The Business of Disinformation: A Taxonomy

Fake news is more than a political battlecry

Creation Publication Circulation
Executive Summary

Since the 2016 U.S. presidential election, the term “fake news” has integrated itself firmly into our daily vernacular. However, fake news is used very broadly to describe: disinformation, propaganda, hoaxes, satire and parody, inaccuracies in journalism, and partisanship.

Disinformation campaigns are not limited to the geopolitical realm – its use is far more pervasive. The sheer availability of tools means that barriers to entry are lower than ever. This extends beyond geopolitical to financial interests that affect businesses and consumers. This paper presents an overview of these different motivations and tools actors can turn to.

In Digital Shadows’ Disinformation Campaign Taxonomy, we lay out the stages used in disinformation campaigns. In doing so, it is possible to develop ways to potentially disrupt these efforts and create greater friction for actors involved.

Table of Contents

Executive Summary .......................................................... 2
From the Popish Plot to the Polish Cyber Army ......................... 3
A Taxonomy of Disinformation ................................................ 4
Creation .................................................................................. 5
Publication ............................................................................... 7
Circulation ............................................................................... 9
Combatting Disinformation .................................................... 11
The Disinformation Age: Forecasting ....................................... 13
End Notes ............................................................................... 14
In the 1670s, England was gripped by news that there was a Catholic conspiracy to assassinate King Charles II, known as the Popish Plot. In reality, this was a fake story concocted by a priest called Titus Oates, who disseminated fake manuscripts that played on the strong anti-Catholic sentiment among the largely Protestant English population. Although Oates was later convicted of perjury, his disinformation campaign led to the execution of at least 22 men. The hysteria also meant that politicians tried to exclude Charles’ brother, James, from assuming the throne because he was a Roman Catholic.

Since the 2016 U.S. presidential election, the term “fake news” has become part of our daily vernacular. Despite its prevalence, its meaning is often confused or misunderstood. Fake news refers to many things: disinformation, propaganda, hoaxes, satire and parody, inaccuracies in journalism, and partisanship. This whitepaper focuses specifically on disinformation campaigns - that is, campaigns that deliberately spread false information in order to deceive their target or audience.

Technological developments have acted as a force multiplier for disinformation activity, reducing the barriers to entry for disinformation peddlers with a variety of motives and capabilities. We have developed Digital Shadows’ Disinformation Campaign Taxonomy for a typical disinformation campaign based on a three-stage attack chain (creation, publication, and circulation), which includes an overview of the methods, tactics and tools associated with running such an operation. By using this model, we can see that there are different stages that defenders can target to help disrupt disinformation campaigns in their infancy. Early identification of these campaigns is critical to increase the likelihood of successful disruption.

From the Popish Plot to the Polish Cyber Army

Figure 1: A timeline of recent disinformation campaigns
It’s not (only) a nation’s favorite pastime

“Our friends in Moscow call it ‘dezinformatsiya’. Our enemies in America call it ‘active measures,’ and I, dear friends, call it ‘my favorite pastime.’”

Col. Rolf Wagenbreth, Director of Department X, East German foreign intelligence

Although disinformation has been closely associated with the activities of nation-states and intelligence services, these campaigns are not always performed for political, geostrategic or military purposes. Over the past two years, we have reported on disinformation attacks that targeted organizations and individuals in a variety of industries, for a range of motives. Ideological or politically-motivated attacks intended to discredit a target were the most common; however, in some cases attackers were driven by factors such as prestige, exposure or even financial gain.

Disinformation campaigns can take many forms; however, most of the examples we’ve seen have three distinct stages: 1) Creation, 2) Publication and 3) Circulation. For each stage, there are countless online tools, software and platforms to allow attackers to create credible and effective disinformation campaigns. However, there are also measures organizations can take to help combat the spread of disinformation.
An attacker looking to spread disinformation will need to create content that they can then distribute widely. Here there are two broad methods: 1) either create fake content that at first glance looks identical to that produced by legitimate news sources or corporate organizations, or 2) compromise a real company and control one of their communication channels by taking over their social media platforms, public websites or modifying company documents.

Site impersonation
Sites such as CloneZone can be used to impersonate genuine news organizations. Though not inherently malicious, the easy-to-use and intuitive software allows users to change the html content and images to create realistic clone pages. There are also many free applications and websites that allow you to create false news headlines and captions, impersonating the style of mainstream media outlets.

Modified Documents
Fraudulent and modified documents have long been a common feature of disinformation campaigns. Fraudulent documents can be used to impersonate legitimate sources which are subsequently sent to news outlets.

Modifying documents can have a similar effect. This can either be created from scratch, or by modifying a legitimate document. This was evident on the eve of the French elections, when files from the Macron leaks appeared to have been altered before being released.
Account Takeover
Attackers will look to exploit poor password security practices, use credentials exposed in data breaches, or phishing campaigns to compromise accounts. From this beachhead into an organization, they can pivot and change content on a particular organization’s website, steal, and modify potentially sensitive documents or take over social media channels to make false claims. We know that most people re-use their usernames and passwords across multiple accounts, and so access to one can give access to many associated accounts.

Digital Shadows analyzed the exposure of the 40 largest global news websites. This was done by checking for their email domains across thousands of breaches that have occurred since 2011. This includes credentials dumped on paste sites, but also larger data files shared online and on criminal forums. For the top 40 global news websites, Digital Shadows detected over 200,000 usernames exposed in various breaches.

Domain Spoofing
By registering domain names that look almost identical to genuine domains, attackers can socially engineer visitors into thinking their content is legitimate. During the French presidential election, a false article alleging that Saudi Arabia was financing Emmanuel Macron was published via a domain spoof of Belgian newspaper Le Soir. A domain spoof is a tactic whereby an attacker registers a domain that closely resembles the target organization and is leveraged for social engineering purposes. The article claimed to be a dispatch from Agence France-Presse, appearing on the domain lesoir.info, a spoof of the legitimate lesoir.be. Members of the Front National, as shown below, subsequently retweeted the article thinking that it was real.

Given that all media organizations don’t have the security maturity and capabilities of the major outlets, attackers often target local news services and smaller media organizations with less robust security.

In order to assess the scale of the situation, Digital Shadows analyzed the top 40 global news websites, checking over 85,000 possible variations on their domain (for example, an “m” may have changed to an “rn”. In doing so, we discovered 2,858 live spoof domains. Of these, 52 were hosting spoof content of some sort. This mirrors experiences of Digital Shadows’ media customers who were alerted to an average of 961 malicious domains over the past two years.

Total number of exposed credentials for the 40 largest global news sites: 206,404

Attackers can use these credentials to perform account takeovers.

Total number of verified impersonation domains for the 40 largest global news sites: 52

Verified impersonation sites could be used for social engineering and creating disinformation.
Once content has been created, an attacker will need to publish their disinformation online. Just like a legitimate campaign, to increase its reach, adversaries will often opt for multiple publication channels and platforms.

### Social media post

Social media is an easy to use medium that allows people to communicate with each other instantaneously. However, the power and ease of using this technology means it can also be maliciously co-opted to spread unverified, dubious or outright false reporting.

We discovered the following “Pump and Dump” service called TheInsider advertised on the dark web, which uses social media posts to inflate share prices. This site claims to work by gradually purchasing major shares in altcoin (cryptocurrencies other than Bitcoin) and drumming up interest in the coin through posts on social media. TheInsider then trades these coins between its multiple accounts, driving the price up, before selling these to unsuspecting traders on currency exchanges looking to buy while share prices are still rising.

Digital Shadows has monitored this site since the beginning of October, when the site claimed to have raised 8.23 bitcoin (BTC), less than a quarter of the 40 BTC target. At the time of writing, the site claims to have surpassed the original goal and has 45.71 BTC invested (approximately $326,000). However, there is not yet evidence that a Pump and Dump scheme has yet taken place, and the possibility remains that it is a scam.

These share manipulation techniques are not new: Martin Shkreli, a former pharmaceuticals company CEO, is said to have used blogging platforms and social media to manipulate share price. More recently, the activities of the online alias “Art Doyle” has been calling for share prices to drop amid rumors. Given the availability and wide range of inexpensive tools, you can see how easy it is to potentially influence perceptions of organizations online for financial gain.

---

Digital Shadows has monitored this site since the beginning of October, when the site claimed to have raised 8.23 bitcoin (BTC), less than a quarter of the 40 BTC target. At the time of writing, the site claims to have surpassed the original goal and has 45.71 BTC invested (approximately $326,000). However, there is not yet evidence that a Pump and Dump scheme has yet taken place, and the possibility remains that it is a scam.

These share manipulation techniques are not new: Martin Shkreli, a former pharmaceuticals company CEO, is said to have used blogging platforms and social media to manipulate share price. More recently, the activities of the online alias “Art Doyle” has been calling for share prices to drop amid rumors. Given the availability and wide range of inexpensive tools, you can see how easy it is to potentially influence perceptions of organizations online for financial gain.

---

We discovered the following “Pump and Dump” service called TheInsider advertised on the dark web, which uses social media posts to inflate share prices. This site claims to work by gradually purchasing major shares in altcoin (cryptocurrencies other than Bitcoin) and drumming up interest in the coin through posts on social media. TheInsider then trades these coins between its multiple accounts, driving the price up, before selling these to unsuspecting traders on currency exchanges looking to buy while share prices are still rising.

Digital Shadows has monitored this site since the beginning of October, when the site claimed to have raised 8.23 bitcoin (BTC), less than a quarter of the 40 BTC target. At the time of writing, the site claims to have surpassed the original goal and has 45.71 BTC invested (approximately $326,000). However, there is not yet evidence that a Pump and Dump scheme has yet taken place, and the possibility remains that it is a scam.

These share manipulation techniques are not new: Martin Shkreli, a former pharmaceuticals company CEO, is said to have used blogging platforms and social media to manipulate share price. More recently, the activities of the online alias “Art Doyle” has been calling for share prices to drop amid rumors. Given the availability and wide range of inexpensive tools, you can see how easy it is to potentially influence perceptions of organizations online for financial gain.

---

Figure 6: A screenshot of the dark web site “TheInsider”

Figure 7: The Twitter profile of Art Doyle
Over the ensuing week, Digital Shadows detected almost 15,000 nearly identical tweets posted by approximately 12,000 Twitter accounts, featuring links to tweets about the Anonymous Poland breach. The account name on many of the Twitter pages was set to “ClintonCorruption” and they featured identical profile pictures. While it is difficult to assess its impact on the outcome of the U.S. election, we believe these accounts were controlled by Anonymous Poland and used as part of an operation to negatively affect Clinton’s chances in the presidential election.

Forum Posts
Like social media, online forums are fertile ground for false stories to take root and be shared by users. The 2016 “Pizzagate” conspiracy theory that emerged near the end of the U.S. election cycle began on forums and messageboards such as 4chan and Godlike Productions. These allegations were then spread widely on social media, before appearing on better-known sites such as Reddit.
Circulation

Like any good news story, content will be shared, liked, reposted and distributed across many different platforms and channels. The more widely a piece of disinformation can be spread, the better the chances of it capturing the public imagination and achieving its objective - whether that is to discredit an opponent, sow discord or to generate profit.

Likes and Retweets

To add legitimacy to their claims and increase readership, attackers will rely on other users and platforms sharing their fake content. This can sometimes be as innocuous as unsuspecting users naively redistributing disinformation to their social networks. In some cases even real news organizations have been duped into including disinformation into their syndication. However, attackers can force the issue by buying social media followers or using tools that automatically share and repost content across a variety of sites.

TweetAttacksPro allows users to download software which controls the activities of social media bots. The software is available for a trial period at just $7. In contrast to the software offered by TweetAttacksPro, ismm.su offers more of a managed service. Users of ismm.su can buy anything from 100 to 100,000 Twitter likes for $1.50 per 1,000 likes, simply by paying and inputting their pages or posts that require social media attention. Furthermore, this site goes beyond just Twitter and Facebook; the site offers services on Shazam, Classmates, Vkontakte, YouTube, and Instagram.

Mentions of these sites across criminal forums can give an indication of their popularity. Ismm.su registered the most mentions (74%), but there are plenty of others: topsoc.ru, soc-proof.su, smmtarget.com, 5ac.ru, smmpanele.ru, smosmm.ru, asset.box, and professor7717.ru. These mentions have also been growing year on year, increasing from 418 in 2015 to 1,381 so far in 2017.
Advertisements
Tools such as BotMasterLabs and ZennoStore claim to promote content across over hundreds of thousands of platforms, including forums, blogs, and bulletin boards. These tools work by controlling large numbers of bots; armies of computers that the individuals control and can configure the bots to post on specific types of forums on different topics. BotMasterLabs, for example, claims to have the ability to post on over 400,000 forums. To further increase the chances of success, these tools have in-built features that bypass captcha methods, which were initially brought in to prevent bots and automated scripts from posting advertisements indiscriminately across these platforms. The business edition of the Botmaster Labs XRumer application can be purchased for only $400.

These techniques are even allegedly used at a nation state level. Google reportedly discovered that Russian operatives spent roughly $100,000 USD on Google ads, Gmail, and YouTube advertising, while St Petersburg content farms used Twitter and Facebook platforms to purchase ads as part of a broad online disinformation effort during the U.S. election. In total, it is estimated the 126 million Facebook users were reached in the U.S. during the election period.\(^7\)

Reviews
But it’s not just for geopolitical goals, advertising also takes place for reviews of goods on ecommerce platforms. In October 2017, the website buyamzreviews[.]com was established. The site describes itself as “a small team and we provide Amazon Ranking, Reviews, Votes, listing optimization, selling promotions”. Pricing ranges from $5 for an unverified review, $10 for a verified review, to a $500 monthly retainer. This is already a challenge for ecommerce sites, but criminals will continue to develop innovative methods to bypass controls.
Combating Disinformation

Combating disinformation is difficult, but it is not a lost cause. There are a variety of measures organizations, distributors, and even individuals can take to help prevent the spread and consumption of disinformation. By using Digital Shadows’ Disinformation Campaign Taxonomy, it’s clear that disinformation campaigns tend to be multi-stage operations. This allows defenders to address campaigns at various stages of their development. However, the earlier in the chain these campaigns can be impacted, the better, especially since once they reach the circulation stage it becomes more a matter of damage limitation and responding to the narrative.

1. Creation
   - Site Impersonation
     When websites or social media accounts attempt to impersonate a company or brand, organizations should follow appropriate takedown measures. However, there are legal issues linked to takedown requests. For example, Digital Millennium Copyright Act (DMCA) requests cannot always be issued because they relate to copyright matters, rather than trademark issues. Registered trademarks of your brand (or other assets) are needed for trademark infringement requests. In the case of CloneZone, for example, it is not possible to spoof sites that have launched a cease and desist order. In these cases, the news sites are blacklisted.

   - Modified Documents
     Digital Shadows has detected cases where threat actors modified legitimate documents and leaked them as part of disinformation campaigns. Threat actors look to maintain markings and headers that make their modified or fabricated documents appear genuine; therefore, organizations should ensure their documents are appropriately marked and data loss prevention software is put in place.

   - Account Takeover
     Many successful account compromises result from poor password security - such as inadequate password and username combinations or reusing passwords across multiple accounts. Attackers’ lives are made even easier given the public availability of passwords from historic data breaches such as LinkedIn, MySpace, and Yahoo.

     Therefore, organizations should enforce complex passwords and discourage password reuse. Organizations should also deploy multifactor authentication and take advantage of Web Application Firewalls to prevent account takeover tools like SentryMBA. These measures should be applied to corporate user accounts as well as official social media accounts used across the organization. Sites like haveibeenpwned[.]com can help organizations to detect when this occurs.

2. Publication
   - Social Media Posts
   - Social Media Bots
   - Forum Posts
   - Likes and Retweets
   - Reviews

3. Circulation
   - Advertisements
   - Original Documents
Combating Disinformation

Creation - Domain Spoofing
With more than 1,500 registered top-level domains, and even more possible misspelled domains, simply buying up digital real estate is no longer feasible. This would be extremely expensive even for one brand or service name; it would also be a very resource intensive process and would likely still not protect an organization from all domain spoofing attempts. As an alternative, organizations should proactively monitor for the registration of malicious domains and have a defined process of dealing with infringements when they occur. An agile and scalable takedown capability is critical for combating domain spoofing.

Publication - Social Media Posts and Social Media Bots
Organizations should be monitoring social media for mentions of their brand. In addition, organizations should attempt to detect social media bots. Though it’s not always immediately obvious, there are often clues that can help determine whether an account is operated by a bot. These include looking at the age of the account, the content being posted, and the number of friends and followers - very new accounts performing lots of activity in a very short period of time should be treated with suspicion. Users can report accounts on Twitter with the “Report” button. Facebook also allows users to report “fake accounts” at the click of a button.

Publication - Forum Posts
Organizations can search for mentions of their brand or staff across forums, which could be instances of malicious actors spreading disinformation. This is particularly important for public organizations, whose share price can be manipulated. Organizations can use Google Alerts to monitor public forums for these mentions, or look to build their own scrapers with open source tools, such as Scrapy that are more robust than Google Alerts.

Circulation - Advertisements
As the recent investigations into the U.S. election have demonstrated, it is not easy to identify fake advertisements on social media. While social media companies have the responsibility to detect and remove these advertisements, much of the solution will be in user awareness. Social media users that are more discerning about the providence of information can cause a reduction in the influence of these advertisements.

Circulation - Likes and Retweets
By actively monitoring social media channels and using activity based intelligence (ABI), you can spot burgeoning news stories and events. This can be done through using social media monitoring software to track hashtags and actors. You can monitor trending activity as it relates to your digital footprint and potentially identify disinformation activity.

This can also be used to spot intellectual property, technical information or other sensitive data being shared and circulated online, as well as providing guidance to help immediately administer takedowns.

Circulation - Reviews
It is important to note that disinformation also extends to financial motivations. As disinformation peddlers become more advanced, fake reviews can be difficult to spot. However, there is help out there. Consumers can take advantage of free sites like Fakespot.com or ReviewMeta.com to better inform them about the likelihood of a specific product having fake reviews.
The Disinformation Age: Forecasting

By using Digital Shadows’ Disinformation Campaign Taxonomy to gain a greater understanding of the tools and tactics used, disinformation can be identified earlier and greater friction can be created for those waging disinformation campaigns.

Disinformation in 2018

There is a myriad of drivers that will affect how disinformation campaigns evolve in the upcoming years. Based on the drivers and assumptions shown below, it’s almost certain that disinformation will continue; the geopolitical situation shows no signs of easing, and there is plenty of sociocultural unease to exploit. While there will be continued efforts to remove suspicious content from social media sites, the low barriers to entry and innovation of threat actors will lead to an increase in disinformation. Moreover, this is not just a risk for political parties in 2018; disinformation affects businesses and individuals too.

Seven Key Drivers for the Future of Disinformation

1. Geopolitical situation. Although this is not the only motivation behind disinformation, the prevalence is closely tied to the geopolitical landscape. Geopolitical friction will inevitably contribute to the creation, publication, and circulation of disinformation.

2. Sociocultural conflict and violence. Russian disinformation campaigns in the U.S. have often capitalized on preexisting sociocultural conflict. This was evident in the creation of the “Blacktivist” Facebook group. The greater the existing social divides, the more opportunities exist for those waging disinformation campaigns.

3. Diligence of social media platforms in removing disinformation. While social media platforms have been criticized for the existence of fake accounts and their acceptance of advertisements, there has been an increased effort to combat this problem. The success of the 2017 German Election in raising public awareness and creating fact-checking services is testimony to this.

4. Organizational awareness. Organizations that are involved in the creation and circulation of news are developing awareness of these issues. Should such organizations take a more proactive approach to monitoring for spoofs and preventing account takeovers, this will help to create more friction for adversaries.

5. Innovation. As this paper has demonstrated, the barriers to entry for disinformation campaigns are remarkably low. This is an area that will continue to innovate and the emphasis on artificial intelligence may pave the way for increasingly convincing forum posts and reviews posted by bots.

6. Distrust of mainstream media. There has been a notable decline in the trust of the mainstream media over the past few years. Over two thirds of Americans now suspect the mainstream media publish fake news. As an alternative, users turn to new sources of information, such as social media, to stay informed. As people tend to seek out information that will confirm their preexisting beliefs or biases, social media facilitates the creation of echo chambers.

Assumptions

1. There will be no significant easing of relations between Russian and the West. Other states (and their proxies) will also look to incorporate information warfare into their overall strategic approach.

2. Consumer demand for social media platforms will favor privacy over censorship. Those platforms that excessively censor information will run the risk of losing users.

3. Organizations will remain ignorant of the financial motivations of disinformation, and how it impacts them. So long as disinformation is seen as not having an impact of finances, businesses will not take the risk seriously. This has a significant impact on the countermeasures.

4. Malicious individuals and groups will always seek ways to subvert mitigation measures and exploit new technology. Social media bots and technology will continue to develop and become more innovative.
End Notes

5. https://www.digitalshadows.com/blog-and-research/anonymous-poland-not-your-typical-hacktivist-group/