Issued 3/28/17

Gift Cards are Being Drained of Funds

Gift cards have once again caused quite a headache for retailers, as cyber criminals are using a botnet to break into and steal cash from money-loaded gift cards provided by major retailers around the globe.

Dubbed **GiftGhostBot**, the new botnet specialized in gift card fraud is an advanced persistent bot (APB) that has been spotted in the wild by cyber security firm Distil Networks. GiftGhostBot has been seen attacking almost 1,000 websites worldwide and defrauding legitimate consumers of the money loaded on gift cards since Distil detected the attack late last month.

According to the security firm, any website – from luxury retailers, supermarkets to coffee distributors – that allow their customers to buy products with gift cards could be targeted by the botnet. Operators of the GiftGhostBot botnet launch brute-force attacks against retailer's website to check potential gift card account numbers at a rate of about 1.7 Million numbers per hour, and request the balance for each number.

Once the gift card account number and its balance is correctly matched, the fraudsters automatically get logged into that account without any authentication. The cyber criminals then record those account numbers to either resell them on the Dark Web or use them to purchase goods.

What's interesting? The beauty of stealing money from gift cards, according to the security firm, is that "it is typically anonymous and untraceable once stolen.”

Here's How to Protect Yourself:

Since retailers are not exposing consumers' personal information, users are strongly recommended to remain vigilant.

- Check your gift card balances and take a screenshot of the page showing your account balance as proof.
- Don’t forget your gift cards and leave it unused. Treat them like cash and use them to prevent fraud.
- Contact retailers and ask for more information if facing problems with cards.
- Inserting a CAPTCHA can help retailers prevent many bots (while not the sophisticated ones but many).
- Retailers should monitor their web traffic regularly to identify any attack. While sophisticated bots constantly rotate their IP address to evade detection, Distil has provided known IP addresses involved in the attack.
- Retailers can also put rate limits on requests to the check your balance page.