INTERNET CRIME COMPLAINT CENTER'S (IC3)
SCAM ALERTS
NOVEMBER 03, 2014

This report, which is based upon information from law enforcement and complaints submitted to the IC3, details recent cyber crime trends and new twists to previously-existing cyber scams.

E-ZPASS SPAM CAMPAIGN

The IC3 has received reports of a phishing scam involving E-ZPass. The E-ZPass group is an association of 26 toll agencies in 15 states that operate the E-ZPass toll collection program. The IC3 has received more than 560 complaints in which a victim receives an e-mail stating they have not paid their toll bill. The e-mail gives instructions to download the invoice by using the link provided, but the link is actually a .zip file that contains an executable with location aware malware. Some of the command and control server locations are associated with the ASProx botnet, which has previously disseminated other spam imitating major retail stores. It does not appear the E-ZPass e-mails actually attempt to entice recipients to pay anything. Rather, the infected machines are reportedly used for advertising click-fraud.

FAKE BREACH DATA SOLD FOR BITCOIN

The IC3 and partners have identified a recent trend which occurs shortly after a high-profile organization suffers a data breach. Along with the normal phishing attacks expected from a high-profile breach, false advertisements offering the "full leaked database" of compromised account credentials for sale have also appeared on various dump sites. Advertised pricing has ranged anywhere from 0.5 – 1.453 Bitcoins, and other virtual currencies are sometimes also accepted. Each advertisement usually includes a small sampling of compromised credentials reported to be from the breach, but further analysis of the sampling indicates the records are invalid.

For more information regarding online scams visit our Press Room page for the most current Public Service Announcements. https://www.ic3.gov/media/default.aspx