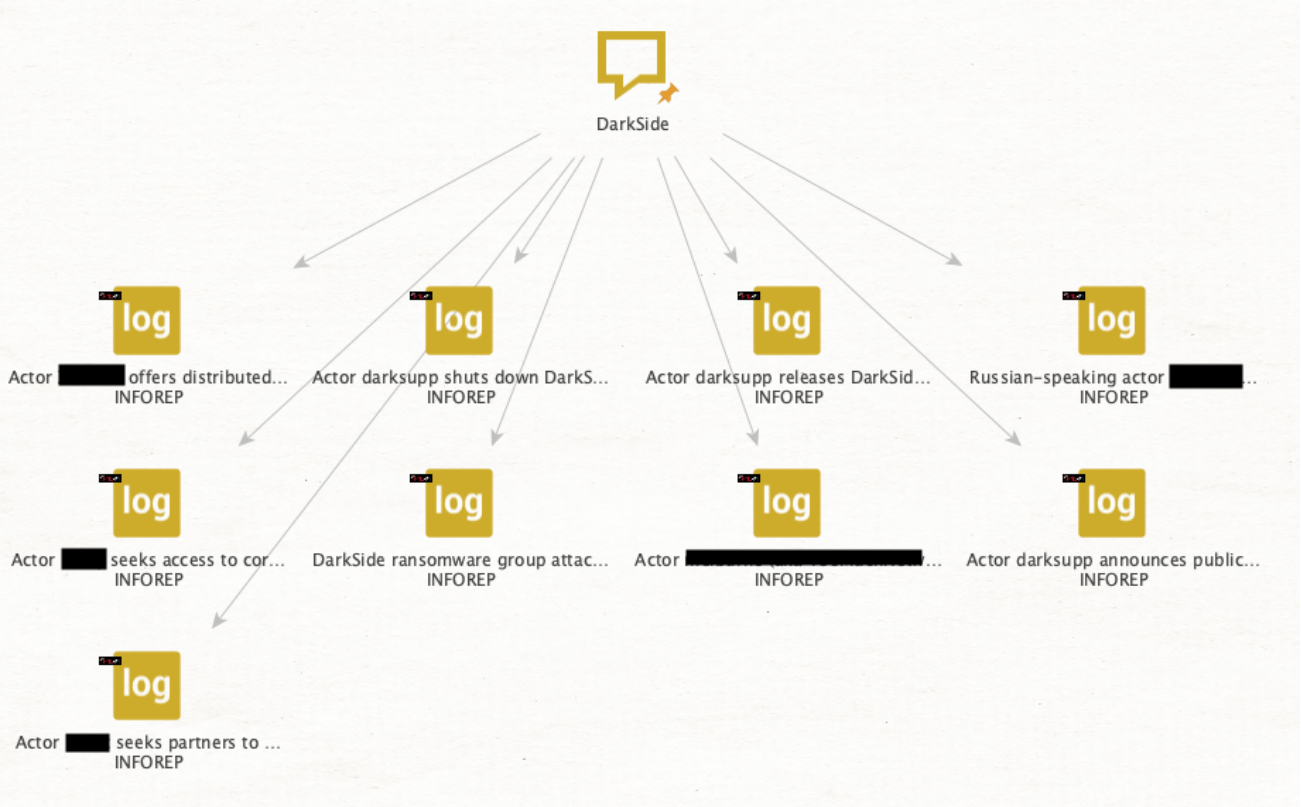
Chasing DarkSide Affiliates: Identifying Threat Actors Connected to Darkside Ransomware Using Maltego & Intel 471

maltego.com/blog/chasing-darkside-affiliates-identifying-threat-actors-connected-to-darkside-ransomware-using-maltego-intel-471-1/



22 Jun 2021 Cyber security investigation tutorial

Liv Rowley

Key Points:

- The May 7, 2021, ransomware attack against Colonial Pipeline is perhaps the most infamous example of a financially-motivated ransomware attack.
- The attack has been attributed to the DarkSide ransomware gang. While DarkSide has folded since the attack, the affiliates that fueled the gang's successful Ransomware-as-a-Service operation are likely continuing their activity.
- Using Maltego and information from Intel 471's reporting and forum data, we can identify six aliases with connections to DarkSide.
- Identifying affiliates is critical to fully understanding the ransomware ecosystem and those who contribute to it.

About DarkSide Ransomware 🔗

The attack against Colonial Pipeline represents one of those rare moments where cybersecurity crosses over into mainstream news. In early May, Americans and others around the world watched as oil prices in the US spiked, the criminal gang involved scrambled to distance itself from the appearance of being in the pocket of Russia, and the firm behind one of the US's largest pipeline systems forked over a multimillion dollar ransom to their network's hijackers.

In the midst of this, the DarkSide ransomware gang shut down their operations and went underground, seemingly spooked by the high level of scrutiny the group has received. The group took down its public-facing "name-and-shame" blog and their cryptocurrency wallets were drained.

Just because DarkSide shuttered operations does not mean that those who have worked alongside DarkSide are retreating. Many of the most potent ransomware gangs in 2021 operate using a Ransomware-as-a-Service (RaaS) model, where crews behind the development and maintenance of the ransomware partner with freelance cybercriminals in order to break into corporate and other high-value networks. These freelancers, typically referred to as "affiliates," are responsible for the ransomware's distribution. These affiliates are temporary partners of the ransomware gang and may work for several ransomware gangs at a given time. Profits from the criminal scheme are divvied up between the gang and the affiliate, with the affiliate typically taking a larger share of the proceeds.

Following the Colonial Pipeline incident, it appears that the DarkSide gang as we currently know it has, at least for the moment, closed down shop. Many of their affiliates, however, are likely to continue operating, reaching out to other ransomware gangs in order to monetize their access.

Using Maltego and Intel 471 data, we can begin to form a picture of some of the known DarkSide affiliates.

Identifying Affiliates Using Intel 471 Reporting 🔗

To start, we will examine reports authored by Intel 471 that mention DarkSide. We will insert a phrase Entity and label it "DarkSide." From there, we will use the Transform **[Intel 471] Phrase to Report**. This will give us numerous reports that mention "DarkSide."

In order to protect the TTPs employed by Intel 471 researchers, we have obfuscated some of the details that appear in this blog. We are hoping that by showing this process, however, we can share what's possible when Maltego and Intel 471 are used together to power

investigations.

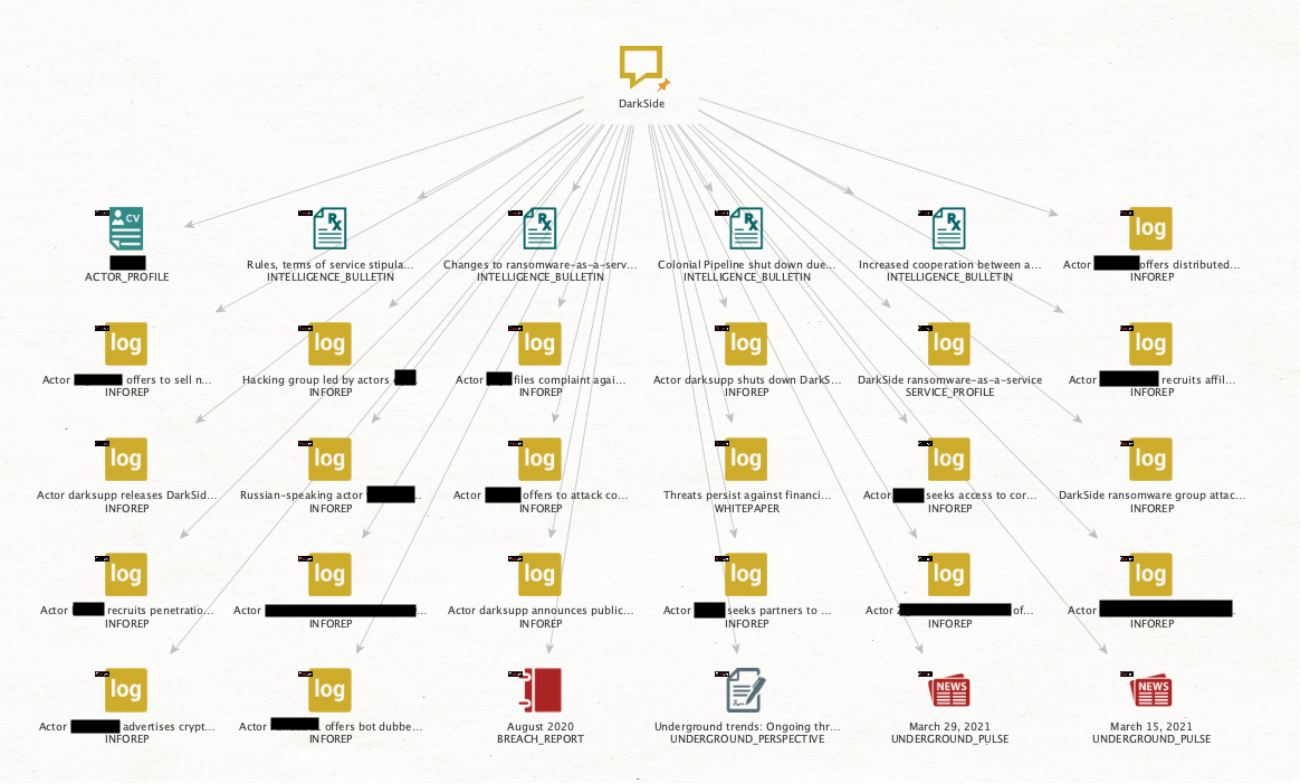


Image 1: Intel 471 reports that contain mentions of "DarkSide."

There are many different reports that are returned. For the sake of this investigation, we will focus on the intelligence reports (with the INFOREP label) and delete all the others. We now have 19 intelligence reports:

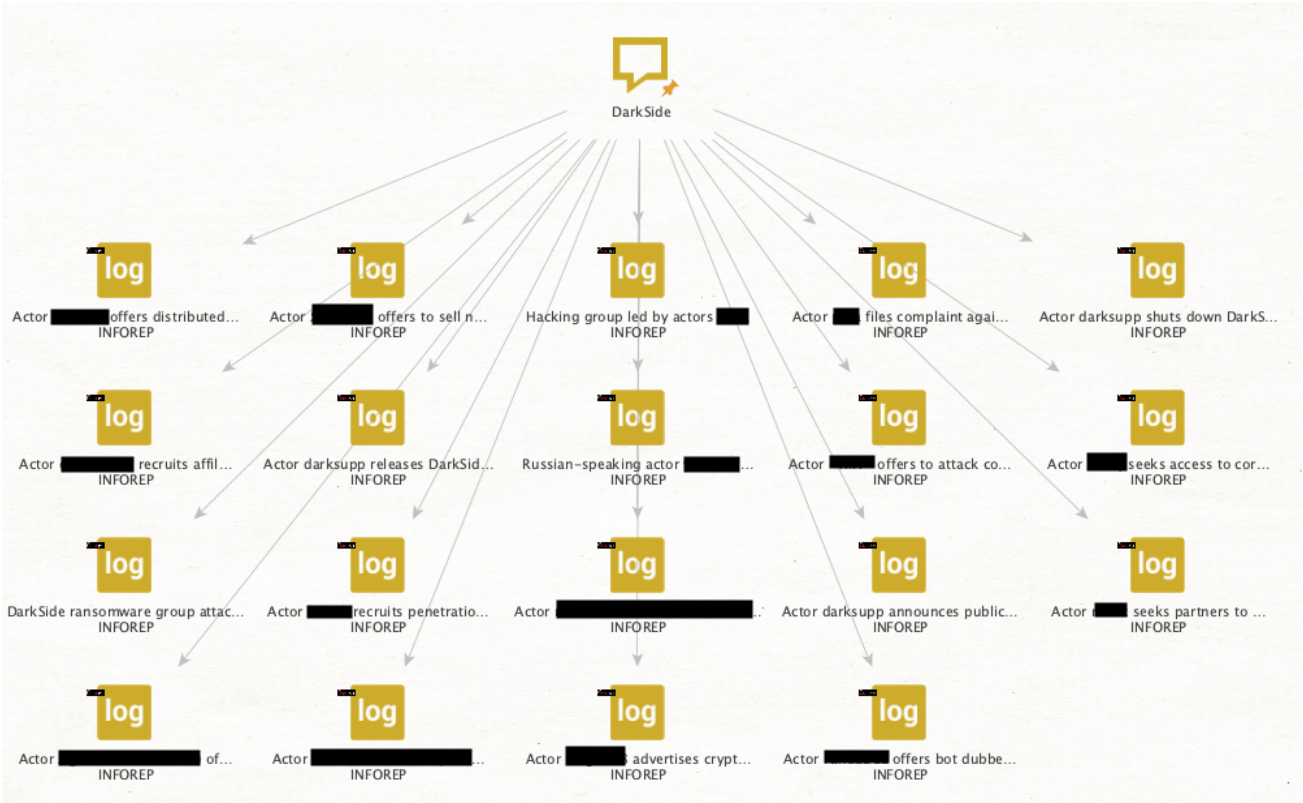


Image 2: Intelligence reports – labeled "INFOREP" – that contain mentions to DarkSide. We focus on intelligence reports in order to try to ensure that the data is most relevant to DarkSide (and not a broader trend report).

Now we must determine which of these reports are actually related to the DarkSide gang and their affiliates. When we view some of the reports directly in Intel 471's Titan portal, we see that a handful of the reports only mention DarkSide in passing; for instance, one report states that a certain threat actor has "denied using the DarkSide ransomware."

In order to work with the content most relevant to DarkSide, we will search for reports that contain the word "DarkSide" in their titles (and not only mentioned in the report body). We can do this by pressing **CTRL + F (CMD +F on a mac)** to open the finder bar and typing "DarkSide". This will now highlight all the reports, along with our initial phrase Entity, that contain the word "DarkSide" in the report's title. In order to select the reports that DON'T mention DarkSide in the title, we can click on the "**Invert Selection**" button (beneath "**Select All**" and "**Select None**" on Maltego's investigate tab). Let's delete those nine Entities that do not contain the word "DarkSide" in the report's title. We will also delete one additional report in which DarkSide is mentioned as an alias of a threat actor, and not related to the ransomware gang.

Note: if your results are a little different here, make sure that your finder search bar is NOT searching for the term "DarkSide" within the properties of the Entities by ensuring that "Properties" is unchecked in the finder bar.

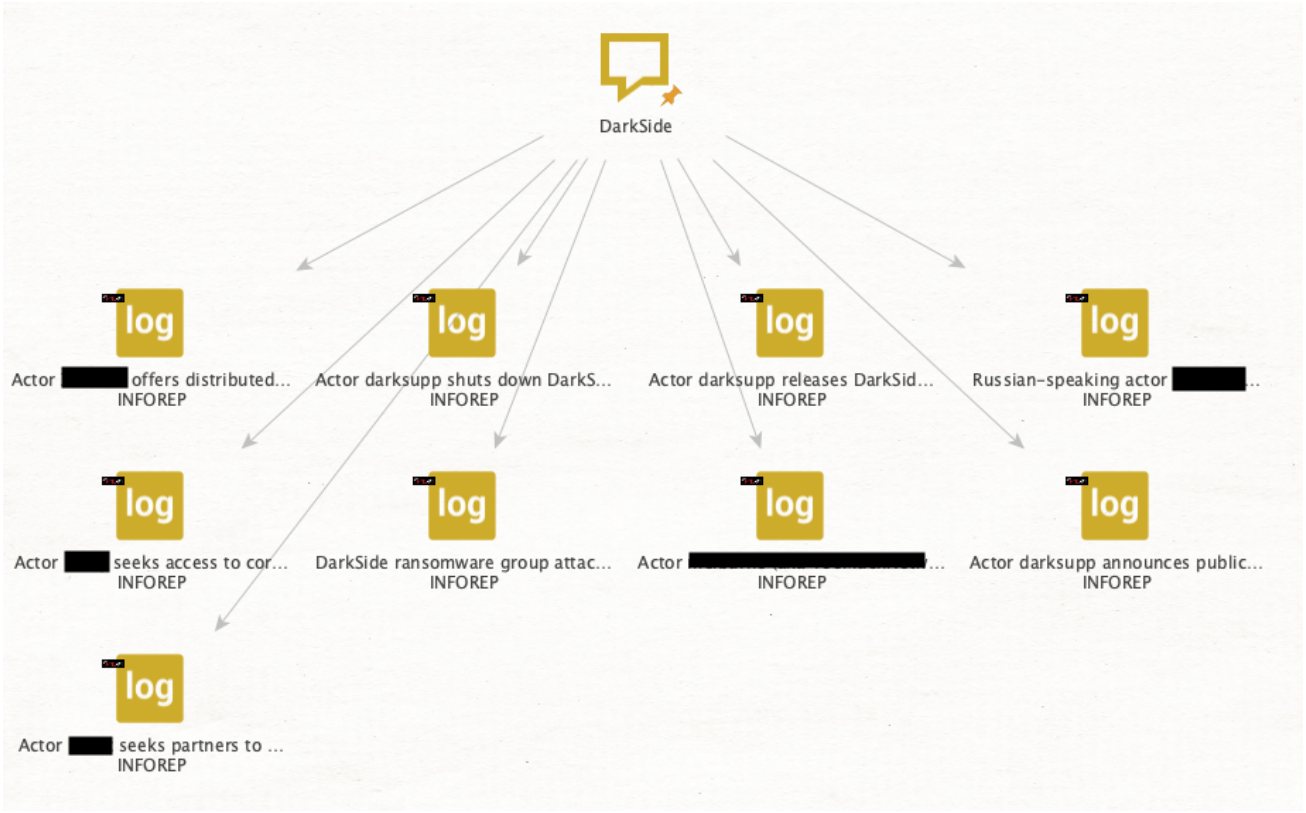


Image 3: Results of reports that include the word "DarkSide" in their title.

We now have nine intelligence reports authored by analysts at Intel 471 that appear to discuss the DarkSide ransomware gang.

Extracting Information on Relevant Threat Actors from Intel 471 Reports 🔗

We have nine intelligence reports that we've deduced are mostly likely to be related to the ransomware gang and their affiliates. We will now run the Transform **[Intel 471] Report to Entities**. This Transform will return lots of cool data from the reports, including emails, domains, Bitcoin addresses, and more.

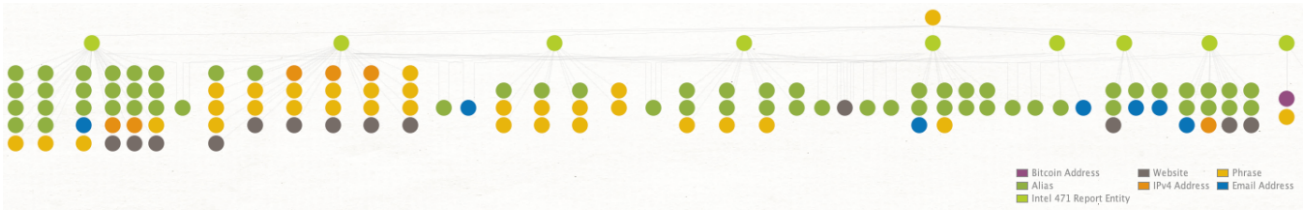


Image 4: Various interesting Entities are returned to us from the reports; we are just going to focus on the aliases.

For this moment though, we just want to concentrate on the aliases that are returned. An alias here is the username of a threat actor. There are 62 aliases returned, and we want to determine which among those are the most relevant threat actors. There are multiple ways an analyst can approach this problem; in this example, we will see which threat actors are mentioned in multiple intelligence reports. We will "**Select by Type** -> **Alias**" and click the "**Add Parents**" button. Now we have selected all the aliases, as well as the intelligence reports that mention those aliases. We want to copy that information to a new graph.

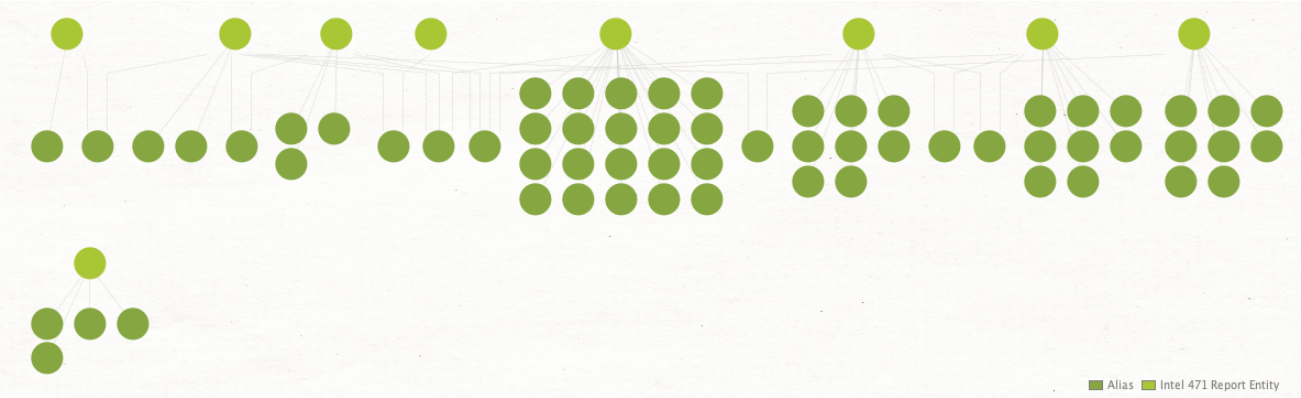


Image 5: The light green Entities represent intelligence reports, while the dark green Entities are aliases mentioned in that report. There are lots of aliases on this graph, so we must cut through the noise and identify the most relevant.

We can see several threat actors mentioned across multiple reports, while others are only mentioned in one report. We are not as interested in those threat actors who have only been written about in a single report, as these individuals are likely less important in relation to DarkSide. We can remove those from the graph by hitting "**Select Leaves**" and deleting them. Now we have aliases that have been mentioned in at least two intelligence reports, leaving us with eight aliases.

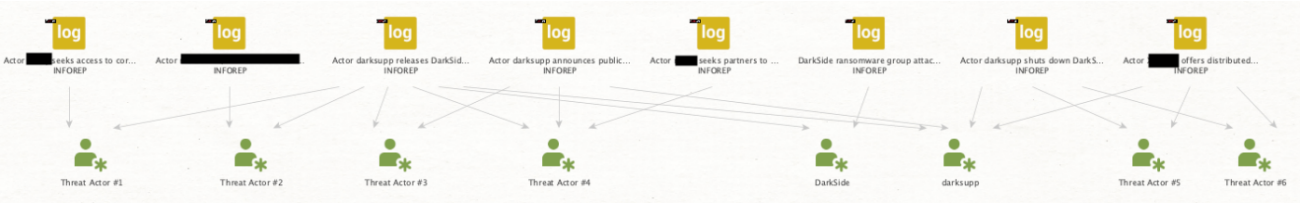


Image 6: Eight aliases appear in multiple DarkSide-related intelligence reports. The names of the threat actors who have not been publicly identified are substituted here with the placeholder "Threat Actor #x."

Some of these aliases are associated with DarkSide operators, such as "DarkSide" and "darksupp." The other six aliases, however, likely belong to threat actors closely linked to the group, as they were mentioned in multiple intelligence reports about DarkSide ransomware. It's possible that these may be affiliates of the gang.

Conclusion 🔗

We have identified eight threat actors who appear to be affiliates of the DarkSide ransomware crew. We can dig into those threat actors more – investigating which forums they are on, who their associates may be, what other ransomware gangs they may have been affiliated with, and how they might be gaining access to these environments.

While it is important to track ransomware gangs, it is also critical that we track RaaS affiliates. RaaS affiliates hold an important position in the ransomware ecosystem because of their specialization in getting a foothold in the networks of valuable targets. Their roles also allow them to enjoy a lot of flexibility, moving easily between ransomware gangs should one disappear or even just offer a more lucrative payment structure.

Intel 471 reporting can help us better contextualize who these individuals are, while Intel 471 forum data can allow us to see what these threat actors are sharing with their cybercriminal peers. Maltego allows us to take this trove of data and speed up our ability to conduct analysis as we pivot between different types of data. With Intel 471 and Maltego together, we can quickly identify and subsequently track these affiliates as the move between gangs and continue their illicit operations.

Don’t forget to follow us Twitter and LinkedIn and sign up to our email newsletter to stay updated on new use cases, tutorials, and event information!