How China's cybercrime underground is making money off big data

intel471.com/blog/china-cybercrime-big-data-privacy-laws

Both of these things are true: Big data is big business, and cybercriminals love money. So it shouldn't be a surprise that these two ideas have blended together in some corners of the cybercrime underground.

Through Intel 471's observation and analysis of open source information and behavior on multiple closed forums, we found actors adopting the use of legitimate big data technology for cybercrime and monetizing the data they obtain on the Chinese-language underground.

The behavior we have analyzed points to a cycle that involves several different layers of cybercriminals, the use of insider information, and unwitting victims in order to earn ill-gotten gains. The schemes themselves proliferate partly due to China's desire to be a global epicenter in big data analytics, especially as it pushes to become synonymous with new technology sectors like the Internet of Things (IoT). With China injecting big data into every economic sector, the environment has become ripe for criminals to create and execute schemes that hide in the noise brought on by the amount of data at hand.

Why the schemes work

As big data becomes a key cog in Chinese industry, the management, regulation, and governance around data has become a growing challenge for the country. Like much of the industrialized economies in the world, China's big data sector is worth hundreds of billions of dollars.

A 2019 report compiled by the China Industrial Control Systems Cyber Emergency Response Team (CICS-CERT) that examined more than 3,000 big data-related companies found that the industry was worth more than 800 billion yuan (about US $122 billion) in 2019. By the end of 2020, the report projected the industry's worth to exceed 1 trillion yuan (about US $156 billion). Another report published earlier this year by a Chinese think tank found big data practices were well integrated with the communications, finance, internet and security industries. Increasingly, it is also becoming a key part of business in sectors such as energy, industry and transportation.

That growth has not been paired with oversight. We observed several problems documented in open source articles that reported the increased difficulty of regulating and governing big data. The lines between private and public data are not clearly defined, while security risks in

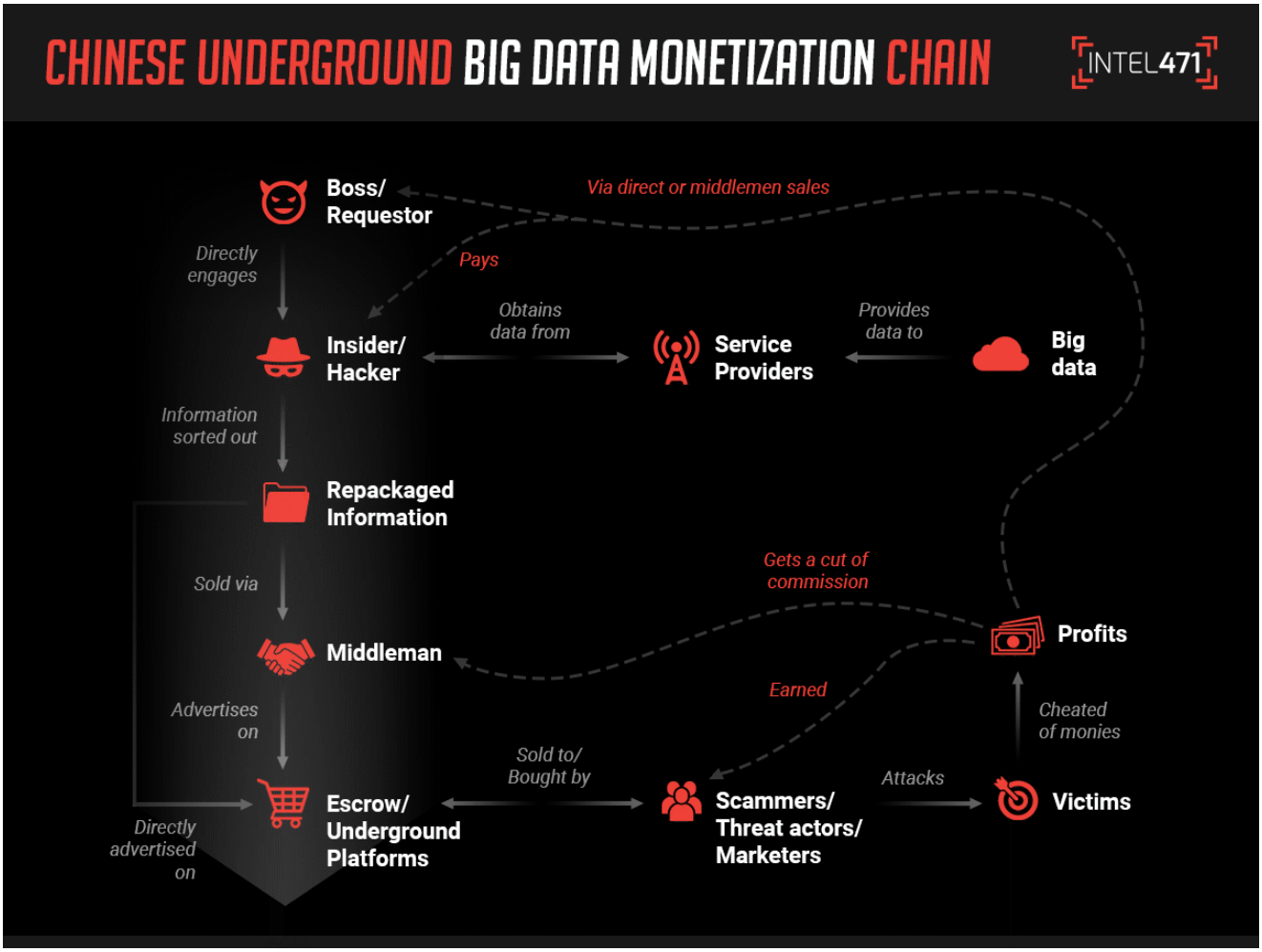
data collection, storage and sharing add to the challenges from a security perspective. The correct usage and protection of personal information in China is largely dependent on the companies themselves.

How the scheme works

We have observed the a data underground monetization chain within the Chinese-language underground consisting of the following groups or individuals with a clear division of labor, responsibilities and a delineated chain of command that includes:

- A boss or requester who requires data for illegal use or commands a group or syndicate dealing with illegal products or services.
- Insiders or hackers who receive instructions directly from a boss and can gain access to raw data and extract the information from a service provider. These individuals profit from the information they provide to the main boss or requester.
- Middlemen who act as intermediaries for the boss and any other individuals requesting to purchase such data products. The middlemen profit by taking a cut of the commission from product sales.
- Escrow and underground platforms which serve as an avenue for the syndicate or middlemen to advertise their products. End users, such as scammers, multiple types of threat actors and even direct marketers can purchase the data or engage the services of such syndicates directly on these platforms.

The graphic below shows how this chain tends to progress:



Where the schemes make money

Intel 471 has observed numerous listings on forums popular in the Chinese cybercrime underground, including:

- One actor in January 2021 offered real-time data for casino gaming, lottery and stocks on a popular forum used by chinese-linked cybercriminals. The data allegedly originated from big data sources of the two of most popular mobile network operators in China.
- An actor in February 2021 offered website and application crawler data collection services on a Chinese-language cybercrime marketplace. The actor claimed to have access to insider channels of Chinese mobile operators for data collection purposes.
- In early March, an actor on a marketplace offered 10,000 user records tied to a parenting application. The offering was described as big data from an undisclosed mobile operator or operators.
- In late March, another actor offered big data information for Canada and the U.S. that included commercial databases of Canadian and U.S. businesses and investors, a hacked Twitter database and Canadian and U.S. citizens' information.

What is being done to stop the schemes

Chinese law enforcement has tried in recent years to hold companies accountable for how they handle. In 2019, seemingly legitimate Chinese companies also were observed providing third-party data crawling services and selling the data collected from unknown victims to reap a profit in addition to being exploited by underground threat actors. Our research identified an article discussing the circumstances surrounding the arrests of the following individuals and entities:

- **Sept. 12, 2019:** Police apprehended the general manager, deputy general manager and marketers of 天翼征信 (Eng. Tianyi Credit) for investigation. Tianyi Credit is a subsidiary of the state-owned telecommunications service provider China Telecom Corp. Ltd.
- **Sept. 11, 2019:** Law enforcement officers suspended and seized the operations of 杭州存信数据科技有限公司 (Eng. Hangzhou Cunxin Data Technology Co. Ltd.) Hangzhou Cunxin Data Technology Co. Ltd. is the physical entity operating 公信宝 (GXB), a blockchain-based decentralized data exchange.
- **Sept. 6, 2019:** Police requested the CEO of 新颜科技人工智能科技有限公司 (Eng. Xinyan Artificial Intelligence Tech Co. Ltd.) assist in investigations.
- **Sept. 6, 2019:** Law enforcement officers apprehended the CEO of the well-known Hangzhou-based big data service company 杭州魔蝎数据科技有限公司 (Eng. Hangzhou Magic Scorpion Data Technology Co. Ltd.) and placed restrictions on the company.

According to the Chinese state broadcaster China Central Television (CCTV) on its annual name-and-shame television program 3.15晚会 (Eng. 3.15 Gala), another 11 companies were exposed for harassing people over the phone, marketing big-data related products and services that are actually against Chinese privacy laws, and other violations of user privacy. Although the companies named were not large in operational scale, they were linked to a bigger group of well-known companies.

Chinese authorities reportedly adopted measures to crack down on the illegal big data trade and tighten regulations governing personal data and privacy. A series of regulatory measures regarding internet privacy protection and the security of personal information reportedly was introduced by the Cyberspace Administration of China in addition to the large-scale crackdown.

Nations that are highly digitized have struggled with privacy over the last decade. We've seen laws like GDPR, CCPA, and PDPA put in place to help citizens exercise some control over the information they generate on the internet. However, if more scenarios like China's underground big data trade are replicated as other countries develop data-reliant economies, regulations and law enforcement are going to face an uphill battle in stopping data trading schemes. The prevalence of these schemes show the importance of securing the data businesses generate on the same levels as the services that keep business running on a day-to-day basis.