splunk>

TECH BRIEF

ADVANCED THREAT DETECTION AND RESPONSE

Using Splunk software to defend against advanced threats

What is an Advanced Threat?

An advanced threat is an adversary that uses multiple attack vectors to obtain or change information. Advanced threats are often difficult to discover, remove and attribute. Advanced threat vectors can include phishing, infecting websites with malware, brute force attacks, social engineering to obtain trusted access, and targeted attacks that include zero-day exploits. An advanced threat will compromise one or more systems, and establish persistence and communication channels to direct activities to accomplish its goals.

An advanced threat executes a sequence of activities to gain entry and trusted access, find the asset of interest, and transfer the asset out of the organization. A popular reference to this attack lifecycle is the kill chain (see Figure 1).

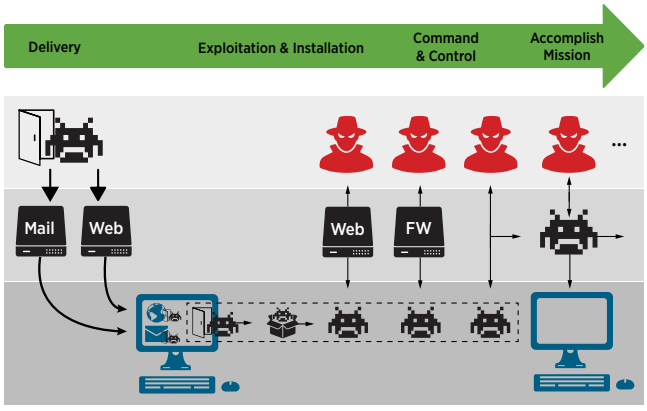

Figure 1: Overview of advanced threat attack lifecycle.

Attack Lifecycle – Kill Chain

Delivery

An advanced threat often begins with the download of malware. Infections can occur by clicking on malicious links or file attachments in emails or visiting an infected or malicious website.

Exploitation and Installation

The malware that is downloaded to the system must be executed (either automatically or executed by a user tricked into clicking some dialog box or by opening up an email attachment). Malware is often hidden or embedded in common documents and web files, such as a PDF document or a JPG image file, and opening or accessing these files executes the malware. Advanced techniques can exploit a known or unknown vulnerability and install itself on the target system.

Once executed, the malware performs a variety of activities to run undetected on the endpoint. For example, the malware may continue by installing programs that “look normal” or by turning off an endpoint security application and/or endpoint logging, or by replacing system files or system programs that are normally allowed to run on the endpoint.

Command & Control

With malicious software installed on the endpoint, the malware communicates with a command and control server to download additional software or to receive instructions. Instructions can include specific files or data to be stolen from the target organization. The communication between the victim(s) and the command and control servers often use common communications protocols that are hidden in plain sight in HTTP, FTP and DNS protocols. The communication may also be encrypted by using SSL over HTTP or by using remote control protocols like RDP.

Accomplish the Mission

With a foothold within the organization and communication channels to direct activities, the adversary has established persistence and can take steps to accomplish its mission. At this stage, advanced threat activities come from valid user accounts and systems that are trusted within the environment.

Advanced Threat Detection and Response

In the advanced threat attack lifecycle, there is an adversary that would like to get into your environment and has an objective against your business. This adversary is motivated and resourced. They utilize multiple attack vectors and techniques to get onto your systems, exploit the trusted access that system has in your network, stay on your systems, and steal from your organization or damage your business. Activities can include lateral movement (find and take over additional endpoints and systems). The adversary uses valid credentials to gain access to endpoints, systems and asset stores. Objectives can include modifying, viewing and stealing information, as well as selling access to your organization. The adversary will want to hide and maintain persistence.

Having access to and analyzing all data can be helpful in detecting and responding to advanced threats. Monitoring for known attacks and unusual activity, and then linking them together using the kill chain method, can help identify compromised hosts and advanced threats that have gotten into your organization. This approach focuses on detecting post-exploit/infection activities with the assumption that an adversary has gotten into the environment (assume you've been compromised). The following examples illustrate techniques to look for compromised hosts and could play an important part of breach response and malware/APT hunting.

Detecting Advanced Threat Activity From the Host Perspective
Unusual File Name
• **What to look for:** Short file names • **Why to look for it:** Attacker wants to run a program that avoids detection • **Source data required:** Endpoint/system logs; file names are in a field called 'file' • **How to detect:** ... | eval file_length=len(file) | where file_length < 4
Rare Executable
• **What to look for:** Rare executables in your environment, especially in a controlled environment • **Why to look for it:** Attacker has to install and run malware in the endpoint • **Source data required:** Log that contains names of running processes, e.g. tasklist in Microsoft Windows or ps in Linux • **How to detect:** ... | stats dc(host) by process | sort + dc(host)
Process/Program Starts Whenever Windows Starts
• **What to look for:** Changes to the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run • **Why to look for it:** Malware needs to run on the endpoint to conduct malicious activity • **Source data required:** Monitor Microsoft Windows registry, e.g. Splunk Forwarder, RegMon or ETDR solution • **How to detect:** createKey | stats count(process_image) by process_ image key_path host
Unusual Administrative Activity
• **What to look for:** Clear event logs • **Why to look for it:** Attacker wants to delete evidence of activities by deleting logs • **Source data required:** Microsoft Windows event logs • **How to detect:** EventCode=1102 OR EventCode=517

Detecting Advanced Threat Activity From the Network Perspective

Unusual Outbound Activity Using DNS - 1

- **What to look for:** High number of DNS requests occurring from a particular client compared to baseline
- **Why to look for it:** Possible advanced threat communication (instruction, stealing data) using DNS protocol
- **Source data required:** DNS logs
- **How to detect:** sourcetype=dns | stats count(clientip) AS Requests by clientip | sort - Requests

Unusual Outbound Activity Using DNS - 2

- **What to look for:** High number of same-sized DNS requests from an internal host, patterns of same-sized DNS request
- **Why to look for it:** Possible advanced threat communication (instruction, stealing data) using DNS protocol
- **Source data required:** DNS logs
- **How to detect:** sourcetype=dns | eval Length=len(query) | stats count(clientip) by Length | sort – Length

Beaconing (Phone Home) to Notify Attacker of Successful Installation

- **What to look for:** Traffic with periodicity – e.g. traffic to the same URL at the same interval every day
- **Why to look for it:** Malware trying to establish communication with command and control server to get instructions
- **Source data required:** Web proxy logs or firewall logs; 'dest' could be a URL, domain or an IP address
- **How to detect:** ... | streamstats current=f last(_time) as next_time by dest | eval gap = next_time - _time | stats count avg(gap) var(gap) by dest

Contact to Command and Control Server, Other Malware Sites

- **What to look for:** Traffic to sites listed as 'none' or 'unknown' by a reputation service or category filter
- **Why to look for it:** Attackers often use new or low traffic domains that have not been evaluated by reputation engines
- **Source data required:** Web proxy logs or firewall logs with reputation
- **How to detect:** source=proxy sc_filter_category=None OR sc_filter_ category=unknown| stats count(clientip) by s_hostname, clientip

Malware Delivery and Installation

- **What to look for:** Fast requests following the download of a portable executable (PDF, Java, .exe, etc.)
- **Why to look for it:** Indicator of initial exploitation, installation and downloading additional malware/files/instructions
- **Source data required:** Web proxy or firewall data that includes complete URL or file names
- **How to detect:** source=proxy [search file=*.pdf OR file=*.exe | dedup clientip | table clientip] | transaction maxspan=60s maxpause=5s clientip | eval Length=len(_raw) | sort –Length

Malware Communicating to Command and Control Server(s)

- **What to look for:** Traffic to or from blacklisted (internal list, threat intelligence sources) addresses/domains
- **Why to look for it:** Advanced threat/malware requires on-going communication with adversary to accomplish its objectives
- **Source data required:** Any log data with IP address or domain name; any data source (log/file) of blacklisted IP or domains
- **How to detect:** source=firewall action=Permit | lookup malicious clientip as dst | stats sum(bytes) by dst

Summary

Splunk software can be used to detect network and host activity that might be indicative of an advanced threat. Unlike many current solutions, Splunk is uniquely suited to collect, index, correlate and analyze all data, and to monitor patterns of activity over the very long periods of time required to see a potential attack. In addition, analytics and numeric functions can be used to create complex searches that employ user-defined thresholds customized to the enterprise architecture. Field extraction, lookup and pivot capabilities can be used to link any combinations of events/activities to understand the event chain required to uncover advanced threats, compromises and potential data breaches.

The information contained in the examples represents only a starting point for observing unusual activity on hosts and on the networks that can be used to detect and respond to advanced threats. These have not been tested in an active environment. Threats and attack vectors are constantly changing and it is up to the reader to stay abreast of conditions that may warrant changes to any security program.

splunk> sales@splunk.com www.splunk.com

TB-Splunk-ATD-103