Getting Started with ATT&CK: Threat Intelligence

Katie Nickels · Follow
Published in MITRE ATT&CK® · 8 min read · Jun 10, 2019

633 2

Since we started our Medium blog last year, we've shared quite a few posts with you about topics like ATT&CKcon 2018, our plans for 2019, and a cool visualization for our roadmaps — we hope you've found those helpful. As we've talked to you, though, we've realized that it would help for us to take a step back and focus on a question many of you have: how do I get started using ATT&CK?

With that in mind, we're staring a new mini-series of blog posts aimed at answering that question for four key use cases: threat intelligence, detection and analytics, adversary emulation and red teaming, and assessment and engineering. If you haven't seen it, we reorganized our website to share content based on these use cases, and our hope is these blog posts will add to those resources.

ATT&CK can be useful for any organization who wants to move toward a threat-informed defense, so we want to share ideas for how to start regardless of how sophisticated your team is. We'll break each of these posts into different levels:

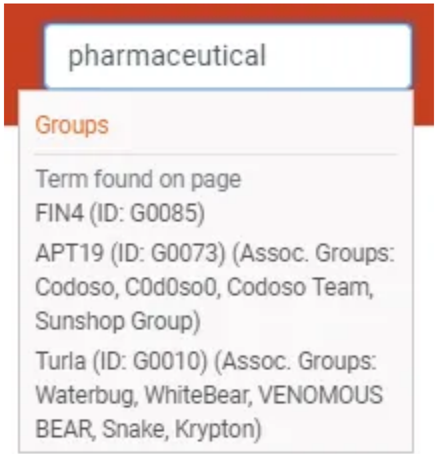
- Level 1 for those just starting out who may not have many resources,
- Level 2 for those who are mid-level teams starting to mature, and
- Level 3 for those with more advanced cybersecurity teams and resources.

Today we're kicking off this series by talking about threat intelligence because it's the best use case (just kidding, rest of my team! 😉). Last summer, I gave a high-level overview of how you can use ATT&CK to advance cyber threat intelligence, and in this post I'll build upon that and share practical advice for getting started.

Level 1

Cyber threat intelligence is all about knowing what your adversaries do and using that information to improve decision-making. For an organization with just a couple analysts who wants to start using ATT&CK for threat intelligence, one way you can start is by taking a single group you care about and looking at their behaviors as structured in ATT&CK. You might choose a group from those we've mapped on our website based on who they've previously targeted. Alternatively, many threat intelligence subscription providers also map to ATT&CK, so you could use their information as a reference.

> ***Example:*** *If you were a pharmaceutical company, you could search in our Search bar or on our Groups page to identify that APT19 is one group that has targeted your sector.*

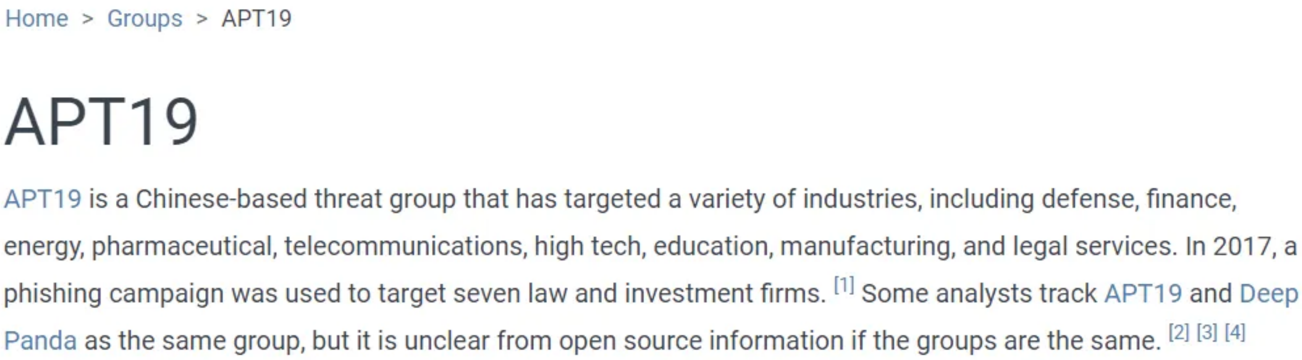


pharmaceutical

Groups

Term found on page
FIN4 (ID: G0085)
APT19 (ID: G0073) (Assoc. Groups: Codoso, C0d0so0, Codoso Team, Sunshop Group)
Turla (ID: G0010) (Assoc. Groups: Waterbug, WhiteBear, VENOMOUS BEAR, Snake, Krypton)

Search for “pharmaceutical”



Home > Groups > APT19

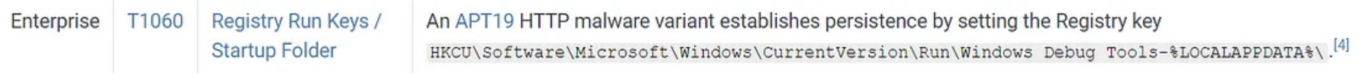
APT19

APT19 is a Chinese-based threat group that has targeted a variety of industries, including defense, finance, energy, pharmaceutical, telecommunications, high tech, education, manufacturing, and legal services. In 2017, a phishing campaign was used to target seven law and investment firms. [1] Some analysts track APT19 and Deep Panda as the same group, but it is unclear from open source information if the groups are the same. [2] [3] [4]

Description of APT19 Group

From there, you can bring up that group’s page to look at the techniques they've used (based solely on open source reporting that we've mapped) so you can learn more about them. If you need more info on the technique because you're not familiar with it, no problem — it's right there on the ATT&CK website. You could repeat this for each of the Software samples that we've mapped the group using, which we track separately on the ATT&CK website.

> ***Example:*** *One technique used by APT19 is Registry Run Keys/Startup Folder.*

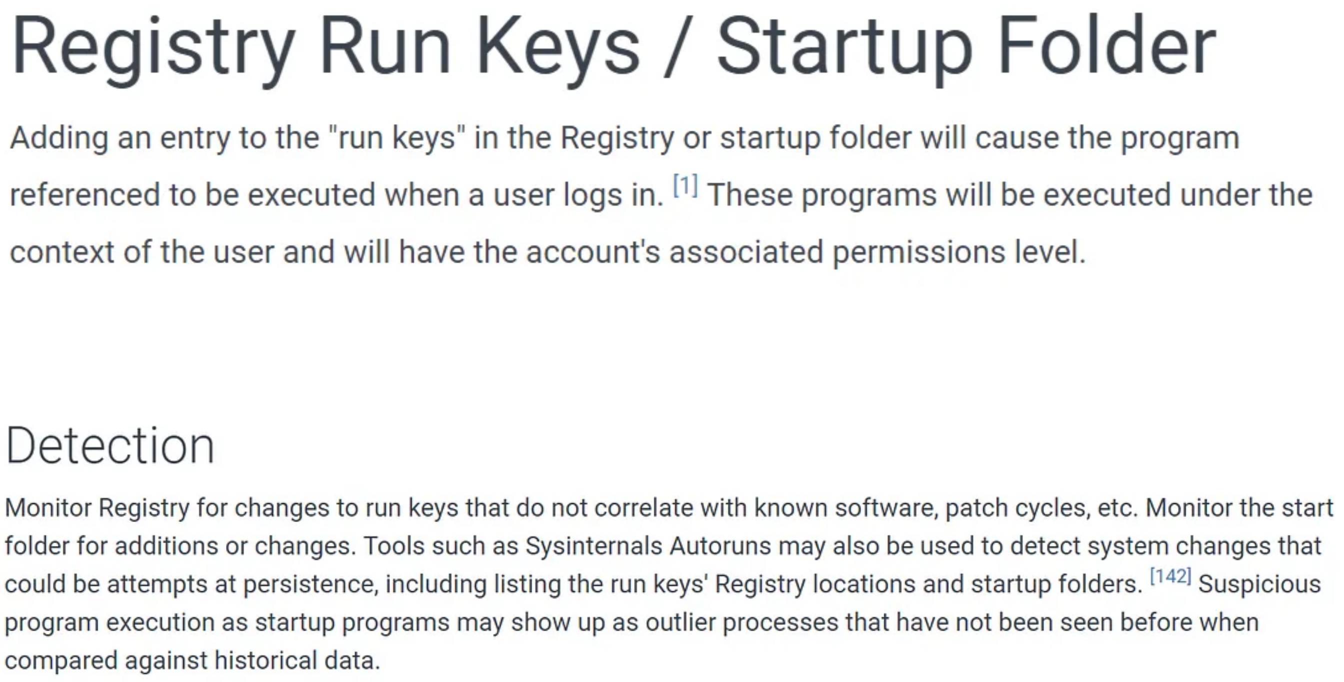


Enterprise	T1060	Registry Run Keys / Startup Folder	An APT19 HTTP malware variant establishes persistence by setting the Registry key `HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Windows Debug Tools-%LOCALAPPDATA%\`.[4]

So how do we make this information actionable, which is the whole point of threat intelligence? Let's share it with our defenders since this is a group who has targeted our sector and we want to defend against them. As you do this, you can check out the ATT&CK website for some ideas to get you started with Detection and Mitigation of techniques.

> ***Example:*** *Let your defenders know about the specific Registry run key APT19 has used. However, they might change that and use a different run key. If you look at the Detection advice for the technique, you see a recommendation is to monitor the Registry for new run keys that you don't expect to see in your environment. This*

> *would be a great conversation to have with your defenders.*



Registry Run Keys / Startup Folder

Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in. [1] These programs will be executed under the context of the user and will have the account's associated permissions level.

Detection

Monitor Registry for changes to run keys that do not correlate with known software, patch cycles, etc. Monitor the start folder for additions or changes. Tools such as Sysinternals Autoruns may also be used to detect system changes that could be attempts at persistence, including listing the run keys' Registry locations and startup folders. [142] Suspicious program execution as startup programs may show up as outlier processes that have not been seen before when compared against historical data.

Detection ideas for the Registry Run Keys / Startup Folder technique

In summary, an easy way to start using ATT&CK for threat intelligence is to look at a single adversary group you care about. Identifying some behaviors they’ve used helps you inform your defenders about how they can try to detect that group.

Level 2