MediumMediumHomepage

Become a member

Sign inGet started

MediumHomepage

Go to the profile of Scott J Roberts

Scott J Roberts BlockedUnblock FollowFollowing
Network Defender, developer, speaker, writer, author of O’Reilly’s Intelligence Driven Incident Response, & SANS instructor. Bad guy catcher.
Feb 15, 2015

APT is a Who not a What… And Why it doesn’t Matter

A small number of topics get intelligence driven incident responders incredibly frustrated:

- Using intelligence to mean smart (I’ll share more about that later this week)
- Bad attribution based on incomplete information and bad assumptions
- Misuse of the term APT (in most cases by marketing departments)

Advanced Persistent Threat remains the buzzword of choice for vendors, but it's used incorrectly, and lots of people know that and don't say anything. As a result I want to go on the record and correct a couple key misnomers.

APT is a Who

My second job after college was working for Mandiant (Now FireEye Services as a Security Consultant. This was a great job where I learned a ton and that was because I worked with such a skilled team. The team that started Mandiant primarily came from the United States Air Force Office of Special Investigations; a team that handled, among other things, some of the first nation state level computer intrusions of the Internet era such as Solar Sunrise, Moonlight Maze, and Titan Rain.

This was a weird time, because (like today) attacks weren't just aimed at military targets but commercial targets as well. AFOSI, as well as other government intelligence & defense groups, investigated using open source and classified methods. For operational security, this leads to classified intelligence.

This classified intelligence was a problem. While the Defense Industrial Base has people with clearances who can handle classified data, other companies, without cleared people, came under attack as well. These DoD/IC teams wanted to help, but couldn't disclose classified information. They came up with a compromise: **sharing indicators and information without disclosing the actual actor behind it. Instead they just referred to the actor using a pseudonym: The Advanced Persistent Threat.** Specifically APT, supposedly coined by Colonel Greg Rattray, was a couple groups of actors primarily operating out of mainland China and believed to be members of the People's Liberation Army. We now know these groups today as *APT1*, *Anchor Panda*, and *Elderwood*, as well as other private designations.

APT is a term to refer to Chinese espionage without saying Chinese espionage. Full stop.

APT is not a What

Compromised companies often make a statement after their incident that the attacker is an *advanced persistent threat*. This leads to the same tired observations by security pundits:

> *As our research team reveals in our Hacker Intelligence Initiative Report, some APTs are relatively simple to execute. ~ Amichai Shulman*

or…

> *Advanced wasn't right because the initial gambit was almost always a low-tech spear phishing attack. Persistent wasn't really accurate because it wasn't the attackers who made things persistent; it was the inability of organizations to read their own logs for anomalies that allowed the breaches to continue over long timeframes. ~ Robert Richardson*

Robert is correct in this case. APTs aren't advanced or persistent, at least not necessarily. But that's because the term wasn't meant to describe *how* the attacks occurred, but *who* the attacker was. The APT term could have been "Actor Potato" or "Group1" or any other codename imaginable.

APT is not a description of an actor based on the sophistication of their techniques, as people often note there's often little that's advanced. They aren't universally persistent; while some groups will linger for months or years, others use *smash and grab* tactics. **The fact is the same: APT is a codename for a who, that who being Chinese espionage, not a description of an attacker based on methods or techniques.**

So why doesn't it matter?

This rant, and even I can call it a rant, isn't out of nowhere. Today Kaspersky released a report about the *Carbanak APT*: A financially motivated attacker operating all over the world(Report: Carbanak_APT_eng.pdf). I have no doubt that this is a great paper worth reading. I have no doubt the group they describe is using some interesting, even advanced, techniques. Perhaps they even stay in an environment for a long period of time, persisting if you will. But I am 100% certain this is a misuse of the term APT.

APT has moved away from its original definition, from a term of art to a term of marketing. It's not descriptive, except to say that the solution has to include hundreds of thousands of dollars in professional services, endpoint monitoring, intelligence portals, and feeds with millions of indicators. Words change, and there is no doubt at this point that APT *means* what marketing says it does, but I think security practitioners can help.

We need a better and honest taxonomy for referring to these attackers. I'll kick things off with:

- State Sponsored Espionage (What we now call APT)
- Financially Motivated Criminals
- Nationalist Activists
- Criminal Activists (So called Hactivists)

Beyond just having a better taxonomy we need to work alongside marketing departments to use accurate, descriptive terms instead of overloaded buzzwords. It may be an uphill fight, but a worthwhile one. I welcome the chance to collaborate with others who care about this.

-The security community has difficult problems on its hands. Seemingly the harder we work to stop threats the more come up. We're already dramatically understaffed as an industry (Leviathan Security Group: Analysis of Cloud vs. Local Storage: Capabilities, Opportunities, Challenges). The last thing we need, the last thing we can afford, is to make our own lives more difficult by abusing overloaded terms to generate fear, uncertainty, and doubt.

I've been working on tool I think could be useful in situations like this. While it's not ready for prime time yet here is a little preview:

Not Found

The requested URL was not found on this server.

Apache/2.4.29 (Ubuntu) Server at webcitation.org Port 443

Originally published at [sroberts.github.io]() on February 16, 2015.

- [Cybersecurity]()
- [Security]()

Like what you read? Give Scott J Roberts a round of applause.

From a quick cheer to a standing ovation, clap to show how much you enjoyed this story.

✕

1

-

BlockedUnblock FollowFollowing

[Go to the profile of Scott J Roberts]()

Scott J Roberts

Medium member since Jul 2017

Network Defender, developer, speaker, writer, author of O’Reilly’s Intelligence Driven Incident Response, & SANS instructor. Bad guy catcher.

- 👏👏

  ×

1

Go to the profile of Scott J Roberts

Never miss a story from **Scott J Roberts**