The Enigmatic Energetic Bear

pylos.co/2020/11/04/the-enigmatic-energetic-bear/

Joe 11/04/2020

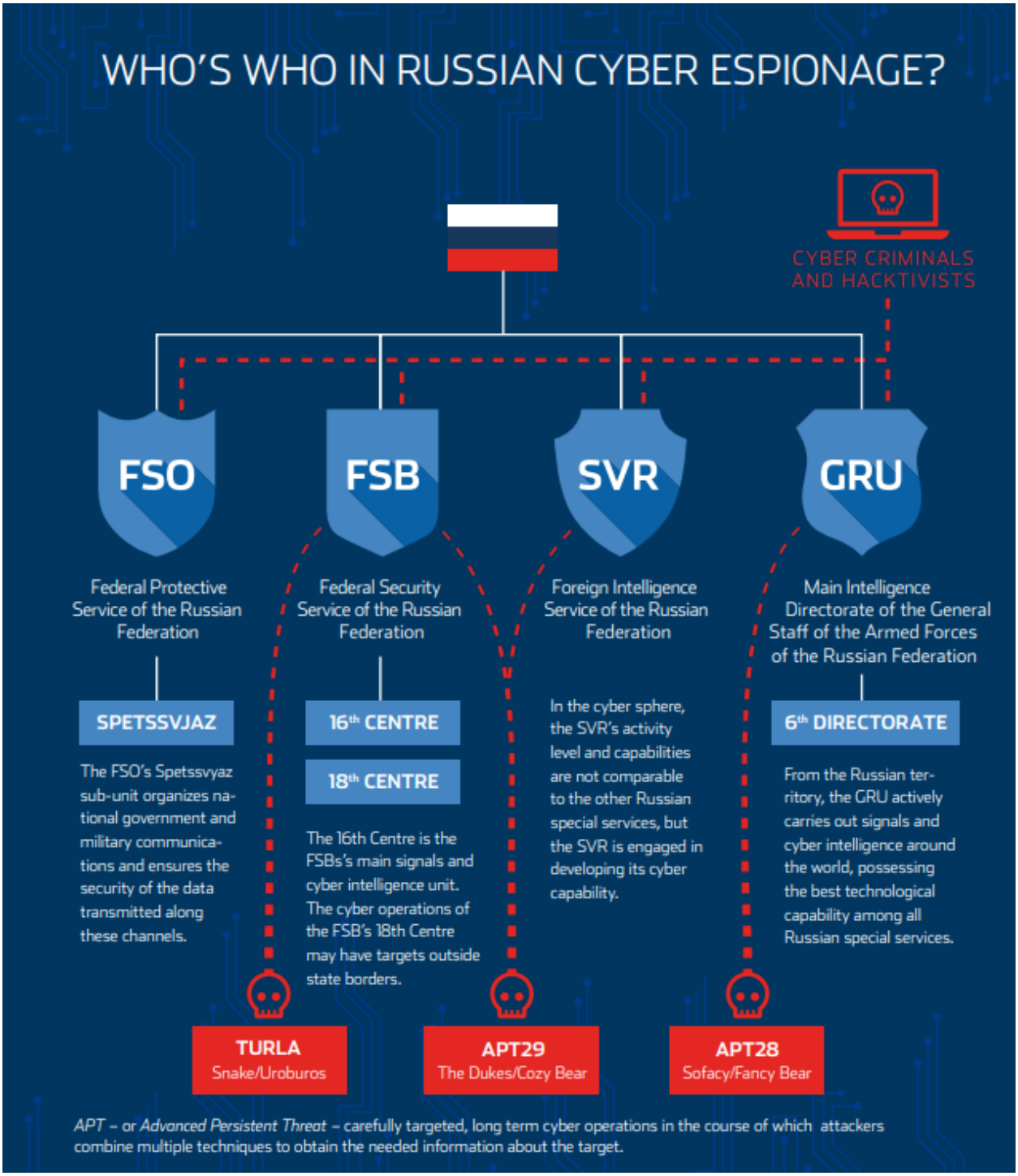
“Energetic Bear” (also known as Dragonfly, Crouching Yeti, etc. etc.) has been in the news lately given a recent series of intrusions targeting local government and critical infrastructure entities in the United States. While the group has gained attention recently, its activities go back at least a decade with the widespread Havex campaign. Despite the group’s longevity and consistent targeting of critical infrastructure, including the electric and oil and gas sectors, the group has not been the focus of much government disclosure. While linked by the US government and other entities to Russian interests, the group has not featured prominently in items such as indictments and sanctions.

For example, Russian military intelligence (GRU) has repeatedly been targeted by the US, UK, and other governments through disclosures and other actions in response to actions associated with the organization. These actions have allowed us to gain incredible insight into GRU operations, including in-depth observations into specific units such as GRU Unit 74455 (“Sandworm”) and Unit 26165 (mostly associated with APT28 or Fancy Bear operations). Other government reporting, such as annual Estonian reporting which has

previously linked specific Russian intelligence agencies with commercially tracked threat actors covers the GRU-linked entities as well as other actors such as APT29/Cozy Bear and Turla, but does not at all address Energetic Bear activity.

One likely reason why Energetic activity has likely not received the same level of interest as GRU-linked entities is the nature and impact (or lack thereof) of operations. Specifically, while GRU operations are linked to multiple disruptive events – the 2015 and 2016 Ukraine power incidents, the 2016 US election interference activities, the 2017 NotPetya incident, among other items – there are no known (deliberate) disruptions or incidents associated with Energetic operations. This is understood and reflected in recent reporting and past

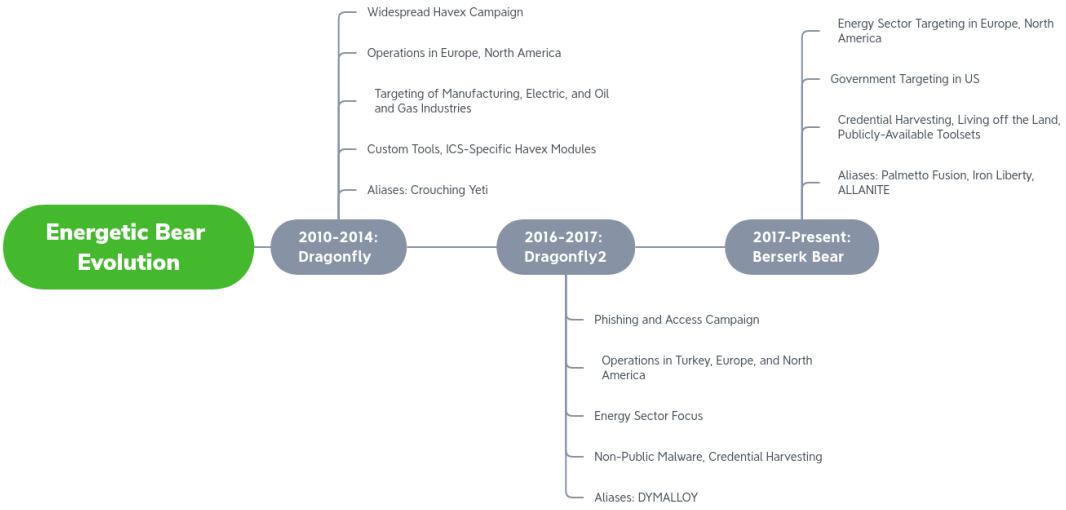
observations on Energetic activity, and likely explains why the group has evaded public sanction by government entities.



Another factor which has likely led to confusion around Energetic is the group's evolution over time and lack of consistent naming. Since emerging around 2010, the group has received multiple names or references: Energetic Bear, Berserk Bear, Crouching Yeti, Iron Liberty, Dragonfly, Dragonfly2, DYMALLOY, ALLANITE, Temp.Isotope, Palmetto Fusion, etc. Additionally, items have either collapsed into each other (e.g., CrowdStrike combining Energetic and Berserk Bear) or separated into distinct (if related) entities (e.g., Dragos

tracking distinct DYMALLOY and ALLANITE entities). Overall this is due to the group's evolution over time, which has manifested in noticeably different behaviors, tools, and at times targets over the past decade.

Yet for all the confusion and lack of observed, intentional impact, Energetic (or whatever you'd like to call them) has attained significant successes within the realm of critical infrastructure intrusions. Among other items, Energetic has:



1. Developed one of only a handful of industrial control system (ICS) specific malware variants through ICS-aware modules for Havex.
2. Successfully breached multiple electric utility environments from 2017 through the present including control system access in isolated instances.
3. Deployed relatively sophisticated intrusion mechanisms, such as network device manipulation for traffic shaping or capture to facilitate campaigns.

Given these observations, we are dealing with an adversary that is clearly among the "top tier" of threat actors, yet one that has hardly become a household name like Sandworm, Turla, or APT29. Potentially driving this discussion is confusion over just "who is Energetic/Dragonfly/ALLANITE/etc.?"

When exploring this topic, looking at primary source publications is most beneficial and least likely to result in error. While some individuals in the private sector can make claims such as "It is the FSB!" while presenting little or no corroborating evidence, a review of publicly available sources can at minimum allow us to glimpse what Energetic is *not*. First and foremost, given the plethora of indictments, disclosures, and named sanctions released by the US, UK, and other governments since 2016, we can clearly say one thing: Energetic is *not* the GRU. Given the catalog of events – including less-than-disruptive items – reviewed by US Department of Justice indictments and UK government and NCSC reporting, we can support the following claims:

1. Energetic is not related to GRU Unit 74455, associated with the vast majority (if not all) Russian-linked critical infrastructure disruptive events.
2. Energetic is *most likely* not related to GRU activity at all, given that the (concerning) actions of this group have never been recorded in other indictments, sanctions, or other items which have mentioned other GRU entities (such as Unit 26165).

That puts us into Russia's non-military intelligence agencies – the FSB and the SVR – as most-likely sponsors of Energetic activity. Here, matters become muddier. As seen in items such as Estonian intelligence reporting (which assesses links to both the FSB and SVR for entities such as APT29), relationships to threats for espionage- or access-focused groups (such as Energetic) becomes much more difficult. While GRU-linked operations in many cases result in noticeable effects (such as the power going off), these operations are designed to not attract attention (at least, not immediately) which makes their disposition somewhat more difficult.

Yet diving into the civilian intelligence angle for Energetic's origins yields some interesting insights. As covered in greater detail elsewhere, Russia's intelligence services are hardly cooperative – yet overlap between the civilian intelligence agencies (FSB and SVR) is more likely than any collaboration or coordination between these entities and military intelligence, the GRU. Furthermore, while GRU-linked entities – from 74455 attacks to 26165 active measures – are linked to operations producing noticeable disruptions, FSB and SVR entities typically focus on "classic" intelligence operations and access development with no intention to produce a discrete incident. This observation holds even for items such as the 2016 US election interference campaign, where GRU-linked entities were indicted given their participation in linked active measures, while FSB/SVR-linked entities (APT29) were largely left out as they did not appear to "use" their access to a disruptive effect.

Based on known Energetic operations to date, which have focused on penetrating environments but no known or intended incidents of disruption, they appear to align with Russia's non-military intelligence agencies (FSB or SVR). While this may seem like so much trivia for defenders, in this case it has significance for those wishing to protect critical infrastructure. Namely, while GRU-linked operations are often linked to direct, near-immediate transition to disruptive operations, FSB/SVR operations are aligned with more classic intelligence operations. This could include developing access and gaining knowledge on environments for later weaponization, but such a shift should only be anticipated in extreme events, such as the march toward more traditional hostilities. As a result, differentiating between these campaigns (and their likely sponsors) is significant in that a GRU-linked intrusion requires immediate remediation given that actor's history and reputation, while an entity aligned with FSB/SVR – although still deeply concerning – can likely be dealt with in a more measured, deliberate manner given the separation between intrusion and future (potential) impacts.

In this case, the ability to perform some degree of threat actor attribution combined with an understanding of likely threat actor intentions (or mission) can be of use to defenders. Looking at Energetic specifically, the actor's campaigns are concerning both for their scope (targeting critical infrastructure in multiple environments for over 10 years) and success (breaching control system environments and similar throughout periods of activity). Yet understanding this actor's likely motivations and mission set – espionage and operational preparation of the environment in the event of possible future hostilities – allows us to properly assess this group's actions and the required immediacy of response. Unlike GRU-linked actions (such as Sandworm events), Energetic operations can likely be monitored and followed over time without the need for immediate remediation in order to gain greater understanding of the adversary, facilitating larger-scale response in the near future. While such a judgment might be perilous for other actors involved in critical infrastructure intrusions, the preponderance of evidence indicates that Energetic activities are *not* operations designed to deploy immediate disruptive effects – thus giving defenders time.

Perhaps it is this observation which makes Energetic less "sexy" than an actor such as Sandworm. Although engaged in penetrations in sensitive areas, Energetic has yet to produce an impact. Conversely, an entity such as Sandworm has caused headline-grabbing incidents that have earned both media and government attention. Yet just because an Energetic intrusion will not result in immediate disruption does not mean we can sleep on this adversary. Rather, such efforts show the methodical, meticulous nature of long-term cyber intrusions into critical infrastructure and related sectors to further national interests. While we may lose sight of such activity amidst the latest ransomware or flashy disruptive incident, campaigns such as those conducted by Energetic are those which will truly matter in the event "cyberwar" ever breaks out, as these intrusions will enable the actions that will cause truly catastrophic impacts.