All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

The four tactical situations of cyber conflict

Many folks appear not to recognize that different tactical situations call for different protection. While the field is not mature by any means, in the same was that Sun Tzu[1] recognized the facts of troop and commander dispositions with respect to the battlefield called for different actions, the cyber warrior and the cyber defender, should learn to recognize the tactical situations that apply to information-related conflict. To date, the four that have been identified are:

- **Distant:** The distant situation is one where the opponent send information inbound and receives returns with no other source of information.
- **Proximate:** In proximity, the opponent sees the same external activities that we see.
- **Enveloped:** In envelopment, the opponent controls all input and observes all input.
- **Overrun:** In overrun, the opponent potentially has all of the capabilities you have.

Attacker objectives

As a general rule, parties many have different objectives. But from the defender's perspective, it is often useful to characterize attackers as undertaking a process by which they (1) gather intelligence (2) seek to gain some level of access to systems, and (3a) seek to expand their access and/or (3b) seek to exploit their access. We will call these levels of access for the purposes of this discussion.

Distant

The distant attacker is always present in the Internet of today. They are in the attack process at level 1 trying to get to level 2. Against level 1 actors, things like firewalls, external facing deceptions, network intrusion detection, and similar methods can be effective to different extents. This is generally preferred for the defender, as keeping them out is a lot easier than dealing with them once they are in.

Proximate

The proximate attacker is generally present whenever you are in public space or in someone else's network. They are also present when they have gained access to another system proximate to your system. In this case, they are in level 1 seeking level 2 access with respect to your system, but at level 3 with respect to proximate systems. Against these threats, many of the same methods work in terms of direct defense as in the distant situation. However, defenses that depend on limited knowledge by the attacker of the external traffic patterns can only be defeated by the induction of false traffic so that the defender makes type 2 (omission) or type 3 (substitution) errors. In this situation encryption is also required to limit intelligence efforts, and even then covert channels typically present in such systems will reveal significant intelligence.

1 Sun Tzu, “The Art of War” (Translated from Chinese By Lionel Giles, 1910) http://all.net/books/tzu/tzu.html

Enveloped

When enveloped, the outside world cannot be relied upon. Encryption and authentication may be of limited effect, but the lack of trusted paths, safe key distribution, safe communications, and other internal support is problematic. From DNS redirected to the wrong place to forcing encryption failures or use of the weakest available mechanisms, envelopment is a bad situation to be in. This almost always translates into situation 2 or 3(b) and unless great care is taken, will lead to 3a. Separation of duties, risk disaggregation, redundancy, and similar methods reduce the effects of limited envelopment. It is often feasible, once recognized, to defeat envelopment with additional channels to the world. A single access path to the Internet are always enveloped at the ISP, even if benevolently.

Overrun

Overrun is, needless to say, the worst situation for the defender. In overrun, the attacker effectively has the same level of control as a systems administrator at the console. Thus they are in situations 3(a) and 3(b). They may also seek to expand their presence bu using attacks at level 1 and 2 against other systems in your environment. In such situations, methods like effective separation of duties, internal deceptions, risk disaggregation, and high surety protective measures are often effective, but at some level of overrun, the system is no longer yours to defend. Recovery in such situations normally calls for a full rebuild and restoration, assuming the overrun is relatively recent.

Preparedness

The solid defender will not only recognize the different situations, but prepare for them. Preparation typically includes (1) some level of situation awareness to detect which situation you are in over time, (2) some level of direct tactical response to react to attacker success, (3) some amount of strategic planning (typically architecture and process) to limit the consequences of different situations, and (4) an ability to recover and adapt out of worst case situations and changes in the external environment.

Summary

Recognizing the tactical situations that may come to exist is fundamental to holding a position and fighting back against the onslaught of the informational enemy. While the art of cyberwar is only in its infancy, clearly, there are different horses for different courses.

- Perimeter defense against the distant attacker works as it always has, and it should be embraced as long as it brings advantages against the distant hordes currently present. Leveraging things like passive deception and firewalls is clearly in your best interest.
- The use of active deception, encryption, authentication, and multiple locations helps against the proximate attacker, and failure to apply these things will likely result in more rapid compromise under proximate attack.
- Envelopment is a tougher situation, but one that can almost always be adapted to in short order is the defender is prepared and adequately resourced. Detection is the key.
- Overrun happens far too often, and usually because a user invites the enemy in through lack of diligence or weak approaches to software by the enterprise.

Knowledge is power. Contemplate your strategy and tactics for the four situations.

