The Challenge of APTs

APTs are threats advanced in method, capability, and resources. This doesn’t always mean they possess advanced technical skills; instead they may have the resources to acquire them. What they do have is an advanced method and approach to achieving their objective. APTs are persistent. They have a specific objective in mind and they will spend months, even years to achieve that objective.

What makes APTs unique and so concerning are their advanced nature and their persistence. They are not an opportunistic criminal trying to find the first unlocked door. They have singled you out for some reason and are ready to spend significant time and resources getting what they want from you.

To compound things, a mature cybercrime economy and supply chain has emerged. APTs and cyber criminals have easy access to for-sale malware, exploits, and for-hire capabilities. This serves as a force multiplier and expeditor when combined with the capabilities an APT already possesses.

The greatest challenge in protecting your organization from APTs is the variety of techniques and capabilities they leverage in a persistent nature. An APT might develop or purchase custom malware designed to take advantage of zero-day exploits that will evade traditional defenses. They might combine this with physical theft and clever social engineering. In the end, they will harness the full spectrum of logical, physical and social attack vectors. APTs and threats like them will continue to increase in number and capability as cyber crime and the supporting economy keeps maturing. We can also expect nation states and cyber-terrorists to continue investing in and honing their cyber warfare arsenals.

APT detection and defense requires a comprehensive approach. It is more than a single technology or process. However, when implemented correctly with good supporting processes, there is no better investment in this defense than SIEM 2.0.
Identify Target Assets
Almost all organizations have something of value to someone else. Identify those assets you possess an APT might value. With the maturation of the cybercrime economy, intellectual property (e.g., trade secrets, source code, design specifications) is increasing in value to cyber criminals. Target assets may also include core capabilities and infrastructure that an APT may want to disrupt for political or monetary gain.

Identify Target Resources
Identify the components of the IT infrastructure that directly host, support, or secure Target Assets. Identify those components, whether at the network, host, application, or data layer, an APT would eventually need to compromise to achieve their objective. For instance, if the Target Asset was source code, the Target Resources would be source code management applications and databases and hosts containing source code copies.

Target Resource Visibility
To protect Target Resources, extensive visibility is required across all impacting activity. Leverage LogRhythm Host Activity Monitoring capabilities to obtain deep visibility across target hosts. All of this information will be collected and centralized in LogRhythm providing extensive visibility into the activity on and around Target Resources.

General Visibility
To protect Target Resources, we need extensive visibility across all impacting activity. Collect any and all log data generated by Target Resources. Leverage LogRhythm Host Activity Monitoring capabilities to obtain deep visibility across target hosts. All of this information will be collected and centralized in LogRhythm providing extensive visibility into the activity on and around Target Resources.

Behavioral Profiling
With visibility in place, we can start to model expected behaviors across the IT infrastructure and Target Resources. This will allow LogRhythm to detect behavioral deviations and anomalies that might indicate the presence of a compromised host or user account, or data being exfiltrated. Behavioral analysis provides a critical layer of threat and intrusion detection since APTs may evade traditional signature and point-based solutions.

Continuous Monitoring
Implement continuous monitoring across Target Resources and the IT infrastructure via LogRhythm’s Advanced Intelligence (AI) Engine. Think of the AI Engine as a team of 24/7 security analysts continuously and tirelessly looking for signs of intrusion, compromise and theft. The AI Engine’s hybrid analysis engine will monitor your log and activity records looking for the presence of an APT based on correlations, patterns, and behaviors.

The Cybercrime Economy
The cybercrime economy has dramatically evolved over the past few years. More stolen assets can be monetized and a mature supply chain has developed allowing for specialization to occur. Tools, skills, and resources can simply be bought. The result is that APTs do not need to directly possess all necessary skills; they can leverage the cybercrime supply chain to obtain custom malware, zero-day exploits, or buy access to an already compromised network (i.e., botnet).

Host Activity Monitoring
LogRhythm System Monitors can be installed on target hosts to monitor and obtain deep visibility into host activity. LogRhythm’s File Integrity Monitoring (FIM) capabilities can detect read and write access to sensitive files. Process Monitor records all process activity on the host. Network Monitor records network connections to and from the host. Data Loss Defender records files transferred to removable media. This level of visibility is required to defend target hosts against APTs.

Host and User Profiling
LogRhythm’s AI Engine monitors for deviations and anomalies to a host’s expected behavioral profile, providing another layer of intrusion detection capability around target hosts. Unexpected processes, abnormal network connections, and access patterns can all indicate a compromised host. LogRhythm’s AI Engine also monitors user activity and detects behavioral anomalies that might indicate the user account is compromised or a user has gone rogue.

Automatic Remediation
In the defense of an APT, detection is the start, prevention the ultimate goal. LogRhythm includes powerful Automatic Remediation capabilities that trigger preventative measures when threatening activity is observed. Whether disabling a compromised user account or terminating a connection between attacker and target, LogRhythm can immediately respond on your behalf. A quorum-based approval model can also be used that requires manual approval prior to response.
Watching for APTs

It’s important to remember that APTs are both “advanced” and “persistent.” An APT is rarely detected through a single event. It will typically unfold over several phases that need to be detected and correlated to discover the true nature of the attempted breach. Gauging the sophistication of an attack and observing the activity immediately surrounding it, provides a better understanding of whether or not an organization is being targeted and/or compromised by an APT.

The following speaks to the three primary phases of an APT and how LogRhythm would detect and defend against each phase via AI Engine combined with Automatic Remediation.

Infiltration

A targeted phishing e-mail is sent to an organization’s executive team that directs them to a compromised web server that downloads customized malware. The malware is not detected by anti-virus software and successfully installs a key logger program. The malware periodically transmits acquired key logger data to an external host.

How LogRhythm Would Detect and Respond:
- Via Host Profiling, the key logger process would be observed as an unexpected process. Automatic Remediation could terminate the unexpected process.
- The transmission of data to an anomalous location might be observed. Automatic Remediation could terminate the transmission and/or implement a router/firewall ACL.

Compromise

An APT has successfully compromised a user account and is using it to slowly probe the network for shared folders containing confidential data.

How LogRhythm Would Detect and Respond:
- Login activity and patterns might emerge indicating the account is compromised. For instance, near concurrent logins from different geographic locations using the same account.
- As the APT scans and accesses other systems, suspicious audit failure activity would be observed such as 10 or more failed authentications to 10 different hosts. This would be observed over hours or days.

Exfiltration

An APT has successfully gained access to an organization’s high-value intellectual property, requiring the data to be removed, either physically or electronically. There are two options—physically walking the data out of the building or electronically sending it out over the wire.

How LogRhythm Would Detect and Respond:
- If exfiltrating physically, an anomalous file transfer might be observed from the target host to a workstation and from the workstation to removable media.
- If exfiltrating electronically, an anomalous network transmission might be observed based on time, amount, and/or location. Automatic Remediation could terminate the network connection and/or implement a router/firewall ACL.

Conclusion

While there is no magic bullet that will completely mitigate the risk APTs present, a well-planned SIEM strategy can go a long way toward protecting your organization. LogRhythm’s integrated SIEM 2.0 solution, combined with the right processes and other core security technologies (firewalls, IDS/IPS, anti-virus/anti-malware, etc), can greatly increase your ability to detect and respond to APTs and reduce the risk these and other threats pose to your organization.

The most expensive data breach included in the 2012 Cost of Cyber Crime study cost a company $46 million to resolve. (Ponemon Institute)

The average organizational cost of a data breach in 2012 increased to $8.9 million. (Ponemon Institute)

© Verizon Breach Investigations Report 2012

*Stolen login credentials*