





# MuddyWater

According to MITRE: “MuddyWater is an Iranian threat group that has primarily targeted Middle Eastern nations, and has also targeted European and North American nations. The group’s victims are mainly in the telecommunications, government (IT services), and oil sectors.” Currently we have few artifacts related to MuddyWater (‘Muddy’), indeed only Powerstats backdoor is actually attributed to it. Their attack are typically “hands driven”, which means they do not use automation lateral movement but they prefer to use opensource tools or sysinternal ones to deliberately move between target network rather than running massively exploits or scanners.



## MuddyWater TTP

Once landed inside a victim machine Muddy looks for local credentials and then moves back and forward by using such a credentials directly on the network/domain controllers. According to MITRE techniques (green) MuddyWater to take an entire target-network might take few months but the accesses are quite silent and well obfuscated. Again it looks like we are facing a group which doesn't need advanced exploitation activities but rather than advanced IT knowledge in order to move between network segments and eventual proxies/nat.

# APT33

According to MITRE: “APT33 is a suspected Iranian threat group that has carried out operations since at least 2013. The group has targeted organizations across multiple industries in the United States, Saudi Arabia, and South Korea, with a particular interest in the aviation and energy sectors.” Analyzing the observed TTPs we might agree that this threat actor looks very close to MuddyWater. If you take a closer look to the Muddy Graph (in the previous dedicated section) and APT33 graph (following) you will see many similarities: many tools are shared, many techniques are shared and even artifacts **Powerstats** (Muddy) and **Powertron** (APT33) share functions and a small subset of code (even if they have different code bases and differ in functionalities). We have more information about APT33 if compared to MuddyWatter, but similarities on TTPs could induce an avid reader to think that we might consider APT33 as the main threat actor while MuddyWater a specific ‘operation’ of the APT33 actor.

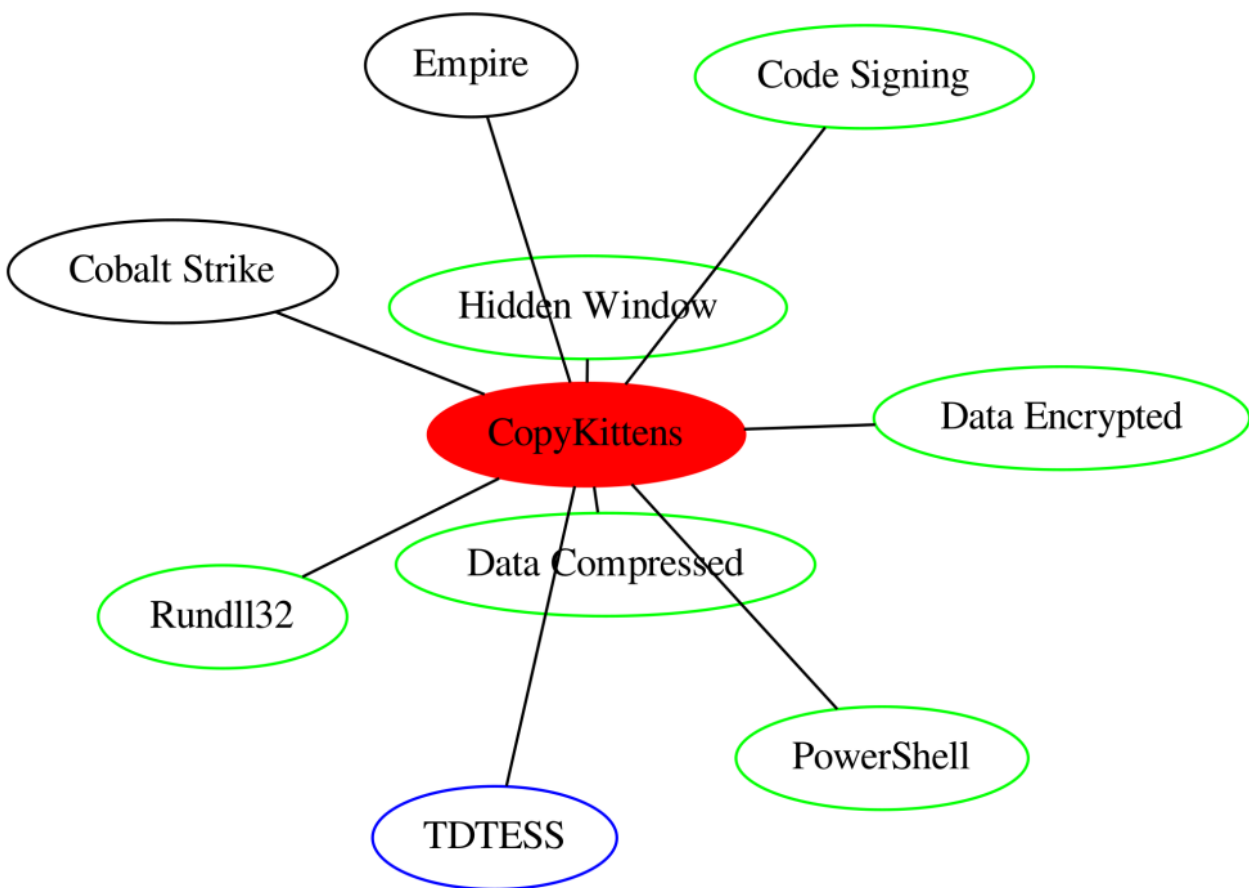


### APT33 TTP

But if you wonder why I decided to keep them separated on such personal and preliminary analysis you could find the answer in the reason in why they do attack. APT33 showed destruction intents by using Malware such as **shamoon** and **stoneDrill**, while Muddy mostly wants to “**backdooring**” the victims.

## CopyKittens

According to MITRE: “CopyKittens is an Iranian cyber espionage group that has been operating since at least 2013. It has targeted countries including Israel, Saudi Arabia, Turkey, the U.S., Jordan, and Germany. The group is responsible for the campaign known as Operation Wilted Tulip.” CopyKittens threat actor actually differ from the previous ones. First of all we see the usage of CobaltStrike, which is an autonomous exploiting system (well actually is much more, but let me simplify it). Cobalt and Empire (a post exploitation framework) taken together would allow the attacker to automate lateral movement. Which is a damn different behavior respect to previous actors. CopyKittens would make much more noise inside an attacked network and would be easier to detect if using such automation tools, but on the other hand they would be much more quick in reaching their targets and run away.



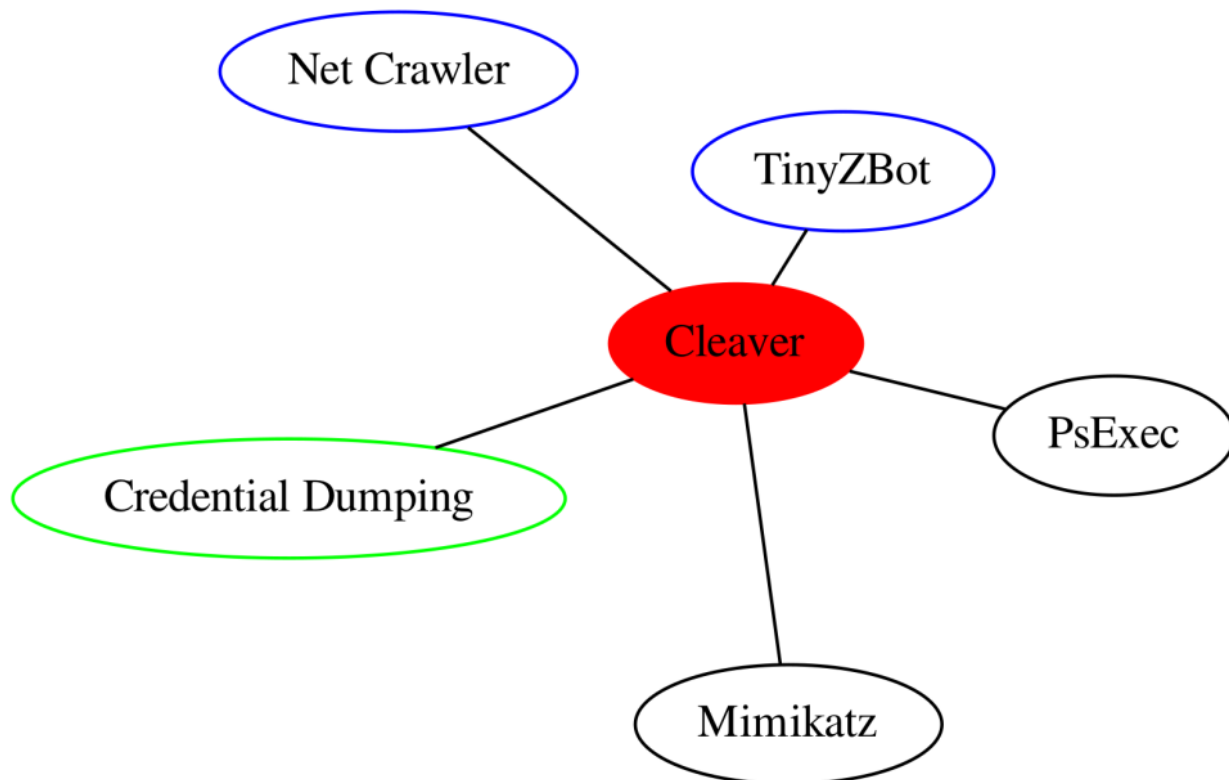
#### CopyKittens TTP

One more characteristic is the “code signing”. While in OilRig, MuddyWater and APT33 we mostly observed “scripting” capabilities, in CopyKittens we are observing most advanced code capabilities. Indeed code signing is used on Microsoft Windows and IOS to guarantee that the software comes from known developer and that it has not been tampered with. While a script (node, python, AutoIt) could be attribute to IT guys as well as developers, developing more robust and complex software ( such as: java, .net, c++, etc) is a skill typically attributed to developers. This difference could be significant in suspecting a small set of different people working on CopyKittens.

## Cleaver

---

According to MITRE: “Cleaver is a threat group that has been attributed to Iranian actors and is responsible for activity tracked as Operation Cleaver. [1] Strong circumstantial evidence suggests Cleaver is linked to Threat Group 2889 (TG-2889).” We have few information about this group, and as you might see there are few similarities. The usage of Mimikatz could be easily adopted for credential dumping, while TinyZBot is a quite interesting tool since it mostly implements spying capabilities without strong architectural design or code execution or data exfiltration.



### Cleaver TTP

Just like **Charming Kitten** (which is not included into this report since it is a quite ongoing mystery even if a **great** report from Clear Sky is available), Cleaver is a threat group that is responsible of **one** of the first most advanced and silent cyber attack attributed to Iran known until now (OpCleaver, by Cylance). Cleaver attack capabilities are evolved over time very quickly and, according to Cylance, active since 2012. They look like to have infiltrated some of the world economic powers (ref: here) such as: Canada, China, England, France, Germany, India, Israel, Kuwait, Mexico, Pakistan, Qatar, Saudi Arabia, South Korea, Turkey, United Arab Emirates, and the United States. In the very first page of the OpCleaver report, the author writes that Cleaver is one of the most advanced threat actors ever. Even if I might agree with Cylance, I personally do not have such evidences so far, so I personally cannot compare Cleaver threat actor to the previous ones.



the used Malware we might agree in aggregating Muddy close to APT33, actually the weight of shared code should be heavier compared to common tools or common techniques, but I did not represent such a detail into graphs.

However two different 'code experience' are observed. The first one mostly focused on scripting (node, python, autoIT) which could underline a group of people evolving from IT department and later-on acquiring cyersecurity skills, while the second observed behavior is mostly oriented on deep development skills such as for example: Java, .NET and C++. On MuddyWater and APT33 side, the usage of scripting engines, the usage of powershell, and the usage of Empire framework tighten together, plus the lack of exploiting capabilities or the lack in developing sophisticated Malware could bring the analyst to think that those threat actors hit their target without the need of strong development capabilities. On the other hand OilRig, Cleaver and CopyKitten looks like to have more software developing skills and looks to be mostly focused on stealth operations.

## **Conclusion**

---

In this post I wrote a preliminary and personal analysis of threat actors attributed by the community to Iran, comparing TTPs coming from MITRE and relations extracted from Malpedia. The outcome is a proposal to consider the numerous groups (OilRig, APT33, MuddyWater, Cleaver, etc..) as a primary meta-threat-actor and dividing them by operations rather real group.