Severity

High

Analysis Summary

Xloader Malware is next in line to another well known Windows-based info stealer called Formbook that's known to void credentials from web browsers and other web-based applications, gather screenshots, log keystrokes, and execute files from attackers controlled domains. Xloader is distributing via spoofed emails containing malicious file attachments of Microsoft documents and infecting about 69 countries. between December 1, 2020, and June 1, 2021, with 53% of the infections reported in the U.S. alone, followed by China's special administrative regions (SAR), Mexico, Germany, and France. This time it was spotted targeting the oil and gas industry.

Impact

- Credential Theft
- Infostealer
- Keylogging

Indicators of Compromise

MD5

- f332a751e2aab14f735aca6809d50c74

SHA-256

- cde7a256a7b8de85acb73ab4697147fbc4c9a8cda56f594b20d278e26c177856

SHA-1

- d8cfa11243268f400a8b36b0007c40e80e07b583

Remediation

- Block all threat indicators at your respective controls.
- Search for IOCs in your environment.