cybereason

Advanced Detection

The Cybereason platform collects and analyzes millions of pieces of data every second and builds an ever-evolving picture of your environment. This document explores how Cybereason addresses specific attacker tactics and techniques.

The platform incorporates the Cybereason Hunting Engine, and uses advanced statistical analysis and behavioral analysis to detect the widest range of attacks of any technology in the market today. Cybereason can automatically identify (in real time) and pull together all the elements of an attack, including techniques like fileless malware, lateral movement, command and control, and unknown malware. Cybereason achieves this through a set of preconfigured, constantly behavior models to spot these threats.

Fileless Malware

Today, a significant proportion of attacks use “fileless” malware - where the malware is not part of a binary executable, but instead gets loaded by another tool like PowerShell. These attacks are undetectable by antivirus solutions, and many can easily avoid “next gen AV” tools. Fileless malware exploits vulnerable applications or uses legitimate administrative tools to propagate. Detecting fileless malware requires deep visibility and complex analytics. Some examples of Cybereason achieves this are:

- **Analyzing memory footprint.** Cybereason gathers information about the memory footprint of all processes and modules. One method the Cybereason Hunting Engine uses is to centrally analyze all code injections to determine whether they are indicative of malware. Legitimate code injections are surprisingly common, so Cybereason also examines all injections and identifies those that do not commonly occur across your organization.
- **Deep parsing of PowerShell commands.** PowerShell is a powerful tool that can invoke encoded binary code in the command line. Cybereason analyzes every PowerShell command, looking for the command line characteristics that imply fileless malware is being loaded. Cybereason also looks for techniques that obfuscate the PowerShell command line using registry keys, environment variables or automation DLLs. Cybereason correlates multiple characteristics to distinguish malware from legitimate but unusual PowerShell usage.

Lateral Movement

Once attackers are inside an organization, they will look to expand their footprint to get access to more critical assets and infrastructure. Detecting lateral movement activity means understanding user activity, process activity and network connections, and distinguishing this from legitimate or administrative activity. Some examples of the types of lateral movement techniques Cybereason can detect include:

- **Pass the hash attacks.** In pass the hash attacks, adversaries steal admin credentials from memory and replay them to gain higher levels of access. This enables them to perform malicious activities but make them appear legitimate. Pass the hash attacks are notoriously difficult to detect, and Cybereason is the only endpoint detection and response platform able to do so. Cybereason correlates and analyzes multiple aspects of user context, process and connection activity behavior to detect these attacks.
- **Malicious use of legitimate tools.** Cybereason analyzes use of remote administrative tools like Windows Management Interface, PsExec and PowerShell to identify patterns of misuse while minimizing false positives. Cybereason also links together the chain of execution across multiple machines using WMI, and looks for remotely executing PsExec to spawn unusual or unknown processes.

Command and Control traffic

One of the first things an attacker will do is establish communication channels with a Command and Control (C2) Infrastructure. This allows the attacker to remotely execute additional commands and exfiltrate data. Cybereason detects outbound connections to command and control infrastructure in several ways, including:

- **Known bad IP addresses from threat feeds.** Cybereason consumes and curates lists of blacklisted IP addresses and domains from commercial and open sources. Cybereason also incorporates custom threat feeds that have been defined and managed by their own threat intelligence team or partners.
- **Incrimination by association.** The Cybereason Hunting Engine maintains a constantly evolving map of all processes, endpoints, users, network connections, files and the relationships between them. If a malicious processes makes an external network connection, then Cybereason marks any other processes making a network connection to the same IP addresses as suspicious.
- **Domain Generation Algorithm.** To maximize persistence and avoid blacklisting, malware and malware operators will frequently change the Command and Control servers they use. Also, to avoid reverse engineering by threat researchers, malware and operators will use cryptographically generated domain names for their command and control infrastructure. Cybereason detects this unusual DNS behavior as an indication of unknown malware.

Unknown Malware

Much of the malware used by more advanced attackers have characteristics never seen before in previous malware. Cybereason might identify processes associated with any of the behaviors outlined in previous sections as unknown malware, especially if they also exhibit other behaviors, like:

- **Anomalous file and process characteristics.** Cybereason examines the properties of running processes and files to identify characteristics of unknown malware. For example if there are irregularities with the file's digital signature or the location in which the file resides, then Cybereason will flag these as suspicious. Cybereason also compares processes and files across your entire endpoint population to identify rare processes. Cybereason also looks for processes that have similar names to others in the environment but have a different process hierarchy or other characteristics.
- **Unknown Ransomware.** Cybereason also examines file and network activity to watch for the unmistakeable signs of ransomware performing mass encryption of users' files. Cybereason uses deception techniques to bait ransomware into attempting to damage worthless files, allowing detection and prevention prior to the ransomware being able to impact the user.