Australian Government
Australian Signals Directorate

ACSC
Australian Cyber Security Centre

Implement the Prime Minister's Cyber Security Guidance with MITRE ATT&CK and AttackIQ

Australian Cyber Security Center Advisory 2020-008: TTPs

On 19 June 2020, Prime Minister Scott Morrison addressed the nation about malicious cyber activity against Australian networks. "We know it is a sophisticated state-based cyber actor because of the scale and nature of the targeting and the tradecraft used," he said, "Our Government's expert agency on Cybersecurity is the Australian Cyber Security Center and it's already published a range of technical advisories."

Specifically, in its Advisory 2020-008 the Australian Cyber Security Center published tactics, techniques and procedures (TTPs) used to target multiple Australian networks, focusing on the MITRE ATT&CK framework of known adversary TTPs. For years the Australian Cyber Security Center (ACSC) has used the MITRE Common Vulnerabilities Exposure (CVE) framework to mitigate risk in operating systems.

"The MITRE ATT&CK Framework Provides the foundation for the industry to speak the same language as it pertains to threats we face and our mitigating controls. This Framework provides a welcome opportunity to simplify things and be consistent."

- **Shaun Vlassis**
Executive Director Cyber Defense & Fraud Engineering

What is MITRE ATT&CK?

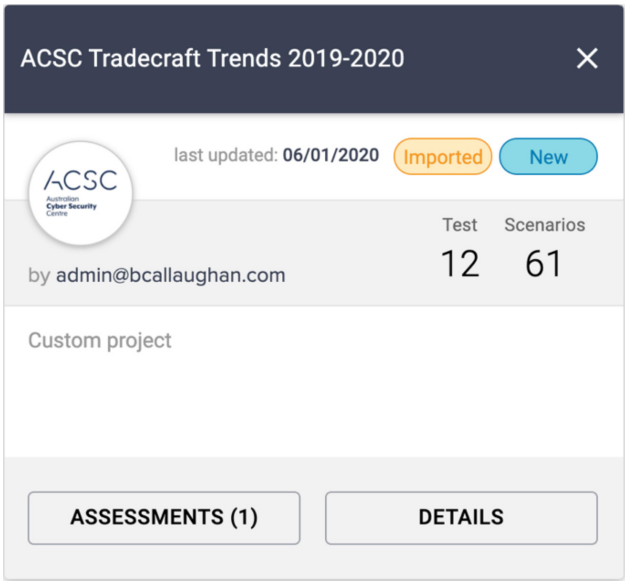
MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

ATT&CK®

AttackIQ Operationalizes MITRE ATT&CK

AttackIQ enables security organizations for the first time to test the effectiveness of their security controls safely and continuously, at scale, in production, and with threat coverage across the MITRE ATT&CK kill chain. AttackIQ grounds organizations in a shared understanding of threats and threat behaviors using the MITRE ATT&CK framework. Through continuous testing by real-world adversary emulations, AttackIQ provides enterprises increased visibility across the organization, increasing defenders' insights and improving total cybersecurity effectiveness. Armed with better insights, security leaders can make better informed decisions about people, products, and processes -- and drive an overall improvement in security. The net result: The Chief Information Security Officer and the security team optimize their resources and achieve better business outcomes.

On 20 May, 2020 the ACSC released a Summary Tradecraft Trend Report detailing 61 TTPs exploited by Advanced Persistent Threats (APT's), then codified those TTPs into a click-button assessment which will produce a report to let you know how protected your enterprise is against those TTPs.



HOW TO PUT IT TO USE

_INITIAL ACCESS
_EXECUTION
_PERSISTENCE
_PRIVILEGE ESCALATION
_DEFENSE EVASION
_CREDENTIAL ACCESS
_DISCOVERY
_LATERAL MOVEMENT
_COLLECTION
_EXFILTRATION
_C&C

Regardless of the maturity of your security program, one principle still holds true: keep it simple. When applying the vast knowledge base of MITRE ATT&CK, start with the most critical areas of concern to you -- go deep, not wide. Test your detection, prevention, and response capabilities end-to-end, and then determine the next tactics of the framework to focus your efforts.

Levels 20 & 21, Tower 2 Darling Park
201 Sussex Street
Sydney, NSW, 2000
Australia
+61 455 055 280

AttackIQ, a leader in the emerging market of breach and attack simulation, built the industry's first platform that enables red and blue teams to test and measure the effectiveness of their security controls and staff. With an open platform, AttackIQ supports the MITRE ATT&CK framework, a curated knowledge base and model for cyber adversary behavior used for planning security improvements and verifying defenses work as expected. AttackIQ's platform is trusted by leading companies around the world.

For more information visit: www.attackiq.com. Or follow AttackIQ on Twitter, Facebook, LinkedIn, Vimeo, and YouTube.