The Register®
Biting the hand that feeds IT

Security

Researcher reveals Chinese e-crime shopping list

Crazy low prices for app 'purchases', or perhaps you'd like a poison PoS unit?

26 Nov 2015 at 07:29, Darren Pauli

21 19

Dodgy developers can have their data-stealing iOS applications boosted to the top ranks of Apple's App Store for as little as US$4000 thanks to services on offer by Chinese hackers.

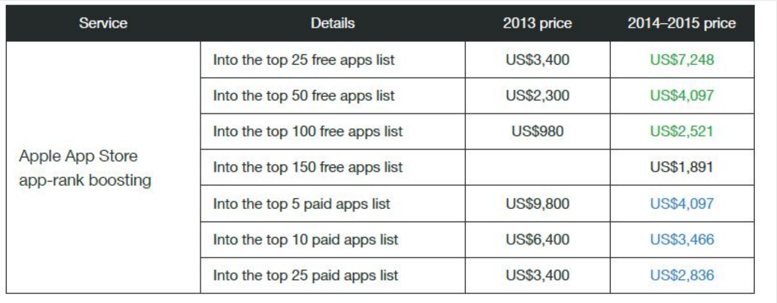
The price will get an application capable of evading Apple's security checks onto the top five paid application list through boosting services.

A payment of $US7200 will get an app onto the sought-after top 25 free apps lists, a price increase of $3800 since 2013.

By contrast deviant developers can score 10,000 downloads for their malicious Android app a paltry US$16.

The findings are part of analysis of the Chinese criminal underground by Trend Micro forward threat researcher Lion Gu.

He finds in the paper *Prototype Nation: Innovations in the Chinese Cybercriminal Underground* [PDF] that many of the security crime offerings in Chinese marketplaces will likely be adopted by hackers in other countries.



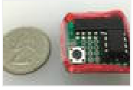
Service	Details	2013 price	2014–2015 price
Apple App Store app-rank boosting	Into the top 25 free apps list	US$3,400	US$7,248
	Into the top 50 free apps list	US$2,300	US$4,097
	Into the top 100 free apps list	US$980	US$2,521
	Into the top 150 free apps list		US$1,891
	Into the top 5 paid apps list	US$9,800	US$4,097
	Into the top 10 paid apps list	US$6,400	US$3,466
	Into the top 25 paid apps list	US$3,400	US$2,836

More like this

Malware Apple Trend Micro Ios

Most read

Why Microsoft yanked its latest Windows 10 update download: It hijacked privacy settings



Hacker predicts AMEX card numbers, bypasses chip and PIN

Second Dell backdoor root cert found

Cyber-terror: How real is the threat? Squirrels are more of a danger

Microsoft Windows: The Next 30 Years

Spotlight

Cyber-terror: How real is the threat?

Gu's price list continues: 80,000 spam iMessages costs $630, corporate email hacking can be done for $95, while a distributed denial of service attack maxing out at 100Mbps from 2000 nodes will cost $79 a month.

The most expensive service he found was cracking encrypted thumb drives which could cost up to $12,600.

Perhaps the most financially devastating fraud identified in the report is the rise of mass-produced infected point of sales terminals which are being bought by scammers and sold to unwitting Chinese businesses allowing customer credit cards to be shipped off to fraudsters over SMS.

Gu finds modified point of sales terminals are being sold by criminal companies to unwitting wholesalers who then resell the devices to retail stores and chains. Next stop: mass credit card theft.

"These mass produced devices have been introduced into otherwise legitimate business equipment sales and supply chain operations," Gu says in the report.

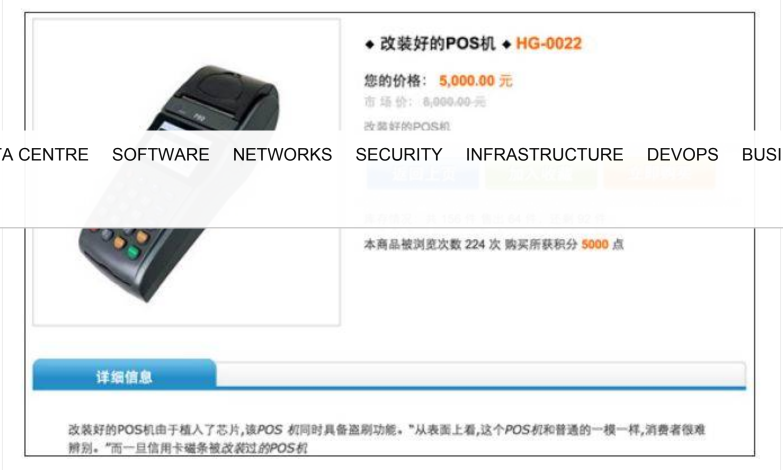
"Legally operating businesses are selling mass produced, malicious payment card devices to other organisations with neither being aware, ultimately victimising the customers of both.

"Some of the PoS skimmers sold underground even have an SMS-notification feature [which] allows cybercriminals to instantly get their hands on stolen data via SMS every time the tampered devices are used."

At least one infected point of sales fraud campaign netted US$236,500 for a company flogging the devices to restaurants and hotels. Some 1100 credit cards were found on the company's servers.

Mass production has also hit the ATM carding space with panels sold for about $600. Those units are sold on the same sites and contain facilities to steal magnetic stripe data and a camera to record PINs.

The device can be upgraded with a keypad overlay to more effectively steal PINs, if you've another US$300 to spend.



◆ 改装好的POS机 ◆ HG-0022

您的价格： 5,000.00 元

市 场 价： ~~6,000.00 元~~

改装好的POS机

库存情况：共 156 件 售出 64 件，还剩 92 件

本商品被浏览次数 224 次 购买所获积分 5000 点

改装好的POS机由于植入了芯片,该*POS* 机同时具备盗刷功能。"从表面上看,这个*POS*机和普通的一模一样,消费者很难辨别。"而一旦信用卡磁条被*改装过的POS机*

DATA CENTRE SOFTWARE NETWORKS SECURITY INFRASTRUCTURE DEVOPS BUSINESS HARDWARE SCIENCE BOOTNOTES FORUMS

Shop clerks can opt for a $140 pocket skimmer which they can use to swipe customer credit cards when out of sight

Courses in how to card are also on offer selling on Tor hidden services and other forums for about $500.

Gu says the devices are being sold on business to business sites like *1688.com* at low cost to attract supply chain businesses.

China is the "birthplace" for broader crime trends, Gu says, with the "most important" innovations occurring in the carding space. ®

Tips and corrections

Post a comment

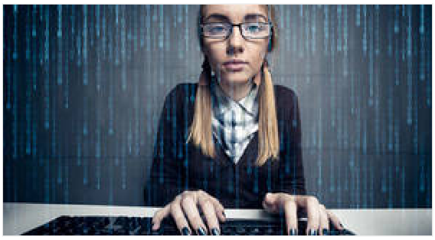
More from The Register

Cyber crims up the ante

Microsoft puts a bullet in

VirusTotal invites Apple

Squirrels are more of a danger



George Osborne fires starting gun on £20m coding comp wheeze

GCHQ director blasts free market, says UK must be 'sovereign cryptographic nation'

Australia on the very brink of cyber-geddon, says ex-spook

If MR ROBOT was realistic, he'd be in an Iron Maiden t-shirt and SMELL of WEE

'Get a VPN to defeat metadata retention' is good advice. Sometimes

with Google Play brainteaser malware

Intelligence-testing app attack shows it isn't just dumb people who get caught

12 Comments

blundering D-Link's leaked key that made malware VIPs on PCs

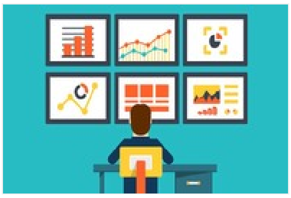
Private code-signing cert revoked at last

2 Comments

fans to play in updated Mac malware sandpit

But Macs don't get viruses ... Oh they do, and increasingly often says Google infosec unit

14 Comments



Ad slingers beware! Google raises Red Screen of malware Dearth

Chrome to take shine off dodgy networks

16 Comments

Nest defends web CCTV Cam amid unstoppable 24/7 surveillance fears

The truth about camera that seemingly keeps recording even when powered off

32 Comments

Google swallows your Docs bill from Microsoft, pitches for user familiarity

Tied to Enterprise Agreement? No worries ...

17 Comments

Whitepapers

The rising value, and falling cost, of desktop virtualisation

When vendors compete, desktop virtualization customers win. Moore's Law and market forces lead to better solutions at a lower cost.

Why application delivery matters in the digital economy

Increasingly, all of the things that make companies successful - productivity, customer satisfaction and brand recognition - emerge from good interactions with applications and services.

Samsung enterprise alliance case studies

Download this paper to see how being a SEAP partner has benefited companies such as Citrix and Aviva.

Magic Quadrant for identity governance and administration

Organizations are moving to IGA solutions such as IBM Security Identity Governance and Administration to help improve compliance and lower total cost of ownership.

AVG defends plans to flog user data as privacy row continues

Phone-fondling docs, nurses sling patient info around willy-nilly

Sponsored links

Sign up to The Register to receive newsletters and alerts

About us

- Privacy
- Company info
- Advertise with us
- Syndication
- Send us news tips

More content

- Subscribe to newsletter
- Top 20 stories
- Week's headlines
- Archive
- eBooks
- Webcasts

Follow us

Mobile website

The Register

Independent news, views, opinions and reviews on the latest in the IT industry. Offices in London, Edinburgh, San Francisco and Sydney.