PERISCOPE

July 6, 2022

TLP: AMBER

WEEKLY UNDERGROUND UPDATE

Last week in the underground, the actors **Dr.Void**, **florawinters** and **-HisExcellency-** offered malware source code and the actors **aimbatter**, **DropServ1s**, **EskobarLaundry** and **fearofgod** offered money mule services. Additionally, the actors **Alextro**, **JohnMr** and **racoonservice** engaged in document fraud, while the actors **BOP**, **iFrame** and **Symbian** targeted the consumer and industrial products sector.

Threat actors offer malware source code

- On June 26, 2022, the actor **-HisExcellency-** offered to develop a variety of Android malware including administration panels, banking trojans, keyloggers, spy applications and ransomware. The actor claimed ready-to-use malware samples are available for testing. The actor allegedly uses the hypertext preprocessor (PHP) and Java programming languages and could sell a copy or full source code of software that would be developed. The actor noted malware installed via Android application package (APK) files, not zero-day Android exploits, would be sold.
- On June 27, 2022, the actor **florawinters** offered to sell source code for an Android APK crypting tool and a Google Play loader. Both programs allegedly were written from scratch. The actor claimed the crypting tool uses a variety of crypting methods and comes with daily updates to bypass detection by antivirus software. The loader allegedly could install several applications, use country filters, automatically execute files after installation and more
- On June 29, 2022, the actor **Dr.Void** offered to sell source code of a private remote access tool (RAT) allegedly written in the C++ programming language. The description claimed the tool has file manager, loader, port scanner and process manager functionality and could run files and web shell scripts remotely and steal data from the process memory.

Threat actors offer money mule services

- On June 24, 2022, the actor **DropServ1s** advertised services of European Union (EU)-based mules who allegedly could complete account verification with several services and payment. The actor also claimed the mules could receive money transfers in the EU.
- On June 24, 2022, the actor **EskobarLaundry** advertised a cashout and money laundering service of the same name. The description claimed the service works in multiple countries and cashes out funds of any origin from individuals, legal entities, payment systems, scam projects and subscriber identity module (SIM) cards. The actor claimed money mules were available to perform cashout and collect money from customers.
- On June 25, 2022, the actor **aimbatter** advertised a cashout service targeting users in Latvia. The actor allegedly could receive all kinds of payments regardless of origin in large volumes into accounts with major banks and accounts opened with stolen personal details. The description claimed the service has a large pool of fully controlled mules that continues to expand.
- On June 25, 2022, the actor **fearofgod** offered drop accounts to handle money transfers in Australia and New Zealand. The amounts allegedly can range from US $3,000 to US $15,000 and will be cashed out the same day the money arrives. The actor also offered accounts with German international bank account numbers (IBAN) ready to receive large-sum transactions.

Threat actors engage in document fraud

- On June 25, 2022, the actor **JohnMr** offered to sell photos and scanned copies of driver's licenses, ID cards, passports, selfies and other documents. The description claimed the documents are authentic, exfiltrated from a private source and belong to real people. The actor claimed more than 500 GB of documents are available, new documents are added almost daily and orders for documents that were not available would be taken
- On June 27, 2022, the actor **racoonservice** advertised a document forgery service of the same name. The description claimed the service could forge credit cards, driver's licenses, ID cards, passports and Social Security numbers (SSNs). The actor claimed the service has its own database of personally identifiable information (PII) with photos of mules and the forged documents are high quality.
- On June 29, 2022, the actor **Alextro** advertised an underground store selling Google Voice accounts, photos and scans of documents with selfies and turnkey e-commerce payment system accounts. The description claimed prospective buyers could purchase driver's licenses, ID cards, passports and personal information records from more than 80 countries. The data for sale allegedly is well suited for opening accounts with betting services and e-commerce payment systems. The store also offered a service to pass identification procedures with two Russian financial services and allegedly uses an automated sales bot to transact the deals.

Threat actors target consumer, industrial products sector

- On June 25, 2022, the actor **Symbian** auctioned a database allegedly dumped from a fast food restaurant chain in China. The database allegedly contains 5.4 million records including addresses, email addresses, genders, mobile phone numbers and usernames.
- On June 26, 2022, the actor **BOP** offered to sell unauthorized access to an undisclosed U.S.-based company allegedly operating in the retail industry. The description claimed the target entity's revenue is US $5 million and the access was maintained via a compromised remote desktop protocol (RDP) account with domain administrator privileges.
- On June 26, 2022, the actor **iFrame** offered to sell unauthorized access to an undisclosed restaurant and cafe operator network with the head office in Asia. The description claimed the victim entity has an annual revenue of US $391 million and point-of-sale (PoS) terminals in multiple countries worldwide. The network allegedly includes more than 10,000 hosts. The actor claimed the access was maintained via compromised virtual private network (VPN) account credentials with domain administrator privileges.