unsealed on 2/9/2020 ft

SEALED

FILED

MAR 06 2020

CLERK US DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA
BY DEPUTY

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA,

Plaintiff,

vs.

KIRILL VICTOROVICH FIRSOV

Defendants.

Magistrate Case No. 20MJ1029

COMPLAINT FOR VIOLATION OF Title 18, U.S.C., Secs. 2, 1029(a)(6)(A) and 1029(c)(1)(a)(i) – Aid and Abet Unauthorized Solicitation of Access Devices; Title 18, United States Code, Sections 2, 1028(a)(8) and 1028(b)(1)(A)(i) – Aid and Abet Trafficking in False Authentication Features

(UNDER SEAL)

The undersigned complainant being duly sworn states:

COUNT ONE

From on or about a date unknown through March 4, 2020, in the Southern District of California and elsewhere, defendant Kirill Victorovich FIRSOV, without the authorization of the issuer of access devices belonging to customers of Company A, to wit account names and passwords used to obtain money, goods, services or any other thing of value, knowingly and with intent to defraud, did aid and abet soliciting buyers through the DEER.IO platform with the purpose of offering and selling information regarding said access devices, said conduct affecting interstate and foreign commerce, in violation of 18 U.S.C. §§ 2, 1029(a)(6)(A) and 1029(c)(1)(a)(i).

lacc

COUNT TWO

From on or about a date unknown through March 5, 2020, within the Southern District of California and elsewhere, defendant Kirill Victorovich FIRSOV did knowingly aid and abet trafficking in false or actual authentication features, to wit, names, dates of birth and U.S. Social Security Numbers for G.V. and L.Y., individuals who reside in the Southern District of California, for use in false identification documents, document making implements, or means of identification; the trafficking of the false or actual authentication features was in or affected interstate or foreign commerce; and the offense involved the production or transfer of an identification document, authentication feature, or false identification document that is or appears to be an identification document or authentication feature issued by or under the authority of the United States, specifically, U.S. Social Security Numbers, in violation of Title 18, United States Code, Sections 2, 1028(a)(8) and 1028(b) (1)(A)(i).

The complainant further states that this complaint is based on the attached statement of facts, which is incorporated herein by reference.

Brian Nielsen
Special Agent, Federal Bureau of Investigation

Sworn to before me and subscribed in my presence, this 6 day of March, 2020.

Honorable LINDA LOPEZ
United States Magistrate Judge

PROBABLE CAUSE STATEMENT

DEER.IO is a Russian-based cyber platform that allows criminals to purchase access to cyber storefronts on the platform to sell their criminal products or services. DEER.IO started operations as of at least October 2013, and claims to have over 24,000 active shops with sales exceeding $17 million to date. Kirill Victorovich FIRSOV is a Russian cyber hacker, and the administrator of the DEER.IO cyber platform. FIRSOV not only managed the platform, he also advertised it on other cyber forums, which catered to hackers.

DEER.IO virtual stores offer for sale a variety of hacked and/or compromised U.S. and international financial and corporate data, Personally Identifiable Information (PII), and compromised user accounts from many U.S. companies. Individuals can also buy computer files, financial information, PII, and usernames and passwords taken from computers infected with malicious software (malware) located both in the U.S. and abroad. Thus far, law enforcement has found no legitimate business advertising its services and/or products through a DEER.IO storefront. Store operators and customers access the storefront via the Internet. Specifically, in this case, the FBI made purchases from the Southern District of California, from DEER.IO storefronts hosted on Russian servers.

The FBI's review of approximately 250 DEER.IO storefronts reveals thousands of compromised accounts posted for sale via this platform and its customers' storefronts, including videogame accounts (gamer accounts) and PII files containing user names, passwords, U.S. Social Security Numbers, dates of birth, and victim addresses. These victims are largely located in Europe and the United States, including victims in the Southern District of California.

The DEER.IO platform offers a turnkey online storefront design and hosting platform, from which cybercriminals can advertise and sell their products (such as

harvested credentials and hacked servers) and services (such as assistance performing a panoply of cyber hacking activities). The DEER.IO online stores are maintained on Russian-controlled infrastructure, which is insulated from U.S. law enforcement. The DEER.IO platform provides shop owners with an easy-to-use interface that allows for the automated purchase and delivery of criminal goods and services.

Once shop access is purchased via the DEER.IO platform, the site then guides the newly-minted shop owner through an automated set-up to upload the products and services on offer through the shop and configure crypto-currency wallets to collect payments for the purchased products and/or services.

A cybercriminal who wants to sell contraband or offer criminal services through DEER.IO can purchase a storefront directly from the DEER.IO website for 800 Rubles (approximately $12.50) per month. The monthly fee is payable by Bitcoin or a variety of online Russian payment methods such as WebMoney, a Russian based money transfer system similar to PayPal.

The shop owner has the option to purchase a storefront name linked to the DEER.IO domain or one of its subdomains, like DEER.ST, DEER.IS or DEER.EE (e.g., https://[SHOP NAME].deer.io, such as ONLYFB.DEER.IO, SHIKISHOP.DEER.IO and SELLACCSS.DEER.IS), or a custom name (e.g., https://[SHOP NAME], such as SQLBAZAR.SHOP and ISIS.RENTS.HOUSE), which directs the prospective buyer to the storefront infrastructure hosted on DEER.IO.

A cybercriminal who wants to purchase from storefronts on the DEER.IO platform can use a web browser to navigate to the DEER.IO domain, which resolves to DEER.IO storefronts. DEER.IO contains a search function, so individuals can search for hacked accounts from specific companies or PII from specific countries, or the user can navigate through the platform scanning stores advertising a wide

array of hacked accounts or cyber criminal services for sale. Purchases are conducted using cryptocurrency, such as Bitcoin, or through Russian-based money transfer systems.

On or about March 4, 2020, the FBI purchased approximately 1,100 gamer accounts from the DEER.IO store ACCOUNTS-MARKET.DEER.IS for under $20 in Bitcoin. Once payment was complete, the FBI obtained the gamer accounts, including the user name and password for each account. Out of the 1,100 gamer accounts, 249 accounts were hacked Company A accounts. Company A confirmed that if a hacker gains access to the user name and password of a user account, that hacker can use that account. A gamer account provides access to the user's entire media library is contained within the account. The accounts often have linked payment methods, so the hacker could use the linked payment method to make additional purchases on the account. Some users also have subscription-based services attached to their gamer accounts.

Company A is located in San Diego, California. Company A operates interactive video gaming platforms, and sells related products and services. Like other video gaming platforms, Company A users have individual gamer accounts protected by user names and passwords.

On or about March 5, 2020, the FBI purchased approximately 999 individual PII accounts from the DEER.IO store SHIKISHOP.DEER.IS for approximately $170 in Bitcoin. On that same date, the FBI purchased approximately 2,650 individual PII accounts from the DEER.IO store SHIKISHOP.DEER.IS for approximately $522 in Bitcoin. From those identities, the FBI identified names, dates of birth and U.S. Social security numbers for multiple individuals who reside in San Diego County, including G.V. and L.Y.

All of these purchases were made by the FBI in San Diego, California from stores on the DEER.IO platform, which is maintained on Russian servers.

REQUEST FOR SEALING

It is respectfully requested that this Court issue an order sealing, until further order of this Court, this complaint and probable cause statement. Sealing is necessary, because premature disclosure of the contents of this probable cause statement and related documents may cause the defendant and/or additional witnesses to this offense to flee, would cause destruction of evidence, and would have a negative impact on this continuing investigation.