Don't Want Your Laptop Tampered With? Just Add Glitter Nail Polish

If you're traveling overseas, across borders or anywhere you're afraid your laptop or other equipment might be tampered with or examined, you've got a new secret weapon to improve security. Glitter nail polish.

Don't laugh. It works.

Security researchers Eric Michaud and Ryan Lackey, making a presentation at the *Chaos Communication Congress* on Monday, highlighted the power of nail polish — along with metallic paints and even crappy stickers — to help people know when their machines have been physically tampered with and potentially compromised.

"Government agencies have so much money, they can build their own custom procedures," said Ryan Lackey, founder of the *CryptoSeal VPN* service. "But if you're a private person who travels to a country to do work, you have to take your stuff."

Physical tampering with machines, whether by governments, corporate competitors or data thieves looking for bounty, is a growing problem. Businesspeople traveling to China in particular have reported problems with data theft and hardware tampering. While drive encryption, strong passwords and software-based measures might keep causal thieves out, traveling offers many ways for prying eyes to physically compromise a laptop, Lackey and Michaud noted. Border areas can be especially dangerous, as authorities can confiscate a laptop or cell phone to "examine" it, then return it with the drives imaged or malware installed.

Once at a destination, many travelers lack the option to carry their laptop at all times. This raises the risk of attackers breaking into a hotel room to steal data or compromise machines.

Не хотите, чтобы в вашем лэптопе кто-то копался? Добавьте блестящий лак для ногтей

Если вы ездите в другие страны, и при пересечении границы или где-то ещё вы беспокоитесь, не будет ли кто-то трогать вашу аппаратуру или обследовать её, то теперь у вас есть новое секретное оружие для повышения безопасности. Блестящий лак для ногтей.

Не смейтесь — это работает.

Исследователи в области безопасности Eric Michaud и Ryan Lackey во время своей презентации на конгрессе *Chaos Communication* в понедельник подчеркнули способность лака для ногтей — наряду с металлизированной краской и даже простенькими наклейками — помочь людям знать, когда в их технику кто-то физически залезает и потенциально может взломать защищённые данные.

"У правительственных учреждений так много денег, что они могут создавать собственные методы защиты", — говорит Ryan Lackey, основатель сервиса *CryptoSeal VPN*. "Но если вы — частное лицо и едете в некую страну на работу, то должны иметь свои заготовки".

Физические манипуляции с компьютерами — занимаются ли этим правительства, корпоративные конкуренты или охотники за чужой информацией в целях получения вознаграждения — становятся всё большей проблемой. Деловые люди, ездящие в Китай, в частности жалуются на проблемы воровства данных и взлома техники. В то время как шифрование диска, надёжные пароли и программные меры могут защитить от случайных воров, путешествия дают много возможностей для любопытных глаз физически добраться до вашего лэптопа, отмечают Lackey и Michaud. Зоны пограничного контроля особенно опасны, поскольку власти могут конфисковать лэптоп или сотовый телефон, чтобы "осмотреть" его, а затем вернуть, предварительно сняв образы с дисков или установив шпионские программы.

Прибыв на место, многие путешественники не имеют возможности всё время таскать свои лэптопы с собой. Это увеличивает риск того, что некий взломщик проникнет в гостиничный

Short of keeping a machine with you 24/7, there is little you can do to be absolutely sure these things don't happen, the researchers said. If there is a serious question, they advise against traveling with sensitive data and wiping or simply discarding potentially compromised devices upon returning home. But those extreme measures don't help you while you're actually on the road, making it critical to know if your machine has been compromised.

Some travelers affix tamper-proof seals over ports or chassis screws. But these seals can in fact be replicated or opened cleanly in minutes by anyone with even minimal training, Michaud and Lackey said. They instead advise borrowing a technique from astronomers called blink comparison. Here's where the glitter comes in.

The idea is to create a seal that is impossible to copy. Glitter nail polish, once applied, has what effectively is a random pattern. Once painted over screws or onto stickers placed over ports, it is difficult to replicate once broken. However, reapplication of a similar-looking blob (or paint stripe, or crappy sticker) might be enough to fool the human eye. To be sure, the experts recommend taking a picture of the laptop with the seals applied before leaving it alone, taking another photo upon returning and using a software program to shift rapidly between the two images to compare them. Even very small differences — a screw that is in a very slightly different position, or glitter nail polish that has a very slightly different pattern of sparkle — will be evident. Astronomers use this technique to detect small changes in the night sky.

By taking the picture with a cellphone that is kept with you at all times, you can be reasonably

номер и сворует данные или защищённую информацию в машине.

Если не держать при себе коипьютер круглосуточно, то у вас немного вариантов, что такое можно сделать, чтобы полностью обезопасить себя от подобных событий, говорят исследователи. Когда вопрос серьёзный, они предостерегают от поездок с "чувствительными" данными и советуют стирать или просто выбрасывать потенциально взломанные устройства по возвращении домой. Но такие крайние меры неприменимы, пока вы на самом деле находитесь в дороге, и становится критичным знать, взламывалась ваша машина, или нет.

Некоторые путешественники ставят противовзломные пломбы на винты портов и шасси. Но с этих пломб на самом деле можно сделать реплики или вскрыть их в несколько минут, не оставив следа, даже обладая минимальными навыками, говорят Michaud и Lackey. Вместо этого они советуют позаимствовать у астрономов методику, которая называется сравнение блинкованием. Вот тут-то и появляется этот блеск.

Идея состоит в том, чтобы создать печать, которую невозможно скопировать. Блестящий лак, нанесённый однажды на ногти, имеет в сущности то, что называется случайным узором. Если вы нанесли его на винты или наклеенные на порты стикеры, то сломав лак, уже будет трудно затем воспроизвести. Конечно, можно повторно нанести похожую каплю (или нарисовать полоску, или приклеить простенький стикер), и этого будет достаточно, чтобы обмануть человечекий глаз. Но на самом деле эксперты рекомендуют сделать снимок лэптопа с установленными пломбами перед тем, как оставить его один, а затем, вернувшись, сделать другой снимок и использовать какую-нибудь компьютерную программу, чтобы сравнить эти изображения, быстро переключаясь между ними. Даже самые малые отличия — винт, который находится чуть-чуть в другом положении, или блестящий лак для ногтей, имеющий немножко другой узор блёсток — станут тут же очевидными. Астрономы используют эту технику, чтобы обнаружить малые изменения на ночном небе.

Делая снимок на сотовый телефон, который всегда при вас, вы можете быть вполне увере-

sure the original picture hasn't been tampered with or replaced. In order to guard against typical user forgetfulness, the experts recommend using a two-stage remote verification system. Such a tool would require that two pictures match exactly, for example, before allowing the user to log in to a potentially vulnerable system such as a VPN.

"This makes it non-skippable by users," said Michaud, CEO of *Rift Recon*. "If the user doesn't do the check, it doesn't work."

The pair said they will within a few months release an inexpensive tool that will support this two-step verification system. Such machine-assisted verification was necessary to help travelers overcome their own mistakes, they argued.

"Users are lazy," Michaud said. "It's really unlikely that we're going to build a system based on users making the correct security decisions all the time."

ны, что оригинальное изображение никто не подредактировал и не заменил на другое. Для того чтобы уберечься от типичной пользовательской забывчивости, эксперты рекомендуют использовать двух-ступенчатую систему удалённой проверки. Такой инструмент потребует, чтобы две картинки совпадали в точности, например, перед тем, как разрешить пользователю войти в потенциально уязвимую систему, такую как VPN.

"Это сделает невозможным для пользователя пропустить его," — говорит Michaud, Главный исполнительный директор *Rift Recon*. "Если пользователь не сделает проверку, он не сработает".

Эти двое говорят, что через несколько месяцев выпустят недорогую программу, которая будет поддерживать эту двухступенчатую систему проверки. Такая машинная проверка необходима, чтобы помочь путешественникам исправлять свои собственные ошибки, убеждают они.

"Пользователи ленивы", — говорит Michaud. "Едва ли мы будем создавать систему, основанную на том, что пользователи всегда принимают правильные решения в отношении безопасности".