Severity

High

Analysis Summary

A huge wave of ZLoader samples has been observed in the past 24 hours. ZLoader is also known as Terdot, DELoader, that loads the Zeus malware on victim machines after initial infection. It is a banking trojan. Like other banking trojans, It’s core capability is to harvest online account credentials for online banking sites (and some other services). When infected users land on a targeted online banking portal, malware dynamically fetches web injections from its command-and-control (C2) server to modify the page that the user sees, so that the information that the user enters into the log-in fields is sent to the cybercriminals. Attackers are found targeting victims with Invoice themed spear phishing malicious documents, in order to infect them with ZLoader. This wave of ZLoader samples also consists of files following the invoice-theme. The filenames are usually “invoice” or “case” with a special character like “.”, “-” or “_” followed by four random digits. The usual target is financial institutions and banks. ZLoader has multiple distribution methods. ZLoader was also found being distributed via malvertising campaigns earlier this September. Another campaign was found distributing ZLoader and other malware via Obfuscated VBScript in June. In April, ZLoader was also found actively targeting financial organizations.

Impact

- Credential Theft
- Financial Theft
- Data Exfiltration

Indicators of Compromise

MD5

- 1b4eb327a40a14ac4afa627125b63056

SHA-256

- 034f61d86de99210eb32a2dca27a3ad883f54750c46cdec4fcc53050b2f716eb

SHA-1

- 2c0bc274bc2fd9dab82330b837711355170fc606

Remediation

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