PERISCOPE

June 29, 2022

TLP: AMBER

WEEKLY UNDERGROUND UPDATE

Last week in the underground, the actors **killerAV** and **wav** offered counter antivirus tools and the actors **blackc0d3**, **mrjoker1118**, **ShadowNatasha** and **X86MIPS** offered exploits. Additionally, the actors **joseph_salazar**, **kelvinsecurity** and **valeanz** targeted universities, while the actors **Elfister**, **method**, **pumpedkicks** and **s.lott** targeted the telecommunications industry.

Threat actors offer counter antivirus tools

- On June 17, 2022, the actor **wav** offered to sell a tool that allegedly can bypass and disable any antivirus protection mechanism. The actor also offered to bind the tool with the customer's software into a single Microsoft Installer (MSI) package to enable its installation via Active Directory.
- On June 21, 2022, the actor **killerAV** offered to sell a counter antivirus tool dubbed AV KILLER. The actor claimed the tool can disable protection mechanisms from Panda, Sophos and Windows Defender, and an option to disable SentinelOne was temporarily unavailable but would be deployed shortly. The actor also offered to modify the tool to target any other antivirus software at the customer's request. The tool allegedly would be provided in the executable ([.]exe) file format and requires administrator privileges to run. The actor also offered to sell a private crypting tool designed for .exe and dynamic-link library ([.]dll) files compatible with 32- and 64-bit operating systems (OSs).

Threat actors offer exploits

- On June 17, 2022, the actor **blackc0d3** advertised a silent Microsoft Word ([.]doc) exploit for the Microsoft Windows Support Diagnostic Tool (MS-MSDT) arbitrary code execution (ACE) vulnerability known as Follina and tracked as CVE-2022-30190. The actor claimed the exploit can bypass Windows Defender at runtime and requires a fully undetectable (FUD) payload.
- On June 17, 2022, the actor **mrjoker1118** offered to sell source code for a silent Microsoft Excel exploit. The description claimed the exploit can bypass Gmail, Outlook and Yahoo protection and its detectability depends on the back door. On June 18, 2022, the actor offered to sell source code for a silent Microsoft Word exploit that has the same features and can bypass the protected view mode.
- On June 20, 2022, the actor **ShadowNatasha** offered to sell a zero-day exploit for the latest version of the WhatsApp instant messaging application. The exploit allegedly can steal message history by sending payloads as images, portable document format ([.]pdf) files or videos. The actor claimed the conversations can be sent to email addresses or servers. The actor also shared the exploit's proof of concept (PoC) code. On June 22, 2022, the actor offered an Android and iOS zero-day exploit to perform remote code execution (RCE) attacks, which allegedly allowed compromising any phone and obtaining all the data stored on a device, such as call logs, contact lists, images, messages and more.
- On June 20, 2022, the actor **X86MIPS** offered to sell an exploit for an RCE vulnerability that allegedly was discovered when the actor tested new software on Windows 10. The description claimed the malicious code can be embedded into a text ([.]txt) or joint photographic experts group ([.]jpeg) file and requires no user interaction to be executed. The actor claimed the exploit runs stealthily and allows an attacker to take control of a target machine or infect it with malware.

Threat actors target universities

- On June 17, 2022, the actor **kelvinsecurity** offered compromised access to an Argentina-based university. The data allegedly contained 23,579 records of personal information including addresses, contact details, dates of birth (DOBs), full names, IDs, occupations and workplace information. The actor shared a few sample screenshots.
- On June 17, 2022, the actor **valeanz** auctioned unauthorized access with user-level privileges to the network of an undisclosed U.K.-based university with an alleged revenue of US $330 million. The actor also suggested some of the network access credentials could come with domain administrator privileges.
- On June 20, 2022, the actor **joseph_salazar** advertised a data set allegedly exfiltrated from a Italy-based university. The actor shared screenshots of the file tree, folders and sample data as proof of the claim.

Threat actors target telecommunications industry

- On June 17, 2022, the actor **s.lott** claimed to be able to swap U.S. T-Mobile subscriber identity module (SIM) cards 24/7 in unlimited quantities. The actor sought to partner with forum users who could supply bank- and cryptocurrency-related logs and invited them to cooperate for a share of profits.
- On June 19, 2022, the actor **Elfister** sought experienced callers fluent in the English language and skilled at social engineering to infect computers at U.K. and U.S. mobile carrier outlets with a remote access trojan (RAT). Candidates allegedly would be provided with direct links to FUD malicious stub files in the [.]exe format, which they would have to convince the store personnel to download and run. The actor also expressed interest in cooperating with people engaged in SIM swapping.
- On June 20, 2022, the actor **method** auctioned unauthorized access with domain administrator privileges to an undisclosed Mauritius-based information and communications technology (ICT) services provider. The description claimed the targeted company had a 1.3 million customer base and revenue of 300 million in an unspecified currency. The actor claimed the victim used Symantec antivirus software that allegedly could be disabled.
- On June 20, 2022, the actor **pumpedkicks** offered to sell information about an alleged local file disclosure (LFD) vulnerability impacting an undisclosed resource of an Italy-based telecommunications company. The actor claimed the impacted server machine runs the Linux OS and the vulnerability allows attackers to read internal system files.