

Взлом Twitter: все дело в “сливе”

ФБР и власти Нью-Йорка проводят расследования беспрецедентной [хакерской атаки](#) на Twitter, в результате которой были взломаны больше сотни официальных аккаунтов американских политиков и знаменитостей. Среди пострадавших - кандидат в президенты США Джо Байден, экс-президент США Барак Обама, миллиардеры Билл Гейтс, Майкл Блумберг и Уоррен Баффет, глава Amazon Джефф Безос, основатель Tesla и SpaceX Илон Маск и многие другие.



Учитывая, аккаунты каких влиятельных личностей были скомпрометированы, широкому резонансу в СМИ и вмешательству ФБР удивляться не приходится. В Bloomberg отмечают, что спецслужбы обычно инициируют расследование в случаях угрозы национальной безопасности, либо, если за атакой прослеживается зарубежный след.

Кстати, губернатор штата Нью-Йорк Эндрю Куомо (Andrew Cuomo) в своем заявлении 16 июля уже [помянул](#) происки иностранных врагов:

"Я поручаю провести полное расследование этого масштабного взлома при содействии Департамента финансовых служб Нью-Йорка и любых других необходимых ведомств, чтобы выявить все факты. Иностранное вмешательство остается серьезной угрозой для нашей демократии. Нью-Йорк будет и впредь возглавлять борьбу за защиту нашей демократии и честность наших выборов всеми возможными способами".

После подобных слов, наверное, не будет большим риском предположить, что скоро могут появиться сообщения о причастности к инциденту пресловутых русских хакеров.

Напомним, что же произошло.

15 июля в сервисе микроблогов на личных страницах знаменитостей стали появляться мошеннические предложения о заработке на биткоинах. Злоумышленники от имени звезд, политиков и миллиардеров предлагали подписчикам отправить на криптовалютный счет деньги, обещая, что в ответ те получат удвоенную сумму.

Впоследствии в ФБР [заявили](#), что учетные записи были взломаны для мошенничества с криптовалютой. В спецслужбе призвали не вестись на обман и не отправлять криптовалюту или деньги.



В Twitter говорят, что атаке подверглись в общей сложности 130 учетных записей известных людей. В 45 из них хакеры смогли сбросить пароли, войти в аккаунты и разместить мошеннические твиты. Некоторые из подписчиков знаменитостей поверили сообщениям и отправили деньги. По имеющимся оценкам, добычей злоумышленников стало более 120 тысяч долларов в биткоинах.

Чтобы вернуть контроль над учетными записями их настоящим владельцам, Twitter пришлось заблокировать атакованные аккаунты либо ограничить их функции.

"Мы работаем над тем, чтобы помочь людям как можно скорее восстановить доступ к своим учетным записям, которые были заблокированы. На это может потребоваться время, поскольку мы предпринимаем дополнительные шаги, чтобы убедиться, что доступ предоставляется законному владельцу", - [написала](#) техподдержка Twitter 16 июня.

Из последующих сообщений следует, что 17 и 18 июля в Twitter продолжали разбираться с последствиями атаки и выяснять, какие из непубличных данных знаменитостей могли узнать злоумышленники. Уже известно, что по меньшей мере в восьми скомпрометированных аккаунтах хакеры загрузили внутреннюю информацию об учетных записях с помощью инструмента "Your Twitter Data". В связи с этим данная функция временно отключена. Кроме того, во взломанных аккаунтах злоумышленники могли видеть скрытую персональную информацию, такую как электронная почта и номер телефона.

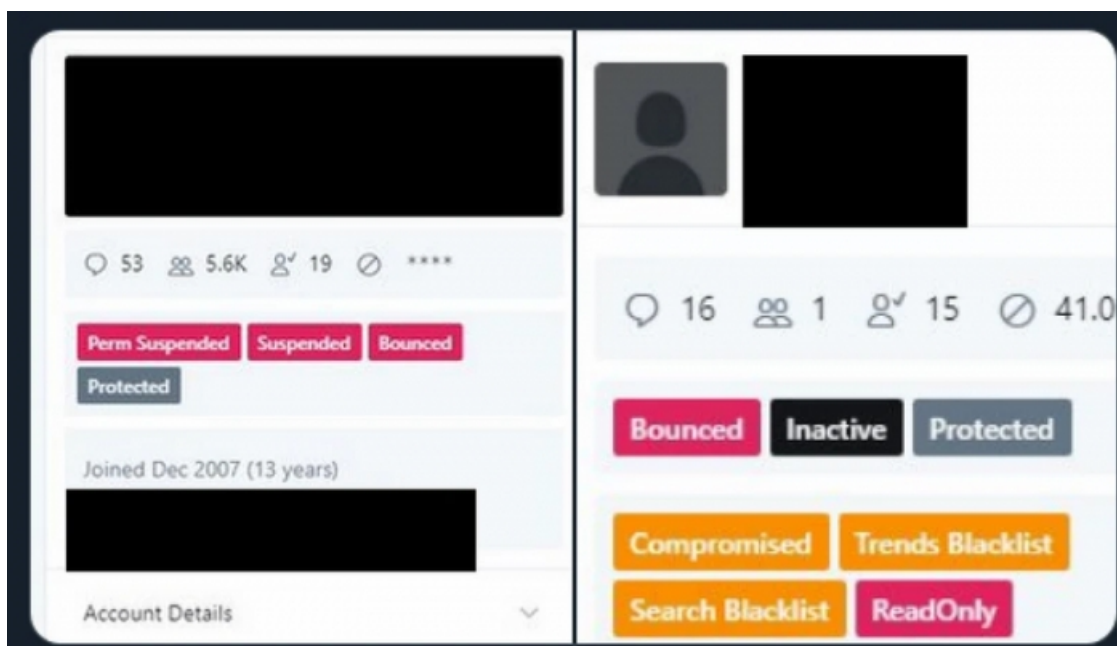
На странице [Twitter Support](#) соцсеть информирует о ходе внутреннего расследования с оговоркой, что выявляемые обстоятельства раскрываются выборочно, чтобы не давать злоумышленникам преимущества. В Twitter пообещали по завершению совместного с властями расследования раскрыть подробности. Также компания предпринимает дополнительные меры по обеспечению безопасности и предотвращению подобных инцидентов в будущем.

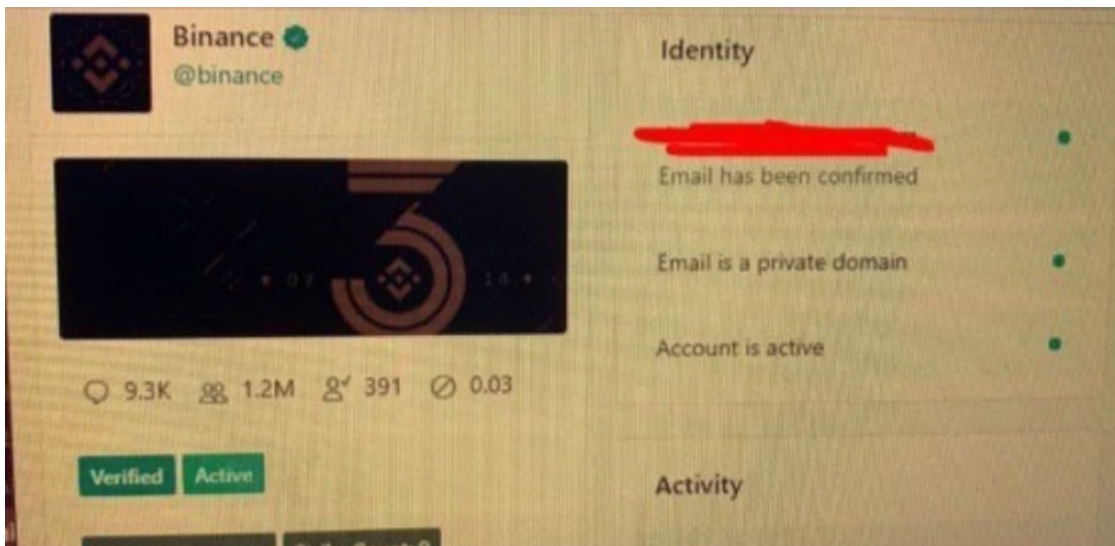


"Мы отлично понимаем, что несем ответственность перед людьми, которые пользуются нашими услугами, и перед обществом в целом. Нам стыдно, мы расстроены и очень сожалеем. Нам предстоит поработать, чтобы восстановить ваше доверие, и мы предпримем все усилия, что привлечь виновных к ответственности. Мы надеемся, что наша открытость и прозрачность в процессе расследования, а также меры для защиты от атак в будущем, помогут нам исправить ситуацию", - говорится в сообщении Twitter от 18 июля.

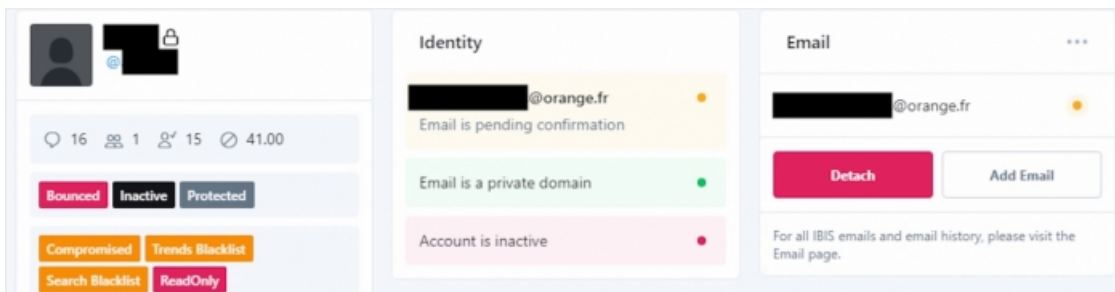
Кто именно стоит за атакой, по состоянию на 20 июля остается неизвестным. Пока что выяснилось, что преступники воспользовались приемами социальной инженерии и оплошностью персонала. Как следует из публикации в [корпоративном блоге](#) сервиса, несколько работников Twitter подверглись манипуляциям со стороны злоумышленников, в результате чего к хакерам попали данные для доступа к внутренним системам и инструментам управления Twitter.

Еще до подтверждения со стороны соцсети журнал Vice Motherboard со ссылкой на два анонимных источника [сообщил](#), что взлома как такового не было. Хакеры просто подкупили сотрудника Twitter. При помощи внутренних инструментов, которые используются персоналом соцсети для административного доступа к аккаунтам, в нескольких учетных записях были изменены привязанные к ним электронные адреса и сброшены пароли. В подтверждение существования такой панели управления издание опубликовало скриншоты.





Аналогичные снимки с экрана, полученные от источников в хакерской среде, появились и на портале [TechCrunch](#). На фото видно, что панель позволяет контролировать учетные записи Twitter, менять ассоциированные с ними email-адреса, блокировать аккаунты и продвигать те или иные твиты, понижая или повышая их цитируемость и выдачу.



Что характерно, когда пользователи начали обсуждать эту тему и размещать на своих страницах скриншоты из СМИ, в Twitter стали удалять сообщения и блокировать аккаунты, где они появлялись. Свои действия в компании объяснили тем, что твиты нарушают внутренние правила сервиса.

Между тем, [The New York Times](#), равно как и TechCrunch, пишут, что атаку с использованием внутренних инструментов Twitter устроил хакер по прозвищу Kirk. Компания Chainalysis, которая специализируется на анализе криптовалютных транзакций, помогла журналистам проследить, что пользователь с таким именем снимал средства с Bitcoin-кошелька, указанного в мошеннических твитах на скомпрометированных страницах знаменитостей.

Личность преступника и мотивы его действий еще предстоит выяснить, но судя по всему, ключевую роль сыграл именно "внутренний слив".

