Microsoft: Hackers target defense firms with new FalseFont malware

By Sergiu Gatlan

Published: 2023-12-21 · Archived: 2026-04-05 13:19:50 UTC

Microsoft says the APT33 Iranian cyber-espionage group is using recently discovered FalseFont backdoor malware to attack defense contractors worldwide.

"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," the company said.

The DIB sector targeted in these attacks comprises over 100,000 defense companies and subcontractors involved in researching and developing military weapons systems, subsystems, and components.


DIE LINKE.
0:00

Also tracked as Peach Sandstorm, HOLMIUM, or Refined Kitten, this hacking group has been active since at least 2013. Their targets span a wide range of industry sectors across the United States, Saudi Arabia, and South Korea, including government, defense, research, finance, and engineering verticals.

FalseFont, the custom backdoor deployed in the campaign unveiled by Microsoft today, provides its operators remote access to compromised systems, file execution, and file transfer to its command-and-control (C2) servers.

According to Microsoft, this malware strain was first observed in the wild around 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," Redmond said.

Network defenders are advised to reset credentials for accounts targeted in password spray attacks to reduce the attack surface targeted by APT33 hackers.

They should also revoke session cookies and secure accounts and RDP or Windows Virtual Desktop endpoints using multi-factor authentication (MFA).

Defense contractors under attack

In September, Microsoft warned of another campaign coordinated by the APT33 threat group that targeted thousands of organizations worldwide, including in the defense sector, in extensive password spray attacks since February 2023.

"Between February and July 2023, Peach Sandstorm carried out a wave of password spray attacks attempting to authenticate to thousands of environments," the Microsoft Threat Intelligence team said.

"Throughout 2023, Peach Sandstorm has consistently demonstrated interest in US and other country's organizations in the satellite, defense, and to a lesser extent, pharmaceutical sectors."

The attacks resulted in data theft from a limited number of victims in the defense, satellite, and pharmaceutical sectors.

An Iran-linked hacking group dubbed DEV-0343 by researchers at Microsoft Threat Intelligence Center (MSTIC) also attacked U.S. and Israeli defense tech companies two years ago, according to an October 2012 Microsoft report.

In recent years, defense agencies and contractors around the world have also landed in the crosshairs of Russian, North Korean, and Chinese state hackers.

Source: https://www.bleepingcomputer.com/news/security/microsoft-hackers-target-defense-firms-with-new-falsefont-malware/