Вот тебе, Bug Bounty, и Юрьев день!

Инструментарий ИБ-специалистов непрерывно совершенствуется, что подталкивает законодателей к внесению изменений в регулирование действий «белых хакеров». Но не только деньги способствуют их сотрудничеству с бизнесом





Текст
ВАДИМ ФЕРЕНЕЦ,
ОБОЗРЕВАТЕЛЬ **«Б.О»**

Современный информационный мир чутко реагирует на некие из ряда вон выходящие происшествия, которые моментально становятся мемами. Их герои начинают олицетворять собою всех жертв или, наоборот, спасителей отечества, привлекая тем самым внимание общественности к тем проблемам и событиям, настоящих героев которых мало кто видел в реальности.

Потренировавшись на кошечках, а именно на толстом коте Викторе, которого не пустили в самолет, а также на коте Твиксе, высаженном проводницей из поезда в лютый мороз, сетевая общественность в октябре 2024 года нашла главного хакера всея Руси. Им оказалась жительница Красноярска, которая обнаружила баг на Wildberries, позволивший ей получать товары бесплатно. До момента задержания она успела оформить заказов на сумму 1,2 млн рублей.

Этот случай наделал шума не меньше, чем происшествия с котиками, а известный ИБ-эксперт **Алексей Лукацкий** посвятил ему целый пост в Telegram: «Если бы эта девушка легально зарегистрировалась в программе Bug Bounty компании Wildberries, то она вполне могла бы получить 500 тыс. рублей за найденные уязвимости и накупить себе всякого разного. Да, это меньше 1,2 млн, но зато честно и без риска присесть на 10 лет. Так, глядишь, ей бы понравилось, и она стала бы постоянной участницей и заработала бы свои миллионы абсолютно честным путем».

Bug Bounty глазами финтеха

Шутки шутками, но героиня этого происшествия невольно породила целую волну экспертных дискуссий вокруг Bug Bounty, которые не утихают до сих пор, а также стала причиной некоторых практических действий участников ИБ-рынка и регуляторов.

Дело в том, что в ходе последних международных ИБ-конференций, в частности Gartner Security & Risk Management Summit 2024 в Великобритании, специалисты хором утверждали,

что классические продукты и услуги в сфере кибербезопасности не просто перестали работать должным образом, но и вообще «умерли». В числе «усопших» оказались Valnurablity и Security Awareness Manager, SIEM и т.д. А Bug Bounty выглядит живее всех живых. И вот тебе, бабушка, и Юрьев день: в Красноярске решили передать привет Лондону и доказать правоту международных экспертов.

Алексей Лукацкий предложил обсудить эту проблематику **Александру Хамитову,** руководителю продуктовой безопасности Wildberries. К ними присоединились **Тимофей Черных,** руководитель продуктовой безопасности Ozon, а также **Анатолий Иванов** со стороны Standoff Bug Bounty.

Первое, что удалось выяснить экспертам: в какой-то степени аналогом рассматриваемого инструмента является тест на проникновение в IT-инфраструктуру (пентест), продолжающий оставаться «живой ИБ-практикой», которая востребована акционерами публичных компаний и влияет на котировки акций на бирже. В отличие от Bug Bounty пентесты проводят специализированные компании силами штатных Blue и Red Teams в течение некоторого времени. Здесь есть некоторое количество законодательных актов, гарантирующих сохранение приватности, а также определение степени покрытия инфраструктуры заказчика пентестом.

Bug Bounty может проводиться непрерывно в течение всего года, даже если он високосный, на базе специализированной платформы с привлечением независимых багхантеров из всевозможных комьюнити с разной специализаций взломов: мобильных приложений, веб-ресурсов, крипторесурсов и т.д. Тестировщики тратят выделенный бюджет по своему усмотрению. Этим Bug Bounty выгодно отличается от пентестов, хотя заменить их собою в силу регуляторных норм пока не может. Но багхантеры не станут работать, если сумма коммерческого предложения будет ниже, чем у иного заказчика.

Что думают в Wildberries по поводу потенциальной тестировщицы из Красноярска, все желающие могут узнать из видео.

Всем хакерам — по белой шляпе

Если с финтехом все более или менее понятно, то в банковской сфере далеко не все решено, хотя в последнее время с появлением цифровых двойников IT-инфраструктуры объектов КИИ, содержащих информацию, относящуюся к разным тайнам, например банковской, кое-что изменилось в лучшую сторону. Но этого явно недостаточно.

В ноябре 2024 года АФТ стало известно, что Минцифры считает необходимым закрепить государственные тарифы на выплаты за участие «белых хакеров» в Bug Bounty. По словам экспертов рынка, это необходимо, чтобы стандартизировать Bug Bounty, а также для того, чтобы сделать использование этой программы обязательным для КИИ и госорганов.

К этому посту АФТ в Telegram моментально появились едкие комментарии: «Есть мнение, что "белые хакеры" не горят желанием попадать в государственные списки или реестры. Поэтому как создать соответствующее правовое поле, пока непонятно». В продолжение этого текста появился другой, не менее язвительный: «А вознаграждение багхантеру надо вручать прямо в кабинете у товарища майора. Непосредственно перед отправкой по этапу».

Однако законодатели полны решимости перевести Bug Bounty в правовое поле, поскольку изучают мировой опыт и понимают все недостатки пентестов в условиях кибервойны. Поэтому 27 декабря 2024 года стало известно, что Совет Федерации работает над новым законопроектом о «белых хакерах». Там предлагают обязать все компании, относящиеся к КИИ, включая банки, проводить такие тестирования, а также закрепить ответственность участников тестирований, операторов IT-платформ и владельцев IT-систем.

По информации «Коммерсанта», Минцифры рассматривает введение государственных тарифов за участие компаний и организаций в Bug Bounty. Известно, что обсуждались выплаты по федеральным округам в 30–50 тыс. рублей. за критические уязвимости, для IT-сервисов — до 1 млн рублей. Однако, как именно маститые эксперты ИБ-рынка рассчитали сумму 500 тыс. рублей потенциального вознаграждения невольной взломщице Wildberries, пока непонятно. Очевидно, различные Bug Bounty-платформы до сих пор надеются на сохранение собственной тарификации услуг багхантеров.

Шаги к открытости

Шутки шутками, а работы по масштабированию Bug Bounty в государственном секторе ведутся с 2022 года, после начала СВО и серьезного роста количества кибератак. 2024 год стал ключевым в законодательном урегулировании этого сегмента ИБ-рынка, поскольку, как отмечалось выше, даже в международном масштабе некоторые ИБ-технологии устаревают на глазах. В декабре 2023 года в Госдуму был представлен законопроект, который призван упорядочить деятельность «белых хакеров». И вот ровно через год в стенах Совета Федерации прозвучали слова: «Bug Bounty — это сила».

Примерно такого же мнения придерживаются в Сбере. Так, 24 декабря 2024 года «СберТех» практически параллельно с новостями из Федерального Собрания предложил независимым исследователям проверить защищенность GitVerse. Это российская платформа для работы с исходным кодом со встроенным ИИ-ассистентом. Независимые багхантеры смогут получить вознаграждение за найденные на платформе уязвимости. Выплаты за обнаруженные баги будут зависеть от уровня их критичности. Максимальный размер выплат достигает 200 тыс. рублей.

Но в отличие от сенаторов в Сбере не скрывают иной подтекст своего начинания. **Анатолий Шипов,** управляющий директор «СберТеха», сказал: «Уверен, что запуск программы на BI.Zone Bug Bounty не только позволит нам оперативно реагировать на потенциальные угрозы, но и станет важным шагом к открытости и сотрудничеству с сообществом ИБ-специалистов».

Очевидно, что в BI.Zone внимательно читают канал АФТ в Telegram и понимают опасения «белых хакеров». Не только в деньгах счастье! Б.О