SECURITY INTELLIGENCE

Security News

Current Threat Activity

Threat Intelligence Center

Threat Encyclopedia

Glossary

Research & Analysis

Awareness & Prevention

Social @ Trend Micro

Events

Free Tools, Apps & Widgets

Search Threat Encyclopedi

Latest Threats

Malware ⊖

BKDR_KASIDET.XXRO

ANDROIDOS_WORMHOLE.HRXA

ELF_XORDDOS.AP

Spam ⊕

Malicious URL ⊕

Vulnerability ⊕

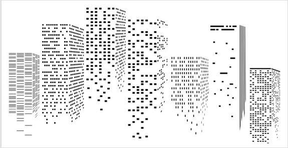
TARGETED ATTACKS

View the latest information, updates, and research on targeted attacks, and advice on how to defend against them.
Learn about targeted attacks

THREAT INTELLIGENCE: THE DEEP WEB

The latest research and information on the deep web and the cybercriminal underground.
Learn more about the Deep Web

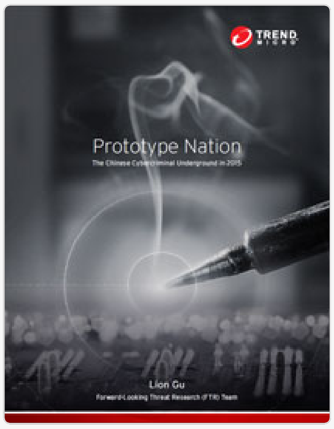
FOLLOW THE DATA



SECURITY NEWS

Prototype Nation: The Chinese Cybercriminal Underground in 2015

November 23, 2015



Prototype Nation
The Chinese Cybercriminal Underground in 2015
Lion Gu
Forward-Looking Threat Research (FTR) Team

View Prototype Nation: The Chinese Cybercriminal Underground in 2015

By the end of 2013, the Chinese cybercrime underground was a very busy economy, with peddled wares that not only targeted PCs, but mobile devices as well—making it its most prolific segment. We also saw cybercriminals abusing popular Web services such as the instant-messaging app (IM), QQ, to communicate with peers.

Today, the Chinese underground is thriving more than ever. Previous explorations in the Chinese underground have indicated that cybercriminals are quick to adapt to technological advancements and existing trends as seen throughout 2015. Data (either leaked or stolen) are now being traded along with prototypes and new functional hardware, like point-of-sales (PoS) and automated teller machine (ATM) skimmers. As the Chinese underground continues to burgeon, we expect to see more cybercriminal activity using these new market offerings:

Leaked data search engines and other offerings

Data leaked in the underground allows cybercriminals to commit various crimes like financial fraud, identity and intellectual property theft, espionage, and extortion. Chinese cybercriminals have managed to enhance the way they share data as seen in the case of SheYun, a search engine created specifically to make leaked data to users available.

Over the last few years, we have been keeping track of the shift of prices of goods and services traded in the Chinese underground. Previously, we saw compromised hosts, DDoS attack tools services, and remote access Trojans (RATs) being sold. Today, social engineering tools have been added to the market.

Carding devices

Cash transactions are slowly becoming a thing of the past, as evidenced by the adoption of electronic and mobile payment means.

- **PoS skimmers** - Tampered PoS devices are sold to resellers who may or may not know that these devices are rigged. Some PoS skimmers come with an SMS-notification feature that allows the cybercriminal to access the stolen data remotely every time the device is used.
- **ATM skimmers** –Commonly sold on B2B websites, these fraud-enabling devices allowed fraudsters to carry out bank fraud and actual theft. The devices have keypad overlays that are used to steal victims' PINs.
- **Pocket skimmers** – These small, unnoticeable magnetic card readers can store track data of up to 2,048 payment cards. They do not need to be physically connected to a computer or a power supply to work. All captured data can be downloaded onto a connected computer.

Our paper, *Prototype Nation: The Chinese Cybercriminal Underground in 2015* provides a closer look into the country's underground market and how it has kept up with events in the real world.

Posted in Cybercrime & Digital Threats, Research, Cybercrime, Cybercriminal Underground Economy Series

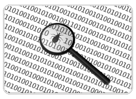
Related Posts

- Five Things We're Thankful for This 2015
- Lesson Learned from ProtonMail Incident: Do Not Pay Cybercriminals
- 2016 Security Predictions: The Fine Line
- The Japanese Underground: Japan's Unique Cybercriminal Economy
- Next-Gen Payment Processing Technologies: What They Are, and How They Work

Recent Posts

- Prototype Nation: The Chinese Cybercriminal Underground in 2015
- InstaAgent App Proves that Social Media View Scam is Still Effective
- Hazards Ahead: Current Vulnerabilities Prelude Impending Attacks
- B2B Extortion? New Ransomware Business Takes 10 Percent Cut from Its Customers
- Five Things We're Thankful for This 2015

We Recommend



HP Pulls Out of Hacking Contest, Citing Changes to Wassenaar Arrangement

Hazards Ahead: Current Vulnerabilities Prelude Impending Attacks

The Trend Micro Expert Insight Series

B2B Extortion? New Ransomware Business Takes 10 Percent Cut from Its Customers

↑ Top of page

CONNECT WITH US ON