PERISCOPE

May 25, 2022

TLP: AMBER

WEEKLY UNDERGROUND UPDATE

Last week in the underground, the actors **deniska**, **jexztbconn** and **Moon_Developer** offered malware source code and the actors **nobugbounty**, **poisonsanmx**, **pumpedkicks** and **remotedesktop** leveraged web shells. Additionally, the actors **Lunopark** and **sayonaragroup** advertised distributed denial-of-service (DDoS) attack services and the actors **meowcat1234**, **posman**, **remotedesktop** and **yktbase** targeted the telecommunications industry.

Threat actors offer malware source code

- On May 13, 2022, the actor **jexztbconn** offered to sell source code of the Taurus and Predator the Thief information stealers. The Predator the Thief code allegedly included versions 2.3.1, 3.0.1 and 3.3.4 and was accompanied by a clipper module, while the administrator panel was not included. The Taurus code included versions 1.2, 1.3, 1.4 and 1.5 and came with the administrator panel and Telegram bot builder. The actor claimed both projects came from the author directly and were offered as is without any support services or updates.
- On May 17, 2022, the actor **deniska** offered to sell source code of a Quasar remote administration tool (RAT)-based trojan. The description claimed the malware had three-tier client-agent-server architecture and supported a cross-platform server with the option to run on Linux and Windows operating systems (OSs). The malware allegedly had multiple plug-ins including console, file manager and keylogger; could record microphone audio and take screenshots; and saved data to a structured query language (SQL)-based SQLite database.
- On May 17, 2022, the actor **Moon_Developer** offered to sell builds or source code of an unnamed RAT. The description claimed the RAT could obtain all computer information, capture screenshots, upload files to Discord on the specified computer, collect a list of all antivirus products installed on the computer and steal information from Chrome and other popular browsers, among other features. The tool allegedly could start remote command prompt sessions, execute commands and start remote PowerShell sessions on the target computer with automatic Antimalware Scan Interface (AMSI) bypass. The actor also claimed the tool did not use port forwarding and only required a Discord account to operate.

Threat actors leverage web shells

- On May 14, 2022, the actor **nobugbounty** advertised unauthorized access via a web shell planted at the website of an undisclosed Brazil-based information technology (IT) company that allegedly provided business intelligence, cloud and enterprise resource planning (ERP) software. The access allegedly allowed an attacker to execute remote code on the system. The actor claimed the compromised company was listed on a stock exchange, employed more than 10,000 people and had annual billings of more than 3 billion in an unspecified currency.
- On May 14, 2022, the actor **poisonsanmx** auctioned access to a compromised master domain name system (DNS) including access to a full database and transactions of an undisclosed Spanish bank. The actor allegedly used a web shell, established a reverse shell connection, bypassed the firewall and gained root privileges.
- On May 15, 2022, the actor **pumpedkicks** offered to sell network and web shell access to an undisclosed subdomain of an Italy-based footwear company. The actor also claimed to have access to the company's Git repository.

- On May 16, 2022, the actor **remotedesktop** auctioned unauthorized access via a web shell to a U.S.-based website that allegedly sold WordPress administrator panels. The actor claimed the website's worldwide traffic rank was 40,000 and 41,000 in the U.S. The site allegedly ranked 109 in its category and was visited more than 1 million times within the last three months.

Threat actors advertise distibuted denial-of-service attack services

- On May 14, 2022, the actor **Lunopark** offered DDoS attack services and claimed to be able to bypass protection from Cloudflare, DDoS-Guard, Fastly, StormWall, vDDoS, vShield and other similar services. The actor also offered to sell application programming interfaces (APIs) to conduct attacks.
- On May 15, 2022, the actor **sayonaragroup** offered a DDoS attack service dubbed SayonaraDDoS. The description claimed the service targeted entities from the IT industry, could conduct attacks with a maximum speed of 280 Gigabits per second (Gbps), cluttered the targeted server bandwidth with a multi-gigabit flow of traffic at the Open Systems Interconnection (OSI) model Transport Layer 4 level and used hypertext transfer protocol (HTTP), synchronize (SYN) and user datagram protocol (UDP) attack vectors, among other features.

Threat actors target telecommunications industry

- On May 15, 2022, the actor **posman** sought to purchase Citrix and virtual private network (VPN) access credentials for telecommunications entities primarily in the U.S. and in other locations. On May 16, 2022, the actor **meowcat1234** also sought to buy Citrix and VPN access credentials for major telecommunications service providers and promised to pay five-figure amounts.
- On May 15, 2022, the actor **yktbase** advertised a database allegedly exfiltrated from an undisclosed internet service provider (ISP) in the Far East. The description claimed the database was dated 2022 and contained users' full names, passport data and phone numbers.
- On May 17, 2022, the actor **remotedesktop** auctioned full access to an undisclosed Europe-based internet protocol TV (IPTV) streaming service provider that allegedly served 170 local companies and offered a proprietary application for Android and iOS devices. The actor claimed passwords for all servers were available, along with administrative and root privileges and access to backups and routers.