I. Even cyclists aren’t safe from cybercrime

‘Vanity – definitely my favourite sin.’ It would seem that it’s not just Al Pacino’s devil in Taylor Hackford’s mystery thriller ‘The Devil’s Advocate’ who thinks so – it seems to be the very guiding principle of the business model followed by burglars and cyber-savvy thieves of premium and high-ticket bikes. The thieves locate their victims through posts about special sports achievements, e.g. via a sports community app, or Twitter, Instagram, LinkedIn or other social media announcements to the more or less interested public that they are currently enjoying a well-deserved holiday far from home.

The exercise tracking app Strava has enjoyed vast popularity for years. But as early as 2014, police in Wales warned that criminals had been using the high performance figures posted by cyclists on Strava to determine that they had been achieved on expensive, even very expensive bikes. With cyclists usually making their full routes public, including their GPS data, it’s child’s play for criminals to discover where to find good loot.

In 2018, Adam Jones from Essex more than learned this the hard way when five top-of-the-range bikes were stolen from his garage successively, while thieves hadn’t even touched his
wife’s lower-priced bike. When addressed about the incident, Strava rejected any responsibility, pointing out that Strava users were encouraged to use the platform’s privacy settings and to think carefully about which information they wanted to share with whom. That being said, Strava also has to be given credit for the fact that other community profiles – such as those offered by sports watch manufacturers such as Garmin or Suunto – could soon see their own proud athletes falling victim to the crafty criminals with a lack of corresponding privacy settings. Even anyone who posts themselves and their bike on Instagram and then refers to their sports app profile using a hashtag is practically inviting miscreants to take advantage of them and their valuables.

The problem now seems to be more current than ever, even if the only difference is that the criminals have now arrived in Switzerland. The Zurich daily *Tages-Anzeiger* reported that in Wallis (which does sound a bit like Wales, except that the bikes stolen here were far more expensive), many valuable bikes were stolen after their owners had previously documented their journeys online.

It has long been known that burglars are particularly fond of choosing their next targets on Facebook, Instagram and other social media platforms. After all, holiday photos posted there make it clear that ‘nobody is going to be at home here for the next few days!’ Here, too, check the privacy settings, tighten them and think carefully about what you want to share with whom. Ultimately, everything should still be where it’s supposed to be when you return.

But if your bike or household items are gone, then you can still order them again from your trusted online shop. Be careful though: make sure that this really is your trusted online shop. Due to the currently long delivery times for bikes in particular, fake shop operators such as vandeyk-sport.com, motaza.shop, neimno.net or others are now exploiting the chance to achieve high click rates and incomes. This is because payment is made in advance, but nothing is delivered. This was also pointed out by Watchlist Internet in May, a website which, along with lists of fraudulent bike shops, also posts lists of general fraudulent online shops, booking platforms, property agencies, etc. Anyone who wants to interrupt the circular economy that is ‘exercise app leads to bike theft – replacement purchase in fake shop doubles the damage’ should exercise caution (and leave no openings for Al Pacino’s devil).

Read more:

- [https://www.wearable.com/cycling/strava-responds-cyclist-bike-theft-story-6554](https://www.wearable.com/cycling/strava-responds-cyclist-bike-theft-story-6554)
- [https://www.k-einbruch.de/aktuelles/detailansicht/auch-einbrecher-nutzen-facebook-instagram-und-co](https://www.k-einbruch.de/aktuelles/detailansicht/auch-einbrecher-nutzen-facebook-instagram-und-co)
II. Rogue ads on the advance

No better than fake shops, more and more fake ads are appearing in search engines (mainly Google and Bing), messaging apps such as WhatsApp and social networks like Facebook. While such deceptively real-looking ads from around ten years ago were still used to spread racist, sexist or other content that would not have stood a chance at publication in serious media, today’s rogue ads are mainly used to load malware or illegal cryptomining trojans onto the devices of unsuspecting users.

The criminals behind the fake ads enjoy a double payday: firstly, for the click on the ad and secondly, for the delivery of malware. The fraudulent pattern is always the same: a deceptively real-looking ad appears at the top of Google’s or Bing’s search results. The criminals use the real brand names, often copying the original teaser text, and refer – and this is the treacherous part – to the original domain of the often-clueless legal brand and domain owner. Clicking on the search result then takes the user to another deceptively real-looking login page. This does not belong to the legal brand and domain owner, but to the criminals, who then tap the login data and, in some cases, load malware such as trojans or seize the infected device, for example, to integrate it into a malware botnet or one for cryptomining.

At SWITCH, we are currently seeing a huge increase in such rogue ads. This may be because neither Google nor Bing seem to be taking the issue seriously or even showing any commitment to eliminating it. A further increase in rogue ad activity could have the potential to harm the search engine advertising business model. As the Harvard Business Review reported in its April 2022 edition, for the first time since the digital marketing hype began, many CMOs want to invest more in analogue marketing again – among other things, due to the increase of ad fraud, credibility issues and the resulting inefficiency of the budget used.

For anyone who wants to know more about rogue ads, SWITCH-CERT published a brief paper ‘Rogue ads on the rise’ as a PDF file, which we are happy to provide on request.

Read more:

https://financialpost.com/news/retail-marketing/rogue-ads
https://www.der-bank-blog.de/top-ten-bankueberfaelle/fotosnecke/11685133/11
https://hbr.org/2022/04/why-marketers-are-returning-to-traditional-advertising

III. When hackers join the team – ransomware and cryptotrojans spreading on Confluence Server and Data Center

The ‘crypto-winter’ is not only leaving its mark in investor profiles, but also in the criminal reports of cybersecurity companies. It appears as if miners want to make up for their
sometimes-dramatic losses by seizing foreign computers. Researchers from Yverdon-les-Bains-based security company Prodraft reported that hackers are using a gap – known about since the beginning of June and classified as ‘critical’ – in the widely used collaboration software Confluence Server and Confluence Data Server to implement the blackmail trojan AvosLocker.

At around the same time, Microsoft warned on Twitter that a further blackmail trojan would spread on unpatched Confluence instances in the form of Cerber2021. And security experts at Check Point discovered that cryptominers were not letting go of the opportunity to seize foreign computers and networks to mine digital money at the expense of computer performance and the electricity bill.

Confluence producer Altassian issued a corresponding warning regarding the issue at the beginning of June, advising users to switch off Confluence Server until suitable patches (which the company provided successively from 3 to 10 June) had made the endangered systems safe again. Altassian also published corresponding ‘What to do’ instructions on their website (link below).

At SWITCH, we saw how malicious GET requests had attempted to download software from the IP address 198.98.48.215, which is used as a Mirai Botnet C2 server. From there, multiple malicious scripts are placed on the server under attack. SWITCH recommends reviewing firewall logs for the IP addresses in question in the period between 2 and 10 June 2022, and also to check whether any data packages had successfully been placed in the infrastructure. Anyone who wants to block the specified IP address should do so at their own risk, as the address has only been used for a short time.

Read more:

IV. Causing a hoot: Meeting Owl Pro more secure, but still four security gaps away from ‘secure’

Swiss cybersecurity company modzero AG pronounced the verdict for four serious security vulnerabilities in the video conferencing software from Boston’s Owl Labs: ‘Currently, modzero does not recommend using Meeting Owl products until effective security fixes and countermeasures are applied.’ The reason: security researchers had discovered four ‘high-risk’ and one ‘critical’ security gap in the products Meeting Owl Pro and Whiteboard Owl and informed the producers of these back in January 2022.
The gaps allow attackers to circumvent the system’s PIN protection with relatively low effort, to record the information shown in a meeting and to obtain access to the network into which the meeting hardware is incorporated. This would make Meeting Owl Pro and Whiteboard Owl a wide-open door for cybercriminals, who could use this method to install backdoors, load in malware and ransomware and compromise an entire company network.

Owl Labs clearly seemed less than amused to be contacted by the Swiss company, but agreed to security updates by mid-March. Despite the known high risk, it was not until the start of June that the Boston company published Update 5.4.1.4, which was intended to close the critical security gap CVE-2022-31460 – but does not provide any patches for the four remaining vulnerabilities. Despite this, it is worth installing the update.

According to information from Owl Labs, attackers can now no longer exploit the access point functions previously usable as a gateway into connected networks. A report by the Owl Labs press centre to heise.de revealed that the company was still aware of the four open gaps, with the report stating that they could not be used to access networks.

At this point, we would like to use this opportunity to raise awareness about the fact that the best safeguards of networks are cancelled out if insufficiently secure external hardware is incorporated into such a network. The often-blamed default settings ‘0000’ or ‘9999’ should also be changed before integrating cameras, microphones or other devices (although it is unfortunately still almost progress if these devices actually have a customisable, at least four-digit code).

Read more:

https://resources.owllabs.com/blog/owl-labs-update

This SWITCH security report was written by Dieter Brecheis and Michael Fuchs.

The SWITCH security report does not represent the views of SWITCH; it is a summary of various reports published in the media. SWITCH assumes no liability for the content or opinions presented in the Security Report nor for the correctness thereof.