Internet Superbugs and the Art of War

Paul Vixie, ISC
NANOG46

Abstract:

The internet has made many things easier in human society, especially including crime. For the last decade the good guys keep losing and the bad guys keep getting rich -- why? Drawing from contemporary examples including the 2008/2009 "conficker worm", from the rise of drug-resistant microbes, and from Sun Tzu's 2,500-year-old "The Art of War", I will try to explain how our approach and our philosophy defeats us even though we remain the superior force.


Softsoap
Naturals
ANTIBACTERIAL

Training Your Opponents

- I did this at MAPS in ~1998
- NANOG did this with Atrivo last year

Received: from remote02.org (unknown [202.126.220.250])
by nsa.vix.com (Postfix) with SMTP id 814CAA13D1
for <paul@vix.com>; Fri, 8 May 2009 14:12:07 +0000 (UTC)
(envelope-from namedroppers@ops.ietf.org)
Date: Fri, 08 May 2009 22:11:57 +0800
From: "Namedroppers" <namedroppers@ops.ietf.org>
To: "Paul" <paul@vix.com>
Subject: i'm do it!!!
Message-ID: <axekvsxmvehidvjtfej@vix.com>

Opposition Economics

- For reasons of efficiency as well as privacy, we all want a minimal response to security problems
- Thus whenever we raise the bar it's only a little too high – not too high at all if attackers improve
- Thus attackers always improve and succeed, and defenders are only prepared for previous attacks
- Thus defenders are not actually controlling costs nor doing any long term good

08:57 <xxx> Oh crap. Conficker just ate my puppy. Hide your women and internetz! Look out!

Subject: new conficker domains registered today, 3/31/09

confickercremoval.net
confickercviruscleaner.com
confickerd.com
confickere.com
confickerf.com
confickerremoval.net
confickerviruscleaner.com
conflicker-removal-tool.com

“Does anyone in your so-called "Working Group" actually do any work in checking the sites you've listed as "malicious"? I've gone to a lot of trouble this week to build a site as a "Resource" for the Conficker Worm. ...”

Cops: "Hands up. Now exponential a number over a prime field.... AHA! We've got you". All within minutes of the sweeping arrest. Epic.

“So of course, the lawyers are not happy…”

"... the provincial government in the north-western Swat valley agreed to implement Sharia law as part of a peace deal with militants there."

“Two ultra-Orthodox Jewish newspapers alter a photo of Israel's cabinet, removing two women so as not to offend readers.”

“Nothing exciting in any of our data stores or sensors, sorry.”

“These are domains which are resolving from today's Conflicker domain names, but which are not resolving to known sink-holes. Most, if not all, of these are pre-existing domains: ...”

“How many Conficker machines are actually good guys running honeypots? :-)

For instance, we have a machine that just sends queries to the 50,000 URLs to see if we get responses (not a Conficker machine but will register in the counts).”

“can we add a -reports sublist and move folks' automated reports there?

many of us are drowning in conficker emails ... useful stuff but we're having difficulty tracking down useful bits.”

“We posted a blog entry with updated information:
...
Sorry this email didn't go out sooner.”

“Monday is Memorial Day in the US and it is a day that many of the US companies give their employees off. So this call will be canceled as I suspect lower than usual participation.”

"...going to see ccTLD Registries dropping out of the containment effort because of the increased, unbudgeted costs they are incurring. And I think we'd be hard-pressed to get them to cooperate in any future containment / abatement efforts."

“They are clunky, and I know how to do it better now, it's a matter of round-tuits. It's mostly been neglected.”

“24x365 abuse coverage is completely unrealistic for small ccTLD registries with the typical mix of hosters, big and small ISPs and larger enterprises as registrars.

And this is just reachability, not actual take-down time. Add a bit of due process into the equation and you certainly will not get instant takedowns.”

The Art of War

Selected Quotations

Deviations From Intent

- Noting that...
  - Internet Security is not war
  - We are not armies or generals
  - Our conflict is mostly not between states

Deception

1.18: All warfare is based on deception.

1.19: Hence, when able to attack, we must seem unable; when using our forces, we must seem inactive; when we are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near.

Augmentation

2.17: ... Our own flags should be substituted for those of the enemy, and the chariots mingled and used in conjunction with ours. The captured soldiers should be treated kindly and kept.

2.18: This is called, using the conquered foe to augment one's own strength.

Lengthy Campaigns

2.19: In war, then, let your great object be victory, not lengthy campaigns.

Fighting

3.2: ... to fight and conquer in all your battles is not supreme excellence [which] consists in breaking the enemy's resistance without fighting.

Tactical Dispositions

4.3: ... the good fighter is able to secure himself against defeat, but cannot make certain of defeating the enemy.

4.4: Hence the saying: One may know how to conquer without being able to do it.

4.5: Security against defeat implies defensive tactics; ability to defeat ... means taking the offensive.

Weak Points and Strong

6.8: ... that general is skillful in attack whose opponent does not know what to defend; and he is skillful in defense whose opponent does not know what to attack.

6.32: ... in warfare there are no constant conditions.

Maneuvering

7.12: We cannot enter into alliances until we are acquainted with the designs of our neighbors.

Choosing Faces

- This is an undeclared assymetric conflict between unidentified attackers and unwilling victims
- Often no law has been broken, or victim's L.E. is outgunned, or attacker's L.E. is corrupt
- The Internet is like a new world in some ways, but it has no government and no laws of its own
- We are all sitting ducks, on permanent defense, waiting for our next opportunity to lose again

Me

- Improve cooperation and information sharing
  - DNS-OARC
  - ISC SIE, NCAP
  - Opsec-Trust
  - This appearance
  - $TBD

You

- “No snowflake in an avalanche ever feels responsible.” (Voltaire)
- Cost shifting
- Outsourcing
- Participation

Us

Discussion