SEALED

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

UNITED STATES OF AMERICA	§	**INDICTMENT**
	§	
	§	[COUNT 1: 18 U.S.C. § 371, Conspiracy to
v.	§	Commit Fraud and Related Activity in
	§	Connection with Computers;
	§	COUNT 2: 18 U.S.C. § 1349, Conspiracy to
MARK SOKOLOVSKY, aka Photix,	§	Commit Wire Fraud;
raccoonstealer, and b1ack21jack77777	§	COUNT 3: 18 U.S.C. § 1956(h),
	§	Conspiracy to Commit Money Laundering;
Defendant.	§	COUNT 4: 18 U.S.C. § 1028A, Aggravated
	§	Identity Theft.]
	§	
	§	A21CR224LY

THE GRAND JURY CHARGES:

At All Times Material To This Indictment:

INTRODUCTION AND OVERVIEW

1. Conspirators residing in Ukraine and elsewhere operated a computer malware known as Raccoon. The conspirators offered the malware as a service to users as a means to harvest personal information, financial information, and passwords from victims without the knowledge of the owners of the victims' computers.

2. Millions of computers around the world have been infected with the Raccoon malware and more than 2 million victims have had their personal information, financial information, and passwords stolen by Raccoon.

BACKGROUND AND DEFINITIONS

3. "Malware" was a term for a malicious software program designed to disrupt computer operations, gather sensitive information, gain access to private computer systems, and

perform other unauthorized actions on computer systems. Common examples of malware included viruses, ransomware, worms, keyloggers, and spyware.

4. "Infostealers" were part of a family of malware generally known as remote access trojans, or "RATs." Infostealers or RATs function primarily through gaining administrative access to a computer without the users' permission, whereafter they perform various illicit functions on an infected device.

5. "Raccoon" was a form of infostealer with functions that included, but were not limited to, the theft of financial information (including cryptocurrency data) as well as saved username and password combinations for websites and other services, capturing screenshots of user activity, and creating or deleting files on a computer. Raccoon was designed to perform these and other functions without alerting the users and/or owners of the infected computer to avoid detection. The information was then sent to one or more servers controlled by the co-conspirators who controlled Raccoon. After Raccoon finished stealing the information, it would then delete itself from the infected computer.

6. Raccoon was a malware-as-a-service, or "MaaS." Like software-as-a-service, or SaaS, MaaS was operated on a lease basis, where customers paid approximately $200 (USD) on a monthly basis to gain access to Raccoon—paying via cryptocurrency like Bitcoin—which allowed them to access and deploy Raccoon, then obtain a copy of the data stolen from their victims. Raccoon was sold on cybercrime forums such as Exploit[.]in. The conspiracy interacted with its criminal customers, providing them with customer service and information about updates to the Raccoon software and functionalities.

7. "Phishing" was a process where specially-crafted emails were distributed to recipients with a purpose of collecting the recipients' credentials and delivering malware.

8. "Crypting" and "crypting services" was a means of facilitating cybercrime by rendering malicious software undetectable by major provider of antivirus software. The services could be used for many types of malware, including infostealers, to disguise the malware via encryption, enabling it to be successfully delivered via email phishing onto victim computers.

9. "Bitcoin" was a type of virtual currency, circulated over the Internet as a form of value. Bitcoin were not issued by any government, bank, or company, but were generated and controlled through computer software operating via a decentralized, peer-to-peer network. To acquire Bitcoin, a user typically purchased Bitcoin from a Bitcoin seller or "exchanger."

10. "Bitcoin addresses" were particular locations to which Bitcoin were sent and received. A Bitcoin address was analogous to a bank account number and was represented as a 26-to-35 character-long case-sensitive string of letters and numbers. Each Bitcoin address was controlled through the use of a unique corresponding private key which was a cryptographic equivalent of a password and was needed to access the Bitcoin address. Only the holder of a Bitcoin address's private key could authorize a transfer of Bitcoin from that address to another Bitcoin address. Little to no personally identifiable information about a Bitcoin account holder was transmitted during a Bitcoin transaction.

11. Á "cryptocurrency tumbler" or "cryptocurrency mixer" was a method of obfuscating the provenance, possession, and movement of cryptocurrencies through a process of "mixing." Because the blockchain is a public record, with analysis anyone can trace the flow of cryptocurrency between different cryptocurrency wallets. However, a tumbler or mixer service combined cryptocurrency from multiple wallets, combines them into a single wallet, then redistributes the cryptocurrency to multiple wallets. The tumbler or mixer extracted a fee for this process of obfuscation.

12. A dark-web marketplace was an online website accessible only through The Onion Router ("Tor") network, which anonymizes the Internet Protocol ("IP") addresses of its underlying servers. The use of Tor also made it difficult to identify the true physical locations of the website's administrators, moderators, and users. In many instances, dark-web marketplaces enabled users to buy and sell illegal goods, including controlled substances, stolen and fraudulent identification documents and access devices, counterfeit goods, malware and other computer hacking tools, firearms, and toxic chemicals. The site also allowed users to buy and sell illegal services, such as money laundering.

13. A secure sockets layer ("SSL") certificate was a digital certificate that authenticates the identity of a website and encrypts information sent to the server. SSL certificates established an online entity's credentials and enabled websites to move from HTTP to HTTPS, which was more secure.

14. A "command and control server" was a centralized computer that issued commands to remotely connected computers. "Command and Control" ("C2") infrastructure consisted of servers and other technical infrastructure that issued commands to control malware.

15. Tor was a computer network designed to facilitate anonymous communication over the Internet. The Tor network did this by routing a user's communications through a globally-distributed network of relay computers in a manner that rendered ineffective any conventional Internet Protocol ("IP") based methods of identifying users. The Tor network also enabled users to operate hidden sites that operated similarly to conventional websites.

16. Company A, whose identity is known to the Grand Jury, was a business headquartered in Austin, Texas which was in the Western District of Texas.

17. Company B, whose identity is known to the Grand Jury, was a business located in San Jose, California, which was in the Northern District of California.

18. Victim 1, whose identity is known to the Grand Jury, was an individual who resided in and whose computer was located in El Paso, Texas which was located in the Western District of Texas.

19. Victim 2, whose identity is known to the Grand Jury, was an individual who resided in Atlanta, GA.

20. Victim 3, whose identity is known to the Grand Jury, was an individual who resided in Tallahassee, FL.

21. Victim 4, whose identity is known to the Grand Jury, was an individual who resided in and whose computer was located in Killeen, Texas which was located in the Western District of Texas.

22. Defendant **Mark SOKOLOVSKY** was a citizen of Ukraine. SOKOLOVSKY used various online monikers including, Photix, raccoonstealer, and b1ack21jack77777. A picture of **SOKOLOVSKY** is attached to this indictment as Attachment A.

COUNT ONE

Conspiracy to Commit Fraud and Related Activity in Connection with Computers
[Violation of 18 U.S.C. § 371 (18 U.S.C. §§ 1030(a)(2)(C) and (a)(4)]

23. Paragraphs one through twenty-two of this indictment are re-alleged and incorporated by reference as though fully set forth herein

24. From sometime before August 2018, the exact date being unknown, and continuing until on or about the date of this Indictment, in the Western District of Texas, and elsewhere, the Defendant,

did knowingly and willfully combine, conspire, confederate, and agree with others known and unknown to the Grand Jury, to commit offenses against the United States, that is: intentionally access a computer without authorization and thereby obtain information from any protected computer (a computer in and affecting interstate and foreign commerce and communication) for the purpose of commercial advantage or private financial gain, and aid, abet, procure, and induce the same; and knowingly and with intent to defraud, access a protected computer, without authorization, and by means of such conduct further the intended fraud by obtaining financial and other data from multiple computers worth in excess of $5,000, and aid, abet, procure, and induce the same, in violation of Title 18, United States Code, Section 1030(a)(2), (a)(4), (c)(2)(B)(i), and (c)(3)(A).

Purpose of the Conspiracy

25. It was the purpose of the conspiracy for defendant **SOKOLOVSKY** and other conspirators to unlawfully enrich themselves by: (a) authoring Raccoon infostealer malware that would, when executed, steal data from victims' computers; (b) maintaining digital infrastructure, including C2 and storage servers to deliver the malware to users as well as store the stolen victim data; (c) collecting payments from users of Raccoon allowing them to use the infostealer against victims; (d) responding to questions and requests from actual and potential Raccoon purchasers, providing the users with information about Raccoon's capabilities and providing updated versions of Raccoon that provided additional capabilities; (e) receiving a copy of the data stolen by Raccoon users from victims.

Manner and Means of the Conspiracy

26. The manner and means by which defendant **SOKOLOVSKY** and other conspirators sought to accomplish the purpose of the conspiracy included, among other things:

a. Conspirators authored Raccoon infostealer malware, which was designed to steal data from victim computers, for the purpose of commercial advantage and private financial gain. Conspirators deployed Raccoon in or around February 2019, but had it under development since at least August 2018. After it was deployed, conspirators have regularly updated Raccoon.

b. Conspirators used Raccoon on numerous victims around the globe, proving its efficacy, before offering its use for sale as a MaaS. In order to lease Raccoon, cryptocurrency was sent to conspirators via a cryptocurrency account. The account was frequently changed in an effort to obscure the owner. Conspirators then sent the cryptocurrency payment to additional cryptocurrency accounts, including ones associated with cryptocurrency exchanges and other dark-web marketplaces known to operate cryptocurrency mixers and escrow accounts.

c. Conspirators were then given access to Raccoon via a log-in name, password, and web address.

d. Conspirators then infected victim computers by sending Raccoon via email phishing, using ruses that included purporting to be a document providing updated COVID-19 information during the global pandemic.

e. Conspirators then used Raccoon to steal any available financial, cryptocurrency, online account names and passwords, and other valuable digital data from the

victim computers. The information was sent to a server controlled by conspirators.

f. The stolen information was accessible to the conspirators who paid for access to Raccoon as well as the conspirators who controlled Raccoon.

g. The information could either be sold in a dark-web marketplace or other online cybercrime forum to those who would exploit it or exploited directly by those who deployed Raccoon.

h. Sokolovsky received a copy of the data stolen by those who leased Raccoon and stored millions of stolen log-in credentials and financial information records in an online drive.

27. See Attachment B for a visualization containing examples of how Raccoon functioned.

Overt Acts

28. In furtherance of the conspiracy and to affect its unlawful objects, defendant **SOKOLOVSKY**and other conspirators committed and caused to be committed the following overt acts in the Western District of Texas and elsewhere:

a. In or around December 2018, **SOKOLOVSKY** registered an SSL certificate that in April 2019 was used on one of the web domains that was hosting Raccoon.

b. On or about April 1, 2019, **SOKOLOVSKY** created a file containing the log-in information for the server that hosted the testing website for Raccoon. The testing website allowed potential purchasers of Raccoon to deploy the infostealer in a controlled environment to demonstrate how it worked.

c. On or about April 3, 2019, **SOKOLOVSKY** created a file containing a copy of the computer code for Raccoon's online infrastructure, including the code designed to process the information stolen by Raccoon.

d. On or about April 8, 2019, a user with the name "raccoonstealer" on the Exploit[.]in online cybercrime forum—which can be reached via Tor as well as the surface web—posted a thread entitled "[АРЕНДА] Raccoon Stealer [maas, loader, c/c++]" which advertised Raccoon for sale. The "raccoonstealer" account was created on April 2, 2019.

e. On or about April 19, 2019, **SOKOLOVSKY** created a file containing log-in information for online accounts and services used by Raccoon, including the information need to access the server hosted at the European web hosting company discussed below.

f. On or about April 21, 2019, an online server controlled by the conspirators received victim log-in credentials for an online account of a user of Company A.

g. On or about April 30, 2019, a coconspirator paid 5.79 euros to a European web hosting company to pay for virtual server rentals covering the time period of April 2, 2019 through April 26, 2019. That server hosted Raccoon's digital infrastructure.

h. On or about May 2, 2019, an online server controlled by the conspiracy received victim log-in credentials for an online account of a user of Company B.

i. On or about June 3, 2019, Victim 1 had their log-in credentials stolen, including for an official U.S. Army information system. On June 19, 2019, unknown individual(s) gained access to Victim 1's cellular account and used it and his

stolen bank account information to access Victim 1's bank account, attempting to steal approximately $15,000 over a period of one month.

j. On or about September 15, 2019, Victim Company 1, based in San Antonio, Texas, had its log-in credentials for a financial technology company stolen (Company B). Those credentials were used on or about October 6, 2019 to steal approximately $5,414 from Victim Company 1's account at Company B.

k. In or around November 2019, a conspirator posted on the Exploit[.]in Raccoon page that crypting services were now being integrated with Raccoon to help users evade detection by antivirus programs.

l. On or about December 22, 2019, Victim 2 had their log-in credentials for Company B stolen. Those credentials were used on or about December 23, 2019, to steal approximately $10,725 from Victim 2's account at Company B.

m. On or about January 1, 2020, Victim 3 had their log-in credentials for Company B stolen. Those credentials were used on or about February 25, 2020, to steal approximately $27,987 from Victim 3's account at Company B.

n. In or around March, April, and May of 2020, Raccoon was delivered to victim computers using various COVID-19 ruses, including via documents and links purporting to contain important COVID-19 health information, but in fact delivering the Raccoon malware onto victim computers, sometimes using the file name "corona[.]exe." One method of delivery included using what appeared to be the internet address of a U.S. Government health agency to redirect unsuspecting victims to download Raccoon.

o. On or about May 6, 2020, an individual sent 0.022 BTC (approximately $200 at the time) to a cryptocurrency address under the control of the conspiracy in order to lease Raccoon for one month. A conspirator then sent an electronic message with log-in, password, and a web link to access Raccoon.

p. On September 1, 2020, **SOKOLOVSKY** created a Git-based source code repository account, which was used to improve and modify the Raccoon code.

q. On or about April 1, 2021 an individual sent 0.003 BTC (approximately $200 at the time) to a cryptocurrency address under the control of the conspiracy in order to lease Raccoon for one month. A conspirator then sent an electronic message with log-in, password, and a link to access Raccoon.

r. On or about May 13, 2021, Victim 4, who resided in Killeen, TX, had their log-in credentials stolen, including for a service which was used by patients of U.S. Army medical facilities to communicate with practitioners regarding medical problems and prescriptions.

All in violation of Title 18, United States Code, Section 371 and Sections 1030(a)(2)(C), (a)(4), (c)(2)(B)(i), and (c)(3)(A).

COUNT TWO
Conspiracy to Commit Wire Fraud
[18 U.S.C. § 1349]

29. Count Two incorporates by reference, as if fully set forth herein, paragraphs one through twenty-two and paragraphs twenty-five through twenty-eight of this Indictment.

30. Beginning sometime before August 2018, the exact date being unknown, and continuing until on or about the date of this Indictment, in the Western District of Texas and elsewhere, the Defendant,

MARK SOKOLOVSKY

did knowingly and intentionally conspire and agree with others known and unknown to the Grand Jury to commit certain wire fraud, that is knowingly and with intent to defraud, having devised and having intended to devise a scheme and artifice to defraud, and to obtain money and property by means of material false and fraudulent pretenses, representations, and promises, in this case, using Raccoon to steal financial information, cryptocurrency, online account information so that users could then fraudulently login as the account holder, and obtain money, as described above, for the purpose of executing the scheme and artifice, to transmit and caused to be transmitted by means of wire, radio and television communication in interstate and foreign commerce certain writings, signs, signals, pictures and sounds, in violation of Title 18, United States Code, Section 1343.

All in violation of Title 18, United States Code, Section 1349.

COUNT THREE
Conspiracy to Commit Money Laundering
[18 U.S.C. § 1956(h)]

31. Count Three incorporates by reference, as if fully set forth herein, paragraphs one through twenty-two and paragraphs twenty-five through twenty-eight of this Indictment.

32. Beginning sometime before August 2018, the exact date being unknown, and continuing until on or about the date of this Indictment, in the Western District of Texas, and elsewhere, the Defendant,

MARK SOKOLOVSKY,

did knowingly combine, conspire, and agree with other persons known and unknown to the Grand Jury to commit offenses against the United States in violation of Title 18, United States

Code, Section 1956, namely:

a. To knowingly conduct and attempt to conduct financial transactions affecting interstate commerce and foreign commerce, which transactions involved the proceeds of specified unlawful activity, that is, Wire Fraud and Computer Intrusion as described in this Indictment related to Raccoon, knowing that the transactions were designed in whole or in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of specified unlawful activity, and that while conducting and attempting to conduct such financial transactions, knew that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i); and

b. To knowingly transport, transmit, transfer and attempt to transport, transmit, transfer funds and monetary instruments, from a place in the United States to a place outside the United States, knowing that the funds and monetary instruments involved in the transportation, transmittal, and transfer represented the proceeds of some form of unlawful activity and knowing that such transportation, transmittal, and transfer was designed in whole or in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of specified unlawful activity, that is, Wire Fraud and Computer Intrusion as described in this Indictment related to Raccoon as described in this Indictment, in violation of Title 18, United States Code, Section 1956(a)(2)(B)(i).

All in violation of Title 18, United States Code, Section 1956(h).

COUNT FOUR
Aggravated Identity Theft
[18 U.S.C. § 1028A]

33. Count Four incorporates by reference, as if fully set forth herein, paragraphs one through twenty-two and paragraphs twenty-five through twenty-eight of this Indictment.

34. On or about June 19, 2019, in the Western District of Texas and elsewhere, the Defendant,

MARK SOKOLOVSKY

did knowingly use, and aid, abet, induce, and procure the use of, without lawful authority, a means of identification of another person, to wit, Victim 1's bank account log-in information as described above, during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), namely Conspiracy to Commit Wire Fraud, as described in Count Two of this Indictment, knowing that the means of identification belonged to another actual person.

All in violation of Title 18, United States Code, Section 1028A(a)(1).

NOTICE OF GOVERNMENT'S DEMAND FOR FORFEITURE
[*See* Fed. R. Crim. P. 32.2]

I.
Conspiracy to Commit Wire Fraud Violations and Forfeiture Statutes
[Title 18 U.S.C. § 1349, subject to forfeiture pursuant to Title 18 U.S.C. § 981(a)(1)(C), made applicable to criminal forfeiture by Title 28 U.S.C. § 2461(c)]

As a result of the criminal violations set forth in Count Two, the United States gives notice to Defendant MARK SOKOLOVSKY (1) of its intent to seek the forfeiture of certain properties upon conviction pursuant to FED. R. CRIM. P. 32.2 and Title 18 U.S.C. § 981(a)(1)(C), made applicable to criminal forfeiture by Title 28 U.S.C. § 2461(c), which states:

Title 18 U.S.C. § 981.
(a)(1) The following property is subject to forfeiture to the United States:

* * *

> **(C)** Any property, real or personal, which constitutes or is derived from proceeds traceable to a violation of section . . . or any offense constituting "specified unlawful activity" (as defined in section 1956(c)(7) of this title), or a conspiracy to commit such offense.

Wire Fraud is an offense constituting "specified unlawful activity" as defined in Title 18 U.S.C. §§ 1956(c)(7) and 1961(1).

II.

Money Laundering Violations and Forfeiture Statutes

[Title 18 U.S.C. § 1956(h), subject to forfeiture pursuant to Title 18 U.S.C. § 982(a)(1)]

As a result of the criminal violations set forth in Count Three, the United States of America gives notice to Defendant MARK SOKOLOVSKY (1) of its intent to seek the forfeiture of certain properties upon conviction pursuant to Fed. R. Crim. P. 32.2 and Title 18 U.S.C. § 982(a)(1), which states:

> **Title 18 U.S.C. § 982.**
>
> **(a)(1)** The court, in imposing sentence on a person convicted of an offense in violation of section 1956, 1957, ... of this title, shall order that the person forfeit to the United States any property, real or personal, involved in such offense, or any property traceable to such property.

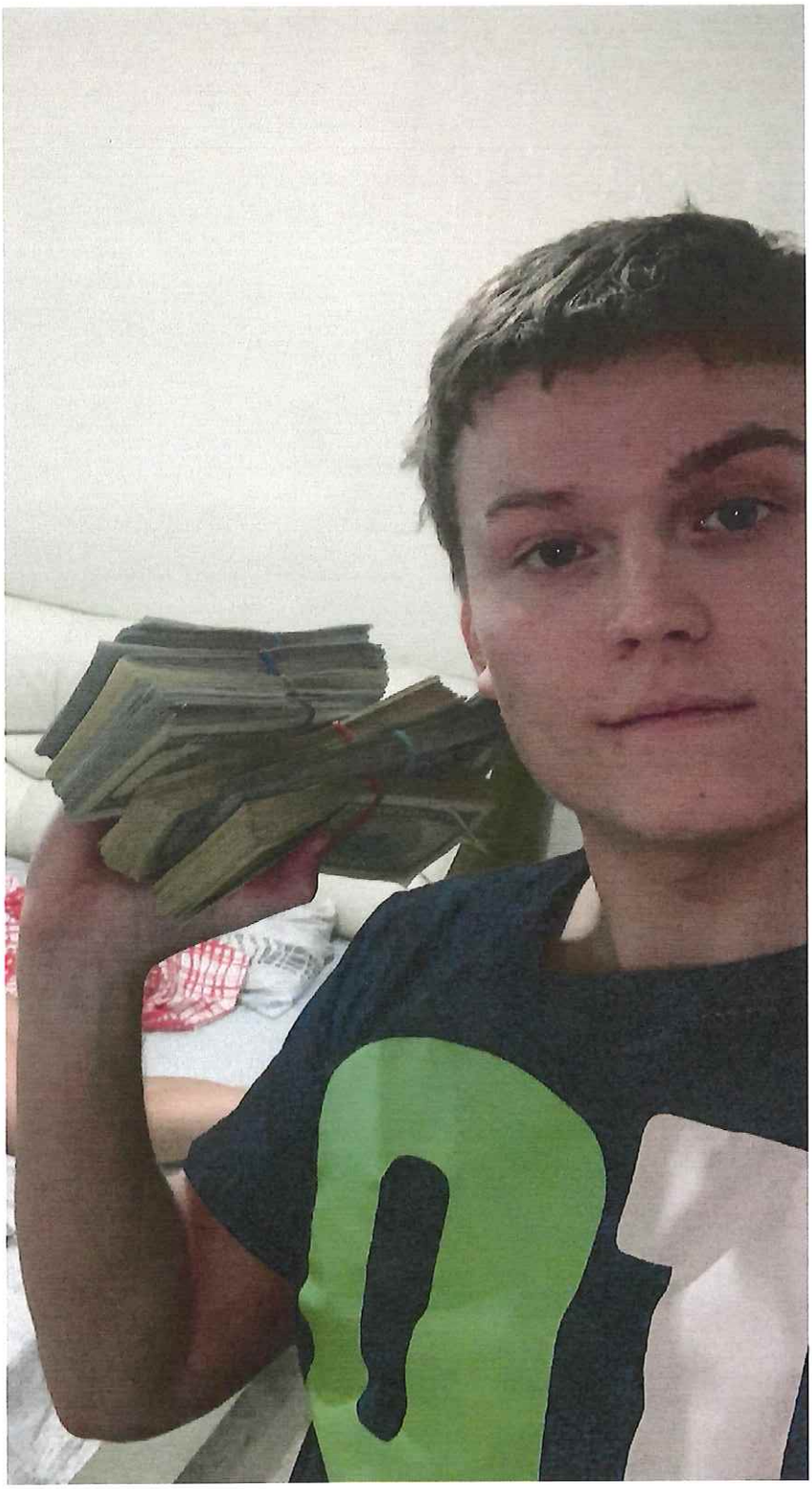
A TRUE BILL.

[redacted]
Original signed by the foreperson of the Grand Jury

ASHLEY C. HOFF
United States Attorney

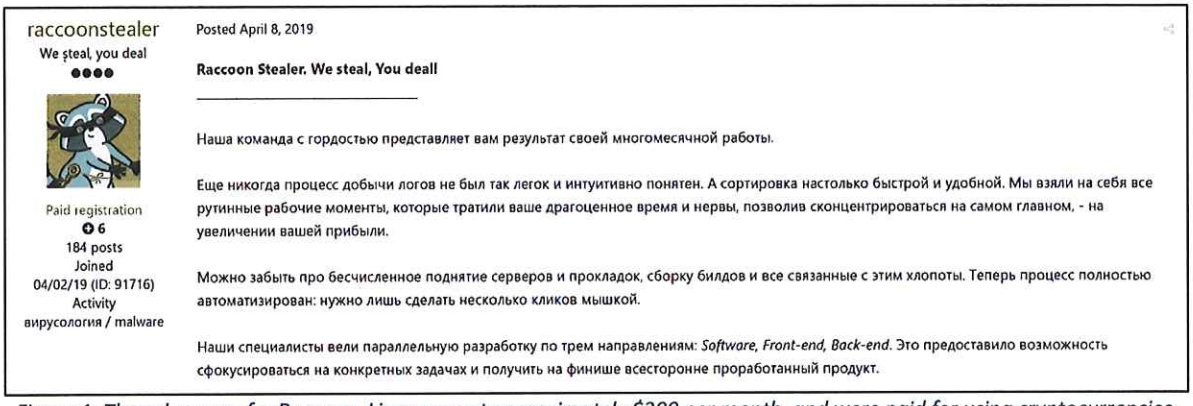
By: _____
MICHAEL C. GALDO
NEERAJ GUPTA
G. KARTHIK SRINIVASAN
Assistant United States Attorneys

Attachment A



ATTACHMENT B: RACCOON

STEP 1: Raccoon is purchased by a user



raccoonstealer
We steal, you deal
●●●●

Paid registration
✪ 6
184 posts
Joined
04/02/19 (ID: 91716)
Activity
вирусология / malware

Posted April 8, 2019

Raccoon Stealer. We steal, You deal!

Наша команда с гордостью представляет вам результат своей многомесячной работы.

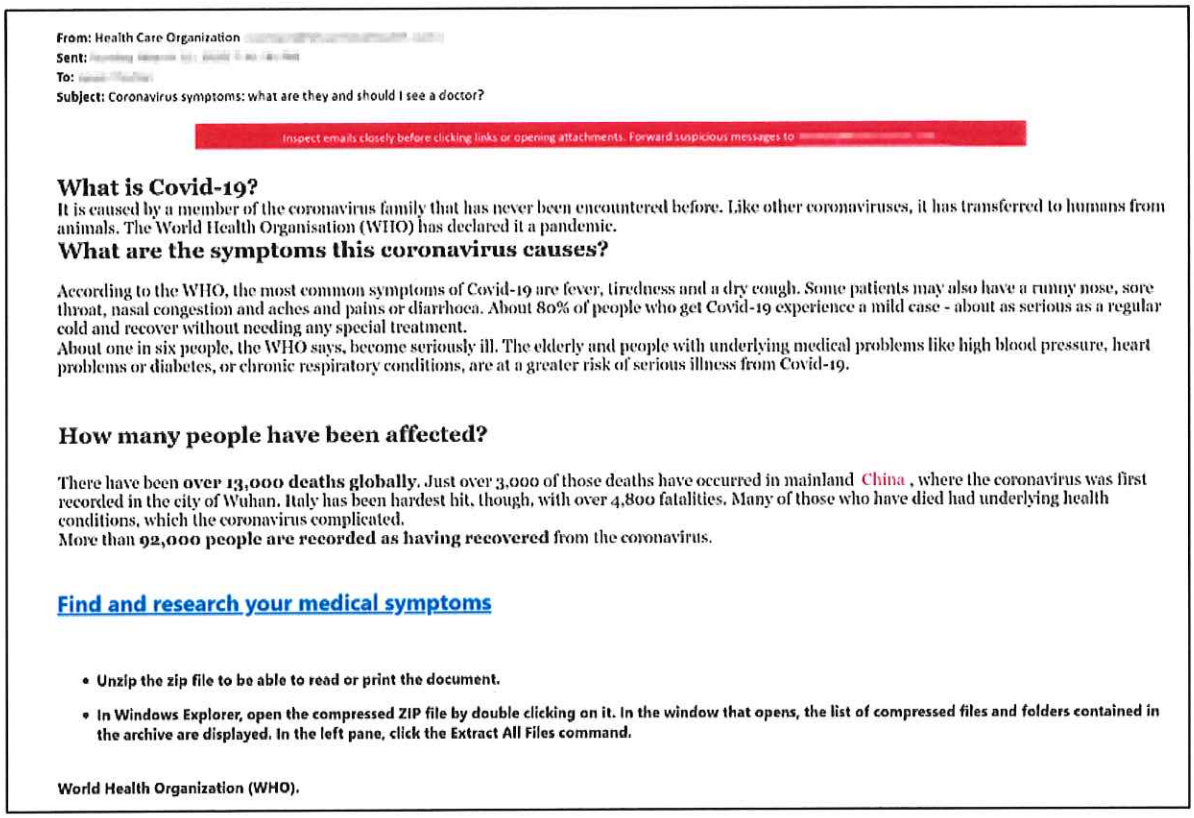
Еще никогда процесс добычи логов не был так легок и интуитивно понятен. А сортировка настолько быстрой и удобной. Мы взяли на себя все рутинные рабочие моменты, которые тратили ваше драгоценное время и нервы, позволив сконцентрироваться на самом главном, - на увеличении вашей прибыли.

Можно забыть про бесчисленное поднятие серверов и прокладок, сборку билдов и все связанные с этим хлопоты. Теперь процесс полностью автоматизирован: нужно лишь сделать несколько кликов мышкой.

Наши специалисты вели параллельную разработку по трем направлениям: *Software, Front-end, Back-end*. Это предоставило возможность сфокусироваться на конкретных задачах и получить на финише всесторонне проработанный продукт.

Figure 1: The sales page for Raccoon. Licenses cost approximately $200 per month, and were paid for using cryptocurrencies, like Bitcoin.

STEP 2: Raccoon is delivered by a user to a victim computer



From: Health Care Organization
Sent:
To:
Subject: Coronavirus symptoms: what are they and should I see a doctor?

Inspect emails closely before clicking links or opening attachments. Forward suspicious messages to

What is Covid-19?
It is caused by a member of the coronavirus family that has never been encountered before. Like other coronaviruses, it has transferred to humans from animals. The World Health Organisation (WHO) has declared it a pandemic.

What are the symptoms this coronavirus causes?

According to the WHO, the most common symptoms of Covid-19 are fever, tiredness and a dry cough. Some patients may also have a runny nose, sore throat, nasal congestion and aches and pains or diarrhoea. About 80% of people who get Covid-19 experience a mild case - about as serious as a regular cold and recover without needing any special treatment.
About one in six people, the WHO says, become seriously ill. The elderly and people with underlying medical problems like high blood pressure, heart problems or diabetes, or chronic respiratory conditions, are at a greater risk of serious illness from Covid-19.

How many people have been affected?

There have been **over 13,000 deaths globally**. Just over 3,000 of those deaths have occurred in mainland China , where the coronavirus was first recorded in the city of Wuhan. Italy has been hardest hit, though, with over 4,800 fatalities. Many of those who have died had underlying health conditions, which the coronavirus complicated.
More than **92,000 people are recorded as having recovered** from the coronavirus.

Find and research your medical symptoms

- **Unzip the zip file to be able to read or print the document.**
- **In Windows Explorer, open the compressed ZIP file by double clicking on it. In the window that opens, the list of compressed files and folders contained in the archive are displayed. In the left pane, click the Extract All Files command.**

World Health Organization (WHO).

Figure 2: An email containing a link that would download Raccoon when accessed.

STEP 3: Raccoon extracts data from the victim computer

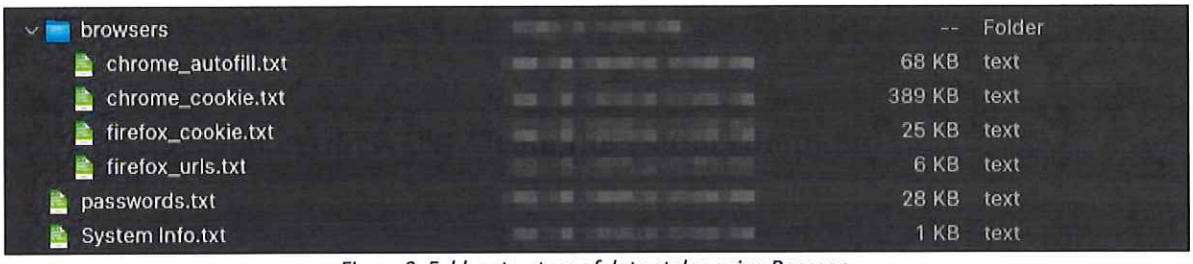


Figure 3: Folder structure of data stolen using Raccoon.

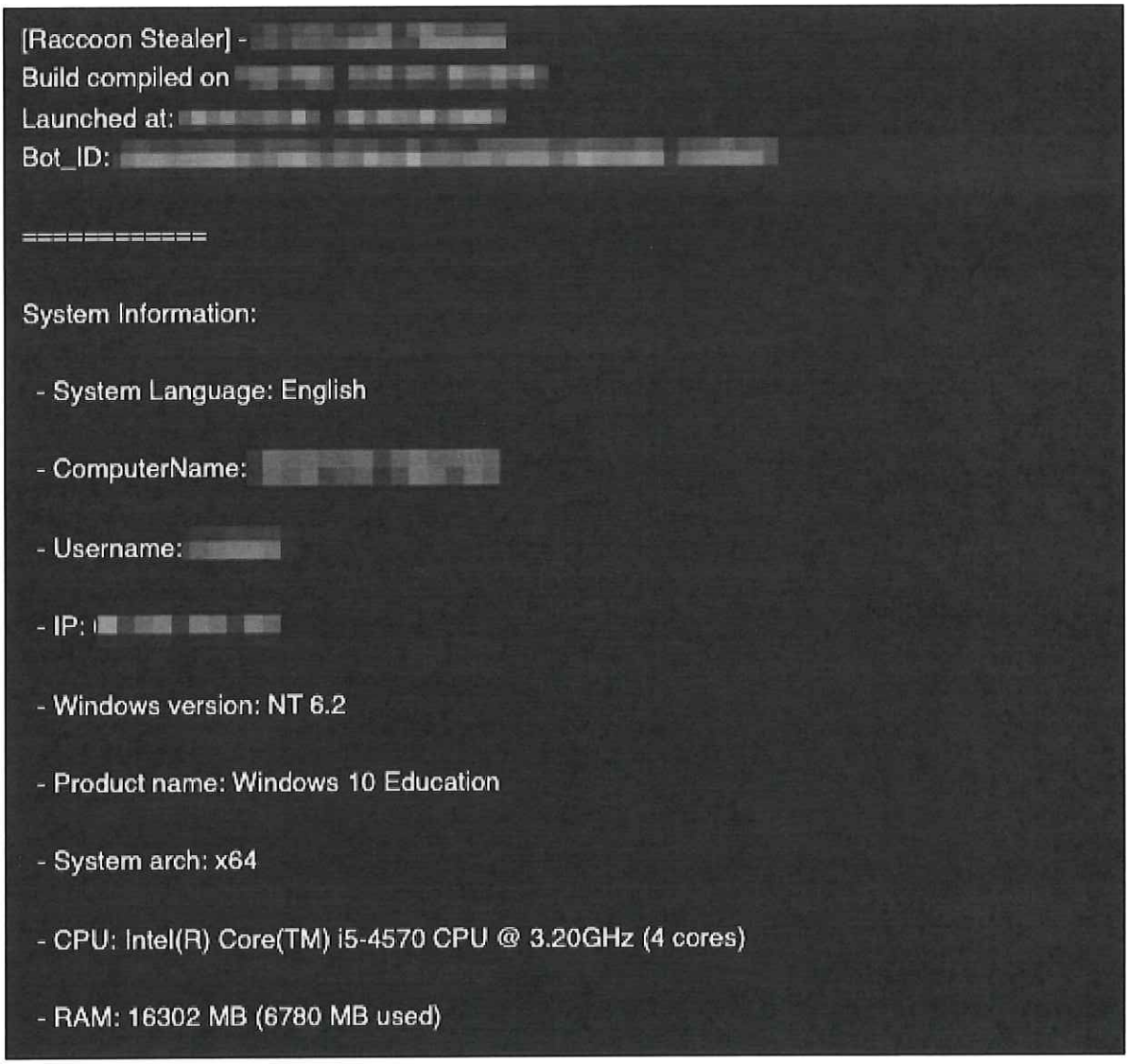


Figure 4: Computer information found in a log file created by Raccoon. Contained within the log were username and password combinations for the individual's financial accounts, in addition to other sensitive information.

STEP 4: User of Raccoon sells the stolen data, or uses it directly

DB	IP	BIN	EXP	TYPE	VEND	LVL	BANK	COUN	ZIP	CITY	STATE	HOLDER	ADDR	PHON	MAIL	PASS	PRICE	BUY
FRESH 01 MEGA SALE VALID 90-95% [18.09]	99.*..	[redacted]	[redacted]	DEBIT	VISA	CLAS	[redacted]	PE	48917	Lansing	MI	[redacted]	+	+	+	+	6.00$	
FRESH 01 MEGA SALE VALID 90-95% [18.09]	69.*..	[redacted]	[redacted]	DEBIT	VISA	CLAS	[redacted]	PE	59101	Billings	MT	[redacted]	+	+	+	+	6.00$	
FRESH 01 MEGA SALE VALID 90-95% [18.09]	72.*..	[redacted]	[redacted]	DEBIT	VISA	CLAS	[redacted]	US	01923	Danvers	MA	[redacted]	+	+	+	+	6.00$	
FRESH 01 MEGA SALE VALID 90-95% [18.09]	32.*..	[redacted]	[redacted]	DEBIT	MC	STAN	[redacted]	US	06525	Woodbridge	CT	[redacted]	+	+	+	+	6.00$	

Figure 5: One of the carding websites used to sell credit cards stolen through the use of Raccoon.

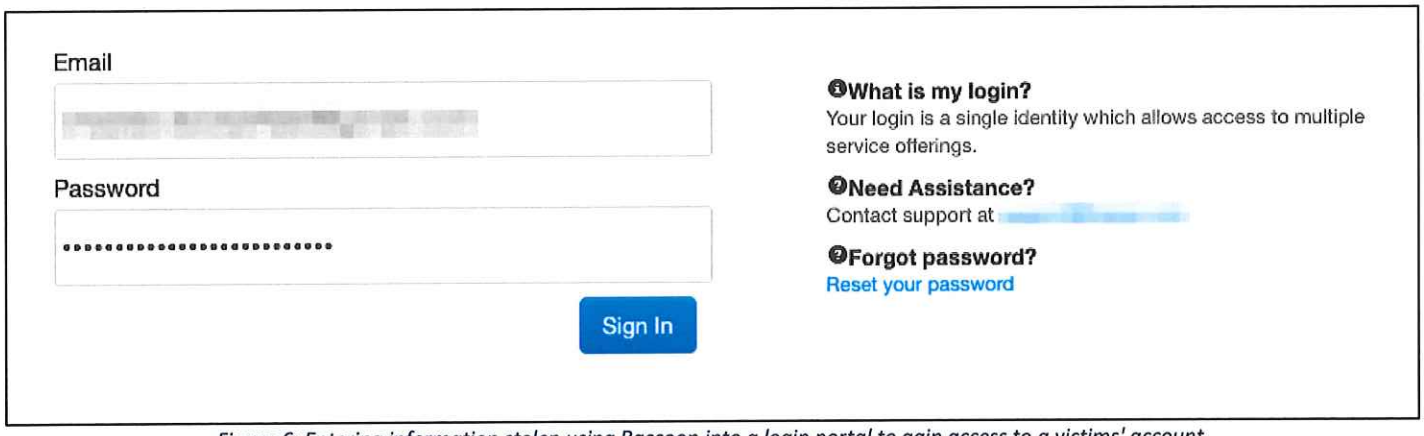


Figure 6: Entering information stolen using Raccoon into a login portal to gain access to a victims' account.