

## Кибепреступники на тропе войны|Les cybercriminels sur le chemin de la guerre

Автор: Татьяна Гирко, Берн-Женева-Лозанна-Цюрих, 17. 02. 2017.



(DR)

Фальшивые счета от Swisscom, содержащие вредоносную программу Dridex, волна мошенничества, накрывшая швейцарские компании... Власти призывают к бдительности и усиливают структуры, которые борются с киберпреступностью.

Les fausses factures de Swisscom contenant le logiciel malveillant Dridex, une vague d'escroqueries visant des entreprises suisses... Les autorités appellent à la vigilance et renforcent les structures qui luttent contre la cybercriminalité.

Документ, как две капли воды похожий на счет от крупнейшей телекоммуникационной компании Конфедерации Swisscom, – так выглядит новая ловушка, в которую рискуют попасть пользователи интернета, сообщает издание La Côte. Центр регистрации и анализа для защиты информационных данных (MELANI) предупредил, что такие файлы содержат вредоносную программу, способную активировать банковские платежи без ведома владельца счета. Этот троянский конь, который по данным газеты Le Monde с 2015 года был выявлен в двух десятках стран, оказался ловко замаскированным, согласно последним поступившим сигналам.

Как убедиться в том, что полученный счет действительно был выставлен Swisscom, и не попасть в ловушку киберпиратов? Во-первых, стоит проверить, фигурирует ли ваше имя в документе: компания напоминает, что всегда обращается лично к клиенту. Нелишне будет повнимательнее присмотреться и к сумме, фигурирующей в счете: если вам предлагают оплатить 594,91 франка или 236,37 франка, то речь идет, скорее всего, о фальшивке, так как Swisscom округляет сумму. Не позволяет себе швейцарская компания и опускать диакритические знаки, используемые во французском и немецком языках, и делать другие орфографические ошибки. Наконец, «золотое правило» пользователей интернета – убедиться, что установленный на компьютере антивирус был вовремя обновлен.

**Von:** Swisscom [mailto:sme.contactcenter@bill.swisscom.com]  
**Gesendet:** Mittwoch, 15. Februar 2017 12:31  
**An:**  
**Betreff:** Rechnungskopie



Sehr geehrte Kundin, sehr geehrter Kunde  
Vielen Dank für Ihren Auftrag.  
Hiermit erhalten Sie die gewünschten Unterlagen.

**CHF 863.43** (zahlbar bis 24.01.2017)

[Rechnung einsehen >](#)

Betroffene Rechnung(en): Januar 2017



Alles Wissenswerte rund um das Thema Rechnung, Verbindungen & aktuelle Kosten finden Sie in Ihrem persönlichen Kundencenter.

**Angaben zur papierlosen Bezahlung**

Post-Konto: 01-38395-9  
Zugunsten von: Swisscom (Schweiz) AG, Contact Center Mobile, CH-3050 Bern  
Referenznummer: 788608635814519370390643231  
Codierzeile: 0100000549394>788608635814519370390643231< 010218415>

*Не спешите оплачивать этот счет! (© GovCERT.ch/twitter)*

В конце января Берн рекомендовал усилить бдительность и швейцарским компаниям. Распространившийся в последнее время способ мошенничества заключается в следующем: фирма получает звонок от человека, представляющегося сотрудником обслуживающего банка, который сообщает о готовящихся обновлениях интернет-банкинга. Ничего не подозревающая жертва устанавливает под «чутким руководством» программу, благодаря которой мошенники получают дистанционный доступ к рабочим компьютерам. Чтобы усыпить бдительность, киберпреступники общаются с представителями компании не один раз, втираясь в доверие благодаря упоминанию в разговоре имен сотрудников финансовых отделов и «тестируя» обновленную систему.

Информационная безопасность остается слабым местом швейцарских компаний, поскольку

киберпреступники постоянно совершенствуют используемые методы. Об этом свидетельствуют результаты недавно опубликованного [исследования](#) компании EY. Однако и власти не сидят сложа руки. Жертвы интернет-мошенничества могут обратиться в Федеральную службу полиции (fedpol) и подать жалобу в кантональную полицию. В Цюрихе на этой неделе решили расширить штат службы, занимающейся борьбой с преступлениями в сети.

На помощь дюжине сотрудников киберцентра, впервые объединившего в 2013 году под одной крышей представителей полиции и юстиции, придут около двадцати новых специалистов. Периметр их работы расширяется с каждым годом: еще десять лет назад расследования в этой сфере сводились в основном к выявлению сети детской порнографии, а сегодня, по словам одного из руководителей центра Даниэля Нуссбаумера, практически не осталось преступлений, авторы которых не пользовались бы интернетом. Так, недавно расследование в «даркнете» (от англ. DarkNet, «темная паутина» – сеть, в которой соединение устанавливается с использованием нестандартных протоколов коммуникации, например, только между «друзьями») позволило выйти на след убийцы, терроризировавшего Цюрих.



(© 24 Heures)

Для кантона, в котором расположены офисы крупнейших банков и транснациональных корпораций, киберпреступность представляет серьезную угрозу. «Такой экономический центр, как Цюрих, должен иметь возможность бороться с этим феноменом», – считает министр юстиции Жаклин Фер. По ее словам, многие швейцарские компании не желают публично обсуждать имеющиеся проблемы в сфере кибербезопасности, опасаясь нанести ущерб своему имиджу. «Но в разговорах с предпринимателями мы чувствуем: они хотели бы, чтобы мы начали действовать», – отметила Жаклин Фер.

В Женеве, по данным газеты 24 Heures, аналогичные функции возложены на бригаду по борьбе с информационной преступностью, которая оказывает поддержку другим полицейским подразделениям в проводимых расследованиях. В ее составе на сегодняшний день – около десяти специалистов, однако власти намерены расширить штат. В кантоне Во за кибербезопасность пока отвечают всего четверо полицейских, однако их деятельность подкрепляется работой четырех сотрудников прокуратуры.

Собрание глав кантональных департаментов юстиции и полиции (CCDJP) в настоящее время обсуждает возможность создания более крупных региональных центров, аналогичных тому, который сегодня работает в Цюрихе. Согласно предварительным планам, цюрихское подразделение могло бы отвечать за безопасность восточной части, на западе работал бы центр, расположенный в Женеве или Цюрихе, а еще один взял бы на себя охоту за киберпреступниками в центре страны. Преступления в сфере информационных технологий все чаще проникают в жизнь обычных граждан, а значит полиция должна научиться эффективно им противостоять.

Больше статей на эту тему вы найдете в [нашем досье](#).



## Добавить комментарий

Пожалуйста, [войдите](#) или [зарегистрируйтесь](#) , чтобы отправить комментарий

---