



## Hippocratic Oath: Good Attacks Revisited infectionvectors.com October 2007

### Overview

Welchia was bad. LaBrea was good. Cox went too far. IRC-Unity didn't go far enough. What defines a vigilante? Does the intent and impact of an action help define whether the actor was justified? We may all agree that there is no good offensive malware, but is there such a thing as good malware offense? This article revisits the debate about Internet vigilantism, starting beyond the legacy discussions about "good worms" and looking at accepted offensive mechanisms for protecting one's web interests.

### Ill Will

If you were walking down the street one day and felt sick, really sick, you may decide to go to a doctor. That doctor may diagnose your condition and offer you a prescription for one or more pharmaceuticals. Those drugs may make your condition better, but could also introduce one or more side effects, which may or may not be quite tolerable given the illness that they cured. All of this occurs because of choices you made after being presented with symptoms that lead you to believe you were very sick.

Imagine walking down the street, not feeling sick (yet) and being diagnosed by some external sensor which read your pulse, body temperature, oxygen/carbon dioxide levels, etc. as being infected with one or more bacteria. Unknown to you, the same sensor then doused you with an invisible radiation which killed the bacteria. If that same radiation killed some beneficial bacteria which, in turn, made you feel a little ill later that night, one may reason that at least the malicious bug was not able to spread to someone else. In either case, being diagnosed and treated without consent (if and when it is even medically possible) is worthy of debate.

The debate in the malware research world took a new turn in July of 2007, as ISP Cox Communications took offensive action against bot masters by intentionally redirecting machines that attempt to reach IRC command and control servers. Once redirected, the client machines are fed IRC commands by a Cox-owned device. The commands clearly intend to remove an IRC bot from the client machine.

From the blog of one of the affected IRC server's administrators:

```
[INFO] Channel view for "#martian_" opened.  
-->| YOU (Drew) have joined #martian_  
--= Mode #martian_ +nt by localhost.localdomain  
--= Topic for #martian_ is ".bot.remove"
```

```

2007 9:50:03 AM    == Topic for #martian_ was set by Marvin_ on Monday, July 23,
2007 9:50:03 AM    == Topic for #martian_ is ".remove"
2007 9:50:03 AM    == Topic for #martian_ was set by Marvin_ on Monday, July 23,
2007 9:50:03 AM    == Topic for #martian_ is ".uninstall"
2007 9:50:03 AM    == Topic for #martian_ was set by Marvin_ on Monday, July 23,
2007 9:50:03 AM    == Topic for #martian_ is "!bot.remove"
2007 9:50:03 AM    == Topic for #martian_ was set by Marvin_ on Monday, July 23,
2007 9:50:03 AM    == Topic for #martian_ is "!remove"
2007 9:50:03 AM    == Topic for #martian_ was set by Marvin_ on Monday, July 23,
2007 9:50:03 AM    == Topic for #martian_ is "!uninstall"
2007 9:50:03 AM    == Topic for #martian_ was set by Marvin_ on Monday, July 23,
2007 9:50:03 AM    <Marvin_> .bot.remove
2007 9:50:03 AM    <Marvin_> .remove
2007 9:50:03 AM    <Marvin_> .uninstall
2007 9:50:03 AM    <Marvin_> !bot.remove
2007 9:50:03 AM    <Marvin_> !remove

```

There are two implications that stand out to Internet researchers:

- 1) Cox has broken the “rules of the road” with the hacks to DNS
- 2) Executing commands on a remote machine without user consent meets numerous definitions of malicious code

But, what is the definition of malicious? If we had a consistent, unambiguous definition then antivirus products may have an easier time deciding what to quarantine, without the need for signatures or complicated heuristics engines. Maybe an IRC bot is clearly in the definition we come up with, maybe it isn't. Maybe one ISP sees requests going to any other ISP's website as malicious.

### **Will, Intent, Results**

Is there a case to be made for some offensive actions within a security plan? Consider the use of the following methods:

- Replacing Image Files with “Warning” Messages When Phishing Sites are Detected
- Black Holing DNS Lookups for Suspect Domains
- Real-time Block Lists (RBLs)
- Advertisement Filtering

Each of these (and related families of measures) has been employed with good intentions to effectively stop a number of potential exploits. However, they can also be classified as offensive measures, in each case the argument can be made that the effect of the tactic is to take action against someone or some organization that did not attack (or intend to attack) the initiator. In addition, the impact of the “security” measure will be to make non-standards-based changes to the way many legitimate users' machines work – without the users' consent.

If these tactics are accepted, would it be alright to use XSS, SQL Injection, or

other means to root a phishing site (with the intention of both taking down the site and identifying affected users, of course)? How about flooding a phishing site with junk data? Phishing sites are often virtual machines residing next to legitimate, lawful websites – meaning an attack on a single IP address or website may harm others that did nothing wrong. Not to mention the reaction many would have when the MPAA begins a “stolen data reclamation” program...

How about using RBLs, DNS black holes, and routing black holes to prevent infections? There is no reason that one cannot do whatever they want to their own systems, except that violating the “rules of the road” may not be in the best interest of the Internet community. If each network (to include giant networks such as those managed by ISPs) begins implementing its own permutation of non-standard hacks to deal with malware attacks, how will event correlation ever be trusted? Complex layers of uniquely configured devices will certainly not improve the trust network managers have in other groups’ logs and incident reports, nor will it improve the speed that is a critical element of successfully defeating most Internet crime. In the end, maybe we are simply asking how close we are to advocating physically cutting circuits and smashing servers when we promote a “good offense” as part of a healthy security plan.

Layers of non-standards-based, automated, complex offensive mechanisms will not offer true security to any organization. While it may offer short-term support to incident response teams, utilizing these means as part of a normal assurance program tangles the only methods we have to beat web-based

crime: reliability and verifiability. The accepted knowledge that the “Internet can simply not be trusted” underpins the cynicism of administrators that would reject this out of hand. Consider, however, that it is nimble reaction times, the ability to correlate events, and the dedication of watchdog groups (both professional law enforcement and volunteer organizations) that affect active elimination of illicit web entities.

If the medical marvel described in the opening paragraphs were possible, and the subject did have a bad reaction to the treatment, would we rely on the hope that someone would be able to figure it out based on logs? Do we truly have so much trust in the verifiability of our systems that automated, offensive actions can be trusted to improve Internet security?

## References

The Wired Blog provides a good rundown:

Ryan Singel, “ISP Seen Breaking Internet Protocol to Fight Zombie Computers – Updated.” Wired, “Threat Level,” 23 July 2007.

<http://blog.wired.com/27bstroke6/2007/07/isp-seen-breaki.html>.

Andrew Matthews’ report shows what entries were changed and the commands that are issued once a client connects to the Cox Communications server. “DNS Hijacking.”

<http://www.exstatica.net/hijacked/>

“Court stops anti-spam firm from blocking junk email”

Stefanie Olsen, 12 May 2004  
silicon.com.

<http://www.silicon.com/research/specialreports/thespamreport/0,39025001,39120619,00.htm>

Unfections. Infectionvectors.com.  
[http://www.infectionvectors.com/library/unfections\\_iv.pdf](http://www.infectionvectors.com/library/unfections_iv.pdf)

“E-Mail Marketers Sue Antispammers”  
Daniel Tynan, April 23, 2003 PCWorld.  
<http://www.pcworld.com/article/id,110400-page,1/article.html>

For more information on sound defense mechanisms for Internet-connected assets, please visit <http://www.infectionvectors.com>.