APT review of the year

By Vicente Diaz

Published: 2018-12-05 · Archived: 2026-04-05 13:16:26 UTC

What were the most interesting developments in terms of APT activity throughout the year and what can we learn from them?

Not an easy question to answer; everybody has partial visibility and it's never possible to really understand the motivations of some attacks or the developments behind them. Still, with the benefit of hindsight, let's try to approach the problem from different angles to get a better understanding of what went on.

On big actors

There are a few 'traditional' actors that are very well known to the security community and that everybody has been tracking for the last few years. It has been business as usual for these actors in 2018 or, if anything, perhaps slightly quieter than usual.

In reality, it is the doctrines and modi operandi of these groups that determine how they react in the event of their operations becoming public knowledge. Some actors will simply abort their campaign and go into clean-up mode, while others carry on as normal. In order to do so, it is common for some of these actors to simultaneously work on several sets of activity. This allows them to compartmentalize operations, and if they are discovered, they simply improve their toolset to avoid detection next time.

We traditionally find many Russian-speaking actors in this second group, and we would like to highlight the 2018 activity of Sofacy, Turla and CozyBear.

Sofacy was probably the most active of the three. Throughout the year we detected it in various operations, updating their toolset and being blamed by authorities for several past operations. We have seen the actor deploying Gamefish and an updated version of its DealersChoice framework against embassies and EU agencies. One of the most high-profile incidents was abuse of Computrace LoJack by this actor in order to deploy its malware on victim machines, in what can be considered a UEFI-type rootkit.

Zebrocy is one of the tools traditionally used by this actor, but in reality the collection of cases where this tool was used can be considered a subset of activity in its own right. We saw different improvements for Zebrocy's subset, including a new custom collector/downloader, new VBA implementing anti-sandboxing techniques and new .NET modules.

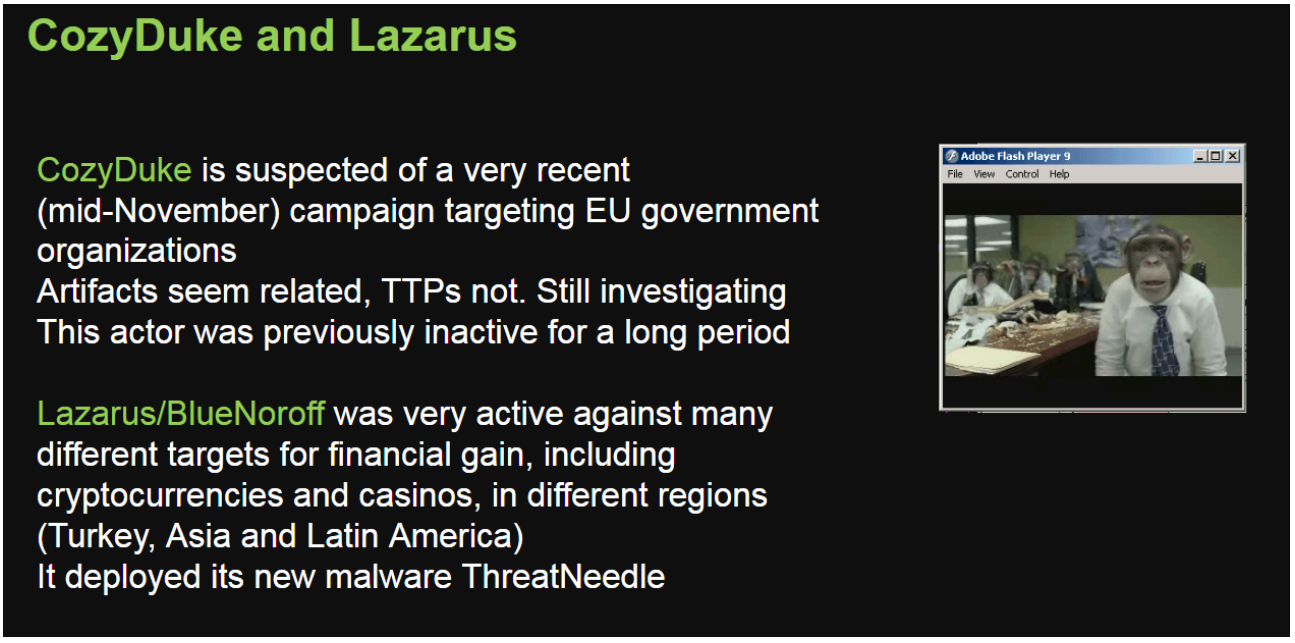
During the year we understood that Sofacy appears to be changing at a structural level and is possibly already being split into different subgroups. With the OlympicDestroyer analysis we learnt that this highly sophisticated false flag operation was somehow related to Sofacy. However, we later observed more activity by the OlympicDestroyer subset in Europe and Ukraine, and it was then that we decided to treat it as the entity we call Hades.

Of particular interest is how, after the publication of the GreyEnergy set of activity that is believed to be a continuation of BlackEnergy/Sandworm, we found additional overlaps between GreyEnergy and Zebrocy, including the use of the same infrastructure and the same 0-day for ICS.

All that seems to link this new Hades actor with the Zebrocy subset of activity, traditionally attributed to Sofacy, as well as part of the BlackEnergy/GreyEnergy/Sandworm cluster.

Regarding Turla, we didn't spot any big structural changes like those described above, though we did see this actor using some interesting implants such as LightNeuron (targeting Exchange servers as described in our previous APT summary for Q2), as well as a new backdoor that, according to ESET, infected Germany's Federal Foreign Office in 2017, as well as other entities in the European Union.

We discovered this actor using a new variant of its Carbon malware in its traditional activity of targeting embassies and foreign affairs institutions throughout the year. It also started using a new framework that we call Phoenix, as well as (unsurprisingly) transitioning to scripting and open source tools for its lateral movement stage.



Finally, some potential CozyDuke activity was detected during November 2018, apparently targeting diplomatic and governmental entities in Europe. The TTPs do not seem to be those that are usually attributed to this actor, which opened the door to speculation about this malware being used by a different group. The facts still seem to confirm that the malware used is attributable to CozyDuke. We are still investigating this new campaign by an actor that has been inactive for months.

It's also worth mentioning Lazarus and BlueNoroff activity in 2018. We observed constant activity from this group targeting different regions including Turkey, other parts of Asia and Latin America, as well as various lines of business that provide it with financial gain, such as casinos, financial institutions and cryptocurrencies. In its more recent campaigns it has started deploying a new malware we call ThreatNeedle.

On false flags

It comes as no surprise to find false flags every now and again, sometimes implemented rather naively. But this year we witnessed what should be considered (so far) the mother of all false flags (more details can be found here). Other than the technical details themselves, what is also worth considering is the real purpose of this attack, and why these sophisticated false flags were planted in the malware.

The first obvious conclusion is that attackers now understand very well what techniques are used by the security industry to attribute attacks, so they have abused that knowledge to fool security researchers. Another consideration is that the main objective of an attack is not necessarily related to stealing information or disrupting operations – imitating an attacker might be more important.

This may actually be part of what some actors are doing at the moment. There are several groups that were apparently inactive for some time but now appear to be back. However, they are using different TTPs that are not necessarily better. As we shall see later, a couple of examples may be CozyDuke and APT10. As a purely speculative thought, it might be that their traditional toolset is now being used by different groups, maybe still related to the original operators. The purpose might be to make attribution more difficult in the future, or simply to distract from their real ongoing operations.

The whole OlympicDestroyer story eventually resulted in the discovery of a new subset of activity related to both Sofacy and BlackEnergy that we call Hades. We will see how these more sophisticated false flags evolve in the future and how they are used to pursue less explicit goals.

On the forgotten ones

Throughout the year we also saw how several old ‘friends’ re-emerged from hibernation with new sets of activity. Here we are talking about several well-known actors that for unknown reasons (a lack of visibility might be one of them) didn’t display much activity in recent times. However, it seems they are back. In some cases they appear in different weaker forms, perhaps with different operators, or just pretending not to be in shape while they run other parallel operations; in others cases they are back with their usual capabilities.

We can summarize all this by dividing it up into the regions that showed most activity during the year. First place went to South East Asia, followed by the Middle East.

For South East Asia we can point to groups such as Kimsuky that developed a brand new toolset at the very beginning of the year, or activity that falls under the always difficult-to-attribute WinNTI ‘umbrella’. However, and most notably, we can highlight groups such as DarkHotel, LuckyMouse, or even APT10.

The OceanSalt campaign was attributed to APT10, though it’s not very clear how strong the connection is. It seems unlikely that this actor, after the public disclosure and so many years of no known activity, would return with anything that might be attributable to them. At the moment, this is difficult to assess.

LuckyMouse, the second Chinese-speaking group from this list, was very active all year. It hacked national data centers to deploy watering-hole attacks against high-profile victims in central Asia, used a driver signed by a Chinese security-related software developer, and is even suspected of being behind attacks against Oman immediately after the signing of a military agreement with India.

Scarcruft used a new backdoor we call PoorWeb, deployed a 0-day in their campaign at the beginning of the year and used Android malware specially designed for Samsung devices. DarkHotel was also back with a 0-day and new activity, targeting their traditional victims. We were able to establish a connection with a medium level of certainty between DarkHotel and the Konni/Nokki set of activity described by other vendors.

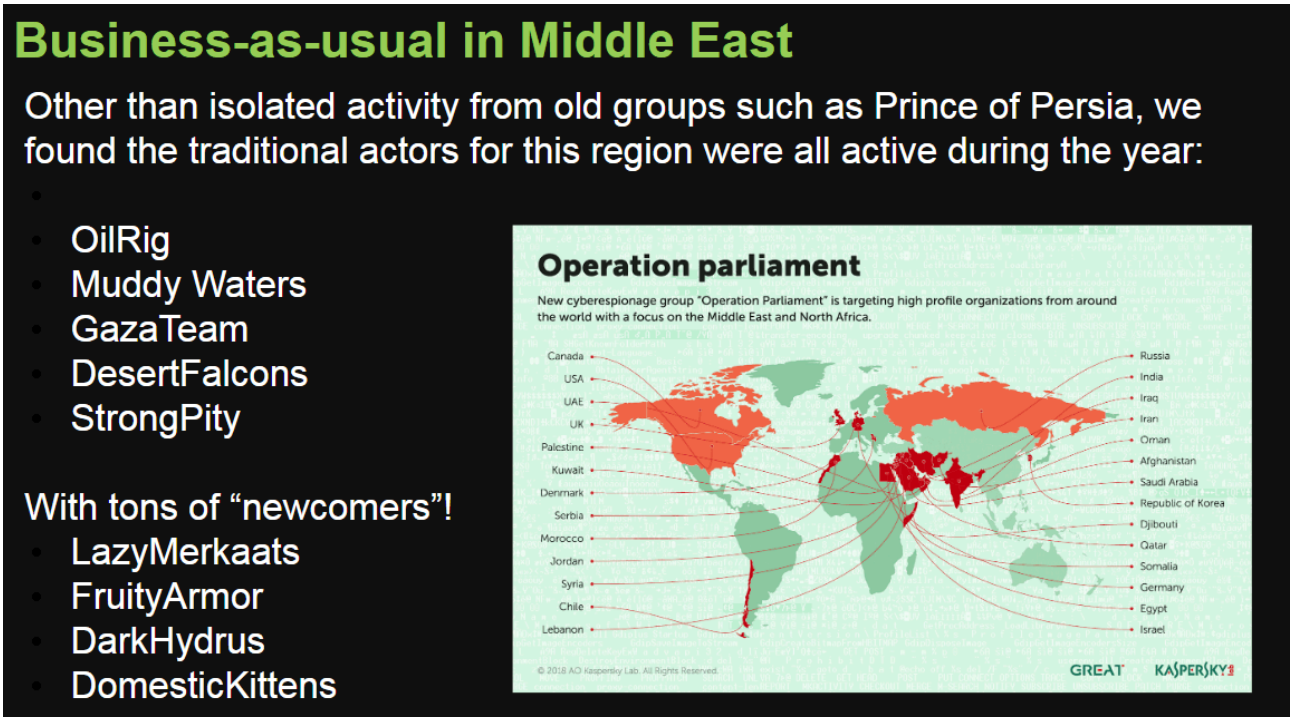
APT10 was especially active against Japanese victims, with new iterations of its malware, as was OceanLotus, which actively deployed watering holes targeting high-profile victims in South Asia with a new custom stager.

In the Middle East we observed groups such as Prince of Persia re-emerge with some activity, along with OilRig. We also detected new MuddyWaters activity, as well as GazaTeam, DesertFalcons and StrongPity among others deploying various campaigns in the region.

On the new kids

At the same time many new sets of activity emerged during the year that were also focused primarily on the Middle East and South East Asia.

This activity was driven by Asian actors such as ShaggyPanther, Sidewinder, CardinalLizard, TropicTrooper, DroppingElephant, Rancor, Tick group, NineBlog, Flyfox and CactusPete – all of them active in the region throughout the year. As a rule, these groups are not that technically advanced, using a variety of approaches to achieve their objectives. They are usually interested in regional targets, with their main objectives being governmental and also military.



In the Middle East we saw activity by LazyMerkaats, FruityArmor, OpParliament, DarkHydrus and DomesticKitten among others. Sets of activity such as that by the Gorgon group are a bit of an exception as they also target victims outside the region.

Finally, we also detected new sets of activity that show an apparent interest in eastern European countries and former Soviet republics. In this group we find DustSquad, ParkingBear and Gallmaker. The latter seems to be interested in overseas embassies as well as military and defense targets in the Middle East.

On the big fishes

Even if some of the activity previously described doesn't seem that technically advanced, it doesn't mean it isn't effective. Looking back we can cite a few public cases where it looks like these attacks are returning to the days when attackers were after major strategic research or blueprints that might be of the interest to state-sponsored groups, and not just some random data.

We have several examples. For instance, APT15 was suspected of targeting a company providing services to military and technology departments of the UK government. Intezer provided extra details about the activity of this group, though it is not clear who the ultimate victim was.

TEMP.Periscope was suspected of hacking maritime organizations related to the South China Sea. It wasn't the only case in which the industry was targeted, as later it was discovered an unknown actor attacked companies related to Italian naval and defense industries.

Groups such as Thrip showed a clear interest in targeting satellite communication companies and defense organizations in the US and South East Asia.

Finally, the US Naval Undersea Warfare Center was attacked, according to the Washington Post, by a group linked to the Chinese Ministry of State Security, resulting in the theft of 614GB of data and blueprints.

The re-emergence of some of these groups and their victims don't seem to be a coincidence. Some observers might even see the return of these big targeted attacks as the end of some sort of tacit agreement.

We also observed several attacks against journalists, activists, political dissidents and NGOs around the world. Many of these attacks involved malware developed by companies that provide surveillance tools to governments.

For instance, NSO and its Pegasus malware was discovered in more than 43 countries according to an external investigation, showing that business in this field is blooming. On a darker note, there were reports on how Saudi dissidents and Amnesty International volunteers were targeted with this malware.

The Tibetan community was also specifically targeted with different malware families, including a Linux backdoor, PowerShell payloads, and fake social media to steal credentials.

Finally, CitizenLab provided details of a campaign where Sandvine and GammaGroup artifacts were used for surveillance through local ISPs in Egypt, Turkey and Syria.

On naming and shaming

This is clearly a new strategy, adopted as a defense mechanism and as a response to the attackers, in some cases being justice able to claim individual working for APT groups. This can later be used in diplomatic offensives and lead to tougher consequences at the state level. It seems that governments are no longer shy of making these

attacks public and providing details of their investigations, while pointing fingers at the suspected attackers. This is an interesting development and we will see how it evolves in the future.

The end of the Obama-era cyber-agreement between the US and China could be the reason for the wave of Chinese-speaking groups making a comeback, as well as the targeting of some of the high-profile 'big fishes' described above. We saw how in this new period of hostility between the two countries, the US obtained the extradition from Belgium of a Chinese intelligence officer charged with conspiring and attempting to commit economic espionage and steal trade secrets from multiple US aviation and aerospace companies.

The US also provided details about a North Korean citizen suspected of being part of the Lazarus group that was behind the Sony Entertainment attack and WannaCry activity, and who is now wanted by the FBI. Maybe in an unrelated note, the US Cert was very active during the year in providing indicators of compromise and detailing Lazarus (HiddenCobra) activity and the tools used by this actor.

After the infamous DNC hack, the US indicted 12 Russian citizens belonging to units 26165 and 74455 of the Russian Main Intelligence Directorate. Seven officers of GRU were also indicted for their alleged role in a campaign to retaliate against the World Anti-Doping Agency that exposed the Russian state-sponsored doping program.

In Europe, UK Officials and the UK National Cyber Security Center attributed the not-Petya attack that took place in June 2017 to Russian military units.

Finally, and in a very interesting initiative, the US Cyber Command launched an 'information warfare' campaign with a message to Russian operatives not to even try influencing the US mid-term election process.

All the above, and several other cases, shows how there seems to be a new doctrine in dealing with such hacking attempts, making them public and providing tools for media campaigns, future negotiations and diplomacy, as well as directly targeting operatives.

On hardware

The closer malware gets to the hardware level, the more difficult it is to detect and delete. This is no easy task for the attackers, as it's usually difficult to find the exploit chain to get that deep in the system, along with the difficulty in developing reliable malware working in such deep levels. That always raises the question of whether this malware already exists, quietly abusing modern CPU architecture characteristics, and we simply don't see it.

Recent discoveries of vulnerabilities in different processors open the door to exploits that might be around for years, because replacing the CPU is not something that can be easily done. It is not clear yet how Meltdown/Specter and AMDFlaws among others might be exploited and abused in the future, but attackers don't really need to rush as these vulnerabilities will probably be around for a long time. Even if we haven't see them being exploited in the wild yet, we believe this is a very valuable piece of knowledge for attackers and maybe also a timely reminder for us all about how important hardware security is.

That leads on to something we actually saw in the VPNFilter attack, in this case targeting networking devices on a massive scale. This campaign, attributed to a Russian-speaking set of activity, allowed attackers to infect hundreds of thousands of devices, providing control of the network traffic as well as allowing MITM attacks. We saw APT actors abusing network devices in the past but never in such an aggressive way.

On other stuff

Triton/Trisis is an industrial-targeting set of activity that gained popularity during the year as it was discovered in some victims, and is suspected of shutting down an oil refinery in an attack where the actor used a 0-day. According to FireEye, this actor might have Russian origins.

In our predictions we already discussed the possibility of destructive attacks becoming normal in situations where tensions exist between two adversaries, using collateral victims to cause harm and send messages in this dangerous grey zone between an open attack and diplomacy.

Financial attackers may not be using very new techniques, but that may be because they don't need to. The Carbanak group was 'beheaded' with the arrest in Spain of one of their leaders; however, that doesn't seem to have had any impact on subsequent Fin7 activity during the year. They deployed their new Griffon JavaScript backdoor targeting restaurant chains. Meanwhile, a suspected subset of this group – the CobaltGoblin group – was also very active targeting banks in a more direct way.
