forth above, Defendant was a central player in a criminal scheme that stole valuable personal information from a staggering number of victims. The conspiracy failed without him. The true downstream impacts of his crimes will likely never be known because the information stolen can be repackaged and sold numerous times. The information cannot be scrubbed from the Internet. Defendant and his co-conspirators enabled cybercrime at industrial scale. He gave amateur hackers and fraudsters with minimal training, technical know-how, and investment a potent weapon to aim at victims. Others did not misuse a tool he and his co-conspirators made. The tagline for Raccoon Infostealer was "We Steal, You Deal." Raccoon Infostealer was used as Defendant and his co-conspirators intended. He knew what he was doing and what others would do with the malware he administered. The nature and circumstances of the offense require a significant term in prison and financial consequences.

In this case, the Court can help set a standard to deter crimes by international cybercriminals. Raccoon Infostealer was an early generation infostealer and that market has only grown since. As the threat intelligence firm SpyCloud estimated earlier this year, perhaps 61% of all data breaches in the past year were malware-related, with infostealers responsible for the theft

of hundreds of millions of credentials. "2024 Malware and Ransomware Defense Report," SpyCloud Labs (Sep. 18, 2024) (*available at https://spycloud.com/newsroom/spycloud-unveils-massive-scale-of-identity-exposure-due-to-infostealers/*). Because users store so much information on computers, each infection can lead to the theft of dozens of credentials for various websites and services. *Id*. Infostealer infections are often precursors to ransomware and other attacks. *Id*. The downstream identity theft can inflict serious financial and psychological harm on victims. The developers of these malware variants are often in foreign countries, some of which are difficult venues for investigation and prosecution. The investigation and prosecution of these cases is time intensive and often depends on good luck in the form of the cybercriminal making a mistake in his or her operational security. Victim notifications can be a practical impossibility. In this case, the Court permitted the government to use various alternative victim notification methods, including an innovative website. Even so, most victims do not know they were affected because the malware deleted itself. Infostealers are thus an important and difficult challenge for law enforcement and the cybersecurity community. This case is a prime opportunity for the justice system to send the message that developing, marketing, and selling malware that enables and executes cybercrime at enormous scale will not be tolerated. A 60-month sentence will send that message.

III. Conclusion

For these reasons, the Court should impose a sentence of 60 months' imprisonment (with credit for time served in Dutch and U.S. custody), a fine of $250,000, forfeiture in the amount and

methods described in the plea agreement, with restitution and supervised release as determined by the Court.

Respectfully submitted,

JAIME ESPARZA
United States Attorney

By: */s/ G. Karthik Srinivasan*
G. KARTHIK SRINIVASAN
Assistant United States Attorney

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing Government's Sentencing Memorandum has been delivered via the CM/ECF automatic notification on this the 16th day of December 2024 to defense counsel.

/s/ G. Karthik Srinivasan
G. KARTHIK SRINIVASAN
Assistant United States Attorney