Symbiot, Inc.
P.O. Box 9646
Austin, TX 78766-9646

On the Rules of Engagement for Information Warfare

Paco X. Nathan, Mike W. Erwin

Contributors: William W. Hurley, Jamie L. Pugh, Frank X. Milano, Rick Waters

1. *Background*

To date, the best practices for information security in the private sector have focused on defense. Tremendous efforts have gone into developing and marketing defensive network tools – so much so that the market space is cluttered with an array of “solutions” which become difficult to distinguish. Capabilities for active countermeasures have, for the most part, been considered outside of the appropriate scope of response for commercial enterprises.

For a complete defense, *offense* must be considered. This paper outlines the use of strategies and tactics which have been refined by thousands of years of warfare, diplomacy, and legal recourse. These are applied in the context of proportional response within the global Internet environment, to initiate Rules of Engagement (ROE) for Information Warfare.

2. *Historical Basis*

Prior efforts to establish proportional response have been limited. For example, some proactive measures have been initiated for targeting network abusers. One example is the Realtime Blackhole Listing$^{\text{SM}}$ (RBL) by Mail Abuse Prevention System LLC[1], which has operated since 1997 – amidst controversy over free speech. Parallel services exist for identifying known perpetrators of Internet fraud. In the former case, the issues surrounding “spam” are less well-defined legally and therefore subject to greater controversy, whereas in the latter case the legal issues concerning fraud are clearly defined.

More general attempts at providing widespread security response include the CERT® Coordination Center[2] established in 1988, initially in reaction to the Morris Internet Worm[3]. The success of CERT has since led to establishment of the US Computer Emergency Readiness Team[4] (US-CERT).

Note that in each of these examples the emphasis is placed on gathering information, disseminating security advisories, and blacklisting known offenders, i.e. information used for defensive purposes.

3. *Trend Analysis*

The *malware* and malicious scripts in circulation today are mostly based on techniques and example code from tutorials[5] which were published nearly a decade ago. These get adapted incrementally as Microsoft or other vendors release their system security patches. This is to say that, so far, only limited efforts have been exposed where attackers have developed capabilities based on available engineering technology. A potential exists for much more effective net-centric hostilities against the public and private infrastructure. The consequences of a well-engineered, targeted effort[6] could be devastating.

In the context of increased globalization, international competitiveness, and other transnational issues, the threat of corporate-to-corporate hostilities cannot be ignored. For some enterprises, this category already represents the bulk of their security issues. In the context of rising levels of terrorist activity, including cells seeking out infrastructure targets, the motivation for sophisticated net-centric hostilities are steadily increasing. Another difficulty faced is the complexity of jurisdiction. For example, a firm in Europe may operate through a shell corporation located in the Caribbean to fund hostile network operations through an ISP located in Beijing, ultimately targeting a competitor in North America. Even with a complex attack such as this, the response in most cases must be determined and executed within seconds; which begs the question: what legal jurisdictions, if any, apply?

Also, in contrast to the typical marketing rhetoric of defensive security approaches, the application of *graduated response* has little correlation with the Hollywood stereotype of hackers; viewed from the perspective of the art of war, the traditional emphasis for information security assumes a perpetual state of contentious ground. This has not borne out in practice. Conversely, ROE procedures are introduced to engage the conflict between professionals in a transnational context.

Taken together, these several factors indicate that both the means and the motives for sophisticated attacks are escalating.

4. *The Doctrine of Necessity and Proportionality*

In effect, the result of "erecting defensive walls" around the perimeter of an enterprise network does not provide an adequate deterrent. Rather, the existence of an enterprise network in the context of the public Internet is defined by the *topological boundary* of its exposed services: to exist, it must respond to traffic, and active security is defined not by passive monitoring or isolation, but as a component of response. The innovation of applying ROE allows for informed, decisive, deliberate actions of graduated response – reflecting an ancient international legal norm – based on the severity of hostile acts and the release authority's decision to issue action orders. This process draws on the lawful military doctrine of *necessity and proportionality*. Necessity is defined by the determination of hostile intent and the subsequent use of force in self-defense, justified in situations that are "instant, overwhelming and leaving no choice of means and no moment for deliberation."[7] Proportionality is defined by the limitation of response by the intensity, duration, and realized effect of each attack.

5. *Analysis of Current Practices*

Information security in the private sector has over-emphasized certain aspects while ignoring others. The current best practices represent an underdeveloped model for security, namely the cycle to detect, mitigate, and prevent. Notable components of this approach include the qualitative analysis of tactics (e.g., BugTraq[8]), detection based on *a posteriori* analysis of attacks (e.g., IDS, A/V, NBAD), trivial first-order analysis of vulnerability scanners, and then mitigation and prevention based on point solutions such as firewalls, VPNs, and IPS.

In retrospect, the current thinking which has led to the defense-only approach may be due to over-emphasis placed on automated response in lieu of incorporating human authority into the intelligence cycle. Also the "computer emergency response team" model has suffered to some extent due to two factors: one being the categorical error in the art of war mentioned above, and another being perhaps its root cause, the reliance on email and newsgroups as communication modes, which tend to negate the effectiveness of multilateral response.

Little effort has been spent on developing and deploying means for the determination of hostile intent, coordinating response against known hostile agents, or developing mechanisms of redress for negotiating pressure against upstream providers.

6. *Practice Based on Rules Of Engagement*

The first level of graduated response relies on the effective determination of hostile acts – using levels of threat based on behavioral models, correlating alerts from a variety of security devices, and factoring possible attacks into categories of false positives vs. background automation (scripts in the wild) vs. trival probes vs. substantive activity.

The second level involves efforts to reconnoiter – performed locally by customers, reporting and profiling the source of incoming probes, malware, exploits, denial of service, etc., back to the *operations center*.

The third level involves the determination of *hostile intent*, based on specific characteristics of the customer operations. In some commercial enterprises the *hostility criteria* may be determined, for example, by the repeated unauthorized downloading of their commercial databases by unknown parties, for others the rate of attempted fraudulent transactions, etc. – in a process of describing specific behaviors as hostile acts or equating particular objective characteristics with hostile intent. Hostility criteria are informed by *situational degradation analysis* (SDA), i.e., planning based on knowledge of one's most likely vulnerabilities, which is used to anticipate attacks.

The fourth level involves communicating clearly identified hostilities back to the operations center. This may include requests for surveillance, calling in support for initiating multilateral efforts to observe and confirm the identity/profile of attackers, their set of upstream providers, and their probable jurisdiction.

The fifth level engages direct and indirect countermeasures, applying proportional intensity, duration, and realized effect. Some responses will be initiated by unilateral decisions on the part of the customer, based on the release authority's determinations. Escalated responses will tend to require multilateral efforts: multiple positive identification of hostile intent, attempted resolutions through upstream providers and local jurisdictions, broadcast blacklisting, etc. In the event that such proactive resolutions prove unsuccessful, retaliatory strikes involving asymmetric force will be coordinated at an appropriate level.

7. A Brief Synopsis of Available Countermeasures

The range of available countermeasures that may be invoked in the context of ROE can be divided into two categories of response: symmetric and asymmetric. Symmetric responses are tactical in nature, initiated directly by the customer. These may be distinguished further between purely automated responses and those determined by decision makers based on their level of authority.

Defensive measures provide a first level of symmetric response: existing security devices may be coordinated through *scale of force* procedures to block a hostile act – or degrade the network quality of service (QoS) for indeterminate acts – based on probable levels of threat. A more substantive escalation of symmetric response invokes *challenging procedures*, which combine management protocols and honey-pots to divert, quarantine, and study the probable hostile acts in progress. The results of such analysis – effectively, forward observation and interrogation – get reported from the field units back to the operations center. Another level of escalation for symmetric response involves *reflection*, a principle for "return fire", i.e. to strike against a hostile source – meeting sufficient thresholds for *eyes on target* to obtain positive identification – *using essentially the same methods which they have engaged*.

These symmetric methods are generally automated by executive policy, with override by operations management. In the practical art of war, they are considered dispersive ground. Additional levels of symmetric response apply *invasive techniques*, which require the authorization of management for specific *arming orders*. Invasive techniques can be categorized as: (1) non-destructive; (2) destructive but recoverable; and (3) destructive, non-recoverable – again with respect to proportional response to the hostile acts.

Asymmetric responses require executive findings based on multiple attributions and prior failed attempts at resolution through the upstream providers and local jurisdictions. In these cases, the operations center may call for a variety of efforts, including: (1) escalated multilateral profiling and blacklisting of upstream providers; (2) distributed denial of service counterstrikes; (3) special operations experts applying invasive techniques; and

(4) combined operations which apply financial derivatives, publicity disinformation, and other techniques of psychological operations. These operations are conducted with appropriate consideration for restrictions on point targets and phase lines in the battlespace.

8. Conclusions

In conclusion, it has become clear that for the enterprise to develop a complete strategy of defense, the full cycle of intelligence met with the rules of engagement must be invoked within the theatre of the Internet. Online assets are eclipsing real-world assets due to the inconsequential costs of conveyance, storage, processing, and control. The consequences for continuing a defense-only approach to information security prepare the way for eventual catastrophic infrastructure hits against the enterprise.

Current malicious activities are prosecuted by little more than privateering by analogy, whereas multilateral responses will be backed by capital, coordination, and thousands of years of praxis. Make no mistake, we are in the midst of an information warfare conflict which we have not been fighting.

[1] http://mail-abuse.org/rbl/

[2] http://www.cert.org/

[3] A good account is available at: http://www.snowplow.org/tom/worm/worm.html

[4] http://www.us-cert.gov/

[5] *Phrack* v. 49, p. 14: http://www.phrack.org/phrack/49/P49-14

[6] For example, http://www.newsfactor.com/perl/story/22298.html

[7] Daniel Webster, US Secretary of State, 1840, in response to a British attack on the *Caroline*.

[8] http://www.securityfocus.com/archive/1