cybereason

5 Emerging Threats Enterprise Security Must Not Ignore

The Cybereason endpoint detection and response platform uses behavioral analysis and machine learning to help companies determine if they are under attack. The company's customers include financial services firms, food and beverage manufacturers, drug makers, technology companies, health-care providers and aerospace contractors around the world.

Over the past six months, Cybereason has spotted and helped companies shut down major threats. After analyzing data from more than 1 million endpoints, our researchers identified these five emerging threats:

1. **Advanced Persistent Threats Target Everyone**

   Once used predominantly by nation-state attackers, APT techniques are now being used by mainstream hackers to breach enterprises to carry out espionage, IP theft and other cybercrimes. Our data clearly shows the increasing prevalence of these complex attacks, especially against mid-sized businesses and large corporations. These attacks evade detection by traditional tools, and maintain stealthy persistence in an organization's network.

2. **Low-Level Threats Evolve Into Complex Hacking Tools**

   Hackers have been spotted upgrading commodity threats like adware and click-fraud malware when installed on endpoints in corporate environments. While those tools are believed to be annoying but harmless, we find that when installed in corporate environments, they are being transformed into complex hacking tools. Hackers are adding components like domain generation algorithms modules and persistence mechanisms. This transformation provides hackers with access to high-value corporate assets, which they can later sell on the dark Web.

3. **Mutating Ransomware**

   Cybereason discovered a massive ransomware operation in which the ransomware tools incorporated random variables to help the attack avoid detection by most antivirus programs. These advanced tools increasingly threaten organizations.

4. Attackers Turn Their Attention to Mac OS X

There's a perception that Mac OS X is impenetrable, especially when compared to Windows. This assumption, however, is wrong. Fewer threats may target OS X but this doesn't mean Macs are immune to attacks. Our research shows that attackers are directing more of their efforts at compromising OS X as the platform's market share increases.

5. The Rise of Fileless Malware and Malware-Free Attacks

Attackers no longer need malware to carry out attacks. Instead, adversaries are using PowerShell, Windows Management Instrumentation and other tools built-in to an operating system for malicious purposes. Called fileless malware attacks, traditional antivirus software programs will not detect these threats since legitimate tools are used by attackers to turn the OS against itself. We have seen growing evidence of hackers adopting malware-free attack methodologies and relying less on malware to carry out attacks.

About Cybereason

Founded by members of the Israeli military's elite cyber-security corps, Unit 8200, Cybereason's technology is based on their deep understanding of complex hacking operations. The Cybereason Endpoint Detection and Response Platform leverages big data, behavioral analytics and machine learning to uncover, in real time, complex cyber attacks designed to evade traditional defenses. It automates the forensic investigation process, connects isolated malicious events and visually presents the full malicious operation. The platform is available as either an on-premise solution or a cloud-based service. Cybereason is privately held and headquartered in Boston with offices in Tel Aviv, Israel and Tokyo, Japan.