ADVANCED ENCRYPTION METHODS USED IN MODERN MALWARE ACTIVITIES WITH RESPECT TO THE INFORMATION SECURITY IN TCP/IP ENVIRONMENT

EUGENE NICKOLOV, PROF. DSC. CEO,
DIMITRINA POLIMIROVA, PHD,

NATIONAL LABORATORY OF COMPUTER VIROLOGY – BAS

- Wireless Security
- Data Security
- Cryptographic Security
- Computer Security
- Steganographic Security
- Communication Security
- Mobile device Security
- Operating System Security
- Application Security
- Web Security
- Emission Security
- Email Security

CONTENT

National Laboratory of Computer Virology – BAS

1. Introduction
2. Definitions
3. Problems
4. Solutions
5. Conclusions
6. Recommendations

1. INTRODUCTION

1. INTRODUCTION

- Growing presence of **malicious activity** in almost all domains of human activity in *TCP / IP environment*.
  - **information security** - one of the common descriptive terms characterizing this trend.
    - The malicious activity effect can be estimated in some reasonable borders by increasing or reducing the value of information security.
- The malicious activity is implemented through pre-planned actions in the form of a **malicious scenario**.

1. INTRODUCTION

- It contains obligatory the preparation of one or several **information attacks**.
  - Each of these attacks involves several phases of implementation, such as:
    - preparing;
    - carrying;
    - concealing.
  - Each one of the attacks has its target related to a particular **information object**.
- The **malicious code** that implements specific parts of the scenario is applied on this information object.

1. INTRODUCTION

National Laboratory of Computer Virology – BAS

- One of the main characteristics of modern information attacks is the use of modern **methods for encoding and decoding** (right and reverse transformation) of the malicious code.
  - The code can be entirely processed by an encoding method or partly by treatment applied only on parts of it.
  - Besides this several methods of coding and decoding could be applied consecutively and their advantages could be combined.
  - These methods use high-speed algorithms that apply the maximum number of processor units.

2. DEFINITIONS

2.1 Malicious activity

2.2 TCP / IP environment

2.3 Information Security

2.4 Malicious scenario

2.5 Information attack

2.6 Information object

2.7 Malicious program code

2.8 Methods for encoding and decoding

2. DEFINITIONS

MALICIOUS ACTIVITY

- Pre-planned action or series of actions on an information infrastructure, which are aimed at its short- or long-term damaging in the legal and / or informational aspect.

TCP/IP ENVIRONMENT

- Combination of software and hardware resources providing compatibility with the protocol family TCP / IP.

2. DEFINITIONS

National Laboratory of Computer Virology – BAS

INFORMATION SECURITY

- Metric which enables to make a relative assessment of the property "data security" during the participation of certain parameters in a known information infrastructure.

MALICIOUS SCENARIO

- Pre-planned sequence of actions on information infrastructure, causing damaging in the legal and/or informational aspect with the possibility for multiple repetitions in several variants by adapting to the changing environment.

2. DEFINITIONS

INFORMATION ATTACK

- Pre-planned actions on the information infrastructure associated with illegitimate read / write operations.

INFORMATION OBJECT

- Organized set of data that has sustainable coordinates for a certain time period and can be named, processed, converted and stored.

2. DEFINITIONS

National Laboratory of Computer Virology – BAS

MALICIOUS PROGRAM CODE

- Specific realization of malicious scenario by the tools of a specific high or low level programming language which causes a change in the normal functioning of the IT infrastructure (cores, processors, memories, peripherals, etc.).

METHODS FOR ENCODING AND DECODING

- Combination of software and / or technical means allowing a conversion of the information in a right and reverse direction in such a way as to ensure, within certain limits the legitimate operations for reading and / or writing the information.

3. PROBLEMS

3.1 Analysis of encoding and decoding methods

3.2 Advantages

3.3 Disadvantages

National Laboratory of Computer Virology – BAS

Important features of the methods for encoding and decoding, used for the malicious code processing: 1/2

HIGH SPEED

- Between four and eight processor cycles when processing the current portion of processor information (four-to eight bytes).

MINIMUM PRESENCE

- Between one and two processor cycles in the processor registers during the preliminary and completed operations.

3. PROBLEMS

3.1 ANALYSIS OF ENCODING AND DECODING METHODS

National Laboratory of Computer Virology – BAS

Important features of the methods for encoding and decoding, used for the malicious code processing: 2/2

SHORT ACTIVITY

- Between one and two processor cycles in the operating memory cells and its cash images.

MINIMUM CONSUMPTION

- Between thirty-two and sixty-four kilobytes of RAM per processor cycle. All these characteristics make the detection of such activity very difficult, as it always has been added to ongoing operations in such a way that the load on the processors or processor cores does not almost change.

- Features that reduce the probability of detecting the malicious activity:
  - data modules with prepared data are used to reduce the resources calling;
  - control modules are used that allow adaptation to CPU load;
  - transport modules are used that allow minimal activity of registers in the processors or processor cores.

3. PROBLEMS

3.3 DISADVANTAGES

- Features that increase the probability of detecting malicious activity:
  - data modules are used that do not allow to overcome the integrity protection realized using checksums by a method that is safe enough,
  - control modules are used that cannot cover entirely the variety of platforms, operating systems, processors and chip-sets, and
  - transport modules are used that cannot provide completely conflict-free routes.

3. PROBLEMS

3.4 IMPACT ON INFORMATION SECURITY

National Laboratory of Computer Virology – BAS

- The tools for achieving a particular degree of information security, (e.g. anti-viruses, firewalls, intrusion prevention systems and security appliances) are affected significantly by the speed and volume characteristics of the involved processor resources used by the methods of encoding and decoding.
- This influence is much more serious in thirty-two bit processors and very moderate in sixty-four bit processors.

4. SOLUTIONS

4.1 Information security enhancement

4.2 Reduction of false alarms

4.3 Reduction of computational costs

4. SOLUTIONS

4.1 INFORMATION SECURITY ENHANCEMENT 1/2

National Laboratory of Computer Virology – BAS

- Researches in this domain suggest that we could seek for solutions to increase the information security by **reducing the benefits** and **increasing the disadvantages** of the methods for encoding and decoding.
- For this purpose inspection program tools could be created that could in fully automatic mode, and after the accumulation of some history data, detect the abnormal and illegitimate activity using the data modules, management modules and transport modules where the methods of encoding and decoding for malicious activity are implemented.

National Laboratory of Computer Virology – BAS

- At this stage some results of experiments are available with similar inspection tools for Intel and AMD family thirty-two bit processors with two and four cores.
- Using "snapshots" at regular very small intervals (from tens to hundreds of nanoseconds) of input-output vectors of information flows and comparing them, a clear margin could be defined for the parameters change (in the load) and hence the threshold for warnings in case of illegitimate activities related to the methods for encoding and decoding.

4. SOLUTIONS

4.2 REDUCTION OF FALSE ALARMS

National Laboratory of Computer Virology – BAS

- To achieve an acceptable level of information security in an information infrastructure it is essential that security and prevention tools generate minimum (if possible zero) quantity of false alarms.
- Any incorrect and/or false signal for malicious activity generates costs and discredits the security system.
- In this regard, the performance of the inspection tools can relatively easily be added or even integrated in the installed security software and hardware tools.
- The combination of different policies and procedures to achieve a certain level of information security is probably one of the best solutions to eliminate the false alarms in the security systems.

4. SOLUTIONS

4.3 REDUCTION OF COMPUTATIONAL COSTS

National Laboratory of Computer Virology – BAS

- Despite the availability of increasingly powerful and high-performance IT infrastructures, the achievement of certain level of information security is measured not only by money spent but by the computational costs (processor cycles, memory cells, redundant data in the buses) for the resources that are not used as intended.
- In this regard, inspection tools which detect the increased activity in encoding and decoding associated with malicious activity significantly reduce the computational costs.

5. CONCLUSIONS

5.1 Malicious program code is always encrypted

5.2 The operational memory stores in clear form only a few bytes

5.3 Processors and cores contain encoded and plain information

5. Conclusions

National Laboratory of Computer Virology – BAS

Malicious program code is always encrypted

- This characteristic of modern malicious activity can be explained by the desire of malicious scenario's to ensure a long life for their ideas.
  - Otherwise, malicious code that is not encoded is easy to neutralize.

5. Conclusions

National Laboratory of Computer Virology – BAS

The operational memory stores in clear form only a few bytes

- To realize itself, the malicious code requires an explicit form for at least a little part of it.
  - This means that any displacement of its active part requires the action of high-speed and high effective (in terms of computational costs) methods for encoding and decoding.

Processors and cores contain encoded and plain information

- The existence of two types of information can be explained by the desire of the malicious code authors to hide very deeply the transformation procedure for maximum security.

6. RECOMMENDATIONS

6.1 Control on the increased activity of resources

6.2 Extended use of checksums

6.3 Specialization of processor cores

6. RECOMMENDATIONS

National Laboratory of Computer Virology – BAS

CONTROL ON THE INCREASED ACTIVITY OF RESOURCES

- The experiments which were carried out and the obtained results show that the inspection tools are able to capture the increased activity of resources related to the use of methods for encoding and decoding.

EXTENDED USE OF CHECKSUMS

- A significant perspective is available for the use of checksums in the management of information flows, especially at points where transformations and branching are available.

6. RECOMMENDATIONS

National Laboratory of Computer Virology – BAS

SPECIALIZATION OF PROCESSOR CORES

- In order to increase the control on the malicious activity in TCP/IP environment it is necessary to create program tools that help to assign to a separate core in a processor the task to manage the security system in the information infrastructure.

THANK YOU!

PROF. DSC EUGENE NICKOLOV, CEO,

PHD, DIMITRINA POLIMIROVA,

National Laboratory of
Computer Virology – BAS

1113 Sofia, Acad. G. Bontchev St., Building 8,
Tel. 359.2.973.3398, Fax 359.2.971.3710,
eugene.nickolov@nlcv.bas.bg,
dimitrina.polimirova@nlcv.bas.bg