Intelligence Insights: June 2024

By susannah.matt@redcanary.com

Archived: 2026-04-05 13:08:12 UTC

⬆ = trending up from previous month
⬇= trending down from previous month
➡ = no change in rank from previous month

*Denotes a tie

Tracking Storm-1811's help desk scams

Our newcomer to the list this month is Storm-1811. Beginning in late April 2024 and continuing throughout May, Red Canary saw an activity cluster that we are tracking as Storm-1811. This is Microsoft's name for a financially motivated threat actor that uses social engineering to gain initial access to environments via remote monitoring and management (RMM) tools—including Microsoft Quick Assist—on victim endpoints.

Storm-1811 leverages different communication methods in ways that increase the effectiveness of their social engineering scams. They use voice phishing (aka vishing) and call users masquerading as tech support, sometimes after reportedly flooding the users' inboxes with emails. In recent attacks they have also reportedly used Microsoft Teams messages to increase their credibility as IT staff, according to Microsoft. The adversary convinces victims to provide remote access through Microsoft Quick Assist or by downloading and running AnyDesk.

After the adversary gains access, we observed Storm-1811 using curl to download additional tools like OpenSSH, ScreenConnect, and NetSupport Manager. Other reported payloads include Impacket, used for lateral movement, and PsExec, used to deploy Black Basta ransomware

Social engineering attacks are, admittedly, hard to combat. Some mitigation strategies to consider are:

- Training users to verify the identity of IT staff that call them via trusted internal methods, for example confirming identities with video calls or requiring a shared secret like the endpoint in question's serial number.
- QuickAssist is installed by default on Windows machines. If it is not in use in your environment, disable or uninstall it.
- Inventory the RMMs that are approved for use in your environment. Investigate security alerts for unapproved RMMs and also suspicious activity related to approved RMMs. If possible, block RMMs commonly used in malicious attacks—for example, NetSupport, AnyDesk and ScreenConnect—that aren't in use in your environment.

Red Canary also saw Storm-1811 use `bitsadmin.exe` to download follow-on payloads. This gives us a detection opportunity.

Detection opportunity: Executing the Background Intelligent Transfer Service (`bitsadmin.exe`) to download files

This pseudo detection analytic identifies execution of the Background Intelligent Transfer Service (`bitsadmin.exe`) with command options to signal file downloads. Adversaries like Storm-1811 use `bitsadmin.exe` to download malware as a way of bypassing application whitelisting solutions. Note that `bitsadmin.exe` may be used legitimately by some administration software in your environment.

process == (`bitsadmin`)

&&

command_line_includes == (`download`)

&&

deobfuscated_command_line_includes == (`bitsadmin` , `download`)

&&

command_line_does_not_include == (`*`)

Note: `*` is a placeholder for strings associated with legitimate use of `bitsadmin` in your environment

---

In case you missed it: Open your scripts with Notepad

Many malware families use scripts as part of their intrusions. They have been popular with adversaries for years, a trend that shows no sign of slowing down. These lures can come in the form of multiple script types, including JavaScript, and delivered multiple ways.

If a trusting user opens that malicious script, one way to mitigate script execution is to create a Group Policy Object (GPO) to change the default behavior of commonly misused script extensions, making them behave like benign text files that open in Notepad and do not automatically execute. On May 31, Jeff Felling and Red Canary published a blog about recent prevalent threats like SocGholish and Gootloader that use this technique, and shared specific details on how to create these GPOs to help protect your environment.
