

RE: Subseven Scans

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2002-08/0063.html>

From: H C (keydet89@yahoo.com)

Date: 08/14/02

Date: Wed, 14 Aug 2002 11:04:54 -0700 (PDT)

From: H C <keydet89@yahoo.com>

To: Robert Buckley <rbuckley@synapsemail.com>, "'Baribault, Gary'" <gary@baribault.net>, grdnwsl

> *"it was determined by examining the contents of the
> drive in question, and seeing a directory
> structure that appeared to be one that had been
> infected.*

What about the directory structure led you to believe it was infected? Was it the presence of certain files? If so, which ones? The existence of "control characters" is inconclusive...as you said, many of these hosts seemed to be home systems. Also, the OP stated that many of the hosts he saw were in Korea...so perhaps the "control characters" were simply foreign language characters.

> *You wont find
> normal people creating directories with
> control codes in them, and since more than 1 out of
> the 20 + hosts had that
> type of sign, its assumed they are in
> fact infected with something.*

Ah...again..."assumed".

> *It also showed signs that these were not
> business systems, and of a home type of system,
> which can lead to a conclusion that they were less
> secure than business
> systems, and more prone to have stuff uploaded on
> them. Most the hosts had
> MS file sharing enabled, with write access from the
> root of the drive. Just
> another sign
> to lead to a formidable conclusion"*

SecurityFocus Incidents: RE: Subseven Scans

As we've discussed, the issue of your actually accessing the machines abounds. From another list, here is an excerpt from CA state law:

1: knowingly and without permission access or caused to be accessed any computer, computer system, or computer network. (PC 502(c)(7))

So, as you can see, this issue I've presented of your accessing the hosts isn't a fantasy I've made up...it's a fact.

- > *leads one*
- > *to believe that this is the work of one person*
- > *hopping from system to*
- > *system, quite possibly to try to break ACL's on the*
- > *borders.*

I'm not really clear on how SYN packets can be used to "break ACL's [sic] on the borders".

- > *There was no effort on my part to determine*
- > *if an infection on an*
- > *attacking host was causing the scan or not. The*
- > *application source of the*
- > *scan made no difference in my analyses"*

Okay. I guess maybe I find it a little hard to believe that you'd go through all the trouble of scanning these remote hosts, accessing the drives, determining that write access is available to the root of the drive, and yet not give any specific data beyond that. After all, there are a number of tools you could have run...many of which I've specifically detailed the usage of in this and other lists...in order to determine the root cause of the scan. Information regarding the root cause would be extremely useful in answering the question posed by the OP..."what is this?"

From the data you have gathered, it's clear that this may be a zombie or remotely controlled app of some kind, perhaps even an IRC bot. However, again I find it difficult to understand why you would go through the trouble of accessing these systems, viewing the file structure, identifying control codes in the directory structure, but never say what the directory structure or control codes are, or even what led you to believe that the systems were infected. After all, since you'd gone that far already, you wouldn't even need write access to the drive to determine what was

actually on the system...a simple "dir" or "tree" command would suffice.

At this point, let me simply state that my intention here isn't to create "drama" or to complain about anyone. I am simply pointing out that on the lists, when an incident like this occurs, very often we take some steps, but don't go far enough. In the long wrong, going half way and speculating about the rest of the issue is actually more harmful to the community as a whole than simply ignoring the SYN packets in the first place.

All I'm suggesting is that if you're going to investigate a situation, do so, but do so fully and completely. The reason I suggest this is b/c for the most part, we (as a community) aren't all that good at detecting and investigating incidents...let alone reporting them. What I've been trying to do by posting to the list and asking questions of other posters has been to increase the level of awareness of what can be done and what should be done to investigate an incident.

> *"The community can benefit from whatever they can.*

The community benefits from whatever is provided by its constituent members.

- > *1: Windows hosts, all of them – fact.*
- > *2: MS Shares at the root level, some of them. – fact.*
- > *3: Sequentially scanned, not simultaneous – fact.*
- > *4: Hosts were not spoofed. – fact.*
- > *5: Some hosts showed signs of virus via the CTRL chars that were used to*
- > *create directories on their shares. – fact.*

Something else to consider is that "tagged" FTP directories have also shown signs of control characters in the directory structure...but those systems were largely used as repositories for copyrighted data, and did not generally lead to active malware, particularly the type of activity described in this thread.

- > *6: How long the attack lasted. – fact.*
- > *7: Was the attack successful. – fact.*

It would seem that the "attack", if that's what you can call it, was hardly successful at all. After all,

SecurityFocus Incidents: RE: Subseven Scans

all you received were SYN packets, correct?

Do You Yahoo!?

HotJobs – Search Thousands of New Jobs

<http://www.hotjobs.com>

This list is provided by the SecurityFocus ARIS analyzer service.
For more information on this free incident handling, management
and tracking system please see: <http://aris.securityfocus.com>

- ***Previous message:*** [Richard Gilman: "Increased IIS scans mainly on 66.0.0.0/8"](#)
- ***In reply to:*** [Robert Buckley: "RE: Subseven Scans"](#)
- ***Next in thread:*** [Robert Buckley: "RE: Subseven Scans"](#)
- ***Messages sorted by:*** [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)