One of the most interesting aspects of this spam operation is the preservation and recovery tactics employed by its operator in order to avoid anti-spam measures.
A single spam operator has used hundreds of thousands of Twitter accounts in a large spam operation over the past year. The operation centers on weight loss and uses accounts impersonating news outlets and celebrities to promote links to companies that sell Green Coffee Bean Extract. The operator leverages readily available affiliate offers to monetize each spam campaign.

One of the most interesting aspects of this spam operation is the preservation and recovery tactics employed by its operator in order to avoid anti-spam measures. These tactics explain how this operation was able to persist for so long.

This paper takes a look inside this spam operation, breaking down its mechanics and explaining the tactics used to maintain persistence on the service. It will also present analytics from short URL services to illustrate the success of each campaign.
Instead of using compromised accounts to tweet spam links, it was using accounts that impersonated brands and celebrities.
Background

In July 2014, Symantec observed a spam campaign promoting miracle weight loss diets on Twitter. This particular campaign differed from a previous campaign we reported on. Instead of using compromised accounts to tweet spam links, it was using accounts that impersonated brands and celebrities.

Through the discovery of these imposter accounts, we identified two additional account types that were being used. The account types used in this spam operation are as follows:

- “Mockingbird” accounts—use brand and celebrity imagery for impersonation
- “Parrot” accounts—fake accounts using stolen tweets and photographs of real women
- “Egg” accounts—act like new users, with no tweets and use the default “egg” avatar

Since Twitter’s logo is a bird, we chose to associate these spam accounts with bird types that possess traits that would describe their primary function in this operation. Both Parrots and Mockingbirds are well known for their ability to impersonate birds and humans.

Understanding how each of these accounts work together is essential in understanding how this operation works.
Mockingbirds: Brand and celebrity impersonation accounts

The first type of Mockingbird account we encountered impersonated the well-known Breaking News Twitter account.

Mockingbird accounts have a singular focus: promoting so-called weight loss tricks. Each Mockingbird account uses doctored before-and-after photos to convince the viewer that the miracle weight loss Green Coffee Bean Extract product works.

Figure 3. Real vs. fake Breaking News account

Figure 4. Two impersonation accounts posting identical tweets
Based on our analysis, the spam operator has created and used a number of brand-centric impersonation accounts over the last year. These include:

- CNN
- E! Online
- TMZ
- ABC News
- MTV News
- Yahoo! News
- Breaking News
- Men’s Health

In addition to brands, the spam operator created impersonation accounts masquerading as celebrities from MTV reality shows, such as Jersey Shore’s Nicole “Snooki” Polizzi, Jenni “JWOWW” Farley, and Geordie Shore’s Vicky Pattinson.

We also noticed that a sampling of spam tweets used images of celebrities like Britney Spears, Renee Zellweger, Christina Aguilera, and Lady Gaga with supposed before-and-after photos highlighting the benefits of miracle weight loss diets.

Retweets and favorites

Each spam tweet from a Mockingbird account would receive nearly 1,000 retweets and 500 favorites. As you might expect, these retweets and favorites are not genuine, as they originate from a secondary account type, which we call the Parrot.
Uncovering a persistent diet spam operation on Twitter

Parrots: An integral part of the operation

We have previously written about how pretty girls sell retweets. Photos of women are often used when creating sock puppet accounts on Twitter. In this spam operation, these women (or Parrot accounts) are used to promote these diet pills to their followers.

“[PARROT] followed you”

On Twitter, people follow users who tweet content that might interest them. In the case of Parrot accounts, they follow any and everyone in the hope that users will follow them back because they are using avatars of attractive women. This tactic has proven to be remarkably effective. Users that do not follow back after a certain period of time are automatically unfollowed by the Parrot account.

Fake people, real content

If these Parrot accounts only retweeted miracle diet spam from the Mockingbird accounts, they would quickly be suspended. This is why the spam operator has a predefined list of tweets queued up that are posted every day by the Parrot accounts. The content typically consists of stolen tweets as well as image memes previously tweeted by real Twitter users.
Fake engagement

In addition to reposting real content, Parrot accounts will also fake engagement with Mockingbird accounts while they are promoting the diet spam.

This fake engagement is largely to convince users who might question these tweets. By showing that each tweet has engagement from Parrot accounts, the operator hopes to convince real Twitter users to see what the hype is all about. Digging deeper into the follower lists of these Parrot accounts, we found a lot of genuine Twitter users, but also a third type of fake account that we call the Egg.

Eggs: Inflating follower counts by the thousands

Twitter users that first join the service but choose not to use an avatar are given a default image of an egg. This Egg account is often how someone new to Twitter may be identified.

In this spam operation, these Egghead accounts are primarily used for one simple purpose: inflating follower counts.

When reviewing the followers of a Parrot account, you will find that a large amount of followers are Egg accounts. They are easily identifiable by the naming conventions used for their user names and full names. Most commonly, their user names contain two words that are separated by one or two underscores. Their full names contain the first word from the user name and a single underscore. However, we have seen a variation on these naming conventions.
conventions over time.

The majority of Egg accounts never compose a single tweet. They will, however, follow Parrot accounts by the hundreds. On average, an Egg account typically follows 409 Parrot accounts. We have seen some Egg accounts following up to 2,000 Parrot accounts, while others have followed less than 100. While these Egg accounts are set to follow only Parrot accounts, we have seen some following Mockingbird accounts.

Figure 12. An Egg account exclusively follows Parrot accounts
As a preservation tactic, the Mockingbird accounts delete their promotional tweets after a set amount of time.
How the spam operation works

1. Mockingbird accounts publish one-to-four tweets in succession, containing text about the miracle weight loss trick along with a before-and-after image and a shortened URL.
2. Within a few minutes, Parrot accounts begin to retweet and favorite these tweets in order for their followers to see them.
3. The Parrot accounts tweet replies back to the Mockingbird accounts, praising these miracle diets.
4. The spam tweets remain up for anywhere between 4-to-12 hours.
5. Mockingbird accounts then delete the miracle weight loss tweets.

Preservation tactics

As a preservation tactic, the Mockingbird accounts delete their promotional tweets after a set amount of time. The time varies, but on average we saw spam tweets from Mockingbird accounts remain up for at least four hours.

Figure 13. How the spamming operation works

Figure 14. Hyphenated tweet acts as a marker for automated software to remove tweets
hours before being deleted. Deleting the tweet makes it appear as though it never existed to begin with. On top of that, it ensures that the Parrot accounts are not easily found, allowing these accounts to persist for some time before Twitter can suspend them.

In addition to deleting tweets, Mockingbird accounts will also post a tweet consisting of nothing more than a series of hyphens. We believe this is a marker used by the spam operator’s automated software to delete the series of tweets that precede it.

Recovery tactics: What happens when accounts get suspended?

Inevitably, Twitter catches on and suspends Mockingbird, Parrot, and Egg accounts. While each account serves a primary purpose, the spam operator has the option of replenishing resources by “raising” each account type.

**Egg to Parrot**

This is the most common way the spam operator raises his accounts. In order to introduce more Parrot accounts into the equation, an Egg account can be easily raised to become a Parrot account. This is evident based on the naming convention used to create Egg accounts, as we have seen a number of Parrot accounts use the same convention.

We have observed accounts during the process of conversion from an Egg account to a Parrot account. This is based on the fact that these accounts have no tweets, are following Parrot accounts, and Egg accounts have been instructed to follow them.

**Parrot to Mockingbird**

A Parrot account is designed to have a high ratio of followers to following. When a Mockingbird account is suspended, the operator can simply rename the Parrot account to whatever brand or celebrity he chooses and he automatically has a built-in set of followers.
We have found some accounts mid-conversion. For instance, one Parrot account was discovered during the process of becoming a Mockingbird account. Based on the user name of MTVOnline (it is actually spelled with a capital ‘i’ instead of a lower case ‘l’), it was clear that the spam operator was planning on creating additional Mockingbird accounts as a result of the suspension of his previous accounts.

Distribution of accounts

Over the course of the last eight months, we have set up scripts that pull information from Twitter’s API in order to identify and classify the various account types involved in this spam operation.

<table>
<thead>
<tr>
<th>Account type</th>
<th>Number of accounts</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eggs</td>
<td>Over 700,000</td>
<td>94.95%</td>
</tr>
<tr>
<td>Parrots</td>
<td>Nearly 40,000</td>
<td>5.04%</td>
</tr>
<tr>
<td>Mockingbirds</td>
<td>Less than 100</td>
<td>0.01%</td>
</tr>
</tbody>
</table>

Based on this data set, we can see that the spam operator has owned nearly three quarters of a million accounts. Because Twitter has suspended some of these accounts previously, we believe the spam operator has controlled at least one million Twitter accounts over time.

Age of accounts

Looking at the age of accounts, we can see some patterns emerge. The oldest Egg account that was part of this operation dates back to September 2013. From there, we can see an uptick in the early part of 2014. The largest increase in Egg accounts happened over the course of three months, from March to May 2014, where nearly a half a million were created.

As for the Parrot accounts, we found a small amount of them were created as far back as January 2012. The creation of these accounts started to increase in June and July of 2013. They began to steadily increase at the beginning of 2014. The biggest spike in Parrot accounts created coincides with the same spike we saw previously in Egg accounts. Our statistics show
that from March to May 2014, 23,000 Parrot accounts were created.

Since there were less than 100 Mockingbird accounts we identified at the time of our research, the distribution may not reflect the totality of the overall spam operation. What we did find was that brands like MTV and E!Online made up one third of the Mockingbird accounts that we saw, followed by TMZ, CNN, and ABC. The fake celebrity accounts were also very popular, with Snooki and Vicki Pattinson accounting for 26 percent of all Mockingbird accounts.

**Figure 19. Breakdown of Mockingbird account impersonations**

**Short URL services and domains**

**Goo.gl**

While this spam operation was active, the operator used a number of short URLs. Initially, the operator used Google’s “goo.gl” short URL service and would generate a number of short URLs each day as part of a daily campaign. On average, each short URL

**Figure 20. Analytics from a goo.gl short URL**
URL would receive 413 total clicks per day with an upper peak of 1,423 total clicks and a low of 135 clicks.

**Bitly**

Starting in November 2014, the operator switched from the Goo.gl short URL service to Bitly. Interestingly, the operator stopped creating multiple short URLs daily, opting instead to repurpose a small subset of short URLs every day. This inflated the overall number of clicks for the spam operation’s short URLs. We identified 26 short URLs created on Bitly by the operator. On average, each Bitly short URL received 12,707 clicks, with an upper peak of 42,319 clicks and a low of 132.

**Domains**

Throughout the course of the spam operation, the operator created a number of .com and .us based domains that served as landing pages for his spam operation. Each domain contained some variations of the words “green,” “coffee,” and “celebrity” as well as other words like “healthy,” “smarter,” “slim,” and the years 2014 and 2015.

![Figure 21. Analytics from a bit.ly short URL](image)

![Figure 22. Words used by spammer in domain names—word size relates to number of times words were used](image)
The landing page for each domain was designed to look like the Women’s Lifestyle website.

The landing pages promoted the miracle diet known as Green Coffee Bean Extract. The spam operator used images of celebrities like Snooki and Maria Menounos to legitimize the success of these miracle diets.

**Affiliate programs**

From the Women’s Lifestyle landing pages, the operator included links to websites that claim to sell Green Coffee Bean Extract. These links are tagged with an affiliate ID in order for the company to identify the referral.

There are a number of companies that utilize affiliate programs to promote these so-called miracle diets. Certain websites aggregate these offers to make it easy for affiliates to browse them. They often include information on how an affiliate can earn money through conversion of leads and what they can expect to be paid out.
In the case of Green Coffee Bean Extract, the affiliate is only paid when a lead submits their credit card (CC) details for an alleged free trial. The affiliate can expect to earn anywhere from $36 to $60 per converted lead.

**Spam operator: connecting the dots**

Despite the use of Mockingbird, Parrot, and Egg accounts, as well as interesting tactics to preserve and recover accounts, the author failed to cover his tracks in certain areas.

Each of the domains was registered without private registration, revealing this individual’s real name and address. The Bitly accounts used for creating short URLs were associated with this individual’s Twitter and Facebook accounts. Lastly, he converted one of his Parrot accounts into a personal account, where he instructed his Parrot accounts to retweet and favorite some of his own tweets. We were able to link this spam operation to a single individual by combining these missteps.
Twitter users should always check to see if the brand or celebrity has been verified before following.
Conclusion

When you consider that Americans spend US$2 billion annually on dietary supplement pills for weight-loss, it is no wonder that scammers are also trying to cash out on this trend. These scammers have been relentless and run the gamut from Instagram to Snapchat and through compromised accounts on Twitter, Pinterest, and Tumblr.

Key takeaways

- **Look for the blue verified badge.** Twitter continues to face the problem of impersonation accounts of brands and celebrities. This spam operation convinced enough users that these imposter accounts were legitimate. Twitter users should always check to see if the brand or celebrity has been verified before following. The blue verified badge denotes that Twitter has verified the authenticity of an account.
- **Be skeptical of new followers.** If a random person follows you, do not automatically follow them back. Look at their tweets. Are they retweeting content that looks like spam? If they are, they are most likely a bot.
- **Numbers can lie.** Even if these random followers have tens of thousands of followers, those numbers can easily be faked. Do not base your decision to follow them back because of how many people follow them.
- **There is no such thing as a miracle diet.** At the end of the day, weight loss requires more than just a dietary supplement. Exercise and healthier eating is necessary in order to see real results when it comes to weight loss.

Dr. Mehmet Oz, a physician and well-known television personality who promoted miracle weight loss diets, was one of the first to publicly endorse the Green Coffee Bean Extract diet supplement in May 2012. The study that Dr. Oz cited was retracted by both of its researchers in October of 2014, because they could not assure the validity of the data obtained from it.

In June 2014, Dr. Oz was asked to testify before a Senate hearing on consumer protection. The Senators questioned Dr. Oz’s use of flowery language to promote miracle diets on his television show. Senator Dean Heller asked point blank whether or not Oz believed that a miracle pill exists. His answer should be referenced when seeing such claims made on social media.

*Dr. Oz: “There is not a pill that’s going to help you long term, lose weight and live the best life without diet and exercise.”*