

Re: Cryptogram Comment

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-08/0759.html>

From: Undisclosed (*nomail_at_dontbeaweaselspammer.com*)

Date: 08/15/04

Date: Sun, 15 Aug 2004 04:11:14 -0400

Tom St Denis wrote:

> *Undisclosed wrote:*

>

>> *Tom, do you bother to read your firewall or IDS logs?*

>

>

> *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...

definitely better than nothing though.

some NAT routers like Linksys can log remotely to a syslog daemon, might want to try messing with that sometime if you keep a box inside the network up all the time.

> *So?*

>

>

>> *have you ever had to disinfect or maybe even reinstall M\$ software for family and relatives that were in all likelihood infected from other Owned machines? Or had to go through setting up basic security for their machines?*

>

>

> *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...

> *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.*

sci.crypt: Re: Cryptogram Comment

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".

>
> *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.

>
>>*unpatched Owned Windows machines are a huge threat to everyone on the*
>>*Internet, if for DoS possibilities alone.*
>
>
> *"So? And this is microsofts fault?"*

YES.

> *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.

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.

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.

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.

>>*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.

>>*someone having a botnet of 10,000 machines is not even out of the ordinary.*

>
>
> *So?*

>
>

>
> *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.

>
>>*the fact we have this state of affairs is manifestly and clearly Microsoft's fault.*

>
> *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.

I certainly didn't before I got into security.

> *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.

sci.crypt: Re: Cryptogram Comment

screw worrying about bugs in individual pieces of software, block entire classes of bugs! (patch too, though, just in case)

have a non-PaXed kernel to boot into for fiddling with assembler though.

btw, thank you for making your libs in C with ASM optional... PaX kills all ASM.

> *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.

>

> *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?

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

> *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.

>

> *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?

I would be happy to put out a patch for everyone from something of mine if it blocked some skiddie from getting a jump off point to attack some old lady in Wichita.

Re: Cryptogram Comment

sci.crypt: Re: Cryptogram Comment

and Bruce is smart – he's not selling software, Counterpane is selling services.

software can be endlessly pirated, but people's time and expertise can't, barring a gun to the head.

>
>
> *I don't see why. It makes perfect sense. Should Ford now do warranty fixes
> on stolen cars/trucks? Should a landlord do repairs to rooms people squat
> in? etc...*

if Ford designed vehicles that could be manipulated to spray flaming gasoline and gasket steam over passersby and intentionally ignored the possibility of removing or putting any security into controlling access to these features or trucks because "security is passe", I would say that Ford should **GODDAMNED WELL FIX THE FUCKING TRUCKS!**

software companies have finagled their way into being almost completely legally immune from liability lawsuits.

Ford would be out of business if they tried what I just described, which is MS's behavior.

>
> *Clearly not. I mean an unmaintained ford truck could be deadly. So by your
> logic Ford should repair it for the "good of mankind". Except we don't
> live in fantasy "everyone is nice" world. Support costs money.*

MS already gets plenty of money from legit users, so they are going to create it anyway.

after that, distribution costs can be reduced to effectively zero.

>
>>*I absolutely agree that MS has no legal requirement to make the patches
>>available.*
>
>
> *What are you talking about? I think MS is legally obliged to make the
> patches available. I just think that means to PAYING CUSTOMERS.*

that's what I meant.

>>*MS has \$50 billion in the bank and a license to print money with the
>>Windows and Office monopolies.*
>>
>>*this is not going to hurt them financially in the slightest.*

> *It sets a dangerous precedent if people are forced to support people who
> wrong them though.*

sci.crypt: Re: Cryptogram Comment

nobody is forcing MS to do anything.

legally, they would be completely within their right to not do it.

they'll just look like bigger assholes than usual for helping to contribute to the present insecurity situation.

> *BTW what's with replying with such a huge delay?*

>

> *Tom*

I just started reading sci.crypt again for the first time in 4 years.