УДК: 004.056.53
Оригинальная статья
Надежность, том 17, №4, 2017 DOI: 10.21683/1729-2640-2017-17-4-36-43

Модели вредоносных программ и отказоустойчивости информационно-телекоммуникационных сетей

Сергей М. Климов, *4 ЦНИИ Минобороны России, Королёв, Россия*
Сергей В. Купин, *4 ЦНИИ Минобороны России, Королёв, Россия*
Дмитрий С. Купин, *МГТУ им. Н.Э. Баумана, Москва, Россия*

Сергей М. Климов

Сергей В. Купин

Дмитрий С. Купин

Резюме. *Целью статьи является разработка моделей, позволяющих дать типовое представление структуры, функций вредоносных программ и получить количественную оценку отказоустойчивости информационно-телекоммуникационных сетей в условиях воздействий вредоносных программ. В статье показана актуальность и важность моделей вредоносных программ и оценки отказоустойчивости информационно-телекоммуникационных сетей при воздействии на них вредоносными программами. В качестве вредоносных программ рассматриваются комплексы программ, которые обладают свойствами скрытного внедрения, организации несанкционированного виртуального канала передачи данных, самораспространения, самомодификации, несанкционированного сбора информации о сети и информационно-технического воздействия на неё. Разработанная в статье структурно-функциональная модель вредоносных программ образована следующей совокупностью схем и описаний функций: структуры скрытного внедрения и установки вредоносных программ с использованием электронной почты, структурно-функциональной схемой основного модуля вредоносных программ и модулей скрытного внедрения, структурно-функциональной схемой вредоносных программ при реализации вредоносных функций, паспорта вредоносных программ. В схемах подробно описаны типовые функции, порядок работы и информационного взаимодействия модулей вредоносных программ внешней и внутренней сетей через несанкционированный виртуальный канал передачи данных. Основные модули вредоносных программ рассмотрены на примере целевой компьютерной атаки Careto. Модель отказоустойчивости информационно-телекоммуникационных сетей в условиях вредоносных программ описывается показателями, характеризующими способность сетей и соответствующих средств защиты информации сохранять и восстанавливать заданные вероятностно-временные характеристики за период воздействия на них вредоносных программ. В качестве показателей рассмотрены следующие: вероятность сохранения информационно-телекоммуникационных сетей и средств защиты информации заданных вероятностно-временных характеристик за период воздействия вредоносных программ, вероятность восстановления вероятностно-временных характеристик информационно-телекоммуникационных сетей и средств защиты информации после воздействия вредоносных программ, коэффициент оперативной готовности информационно-телекоммуникационных сетей выполнять заданные вероятностно-временные характеристики в условиях вредоносных программ и в произвольный момент времени, математическое ожидание времени воздействия вредоносных программ, математическое ожидание времени восстановления вероятностно-временных характеристик информационно-телекоммуникационных сетей и средств защиты информации. Предполагается, что значения параметров, необходимых для расчета показателей модели отказоустойчивости информационно-телекоммуникационных сетей получены в рамках имитационного моделирования сетей в условиях вредоносных программ на стендовом полигоне. В выводе отмечается, что разработанные модели позволяют определить общую структуру скрытного внедрения и установки атакующих вредоносных программ с использованием электронной почты, структурно-функциональную схему основного модуля вредоносных программ и модулей скрытного внедрения, структурно-функциональную схему вредоносных программ при реализации вредоносных функций, паспорт вредоносных программ, а также оценить отказоустойчивость информационно-телекоммуникационных сетей и средств защиты информации в условиях воздействия вредоносных программ, количественно оценить вероятностно-временные показатели отказоустойчивости, восстанавливаемости и готовности сетей.*

Ключевые слова: *вредоносные программы, информационно-телекоммуникационные сети, средства защиты информации, отказоустойчивость.*

Формат цитирования: *Климов С.М., Купин С.В., Купин Д.С. Модели вредоносных программ и отказоустойчивости информационно-телекоммуникационных сетей // Надежность. 2017. № 4. С. 36-43. DOI: 10.21683/1729-2640-2017-17-4-36-43*

Введение

В настоящее время наибольшую угрозу представляют целевые компьютерные атаки, организованные нарушителями с использованием скрытно внедряемых и самораспространяемых вредоносных программ (ВП). Данные программы не всегда оперативно выявляются современными средствами защиты информации (СЗИ), такими как средства антивирусной защиты, обнаружения, предупреждения и ликвидации последствий компьютерных атак. Как правило, нарушители используют уязвимости «нулевого дня» в значительных объемах программ операционных систем (ОС), сетевых сервисов и протоколов для скрытного внедрения элементов ВП в информационно-телекоммуникационные сети (ИТКС).

Под ВП будем понимать комплекс программ для организации скрытного внедрения, создания несанкционированных виртуальных каналов передачи данных, самораспространения, самомодификации и реализации целенаправленных и массированных информационно-технических воздействий (компьютерных атак) на ИТКС с целью нарушения безопасности информации и устойчивости функционирования.

Комплексы ВП обладают сложной для анализа программной реализацией, используют для разработки и выполнения существенные информационные ресурсы, в них нашли применение алгоритмы сжатия, шифрования и маскирования деструктивных действий. Современные целевые массированные компьютерные атаки, например, WannaCry в 2017 году, с использованием ВП охватывают сотни тысяч компьютеров по всему миру и нарушают устойчивость функционирования ИТКС в банковской сфере, энергетике, медицине, связи, транспорте и других критически важных областях жизнедеятельности [1-2].

В данной статье предложена структурно-функциональная модель ВП, которая разработана на примере анализа программного кода целевой компьютерной атаки Careto, приведенного в аналитических материалах Лаборатории Касперского [3]. Кроме того, в статье осуществляется интерпретация типовой модели структуры и функций для широкого класса ВП.

Средства ВП Careto позволили нарушителям поразить 380 уникальных объектов в 31 стране. С использованием ВП Careto нарушители похищали сведения о средствах вычислительной техники, закрытые ключи шифрования, настройки виртуальных частных сетей VPN, ключи закрытых протоколов передачи данных SSH, файлы RDP, а также файлы различных форматов данных. Как правило, внедрение ВП осуществляется через сеть Интернет, соответствующее коммуникационное оборудование ИТКС и несанкционированное подключение внешних электронных носителей информации [3].

Комплекс ВП Careto устанавливается в сети с помощью модуля установки и обеспечивает нарушителю удаленный доступ к ИТКС, скрытно от пользователя, а также выполнение набора команд, поступающих от сервера удаленного управления, для сбора сведений о сети, уязвимых сервисах и хранимой информации. В случае успешного проникновения в ИТКС модуль установки ВП Careto извлекает необходимые компоненты для корректного функционирования ВП Careto и последующего развертывания в сети.

По сути ВП Careto и подобные ей программы обусловливают возникновение в ИТКС компьютерных инцидентов двух типов:

1. Проникновение и организация несанкционированного, виртуального и скрытного канала сбора, передачи и обработки информации об ИТКС.

2. Скрытное развертывание элементов ВП в ИТКС и реализация целенаправленного и массированного воздействия.

Целенаправленные и массированные воздействия ВП на уязвимости ИТКС приводят к практически мгновенному (при передаче данных по волоконно-оптическим линиям связи) нарушению устойчивости функционированию элементов ИТКС даже при наличии СЗИ.

Для обеспечения устойчивости функционирования ИТКС в условиях ВП необходимо разработать модели, которые определят типовые структуры и функции ВП, позволят их реализовать в виде имитационной модели на стендовом полигоне [4] и получить количественную оценку устойчивости ИТКС в условиях деструктивных воздействий [5 – 7].

Имитационные модели ИТКС позволят воспроизвести наиболее критические ко времени регламенты и технологические циклы управления, а модели СЗИ – отработать соответствующие функции средств защиты информации от ВП. Наиболее рационально стендовые полигоны для тестирования и проверки ИТКС в условиях ВП реализовать в виде совокупности центров обработки данных, информационных систем на базе виртуальных машин, имитаторов ВП взаимосвязанных сетевым коммуникационным оборудованием.

Под отказоустойчивостью ИТКС будем понимать способность сети и СЗИ обеспечивать установленные регламенты выполнения технологических циклов управления (вероятностно-временные характеристики) в условиях воздействия ВП на заданном интервале времени.

Наличие потенциальных уязвимостей в современных ИТКС обусловливает возможность внедрения в них ВП и реализации деструктивных воздействий, приводящих к нарушению устойчивости функционирования. Поэтому разработка моделей, позволяющих формализовать структуру и процесс работы ВП, оценить отказоустойчивость ИТКС в условиях воздействия ВП, является актуальной.

Постановка задачи

В рамках статьи разработаны:

1. Структурно-функциональная модель ВП, включающая следующие компоненты:

- общую структуру комплекса ВП;

- структуру скрытного внедрения и установки ВП с использованием электронной почты;

- структурно-функциональная схема основного модуля ВП (Careto) и модулей скрытного внедрения (SGH, SBD);

- структурно-функциональную схему модуля ВП (SGH), описывающую основные функциональные возможности комплекса ВП;

- паспорт ВП.

2. Модель отказоустойчивости ИТКС в условиях ВП, которая основана на экспериментальных испытаниях сегментов ИТКС и соответствующих СЗИ при имитации воздействия на них ВП.

На рисунке 1 представлена общая структура ВП, компоненты которых распределены во внешней, внутренней сети и взаимодействуют через несанкционированный виртуальный канал передачи данных (информационный канал созданный средствами нарушителя). Известны реализации кода ВП Careto для 32-х и 64-х разрядных версий операционных систем (ОС) Windows и Linux, а других типов ВП – и для мобильных приложений Android и Apple iOS [1, 3].

В структуре ВП предусмотрены внешние средства управления внедренными во внутреннюю сеть модулями на основе применения сервера управления ВП и модуля доставки (ретрансляции) и информационного взаимодействия ВП. Внедренные в ИТКС модули ВП осуществляют сбор данных о сетевой конфигурации (доступных IP, MAC-адресах и номерах портов коммуникационного оборудования), типе операционной системы и СЗИ, перехватывают информацию с экрана (графические изображения экрана рабочего стола пользователя), клавиатуры и носителей, подключенных к компьютерам. Модуль доставки осуществляет выдачу команд управления для выполнения деструктивных функций внедренными во внутреннюю сеть модулями, а затем ретранслирует собранную информацию на сервер управления ВП и заносит её в базу данных. На сервере ВП предусмотрена возможность реализации атакующих функций компьютерных атак на ИТКС путем выбора из соответствующей базы данных и отправки кода специальных программ эксплойтов на уязвимости внутренней поражаемой сети. Кроме того, ВП может использовать различные инструменты из проекта Metasploit Framework, в том числе для повышения привилегий ВП в операционной системе.

Во внутренней сети функционируют следующие основные модули ВП:

1. Модули скрытного внедрения (драйверы загрузки) и взаимодействия элементов ВП между собой, которые включают в свой состав средства получения первоначального доступа к элементам ИТКС, скрытной загрузки в операционную систему и обхода СЗИ, а также интерфейсные программы организации информационного взаимодействия с внешней сетью и между модулями внутренней сети.

2. Модули скрытного самораспространения ВП в ИТКС, представляющие собой программные средства

Общая структура атакующих вредоносных программ
(*на примере ВП «Careto» 380 заражений в 31 стране*)

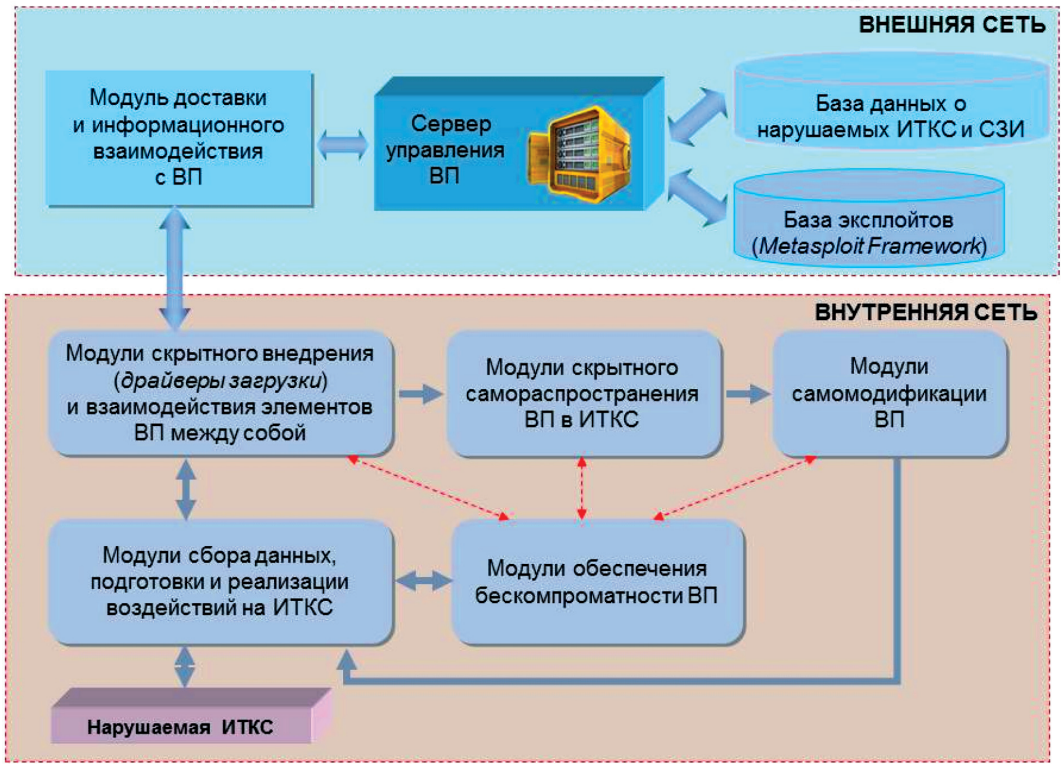

Рисунок – 1. Общая структура комплекса ВП

Рисунок – 2. Структура скрытного внедрения и установки ВП с использованием электронной почты

работы с привилегиями системного администратора, средства загрузки, обеспечивающие перехват прерываний операционной системы, скрытый переход к исполнению кода ВП и приоритетное навязывание выполнения его функций.

3. Модули сбора данных, подготовки и реализации воздействий на ИТКС, сущность работы которых заключается в функционировании множества программ-имплантов, перехватывающих проводной и беспроводный сетевой трафик, нажатия клавиш, сеансы и ключи при работе программ, извлекающих информацию из компьютерного оборудования, сохраняющих снимки экрана и контролирующих операции с файлами. Вредоносный модуль формирует необходимые для воздействия исходные данные об инфицированной ИТКС, обеспечивает развертывание остальных компонентов комплекса ВП и доводит код компьютерной атаки до поражаемых элементов ИТКС.

4. Модули самомодификации ВП являются программными компонентами, обеспечивающими адаптацию ВП к параметрам аппаратно-программной среды нарушаемой ИТКС путем извлечения и развертывания программ, необходимых для организации канала несанкционированного подключения к сети, версиям ОС, а также направления запроса к серверу ВП с исходными данными для дополнительных вредоносных модулей.

5. Модули обеспечения бескомпроматности ВП – совокупность модулей скрытия действий ВП путем использования ложных сертификатов программного обеспечения и электронной подписи, шифрования вну-

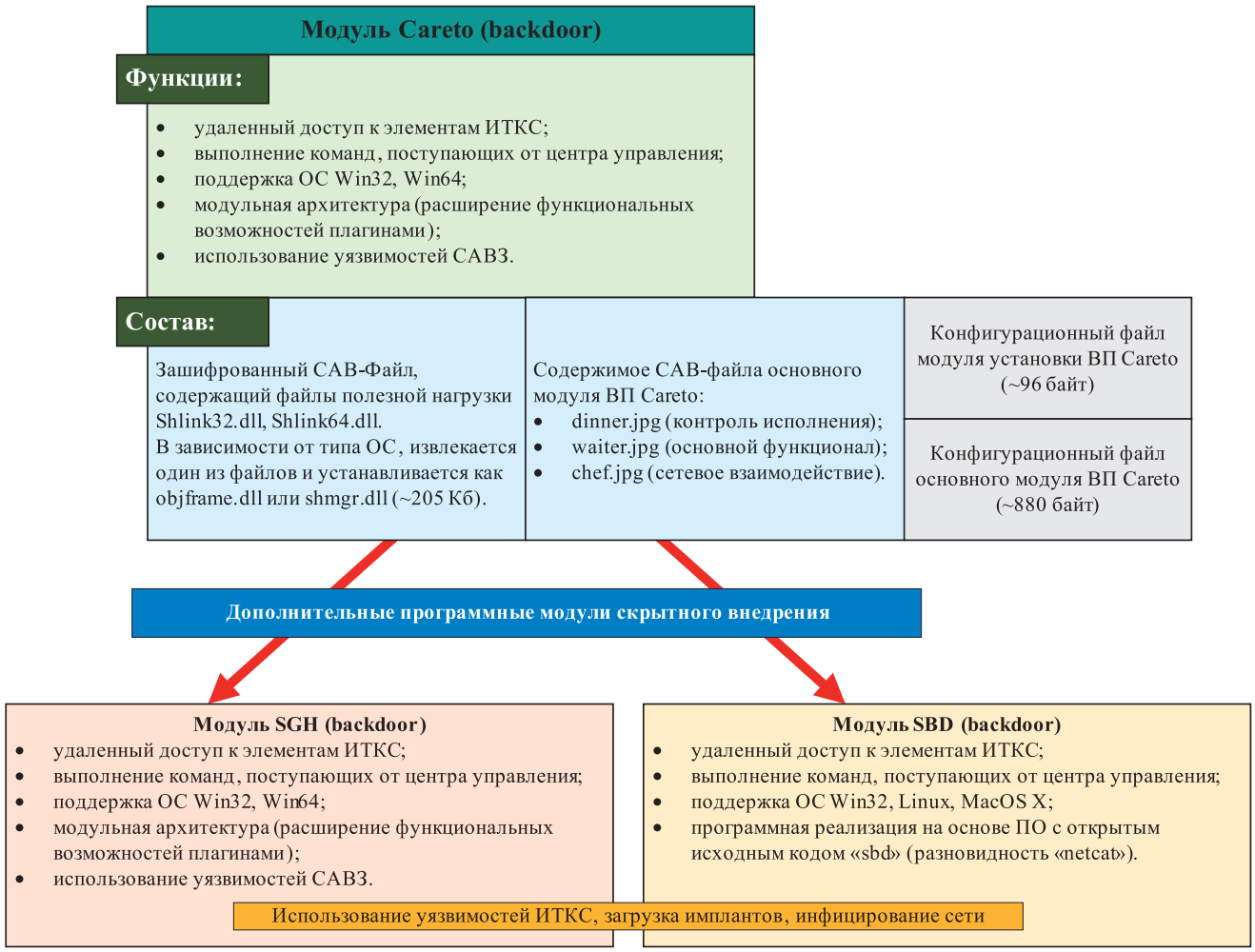

Рисунок – 3. Структурно-функциональная схема основного модуля ВП и модулей скрытного внедрения (на примере ВП Careto)

треннего и внешнего трафика, уничтожения следов ВП в файлах и памяти компьютерных устройств.

На рисунке 2 приведена структура скрытного внедрения и установки ВП с использованием электронной почты.

Скрытное внедрение, самораспространение и установка ВП осуществляется следующим образом. Нарушитель подготавливает фишинговое сообщение электронной почты, которое содержит ссылку на вредоносный сетевой ресурс. В результате открытия ссылки пользователем происходит внедрение ВП в открытый сегмент ИТКС. Затем пользователя перенаправляют на абсолютно легитимный сетевой ресурс с целью сокрытия факта компрометации системы.

Для маскировки ВП нарушители используют поддомены, основанные на вредоносных сетевых ресурсах. Данный механизм маскировки нацелен на то, что, если сетевое имя ресурса очень длинное, то браузер обрезает название с конца, оставляя название поддомена.

Далее путем использования файла-сценария сбора информации о поражаемых целях в ИТКС производится подготовка данных об уязвимостях и доступных для нарушения информационных ресурсах. Например, используются уязвимости в продуктах Adobe Flash (код уязвимости CVE-2012-0773) и Java (код уязвимости CVE-2011-3544). На основе собранной в ИТКС информации выбирается из базы данных необходимая программа эксплойт и загружается под видом расширения для определенного браузера. Затем они ретранслируются в ИТКС для установки ВП класса бэкдор (backdoor). После успешной компрометации ИТКС пользователь перенаправляется на легитимный сетевой ресурс, например, новостной портал.

Предполагается, что в ходе проникновения содержимого вредоносного сообщения электронной почты в ИТКС ему удается обойти стандартные СЗИ. Нарушитель указывает уникальную ссылку на определенный эксплойт и отправляет её пользователю в фишинговом письме, который сам его загружает. Для маскирования ссылок на эксплойты, ссылки укорачиваются с помощью определенных сервисов.

Структурно-функциональная схема основного модуля ВП и модулей скрытного внедрения (на примере ВП Careto) приведена на рисунке 3. Как можно заметить из рисунка 3, основу ВП Careto составляют основной модуль Careto, осуществляющий первоначальное внедрение в ИТКС, и модули организации несанкционированных каналов передачи данных, скрытного распространения и реализации информационно-технического воздействия SGH и SBD.

На рисунке 4 представлена структурно-функциональная схема модуля ВП SGH, описывающая основные функциональные возможности комплекса ВП. Данный тип ВП представляет собой один из модулей сбора

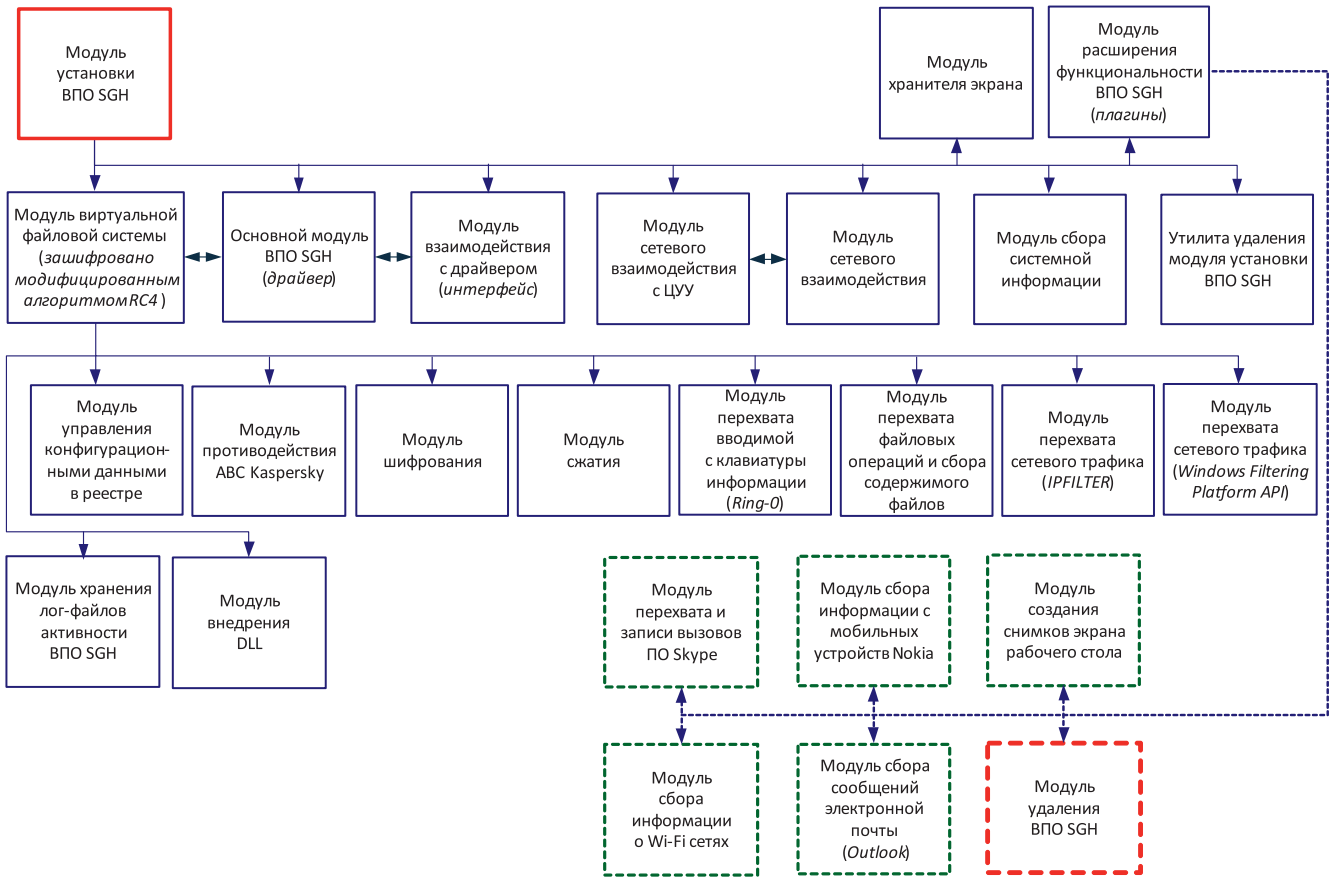

Рисунок – 4. Структурно-функциональная схема модуля ВП (SGH), описывающая основные функциональные возможности комплекса ВП

данных, подготовки и реализации воздействий на ИТКС класса бэкдор (backdoor). Этот модуль предоставляет скрытный и удаленный доступ нарушителю к ИТКС, выполняет различные команды, поступающие от сервера удаленного управления ВП. Ввиду того, что ВП Careto обладает функционалом загрузки дополнительных ВП SGH и SBD, можно заключить, что структурно-функциональная схема, а также описание модулей ВП SGH полностью характеризуют вредоносные функции целого комплекса ВП Careto.

Основные вредоносные функции ВП на примере модуля SGH ВП Careto представим описанием функций его составных модулей следующими образом:

Модуль хранителя экрана – ожидает, когда станет доступным рабочий стол с именем «screen-saver», и затем создаёт другой рабочий стол со своим именем, загружает браузер по умолчанию. Функция «DllEnumClass» удаляет модуль хранителя экрана или удаляет его имя из конфигурационной информации, в зависимости от версии ОС Windows.

Модуль расширения функциональности – считывает список дополнительных модулей SGH из конфигурационной информации, загружает эти модули и периодически опрашивает, результаты отправляет на сервер удаленного управления через интерфейс, который обеспечивает модуль сетевого взаимодействия.

Модуль взаимодействия с драйвером – представляет собой интерфейс для работы с драйвером «scsimap.sys» пользовательского уровня.

Модуль сетевого взаимодействия с сервером удаленного управления – устанавливает соединение с модулем сетевого взаимодействия, используя именованный канал, указанный в конфигурационной информации модуля SGH, осуществляет сетевое взаимодействие с сервером удаленного управления.

Модуль сетевого взаимодействия – предоставляет сетевые функции другим модулям SGH через именованный канал.

Модуль сбора системной информации – представляет собой сборщик низкоуровневой информации об ИТКС (список файлов на диске, базовый адрес файлов PE формата, созданных после указанной даты, характеристики аппаратно-программной платформы).

Модуль управления конфигурационными данными в реестре – формирует унифицированную конфигурационную информацию модуля SGH, которая используется остальными модулями.

Модуль противодействия средствам антивирусной защиты – использует уязвимости в старых версиях антивирусного ПО (например, Kaspersky Workstation 6.0.4 и KAV/KIS 8.0 – уязвимости устранены в 2008 г.) с целью обеспечения скрытного функционирования на ИТКС.

Модуль шифрования – предоставляет криптографические функции другим модулям (алгоритмы шифрования AES-128, RC4).

Модуль сжатия – предоставляет функции сжатия другим модулям (алгоритм сжатия LZNT1).

Модуль перехвата вводимой с клавиатуры информации – представляет собой перехватчик клавиатуры (кейлоггер), работающий в режиме ядра.

Модуль перехвата файловых операций и сбора содержимого файлов – перехватывает операции с файлами, собирает информацию и содержимое файлов в соответствии с правилами фильтрации.

Модуль перехвата сетевого трафика – модули предоставляют средства перехвата сетевого трафика.

Модуль хранения лог-файлов активности SGH – создаёт два файла-хранилища на основе получения информации, собранной другими модулями и сохраняет их в журнале активности ИТКС в форме записей с метками времени и текстовой информацией.

Модуль внедрения DLL – регистрирует функцию для обработки событий создания процесса и загрузки библиотеки в адресное пространство процесса с использованием правил загрузки, которые определяют расположение внедряемых библиотек DLL и список имен процессов-целей для внедрения.

Модуль перехвата и записи вызовов программы Skype – перехватывает ряд функций и данных программы Skype, маскирует себя под системную библиотеку.

Модуль сбора информации с мобильных устройств Nokia – похищает информацию с мобильных устройств Nokia.

Модуль создания снимков экрана рабочего стола – создает снимки рабочего стола и отмечает расположение курсора мыши.

Модуль сбора информации о Wi-Fi сетях – собирает информацию о беспроводных сетях, доступных интерфейсу Wi-Fi скомпрометированной ИТКС.

Модуль сбора сообщений электронной почты – использует интерфейс программы Microsoft Outlook и запрашивает его из перехваченных системных функций OLE2.

Модуль удаления вредоносных программ SGH – полностью удаляет элементы ВП из ИТКС.

Типовой паспорт реализации угроз ВП на уязвимые места в ИТКС определим с использованием ГОСТ Р 56546-2015 (таблица 1) на примере ВП Careto, описывающий ключевые моменты его функционирования и рекомендации по устранению уязвимостей ИТКС.

В дальнейшем типовой паспорт угроз ВП предлагается использовать для расследования компьютерных инцидентов и построения адаптивных средств обнаружения ВП на основе их поведенческого анализа в рамках функционирования системы обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Модель отказоустойчивости ИТКС необходима для обеспечения её функциональной надежности в условиях воздействия ВП, основана на экспериментальных испытаниях функциональных аналогов сегментов ИТКС и соответствующих СЗИ при имитации воздействия на них ВП на стендовом полигоне. Модель представляется совокупностью показателей, определенных выражениями (1 – 5):

Таблица 1 – Типовой паспорт угроз ВП

Элементы описания ВП	Описание ВП
Наименование	Careto
Тип	бэкдор, модульный
Дата обнаружения	2014
Краткое описание	ВП скрытно внедряется и предоставляет нарушителю удаленный доступ к ИТКС, выполняет различные команды, поступающие из сервера удаленного управления
Объект ВП	государственные учреждения и коммерческие организации
Степень опасности	высокая
Структура ВП	- модуль установки; - основной модуль; - модуль сетевого взаимодействия с центром удаленного управления; - функциональный модуль; - модуль контроля исполнения функционального и сетевого модуля; - модуль удаления; - модуль сбора системной информации и аутентификационных данных (возможна загрузка дополнительных модулей из центра удаленного управления).
Основные функциональные возможности	- файл конфигурации и файл полезной нагрузки (payload) зашифрованы модифицированным алгоритмом RC4; - закрепление в автозагрузке в качестве COM-объекта; - внедрение вредоносного кода в процессы explorer.exe, iexplore.exe, firefox.exe, chrome.exe; - перезапись кодовой секции системных библиотек; - безопасное закрытие обработчиков процесса работы модулей; - прием и передача данных шифруется алгоритмами AES и RSA; - запуск исполняемых файлов с определенными аргументами; - получение CAB-файла, извлечение из него файла и последующий запуск с определенными аргументами; - извлечение исполняемого модуля из CAB-файла и последующий запуск в памяти; - изменение конфигурационного файла, смена сервера удаленного управления; - сбор информации об ИТКС и передача на сервер удаленного управления; - полное удаление ВП из ИТКС.
Индикаторы компрометации ИТКС	**(Файлы, фрагмент)** %AppData%\Microsoft\objframe.dll|shmgr.dll|Shlink(32|64).dll **(Реестр, фрагмент)** [HKLM\Software\Classes\CLSID\{E6BB64BE-0618-4353-9193-0AFE606D6F0C}\Inproc-Server32] = «%System%\browseui.dll» **(Сети, фрагмент)** hxxp://202.75.58.153/cgi-bin/commcgi.cgi Поле User-Agent: Mozilla/4.0 (compatible; MSIE 4.01; Windows NT)
Способ обнаружения	**(Средства антивирусной защиты, фрагмент)** Kaspersky: Trojan.Win32|Win64.Careto.*
Возможные меры по устранению	- переустановка ОС и форматирование носителей информации; - проведение ручной проверки индикаторов компрометации ИТКС (элементы автозагрузки, сетевое взаимодействие, активность файловой системы, анализ лог-файлов ОС); - обновление средств антивирусной защиты и проведение полной проверки ИТКС.
Сведения о ВП	https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/unveilingthemask_v1.0.pdf

1. Вероятностью сохранения ИТКС и СЗИ заданных вероятностно-временных характеристик за период воздействия ВП:

$$P_{\text{С}}^{\text{ИТКС}}(t_{\text{ВП}})=\left[1-\prod_{i=1}^{N}P_{\text{ВП}i}(t_{\text{ВП}})\right]\sum_{j=1}^{N}P_{\text{СЗИ}j}(t_{\text{ВП}})\sum_{k=1}^{N}P_{\text{У}k}(t_{\text{ВП}}), \quad (1)$$

где $t_{\text{ВП}}$ – время воздействия ВП;

$P_{\text{ВП}i}$ – вероятность i-го успешного воздействия ВП на элементы ИТКС и СЗИ, N – ряд натуральных чисел;

$P_{\text{СЗИ}j}$ – вероятность успешного предупреждения и обнаружения ВП j-м элементом СЗИ;

$P_{\text{У}k}$ – вероятность успешного устранения k-й уязвимости в ИТКС и СЗИ.

2. Вероятностью восстановления вероятностно-временных характеристик ИТКС и СЗИ после воздействия ВП:

$$P_{\text{вос}}^{\text{ИТКС}}\left(t_{\text{вос}}\right)=\left\{1-\prod_{i=1}^{N}\left[1-S_{\text{ИТКС}i}e^{-\lambda_{\text{ИТКС}i}t_{\text{вос}}}\right]\right\}\cdot$$

$$\cdot\left\{1-\prod_{j=1}^{N}\left[1-S_{\text{СЗИ}j}e^{-\mu_{\text{СЗИ}j}t_{\text{вос}}}\right]\right\}, \quad (2)$$

где $t_{\text{вос}}$ – время восстановления ИТКС и СЗИ;

$S_{\text{ИТКС}}$, $S_{\text{СЗИ}}$ – весовые коэффициенты, имеющие значения [0, …, 1] и характеризующие количество сенсоров в ИТКС и СЗИ, которые выявили и противодействовали модулям ВП;

$\lambda_{\text{ИТКС}}$ – интенсивность восстановления элементов ИТКС;

$\mu_{\text{СЗИ}}$ – интенсивность восстановления компонент СЗИ.

3. Коэффициентом оперативной готовности ИТКС и СЗИ выполнять заданные вероятностно-временные характеристики в условиях воздействия ВП и в произвольный момент времени:

$$K_{\text{Г}}^{\text{ИТКС}}=\frac{t_{\text{ИТКС}}}{\sum_{i=1}^{N}\left(t_{\text{ИТКС}i}+t_{\text{сб}i}^{\text{ВП}}\right)}, \quad (3)$$

где $t_{\text{ИТКС}}$ – период времени работоспособного состояния ИТКС;

$t_{\text{сб}}^{\text{ВП}}$ – период сбоев (отказов) в результате воздействия ВП.

4. Математическим ожиданием времени воздействия ВП:

$$m_{\text{ВП}}=\frac{\sum_{i=1}^{N}t_{\text{ВП}i}}{N_{\text{общ}}^{\text{ВП}}}, \quad (4)$$

где $t_{\text{ВП}i}$ – i-е значения времени воздействия ВП;

$N_{\text{общ}}^{\text{ВП}}$ – суммарное количество измерений времени воздействия ВП в ходе имитационного моделирования на стендовом полигоне.

5. Математическим ожиданием времени восстановления вероятностно-временных характеристик ИТКС и СЗИ:

$$m_{вос}=\frac{\sum_{j=1}^{N}t_{\text{вос}j}^{\text{ИТКС}}+\sum_{j=1}^{N}t_{\text{вос}j}^{\text{СЗИ}}}{N_{\text{общ}}^{\text{ИТКС}}+N_{\text{общ}}^{\text{СЗИ}}}, \quad (5)$$

где $t_{\text{вос}j}^{\text{ИТКС}}$ – время восстановления j-го элемента ИТКС;

$t_{\text{вос}j}^{\text{СЗИ}}$ – время восстановления j-го компонента СЗИ;

$N_{\text{общ}}^{\text{ИТКС}}$ – суммарное количество измерений времени восстановления элементов ИТКС в условиях воздействия ВП;

$N_{\text{общ}}^{\text{СЗИ}}$ – суммарное количество измерений времени восстановления компонент СЗИ в условиях воздействия ВП.

Заключение

В статье предложены модели, которые позволяют определить общую структуру скрытного внедрения и установки ВП с использованием электронной почты, структурно-функциональную схему основного модуля ВП и модулей скрытного внедрения (на примере ВП Careto), структурно-функциональную схему ВП при реализации вредоносных функций, паспорт ВП, а также количественно оценить вероятностно-временные показатели отказоустойчивости, восстанавливаемости и готовности сетей ИТКС в условиях воздействия ВП.

Библиографический список

1. Анатомия таргетированной атаки. В. Левцов, Н. Демидов. Журнал «Information Security/ Информационная безопасность» № 2, 2016. – с. 36 – 39.

2. Угрозы информационной безопасности в кризисах и конфликтах XXI века / Под ред. А.В. Загорского, Н.П. Ромашкиной – М.:ИМЭМО РАН, 2015. – 151 с.

3. Сорванная «Маска» – замаскированный APT. Аналитические материалы Лаборатории Касперского. https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/unveilingthemask_v1.0.pdf

4. Климов С.М., Астрахов А.В., Сычев М.П. Методические основы противодействия компьютерным атакам. Электронное учебное издание. – М.: МГТУ имени Н.Э. Баумана, 110 с, 2013.

5. Шубинский И.Б. Надежные отказоустойчивые информационные системы. Методы синтеза/ И.Б. Шубинский. – Ульяновск: Областная типография «Печатный двор», 2016. – 544 с., ил. – («Журнал надежность»).

6. К. Капур, Л. Ламберсон. Надежность и проектирование систем. Под ред. И.А. Ушакова. Пер. с англ. – М.: «Мир», 1980. – 604 с., ил.

7. Величко В.В., Попков Г.В., Попков В.К. Модели и методы повышения живучести современных систем связи. – М.: Горячая линия – Телеком, 2016. – 270 с.: ил.

Сведения об авторах

Сергей М. Климов – доктор технических наук, профессор, начальник управления 4 ЦНИИ Минобороны России, Королёв, Россия, e-mail: klimov.serg2012@yandex.ru.

Сергей В. Купин – научный сотрудник 4 ЦНИИ Минобороны России, Королёв, Россия, e-mail: serkup1970@mail.ru.

Дмитрий С. Купин – преподаватель МГТУ им. Н.Э. Баумана, Королёв, Россия, e-mail: t3ft3lb@gmail.com.

Поступила 08.06.2017