PERISCOPE

June 1, 2022

TLP: AMBER

WEEKLY UNDERGROUND UPDATE

Last week in the underground, the actors **ШЕФ**, **Enoc** and **malwarecoy** advertised malware with hidden virtual network computing (HVNC) functionality and the actors **samolist** and **YRP Service** engaged in reshipping fraud. Additionally, the actors **citrix**, **okito** and **swift_** leaked data from banking and financial companies, while the actors **justvmexit**, **peteandchels** and **William Hill** offered phishing projects and the actors **Bertrand**, **chiftlocal**, **inthematrix1** and the Ragnar ransomware-as-a-service (RaaS) operator or operators targeted software companies.

Threat actors advertise malware with hidden virtual network computing functionality

- On May 20, 2022, the actor **ШЕФ** sought to partner with a traffic provider for private custom-developed malware with HVNC functionality. The actor allegedly only was interested in traffic from Australia, Canada and the U.S. The HVNC tool allegedly had a high frames per second (FPS) rate, came with automated cookie loading functionality and a loader and was fully undetectable (FUD) by antivirus tools. The actor promised to handle crypting and provide the control panel for a test.
- On May 20, 2022, the actor **malwarecoy** offered to rent out an Android bot with HVNC functionality that could be used to target banks. The actor claimed the bot was written from scratch and had an automatic transfer system (ATS), cryptocurrency grabber and injection features. The actor also offered to provide a loader on the Google Play service to spread the malware.
- On May 23, 2022, the actor **Enoc** sought a partner who could offer a country to target using the actor's keylogger banking malware that allegedly was similar to but more efficient than an HVNC tool. The actor offered to demonstrate the malware in action and conduct spam campaigns to obtain email databases.

Threat actors engage in reshipping fraud

- On May 20, 2022, the actor **samolist** advertised reshipping mule services. The actor claimed to have China-based mules who could receive packages and reship them to the Commonwealth of Independent States (CIS) or other countries. The actor offered three cooperation options including ordering and delivering goods for a lower cost from Chinese wholesale marketplaces such as Taobao or 1688, reshipping goods or buying non-marketable goods.
- On May 23, 2022, the actor **YRP Service** advertised a mule service of the same name. The actor claimed to have mules in many countries worldwide and allegedly would provide buyers for merchandise. The mules allegedly could place phone calls if necessary and receive packages in Asia, Europe and the U.S.

Threat actors leak data from banking, financial companies

- On May 20, 2022, the actor **citrix** offered to sell a backup database allegedly dumped from an undisclosed U.S.-based consumer banking and finance company. The description claimed the database contained information on 393,849 customers and 34 employees, including bank account data, dates of birth (DOBs), driver's licenses, email addresses, employment data, full names, phone numbers and Social Security numbers (SSNs).

- On May 20, 2022, the actor **okito** offered to sell a customer database allegedly dumped from an undisclosed Singapore-based bank in May 2022. The description claimed the database contained more than 1.4 million records including addresses, bank account numbers, DOBs, email addresses, full names, National Registration Identity Cards (NRICs) and phone numbers. The actor provided a database sample as proof of the claim.
- On May 20, 2022, the actor **swift_** offered to sell a data set allegedly exfiltrated from an undisclosed U.S.-based company operating in the financial sector. The database allegedly contained full information on 10 million users including addresses, email addresses, DOBs, names, phone numbers and SSNs. The actor claimed the database was available in batches of 5 million records or as a whole and would not be sold more than once.

Threat actors offer phishing projects

- On May 22, 2022, the actor **peteandchels** offered to sell a phishing page for the OpenSea decentralized non-fungible token (NFT) platform. The clone allegedly was designed to capture cryptocurrency wallet seed phrases and looked almost identical to a legitimate page. The actor also offered to provide a cloaked link to an individual ready to cooperate on a profit-sharing model and forward traffic to the phishing page.
- On May 25, 2022, the actor **justvmexit** offered to rent out a Coinbase cryptocurrency company phishing panel developed in the JavaScript and Python programming languages. Potential buyers allegedly could control the panel via Telegram and set it up on any control panel (cPanel) administrative panel or Nginx server. The actor also claimed a fake two-factor authentication (2FA) page was available. Users interested in purchasing the source code were invited to place bids privately.
- On May 25, 2022, the actor **William Hill** auctioned a phishing page for a major U.S.-based technology company. The description claimed the page had a live administration panel that allowed the user to direct a victim to any webpage and display any target pages. The website allegedly could be used to collect payment card data and text messages.

Threat actors target software companies

- On May 21, 2022, the actor **chiftlocal** auctioned unauthorized access to an undisclosed European Union (EU)-based company that allegedly created products for construction, cybersecurity, software and technology. The description claimed the company employed 88,000 people and its revenue was US $18 billion. The access allegedly was maintained via compromised virtual private network (VPN) account credentials with user-level privileges. The actor claimed numerous other companies could be accessed via the targeted entity.
- On May 22, 2022, the actor **inthematrix1** auctioned unauthorized access to an undisclosed Canada-based software company with a revenue of US $6 million. The access allegedly came with local administrator privileges and was gained via remote desktop protocol (RDP) credentials.
- On May 23, 2022, the Ragnar RaaS operator or operators claimed to compromise a Germany-based land surveyor. The actor allegedly obtained access to the victim's sensitive data through a vulnerability and shared screenshots of leaked documents and personal information as proof of the claim. The actor also published a link to a password-protected archive that allegedly contained all the compromised information.
- On May 24, 2022, the actor **Bertrand** offered internal access to an India-based software development company. The access allegedly could be used to deploy ransomware and other malicious programs.