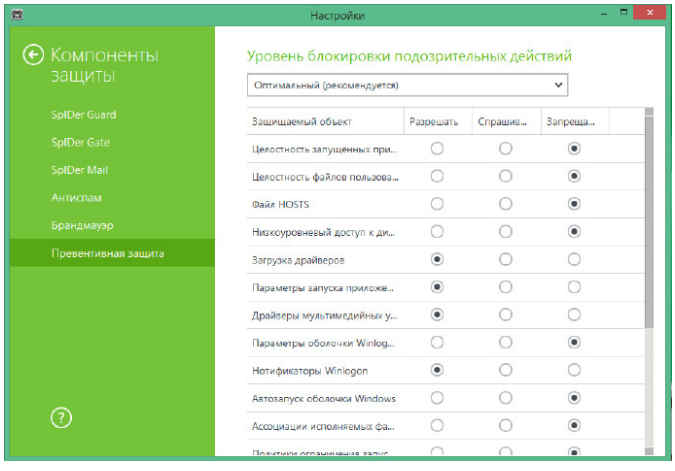
Dr.Web: Страж SpIDerGate никогда не дремлет

Средняя розничная цена: от 1290 руб.
Сайт: drweb.ru

Целью сетевых злоумышленников современности — киберпреступников, интернет-мошенников, хакеров — зло многолико, являются деньги. Романтичные времена героев-хакеров остались в прошлом. Не таком далеком, но, увы, прошлом. В борьбе за деньги все средства хороши. Можно, конечно, по старинке взломать компьютер и заразить его. Да, так делают и сейчас — форумы на хакерских ресурсах переполнены постами на эту тему. Но много ли возьмешь с одной машины, и гарантирован ли успех и доход? А вдруг атаку заметят бдительные специалисты?

Гораздо проще и выгоднее взломать посещаемый сайт и заразить его вирусом или создать поддельный ресурс, имитирующий настоящий, и заманить на него потенциальных жертв. Например, разослав фишинговое письмо от имени реальной компании и поместив в это письмо ссылку на сайт мошенников.

Первой преградой на пути вирусов становится компонент, который анализирует поступающий на компьютер трафик прежде, чем он поступит в какое-либо приложение. В случае Dr.Web такой компонент называется веб-антивирусом SpIDerGate. Мало кто знает, что две заглавные буквы в середине слова означают инициалы автора антивируса.



Превентивная защита

Набор специальных запретительных мер позволяет организовать на ПК мощный бастион на пути вирусов и хакеров

Естественно, злоумышленники понимают, что присутствие их «творения» нежелательно на компьютере или смартфоне, и стремятся обойти преграду в виде антивируса. Как это сделать? Естественно, использовать в этих целях самого пользователя!

Великий комбинатор знал 400 «сравнительно честных способов отъема денег». Современные злоумышленники каждый день изобретают новые. Большинство пользователей, к сожалению, работают, не ограничивая себя и своих близких в возможности установки новых программ. Поэтому уже давно классикой стал случай, когда злоумышленник на сайте или в ходе телефонного разговора (такой вид мошенничества именуется вишингом) рекомендует отключить антивирус («кряк надежный, но на него ругается вебер, поэтому отключите его перед установкой»).

Пиратство и доверчивость — ворота для вирусов

Если не использовать никаких средств защиты, можно стать легкой добычей киберзлоумышленников. Мошенники очень любят ссылки. Само сообщение может выглядеть как реклама товара, просьба о помощи или уведомление о налоговой проверке. Но в письме или приложенном к нему файле будет ссылка. Иногда совпадающая с доменом отправителя письма, а иногда и нет. Мошенники составляют тексты писем с использованием психологии потенциальных жертв. Изображения, шрифт, его размер и цвет тщательно подбираются с учетом приемов воздействия на эмоции получателя. Само письмо может быть вполне безвредно – и потому легко обманет антиспам фильтр. Но «клик» по ссылке ни к чему хорошему не приведет.

И на страже снова встанет SpIDerGate, а точнее — та его часть, которая анализирует ресурсы Сети на принадлежность к заведомо вредоносным. И, наведя курсор на картинку или ссылку, можно будет увидеть сообщение blocked, что означает, что ваш страж не дремлет.

Большинство потенциальных жертв до сих пор думают, что они смогут заметить факт заражения. Поэтому для них большим сюрпризом становится появление на экране сообщения с предложением о выкупе собственных данных.