



The Ransomware Diaries:
Volume 2

A Ransomware Hacker Origin Story

Jon DiMaggio

April 25, 2023



WARNING:

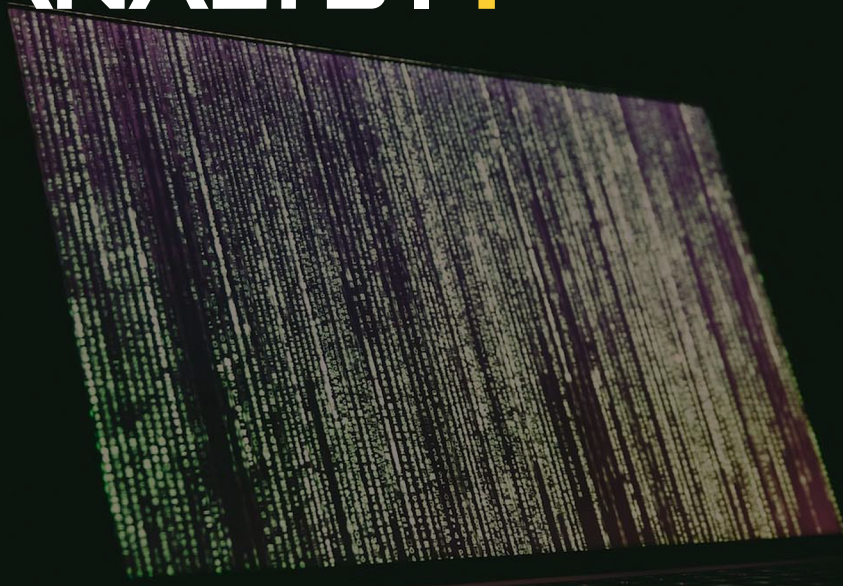
PLEASE DO NOT TRY THIS AT HOME.

**ENGAGING WITH RANSOMWARE
CRIMINALS SHOULD ONLY BE CARRIED OUT
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!



Contents

| | |
|--|-----------|
| Preface | 4 |
| Insights | 5 |
| LockBit Forever! | 7 |
| The Ransomware Manual: Volume 1 | 12 |
| The Ransomware Manual: Volume 2 | 18 |
| The Interview | 24 |
| The REAL REvil | 32 |
| The 2020 Paper Contest | 34 |
| Does Not Play Well With Others | 39 |
| Is This Goodbye? | 41 |
| Don't Look Back | 45 |
| Final Entry | 46 |

Preface

Would you want to talk with a ransomware hacker who partnered with some of the world's most notorious ransomware gangs? Well, that is exactly what I set out to do after writing the previous edition of the Ransomware Diaries, and let me tell you, this story won't leave you disappointed.

Instead, you will learn about a man who entered organized crime at a young age and was groomed and mentored by an important, well-connected figure within the ransomware community.

The story I will tell you has a lot of twists – some of which may be upsetting, and others that will help you understand the person behind the crimes. More importantly, it will provide insight into the profile of the type of person you may chase across your organization's networks, or worse, communicate with as you negotiate an extortion payment after a ransomware attack.

You may wonder how I could have gained the trust of a criminal and convinced someone to share their story and reveal personal details about their life of crime.

After I published the [Ransomware Diaries](#) on January 16, 2023, a lot changed in my life. I had just revealed my identity to some of the worst criminals in the world. More importantly, they knew I betrayed them and used the relationship to produce intelligence that could be leveraged against them. It was a bit overwhelming, and I expected anger and threats. Instead, I got interview requests! It's certainly not how I thought things would turn out, but I found myself in a position to capture a side of ransomware rarely seen by most of us: The human side.

The story I will tell you is not mine, but it is the account of a man who was once no different than you or me. Unfortunately, poor decisions and hardships in his life pushed him to a dark place, from which he never returned.

This is Bassterslord's story.

Insights

Below is a list of insights I learned while conducting research into Bassterlord. However, the fascinating aspect of this story evolved from the content shared in the “Interview” section of this report. There, in the interview, I really began to see the events and triggers that changed Bassterlord as a person, which allowed me to understand how he became the criminal he is today. In conjunction with ransomware attacks and direct connections with high-level ransomware criminals, this back story detailed in our interview will reveal the real impact of Bassterlord’s story.

Here are some important details I learned about Bassterlord:

- Bassterlord is a ransomware affiliate who runs his team, known as the National Hazard Agency. Originally, he was a junior team member, but as time progressed, he moved up the ranks and is now its leader.
- Bassterlord partnered with at least four ransomware gangs: REvil, RansomEXX, Avadon and LockBit.
- Bassterlord is a Caucasian male around 27 years old, born, raised, and living in Lugansk, Ukraine. He operates on Russian underground forums under the monikers “Fisheye,” “Bassterlord,” “Buster,” and “National Hazard Agency,” which is also the name of his team.
- Lalartu (AKA Sheriff), a known persona in ransomware since 2019 who played a role in gangs such as GandCrab, REvil, Conti, and others, mentored Bassterlord and taught him how to conduct ransomware attacks. Lalartu also introduced and vouched for Bassterlord’s admittance into the REvil ransomware gang.
- Bassterlord authored two training manuals – one which he distributed for free on Russian hacking forums, and the other which he sold for \$10k per copy. Bassterlord also directly trained other hackers, teaching them how to conduct ransomware attacks.
- Prodaft, a cyber security company, obtained Bassterlord’s manual and is allegedly trying to dox Bassterlord and reveal his true identity.
- Bassterlord is also an “access broker,” selling access into compromised victim environments in addition to his ransomware operation.
- Bassterlord is behind several high-profile attacks against organizations such as Uruguayan Navy, India’s Department of Revenue, and was associated with the attack against Maximum Industries, a contractor of SpaceX, amongst several others.

- Bassterlord won first place in the 2020 Summer Paper Contest, held on a Russian hacking forum and sponsored by LockBit. This led to Bassterlord's recruitment into the lockBit ransomware gang.
- Bassterlord has inside knowledge of the original REvil gang and its inner operations and personnel – some of which he shared during our conversations.
- One of REvils top affiliates went missing shortly after U.S. President Joe Biden and Vladimir Putin met in June 2021. This was the beginning of the investigation by the FSB, and how they obtained the names and information of the men they eventually arrested seven months later.
- After the meeting between U.S. and Russian presidents in 2020, centering around REvil ransomware, Bassterlord was summoned and questioned by the FSB about his role in the operation.
- Bassterlord travels to Russia occasionally to address his medical needs.
- Bassterlord is associated with an attack against the DoD Defense Finance and Accounting Service, which is detailed in the second volume of his training manual.

Author's Note: There were several formats I could use to depict the information I am about to share. I could have started at the earliest point in time when a significant event took place and moved forward, sequentially telling this story. Instead, I have chosen to tell it from my own perspective, as it played out during my investigation.

LockBit Forever!

In late February 2023, 3xp0rt, a researcher I follow, tweeted about a persona named Bassterlord, who had announced he was going to begin working with LockBit as of March 1st. In the tweet, 3xp0rt included a screenshot from a Tox conversation between Bassterlord and LockBit:

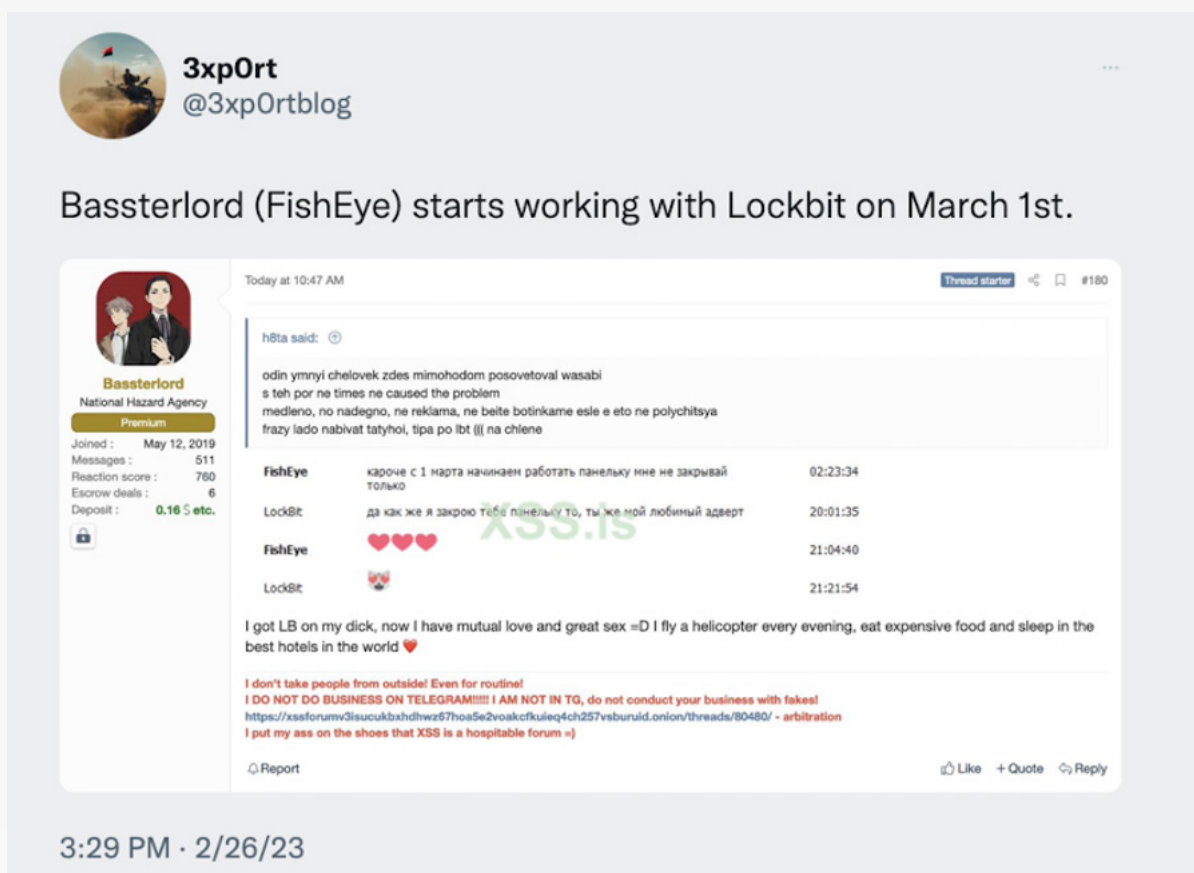


Figure 1: Tweet from 3xp0rt showing a post from Bassterlord announcing that he was joining LockBit

I had heard the name Bassterlord in the past and read some of his posts on hacking forums while researching REvil in 2021. Back then, I did not think much of the persona. Yet, I remembered enough that his name was familiar, so I paid attention to his claim about joining LockBit.

According to the tweet, Bassterlord was the newest affiliate to join the LockBit ransomware operation. This was intriguing because several years ago, Bassterlord had done a Q&A on the same forum seen in 3xp0rt's tweet. I especially remembered the forum post because of two things Bassterlord mentioned.

First, he was associated with Revil, Lockbit, Ransomexx and Avaddon. Back then, I did not think he was a full-fledged affiliate, but instead, a member of an affiliate team learning how to conduct ransomware attacks. I based this on one of his comments stating that he aspired to run his own affiliate team. Still, as a supporting member of an affiliate team who partnered with the REvil ransomware gang during its prime, gave Bassterlord street credibility and unique experience.

Second, after the Q&A, there was one additional statement Bassterlord made, which seemed benign but was a sign of what was coming.

His statement seemed benign, but **was a sign** of what was coming

“Do not look for literature, look for a mentor who will teach either for a fee or for free. Because first-hand information is better perceived than a read book. Yes, and I haven't seen books on ransom, yet = D (if anyone finds it, I'll be the first to buy)” -Bassterlord

Fast forward to today, hearing the news of Bassterlord's latest LockBit affiliation, I thought perhaps he was leading his own team. I wanted to know more, and so my search for Bassterlord began!

To start, I identified Bassterlord's dark web footprint. Bassterlord had accounts on two dark web forums, which I knew were used regularly by ransomware criminals. The account profiles I identified can be seen in Figure 2.

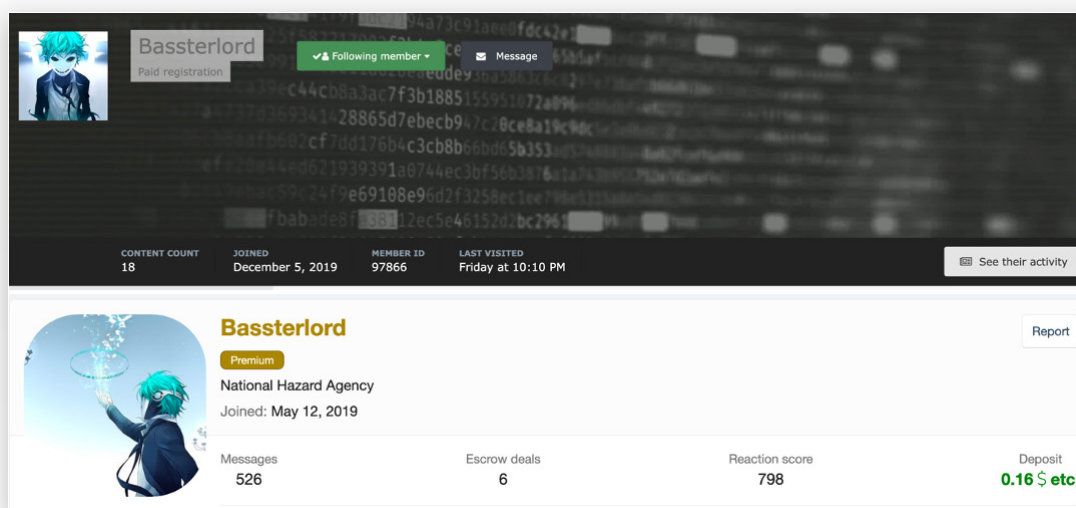
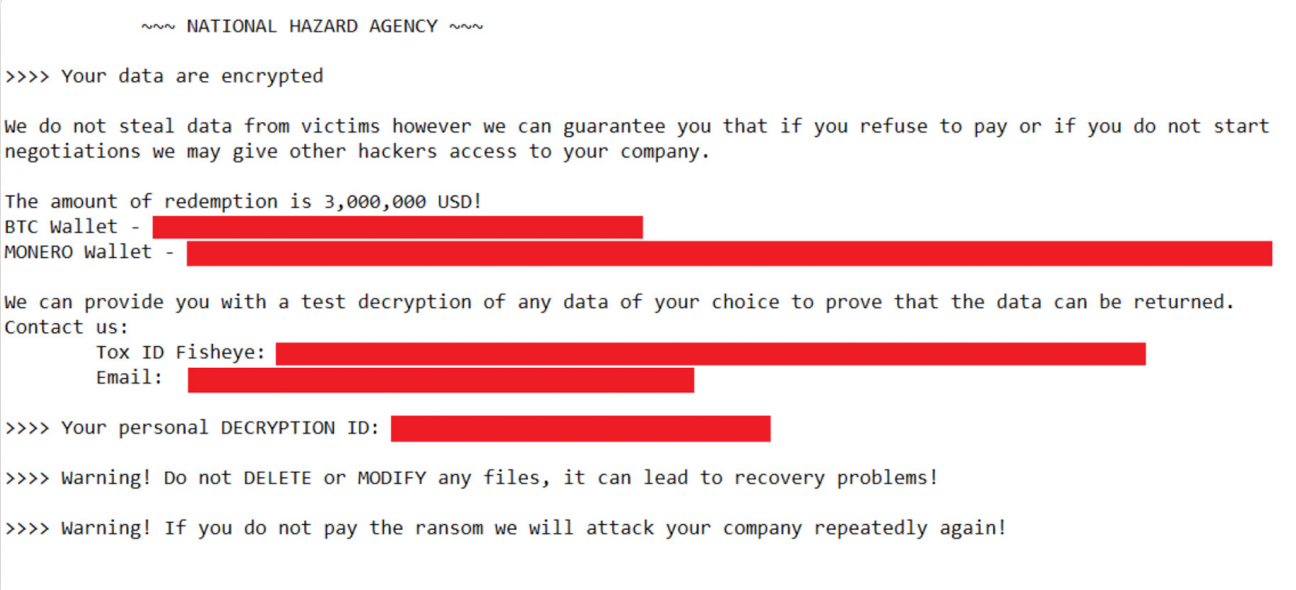


Figure 2: Bassterlord profiles found on Russian-based underground forums

Bassterlord associated himself with a group known as the “National Hazard Agency,” which he listed in his profile. I was unfamiliar with the name but found a tweet by Germán Fernández (@1ZRR4H) referencing a ransom note from a team with the same name. Fernández also said the note was generated from a LockBit Ransomware payload. This is the ransom note Fernández found:



~~~ NATIONAL HAZARD AGENCY ~~~

>>>> Your data are encrypted

We do not steal data from victims however we can guarantee you that if you refuse to pay or if you do not start negotiations we may give other hackers access to your company.

The amount of redemption is 3,000,000 USD!

BTC Wallet - [REDACTED]

MONERO Wallet - [REDACTED]

We can provide you with a test decryption of any data of your choice to prove that the data can be returned. Contact us:

Tox ID Fisheye: [REDACTED]

Email: [REDACTED]

>>>> Your personal DECRYPTION ID: [REDACTED]

>>>> Warning! Do not DELETE or MODIFY any files, it can lead to recovery problems!

>>>> Warning! If you do not pay the ransom we will attack your company repeatedly again!

Figure 3: National Hazard Agency ransom note first identified by [@1ZRR4H](#)

This was strange. As detailed in my previous research, a LockBit ransomware builder was leaked by a disgruntled developer on September 22, 2022, making it available to anyone who knew where to find it. The tweet showing the ransom note was posted just a few days later, on September 30. I believe this was an instance of criminals altering the leaked ransomware to drop their note, as opposed to LockBit’s.

Suppose my theory about the leaked ransomware is correct. In that case, Bassterlord and the National Hazard Agency obtained and modified the LockBit source code and presumably used it in an attack within an eight-day period. This is not much time, but I don’t know how else they would modify LockBit’s ransomware to deliver a custom ransom note.

It’s also odd that the attacker states they don’t steal data, but will give hackers access to the victim company and attack it repeatedly if they don’t pay the ransom. This is not the typical message I see from ransomware attackers.

Even more perplexing, why would LockBit recruit an affiliate who used their leaked builder? Based on this note, Bassterlord and crew were bypassing LockBit to keep all of the ransom profit for themselves. If not, they would simply use the authentic LockBit

ransomware payload and the resources LockBit provides within its admin panel. All builders in the admin panel drop a LockBit payload with its ransom note directing victims to its infrastructure for chat negotiations. This note did not.

I realized if wanted to learn more about Bassterlord and his team I needed to do two things. First, I needed to review the previous threads and conversations between Bassterlord and other criminals on the underground forums. Second, I needed to find a way to get information directly from the source — Bassterlord or one of his team members. I began with the underground forum known as Exploit. What I found shocked me.



## PART II: THE **RANSOMWARE** MANUALS



Artwork Credit: Yuumei  
(Wenqing Yan)  
<https://www.yuumeiart.com>

# The Ransomware Manual: Volume 1

I spent the next few days reading through Bassterlord's conversations with other criminals. The most significant conversation I reviewed discussed a ransomware training manual, which Bassterlord released in mid-2021. The purpose of each manual was to teach criminals how to conduct ransomware attacks. Until now, I had never encountered training material designed to teach someone how to commit ransomware crimes. Yet, here I was, staring at evidence showing that Bassterlord did exactly that.

Remember that Bassterlord made a statement about wanting a book detailing how to conduct ransomware attacks, which he said did not exist? Apparently, Bassterlord got tired of waiting and decided to create his own. Figure 4 displays the post detailing Bassterlord's first ransomware training manual.

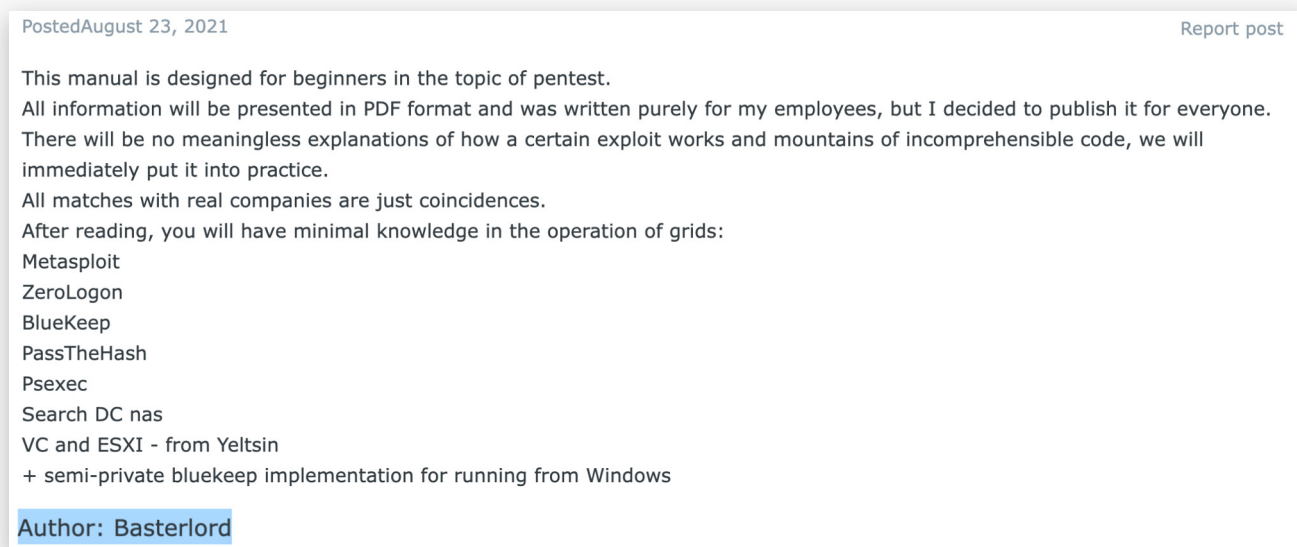


Figure 4: Underground forum post with details to download Volume 1 of the Ransomware Manual

Unfortunately, I can't share the manual with you because it would encourage untrained hackers to commit ransomware attacks. Researchers and analysts who have access to the forum will figure out how to find it; otherwise, they probably don't need access. However, I am going to share some content in order to give you a better understanding of the manual and insight into its author.

The images in the figures below display examples of the manual's content, such as the cover and random pages, which I had translated into English.

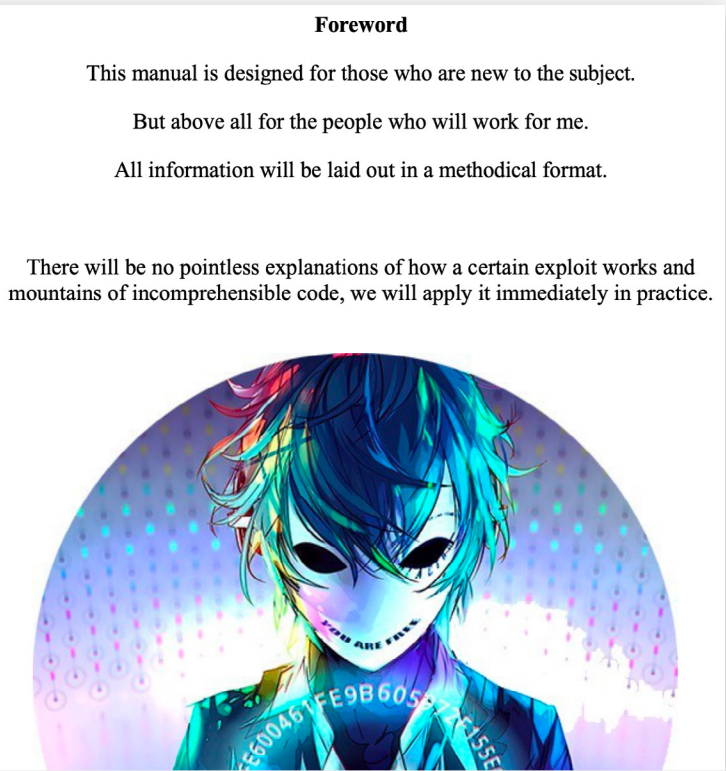


Figure 5: Cover and Forward section of the ransomware manual vol 1

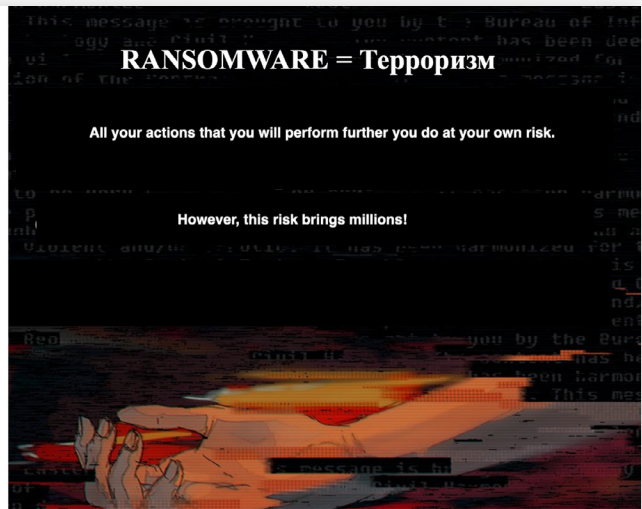
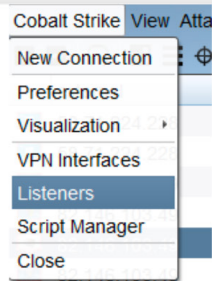
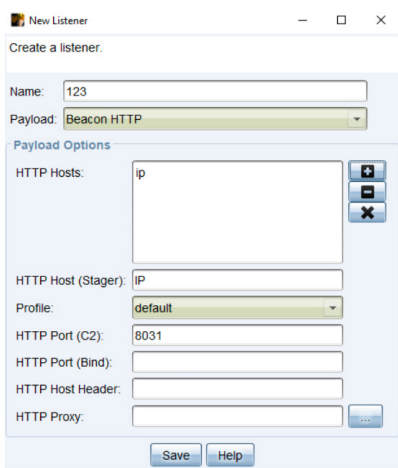


Figure 6: Various pages from the ransomware manual Volume 1



### Creating a listener.



After all the action, if you want to minimally erase the traces of his stay and postpone the break-in.

On the machines that you logged in with the rdp, you can open a paveshell and prescribe the following:

```
wevtutil el | Foreach-Object {wevtutil cl "$_"}
```

This regular will erase all logs.

Also commands to delete hidden accounts cmd net

```
user support Pa$$wo0rd /delete
```

```
net group "Domain Admins" support /delete
```

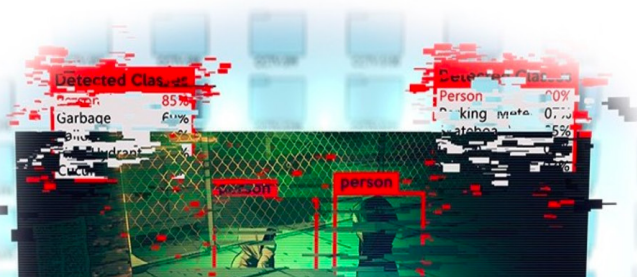


Figure 7: Various pages from the Ransomware Manual Volume 1

**enter the domain admin login without domain and its password. now everything is ready for authorization, enter the esx host using the domain admin credentials and reset the root pass**

**Then just ssh to the esx Shut down the machines**

**And you do dirty things =>**

Figure 8: Message from Ransom Manual Volume 1

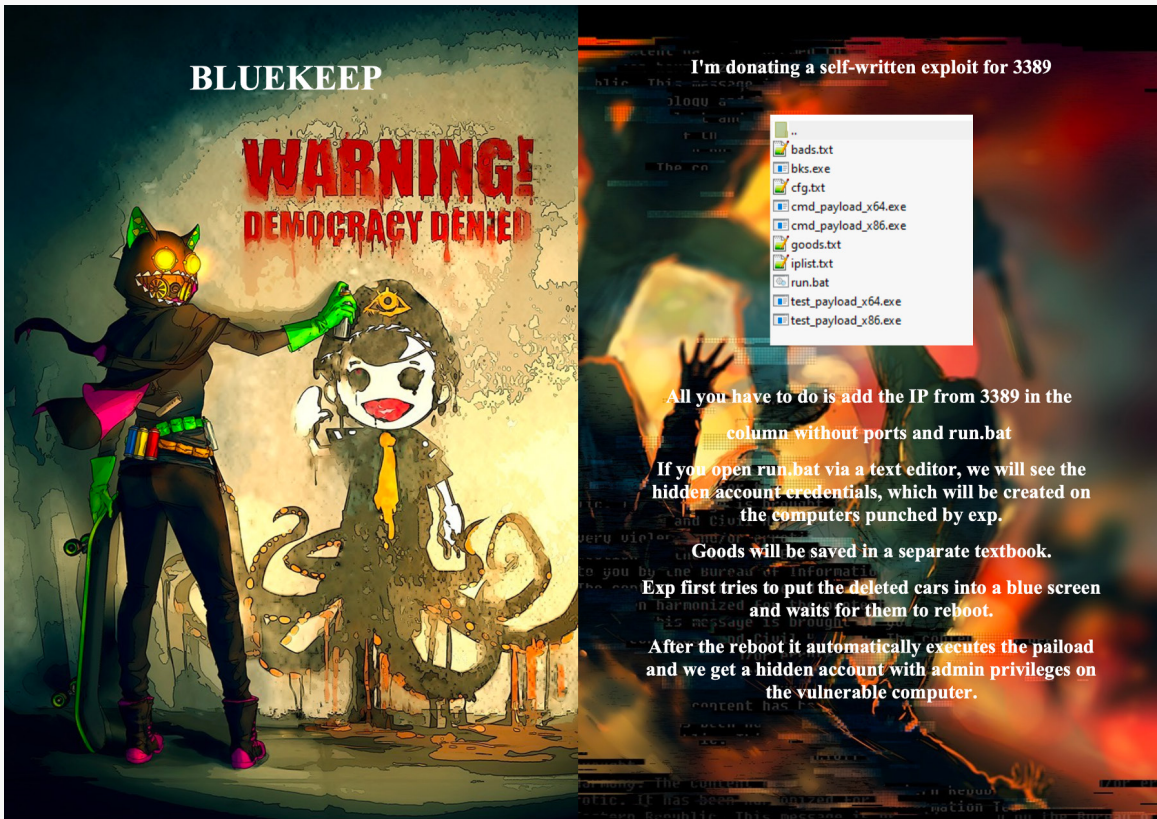


Figure 9: Random pages from the Ransomware Manual Volume 1

I also discovered multiple archives containing hacktools, exploits and scripts, which Bassterlord provided for use with his training material. In the scripts, Bassterlord used the password “ZergRush6599!%\$#@” for his training purposes. I point this out in case Bassterlord or his trainees reused this password for other resources.

| Name           | Date Modified            | Size   | Kind             |
|----------------|--------------------------|--------|------------------|
| 1.exe          | Mar 29, 2016 at 4:35 AM  | 1.7 MB | Windo...EXE File |
| 32 (2).exe     | Aug 11, 2022 at 9:16 PM  | 1.4 MB | Windo...EXE File |
| 123.deb        | Oct 30, 2022 at 6:39 AM  | 4.2 MB | Document         |
| 12313eeee3.exe | Aug 11, 2022 at 9:16 PM  | 381 KB | Windo...EXE File |
| a.exe          | Aug 13, 2022 at 3:19 PM  | 5 MB   | Windo...EXE File |
| a2.exe         | Aug 11, 2022 at 9:16 PM  | 5.8 MB | Windo...EXE File |
| bluekeep.zip   | Jan 23, 2023 at 1:45 AM  | 159 KB | ZIP archive      |
| lazagne.exe    | Aug 11, 2022 at 9:16 PM  | 6.6 MB | Windo...EXE File |
| netscanold.exe | Aug 14, 2022 at 9:41 PM  | 1.6 MB | Windo...EXE File |
| netscanold.xml | Jan 23, 2023 at 1:43 AM  | 60 KB  | XML text         |
| procdump.exe   | Aug 11, 2022 at 9:16 PM  | 385 KB | Windo...EXE File |
| psexec.exe     | Aug 14, 2022 at 1:19 PM  | 339 KB | Windo...EXE File |
| pstool.exe     | Aug 11, 2022 at 9:16 PM  | 502 KB | Windo...EXE File |
| pstoolq.exe    | Aug 11, 2022 at 9:16 PM  | 400 KB | Windo...EXE File |
| pstoolTS.exe   | Aug 11, 2022 at 9:16 PM  | 614 KB | Windo...EXE File |
| svchost.exe    | Aug 13, 2022 at 10:19 PM | 8.7 MB | Windo...EXE File |
| svvchost.exe   | Aug 11, 2022 at 9:16 PM  | 1.1 MB | Windo...EXE File |

Figure 10: Hacktools provided by Bassterlord

If you did not have the skillset to conduct the initial breach, no problem. Bassterlord is also an access broker, in addition to a ransomware criminal.

At the time he released the manual, Bassterlord posted multiple sales ads purposed to sell access into companies he breached. While Bassterlord gave away the manual and hacking resources for free, he made money by selling access to these companies. This way, his criminal students would have an environment to practice the tactics and methods detailed inside the manual. Bassterlord sold access to several companies, including the gas and electric company seen for sale in Figure 11.

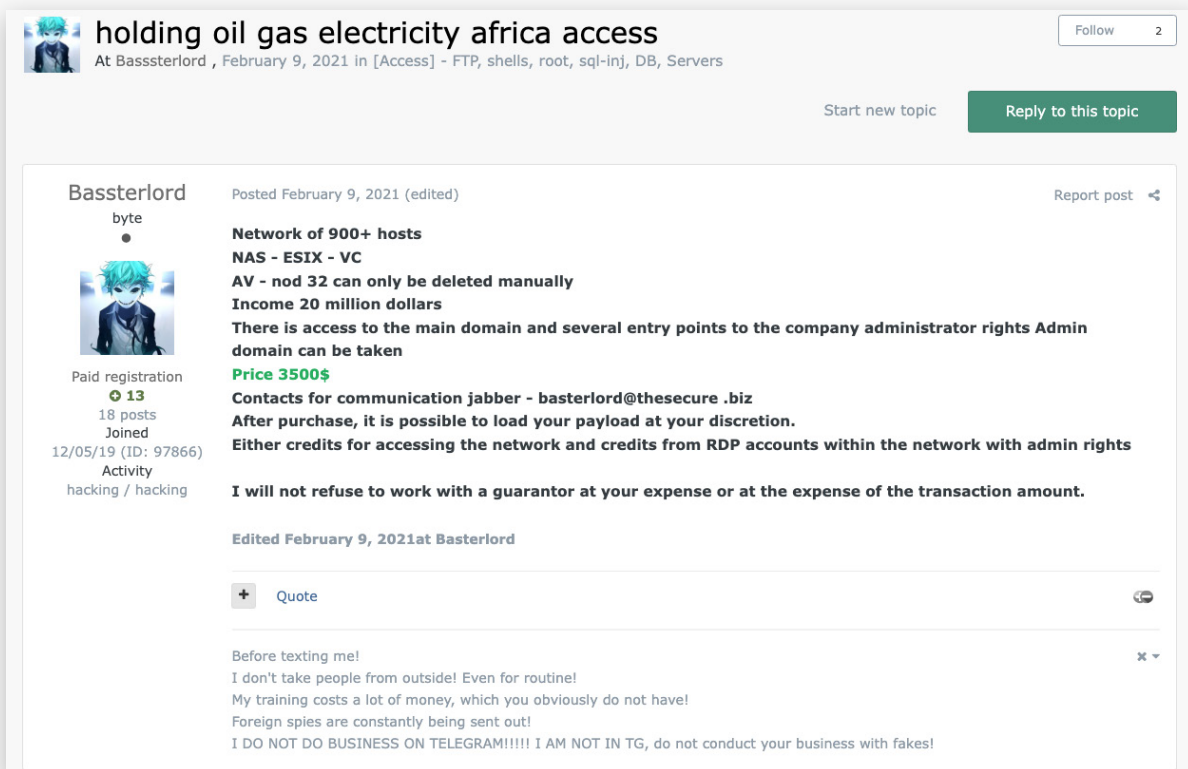


Figure 11: A Bassterlord post selling access to gas and electrical company in Africa

Bassterlord received praise from criminals throughout the ransomware community for releasing the ransomware manual. However, the first person to compliment the up-and-coming criminal was none other than LockBit himself. LockBit used one word to express his sentiment about Bassterlord's work:

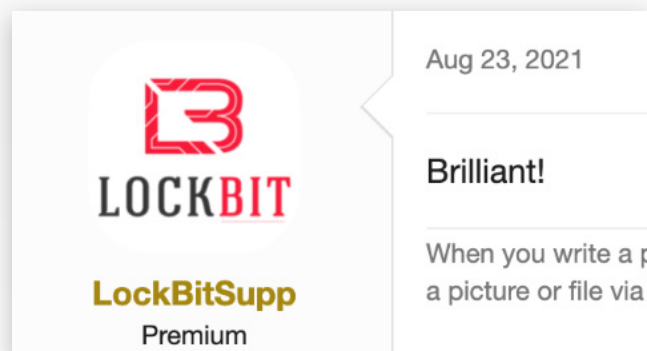


Figure 12: LockBit's response to the Ransom Manual Volume 1



I am surprised that the Ransomware Manual has not been discussed further or distributed outside of underground forums. If it had, I think Bassterlord would have gained greater notoriety and fame – which I later learned is very important to him. This may be the reason Bassterlord created a second manual – the Ransomware Manual Volume 2 – a year and a half later.

Next, we will discuss Volume 2, which has its own interesting story. To say the least, things have not gone as Bassterlord intended.

# The Ransomware Manual: Volume 2

On December 22, 2022, Bassterlord posted an announcement about the highly anticipated second volume of the Ransomware Manual. He completed his work, and this time he was not giving it away – the second manual would have a steep price tag.

Bassterlord offered to sell the manual and complete rights to it for \$200k. When no one was willing to pay, Bassterlord decided to sell a limited number of copies at \$10k each and then terminate distribution, though it's unclear how he intended to prevent the buyer from sharing or distributing it further.

To generate interest, Bassterlord promised Volume 2 would include information you could use to access organizations he had already breached. Bassterlord made this statement giving insight into why he wrote the second manual:

*I am writing a manual simply because I do not see any normal alternatives where there is no abstruse explanation of how this or that exploit works. I have nothing against people who write articles. I'll tell you a secret - how it works doesn't give a fuck about anyone except cybersecuritys (researchers) and coders, everyone is interested in how to put it into practice and make money on it!*

*It is practically impossible to prove my involvement in hacking. I don't store any data on my PC. I live very modestly in one, I don't go abroad.*

*By the way, a cool coincidence just a couple of days ago HIMARS (American Multiple Launch Rocket System) flew into the house of one of my employees =D My greetings to Uncle Sam! Thanks =D -Bassterlord*

There are a few important intel elements to take away from Bassterlord's statement. Based on what I know from Volume 1, in conjunction with information provided about Volume 2, Bassterlord gave the first volume with attack tools and resources away for free, then sold access to target companies separately to make money. However, for Volume 2, you had to buy it as a package in which the details and access were included.

Further, in his statement, Bassterlord claims that U.S. missiles were used to target an area where one of his "employees" reside. Bassterlord is likely referring to one of the members of his ransomware affiliate team. The obvious questions are: What region of the world is he referring to, and does he also live in this area or just his employee? These are questions

I did not have an answer to. Figure 13 is Bassterlord's post, with the cover of the Ransom Manual Volume 2.

Man for working with networks version 2.0 (2023) Discussion!

1 2 3 ... 12 Next ▶

Dec 5, 2022

**Bassterlord**  
National Hazard Agency  
Premium

Joined: May 12, 2019  
Messages: 526  
Reaction score: 803  
Escrow deals: 6  
Deposit: 0.16 \$ etc.




Figure 13: The Ransomware Manual Volume 2


Similar to Volume 1, the cover was interesting. In less than a month, Bassterlord sold eight copies of the second volume. On December 30, Bassterlord stated:

*"I already said I won't release to the public! It will only be available for the price tag of \$10k. I have 2 copies left."*

Bassterlord could have sold far more than 10 copies. The limited sale was a tactic Bassterlord used to drive hype and entice criminals to purchase the manual before all 10 copies sold out.

Several days later, on January 4, 2023, the sale of the Ransomware Manual Volume 2 officially ended. The buzz from its sale increased Bassterlord's popularity across underground crime forums and within the Russian ransomware community. However, Bassterlord's celebration was short-lived.

The following month, on February 4, something unexpected happened. Prodaft, a cyber security company, posted on Twitter and [LinkedIn](#) marketing a new report they wrote based on Volume 2 of Bassterlord's manual, which they had obtained.




**Bassterlord**  
National Hazard Agency  
Premium

Joined: May 12, 2019  
Messages: 526  
Reaction score: 803  
Escrow deals: 6  
Deposit: 0.16 \$ etc.


Feb 3, 2023 Thread starter

h8ta said: [↻](#)


neugele nikto ne soliet, dage interesno stalo



**PRODAFT**  
@PRODAFT · Follow



A manual that teaches you how to build up your ransomware skills? 🐼  
 We obtained a technical [#manual](#) that is currently being distributed in the underground forums for around \$10k - for anyone w/ limited technical skills who'd like to learn more about... well, using [#ransomware](#) 🙄



3:32 AM · Feb 2, 2023 ⓘ

[Read the full conversation on Twitter](#)

40 ❤️ Reply [Copy link](#)

Read 4 replies

Rejoice leaked. However, they won't leak the full man and how it's done, because they will simultaneously publish the secret that is inside, and for this they will grab them by the ass => Well, as promised, even if the info is leaked, it remains relevant.

If you want and have brains, there will always be offices to work off, so it remains =>

Well, the condoms are still those, at least the author was mentioned = D (where the copyright is a bitch, I will file a lawsuit 😄)

Well, judging by the presence of specialists in BTC research, they already understood that denyushki first flew to the china exchange and then turned into a tether and later into a monerka 🙄

The warning that was inside worked, they understand that there will be an akhtung if a full mana is published 🙄

Figure 14: Prodaft post about Bassterlord's manual

Initially, based on Prodaft's marketing of the manual, the cybersecurity community expected a public report to be released. If not, why would Prodaft put out marketing and PR surrounding their report?

However, it would appear Prodaft changed its mind, because at the time of this writing, they have not released a report publicly. Based on [comments](#) on LinkedIn and Twitter, such as: "So, Where is it !!?", the cyber security community was excited and expected something to be published.

To be fair, I understand why Prodaft did not publish the content itself, as that would be irresponsible. Nevertheless, I honestly don't understand why they made the posts if they did not intend to publish anything at all.

This did not sit well with me and came across like a PR stunt, but Prodaft puts out good content so perhaps they just got ahead of themselves on this one. More importantly, as Basterlord states in his post, "they won't leak the full manual on how it's done, because they will simultaneously publish the secrets inside, and for this, they will bite themselves in the ass." For once, Basterlord and I agree. That is the same reason I am not publishing Volume 1.

Considering what  
I read in Volume 1,  
I know Volume 2 is the  
real deal

Keep in mind that I have not seen Volume 2, but considering what I read in Volume 1, I know Volume 2 is the real deal. Yet, I needed to know more about the companies and organizations on the cusp of getting breached, or worse, already had been exposed to the information and access provided within this manual. I wanted to leverage the criminal connections I made while doing my previous investigation into LockBit, but that was not an option.



# Part III: THE INTERVIEW

# The Interview

After publishing the Ransomware Diaries, many criminals, including LockBit, read and discussed the research. Some even messaged me directly. It is never good for criminals to know who you are and realize you spend your days trying to disrupt their operations. Still, since they did know, I saw this as an opportunity to leverage my recent attention from criminals to gain Bassterlord's trust.

I planned to contact Bassterlord directly, as myself, which is not something I have done in the past. If it didn't work, this story would end before it began. Since Bassterlord claimed he was now working with LockBit, I hoped he would know who I was. To contact him, I first needed to obtain his Tox ID, which I had identified within his profile on the underground forums.

If you are unaware, Tox or qTox, is a secure encrypted communication protocol that can be configured to run over Tor nodes, adding another layer of security. Unfortunately, for these reasons, it has become very popular to use amongst ransomware gangs.

Next, I created a Tox ID and gave it the alias "Not\_Jon." If my stealthy username left any doubt, I also used my face for the avatar. Then, I added BassterLord's Tox ID into the chat window and sent him a connection request with a simple question: Can we talk?

I asked Bassterlord if he knew who I was and assured him I was not trying to dox him, which was true. I have no interest in publishing the identity of cyber criminals publicly, as it has repercussions. That is a headache for law enforcement. Instead, I aimed to obtain information that could help stop future attacks and/or prevent another company from falling victim to Bassterlord and his crew. I also wanted to build a profile on Bassterlord to better understand and characterize the type of person who conducts ransomware attacks.

My transparency about my identity and intentions seemed to work, and surprisingly, Bassterlord responded within a few hours of reaching out. He said he knew who I was and would talk to me.

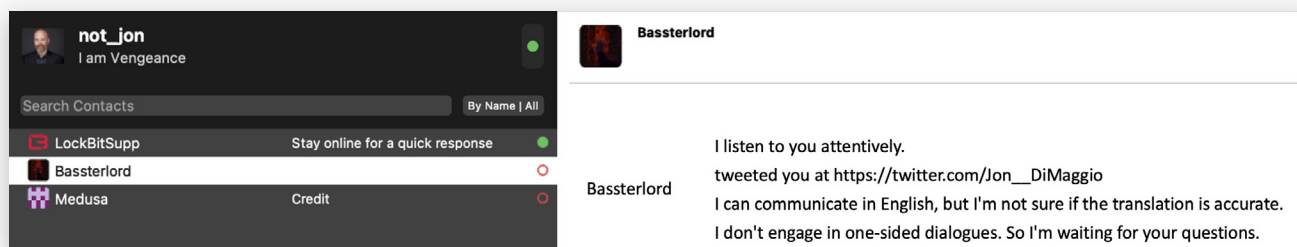


Figure 15: The beginning of my interaction with Bassterlord, translated for viewing purposes



Let's pause for a moment. You see, it's one thing to chase packets but another to chase people. I often take risks to do my job; sometimes, it can be scary. This was one of those times. I was directly communicating with one of the most well-connected ransomware hackers in the world. I was hoping for this, but, honestly, it put me on edge.

So, I sat staring at my Tox window as Bassterlord awaited my response. I knew if I wanted to gain his trust, it would take more than one conversation. Further, I was also concerned that I might scare him off if I asked too many questions early on. So, I decided to start off with something simple.

I asked Bassterlord how Prodaft obtained his manual. Bassterlord believed Prodaft had purchased it from one of his buyers, but he said they did not buy it from him. Alternatively, Prodaft could have used a well-developed fake persona and convinced Bassterlord to sell the document directly. Honestly, I don't think Bassterlord knows how Prodaft obtained the manual, but it was clear it was now in their possession.

Still, there is another theory that a popular persona from the forum who goes by the moniker "Bratva" presented in a discussion with Bassterlord.

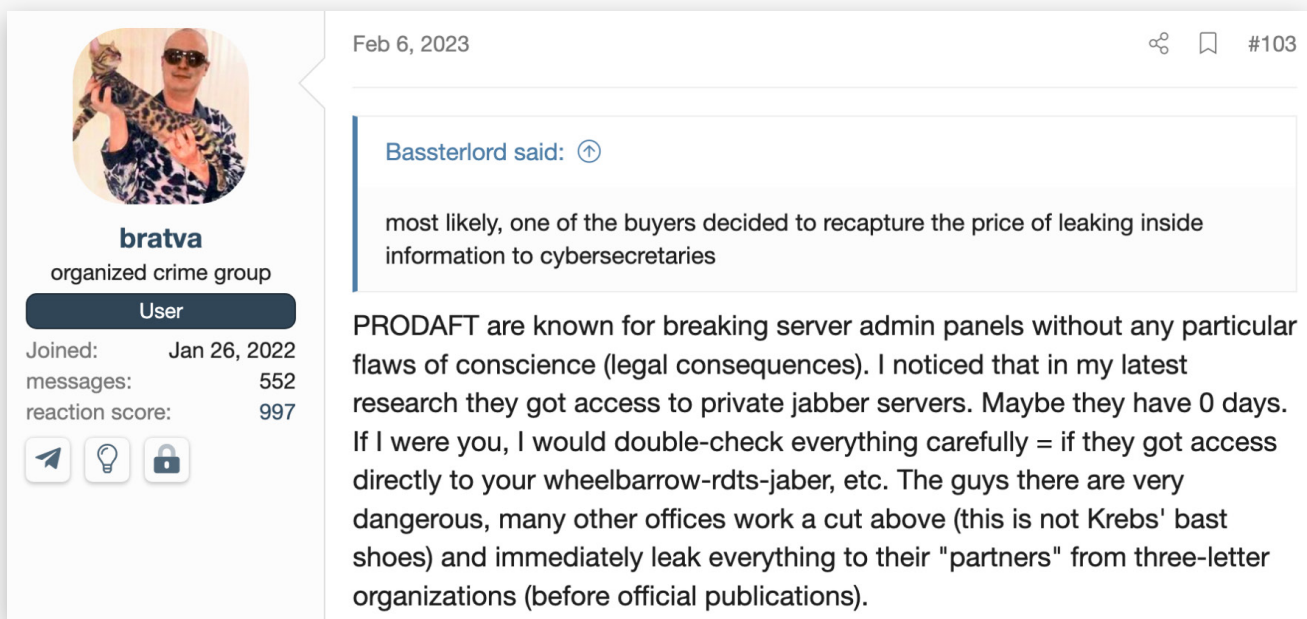


Figure 16: Criminal theory on how Prodaft obtained the Ransomware Manual.

Overall, I am glad Prodaft obtained the manual and drew attention to the situation. Further, if Prodaft passed it to law enforcement and government intelligence agencies, that only helps in the fight against ransomware. My only concern is if the wrong government gains access, it could be used for nefarious purposes. But, [Prodaft](#) is a Swiss-based company, so I don't think that is the case.

My next question was if Bassterlord knew why Prodaft did not publish the manual or their report, as their social media had suggested.

Bassterlord said the manual includes a document belonging to the Defense Finance and Accounting Service of the Department of Defense that is marked confidential.

**Bassterlord told me someone initially gained access to DoD infrastructure by compromising an employee from a company that provides accounting and auditing services for the entire US military!**

**Bassterlord also claimed that access to the DoD system was provided within his manual, which is why Prodaft would not publish it.** Really, I needed proof that this claim was true, which Bassterlord would not provide. Despite his lack of cooperation, later, I did my own investigating and found a related image on the dark web that Bassterlord had shared with other criminals for bragging rights, which can be seen in Figure 17.



*Figure 17: Example of a document allegedly stolen from a DoD system.*

Your guess is as good as mine if Bassterlord really does have access to a DoD system, but he certainly put a lot of effort into making up the story if he is lying.

Next, I decided to ask him why he believed Prodaft was trying to dox him. I hoped a more empathetic approach would help gain Bassterlord's trust. He told me Prodaft was using aggressive hacking tactics to reveal his identity. He was upset they were trying to obtain his private and sensitive information, which could reveal who he was. Ironically, now, Bassterlord knows how his victims feel.

Additionally, Bassterlord said that just 20 minutes earlier, someone he believed was Prodaft contacted him on Tox, threatening to reveal his identity. He told me he was very upset and has a "panic disorder," which he manages with antidepressants. He said that because of what was taking place with Prodaft, he was considering shutting down his operation. I think Bassterlord is telling the truth about his medical concerns, but I don't believe he is planning to cease ransomware attacks. I believe this is just the beginning for Bassterlord.

I also remembered something Bassterlord said that helped me to determine he was not from Russia. Bassterlord mentioned he had health and vision problems previously. After he began to make money from ransomware, he traveled to Russia, where he received medical attention.

I believe this took place between 2017 – 2019. That implies he does not live in Russia. Most of the ransomware gangs I investigate originate from Russia; however, affiliates come from all over the world, so I asked Bassterlord where he was from. Surprisingly, he told me and I believe his answer is true based on everything I now know.

*I used to live in Lugansk (Ukraine), like many just studying at the beginning of the war.*  
-Bassterlord

Bassterlord is from Ukraine. He said he “used to live in Lugansk.” Despite Bassterlord’s claim that he relocated, I know he is still in a Russian-controlled area. I believe he is still living in the Luhansk People’s Republic in the area near Kadiivka or Donetsk, which he talked about.

Further, in a forum discussion, Bassterlord posted the below image showing him (allegedly) walking down a road with the caption “Metal/steel facility in Alchevsk,” a city within the Luhansk region of Ukraine:

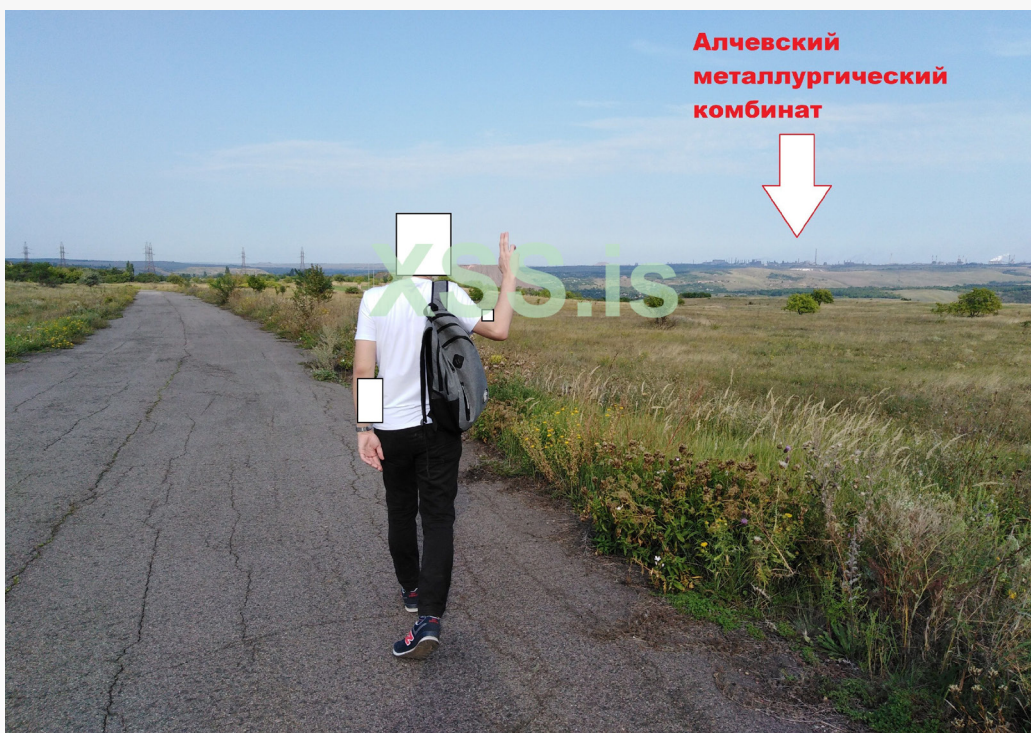


Figure 18: Bassterlord walks home near the Metal/steel facility in Alchevsk

To validate, I zoomed in on the backdrop of the photo. You can see the smoke towers and industrial infrastructure, which match other images of Alchevsk I reviewed from public sources. The area is known for its factories and steel mills.



Figure 19: Alchevsk steel mills in the background of Bassterlord's photo

In addition, I believe Bassterlord is around 27 years old, based on the timeframe of events Bassterlord discussed. His age is significant because, while young, he grew up in Ukraine before Russia's invasion, which led to their occupation of the region in which Bassterlord lived.

He was 17 in 2014, when Russia first invaded Ukraine. Yet, for reasons I do not understand, his anger is directed toward democracy and the U.S. instead of Russia – the country that robbed him of his freedom.

I don't know if he was raised this way or if he was influenced by heavy Russian propaganda after the invasion. I thought the question might end our conversation, so I chose not to ask.

Bassterlord continued:

*When I was a student, I had a girlfriend. She was my first love but in the end she just said to me - "you'll never make a lot of money sitting at a computer" and dumped me, which motivated me to work 10 times harder. **Anger is my motivator. We parted, but the incident was remembered.** Now I'm a millionaire. Also, I was bullied a lot in school, but I just made it to 11th grade and graduated that hell.*

*Another time, in high school, I said that I was going to learn English and I heard a lot of laughter in response, including from my teacher. I ended up getting into college and getting a passing grade.*

*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*

*It helped me to work from home but the salary was minimum. So, I worked as a night shift watchman, at an abandoned school. In the winter, the cold got to my bones. The school was completely cut off and I had to wear two coats to keep warm. -Bassterlord*

His story was unfortunate, but it did not seem significant enough to drive him to a life of crime. If I met Bassterlord without knowing what he does, I would consider him a nice guy, which is why I felt there had to be more to this story. He is personable and likable, which is not how he presents himself to the ransomware community.

Now, in my experience, there are two types of criminals. The first are just born bad. You don't have to know they committed a crime to determine they are true evil. The second type is not bad at first, but influenced by a life situation or make poor decisions that lead them into a life of crime. This type of criminal would often never commit a crime if they had been in a different environment. My initial feeling after spending time with Bassterlord was that he was the latter. So, I asked him why he decided to become a criminal, and again, it surprised me how candid he was in his response.

*During the war there were frequent power and communication blackouts. Once, my mother had a kidney attack. But since there was no power I had to look for a way out. I ran out of the driveway, and I saw my neighbor driving his car out of the backyard.*

*I just lie down on the hood and say, "Help me, I'll give you anything to take [my mother] to the hospital. It all worked out after that, I was on my way home with fighter jets flying over my head. I understood that I simply had no money for treatment. -Bassterlord*

Bassterlord was in the middle of an invasion, and his mother required serious medical attention that came with a cost Bassterlord could not afford. They had no power, money, or medical resources. Bassterlord did not even have a way to transport his mother to obtain medical care and had to plead for help from a neighbor.

Once they finally arrived at a hospital, doctors diagnosed and treated Bassterlord's mother and she fully recovered. However, due to the medical attention, Bassterlord's family took on great debt, which they struggled to pay, adding additional stress to their family.

Many of you reading this will relate to the frustration due to the high cost of medical treatment, even here in the U.S. I can imagine that stress is even more significant in a time of war when you are unsure of what tomorrow will bring.

This would be traumatic for anyone, regardless of their life circumstances. I am not sympathetic to Bassterlord, but I am empathetic to the trauma he faced as a young man. It does not give him an excuse to harm and steal from others, but it helps me understand what led him to make his decisions.

Honestly, if my own mother needed medical attention and could not pay for it, I would want to find a way to help her too. However, I would not hack and extort people and organizations worldwide to do it.

Bassterlord's account tells me a lot about his mindset and personality. He felt oppressed and mistreated, and uses that as justification for his actions. Additionally, he continued to steal for his own greed and self-benefit long after the medical debt was paid.

From my point of view, this is an excuse. Life is hard, but hurting others because you were dealt a bad hand is unacceptable. I was glad Bassterlord's mother was okay, even though I don't know him or his mother, but I was afraid to ask him how he paid the debt back. I already knew the answer, but I asked anyway.

*I got home, went (logged into) to XSS (Russian hacking Forum), and created a topic there that I'm looking for a job and I'm not afraid to work (cybercrime) in any country in the world and that I needed at least minimal money. I was contacted by a person with the nickname National Hazard Agency and was offered a job on malicious spamming.*

*At the time I had minimal spam skills, he briefly explained that he was encrypting companies (ransomware). He was trying to teach me. He showed me how to compromise Pulse secure VPN from his desktop, and I watched him work, but I didn't understand much.*

*Subsequently, I managed to infect two companies through spam mailing, one of which was [NEDBANK](#). I got my first money of about 10 thousand dollars. At that time for a person living in a time of shelling is a huge amount of money. This is just was the beginning!*  
*-Bassterlord*

This was the moment that Bassterlord became a criminal. At that time, he was not yet skilled in the trade. He was a junior member of the National Hazard Agency team, which also conducted several data breach-only attacks in addition to ransomware. This is where Bassterlord began supporting ransomware attacks and their extortion efforts.

In addition to NEDBANK, in the first several years of his criminal career, I found supporting evidence from conversations with other criminals that Bassterlord participated in attacks against [New Mexico State University](#), [MOBYTV](#), [Panasonic India](#), [Olympus Camera Company](#), and RockStar video games.

Bassterlord spoke of ransoming these companies as though it were a normal job. But he knew the money he made was not a normal salary.

*I didn't come to Ransom for the good life as you know. I remember my first \$150,000 payout as I recall I almost had a stroke from the impossibility of what was going on.*

*There are many professionals in the CIS, who are paid much less for their skills than they should be, and I'm no exception, imagine what I could become a pentester if I get at least*

*30-40 thousand dollars a month. I wouldn't go ransom, but at the moment I am.*

*Not many people know this, but I donate this money to charity and I've saved a few lives and I think it's only fair. I'm not bad but I'm not good either. I believe in karma. -Bassterlord*

Later, Basterlord told me he had used his money to help others and saved at least two lives. I can confirm that he paid for an expensive medical procedure for another member of the forum. The member validated Bassterlord's claim, and I also saw the money transfer from analyzing the bitcoin transactions.

This is a good start, but if Bassterlord wants to make things right, he should pay back all the companies he extorted. I won't hold my breath.

# The REAL REvil

None of the attacks Bassterlord assisted in could have been possible without the guidance and mentorship of other ransomware criminals. It is not clear how many people helped Bassterlord, but they were associated with the National Hazard Agency. I knew his mentors had to be well-connected in the ransomware world, so I asked.

Bassterlord told me about one of his mentors: **“this man, Lalartu, was an important figure in Ransomware.”** I was very aware of the name Lalartu, but before I could comment, Bassterlord stated Lalartu was **“behind the attack on Travelex and sold the Grand Crab source code to REvil. That’s how REvil got started.”**

This aligned with a claim I made in my research paper, [A History of REvil](#), that GandCrab had not rebranded as REvil but was formed from one of their affiliate teams.

While it does not translate well and is not directly relevant to Bassterlord, the image below shows Lalartu in a discussion about ransomware with GandCrab from 2019. There are many conversations the two criminal personas had in 2019, which I am showing to add credibility to Bassterlord’s claim.

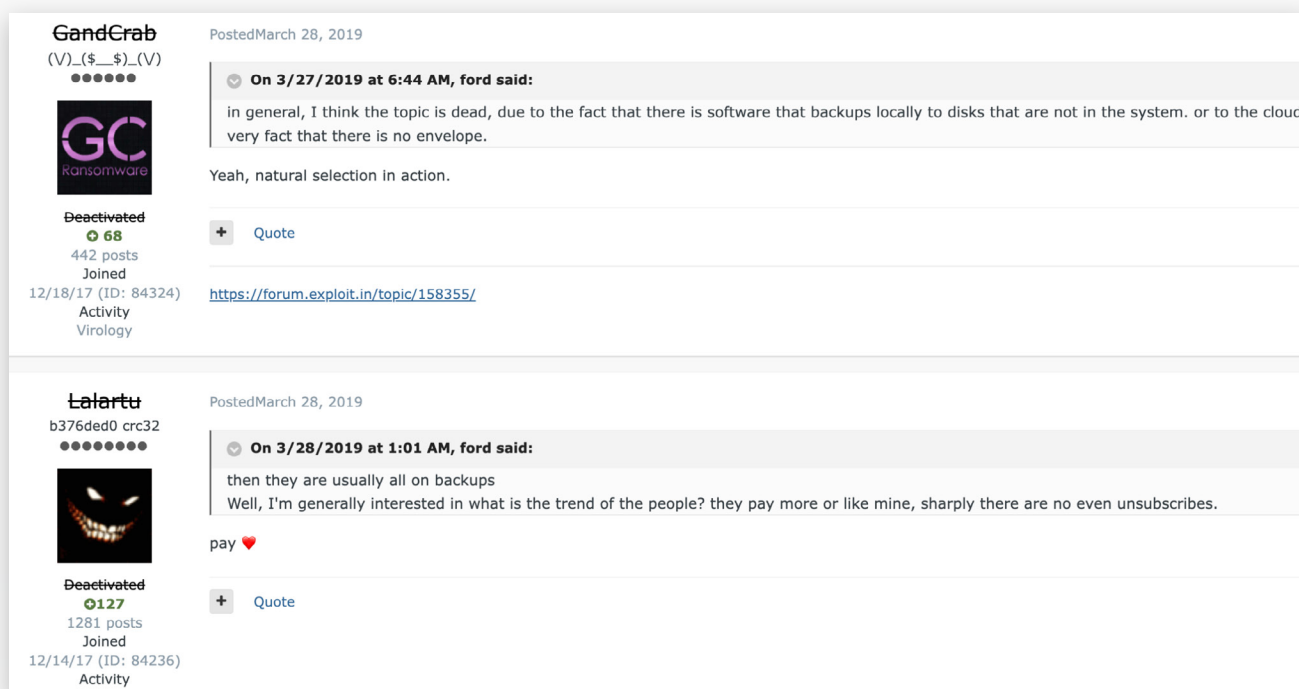


Figure 20: Lalartu in conversation about ransomware lockers with GrandCrab in 2019

Later, Lalartu went on to support Conti ransomware operations and used the moniker “Sheriff.” The relationship between the two men makes sense. You see, to work for a



ransomware gang as an affiliate hacker, you must pass an interview conducted by gang members. More importantly, you also need other known criminals to vouch for you.

Lalartu provided this validation between Bassterlord and REvil. Over the next year, Bassterlord worked ransomware attacks for REvil under the mentorship of the National Hazard Agency, learning and helping to conduct attacks.

I have spent a lot of time researching REvil over the years and wanted to see if Bassterlord could explain what happened to the primary persona behind the gang, UNKN (AKA UNKNOWN). This persona was used similarly to how Lockbit uses the “LockBitSupp” persona. Whoever was behind it was a senior member of the gang and had a lot of inside knowledge. UNKN was also the gang’s voice within the criminal underground community.

Based on the conversations this account had with senior members of other gangs, such as LockBit, I believe one of the primary people behind the account may have been REvil’s original leader. However, at the height of REvils tenure, UNKN disappeared, and the account went dark, leaving many questions within the ransomware community. Some speculated he was dead or arrested, while others thought he may have retired. I asked Bassterlord about UNKN, hoping to learn more.

Bassterlord told me that while supporting REvil ransomware operations, he tried to contact UNKN and was told there was more than one person behind the account.

I still believe, based on the tone, language use, knowledge and affiliations I saw associated with the UNKN account, that it was manned by the leader of the gang. Yet, I don’t see any reason for Bassterlord to lie.

I also agree that because this was the primary account used to manage relationships and recruit ransomware hackers, it likely required more than one person to maintain a presence and respond to requests promptly.

Bassterlord also told me something interesting about the REvil arrests. He said that the men whom the FSB arrested in January 2022 were not senior gang members but affiliates and low-level players. I suspected this and now have confirmation from someone with inside knowledge about the situation.

However, I did not know that **according to Bassterlord, one of REvils top affiliates went missing shortly after U.S. President Joe Biden and Vladimir Putin met in June 2021. This was the beginning of the investigation by the FSB and is how they obtained the names and information of the men they eventually arrested seven months later.**

**Bassterlord was told there was more than one person behind UNKN.**

As I stated in my previous work on REvil, the arrests had a major effect on the psyche of ransomware criminals who, for the first time, began to fear they may pay for their crimes. I asked Bassterlord about this and he told me after the arrests: ***“my psyche completely broke down and I started catching panic attacks also affected by the arrest of the REvils and I was even summoned to the FSB.”***

Fortunately for Bassterlord, he was questioned and released. This is also why I believe Bassterlord is still in the Lugansk region of Ukraine, which is under Russia’s control. If he had been in another part of Ukraine, there would have been no reason for him to respond to the FSB.

***I found Bassterlord’s affiliation with REvil fascinating, but so far, all of his responses discussed his criminal activities as a junior member of an affiliate team.*** This is still of interest, but I wanted to know about how he came to work with Ransomware groups as a direct partner. It is one thing to facilitate a small part of an operation but another to run and control your own team.

From the recent tweet shown in Figure 1, I knew that Bassterlord was now working and communicating directly with LockBit. I guessed that their relationship began when he supported them in this secondary role with the Hazard team, similar to his relationship with REvil, but I was wrong. Instead, the love story between Bassterlord and Lockbit began in a very familiar place. *The 2020 Summer Paper contest...*

## The 2020 Paper Contest

At the time, LockBit was not the ransomware gang they are today. They were still a lesser-known group and certainly not one of the big fish in the ransomware sea. In an attempt to change that, LockBit sponsored a contest on one of the underground Russian hacking forums.

You will be familiar with this contest if you read Volume 1 of the Ransomware Diaries. To participate, you needed to conduct research on various hacking and exploitation techniques listed in the contest rules, and LockBit would choose the winner and award them a \$5,000 prize for their work. An ad for the competition can be seen in Figure 21 below.

We're kicking off the ?summer PAPER CONTEST #4! With a prize fund - 15.000\$

```
#!/usr/bin/python
import socket
import sys
evil = "\n" * 1000
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
connectrs.connect(("192.168.111.128", 21))
s.recv(1024)
s.send("USER anonymous\n\n")
s.recv(1024)
s.send("PASS anonymous\n\n")
s.recv(1024)
s.send("MKO" + evil + "\n\n")
s.recv(1024)
s.send("QUIT\n")
```

**LOCKBIT**

Летний конкурс статей

**\$15000**  
призовой фонд

Напиши статью -  
заработай на отдых

Figure 21: LockBits hacking article competition as seen on an underground hacking forum

Bassterlord submitted a paper about using various phishing techniques to gain access to targets for ransomware attacks. The paper detailed methods to compromise a target with or without an exploit. I have not seen the paper, and Bassterlord would not share it with me, so I can only assume it had techniques he did not want to be made public.

More importantly, Bassterlord received notable mention as one of the top five finalists selected in the contest. In addition to winning a monetary prize, Bassterlord got the attention of LockBit, who asked him to join their operation as a direct hacker affiliate.

*I wrote my first article about my previous work experience on spamming for ransomware infections. I won and I received prize money from LockBit and an invitation to their affiliate program. -Bassterlord*

This was when Bassterlord became independent and began doing his own work. It's unclear to me if he still supported REvil or if that is when his affiliation ended, since skilled affiliates often double-dip and support multiple teams.

Either way, Bassterlord had the opportunity to make more money as a direct affiliate partnering with Lockbit, in comparison to being a paid member of an affiliate team. This would be similar to working for an organization as an employee vs. owning your own company. You can make money with both but should make a lot more with your own company.

I asked Bassterlord what it was like working directly for Lockbit. He said he made really good money, though he also worked for the Avaddon ransomware gang at the same time. Bassterlord said Avaddon was quite good at developing their affiliate program and focused heavily on ease of use and features. Avaddon supported their operation by asking for feedback and constantly trying to improve their affiliate user experience, according to Bassterlord.

*“Avaddon is quite good developing its affiliate program, quite adequate supports who are always in touch on all issues” -Bassterlord*

This is ironic because today, LockBit runs its operation with the same focus on “customer service and support” regarding its affiliate program. Not long after joining LockBit, however, Bassterlord decided to leave Avaddon’s program due to issues with their ransomware encryption capability, which allowed victims to regain access to their data without paying the ransom.

I asked Bassterlord if he was willing to share the names of any of the victims he attacked and ransomed while working with LockBit. He told me he was behind several high-profile LockBit attacks. I am not aware of them all, but one was against India’s Department of Revenue and the second against the **Uruguay Navy**. Additionally, Bassterlord said he still has their data.

It is unclear to me if Bassterlord took time away from ransomware or moved on to partner with another crime syndicate, but sometime in 2021, Bassterlord stopped working with LockBit. Despite this, Bassterlord maintained his relationship and helped identify and fix a bug in LockBit ransomware in March 2021. This was before LockBit began its bug bounty program, so I don’t know if LockBit rewarded him, but Bassterlord clearly was in good standing, which explains how he was able to return later in March 2023.

Since March, Bassterlord has been busy. One of his first victims since rejoining Lockbit was an Australian-based company. He did not tell me the victim’s name, but the day before our conversation, on March 16, Australian transport company, Booth Transport, was listed on LockBit’s data Auction site.

***According to their website, Booth is “Australia’s Top Bulk Food, Container Transport & Logistics Providers.***

To be clear, I can’t confirm that Booth was Bassterlord’s victim. Based on my conversation and research, in combination with the timing and location of the breach, I can say with medium confidence that this was likely Bassterlord’s and his team’s work. However,

Bassterlord was behind multiple attacks in March, amongst several posted to LockBit's site, making it difficult to validate.

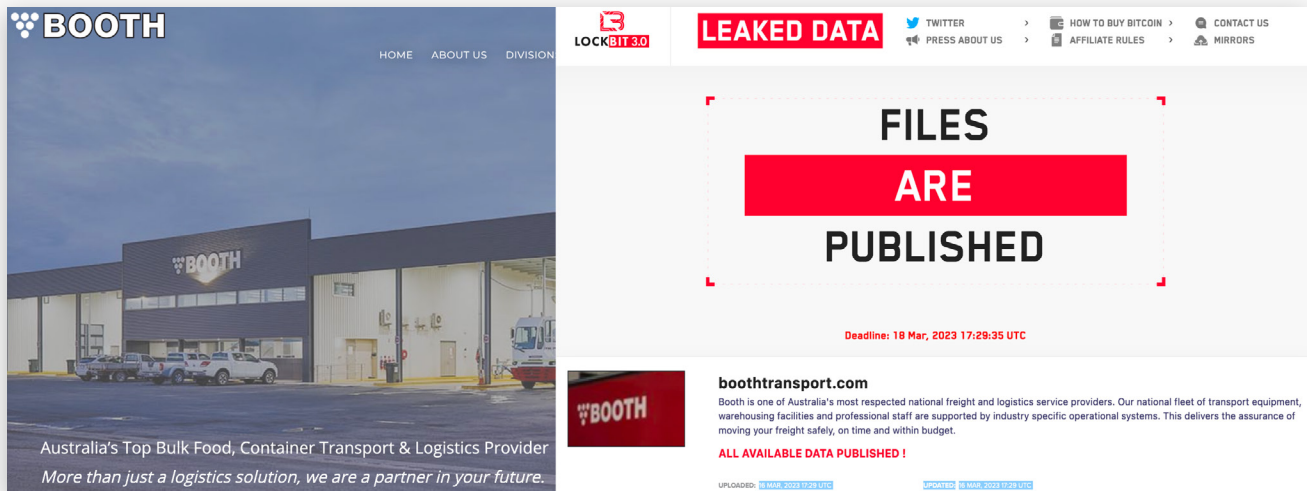


Figure 22: Booth Transport listed as LockBit's latest victim on their data auction site.

On March 27, according to Bassterlord, another Australia-based victim paid a ransom. An image posted by Bassterlord as evidence of the payment can be seen in Figure 23, below.

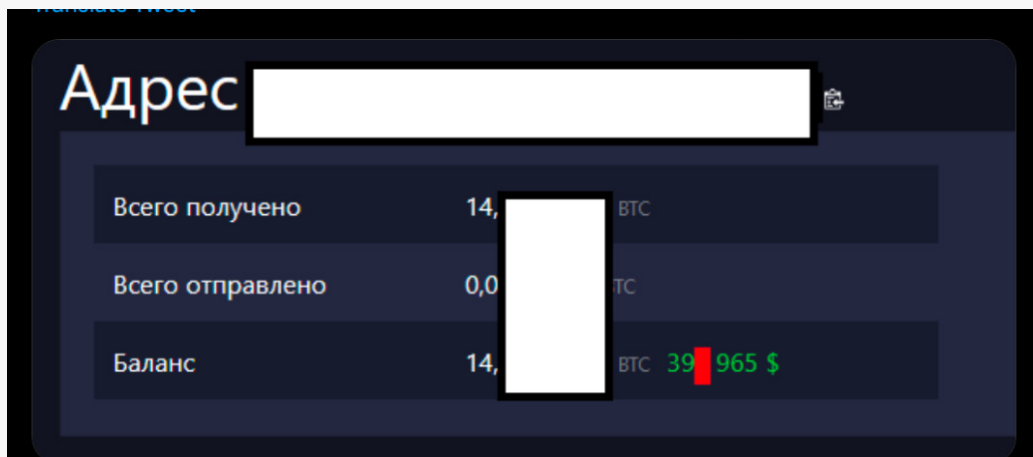


Figure 23: Evidence of payment posted by Bassterlord

Bassterlord also discussed the Maximum Industries breach. Maximum Industries is a contractor supporting Space X. If you recall, LockBit planned to release sensitive engineering and design-related documents that Maximum Industries created for Space X.

Once again, I do not know the extent, if any, that Bassterlord played in this ransom, but he was very knowledgeable and had information I would only expect from someone close to the attack.

He also made a post on Twitter insinuating that the initial access into Maximum Industries came from a phishing attack, which is his expertise, as seen in Figure 24 below.



Figure 24: Bassterlord [post](#) on SpaceX / Maximum Industries

I have always said the ransomware community is much smaller than people know. Bassterlord’s knowledge of the attack may originate from his relationship with LockBit, but he also may be the actor behind the operation.

# Does Not Play Well With Others

I mentioned earlier that Bassterlord came across as a likable person when I spoke with him, yet, he had a very different persona publicly. The difference in personality may be due to the fact that I wanted Bassterlord to feel comfortable talking to me, and I was neutral and friendly in my approach.

While we will never be friends, that does not mean we have to be enemies either. I honestly try to remember this is my job, it's not personal, and I do my best not to judge people, though it can be difficult at times. But one thing I always maintain is who I am and how I conduct myself. If you are going to put yourself out there, then commit to it or don't say anything.

You see, after Bassterlord made a strange post referencing the TV show Breaking Bad, a malware researcher decided to leave an unfavorable comment on the post. You can see Bassterlord's response in Figure 28.

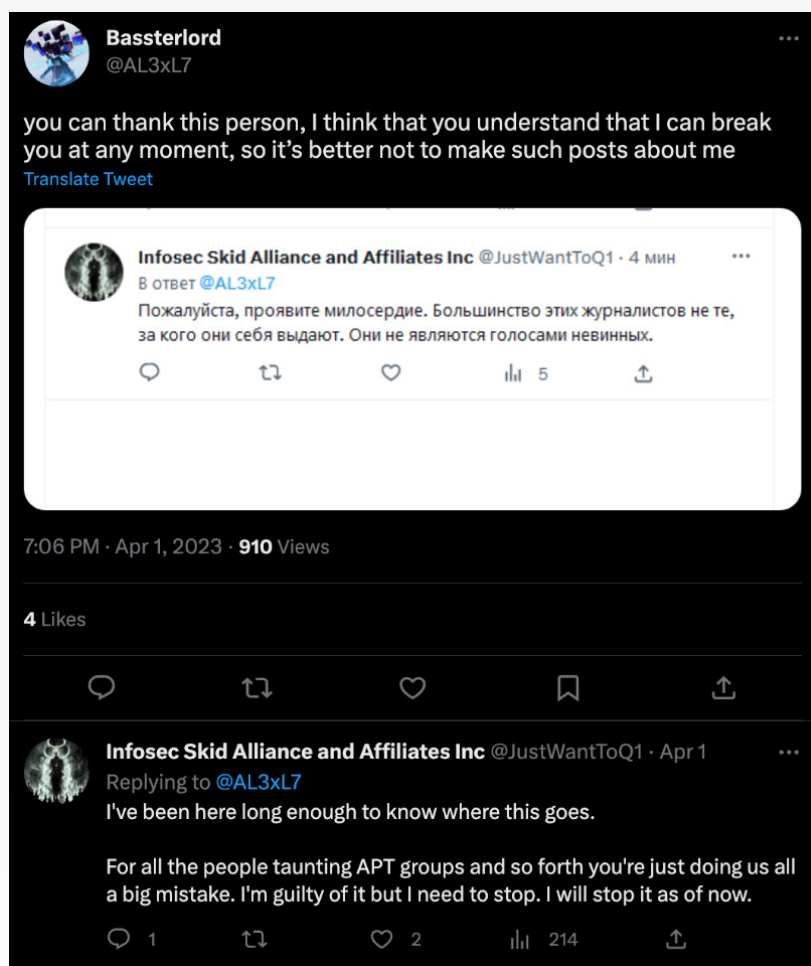


Figure 25: Skid alliance [tucking their tale](#) and running

This type of exchange does no good. If you are going to challenge a bad guy, then stand your ground, or don't do it at all because it makes the rest of us look weak. I assure you, we are not all weak.

There are many of us that put ourselves out there every day, even with the risk of physical harm. If everyone backed down like this, we would not have a chance in our fight against criminals like Bassterlord.

On the other hand, you have researchers like 3xp0rt, who, similar to Bassterlord, is from Ukraine. I bet 3xp0rt especially hates hackers from Ukraine, like Bassterlord, who support Russia. 3xp0rt had a special message for Bassterlord:



Figure 26: Altercation between 3xp0rt and Bassterlord



I began this research with the intent to focus on the connections to ransomware gangs and their victims. Yet, after engaging Bassterlord, the focus changed, and the man behind the mask and his life events took their own form. I saw this as an opportunity to profile a ransomware affiliate, which I have never done. I realized this was an opportunity to understand how a person goes from living a lawful life to becoming a ransomware criminal.

## Is This Goodbye?

Over the course of my conversations, Bassterlord stated that he had issues with panic attacks, amongst other health concerns, and previously traveled to Russia where he was diagnosed and treated. I believe the condition is likely worsening due to stress caused by the fear that Prodaft has released his identity to law enforcement. This may provide insight into what Bassterlord did next.

On March 28, 2023, Bassterlord posted the following message on Twitter:

*I will live like an ordinary person ... I hope I have not offended anyone and will not return to this (ransomware) again. In any case, I will remain in the history of Ransomware.*  
-Bassterlord

Around the same time, VX-Underground tweeted an image of a Tox conversation in which Bassterlord notified LockBit of his departure from their program. While he was leaving, the rest of his team would continue to operate.

I am skeptical and unsure if I believe that Bassterlord is really walking away from ransomware. Bassterlord had received a lot of public attention since Prodaft obtained his manual. He feared over who may come for him if they had his real identity. He also feared the FSB, who previously summoned and questioned him.

Still, it would be easy for Bassterlord to fake his retirement. He has a team, the National Hazard Agency, which I believe he now leads. Bassterlord could simply fall into the background, stop making public posts, and allow someone from his team to become the voice. How would we know? Bassterlord could keep committing ransomware crimes and continue growing his wealth. I can't prove this, but I believe it to be true. Additionally, I asked LockBit if Bassterlord really retired.

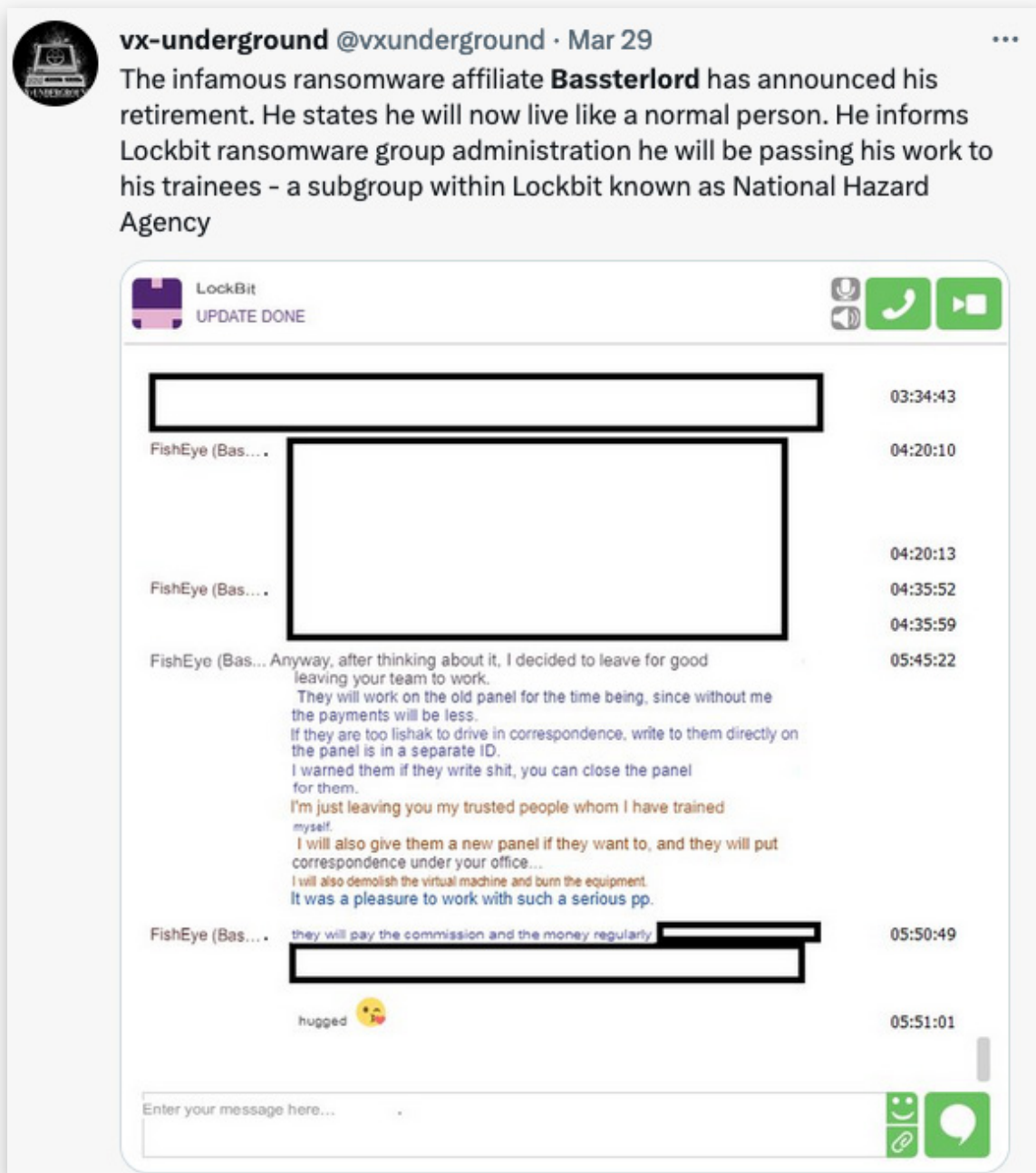


Figure 27: Bassterlord [notifies](#) LockBit of his departure from their affiliate program

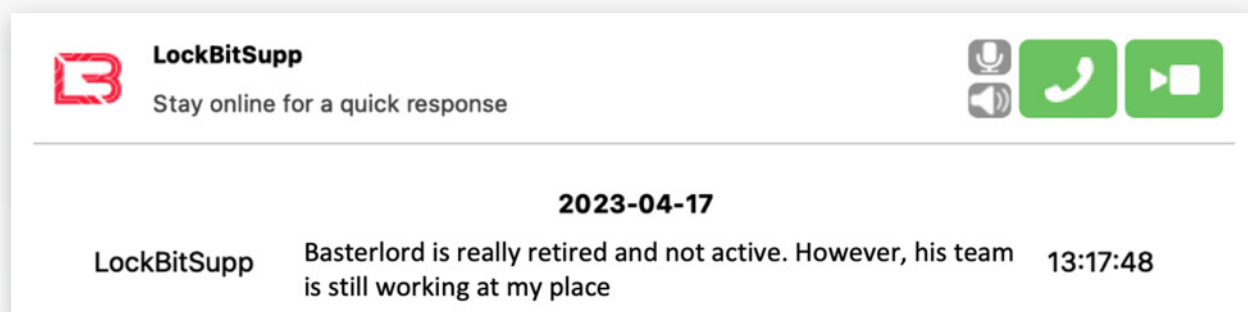


Figure 28: LockBit comments on Bassterlord's retirement

LockBit says it is true, however his team actively works LockBit ransomware attacks. Bassterlord also receives a percentage of profit that his team makes from their attacks. This may not prove Bassterlord still leads the group, but it certainly incriminates him with the crime.

Shortly after, Bassterlord changed his profile. No longer was it his persona, but instead, it is his team's. This may not prove my theory, but it certainly supports it. If he was really going to retire, would he still need to maintain a presence on criminal forums? Now he can continue to communicate under the persona and cover of his team.

You can see the profile change below. Visibility into the former profile name is only available to previous followers for a limited timeframe, then it disappears. After that, unless you have prior knowledge, you would never know the account's former alias.

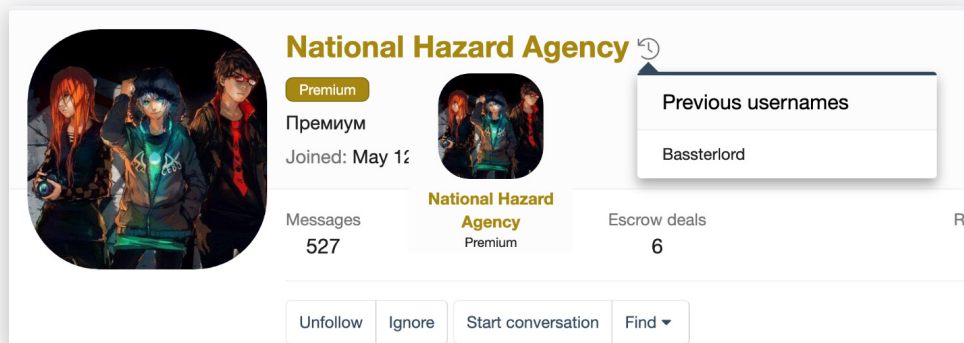


Figure 29: Bassterlord changes his persona to reflect his team's name

Bassterlord was not alone in celebrating his pretend retirement. Prodaft made their own celebratory Tweet, which, to say the least, triggered Bassterlord.


*I know why you didn't publish the manual and you know exactly what's inside! So don't go hype on my leaving I will always have an answer and believe me you will choke on it! You, specifically, had nothing to do with my leaving! -Bassterlord*

Time will tell, but I do not think this is the last we will see of Bassterlord. Regardless, if Prodaft did identify him, he will be looking over his shoulder for the rest of his life.




**PRODAFT**   
@PRODAFT



New goal unlocked  : Doing your job so well that the threat actor decides to retire 

Another interesting turn happened in the deep waters of underground forums when a threat actor Bassterlord announced his retirement.

If you remember the news about the ransomware manual we revealed a few weeks ago, then you know Bassterlord was the mastermind behind it. Since the manual was published, it looked like law enforcement authorities started eyeing this particular individual, so he decided to...live like a normal person from now on. Allegedly having enough money (of questionable origin) to do so, he decided to leave his legacy to the rest of the team.

According to his own words, they will continue working on the C2 panel and keep infecting victims. Well...we will see for how long. Good to know where we need to look in the future then... 

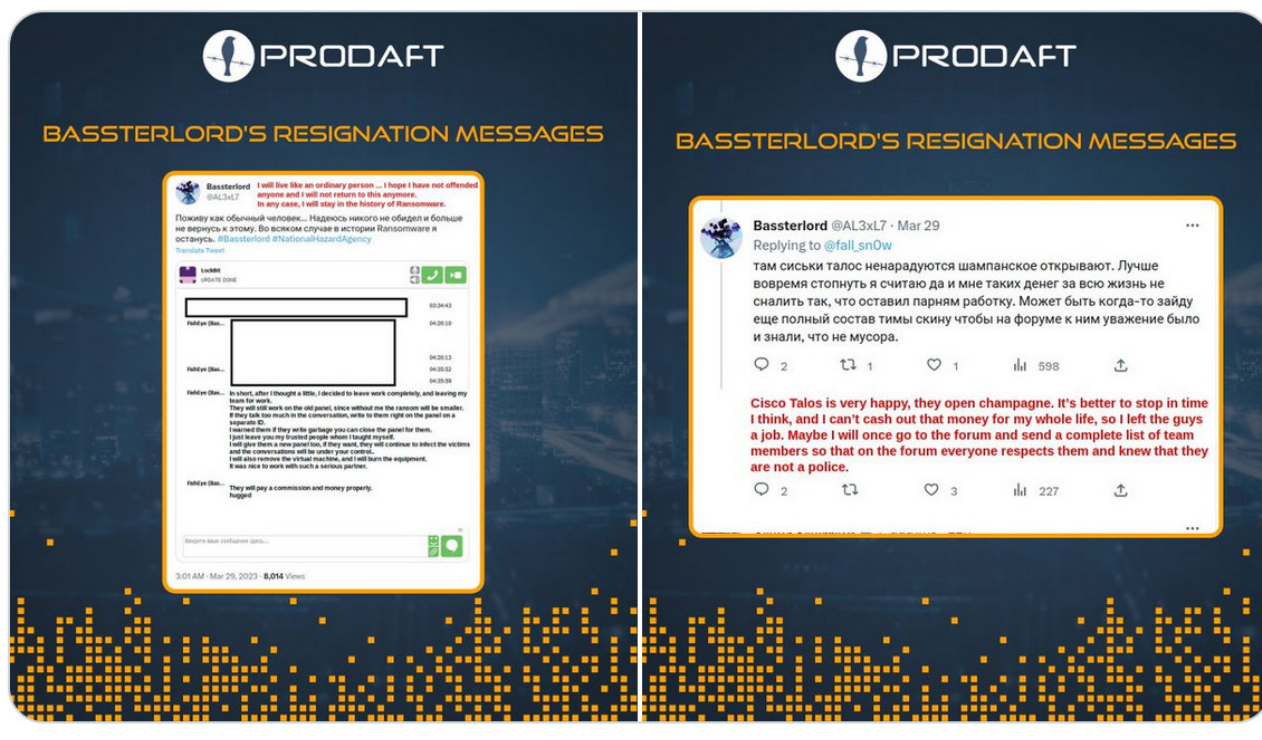


Figure 30: Prodaft's [victory lap](#)

# Don't Look Back

I have not spoken with Bassterlord since the end of March 2023, and unless my report somehow angers him, I don't think I will ever hear from him again. Still, over the course of this investigation I have learned a lot about both the internal operations of ransomware gangs and how affiliates operate.

While this report is different from anything I have written in the past, I don't think I have ever published research without a diagram to bring everything together visually, and I don't intend to start now!

As Bassterlord makes his exit, let's look back at his criminal career, the connections he made, and the victims he hurt.

Figure 31 displays both the criminals and gangs Bassterlord partnered with, in addition to the companies he extorted over the course of his criminal career.

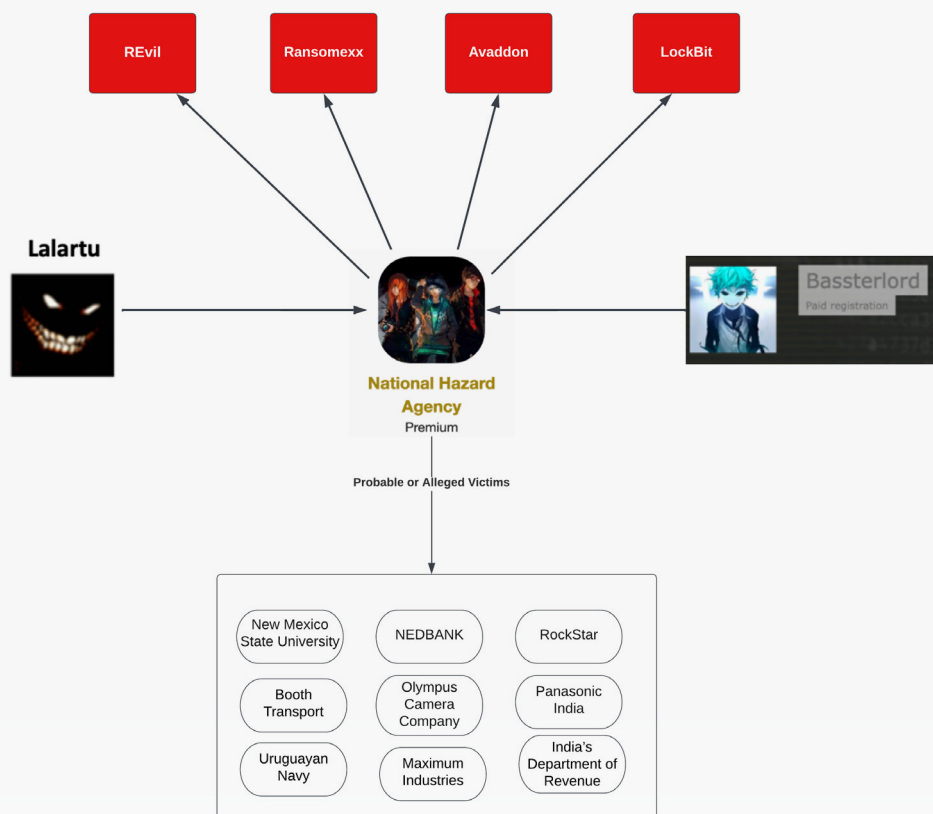


Figure 31: Bassterlord Association Diagram (do not use for attribution)

Figure 31 is only based on the targets and associations I am aware of, and in reality, the list is likely broader.

# Final Entry

Today, I see Bassterlord for who he is. I see his greed, his lies, and even his pain. More importantly, when I look behind his mask, I see a thief who lives in darkness, yearning for acceptance and fame from the criminal community.

Unfortunately, criminals were the only ones to extend a hand when Bassterlord needed help the most. What he did not realize is that these men were simply using him. They never cared about him and they saw Bassterlord as a vulnerable person they could exploit to make themselves richer. Bassterlord, these are not your friends.

Bassterlord's turning point occurred after his family accrued great debt to treat his mother's condition. Ironically, Bassterlord partners with ransomware gangs who victimize and extort both hospitals and medical facilities to benefit their own wealth, preventing patients from receiving life-saving treatment.

Bassterlord's partner, LockBit, even targeted a children's cancer hospital just a few weeks prior to Bassterlord joining the gang. Bassterlord is not considering how it would have felt if he and his family had been denied treatment because of a cyber-attack when his mother was ill. Now, he supports a criminal organization that puts others in that exact situation.

I don't think Bassterlord believes he will be arrested, ***though he is easier to reach in Ukraine as opposed to Russia.*** I don't know how Bassterlord's story will end, but I don't think it will end well.

At best, under the protection of the Russian government, Bassterlord will remain free, spending the rest of his life paranoid, living in the shadows supporting the country that invaded his home. It is likely that foreign governments and law enforcement agencies know exactly who Bassterlord is. If Russia does not win this war, or at a minimum, maintain the Lugansk region of Ukraine, he may have a knock on the door sooner than he thinks.

Bassterlord, I know you are reading this, and I have a few parting words. It's not too late to get yourself and your family out of the warzone you call home. You have access and inside knowledge into some of the top ransomware gangs — especially LockBit. Leverage this, while you still can.

I can connect you to people and agencies that can help if you are willing to work with them. If you don't take advantage of the opportunity in front of you, you will spend the rest of your life looking over your shoulder. You know how to reach me, ***but your leverage has an expiration date, and time is running out.***

***Good luck.***

#### ABOUT AUTHOR:

### Jon DiMaggio, Chief Security Strategist

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.

 @UseAnalyst1

 [analyst1.com/blog](https://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.