مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

# Ransomware Campaign Abusing Sophos Executables

Tracking #:432315801

Date:30-04-2024

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council observed a ransomware campaign that exploits legitimate Sophos executables and DLLs.

## TECHNICAL DETAILS:

A ransomware campaign has been identified that exploits legitimate Sophos executables and DLLs by tampering with their original content, altering the entry-point code, and embedding decrypted payloads as resources. This deceptive tactic aims to infiltrate systems by impersonating genuine files. The compromised Sophos files were traced back to the 2022.4.3 version of the Windows Endpoint product. By manipulating legitimate files, threat actors attempt to evade detection and compromise systems. The ransomware encrypts files, appends specific extensions, and deploys ransom notes, demanding payment for decryption keys.

This malicious behaviour is not new in the cybersecurity industry, with attackers using various tactics to infiltrate systems. The campaign has affected multiple defenders, including AVG, BitDefender, Emsisoft, and Microsoft, with payloads like Cobalt Strike, Brute Ratel, Qakbot, and Latrodectus being identified. The attackers have compromised digital signatures and utilized fake installers to distribute malicious files.

Latrodectus is a lesser-known malware loader with certain C2 capabilities, associated with the same criminal group responsible for IcedID and Danabot. It has been observed loading Danabot and is part of the ransomware campaign targeting Sophos executables. This loader is a part of the broader malicious activities aimed at infiltrating systems and compromising cybersecurity defenses.

**Indicators of Compromise:**
Attached File

## RECOMMENDATIONS:

- Block the attached IOCs on network and use the latest Threat Intelligence data to stay aware of actual TTPs and IOCs used by threat actors.
- Update Sophos Endpoint to the latest version.
- Run a full system scan to identify and isolate infected machines.
- Backup Data: Maintain offline backups of data, ensuring they are encrypted, immutable, and cover the entire organization's data infrastructure.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

## REFERENCES:

https://news.sophos.com/en-us/2024/04/26/malware-campaign-abuses-legit-defender-binaries/