

UNAUTHORIZED-COMMUNICATION DETECTING APPARATUS AND PROGRAM

TECHNICAL FIELD

The present invention relates to an unauthorized-communication detecting apparatus
5 and program, and more specifically, to a technology for detecting unauthorized communication
of a client apparatus.

RELATED ART

In the related art, there are known unauthorized malicious computer programs
(hereinafter, referred to as malware) to pose threats such as information leakage. For example,
10 in a case where malware is installed in a client apparatus such as a personal computer, there is a
possibility that the malware may influence an apparatus such as a server apparatus which
performs communication with the client apparatus.

Non-patent Literature 1: Moheeb Abu Rajab, Jay Zarfoss, Fabian Monrose, Andreas
Terzis, "A Multifaceted Approach to Understanding the Botnet Phenomenon", the Internet
15 <URL:<http://conferences.sigcomm.org/imc/2006/papers/p4-rajab.pdf>>

SUMMARY

An object of the present invention is to provide an unauthorized-communication
detecting apparatus and program for detecting unauthorized communication of a client apparatus.

According to an invention of claim 1, there is provided an unauthorized-communication
20 detecting apparatus comprising: measuring means for measuring a transition of a communication
state value between the unauthorized-communication detecting apparatus and a client apparatus;
transition pattern storage means for storing a transition pattern of the communication state value;
and unauthorized-communication detecting means for detecting unauthorized communication of
the client apparatus on the basis of the transition pattern and a transition of the measured
25 communication state value.

According to an invention of claim 2, there is provided the unauthorized-
communication detecting apparatus according to claim 1, wherein the communication state value
is usable communication bandwidths or occupied communication bandwidths.

According to an invention of claim 3, there is provided the unauthorized-
30 communication detecting apparatus according to claim 1 or 2, wherein the unauthorized-
communication detecting means selects a portion of the transition of the measured
communication state value on the basis of correlation values relative to the transition pattern, and
in a case where the difference between the selected portion and the transition pattern satisfies a
predetermined condition, the unauthorized-communication detecting means detects the
35 unauthorized communication of the client apparatus.

According to an invention of claim 4, there is provided the unauthorized-