Elizabethan England has nothing on modern-day Russia

blog.talosintelligence.com/2021/05/privateer-groups.html

This post was authored by *Warren Mercer* and *Vitor Ventura*

The threat landscape is changing. Organizations need to defend against an ever-evolving tranche of threat actors. For a long time, the lines that distinguish state-sponsored and crimeware groups were well-defined. We believe this is no longer the case. In today's landscape, there are groups that, although their modus operandi (MO) is consistent with

crimeware groups, act like state sponsored groups. This poses new challenges to the defending organizations as these groups become more prevalent and dangerous which, depending on the organization's risk profile, may require more attention.

In light of recent events, we believe it's time to recognize that a new category can be defined, one where the ransomware syndicates enjoy some kind of protection from Governments, even if not intentionally. Therefore, Talos proposes the term "privateers" to describe actors who benefit either from government decisions to turn a blind eye toward their activities or from more material support, but where the government doesn't necessarily exert direct control over their actions. Which in itself does not diminish the responsibility these governments share with these groups by protecting them or simply allowing them to operate by turning a blind eye.

State-related threats

It's easy to split state-related actors in two main categories: ones that have been directly associated with state structures, like the U.S.'s National Security Agency, APT28, APT29, APT1, and the ones that, in spite of not being directly associated with a specific state, there is a common agreement in the infosec community that they benefit from decisions that the state makes to support them.

The first kind of groups' (tier one) motivations, usually, are not monetary, and as such, they don't have a monetization scheme. They usually have small infrastructure, which is completely destroyed once the campaign ends or is somehow exposed. These are groups that try to make their operations as stealthy as possible that don't want to attract attention to themselves. In specific operations like SolarWinds, CCleaner or VPNFilter they act as stealthy as possible in the preparation/reconnaissance stage, knowing that the final act will probably expose them, hoping to execute as much as possible their agenda before exposure happens.

As one example of the second category (tier two), look at Gamaredon (or Armageddon or Arma, as some know them). The group is complex, originating from Ukraine in the wake of Russia's annexation of Crimea. They are not part of the traditional Russian intelligence apparatus, but we have high confidence that much of the intelligence they gather from their operations are passed to Russian interests. In this case, we have a state-related threat that isn't an element of the sponsoring state, but receives active support and direction from that state sponsor.

Gamaredon do not pinpoint their victims, quite the opposite they target large swaths of users. Their infrastructure is massive — they have hundreds of domains — and they do not significantly change their malware or infrastructure despite being exposed. However, they share the non-deterrence aspect of the tier one groups.

There are two other categories that are state related; "Mercenary" groups that a state can hire to perform specific actions and "privateer" groups we detail in the next section. Mercenary groups can often fall into the first tier of state-related categories based on the exact campaign they're asked to carry out, so we will not be detailing those here.

The "Privateer" groups

Privateer groups are not sponsored directly by a state and are financially motivated, but they do benefit from direct or indirect protection from that state. This frequently manifests as a lack of law enforcement action, even when requested through normal channels by other countries. The protecting state doesn't receive direct benefit from these groups, but it is shielded from their activities, which frequently target the geopolitical adversaries of the protecting state. There is also the possibility that the protecting state may pressure the privateer group to engage in specific actions or target specific entities.

The only other kind of actors that have this level of protection are the ones that operate directly on a state structure. For example, actors the U.S. Department of Justice charged for a cyber attack on credit reporting agency Equifax had direct connections to the China's People's Liberation Army PLA 54th Research Institute. The DOJ has carried out other indictments against state-sponsored actors including the Lazarus Group, a North Korean citizen involved in the WannaCry incident and the six GRU officers involved in several cases of computer hacking.

DarkSide could be considered one such "privateer" group. This ransomware family, which was recently responsible for targeting a major oil pipeline in the U.S., checks the target's keyboard configuration to avoid any user whose keyboard is in the Cyrillic language. Lockbit could also be considred a privateer group, given that an operator for that group told Talos that they would not target Russia or any Russian-allied countries.

It is worth noting that, historically, no ransomware operator has ever been detained in any of the Commonwealth of Independent Countries (CIS) as long has they don't target its member states. However, if a ransomware group targets any of these countries they will be investigated and taken down. An example of one such group is Lurk, which was linked to the Angler exploit kit. The operator behind Lurk was arrested in Russia after the group targeted Russian banks.

These groups usually fall in the crimeware category, however, we propose that they are not simple crimeware gangs. These are highly organized groups, with a plethora of support services they provide to their affiliates. Their operations and lack of deterrence from their home state makes them a persistent threat to the community. This cannot be said for typical spammers or ordinary password stealers. "Privateers" are in the "big game hunting" space, exfiltrating hundreds of gigabytes of information. This indicates a certain level of

sophistication. Although they don't stack up to top-tier state-sponsored groups, "privateer" groups are far more sophisticated than regular crimeware groups and should be identified as such.

"Privateer" groups criteria

Since we are introducing a new classification, we felt it appropriate to outline what makes a group a "privateer" in Talos' eyes. We have decided on the following criteria to identify when a group should be considered a privateer. There may be other considerations, but at a minimum, we believe the following must be met:

1. Benefit from, either directly or indirectly, state protection and/or tolerance.
2. The country does not cooperate with foreign law enforcement, intelligence services or offer extradition.
3. Big-game hunting victimology ie; large enterprise or governmental organisations.
4. It must have a sophisticated organization, i.e. has affiliates or third parties involved.
5. Potential for societal disturbance.

We are aware that some groups may not specifically check every box here and there is potential for this criteria to change. The privateer group should remain exclusive to actors who meet the aforementioned criteria.

Conclusions

The term "APT" has a broad meaning that's being used in more loose terms nowadays. This term often includes the state-sponsored groups. However, we believe state-sponsored should be referred as state-related and be split into three distinct categories: ones working on behalf of specific state organizations, ones closely related to state actors, but with no clear organization affiliation and with no apparent financial motivation, and, finally, ones that are not directly related to state organizations but benefit from state protection, directly or indirectly.

The first tier includes actors like the Lazarus Group (aka APT38), a state-sponsored actor carrying out attacks for direct gains for a nation-state. The second tier includes groups like Gamaredon and PROMETHIUM. These groups don't seem to be directly linked to state organizations but are believed to work for states. These don't share the same level of sophistication as prime APTs but are not primarily financially motivated.

Finally, we have groups like the DarkSide syndicate that we are referring to as "privateers." Privateers benefit from a certain level of state protection or acceptance without any real links to the states. These privateer groups are becoming increasingly prevalent and will likely significantly change the threat landscape in the years to come.