

Re: After i go to this Web Sit i have many virus he instal he want without permission ! its very Dangerous ! Plz Help

Source:

<http://www.tech-archive.net/Archive/Scripting/microsoft.public.scripting.virus.discussion/2004-04/0193.html>

From: Bill Sanderson (*Bill_Sanderson_at_msn.com.plugh.org*)

Date: 04/15/04

Date: Thu, 15 Apr 2004 00:32:24 -0400

I guess I'd say that the log excerpt makes it sound like the issue is at the server end.

There's a Microsoft.public.windowsupdate where they might know for sure, but they are also probably really swamped!

That's interesting about the existence of the folder—not sure what it means—we'd all hope that the attributes of the patches—removability or not—are the same regardless of the delivery method, and I think they are.

I still don't understand why download would fail for particular patches over that length of time and # of tries—but there may be more to the errors that I can guess.

I did notice that patching via Shavlik's HFNETCHK was duck soup compared to trying to pull directly from WindowsUpdate.

I believe Shavlik pulls the patches from their own servers—not absolutely certain.

This brings up an issue I'd not thought much about—if you are intending to provide free patches and free downloading of them, you'd better be darn sure that the infrastructure is up to snuff, or you'll have entrepreneurial folks out there providing your patches at premium rates, but with guaranteed ease of access—shades of the \$19.95 scammers.

"Phil Weldon" <notdisclosed@example.com> wrote in message news:Ljnfcl.10681\$K05.1418@newsread2.news.pas.earthlink.net...

- > *Yes, the successful install came through Auto Update; the alert was*
- > *to*
- > *tell me Auto Update was at work. The updates took a reasonable amount*
- > *of time (via ADSL ~ 1 Mbit/sec limit), it's just that three of five*
- > *gave*

Re: After i go to this Web Sit i have many virus he instal he want without permission ! its very Dangerous ! P

lic.scripting.virus.discussion: Re: After i go to this Web Sit i have many virus he instal he want without permission ! its very

> the message " X did not install."
>
> The only difference I see in the aftermath is that
> \$NtUninstallkBxxxxx\$ folders exist for the successful patches via Auto
> Update, but not for the two that were successful via the "Windows
> Update"
> button on the 13th of April.
>
> For what it is worth, below is the end of the log file for one
> attempt
> to install KB828741 on April 13th, 2004. It would have been nice if a
> bit of the information in the log file had been used in the "X did not
> instal" message.
>
> EXCERPT BEGINS_____

>
> HttpSendRequest unsuccessful (12029)
> ***
>
> Failed DownloadAndPatchFiles, GLE=0x00002EFD
>
> ***
>
> Max download retries exceeded, GLE=0x00002EFD
>
> ***
>
> DoInstallation:DownloadPatchFiles failed
> ***
>
> VerifySize: Unable to verify size: Source = NULL: c:\windows\oem10.cat
>
> ***
>
> KB828741 installation did not complete.
> ***
>
> Update.exe extended error code = 0x2efd
> ***
> EXCERPT ENDS_____

>
> --
> Phil Weldon, pweldonatmindjumpdotcom
> For communication,
> replace "at" with the 'at sign'
> replace "mindjump" with "mindspring."
> replace "dot" with "."
>
> "Bill Sanderson" <Bill_Sanderson@msn.com.plugh.org> wrote in message
> news:uS3AvLpIEHA.3556@TK2MSFTNGP10.phx.gbl...
>> I patched a couple of dozen machines last night, and only saw one failure

Re: After i go to this Web Sit i have many virus he instal he want without permission ! its very Dang@rous ! P

lic.scripting.virus.discussion: Re: After i go to this Web Sit i have many virus he instal he want without permission ! its very

>> *that resembled your report--on one machine, all 5 patches failed (this
>> was
>> XP, not Windows 2000.) I figured I'd hit some button wrong by
>> mistake--WindowsUpdate was very slow and balky, and I was cycling between
>> 3-6 machines at a time via Remote Desktop.
>>
>> So--I just redid the process at that machine and it went through just
> fine.
>>
>> So you tried numerous times, over the course of parts of two days, and
>> got
>> the same failure pattern, but eventually, it resolved and the two "bad"
>> ones installed?
>>
>> Wierd--I'm having some trouble imagining a mechanism that'd give that
>> effect.
>>
>> Hmm - when you say "Today, I got an update alert" does that mean that
>> the
>> successful install came in via AutoUpdate, rather than via WindowsUpdate?
>>
>> I don't know enough about how the two different update mechanisms work to
>> comment intelligently about why this might happen.
>>
>> "Phil Weldon" <notdisclosed@example.com> wrote in message
>> news:kqjfc.9746\$k05.8895@newsread2.news.pas.earthlink.net...
>> > And Interesting Thing happened when I tried to apply the security
> patches
>> > released on 13APR04 to my notebook running Windows 2000. On the 13th I
>> > clicked on the 'Windows Update' button. The Windows Update began,
>> > and
>> > found five critical updates. I selected all five, but only two would
>> > install successfully:
>> > (KB837001 MS04-014), (KB828741 MS04-012), and (KB835732 MS04-011)
>> > would download, but not install. After four or five attempts,
> yesterday
>> > and today, all of which failed [the updater announced the failure,
> but
>> > gave no error codes nor explanation but to try the installation
>> > again.]
>> > Later today a got an update alert, and the three failing updates were
>> > successfully installed.
>> >
>> >
>> > --
>> > Phil Weldon, pweldonatmindjumpdotcom
>> > For communication,
>> > replace "at" with the 'at sign'
>> > replace "mindjump" with "mindspring."
>> > replace "dot" with "."
>> >*

Re: After i go to this Web Sit i have many virus he instal he want without permission ! its very Dang@rous ! P

lic.scripting.virus.discussion: Re: After i go to this Web Sit i have many virus he instal he want without permission ! its very

>>>
>>> *"Bill Sanderson" <Bill_Sanderson@msn.com.plugh.org> wrote in message*
>>> *news:ObSW4xjIEHA.2236@TK2MSFTNGP10.phx.gbl...*
>>>> *Exactly--and as Fraizer has said--that, which he applied after it was*
>>>> *available, should resolve his problem.*
>>>> *(and that of all the rest of us as well!)*
>>>>
>>>> *Hey folks--if everybody else is still reading along: There were a*
> *LARGE*
>>>> *number of remote code execution vulnerabilities patched in this*
> *go-round.*
>>>>
>>>> *This almost guarantees a lot of attempts to exploit these in the form*
> *of*
>>>> *worms in the not-too-distant future.*
>>>>
>>>> *Encourage all your friends and relations to get patched asap??*
>>>>
>>>> *"David H. Lipman" <DLipman~nospam~@Verizon.Net> wrote in message*
>>>> *news:eY9ADhcIEHA.3528@TK2MSFTNGP09.phx.gbl...*
>>>>> *4/13/2004 10:25:05 PM Deleted DLIPMAN-1\lipman*
>>>>> *D:\temp\IE6\Temporary*
>>>>> *Internet*
>>>>> *Files\Content.IE5\Z0WFDAGD\popupnew[1].htm Exploit-MhtRedir.gen*
>>>>>
>>>>>
>>>>> *Exploit-MhtRedir.gen*
>>>>>
>>>>> *http://vil.nai.com/vil/content/v_101170.htm - MS Vulnerabilities*
>>>>> *MS04-011 - 014*
>>>>>
>>>>> *Dave*
>>>>>
>>>>>
>>>>>
>>>>> *"Fraizer" <NOfraizerfrSPAM@yahoo.fr> wrote in message*
>>>>> *news:407c7030\$0\$20165\$636a15ce@news.free.fr...*
>>>>> *| hello all*
>>>>> *|*
>>>>> *|*
>>>>> *|*
>>>>> *| - After i go to this F***** Web site <http://www.appzplanet.com/> i*
>>> *have*
>>>> *this*
>>>>> *| Virus:*
>>>>> *|*
>>>>> *|*
>>>>> *| Under Kaspersky Anti-Virus 4.5.0.95 ->*
>>>>> *"TrojanDropper.Win32.Bridge"*
>>> *AND*
>>>>> *| Under The Cleaner Pro 4.1 build 4252 -> (ABetterInternet) Type:*

Re: After i go to this Web Sit i have many virus he instal he want without permission ! its very Dangerous ! P

lic.scripting.virus.discussion: Re: After i go to this Web Sit i have many virus he instal he want without permission ! its very

```
>>> Browser  
>>>> | Hijacker  
>>>>  
>>>  
> |
```

```
>>> --  
>>>>  
>>>  
> |
```

```
>>> --  
>>>> | --  
>>>> | C:\Program Files\Internet Explorer\setup.exe  
>>>> |  
>>>> |  
>>>> | Under Kaspersky Anti-Virus 4.5.0.95 -> "TrojanSpy.Win32.e" AND  
>>>> Under  
>>>> The  
>>>> | Cleaner Pro 4.1 build 4252 -> (ABetterInternet) Type: Browser  
>>>> Hijacker  
>>>>  
>>>  
> |
```

```
>>> --  
>>>>  
> |
```

```
>>>> | C:\WINDOWS\system32\*.exe (in file properties i have this  
> version  
>>>> :  
>>>> 1, 0,  
>>>> | 0, 1)  
>>>> |  
>>>> |  
>>>> |  
>>>> | Under Kaspersky Anti-Virus 4.5.0.95 ->  
>>>> "TrojanDownloader.Win32.Bridge"  
>>>> AND  
>>>> | Under The Cleaner Pro 4.1 build 4252 -> (ABetterInternet) Type:  
>>> Browser  
>>>> | Hijacker  
>>>>  
>>>  
> |
```

```
>>> --  
>>>>  
>>>
```

Re: After i go to this Web Sit i have many virus he instal he want without permission ! its very Dangerous ! P

lic.scripting.virus.discussion: Re: After i go to this Web Sit i have many virus he instal he want without permission ! its very

> /

>> > --

>> >> > / -----

>> >> > / C:\WINDOWS\system32\bridge.dll (in file proprieties i have this

>> > version

>> >> > :

>> >> > / 1, 0, 0, 116 and description : bridge Module)

>> >> > /

>> >> > /

>> >> > / After i erase all this files

>> >> > /

>> >> > /

>> >> > /

>> >> > / - And this web sit put me a file (ActiveX Controle) like this

>> >> > / {1000000000-1000-0000-1000-000000000000} in the Internet

>> >> > proprieties->

>> >> > / General -> Temoprary Internet Files After click on Config and

>> >> > click

>> >> > on

>> >> > / Display Object u have this window : C:\WINDOWS\Downloaded Program

>> > Files\

>> >> > and

>> >> > / u see this file (ActiveX) {1000000000-1000-0000-1000-000000000000}

>> > withe

>> >> > / other normals Files like : Update Class; Shockwave Flash Obkect;

>> > Office

>> >> > / Update Installation Engine... he execute this : file://C:\Program

>> >> > / Files\Internet Explorer\setup.exe

>> >> > /

>> >> > /

>> >> > / - And i see he install me a program (i see in Add/uninstall

> Programs)

>> >> > the

>> >> > / name : "Bridge" (Maybe he install me another think :()

>> >> > /

>> >> > /

>> >> > / - and he put me if i remeber (because i erase) a Rundll/bridge.dll

> or

>> >> > / somthink like this...

>> >> > /

>> >> > /

>> >> > / + After i erase all this files i do a Scan with Ad-aware 6.0 and i

>> > have

>> >> > this

>> >> > / log file : (i earase all)

>> >> > /

>> >> > / WINFAVORITES

>> >> > / -----

>> >> > / obj[0]=RegKey : Bridge.brdg

>> >> > / obj[1]=RegKey : Bridge.brdg.1

Re: After i go to this Web Sit i have many virus he instal he want without permission ! its very Dang6rous ! P

lic.scripting.virus.discussion: Re: After i go to this Web Sit i have many virus he instal he want without permission ! its very

>>> > / obj[2]=RegKey : CLSID\{9C691A33-7DDA-4C2F-BE4C-C176083F35CF}
>>> > / obj[3]=RegKey : TypeLib\{DDAF2479-6F00-4599-998A-3ED75686C6D0}
>>> > / obj[4]=RegKey : Interface\{4FDBDBAD-FEFE-4C4C-9CC1-1181052AFB12}
>>> > /
>>> > /
>>> > /
>>> > /
>>> > / PLEASE help me :((i format all my computer and install again and
>>> > i
>>> > have
>>> > the
>>> > / same problem)
>>> > /
>>> > / sorry if my english is poor. :(
>>> > /
>>> > /
>>> > /
>>> > / PS: When i go to this link : <http://www.appzplanet.com/> the first
>>> > time
>>> > he
>>> > / open a porno popup AND another window but this time He Ask Me if i
>>> > accept a
>>> > / certificat if i remeber but i dont klik on Yes or No i just closed
>>> > the
>>> > / window... and i see i have this problem i clean all like this and
>>> > after
>>> > i
>>> > / check my system because i dont undstand why.. i think its files
>>> > after
>>> > i
>>> > run
>>> > / it but no and now i try many think i go again in the web sit and I
>>> > Have
>>> > The
>>> > / Same Problems.. Now i Knwo But in the Seconde Time when i go i
>>> > have
>>> > little
>>> > / Difference ! -> He just open a porno popups But he Dont ask me for
>>> > the
>>> > / certificat... (if i closed the Certificat mean yes or what ???
>>> > what
>>> > i
>>> > do
>>> > to
>>> > / have again ask me for certificat ??). [I IDENTIFY THIS ITS FOR
>>> > SHOKWAVE
>>> > / PLAYER BECAUSE THIS F*** WEB SITE WANT THIS TO RUN A Bandau
>>> > / publicity...]
>>> > /
>>> > /

Re: After i go to this Web Sit i have many virus he instal he want without permission ! its very Dang@rous ! P

lic.scripting.virus.discussion: Re: After i go to this Web Sit i have many virus he instal he want without permission ! its very

>> >> > / *PS2: I dont know if for another web sit i have this same*
>> >> > *problems..*
> *i*
>> >> > *afraid*
>> >> > / *to go :(*
>> >> > /
>> >> > /
>> >> > / *PS3: when i tell you this : """"(Maybe he install me another think*
>> >> > *:()"""" i*
>> >> > / *found this in Add/uninstall Programs ""Internet Explorer Q832894""*
> *i*
>> >> > *dont*
>> >> > / *know if its official or not... but i go in windows update to chek*
> *if*
>> >> > *i*
>> >> > / *download this in my hitorical download and i see nothink when i*
>> >> > *search*
>> >> > *withe*
>> >> > / *this name "Q832894" in the window and i try to uninstall but he*
> *dont*
>> >> > *want he*
>> >> > / *tell "INF File Invalid" (in Add/uninstall Programs) (Note: i dont*
>> >> > *tell*
>> >> > *this*
>> >> > / *its not normal i just tell u all i see to help :()*
>> >> > /
>> >> > /
>> >> > / *PS4: when i right this msg i see 7 critycals updates (3.6 mo..) in*
>> >> > *windows*
>> >> > / *update since this morning to know :) 7 since 12 Hours... bused xp*
> *OS*
>> >> > *tsss...*
>> >> > /
>> >> > /
>> >> > / *PS5: !! --> i just try with another computer with Windows XP pro*
> *Too*
>> > *and*
>> >> > *i*
>> >> > / *have exactly the same problem !!!!!!! he install me the same files*
>> > *same*
>> >> > / *registery etc... !!! all same !!! its the Web sit this Fu****
> *(sorry)*
>> > *web*
>> >> > *sit*
>> >> > / *! He Ask You Nothink ! He install without confirmation ! u have*
> *juste*
>> > *to*
>> >> > *go*
>> >> > / *to the web sit and he do all without you now !*
>> >> > /
>> >> > /

Re: After i go to this Web Sit i have many virus he instal he want without permission ! its very Dang@rous ! P

lic.scripting.virus.discussion: Re: After i go to this Web Sit i have many virus he instal he want without permission ! its very

>> >> > /
>> >> > /
>> >> > /
>> >> > /
>> >> > /
>> >> >
>> >> >
>> >>
>> >>
>> >
>> >
>>
>>
>
>

Re: After i go to this Web Sit i have many virus he instal he want without permission ! its very Dang@rous ! P