

## Re: Cryptogram Comment

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-08/0761.html>

---

**From:** Tom St Denis ([tomstdenis\\_at\\_iahu.ca](mailto:tomstdenis_at_iahu.ca))

**Date:** 08/15/04

Date: Sun, 15 Aug 2004 12:42:36 GMT

Undisclosed wrote:

>> *I don't have a firewall. I have a NAT and I rely on it not to be an  
>> insecure POS [yes it has latest firmware...]  
>  
> probably a bad idea, if you're dealing with normal cheap NAT router  
> boxes...*

Actually not really. I run ssh as sshd, apache as apache and nothing else. So even if you did manage to "r00t" my only two servers you don't get access to my box anyways. The NAT is just a simple first line defense [e.g. keeps nmap/ping script kiddies away].

>> *Most of my family/friends either run Gentoo Linux or are smart enough not  
>> to  
>> bother me with Windows questions. So this is largely moot.  
>  
> that's good.  
>  
> it's not a moot question for me or 95% of other comp geeks on this  
> planet...*

Again so?

>> *Most of my friends with messed up XP installs either do it themselves  
>> [e.g. run every game/tool/keygen/etc they can find] or run pirated copies  
>> of  
>> tools which are usually beta/unpatched/etc. So I don't care if their  
>> machines are broken.  
>  
> the people who's boxes I fix usually buy all their software, and don't  
> even really know there are such things as "keygens".  
>  
> the worst thing they can be accused of is "clicking on everything".*

That's like saying that someone with a DUI conviction "the worst thing they can be accused of is 'driving while drunk'". Where did personal responsibility go?

## sci.crypt: Re: Cryptogram Comment

>> *So? They should take a hint and be more responsible for their computer.*  
>  
> *that's great to say, except it just doesn't happen, and the rest of us*  
> *have to deal with the aftermath.*

So Ford is to blame for drunk drivers?

>> *An unpatched Linux box can be just as*  
>> *dangerous. So do we hold Linus personally responsible for an unpatched*  
>> *2.2.0 box?*  
>  
> *every Linux distro I've ever dealt with made it very clear for a very*  
> *long time that security updates were required, gave clear notice of*  
> *vulnerabilities on their websites, and gave clear instructions on how to*  
> *get them.*

WinXP by default has automatic updates turned on. I think the most it requires of you is to click "ok" after they're downloaded.

And despite what you're leading too I've ssh'ed into [invited] quite a few outdated 2.4 boxes just in the last year or so.

> *I have not seen ANY instructions coming with the software or machine to*  
> *end users of home Windows machines to use Windows Update regularly or*  
> *manually install patches.*

It's in the start menu for crying out loud. That and at this stage of the game if you don't know about "updates" you shouldn't be running a computer. Just like if you don't know to tune up your car every year [or so] then you shouldn't be driving.

> *that's perfectly fine, as long as you then turn on auto-updates by*  
> *default and inform the user you are doing so, which MS didn't do until*  
> *XP SP2.*

Um it's in SP1 afaik and perhaps prior.

> *incidentally, Linux distros have been trying to remedy their security*  
> *problems for a lot longer than MS has.*  
>  
> *adding Execshield and SELinux to Fedora Core will make it significantly*  
> *harder to exploit.*  
>  
> *meanwhile MS reinvented Stackguard without reading the literature, and*  
> *ended up with a broken security system.*  
>  
> *and Linux and other open OS's make all patches FREE to redistribute.*

You totally missed the point. The known exploits that turn into things like code red and blaster are usually reported by MSFT themselves months before. Just nobody applies the patches.

Re: Cryptogram Comment

sci.crypt: Re: Cryptogram Comment

Now I'm not saying MSFT writes quality software. I'm just saying if people took a two-fold improvement to computer usage [e.g. don't use IE and do update patches] that 99% of these "attacks" would disappear.

Specifically that it's \*unmaintained\* boxes that are getting attacked.

>>>*there are botnets of infected Windows machines that are up to 100,000 machines in size.*

>>

>>

>> *So?*

>

> *SO, they could shut down the Net.*

>

> *why does someone have this power? In large part, because MS software is egregiously sloppy.*

Again not disagreeing with their lack of quality software. These "botnets" only exist though because people are lazy. My parents for example run WinXP from "out of the box" [without reinstalling] for over a year now [24/7]. Their box isn't a "zombie". I wonder why that is....

>> *And how is any of this relevant to the idea that Windows should support unlicensed users.*

>

> *the idea is to drain the swamp.*

>

> *patched Windows boxes are harder to attack.*

>

> *that makes it harder to build 6-figure botnets.*

>

> *there are so many pirated machines, that, basically, to drain the swamp,*

> *you must also patch pirated machines.*

Yeah, because all licensed users update too. Providing the patch for unlicensed users won't fix the problem you're talking about. Because.... the VERY same people who didn't update before code red, blaster, welchia, etc... are the same people who won't update when SP2 is made available.

What you should be promoting is more computer literacy. People should know more about their computers so that they can maintain them [or be smart enough to know when they need fixing]. They should be liable for what their computers do as well.

But this is amerikan. Why take responsibility for your actions when you can just scapegoat MSFT. GOOOOOOOOO the downfall of SOCIETY!

>>>*the fact we have this state of affairs is manifestly and clearly*

>>>*Microsoft's fault.*

>>

>

sci.crypt: Re: Cryptogram Comment

>> *It clearly is not. Most if not all recent "outbreaks" are the result of  
>> a CLEARLY DOCUMENTED BUG with a FIX that people are just TOO LAZY too  
>> apply.*

>

> *dude, I don't know what planet you are on...*

>

> *but the average person has no clue they should even BE applying security  
> patches to their computer regularly.*

And that's their fault.

> *I certainly didn't before I got into security.*

Dude, I was updating various packages I ran [windows, djgpp, etc] when I was kid with my first [well my own] MII computer.

>> *This isn't a problem solely of Windows. I routinely rebuild and update  
>> software on my Gentoo box. Everything from new browsers to new support  
>> libs [like the recent libpng bug].*

>

> *same here.*

>

> *have you tried Gentoo Hardened? very cool.*

Not yet, though I can't swing the downtime. See I do \*work\* with my PC. I did manage the kernel update though. ;~)

>> *The problem with zombies is CLEARLY the end users who just don't maintain  
>> their boxes.*

>

> *if you sold a car to a guy from Outer Slobdovia who just got a driver's  
> license and never had even seen a car before that, then you*

> *intentionally do not tell a person they need to do regular maintenance*

> *even though you knew you should tell him...*

>

> *who's responsible?*

>

> *home users are the guy from Slobdovia.*

No home users are asshat amerikans who work all day frauding er... marketing crap we don't want, can't use and don't need all so they can take home pay, buy things from people who are also selling things we can't use, don't want and don't need.

Then they buy their PC XJ-74-2000-Super from Gateway or Dell, bring it home and hook it up to more bandwidth than the average university had during the late 80s. After that it's "timmy's gaming machine" and "little lisa's homework thingy".

So they have this box with usually over 3000MIPs and a decently fast net connection and let it run rampant. Sure timmy, you go waste GBs of

sci.crypt: Re: Cryptogram Comment

bandwidth pirating crappy RIAA audio. Oh, got a virus? Oh well, you still have 2700MIPS left. Just let it run!

In Canada [iirc] there are emission test requirements on cars. You can't just drive a car until it dies. It has to be safetied and it has to be reasonably clean. So your argument is largely moot. We \*already\* have regulations on cars.

Why is it so hard to say "you have a virus customer. Clean your computer or you're not getting net access". Like a simple system would be this.

The first time you're caught sending a virus [or spam] you're told "you have 72 hrs to clean up your box". So they disconnect [or throttle your net] for 72hrs and you have to clean it up. The second time you get caught you have to "safety" your computer [e.g. take it back to best buy for repair]. Make it law so that all ISPs have to follow it and you'll see some results.

But of course you can't do this... I mean it's totally fair for the few to waste the net experience for the rest. I mean it's right that I have a 25:1 spam/legit ratio on my email. It's totally ok that bandwidth is squander for piracy and other purposes.

>> *I don't pretend to support microsoft. I think their software is shit.*  
>> *That being said I run a Windows laptop which I've plugged into hostile*  
>> *networks before and I've never been infected with any crap that I see*  
>> *people at my college ROUTINELY get [like that damn blaster worm].*  
>  
> *that's great.*  
>  
> *now how would you feel if all the Owned boxes on the network started*  
> *DoSing you just to be nasty since they couldn't snag your machine?*

I'd say that's a normal day at the office. See our school uses Win2K for everything. It's a horrible server which often screws up DHCP. It's not uncommon to be disconnected from the net while there.

> *or better yet, how will you feel when those boxes are all sending out*  
> *the spam that floods our mailboxes?*

I don't get the questions? Sure I'd hate a DoS and spam. The question is who is supposed to fix this? MSFT sends the patches out, it's the school [and users who bring in their own HD/laptops] who don't apply them. They're the ones who don't use firewalls, etc...

>> *You can make a windows box relatively safe. Just the users are too lazy*  
>> *to*  
>> *do so. It's just so easy to buy a Dell and never update it for the 7*  
>> *years you'll run it....*  
>  
> *Dell, until recently, never even told customers to regularly update when*  
> *they got their machines.*

sci.crypt: Re: Cryptogram Comment

I'm sure Ford doesn't advertise "The new F-150 the truck you have to maintain every year!" It's kinda implied that things need repair from time to time.

>> *Free patches to his customers. Why would Bruce offer patches to people*  
>> *who pirate his software?*  
>>  
>  
> *I don't know, maybe he actually cares about Internet security and shit?*

Or he says that because he's a mouth piece trying to drum up business?

<snip blah>

This is all "same ol same ol" tiring.

The simple facts are

- Microsoft sucks bad.
- It's your fault for using their software
- You're responsible for your own computer [hey windows insecure? switch oses]

Tom