Cyberattacks can be time bombs that may tick a while before being triggered

October 27 2015, by Gert Jan Van Hardeveld

Take your pick. Credit: Mighty Travels, CC BY

Cyberattacks such as that recently suffered by telecoms firm TalkTalk can result in hair-raisingly large losses: TalkTalk may have lost the details of 4m customers, while in just the last few months Carphone Warehouse lost 2m, Experian lost 15m T-Mobile customers' details, and dating website Ashley Madison lost 32m users' details. The impression is that all this data is a danger to us in the wrong hands, but where does it end up, how is it used, and by whom?

Stolen data such as credit card or personal identity details turn up for sale on websites and on sites in the dark web, accessed through Tor – an anonymisation network that makes it near-impossible to discover the origin and destination of web traffic, nor the identities of those involved. Using a Tor-enabled browser, it's possible to browse webpages on the standard web anonymously. It's also possible to access what are called Tor hidden services, essentially anonymised websites in the dark web, using the .onion domain suffix.

TalkTalk has alerted its customers to the possibility that their full name, address, date of birth and credit card details may have been compromised – although later reports suggest the breach may not have been as serious as first thought. However, complete card and customer details are a valuable commodity in online underground markets and can be used to make fraudulent transactions.

The personal details of TalkTalk customers, like those of previous hacks, could show up as products for sale on specialised underground "carding" forums. Carding is the act of using stolen personal information for profit. The price of a set of card details or personal information varies according to the amount of information available on a particular individual and how recent the cards have been obtained. Prices generally flucutate from US$45 to US$2 per card, with more freshly acquired cards the most expensive.

There are many ways to acquire card details using physical means such as skimming devices installed on cash machines or pay points. But those online generally come in two types. High-quality stolen data, known as "fullz", include all the information on an individual needed for fraudulent purposes. This usually includes the cardholder's date of birth, mother's maiden name, or other identity details commonly used as security questions. Other useful products are sold as CVV (what card companies call card verification values), the full details from a card required for making purchases such as expiration date and check code printed on the card's signature strip, as well as the card number and cardholder's name.

Cashing in

There are many ways for a buyer of stolen card details to try to profit from their purchase. Generally small amounts of cash can be withdrawn from an account to try to avoid detection by both bank and victim. Larger transactions will be noticed more quickly and get cancelled. A common method is to use stolen card details to make online purchases, often from relatively small online shops that are likely to have fewer fraud prevention measures such as verifying the cardholder's address.

In other cases, novel and complex techniques will be used, to get involved in fake webshops or warranty fraud, for example, for which the methods are also available to purchase in underground forums – often for thousands of dollars. Some advanced methods involve using dozens of stolen credit cards each week, generating the carder several thousands of dollars a week. Tutorials sometimes even come with personal one-to-one tutoring by the criminal hacker who has devised the method. More common carding techniques are explained in tutorials that are available for under US$100.

Another essential element for the carder to consider is a "drop" – a safe delivery address that doesn't reveal the carder's identity. By delivering fraudulently-purchased products to drops such as an empty house, anonymous post box, or the apartment of a trusted friend, it's less likely the carder will be traced by law enforcement. The carder will aim to keep any potential evidence to a minimum, for example by using cryptocurrencies like Bitcoin to purchase the stolen details in the first place, or by relaying their internet connection through one or more intermediary proxy servers in order to make it harder to trace.

A criminal service

A major problem facing those fighting cybercrime is how it has evolved into full-service commercial entities. Those without the hacking skills to pull off complicated attacks and cover their trails can find tutorials, techniques and even hackers-for-hire online – for a price. Underground criminal forums online and in the dark web are training grounds for cybercriminals-to-be, and the bar of skills required for entry is dropping.

Carders will try to justify their behaviour in discussions by arguing that banks reimburse their victims most of the time. Even so, victims suffer the shock and inconvenience of losing often substantial amounts of money, and the rising costs borne by banks and insurers are passed on to society.

Certainly for customers of TalkTalk and other firms subjected to data losses, there is no quick fix: a particular card may be cancelled, but their personal details and identities may swirl around online for many years yet. They will need to be vigilant for unusual activity in their bank accounts, and alert to unusual phone calls or emails that may be scammers at work.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation

Citation: Cyberattacks can be time bombs that may tick a while before being triggered (2015, October 27) retrieved 10 April 2024 from https://phys.org/news/2015-10-cyberattacks-triggered.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.