Private Sector Offensive Actors

Caramel Tsunami

Microsoft Security actively investigates and tracks threat actors in order to help protect customers, our platform and services from adversaries.

The actor Microsoft tracks as SOURGUM is a private-sector offensive actor (PSOA) that operates as the company called Candiru, based out of Israel that develops a sophisticated toolset to install malware on a victim through exploiting Windows 0-days, such as the now-patched CVE-2021-31979 and CVE-2021-33771, and popular browsers. Browser exploits appear to be served via single-use URLs sent from messaging applications such as WhatsApp. They generally sell these cyberweapons as part of a "hacking-as-a-service" package that is sold to government agencies and malicious actors around the world who then use them in their own operations. A popular malware that SOURGUM installs upon compromising a system through a browser exploit or Windows 0-day is DevilsTongue, a complex modular, multi-threaded piece of malware with several novel capabilities. Please read more about this actor here - https://blogs.microsoft.com/on-the-issues/2021/07/15/cyberweapons-cybersecurity-sourgum-malware/.

Learn more

Also known as:

- SOURGUM

Country of origin:

Israel

Microsoft Security