СЕКЦІЯ 22. ЕЛЕКТРОМАГНІТНА СТІЙКІСТЬ

DEVELOPMENT of TECHNIQUES to IDENTIFY MALICIOUS CODE in COMPUTER NETWORKS

Rybka Ernest
National Technical University
«Kharkiv Polytechnic Institute»,
Kharkiv

Today the actuality of the problem of cyber security is not in doubt. Every day, each of us is faced with the use of information technology. From social networking, posting information about their personal data on the Internet, to use ATMs, bank accounts and so on.

The most dangerous in the area development of malicious software is a botnet network. A botnet is a number of Internet-connected devices used by a botnet owner to perform various tasks. Botnets can be used to perform DDoS, steal data, send spam, allow the attacker access to the device and its connection.

To hiding the presence of botnet networks actively used technology polymorphism, that involves a mutation code in the process of functioning.

Today, many methods used to detect malicious files but they have a high percentage of false positives.

A new method for detecting botnet networks based on the use of a multi-agent system using various sensors and based on principles relating to known levels of polymorphism.

The model of the polymorphic virus is taken as the basis. The levels of the cortex are evolved.

The first-level model $M_1 = (A, X, G, V, U, \xi, Q, P, R)$,
The second-level model $M_2 = (A, E, U, P, Z, R)$
The model of the third and fourth levels $M_{3,4}= (A, E, U, B, Y, D, R)$
The fifth-level model $M_5 = (A, B, X, G, U, \xi, H, D, R)$
The sixth level model $M_6 = (A, E, U, C, R)$

It has been proposed to include in the MAC agent a new sensor that allows launching and executing over potentially malicious software. Reactions to specified actions give a conclusion about the presence in it of a polymorphic code.

The re-running of suspicious software may indicate a possible change in the program body as a result of performing encryption. This detection is possible due to the creation of so-called "fingerprints" To the reference and modified file K 'and their subsequent comparison.

Imprint K is formed by a certain binary sequence.

$K = \alpha, \beta, \chi, \delta, \varepsilon$. Where α - the name of the file; β -file size; χ - date of the last change; δ -system attributes; ε -128 bit code MD5