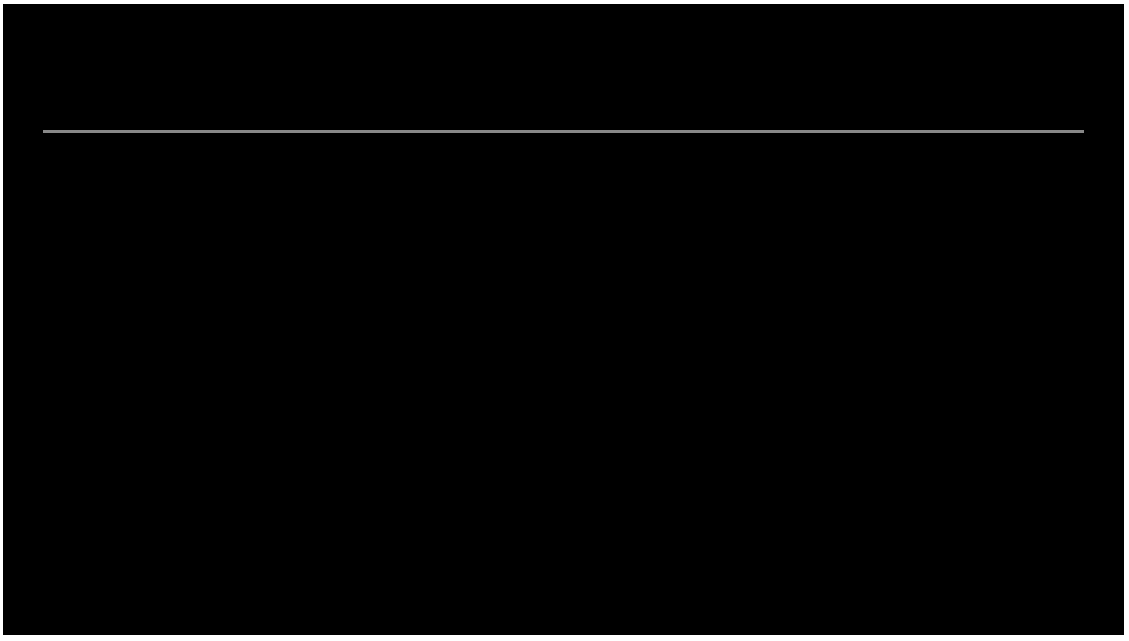
Storm-1811 exploits RMM tools to drop Black Basta ransomware

By susannah.matt@redcanary.com

Archived: 2026-04-05 13:53:41 UTC

Red Canary has detected likely Storm-1811 activity in multiple customers in the past few weeks. Storm-1811 is Microsoft's name for a financially motivated threat actor that uses social engineering to impersonate help desk employees or other IT admins to gain initial access to environments via remote monitoring and management (RMM) tools—in this case Microsoft Quick Assist—on victim endpoints. Without prompt response, this activity can lead to Black Basta ransomware in your environment.



Storm-1811's attack path

Consistent with the Storm-1811 activity we reported in our June 2024 Intelligence Insights, the recently observed activity began with email bombing to flood a victim's inbox with spam, followed by the adversary, posing as an IT admin offering to help with the email problem, contacting the user via phone or a link to join a Microsoft Teams call. Once in contact, the adversary guided the user into running Microsoft Quick Assist or downloading and running AnyDesk or TeamViewer to provide remote access. The attack continued with reconnaissance, lateral movement, and the establishment of an SSH tunnel backdoor.

Take action

We recommend taking the following precautions to prevent this activity from reaching your environment.

Enhance endpoint visibility

- Deploy detection and response sensors across systems
- Unmonitored endpoints = attacker playground; visibility limits adversary freedom

Monitor RMM tools

- Maintain an approved tools list and monitor or deny unauthorized RMM tools
- Legitimate tools can be exploited—know what's in your environment

Secure Microsoft Teams usage

- Disable external access by default
- Allowlist trusted partner domains
- Limit file-sharing capabilities to reduce risks from unauthorized tools

You can find more information on Black Basta ransomware in CISA's recent #StopRansomware advisory.
