



RANSOMWARE DIARIES

VOLUME 6:

LIE TO ME

BASSTERLORD RANSOMWARE STORY

by **Jon DiMaggio**

Chief Security Strategist

WARNING:

PLEASE DO NOT TRY THIS AT HOME. ENGAGING WITH RANSOMWARE CRIMINALS SHOULD ONLY BE ATTEMPTED BY TRAINED PROFESSIONALS. WHILE IT SEEMS "COOL" TO INTERACT WITH BAD GUYS, DOING SO PUTS YOU AND YOUR EMPLOYER AT GREAT RISK. PLEASE DO NOT ATTEMPT TO EMULATE WHAT YOU SEE IN THIS REPORT UNLESS YOU HAVE THE KNOWLEDGE, EXPERIENCE, AND SKILL SET TO PERFORM SUCH ACTIONS.

THANK YOU!



ABOUT THIS REPORT:

This was difficult to write because I have become fond of Bassterlord (the person, not the criminal) throughout our relationship. I will never be empathetic to the crimes he commits, and I will always do my job and do everything in my power to stop criminals and help law enforcement, regardless of how I feel about the person I am writing about. However, in this case, I would not have published this research publicly if Bassterlord had not called out my work directly. I think it is important to show evidence when making attribution claims, and I hope this report ends any speculation as to whether Bassterlord and Ivan are the same person. I also want to thank Azim Khodjibaev, who collaborated with me and supported me throughout my research while writing this report.



INTRODUCTION

In February of 2023, I contacted an infamous, well-connected hacker known throughout the ransomware community by the moniker "Bassterlord," whom I wrote about extensively in the Ransomware Diaries Volume 2. Over the years, he went by several monikers, including AL3xL7, Fisheye, Sinner911, and Bassterlord, the name which he made infamous throughout the ransomware community. Bassterlord was different than most of the ransomware criminals I have encountered. He was likable, polite, and willing to discuss his story and experiences.

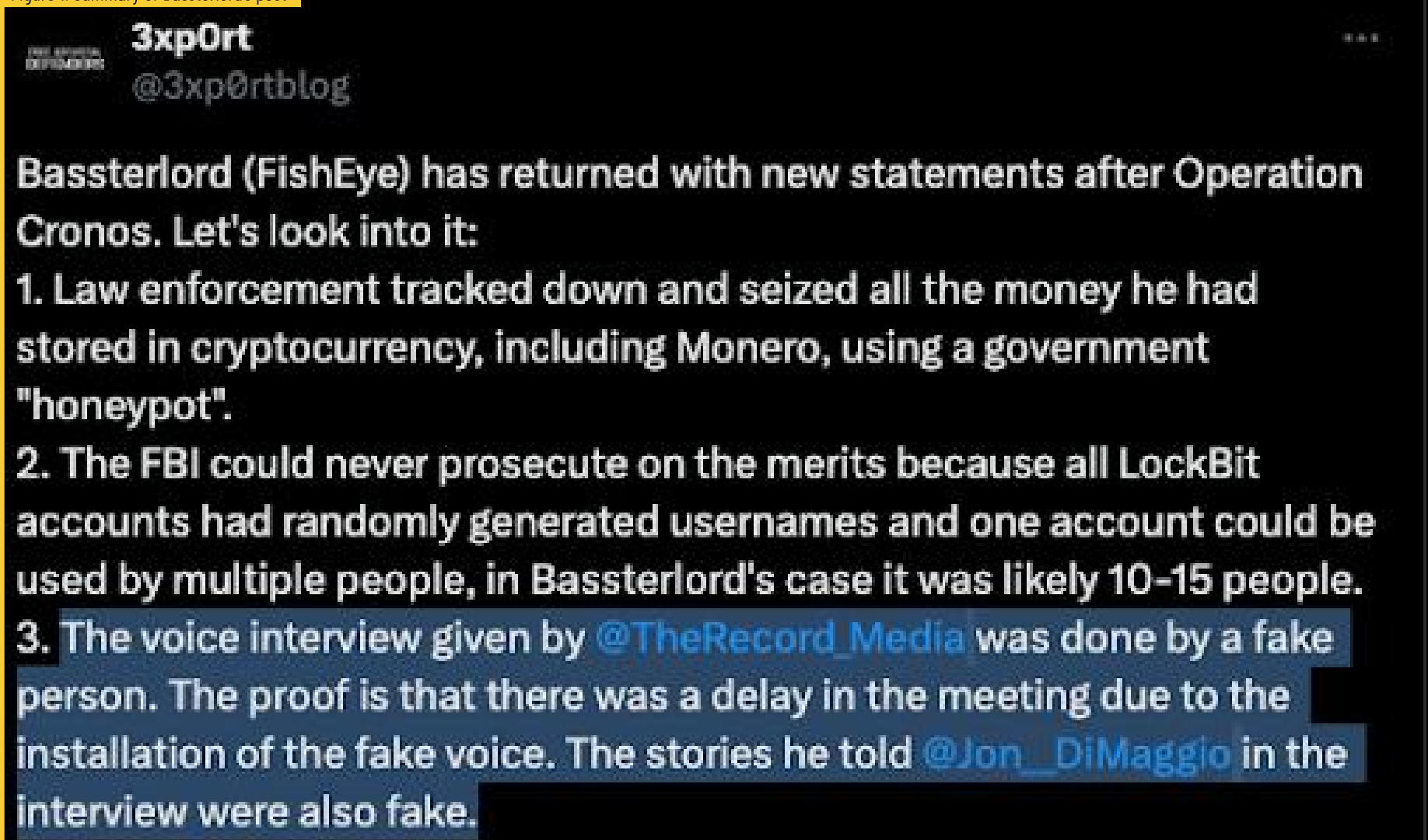
Bassterlord shared how he went from a child born in the center of a war-torn region of Ukraine to a notorious hacker who terrorized companies throughout the world. I told that story already, and it turns out, according to Bassterlord, that it may not be completely true!

In March 2024, Bassterlord posted to a popular dark web forum, proclaiming he fabricated the story he shared with both myself and the Click Here podcast, who also interviewed the hacker previously.

“All stories told during the interview were made up (sorry Jon). From the first to the last one. I should admit that few people believed in them.”
-Bassterlord

3xp0rt, a fellow security researcher, summarized additional points made in Bassterlord's post, seen in **Figure 1**.

Figure 1: Summary of Bassterlord's post



3xp0rt
@3xp0rtblog

Bassterlord (FishEye) has returned with new statements after Operation Cronos. Let's look into it:

1. Law enforcement tracked down and seized all the money he had stored in cryptocurrency, including Monero, using a government "honeypot".
2. The FBI could never prosecute on the merits because all LockBit accounts had randomly generated usernames and one account could be used by multiple people, in Bassterlord's case it was likely 10-15 people.
3. The voice interview given by @TheRecord_Media was done by a fake person. The proof is that there was a delay in the meeting due to the installation of the fake voice. The stories he told @Jon_DiMaggio in the interview were also fake.



Essentially, Bassterlord discredited months of my work and his interview on [Recorded Future News', Click Here](#) podcast. So today, I am addressing his claim to make my own assessment and determine if Bassterlord deceived us both.

To accomplish this, I conducted HUMINT engagements with Bassterlord and his associates, performed extensive OSINT research, and reviewed Bassterlord-related threat data. Then, I compared known events with the Bassterlord persona and the individual named in the Department of Justice (DoJ) indictment to make my assessment.

GUEST OF HONOR ON THE MOST WANTED LIST!

On February 5th, 2024, the United States Department of Justice indicted Bassterlord, and the indictment did not paint a pretty picture. As detailed in the Ransomware Diaries Volume 2, Bassterlord is a hacker who ran the ransomware affiliate group National Hazard Agency (NHA) and has stolen millions from companies worldwide through ransomware extortion crimes. Bassterlord is most notably known for his time working for another big-name criminal operation, the LockBit ransomware gang. While Bassterlord is most known for his criminal operations with LockBit, he has worked with multiple criminal gangs throughout his career, including REvil, Hive, RansomEXX, and Avadon, and has relationships with both BlackCat/AlphV and Hunters International.

More importantly, the Indictment revealed Bassterlord's real name, "Ivan Kondratiev", a.k.a. Ivan Kondratyev (Russian: **Иван Кондратьев**). However, Bassterlord claims law enforcement named the wrong person in the indictment, claiming he is not Ivan Kondratyev but instead purchased Ivan's passport to use as a false identity to avoid arrest. Ivan confirmed the story in an interview shortly after news of the indictment:

“

I just sold an account with a passport to another guy, and now everyone is giving me f*ck for it. I don't give a fuck who this is and what the fuck is going on. Everyone is calling me, asking for something. Some Americans, I don't care what they want.

-Ivan Kondratyev

”

Note: I always do my best to cite any source I use. However, the blog from which the quote above originates appears in [VirusTotal](#) as malicious (one vendor marked it as phishing). For that reason, I am unable to include the citation. However, if you still want to view the blog, at your discretion, understanding it's marked malicious, you can search the blog author's handle, "[@greedywillfuckurmum](#)," and find the blog on his teletype page. The blog may be marked phishing due to the subject matter, not because it's malicious, but I must err on the side of caution (and so should you).

I suspect Bassterlord concocted this story to create plausible deniability, aiming to deflect increased attention from law enforcement. This indictment was a small part of one of the most extensive anti-ransomware operations to date, Operation Cronos, launched by the National Crime Agency (NCA) in February 2024. Unfortunately, like many Russian cybercriminals, Bassterlord is protected from prosecution by the Russian government, making an arrest unlikely unless he leaves the country. Still, Bassterlord put himself in a situation where he will have to look over his shoulder for the rest of his life.



High-profile ransomware attackers often attract special attention from the Russian government, particularly after being named by multi-agency law enforcement organizations and possessing large sums of unspent money hidden in plain sight. However, Bassterlord claims the US government seized all the profit he made during his criminal operations. Below is an image of the federal indictment and OFAC sanctions placed against Bassterlord.

The following individuals have been added to OFAC's SDN List:

KONDRATIEV, Ivan Gennadievich (Cyrillic: КОНДРАТЬЕВ, Иван Геннадьевич) (a.k.a. KONDRATEV, Ivan; a.k.a. KONDRATYEV, Ivan; a.k.a. "@AL3XL7"; a.k.a. "@BASSTERLORD"; a.k.a. "@BASSTERLORD 0170742922"; a.k.a. "@SINNER6546"; a.k.a. "@SINNER911"; a.k.a. "BASSTERLORD"; a.k.a. "EDITOR"; a.k.a. "FISHEYE"; a.k.a. "INVESTORLIFE1"; a.k.a. "JACKROCK#3337"; a.k.a. "SIN998A"), Novomokovsk, Russia; DOB 08 Apr 1996; nationality Russia; Email Address sinner4iter@gmail.com; Gender Male; Digital Currency Address - XBT bc1q5jqgm7nvrhaw2rh2vk0dk8e4gg5g373g0vz07r; alt. Digital Currency Address - XBT 32pTjxTNI7snk8sodrgfmdKao3DEn1nVJM; alt. Digital Currency Address - XBT 15cRqR3TXS1JehBGWERuxFE8NhWZzfoeeU; alt. Digital Currency Address - XBT 1A7SKE2dQtezLktCY8peLsdAtkqxV9r1dC; alt. Digital Currency Address - XBT bc1q8ew45w2agdffrnwp6adt2gqrc9n4mkev9ns29c; alt. Digital Currency Address - XBT bc1qagp0gy58v8hqvw4p2wsphcxg067rrppp45hexr; alt. Digital Currency Address - XBT bc1qn6segn8km4nfdp9vvueu6msfjsaxaqgun9h60n9; alt. Digital Currency Address - XBT bc1qx9upga7f09tsetqf78wa3qrmcjar58mkwz6ng6; Digital Currency Address - ETH 0xf3701f445b6bdafedbca97d1e477357839e4120d; Secondary sanctions risk: Ukraine-/Russia-Related Sanctions Regulations, 31 CFR 589.201; Passport 7019934211 (Russia) (individual) [CYBER2].

Figure 2: DoJ indictment and OFAC Sanctions

NEVER GIVE UP THE CON

Shortly after Bassterlord's indictment, and just before his post claiming the NCA charged the wrong person, I received a message on X (Formerly Twitter) directing me to the blog mentioned earlier, written by **@greedywillfuckurmum**:

Ashuski
@ai87610
Joined March 2024
Not followed by anyone you're following

Ashuski @ai87610 · Mar 10
teletype.in/@greedywillfuc...
#bassterlord

Mar 10, 2024, 6:55 PM

He added that he sold the account and the passport photo for 50,000 rubles, which is significantly higher than the average market rates. According to Kondratyev, the deal took place back in 2020, when an unknown person contacted him on Telegram, looking for "people from Lugansk" ready to sell. At the same time, he admitted that he would write a statement to law enforcement authorities that he had been "drawn into a scheme of deceit".

This is a typical scheme of fraud in Russia when people are tricked out of their documents for verification on the exchange

It's not a Bassterlord

Mar 10, 2024, 6:57 PM

Figure 3: Direct message sent on X about Bassterlord



The sender, “**Ashuski**,” created the account on March 10, 2024, which is also the day it was used to send me the message shown in Figure 3. Notably, the alias “Ashuski” appears to have been created to impersonate my friend and fellow researcher, Azim Khodjibaev, who has an account named “**Ashukuhi**”. Azim and I have conducted extensive research on Bassterlord and collaborated publicly on this topic.

In the blog, the author interviews Ivan and details his claim that the Department of Justice (DoJ) identified and indicted the wrong person. The blog also provides images of messages between Ivan and the blog author. In the communications, Ivan tells his side of the story, explaining that he sold his identity for financial gain and has no idea who Bassterlord is or why he is being indicted. If you believe Ivan, he is an innocent man completely blindsided by the charges against him. Of course, this story is not true. Still, to be fair, I need to assess his claim.

THE ASSESSMENT

Next, let’s compare the details from my research and my conversations directly with Bassterlord against details of Ivan Kondratiev’s life. My interviews took place before the indictment, and many cyber-related artifacts and forum posts dating back to 2019 support the details and events Bassterlord shared with me, leaving much information to review. To begin, let’s start with something basic... his name.

SAY MY NAME!

Bassterlord goes by many aliases, including FishEye, AL3XL7, and Sinner, among others listed in the [OFAC Specially Designated Nationals List](#). Though he now denies being Ivan Kondratiev, this wasn’t always the case. Before the indictment and sanctions, Bassterlord often introduced himself as “Ivan.” He used this name with me, with the researcher Azim Khodjibaev, and even in Bassterlord’s public interview on the [Click Here](#) podcast.

“**Click Here**”: What would you like us to call you?

Bassterlord: **Let’s just simply use the name Ivan** It’s a pretty popular name, and I’m more used to it.

Figure 4: Transcript from Bassterlord interview with Click Here demonstrating Bassterlord’s use of the name Ivan

I didn’t realize Ivan was Bassterlord’s real name at the time. In hindsight, how carelessly he used his real-world first name is surprising. Bassterlord’s lack of discretion regarding his actual first name is now apparent. This was a terrible OPSEC decision! Bassterlord believed no one would ever obtain his real-world identity, and now that he is deanonymized and his name is Ivan, I am sure he regrets the decision. Knowing Bassterlord, I believe he thought no one would ever believe he would use his own name in interviews with researchers and the media. Using his real first name also provides deniability because no one would do that if they thought they would get caught. Now that we know his name is Ivan, let’s address where Bassterlord and Ivan lived.



THERE'S NO PLACE LIKE HOME

During one of our first engagements, Bassterlord told me, "I used to live in Luhansk (Ukraine) and more recently moved to Russia." This aligns with the information in the indictment related to Ivan Kondratyev.

b. KONDRATYEV was a citizen of the Russian Federation and resided in either Ukraine or the Russian Federation.

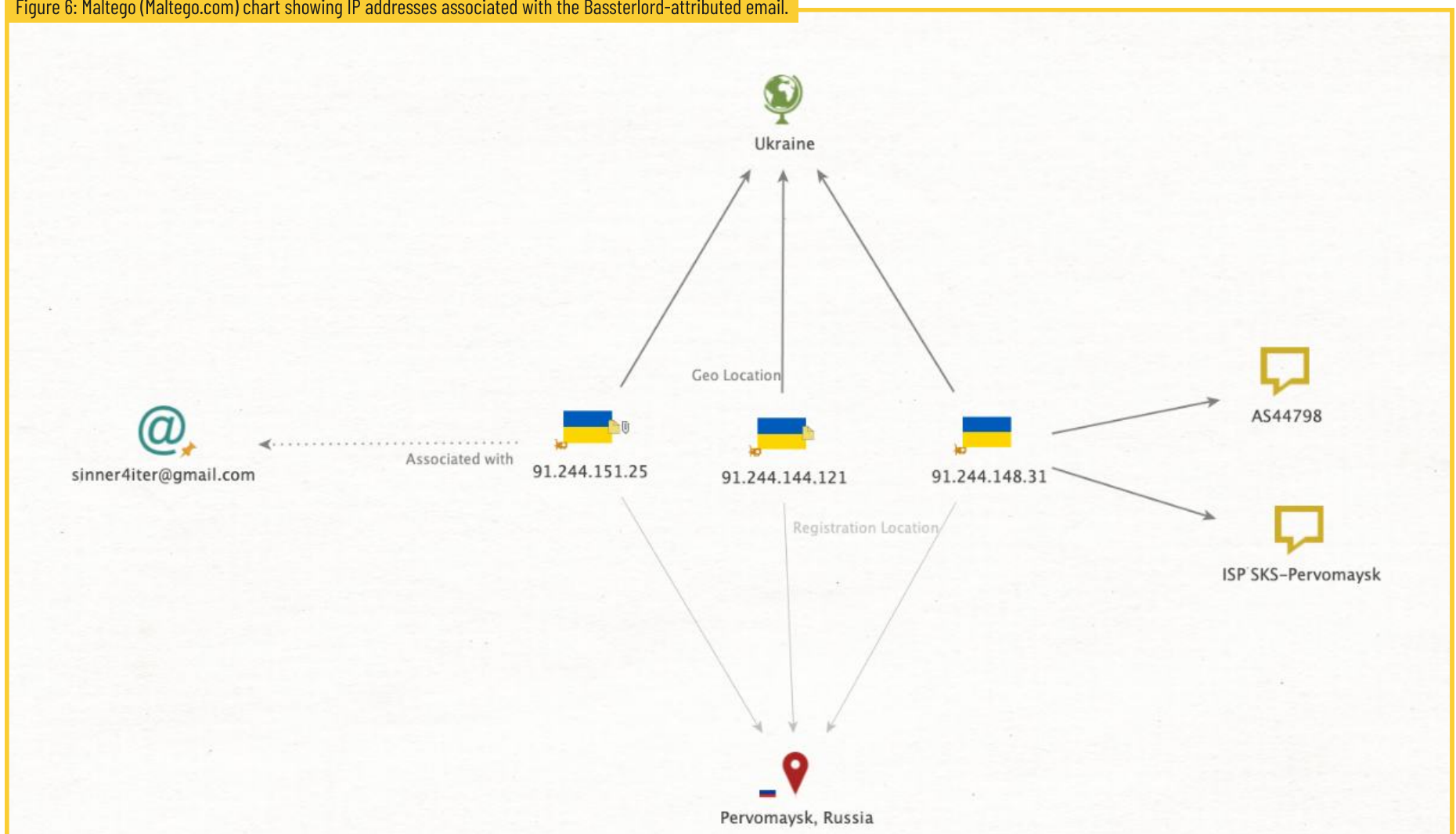
Figure 5: Segment from DoJ indictment referencing the living locations of Ivan Kondratyev.

To discover more information, I went through the accounts and aliases detailed in the indictment and sanctions to locate the region where the accounts were accessed. I took each indicator (account or alias) and searched across dark web data derived from information stealers and database breaches. I identified several of Ivan's accounts within stolen/leaked data and identified the IP addresses used to access each account captured when the data was stolen. An example of the data I retrieved can be seen below:

```
"email_address":
"sinner4iter@gmail.com",
"ipaddress": "91.244.151.25",
"password": "1s5b8c9r",
"indexed": "2018-05-04"
```

Then, I cross-referenced the IP addresses used to log into the account and removed all proxy/VPN-related IP addresses. When I was done, I had three high-fidelity IP addresses used to access Ivan-related accounts. The geolocation of each showed the IP addresses were located in Ukraine and registered to a Russia-based ISP:

Figure 6: Maltego (Maltego.com) chart showing IP addresses associated with the Bassterlord-attributed email.



These IP addresses were obtained (stolen) between 2018 and 2021 when Bassterlord claimed to have resided in Ukraine. Furthermore, based on information associated with the email account and the geographical location (Geolocation) of each IP address linked to Ivan's accounts, all the IPs were in a region within the **Luhansk People's Republic** (LPR), precisely where Bassterlord told me he grew up. Based on this information, I believe that Bassterlord told me the truth during our previous interview regarding his upbringing and the place he called home.

The information I found through stolen data related to Ivan also provided insight into his views of the United States. As seen below, Ivan previously used the sinner4iter email address to register the X account "it9111".

```
"email_address":
"sinner4iter@gmail.com",
"username": "it9111",
"indexed": "2023-03-31"
```

Security researcher Baptiste Robert previously mentioned this X account as well, noting the profile information included the location "Bryanka, Luhansk Oblast, Ukraine." Further, the "it9111" account only followed two other accounts, one of which is purposed to notify residents of the Luhansk region of Ukraine of military events, such as bombings and missile attacks. Many of the posts detailed military events where Ukrainian forces used American-supplied weapons.

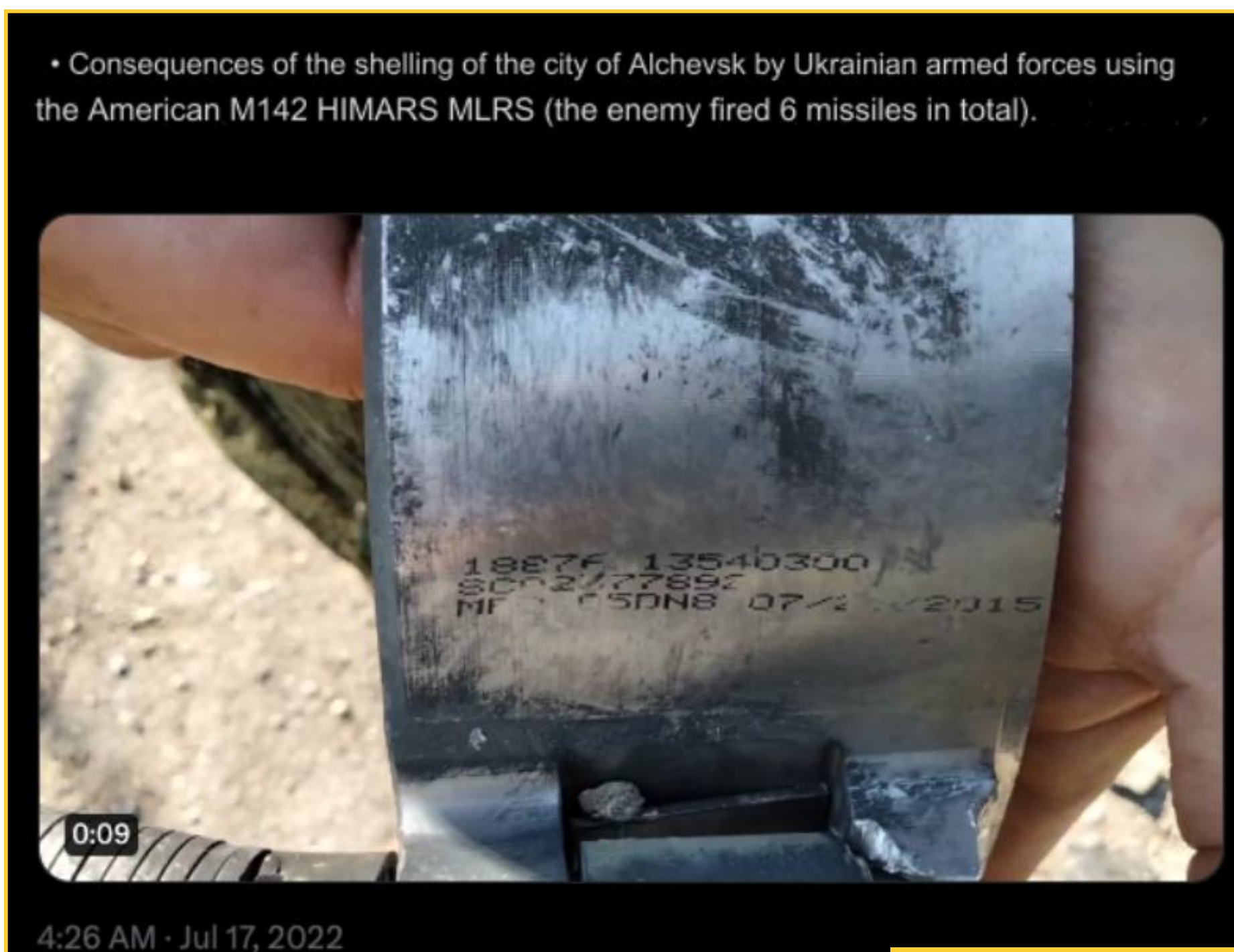


Figure 7: Post referencing US weapons used by Ukraine.



However, instead of discussing the surrounding events, such as the Russian invasion that began in 2014, it claims that Ukraine used US weapons to conduct a “genocide of Russians.” This shows another similarity in the political alignment and beliefs shared between Bassterlord and Ivan. Both personas shared the same anti-US opinions that Bassterlord communicated throughout our relationship. To be fair, Bassterlord never talked about genocide or killing anyone and always respected that we have different views, never making it personal. While circumstantial, these minor similarities, and other evidence support the idea that Bassterlord and Ivan share many similarities in location and personal beliefs.

IVAN, THE BAD ASS DESIGNER

When I first began engaging Bassterlord, we discussed many topics about his life. During the early conversations, Bassterlord told me about his career endeavors outside of ransomware, which included designing and creating graphic images for a clothing company that operated out of Russia.

“**Just so you understand, I was living on 20k rubles a month. Before that I worked as a freelance designer. By the way an interesting fact, half images on children’s and adult clothing in 2019 in Russia were drawn by me =D**
-Bassterlord”

At the time, I was not sure this information would be relevant if it were even true, and I almost did not include the claim in my reporting. Fortunately, I did, and now, it provides further evidence to attribute Bassterlord and Ivan Kondratyev.

To explain, I created **Figure 8** below, which you can use to follow along as I walk through my analysis.

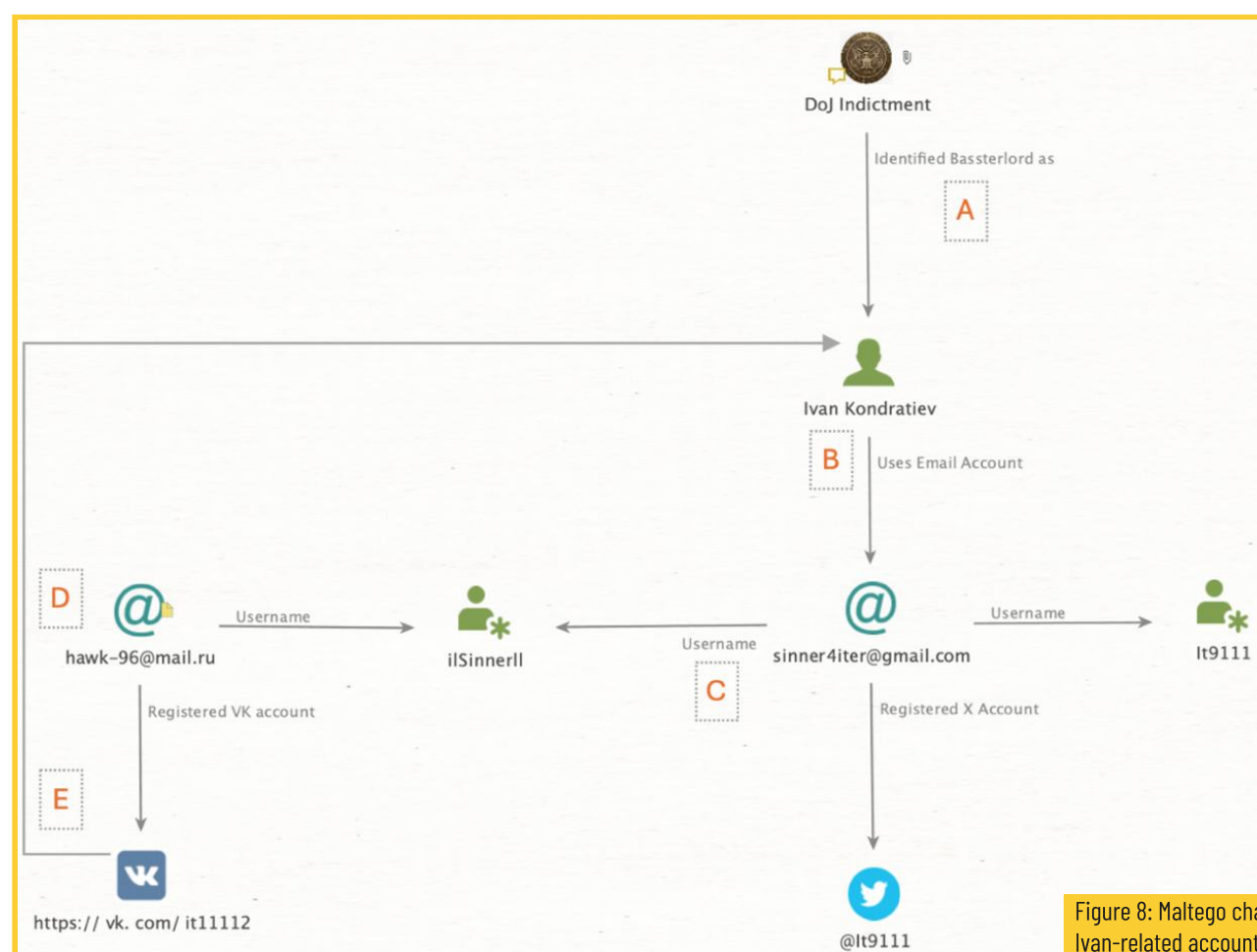


Figure 8: Maltego chart showing links to Bassterlord and Ivan-related accounts (Maltego.com)



- 1 Ivan Kondratyev was named as Bassterlord by law enforcement and OFAC
- 2 OFAC sanctions attribute the email address Sinner4iter[@]gmail.com to Ivan Kondratyev.
- 3 The Sinner4iter email address is used to register several accounts with usernames It9111 and ilSinnerll, amongst others.

Record #1:

```
"userid": "4630416",
"email_address": "Sinner4iter[ @ ]gmail.com",
"username": "ilSinnerll",
```

Record #2:

```
"email_address": "sinner4iter[ @ ]gmail.com",
"username": "It9111",
```

- 4 The username ilSinnerll is also associated with the email "hawk-96[@]mail.ru".

Record #3:

```
"email_address": "hawk-96[ @ ]mail.ru",

"username": "ilsinnerll",
"IP address": "91.244.148.31",
"fullname": "Ivan Kondratyev",
"city": "Braynka",
"state": "Lughansk",
"country": "UA",
"postcode": "94100",
"indexed": "2020-11-18"
```

- 5 The email address hawk-96[@]mail.ru is used to register VK account "it911112," similarly themed to Ivan's X account.

Taking a closer look into the "it911112" VK account, it showed that Ivan used his real name "Ivan v" to register the account, which is tagged as "Personal designer" and is a member of the VK group "creative9111", which is used to sell clothing to a primarily Russian customer base.




Figure 9: "it911112" VK account details showing links to Ivan.



I looked for posts within the group associated with Ivan and found the below message wishing Ivan a happy birthday. The group moderator made the birthday post on April 8th, the exact date of birth mentioned in the Bassterlord-related OFAC sanctions.

Figure 10: Post to Ivan wishing him a happy birthday on 8 April, matching the information associated with Bassterlord identified in OFAC sanctions.



KNITTED FABRIC (wholesale knitted fabric)
8 Apr 2020

Congratulations to our admin, the designer of our prints, and also to my beloved brother Ivan <https://vk.com/it11112> Happy birthday.
Thanks to him, our TRIKLOTNO is successfully developing, growing and gaining new clients.
Thank you my beloved bro

SPECIALLY DESIGNATED NATIONALS LIST UPDATE

The following individuals have been added to OFAC's SDN List:

KONDRATIEV, Ivan Gennadievich (Cyrillic: КОНДРАТЬЕВ, Иван Геннадьевич) (a.k.a. KONDRATEV, Ivan; a.k.a. KONDRATYEV, Ivan; a.k.a. "@AL3XL7"; a.k.a. "@BASSTERLORD"; a.k.a. "@BASSTERLORD 0170742922"; a.k.a. "@SINNER6546"; a.k.a. "@SINNER911"; a.k.a. "BASSTERLORD"; a.k.a. "EDITOR"; a.k.a. "FISHEYE"; a.k.a. "INVESTORLIFE1"; a.k.a. "JACKROCK#3337"; a.k.a. "SIN998A"), Novomokovsk, Russia; **DOB 08 Apr 1996** nationality Russia; Email Address sinner4iter@gmail.com; Gender Male; Digital Currency Address - XBT

Another "it91112" related VK post includes the Telegram address "@sinner9111," which varies by one character from the account "@sinner911," listed by OFAC as a Bassterlord-related Telegram account.

Figure 11: VK group post showing Ivan's accounts in 2017



KNITTED FABRIC (wholesale knitted fabric)
27 Dec 2017

Attention! I provide print rendering services (any print from the site ru.depositphotos.com 1000r, without processing) The price is attached below. (or by the link) [vk.cc/7fPXOs](https://vk.com/it11112)) Contacts for communication (<https://vk.com/it11112> - PAGE BLOCKED UNTIL 01/03/18) so far only mail - hawk-96@mail.ru Skype [xhawkx5](https://www.skype.com/user/xhawkx5) or WhatsApp - +380990450189 (Ivan) Telegram - [@Sinner9111](https://t.me/Sinner9111)

3 Likes, 1 Share, 1.5K Views

Take note of the date the above post was made, **2017**. This is significant since it is associated with the Bassterlord associated accounts, sinner4iter@gmail.com and [@Sinner9111](https://t.me/Sinner9111), because, according to Ivan himself, he did not sell his passport to Bassterlord until **2020**, making the account similarities and associations hard to explain.

“**He (Ivan) added that he sold the account and photo with a passport for 50 thousand rubles, which is significantly higher than the average price. According to Kondratyev, the deal took place back in 2020.**

-@greedywillfuckurmum

”


I understand why Bassterlord lied, but the problem with lying is you must remember your lies. When you lie in cybercrime, you need to make sure you don't reuse accounts or use similar themes when creating accounts used to conduct criminal activity. Most of the VK posts associated with Ivan have now been deleted; however, I found an archived post of one of the graphics Ivan made while working as a designer for a clothing company, shown in **Figure 12**.



Figure 12: Design work created by Ivan

As you can see, **Bassterlord was telling me the truth when he claimed he previously worked as a clothing designer**, and to be honest, he was pretty good at it. More significantly, two OFAC-named designators, "sinner4iter[@]gmail.com" and "[@]Sinner9111", are associated with the VK account linked to both Ivan and clothing design. Of everything Bassterlord told me, I would have expected the graphic designer story to be false. However, with this seemingly insignificant claim, Bassterlord was telling the truth even then.

IT'S ALL IN THE ASCII ART

Even threat actors use social media, and Bassterlord was no exception. Until Bassterlord was indicted, he used the X (formerly Twitter) account @AL3xL7, and the alias "Bassterlord" to post and communicate publicly with researchers and other criminals. Now that I had Ivan's VK account, I looked for similarities between the profiles of both accounts, which can be seen in the figure below.

ID	42241549
Alias	it11112
Name	Ivan
Surname	Kondratiev
Status	\\(ツ)/
Celebrity	No
Date of birth	08.04.1996
Marital status	not specified
Floor	Man
About me	
Languages	Russian, English
Music	Open playlist
Movie	Who am I; Mr. Robot; Citizenfour. Snowden's Truth; The 5th Estate
On the net	No
Quotes	chrome://net-internals/ http://bgp.he.net/cc http://vk.com/upload.php?act=myip https://whoer.net/ru https://www.countryipblocks.net/country_selection.php
City	Lugansk
Was network	April 27th 2016, 12:32:54 Android
Release	0
Has a mobile phone	Yes
Subscribers	199

Figure 13: Comparison of Bassterlord's X account and Ivan's VK account demonstrating the similarities.

Both accounts share the same ASCII art and list Luhansk as their location.



CAN I GET YOUR AUTOGRAPH?

So far, I have presented evidence to support law enforcement's claim that Ivan Kondratyev and Bassterlord are, in fact, the same person; however, from an attribution aspect, it's no smoking gun. The evidence I will share next is much more substantial and allows me to assess with high confidence that the two men are, in fact, the same person.

While I could not publish the information when I wrote the Ransomware Diaries Volume 2, I previously obtained a copy of Bassterlord's passport, in which he redacted most of the identifiable information. The passport originated from Bassterlord himself, and while redacted, he forgot to remove one extremely sensitive piece of information: his signature!



Figure 14: Redacted Bassterport

In **Figure 14**, you can see Bassterlord's signature and year of birth, 1996—the same year Ivan was born. I didn't know his identity at the time, and the story claiming he purchased credentials to assume a third party's identity didn't exist. Still, I thought it would be crazy to share your passport, even if redacted, and I needed to determine if the signature was legitimate. So, after I published the Ransomware Diaries about Bassterlord, I asked him to sign a copy. To my surprise, he agreed and sent me a signed copy of the report. I compared the signatures from the report and his passport, which, as you can see in Figure 14, were both signed by the same person!



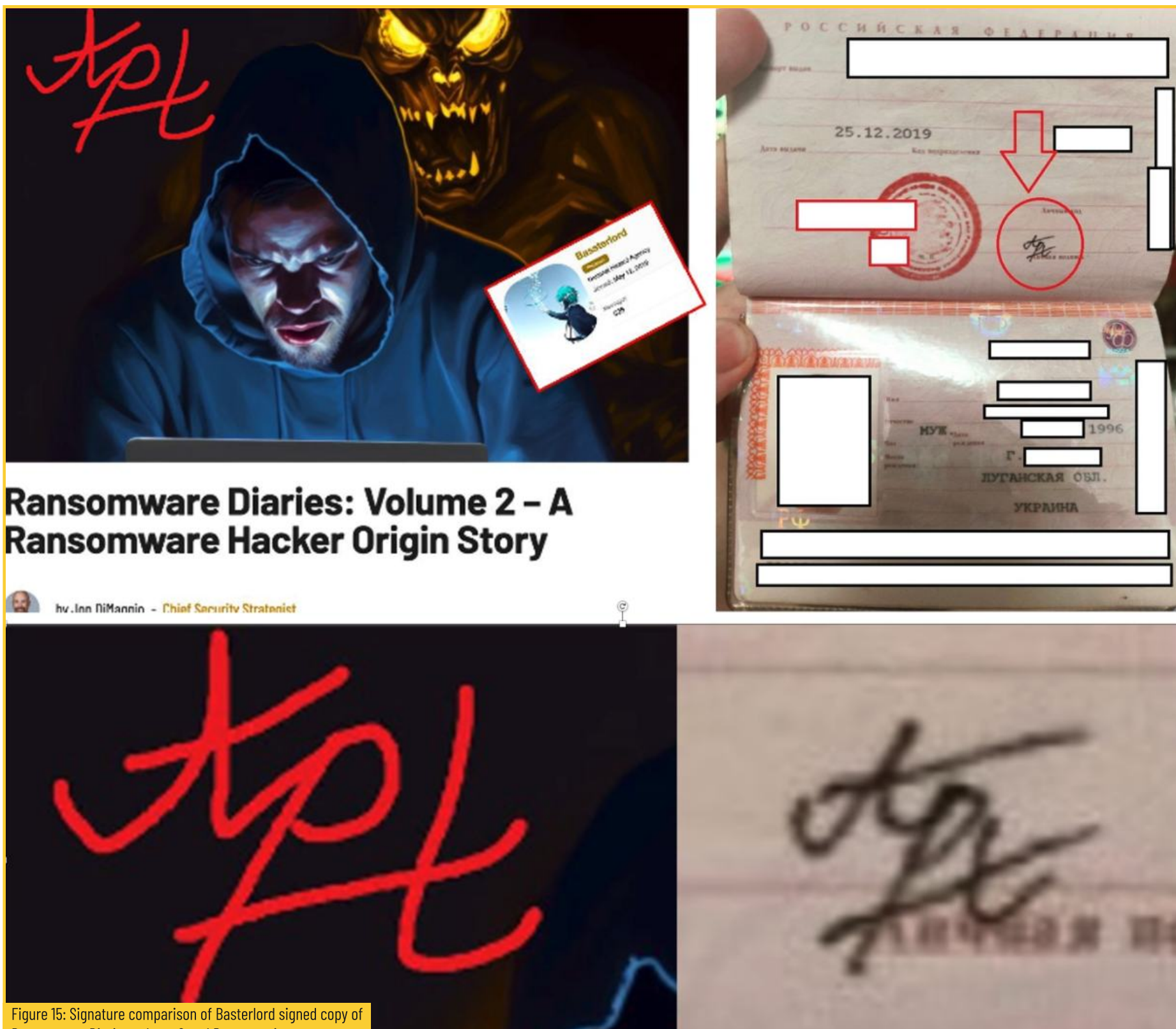


Figure 15: Signature comparison of Basterlord signed copy of Ransomware Diaries volume 2 and Passport signature.

The other significant detail is the date it was issued, December 25th, 2019, a year before when Bassterlord allegedly made the purchase from Ivan Kondratyev. If Bassterlord were not Ivan, how would these signatures match? The passport signature belongs to Ivan; however, Bassterlord's signature five years later, in 2024, is clearly from the same person. Based on this evidence, I can confidently say that **Bassterlord is Ivan Kondratyev**.

CONCLUSION

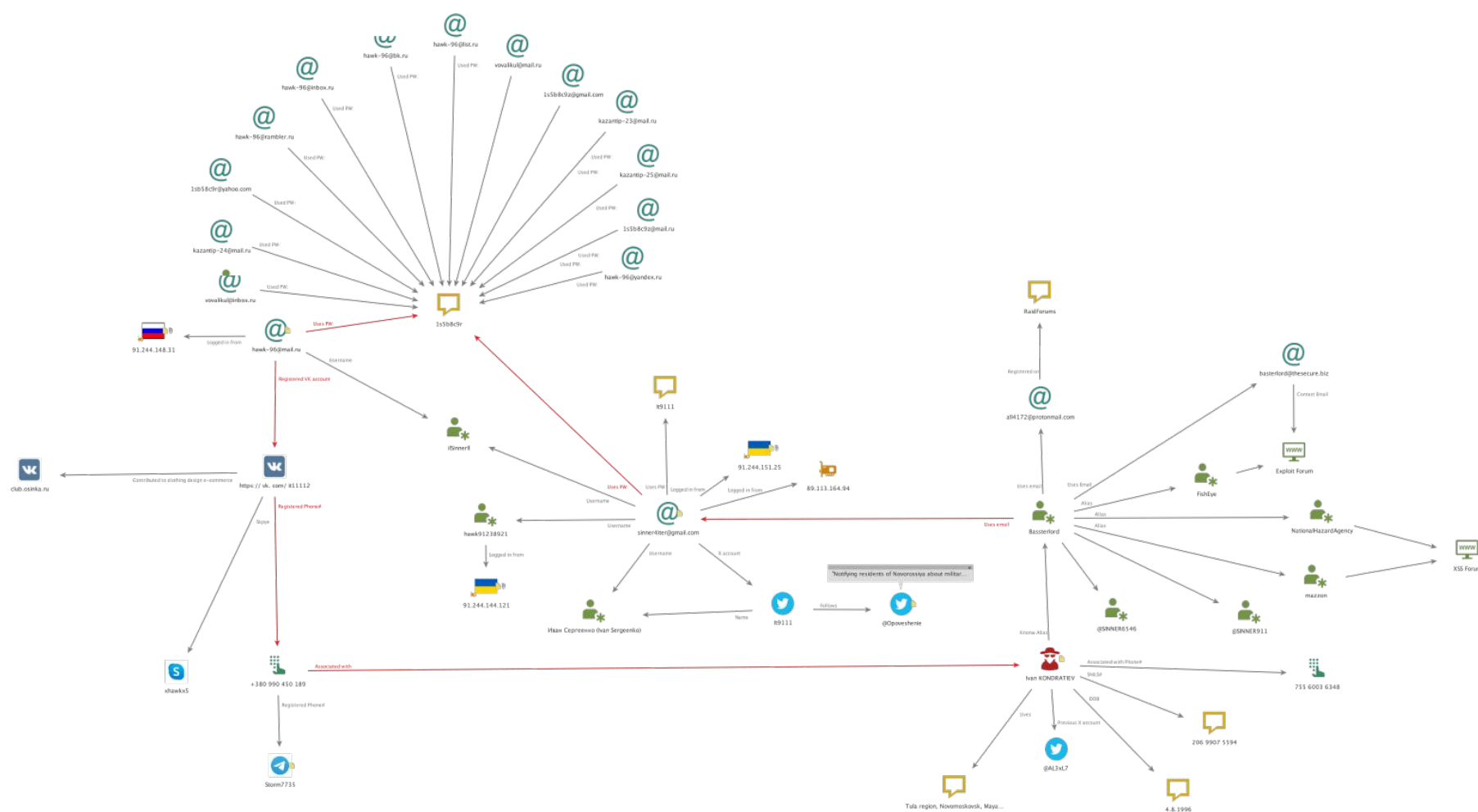
Bassterlord is a smart guy, but he is not a mastermind who planned out his criminal career long before it began, executing an extended, complex scheme to ensure he was never caught. I don't believe that story, nor do I believe he fabricated everything he told me in the Ransomware Diaries Volume 2 or during his interview on the Click Here Podcast.

The more significant problem with this story is if Bassterlord successfully planned and conspired to set up an innocent person to take the fall, why would he admit that now? If it were true, he would have gotten away with placing blame on another person. He would be free while law enforcement pursued the wrong individual. Announcing his plan afterward would only draw more attention to finding the real Bassterlord. Of course, the story is not true, and now, I have evidence to support the attribution.



APPENDIX:

Maltego Diagram:



IOCS:

VALUE	TYPE	NOTE
sinner4iter@gmail.com	Email	Named in OFAC announcement.
hawk-96@mail.ru	Email	Associated with ilSinnerll alias also seen used with the sinner4iter@gmail.com account named in OFAC sanctions.
ilSinnerll	Username	Associated with hawk-96[@]mail.ru and sinner4iter[@]gmail.com
@AL3xL7	Twitter	Bassterlord's former X account



Bassterlord	Alias	Named in OFAC announcement and former alias on Exploit and XSS forums
Editor	Alias	Named in OFAC announcement.
FishEye	Alias	Named in OFAC announcement and former alias on Exploit forum
NationalHazardAgency	Alias	XSS Alias used after updating and changing the "Bassterlord" XSS alias
mazzon	XSS Alias	Bassterlord used this alias in Spring winter - spring 2024 on XSS forum
all4172@protonmail.com	Alias (Raid)	Bassterlord associated mail used to register "Bassterlord" account on RaidForums
basterlord@thesecure.biz	Email	Contact email on Exploit forum
@t9111	Twitter alias	The X account has the same password as sinner4iter@gmail.com named by OFAC
VKontakte group: https://vk[.]com/creative9111	VK Group Account	Ivan's clothing line group page on VK
https://vk[.]com/it11112	VK account	Ivan's VK account (same username as his Twitter account)
Storm7735	Telegram	Same phone # used in https://vk[.]com/it11112
https://ok[.]ru/profile/601223319321	OK Profile	The same phone number use to register X and Telegram Account
xhawkx5	Skype	The same phone number used to register X account and Telegram Account
"+380990450189"	Phone # (VOIP)	Phone # Used for WhatsApp account



@BASSTERLORD 0170742922	Alias	Named in OFAC announcement.
@SINNER6546	Alias	Named in OFAC announcement.
@SINNER6546	Alias	Named in OFAC announcement.
bc1q5jqgm7nvrhaw2rh2vk0dk8e4gg5g373g0vz07r	XBT (Crypto Currency)	Named in OFAC announcement.
32pTjxTNI7snk8sodrgfmdKa o3DEn1nVJM	XBT (Crypto Currency)	Named in OFAC announcement.
15cRqR3TXS1JehBGWERuxFE 8NhWZzfoeeU	XBT (Crypto Currency)	Named in OFAC announcement.
1A7SKE2dQtezLktCY8peLsdAt kqxV9r1dC	XBT (Crypto Currency)	Named in OFAC announcement.
bc1q8ew45w2agdffrnwp6adt 2gqrc9n4mkev9ns29c	XBT (Crypto Currency)	Named in OFAC announcement.
bc1qagp0gy58v8hqvw4p2ws phcxg067rrppp45hexr	XBT (Crypto Currency)	Named in OFAC announcement.
bc1qn6segn8km4nfdp9vueu 6msfjsaxaqqun9h60n9	XBT (Crypto Currency)	Named in OFAC announcement.
bc1qx9upga7f09tsetqf78wa3 qrmcjar58mkwz6ng6	XBT (Crypto Currency)	Named in OFAC announcement.
0xf3701f445b6bdafedbca97d 1e477357839e4120d	ETH (Crypto Currency)	Named in OFAC announcement.
Passport 7019934211 (Russia)	Passport ID #	Named in OFAC announcement.
KONDRATIEV, Ivan Gennadievich	Name	Bassterlord-associated mail used to register "Bassterlord" account on RaidForums
91.244.151.25	IP Address	IP associated with leak data from Bassterlord email sinner4iter@gmail.com
91.244.144.121	IP Address	IP associated with leak data from Bassterlord email sinner4iter@gmail.com



89.113.164.94	IP Address	IP associated with leak data from Bassterlord email sinner4iter@gmail.com
91.244.148.31	IP Address	IP associated with leak data from Bassterlord email sinner4iter@gmail.com



ABOUT AUTHOR

Jon DiMaggio is a Senior Threat Intelligence Analyst and has over 14 years of experience. He possesses advanced expertise in identifying, tracking, and analyzing Advanced Persistent Threats (APTs). Additionally, Jon speaks at national level conferences such as RSA and BlackHat. He conducts interviews based on his research with media organizations such as Fox, CNN, Bloomberg, Reuters, Wired magazine, and several others.

ABOUT US

Analyst1, engineered by cyber threat analysts, offers an enterprise-scale platform that operationalizes threat intelligence and enables security teams and analysts to focus on deeper analysis and response. With Analyst1, organizations gain visibility into advanced persistent threats attempting to infiltrate their networks.

 [@analyst1](https://twitter.com/analyst1)

 analyst1.com/blog

Any technical information that is made available by Analyst1 is the copyrighted work of Analyst1 and is owned by Analyst1.

NO WARRANTY . The technical information is being delivered to you as is and Analyst1 makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Analyst1 reserves the right to make changes without prior notice

