DIGITAL DEFENCE

Advanced Persistent Threat (APT) Simulation

Protect
Service

OVERVIEW

The nature of the threat against networks has changed; attackers are now employing Advanced Persistent Threats, APTs – malicious software designed to use effective automated attacks to enter and move through a network, communicating only when necessary and using encrypted and difficult to detect communications channels. APTs attacks are specifically designed to access financial resources or confidential information during a long-term compromise that can last months, or even years.

DigitalDefence's APT Testing service allows you to simulate a customized attack that is designed to by-pass traditional network controls. The test APT is benign in its actions and it does not employ any destruction actions against your production network; however, because it is based on a real threat, it acts like an APT in every other way. It attempts to compromise the network, and move from system to system. It will communicate with an external command and control server using overt communications. Finally, the test APT will attempt to exfiltrate large amounts of dummy data via the communications channel. This will allow the organization's network perimeter defenses, intrusion detection and prevention systems, data leak prevention mechanisms and endpoint security to be tested.

BENEFITS

- Take penetration testing activities to the next level; validate your network security using the most realistic real-world risks
- Consolidate your network controls to detect an advanced attack, identify weaknesses that traditional methodologies missed, and prioritize the defensive steps required to protect your organization in a cost-effective manner
- Validate your incident response plan

Improve corporate risk reduction with strategic security and privacy services.

Is the Advanced Persistent Threat (APT) Simulation Service right for your company?

- The dominant malware threat is described as "advanced" and "persistent" - do you have the ability to find and remove an APT from your network?
- Do you wish to extend your security testing regime beyond "classical" penetration testing?
- Do you need to raise staff awareness on the impact of malicious software on the network?

Protect
Service

- Ensure compliance by demonstrating your commitment to protecting your employees and business against APTs; supports staff education, awareness and training programs

SERVICE DESCRIPTION

A simplified example of an APT simulation would include:

- DigitalDefence testers will research public sources and directly probe the client's network to map the potential attack surfaces and target points
- Testers will create proposed attack maps to compromise the network
- One or more APTs will be customized to attack the client network; several entry vectors (e.g. social engineering, attack through social media, zero day exploits, known exploits, compromise of misconfigurations identified during the reconnaissance) and payloads will be selected
- The attack against the network is launched
- Once a successful exploit has been achieved, the tester will secure access by establishing multiple connections that support remote access to the APT
- DigitalDefence APTs will simulate typical activities of wild-type APTs (looking for proprietary material, encrypting data, covering tracks, etc)
- Testers will use the initial compromise points to pivot through the network
- Sample data will be exfiltrated through the network back to a secure site using overt and covert means

At all times, DigitalDefence testers will work the in-house technical staff to validate the impact of the APT on the internal network, and determine if existing controls can identify and respond to the simulated APT attack.

What Makes an APT Such a Deadly Threat?

- They use advanced techniques to by-pass traditional network controls — targeted social engineering campaigns, 0-day exploits, and customized attacks
- Designed to be persistent—the APT is continuously monitored and controlled using a "low and slow" approach; covert communications allow the APT to remain undetected for months to years
- APTs are a threat because they not only have the ability to enter and remain on a network undetected, but because it is intended that they achieve a specific goal. They are not automated code; their actions are coordinated by human attackers with a specific purpose

About DigitalDefence

DigitalDefence provides complete protection against data security breaches. We provide the advisory services that align security with your business strategy and practices. Our protection services secure your data by assessing vulnerabilities and validating security controls using audits and penetration testing, or "ethical hacking". And should you suffer a security or privacy breach, we provide the 24x7 response services and expertise to minimize financial and reputational loss.

DigitalDefence Inc.
Toll-Free 800-385-1632 | Tel 519-771-8808
info@digitaldefence.ca | www.digitaldefence.ca

Disclaimer

This document is for informational purposes only. DigitalDefence makes no warranties, express or implied, in this document.