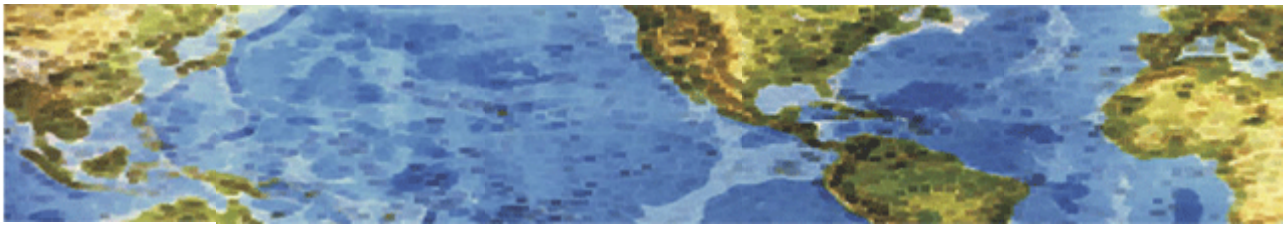
HALL ASSOCIATES



Risk-Based Decision Making Commentary
21 February 2014 Newsletter

Fire Sale on Cards Stolen in Target Breach

Last year's breach at Target Corp. flooded underground markets with millions of stolen credit and debit cards. In the days surrounding the breach disclosure, the cards carried unusually high price tags — in large part because few banks had gotten around to canceling any of them yet. Today, two months after the breach, the number of unsold stolen cards that haven't been cancelled by issuing banks is rapidly shrinking, forcing the miscreants behind this historic heist to unload huge volumes of cards onto underground markets and at cut-rate prices.

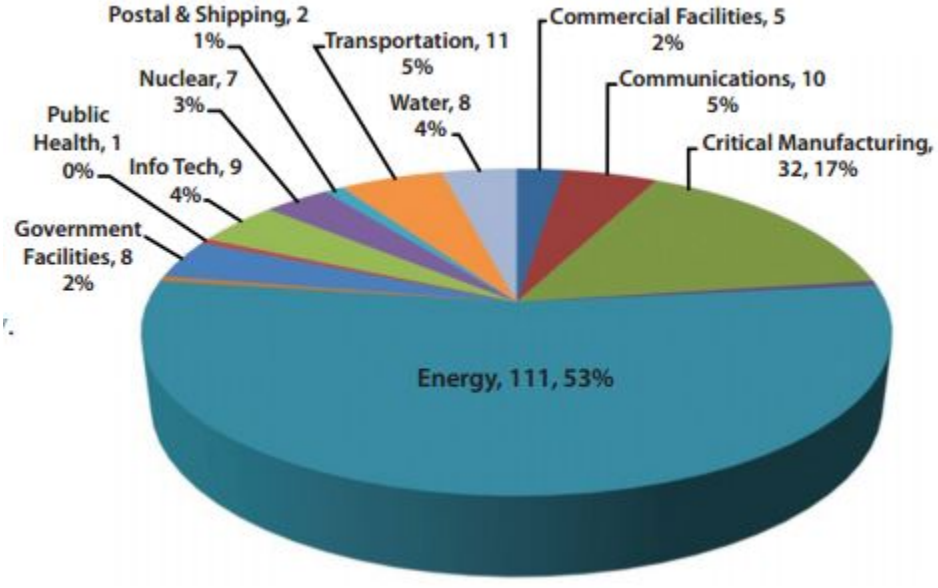
Earlier the underground card shop Rescator moved at least 2.8 million cards stolen from U.S.-based shoppers during the Target breach. This chunk of cards, dubbed "Beaver Cage" by Rescator, was the latest of dozens of batches of cards stolen from Target that have gone on sale at the shop since early December. The Beaver Cage batch of cards have fallen in price by as much as 70 percent compared to those in "Tortuga," a huge chunk of several million cards stolen from Target that sold for between $26.60 and $44.80 apiece in the days leading up to Dec. 19 — the day that Target acknowledged a breach. Today, those same cards are now retailing for prices ranging from $8 to $28. The oldest batches of cards stolen in the Target breach –i.e., the first batches of stolen cards sold –are at the top of legend in the graphic above; the "newer," albeit less fresh, batches are at the bottom.

The core reason for the price drop appears to be the falling "valid rate" associated with each batch. Cards in the Tortuga base were advertised as "100 percent valid," meaning that customers who bought ten cards from the store could expect all 10 to work when they went to use them at retailers to purchase high-priced electronics, gift cards and other items that can be quickly resold for cash. This latest batch of Beaver Cage cards, however, carries only a 60 percent valid rate, meaning that on average customers can expect at least 4 out of every 10 cards they buy to come back declined or canceled by the issuing bank. http://krebsonsecurity.com/2014/02/fire-sale-on-cards-stolen-in-target-breach/

TRENDS IN INCIDENT RESPONSE IN 2013 OVERVIEW

ICS-CERT continued its cyber incident response and risk reduction mission in 2013 by responding to an increasing number of incidents (footnoted) targeting our Nation's critical infrastructure. It's important to note that all incident reporting to ICS-CERT is done on a voluntary basis. As such, the statistics highlighted below are not representative of the actual activity occurring across all sectors. ICS-CERT strives to conduct outreach to all sectors to build relationships of trust and encourage reporting of cyber incidents. The following incident attributes have been tracked and are being shared for greater community awareness.

In 2013, ICS-CERT responded to 256 incidents reported either directly from asset owners or through other trusted partners. The majority of these incidents were initially detected in business networks of critical infrastructure organizations that operate industrial control systems (ICS). In each case, ICS-CERT evaluates the incident to determine the presence and extent of the intrusion with a focus on identifying lateral movement into the control environment or ex-filtration of sensitive ICS information from the business network. Common initial infection vectors were unauthorized access of Internet facing devices, scanning and probing of publicly accessible assets, malware transfer via removable media, exploitation of software/hardware vulnerabilities, and spear-phishing attacks. Because reporting of cyber incidents is done on a voluntary basis, it is estimated that many more incidents are occurring but are not reported. In addition, based on previous incident response efforts, ICS-CERT assesses that many incidents are not detected due to a lack of sufficient detection or logging capabilities



https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2013.pdf