Кто такие «хакеры»

Когда компьютеры только появились, слово «хакер» было уважительным. Его использовали для обозначения компьютерных гениев, способных переписать часть ядра операционной системы, чтобы она стала лучше работать или «сбросить» всеми забытый администраторский пароль. Хакеров уважали за умение нестандартно мыслить и находить разумные решения самым сложным проблемам.

Однако с течением времени оригинальное значение слова было утеряно, поскольку далеко не все «хакеры» ограничивались изменениями ядер ОС и восстановлением паролей по просьбам своих коллег. Некоторые из них начали вторгаться в плохо защищенные компьютерные системы, чтобы «доказать, что это возможно» и, наконец, перешли зыбкую границу взлома с целью кражи какой-либо важной информации или системных ресурсов.

Компьютерное сообщество, столкнувшееся с размыванием значения термина «хакер», ввело в обиход несколько дополнительных терминов, например, «script kiddie» и «cracker». Термин «script kiddie» используется для обозначения людей, не обладающих существенными познаниями в области хакерства и просто использующих для взлома чужие хакерские утилиты — скрипты, эксплойты и т. п. Термин «cracker» обозначает человека, находящегося где-то между script kiddie и хакером по уровню своих знаний. Он умеет взламывать программы и, например, избавляться от защиты от копирования, но недостаточно умен, чтобы самостоятельно находить новые уязвимости или писать хакерские утилиты.

Все еще более усложнилось, когда некоторые «кандидаты» в хакеры начали использовать хакерские утилиты, созданные кем-то другим, взламывать программы и воровать сервисы, в то же время, делая нечто общественно полезное, а «крэкеры» перестали ломать программы и удалять защиту от копирования, а принялись взламывать компьютеры в интернете. Из-за всех этих пертурбаций значение термина «хакер» стало гораздо менее «черно-белым», и в итоге были представлены термины «black hat», «white hat» и «grey hat».

Black hat — плохой, «черный» хакер, который взламывает программы и иные системы с целью кражи информации, запускает DDoS-атаки и крадет номера кредитных карт. «White hat», «белый» хакер, наиболее близок к оригинальному значению термина «хакер» — много знающий программист и эксперт по безопасности, использующий свои таланты чтобы помогать повышать безопасность компьютерных систем и ловить преступников. Где-то между ними находятся «grey hat», серые хакеры, которые занимаются всем понемногу.

Термины «хакер», «крэкер» и «script kiddie» часто используются в интернете и других средствах массовой коммуникации, хотя люди, занятые в области обеспечения информационной безопасности, предпочитают разделение хакеров на «белых» и «черных». Наконец, все эти термины субъективны, зависят от причастности пользующегося ими человека к одной или другой группе и могут провоцировать долгие споры о том, кто же на самом деле «черный», а кто — «белый» хакер.

**Хакер** - человек, который занимается цифровым взломом, крадет, удаляет или подменяет данные, выводит оборудование из строя. Словом, осуществляет несанкционированный доступ к цифровой информации и электронным системам. В переводе с английского hack означает "рубить, кромсать".

**Хакеры раньше и сейчас - в чем разница?**

Изначально хакеры не взламывали системы. Они просто находили ошибки в ПО и исправляли их каким-то особенно красивым и изящным способом. Собственно, hack пришло из сленга хиппи, самый близкий аналог в русском - "врубаться".

Сегодня слово "хакер" чаще всего применяют именно ко взломщикам. Это люди, которые своими действиями нарушают закон. Они используют уязвимости в программном обеспечении, чтобы обойти защиту.

**Зачем хакеры похищают информацию**

Данные похищают не из спортивного интереса. Чаще всего их можно дорого продать - особенно если речь идет о промышленном шпионаже в крупных корпорациях. Но данные из личных почтовых ящиков или аккаунтов в социальных сетях также имеют свою цену. Например, компрометирующие фото или переписку можно использовать в суде при разделе имущества супругов. Некоторые охотятся за интинмыми фотографиями знаменитостей, чтобы получить за них выкуп или заработать на продаже таблоидам.

**Хакеры бывают разные**

У хакеров, как и у ИТ-специалистов в целом, есть специализации. Например, **фишеры** собирают данные аккаунтов (в том числе банковских) через формы на фальшивых сайтах или поддельные приложения. Затем они перехватывают контроль над аккаунтом и, к примеру, опустошают банковский счет жертвы.

Есть **хакеры, которые занимаются брутфорсом** (перебором паролей). Чтобы ускорить процесс, они могут создавать целые ботнеты - сети компьютеров, которые совместно занимаются решением одной задачи. Обычно владельцы таких компьютеров даже не подозревают об этом - технику поражает вирус и использует её ресурсы в своих целях. К слову, **разработчики вирусов - тоже хакеры.**

В последнее время хакерство приобрело масштабы катастрофы. **Хакеры промышляют даже в Minecraft и других компьютерных играх** - крадут ресурсы и игровые предметы, чтобы сбыть на внутриигровом рынке за реальные деньги. Недавно [**обнаружили**](https://motherboard.vice.com/en_us/article/vb9v33/github-bitbucket-repositories-ransomware)хакеров, которые удаляли репозитории кода на GitHub и требовали выкуп у разработчиков. Массово взламывают криптовалютные кошельки или устанавливают майнеры (программы для добычи криптовалюты) на чужие компьютеры или смартфоны.

**Хакеры могут устроить катастрофу**

Если проникнуть в систему энергоснабжения, можно обесточить целый город. Если перехватить управление над АЭС - устроить второй Чернобыль. К счастью, это пока скорее теория - стратегические объекты хорошо защищены, взламывать их как минимум очень дорого.

**Что просят хакеры, когда шантажируют жертву**

Плату за возврат данных или восстановление доступа, к слову, всё чаще просят в биткоинах или другой криптовалюте. Такие платежи сложнее отследить.

**Добрые белые хакеры**

Есть хакеры, которые занимаются взломом систем для повышения их безопасности. Это белые, или этичные хакеры. Они пытаются найти дыры в системе и способы её взлома, а затем передать данные об этом разработчикам.

Белые хакеры не зарабатывают на продаже краденных данных. Они часто работают добровольно или за плату, которую изначально установил заказчик. Этичные хакеры могут участвовать в программах bug bounty - когда создатели ПО гарантируют награды за поиск уязвимостей в новой системе.

**Как стать хакером?**

Для этого нужно иметь глубокие знания. При этом получать их придется самому, потому что на хакера в университетах не учат. Важно владеть разными языками, уметь мыслить нестандартно, быть креативным и уметь быстро находить решения непростых задач.