NO HONOR AMONG TROLL FACES: THE LATEST LAWFARE AGAINST PRIGOZHIN'S TROLLS

Yesterday, Treasury sanctioned four people for election interference. Rudy Giuliani associate Andreii Derkach has gotten most of the attention. But Treasury also sanctioned three people associated with Yevgeniy Prigozhin's troll operation.

> Today, Treasury also designated three IRA actors pursuant to E.O. 13694, as amended by E.O. 13757, and E.O. 13848 for having acted or purported to act for or on behalf of, directly or indirectly, the IRA, an entity designated pursuant to E.O. 13694, as amended, and E.O. 13848. Russian nationals Artem Lifshits, Anton Andreyev, and Darya Aslanova, as employees of the IRA, supported the IRA's cryptocurrency accounts. The IRA uses cryptocurrency to fund activities in furtherance of their ongoing malign influence operations around the world.

The identifying information announcement provides not just passport and date of birth information (which is normal), but for two of the sanctioned individuals, it includes 17 and 6 crypto-currency addresses, respectively.

> ANDREYEV, Anton Nikolaeyvich (Cyrillic: АНДРЕЕВ, Антон Николаевич), 9 3 Bloshevikov Prospect Apt 35, Saint Petersburg, Russia; DOB 03 Mar 1985; POB Saint Petersburg, Russia; nationality Russia; Email Address antonandreyv@gmail.com; Gender Male;
>
> Digital Currency Address – XBT

1Fz29BQp82pE3vXXcsZoMNQ3KSHfMzfMe3;

alt. Digital Currency Address – XBT
1AeSq93WDNdLoEJ92sex7T8xQZoYYm8BtS;

alt. Digital Currency Address – XBT
1AoxtfiBQ22DvbhqAN9Ctb8sULMRhrdwTr;

alt. Digital Currency Address – XBT
18Qj1THHuETfYhuRDZycXJbWwDMGw73Poa;

alt. Digital Currency Address – XBT
1MnbhWe5wr7Ut45ReyQsm96PwnM9jD7KaH;

alt. Digital Currency Address – XBT
1DYFJ6CuBvrxyoQSuBzVsNcetY9tvdsrag;

alt. Digital Currency Address – XBT
15Pt4NwZaUmMUwS2bQbyyncc7mzgWShtv8;

alt. Digital Currency Address – XBT
1PhqQpaGCrqSxQ6QDXcv14QCd1U98Zp34E;

alt. Digital Currency Address – XBT
13YBQr2Cp1YY3xqq2qngaPb7ca1o4ugeq6;

alt. Digital Currency Address – XBT
1KgudqxMfYaGzqAA7MS4DcsqejtMteqhix;

alt. Digital Currency Address – XBT
1FRyL9gmFGbzfYDAB4iY9836DJe3KSnjP9;

alt. Digital Currency Address – XBT
1DbShx4r8i2XesthoDBf5EkYWz5dsKEusV;

Digital Currency Address – ETH
0x8576acc5c05d6ce88f4e49bf65bdf0c62f9135
3c;

Phone Number 79315403678;

Digital Currency Address – LTC
LWnbjLYUfqeokfbWM4FcU7uk2FP2DSxuWS;

alt. Digital Currency Address – LTC
LaYUy1DGfVSuSF5KbPhbLrm8kRotqiwUJn;

Digital Currency Address – ZEC
t1WSKwCDL1QYRRUrCCknEs5tDLhtGVYu9KM;

Digital Currency Address – BSV
12sjrrhoFEsedNRhtgwvvRqjFTh8fZTDX9;
Passport 4005504207 (Russia)

> (individual) [CYBER2] [ELECTION-EO13848].
>
> [snip]
>
> LIFSHITS, Artem Mikhaylovich (Cyrillic: ЛИФШИЦ, Артем Михайлович), Primorsky Prospect 159, Saint Petersburg 197374, Russia; DOB 26 Dec 1992; nationality Russia; Email Address mycryptodeals@yandex.ru; alt. Email Address artemlv@hotmail.com; Gender Male;
>
> Digital Currency Address – XBT 12udabs2TkX7NXCSj6KpqXfakjE52ZPLhz;
>
> alt. Digital Currency Address – XBT 1DT3tenf14cxz9WFNxmYrXFbB6TFiVWA9U;
>
> Digital Currency Address – ETH 0x901bb9583b24d97e995513c6778dc6888ab6870e;
>
> alt. Digital Currency Address – ETH 0xa7e5d5a720f06526557c513402f2e6b5fa20b00;
>
> Phone Number 79110354982;
>
> Digital Currency Address – LTC Leo3j36nn1JcsUQruytQhFUdCdCH5YHMR3;
>
> Digital Currency Address – DASH Xs3vzQmNvAxRa3Xo8XzQqUb3BMgb9EogF4; Passport 719032284 (individual) [CYBER2] [ELECTION-EO13848].

Yesterday, EDVA also announced a single criminal charge of conspiracy to commit wire fraud against one of the sanctioned people, Artem Lifshits, who in 2017 was head of the "Translator Department [or Project]," which is what the troll project focusing on the US is called. As the excerpt above notes, Lifshits actually got fewer of his cryptocurrency accounts sanctioned than another of the targets, Anton Andreyev.

I'd like to look at how the criminal complaint

complements the two other sets of charges against Prigozhin's troll operation, the indictment against 13 of the actual trolls as well as some of the companies involved (here's a very long post on that prosecution), and Prigozhin himself and a complaint against one of the accountants involved, Elena Alekseevna Khusyaynova (here's my post on that). Along with renewing and fleshing out the case against Prigozhin, the complaint may be an effort to sow discord within Prigozhin's operation, by alerting him that some of his employees may be helping themselves to company troll funds.

The affidavit by a Secret Service Agent supporting the complaint incorporates the other two legal actions and includes them as exhibits to this charge. It even includes a footnote explaining why DOJ dismissed the charges against Prigozhin's shell companies.

> On March 16, 2020, the United States dismissed Concord Management and Consulting LLC from the Indictment. Concord "availed itself of the Court's jurisdiction to obtain discovery from the United States . . . while positioning itself to evade any real obligations or responsibility," even refusing to produce a corporate representative despite "appearing" through counsel. Mot. to Dismiss Concord Defs., 2, 6, United States v. Internet Research Agency, et. al, 1:18-cr-32 (DLF) (D.D.C. Mar. 16, 2020). In light of the defendant's conduct, the United States dismissed these parties from the Indictment, stating substantial federal interests were no longer served by continuing the proceedings against them. See id. at 9. The Indictment remains pending and active as to thirteen named individual defendants and the IRA.

After some introductory matter, the affidavit:

- Describes the Lakhta

disinformation project generally, including a brief overview of its attempts to sow discord between December 2016 through May 2018, incorporating some but not all of the examples from the Khusyaynova complaint, and adding a few new ones, including three paragraphs on use, starting in July 2019 of a cover company located in Accra, Ghana.

- Describes how in October 2018 the Secret Service started investigating the role of cryptocurrency in the operation.
- Explains that Lifshits served as head of the Translator Department.
- Describes how Lifshits transferred money from a BTC account opened using the stolen identity of "T.W." to his own personal account, the central allegation of wire fraud laid out in the indictment.

The basic proof accusing Lifshits of using T.B.'s stolen identity to open a Bitcoin account that he then used to transfer money into his own account relies on very basic metadata analysis obtained using legal process:

- Evidence backing the selectors of Lifshits tie to his biological person and

one of the cryptocurrency accounts he transferred money into (including two other Internet troll employees' address book entries with his phone number, one of which referred to him as "Troll Face").

- Evidence showing Lifshits applying to Project Lakhta in July 2015 and appearing on rosters of Project Lakhta employees dated January 28, 2017 to October 26, 2017.
- A description of finding order confirmations in the known IRA email, allforusa, from a criminal marketplace that sold fraudulent identities (this might be Richard Pinedo's site).
- Two paragraphs describing interviews with T.W. and another identity theft victim, T.B., in which they said he had never owned any cryptocurrency themselves and had not authorized anyone to do so on their behalf.
- IP analysis showing Lifshits accessing cryptocurrency addresses (including his own) from an IRA IP address, as well as from a US-based account set up using a

stolen identity but controlled by IRA.

- IP address analysis showing him accessing the T.W. cryptocurrency account at the same time he accessed one of his own accounts, into which he transferred funds.
- User Agent String analysis showing those accounts being accessed by the same browser.
- IP analysis establishing venue in EDVA via some AWS servers.

In other words, the complaint, after invoking the two other legal actions against IRA and Prigozhin, finds one manager amid Prigozhin's employees and shows some very basic metadata evidence — relying on neither intelligence nor some of the more sophisticated blockchain analysis the US government would like to hide — to accuse the manager, Lifshits, of wire fraud because of a financial transfer involving the stolen identity of an American.

There are two interesting aspects of the complaint, besides the way it slowly builds the case against Prigozhin via interlocking accusations.

First, a key passage of all this describes that Lifshits made this transfer "for personal gain."

> 60. On or about December 29, 2017, LIFSHITS accessed and used the T.W. Exchange 1 Account to conduct an electronic transfer of funds from the T.W. Exchange 1 Account to his personal Exchange 3 account. This transaction is publicly viewable on the Bitcoin blockchain and USSS confirmed its

> existence through other investigative means.
>
> 61. On or about December 29, 2017, LIFSHITS used United States IP Address 1 at 15:35 UTC to access his Exchange 3 account. Then, three minutes later, he used the same IP address to access the T.W. Exchange 1 Account. This is on the same day that the T.W. Exchange 1 Account sent an electronic funds transfer to LIFSHITS' Exchange 3 account.
>
> 62. With this transaction, LIFSHITS (1) intentionally and voluntarily devised or participated in a scheme to defraud – as evidenced by controlling and using a fraudulent cryptocurrency account, and (2) used interstate wire communications to further the fraud – as evidenced by the online cryptocurrency transactions.

It doesn't say, one way or another, whether this was a sanctioned transfer of funds out of an IRA-controlled account or not. The government *may* have used this 34-page affidavit not only to flesh out the case against Prigozhin, but also to reveal that one of his employees is bilking him, effectively stealing trolling funds.

But the complaint also mentions a Co-Conspirator 1, who along with Lifshits bought identities using cryptocurrency.

> Law enforcement obtained a search warrant for the contents of the email account allforusa@yahoo.com, which as stated above is associated with a cryptocurrency account linked to both LIFSHITS and Co-Conspirator 1. During a review of the emails, law enforcement located "Order Confirmation" emails received from an online criminal marketplace that sells fraudulent passports and similar identification

> documents (the "Criminal Marketplace"). These emails corresponded to purchases of United States driver licenses that reflected the real names, addresses, and dates of birth of United States identity theft victims. This type of personally identifiable information is a "means of identification" as defined in Title 18, United States Code, Section 1028(d)(7).

It describes Co-Conspirator 1 as the sole other beneficiary of transfers out of a different IRA trolling account (though also suggests that one of the guys charged in the larger indictment might also be conducting such transfers as well).

> The T.W. Exchange 1 Account reflected debits to several beneficiaries, including accounts registered to LIFSHITS and another known Project Lakhta member ("Co-Conspirator 1"). The IP activity associated with the T.W. Exchange 1 Account also matched the IP address activity of cryptocurrency accounts registered to LIFSHITS and Vladimir Venkov, who is charged in the USAO-DC Indictment.

It then introduces an account based off a different stolen identity, that of T.B., from which funds were transferred into an account controlled by the Co-Conspirator.

> USSS identified a second account, which was hosted at another United States cryptocurrency exchange ("Exchange 2"). The Exchange 2 account was registered to a known Project Lakhta email account, allforusa@yahoo.com (hereinafter the "AllforUSA Exchange 2 Account").7 Project Lakhta members opened the AllforUSA Exchange 2 Account using the identifiers of T.B. According to Exchange 2's records, Project Lakhta members solely funded the AllforUSA

> Exchange 2 Account with an incoming credit from an account also in the name of T.B. at a United States-based financial institution. This credit was used exclusively to fund outgoing payments to a Blockchain wallet that USSS investigators determined was controlled by Co-Conspirator 1.

Now, it may be that the government only introduced Co-Conspirator 1 to establish venue in EDVA (which went through the T.B. account).

But it sure sounds like it is describing Co-Conspirator 1 as engaging in the same kind of transfers from IRA accounts into his own personal accounts that it describes Lifshits as doing.

Perhaps stealing from the troll till is considered part of their official compensation (elsewhere, the complaint cites the salary of Lifshits, so the US government may know the answer). Or perhaps these guys whose cryptocurrency addresses just got published in a US sanction announcement have been stealing from Prigozhin, in which case the US Treasury just provided Prigozhin a lot of hints about how to prove it.