HACKING A CORPORATE SOCIAL MEDIA PAGE

ZEROFOX RESEARCH

John Seymour – Senior Data Scientist

Publicly-facing social media accounts are high-value targets for attackers. Individuals and organizations alike struggle to safeguard their profiles against compromise, leading to cybervandalism, hacktivism and worse.

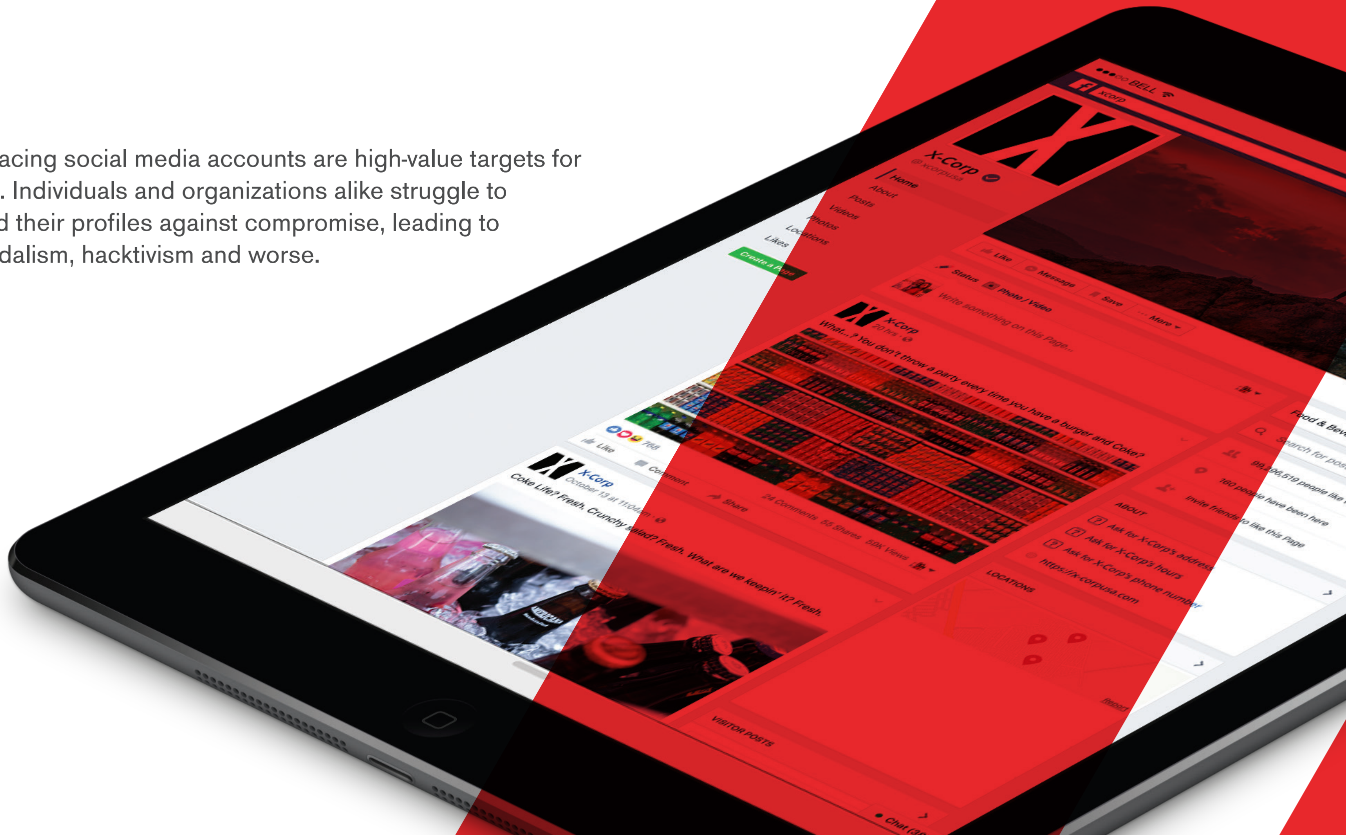

X-Corp
Home
About
Posts
Videos
Photos
Locations
Likes
Create a Page
What... ? You don't throw a party every time you have a burger and Coke?
Coke Life? Fresh. Crunchy salad? Fresh. What are we keepin' it? Fresh.
ABOUT
Ask for X-Corp's address
Ask for X-Corp's hours
Ask for X-Corp's phone number
https://x-corpusa.com
LOCATIONS
VISITOR POSTS

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY & FINDINGS

Social media account takeovers are an increasingly common occurrence, affecting the likes of politicians, celebrities, brands, other high-profile accounts and even Mark Zuckerberg, the father of the social media revolution. However, no study has been performed to analyze the prevalence, cost, motivations, and methodology of such attacks. Understanding these would be incredibly helpful for defense, for example, it could be used for effective distribution of preventative efforts. To that end, ZeroFOX Research has investigated successful account takeovers in the past 4 years and aggregated pertinent details into this white paper.

ZeroFOX Research collected over 2000 unique news articles, blog posts, social media help forum requests, and alerts from the ZeroFOX platform occurring between January 2012 and September 2016 regarding social media account takeovers. We triaged this dataset into 347 successful attacks against unique high-profile individuals or businesses and used this corpus to analyze the prevalence and cost of similar account takeovers. We then investigated the motivations of malicious actors to understand who is at risk. Finally, we looked into the tactics, techniques, and procedures surrounding account takeovers.

2. PREVALENCE OF ACCOUNT TAKEOVERS

A social media profile is a valuable tool for corporations and celebrities to spread awareness, but it's also a broad, easily exploited, and often unregulated attack surface. If the page itself is compromised, the brand can become tarnished and trusting users can be enticed to click malicious links, directing to phishing pages, scams, or exploits. Two questions arise: how often do such attacks occur, and how can we quantify the damage done?

In order to answer these questions, we collected instances of successful account takeovers of high-profile individuals and businesses. We gathered public information regarding account takeovers, including news articles, blog posts, and social media help forum requests. We augmented this dataset with alerts from our product. The post-augmentation dataset consisted of over 2000 possible instances of successful account takeovers during the time period from January 2012 to September 2016.

However, this dataset included duplicate attacks as well as attacks that were caught before any changes to social media profiles could be made. We manually triaged the duplicates and unsuccessful attacks from the dataset. As we performed this inspection, we noticed that some targets were successfully taken over multiple times. If a target was successfully taken over more than once, we chose to include each time the target was successfully taken over as a separate instance.

After triage, 347 unique instances of successful account takeovers remained. A plot of these account takeovers over time, as well as an estimate for the total number of successful account takeovers by the end of 2016, is below. We noticed an upward trend over time, signifying that more accounts are successfully taken over each year. At the time of this writing (September 2016), there have already been 83 successful account takeovers against corporations and celebrities in 2016: a 12% increase over all of 2015.

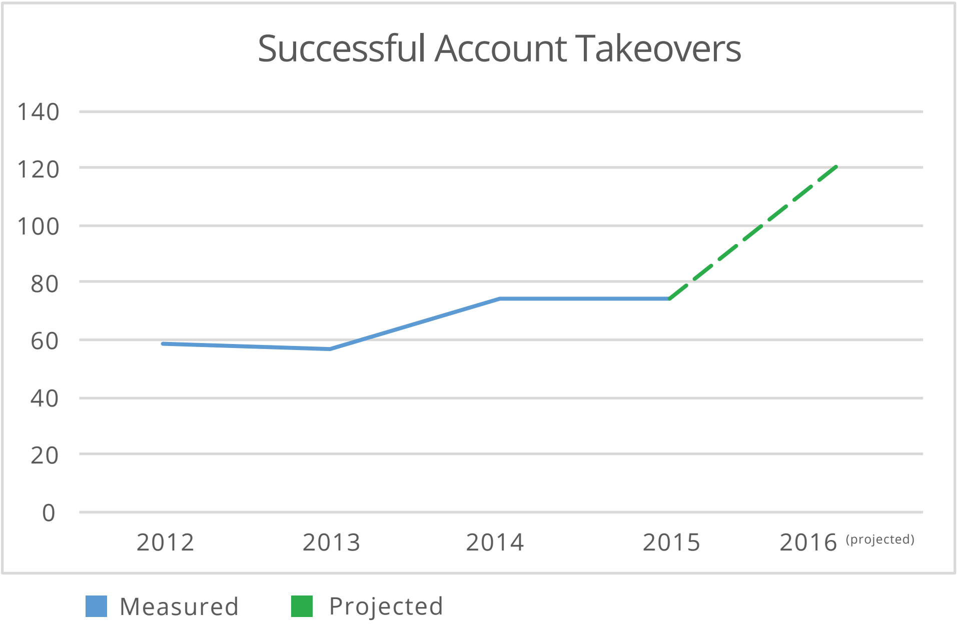
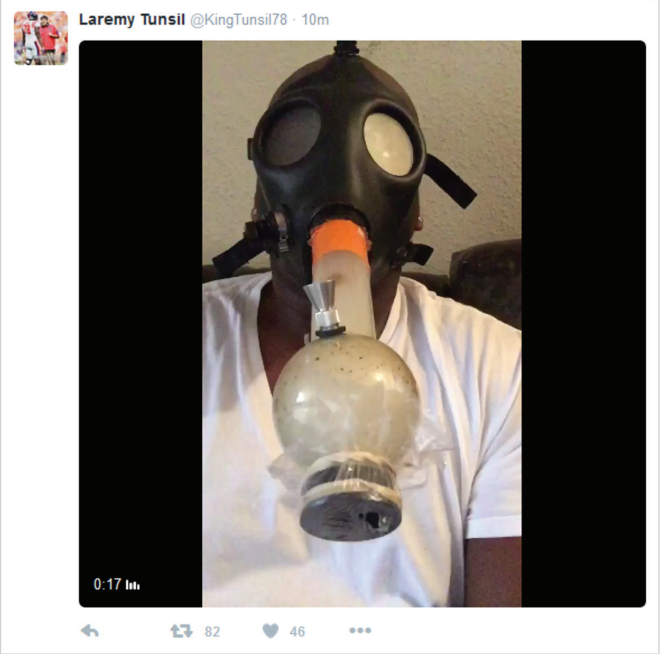


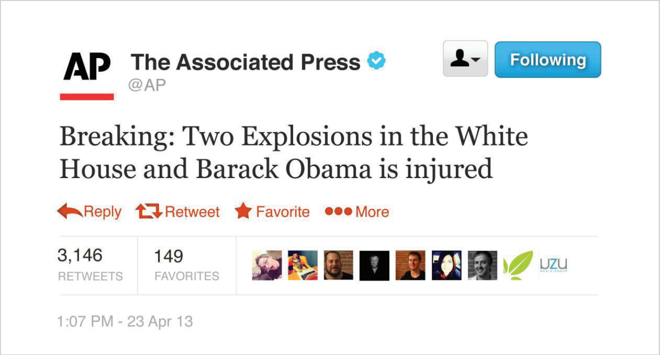
FIGURE 1.
Plot of Successful Account Takeovers over Time.

2.1 COST OF AN ACCOUNT TAKEOVER

Measuring the cost of breaches is more difficult; most instances of account takeovers do not reveal the full impact of the breach. We can, however, point to specific instances where the cost of the breach has been quantified. For example, the 2016 takeover of NFL rookie Laremy Tunsil's Twitter and Instagram accounts caused an estimated $21 million in damages.[1] In 2013, the Dow Jones industrial average dropped almost an entire percent because of fake tweets posted to the Twitter account of the Associated Press.[2] The attempted takeover of @jb, also in 2013, would have resulted in over $500,000 in damages and killed his startup had the attack been successful.[3] Clearly, these account takeovers have potentially huge financial impacts to the victims.



Laremy Tunsil @KingTunsil78 · 10m



The Associated Press @AP

Breaking: Two Explosions in the White House and Barack Obama is injured

3,146 RETWEETS

149 FAVORITES

1:07 PM - 23 Apr 13

HACKTICOOL

The blog of a husband, dad, and co-founder of Droplr.

How I Almost Lost My $500,000 Twitter Username

[1] "Laremy Tunsil: Twitter hack could cost NFL rookie millions - CNN.com." 2016. 15 Sep. 2016 <http://edition.cnn.com/2016/04/29/sport/laremy-tunsil-ole-miss-nfl-draft-twitter-hack/

[2] "A Fake AP Tweet Sinks the Dow for an Instant - Bloomberg." 2013. 15 Sep. 2016 <http://www.bloomberg.com/news/articles/2013-04-23/a-fake-ap-tweet-sinks-the-dow-for-an-instant>

[3] "How I almost lost my $500000 Twitter user name @jb... - Ars Technica." 2014. 15 Sep. 2016 <http://arstechnica.com/security/2014/01/how-i-almost-lost-my-500000-twitter-username-jb-and-my-startup/>

3. MOTIVATION OF ATTACKERS

Fortunately, this corpus often includes details as to why the attackers took over the social media accounts of their victims. In some instances, the hackers themselves disclosed their motivations through posts on the compromised account or their own accounts. In others, we can discern their motivations based on the end payoff. In our data, we found four major motivators for celebrity or corporate social network takeovers:

MONEY:

Although technically against the Terms of Service, people are willing to pay real money for handles on social networks. Several transfers have even been endorsed by the social networks, notably the sale of @Israel for over $100,000 and the deal where @ CNNbrk rents out his username as part of his consulting practice.[4,5] However, this value also attracts thieves; the hacker behind the aforementioned attempt on @jb stated he was after the Twitter handle, worth $500,000. Naoki Hiroshima's Twitter account was taken over because it was worth over $50,000.[6,7] Even common accounts are traded on dark markets just like credit cards.[8]

STREET CRED:

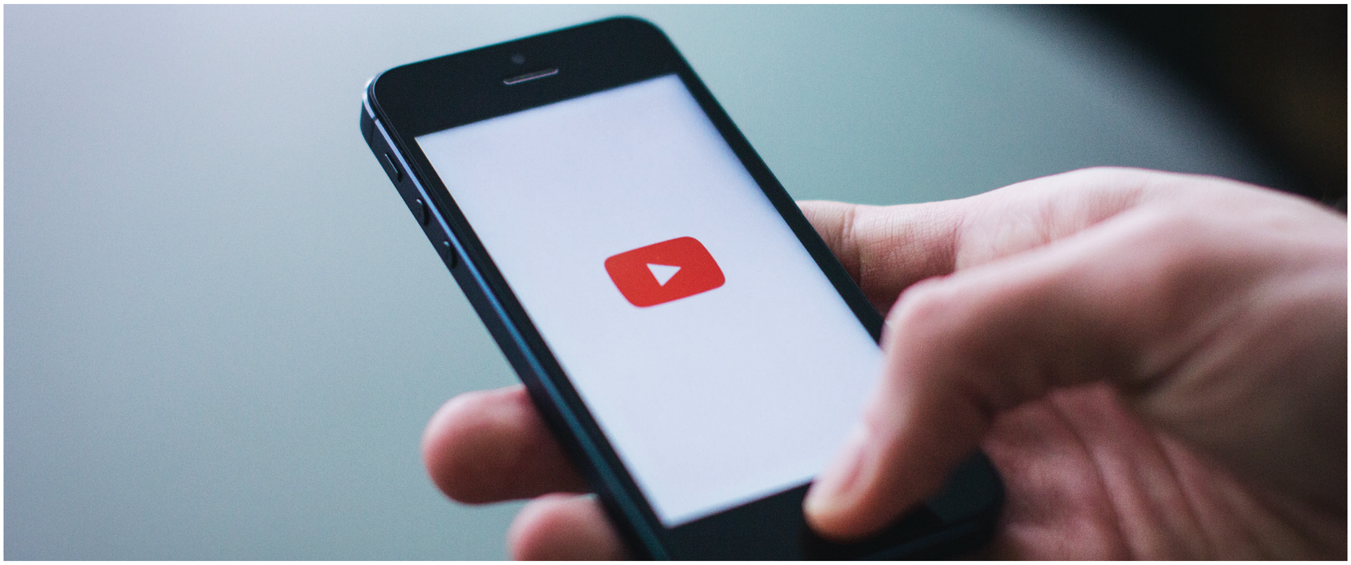
Some hackers post messages claiming responsibility for their hacks. There is risk involved in associating with an attack; it often helps law enforcement determine the perpetrator. Thus, we presume that this is a motivator for the attack in the first place. Notable examples of attacks motivated by street cred include the May 2016 Katy Perry takeover by sw4ylol and the June 2016 Zendesk takeover by NULLC0RE.[9,10]

DAMAGE:

Finally, some takeovers occur simply because the perpetrator wants to cause damage. The hacker behind Mat Honan's epic hacking just wanted to take his three-character Twitter handle, "fuck shit up, and watch it burn."[11] "For the lulz" is a repeated phrase associated with Anonymous, who took over ISIS Twitter accounts and changed profile banners to rainbows.[12] The payoff for the August 2016 Twitter takeover of Cincinatti Zoo director, Thane Maynard seemed to be just posting memes.[13] Additionally, there's no clear reason why someone would take over Lea Michele's Twitter account to post fake news about her pregnancy.[14]

POLITICAL MESSAGES:

Some groups have the ultimate goal of spreading propaganda or threats. Such was the case when CyberCaliphate took over US Central Command's Twitter and YouTube accounts, pretending to post classified documents, or when the Syrian Cyber Army took over the Twitter accounts of 60 Minutes and 48 hours to post anti-Obama tweets.[15,16] The Syrian Cyber Army also claimed credit for the Associated Press hack which caused a dip in the Dow Jones industrial average.[17]



This information can be used both to understand who is at the most risk for account takeovers and to motivate potential solutions. If even common Twitter accounts are traded on darkweb markets, all accounts carry some amount of risk. However, accounts with rare handles, such as usernames with low character counts or usernames without underscores or numbers, are particularly likely to have takeover attempts because of the inherent monetary value of the account username. Accounts with many followers, especially political accounts, celebrities or news stations, also carry increased risk to takeover attempts, due to the value for disseminating propaganda and threats. Accounts perceived to be challenging to break into, including those related to information security, risk attempted takeovers for bragging rights.

[4] "Twitter user sells @Israel username for six-figure sum - The Guardian." 2016. 15 Sep. 2016 <https://www.theguardian.com/technology/2010/sep/14/twitter-user-sells-israel-username>

[5] "Confirmed: CNN Acquires CNNBrk Twitter Account ... - TechCrunch." 2016. 15 Sep. 2016 <https://techcrunch.com/2009/04/15/confirmed-cnn-acquires-cnnbrk-twitter-account/>

[6] "How I almost lost my $500000 Twitter user name @jb... - Ars Technica." 2014. 15 Sep. 2016 <http://arstechnica.com/security/2014/01/how-i-almost-lost-my-500000-twitter-username-jb-and-my-startup/>

[7] "How I Lost My $50,000 Twitter Username – Medium." 15 Sep. 2016 <https://medium.com/@N/how-i-lost-my-50-000-twitter-username-24eb09e026dd>

[8] "Ablon, Lillian, Martin C Libicki, and Andrea A Golay. Markets for cybercrime tools and stolen data: Hackers' bazaar. Rand Corporation, 2014.

[9] "Hackers Hijacked the World's Most Followed Twitter Account - Fortune." 2016. 15 Sep. 2016 <http://fortune.com/2016/05/31/hackers-hijacked-the-worlds-most-followed-twitter-account/>

[10] "Zendesk chief's Twitter account hacked - BBC News." 2016. 15 Sep. 2016 <http://www.bbc.com/news/technology-36480997>

[11] "How Apple and Amazon Security Flaws Led to My Epic Hacking | WIRED." 2016. 15 Sep. 2016 <https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/>

[12] "Anonymous hacks pro-ISIS Twitter accounts, fills them with gay pride ..." 2016. 15 Sep. 2016 <http://www.cbsnews.com/news/anonymous-hacks-pro-isis-twitter-accounts-fills-them-with-gay-pride/>

[13] "Cincinnati Zoo Director Thane Maynard's Twitter account hacked - Story." 2016. 15 Sep. 2016 <http://www.wcpo.com/news/local-news/hamilton-county/cincinnati/cincinnati-zoo-director-thane-maynards-twitter-account-hacked>

[14] "Lea Michele Not Pregnant: Glee Star Twitter Hacked After Chris Colfer ..." 2014. 15 Sep. 2016 <http://www.usmagazine.com/celebrity-news/news/lea-michele-not-pregnant-glee-star-twitter-hacked-after-chris-colfer-201447>

[15] "CENTCOM Twitter account hacked, suspended - CNNPolitics.com." 2015. 15 Sep. 2016 <http://www.cnn.com/2015/01/12/politics/centcom-twitter-hacked-suspended/>

[16] "'60 Minutes' and '48 Hours' Twitter Accounts Hacked, Sent Anti-Obama ..." 2016. 15 Sep. 2016 <http://www.newsbusters.org/blogs/nb/noel-sheppard/2013/04/21/60-minutes-and-48-hours-twitter-accounts-hacked-sent-anti-obama>

[17] "Hackers compromise AP Twitter account - Associated Press." 2016. 15 Sep. 2016 <http://bigstory.ap.org/article/hackers-compromise-ap-twitter-account>

4. ATTACKER TACTICS, TECHNIQUES, AND PROCEDURES

Unsurprisingly, most account takeovers occur because of poor password hygiene. For example, LinkedIn's database was leaked in 2012, and Twitter's accounts database was leaked in 2013.[18,19] Although the passwords were hashed and salted in both cases, password reuse has led to some celebrity accounts being taken over, notably the Twitter and Pinterest takeovers of Mark Zuckerberg.[20]

Corporations tend to have additional issues with password hygiene, for two reasons. First, some social media teams use a shared password, which may be shared insecurely or weak enough for teams to memorize.[21] Second, many corporations loan or share social media accounts with 3rd party marketing agencies or for PR events.[22,23] Properly using password managers to share passwords, having unique passwords for each website visited, and using 2 Factor Authentication (2FA) thwarts many account takeover attempts.

> RATHER THAN ATTACKING SOCIAL MEDIA ACCOUNTS DIRECTLY, HACKERS HAVE BEEN OBSERVED SOCIAL ENGINEERING APPLE, AMAZON, PAYPAL, AND GODADDY IN ORDER TO GAIN ACCESS TO ACCOUNTS.

For taking over more valuable accounts, such as those of celebrities and corporations, a common tactic is social engineering a third party. In this method, the main goal is to either change the account recovery email or extort the user into giving up their account. Rather than attacking social media accounts directly, hackers have been observed social engineering Apple, Amazon, Paypal, and Godaddy in order to gain access to accounts.[24,25] Hackers have also abused policies in email services like Hotmail to obtain account credentials, and socially engineered cell providers to get around 2FA.[26,27] Issues with the SMS implementation of 2FA give users a false perception of security. Even if someone takes appropriate precautions, a third party can allow a hacker access to the social media account settings.

Finally, vulnerabilities within the social media applications themselves can give account access to attackers. For example, in 2014, a vulnerability in Instagram allowed for anyone on the same network to sniff Instagram session tokens.[28] This means that anyone logged in on public wifi could have their accounts taken over, at least until until the vulnerability was patched. Moreover, 70.85% of the smartphone market consists of Android phones, and they're known to have vulnerabilities too.[29,30] Since most social networks are primarily mobile-oriented, it's another attack vector.[31] Finally, nothing is stopping employees at the social networks from being targeted themselves; celebrities were hacked in 2009 because of a social media employee's weak password.[32]

[18] "Zendesk chief's Twitter account hacked - BBC News." 2016. 15 Sep. 2016 <http://www.bbc.com/news/technology-36480997>

[19] "Questions and answers about the Twitter hack – Naked Security." 2014. 15 Sep. 2016 <https://nakedsecurity.sophos.com/2013/02/02/twitter-hack-questions/>

[20] "Mark Zuckerberg's password was 'dadada'. What hope do the rest of ..." 2016. 15 Sep. 2016 <http://www.telegraph.co.uk/technology/2016/06/06/mark-zuckerbergs-password-was-dadada-what-hope-do-the-rest-of-us/>

[21] "How do companies share their social media passwords with marketing ..." 2016. 15 Sep. 2016 <https://www.quora.com/How-do-companies-share-their-social-media-passwords-with-marketing-agencies-and-freelancers>

[22] "In Which A Twitter Account Takeover Goes Very, Very Awry - Adweek." 2015. 15 Sep. 2016 <http://www.adweek.com/socialtimes/la-kings-twitter-account/484799>

[23] "Comedian Rob Delaney Takes Over @MLB Twitter Account, Hilarity ..." 2015. 15 Sep. 2016 <http://www.adweek.com/socialtimes/rob-delaney-mlb/483318>

[24] "How Apple and Amazon Security Flaws Led to My Epic Hacking | WIRED." 2016. 15 Sep. 2016 <https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/>

[25] "How I Lost My $50,000 Twitter Username – Medium." 15 Sep. 2016 <https://medium.com/@N/how-i-lost-my-50-000-twitter-username-24eb09e026dd>

[26] "What I Learned When a Hacker Stole My Identity and Took Over My ..." 15 Sep. 2016 <http://www.inc.com/jeff-bercovici/i-got-hacked.html>

5. CONCLUSIONS

This work demonstrates the first survey of celebrity and corporate account takeover on social media. Our approach is data-driven, using over 2000 unique news articles to establish prevalence and cost. We also used this corpus to examine motivations and tactics of the attackers. We found that while traditional security measures such as strong passwords and 2FA eliminate most risk of account takeover, the value of social media accounts is high enough that attackers circumvent these precautions.

A mechanism which automatically scans content posted by the user, detects when an account might have been taken over, and locks the account if it is taken over would be a valuable tool for the social networks. Such a tool is possible using machine learning, and a working prototype has already been created.[33]

Best practices for avoiding a social account compromise:

- Enable two-factor authentications on all social media channels.
- Never give account or page credentials to anyone who emails or direct messages you, especially if they claim to be customer support from the network itself.
- Never click too-good-to-be-true offers or dubious news articles, as these often lead to malicious apps or malware exploits.
- Never download any unsolicited apps, especially ones that have permissions to post on your behalf.
- Update your passwords and security settings regularly.
- Avoid password reuse at all costs.
- Be wary that your connections may be hijacked as a springboard to socially engineer other people profiles. Validate any odd or out-of-character requests through third party communications.

[27] "Cell carrier was weakest link in hack of Google, Instagram accounts ..." 2014. 15 Sep. 2016 <http://arstechnica.com/security/2014/11/cell-carrier-was-weakest-link-in-hack-of-google-instagram-accounts/>

[28] "How anyone can hack your Instagram account – Naked Security." 2014. 15 Sep. 2016 <https://nakedsecurity.sophos.com/2014/07/30/how-anyone-can-hack-your-instagram-account/>

[29] "Apple's mobile market share sees big drop in May as Android skyrockets." 2016. 15 Sep. 2016 <http://bgr.com/2016/06/02/apples-mobile-market-share-sees-big-drop-in-may-as-android-skyrockets/>

[30] "Android's 6 biggest security flaws 2016 | Security | Techworld." 2016. 15 Sep. 2016 <http://www.techworld.com/security/androids-6-biggest-security-flaws-2016-3622116/>

[31] "Here's How Many People Are on Facebook, Instagram, Twitter and ..." 2016. 15 Sep. 2016 <http://www.adweek.com/socialtimes/heres-how-many-people-are-on-facebook-instagram-twitter-other-big-social-networks/637205>

[32] "How celebrity Twitter accounts were hacked, and ... - Naked Security." 2014. 15 Sep. 2016 <https://nakedsecurity.sophos.com/2009/01/07/celebrity-twitter-accounts-hacked/>

[33] "Text analysis of Trump's tweets confirms he ... - Variance Explained." 2016. 15 Sep. 2016 <http://varianceexplained.org/r/trump-tweets/>

HACKING A CORPORATE SOCIAL MEDIA PAGE

ZEROFOX RESEARCH

John Seymour – Senior Data Scientist

Publicly-facing social media accounts are high-value targets for attackers. Celebrities and organizations alike struggle to safeguard their profiles against compromise, leading to cybervandalism, hacktivism, and worse.

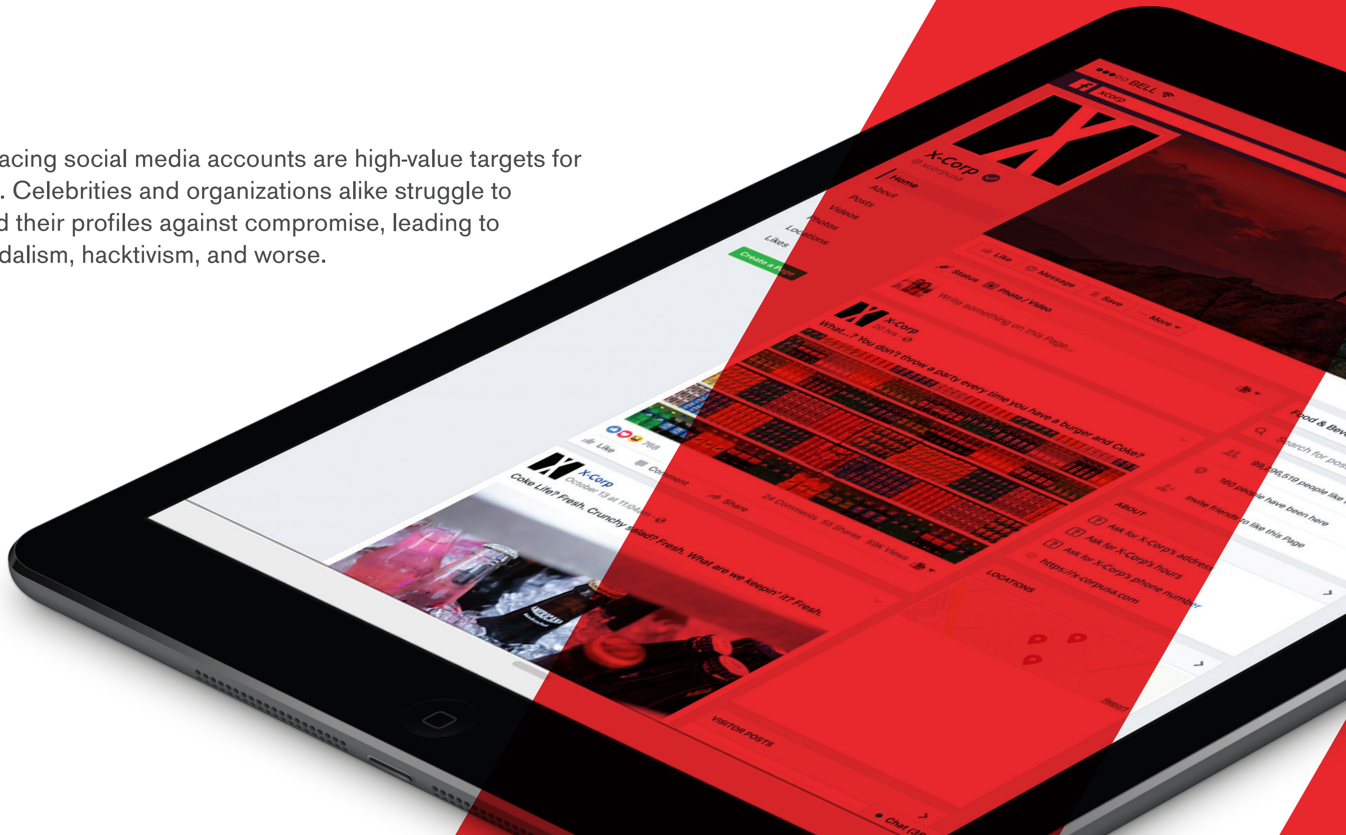

X-Corp
Home
About
Posts
Videos
Photos
Locations
Likes
Create a Page
What... ? You don't throw a party every time you have a burger and Coke?
Coke Life? Fresh. Crunchy salad? Fresh. What are we keepin' it? Fresh.
ABOUT
LOCATIONS
VISITOR POSTS

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY & FINDINGS

Social media account takeovers are an increasingly common occurrence, affecting the likes of politicians, celebrities, brands, other high-profile accounts and even Mark Zuckerberg, the father of the social media revolution. However, no study has been performed to analyze the prevalence, cost, motivations, and methodology of such attacks. Understanding these would be incredibly helpful for defense; for example, it could be used for effective distribution of preventative efforts. To that end, ZeroFOX Research has investigated successful account takeovers against celebrities and organizations in the past 4 years and aggregated pertinent details into this white paper. ZeroFOX also considered attacks to individual and small business accounts, which is detailed in the conclusion. These attacks are less costly than those covered in the body of the study, but occur much more frequently.

ZeroFOX Research collected over 2000 unique news articles, blog posts, social media help forum requests, and alerts from the ZeroFOX platform occurring between January 2012 and September 2016 regarding social media account takeovers of celebrities and major organizations. We triaged this dataset into 347 successful attacks against unique high-profile individuals or businesses and used this corpus to analyze the prevalence and cost of similar account takeovers. We then investigated the motivations of malicious actors to understand who is at risk. Finally, we looked into the tactics, techniques, and procedures surrounding account takeovers.

HIGHLIGHTS

- A detailed survey of 347 high-profile accounts compromised over the past 4.5 years
- A breakdown of hackers motivations, including money, political messages, and just “for the lulz”
- Common attacker tactics, techniques, & procedures and methods of breaking into a high-value account
- Best practices for securing your accounts on social media

2. PREVALENCE OF ACCOUNT TAKEOVERS

A social media profile is a valuable tool for corporations and celebrities to spread awareness, but it's also a broad, easily exploited, and often unregulated attack surface. If the page itself is compromised, the brand can become tarnished and trusting users can be enticed to click malicious links, directing to phishing pages, scams, or exploits. Two questions arise: how often do such attacks occur, and how can we quantify the damage done?

In order to answer these questions, we collected instances of successful account takeovers of high-profile individuals and businesses. We gathered public information regarding account takeovers, including news articles, blog posts, and social media help forum requests. We augmented this dataset with alerts from our product. The post-augmentation dataset consisted of over 2000 possible instances of successful account takeovers during the time period from January 2012 to September 2016.

However, this dataset included duplicate attacks as well as attacks that were caught before any changes to social media profiles could be made. We manually triaged the duplicates and unsuccessful attacks from the dataset. As we performed this inspection, we noticed that some targets were successfully taken over multiple times. If a target was successfully taken over more than once, we chose to include each time the target was successfully taken over as a separate instance.

After triage, 347 unique instances of successful account takeovers of celebrities and major organizations remained. A plot of these account takeovers over time, as well as an estimate for the total number of successful account takeovers by the end of 2016, is below. We noticed an upward trend over time, signifying that more accounts are successfully taken over each year. At the time of this writing (September 2016), there have already been 83 successful account takeovers against corporations and celebrities in 2016: a 12% increase over all of 2015.

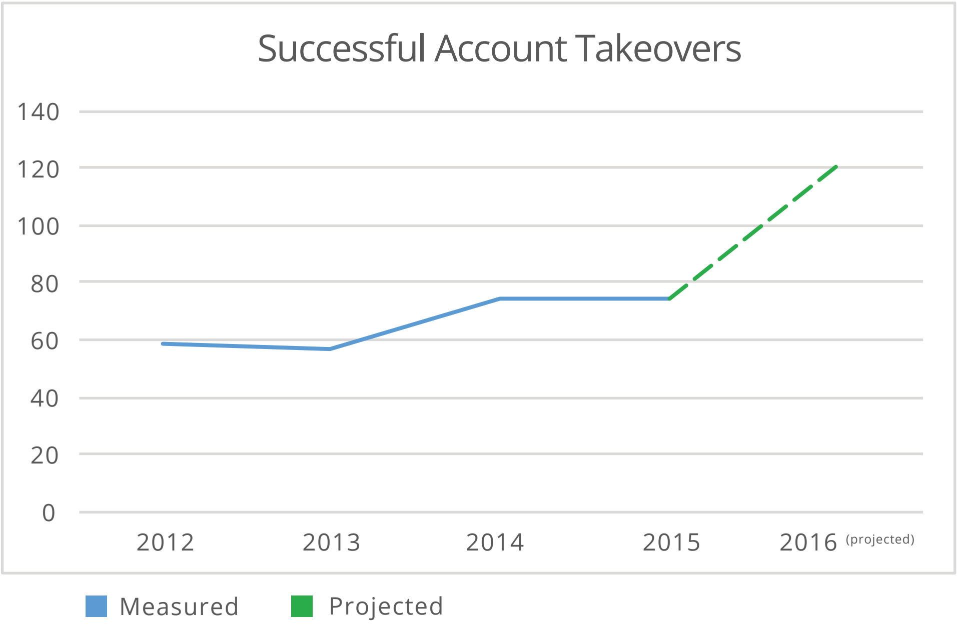
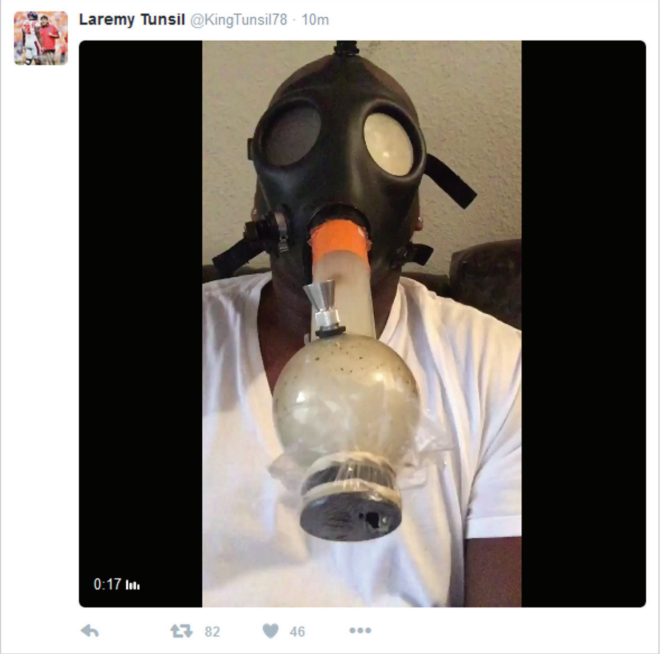


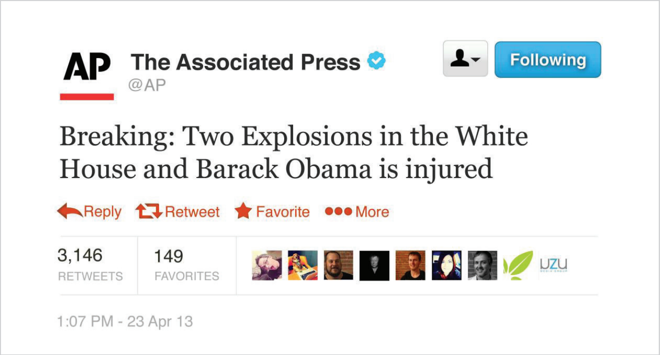
FIGURE 1.
Plot of Successful Account Takeovers over Time.

2.1 COST OF AN ACCOUNT TAKEOVER

Measuring the cost of breaches is more difficult; most instances of account takeovers do not reveal the full impact of the breach. We can, however, point to specific instances where the cost of the breach has been quantified. For example, the 2016 takeover of NFL rookie Laremy Tunsil's Twitter and Instagram accounts caused an estimated $21 million in damages.[1] In 2013, the Dow Jones industrial average dropped almost an entire percent because of fake tweets posted to the Twitter account of the Associated Press.[2] The attempted takeover of @jb, also in 2013, would have resulted in over $500,000 in damages and killed his startup had the attack been successful.[3] Clearly, these account takeovers have potentially huge financial impacts to the victims.



Laremy Tunsil @KingTunsil78 · 10m



The Associated Press
@AP

Breaking: Two Explosions in the White House and Barack Obama is injured

3,146 RETWEETS
149 FAVORITES

1:07 PM - 23 Apr 13

HACKTICOOL

The blog of a husband, dad, and co-founder of Droplr.

How I Almost Lost My $500,000 Twitter Username

[1] "Laremy Tunsil: Twitter hack could cost NFL rookie millions - CNN.com." 2016. 15 Sep. 2016 <http://edition.cnn.com/2016/04/29/sport/laremy-tunsil-ole-miss-nfl-draft-twitter-hack/

[2] "A Fake AP Tweet Sinks the Dow for an Instant - Bloomberg." 2013. 15 Sep. 2016 <http://www.bloomberg.com/news/articles/2013-04-23/a-fake-ap-tweet-sinks-the-dow-for-an-instant>

[3] "How I almost lost my $500000 Twitter user name @jb... - Ars Technica." 2014. 15 Sep. 2016 <http://arstechnica.com/security/2014/01/how-i-almost-lost-my-500000-twitter-username-jb-and-my-startup/>

3. MOTIVATION OF ATTACKERS

Fortunately, this corpus often includes details as to why the attackers took over the social media accounts of their victims. In some instances, the hackers themselves disclosed their motivations through posts on the compromised account or their own accounts. In others, we can discern their motivations based on the end payoff. In our data, we found four major motivators for celebrity or corporate social network takeovers:

MONEY:

Although technically against the Terms of Service, people are willing to pay real money for handles on social networks. Several transfers have even been endorsed by the social networks, notably the sale of @Israel for over $100,000 and the deal where @ CNNbrk rents out his username as part of his consulting practice.[4,5] However, this value also attracts thieves; the hacker behind the aforementioned attempt on @jb stated he was after the Twitter handle, worth $500,000. Naoki Hiroshima's Twitter account was taken over because it was worth over $50,000.[6,7] Even common accounts are traded on dark markets just like credit cards.[8]

STREET CRED:

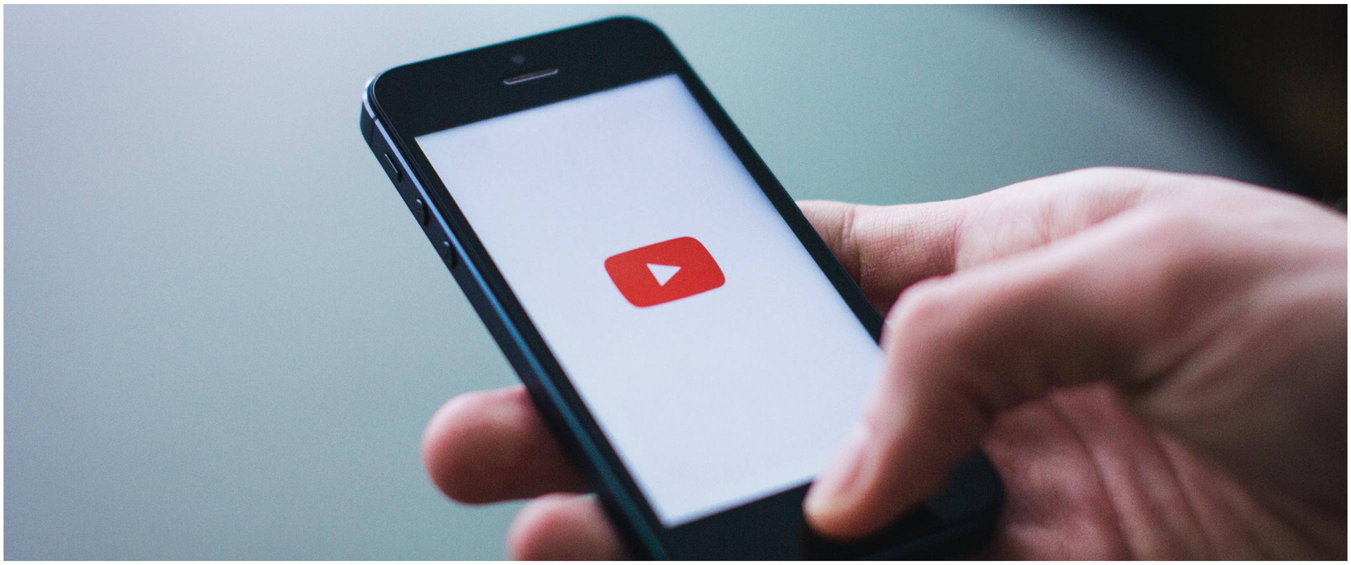
Some hackers post messages claiming responsibility for their hacks. There is risk involved in associating with an attack; it often helps law enforcement determine the perpetrator. Thus, we presume that this is a motivator for the attack in the first place. Notable examples of attacks motivated by street cred include the May 2016 Katy Perry takeover by sw4ylol and the June 2016 Zendesk takeover by NULLC0RE.[9,10]

DAMAGE:

Some takeovers occur simply because the perpetrator wants to cause damage. The hacker behind Mat Honan's epic hacking just wanted to take his three-character Twitter handle, "fuck shit up, and watch it burn."[11] "For the lulz" is a repeated phrase associated with Anonymous, who took over ISIS Twitter accounts and changed profile banners to rainbows.[12] The payoff for the August 2016 Twitter takeover of Cincinatti Zoo director, Thane Maynard seemed to be just posting memes.[13] Additionally, there's no clear reason why someone would take over Lea Michele's Twitter account to post fake news about her pregnancy.[14]

POLITICAL MESSAGES:

Some groups have the ultimate goal of spreading propaganda or threats. Such was the case when CyberCaliphate took over US Central Command's Twitter and YouTube accounts, pretending to post classified documents, or when the Syrian Cyber Army took over the Twitter accounts of 60 Minutes and 48 hours to post anti-Obama tweets.[15,16] The Syrian Cyber Army also claimed credit for the Associated Press hack which caused a dip in the Dow Jones industrial average.[17]



This information can be used both to understand who is at the most risk for account takeovers and to motivate potential solutions. If even common Twitter accounts are traded on darkweb markets, all accounts carry some amount of risk. However, accounts with rare handles, such as usernames with low character counts or usernames without underscores or numbers, are particularly likely to have takeover attempts because of the inherent monetary value of the account username. Accounts with many followers, especially political accounts, celebrities or news stations, also carry increased risk to takeover attempts, due to the value for disseminating propaganda and threats. Accounts perceived to be challenging to break into risk attempted takeovers for bragging rights.

[4] "Twitter user sells @Israel username for six-figure sum - The Guardian." 2016. 15 Sep. 2016 <https://www.theguardian.com/technology/2010/sep/14/twitter-user-sells-israel-username>

[5] "Confirmed: CNN Acquires CNNBrk Twitter Account ... - TechCrunch." 2016. 15 Sep. 2016 <https://techcrunch.com/2009/04/15/confirmed-cnn-acquires-cnnbrk-twitter-account/>

[6] "How I almost lost my $500000 Twitter user name @jb... - Ars Technica." 2014. 15 Sep. 2016 <http://arstechnica.com/security/2014/01/how-i-almost-lost-my-500000-twitter-username-jb-and-my-startup/>

[7] "How I Lost My $50,000 Twitter Username – Medium." 15 Sep. 2016 <https://medium.com/@N/how-i-lost-my-50-000-twitter-username-24eb09e026dd>

[8] "Ablon, Lillian, Martin C Libicki, and Andrea A Golay. Markets for cybercrime tools and stolen data: Hackers' bazaar. Rand Corporation, 2014.

[9] "Hackers Hijacked the World's Most Followed Twitter Account - Fortune." 2016. 15 Sep. 2016 <http://fortune.com/2016/05/31/hackers-hijacked-the-worlds-most-followed-twitter-account/>

[10] "Zendesk chief's Twitter account hacked - BBC News." 2016. 15 Sep. 2016 <http://www.bbc.com/news/technology-36480997>

[11] "How Apple and Amazon Security Flaws Led to My Epic Hacking | WIRED." 2016. 15 Sep. 2016 <https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/>

[12] "Anonymous hacks pro-ISIS Twitter accounts, fills them with gay pride ..." 2016. 15 Sep. 2016 <http://www.cbsnews.com/news/anonymous-hacks-pro-isis-twitter-accounts-fills-them-with-gay-pride/>

[13] "Cincinnati Zoo Director Thane Maynard's Twitter account hacked - Story." 2016. 15 Sep. 2016 <http://www.wcpo.com/news/local-news/hamilton-county/cincinnati/cincinnati-zoo-director-thane-maynards-twitter-account-hacked>

[14] "Lea Michele Not Pregnant: Glee Star Twitter Hacked After Chris Colfer ..." 2014. 15 Sep. 2016 <http://www.usmagazine.com/celebrity-news/news/lea-michele-not-pregnant-glee-star-twitter-hacked-after-chris-colfer-201447>

[15] "CENTCOM Twitter account hacked, suspended - CNNPolitics.com." 2015. 15 Sep. 2016 <http://www.cnn.com/2015/01/12/politics/centcom-twitter-hacked-suspended/>

[16] "'60 Minutes' and '48 Hours' Twitter Accounts Hacked, Sent Anti-Obama ..." 2016. 15 Sep. 2016 <http://www.newsbusters.org/blogs/nb/noel-sheppard/2013/04/21/60-minutes-and-48-hours-twitter-accounts-hacked-sent-anti-obama>

[17] "Hackers compromise AP Twitter account - Associated Press." 2016. 15 Sep. 2016 <http://bigstory.ap.org/article/hackers-compromise-ap-twitter-account>

4. ATTACKER TACTICS, TECHNIQUES, AND PROCEDURES

Unsurprisingly, most account takeovers occur because of poor password hygiene. For example, LinkedIn's database was leaked in 2012, and Twitter's accounts database was leaked in 2013.[18,19] Although the passwords were hashed and salted in both cases, password reuse has led to some celebrity accounts being taken over, notably the Twitter and Pinterest takeovers of Mark Zuckerberg.[20]

Corporations tend to have additional issues with password hygiene, for two reasons. First, some social media teams use a shared password, which may be shared insecurely or weak enough for teams to memorize.[21] Second, many corporations loan or share social media accounts with 3rd party marketing agencies or for PR events.[22,23] Properly using password managers to share passwords, having unique passwords for each website visited, and using 2 Factor Authentication (2FA) thwarts many account takeover attempts.

> RATHER THAN ATTACKING SOCIAL MEDIA ACCOUNTS DIRECTLY, HACKERS HAVE BEEN OBSERVED SOCIAL ENGINEERING APPLE, AMAZON, PAYPAL, AND GODADDY IN ORDER TO GAIN ACCESS TO ACCOUNTS.

For taking over more valuable accounts, such as those of celebrities and corporations, a common tactic is social engineering a third party. In this method, the main goal is to either change the account recovery email or extort the user into giving up their account. Rather than attacking social media accounts directly, hackers have been observed social engineering Apple, Amazon, Paypal, and Godaddy in order to gain access to accounts.[24,25] Hackers have also abused policies in email services like Hotmail to obtain account credentials, and socially engineered cell providers to get around 2FA.[26,27] Issues with the SMS implementation of 2FA give users a false perception of security.[28] Even if someone takes appropriate precautions, a third party can allow a hacker access to the social media account settings.

Finally, vulnerabilities within the social media applications themselves can give account access to attackers. For example, in 2014, a vulnerability in Instagram allowed for anyone on the same network to sniff Instagram session tokens.[29] This means that anyone logged in on public wifi could have their accounts taken over, at least until until the vulnerability was patched. Moreover, 70.85% of the smartphone market consists of Android phones, and they're known to have vulnerabilities too.[30,31] Since most social networks are primarily mobile-oriented, it's another attack vector.[32] Finally, nothing is stopping employees at the social networks from being targeted themselves; celebrities were hacked in 2009 because of a social media employee's weak password.[33]

[18] "Zendesk chief's Twitter account hacked - BBC News." 2016. 15 Sep. 2016 <http://www.bbc.com/news/technology-36480997>

[19] "Questions and answers about the Twitter hack – Naked Security." 2014. 15 Sep. 2016 <https://nakedsecurity.sophos.com/2013/02/02/twitter-hack-questions/>

[20] "Mark Zuckerberg's password was 'dadada'. What hope do the rest of ..." 2016. 15 Sep. 2016 <http://www.telegraph.co.uk/technology/2016/06/06/mark-zuckerbergs-password-was-dadada-what-hope-do-the-rest-of-us/>

[21] "How do companies share their social media passwords with marketing ..." 2016. 15 Sep. 2016 <https://www.quora.com/How-do-companies-share-their-social-media-passwords-with-marketing-agencies-and-freelancers>

[22] "In Which A Twitter Account Takeover Goes Very, Very Awry - Adweek." 2015. 15 Sep. 2016 <http://www.adweek.com/socialtimes/la-kings-twitter-account/484799>

[23] "Comedian Rob Delaney Takes Over @MLB Twitter Account, Hilarity ..." 2015. 15 Sep. 2016 <http://www.adweek.com/socialtimes/rob-delaney-mlb/483318>

[24] "How Apple and Amazon Security Flaws Led to My Epic Hacking | WIRED." 2016. 15 Sep. 2016 <https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/>

[25] "How I Lost My $50,000 Twitter Username – Medium." 15 Sep. 2016 <https://medium.com/@N/how-i-lost-my-50-000-twitter-username-24eb09e026dd>

[26] "What I Learned When a Hacker Stole My Identity and Took Over My ..." 15 Sep. 2016 <http://www.inc.com/jeff-bercovici/i-got-hacked.html>

5. CONCLUSION

This work demonstrates the first survey of celebrity and corporate account takeover on social media. Our approach is data-driven, using over 2000 unique news articles to establish prevalence and cost. We also used this corpus to examine motivations and tactics of the attackers. We found that while traditional security measures such as strong passwords and 2FA eliminate most risk of account takeover, the value of social media accounts is high enough that attackers circumvent these precautions.

Although our focus in this paper has been high-profile account compromises (which presents the greatest risk for many major brands and celebrities), assessing the true scope of the account takeover problem, including personal accounts and small business profiles, requires a different methodology.

Surveys have been conducted for estimating the total number of account takeovers. Norton reports that 1 out of 6 users reported having an account or accounts hacked.[34] However, a more recent University of Phoenix report places that number much higher, reporting 2 out of 3 of all U.S. adults having accounts hacked. [35]

[27] "Cell carrier was weakest link in hack of Google, Instagram accounts ..." 2014. 15 Sep. 2016 <http://arstechnica.com/security/2014/11/cell-carrier-was-weakest-link-in-hack-of-google-instagram-accounts/>

[28] "So Hey You Should Stop Using Texts for Two-Factor Authentication." 2016. 15 Sep. 2016 <https://www.wired.com/2016/06/hey-stop-using-texts-two-factor-authentication/>

[29] "How anyone can hack your Instagram account – Naked Security." 2014. 15 Sep. 2016 <https://nakedsecurity.sophos.com/2014/07/30/how-anyone-can-hack-your-instagram-account/>

[30] "Apple's mobile market share sees big drop in May as Android skyrockets." 2016. 15 Sep. 2016 <http://bgr.com/2016/06/02/apples-mobile-market-share-sees-big-drop-in-may-as-android-skyrockets/>

[31] "Android's 6 biggest security flaws 2016 | Security | Techworld." 2016. 15 Sep. 2016 <http://www.techworld.com/security/androids-6-biggest-security-flaws-2016-3622116/>

[32] "Here's How Many People Are on Facebook, Instagram, Twitter and ..." 2016. 15 Sep. 2016 <http://www.adweek.com/socialtimes/heres-how-many-people-are-on-facebook-instagram-twitter-other-big-social-networks/637205>

[33] "How celebrity Twitter accounts were hacked, and ... - Naked Security." 2014. 15 Sep. 2016 <https://nakedsecurity.sophos.com/2009/01/07/celebrity-twitter-accounts-hacked/>

[34] "2012 Norton Cybercrime Report." 2012. 15 Sep. 2016 <http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf>

[35] "Nearly Two-Thirds of U.S. Adults with Social Media Accounts Say..." 2016. 15 Sep. 2016 <http://www.businesswire.com/news/home/20160427006133/en/Two-Thirds-U.S.-Adults-Social-Media-Accounts-Hacked>

[36] "Facebook hack attacks strike 600,000 times per day, security firm reports." 2011. 15 Sep. 2016 <http://www.nydailynews.com/news/national/facebook-hack-attacks-strike-600k-times-day-article-1.968681>

[37] "Facebook Sees 600,000 Compromised Logins Per Day." 2011. 15 Sep. 2016 <https://techcrunch.com/2011/10/28/facebook-sees-600000-comprised-logins-per-day/>

[38] "Big Brother 2.0: 160,000 Facebook pages are hacked a day." 2015. 15 Sep. 2016 <http://nypost.com/2015/03/01/big-brother-2-0-160000-facebook-pages-are-hacked-a-day/>

[39] "Text analysis of Trump's tweets confirms he ... - Variance Explained." 2016. 15 Sep. 2016 <http://varianceexplained.org/r/trump-tweets/>

Also useful are the social network reports on compromised logins. In 2011, Facebook reported that .06% of all log-ins were “compromised.”[36] Their language leaves some room for interpretation, but TechCrunch extrapolated that an astounding 600,000 logins per day are compromised.[37] Although this may not discount multiple compromised logins on the same accounts, and while security measures on the networks themselves have improved since, the number of social media account owners has also significantly increased, resulting in larger attack surface. According to a more recent article comes from the New York Post in 2015, 160,000 Facebook accounts are compromised per day.[38] Although estimates of account takeovers vary, one thing is clear: it happens all the time.

ALTHOUGH ESTIMATES OF ACCOUNT TAKEOVERS VARY, ONE THING IS CLEAR:
IT HAPPENS ALL THE TIME.

- For high-value and average social media users alike, we recommend the following best practices to lessen the risk of account takeover:
- Enable two-factor authentications on all social media channels.
- Never give account or page credentials to anyone who emails or direct messages you, especially if they claim to be customer support from the network itself.
- Never click too-good-to-be-true offers or dubious news articles, as these often lead to malicious apps or malware exploits.
- Never download any unsolicited apps, especially ones that have permissions to post on your behalf.
- Update your passwords and security settings regularly.
- Avoid password reuse at all costs.
- Be wary that your connections may be hijacked as a springboard to socially engineer other people profiles. Validate any odd or out-of-character requests through third party communications.

However, there are cases where these security practices are circumvented. In such cases, a mechanism which automatically scans content posted by the user, detects when an account mayight have been taken over, and locks the account if it is taken over would be a valuable tool for the social networks. Such a tool is possible using machine learning, and a working prototype has already been created.[39]