

[NEWS] 55808 Trojan Analysis

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-06/0077.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 06/23/03

To: list@securiteam.com

Date: 23 Jun 2003 10:10:51 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at canadasales@beyondsecurity.com

55808 Trojan Analysis

SUMMARY

Intrusec has completed an initial analysis of a Trojan that appears to be one of several that is responsible for generating substantial scanning traffic across the Internet with a TCP window size of 55808. The Trojan we have isolated appears to match many of the characteristics that others in the security community have reported for this Trojan. However, we do not believe that the specific Trojan we have identified is the sole source of the traffic generated, and do not know that it is a primary source.

The information we've been able to gather leads us to believe that the Trojan we have captured is not the original source of the 55808 traffic that has been seen, but is rather a "copycat", created to mimic the behavior of another Trojan or worm. The behavior of this copycat appears to be based on press releases, news articles, and mailing lists that described its hypothetical behavior and known output. Nonetheless, this copycat Trojan appears to be actively deployed on systems across the Internet and is something security professionals should be aware of. Details contained in this analysis will be updated, and linked to numerous analyses that will be done by other security researchers, as they become

available.

Please visit and link to <http://www.intrusec.com/55808.html> to receive the latest information available regarding this Trojan. There is apt to be great discussion about the nature of this "Trojan" and whether in fact it is accurately characterized as a Trojan, backdoor, zombie, or worm. While the specific binaries we have captured are probably described as a Trojan or zombie, there is no assurance that other variants of this Trojan may not be far more malicious in nature and contain worm or backdoor functionality. We are referring to the Trojan we have captured, and the presumed other existing Trojans generating similar traffic as "55808 Trojans," and the specific binary we have analyzed as "55808 Trojan – Variant A." All discussion in our analysis section refers specifically to the 'A' variant we have captured. Internet Security Systems subsequent to the release of this alert dubbed this "Stumbler", and refers to this same Trojan by that name.

DETAILS

Analysis:

This Trojan aims to be a distributed port scanner whose presence is very difficult to detect. It port scans random addresses across the IP address space, with a random source address also spoofed. By spoofing the source address, the Trojan is able to avoid easy detection, but it also means it can not receive the results of the TCP SYN that is sent. However, since the Trojan also sniffs the network it is on in promiscuous mode, it is likely, over time, to pick up scans from other installations of Trojans that randomly selected a source address that happened to be on its subnet. As the number of Trojans installed across the Internet grows, more spoofed packets will be sent out by each Trojan, and more of the spoofed source addresses will be captured by other Trojans.

Each time a reply to a Trojan is seen, indicating an open port has been found, it is written to a file and saved. Daily, the Trojan will then deliver the list of open ports it recorded while sniffing to a file and deliver that file to a predefined IP address.

In addition, a specially crafted packet can be sent to the subnet the Trojan is listening on which contains in its sequence number the IP address the Trojan should deliver the open port list to daily. However, in the current incarnations of this Trojan this functionality appears to be disabled.

Finally, the Trojan contains a feature whereby if it fails to connect to the IP address it is supposed to deliver its open ports list to, it will automatically attempt to remove itself from the system.

The Trojan we have identified has been a file named 'a' that resides in /tmp/.../a on the file system. Its packet collection activity monitors for any packet with a window size of 55808 and records all packets matching

Securiteam: [NEWS] 55808 Trojan Analysis

that window size. The packet capture is written to its current directory (/tmp/.../ typically) in a file named 'r'.

There is a default IP address of 12.108.65.76 that the Trojan attempts to make a standard connection (not spoofed) to on TCP port 22 and deliver the packet capture after it has been running for 24 hours, however this appears to have been randomly selected as it is not an active system on the Internet, and it is potentially dynamically modifiable by a packet that can be sent to the Trojan.

The Trojan appears to contain some functionality to change the IP address it delivers its packet captures to, but this functionality is not operational in the Trojan we have obtained. It appears the stubbed out code, if activated, would function as follows: If a packet is captured that contains a window size of 55808 and a TCP option window scale of 2, the Trojan modifies the IP address packet captures are delivered to based on the sequence number of that packet.

While a novel concept, this Trojan seems largely to have been written as a proof of concept relative to the ideas Lancopo described as a '3rd generation Trojan.' Other than generating large amounts of network traffic, it contains no self-replicating or malicious behavior, and a few high-speed port scans from compromised host would be a far more effective and efficient means to map open ports on the Internet than this type of Trojan.

We have only observed the Trojan on Linux systems to date. However, the program itself is quite portable to other UNIX variants, so it is possible if not likely that it may also exist on other UNIX distributions. It is also possible that the 'original' Trojan is Windows-based.

The Trojan appears to be installed on a system either manually, or through an external exploit that is unrelated to the Trojan itself. There is no exploit code or means to install itself on a host built-in to the Trojan itself. It is easy to identify that a system on your network has been infected with this or a related Trojan due to its extremely noisy network activity it generates with TCP packets with a window size of 55808. However, other legitimate services may intentionally or incidentally also send packets with this same window size, so do not solely rely upon the presence of such a packet as guaranteeing the existence of such a Trojan. Security vendors who claim that identifying massive quantities of port scanning originating from their network as a unique feature of their software should be taken with a grain of salt. It is more difficult to identify the specific system on your network that has been infected with this Trojan due to its spoofing activities other than for its daily non-spoofed connection to remote port 22. Tools that can assist you in locating the actual physical source of these spoofed packets (through looking at MAC addresses and ARPs) may be quite useful.

ADDITIONAL INFORMATION

Securiteam: [NEWS] 55808 Trojan Analysis

Additional Links:

<<http://www.eweek.com/article2/0,3959,1130759,00.asp>>
<http://www.eweek.com/article2/0,3959,1130759,00.asp>

<http://gcn.com/vol1_no1/daily-updates/22371-1.html>
http://gcn.com/vol1_no1/daily-updates/22371-1.html

<http://www.lancope.com/news/Virus_Alert_Trojan.htm>
http://www.lancope.com/news/Virus_Alert_Trojan.htm

The information has been provided by <<mailto:djm@intrusec.com>> David J. Meltzer of Intrusec.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.