

Re: Windows 2000 users accounts get locked out

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2004-05/1249.html>

From: Merrick (*anonymous_at_discussions.microsoft.com*)

Date: 05/24/04

Date: Sun, 23 May 2004 20:24:02 -0700

Hi Steve,

I really appreciated your patience and help. After weeks of trouble shooting, I think I am zooming down to the source. Yes, it looks like a trojan that came into my servers or our users PC.

I managed to stabilised the condition by cleaning each individual PC and it seems to be helping for now.

Will check out the links and will strengthen the protection as suggested. You have been a great help!

Will update you once i have managed to control the situation. !!

Regards

Merrick

>-----Original Message-----

>Hi Merrick.

>

>Typically that sounds like an outside the network attack from attackers that

>were able to enumerate your users via file and print sharing ports somewhere

>along the line. You say it does not happen when the users go home. If they

>shut down their machines either the machine causing the attack is shut down

>or the machine being attacked is shut down. One thing you might want to

>consider is the possibility a machine on your network has a backdoor into

>your network via a trojan or remote control software which may not be

>detected by virus scan software and would require a program dedicated to

>finding trojans such as those in the links below. I am surprised that you

>are not finding any Event ID 529 or 681 if auditng of failed logon events is

>enabled on all computers. You also may want to look into debug logging of
>netlogon as described a while back. Ideally you also want your perimeter
>firewall configured with a default block all outbound rule and then create
>exceptions for the authorized outbound traffic [53/80/443 and such] which can
>help prevent successful remote control attacks --- Steve
>
><http://swatit.org/download.html>
><http://www.pestpatrol.com/PestPatrolSBE/>
>
>"Merrick" <anonymous@discussions.microsoft.com> wrote in message
>news:10b6e01c44090\$88e31bf0\$a001280a@phx.gbl...
>> Hi Steve
>> Those machine names I mentioned are not in my network. I
>> have no idea why my users which are valid and the network
>> domain name which is also valid were locked out from funny
>> machine names! I have tried to capture 529 and 681 but my
>> eventcomb did not managed to find any of those errors.
>> As for my firewall, I have tried to scan them from outside
>> and my ports are blocked.
>> One thing for sure is when all my users are gone for the
>> day, no more locked out happen. But once they are back for
>> work, the locked out happens again. Apparently the locked
>> out issues were not someone trying to come in from beyond
>> my firewall.
>> I am still trying to figure out where the locked out
>> happen. Thanks for the help though!
>>
>> have a great weekend!
>>
>> >-----Original Message-----
>> >Hi Merrick.
>> >
>> >You say that those machines are on your network or not??
>> Can you ping those machines
>> >by their name and get a response? The caller machine is
>> the name of the machine that
>> >the user was attempting to logon from at the time of the

>> *lockout. If those computers*
>> *>are on your network, you need to find out why they are*
>> *trying to logon as your users,*
>> *>such as a virus infection. If they are not from your*
>> *network then how are they*
>> *>getting access? You said your firewall is configured*
>> *correctly? Is your firewall*
>> *>allowing any access from the internet such as a web*
site,
>> *vpn, or Terminal Services?*
>> *>The event ID displays what user is locked out and from*
>> *what machine but if you can*
>> *>find any failures for logons on any domain machine such*
>> *as 681 or 529, that would be*
>> *>helpful as it will help determine what domain computers*
>> *are being targeted for these*
>> *>failed logon attempts and then you could use a packet*
>> *sniffer such as Ethereal to*
>> *>monitor the traffic from the machine causing the*
lockout
>> *to possibly help determine*
>> *>what is going on.. --- Steve*
>> *>*
>> *>"Merrick" <anonymous@discussions.microsoft.com> wrote*
in
>> *message*
>> *>news:1021301c43f28\$407ea5a0\$a601280a@phx.gbl...*
>> *>> Hi Steve and serverguy*
>> *>>*
>> *>> Great help!*
>> *>> Yes i did a netdiag and seems ok but dcdiag generated*
>> *some*
>> *>> errors: one of which: "[warning] The DNS host*
name 'xxx'
>> *>> valid only on Windows 2000 DNS servers. [DNS_ERROR-*
NON-
>> *>> RFC_NAME], [WARNING] Cannot find a primary*
>> *authoriatative*
>> *>> DNS server for the name 'xxxx' may not be registered*
in
>> *>> DNS"*
>> *>> Managed to read up some issues and rerun dcdiag and*
>> *>> cleared all the erros. Still my accounts get locked*
out.
>> *>> The worst is my event log from eventcomp shows that*
my
>> *>> valid users are being locked out by all sorts of*
foreign
>> *>> manchine name, one of which is this:*
>> *>> 644,AUDIT SUCCESS,Security,Fri May 21 16:06:46*
2004,NT

microsoft.public.win2000.security: Re: Windows 2000 users accounts get locked out

>> >> *AUTHORITY\SYSTEM, User Account Locked Out: Target*
>> >> *Account Name: "valid user id" Target Account ID:*
>> %
>> >> *("numbers") Caller Machine Name: ANGEL Caller*
>> *User*
>> >> *Name: "my servername"\$*
>> >>
>> >> *The Caller Machine Name: Angel is a remote machine*
>> *name*
>> *in*
>> >> *my network. I have no idea what is that! A few others*
>> >> *Caller Machine Name are PROXYSRV, GNSERVER,*
>> *SERVIDOR ..??*
>> >> *what are those!?. Am trying to scan all my users for*
>> *virus*
>> >> *now.*
>> >>
>> >> *Thanks for helping !*
>> >> *Regards*
>> >> *Liew*
>> >>
>> >> >-----*Original Message*-----
>> >> >*Event ID 642 will be recorded with every Event ID*
>> *644 -*
>> >
>> >> *that is normal. If you want*
>> >> >*to modify password/lockout policy you have to do it*
>> *at*
>> >> *the domain level which would*
>> >> >*be "Domain Security Policy" in a default*
>> *installation -*
>> >> *it will NOT work if you do it*
>> >> >*in Domain Controller Security Policy.*
>> >> >
>> >> >*Have you found any failed logon event ID's on any*
>> *domain*
>> >> *computer? That is the place*
>> >> >*to start to track down the problem to see if you*
>> *have*
>> *an*
>> >> *infected machine or what.*
>> >> >*The error for ,***StartServiceW Failed!*** would*
>> *only*
>> *be*
>> >> *pertinent if you found that*
>> >> >*on a computer experiencing account lockouts AND the*
>> >> *lockout time corresponded to the*
>> >> >*time for that event in the alockout.dll log.*
>> >> >
>> >> >*Have you had a chance to run netdiag and dcdiag on*
>> *the*

Re: Windows 2000 users accounts get locked out

microsoft.public.win2000.security: Re: Windows 2000 users accounts get locked out

>> >> *domain controller and netdiag*
>> >> *>on a domain client? If so did the results look good*
or
>> >> *were there any reported*
>> >> *>problems? --- Steve*
>> >> >
>> >> >*"Merrick" <anonymous@discussions.microsoft.com>*
wrote
>> *in*
>> >> *message*
>> >> *>news:eed101c43d78\$7eb1fc20\$a401280a@phx.gbl...*
>> >> >> *Hi Steve,*
>> >> >> *You have been a great help! I really appreciated*
it.
>> *As*
>> >> *to*
>> >> >> *my problem:*
>> >> >> *1.) I have disabled my accounts lockout policy in*
my
>> >> >> *domain controller security policy but i still get*
>> >> >> *accounts*
>> >> >> *locked out, yes the administrator is always locked*
>> >> >> *out.*
>> >> >> *2.) I have included 644 and 642 in my eventcomb*
and
>> *for*
>> >> >> *every 644 i got one 642. MS provide very little*
>> >> >> *information on 642 and am still trying to gather*
>> >> >> *information on that. it seems like my secure*
channel
>> *is*
>> >> >> *leaking.*
>> >> >> *3.) I have also planted alockout.dll in one of my*
>> >> *clients*
>> >> >> *and one particular line is worrying me:*
>> >> *C:\WINNT\system32*
>> >> >> *\svchost, ***StartServiceW Failed!*** (0), Service:*
>> >> >> *Service: Background Intelligent Transfer Service*
>> >> >> *(C:\WINNT\System32\svchost.exe -k BITSgroup), RC*
was:
>> >> >> *Incorrect function. (1), GLE was: Overlapped I/O*
>> >> >> *operation is in progress. (997): Any comment?*
>> >> >>
>> >> >> *Hope you can help! Many Thanks in advance!*
>> >> >>
>> >> >>
>> >> >> >-----Original Message-----
>> >> >> >*Hi again Merrick.*
>> >> >> >
>> >> >> >*If you have not done such, set your account*
lockout

Re: Windows 2000 users accounts get locked out

>> >> >> *threshold for number of*
>> >> >> *>bad attempts to at least ten. You should be*
seeing
>> >> *failed*
>> >> >> *logon attempts*
>> >> >> *>such as Event ID 529 on some computers in the*
>> *domain.*
>> >> >> *These failed logons*
>> >> >> *>could be on any computer in the domain – not just*
>> >> *domain*
>> >> >> *controllers. Be*
>> >> >> *>sure you have auditing of "logon events" for*
failure
>> >> >> *which is different than*
>> >> >> *>account logon events enabled in Domain Security*
>> *Policy*
>> >> >> *and Domain Controller*
>> >> >> *>Security Policy. You may also need to configure*
it
>> *at*
>> >> *the*
>> >> >> *OU level if you*
>> >> >> *>are using Organizational Units with their own*
Group
>> >> >> *Policies that have*
>> >> >> *>auditing disabled. You can check the Local*
Security
>> >> >> *Policy of any domain*
>> >> >> *>computer and look at the "effective" settings for*
>> >> >> *auditing to see if it is*
>> >> >> *>enabled. Those failed logon events will give a*
lot
>> *of*
>> >> >> *helpful info on why*
>> >> >> *>the logons are failing and from what computers*
the
>> >> *logon*
>> >> >> *attempts are coming*
>> >> >> *>from.*
>> >> >> >
>> >> >> *>In addition I would run some diagnostics on the*
>> *domain*
>> >> >> *controller and then a*
>> >> >> *>couple domain computers. First run netdiag on the*
>> >> *domain*
>> >> >> *controller looking*
>> >> >> *>for any failed tests/errors/warnings*
particularly
>> >> >> *relating to dns, domain*
>> >> >> *>membership, and dclist. Then run dcdiag on the*
>> *domain*

microsoft.public.win2000.security: Re: Windows 2000 users accounts get locked out

>>>> *controller looking for*
>>>> *>failed tests again. After that do the same with*
>> *netdiag*
>>>> *on one of the domain*
>>>> *>members. On the domain controller and domain*
member
>>>> *run "*
>>>> *netdiag*
>>>> *>/test:ipsec " which will show if an ipsec policy*
is
>>>> *assigned that can cause*
>>>> *>problems in a domain. You can post results here*
in a
>>>> *reply if any problems*
>>>> *>are found. Those tools are found on the install*
>> *cdrom*
>>>> *in*
>>>> *the support/tools*
>>>> *>folder where you will need to run the setup*
>> *there. --*
>>>>
>>>> *Steve*
>>>>>
>>>>>
>>>>> *"Merrick" <anonymous@discussions.microsoft.com>*
>> *wrote*
>>>> *in*
>>>>> *message*
>>>>> *>news:e7fb01c43cb0\$4343bd40\$a001280a@phx.gbl...*
>>>>>> *Hi guys! thanks for the help. I have scan my*
>>>> *firewall as*
>>>>>> *suggested by Steven and all my ports are*
secured.
>> *I*
>>>> *have*
>>>>>> *also increase my password threashold to 10*
>> *minutes. I*
>>>>>> *have*
>>>>>> *> patched all my software for my servers and*
users.
>>>> *All my*
>>>>>> *users are using Windows 2000 only. I have also*
>>>> *rename my*
>>>>>> *administrator for my server. I have downloaded*
>>>>>> *EventCombMT*
>>>>>>> *from MS and managed to search all my events*
log. I
>>>> *have*
>>>>>> *a*
>>>>>>> *long list of event ID: 644. Yet when i go*
through

Re: Windows 2000 users accounts get locked out

>> *the*
>> >> >> *list*
>> >> >> >> *I still don't understand why my users are*
getting
>> >> *locked*
>> >> >> >> *out! This happened suddenly and I have never*
>> *changed*
>> >> *any*
>> >> >> >> *thing to my servers. My accounts is still*
getting
>> >> *locked*
>> >> >> >> *out and yet I still dont know why! Please help.*
>> *Many*
>> >> >> >> *thanks in advance!*
>> >> >> >> *Merrick*
>> >> >> >
>> >> >> >
>> >> >> >.
>> >> >> >
>> >> >
>> >> >
>> >> >.
>> >> >
>> >
>> >
>> >.
>> >
>
>
>.
>