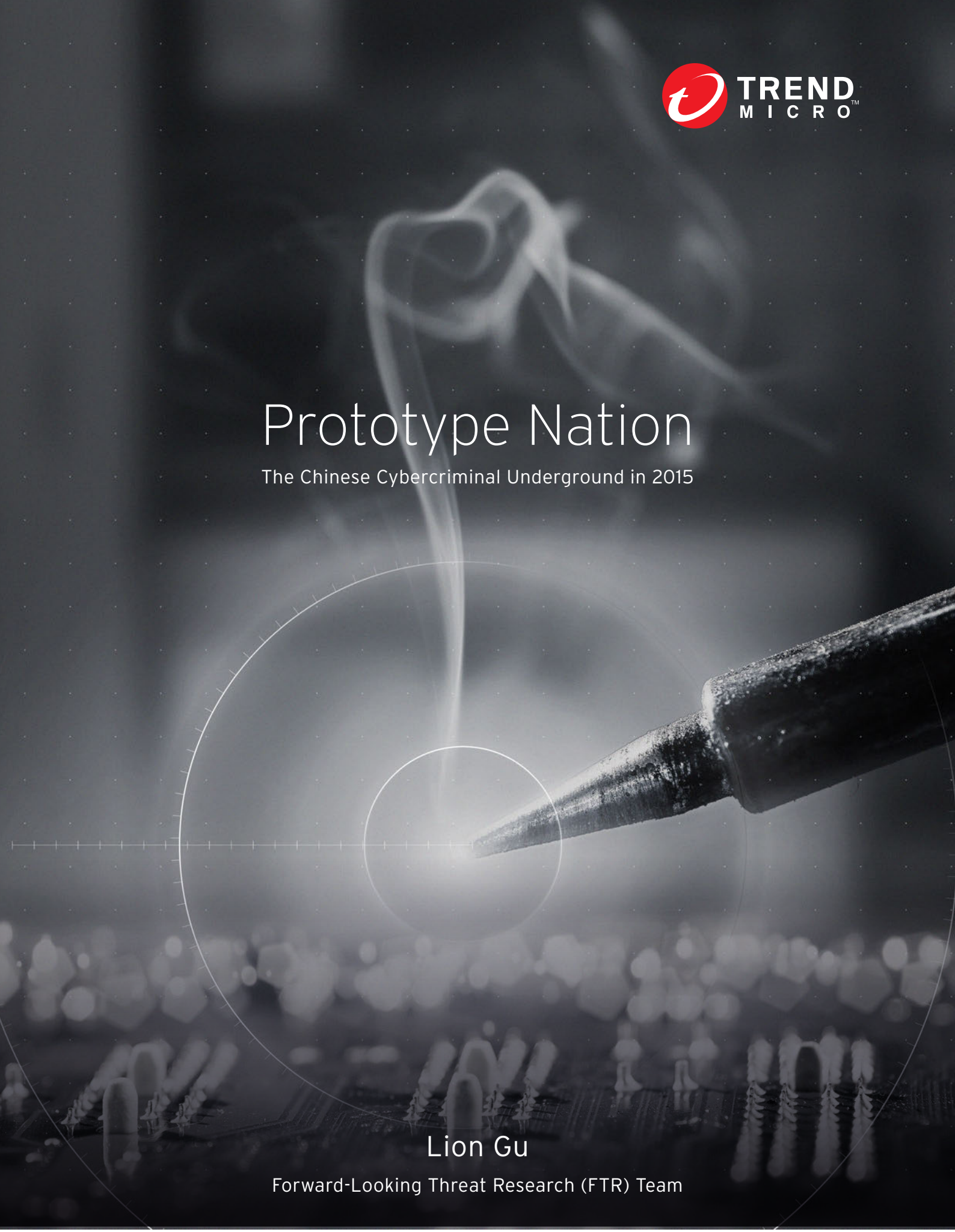


Prototype Nation

The Chinese Cybercriminal Underground in 2015

Lion Gu

Forward-Looking Threat Research (FTR) Team

A **TrendLabs**[SM] Research Paper

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an “as is” condition.

Contents

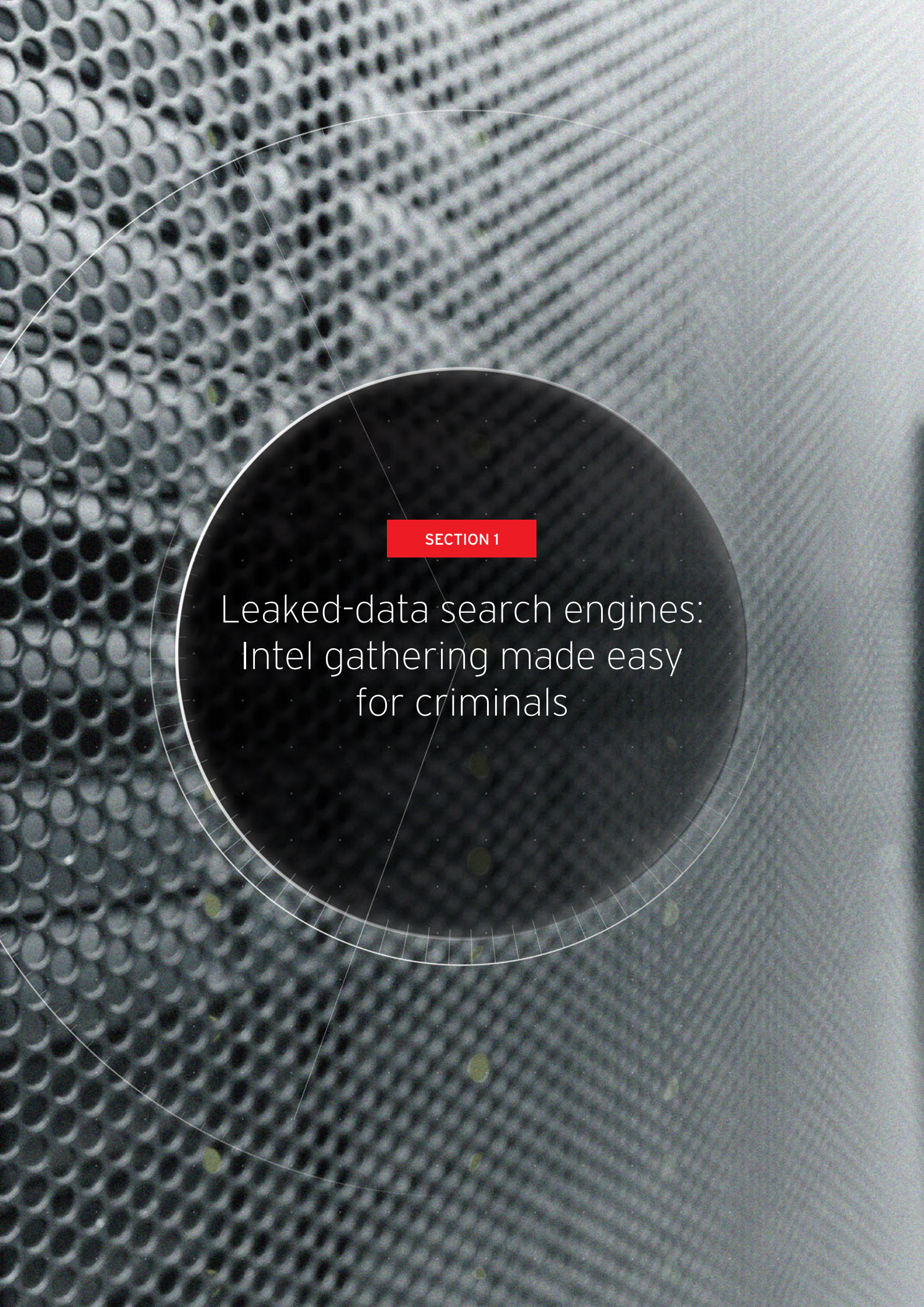
Two years after publishing our last report on the wares and services traded in the bustling Chinese underground[1], we found that the market's operations further expanded. Traditional malware designed to run on all platforms as well as mentorship and hacking services are still heavily present. But with time come new innovations—ones that are now gaining popularity among China's tech-savviest crooks. New hardware and channels have gone beyond being mere proofs of concept (PoCs) to become the working models driving the cybercrime trends in China today.

We saw increased Chinese underground activity over a 10-month period. Chinese-speaking cybercriminals, regardless of nationality, continued to abuse popular Web services like the instant-messaging (IM) app, QQ, to communicate with peers. Through these channels, they offer botnet services used to instigate distributed denial-of-service (DDoS) attacks along with products like exploit kits.

Our past explorations of the Chinese underground, including their thriving mobile underground[2], showed how quickly cybercriminals adapted to technological advancements and existing trends. 2015 was no different, as evidenced by the presence of several recently developed leaked-data search engines.

We have also seen the production and sale of new hardware like point-of-sale (PoS) and automated teller machine (ATM) skimmers. These come with training services that teach cybercriminals how to use the said hardware. Skimmers like these offer cybercriminals a lucrative business model that can negatively affect small and medium-sized businesses (SMBs).

The presence of these offerings show just how well the Chinese underground has not only kept up with events in the real world, but how it is also leading the way in terms of cybercriminal innovation. Other markets—especially those in regions with frequent data-breach- or PoS-related cases—may soon follow.



SECTION 1

Leaked-data search engines: Intel gathering made easy for criminals

Leaked-data search engines: Intel gathering made easy for criminals

The Deep Web is simply the vast and hidden section of the Internet that is not accessible via search engines[3]. A huge chunk of the Deep Web deals with cybercriminal activities and illegal services, a part of which has to do with leaked personal data, including addresses and other sensitive information.

The recent spate of data breaches has resulted in a surplus of data dumps for sale on underground websites[4]. These dumps contain personally identifiable information (PII) and credit card credentials (now sold in bulk, irrespective of brand). PayPal, poker, and even Uber accounts can now also be found via leaked-data search engines, a first in the Chinese and other underground markets.

The data leaked underground allows attackers to commit crimes like financial fraud, identity and intellectual property theft, espionage, and even extortion. Armed with sensitive or potentially damaging information on a politician, for instance, like leaked personal details on an extramarital affair website, a cybercriminal can discredit the target who may be lobbying for the approval of, say, the national cybercrime bill.

Free search engines and forums

CnSeu (cnseu.pw/) is a forum for trading leaked data. Users buy and sell leaked data using forum coins or credit points that can be purchased on Alipay with corresponding amounts in RMB (RMB 1 = 10 forum coins = ~US$0.16*).

** Currency exchange rate as of 26 October 2015 was used for all conversions in this paper (US$1 = RMB 6.34)*

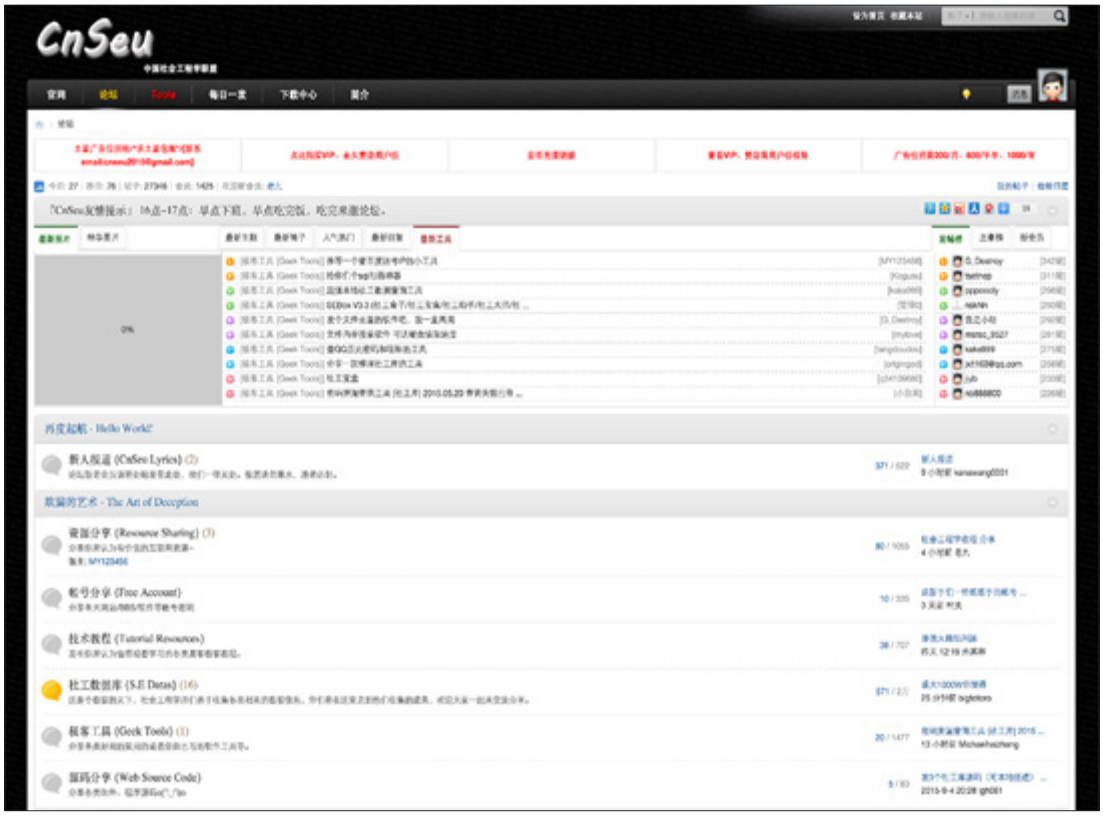


Figure 1: *CnSeu provides users a means to communicate with peers about various topics related to cybercrime resources, tutorials, and tools*

While forums have been keeping cybercriminals connected with one another, they managed to come up with even more ways to offer stolen data. SheYun, a search engine specifically created to make leaked data available to users, is one such way.

Figure 2: *SheYun's search database contains leaked data ranging from bank account credentials to poker account information; users simply have to provide usernames (输入用户名), QQ details, and email addresses to avail of its services*

SheYun also has a database of government-related information that its users can get data from, and ironically, a privacy-protection feature for those who wish to prevent certain data from appearing as search results.

Figure 3: *SheYun users who wish to prevent certain information from appearing as search results can avail of its privacy-protection feature, which costs RMB 100 (~US$16) per keyword; a message saying details are protected by the engine's protection service (*抱歉，此账号已加入*SheYun* 隐私保护服务，详情请看*) appears each time keywords pointing to them are used*

Premium products and services

In 2013, the most popular Chinese underground offerings were compromised hosts, DDoS attack tools and services, and remote access Trojans (RATs)[5].

This year, we discovered new product and service offerings in the Chinese underground. These include social engineering toolkits, comprehensive tool sets required to carry out successful social engineering attacks.

Social Engineering Master (社工大师) is one such tool. It allows cybercriminals to search through leaked data, send spoofed emails, and create fake IDs using templates, among others, for a meager sum of ~RMB 317 (US$50). Users who access Social Engineering Master are automatically redirected to an online payment page if they want to avail of its products and services.

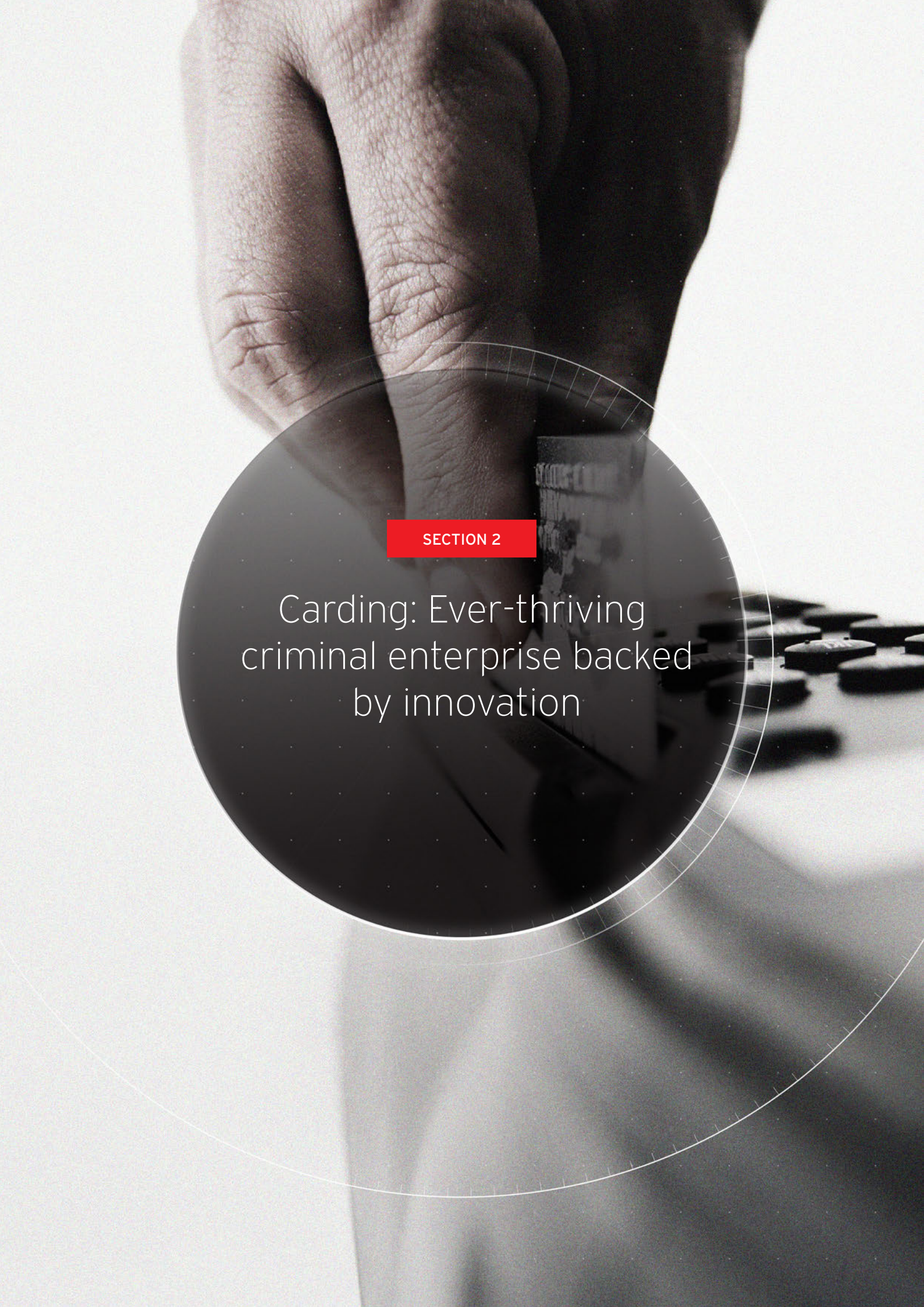
Figure 4: *Social Engineering Master's comprehensive list of features include the ability to obtain data (MD5 hashes, PII, and mobile numbers) from dumps, QQ groups, and hotel registers, along with templates for phishing emails and fake IDs as well as fake WeChat, Alipay, and QQ Wallet balances; it also comes with exploit kits, phishing websites, and Trojan downloaders, among other cybercrime tools*

Figure 5: *Social Engineering Master's main interface contains links to pages where its various features (password [查密码], hotel check-in data [开房记录], QQ group data [查Q关系], all other data [查老密], old password [查老密], and people queries [搜索找人]; social engineering tools [社工搜索]; email-spoofing templates [邮件发送]; fake government [身份证正反] and online ID creation tools [身份伪造]; a social engineering dictionary [社工字典]; fake Alipay [支付宝], WeChat [微信], and QQ Wallet [QQ钱包] balance-modification tools; as well as ready-made exploit kits [网马], QQ Trojans [QQ木马], phishing kits [钓鱼程序], and downloaders [下载者]) can be accessed*

Apart from SheYun, paid engines that allow users to search for cybercriminal offerings also abound. PassBase is one example of such.

Figure 6: *Using PassBase costs RMB 68 (~US$11) per year; its home page warns users about using dangerous query search terms (*请不要使用危险字符查询*)*

Figure 7: *TuoMiMa's service also costs RMB 68 (~US$11) to access its database of dumps, much like SheYun's*



SECTION 2

Carding: Ever-thriving criminal enterprise backed by innovation

Carding: Ever-thriving criminal enterprise backed by innovation

The noncash transaction volume in China has drastically grown over the past two years, made apparent by the adoption of electronic and mobile payment means. Alongside countries in the "emerging Asia" group[6], China is expected to register a 27% noncash payment growth rate, driven by increased Internet use and mobile payment transactions.

Cybercriminals quickly jumped on the noncash payment bandwagon. They now offer carding devices like PoS and ATM skimmers to interested buyers at fairly reasonable prices.

Despite the development of mobile payment systems as PoS terminal alternatives, most SMBs still favor the use of PoS systems for receiving payment. SMBs have thus become easy carding scheme targets. Carding has to do with unsavory forums and websites involved in the increasingly regimented process of stealing and laundering credit card information[7].

Various publicly accessible websites sell PoS, ATM, and credit card pocket skimmers. Skimmers refer to devices that extract data from payment card magnetic strips[8]. In a previously published in-depth study of PoS malware[9], we said skimmers cannot be readily mass deployed for maximum effectiveness; the Chinese underground has now proven otherwise.

Credit card fraud made headlines in February last year, when an individual from Hangzhou was tried in the United States (US) for a successful spam run[10] that cost card providers roughly RMB 5,130,000 (~US$808,855).

PoS skimmers

We found PoS skimmers on the business-to-business (B2B) e-commerce site, 1688.com. These devices were bought by retailers who then resell them to small businesses that are always on the lookout for the most reasonable prices. These resellers may or may not know that the gadgets they are peddling have been tampered with.

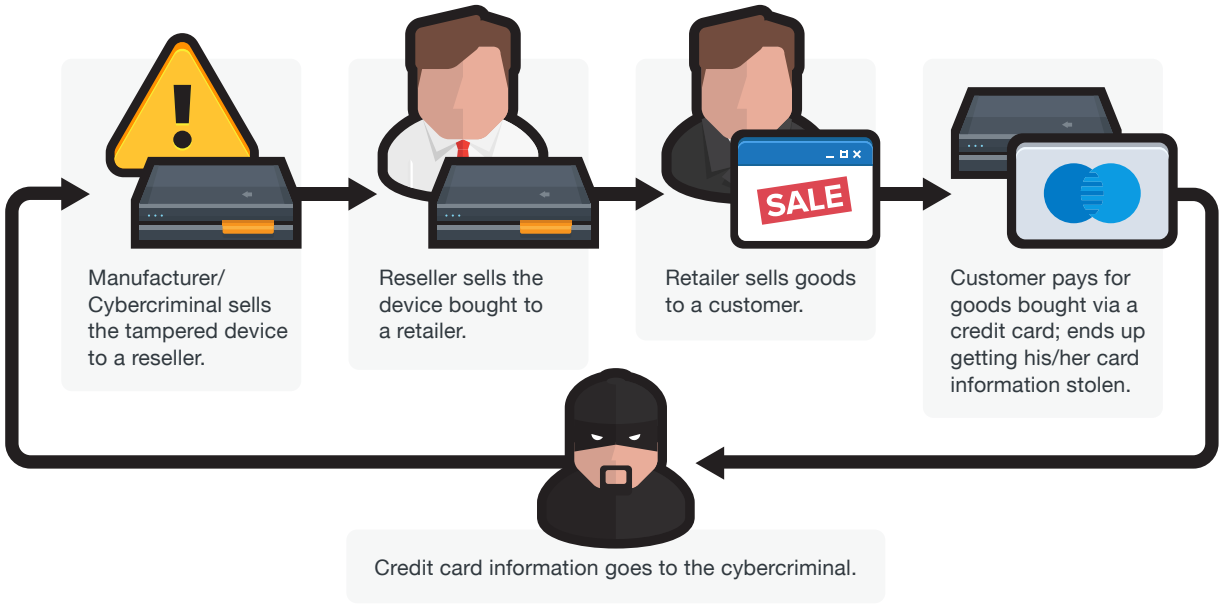


Figure 8: *Typical modus operandi that PoS skimmer sellers use*

Figure 9: *PoS skimmers are sold for RMB 5,000 (~US$788) each on Izise.com; the site is run by a cybercriminal who specializes in selling customized PoS terminals that look no different from those that have not been tampered with, but come with a special chip that allows criminals to authorize otherwise unauthorized purchases*

Some of the PoS skimmers sold underground even have an SMS-notification feature. This allows cybercriminals to instantly get their hands on stolen data via SMS every time the tampered devices are used. Cybercriminals do not even have to physically collect stolen information from installed devices, allowing them greater flexibility and convenience. They can also more easily expand their operational scope by merely installing their skimmers into more PoS devices across stores, countries, and even regions.

Such was the case that made the news just this August[11]. A company reportedly sold the modified devices to a number of small restaurants and hotels. Investigators found 1,100 sets of stolen card information stored in the company's servers. Despite the small number of stolen credit card records, the scammers were still able to cost victims a fairly significant amount—RMB 1.5 million (~US$236,507).

Figure 10: *PoS skimmer with an SMS-notification feature sold for RMB 8,000 (~US$1,261) on 1688.com; the device has been modified to allow cybercriminals to instantly receive credit card numbers (including card verification values [CVVs]) via SMS when used*

Figure 11: *Even chip-and-personal identification number (PIN) card users are unsafe, as some PoS skimmers come with PIN pad skimmers that also have SMS-notification features*

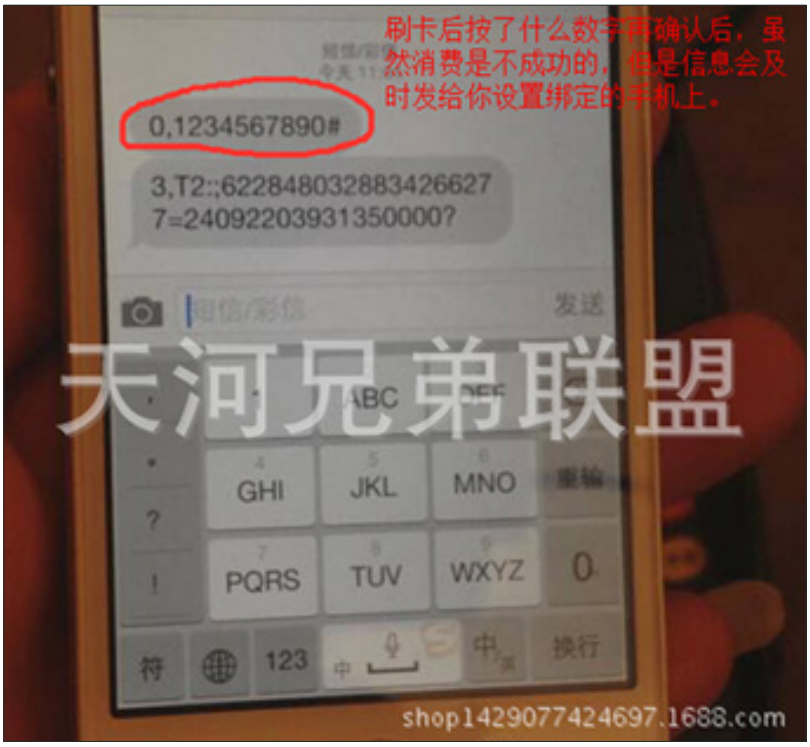


Figure 12: *PoS skimmers with SMS-notification features instantly send stolen data in the format shown above (PIN and credit card number) to cybercriminals*

ATM skimmers

In March 2014, we saw a cybercriminal produce and sell ATM skimmers and fake PoS terminals in several underground forums[12]. These fraud-enabling devices reportedly originated from China. The sale of such devices continued and thrived. What is more worrisome though is that our fear then—that mass production of fraud-enabling devices could very well ensue—has seemingly come true.

Figure 13: *ATM skimmers cost RMB 4,000 (~US$631) each; these came installed with a microchip that records payment card track data or the confidential information stored on a card's magnetic strip, along with a microcamera that allows cybercriminals to obtain a victim's PIN*

ATM PIN skimmers are also commonly sold on B2B websites, offering cybercriminals more ways to successfully carry out bank fraud and actual theft. For a sum of RMB 2,000 (~US$315), fraudsters can use these as keypad overlays in order to more effectively steal victims' PINs. These come with a small memory chip that saves all captured PINs that cybercriminals can physically retrieve in order to gather the information they need to complete their fraudulent acts.

Figure 14: *ATM PIN skimmer sold on the e-commerce website, lzise.com, for RMB 2,000 (~US$315)*

Pocket skimmers

Mass-produced pocket skimmers come in handy for crooks who do not wish to physically tamper with ATMs and PoS terminals in order to steal. These are small and so easily go unnoticed. An unscrupulous store staff member can, for instance, swipe an unwitting customer's card on a pocket skimmer in order to steal track data that he/she can later use for fraud.

Figure 15: *Pocket skimmers are sold for RMB 900 (~US$142) on 1688.com's digital appliances section*

Pocket skimmers are small magnetic card readers that can store track data from up to 2,048 payment cards. They do not need to physically be connected to a computer in order to work. They do not even require an external power supply and can read the data stored on the magnetic strip of any kind of credit card. All stored information can then be downloaded onto a connected computer.

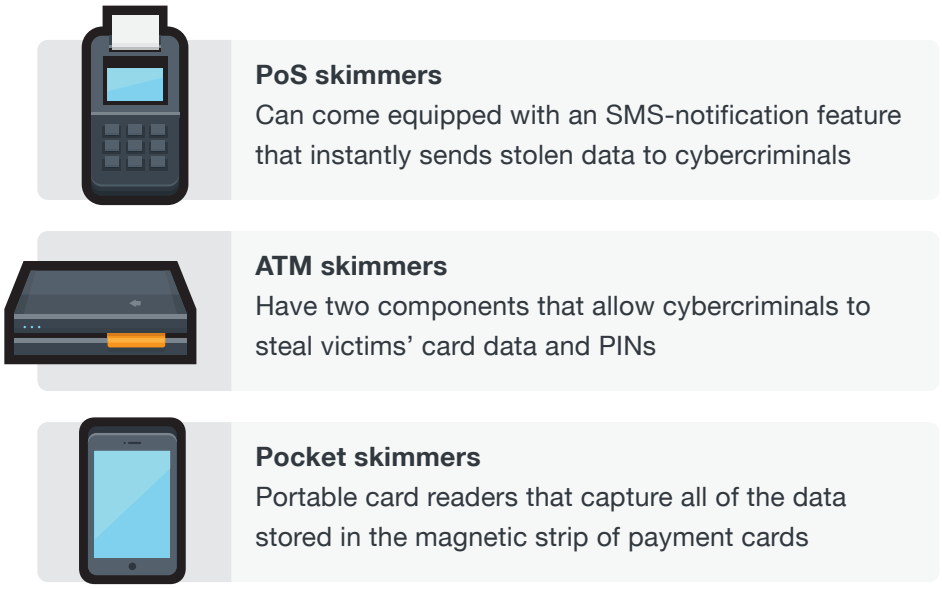


Figure 16: *Skimmers produced and sold in the Chinese underground*

Skimmer tutorials and materials

Hardware specially made to instigate crime are not the only offerings in the Chinese underground. Training services and materials that would-be cybercriminals can make use of also abound.

We found underground dealings in phpBB, an open source forum where users traded information on carding device training and materials. Aided by our Deep Web Analyzer[13], we were able to locate Tor文交流论坛, a website on The Onion Router (TOR) where the phpBB forum was hosted. Access to TOR is blocked in China so the network is hardly used. But since carding has become such a hot commodity in the country, related products and services have cropped up in TOR sites.

Figure 17: *Forum post where carding courses are offered in exchange for bitcoins (2BTC [~US$569.58] ** per "bible," a guide to carding, that will made available in two weeks' time; buyers are guaranteed to get returns on their investment after a week or two); discounts are offered to previous customers; ads for domestic and international credit card track data are also seen*

Figure 18: *Forum post that offers the "Alpha02 CARDING Christmas Version（学院圣诞版)" bible, which teaches users to use carding hardware and software for 0.3BTC (~US$85.44; 50% off discounted rate)*

Similar offerings that can be used to abuse Internet of Things (IoT) devices can also be seen in the Chinese underground. Readily available devices and knowledge shared in anonymous forums will usher in a new wave of more skilled and confident cybercriminals in China.

SECTION 3

Market offerings: As robust as they are unique

Market offerings: As robust as they are unique

Since 2012, we have been providing updated lists of the products and services peddled in the Chinese underground. These offerings are available to any enterprising criminal from anywhere in the world.

Most of the wares we spotted were designed to target Chinese citizens. Americans, Europeans, and the Japanese may experience monetary losses as well since credit card dumps from their countries are also sold in the Chinese underground. Local cybercriminals can either use the credit card data for their own personal gain or sell them to other buyers.

We also noted that bulletproof hosting still plays a significant role in Chinese cybercriminal marketplace. Several local phishing sites as well as sites that sell counterfeit wares all rely on these hosting services to stay up. It's also possible that leaked-data search engines use such services to store the data dumps.

Take a look at the Chinese underground's latest offerings with updated prices from 2013 to 2014 or 2015.

Services

Note that prices in green text under the 2014–2015 column indicate increases while those in blue indicate decreases.

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

Service	Details	2013 price	2014–2015 price
Botnet rental	With 100 Windows 2003 or 2008 bots	US$48	US$24
Carding tutorial			US$0.30–570
Cracking	Encrypted .RAR, .ZIP, .DOC, .XLS, and .EXE files	US$45	US$44
	Protected dongles	US$807–12,919	US$788–12,605
	Software registration codes	US$161	US$158
	Software user-number limitations	US$242	US$236
DDoS attack	100Mbps; 100–2,000 bots (monthly subscription)	US$95–596	US$79
Dedicated server hosting	With DDoS protection (monthly subscription)	US$81–775	US$284–10,669
Document copy rework		US$19	US$19
Email spamming	20,000 email addresses	US$161	US$47
	50,000 email addresses	US$323	US$95
Hacking	QQ and WeChat accounts	US$48–129	US$79
	Personal email accounts	US$48	US$47
	Corporate email accounts	US$81	US$95
	Sina Weibo accounts	US$48	US$63
iMessage® spamming	20,000 messsages		US$205
	50,000 messages		US$433
	80,000 messages		US$630
Privacy protection on leaked-data search engines			US$11–16
Programming	RAT toolkits	US$161	US$158
	Trojans	US$323–8,075	US$315–7,878
Proxy server hosting	Hypertext Transfer Protocol (HTTP), HTTP Secure (HTTPS), or Socket Secure (SOCKS) (monthly subscription)	US$0.16–16	US$15
Security software checking	Makes sure malware are not detected by security software	US$13–19	US$13–19

Service	Details	2013 price	2014–2015 price
SMS spamming	10,000 text messages		US$126
	80,000 text messages		US$882
	100,000 text messages		US$945
Trojan toolkit access	Fengtian remote access toolkit (monthly subscription)		US$47
	MBZ remote access Toolkit (annual subscription)		US$95
Virtual private network (VPN) server hosting	Monthly subscription	US$3	US$3

Products

Note that prices in green text under the 2014–2015 column indicate increases while those in blue indicate decreases.

Product	Details	2013 price	2014–2015 price
ATM PIN skimmers			US$315
ATM skimmers			US$1,261
Banking credential packages	Includes ATM cards, IDs, dongle passwords, and subscriber identity module (SIM) cards		US$126–158
Fake websites	QQ, TaoBao Bank of China, and Industrial and Commercial Bank of China (ICBC)	US$81	US$79
	Various online games	US$16–32	US$16–32
	Online game trading sites	US$81–97	US$79–95
Leaked data packages			US$0.16
Local third-party app (for Android™) popularity boosters	10,000 downloads	US$7	US$8–16
	100 comments		US$32
Pocket skimmers			US$142
PoS skimmers			US$788
Scanned fake documents	Chinese, US, and Canadian passports	US$5	US$5

Product	Details	2013 price	2014–2015 price
Serial keys	Windows® 10 Pro		US$2
	Microsoft™ Office® 2016		US$6
	AutoCAD® 2015		US$12
Sina Weibo popularity boosters	10,000 followers		US$7–161
	5,000 tweets		US$55
	1,000 comments		US$8–63
	5,000 votes (for awards, maybe)		US$55–79
Social engineering toolkits			US$50
Traffic	500 Internet Protocol (IP) addresses per day	US$0.26	US$0.25
	1,000 IP addresses per day	US$0.42	US$0.41
	5,000 IP addresses per day	US$2	US$2
	10,000 IP addresses per day	US$5	US$5
	50,000 IP addresses per day	US$38	US$37
	100,000 IP addresses per day	US$95	US$92
	500,000 IP addresses per day	US$473	US$462
Trojans	QQ account stealers	US$32	US$32
	TaoBao account stealers	US$323	US$315

References

1. Lion Gu. (3 September 2014). *Trend Micro Security Intelligence.* "The Chinese Underground in 2013." Last accessed on 22 October 2015, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-chinese-underground-in-2013.pdf.

2. Lion Gu. (13 November 2014). *Trend Micro Security Intelligence.* "The Mobile Cybercriminal Underground Market in China." Last accessed on 22 October 2015, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-mobile-cybercriminal-underground-market-in-china.pdf.

3. Vincenzo Ciancaglini. (22 June 2015). *TrendLabs Security Intelligence Blog.* "Digging into the Deep Web." Last accessed on 23 October 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/digging-into-the-deep-web/.

4. Numaan Huq. (11 September 2014). *Trend Micro Security Intelligence.* "PoS RAM Scraper Malware: Past, Present, and Future." Last accessed on 22 October 2015, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-pos-ram-scraper-malware.pdf.

5. Lion Gu. (3 September 2014). *TrendLabs Security Intelligence Blog.* "The Chinese Underground in 2013." Last accessed on 26 October 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/the-chinese-underground-in-2013/.

6. Finextra Research. (6 October 2015). *Finextra.* "China and India Drive Noncash Payments Growth." Last accessed on 22 October 2015, http://www.finextra.com/news/fullstory.aspx?newsitemid=27940.

7. Deepdotweb. (17 August 2015). *Deep.Dot.Web.* "Cybercrime: The Study of Carding." Last accessed on 22 October 2015, https://www.deepdotweb.com/2015/08/17/cybercrime-the-study-of-carding/.

8. Brian Krebs. (2015). *Krebs on Security.* "All About Skimmers." Last accessed on 22 October 2015, http://krebsonsecurity.com/all-about-skimmers/.

9. Trend Micro. (22 September 2015). *Trend Micro Security News.* "Follow the Data: Dissecting Data Breaches and Debunking the Myths." Last accessed on 23 October 2015, http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/follow-the-data.

10. Xu Lin. (19 February 2014). *QNSB.* "江西小伙在杭州盗刷美国信用卡套现513万受审." Last accessed on 23 October 2015, http://www.qnsb.com/news/html/2014/caijing_0219/53812.html.

11. Wangen Hui. (17 August 2015). *V.gmw.cn.* "你还敢用POS机刷卡么？小心改装POS机盗刷银行卡." Last accessed on 23 October 2015, http://v.gmw.cn/2015-08/17/content_16696986.htm.

12. Trend Micro. (21 March 2014). *TrendLabs Security Intelligence Blog.* "Mass-Produced ATM Skimmers, Rogue PoS Terminals via 3D Printing?" Last accessed on 23 October 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/mass-produced-atm-skimmers-rogue-pos-terminals-via-3d-printing/.

13. Dr. Vincenzo Ciancaglini, Dr. Marco Balduzzi, Robert McArdle, and Martin Rösler. (2015). *Trend Micro Security Intelligence.* "Below the Surface: Exploring the Deep Web." Last accessed on 23 October 2015, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_below_the_surface.pdf.

Created by:

TrendLabs

The Global Technical Support and R&D Center of **TREND MICRO**

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver topranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit www.trendmicro.com.

TREND MICRO™

Securing Your Journey to the Cloud