

Detecting Advanced Persistent Threats

Using Splunk for APT

What is an Advanced Persistent Threat?

An advanced persistent threat (APT) is a targeted effort to obtain or change information by means that are difficult to discover, difficult to remove and difficult to attribute.

So, what's the data that attackers are after, how are they looking to obtain or change it and why are their attacks so difficult to discover, remove and attribute?

How Attacks are Perpetrated

In Search of Victim Zero – Using data from social networks such as LinkedIn or Facebook, attackers can craft an email to a targeted user containing some attachment (PDF or ZIP) that entices the user to open it.

This attachment could be named “Organizational Changes” <insert boss's name here>. The employee clicks on the attachment, the malware is inserted onto the users system and sends a signal outbound to a specific domain. This process is continuously repeated with slight differences tailored to the individual receiving the email.

High Value Targets

Email – Emails (and attachments) are a rich source of data that may be of high value. Emails can contain discussion threads that can point to other high value targets in the IT infrastructure.

The emails can be a source of intelligence that can lead to spear-phishing emails that contain malicious attachments or links to attacks. Windows users keep a significant amount of email on their machines in a local .PST file—in many instances this file can be as large as a gigabyte.

Attachments can contain financial data or other highly sensitive information. In addition to going after the emails on a users local machine, attacks can also target the email server itself.

Public Key Infrastructure Data – According to Mandiant™ Inc.'s M-Trends Report 2011, while the majority of APT cases started with an email as an attack vector, “Attackers have increasingly focused on obtaining PKI-related data resident within a compromised network.” PKI data can be used to authenticate to a client VPN as well as decrypt SSL traffic from servers.

Mandiant's investigations discovered that “victim zero in a current investigation was actually victim 127 in an intrusion dating back several years.”

The Spread of APT – The proliferation of APT is accomplished in a variety of ways but the most prevalent is via Windows services. Again according to Mandiant, RIP Listener Service (IPRIP), the Wireless Zero Configuration service (wzcsvc) and Background Intelligent Transfer Service (BITS) are all either used or replaced by a rogue service. Victim zero uploads the malware to a remote computer file share, which is executed using the at.exe command.

Seeing Malware

Host Based Evidence of Possible Malware – According to Mandiant – Monitor for the following changes to hosts (assumes a Splunk Universal Forwarder is resident on the host):

Potential email theft

- Monitor hosts for the existence of executable named with a single letter (g.exe or m.exe)
- Watch for the creation or changes to C:\Windows\Help\help\<user>\
- Watch for the creation or rapid growth in size of files and directories in the C:\Windows\Help\Help\user subdirectory
- Watch for changes to the Windows registry file

Watching for the spread of malware

- Watch for changes to enablement or changes to Wireless Zero Configuration Service (wzcsvc)
- Watch for changes to enablement or changes to RIP Listener Service (IPRIP)
- Watch for changes to enablement or changes to Background Intelligent Transfer Service (BITS)
- Watch for changes to the task list for at.exe. (SchedLau.txt)

Other indicators of system compromise

- Watch for changes to Services.exe
- Monitor that Windows File Protection is enabled
- Monitor for changes to the group policy object at C:\Windows\System 32\GroupPolicy\User\Scripts\scripts.ini
- **Network based evidence of Malware** – Mandiant's report is less specific here so we've come up with a few of our own:

DNS (If using Active Directory's DNS functionality, turn on debug mode to get the URLs into the log data.)

- Baseline DNS requests and watch for too many from a particular client. The malware may be network mapping from the inside out
- Monitor for hosts that are making the same DNS request at a consistent interval (watching for 'beaconing hosts')
- Monitor for the same sized DNS requests from internal hosts

Web Proxy

- Monitor for mismatches between the extension of a requested file and the mime type of the file returned
- Monitor and investigate visits to sites that are listed to be of a 'None' or 'unknown' category by a reputation service or category filter

- Monitor for fast requests following the download of a PDF, java, or exe. If a download is preceded by rapid requests for more files this is a potential indicator of a dropper
- Monitor accesses to web mail services – watch for IPs outside of your allowed pool accessing outbound – possible exfiltration of data

Firewall

- Use ‘allowed’ ingress and egress traffic to determine how many internal systems may be communicating with a malicious IP addresses to know how much data was transferred and the time(s) the activity occurred
- Monitor for abnormal amounts of out-bound traffic to certain domains. Use a ‘look-up’ to a watch-list (see Splunkbase for information on how to perform a look-up to a database or .CSV file of ‘bad sites’).
- Watch for mismatches of a known protocol to an uncommon port or unknown protocol on a common port (e.g., FTP traffic on TCP 22 should at least initiate on TCP 21 or unknown protocol on TCP 22 – TCP 22 is generally used for SSH). Watch for potential false positives for Skype and streaming media.

Using Splunk

Monitoring a combination of network data and host file integrity monitoring data can be key for detecting APTs. Unlike many current solutions, Splunk Enterprise is uniquely suited to monitor patterns of activity in data over the very long periods of time required to see a potential attack. In addition, Splunk’s analytics and numeric functions can be used to create complex searches that employ user defined risk-based thresholds customized to the enterprise architecture.

The information contained in search suggestions and examples below represents only a starting point for observing anomalous activity on hosts and on the networks and is not meant as a complete APT program. The searches have not been tested in an active environment. Attack vectors are constantly changing and it is up to the reader to stay abreast of conditions that may warrant changes in APT strategy.

Splunk: Sample Searches for APT

Host based (Splunk Universal Forwarder on Host)

Monitor hosts for particular executables.

- `...| eval file_length=len(file) | where file_length == 4`
- Watch for the creation or rapid growth in size of files and directories in the `C:\Windows\Help\Help\user` subdirectory.
- `index=helpchanges | delta filesize AS Size_Change |`
- `table _time filesize Size_Change | sort - _time`
Watch for changes to the `HKEY_LOCAL_MACHINE\`

`SOFTWARE\Microsoft\Windows\CurrentVersion\Run.`
Here the attacker wants to restart his code each time Windows starts.

- `createKey | stats count(process_image) by process_image key_path host`

Network Based

Too many DNS lookups occurring from a particular client.

- `sourcetype=dns | stats count(clientip) AS Requests by clientip | sort - Requests`

Too many same-sized DNS requests from an internal host, indicating a possible exfiltration.

- `sourcetype=dns | eval Length=len(query) | stats count(clientip) by Length | sort - Length`

Watch for hosts that talk to the same URL at the same interval every day (“Beaconing” of servers to websites). Sites with a low `var(gap)` value are discovered.

- `... | streamstats current=f last(_time) as next_time by site | eval gap = next_time - _time | stats count avg(gap) var(gap) by site`

Site visits that are listed as a ‘none’ or ‘unknown’ by a reputation service or category filter.

- `source=proxy sc_filter_category=None OR sc_filter_category=unknown| stats count(clientip) by s_hostname, clientip`

Fast requests following the download of a .PDF, java, or exe. If a download is preceded by rapid requests for more files this is a potential indicator of a dropper.

- `source=proxy [search file=*.pdf OR file=*.exe | dedup clientip | table clientip] | transaction maxspan=60s maxpause=5s clientip | eval Length=len(_raw) | sort -Length`

The internal systems identified during an investigation that were communicating with a malicious IP address.

- `source=firewall action=Permit | lookup malicious clientip as dst | stats sum(bytes) by dst`

Free Download

[Download Splunk](#) for free. You’ll automatically get all of the Enterprise features of Splunk for 60 days and you can index up to 500 megabytes of data per day. Or if you want to get started right away with an Enterprise license contact sales@splunk.com.