More on APTSim

By Ar-themes

Archived: 2026-04-05 17:42:47 UTC

Today I wanted to talk a bit more about APTSim. We all know by now that the bad guys always get in. Especially determined, well funded and well equipped attackers. We know roughly HOW they are getting in which is usually via a targeted Phish, SQLinjection, malicious URL, etc. Things that are hard to defend against because they depend on a human element or trust partnerships between organizations.

What we don't think about is the fact that our Incident Response and detection teams don't get exercised sufficiently (or ever) which makes them much less effective than they could be. We also don't think about modeling and understanding what real attack traffic looks like so we can tune our defenses against it. REAL traffic, not Nessus scans or CoreImpact exploits.

How can we know that our people and systems are actually able to detect the types of attacks we really care about if we don't know what each attack looks like in every data source we have. Is there a windows event log entry reflecting a change in service permissions? Can the timing pattern in the call home beacon be seen in net flow? What does an exfil file hidden in the recycle bin via user SID look like, and is it visible?

If you know all the malicious inputs to the system ahead of time, then you can determine all the data sources you have that show indicators that something has happened, rather than waiting until an attack happens to attempt to track it all back and hope for the best.

This subject is a bit more tricky so lets approach it first with an example. Using HERMES, we analyzed some samples and activity from a group of APT actors that we call "UPS". The typical UPS attack performed the following activities (this information was compiled from IR activity and shared data from other victims):

- Generate a particularly timed beacon that communicates over HTTP
- Drop the command line Chinese language version of winrar on the target
- Replace sticky keys with cmd.exe for persistence and access via RDP
- Turn on RDP if it's not already enabled
- Index and archive all office documents, compress and encrypt them with RAR and a specific password and store them in the recycle bin
- Enable the support_388945a0 account and add it to the local admin group
- Exfiltrate the data encoded over port 443 (but not SSL)
- Setup an insecure service for persistence / privilege escalation

That is a fairly comprehensive list of attacker activity and each action generates either specific network traffic, log entries, and files on the target. So what we do with APTSim is to take all the above information and create a piece of pseudo-malware that takes the same actions, except in a safe and controlled manner, and includes cleanup components so it can be removed when the exercise is complete.

Customers have different preferences as to how we take the next step but generally one of a few options is commonly used:

- AR has VPN access to the customer network
- AR has shipped a special box which the customer plugs into their network
- AR conducts a physical penetration to launch the APTSim via a malicious USB key, custom developed Teensy, or other hardware implanted in customer equipment
- AR generates a targeted phish mirroring the initial vector used by the original actors whether that's a malicious attachment or a URL, etc.
- The customer executes the APTSim model themselves

The APTSim model then connects back to our command & control center, takes all the same actions as the real attacker, exfiltrates data and then the customer is notified of what activity took place. The notification is a short document contains log entry examples, PCAP examples, time and dates, ports used, in short everything that is needed to detect the activity as well as track it back post event.

If the attack simulation is not detected then AR will assist you in tuning your defenses whether that means new rules for your Cisco ASA's, custom ClamAV or Snort signatures, specialized Splunk apps, etc.

Rather than a barely useful once a year event, this process is ongoing, monthly or as new attacks are found and analyzed. When one of the organizations in your business sector is hit, within a very short period of time you know the crucial details of the attack, are tested to see if it could hit you as well, and finally are ready to defend before the attackers come for you. This is being proactive rather than reactive.

For more information hit up info [at] attackresearch.com.

V.

Source: http://carnal0wnage.attackresearch.com/2012/09/more-on-aptsim.html