PERISCOPE

June 22, 2022

TLP: AMBER

WEEKLY UNDERGROUND UPDATE

Last week in the underground, the actors **f1lt**, **GenesisStore** and **silverspace88** advertised underground marketplaces and the actors **Developer-Test**, **lucrostm**, **NeUveren** and **Solmyr** offered remote access trojan (RAT) malware. Additionally, the actor **mont4na**, the Industrial Spy breached data marketplace operators, the Cuba ransomware-as-a-service (RaaS) operator or operators and the Everest RaaS operator or operators targeted the manufacturing sector, while the actors **advalex**, **MRX1** and **redpoint** offered crypting tools and services.

Threat actors advertise underground marketplaces

- On June 11, 2022, the actor **silverspace88** offered to sell invites to an underground store selling compromised payment cards. The store allegedly operates in a semiprivate mode and has about 32,800 cards uploaded to it. The actor claimed the validity rate of the records would be within the 90% and 95% range and invalid card details would be refunded.
- On June 13, 2022, the actor **f1lt** auctioned the full source code and database of an undisclosed underground marketplace. The actor claimed the database contains 26,000 accounts with a total balance exceeding 3 bitcoins (about US $20,623) and there is an option for manual withdrawals. The actor added the marketplace is one year old and the data was dumped two weeks ago.
- On June 13, 2022, the actor **GenesisStore** announced the restored operation of the Genesis Store underground shop of compromised access credentials. According to the actor, the shop initially would be accessible for existing users only and new invitations would be provided soon. The actor also intended to further add new bots and update the shop plug-in to version 7.0+.

Threat actors offer remote access trojan malware

- On June 10, 2022, the actor **lucrostm** offered to sell or rent out a RAT for devices running Windows operating systems (OSs). The description claimed the malware works secretly, uses an innovative persistence technique, is fully undetectable (FUD), uses anti-debugging and anti-virtual machine (VM) techniques, can work without a server but would be less stealthy, among other features. Potential users can buy the malware's source code or a lifetime license or rent out the malware on a monthly basis.
- On June 11, 2022, the actor **Developer-Test** offered to sell an alleged custom RAT. The actor emphasized the tool was not for rent but for sale with the source code and claimed a demonstration video could be provided as proof of the claim.
- On June 13, 2022, the actor **NeUveren** offered to sell a RAT designed to target macOS devices. The listed features included establishing a reverse shell connection, gaining a foothold and managing the file system. The actor allegedly intended to provide the source code and copyright for the malware to the buyer, and modify its functionality to suit the client's needs.

- On June 14, 2022, the actor **Solmyr** offered to rent out an upgraded version of the Warzone RAT dubbed Warzone Poison version 3.0. The description listed the main malware features such as escalating privileges, establishing hidden remote desktop (HRDP) sessions, hidden virtual network connection (HVNC), information-stealer, keylogger, reverse proxy functionality and more. The same day, **Solmyr** started another post thread where the actor listed specific improvements and updates made as well as new features added to version 3.0, including HRDP support for more Windows OS versions and recovery of cookies from Chrome.

Threat actors target manufacturing sector

- On June 11, 2022, the Everest RaaS operator or operators claimed the compromise of a U.K.-based construction company. According to the description, more than 80 GB of data was downloaded from the company's servers, including contracts, financial documents, internal correspondence and emails, personal data of employees, tax forms and tenders. The company's management allegedly was notified of the incident and possible consequences. The operator or operators provided a few sample documents as proof of the data breach.
- On June 13, 2022, the actor **mont4na** offered to sell website source code impacting an undisclosed subdomain of an Italy-based vehicle parts. The offer allegedly included a 1.1 GB file. The actor also offered a data set and website source code allegedly leaked from an Italy-based luxury fashion brand. The offer included a 44 MB file and a structured query language ([.]sql) 1.2 MB file.
- On June 13, 2022, the Cuba RaaS operator or operators claimed the compromise of a Taiwan-headquartered computer memory chip manufacturer. The description claimed the data leak included account movements, balance sheets, correspondence with bank employees, financial documents, source code and tax documents.
- On June 14, 2022, the Industrial Spy breached data marketplace operators offered to sell information allegedly leaked from a U.K.-based industrial machinery and equipment company. The offer allegedly includes 487.8 GB of data and would be valid for six days.

Threat actors offer crypting tools, services

- On June 10, 2022, the actor **advalex** offered to sell a malware crypting tool for PowerShell scripts. The tool allegedly loads a malicious script from a cloud host using a link and generates an obfuscated file. The description claimed the program was written in the Java programming language, can be easily modified and uses a shell code to patch Windows Antimalware Scan Interface (AMSI).
- On June 12, 2022, the actor **MRX1** advertised the crypting tool dubbed DEAF CRYPTER. The actor claimed the tool can be used to crypt all kinds of RAT malware and added the tool was tested and proved to be effective on njRAT, Quasar and Venom RATs. The description claimed malware crypted with the tool can bypass Windows Defender, avoiding detection at runtime and scantime, however, the tool allegedly can not bypass protection mechanisms from other antivirus programs.
- On June 12, 2022, the actor **redpoint** offered crypting services for Cobalt Strike and loader, ransomware, RAT and other varieties of malware. The actor allegedly utilizes a stub written in the C++ programming language using the LoadPE portable executable (PE) method and can crypt dynamic-link library ([.]dll) and executable ([.]exe) files compatible with x64 and x86 OSs. According to the actor, the crypted files can bypass Windows Defender.