Customer Guidance for the Dopplepaymer Ransomware

By simon-pope

Published: 2019-11-20 · Archived: 2026-04-05 14:07:11 UTC

Microsoft has been investigating recent attacks by malicious actors using the *Dopplepaymer*ransomware. There is misleading information circulating about Microsoft Teams, along with references to RDP (*BlueKeep*), as ways in which this malware spreads. Our security research teams have investigated and found no evidence to support these claims. In our investigations we found that the malware relies on remote human operators using existing Domain Admin credentials to spread across an enterprise network.

We want to help businesses and governments around the world better protect themselves from these attacks. Protection from *Dopplepaymer* and other malware is already available for customers using Windows Defender, and we will continue to enhance these protections as we identify new emerging threats.

Globally, ransomware continues to be one of the most popular revenue channels for cybercriminals as part of a post-compromise attack. They tend to target enterprise environments through methods like social engineering, enticing an employee to click a link to visit an infected site, and opening downloaded or emailed infected documents and programs on their computers.

Security administrators should view this threat as additional motivation to enforce good credential hygiene, least privilege, and network segmentation. These best practices can help prevent *Dopplepaymer* operators and other attackers from disabling security tools and using privileged credentials to destroy or steal data or hold it for ransom.

More information on ransomware and how to stay safe online is available here.

— Mary Jensen and Dan West, Senior Security Program Managers, MSRC

- BlueKeep
- Doppepaymer
- Malware
- Microsoft Teams
- Ransomware
- RDP
