Chunk 1 - Threat Overview

APT29, also known as Cozy Bear, was observed conducting phishing attacks against government organizations.
These campaigns leveraged spear-phishing emails containing malicious links that led to malware installation.
The malware used in this operation was identified as SUNBURST.

Chunk 2 - Technical Details

The threat actor exploited vulnerability CVE-2020-0601 to gain access to internal systems.
After initial access, they used the CommandAndControl protocol over HTTP to exfiltrate data.
Indicators of compromise include the IP address 192.168.1.10 and domain update.malicious[.]org.