Microsoft Threat Intelligence
@MsftSecIntel
Dec 21 • 6 tweets • 1 min read • Read on X

Microsoft has observed the Iranian nation-state actor Peach Sandstorm attempting to deliver a newly developed backdoor named FalseFont to individuals working for organizations in the Defense Industrial Base (DIB) sector.

FalseFont is a custom backdoor with a wide range of functionalities that allow operators to remotely access an infected system, launch additional files, and send information to its C2 servers. It was first observed being used against targets in early November 2023.

The development and use of FalseFont is consistent with Peach Sandstorm activity observed by Microsoft over the past year, suggesting that Peach Sandstorm is continuing to improve their tradecraft.

Microsoft Defender Antivirus detects FalseFont as Backdoor:MSIL/FalseFont.A!dha. The following IOCs can help orgs hunt for FalseFont in their environment:
C2: Digitalcodecrafters[.]com
SHA-256: 364275326bbfc4a3b89233dabdaf3230a3d149ab774678342a40644ad9f8d614

Additional mitigation information to help organizations harden their attack surface against Peach Sandstorm campaigns can be found here:

Peach Sandstorm password spray campaigns enable intelligence collection at high-value targets | Microsoft Security Blog
Since February 2023, Microsoft has observed a high volume of password spray attacks attributed to Peach Sandstorm, an Iranian nation-state group. In a small number of cases, Peach Sandstorm successful…
https://msft.it/6018ib1W8

Microsoft continues to track Peach Sandstorm and detect associated activity through Microsoft Defender XDR.