

Re: Microsoft Says Recovery from Malware Becoming Impossible

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2006-04/msg00489.html>

- *From:* Imhotep <imhotep@xxxxxxxxxx>
 - *Date:* Mon, 24 Apr 2006 21:05:00 -0400
-

Roger Abell [MVP] wrote:

"Imhotep" <imhotep@xxxxxxxxxx> wrote in message
news:keydnc9nII1SPdfZRVn-jA@xxxxxxxxxxxxxxxx

Roger Abell [MVP] wrote:

"Imhotep" <imhotep@xxxxxxxxxx> wrote in message
news:vJ-dnOpNaahB59TZnZ2dnUVZ_tGdnZ2d@xxxxxxxxxxxxxxxx

Michael D. Ober wrote:

The only OS that this warning doesn't appear to apply to is OpenVMS. Linux (and by extension, Mac OS-X) and Unix are also subject to this same problem.

Mike.

"Imhotep"
<imhotep@xxxxxxxxxx>
wrote in message
news:R5idnZNIU5BZ-NXZnZ2dneKdnZydnZ2d@xxxxxxxxxxxxxxxx

"LAKE
BUENA
VISTA,
Fla.-In a
rare

Re: Microsoft Says Recovery from Malware Becoming Impossible

discussion
about the
severity of
the
Windows
malware
scourge, a
Microsoft
security
official said
businesses
should
consider
investing in
an
automated
process to
wipe
hard drives
and
reinstall
operating
systems as a
practical
way to
recover
from
malware
infestation."

"When you
are dealing
with
rootkits and
some
advanced
spyware
programs,

the

only
solution is
to rebuild
from
scratch. In
some cases,
there really
is

no

Re: Microsoft Says Recovery from Malware Becoming Impossible

way to
recover
without
nuking the
systems
from orbit,"
Mike
Danseglio,
program
manager in
the Security
Solutions
group at
Microsoft,
said in a
presentation
at the
InfoSec
World
conference
here."

<http://www.eweek.com/article2/0,1895,1945808,00.asp>

Imhotep

What kind of 'stuff' are you smoking???? Do
you have any idea how
stupid you
sound?

I have been using Linux for 10 years, never
caught anything. If I had a
dollar everytime I caught something on
Windows I could retire very
wealthy.
The truth is that malware is 99.9 % a
Windows problem. So stop lying
about it!

Imhotep

I would suggest that that is in fact an assessment of skill.
I have (iniitally, had to) run Windows versions for a dozen
years now,
starting with NT 3.50, and have not caught anything.
I will admit that in the dozen or so years before that when I
ran

Re: Microsoft Says Recovery from Malware Becoming Impossible

*nix brands exclusively it was much easier to not "catch" anything, but that was partly the threat level and partly the simplicity of the user authorization model.

Roger

User authorization model weak? Not at all. I run a linux "domain" where the back end authentication and authorization system is LDAP. It is very strong and allows very granular configurations. For all you non technicians reading this AD IS LDAP! Roger, I think you are little out-of-the-times with regards to the linux World, but that is ok.

With regards to crapware the FACT remains it is a Windows problem!!! I too have been using Windows going back to DOS 2.(something) and Unix since college and have never, let me repeat that, never had a problem with it.

The reason you have the crapware situation is:

- 1) Microsoft illegally dominates the PC World, why should THEY spend money improving the software when people are stupid enough to ask for more everytime they are spanked using it?
- 2) They make money by forcing you to upgrade because the latest version of MS has "highly improved security enhancements". (hahaha)
- 3) Within Microsoft the Marketing has more authority then the Engineering department.
- 4) Microsoft believes in the time proved lie of "security by obscurity". MS often takes a known standard and alters it so it does not work well with anything but MS products. This has been shown to be a fatal flaw. When strategic marketing over rides time proven technology standards you are in for a lot of bugs, security holes and problems. But, hey, it does help their marketing strategy!
- 5) Recently, in an article I posted, you saw Microsoft basically say, crapware is out of control and you (the customer) need to *BUY* software that rebuilds your PC frequently. Think about that statement for a minute. That would be like if you bought a defective car and the manufacture said "You need to just go out an replace the engine very 5k miles". You can bet that if a manufacturer said that to me, I would never buy a car from that manufacturer again. But, again, people are stupid. The more MS spanks them the more they want....it is funny in a way.

Re: Microsoft Says Recovery from Malware Becoming Impossible

If you are up to the challenge, let do this. Why don't you get a list of all the spyware, adware and general crapware that can infect Linux and I will get a corresponding list for Windows. Then we can draw our own conclusions about the percentages? Up for the challenge?

Imhotep

I am not sure how you got me into this reply Imhotep . . .

....oh just a friendly debate...

I said nothing about size of per-OS crapware lists.

...good, you did not take that bet. That bet is a suckers bet. Everyone knows that crapware is a MS problem. For every 1 non windows system crapware, I could list 5,000 Windows only crapware...with ease.

You are probably correct on my time having come to check out whether a rich authorization model can now be accomplished in the *nix environments with their addon Ldap variants.

Ok, first where did Kerberos come from? Hummmm, how about MIT. And what OS has it run on for 15 years or more? Hummm, UNIX!!!! Feel free to verify that fact...

Second, let's look at Microsoft authentication since we have a sticking point here. What authentication was NT Authentication base solely on? Hummmm, RADIUS! That is right neither NT Authentication nor Kerberos were invented by Microsoft, they were "borrowed"! But hey, at least Microsoft has not tried to patent it yet, like IM smiles and mice "double clicks"...

Third, UNIX has a richer authentication scheme than Windows has ever had...face it if you dare or ignore it if you can stand the truth, but, a fact is a fact...

Most of what you have said shows an all too common flaw. Use of "Microsoft = it" and "Microsoft = they" as in Microsoft does this because, or as in Microsoft wants such It is as if you are actually speaking about some entity that acts with one mind.

The actions of a company must be treated as such. Since I do not, nor can I,

Re: Microsoft Says Recovery from Malware Becoming Impossible

Re: Microsoft Says Recovery from Malware Becoming Impossible

Speak about the internals of the company. All I can comment about is the final actions of it (Microsoft)...

There are two points with which I can mostly agree in what was said. That the antivirus, antispam, antimalware industries exist in a sense an indictment of past decisions about Windows, which same I have stated to "Microsoft"; and also your item 3 which was definitely too true in the past (for me the jury is still out on current situation). I find it a fundamental flaw to judge one's child today based on what they were and did 5 years ago.

When someone is on trial, is their past actions not valid in presenting a pattern? If it works in a court of law, then it is just here...

In the same vein, continuing to berate the MS of today based on the actions of the MS that was just discovering that there was a network is not useful except for making maleficent verbage. Just as failing to recognize that people change, this fails to recognize that the people and the processes and objectives have changed.

I am sorry but I have not seen a change. I have seen things get worse, and worse, and worse. You speak of "cutting them a break for their past indiscretions. However, their current indiscretions are worse than their past indiscretions!!!!!!!!!!!!!!

Moving on, "MS" (today) does not believe in security by obscurity, although "they" can see what value exists in layered security and (non-security) layers that slow up / make difficult.

You say MS takes standards and alters them so they do not interop, but I do not see this. Instead I see a long history, stretching back to the point where MS began its long dev effort on NT5, where MS is working on the IETF working groups, submitting RFC and having representation on the task forces (like most other major vendors). I assume you are thinking of the Kerberos implementation, or of the choice of using in DNS names;

If you are referring to Dynamic DNS the character " " is valid for DDNS zone names. However, in DNS names (ie DNS name resolutions not DDNS zone names) the " " is illegal. You can still call you MS machine with a " " and thus causing Mail problems if it is a Mail gateway...that is a flaw going back 15 years!!!!!!!!!!!!!!

On Kerberos, they did alter the **real** kerberos algorithm. Thus making UNIX

Re: Microsoft Says Recovery from Malware Becoming Impossible

Kerberos (the original and thus copied by MS) inoperable with the watered down kerberos offered by Microsoft....

as certainly you cannot be thinging
of the MS efforts to get a standard model in the browser and to get
a standard was to do client-side scripting

Server side scripting has been around for sometime. Certainly before MS ever thought about it. But that aside, MS has never tried to standardize on browser protocols. If you remember, let's go back now (I am showing my age). Netscape was killing IE. Then MS started adding non standard elements to IE and thus forcing people to use IE...Even today, in the current situation of browser interoperability, is a leftover from these days...

just as you cannot be
thinging of the RTF and now XML based ways for data sharing
that are built into the ways the Office products can persist/read.

And who actually invented XML??? I will give you a hint it was NOT Microsoft, although they tried to patent it like other technologies that they "borrow" ...

In point of fact, MS only used was was already in the RFC for Kerberos and DNS, but they got a lot of negetive because they did not do things as others had – even though fully RFC compliant.

Untrue. Kerberos specifies that you must receive a "ticket" per resource, thus minimizing the window a hacker/sniffer has to decode it. Microsoft watered the protocol down by giving the user a "ticket" per logged in session....

What I also see is a lot of denial about this. I remember an eZine blast once, when use of XML and SLT etc. started to go mainstream, about how MS was being copy-cat, again jumping on board late to the party, etc.. Somehow that author managed to overlook MS deep involvement in bringing XML use into the mainstream, and its deep investment and support of XML reaching back to 1997.

"Deep involvement" with XML. Oh come on!!!! XML was worked on by many of thousands of OPEN SOURCE DEVELOPERS, in fact a good 90%.

On XSLT, I will cut you a break as you are correct. Microsoft was working on a committee with many other companies for XSLT. Then left and developed an

Re: Microsoft Says Recovery from Malware Becoming Impossible

incompatible protocol called xml-rpc...

But eZine is correct Microsoft, generally speaking, has been playing catch-up for sometime...

Similarly

with current efforts to continue WS* and interoperable identity solutions – there will be people able to overlook the intellectual property contributions made by MS, perhaps not even seeing that they are misinterpreting the facts of history.

I really think that the history is against you on that claim about not being a player in the standards orgs and in use of standards.

Intellectual property??? Let's review what I said before in the contexts for Intellectual property:

Kerberos: Developed by MIT and running on UNIX for 15+ years -- taken by Microsoft

Windows NT Authentication: Taken from RADIUS.

XML: Developed by OPEN SOURCE PROGRAMMERS! Taken by Microsoft

XML-RPC: Developed partially by MS but also by many others (from the XSLT work)

....should I go on....

And, speaking of moving on, XP will have been the common desktop and have an age of 6 years when its successor releases. If engine technology were advancing as fast as software, I would probably want to replace the engine in my car by then (heck, I have been wishing they had introduced serious hybrids a couple years earlier when I was at buy-time).

Come on Roger! You know exactly the point I was making. The point was:

"That would be like if you bought a defective car and the manufacturer said 'You need to just go out and replace the engine every 5k miles'. You can bet that if a manufacturer said that to me, I would never buy a car from that manufacturer again. But, again, people are stupid. The more MS spansks them the more they want....it is funny in a way."

The fact was, rebuilding your machine, as suggested by Microsoft in a recent article I posted, every 3 months or so because crapware has infested it, is lame and pathetic. Especially, when you factor in that it is Microsoft's

Re: Microsoft Says Recovery from Malware Becoming Impossible

Re: Microsoft Says Recovery from Malware Becoming Impossible

fault for not being able to fix their own software!!!. Why should the average user have to suffer because Microsoft is incapable of writing quality safe software???? Isn't it pathetic that they are trying to pass the buck due to their own incompetence?

In the case of XP's replacement with Vista, as with the replacement of Win9x, or NT 4, etc. there is nothing forcing upgrading, and the rather liberal support length in the product life-cycle is why we have so many of the old, and never supportable DOS variant OSs still in use today.

Come on Roger! That is totally a subjective statement!

You have it wrong if you think the OS side of the MS business is a cash cow. If it were not for the density of systems in the consumer base and for the use in-house for MS internet business efforts, the OS development and life-cycle support would probably not happen, certainly not with the present investment levels.

Their cash cow is their Office line. Which is why they are fighting Massachusetts and the Open Document Standard. If you have an open standard for documents how could Microsoft justify 400 dollars for MS Office??? I would talk about this for a while, but I will let you off the hook for today...

Imhotep

.