Intrusion Detection FAQ: Assessing Outbound Traffic to Uncover Advanced Persistent Threat (APT) *Binde, McRee, O'Connor*

Advanced Persistent Threat (APT) describes attacks by highly competent adversaries who are determined to obtain the information assets targeted for acquisition. Objectives can be political, economic, technical or military in nature. Layered defensive tactics (multiple layers and means of defense) can prevent security breaches and, in addition, buy an organization time to detect and respond to an attack, reducing the consequences of a data breach.

APT detection can be undertaken with open source tools such as OSSEC, Snort, Splunk, Sguil, Scapy and Squert. Approaches to detection include the following methodologies.

Rule Sets or signatures detect network behaviors commonly associated with APT by matching traffic with known malicious patterns. This includes activity such as:

- phishing email campaigns
- PI-RAT (Poison Ivy Remote Access Toolkit) start up
- "known bad" Windows registry entries
- detect PI-RAT shell code within Microsoft Office and PDF files

Statistical and correlation methods identify possible issues through analysis of event frequency and occurrence simultaneous with other events.

Fast-flux rapidly swaps the IP addresses associated with a domain name, often as frequently as every 3 minutes. The DNS response changes with each query request from the victim host. Statistical frequency analysis of log files ascertain whether warning thresholds evincing fast flux are reached. As fast flux increases the difficulty of tracking exfiltration efforts, finding evidence of fast flux on the network is an indication of probable APT activity.

Splunk correlates events from multiple log sources. Different log sources all indicating PI-RAT behavior provide stronger evidence of APT presence. Splunk queries can be defined to issue alerts when these specific correlations are found.

Manual approaches are employed when no signature is yet in place to identify malicious traffic. Odd egress traffic, internal network scans, DNS logs, and anomalous traffic (as compared to known good netflow baselines) are examples. LizaMoon has been used to establish the first foothold in the target environment, allowing determined attackers to install malware for later exploitation. Such events prompt a device to be placed on a watchlist for examination by an analyst.

Automatic Blocking of Data Exfiltration examines outgoing traffic and automatically blocks traffic based on characteristics of the traffic. Use of RAR files to disguise sensitive data is a known technique and is blocked. If feasible to restrict outgoing network access to business hours, the opportunity for APT is limited as well. Finally, blocking network access to devices known to host malicious content or previously used in an attack provides an additional layer of defense against APT.