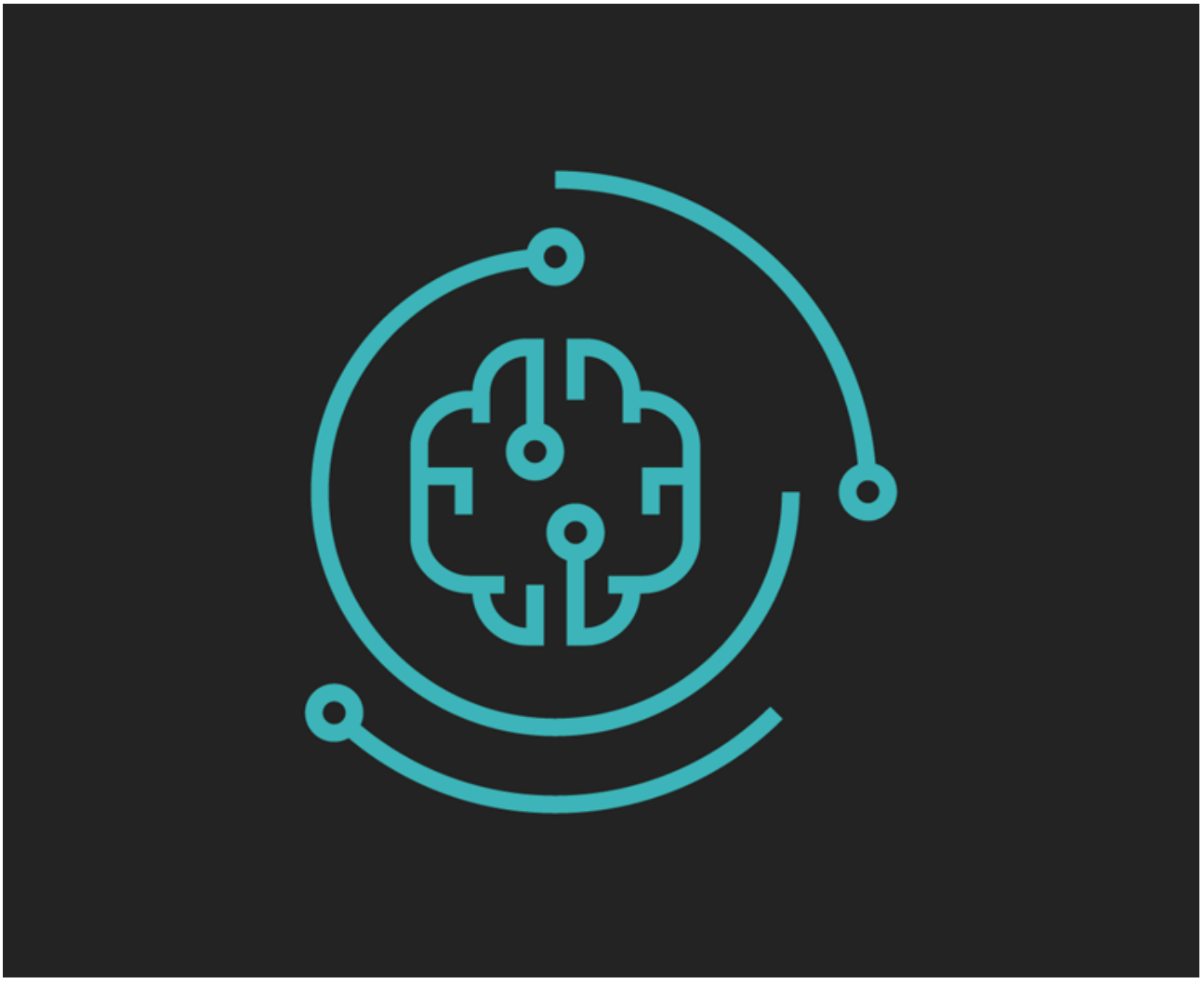
Advisory: Misuse of Visual Studio Code for traffic tunnelling

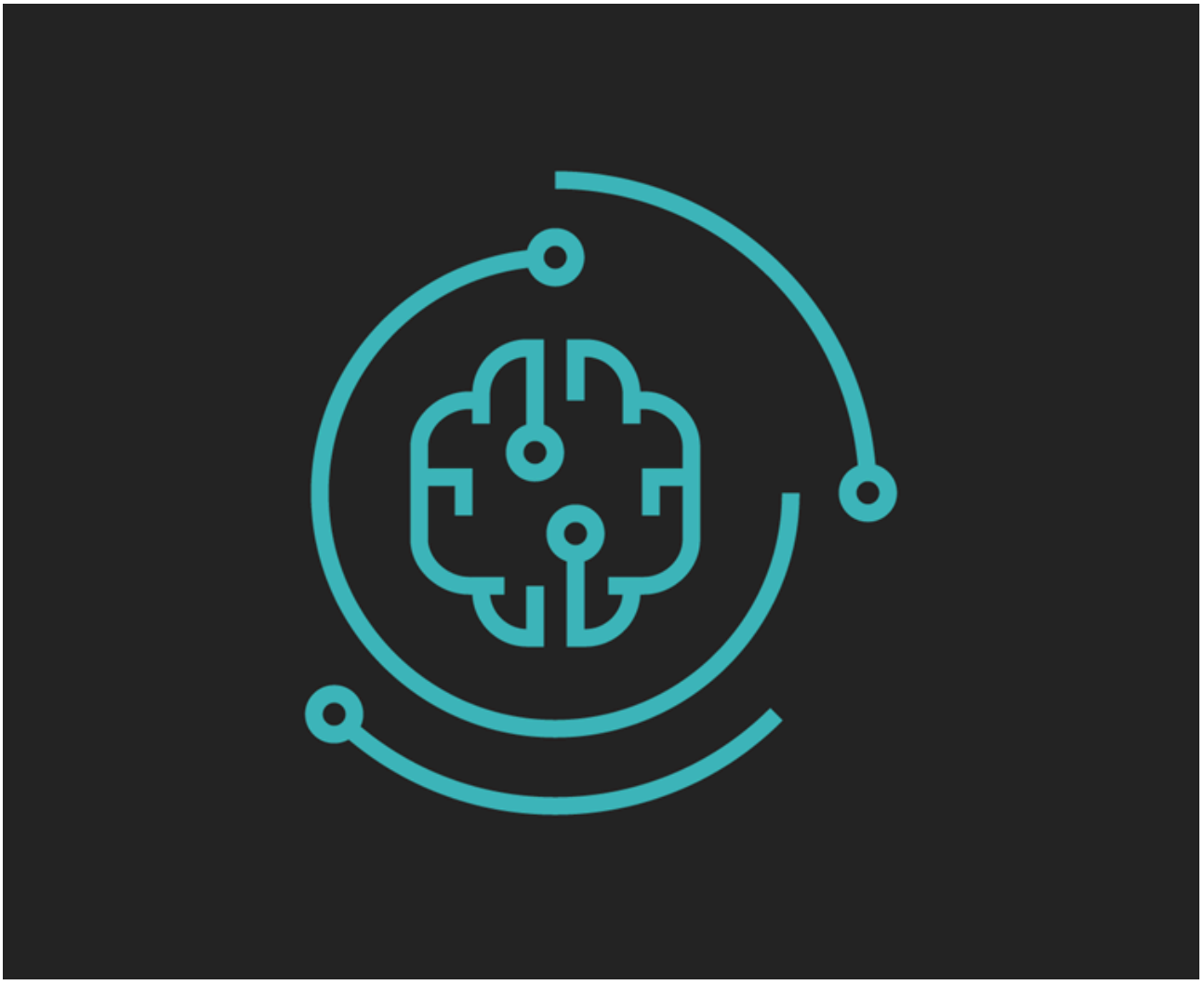
Archived: 2026-04-06 02:58:35 UTC

Blog

Published date:23.05.2024



Adversary misuse of remote development extensions in Visual Studio (VS) Code observed in the wild.



Written by:

By Threat Intelligence Team

mnemonic

Background

In May 2024, mnemonic responded to an incident involving adversary use of VS Code's remote development extensions.

The misuse of this technique has recently been observed in a cyber espionage context, but has not been previously linked to what we assess is cybercrime activity.

The technique has been theorised previously, but reports of it being utilised in the wild are limited to these two instances.

Threat Intelligence assessment

We recently observed this technique used in the wild by a threat actor likely attempting to gain foothold on a domain controller. We have not been able to ascertain the threat actor's goal in this specific incident, but we assess that this was possibly performed by an initial access broker (IAB).

This assessment is based on the tactics, techniques, and procedures (TTPs) used by the threat actor.

Activity	**MITRE ATT&CK mapping**
1. Attempted to brute-force VPN credentials	T1110.004 - Credential Stuffing
2. Authenticated via VPN using compromised single-factor credentials	T1078 - Valid Accounts
3. Established RDP connection directly to the domain controller	T1021.001 - Remote Services: Remote Desktop Protocol
4. Created a new service initiating code.exe in tunnel mode	T1543.003 - Create or Modify System Process: Windows Service
5. Utilised 7-Zip to prepare ntds.dit for exfiltration	T1560.001 - Archive Collected Data: Archive via Utility
6. Exfiltrated ntds.dit archive using code.exe tunnel	T1048 - Exfiltration Over Alternative Protocol
7. Terminated the code.exe process	T1489 - Service Stop
Activity	**MITRE ATT&CK mapping**
1. Attempted to brute-force VPN credentials	T1110.004 - Credential Stuffing
2. Authenticated via VPN using compromised single-factor credentials	T1078 - Valid Accounts
3. Established RDP connection directly to the domain controller	T1021.001 - Remote Services: Remote Desktop Protocol
4. Created a new service initiating code.exe in tunnel mode	T1543.003 - Create or Modify System Process: Windows Service
5. Utilised 7-Zip to prepare ntds.dit for exfiltration	T1560.001 - Archive Collected Data: Archive via Utility
6. Exfiltrated ntds.dit archive using code.exe tunnel	T1048 - Exfiltration Over Alternative Protocol

7. Terminated the code.exe process	T1489 - Service Stop

The threat actor used approximately three hours to execute their attack chain.

Recommendations

We strongly advise to configure and deploy the set of Group Policy Objects (GPOs) described by Microsoft. The following policies are supported:

- Disable anonymous tunnel access
- Disable tunnel access in general
- Only allow tunnel access from specific Microsoft Entra tenant IDs

On a network level, access can be blocked by dropping or blocking outbound access to *global.rel.tunnels.api.visualstudio.com*.

mnemonic also recommends searching for any suspicious services initiating code.exe on servers where it should not be running, such as on domain controllers.

In addition, mnemonic recommends monitoring for network traffic directed towards *global.rel.tunnels.api.visualstudio.com* from servers or network zones that should not be communicating with this service.

Detection coverage for Argus MDR customers

We have deployed detection to all Argus MDR customers based on the abovementioned incident and are continuously monitoring the situation to develop additional detection logic.
