PERISCOPE

April 20, 2022

TLP: AMBER

WEEKLY UNDERGROUND UPDATE

Last week in the underground, the actor **VoltZ**, the hacktivist group Anonymous and the Quantum ransomware-as-a-service (RaaS) operator or operators leaked personal data of company CEOs and employees, while the actors **cake_baker**, **CashWeekend** and **ExitQ** advertised call services. Additionally, the actors **AgainstTheWest**, **Cyberia-Sun** and **SherlockHolmes** targeted financial institutions in Asia and the actors **krakkennn**, **xmastercardx** and the Distributed Denial of Secrets aka DDoSecrets leak website operator or operators continued to target Russia.

Threat actors leak personal data of company CEOs, employees

- On April 10, 2022, the actor **VoltZ** offered to sell a database that allegedly contained information on employees from two U.S.-based telecommunication organizations. The compromised data allegedly contained full names, system roles, user IDs and more. The actor allegedly collected the data using an exploit and offered to provide a sample to prospective buyers.
- On April 11, 2022, the Quantum RaaS operator or operators claimed the compromise of an Australia-based airline. The compromised data set allegedly contained customer data, financial records, human resources (HR) records and information on most company employees, including payroll and personal data.
- On April 12, 2022, the hacktivist group Anonymous provided personal information of eight CEOs of oil companies the group claimed were "destroying the environment." The doxxing campaign allegedly impacted CEOs of U.S.-based energy companies. The information included addresses, dates of birth (DOBs), email addresses, full names, phone numbers, vehicle details and information on visits to the White House.

Threat actors advertise call services

- On April 11, 2022, the actor **cake_baker** advertised a Telegram bot designed to obtain one-time passwords (OTPs) sent in text messages. The description claimed users would need to enter the victim's phone number and the targeted website name, such as Binance, Coinbase or Google, for the victim to receive a phone call ostensibly from an automated service of the site. Customers were offered one call for free and could choose between subscription plans based on the number of phishing calls.
- On April 11, 2022, the actor **CashWeekend** advertised a phone call service that allegedly could call online stores, banks and payment systems. The description claimed the service could make calls with caller ID spoofing; compose emails, text messages and scenarios; receive phone calls and text messages; and reroute packages and place them on hold. Service operators allegedly could speak the English, French, German and Spanish languages.
- On April 14, 2022, the actor **ExitQ** sought a call operator to join the actor's team. The caller was expected to be fluent in English and provide call logs for every target entity, among other things. The actor claimed to provide a target company's website, a brief overview of the company, access to company data and a list of company employees with their personal data including addresses, email addresses and mobile phone numbers.

Threat actors target financial institutions in Asia

- On On April 9, 2022, the actor **AgainstTheWest** claimed to compromise a China-based online private commercial bank. The actor provided a link to a Twitter thread with more information and a link to download the compromised data.
- On April 9, 2022, the actor **SherlockHolmes** offered to sell a database that contained Singapore bank customer data. The database allegedly included addresses, bank names, DOBs, email addresses, employers, full names, international bank account numbers (IBANs), job titles, national registration identity card (NRIC) numbers and phone numbers.
- On April 10, 2022, the actor **Cyberia-Sun** auctioned unauthorized access to the network of an Indonesia-based company that allegedly operated in the financial and banking industry. The actor claimed the targeted entity's revenue was US $112 million and its stock symbol was "QF8." Open source research indicated the victim was related to an investment consulting company. The access allegedly was obtained via compromised virtual private network (VPN) account credentials with local administrator-level privileges.

Threat actors continue to target Russia

- On April 11, 2022, the actor **xmastercardx** shared a database that allegedly contained personally identifiable information (PII) of Russian pensioners. The actor claimed the database contained more than 250,000 records with data such as cities, DOBs, email addresses, names and phone numbers. The exfiltrated database allegedly was dated 2021.
- On April 12, 2022, the DDoSecrets site operator or operators released 116 GB of data with 130,000 emails the Anonymous hacktivist group allegedly exfiltrated from the office of the governor of Tver Oblast, Russia. On April 13, 2022, the operator or operators released information impacting two Russian companies that allegedly also was sourced from the Anonymous hacktivist group. On April 14, 2022, the operator or operators shared another Anonymous data leak that impacted Russia's Ministry of Culture and included 446 GB of data with 230,000 emails.
- On April 13, 2022, the actor **krakkennn** shared a list of Russian soldiers who allegedly participated in attacks on Mariupol, Ukraine. The actor claimed the list contained records of personnel of the 1st Company of the 382nd Separate Marine Battalion of the Black Sea Fleet and the part of the 810th Separate Marine Brigade.