



Cybercrime and the Deep Web

Forward-Looking Threat Research (FTR) Team

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

4

What makes each underground market unique?

8

What does each underground market offer?

The cybercriminal underground economy changes every minute. Constantly evolving cybercriminal tools and techniques can put anyone at risk in a split second.

Trend Micro researchers have been monitoring the underground economy for years. We were the first to describe how the different underground markets in Russia, China, Brazil, Japan, Germany, and North America vary. Each country's market is as distinct as its culture. The Russian underground, for instance, can be likened to a well-functioning assembly line where each player has a role to play. It acts as the German market's "big brother" as well in that it greatly influences how the latter works. The Chinese market, meanwhile, boasts of robust tool and hardware development, acting as a prototype hub for cybercriminal wannabes. Brazil is more focused on banking Trojans while Japan tends to be deliberately exclusive to members.

We were also among the first security vendors to dive deep into the underground. Our researchers have been digging into as many seedy markets as possible, each year adding a new country/region to our growing list, to gather precious intel. This allows us to know and monitor what wares cybercriminals sell to their peers, what makes them tick, and how they behave.

Cybercriminals from every corner of the world take advantage of the anonymity of the Web, particularly the Deep Web, to hide from the authorities. Infrastructure and skill differences affect how far into the Deep Web each underground market has gone. Chinese cybercriminals, for instance, do not rely on the Deep Web as much as their German and North American counterparts do. This could, however, be due to the fact that the "great firewall" of China prevents its citizens (even the tech-savviest of its cybercrooks) from accessing the Deep Web. The fact that Germany and North America more strictly implement cybercrime laws may have something to do with their greater reliance on the Deep Web, too.

Crimes aided by wares bought underground can span from simple electronic thievery and selling contraband like drugs and firearms to shocking real-world crimes like engaging in child pornography and offering assassination services.

We will continue to aid in seizing cybercriminals across the globe through public-private partnerships (PPPs) and providing intel that law enforcement agencies can use to further their anti-cybercrime efforts. As we go along making the world safe for the exchange of digital information, we will continue to monitor and report the latest in cybercrime developments so our customers can stay safe from these kinds of threats.

SECTION 1

What makes each underground market unique?



What makes each underground market unique?

Our fight against cybercrime has taken us to six markets so far—Russia, Japan, China, Germany, North America (United States [US] and Canada), and Brazil. And what we found is this—a “global cybercriminal underground market” does not exist. The cybercriminal underground economy is diverse—each market is as unique as the country or region that it caters to.

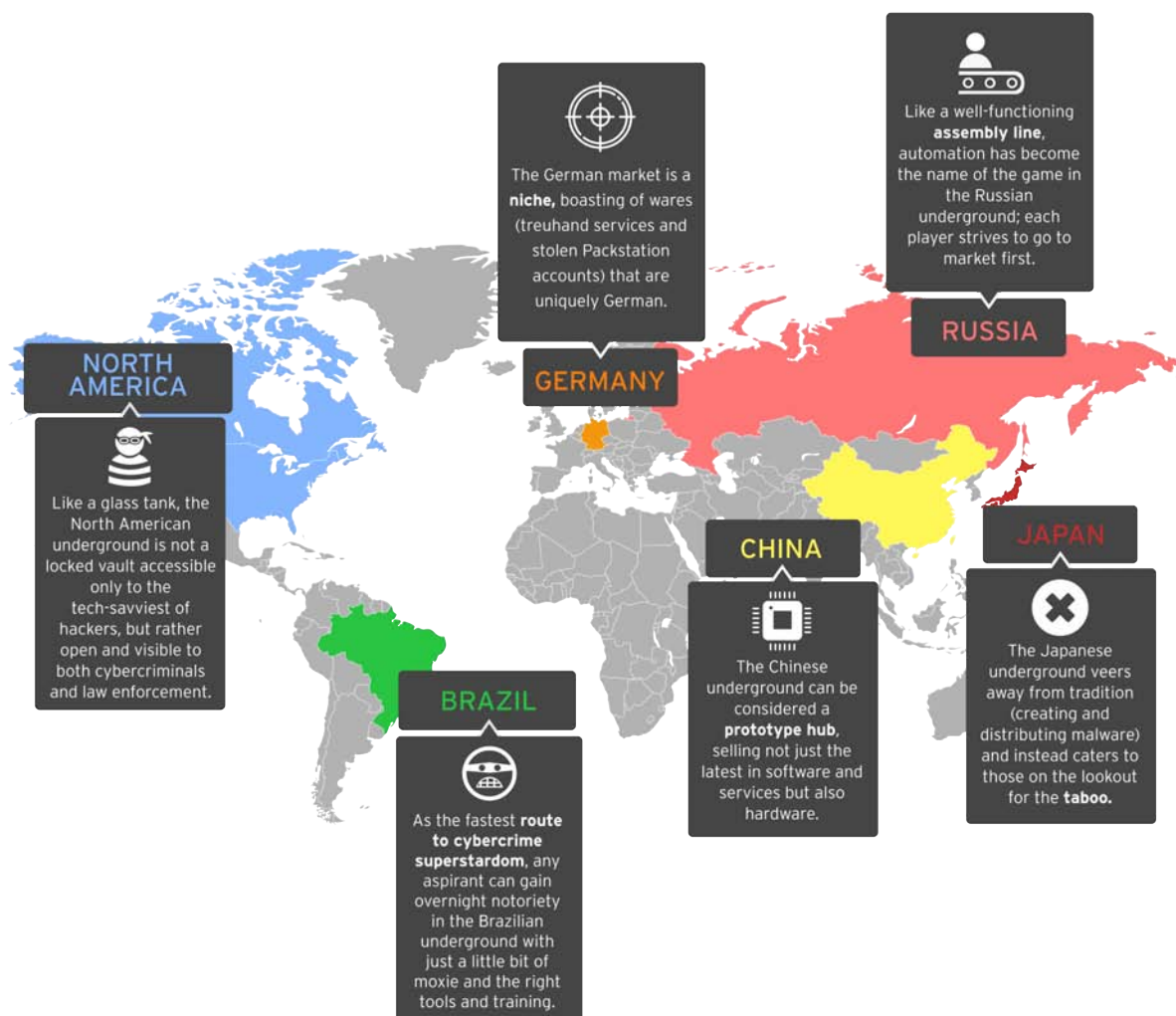


Figure 1: General descriptions of the various underground markets

In our deep dives into the different country/regional markets, we found that:

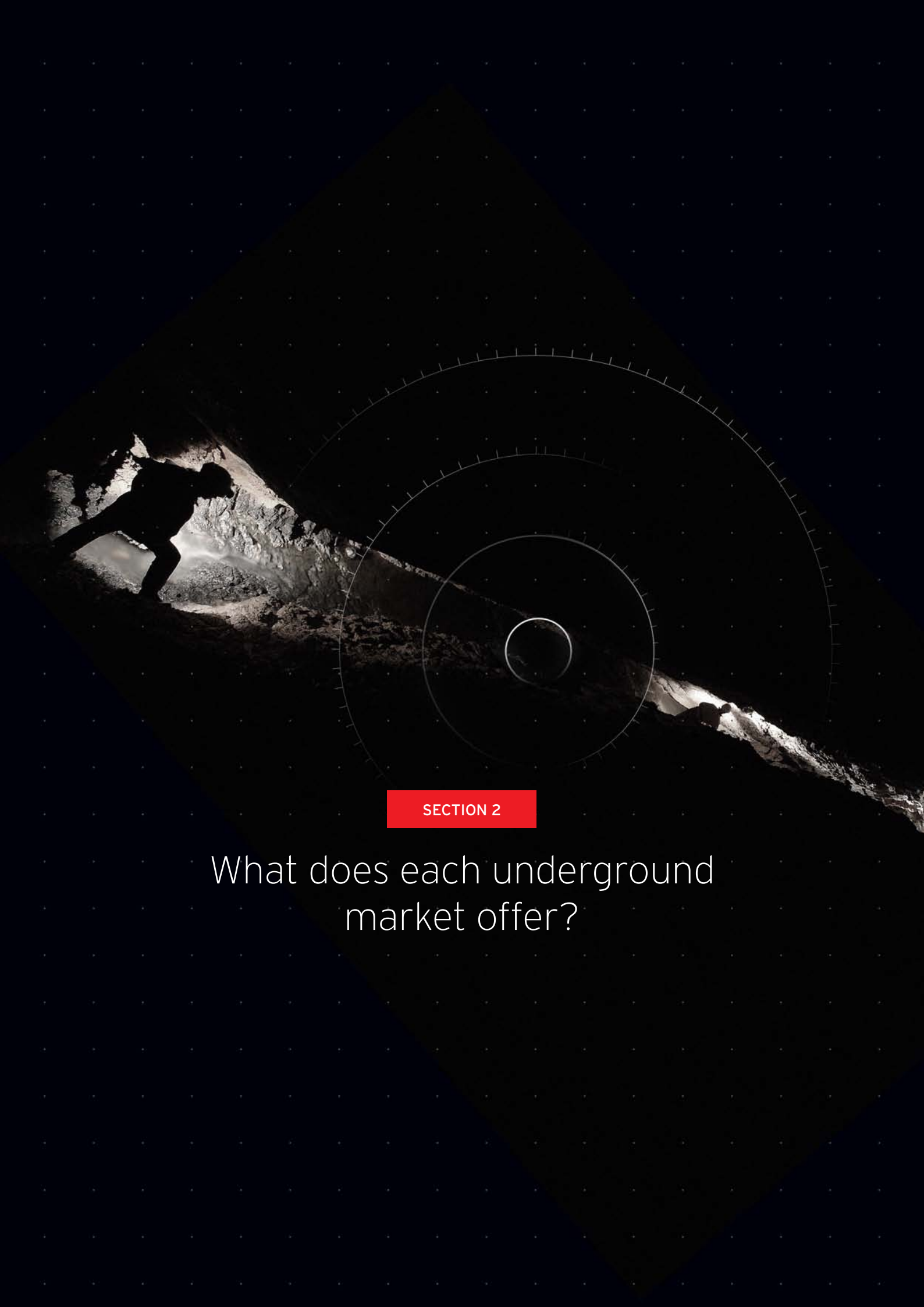
- Much like a well-functioning assembly line, automation has become the name of the game in the Russian underground¹. Stiff competition pushes sellers to step up their game by providing goods in the shortest amount of time and most efficient manner possible. Marketplaces like fe-ccshop.su, which sells credit card dumps and Rescator, which offers carding services through Lampeduza, among others, have taken the place of yesteryear's forums. As in the past, escrows or "garants" still played an important part in business dealings. They continue to guarantee buyers' and sellers' anonymity. As one of the pioneers in the underground economy, the Russian market also plays big brother to its budding counterparts, particularly that of Germany.
- As a market that seems to cater more to the taboo rather than the downright illegal, gating is common in Japan². Trading places, usually closed (for members only) bulletin board systems (BBSs) and forums, are exclusive to native Japanese users/speakers. The use of special jargon was also seen to evade the authorities who strictly implement the country's cybercrime laws. Like its counterparts, anonymity comes at a premium in Japan. But unlike most other markets, cybercriminals in Japan accept more unusual kinds of payment—gift cards and forum points instead of bitcoins or cash paid via money transfer.
- The Chinese underground³ is a teeming hub of prototypes. It not only sells the usual array of software and services found in its counterparts, but also hardware. It adapts the fastest to the latest in cybercrime trends and leads the way in terms of cybercriminal innovation. And true to its adaptive nature, it now boasts of uncommon offerings like leaked-data search engine privacy protection services that can only be dubbed "made in China."
- Unlike its counterparts, the North American underground⁴ does not rely on limiting access for sustainability. It does not close its doors to novices. It encourages cybercriminal activity. It is not a locked vault accessible only to the tech-savviest of hackers but rather a glass tank—open and visible to both cybercriminals and law enforcement.

While the Canadian underground⁵ is not as large or well-developed as others, it is viable. Unlike the US underground, it primarily sells fake/stolen documents and credentials (fake driver's licenses and passports, stolen credit card and other banking information, and credit "fullz" or complete dumps of personal information). It does not exclusively cater to local customers but also sells to cybercriminals in the US and even the Middle East.

- Germany's underground market⁶ has a similar structure to the Deep Web. It offers as many wares as possible to stay up, probably due to limitations like language barrier and its overall size. It caters to a niche set of customers. Its offerings, like a new dropping means that does not require actual droppers and instead relies on fake deliveries by exploiting "Packstation services⁷," which are only familiar to Germans who use its legitimate version offered by DHL. As a still-budding market, it is safe to assume that German cybercriminals often visit the Russian underground to learn from their big brothers. Collaboration between German and Russian market players most likely happens, as evidenced by overlapping profiles, shared resources and parallel sites, and cross-market advertising.

- Dubbed the “fastest route to cybercriminal superstardom,” the Brazilian underground⁸ lets any criminal aspirant gain overnight notoriety so long as he/she has moxie and is armed with the right tools and training. Most of Brazil’s cybercrooks are young and bold, with no regard for the law. They show blatant disregard for the law by the way they use the Surface Web, particularly popular social media sites like Facebook and other public forums and apps. Using online aliases on these sites, they make names for themselves, flagrantly showing off the spoils of their own mini operations. Though they share know-how to peers, they mostly work independently, doing their best to outdo the competition and ascend the ranks to become the top players in their chosen fields.

Despite the nonexistence of a global underground market, cybercriminals worldwide do collaborate with one another. They share tools, intel, know-how, and even best practices with peers. One such tool common across markets is the Deep Web⁹, which better guarantees anonymity—a must when dealing with the taboo and the downright illegal.



SECTION 2

What does each underground
market offer?

What does each underground market offer?

Data breach dumps, exploit kits, malware, and fake documents are underground market staples. But not everyone may know that each market has certain “exclusives.”

Unlike drugs and weapons that are seen in most markets, murder-for-hire or assassination services can only be seen in North America, which more heavily relies on the Deep Web than its counterparts. Stolen Packstation accounts, meanwhile, are uniquely German. Any and every kind of hardware (all kinds of skimming equipment and social engineering toolkits) that cybercriminals can use to carry out their schemes abound in the Chinese underground. In Brazil, modified Android apps with prepaid credits paid for with stolen credit cards and similar wares before peddled in the country’s backstreets have now made their way online.

OFFERING	Russia	Japan	China	Germany	US	Canada	Brazil
Agora invitation code/.onion site access					•		
ATM PIN pad skimmers			•				•
ATM skimmers			•				•
Bots			•	•			
Child-porn related goods		•					
Counterfeit money							•
Credit card clones					•	•	•
Credit card number generators							•
Crypters	•		•	•	•		•
Data dumps	•	•	•	•	•	•	•
Drugs		•		•	•	•	
Exploit kits	•		•	•	•		•
Fake documents	•	•	•	•	•	•	•
Fake websites			•		•	•	
How-to guides/modules			•		•	•	
Malware	•	•	•	•	•		•
Modified Android apps with prepaid credits paid for with stolen credit cards							•

OFFERING	Russia	Japan	China	Germany	US	Canada	Brazil
Modified smart card readers and writers							•
Phone number databases		•			•	•	•
Pocket payment card skimmers			•				•
Point-of-sale (PoS) skimmers			•				•
Serial keys			•	•			
Social engineering toolkits			•				
Stolen Packstation accounts				•			
Weapons		•			•		
Web popularity boosters			•		•	•	•
Web traffic	•		•	•			

Note: The list of products above is not exhaustive. It has been limited to the products seen in the country markets at the time research was conducted.

Table 1: Products sold in the various underground markets

OFFERING	Russia	Japan	China	Germany	US	Canada	Brazil
Antimalware proofing	•		•				
Antispam proofing	•						
Apple App Store app rank boosting			•				
Bitcoin tumbling		•					
Bulletproof hosting	•		•	•	•		
Coding/Programming			•	•			
Compromised server access	•			•	•		
Compromised credit card panel access							•
Cracking			•				
Crypting					•		
Distributed denial-of-service (DDoS) attack	•		•		•		
Document copy rework			•				
Dropping	•						
Escrow/Garant/Treuhand	•			•			
Fast fluxing				•			
Hacking			•				
Internet and CATV access plan bump-up							•
Leaked-data search engine privacy protection/subscription			•				
Mule		•					
Murder for hire					•		
Payment card validity checking	•						
Personally identifiable information (PII) querying							•
Proxy	•		•	•	•		

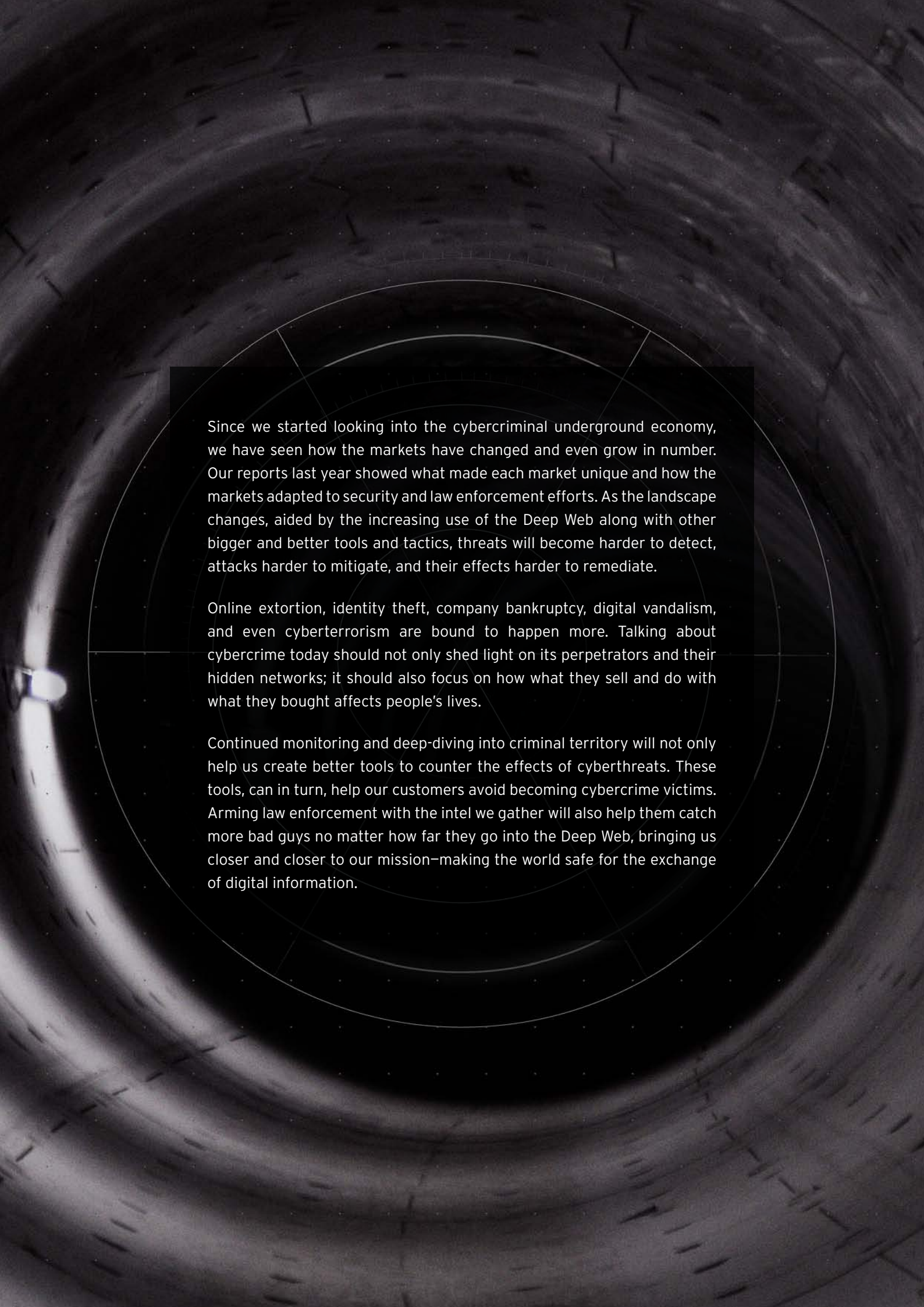
OFFERING	Russia	Japan	China	Germany	US	Canada	Brazil
Spamming	•		•				
Spying using Web cameras		•					
Translation	•						
Trojan toolkit access subscription			•				
Tutorial	•	•	•		•		

Note: The list of services above is not exhaustive. It has been limited to the services seen in the country markets at the time research was conducted.

Table 2: Services sold in the various underground markets

Country markets not only differ in terms of offerings; their business models vary, too. Cybercriminals in China and Brazil, for instance, favor instant-messaging apps and social networks for business transactions. Closely guarded (for members only) BBSs, meanwhile, heavily figured in Japan. And cybercriminals in Germany and North America, which have more strictly implemented laws, are starting to delve further into the Deep Web to better hide from the prying eyes of law enforcement.

German and North American cybercriminals, compared with those from other countries, more heavily rely on the Deep Web. But that does not mean that crooks from Russia, China, Japan, and Brazil do not take advantage of the anonymity that it offers. The same wares found in the different country markets are available in Deep Web marketplaces. The only difference—trade is more or less “borderless” in the Deep Web. Anyone can exchange goods with everyone else, regardless of race, color, or creed.



Since we started looking into the cybercriminal underground economy, we have seen how the markets have changed and even grow in number. Our reports last year showed what made each market unique and how the markets adapted to security and law enforcement efforts. As the landscape changes, aided by the increasing use of the Deep Web along with other bigger and better tools and tactics, threats will become harder to detect, attacks harder to mitigate, and their effects harder to remediate.

Online extortion, identity theft, company bankruptcy, digital vandalism, and even cyberterrorism are bound to happen more. Talking about cybercrime today should not only shed light on its perpetrators and their hidden networks; it should also focus on how what they sell and do with what they bought affects people's lives.

Continued monitoring and deep-diving into criminal territory will not only help us create better tools to counter the effects of cyberthreats. These tools, can in turn, help our customers avoid becoming cybercrime victims. Arming law enforcement with the intel we gather will also help them catch more bad guys no matter how far they go into the Deep Web, bringing us closer and closer to our mission—making the world safe for the exchange of digital information.

References

1. Max Goncharov. (28 July 2015). *Trend Micro Security News*. “The Russian Underground Today: Automated Infrastructure, Sophisticated Tools.” Last accessed on 1 February 2016, <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/russian-underground-automized-infrastructure-services-sophisticated-tools>.
2. Akira Urano. (13 October 2015). *Trend Micro Security News*. “The Japanese Underground: Japan’s Unique Cybercriminal Economy.” Last accessed on 1 February 2016, <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-japanese-underground>.
3. Lion Gu. (23 November 2015). *Trend Micro Security News*. “Prototype Nation: The Chinese Cybercriminal Underground in 2015.” Last accessed on 1 February 2016, <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/prototype-nation-the-chinese-cybercriminal-underground-in-2015>.
4. Kyle Wilhoit and Stephen Hilt. (7 December 2015). *Trend Micro Security News*. “North American Underground: The Glass Tank.” Last accessed on 1 February 2016, <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/north-american-underground-the-glass-tank>.
5. Natasha Hellberg. (5 January 2016). *Trend Micro Security Intelligence Blog*. “What About Canada, Eh?—The Canadian Threat Landscape.” Last accessed on 1 February 2016, <http://blog.trendmicro.com/trendlabs-security-intelligence/what-about-canada-eh-the-canadian-threat-landscape/>.
6. Max Goncharov. (8 December 2015). *Trend Micro Security News*. “U-Markt: The German Cybercriminal Underground.” Last accessed on 1 February 2016, <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/u-markt-the-german-cybercriminal-underground>.
7. DHL. (2016). *DHL*. “DHL recipient service—Packstation.” Last accessed on 3 February 2016, <http://www.dhl.de/en/paket/pakete-empfangen/packstation.html>.
8. FTR Team. (12 January 2016). *Trend Micro Security News*. “Ascending the Ranks: The Brazilian Cybercriminal Underground in 2015.” Last accessed on 1 February 2016, <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/brazilian-cybercriminal-underground-2015>.
9. Dr. Vincenzo Ciancaglini, Dr. Marco Balduzzi, Robert McArdle, and Martin Rösler. (22 June 2015). *Trend Micro Security News*. “Going Deeper: Exploring the Deep Web.” Last accessed on 1 February 2016, <http://www.trendmicro.com.ph/vinfo/ph/security/news/cybercrime-and-digital-threats/exploring-the-deep-web>.

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 top-ranked 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.



Securing Your Journey
to the Cloud