Цель хакеров

ВЯЧЕСЛАВ МЕДВЕДЕВ

В истории войн был период, когда для завоевания территории нужно было захватить расположенные на ней города. Изобретались все новые типы осадных орудий, рылись подкопы, подкупались предатели. А потом некто умный сообразил, что города эти не так уж и нужны — можно просто оставить их в осаде и в свое удовольствие пользоваться ресурсами, расположенными вне их границы. А горожане, чувствующие себя неуязвимыми внутри красивых стен, рано или поздно сами затащат к себе троянского коня — ибо нет пределов непослушанию и любопытству.

Тенденцией нынешнего года для мира компьютеров стал возросший интерес злоумышленников к никем не защищенным местам. Установка антивируса пользователями на свои рабочие и домашние машины давно стала обязательным делом ("у всех есть, и я поставил"). Но при этом меры по защите всего того, что не является рабочими станциями да еще файловыми серверами, предпринимаются крайне редко. И у хакеров созрела вполне логичная мысль, что штурмовать априори защищенный пункт, конечно, можно — но насколько проще внедриться туда, где угрозы никто не ждёт.

Linux? Система, по мнению почти всех ее приверженцев, написанная профессионалами, неуязвимость которой обеспечивается открытостью кода — "дыру" в программе просто невозможно скрыть! Но не так давно были найдены существовавшие многие годы уязвимости Heartbleed и Shellshock (желающие сравнить количество выявленных в этом году уязвимостей хотя бы с прошлогодними показателями могут воспользоваться любой поисковой системой). Shellshock, например, позволяет злоумышленникам выполнять произвольные команды на инфицированных устройствах, операционные системы которых основаны на ядре Linux и имеют в своем составе оболочку Bash. Такими устройствами могут быть серверы, модемы, роутеры, камеры наблюдения и масса других подключенных к Интернету аппаратных средств со встроенными операционными системами, причем ПО для многих из них практически не обновляется. На что, естественно, вирусописатели отреагировали мгновенно: в самом конце сентября были выявлены бэкдоры, атакующие Linux-устройства, — Linux.BackDoor.Shellshock.1 и Linux.BackDoor.Shellshock.2.

При этом если раньше вредоносные программы портировались на Linux, то китайские вирусописатели, отметившиеся в первой половине лета распространением огромного количества троянцев для Linux, созданных с целью организации массированных DDoS-атак, пошли иным путем, выпустив Trojan.DnsAmp.1 — Windows-совместимую версию одного из троянцев Linux.DnsAmp. После запуска Trojan.DnsAmp.1 отправляет на серверы злоумышленников информацию об инфицированном компьютере и ожидает команды, когда начинать DDoS-атаку. Помимо этого троянец может загрузить и запустить на исполнение другую вредоносную программу.

Mac OS X? Продукт культовой компании, предмет желания и подражания для многих. Только за сентябрь вирусные базы Dr.Web пополнились информацией о бэкдоре Mac.BackDoor.Ventir.1, шпионе Mac.BackDoor.XSLCmd и троянце Mac.BackDoor.iWorm, позволившем хакерам создать новый ботнет из "маков".

И это примеры только новых троянцев для систем на основе Linux и Mac OS X — если раньше появление вируса для данных ОС было практически событием года, то теперь оно превратилось в обыденность.

Но если уязвимость стала известной — могут ли в Багдаде спать спокойно, используя штатные средства безопасности? Согласно отчету Synack, XProtect — решение безопасности компании Apple — "позволяет выявить лишь активный установщик вирусного ПО… Те компьютеры, которые были заражены еще до выхода новой версии XProtect, все еще остаются инфицированными".

Производители антивирусов мгновенно отреагировали на изменение интересов хакеров. Если раньше средства защиты для Linux и Mac OS X по сути ограничивались файловым монитором и антивирусным сканером для периодических проверок, то новые версии Dr.Web для Linux и Dr.Web для Mac OS X, вышедшие в этом году, включают функционал антивирусной проверки HTTP-трафика, блокирующий возможность использования вредоносными программами еще незакрытых уязвимостей, а также офисный контроль, ограничивающий доступ к потенциально вредоносным ресурсам.

Любители конспирологии только хмыкнут с пониманием, но для тех, кто знает, как на самом деле создаются сейчас вредоносные программы, совсем не секрет, что их настоящие производители давно поставили производство на поток и способны выпускать десятки и сотни новых образцов в день — и расширение систем сбора новейших вредоносных программ уже не позволяет выявлять большинство выпущенных в эти сутки инфекций. Для противодействия ураганному натиску злоумышленников антивирусные решения для всех ОС улучшили системы сканирования запущенных процессов для обезвреживания активных — ранее неизвестных — угроз. Не стали исключением и решения для "альтернативных" систем.

Но вернемся к тому, какие объекты подвергаются заражению. По счастью, инфекции для мышек, аккумуляторов и принтеров остались на уровне концептов. А вот троянец для NAS был обнаружен в "дикой природе": Trojan.Encoder.737 шифровал файлы, хранящиеся в сетевых хранилищах производства компании Synology, и, что вполне логично, требовал выкуп за расшифровку.

Год назад вызвала фурор первоапрельская шутка компании "Доктор Веб" о вирусе для бортового компьютера автомобиля, однако прошло совсем немного времени, и, похоже, шутка превращается в грустную реальность — уже зафиксированы удачные попытки перехвата управления не только автомобилями, но и кораблями. Интернет вещей, пришествие которого проповедуют сегодня, по своей идеологии беззащитен перед злоумышленниками. Его проблемы, как ни парадоксально, сходны с проблемами защиты систем управления технологическими процессами (АСУТП), банкоматов и терминалов. Как правило, все подобные устройства имеют крайне малый объем оперативной памяти, слабые процессоры и т. д. Внедрение вирусов в эти системы возможно — а вот для антивирусов ресурсов уже не хватает. Что делать?

Да очень просто — заглянуть на сайты антивирусных вендоров. Защита незащищаемого обеспечивается с помощью антивирусных шлюзов: ничто вредоносное не должно пересечь границу. Традиционно компании пренебрегали использованием шлюзовых решений — и хакеры с готовностью пользуются плодами экономии.

Как ни странно, но созданию и функционированию надежной системы защиты препятствуют две вещи: слабая информированность специалистов по информационной безопасности о современных угрозах и мерах по защите от них и пренебрежение пользователей мерами безопасности. Хотя вторую проблему можно свести к первой.

Автор — ведущий аналитик отдела развития компании "Доктор Веб".