Kill Chain Phase	Detail
Reconnaissance	Created a passive domain server and mimicked orion network communications
Weaponisation	Introduced code that would notify the attackers if SolarWinds started a new software project
Delivery	Gained access to server using password found on public messaging app “solarwinds123”
Exploitation	Accessed Cybersecurity and Infrastructure Security Agency computers
Installation	Monitored network using malicious build files
Command and Control	Automated process to replace code
Actions on Objectives	Attackers can sidestep API authentication

Mitigations

Reconnaissance - SolarWinds should not post client lists on website

Weaponisation - use checksum to verify compilation integrity

Delivery - use passwordless authentication

Exploitation - Air gap critical systems

Installation - scan build files

C2 - do not allow macros in compiling code

AOO - APIs should require physical keys

Tools-

2 factor authentication, code scanning tools such as sentry.