OVERVIEW

Mandiant's Threat Assessment is a unique service that allows organizations to evaluate their networks for the presence of advanced attack group activity. Threat Assessments have helped organizations identify and address issues that, in some cases, had existed for years and resulted in the theft of valuable intellectual property.

DESIGNED TO IDENTIFY TARGETED ATTACKS

Over the past several years, advanced attack groups – often backed by organized crime syndicates and nation states – have targeted government and private sector organizations. These advanced attackers seek to remain undetected so that they can steal data over an extended period of time. They develop custom malware and use tactics that can often be difficult to detect using conventional approaches.

Example: Lifecycle of a Targeted Attack

EVIDENCE OF ATTACK GROUPS

Mandiant uses experience gained over hundreds of investigations when assessing networks for the presence of various indicators of compromise including:

Re-Used Custom Malware: Custom malware is often developed at great expense to the attack group. Consequently, they prefer to reuse it – or variants that have similar characteristics. Attack groups can oftentimes be discovered by identifying malware analyzed during prior investigations.

Persistence Mechanisms: A number of techniques can be used to establish persistence in a system. Windows registry entries can store malware execution parameters, malware can be placed in the Start Up folder and legitimate system binaries can be trojanized. Knowing what attack groups commonly do allows Mandiant to look for instances of those persistence mechanisms.

Lateral Movement Techniques: Most advanced attack groups obtain valid privileged credentials and use them to assess the environment. Knowing how they obtain those credentials and what tools they use to access other systems enables Mandiant to search for log and forensic evidence that is indicative of that attacker activity.
Mandiant's threat assessment service helps organizations evaluate if they have been compromised by advanced attack groups and if attackers are currently active in their environment.

Mandiant’s threat assessment service helps organizations evaluate if they have been compromised by advanced attack groups and if attackers are currently active in their environment.

MANDIANT’S APPROACH

The Threat Assessment couples Mandiant's specialized knowledge of advanced attackers' tools, techniques and practices with Mandiant's proprietary technology to determine if attackers are currently in the environment or have been active in the past. The major activities Mandiant performs during a Threat Assessment are:

- **Deploying Network- & Host-Based Inspection Technology**
  Proprietary technology is deployed at Internet egress points and on host systems such as servers, workstations and laptops.

- **Assessing Environment Using Intelligence from Prior Investigations**
  Mandiant has developed a detailed library of Indicators of Compromise (IOCs) that utilize host-based artifacts and network traffic signatures to identify the presence of attackers. Mandiant consultants apply these IOCs to evaluate network traffic, servers, workstations and laptops within the network for evidence of current and past attacker activity.

- **Assessing the Environment for Anomalies**
  Mandiant uses its knowledge of attack groups and their tendencies to assess hosts and network traffic for evidence of attacker activity. In this phase the focus is on “edge analysis” – systems or traffic that have different attributes than are typically seen in the environment.

- **Analyzing Evidence**
  When Mandiant identifies Indicators of Compromise or anomalies, consultants draw on skills that range from forensic imaging to malware and log analysis. Mandiant performs these activities to confirm the finding reflects malicious activity or to determine the finding is a false positive.

- **Summarizing Findings**
  At the conclusion of the Threat Assessment, Mandiant provides a detailed report that summarizes the steps taken during the assessment, the major findings and recommendations for next steps – if appropriate.

UNIQUE EXPERIENCE

Mandiant’s Threat Assessments have identified targeted intrusions within highly challenging environments and in situations where attackers had gone undetected for months.

Case Study

- Law enforcement informed a law firm that they were the target of an advanced attack group. Because this information was obtained during a classified investigation no information could be shared with the law firm.

- Mandiant used its proprietary technology to evaluate all Windows systems in the environment. It found one system contained malware developed by an advanced attack group that Mandiant had seen in a prior investigation.

- Malware analysis led to the identification of IP addresses being used by the malware. Subsequent firewall log analysis led to the identification of a dozen systems communicating with those IP addresses.

- The Threat Assessment became an incident response investigation. By the end of the investigation it was determined that the attacker had been in the environment for at least two years, had compromised more than thirty systems and had been stealing all email from several senior partners throughout the entire time period.