

Detecting Advanced Threats

The biggest challenge in protecting your organization from advanced threats is the unique and complex nature of each assault. Attackers frequently incorporate advanced custom malware designed to take advantage of specific exploits -- in many cases employing a series of highly-sophisticated zero day attacks. They frequently combine malware with well-planned physical theft and clever social engineering to harness a full spectrum of logical, physical and social attack vectors.

After detecting a compromise, it's difficult to immediately determine if the compromise was due to an Advanced Threat based on a single event or a simple behavior sequence. An attacker launching an advanced threat will typically employ several phases. Each step needs to be detected individually and then correlated with the others to discover the true nature of the attack. Gauging the sophistication level of an attack and observing the activity immediately surrounding it provides a better understanding of whether or not an organization is being targeted by an advanced threat.



The following represents three possible components of an advanced threat, how they can be detected, and how to take action with LogRhythm.

Breaking and Entering	Cracking the Safe	The Getaway
Customer Challenge		
Recent, high-profile attacks have been initiated by targeting specific groups within the organization. They disguise phishing emails as legitimate corporate communications, delivering payloads such as malicious PDFs that when opened perform function such as installing a root kit.	After successfully gaining access to a network, an attacker will avoid detection, often cloaking his behavior by using authorized credentials to emulate a legitimate user. For example, many attackers (human or malware) will log in to a genuine user account and will use it to slowly probe the network for shared folders containing confidential data.	Once attackers have successfully gained access to an organization's high-value intellectual property, they can remove data either electronically or physically. They can either download information directly from the server to a removable storage device or they can send it out over the wire.
LogRhythm Solution		
LogRhythm can look for relevant logs being generated within defined time intervals. Recognizing patterns of pre-execution and post-execution behavior of certain types of malware can identify zero-day exploits that standard AV might miss.	LogRhythm can look for a number of unique values over a specified period of time, such as a port probe originating from one account that is systematically scanning the network. Specific rules can be turned on to continuously look for slow port probes.	LogRhythm analyzes log and event data from targeted resources and peripheral assets and correlates it with fully integrated file integrity, network connection, process and removable media monitoring logs. This provides immediate, detailed information on who is accessing and/or attempting to steal confidential data and how it is being done.
Additional Features		
Once an attack has been identified LogRhythm can initiate automated remediation with the option to require up to three steps of authorization prior to taking action. This can include adding an origin IP to a firewall ACL or quarantining an internal host that has been compromised and is propagating an attack.	LogRhythm's active remediation can be configured to disable any account in response to suspicious behavior, such as initiating port scanning on the network or unauthorized access attempts to servers containing confidential data.	LogRhythm's Data Loss Defender can also be configured to actively prevent the removal of data via USB thumb drive. It actively protects your endpoints from data theft by automatically ejecting a drive before a connection is established, preventing critical information from being copied to a removable storage device.