SWITCHcert Security Report

December 2016

SWITCH

I. Power and cybercrime – massive quantities of user data stolen in two recent hacks

Over 400 million customers of Friend Finder Network Inc. found themselves laid bare when servers belonging to the firm, which runs sites including adultfriendfinder.com, cams.com and penthouse.com, were hacked in October 2016. The biggest data theft of the year saw details of 412,214,295 accounts fall into the wrong hands (or at least the wrong drives). This hack is embarrassing not just for the users, but also for the site operator on a number of levels. For one thing, Friend Finder Network had already been hacked in May 2015. For another, research by leakedsource suggests that data were also stolen that related to almost 16 million further accounts that were still being stored by Friend Finder Network despite the fact that their deletion had been requested some time ago. Last but not least, leakedsource accuses the sex site operator of gross negligence because it allegedly stored passwords as plain text or anything but SHA1 hashes. There is a little comfort for the users affected in that, according to ZDNet, at least no details of "sexual preferences" were stolen in the latest hack. However, it is not clear whether the same is true for livecam footage from the firm's sites as Friend Finder Network refused to answer any further questions on the data theft.

A second major data theft, which occurred last month, also points to serious failings, this time on the part of government websites in Italy. A hacker called Kapustkiy succeeded in stealing 45,000 users' details with a simple SQL injection. These included access information for services in a number of Italian cities. The fact that the Italian authorities have up to now completely ignored the hack is particularly worrying. Kapustkiy claims that he has informed the website administrators of the leak himself but received no response as yet. Questions on this subject from various security sites have also gone unanswered by the official government authorities. At any rate, the compromised site has now been taken down, fixed and put back online.

Read more here:
https://www.leakedsource.com/blog/friendfinder
https://www.theguardian.com/technology/2016/nov/14/adult-friend-finder-and-penthouse-hacked-in-largest-personal-data-breach-on-record
http://de.engadget.com/2016/11/14/friendfinder-networks-gehackt-uber-412-millionen-nutzerkonten-b
http://www.zdnet.com/article/adultfriendfinder-network-hack-exposes-secrets-of-412-million-users
http://news.softpedia.com/news/hacker-breaks-into-italian-government-website-45-000-users-exposed-510332.shtml
http://securityaffairs.co/wordpress/53575/data-breach/kapustkiy-italian-website.html

II. When supposed security add-ons actually spy on your browsing habits

Web of Trust is a browser extension with a name that inspires confidence, and it was recommended as a useful security add-on for years. In November, however, it was found to be spying on users and forwarding their data to third parties. Reporters at the German broadcaster NDR had managed to analyse a block of user data offered for sale on the open market by a foreign provider. It listed all of the websites visited in August by some three million users, with over three billion entries containing the date, user ID and browsing history with multiple website addresses. These are especially valuable on the market for Big Data analysis and related services, which is thought to be worth around USD 122 billion (IDC estimate for 2015), because they offer particularly good transparency as regards users and their browsing and information behaviour.

This "betrayal" by Web of Trust (WOT), discovered when the NDR reporters searched for the source of the data, seems all the more shameless in light of the fact that WOT promises users safer, more trustworthy browsing. To this end, it checks the integrity of an address entered into the browser and displays its trustworthiness quickly and simply using a traffic light symbol. However, WOT states in its small print that these data are stored and forwarded to third parties, although it stresses that they remain anonymous. The reporters can prove that they can nevertheless be combined with other data to produce deanonymised, personal user profiles, which are illegal in Germany and Switzerland. Their suspicion that other add-ons, including Proxtube, were also selling out their users was also confirmed.

Some 120,000 smartphones sold in the US by Chinese manufacturer Blu also practised extensive spying. In mid-November, researchers at the US security firm Kryptowire published an explanation of how ADUPS, the firmware supplied by Shanghai ADUPS Technology Co. Ltd. for BLU R1 HD Android devices, was sending users' contacts, messages and location to servers in China every three days. ADUPS immediately took pains to stress that it had no links to the Chinese government. However, its customers also include smartphone and tablet manufacturers ZTE and Huawei. Unlike ADUPS, both of these companies are staying completely silent on this issue, although Swiss newspaper NZZ was able to find out that ADUPS is installed on around 700 million mobile devices and automotive systems. Huawei is the second-biggest network equipment supplier in the world and also a major player in Switzerland, working with almost all the country's telecom providers. In fact, it acquired Sunrise's IT unit in September 2016.

Read more here:

http://www.tagesschau.de/inland/tracker-online-101.html
http://www.ndr.de/nachrichten/netzwelt/Nackt-im-Netz-Millionen-Nutzer-ausgespaeht,nacktimnetz100.html
https://www.heise.de/newsticker/meldung/Millionen-Surf-Profile-Daten-stammen-angeblich-auch-von-Browser-Addon-WOT-3453820.html
https://www.heise.de/newsticker/meldung/Bericht-Auch-Add-on-Proxtube-leitet-Surf-Historie-aus-3491498.html
https://netzpolitik.org/2016/nackt-im-netz-auch-das-browser-plugin-proxtube-sendet-deine-besuchten-webseiten-an-dritte-sofort-loeschen
http://www.nzz.ch/digital/it-sicherheit-smartphones-schickten-daten-aus-den-usa-nach-china-ld.128678

III. Mirai part II – botnet knocks out 900,000 Telekom routers

The global botnet Mirai brought large parts of the Internet to a standstill in the US and worldwide back in October by staging massive distributed denial of service attacks via Internet of Things devices. This monster malware network struck again on a grand scale over the final weekend of November, knocking out around 900,000 Deutsche Telekom routers, in some cases for quite a long time. Users attempting to connect to the Internet via a Speedport router from the German firm were unable to access websites and e-mail, make phone calls or watch TV. Deutsche Telekom's experts worked hard to provide a software update as quickly as possible and prompted users over terrestrial radio and TV to perform a manual reset by unplugging their routers from the mains and the Internet, waiting five minutes and then plugging them back in so that the update could be installed automatically. The company appears to have succeeded in restoring all connections by the following Monday evening.

However, various commentators, including German newspaper FAZ, painted an almost apocalyptic picture and called for much more stringent regulation to improve the infamously poor (and sometimes non-existent) security features of Internet of Things devices, which we have repeatedly highlighted in the Security Report. In view of the financial cost of cybercrime, estimated at EUR 22-25 billion in Germany alone, a few cents extra per device seems like a reasonable price to pay – especially as many experts believe that Mirai is just the start of a wave of large-scale attacks on digital networks.

Read more here:

http://www.n-tv.de/technik/Stoerung-bei-Telekom-Hacker-sollen-verantwortlich-sein-article19198236.html
http://www.faz.net/aktuell/feuilleton/medien/nach-dem-telekom-hacking-der-preis-der-sicherheit-14556876.html
http://www.n-tv.de/technik/Monster-Botnetz-griff-Telekom-Router-an-article19207981.html
http://www.bocquel-news.de/Hacker-Attacken-Schäden-finanziell-aushebeln.36384.php

IV. It's not all bad news – Avalanche botnet taken down

In connection with the Mirai attack on Deutsche Telekom, the head of the German Federal Office for Information Security (BSI) spoke of a "hare-and-tortoise race". It is a race the good guys appear to have won for once as the phishing network Avalanche has been destroyed. Avalanche was among the leading cybercrime networks. It allowed hackers to steal e-banking login details and withdraw money from the compromised accounts. The botnet structure had also been used to spread e-mails containing malware since 2009.

Like Mirai, Avalanche ranked among the biggest botnet infrastructures of all. Cybercrime experts from 41 countries, including members of the FBI, the BSI and other agencies, simultaneously impounded 39 servers and hundreds of thousands of domains around the world in a concerted action and freed over 50,000 infected computers from the cybercriminals' control in Germany alone.

Read more here:

http://www.golem.de/news/avalanche-botnetz-weltweites-cybercrime-netzwerk-zerschlagen-1612-124829.html
http://www.zeit.de/digital/datenschutz/2016-12/phishing-netzwerk-avalanche-botnetz-infrastruktur-zerschlagen
https://krebsonsecurity.com/2016/12/avalanche-global-fraud-ring-dismantled

The SWITCHcert Security Report was written by Dieter Brecheis and Michael Fuchs.

It does not reflect the opinions of SWITCH but is instead a summary of articles published in various media. SWITCH accepts no liability for the content or opinions contained in the Security Report or for its correctness.