Инъекция памяти

Все программное обеспечение, работающее на вашем компьютере, работает внутри памяти. Ничто не выполняется на вашем компьютере, если он не загружен с диска, не работает внутри памяти и не обрабатывается вашим процессором. Таким образом, очевидно, что вредоносное ПО само по себе должно каким-то образом проникнуть в память, чтобы иметь возможность работать.

И много разных беговых процессов, которые вы найдете в своей памяти. В Windows есть библиотеки DLL или Dynamic-Link. Есть потоки, буферы, функции управления памятью и другие вещи, которые хранятся и работают внутри памяти вашего компьютера.

Таким образом, вредоносное ПО имеет ряд вариантов запуска на вашем компьютере. Он может работать как отдельный процесс в памяти. Или он может найти существующий процесс и внедриться в середину этого процесса.

Вот блок-схема, описывающая процесс или приложение, которое работает внутри памяти. В этом процессе есть начальный адрес и конечный адрес. И если бы вы хотели внедрить вредоносное ПО в этот процесс, вам нужно было бы внедрить его где-то между этими двумя адресами. Это не только позволяет вредоносному ПО избежать обнаружения с помощью вредоносного ПО, которое просто ищет вредоносный процесс, но также позволяет этому вредоносному ПО иметь те же права и разрешения, что и процесс, в который оно внедряет. Это означает, что это очень простой способ для вредоносного ПО внезапно иметь привилегированное эскалацию или более высокие права и разрешения, чем те, которые оно обычно имело бы в этой системе.

Одна из наиболее распространенных форм внедрения вредоносного ПО называется DLL-инъекцией. DLL означает библиотеку Dynamic-Link. Так что это фактически тип исполняемого файла в вашей системе, который может использовать множество различных процессов и приложений. Чтобы это сработало, злоумышленникам сначала необходимо установить эту вредоносную DLL на какое-то хранилище, к которому может получить доступ ваша система. Злоумышленник хочет, чтобы эта DLL запускалась как часть целевого процесса. Но очевидно, что DLL еще не является частью этого приложения.

Однако реализация этого относительно проста для злоумышленника. Злоумышленник прокладывает путь туда, где вредоносная DLL находится где-то на накопителе, и помещает этот путь или ссылку на этот путь внутрь целевого процесса. По мере выполнения процесса он достигает точки, когда ему необходимо ссылаться на эту DLL. Он выходит на диск, втягивает вредоносную DLL и загружается в память. И теперь вредоносное ПО работает в этой системе.