Microsoft Store app used to deliver Vinci RAT via fake snipping tool site



eSentire describes an attack in which a Microsoft Store app delivered Vinci RAT, a remote access trojan. Victims are redirected to a fake snipping tool site that serves a Microsoft-signed installer.

- Researchers disclosed an attack that used a Microsoft Store application to deliver Vinci RAT.
- Vinci RAT is a remote access trojan that allows remote control of a system.
- According to eSentire, the chain starts with a redirect to a fake snipping tool site.
- The site serves a Microsoft-signed installer named Snipping-Tool.exe.
- The source excerpt does not give victim numbers or further technical detail.

Cybersecurity researchers have published details of an intrusion in which an attacker used a Microsoft Store

application to deliver a remote access trojan known as Vinci RAT. The findings are attributed to eSentire.

What was reported

According to eSentire, the attack begins when a user is redirected to a bogus website posing as a source for a snipping tool. From that site, a Microsoft-signed installer named "Snipping-Tool.exe" is delivered. The trojan can give the operator remote control of the infected system.

The available source text is an excerpt, so it does not describe the later stages of the infection, the scale of the campaign or the actors involved. We have not added anything beyond what was reported.

Why it matters

A digital signature from Microsoft and a link to the Microsoft Store can make an installer look trustworthy to users and to some controls. Institutions that rely on signature or store origin as a sign of safety should recognise that this signal alone was not enough here.

What to do next

Treat utilities such as screen capture tools as software that needs approval, even when they appear to come from a trusted store. Check whether the named installer or domain appears in your environment, and remind staff to install tools only through approved channels.

What to do now

1. Search endpoint and proxy logs for the domain snipp.codes-team[.]com and for Snipping-Tool.exe.
2. Block the named domain at the web gateway and DNS layer.
3. Restrict Microsoft Store and user software installation to an approved application list.
4. Do not treat a Microsoft signature alone as proof of safety; apply allow-listing and reputation checks.
5. Remind staff to obtain utilities only from approved internal channels, and to report unexpected redirects.
6. If the installer is found, isolate the device and start incident response.