PERISCOPE

July 20, 2022

INTEL471

TLP: AMBER

WEEKLY UNDERGROUND UPDATE

Last week in the underground, the actors **merc4n** and **vlhoscc** targeted the Internet-of-Things (IoT) industry and the actors **Amnesty**, **framework**, **growder** and **potompridumayu** offered malware with information-stealer functionality. Additionally, the actors **RagnarokClub**, **TalkCat8** and **xtokenss** offered underground call services, while the actors **inthematrix**, **POMA**, **Schizofren** and **sothebys** targeted entities in Ukraine.

Threat actors target Internet-of-Things industry

- On July 9, 2022, the actor **vlhoscc** claimed to compromise and leak data from an IoT devices manufacturer and seller. The description claimed the company primarily has corporate customers and the data contains information on orders including email addresses, names, tracking numbers, application extended unique identifiers (EUIs), device EUIs and serial numbers of ordered devices. On July 10, 2022, the actor started a post thread claiming to have access to an administrator panel of a store selling IoT devices and sought advice on what can be done with it.
- On July 11, 2022, the actor **merc4n** offered to sell an alleged zero-day exploit for IoT devices written in the Python programming language. The actor claimed the source code would be encoded and a version with open source code would be available at a slightly higher price. The exploit allegedly was developed July 10, 2022, and can be used to connect to any IoT devices supporting the message queuing telemetry transport (MQTT) protocol or running the Home Assistant software.

Threat actors offer malware with information-stealer functionality

- On July 8, 2022, the actor **framework** sought a partnership to provide traffic for a botnet through advertising, spamming and targeted campaigns. The description claimed the malware uses a unique method to gain persistence, executes commands through workers, has a low detection rate and evades detection by corporate antivirus tools. The malware allegedly has socket secure internet protocol (SOCKS5) proxy and stealer functionality and can create multiple sessions; delete directories, files and itself; inject web shells; grab system information; take screenshots; upload and download files; and view directories, install applications and processes.
- On July 8, 2022, the actor **potompridumayu** offered to sell an information stealer dubbed HOLDTHISMONEY. The malware allegedly can grab activity history, cookie files and passwords from all popular Blink or Gecko-based browsers and Discord, Steam and Telegram sessions. Other features allegedly include grabbing all desktop files, hardware information and popular cryptocurrency wallets. The actor indicated the stealer comes with a web panel that has a file loader, can reject repeated logs and empty records, allows the operator to configure the stealer and offers options to download, delete or view logs.
- On July 9, 2022, the actor **growder** offered to rent out an Android bot dubbed OWL that allegedly is compatible with Android versions 8 through 12. The description claimed the malware has Gmail grabber and keylogger functionality and can lock a device; open applications and links; forward and make calls; delete, grab and send text messages; delete, send and view push notifications; and steal Google Authenticator verification codes and seed phrases for cryptocurrency wallets. The actor also claimed more than 450 custom web-injects are available.

- On July 13, 2022, the actor **Amnesty** offered to sell five copies of "wallet drainer" malware that steals fungible and non-fungible tokens (NFTs) from MetaMask and Trust Wallet accounts. The description claimed once a target wallet is linked, the malware script checks Ethereum request for comments (ERC)-20, ERC-721 and ERC-1155 tokens, searches for the most expensive one and the victim is prompted to approve it with a spoofed address. The actor allegedly is willing to assist buyers with selecting traffic sources and guidance on other issues.

Threat actors offer underground call services

- On July 8, 2022, the actor **RagnarokClub** offered calling services for a variety of fraudulent purposes such as holding or redirecting parcels, inquiring about a bank card balance, placing and confirming orders, retrieving porting authorization codes (PACs), verifying payment system activity and more. The description claimed the callers are male or female English-native speakers with U.S. or U.K. accents. The service allegedly also covers the German and French languages.
- On July 11, 2022, the actor **TalkCat8** offered calling services for any purpose. The description claimed calls in the Dutch, English, German, Italian and Polish languages by female and male speakers could be made.
- On July 12, 2022, the actor **xtokenss** offered to sell a one-time password (OTP) interception utility that allegedly can be used to target customers of any bank, and claimed OTPs are obtained from victims by making calls to them.

Threat actors target entities in Ukraine

- On July 9, 2022, the actor **Schizofren** offered to sell access to a Ukraine-based private gas company. The access allegedly was obtained using compromised account credentials of the domain administrator of the victim's website. The description claimed the targeted entity has a revenue of more than US $140 million and employs more than 1,000 people. Follow-up comments indicated the actor subsequently was banned for breaking rules pertaining to targeting users in Russia and the CIS countries.
- On July 9, 2022, the actor **sothebys** offered to sell Ukrainian debit cards issued by several Ukraine-based banks. The cards allegedly can be fully relinked based on the customer's data and shipped to any country except for Russia and Belarus. The actor claimed the cards can be used to receive international money transfers via a variety of payment systems, for traffic reselling or for other activity.
- On July 10, 2022, the actor **inthematrix** offered to sell unauthorized access with local administrator privileges to an undisclosed Ukrainian government entity. The access allegedly was gained via compromised remote desktop protocol (RDP) account credentials. The description claimed more than 1 TB of data was available on the victim's local drives.
- On July 12, 2022, the actor **POMA** offered to sell bank cards allegedly issued in the names of fully controlled Ukrainian mules. The actor promised to give a one-month warranty for the cards and provide technical support to the buyer. The cards allegedly came with access to online banking, cardholder data, memorable words, personal identification number (PIN) codes and subscriber identity module (SIM) cards.