Hackers Exploiting Microsoft's Quick Assist Tool to Deliver Ransomware

Date: 28th May 2024 | Severity: Medium

Summary

Hackers often target remote assist tools because they create a direct channel to access desired systems with minimum effort. These tools have been built for remote control and access purposes, which makes them very appealing targets for attackers looking to hack networks or take over specific devices. Microsoft observed the Storm-1811 group using Quick Assist for social engineering attacks that deploy Black Basta ransomware.

Attack Vectors

- The attacks begin with vishing, exploiting Quick Assist's remote access for initial compromise, and then delivering malware like:- Qakbot Cobalt Strike
- Microsoft is improving Quick Assist warnings against tech support scams while detections block malicious activity. Blocking unused remote tools and user education on recognizing scams can reduce risk. Threat actors involved in threat activities impersonate IT support to undertake vishing attacks and trick target persons into giving them Quick Assist remote access. They usually do this by pretending to fix a problem or offering spam help as a response to email flooding.
- While on the call, Microsoft said they got the victim to initiate Quick Assist, enter the given code, enable screen sharing, and grant control access, consequently fully compromising the device. Control is taken over through Quick Assist during which scripts are run to download malicious payloads that sometimes pretend to be spam filter updates in order to harvest credentials.
- Some of the observed payloads included Qakbot and remote management tools such as ScreenConnect and Cobalt Strike, which finally led to the deployment of Black Basta ransomware by the Storm-1811 group using their access from Qakbot and Cobalt Strike.
- After initial access, the attackers use ScreenConnect for persistence and lateral movement, NetSupport Manager for remote control, and OpenSSH tunneling. They perform domain enumeration and use PsExec to deploy Black Basta ransomware received from the Qakbot and Cobalt Strike access by Storm-1811. Black Basta is closed ransomware distributed by a few actors. Relying on initial access brokers while focusing on pre-ransomware stages reduces the threat impact.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• 71d50b74f81d27feefbc2bc0f631b0ed7fcdf88b1abbd6d104e66638993786f8 • 0f9156f91c387e7781603ed716dcdc3f5342ece96e155115708b1662b0f9b4d0 • 1ad05a4a849d7ed09e2efb38f5424523651baf3326b5f95e05f6726f564ccc30 • 93058bd5fe5f046e298e1d3655274ae4c08f07a8b6876e61629ae4a0b510a2f7 • 1cb1864314262e71de1565e198193877ef83e98823a7da81eb3d59894b5a4cfb
Domains	• upd7a[.]com • upd7[.]com • upd9[.]com • upd5[.]pro
URLs	• instance-olqdnn-relay.screenconnect[.]com • greekpool[.]com • zziveastnews[.]com • realsepnews[.]com

Recommendation

- Block and uninstall unused remote tools like Quick Assist, and use secure alternatives like Remote Help.
- Educate users on identifying tech support scams and not providing unauthorized remote access.
- Report suspected malicious remote sessions and tech support scams.
- Train users on protecting info, spotting phishing, and reporting recon attempts.
- Implement anti-phishing solutions like Defender for Office 365.
- Enable cloud-delivered protection and tamper protection in antivirus.
- Turn on network protection against malicious domains.
- Use automated investigation and remediation in Defender for Endpoint.
- Follow Microsoft’s ransomware hardening guidance.

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://cybersecuritynews[.]com/hackers-exploiting-quick-assist-ransomware/
- https://www[.]securityweek[.]com/microsoft-quick-assist-tool-abused-for-ransomware-delivery/