LevelBlue - Open Threat Exchange

By AlienVault

Archived: 2026-04-05 23:21:55 UTC

FileHash-MD5: 9 | **Domain:** 4

Sofacy (also known as “Fancy Bear”, “Sednit”, “STRONTIUM” and “APT28”) is an advanced threat group that has been active since around 2008, targeting mostly military and government entities worldwide, with a focus on NATO countries. More recently, we have also seen an increase in activity targeting Ukraine. In the months leading up to August, the Sofacy group launched several waves of attacks relying on zero-day exploits in Microsoft Office, Oracle Sun Java, Adobe Flash Player and Windows itself. For instance, its JHUHUGIT implant was delivered through a Flash zero-day and used a Windows EoP exploit to break out of the sandbox. The JHUHUGIT implant became a relatively popular first stage for the Sofacy attacks and was used again with a Java zero-day (CVE-2015-2590) in July 2015.
