Using Splunk UBA to Detect Cyberattacks

Highlights

- **Detection of malware, advanced persistent threat and hidden attacks**
- **Numerous anomaly and threat models focused towards external threat detection**
- **Fully automated and continuous threat monitoring—no rules, no signatures, no human analysis**

Enterprises are constantly under attack from external perpetrators such as hacktivists, cyber-criminals, and nation states. These attacks often come in the form of malware, APTs or zero-day attacks delivered through web content, phishing campaigns or removable media.

The Challenge

The reason external attacks are successful is because attackers have become sophisticated; malware is polymorphic and programmed to evade common signatures, rules and perimeter-based defense mechanisms. Further, once within the network, attackers are able to stealthily navigate the network, compromise accounts, find valuable assets, and gradually exfiltrate data. In spite of innovations like next-generation anti-malware solutions, threat intelligence feeds, and collaboration initiatives like FS-ISAC, these "below-the-radar" attack techniques manage to evade even the smartest security tools today.

The Solution

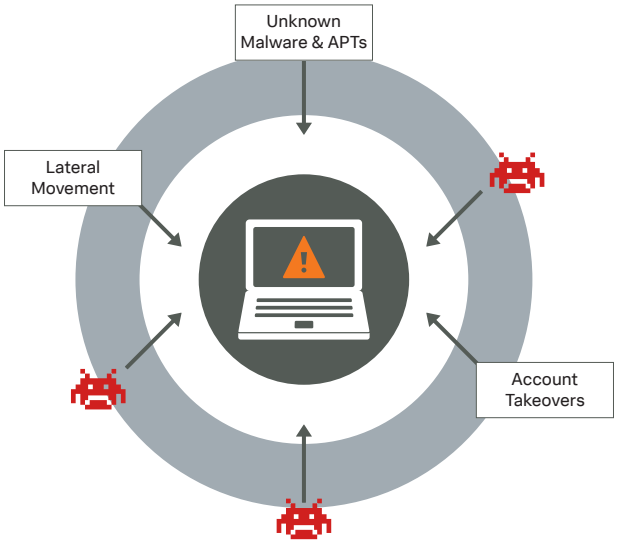
The common thread across various forms of cyberattacks is the deviation of a compromised user's or asset's behavior from its past or its peer groups. This changing behavior of entities provides indicators of compromise (IoC) which can be woven together to distinguish a threat.

Behavior of entities, especially users, devices, system accounts, and privileged accounts, can be mined to reveal anomalies, even when they occur in low frequency and over extended periods of time.

Splunk User Behavior Analytics (Splunk UBA) not only captures the footprint of these threat actors as they traverse enterprise, cloud and mobile environments, but also runs them through its advanced machine learning algorithms to baseline, detect deviations and find anomalies continuously.

These aberrations are then stitched into meaningful sequences over time using pattern detection and advanced correlation to reveal the actual kill chains, which are not only comprehensible but also immediately actionable.

A kill chain is a sequence of malicious activities resulting in a breach. Frequently, there are several events in each stage of the sequence that reveal the path and behavior of an attacker. In contrast to alerts corresponding to violations of known thresholds, a behavior-based threat detection approach uses machine learning with extreme context awareness, thereby maximizing the probability of finding true, hidden threats while greatly minimizing the rate of false positives. In short, a kill chain is the true picture of an attack.



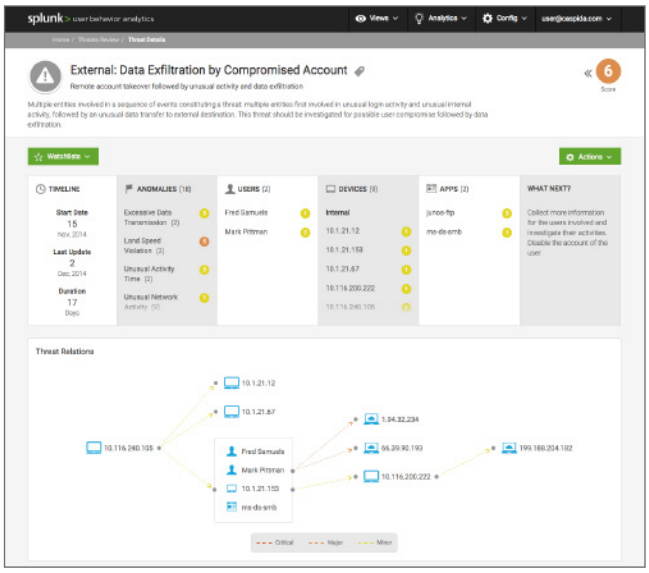
Sample Threats Detected

- **Account Takeover (ATO) –** compromise of privileged and regular accounts by external, malicious entity
- **Lateral Movement –** navigation of malware within a network
- **Command and Control Activity –** periodic beaconing activity by malware to communicate with CnC infrastructure
- **Data Exfiltration –** the act of stealing private, confidential and sensitive data within an organization by malware or an attacker
- **Browser Exploits and Malware Activity –** infection discovery of polymorphic attacks and advanced persistent threats (APTs)

Why Behavior Analytics from Splunk?

Machine learning, statistical profiling and other anomaly detection techniques need a foundation. A massively scalable and readily available data platform is required to support advanced analytics—one that provides users accessibility, quality and data coverage from a range of security and enterprise systems. The entire lifecycle of security operations: prevention, detection, response, mitigation, to the ongoing feedback loop, must be unified by continuous monitoring and advanced analytics to provide context-aware intelligence. The threat detection capabilities in Behavior Analytics extend the search/pattern/expression (rule) based approaches currently in Splunk and Splunk ES for detecting threats.

Splunk can provide the data platform and security analytics capabilities needed to allow organizations to monitor, alert, analyze, investigate, respond, share, and detect known and unknown threats regardless of organizational size or skillset.



Splunk User Behavior Analytics - Threats Review

"Account takeover is one of the most significant debilitating challenges we face as a major B2C company; the resulting cyber-fraud costs us millions and current security tools are no longer able to keep up with today's sophisticated attacker. A new, behavior-based paradigm is what we need."

— CISO, major consumer financial company

Learn more about Splunk User Behavior Analytics by contacting ubainfo@splunk.com.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com

20-13557-Splunk-UBA to Detect Cyberattacks-108-TB