

AO 91 (Rev. 02/09) Criminal Complaint

United States District Court

for the
Western District of New York



United States of America

v.

Case No. 23-MJ-5044

WUL ISAAC CHOL

Defendant

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about June 13, 2019, the exact date being unknown, in the Western District of New York, and elsewhere, the defendant, WUL ISAAC CHOL, knowingly and with intent to defraud, possessed fifteen or more unauthorized access devices, as defined in Title 18, United States Code, Section 1029(e)(3), that is, stolen login credentials, said possession affecting interstate and foreign commerce in that the defendant purchased the unauthorized access devices from a website based outside the United States.

All in violation of Title 18, United States Code, Section 1029(a)(3).

This Criminal Complaint is based on these facts:

Continued on the attached sheet.

Complainant's signature

BRYAN SCHEIBER
SPECIAL AGENT
FEDERAL BUREAU OF INVESTIGATION

Printed name and title

Sworn to before me and signed telephonically.

Date: April 3, 2023

Judge's signature

City and State: Buffalo, New York

HONORABLE MICHAEL J. ROEMER
UNITED STATES MAGISTRATE JUDGE

Printed name and title

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Bryan Scheiber, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of a criminal complaint charging WUL ISAAC CHOL (hereinafter "CHOL"), with violations of Title 18, United States Code, Section 1029(a)(3) (knowingly and with intent to defraud, possessing fifteen or more devices which are counterfeit or unauthorized access devices).

2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since June 2021. I am currently assigned to the Cyber Squad, Buffalo Division, in Buffalo, New York, where I work on investigations relating to criminal and national security cyber intrusions. I received my Bachelors and Masters degrees in Computer Science, have a Graduate Certificate in Computer Security and Information Assurance and hold several private sector computer security certifications. Prior to becoming an FBI Special Agent, I was a Computer Scientist with the FBI's Washington Field Office. My work in the FBI, as well as the training I have received, has familiarized me with identifying and handling evidence found in digital media, network analysis, and digital forensics. As a Special Agent with the FBI, I am empowered by law to investigate and make arrests for offenses against the United States.

3. The facts set forth are based upon my personal observations, my training and experience, and information obtained during the course of the investigation from other members of law enforcement, involving the review of records, interviews of witnesses, and information and reports provided. Because this affidavit is submitted for the purpose of establishing probable cause to support the issuance of a Criminal Complaint and Arrest Warrant, I have not included each and every fact known by the government for this investigation.

PROBABLE CAUSE

Background Regarding the Genesis Market Investigation

4. Since August 2018, the FBI has been investigating an illicit online marketplace named Genesis Market. Genesis Market is primarily hosted at the Internet domain “genesis.market.”¹ Genesis Market’s operators compile stolen data (e.g., computer and mobile device identifiers, email addresses, usernames, and passwords) from malware-infected² computers around the globe and package it for sale on the market.³ Genesis Market has been the subject of various cybersecurity presentations and news stories. For example, CBS News ran a story on Genesis Market in September 2021.⁴

5. The packages advertised for sale on Genesis Market vary by price and many packages are available for around \$10 to \$20 per package. The price appears to vary based on three primary factors: (1) the number of online accounts (“resources”) associated with the package (e.g., accounts with legitimate

¹ A domain name is a way to identify computers on the Internet, using a series of characters that correspond with a particular IP address. Genesis Market is also associated with certain backup domains in case the primary domain is shut down or taken offline for any reason. Those backup domains include the website “g3n3sis.org,” as well as the TOR domain “genesiswiwn7p7lmbvimup7v767e64rcw6o3kfcnobu3nxistepx2qd.onion.” TOR is short for “The Onion Router” and is free, publicly available software for enabling anonymous communication over the internet. The TOR software is designed to enhance users’ privacy online by bouncing their communications around a distributed network of relay computers run by volunteers around the world, thereby masking the user’s actual IP address, which could otherwise be used to identify a user.

² Malware, or malicious software, refers to any piece of software that is written to damage and/or steal data from an Internet connected device. Viruses, trojans, spyware, and ransomware are all different types of malware.

³ Genesis Market refers to these packages of stolen data as “bots” on their site; however, typically, an Internet bot refers to a piece of software that runs automated tasks over the Internet. Since Genesis Market’s use of the word “bot” strays from the normal meaning, the term “package” is used throughout this request.

⁴ See Dan Patterson, *Inside Genesis: The market created by cybercriminals to make millions selling your digital identity*, September 9, 2021, available at <https://www.cbsnews.com/news/genesis-cybercriminal-market-ransomware/> (last visited March 13, 2023).

credentials for platforms like Amazon, Netflix, Gmail, etc. are more valuable); (2) how recently the package was compromised with malware; and (3) whether there is a “fingerprint” associated with the package. A fingerprint is a group of identifiers that third-party applications or websites use to identify a computer or device. These fingerprints allow the applications or websites to confirm that the device is a trusted source. In situations where a fingerprint is associated with a package, Genesis Market provides the purchaser with a proprietary plugin (*i.e.*, an Internet browser extension that provides additional functionality). This proprietary plugin amplifies that purchaser’s ability to control and access the package’s data and masquerade as the victim device.

6. Genesis Market’s operators have advertised Genesis Market on prominent online criminal forums, including exploit.in and xss.is. Those advertisements include news, updates, and information regarding Genesis Market. For example, the advertisements have included (1) information about packages for sale on Genesis Market; (2) specific replies to users requesting packages located in specific countries; and (3) updates regarding the tools available through Genesis Market.

7. Genesis Market users can gain initial access to Genesis Market via an invitation from a Genesis Market operator on a cybercriminal forum, or via an invitation from an individual who already has an account on Genesis Market. The invitations are for one-time use and in the form of an alphanumeric text string. Once a prospective new user receives an invitation, the new user can go to a Genesis Market domain to create a username and password. Genesis Market then requests the new user to associate their Jabber ID⁵ or email address with that new account. Analysis by law enforcement has found that a Jabber ID or email address is not absolutely required when registering an account, nor is the Jabber ID or email address verified by Genesis Market administrators. Nonetheless, the vast majority of Genesis

⁵ Jabber is a chat and communications platform akin to AOL Instant Messenger. It is prominent among cybercriminal operators because it is considered exceptionally secure.

users have registered with a Jabber ID or email address, as it is one of the fields to enter registration data when creating a new account.

8. While conducting covert operations, law enforcement has observed that for new users logged into Genesis Market, the front page generally displays a “dashboard” of information, including the number of packages listed for sale and a “Genesis Wiki” page that walks a new user through Genesis Market’s platform and how to use it. Below is a screenshot taken April 1, 2021, of the front page of Genesis Market.⁶ The front page displays the total amount of “bots” (packages) available for sale on Genesis Market at that time, categorized by country. This page appears immediately after the user logs into his or her account. The tabs on the left allow for the Genesis Market user to traverse the market:

⁶ Portions of the screenshots in this affidavit have been redacted or omitted to conceal information that might identify accounts used covertly by investigators.

genesis

Dashboard Home

Genesis Wiki

News

Bots 250k+

Generate FP

Orders

Purchases 10T

Payments 8

Tickets 1

Software 6.3.119.0

Profile

Invites

Logout

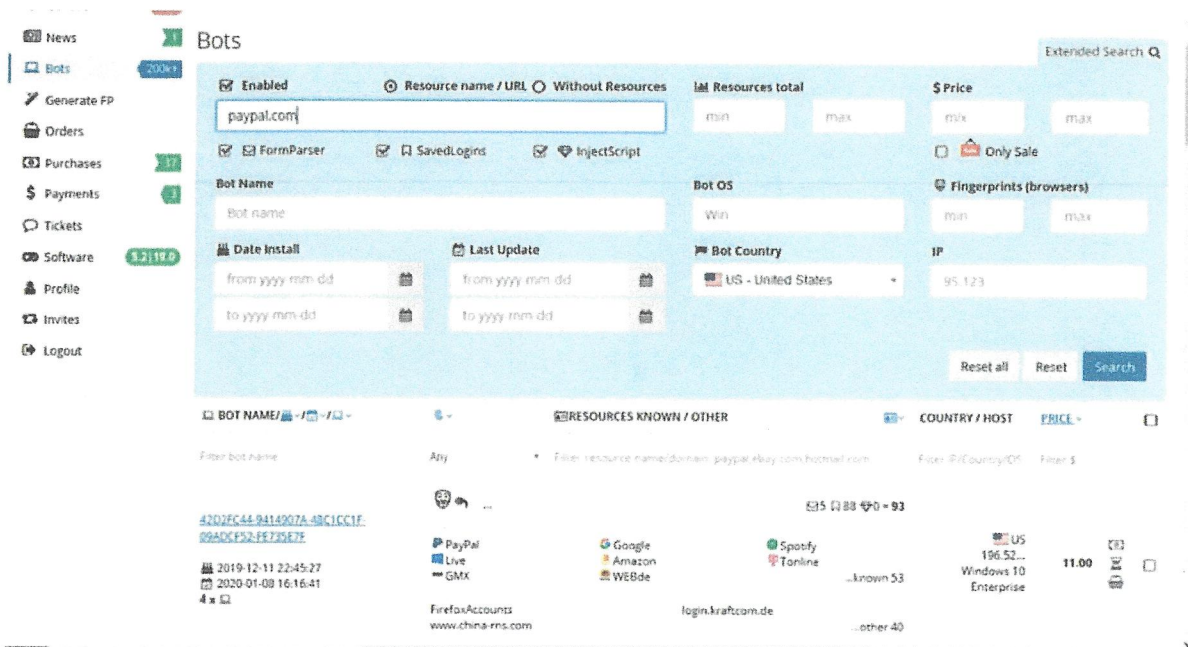
Have insider info about Genesis market related investigation? Write us, we are interested.

Available Bots

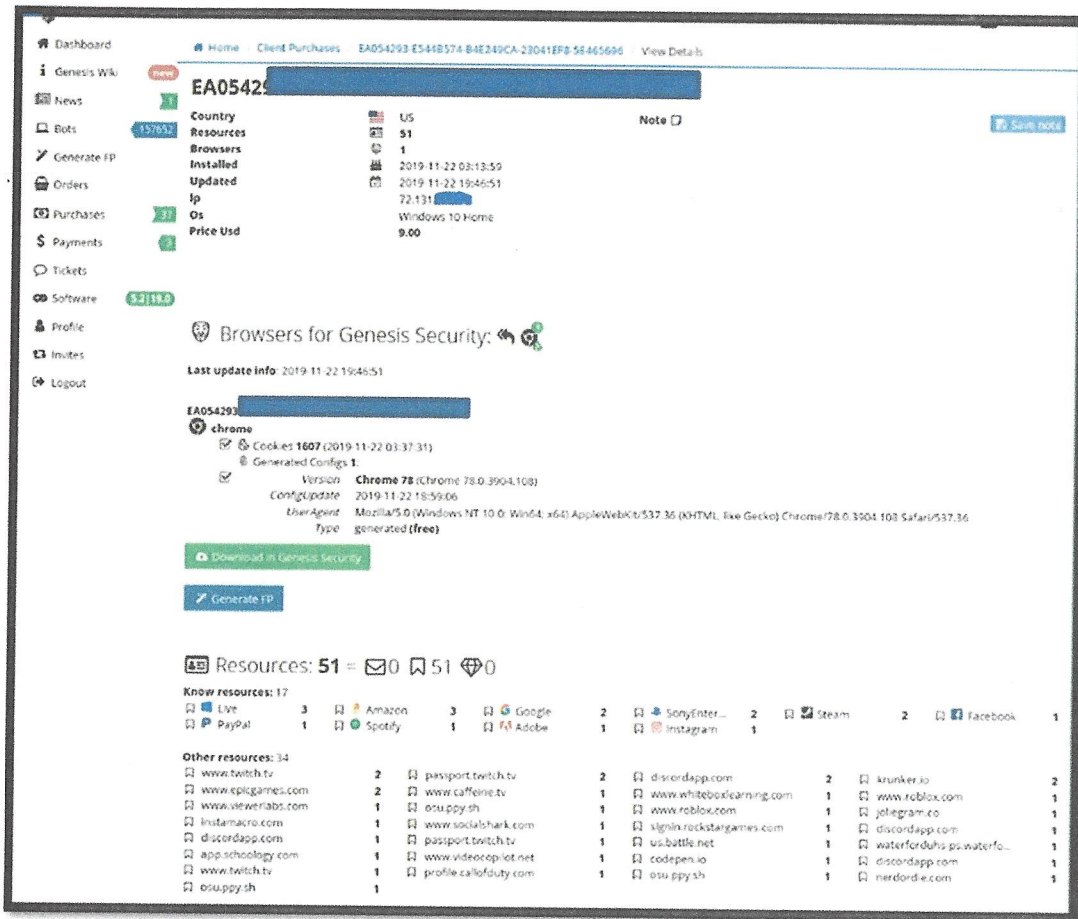
COUNTRY	LAST 24H	LAST WEEK	LAST MONTH	AVAILABLE
Overall				
218	+22	+4210	+25476	372326
Grouped by				
US	+3	+477	+2388	12625
IT	+2	+557	+2878	52196
FR	+3	+345	+2018	38073
ES	+1	+314	+1931	23370
PL	+1	+305	+1826	14694
AR	+1	+256	+1795	11532
RO	+4	+320	+1648	17309
PT		+177	+1154	22928
CL		+180	+1141	6050
HU		+156	+943	9353
GR		+148	+793	5969
NP		+91	+676	5553
NL	+1	+115	+668	7527
CA		+92	+640	2688
BG	+1	+87	+539	4473
BE		+96	+465	6827
SK		+59	+375	2822
AU		+48	+364	3127
SE	+2	+56	+363	4971
HR		+74	+340	2558
GE		+58	+320	1337

more 126

9. Genesis Market also features a search function that allows a user to search for packages based on areas of interest (*e.g.*, banking information, social media accounts, etc.), country of origin, price, and the date of infection (*i.e.*, the date the victim device was infected with malware). Below is a screenshot taken on November 13, 2020, showing the search function on Genesis Market:







10. When a user purchases a package, the user receives access to all the identifiers associated with the package, including, but not necessarily limited to, device information, such as operating system, IP address, keyboard language, and time zone information, as well as access credentials, such as usernames and passwords, for compromised accounts. Below is a screenshot taken on November 22, 2019, of an FBI Online Covert Employee’s purchase of a Genesis Market package:



11. Below is a screenshot dated November 22, 2019, relating to the same victim package as above, showing the email addresses and passwords (both of which are redacted for the purposes of this affidavit) that are provided to the purchaser of the victim package:

Last update Saved Logins: 2019-11-22 08:55:29
 Last update Form Parser: 1970-01-01 00:00:00
 Last update Inject Script: 1970-01-01 00:00:00

RESOURCE NAME / URL / LOGIN / PASSWORD / ...	SOURCE	DATASETS	BROWSER	KNOWN	GRABBED / UPDATED
https://www.viewerlabs.com/register *Login*: [redacted]@gmail.com *Password*: [redacted]	Saved Logins	LoginData	chrome	no	2019-11-22 03:13:59 2019-11-22 08:55:29
EA054293-E544B574-B4E249CA-23041EF8-5E465696					
 Sony Entertainment Network https://account.sonyentertainmentnetwork.com/	Saved Logins	LoginData	chrome	yes	2019-11-22 03:13:59 2019-11-22 08:55:29
EA054293-E544B574-B4E249CA-23041EF8-5E465696					
https://www.whiteboxlearning.com/login *Login*: [redacted] *Password*: [redacted]	Saved Logins	LoginData	chrome	no	2019-11-22 03:13:59 2019-11-22 08:55:29
EA054293-E544B574-B4E249CA-23041EF8-5E465696					
 Amazon https://www.amazon.com/ap/signin	Saved Logins	LoginData	chrome	yes	2019-11-22 03:13:59 2019-11-22 08:55:29
EA054293-E544B574-B4E249CA-23041EF8-5E465696					
https://www.roblox.com/ *Login*: [redacted] *Password*: [redacted]	Saved Logins	LoginData	chrome	no	2019-11-22 03:13:59 2019-11-22 08:55:29
EA054293-E544B574-B4E249CA-23041EF8-5E465696					
 Google https://accounts.google.com/signin/v2/identifier	Saved Logins	LoginData	chrome	yes	2019-11-22 03:13:59 2019-11-22 08:55:29
EA054293-E544B574-B4E249CA-23041EF8-5E465696					
 Live https://login.live.com/ppsecure/post.srf *Login*: [redacted]@mail.com *Password*: [redacted]	Saved Logins	LoginData	chrome	yes	2019-11-22 03:13:59 2019-11-22 08:55:29

12. When users have questions or issues with Genesis Market, they can submit “tickets” via a “Ticket” tab on the Genesis Market website, which enables them to communicate with Genesis Market operators.

13. Purchases made through Genesis Market are conducted using virtual currency, such as bitcoin.⁷ Before a purchase can be made, however, the user must first deposit a sum of virtual currency into their Genesis Market account. This is done through the “Payments” tab on the Genesis Market website, wherein the user can choose the type of virtual currency they want to use. If the user chose bitcoin, for example, the user would then (1) enter the amount in U.S. dollars that they want credited to their account, (2) receive a one-time-use bitcoin address, along with the converted bitcoin amount, and then (3) they would use that bitcoin address to send bitcoin to Genesis Market.⁸ Once the user sends the bitcoin to the one-time-use address, the user is prompted to wait several minutes for the transaction to complete, and then the user will ultimately see that their Genesis Market account is credited with the requested amount. Once the account is credited, the user can purchase packages from Genesis Market.

14. As of October 17, 2022, there were approximately 450,000 packages listed for sale on Genesis Market. Each package represents a single, compromised computer or device. According to Genesis Market’s website, the packages are located across North America (including throughout the United States), Europe, South America, and parts of Asia.

15. As part of the investigation, the FBI has covertly operated several Genesis Market accounts and has funded the purchase of approximately 115 packages through Genesis Market. Through these accounts, the FBI has monitored activity on Genesis Market and interacted with Genesis Market

⁷ Virtual currencies, such as bitcoin, are digital tokens of value circulated over the Internet as substitutes for traditional fiat currency. Virtual currencies are not issued by any government or bank like traditional fiat currencies such as the U.S. dollar, but rather are generated and controlled through computer software. Bitcoin is currently the most well-known virtual currency in use. Investigators found that Genesis Market also accepted Litecoin (an alternative to bitcoin), and in 2022 started accepting Monero (an anonymity enhanced virtual currency).

⁸ Over the course of the investigation, investigators found that Genesis Market utilized a third-party service, the identify of which is known to law enforcement and known to be associated with criminal activity, to process the virtual currency transactions.

operators through the “Ticket” function. The FBI has reviewed the data from purchased packages and determined that Genesis Market is, in fact, collecting and selling victims’ personal identifying information that has been stolen from devices located around the world. For instance, FBI agents identified seven packages that consisted of data taken from devices of victims located in Wisconsin. FBI agents showed seven victim device owners the usernames and passwords that the agents had obtained via Genesis Market, and the victims confirmed that the usernames and passwords belonged to them and had been stolen.

16. In December 2020, law enforcement, via mutual legal assistance request and in coordination with authorities in another country, obtained a forensic image of a server that contained the Genesis Market database (referred to herein as “Database A”). The database included, among other things, Genesis Market’s administrator logs; user logs; lists of all packages sold on the marketplace; payment transaction logs; malware used by Genesis Market administrators; and other pieces of information related to the market.

17. The data included information from more than 33,000 Genesis Market user accounts, including usernames and email addresses; IP address history; search history; virtual currency transactions; the number of packages purchased by the user; and the data contained within the packages purchased by the user.

18. After law enforcement obtained a copy of the Genesis Market Database A server, the Genesis Market operators removed their website from that server and utilized hosting infrastructure from other companies in other countries.

19. Then, in May 2022, law enforcement, via mutual legal assistance request and in coordination with authorities in another country, obtained a forensic image of a server that contained the Genesis Market database (referred to herein as “Database B”). The database included the same types of

information described above, including information from more than 55,000 Genesis Market user accounts.

CHOL's Activity on Genesis Market

20. The Genesis Market data showed that, from June 13, 2019 to May 10, 2022, a user whose account name was connectgcross ("CONNECTGCROSS") accessed Genesis Market approximately 104 times and purchased 21 packages on Genesis Market that included 778 stolen account credentials. The registration data for CONNECTGCROSS showed the account was created on June 13, 2019; listed a Jabber ID of connectgcross@jabber.com; and showed CONNECTGCROSS deposited \$105.08 to their marketplace account.

21. CONNECTGCROSS made their first bitcoin deposit and purchase in the Genesis Market on June 13, 2019. CONNECTGCROSS made a later bitcoin deposit ("TRANSACTION 1") to Genesis Market on July 21, 2019 that was traced to a cryptocurrency exchange that could be served legal process to determine the source of the funds.

22. TRANSACTION 1 on July 21, 2019 was for 0.00242105 bitcoin with the transaction hash a64feff723584b9bf7eb72d194c7ae7130e953073e6819635068e33d309685c0. Investigators found TRANSACTION 1 originated from a cryptocurrency exchange named Coinbase. Coinbase records showed TRANSACTION 1 was sent from a Coinbase account ("COINBASE ACCOUNT 1") that listed the owner as "Wul Chol" with 20 Ferguson Avenue, Buffalo, NY 14213 as the customer's address. Coinbase provided Know Your Customer ("KYC") information for COINBASE ACCOUNT 1, which included photographs of CHOL, CHOL's New York State identification card and CHOL's United States Passport card.

23. In December 2022, the FBI conducted checks on CHOL using government, commercial and open source databases. Database queries confirmed the personal and driver license information provided by CHOL when registering and maintaining his Coinbase accounts.

24. The Genesis Market data showed that CHOL purchased the following packages on the marketplace:

- a. PACKAGE 1, which included compromised credentials for a victim's eBay, Amazon.co.uk, LinkedIn, RyanAir, AirBnb accounts.
- b. PACKAGE 2, which included compromised credentials for a victim's Google, Starbucks, Adobe.com, Twitter, Instagram, Codecademy, Github and Pinterest accounts.
- c. PACKAGE 3, which included compromised credentials for a victim's Ancestry, SquareUp, Live.com, Facebook, Amazon, LinkedIn and Missouri Department of Revenue accounts.
- d. PACKAGE 4, which included compromised credentials for a victim's Facebook, AOL, Dunkin Donuts, Netflix and Miami-Dade County Public Schools accounts.
- e. PACKAGE 5, which included compromised credentials for a victim's Dropbox, SquareUp and Paypal accounts.
- f. PACKAGE 6, which included compromised credentials for a victim's GoDaddy, Facebook, Google, Stripe, Mailchimp, Twitter, United Airlines, LinkedIn, Shutterstock, Airbnb, Costco, Earthlink Email, JetBlue, MagicJack, California DMV, L.A. Care Health Plan, SquareUp, Netflix, The Superior Court of California Country of Los Angeles Jury Duty Portal and DirectTV accounts.
- g. PACKAGE 7, which included compromised credentials for a victim's Google, AOL, Pandora, Dallas Baptist University Online Library, Central Seminary email, Paypal, Dropbox, Bank of America, Instagram, Twitter, MetroPCS and Facebook accounts.
- h. PACKAGE 8, which included compromised credentials for a victim's eBay and British Gas accounts.

- i. PACKAGE 9, which included compromised credentials for a victim's Facebook, TransferWise, Google, Indeed, Vodafone, Pizza Hut, Instagram, Netflix, eBay, Booking.com, Airbnb and Paypal accounts.
- j. PACKAGE 10, which included compromised credentials for a victim's Amazon, Pennsylvania College of Technology, Epic Games, Comcast, NewEgg, Grammarly, Scholarship Owl, Apple, Visa, College Board, Spotify and Hulu accounts.
- k. PACKAGE 11, which included compromised credentials for a victim's Japan Post, Amazon and Mercari accounts.
- l. PACKAGE 12, which included compromised credentials for a victim's Google, AT&T, Yahoo, TextNow, Iowa Workforce Development Unemployment Insurance Weekly Claim, Apple Store, Paypal and Github accounts.
- m. PACKAGE 13, which included compromised credentials for a victim's Facebook, Yahoo, Instagram, Google and Match.com accounts.
- n. PACKAGE 14, which included compromised credentials for a victim's Facebook, Dropbox and Airbnb accounts.
- o. PACKAGE 15, which included compromised credentials for a victim's Airbnb, Netflix, Amazon, Groupon, Facebook, Movistar and Live.com accounts.
- p. PACKAGE 16, which included compromised credentials for a victim's Google, Steam, Sony, Apple and Google accounts.
- q. PACKAGE 17, which included compromised credentials for a victim's Zoom, Live.com, Pinterest, Discord, Netflix, Instagram and Hulu accounts.
- r. PACKAGE 18, which included compromised credentials for a victim's Discord, Instagram, Nintendo, Epic Games, Twitter, Google, Live.com, League of Legends, Apple, Steam, Twitch, Github and Sony accounts.

- s. PACKAGE 19, which included compromised credentials for a victim's Amazon, Facebook, Epic Games, Rockstar Games, Paysafecard, Twitch and LogMeIn accounts.
- t. PACKAGE 20, which included compromised credentials for a victim's Discord, Riot Games, Google, Discord and Hulu accounts.
- u. PACKAGE 21, which included compromised credentials for a victim's Netflix, Live.com, Pinterest, Nintendo, Riot Games, Instagram, Twitch and Discord accounts.

25. On December 19, 2022, the Honorable Jeremiah J. McCarthy, Magistrate Judge for the Western District of New York, signed a search warrant for CHOL's Facebook account, with the Facebook username wul.chol.1.

26. CHOL used the IP address 192.135.227.228 to access Genesis Marketplace on the following dates: June 17, 2019, June 18, 2019, and July 19, 2019. CHOL used the same IP address, 192.135.227.228, to access his Coinbase account on the following dates: May 29, 2019, May 31, 2019, June 2, 2019, June 9, 2019, June 10, 2019, and June 28, 2019. Finally, CHOL used the same IP address, 192.135.227.228, to access his Facebook account on June 22, 2019.

27. The IP address 192.135.227.228 is registered to the Buffalo & Erie County Public Library. Information from CHOL's Facebook account, which is described in more detail below, shows that CHOL visited the library on multiple days that correspond with the activity described in the prior paragraph.

- a. On June 2, 2019 at 3:49 PM Eastern Time, CHOL messaged a Facebook user to pick him up from the library. CHOL's Coinbase account was accessed from the Buffalo & Erie County Public Library IP address 192.135.227.228 on June 2, 2019 at 2:42 PM Eastern Time.

- b. On June 9, 2019, CHOL messaged a Facebook user that he was going to the library.
CHOL's Coinbase account was accessed from the Buffalo & Erie County Public Library IP address 192.135.227.228 on June 9, 2019 at 8:19 PM.
- c. On June 12, 2019, CHOL messaged a Facebook conversation at 3:48 PM Eastern Time that he would arrive at the library at 4:30 PM that day, during normal business hours.
- d. On June 18, 2019, a Facebook user messaged CHOL where he was, to which CHOL responded "Library." That same day, CHOL accessed Genesis Market from the Buffalo & Erie County Public Library IP address 192.135.227.228.
- e. On June 26, 2019, a Facebook user messaged CHOL where he was, to which CHOL responded "Library."
- f. On June 29, 2019, CHOL informed a Facebook user that he was at the library.

28. CHOL's Facebook account included an instant message conversation between CHOL and a Facebook user ("FACEBOOK USER 1") on December 23, 2019 where CHOL told FACEBOOK USER 1 that they had read an article about sites that sell fake "joints" and resold joints to make "bread."⁹ In my training and experience, I know that "joints" is a term used for bank accounts and "bread" is a term used for money.

⁹ It is unclear whether the website CHOL refers to is Genesis or another website.

Author Wul Chol (Facebook: 100007877380676)
Sent 2019-12-23 09:47:10 UTC
Body But if ur not confident in ur pieces just do in store pick up

Author ██████████ FACEBOOK USER 1
Sent 2019-12-23 09:47:23 UTC
Body Lol ight

Author Wul Chol (Facebook: 100007877380676)
Sent 2019-12-23 09:50:10 UTC
Body But nah the reason u probably ain't trying to fuck with pieces is cuz the sites u fucking with

Author Wul Chol (Facebook: 100007877380676)
Sent 2019-12-23 09:51:58 UTC
Body I read a article about sites that most sell fake joints and resold joints just to make bread and that its not the person its just the site that's fucked up

29. CHOL's Facebook account included an instant message conversation between CHOL and FACEBOOK USER 1 on March 30, 2020 where CHOL and FACEBOOK USER 1 discuss a site where CHOL and FACEBOOK 1 had obtained "fullz." In my training and experience, I know that "fullz" are stolen identities or stolen credit card information, where the word "full" means full data or full credentials.

Author ██████████ FACEBOOK USER 1
Sent 2020-03-30 17:50:48 UTC
Body What's that site me and u got the fullz from

Author ██████████ FACEBOOK USER 1
Sent 2020-03-30 17:51:04 UTC
Body And we did western union then hak picked it up

Author ██████████ FACEBOOK USER 1
Sent 2020-03-30 18:23:01 UTC
Body ██████████ sent a photo.

Author Wul Chol (Facebook: 100007877380676)
Sent 2020-03-30 19:32:05 UTC
Body Ironman

Author Wul Chol (Facebook: 100007877380676)
Sent 2020-03-30 19:32:15 UTC
Body Why

Author Wul Chol (Facebook: 100007877380676)
Sent 2020-03-30 19:34:22 UTC
Body I think ironmancash something like that

Author [REDACTED] FACEBOOK USER 1
Sent 2020-03-30 19:34:46 UTC
Body Bet I knew it was cause I'm finna get more fullz for western

Author Wul Chol (Facebook: 100007877380676)
Sent 2020-03-30 19:35:36 UTC
Body Right but its a site that got good pieces that flappy showed me

Author [REDACTED] FACEBOOK USER 1
Sent 2020-03-30 19:36:04 UTC
Body What is is ? Cause I asked him mad times yesterday but he was drunk asl

Author [REDACTED] FACEBOOK USER 1
Sent 2020-03-30 19:36:08 UTC
Body And kept forgetting

Author Wul Chol (Facebook: 100007877380676)
Sent 2020-03-30 19:37:18 UTC
Body I sent it to ur tele

30. CHOL's Facebook account included an instant message conversation between CHOL and FACEBOOK USER 1 on December 14, 2019 where CHOL and FACEBOOK USER 1 discuss "gen".

Author Wul Chol (Facebook: 100007877380676)

Sent 2019-12-14 16:18:46 UTC

Body Yo u tried that gen shit

Author [REDACTED] FACEBOOK USER 1

Sent 2019-12-14 16:19:40 UTC

Body Naw i was busy and my tele fucked up he just sent me the link rn

Author Wul Chol (Facebook: 100007877380676)

Sent 2019-12-14 16:19:58 UTC

Body What link

Author [REDACTED] FACEBOOK USER 1

Sent 2019-12-14 16:22:33 UTC

Body For the gen shit

Author Wul Chol (Facebook: 100007877380676)

Sent 2019-12-14 16:24:08 UTC

Body Oh ight

31. CHOL's Facebook account included instant messages between CHOL and FACEBOOK USER 1 on December 16, 2019 where CHOL and FACEBOOK USER 1 discuss using "gen" to obtain "gitfys" with "bread" in them. In my training and experience, I know that "gitfys" is a term used for gift cards.

Author Wul Chol (Facebook: 100007877380676)

Meta Platforms Business Record

Page 28885

Sent

2019-12-16 21:06:36 UTC

Body I tried the gen shit yesterday its type long

Author FACEBOOK USER 1

Sent 2019-12-16 21:06:50 UTC

Body lk bra its confusing asf to me

Author Wul Chol (Facebook: 100007877380676)

Sent 2019-12-16 21:07:38 UTC

Body Nah its easy but it takes a min to get gitfys with bread in em

Author FACEBOOK USER 1

Sent 2019-12-16 21:07:56 UTC

Body It hit for u or naw

Author Wul Chol (Facebook: 100007877380676)

Sent 2019-12-16 21:09:48 UTC

Body Naw the numbers gout gave me dead and u need good numbers to get good giftys one of gout mans on tele got the gen sauce down like crazy

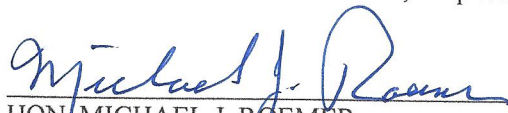
32. Based on the foregoing, I respectfully submit that there is probable cause to believe that WUL ISAAC CHOL did violate Title 18, United States Code, Section 1029(a)(3) in that CHOL did knowingly and with intent to defraud possess 15 or more unauthorized access devices. I respectfully request that the Court therefore issue the attached criminal complaint and an arrest warrant. To allow the arrest warrant to be effectuated, I also request that the Court seal the requested criminal complaint, this affidavit, and the arrest warrant.

Respectfully submitted,



Bryan Scheiber
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me, telephonically, on Mar. April 3, 2023, 2023



HON. MICHAEL J. ROEMER
UNITED STATES MAGISTRATE JUDGE