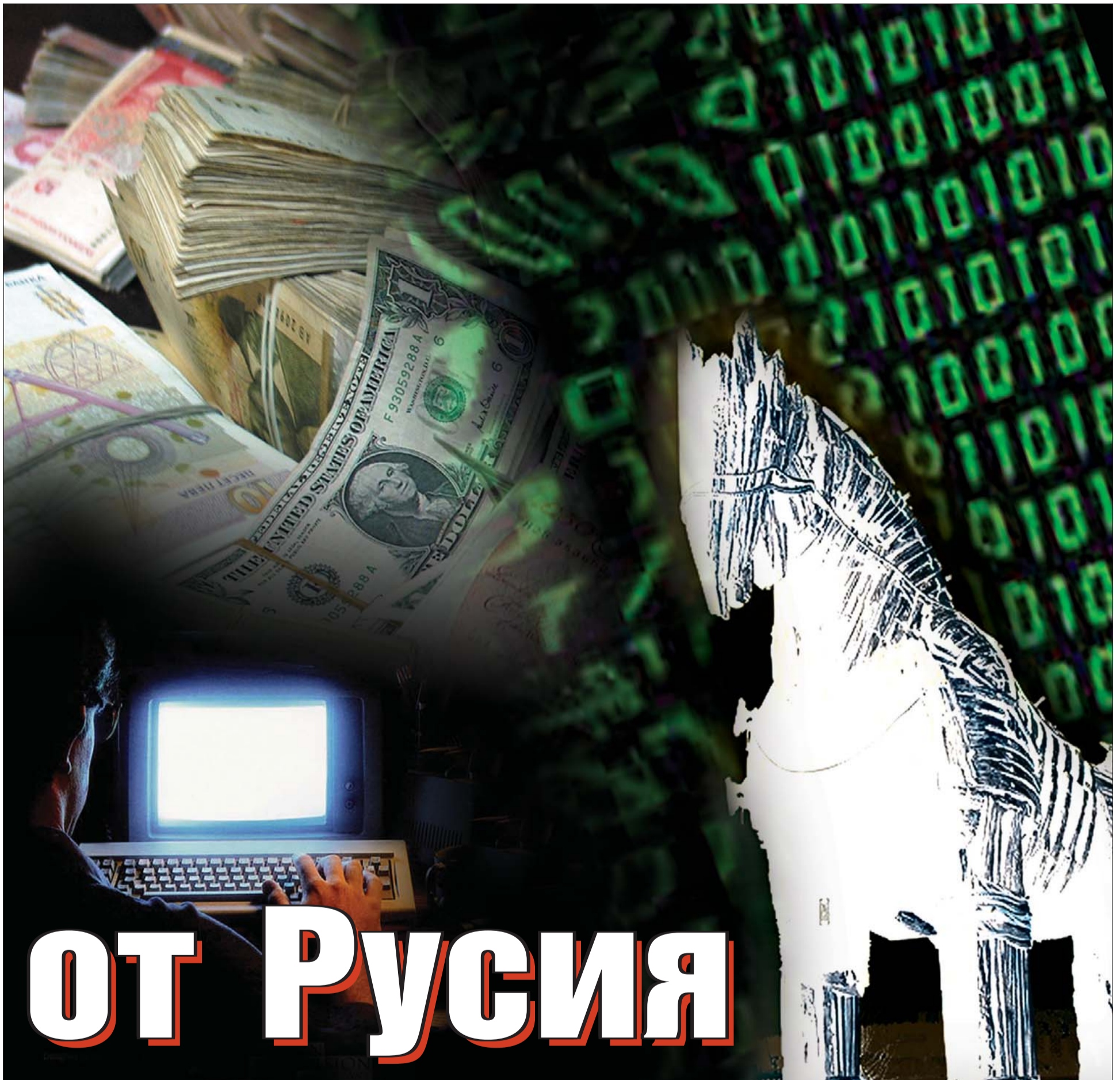


МЕНЮ: Банки масово отказват да плащат при кражба - на 14-а стр.
Електронен подпис и четец пазят парите от хакери - на 15-а стр.

Троянски кон



от Русия

Над 200 хил. евро са източени от сметки в наши банки това лято чрез руски "Троянски кон" и български "мулета". За това алармираха от Главната дирекция за борба с организираната престъпност (ГДБОП).

Въпреки животинския жаргон измамите нито са смешни, нито елементарни. Това са организирани компютърни кражби, които **изпразват сметки на хора и фирми, ползващи услугата електронно банкиране**

"Троянският кон" е програма, за която се твърди, че притежава някаква полезна цел (например - програма за MP3, за теглене на филми или имейли), но всъщност се оказва, че превзема канали или изтрива съдържание от твърдия диск, а в нашия случай - краде поверителни данни (пароли и сертификати за достъп до сметки).

Братушки точат банкови сметки у нас с вирус. Наши мулета им пращат парите

СТЕФАН ТАШЕВ

"До момента има установени около 50 неправомерни трансакции и опити за такива. Щетите, нанесени на клиентите на български банки, възлизат на над 200 хил. евро, като общият размер на трансакциите и опитите е за 400 хил. евро", обяснява Явор Колев, началник-сектор "Компютърните престъпления" в ГДБОП.

Бумът на тези измами е засечен от началото на април. Последният случай бе оповестен на 16 октомври, когато врачанският бизнесмен Веско Каменов, собственик на фирма "Бетон ЦВ" ЕООД, се оплака,

че от сметката му в "Уникредит Булбанк" са източени 50 хил. лв. Парите на Каменов били прехвърлени без негово знание по сметки в различни банки на четири души. След подаване на първите сигнали за подобни компютърни измами антимафиотите засичат цялата схема.

"Чрез създаване на зловреден софтуер, "троянски кон", от рода на Trojan.Pws.Sinowal, се заразява компютърът на клиента на банката, който ползва услугата електронно банкиране. Заразяването може да стане по много начини - чрез

нежелана кореспонденция, или т.нар. спам, при посещение на различни сайтове, чрез кликване на различни линкове и барове", обяснява Явор Колев.

Използваният "троянски кон" е предназначен предимно за

крадене на пароли от банкови сайтове, на имена, номера на кредитни карти, SSL сертификати

и друга информация, като голяма част от интернет комуникацията на потребителя, записана в Temp директорията на Windows, се изпраща в реално време на определени за целта интернет сървъри, установили антимафиотите. "Троянският кон" имал способността да се обновява автоматично. Предполага се, че произходът на зловредния софтуер е от Русия.

(Продължава на 15-а стр.)