PERISCOPE

June 8, 2022

TLP: AMBER

WEEKLY UNDERGROUND UPDATE

Last week in the underground, the actors **cryptoman** and **diego033** sought ransomware affiliates and the actors **Ellnoir**, **Utilman**, the Distributed Denial of Secrets aka DDoSecrets leak website operator or operators and the Hive ransomware-as-a-service (RaaS) operator or operators targeted media companies. Additionally, the actors **BlackMass**, **ioweusa** and **vikis** engaged in cashout and payment card fraud, while the actors **Marx** and **Poison_bot** offered Android malware and the actors **Elon_Musk**, **foxdrw** and **otrisovka911** offered document forgery services.

Threat actors seek ransomware affiliates

- On May 28, 2022, the actor **diego033** announced the actor's team resumed operations apparently related to ransomware and sought affiliates to supply access to corporate networks. The actor allegedly was interested in access via Citrix, Fortinet, remote desktop protocol (RDP), SonicWall and virtual private network (VPN) account credentials as well as via command prompt (CMD). The ransomware operators allegedly targeted networks in Europe and the U.S.
- On May 30, 2022, the actor **cryptoman** sought partners to provide access to companies that allegedly would be monetized via ransomware campaigns. The actor expressed interest in access via VPN credentials with administrator and user privileges to targets with annual revenues exceeding 50 million in an unspecified currency and sought access to 10 corporate networks a week. The actor's team allegedly demanded victim companies pay 1% to 3% of their revenue and the partner allegedly would receive 15% of the ransom amount.

Threat actors target media companies

- On May 29, 2022, the actor **Ellnoir** offered to sell unauthorized access to an undisclosed Brazil-based media company that owns several TV and sound broadcasting channels, news websites and an information website with a revenue of more than US $120 million and more than 500 employees. The access allegedly came with domain administrator privileges and was gained via RDP credentials. The description claimed the compromised company had more than 1,700 hosts on the network and used the Avast and Kaspersky antivirus software.
- On May 29, 2022, the actor **Utilman** announced a data leak allegedly impacting a Turkish online radio station. The actor claimed the compromised website had 3,700 users and provided a link to the data in three different combinations that included email login, username and password; email login and password; and username and password records stored in comma-separated values ([.]csv) files.
- On May 30, 2022, the Hive RaaS operator or operators claimed to leak data from a Colombian television network. The operator or operators claimed the data was encrypted May 22, 2022, and shared a link to a data sample as proof of the claim.
- On June 2, 2022, the DDoSecrets site operator or operators released a data set allegedly leaked from a Russian privately held regional group of radio stations. The description claimed the data leak was sourced from the Anonymous hacktivist group and was 823 GB with 1.5 million emails.

Threat actors engage in cashout, payment card fraud

- On May 30, 2022, the actor **BlackMass** offered to sell fresh databases dumped from undisclosed Argentinian entities. The databases allegedly included Track 1 and Track 2 data without personal identification numbers (PINs). The actor claimed to have a regular supply of about 500 pieces every 10 days and intended to find a reseller or shop for long-term cooperation.
- On May 30, 2022, the actor **ioweusa** advertised a cashout service dubbed CULLINAN CASH OUT | DARK ACADEMY. The description claimed the service worked without intermediaries, used the service's own accounts to receive funds, could receive as much as US $300,000 per day, made instant payouts and cashed out funds using near-field communication (NFC) technology and a merchant account of the Paymob service. The actor claimed the service worked with virtual credit cards (VCCs) of banks and financial services.
- On May 30, 2022, the actor **vikis** announced the launch of a new unnamed underground store selling compromised payment card data and sought investors and vendors. The actor claimed the store was developed from scratch, was completely crypted and secure and used a proprietary payment card validity-checking tool that was in the beta testing stage. The actor also started a separate post thread advertising the payment card-checking tool coded in the hypertext preprocessor (PHP) programming language. The actor claimed the checker ran using a Stripe merchant account with the option to be configured for any merchant service and could check 1,000 to 5,000 and potentially as many as 50,000 payment cards a day.

Threat actors offer Android malware

- On May 27, 2022, the actor **Poison_bot** offered to rent out the POISON Android botnet that allegedly was compatible with Android versions 8 through 12. The description claimed the malware could obtain administrator rights and a list of installed applications, read and stealthily intercept short message service (SMS) texts, send and stealthily intercept fake push notifications and send SMS messages to phone numbers in the contact list. Other features included clearing the application cache, forwarding calls and deleting, launching and scanning applications. The actor claimed the botnet still was under development and more features would be added.
- On May 31, 2022, the actor **Marx** offered an Android loader uploaded to the Google Play platform. The actor sought a partner with a good botnet and a cashier who understood the job.

Threat actors offer document forgery services

- On May 28, 2022, the actor **otrisovka911** advertised a document forgery service of the same name. The actor allegedly was in this business for almost three years and gained enough experience to complete unconventional and complicated orders. The actor specifically offered to provide counterfeit bank cards and statements, ID cards, driver's licenses, medical certificates, passports and virtual and physical checks, as well as edit photos and screenshots and supply ready-to-use Photoshop document (PSD) templates.
- On May 31, 2022, the actor **Elon_Musk** offered Ukrainian border-crossing services to bypass restrictions imposed by martial law. The actor offered to register individuals as volunteers in the Shliakh government system for one month with an option to extend the validity period for another month, making it possible for them to cross the border officially and receive proper stamps on documents. The actor also offered the option to bypass official checkpoints with the help of accomplices who would transfer individuals through "secret pathways" to European territory.
- On May 31, 2022, the actor **foxdrw** advertised a document forgery service of the same name. The description claimed the service offered high-quality forgeries of a variety of documents from multiple countries, leveraged a personal approach and fulfilled orders in a timely manner. The actor allegedly cooperated with forgery experts worldwide and provided a wide range of services.