Advanced Persistent Threat: What is the Danger, and How Should I Prepare?

Advanced Persistent Threat, or APT, is one of the most insidious cyber threats in technology today: Once intruders get into a system, they may linger for months or even years before they strike. The results can have devastating consequences, including large-scale theft of intellectual property (IP), personally identifiable information (PII), or other sensitive data.

APT poses serious risks for any IT system, whether at a large enterprise or a small government agency. With more sensitive information online and in the cloud every day—think military systems designs or other classified government information—the stakes only become higher. Here's what you should know about APT—and what you should do to prepare for and, if necessary, to respond to an APT intrusion.

Advanced Persistent Threat: Know Your Foe and What's at Stake

1. Given that today's personal devices—your iPhone, your tablet, maybe even your smart watch—have as much computing power as your laptop, their widespread use (including the apps used on them) expands the attack surface well beyond that of even just a few years ago. Even with an agency-wide mobile-device management solution in place, end-point devices still present network security liabilities that could provide a one-way ticket in for APT.

2. Once in the network, APT quietly and randomly probes for vulnerabilities, planting seeds along the way as bad actors assess the environment, build a plan, and eventually execute. After an indefinite amount of time, actors strike fast and strategically, pulling everything they want—whether it's millions of federal employee records or highly sensitive IP—before network operators realize what's happened.

3. APT is dangerous because it is so difficult to detect, and it's complicated to track because bad actors work so subtly over long periods of time. The vast majority of departments don't have the processing power or memory to maintain long-term network activities logs, so it's nearly impossible to uncover anomalous network patterns or behavior spread over time. Think of everyone you don't necessarily know that rang your doorbell over the past year: handymen, salespeople, political canvassers, people with the wrong address. Unless you've logged every single individual's name, face and fingerprints, you'll never track down which one broke in while you were on vacation.

Cloudera, Inc. 395 Page Mill Road Palo Alto, CA 94306

Taking on APT: Know Your Network and Partner Up

1. By the time a breach has occurred, it's too late—all decision-makers can do is determine how the APT gained access and patch accordingly. But with the right tools and experts, IT security teams can also identify potential risks and shore up systems before an APT intrusion happens. This requires a proactive approach with a comprehensive assessment: Where are the gaps? Who is probing the network, and when, where and how? Preemptively addressing potential threats and latent vulnerabilities can help steel defenses, including the ones already in place.

2. The most effective security partners can institute adaptable architectures that establish not only a more comprehensive, real-time view of the threat surface, but also the capacity to collect, store, and translate vast volumes and varieties of data, such as network activity and machine logs, at high velocity. These tools can then be used to conduct extensive analyses using real-time threat intelligence streams and deep machine learning. Capabilities like Cloudera's open source-driven platforms do this by capitalizing on the data-science knowledge, expertise, applications, and open-source projects distinct to its cyber community—and common structures can be set up within months, if not weeks.

3. Today most agencies can only track in near-real time, and they can only store and evaluate a few months' worth of network data. But as threat actors become more sophisticated and critical data becomes more digitized, departments need a flexible, adaptive architecture that empowers more agile, progressive decision-making. Open source capabilities can help the public sector modernize affordably by implementing co-located, coexisting technologies that strengthen current systems and advance defenses against APT.

The Bottom Line is that most agencies seek but struggle to implement rapidly evolving best practices that hinge on proactive engagement, detection, and mitigation. It's a common and consistent challenge to be agile and adaptable—and to protect and defend at scale—with limited, heavily regulated resources. But with the right partners, the public sector can capitalize on open source capabilities—maximizing legacy systems and resources and leaning in more effectively with what they have.

CLOUDERA

Cloudera, Inc. 395 Page Mill Road Palo Alto, CA 94306