УДК 004.056

СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ ВРЕДОНОСНЫХ ПРОГРАММ, ФУНКЦИОНИРУЮЩИХ ДО ЗАГРУЗКИ ОПЕРАЦИОННОЙ СИСТЕМЫ

Аспирант каф. ИУ8 Кубарев А.В.
Московский государственный технический университет им.Н.Э.Баумана

Одним из способов обеспечения скрытности функционирования вредоносных программ (ВП) является загрузка и исполнение кода на этапе, предстоящем загрузке операционной системы. ВП, обладающие указанными возможностями принято называть «буткитами» (bootkit) [1].

Поскольку в процессе функционирования буткиты реализуют «полезную нагрузку», имеются некоторые демаскирующие признаки их деятельности. Так как ВП часто предназначены для сокрытия различных сущностей на пользовательском уровне или на уровне операционной системы, возможно производить сравнение доступных сущностей на одном из этих уровней и на дополнительном уровне (например, получить представление процессов на аппаратном уровне и сравнить его с представлением на операционном уровне). По результатам сравнения представлений разных уровней, можно сделать вывод о наличии буткита. Часто буткитами применяются методы перехвата системных функций (изменение поведения какой-либо системной функции путём подмены указателя на какой-либо ресурс или функцию), которые возможно проследить путем анализа различных областей памяти. Также ВП используются для удаленного управления СВТ или создания бот-сетей, что всегда сопровождается изменением объема трафика, а также увеличением расходования ресурсов СВТ. Наличие указанных признаков может быть показателем функционирования буткита.

Таким образом, для определения факта функционирования буткита возможно применять следующие методы: сравнительный анализ представлений, анализ сетевого трафика, анализ расходования ресурсов СВТ, анализ различных областей памяти СВТ [2,3].

Литература

1. Гарнаева, М.А. Kaspersky Security Bulletin 2013. Вопросы кибербезопасности / М.А. Гарнаева, К. Функ – 2014. № 3 (4). С. 65-68

2. Марков, А.С. Организационно-технические проблемы защиты от целевых вредоносных программ типа Stuxnet / А.С. Марков, А.А. Фадин // Вопросы кибербезопасности – 2013. № 1 (1). С. 28-36.

3. Барабанов, А.В. Моделирование угроз безопасности информации, связанных с функционированием скрытых вредоносных компьютерных программ / А.В. Барабанов, М.И. Гришин, А.В. Кубарев // Вопросы кибербезопасности – 2013. № 1 (1). С. 28-36.