Severity

High

Analysis Summary

Originally a small banking Trojan, Gozi has undergone massive changes in the number of variants available to threat actors. Operating continuously since 2007, Gozi has infected millions of machines and done untold damage to all types of industries and users. At its core, Gozi variants carry similar traits across the board. Some of the similarities between versions are strings contained within the binary's .bss section, man-in-the-browser attack, specific C2 check-in format, obfuscation of the C2 check-in, keylogging, email, FTP, IM accounts data and certificate grabbing, among others. Some of the specific strains carry differences that could easily be overlooked as most of the functionality of the RAT remains the same across the board. Goziat, an older variant, makes use of built-in Windows utilities and uses a different resource directory instead of the standard "images" directory. This variant typically targets .at top-level domains. Another variant, Gozi2RM3 or Gozi IAP2.0, has changes to the C2 structure. Communication is set in two stages. Stage 1 contains a hardcoded C2 in the initial infection binary. An ISP/geolocation deny list is also employed to pre-filter connections that could be researchers. Once the first stage is passed, the second stage pushes the main payload and true configuration. As with Gozi2RM3, a geofencing solution is in place. This particular variant has been bundled with a loader used by Emotet and Dridex. There are several variants of Gozi which have become unused. These include Dreambot, Saigon, and ISFB3/Ursnif-A. It's easy to mistake one strain of Gozi for another; however, with the differences pointed out, triage and analysis should help to identify which strain of malware is presented.

MIL0000907412.xlsm

Impact

- Information theft
- Exposure of sensitive data

Indicators of Compromise

Filename

- MIL0000907412[.]xlsm

MD5

- d40bfad72dd13a14ed745827ba2a40fc

SHA-256

- b3611898ab09f4bc4cee71dd84e14cbe2e1262ab6b2147ac2a4a2578f815f531

SHA-1

- d5cd2e93fb8330f6830b03d389ee328696367f00

Remediation

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