Models of malicious software and fault tolerance of information communication networks

Sergey M. Klimov, *4th Central Research and Design Institute of the Ministry of Defence of Russia, Korolyov, Russia*
Sergey V. Kupin, *4-th Central Research and Design Institute of the Ministry of Defense of Russia, Korolyov, Russia*
Dmitry S. Kupin, *Bauman MSTU, Moscow, Russia*


Sergey M. Klimov


Sergey V. Kupin


Dmitry S. Kupin

Abstract. *The aim of this paper is to develop a model that would enable a standardized representation of malicious software's structure, functions and to get a quantitative estimation of the fault tolerance of information and telecommunication networks affected by malicious software. The paper shows the relevance and importance of the malicious software models and evaluation of the fault tolerance of information and telecommunication networks affected by malicious software. Malicious software refers to software systems able to covertly deploy, establish unauthorized virtual data communication channel, self-propagate, self-modify, conduct unauthorized collection of information on the network and information technology interference against it. The structural and functional model of malicious software developed in this paper is composed of the following set of diagrams and function descriptions: structures of covert deployment and malicious software installation using electronic mail, structural and functional diagram of the main module of malicious software and covert deployment modules, structural and functional diagram of malicious software while implementing malicious functions, malicious software certificate. The diagrams detail the standard functions, operating procedures and information interaction of malicious software modules of the external and internal networks via an unauthorized virtual data communication channel. Primary malicious software modules are considered through the example of the Careto targeted computer attack. The model of fault tolerance of information and telecommunication networks affected by malicious software is described by indicators that characterize the ability of the networks and information security facilities to maintain and recover specified probabilistic and temporal characteristics over the period of malicious software activity. The following indicators are considered: probability that information and telecommunication networks and information security facilities maintain the specified probabilistic and temporal characteristics over the period of malicious software activity, probability that information and telecommunication networks and information security facilities recover the probabilistic and temporal characteristics after the effects of malicious software activity, factor of operation availability of information and telecommunication networks to perform the specified probabilistic and temporal characteristics under malicious software activity at an arbitrary moment in time, mathematical expectation of the duration of malicious software activity, mathematical expectation of the recovery time of the probabilistic and temporal characteristics of information and telecommunication networks and information security facilities. It is assumed that the values of the parameters required for the calculation of the indicators of the fault tolerance model of information and telecommunication networks were obtained as the result of a testbed simulation of the networks affected by malicious software. In the conclusion it is noted that the developed models enable the identification of the general structure of covert deployment and installation of attacking malicious software using electronic mail, structural and functional diagram of the main module of malicious software and covert deployment modules, structural and functional diagram of malicious software while implementing malicious functions, malicious software certificate, as well as evaluate the fault-tolerance of information and telecommunication networks and information security facilities affected by malicious software, quantify the probabilistic and temporal fault tolerance, recoverability and availability characteristics of networks.*

Keywords: *malware, information and telecommunication networks, information security facilities, fault tolerance.*

For citation: Klimov SM, Kupin SV, Kupin DS. Models of malicious software and fault tolerance of information communication networks. Dependability 2017;4: 36-43. DOI: 10.21683/1729-2640-2017-17-4-36-43

Introduction

Today, the highest threat comes from targeted computer attacks organized by intruders using covertly deployable and self-propagating malicious software (malware, MW). Such software is not always quickly detectable by state-of-the-art information security facilities (ISF) such as antivirus protection, computer attack detection, prevention and recovery systems. Usually, intruders exploit zero-day vulnerabilities in many programs of operating systems (OS), network services and protocols for covert deployment of MW elements into information and telecommunications networks (ITCN).

MW shall refer to a software system for covert deployment, establishment of unauthorized virtual data communication channels, self-propagation, self-modification and implementation of massive targeted information technology interference (computer attack) against ITCN for the purpose of disrupting information security and operational stability.

MW systems have difficult to analyze software implementation, their development and execution involves considerable information resources, they use algorithms for compression, encryption and masking of destructive actions. Today's massive targeted computer attacks, such as WannaCry in 2017, that involve MW affect hundreds of thousands of computers worldwide and disrupt the operational stability of ITCN of the banking, energy, healthcare, communication, transportation and other critical industries [1-2].

This paper proposes a structural and functional model of MW that was developed involving the analysis of the Careto targeted computer attack's source code set forth in the Kaspersky Laboratory analytical findings. Additionally, the paper interprets a standard structural model and functions of a wide range of MW.

Careto facilities enabled the intruder to attack 380 unique objects in 31 countries. Using Careto the intruders stall information on computer facilities, private encryption keys, VPN settings, SSH settings, RDP files, as well as files of various data formats. Typically, MW deployment is performed via the Internet, suitable ITCN communication equipment and unauthorized connection of external data storage device [3].

The Careto MW system is installed in the network with the installation module and provides the intruder with remote access to the ITCN without the user's knowledge, performs a set of commands received from the remote control server in order to collect information on the network, vulnerable services and stored data. In case of successful ITCN penetration the Careto installation module extracts the components required for correct Careto operation and subsequent deployment in the network.

Essentially, Careto and similar programs enable two types of computer incidents in the ITCN:

1. Penetration and organization of unauthorized, virtual, covert channel for collection, transmission and processing of information on the ITCN.

2. Covert deployment of MW elements in the ITCN and implementation of massive targeted interference.

Massive targeted MW interference against the ITCN vulnerabilities cause practically immediate (in case of data communication via fiber-optic channels) disruption of functional stability of the ITCN even if ISF are in place.

In order to ensure the functional stability of ITCN affected by MW, it is required to develop models that will define standard MW structures and functions, allow implementing them in the form of testbed simulation models [4] and quantify ITCN resilience when affected by destructive actions [5-7].

ITCN simulation models allow reproducing the most time-critical regulations and control cycles, while ISF models enable developing the respective information security facilities. The most rational configuration of the testbed for verification of ITCN behavior under MW would be a set of data processing centers, information systems based on virtual machines, MW simulators interconnected by means of network communication equipment.

ITCN fault tolerance shall be understood as the ability of the network and ISF to ensure compliance with the specified regulations of control cycles performance (probabilistic and temporal characteristics) under MW within the given time interval.

The presence of potential vulnerabilities in the modern ITCN enables MW deployment and implementation of destructive actions that disrupt functional stability. Therefore, the development of models allowing formalizing the structure and operation process of MW, evaluate ITCN fault tolerance under MW is of relevance.

Problem definition

The following was developed as part of this paper's preparation:

1. MW structural and functional model including the following components:

– general MW system structure;

– structure of MW covert deployment and installation using electronic mail;

– structural and functional diagram of Careto main module and covert deployment modules (SGH, SBD);

– structural and functional diagram of the MW module (SGH) that describes the primary functional capabilities of the MW system;

– MW certificate.

2. Model of ITCN fault tolerance under MW based on experimental testing of ITCN segments and appropriate ISF with simulation of MW against them.

Figure 1 shows the general structure of MW of which the components are distributed over the internal and external networks and interact over the unauthorized virtual data communication channel (established by the intruder). There are known Careto codes for 32 and 64-bit Windows and Linux operating systems (OS), as well as other types of MW for mobile applications of Android and Apple iOS [1,3].

MW structure includes external facilities for controlling the modules deployed in the internal network based on MW control server and delivery (translation) and information interaction module. The MW modules deployed in the ITCN collect data on the network configuration (accessible IPs, MAC addresses and port numbers of communication equipment), type of operating system and ISF, intercept information from the display (user's desktop image), keyboard and connected storage media. The delivery module issues control commands for implementation of destructive functions by the modules deployed in the internal network and then delivers the collected information to the MW control server and stores it in a database. The MW server enables the implementation of the offensive functions of computer attacks against ITCN by means of selection out of a database and sending of a code of special program exploits to the vulnerabilities of the target internal network. Additionally, MW can use various Metasploit Framework tools, e.g. in order to increase MW privileges in the operating system.

The following primary MW modules operate in the internal network:

1. Covert MW elements deployment (loading drivers) and interaction modules that include the facilities for initial access to ITCN elements, covert downloading onto the operating system and ISF evasion, as well as interface programs for organization of information interaction with the external network and between the modules of the internal network.

2. Modules of covert self-propagation of MW in ITCN in the form of software tools for system administrator privileges management, load facilities that ensure interception of operating system traps, covert transition to MW code execution and priority imposing of its functions implementation.

3. Modules of data collection, preparation and implementation of ITCN attacks, of which the key functions consist in the operation of a set of implant programs that intercept wire and wireless network traffic, keystrokes, sessions and keys during programs operation, extract information from computer equipment, save screenshots and control file operations. The malicious module generates the input data on the target ITCN required for interaction, enables deployment of the remaining components of the MW system and delivers the computer attack code to the target ITCN elements.

4. MW self-modification modules are program components that ensure MW adaptation to the parameters of the hardware and software environment of the target ITCN by means of extraction and deployment of programs required for the organization of an unauthorized connection to the network, OS versions, as well as sending a request to the MW server with input data for additional malicious modules.

5. MW covertness modules, i.e. a set of modules that conceal MW actions by means of fake software certificates and electronic signature, internal and external traffic encryption, removal of traces of MW in computer files and memory.

Figure 2 shows the MW covert deployment and installation structure using electronic mail.

Covert deployment, self-propagation and installation of MW are performed as follows. The intruder prepares a phishing e-mail message that contains a link to a malicious network resource. When the link is opened by the user, MW is deployed in the open segment of the ITCN. Then the user is redirected to a legitimate network resource in order to conceal the fact that the system is compromised.

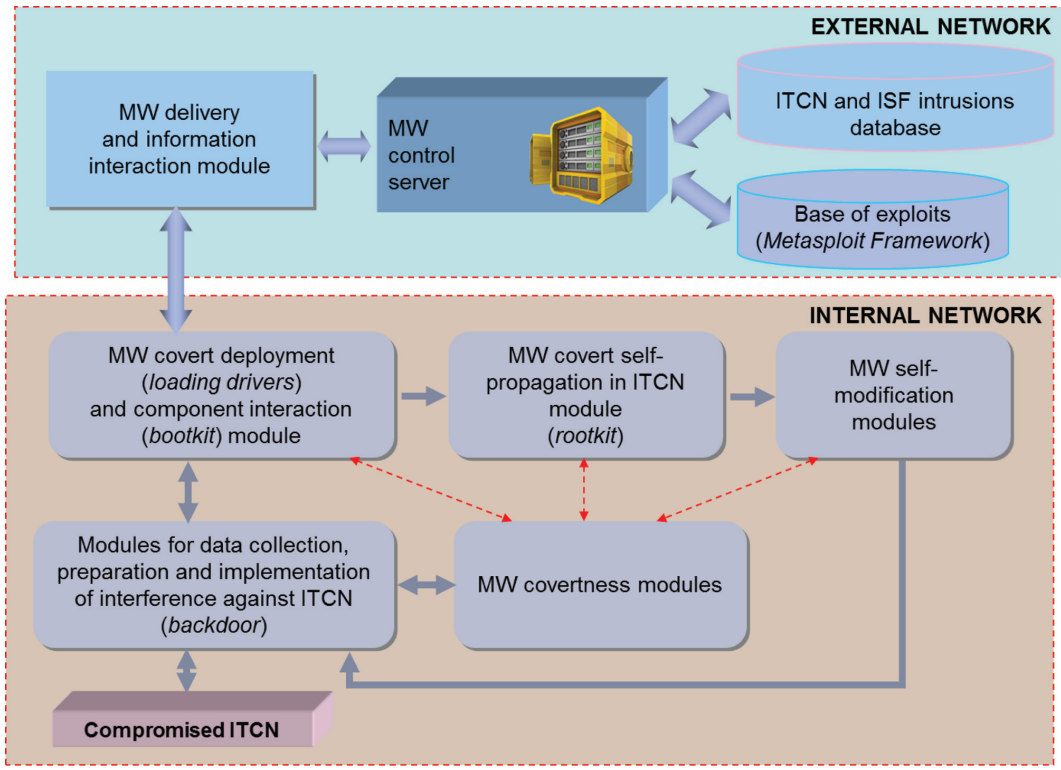

Figure 1. General MW system structure

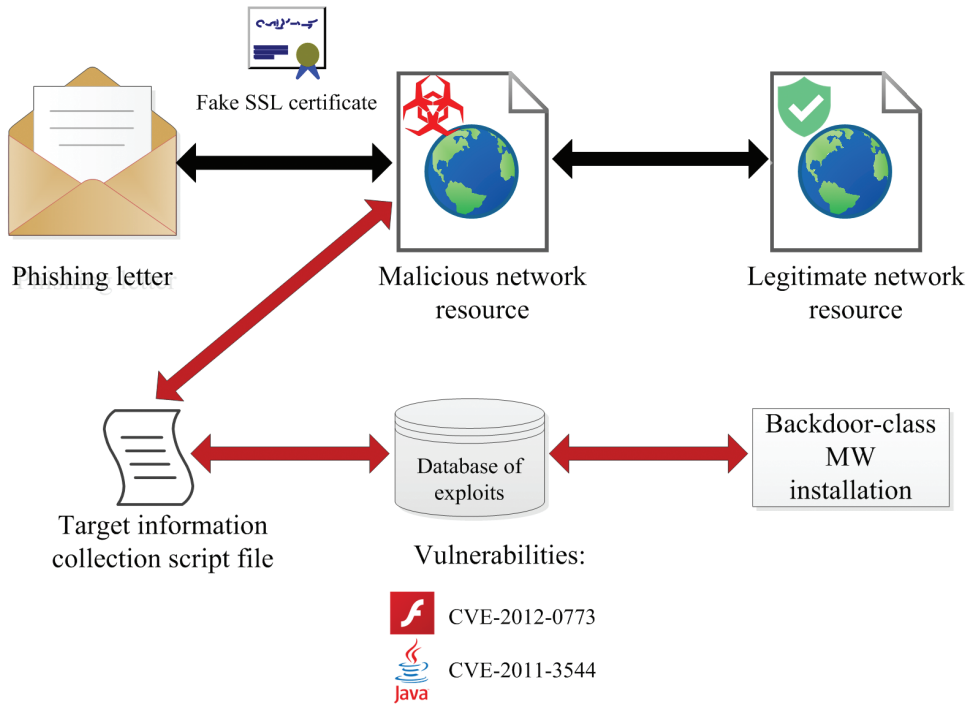

Figure 2. Structure of MW covert deployment and installation using electronic mail

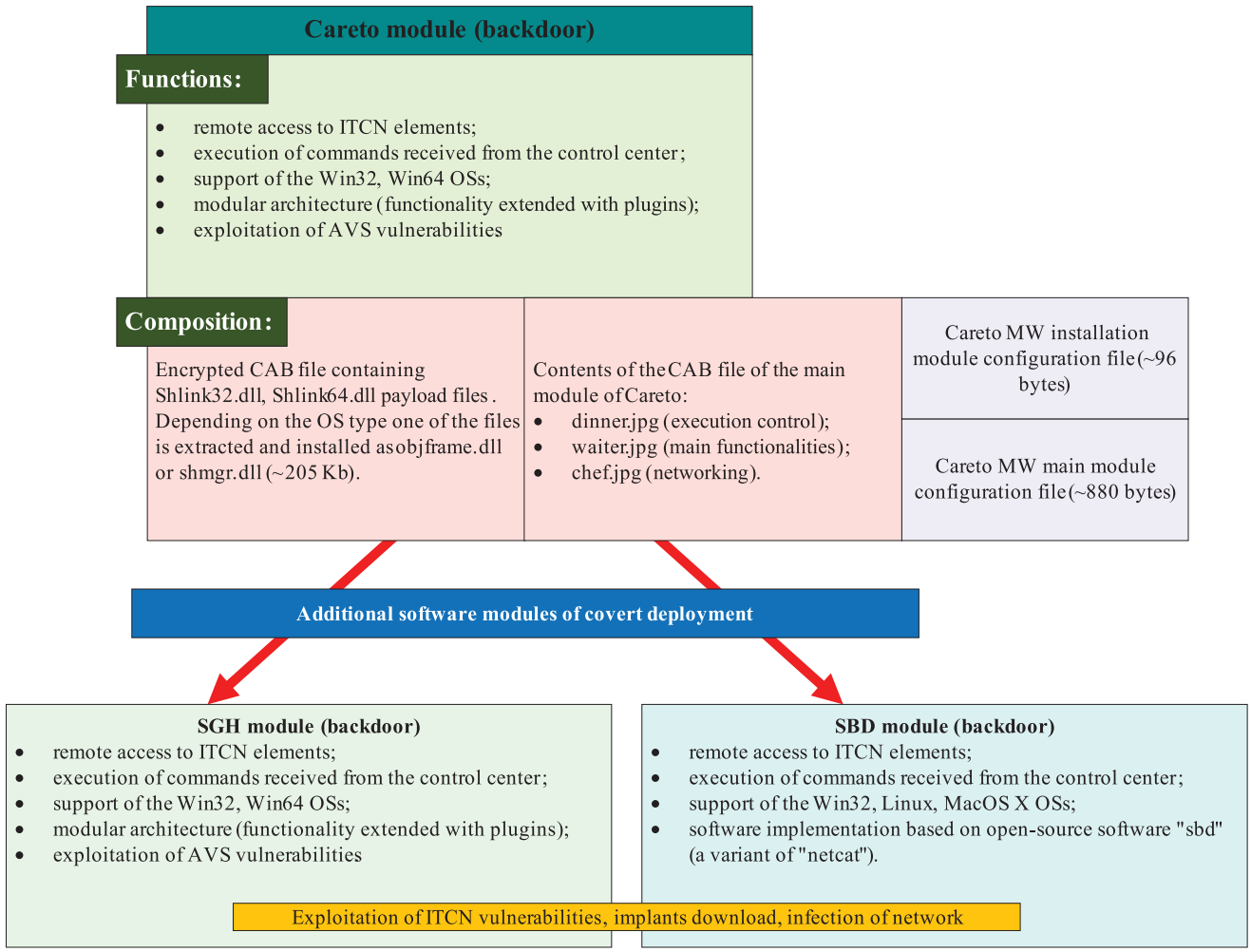

Figure 3. Structural and functional diagram of main MW module and covert deployment modules (exemplified by Careto)

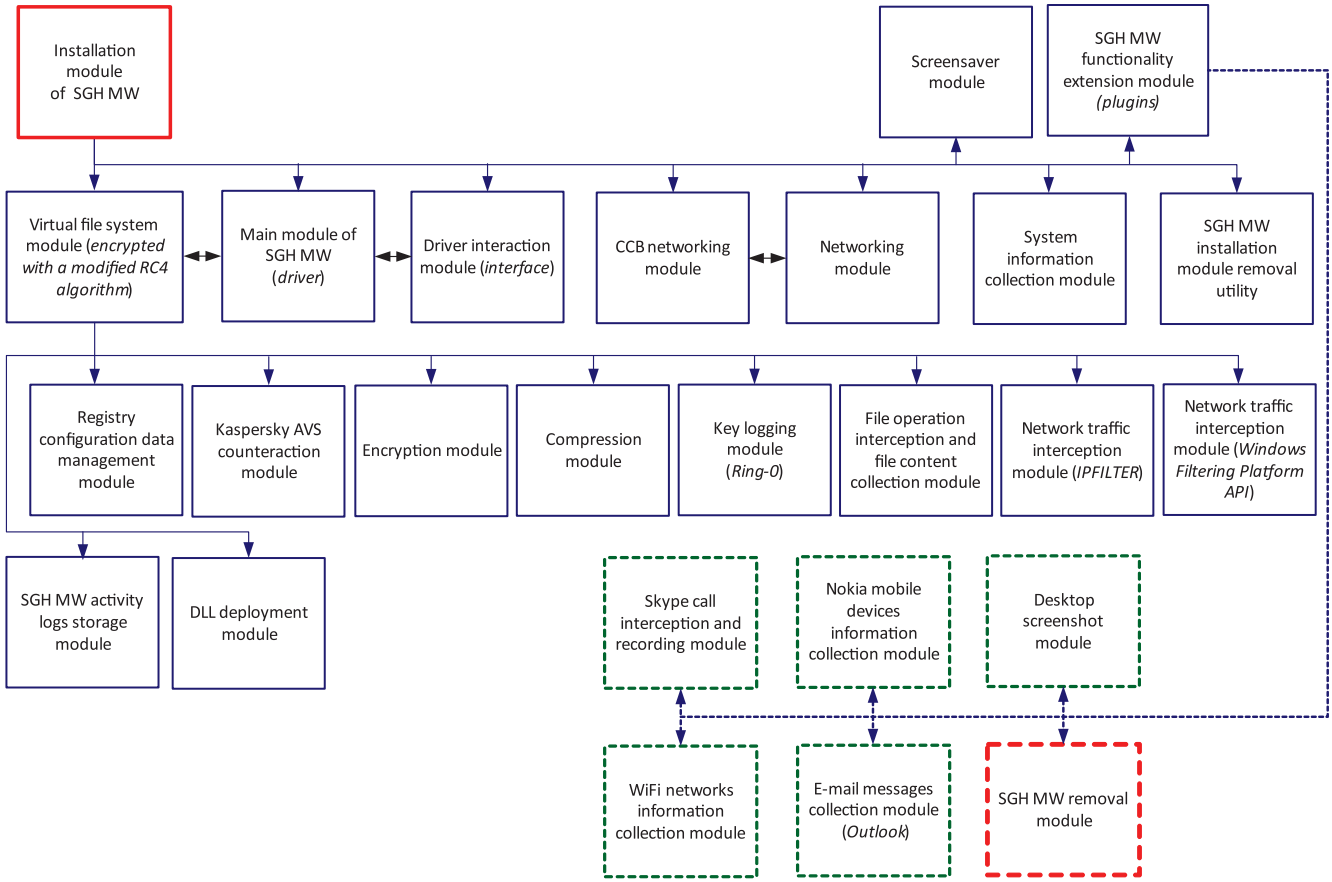

Figure 4. Structural and functional diagram of the MW module (SGH) that describes the primary functional capabilities of the MW system

In order to mask the MW the intruders use subdomains based on malicious network resources. The purpose of the masking mechanism is used on the assumption that if the name of the network resource is very long the browser cuts the name from the end leaving the name of the subdomain.

Then, by using a script file for collection of information on the targets within the ITCN, data on the vulnerabilities and information resources available for intrusion is prepared. For instance, vulnerabilities in Adobe Flash products (vulnerability code CVE-2012-0773) and Java (vulnerability code CVE-2011-3544) are used. Based on the information collected in the ITCN, the required exploit is selected out of the database and loaded as an extension of a browser. Then it is forwarded to the ITCN to ensure the installation of a backdoor-class MW. After a successful compromise of the ITCN the user is redirected to a legitimate network resource, e.g. a news portal.

It is assumed that during its penetration into the ITCN the content of the malicious message evades the standard ITF. The intruder specifies a unique link to a certain exploit and sends it to the user in the phishing letter. The user then loads it. In order to mask the links to exploits, the links are shortened using respective services.

The structural and functional diagram of the main MW module and covert deployment modules (exemplified by Careto) is given in Figure 3. As it can be seen in Figure 3, Careto mainly consists of the main module that performs the initial deployment in the ITCN and the modules for organization of unauthorized data communication channels, covert propagation and implementation of information technology interference (SGH and SBD).

Figure 4 shows the structural and functional diagram of the SGH MW module that describes the primary functional capabilities of the MW system. This type of MW is one of the modules for data collection, preparation and implementation of backdoor-class interference against ITCN. This module provides the intruder with covert remote access to the ITCN, performs various commands received from the MW remote control server. As Careto has the capability to download additional SGH and SBD MW, it can be concluded that the structural and functional diagram, as well as the description of the SGH modules completely characterizes the malicious functions of the whole Careto MW system.

Let us present the primary malicious function of MW, as exemplified by the SGH module of Careto, with a description of the functions of its component modules as follows:

Screensaver module that waits for the moment when the desktop with the name “screen-saver” becomes available, then creates another desktop with its own name, loads the default browser. The «DllEnumClass» function removes the screensaver module or deletes its name from the configuration information, depending on the version of the Windows OS.

Functionality extension module that reads the list of additional SGH modules from the configuration information,

Table 1. Standard MW vulnerabilities certificate

MW description elements	MW description
Name	Careto
Type	backdoor, modular
Detection date	2014
Brief description	The MW covertly deploys and provides the intruder with a remote access to the ITCN, performs various commands received from the remote control server
MW target	public agencies and businesses
Hazard level	High
MW structure	- installation module - main module - remote control center networking module - functional module - execution control module of the functional and network module - removal module - system information collection and data authentication module (additional modules may be downloaded from the remote control center).
Primary functionality	- configuration file and payload file encrypted with a modified RC4 algorithm; - inclusion into startup group as a COM object; - injection of malicious code into explorer.exe, iexplore.exe, firefox.exe, chrome.exe processes; - rerecording of the code sections of the system libraries; - safe closure of module engines; - reception and transmission of data is encrypted with AES and RSA algorithms; - launch of executable files with certain arguments; - reception of CAB file, extraction of file and subsequent launch with a certain argument; - extraction of executable module from CAB file and subsequent launch in the memory; - modification of configuration file, change of remote control server; - collection of information on ITCN and transmission to the remote control server; - complete removal of MW from ITCN.
ITCN compromise indicators	**(Files, fragment)** %AppData%\Microsoft\objframe.dll|shmgr.dll|Shlink(32|64).dll **(Registry, fragment)** [HKLM\Software\Classes\CLSID\{E6BB64BE-0618-4353-9193-0AFE606D6F0C}\InprocServer32] = «%System%\browseui.dll» **(Networks, fragment)** hxxp://202.75.58.153/cgi-bin/commcgi.cgi User-Agent field: Mozilla/4.0 (compatible; MSIE 4.01; Windows NT)
Detection method	**(Virus protection facilities, fragment)** Kaspersky: Trojan.Win32|Win64.Careto.*
Possible elimination measures	- OS reinstallation and formatting of data storage media; - manual check of ITCN compromise indicators (startup group elements, network interaction, file system activity, OS log files analysis); - antivirus facilities update and complete check of ITCN.
Information on MW	https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/unveilingthemask_v1.0.pdf

loads those modules and regularly polls them, sends the results to the remote control server via the interface provided by the network interaction module.

Driver interaction module that represents an interface for the user level "scimap.sys" driver.

Module for network interaction with the remote control server that establishes connection with the network interaction module by means of the above channel specified in the SGH module's configuration information, performs network interaction with the remote control server.

Network interaction module that provides network features to other SGH modules via the above channel.

System information module that collects low-level information on the ITCN (list of files on the disk, base address of

the PE format files created after the specified date, hardware and software platform characteristics).

Registry configuration data management module that creates normalized configuration information for the SGH module that is used by the other modules.

Antivirus protection counteraction module.

Encryption module that provides cryptographic features to the other modules (AES-128, RC4 encryption algorithms).

Compression module that provides compression features to the other modules (LZNT1 compression algorithm).

Keystroke interception module, a keylogger that operates in kernel mode.

File operations interception and content collection module that intercepts file operations, collects information and file contents in accordance with filter rules.

Network traffic interception module that provide network traffic interception facilities.

SGH activity log files storage module that creates two storage files based on the acquired information collected by other modules and saves them in the ITCN activity log in the form of entries with timestamps and text information.

DLL deployment module that registers the function of management of the events of process creation and loading of library into the process space based on loading rules that define the location of the deployed DLL libraries and list of names of the target processes for deployment.

Skype calls interception and recording module that intercepts a number of Skype functions and data while masking itself as a system library.

Nokia mobile devices information collection module that steals information from Nokia mobile devices.

Desktop screenshot creation module that creates desktop screenshots and records the cursor positions.

Wi-Fi networks information collection module that collects information on wireless networks accessible via the Wi-Fi interface of the compromised ITCN.

Electronic mail messages collection module uses the Microsoft Outlook interface and prompts it from the intercepted OLE2 system functions.

SGH malware removal module that completely deletes MW elements from the ITCN.

We shall define the standard certificate of MW activities implementation against ITCN vulnerabilities using the GOST R 56546-2015 (Table 1) and the example of the Careto MW that describes the key features of its operation and recommendations for the elimination of ITCN vulnerabilities.

Subsequently, it is suggested to use the standard MW certificate in investigations of computer incidents and design of adaptive MW detection facilities based on their behavioural analysis as part of a system for computer attack detection, prevention and recovery.

The ITCN fault tolerance model is required to insure the network's functional dependability when affected by MW. It is based on experimental tests of functional analogues of ITCN segments and associated ISF that involved testbed simulation of MW attacks against them. The model consists of a set of indicators defined by formulas (1-5):

1. Probability of ITCN and ISF maintaining the specified probabilistic and temporal characteristics over the MW period:

$$P_M^{ITCN}(t_{MW}) = \left[1 - \prod_{i=1}^{N} P_{MWi}(t_{MW})\right] \sum_{j=1}^{N} P_{ISFj}(t_{MW}) \sum_{k=1}^{N} P_{Ek}(t_{MW}), \quad (1)$$

where t_{MW} is the time of MW action;

P_{MWi} is the probability of i-th successful MW action against ITCN and ISF elements, N is a sequence of natural numbers;

P_{ISFj} is the probability of successful prevention and detection of MW by the j-th ISF element;

P_{Ek} is the probability of successful elimination of the k-th vulnerability in the ITCN and ISF.

2. Probability of recovery of the probabilistic and temporal characteristics of ITCN and ISF affected by MW:

$$P_{rec}^{ITCN}(t_{rec}) = \left\{1 - \prod_{i=1}^{N}\left[1 - S_{ITCNi} e^{-\lambda_{ISF\,i}\, t_{rec}}\right]\right\} \cdot \left\{1 - \prod_{j=1}^{N}\left[1 - S_{ISFj} e^{-\mu_{ISF\,j}\, t_{rec}}\right]\right\}, \quad (2)$$

where t_{rec} is the recovery time of ITCN and ISF characteristics;

S_{ITCN}, S_{ISF} are the weight numbers of [0, …, 1] that characterize the number of sensors in the ITCN and ISF that detected and countered the MW modules;

λ_{ITCN} is the recovery rate of ITCN elements;

μ_{ISF} is the recovery rate of ISF components;

3. The coefficient of ITCN and ISF operational availability to perform specified probabilistic and temporal characteristics under MW at an arbitrary moment in time.

$$K_A^{ITCN} = \frac{t_{ITCN}}{\sum_{i=1}^{N}\left(t_{ITCNi} + t_{fi}^{MW}\right)}, \quad (3)$$

where t_{ITCN} is the time period of ITCN operability;

t_r^{MW} is the period of faults (failures) as the result of MW activity.

4. The mathematical expectation of the MW action time:

$$m_{MW} = \frac{\sum_{i=1}^{N} t_{MWi}}{N_{tot}^{MW}}, \quad (4)$$

where t_{MWi} are the i-th values of MW action time;

N_{tot}^{MW} is the total number of measurements of MW action time as part of testbed simulation.

5. The mathematical expectation of recovery time of the probabilistic and temporal characteristics of ITCN and ISF:

$$m_{rec} = \frac{\sum_{j=1}^{N} t_{recj}^{ITCN} + \sum_{j=1}^{N} t_{recj}^{ISF}}{N_{rec}^{ITCN} + N_{tot}^{ISF}}, \quad (5)$$

where t_{recj}^{ITCN} is the recovery time of the j-th ITCN element;

t_{recj}^{ISF} is the recovery time of the j-th ISF element;

N_{tot}^{ITCN} is the total number of measurements of ITCN elements recovery when affected by MW;

N_{tot}^{ISF} is the total number of measurements of ISF components recovery when affected by MW.

Conclusion

The paper suggests models that allow identifying the general structure of covert deployment and installation of MW using electronic mail, structural and functional diagram of the main MW module and covert deployment modules (using the example of the Careto MW), structural and functional diagram of MW when implementing malicious functions, MW certificate, as well quantifying the probabilistic and temporal characteristics of fault tolerance, recoverability and availability of ITCN affected by MW.

References

1. Levtstov V., Demidov N. Anatomia targetirovannoy ataki [Anatomy of a targeted attack]. Information Security 2016;2:36–39.

2. Zagorsky A.V., Romashkina N.P., editors. Ougrozy informatsionnoy bezopasnosti v krizisakh i konfliktakh XXI veka [Information security threats in the XXI century's crises and conflicts]. Moscow: IMEMO RAS; 2015 [in Russian].

3. Unveiling "Careto" – The Masked APT. Kaspersky Llab's Analytical materials. <https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/unveilingthemask_v1.0.pdf>

4. Klimov S.M., Astrakhov A.V., Sychiov M.P. Metodicheskie osnovy protivodeystvia kompiuternim atakam. Elektronnoye ouchebnoe izdanie [Basic methods of computer attack reaction. Electronic study guide]. Moscow: Bauman MSTU; 2013 [in Russian].

5. Shubinsky I.B. Nadiozhnie otkazoustoychivie informatsionnie sistemy. Metodi sinteza [Dependable failsafe information systems. Synthesis methods]. Ulianovsk: Oblastnaya tipografia Pechatny dvor; 2016 [in Russian].

6. Kapur K., Lamberson L. Reliability in engineering design. Moscow: Mir; 1980.

7. Velichko V.V., Popkov G.V., Popkov V.K. Modeli i metody povyshenia zhivuchesty sovremennykh sistem sviazi [Models and methods of improving the resilience of present day communication systems]. Moscow: Goriachaia linia-Telekom; 2016 [in Russian].

About the author

Sergey M. Klimov, Doctor of Engineering, Professor, Head of Division, 4-th Central Research and Design Institute of the Ministry of Defense of Russia, Korolyov, Russia, e-mail: klimov.serg2012@yandex.ru.

Sergey V. Kupin, Researcher, 4-th Central Research and Design Institute of the Ministry of Defense of Russia, Korolyov, Russia, e-mail: serkup1970@mail.ru.

Dmitry S. Kupin, teacher, Bauman MSTU, Korolyov, Russia, e-mail: t3ft3lb@gmail.com.

Received on 08.06.2017