No pandas, just people: The current state of China's cybercrime underground

intel471.com/blog/china-cybercrime-undergrond-deepmix-tea-horse-road-great-firewall

China's internet is a lot different than the rest of the world. Yet, that hasn't stopped its population from engaging in cybercrime.

Despite the various measures the Chinese government has taken to censor and surveil its residents on the internet, a significant cybercrime underground full of financially motivated actors exists. Efforts like "The Great Firewall" or government crackdowns on content related to cybercrime force actors to put in remarkable effort to maneuver around those roadblocks in order to access, create or participate in criminal marketplaces that mirror those more commonly known to the rest of the world.

Data from Intel 471 show that the Chinese cybercrime underground proliferates through use of common methods or platforms, but behaves differently in large part due to the caution that actors take with regard to their identity. While the average citizen must follow the heavy handed nature of the government's surveillance of cyberspace, Chinese threat actors take special precautions to protect their forums, TTPs and themselves. This leads to the Chinese cybercrime underground being disorderly when compared to others, particularly Russia, which tend to be much more organized.

Where is the Underground?

Forums hosted on the Tor network have barriers to entry for most Chinese users as the government blocks Tor on the Chinese internet. In order for actors operating in mainland China to access these services, they need a VPN or similar measure capable of evading government detection. Guides and toolkits that allow a user to accomplish this task are often available on the underground. However, if actors do break through — or are operating from other popular Chinese cybercriminal hubs like Hong Kong, Malaysia, Myanmar, The Philippines, and Taiwan — there are a host of forums used by cybercriminals.

DeepMix Market

DeepMix Market is one of the most well-known Chinese underground marketplaces, even after disappearing for several weeks in 2019 after a sustained DDoS attack. It eventually resurfaced in December 2019, with enhanced protections for its users.

The marketplace's offerings are categorized into several sections, including "data-information," "service-orders," virtual resources, physical goods, techniques and tutorials, and carding materials/CVVs, among others. It also uses heightened measures to ensure anonymity, such as discouraging users to post contact details, encouraging users to buy and

sell things via the in-forum system, and forcing users to use small numeric handles to identify accounts. Actors on DeepMix have used the same handles for long periods of time in order to build brand awareness, reflecting that reputation is still paramount even as identity is a highly sensitive subject.

United Chinese Escrow Market

The United Chinese Escrow Market, or UCEM, was established in June 2018 to sell goods and services like those on DeepMix, but differs in that users can set up their own independent shops instead of relying on one central purchasing hub. Marketplace postings are listed in U.S. dollars, but bitcoin is the only accepted currency for transactions, with an exchange rate determined by a third-party payment service provider. The site also has functions similar to other ecommerce sites, including sections where users can discuss their transaction experience, an internal mailbox function to communicate with other members, a bitcoin wallet management section.

Tea Horse Road

Established in June 2019, Tea Horse Road is similar to UCEM and DeepMix in allowing for trading different goods and services, but the site also includes a forum where users discuss or sell data, vulnerabilities or other virtual and physical goods. Earlier this year, Intel 471 saw a number of marketplace users spin up Telegram channels that were affiliated with the site, made in order to provide an extra layer of security when discussing listings or other site-related matters. These channels are very active, with users heavily engaged in discussions while being careful not to include information that might reveal account handles on the actual site.

Free City

Free City is similar to Tea Horse Road, particularly due to use of Telegram channels. The marketplace has seven sections for users: data and intel, services and order replacement, virtual resources, physical goods, specialized products, CVV and carding, and private escrow transactions. The Telegram channels allow users to discuss what's for sale in the forums, while also hosting tutorials and other information related to making purchases.

Open Web forums

Open web hacking forums where Chinese cybercriminals congregate do exist, but often get shut down by the Chinese government. There have been numerous initiatives launched under Chinese President Xi Jinping that have led to the crackdown of what the government has deemed to be illicit internet content. In April 2020, China's Ministry of Public Security announced it punished 1,522 people for public security and notified other departments to

give 433 party and political sanctions for matters related to cybercrime. Some of the more popular open web forums, like HLODAY or HZDG (华中帝国, also known as China Central Empire), have gone down during this time.

More often, skilled Chinese actors make their way to international forums, such as Exploit, Hack Forums, Raid Forums and XSS. These actors advertise tools and services like any other member: compromised payment cards, information or data, ransomware, cryptomining malware and more.

Messaging Clients

The Telegram channels tied to Tor services is indicative of another trend: Chinese actors like to use messaging clients to converse with each other in the underground. This is partly due to the familiarity of the greater Chinese population with messaging platforms like WeChat and QQ, which are extremely popular among Chinese internet users. However, those platforms fall under the same government restrictions as the rest of the country's internet. Therefore, we have seen Chinese actors move to non-native messaging services like Telegram. Non-native services decrease the likelihood of linking online personas to real offline identities, as well as provide end-to-end encryption to ensure greater anonymity.

How are they accessing the underground?

Because of the anonymity and censorship circumvention needed to develop and sell malware or stolen data, Chinese actors have learned to be extremely adaptable. The Chinese government's efforts to watch its population's internet activity means there is no anonymous access, since an IP address can be tied to an actual person. This results in the anonymity of a Chinese actor being "thinner" than in other areas of the world.

In order to evade detection, Chinese actors will change IP addresses by joining different WiFi networks and getting modems to request a new dynamic host configuration protocol (DHCP) addresses, use the TOR network, leverage VPN and proxy services to bypass the Great Firewall, use codewords to avoid keyword filters, and tools such as shadowsocks relay (ssr) and V2Ray.

Additionally, the fact that some actors do manage to bypass the censorship measures and access international sites and services means that although the latest tools and techniques are available to the Chinese underground, not everyone has access to them. This has led to a trend of Chinese actors modifying source code of freeware and malware families to develop their own versions for use, distribution and sale, or using popular forums such as GitHub to refine their skills, fine tune tools or access the latest malware.

What do they sell on the underground?

Because getting around the Great Firewall can be so difficult, a lot of the malware being pushed on Chinese cybercriminal underground forums is built upon existing tools. Intel 471 has observed numerous Remote Access Trojans (RATs) that are variants of already known malware or pentesting tools, such as:

- Anubis
- AsyncRAT
- Cobalt Strike
- Ghost
- Gray Pigeon
- Gray Wolf
- NjRAT
- Spynote

We also observed popular tools such as worms, brute forcers, DDoS tools and post-exploitation tools, as well as exploits for vulnerabilities in web servers for Apache, Oracle and Microsoft Windows. There was also interest in software that mines cryptocurrencies while also attempting to steal wallets or credentials to access online wallets. Additionally, both international (GandCrab, WannaCry) and domestic (FilesLocker) variants of ransomware were placed on various forums.

Specific behavior that stood on these forums was: hacking of illegal gambling sites, QQ tools, blackhat search engine optimization services, spamming, scamming, and other actions that lead to ripping off other members of the cybercriminal underground.

What does the future hold?

As long as the Chinese government shows the ability and desire to crack down on its population's internet activity, highly-skilled actors will continue to closely guard their skills and identity in an effort to avoid being caught. Petty criminals and script kiddies may thrive while the proficient will continue to fly under the radar by avoiding public posts of high-profile breaches, access and or custom tools. With the censorship and surveillance practices carried out by the Chinese government unlikely to stop, the variety of forums, as well as different TTPs employed by actors, likely will continue to adapt and evolve in order to make as much money as possible.

The above information has been pulled from an Intel 471 whitepaper that has further in-depth information on the Chinese cybercrime underground. To inquire about the whitepaper and more how Intel 471 enables proactive security teams, get in contact with us.