DARKTRACE

Crimson Echo: Operationalizing for the Analyst

Threat hunting for Chinese-nexus actors frequently begins with a review of existing adversary profiles. These resources will detail traits of such actors to provide analysts with context to help form their hypotheses for investigation.

Attributable elements typically include details related to the infrastructure, tooling targeting, and motivations of these groups. For threat hunting specifically, analysts will keenly review the associated tactics, techniques, and procedures (TTPs) for these groups. While such documents can provide an effective point of reference, the various iterations and overlapping organizational lines that characterize China-nexus threat actors presents its own challenge.

Therefore, analysts can begin to operationalize the insights of this report by using the targeting, TTPs, motivations, and general tooling sets as a starting point for a generalized model of "China-nexus activity". Analysts should use the TTP clusters, co-occurrence patterns, and dwell-time data from this report as the baseline model for Chinese-nexus threat hunts.

By using a higher-level framework for Chinese-nexus activity, hypothesis generation and overall direction for threat hunting, as well as the prioritization of such activities should become clearer.

However, the identification of Chinese-nexus groups within an organization's networks requires further information given the variability within compromise type and the adaptability of such groups. While an analyst could use a technique, such as DLL side loading, as a starting point, the exact context for such a technique is still missing. An investigator still does not know key elements such as the frequency and prevalence of the technique based on their systems, the TTPs that may appear alongside evidence of sideloading, how long into the compromise would one expect to see such a technique, and what elements of the kill chain would likely follow.

Contextual metrics lend themselves to a more effective threat hunt and allow analysts to better identify relevant sets of activity within more generic heuristic detection mechanisms.

Darktrace analysts structured this report not only as a general framework as noted, but also data-driven insights to operationalize the findings. This information provides a frame for threat hunters: the level of risk, and the nature of the threat faced by the organization with respect to Chinese-nexus groups.

Each subsequent section increases in specificity for investigators. The report details the commonly observed TTPs and their distribution across cases and region. The report then notes the co-occurrence of such TTPs to identify what combinations of activity a defender may expect to see on their networks over the entire course of the operation.

Compromises involving Chinese-nexus groups can extend for months, if not years. Therefore, data relating to the dwell time between initial access and specific tactic events is also presented, so to inform the timeframes of threat hunts and set expectations as to when a specific technique may be seen.

However, knowledge that there could be a cluster of lateral movement activity after certain periods of time does not address the challenge of properly identifying this cluster with the noise of everyday activity, even with TTP insights.

This challenge is particularly true for large organizations with complex, high-volume environments, where distinguishing true malicious clusters from routine operational noise requires contextual metrics.

Therefore, the results section ends with a review of the nature of activity clusters to provide defenders with further guidance on the nature and content of such activity clusters. In conjunction these insights and metrics allow SOC analysts and cyber professionals to not only gain a better understanding Chinese-nexus cyber operations, but also proactively hunt for it in their networks.

DOWNLOAD THE FULL REPORT ↗