PERISCOPE

May 4, 2022

TLP: AMBER

WEEKLY UNDERGROUND UPDATE

Last week in the underground, the actors **cheshire666**, **Enzo**, **mikeoxmaul** and **Shamel** offered information-stealer malware and the actors **AlexCrep0009**, **Bototp**, **robertmorrison**, **vlhoscc** and **William Hill** targeted banks and payment services. Additionally, the actors **cryptoman** and **pumpedkicks** leveraged network appliance and endpoint vulnerabilities, while the actors **BusinessOrg**, **misa amane** and **Tornado6548** engaged in cashout and money laundering schemes.

Threat actors offer information-stealer malware

- On April 22, 2022, the actor **cheshire666** offered multifunctional botnet malware dubbed Aurora. The description claimed the malware had cryptocurrency clipper, proxying and stealer functionality and potential customers could purchase a monthly subscription. The actor also intended to share three malware samples with reputable forum members, presumably in exchange for feedback.
- On April 25, 2022, the actor **Enzo** offered to rent the reborn Shockloader hypertext transfer protocol (HTTP) botnet and stealer. The description claimed the malware was fully undetectable (FUD) at scantime and semi-FUD at runtime and came with an external builder and HTTP panel that could be installed on the actor's team's servers. The malware allegedly could be used to run a variety of commands and adjust settings related to online and offline bots, as well as collect system information and data from browsers and messengers, among other things.
- On April 25, 2022, the actor **mikeoxmaul** offered to sell or rent a private remote access trojan (RAT) with stealer functionality targeting Windows operating systems (OSs). The actor stated the software client was written in the Assembly, C and C++ programming languages and fully avoided detection by antivirus tools. The software allegedly used the HTTP and transmission control protocol (TCP) depending on the active module, achieved persistence via the registry and scheduled tasks, could steal cookies and credentials from Chrome and Firefox browsers, could use the remote desktop protocol (RDP) and could capture screenshots. The actor also offered to sell the malware source code and services to keep the malware FUD.
- On April 25, 2022, the actor **Shamel** offered to sell custom-developed stealer malware dubbed 7.62mm. The actor claimed the tool was FUD and could collect data from browsers and browser extensions, cryptocurrency wallets and session data from multiple messaging clients. The stealer file allegedly was available in the dynamic-link library ([.]dll) and executable ([.]exe) file formats.

Threat actors target banks, payment services

- On April 23, 2022, the actor **AlexCrep0009** offered to sell unauthorized access via a web shell to a Romania-based bank. The description claimed the actor could upload the potential buyer's back door to the targeted bank's server.
- On April 23, 2022, the actor **vlhoscc** offered a one-time password (OTP) interception service. The actor allegedly would provide the service for free initially to test the bot and promised to achieve a success rate of 70% to 80% if victims responded to the bot calls. The description claimed the bot was designed to target users in Canada, France, the U.K. and the U.S. and intercepted 3-D Secure verification codes; codes for enabling near-field communication (NFC) payments through Apple Pay, Google Pay and Samsung Pay; codes from services such as PayPal; and emails.

Copyright 2022 Intel 471 Inc.

- On April 24, 2022, the actor **robertmorrison** offered to sell databases allegedly from Russian banks. The actor claimed the databases contained more than 2.8 million records from 2017 to 2021 stored as comma-separated values ([.]csv), Microsoft Excel spreadsheet ([.]xlsx) and text ([.]txt) files. Most records allegedly included addresses, dates of birth (DOBs), email addresses, phone numbers and more.
- On April 25, 2022, the actor **Bototp** offered to sell an OTP bot that allegedly allowed capturing OTPs and short message service (SMS) codes in seconds by entering the target phone number and website link. The actor claimed to represent the only service offering a 100% success rate intercepting OTPs and text messages and targeted all mobile phones and networks in any country. The bot allegedly could capture bank account numbers; Apple Pay, Google Pay and Samsung Pay codes; cryptocurrency wallets; driver's license numbers; payment card details; personal identification numbers; Social Security numbers (SSNs); and other data that later was sent to the user's Telegram accounts or panels.
- On April 27, 2022, the actor **William Hill** offered to sell phishing websites targeting three major European banks in Italy and Norway. The actor allegedly developed each website clone and its administrative panel and promised assistance with the setup process and further support. The scam websites allegedly were used to collect full personal information, payment card details, passwords, push notifications, text messages, tokens and usernames.

Threat actors leverage network appliance, endpoint vulnerabilities

- On April 26, 2022, the actor **pumpedkicks** offered to sell data on 16,000 Fortinet secure sockets layer (SSL) virtual private network (VPN) hosts impacted by the CVE-2018-13379 path traversal vulnerability. The compromised data allegedly consisted of IP addresses, logins and passwords and was up-to-date as of April 25, 2022. The actor claimed the targets included banks, hospitals and universities from countries worldwide but primarily the U.S.
- On April 27, 2022, the actor **cryptoman** offered to sell an exploit that allegedly impacted hosts running the Cisco AnyConnect VPN client. The actor claimed the exploit used a list of IP addresses as input data and provided usernames and passwords in the form of MD5. The actor expressed readiness to provide proof the code worked.

Threat actors engage in cashout, money laundering schemes

- On April 23, 2022, the actor **BusinessOrg** offered a cashout service working with cryptocurrency. The service allegedly offered to deliver cashed out funds through dead drops or by courier in Cambodia, Dubai, Kazakhstan, Russia, Thailand, Ukraine and potentially other locations. The service also could make money transfers to Chinese accounts and Russian Tinkoff payment cards and quick response (QR) codes.
- On April 25, 2022, the actor **misa amane** offered several money laundering schemes that allowed cashing out and exchanging any cryptocurrency including bitcoin and Monero. The actor allegedly worked with illegitimately obtained funds and exchange operations usually took several hours.
- On April 28, 2022, the actor **Tornado6548** offered cashout services and sought customers with bank account credentials from logs, Ukrainian payment cards with 2D Payment Gateway enabled, worldwide cards protected with 3-D Secure protocol and virtual credit cards (VCCs) opened with stolen personal details. The actor claimed customer funds would be cashed out within an hour and they would receive instant payouts in bitcoins.

Copyright 2022 Intel 471 Inc.