Mphasis
The Next Applied

LilacSquid: The Stealthy Trilogy of PurpleInk, InkBox and InkLoader

Date: 04th June 2024 | Severity: High

Summary

- The LilacSquid threat group (AKA UAT-4820), first reported by Cisco Talos in May 2024, has been active since at least 2021. The APT group targets organizations from various sectors, such as information technology, energy, and pharmaceuticals, located in the United States, Europe, and Asia.
- LilacSquid gains initial system access either by exploiting known vulnerabilities in public-facing application servers or by leveraging compromised remote desktop protocol (RDP) credentials. Once inside the system, the threat actors deploy open source tools, including Secure Socket Funneling (SSF) to establish tunnels to remote servers, and MeshAgent to maintain remote access and download the PurpleInk malware, LilacSquid's custom version of Quasar RAT.

Attack Vectors

- ”The campaign is geared toward establishing long-term access to compromised victim organizations to enable LilacSquid to siphon data of interest to attacker-controlled servers,” Cisco Talos researcher Asheer Malhotra said in a new technical report published today.
- Targets include information technology organizations building software for the research and industrial sectors in the U.S, energy companies in Europe, and the pharmaceutical sector in Asia, indicating a broad victimology footprint.
- Attack chains are known to exploit either publicly known vulnerabilities to breach internet-facing application servers or make use of compromised remote desktop protocol (RDP) credentials to deliver a mix of open-source tools and custom malware.
- The campaign's most distinctive feature is the use of an open-source remote management tool called MeshAgent, which serves as a conduit to deliver a bespoke version of Quasar RAT codenamed PurpleInk.
- Alternate infection procedures leveraging compromised RDP credentials exhibit a slightly different modus operandi, wherein the threat actors choose to either deploy MeshAgent or drop a .NET-based loader dubbed InkLoader to drop PurpleInk.
- A successful login via RDP leads to the download of InkLoader and PurpleInk, copying these artifacts into desired directories on disk and the subsequent registration of InkLoader as a service that is then started to deploy InkLoader and, in turn, PurpleInk,” Malhotra said.

- PurpleInk, actively maintained by LilacSquid since 2021, is both heavily obfuscated and versatile, allowing it to run new applications, perform file operations, get system information, enumerate directories and processes, launch a remote shell, and connect to a specific remote address provided by a command-and-control (C2) server.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• 2eb9c6722139e821c2fe8314b356880be70f3d19d8d2ba530adc9f466ffc67d8 • f81b9820f6fa7f11c8d4d223f57a579c • 75165906a74ad25299780e568bfac9782023d1f7
IP	• 199.229.250[.]142 • 67.213.221[.]6 • 45.9.251[.]14 • 192.145.127[.]190

Recommendation

- Enumerate the process and send the process ID, name and associated Window Title to the C2.
- Terminate a process ID (PID) specified by the C2 on the infected host.
- Run a new application on the host – start process.
- Get drive information for the infected host, such as volume labels, root directory names, drive type and drive format.
- Enumerate a given directory to obtain underlying directory names, file names and file sizes.
- Read a file specified by the C2 and exfiltrate its contents.
- Replace or append content to a specified file.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https://blog.talosintelligence.com/lilacsquid/
- https://thehackernews.com/2024/05/cyber-espionage-alert-lilacsquid.html
- https://www.darkreading.com/cyberattacks-data-breaches/lilacsquid-apt-employs-open-source-tools-quasarrat