PERISCOPE

INTEL471

June 15, 2022

TLP: AMBER

WEEKLY UNDERGROUND UPDATE

Last week in the underground, the actors **aion** and **SebastianPereiro** offered exploits for vulnerabilities in Microsoft Windows products and the actors **marosty1001**, **mlx22**, **NotKover** and **zelizzard** offered loader malware. Additionally, the actor **black_palm** and the LV ransomware-as-a-service (RaaS) operator or operators targeted entities in Malaysia, while the actors **AmperVolt**, **RocketRacoon**, **Tooppaazz** and the LockBit 2.0 RaaS operator or operators targeted the life sciences and health care sector.

Threat actors offer exploits for vulnerabilities in Microsoft Windows products

- On June 6, 2022, the actor **aion** offered to sell an alleged exploit for a remote code execution (RCE) vulnerability in Microsoft Support Diagnostic Tool (MSDT) tracked as CVE-2022-30190. The description claimed the exploit allowed an attacker to build rich text format ([.]rtf) documents that allegedly could run arbitrary code on the target system when opened or previewed. The actor claimed the malicious files could bypass Windows Defender and most common antivirus programs and provided a demonstration video as proof of the claim.
- On June 6, 2022, the actor **SebastianPereiro** offered to sell an exploit for the CVE-2022-26925 local security authority (LSA) spoofing vulnerability impacting Microsoft Windows products that allegedly was patched in May 2022. The actor claimed the exploit allowed pre-authentication RCE and required local administrator or system privileges in the system the attack would be conducted from with Windows Defender and other antivirus protection mechanisms disabled. The actor offered potential customers an option to purchase the exploit for Windows operating systems (OSs) and a build for Linux Oss.

Threat actors offer loader malware

- On June 3, 2022, the actor **mlx22** offered to sell multifunctional malware with loader and stealer features and an administrator panel dubbed Milonyx. The malware allegedly requires administrator privileges at start; uses payloads that run in the system as a 32-bit Component Object Model (COM) Surrogate process; can add tasks to autorun and schedule task execution; recovers gaming files, history, logins and passwords; and downloads logs with this data from the infected machines. The actor provided screenshots as proof of the claim.
- On June 3, 2022, the actor **zelizzard** offered to rent out the Aurora loader. The malware allegedly was written in the C and Golang programming languages and comes with a crypting tool in the C++ programming language. The actor claimed the malware has cryptocurrency clipper, information-stealer and proxying capabilities and the malware builds were created for free using a polymorphic builder.
- On June 6, 2022, the actor **marosty1001** advertised a malware loader allegedly planted on the Google Play platform as a functional Android application. The description claimed the loader can possess legitimate features such as displaying cryptocurrency-related information, document scanning and photo editing. Once users open the application, they allegedly would receive a push notification asking them to download an Android application package (APK) file, install and open it.
- On June 8, 2022, the actor **NotKover** offered to sell a native malware dropper dubbed Meoware. The description claimed the software was written using the Rust programming language, is compatible with Windows OS versions 10 and 11 and can bypass Windows Antimalware Scan Interface (AMSI). The actor claimed the dropper could be used to deliver an unlimited number of files.

Threat actors target entities in Malaysia

- On June 3, 2022, the actor **black_palm** offered to sell unauthorized access via compromised Fortinet account credentials to an undisclosed Malaysia-based company. The description claimed the victim entity has an annual revenue of US $1.5 billion and employs nearly 4,000 people.
- On June 4, 2022, the LV RaaS operator or operators claimed to compromise a Malaysia-based semiconductor manufacturer. The operator or operators allegedly leaked 1 TB of information including documents such as a nondisclosure agreement (NDA) and customer, employee, insurance and financial data.

Threat actors target life sciences, health care sector

- On June 4, 2022, the LockBit 2.0 RaaS operator or operators claimed the compromise of a Texas, U.S.-based health care provider. The description claimed the leak consisted of 45 GB of data including financial reports and customers' sensitive data. The same day, the operator or operators also claimed to compromise a South Africa-based pharmaceutical company and threatened to publish all the leaked data.
- On June 6, 2022, the actor **RocketRacoon** offered to sell access to an undisclosed Bangladesh-based pharmaceutical company with an alleged annual revenue of 237 million in an unspecified currency. The offer also included access to an undisclosed Germany-based company allegedly in the grain farming field with a revenue of more than 386 million in an unspecified currency. The description claimed access to both entities was maintained via compromised remote desktop protocol (RDP) credentials and came with local administrator privileges.
- On June 6, 2022, the actor **Tooppaazz** offered to sell a data set allegedly from a U.S. national health insurance program. The actor claimed the data set contained freshly collected records and included patients' personal details such as dates of birth (DOBs), email addresses, full names, insurance policy details, phone numbers and doctors' full names and national provider identifier (NPI) numbers.
- On June 8, 2022, the actor **AmperVolt** sought to purchase access to hospitals in Europe and the U.S. The actor allegedly only was interested in access to general and public hospitals and claimed the targets would not be infected with ransomware.