Severity

High

Analysis Summary

The BazarLoader malware is a backdoor or malware that is installed on a Windows host that has been compromised. Bazar Loader has targeted a wide range of enterprises in North America and Europe since its launch in April 2020. BazarLoader presently employs a BazarCall technique to infect the victim's machine and give attackers backdoors that can be used to deliver follow-up malware, monitor the environment, and target more susceptible hosts on the network in the future. The malware was discovered as part of the Team9 malware family, which was linked to the Trickbot development team.

Impact

- Data Exfiltration
- Credential Theft
- Exposure of Sensitive Data

Indicators of Compromise

MD5

- bfe434f1b9025699318b22e3cd682d0b

SHA-256

- 8c281412e64050c64d1e734d844ecc6a94e7187378365d5d9ade89e67871d20e

SHA-1

- 3e4c96cd6e9aa227e4ac95fb4f31cdb952933883

Remediation

- Block all threat indicators at your respective controls.
- Keep Windows up-to-date.
- Keep an eye out for malicious emails and upgrade spam properties in email applications.
- Never download files from malicious websites.