

Hackers become even more accessible - blueAPACHE

Canonical: <https://www.blueapache.com/blog/hackers-become-even-more-accessible-2>

Details:

Summary

This post reports on a marketplace-style website, registered in New Zealand, that connects people seeking hackers for hire with hackers offering their services, and uses it to warn that hacking-for-hire has become easier to access even though targeted attacks, phishing, social engineering and malware were already rising through 2014 and into 2015. It is written for Australian business leaders and IT managers assessing their own exposure to targeted cybercrime, and it sets out the criminal penalties, up to ten years' imprisonment, that apply to hacking offences under Australian Commonwealth law. The core warning still applies today: commodified access to attackers, through marketplaces, forums or now more automated criminal tooling, remains a live risk factor, and the legal position on unauthorised access in Australia is unchanged.

Key facts

Label	Value
Published	2015
Topic	A marketplace connecting customers with hackers for hire, and the resulting rise in accessible targeted attacks
Services referenced	Security posture review and protection advice from an account team
Legal reference cited	Australian hacking offences carry penalties of up to ten years' imprisonment, defined under Part 10.7, Computer Offences, of the Criminal Code Act 1995 (Cth), as stated by the post
Offence categories listed	Computer intrusions, unauthorised modification or destruction of data, denial-of-service attacks, distributed denial-of-service attacks using botnets, and creation or distribution of malicious software
blueAPACHE security services relevant today	emPOWER Managed Detection and Response provides 24/7 alert notification, triage and remediation across the full IT environment; emPOWER Human Risk Management addresses phishing and human-centred risk

Article

A new website has been launched that mirrors oDesk.com, Freelancer.com, Elance.com and similar freelancing sites that connects consumers with service providers. This time round, the service is hacking. Registered in New Zealand, the site connects customers and professional hackers for hire. Since launching in November, hundreds of posts from users seeking hackers have been added requesting everything from accounts being hacked to grades being tweaked. There are almost 1000 hacker profiles on the site offering services. While hiring hackers online isn't new; having such ease of access locally is. The site's terms and conditions forbid "use the Service for any illegal purposes," and their FAQ encourages visitors to report any illegal jobs so they can be removed. Even so, the general public now have much easier access to a large number of hackers that they can potentially engage in offline discussions to discuss other more dubious hacking projects. We saw more targeted attacks on organisations reported in 2014 than ever before. Data breaches are creating headlines with greater regularity, and targeted attacks through social engineering, brute force attacks, phishing and malware are key threats in 2015. This site, no matter how much they try to prohibit it; has the potential to result in even more. According to the New York Times, the founders of the website are too afraid to go public. The article stated they had received legal counsel about how to structure the website to avoid liability for any wrongdoing by people either seeking to hire a hacker or by hackers agreeing to do a job.

It is important to remember that Australian hacking laws carry penalties of up to ten years imprisonment.

Hacking refers to the unlawful or unauthorised access to, or modification of, restricted data. High tech crime offences are defined in Commonwealth legislation within Part 10.7 – Computer Offences of the Criminal Code Act 1995 and include:

Computer intrusions (for example, malicious hacking)

Unauthorised modification of data, including destruction of data

Denial-of-service (DoS) attacks

Distributed denial of service (DDoS) attacks using botnets

The creation and distribution of malicious software (for example, viruses, worms, trojans).

More information

To discuss your security status and how to protect your business, contact your account team.

Related

[/services/empower-security-top-level](#)

[/empower-services/security](#)

[/services/managed-detection-response](#)

[/services/human-risk-management](#)

[/case-studies/blueapache-security](#)

Frequently asked questions

What did the hacker-for-hire website described in the post actually offer? It functioned like a freelancing marketplace, similar in structure to oDesk, Freelancer or Elance, but for hacking services. The post notes it carried close to a thousand hacker profiles and hundreds of posts from people seeking services ranging from account intrusion to changing academic grades.

Was the site itself illegal to operate? The post reports that the site's terms and conditions prohibited use "for any illegal purposes" and its FAQ encouraged users to report illegal jobs. According to the New York Times, as cited in the post, the founders had taken legal counsel on structuring the business to avoid liability for wrongdoing carried out by users.

What penalties apply to hacking offences in Australia? The post states that Australian hacking laws carry penalties of up to ten years' imprisonment. Offences are defined in Part 10.7, Computer Offences, of the Criminal Code Act 1995 (Cth), and include computer intrusions, unauthorised modification or destruction of data, denial-of-service and distributed denial-of-service attacks, and creating or distributing malicious software.

What attack methods does the post identify as the key threats of the period? Social engineering, brute force attacks, phishing and malware, alongside a general rise in targeted attacks against organisations reported through 2014.

Why does easier access to hackers matter even if the marketplace itself tries to prohibit illegal use? The post's concern is that a public marketplace lowers the barrier to finding a hacker at all, and that initial contact can move to private, off-platform discussions of more serious or illegal work regardless of what the site's own terms prohibit.

Is commodified access to attackers still a relevant risk today? Yes. The specific website named in the post is a 2015 example, but marketplaces and forums offering hacking, credential and access-broker services have continued to exist since, and phishing and social engineering remain leading routes into organisations.

What managed security services address the threats described in this post? blueAPACHE's emPOWER Managed Detection and Response provides continuous monitoring, threat hunting and incident response across a customer's environment, and emPOWER Human Risk Management addresses phishing simulation, email threat detection and insider risk, the human-targeted side of the threats this post describes.

Who should a business contact to review its exposure to these kinds of threats? The post directs readers to their blueAPACHE account team to discuss their security status and how to protect their business; current service detail is available on the security service pages linked above.

Source

<https://www.blueapache.com/blog/hackers-become-even-more-accessible-2/>

Knowledge Base

Did the hacker-for-hire site allow illegal activity according to its terms?

No. The site's terms and conditions forbade using the service for any illegal purposes, and its FAQ encouraged visitors to report any illegal jobs so they could be removed. However, this didn't prevent easier public access to hackers who could be engaged offline for more dubious projects.

Why were the founders of the hacker-for-hire site reluctant to go public?

According to the New York Times, as cited in the article, the founders were too afraid to go public and had received legal counsel on how to structure the website to avoid liability for wrongdoing by either people hiring hackers or hackers agreeing to do a job.

What penalties do Australian hacking laws carry, ?

Australian hacking laws carry penalties of up to ten years imprisonment.