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

- 3276454ebcedec7d26569941909ed591
- 5e3bf7458c6d8e6e880db72fcdf61f3a
- 96cebbecd390842784c0e777a69677ba
- 9cf986a644dd4f06d9387f25a6da6085
- ce956c480e303a9f77422054365f8e37
- b49b83a98efff5f00dba36d77847bed9
- f8d00a8981cf4f18025e2746717e2578

SHA-256

- 0a2b10135d3a172952ae033b91474801f0de67c29b2a85dc747417d8da12b853
- 29e8bf78ac6bfd95c21e2cbb06a0a9d8088fe9e759673c81eeadd96d681b73ed
- 0f30906e13c08e424cfbeab1b11b5e9e9288798e6de9be535709c56228bbc4a4
- 03bd708a5f9411d190d3ac363d0b01eaa4d0c8625d9b68951e5a6448d659495c
- e3fb27a6761d3a9403ff5b3ddbc86e5231664980149c8fd85bcfb319cc1ebb8c
- cf2e63e3364f3ae892bd60b53ce4b8b2ff5b6e60aff138e8e0f7e18aac63c5c4
- 32c049803e5e151d305c79a1067920a7eaa2dabb92fa7f33ef950097bba016f2

SHA-1

- fdb8598e443f640127bd841bc22ee2debd5cc9cf
- dbe5b4db4b61702f523b86be1d73b742b8d120eb
- b7d3a99c33470b0dea074ba1dfb2f2212db8f8a6
- 80a3cdfe0972a699c38e044a539d49c70007d22b
- 8e5f8b5043e92d425a3731cb2c12bec880279974
- b9b38f4de57d69bf417c9bb06041161ab585f941
- 540762036aa16f29b29b681483c4516ecad93e75

Remediation

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