

Re: Microsoft Says Recovery from Malware Becoming Impossible

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2006-04/msg00498.html>

- *From:* "Roger Abell [MVP]" <mvpNoSpam@xxxxxxx>
 - *Date:* Mon, 24 Apr 2006 22:44:54 -0700
-

"Imhotep" <imhotep@xxxxxxxxxx> wrote in message
news:XYKdnV0Pjooi6NDZ4p2dnA@xxxxxxxxxxxxxxxx

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

Re: Microsoft Says Recovery from Malware Becoming Impossible

same
problem.

Mike.

"Imhotep"
<imhotep@xxxxxxxx>

wrote in
message

news:R5idnZNIU5BZ-NXZnZ2dneKdnZydnZ2d@xxxxxxxxxxxxxxxx

"LAKE
BUENA
VISTA,
Fla.—In
a
rare
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

Re: Microsoft Says Recovery from Malware Becoming Impossible

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

way
to
recover
without
nuking
the
systems
from
orbit,"
Mike
Danseglio,
program
manager
in
the

Re: Microsoft Says Recovery from Malware Becoming Impossible

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

Re: Microsoft Says Recovery from Malware Becoming Impossible

before that when I ran
*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
technies
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".

Re: Microsoft Says Recovery from Malware Becoming Impossible

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 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.

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.

Re: Microsoft Says Recovery from Malware Becoming Impossible

..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...

And what difference does not make that Project Athena originated what became an industry standard ???

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"...

You sound so silly.
You bark if MS uses a standard and you bark if they don't.

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...

balony

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.

Re: Microsoft Says Recovery from Malware Becoming Impossible

The actions of a company must be treated as such. Since I do not, nor can I, speak about the internals of the company. All I can comment about is the final actions of it (Microsoft)...

and, often quite out of date

There are two points with which I can mostly agree in what was said. That the antivirus, antispam, antimalware industries exist is 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...

glad I am not your child

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!!!!!!!!!!!!!!

You should lift you head above the water occassionally for some air.

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.

Re: Microsoft Says Recovery from Malware Becoming Impossible

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!!!!!!!!!!!!!!

If a flaw it is just more in the exceeding long, uncured history of sendmail issues.

Otherwise, your comments is Wrong. Wrong. And Wrong. Zones are zones. Updates can be dynamic, or not, or both.

Anyway this about "_" has nothing directly related to use the Update messages (your so-call DDNS) except that, like SRV records, MS became the first vendor to cause widely spread use of Update messages.

You need to read RFC 2181 (standards track, 1997) specifically the second paragraph under heading number 11.

<quote>

The DNS itself places only one restriction on the particular labels that can be used to identify resource records. That one restriction relates to the length of the label and the full name.

... .

Similarly, any binary string can serve as the value of any record that includes a domain name as some or all of its value

... .

Implementations of the DNS protocols must not place any restrictions on the labels that can be used. In particular, DNS servers must not refuse to serve a zone because it contains labels that might not be acceptable to some DNS client programs.

</quote>

The fact that the existing community did not like the entirely valid use of "_" does not make it wrong.

However, as with many other things, myths of MS misbehavior die hard amongst some.

Re: Microsoft Says Recovery from Malware Becoming Impossible

On Kerberos, they did alter the *real* kerberos algorithm. Thus making UNIX Kerberos (the original and thus copied by MS) inoperable with the watered down kerberos offered by Microsoft....

more baloney.

The definitions clearly allow for the implementation specific use of the field that caused the so-called inoperability. MS did nothing other than what DEC did, use the field in the manner defined when they built out DCE use of it.

as certainly you cannot be thinking 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

Someone was speaking of server-side ?? scripting?

The doc object model is used in the browser.

Scripting was coming into wide use for dynamic browser behavior and Netscape was taking things into a proprietary (JSS if I recall correctly) direction, while MS with the W3 evolved and defined what we have now.

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

do you have a distorted memory of events.

IE barely existed. Netscape dominated.

The existing DOM is largely from contributions of many participants, with Microsoft being very active. IE 4 was the first browser to fully implement the standard that was adopted (in fact, except for one tag that was renamed, it fully implemented the standard before it became the standard), while at the time one had to use JSS and other kludges in Netscape to get the same clientside functionality.

to IE and thus forcing people to use IE...Even today, in the current situation of browser interoperability, is a leftover from these days...

Re: Microsoft Says Recovery from Malware Becoming Impossible

just as you cannot be
thinking 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"...

Dude.

What part of standards do you fail to understand???

What part of the intent of them being in the public domain

do you not catch on to ???

In point of fact, MS only used what was already in the RFC for
Kerberos and DNS, but they got a lot of negative 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....

You really do not understand either Kerberos, Windows use of
Kerberos, or as it sounds more likely both.

The TGT is not the service ticket.

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%.

I recall going to something call Web TechEd in 1997 out in Palm Springs.
XML was one of the big MS messages at that time – "line up, this will
drive into the product line", etc. And, they were working along with the
others in the community to make it happen.

Re: Microsoft Says Recovery from Malware Becoming Impossible

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 incompatible protocol called xml-rpc...

correct as I have been in many of the other statements in my post which you have a private view/history about
You as too many in the world amazingly do not see how much intellectual property, time and resources, human talent, etc. has been contributed in raising the technical level of many aspects of the industry.
It is truly amazing the blindness that abounds.

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

on XML that is a blind statement, IOW, it is bull

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 an 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....

Why, repetition is death, especially when false

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:

Your words where to effect that the MS engine is driven by some mythical mind that only wants more sales on a set calander basis

"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."

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 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?

This extremist crude has been dispensed elsewhere.

The rebuild recommendation is just a statement of the reality that most people are not able to recognize whether a machine is or is not clean, and those people are exactly the ones likely to have not run the system in a manner that kept it from becoming infested.

Again – I and many I know have run single builds for many many years with no issues. It is really not so much the OS as it is the user and their usages. If you look you might even see that W2k3 has fewer

Re: Microsoft Says Recovery from Malware Becoming Impossible

critical patches (not IE now) than say sendmail (guess at one likely candidate) in the same set of years.

Did you realize that IIS 6, apparently the currently most widely used webserver, has not had one single critical security patch since released? and the IIS 5 has not had one since the last patch rollup which was somewhere around 2001 ?

No, I guess you did not know . . .

Again, why would I want to be using 5 or 10 year old technology?

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!

Actually it is quite objective. And true.
Is that the best you can do ??

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, there is when all is said and done one place (at the least) where we are roughly in agreement – life would have been better if IE had not taken the road it has travelled. MS software (as if that is A thing, gets a bad rap due to experiences people have had, most probably due to the presence of IE on their machines, and yet they associate and extrapolate the "issue" as an ill in other MS software, like the OS. Of course, MS saying that, making them that, they are

Re: Microsoft Says Recovery from Malware Becoming Impossible

inseparable does not help people see a trigger as a trigger but only
an arsenal as an arsenal.

I tire of this . . .

—

ra

.