Detection of Drive-by Compromise, Detection Strategy DET0782

Archived: 2026-04-05 16:53:04 UTC

AN1914

Monitor for unusual network traffic that may indicate additional tools transferred to the system. Use network intrusion detection systems, sometimes with SSL/TLS inspection, to look for known malicious scripts (recon, heap spray, and browser identification scripts have been frequently reused), common script obfuscation, and exploit code.
Firewalls and proxies can inspect URLs for potentially known-bad domains or parameters. They can also do reputation-based analytics on websites and their requested resources such as how old a domain is, who it's registered to, if it's on a known bad list, or how many other users have connected to it before.
Monitor for behaviors on the endpoint system that might indicate successful compromise, such as abnormal behaviors of browser processes. This could include suspicious files written to disk.
Monitor for newly constructed files written to disk through a user visiting a website over the normal course of browsing.
Monitor for newly constructed network connections to untrusted hosts that are used to send or receive data.

Log Sources
