Severity

High

Analysis Summary

Ursnif banking trojan also known as Gozi and Dreambot has been around for more than 10 years. It gained popularity in 2015 when its source code was published on Github and since then the moderators have always tweaked some changes to make use of their arsenal according to their gains. Mainly attacking banks and other financial institutions. As banking security has hardened and more customers have used mobile banking apps, attackers have switched to using Trojans such as Ursnif to steal other types of data, including email configurations, as well as credentials and passwords stored in the web browsers and even digital wallets. Threat actors use different techniques to make a victim fall into their trap. In many cases, a phishing email is sent to a victim that contains a malicious attachment — typically an Excel spreadsheet. If the victim clicks on an “Enable Content” button, they will not see the spreadsheet; rather an embedded macro code, which contains PowerShell commands and that’s how the infection begins to unfold.

Impact

- Information Theft
- Financial Loss
- Exposure of Sensitive Information

Indicators of Compromise

MD5

- 5572213d17be7de71f36fa68eb6808a8

SHA-256

- f58f9c8e6a62223efa263da10850e188004471cb2be65264b7f91f27ebab0766

SHA-1

- 5e8b27d57f6c9dc02cf2e30d47f8ed439f0fa20e

Remediation

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