

Прочие вредоносные программы

The FireCube
A little gift from hell...

Wu2k

00° 030° 040° 050° 060° 100° 120° 150°

DoS, DDoS — сетевые атаки

Программы данного типа реализуют атаки на удаленные сервера, посылая на них многочисленные запросы, что приводит к отказу в обслуживании, если ресурсы атакуемого сервера недостаточны для обработки всех поступающих запросов (DoS = Denial of Service).

A little gift from hell... **FireCube**

DoS-программы реализуют атаку с одного компьютера с ведома пользователя. DDoS-программы (Distributed DoS) реализуют распределенные атаки с разных компьютеров, причем без ведома пользователя зараженного компьютера. Для этого DDoS-программа засылается любым способом на компьютер «жертв-посредников» и после запуска в зависимости от текущей даты или по команде от «хозяина» начинает DoS-атаку на указанный сервер в сети.

The FireCube
A little gift from hell...

Exploit, HackTool — взломщики удаленных компьютеров

Хакерские утилиты данного класса предназначены для проникновения в удаленные компьютеры с целью дальнейшего управления ими (используя методы троянских программ типа «backdoor») или для внедрения во взломанную систему других вредоносных программ.

Хакерские утилиты типа «exploit» при этом используют уязвимости в операционных системах или приложениях, установленных на атакуемом компьютере.

A little gift from hell... FireCube

Flooder — «замусоривание» сети

Данные хакерские утилиты используются для «забивания мусором» (бесполезными сообщениями) каналов интернета — IRC-каналов, компьютерных пейджинговых сетей, электронной почты и т. д.

The FireCube
A little gift from hell...

Wu2k

00° 030° 040° 050° 060° 100° 120° 150°

Constructor — конструкторы вирусов и троянских программ

Конструкторы вирусов и троянских программ — это утилиты, предназначенные для изготовления новых компьютерных вирусов и «троянцев». Известны конструкторы вирусов для DOS, Windows и макро-вирусов. Они позволяют генерировать исходные тексты вирусов, объектные модули, и/или непосредственно зараженные файлы.

The FireCube
A little gift from hell...

Некоторые конструкторы снабжены стандартным оконным интерфейсом, где при помощи системы меню можно выбрать тип вируса, поражаемые объекты, наличие или отсутствие самошифровки, противодействие отладчику, внутренние текстовые строки, выбрать эффекты, сопровождающие работу вируса и т. п. Прочие конструкторы не имеют интерфейса и считывают информацию о типе вируса из конфигурационного файла.

The FireCube
A little gift from hell...

Nuker — фатальные сетевые атаки

Утилиты, отправляющие специально оформленные запросы на атакуемые компьютеры в сети, в результате чего атакуемая система прекращает работу. Используют уязвимости в программном обеспечении и операционных системах, в результате чего сетевой запрос специального вида вызывает критическую ошибку в атакуемом приложении.

A little gift from hell...

FireCube

Wu2k

00° 030° 040° 050° 060° 100° 120° 150°

Bad-Joke, Ноах — злые шутки, введение пользователя в заблуждение

К ним относятся программы, которые не причиняют компьютеру какого-либо прямого вреда, однако выводят сообщения о том, что такой вред уже причинен, либо будет причинен при каких-либо условиях, либо предупреждают пользователя о несуществующей опасности. К «злым шуткам» относятся, например, программы, которые «пугают» пользователя сообщениями о форматировании диска (хотя никакого форматирования на самом деле не происходит), детектируют вирусы в незараженных файлах, выводят странные вирусоподобные сообщения и т. д. — в зависимости от чувства юмора автора такой программы.

FileCryptor, PolyCryptor — скрытие от антивирусных программ

Хакерские утилиты, использующиеся для шифрования других вредоносных программ с целью скрытия их содержимого от антивирусной проверки.

The FireCube
A little gift from hell...

Wu2k

00° 030° 040° 050° 060° 100° 120° 150°

PolyEngine — полиморфные генераторы

Полиморфные генераторы не являются вирусами в прямом смысле этого слова, поскольку в их алгоритм не закладываются функции размножения, т. е. открытия, закрытия и записи в файлы, чтения и записи секторов и т. д. Главной функцией подобного рода программ является шифрование тела вируса и генерация соответствующего расшифровщика.

Обычно полиморфные генераторы распространяются их авторами без ограничений в виде файла-архива. Основным файлом в архиве любого генератора является объектный модуль, содержащий этот генератор. Во всех встречавшихся генераторах этот модуль содержит внешнюю (external) функцию — вызов программы генератора.

A little gift from hell... FireCube

VirTool

Утилиты, предназначенные для облегчения написания компьютерных вирусов и для их изучения в хакерских целях.

The FireCube
A little gift from hell...

Wu2k

00° 030° 040° 050° 060° 100° 120° 150°