It's Time to End Information Anarchy

from:
https://web.archive.org/web/20011109045330if_/http://www.microsoft.com:80/technet/treeview/default.asp?url=/technet/columns/security/noarch.asp

By Scott Culp
October 2001
*Code Red. Lion. Sadmind. Ramen. Nimda.*In the past year, computer worms with these names have attacked computer networks around the world, causing billions of dollars of damage. They paralyzed computer networks, destroyed data, and in some cases left infected computers vulnerable to future attacks. The people who wrote them have been rightly condemned as criminals. But they needed help to devastate our networks. And we in the security community gave it to them.
Itís high time the security community stopped providing blueprints for building these weapons. And itís high time computer users insisted that the security community live up to its obligation to protect them. We can and should discuss security vulnerabilities, but we should be smart, prudent, and responsible in the way we do it.

Arming the enemy

First, letís state the obvious. All of these worms made use of security flaws in the systems they attacked, and if there hadnít been security vulnerabilities in Windows®, Linux, and Solaris, none of them could have been written. This is a true statement, but it doesnít bring us any closer to a solution. While the industry can and should deliver more secure products, itís unrealistic to expect that we

will ever achieve perfection. All non-trivial software contains bugs, and modern software systems are anything but trivial. Indeed, they are among the most complex things humanity has ever developed. Security vulnerabilities are here to stay.

If we canít eliminate all security vulnerabilities, then it becomes all the more critical that we handle them carefully and responsibly when theyíre found.Yet much of the security community handles them in a way that fairly guarantees their use, by following a practice thatís best described as *information anarchy*. This is the practice of deliberately publishing explicit, step-by-step instructions for exploiting security vulnerabilities, without regard for how the information may be used.

The relationship between information anarchy and the recent spate of worms is undeniable.Every one of these worms exploited vulnerabilities for which step-by-step exploit instructions had been widely published. But the evidence is more far conclusive than that. Not only do the worms exploit the same vulnerabilities, they do so using the same techniques as were publishedĖ in some cases even going so far as to use the same file names and identical exploit code. This is not a coincidence. Clearly, the publication of exploit details about the vulnerabilities contributed to their use as weapons.

Good Intentions Gone Awry

Supporters of information anarchy claim that publishing full details on exploiting vulnerabilities actually helps security, by giving system administrators information on how to protect their systems, demonstrating the need for them to take action, and bringing pressure on software vendors to address the vulnerabilities. These may be their intentions, but in practice information anarchy is antithetical to all three goals.

Providing a recipe for exploiting a vulnerability doesnít aid administrators in protecting their networks. In the vast majority of cases, the only way to protect against a security vulnerability is to apply a fix that changes the system behavior and eliminates the vulnerability; in other cases, systems can be protected through administrative procedures. But regardless of whether the remediation takes the form of a patch or a workaround, an administrator doesnít need to know how a vulnerability works in order to understand how to protect against it, any more than a person needs to know how to cause a headache in order to take an aspirin.

Likewise, if information anarchy is intended to spur usersinto defending their systems, the worms themselves conclusively show that it fails to do this. Long before the worms were built, vendors had delivered security patches that eliminated the vulnerabilities. In some cases, the fixes were availablein multiple forms Ė singleton patches, cumulative patches, service packs, and so forth Ė as much as a year in advance. Yet when these worms tore through the user community, it was clear that few people had applied these fixes.

Many people have faulted the patching process itself for the low uptake rate. Fair enough Ė we do need to make it easier for users to keep their systems secure, and Microsoft acknowledged this very point in a recent major security announcement. But if the current methods for protecting systems are ineffective, it makes it doubly important that we handle potentially destructive information with care.

Finally, information anarchy threatens to undo much of the progress made in recent years with regard to encouraging vendors to openly address security vulnerabilities. At the end of the day, a vendorís paramount responsibility is to its customers, not to a self-

described security community. If openly addressing vulnerabilities inevitably leads to those vulnerabilities being exploited, vendors will have no choice but to find other ways to protect their customers.

Responsible Handling is Key

This is not a call to stop discussing vulnerabilities. Instead, it is a call for security professionals to draw a line beyond which we recognize that we are simply putting other people at risk. By analogy, this isnít a call for people for give up freedom of speech; only that they stop yelling ďfireĒ in a crowded movie house.

Most of the security community already follows common-sense rules that ensure that security vulnerabilities are handled appropriately. When they find a security vulnerability, they inform the vendor and work with it while the patch is being developed.When the patch is complete, they publish information discussing what products are affected by the vulnerability, what the effect of the vulnerability is Ė that is, the type and extent of damage that an attacker could cause through it Ė and what users can do to protect their systems. This type of information protects users by giving them the information they need to decide whether to apply the fix, but it doesnít put them at risk.

Some security professionals go the extra mile and develop tools that assist users in diagnosing their systems and determining whether they are affected by a particular vulnerability. This too can be done responsibly. In many cases, itís possible to build a tool that performs non-destructive testing and can only be used by a legitimate system administrator. In other cases, the specifics of the vulnerability make it impossible to limit how the tool could be used Ė but in cases like these, a decent regard for the well-being of the user community

suggests that it would better to not build the tool than to release it and see it misused.

What You Can Do

Ending information anarchy will not end the threat of worms. Ethics and intelligence arenít a package deal, and some of the malicious people who write worms are quite smart. Even in the best of conditions, it will still be possible to write worms. But the state of affairs today allows even relative novices to build highly destructive malware. Itís simply indefensible for the security community to continue arming cybercriminals. We can at least raise the bar.

This issue is larger than just the security community. All computer users have a stake in this issue, and all of us can help ensure that vulnerabilities are handled responsibly. Companies can adopt corporate policies regarding how their IT departments will handle any security vulnerabilities they find. Customers who are considering hiring security consultants can ask them what their policies are regarding information anarchy, and make an informed buying decision based on the answer. And security professionals only need to exercise some self-restraint.

For its part, Microsoft will be working with other industry leaders over the course of the coming months, to build an industry-wide consensus on this issue. Weíll provide additional information as this effort moves forward, and will ask for our customersí support in encouraging its adoption. Itís time for the security community to get on the right side of this issue.

Scott Culp is the Manager of the Microsoft Security Response Center