

RE: Kaseya

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2008-05/msg00187.html>

- *From:* "Kevin Reiter" <KReiter@xxxxxxxxxxxxxx>
 - *Date:* Thu, 29 May 2008 12:04:01 -0400
-

That's incorrect. The administrator (MSP in this case) controls which machine(s) get the agent installed – nothing is done automatically, unless the install is done via a login script. A scan of the network segment is done, and a list of machines discovered (Windows, printers, *nix, etc.) is displayed, and the MSP manually decides which machines get an agent installed. There are different agent configurations that can be created, depending on the operating system, client, location, and other variables. This isn't a simple application.

Again, there is no "appliance" anywhere. Period.

Another thing to note is the fact that psexec is used for remote tasks. psexec lives only on the server, which is located at the MSP's data center/NOC, and communications between the agent and the server are encrypted. Sniff away..

I highly recommend that you download the free evaluation version of Kaseya and contact their technical support to get an accurate understanding of how this specialized product actually works.

–Kevin

-----Original Message-----

From: listbounce@xxxxxxxxxxxxxxxxxxxxx
[mailto:listbounce@xxxxxxxxxxxxxxxxxxxxx] On Behalf Of Utz, Ralph
Sent: Tuesday, May 27, 2008 3:39 PM
To: pen-test list
Subject: RE: Kaseya

Well, from what I understand it gather's it's data by ping scanning the network and referencing the results to it's database of PCs that it's agent is installed on. If there is an IP that isn't in the database that comes up hot, it trys to access the IPC\$ share I believe. If it can access it, it flags it as a Windows box and trys to install it's agent on the device. If not, it leaves it and moves on.

Weaknesses that stand out to me are 2 things. One being that depending on how often you have the appliance set to scan and how old your network gear is, it could flood your network. Two being that in order to access the IPC\$ share on all the machines, you have to use a domain account that has rights to install software on the machine. Most times this ends up with the MSP requiring a domain admin account because no one wants to fool with delegating permissions.

RE: Kaseya

So in theory, you have an appliance that floods your network with pings and possible clear txt attempts at using a domain admin account.

-----Original Message-----

From: listbounce@xxxxxxxxxxxxxxxxxxxxx [mailto:listbounce@xxxxxxxxxxxxxxxxxxxxx]

On Behalf Of M.B.Jr.

Sent: Saturday, May 24, 2008 2:01 PM

To: pen-test list

Subject: Kaseya

Hello list,
there's this infrastructure tool set for automating managed services, named Kaseya (proprietary technology).

Basically, the managed-services-provider controls one of his customers' remote LANs with two intercommunicating "appliances":

- * a Kaseya dedicated server located at the MSP data center; and
- * a "probe" equipment at the remote LAN.

The audit team to which I belong is about to examine the probe-featured LAN.

Right now, we're researching whether this "solution" can cause the LAN some weaknesses; the resulting research's report is going to shape the logical tests.

So, the question is (I guess):
does anyone know of any Kaseya-enhanced LAN security implication/vulnerability?

Thank you,
yours sincerely,

Marcio Barbado, Jr.

This message may contain confidential or proprietary information and is intended solely for the individual(s) to whom it is addressed. If you are not a named addressee you should not disseminate, distribute or copy this e-mail or act upon the information contained herein. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system.

This list is sponsored by: Cenxic

Top 5 Common Mistakes
in Securing Web Applications
Find out now! Get Webinar Recording and PPT Slides

RE: Kaseya

RE: Kaseya

www.cenzic.com/landing/securityfocus/hackinar
