FAKE NEWS, INC.

Andrew Brandt
SophosLabs, USA

andrew.brandt@sophos.com

ABSTRACT

An anonymous tip from an Internet user late in 2017 pointed me to what looked, at first glance, like the website of what claimed to be a small-town newspaper based in Illinois, USA, but under scrutiny, things didn't really add up. The newspaper's own page about itself listed a real street address, but the town in which the newspaper was supposed to be located was hundreds of miles from the small town whose name graced the paper's masthead, on a street and at a numbered address that didn't exist in either town. That alone got me curious and I began digging for more information, none of which made any sense.

The site's web hosting also raised questions: for what should have been a small, local independent paper, the site was hosted on an IP address located on the other side of the Atlantic. While the domain registration was private, there were hundreds of other domains hosted on the same IP address range that all appeared to be named for small towns across the United States, Canada and Europe. The sites shared certain characteristics, but none of the information provided by the sites about themselves withstood even casual scrutiny – all of them used falsified street address and telephone number information on their 'About' page – and it is doubtful that any of the 'papers' actually existed. Moreover, the 'news' coverage hosted on this large interconnected network of websites shared a curious fascination with a specific spin on international political coverage and a complete absence of local news to a degree that seemed extremely odd and out of place for a typical small, middle-American newsroom.

In this session, I will disclose the results of my investigation of the network and information breadcrumb trail that led from one of these sites to hundreds more, and then on to the ostensible owner of the network, whose family also runs a small private taxi company based in a suburb of London, out of his home. As the world grapples with massive disinformation campaigns waged by the intelligence agencies of hostile nations, we should not forget that such activities are not limited to the purview of the Bears or Pandas of the world, and that even relatively small operations such as this one can be abused to broadly manipulate public opinion and sow chaos on a confused and troubled planet.

INTRODUCTION

When I received an anonymous tip about a small, unknown online news site whose international coverage was being widely shared across social media, I didn't realize I'd spend the next year chasing a phantom down a rabbit hole. What looked, at first glance, like the website of what claimed to be a small-town newspaper based in Illinois, not only failed to support its self-proclaimed *bona fides* under the most rudimentary scrutiny, but raised far more questions than it answered.

The alleged newspaper calls itself 'Newburgh Gazette'. The masthead on its website (newburghgazette.com) carries the tagline 'Serving Newburgh, IL since 1928'. In many ways, the site resembles those unremarkable local news pages operated by small news organizations across the US, but it didn't take long for its facade to crumble and for the site to reveal its suspicious origins.

Figure 1: The masthead of 'Newburgh Gazette'.

WHO AND WHERE IS THE 'NEWBURGH GAZETTE'?

According to *Wikipedia*, Newburg (no 'h') Township, located in the far west of Illinois, has a population of fewer than 1,000 people. It is the only locale in the state of Illinois by that name (there is no town named 'Newburgh, IL'). Situated about 50 miles from the Mississippi River, which demarcates the political border between the states of Illinois and Missouri, Newburg Township is more than 250 miles from the city of Chicago and more than 100 road miles away from the nearest city, St. Louis, Missouri.

In the neighbouring state of Indiana, there is a town of more than 3,000 residents named Newburgh, lying along the Ohio river at the extreme southern edge of that state. Residents of Newburgh, IN can look south across the river and see Kentucky. But the US postal abbreviation for the state of Indiana is not what is printed on the 'Newburgh Gazette' masthead.

If the website's name and masthead raise questions, so too does the mailing address shown on the site's 'Contacts' page. 'If you have questions and wishes, please contact us at the following coordinates,' the site reads, using an improbably bizarre combination of words that no sober, English-speaking editor or publisher born on planet Earth would intentionally write.

The address listed on the page, '433 Cecil Street, Buffalo Grove, IL Illinois, 60089', references an actual town in the state of Illinois, but redundantly uses both the state's full name and its two-character postal abbreviation. But the bigger issue is that the Chicago suburb of Buffalo Grove, IL has no street within its town limits named Cecil Street (though you can find a Cecil St. more than 560 miles east, in the similarly named city of Buffalo, NY). Why a newspaper purportedly serving a community of fewer than 1,000 people would locate its offices 283 road miles away strains credulity.

Just a few years ago, a site like this might not have raised concerns. But as the world finds itself in an increasingly hostile environment, with various entities decrying the work of trustworthy and well-known media organizations and journalistic institutions as 'fake news,' it's essential to get to the bottom of this story.

WHO AND WHERE IS THE 'NEWBURGH GAZETTE'?

The goal of this paper (and presentation) is not to provide an analysis of whether the news published by a given site is real,

but to discuss how what the site says about itself appears to be a work of fiction, and to describe how this fiction, which violates basic, fundamental rules and practices designed to support journalistic integrity, inadvertently revealed the tip of a much larger iceberg of sites with an outsized reach on social media, and whose ownership and purpose is unclear.

When a news organization touts its 90-year history in its masthead, it typically has had a web presence for some time. 'Newburgh Gazette', as a web domain, dates back only to the early days of 2017.

The site's domain was registered using *WhoisGuard*, one of several so-called private WHOIS services that, for an additional fee, provides a proxy name and address that domain registrants can use to mask their identities. There's nothing nefarious about services like this: legitimate businesses use private WHOIS services to reduce spam email and nuisance postal mail sent to the domain's registered address. The use of a private WHOIS by a registrant does make it more difficult to track the registrant's activity.

For the first two months after the domain was registered, *Domaintools* reports that it was hosted at the IP address 149.56.190.10. Interestingly, that IP address co-hosted more than 350 other domains, most of which shared certain characteristics with 'Newburgh Gazette'.

Virtually all the domain names hosted on that IP were composed of a geographic location or a common news category ('financial', 'business', 'health', etc.), followed by one or more words typically associated with the names commonly used by news organizations, such as 'weekly', 'observe', 'daily', 'tribune', 'press', 'reporter', 'journal', 'chronicle', and many others. These domain names also followed the language conventions of the geographic region from which they purported to originate, such as an Italian city name preceded by 'corriere' ('courier') or a Spanish region followed with 'noticias' ('news') or 'diaria' ('daily').

Domain names aside, many of the sites behind those domain names also share what appears to be a similar content management system, or CMS, with only cosmetic details distinguishing one site from another. And nearly all of these sites feature a contact page with a fictional postal address, on a street that doesn't exist in the town the 'news site' purports to serve or where it claims to be based.

Also notable is the conspicuous absence on these sites of local news coverage by bylined reporters targeting their specific geographic area. In some cases, the CMS serving content for an ostensibly American town contained user-interface elements in the Russian language, such as the word 'следующая' (pronounced 'sleduyushchaya', it means 'next') adjacent to the pagination indicators.

WHAT'S THE ENDGAME?

Not all of the domains had been registered using private WHOIS services. The WHOIS records for many of the domains tied back to real email addresses, and searching for other domains registered using those same email addresses led to the discovery of additional domains which featured the same characteristics, naming conventions, and contact information that appeared to be misleading or simply false.

Many of these domains were hosted on different IP addresses, and performing a reverse DNS lookup of these other IP addresses revealed yet more domain names that fit these curiously specific characteristics *and* which also seemed to lack any kind of real connection to the geographic region of the world they purport to serve.

Each new batch of suspiciously crafted domains led to yet more unique registrant details that led to even more domains, more IP co-hosting arrangements, and another recursive level of searches revealing an expanding collection of several thousand domains.

And yet, with all that, it's still not clear what the endgame is for the people registering and running these sites. With a network that runs in the hundreds, I still find social media profiles posting links to some of these sites every day, and there remain many unanswered questions: is this a disinformation campaign, or just a way for a site to build up a domain's non-negative reputation so it can be used in for malicious purposes later? Is it a callously cynical way of earning advertising revenue, or a buildup to a future attack in which the world is flooded with stories of questionable veracity, or in which one or more of these sites is used to host or control malware? Where is the money coming from to pay for all the registrations (including private WHOIS services), hosting, development, and promotion on social media?

Performing this kind of investigation doesn't require special tools, but it is about to become much harder. The new GDPR rules which took effect this year have already severely impacted domain registration WHOIS records. GDPR may, perversely, make it far more difficult to track not only sham domain registrations but also domains registered by other threat actors involved in phishing or malware campaigns.

What is clear is that fostering a general distrust of the honesty and integrity of news organizations has been a key element in the authoritarian, dictatorial playbook for a long time. The mere existence of a huge network of 'news' sites with no apparent legitimate management or staff, poses a threat to the public trust in news organizations in general, even if those sites are just reposting wire stories. Such a campaign designed to engender distrust in truth is extremely dangerous. Real journalists stand behind their work proudly, and all of us who care about a world grounded in objective truth should be concerned.