MITRE research opens window into cyber attacker behavior

McLean, Va., June 16, 2015—The MITRE Corporation has released ATT&CK™—Adversarial Tactics, Techniques & Common Knowledge—a framework that for the first time consolidates and provides concise, more complete descriptions of what cyber attackers do once inside and embedded in a computer network.

ATT&CK can help organizations quickly detect cyber threats and identify and categorize cyber adversary behaviors. This insight allows a tailored response to a cyber breach and a recovery plan specific to the breach—saving valuable time and resources. The ATT&CK license is available for free.

"Practitioners know there is a lot of guidance available about the pre-exploit phase to prevent an attack, but there's very little information about how to detect an adversary after they infiltrate the network," said Blake Strom, MITRE cybersecurity researcher, who led the work. "ATT&CK is the first step in filling this gap. Our ultimate goal is to create a community to raise awareness about what actions might be seen during an intrusion."

Based on MITRE research about cyber adversary behavior, as well as penetration testing and red teaming, ATT&CK provides a body of knowledge characterizing the post-access activities and techniques of adversaries. The work was funded in part through MITRE's independent research program, which focuses on using advanced and emerging technologies, or creatively using current technology, to explore solutions to national challenges.

Developers of defensive tools and policies can identify where their value and strengths are in relation to the ATT&CK framework. And the cyber security research community can use ATT&CK as a reference point to drive future investigation.

Gary Gagnon, MITRE senior vice president and chief security officer, said, "ATT&CK widens the lens on the cyber attack life cycle. Now we have a better understanding of the moves of an adversary inside a network. This level of detail makes a quick, accurate and proportionate response possible. Blake's work has added a key tool to the cybersecurity arsenal—and more importantly started a dialogue that I hope many will take part in."

Strom encourages the community to help further develop the ATT&CK framework. Contributions will help focus community efforts on areas not covered by current defensive technologies and best practices.

Related Resources
ATT&CK https://attack.mitre.org

MITRE

Media Resources: mitre.org/news/media-resources

Social Media
Retweet:
Share on Facebook:
Share on Google+:

About The MITRE Corporation
The MITRE Corporation is a not-for-profit organization that operates research and development centers sponsored by the federal government. Learn more about MITRE.

The MITRE Corporation, mitre.org
Follow us: twitter.com/mitrecorp; facebook.com/MITREcorp
@MITREattack: https://twitter.com/MITREattack

Karina Wright
Media & Community Relations Lead
khw@mitre.org (703) 983-6125

MITRE